3 Device Management Commands

3.1 Device Status Checking Commands

3.1.1 Command Support

Commands provided in this section and all the parameters in the commands are supported by all switch models (except the S5731-L and S5731S-L), unless otherwise specified. For details, see specific commands.

3.1.2 check hardware health

Function

The **check hardware health** command displays health check information about the device.

Format

check hardware health [**slot** *slot-id*]

Parameters

Parameter	Description	Value
slot *slot-id*	Specifies a slot ID.	The value must be set according to the device configuration.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Before upgrading a device's software package, run this command to check the health check information about the device. Ensure that all check items are normal before the upgrade to prevent a device upgrade failure.

Example

Display health check information about the device.

```
<HUAWEI> check hardware health
------------------------------------------------------------------------
Hardware health information of slot 0
------------------------------------------------------------------------
Board ID                          : Normal
PCB version                       : Normal
Bom ID                            : Normal
Flash read state                  : Normal
NAND bad block check result       : Normal
Remaining space                   : Normal
NOR flash erase state             : Normal
CPLD erase state                  : Normal
CPLD self-check                   : Normal
DDR single-bit ECC error count    : 0
Cache single-bit ECC error count  : 0
Power PWR1(CML)                   : Normal
Power PWR1(TEMPERATURE)           : Normal
Power PWR1(VIN_UV)                : Normal
Power PWR1(IOUT_OC)               : Normal
Power PWR1(VOUT_OV)               : Normal
```



```
Power PWR1(OFF)                    : Normal
Power PWR1(BUSY)                   : Normal
Power PWR1(UNKNOWN)                    : Normal
Power PWR1(OTHER)                  : Normal
Power PWR1(FANS)                   : Normal
Power PWR1(POWER_GOOD)                 : Normal
Power PWR1(MFR)                    : Normal
Power PWR1(INPUT)                  : Normal
Power PWR1(IOUT/POUT)                  : Normal
Power PWR1(VOUT)                   : Normal
Board corrosion                  : No
```

Table 3-1 Description of the **check hardware health** command output and troubleshooting methods for abnormal devices

Item	Description	Troubleshooting methods for abnormal devices
Hardware health information of slot x	Health check information about the device.	-
Board ID	Status of the Printed circuit board (PCB) check. ● Normal: The status is normal. ● Abnormal: The status is abnormal.	If the device hardware is damaged, collect alarm and configuration information and contact technical support personnel.
PCB version	Status of the PCB version check. ● Normal: The status is normal. ● Abnormal: The status is abnormal.	If the device hardware is damaged, collect alarm and configuration information and contact technical support personnel.
Bom ID	Status of the Bom ID check. ● Normal: The status is normal. ● Abnormal: The status is abnormal. **NOTE** This field is not available for the S6720-EI and S6720S-EI.	If the device hardware is damaged, collect alarm and configuration information and contact technical support personnel.
Flash read state	Status of the flash read/write check. ● Normal: The status is normal. ● Abnormal: The status is abnormal.	If the device hardware is damaged, collect alarm and configuration information and contact technical support personnel.

Item	Description	Troubleshooting methods for abnormal devices
NAND bad block check result	Status of the bad block check of the NAND flash. ● Normal: The status is normal. ● Abnormal: The status is abnormal. **NOTE** This field is not available for the S6735-S.	If the device hardware is damaged, collect alarm and configuration information and contact technical support personnel.
Remaining space	Status of the flash remaining space check. ● Normal: The status is normal. ● Abnormal: The status is abnormal.	1. Enter the device directory. a. If the switch has a hard disk, run the **cd hda1:** command to enter the hard disk directory. b. If the switch has a flash rather than a hard disk, run the **cd flash:** command to enter the flash directory. 2. Run the **dir** command to check the size of the remaining storage space. If the remaining space is not enough, run the **delete** command to delete unneeded files. 3. Run the **dir** command to check whether the size of the remaining storage space is greater than the size of the PDF file. ● If so, go to Step 5. ● If not, go to Step 4. 4. Collect log information and configuration information, and then contact technical support personnel. 5. End.

Item	Description	Troubleshooting methods for abnormal devices
NOR flash erase state	Status of the erase and write check of the NOR flash. ● Normal: The status is normal. ● Abnormal: The status is abnormal. **NOTE** This field is not available for the S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5735-S, S500, S5735S-S, and S5735-S-I.	If the device hardware is damaged, collect alarm and configuration information and contact technical support personnel.
CPLD erase state	Status of the CPLD erase and write check. ● Normal: The status is normal. ● Abnormal: The status is abnormal. **NOTE** This field is not available for the S6720-EI and S6720S-EI.	If the device hardware is damaged, collect alarm and configuration information and contact technical support personnel.
CPLD self-check	Status of the CPLD self-check. ● Normal: The status is normal. ● Abnormal: The status is abnormal.	If the device hardware is damaged, collect alarm and configuration information and contact technical support personnel.
DDR single-bit ECC error count	DDR single-bit ECC error frequency.	If the device hardware is damaged, collect alarm and configuration information and contact technical support personnel.
Cache single-bit ECC error count	Cache single-bit ECC error frequency.	If the device hardware is damaged, collect alarm and configuration information and contact technical support personnel.

Item	Description	Troubleshooting methods for abnormal devices
Power PWR1(CML)	Whether the communication of the power module is normal: ● Normal: The status is normal. ● Abnormal: The status is abnormal. If this parameter is not supported, a hyphen (-) is displayed.	If the power supply is faulty, collect alarm and configuration information, and contact technical support personnel.
Power PWR1(TEMPERATURE)	Whether the temperature of the power module is abnormal: ● Normal: The status is normal. ● Abnormal: The status is abnormal. If this parameter is not supported, a hyphen (-) is displayed.	If the power supply is faulty, collect alarm and configuration information, and contact technical support personnel.
Power PWR1(VIN_UV)	Whether the input voltage of the power module is below the lower threshold: ● Normal: The status is normal. ● Abnormal: The status is abnormal. If this parameter is not supported, a hyphen (-) is displayed.	If the power supply is faulty, collect alarm and configuration information, and contact technical support personnel.
Power PWR1(IOUT_OC)	Whether the power module has output overcurrent: ● Normal: The status is normal. ● Abnormal: The status is abnormal. If this parameter is not supported, a hyphen (-) is displayed.	If the power supply is faulty, collect alarm and configuration information, and contact technical support personnel.

Item	Description	Troubleshooting methods for abnormal devices
Power PWR1(VOUT_OV)	Whether the output voltage of the power module exceeds the upper threshold: ● Normal: The status is normal. ● Abnormal: The status is abnormal. If this parameter is not supported, a hyphen (-) is displayed.	If the power supply is faulty, collect alarm and configuration information, and contact technical support personnel.
Power PWR1(OFF)	Whether the power module is powered off: ● Normal: The status is normal. ● Abnormal: The status is abnormal. If this parameter is not supported, a hyphen (-) is displayed.	If the power supply is faulty, collect alarm and configuration information, and contact technical support personnel.
Power PWR1(BUSY)	Whether the power module is busy and does not respond: ● Normal: The status is normal. ● Abnormal: The status is abnormal. If this parameter is not supported, a hyphen (-) is displayed.	If the power supply is faulty, collect alarm and configuration information, and contact technical support personnel.
Power PWR1(UNKNOWN)	Whether the power module status is unknown: ● Normal: The status is normal. ● Abnormal: The status is abnormal. If this parameter is not supported, a hyphen (-) is displayed.	If the power supply is faulty, collect alarm and configuration information, and contact technical support personnel.

Item	Description	Troubleshooting methods for abnormal devices
Power PWR1(OTHER)	Whether the power module is faulty due to any other reasons: ● Normal: The status is normal. ● Abnormal: The status is abnormal. If this parameter is not supported, a hyphen (-) is displayed.	If the power supply is faulty, collect alarm and configuration information, and contact technical support personnel.
Power PWR1(FANS)	Whether the fan of the power module is faulty: ● Normal: The status is normal. ● Abnormal: The status is abnormal. If this parameter is not supported, a hyphen (-) is displayed.	If the power supply is faulty, collect alarm and configuration information, and contact technical support personnel.
Power PWR1(POWER_GOOD)	Whether the output of the power module is normal: ● Normal: The status is normal. ● Abnormal: The status is abnormal. If this parameter is not supported, a hyphen (-) is displayed.	If the power supply is faulty, collect alarm and configuration information, and contact technical support personnel.
Power PWR1(MFR)	Whether a user-defined fault occurs on the power module: ● Normal: The status is normal. ● Abnormal: The status is abnormal. If this parameter is not supported, a hyphen (-) is displayed.	If the power supply is faulty, collect alarm and configuration information, and contact technical support personnel.

Item	Description	Troubleshooting methods for abnormal devices
Power PWR1(INPUT)	Whether the input of the power module is normal: ● Normal: The status is normal. ● Abnormal: The status is abnormal. If this parameter is not supported, a hyphen (-) is displayed.	If the power supply is faulty, collect alarm and configuration information, and contact technical support personnel.
Power PWR1(IOUT/POUT)	Whether the output current or power of the power supply is faulty: ● Normal: The status is normal. ● Abnormal: The status is abnormal. If this parameter is not supported, a hyphen (-) is displayed.	If the power supply is faulty, collect alarm and configuration information, and contact technical support personnel.
Power PWR1(VOUT)	Whether the output voltage of the power module is normal: ● Normal: The status is normal. ● Abnormal: The status is abnormal. If this parameter is not supported, a hyphen (-) is displayed.	If the power supply is faulty, collect alarm and configuration information, and contact technical support personnel.
Board corrosion	Whether the device is corroded. ● Yes: Corrosion occurs. ● No: Corrosion does not occur. If this parameter is not supported, a hyphen (-) is displayed.	If the device hardware is damaged, collect alarm and configuration information and contact technical support personnel.

3.1.3 display built-in power

Function

The **display built-in power** command displays the built-in power supply status of switches with extended temperature range.

NOTE

Only S5720I-28X-SI-AC and S5720I-28X-PWH-SI-AC support this command.

Format

display built-in power

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display built-in power** command to check whether the built-in power supply status of switches with extended temperature range is normal.

If some member switches do not support this command, the system displays a prompt message.

Example

Display the built-in power supply status of switches with extended temperature range.

```
<HUAWEI> display built-in power
-------------------------------------------------------------
 Slot    PowerID     State
-------------------------------------------------------------
 1       PWR1        Normal
         PWR2        Abnormal
 2       PWR1        Normal
         PWR2        Abnormal
-------------------------------------------------------------
Info: Slot 0 does not support the command.
```


Table 3-2 Description of the **display built-in power** command output

Item	Description
Slot	Slot ID.
PowerID	Power supply ID.
State	Power supply status: • Abnormal • Normal

3.1.4 display battery information

Function

The **display battery information** command displays lithium battery information.

NOTE

Only the S5735-S8P2X-IA200H1 supports this command.

Format

display battery information

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run this command to view lithium battery information.

Example

Display lithium battery information.

```
<HUAWEI> display battery information
Info: This operation may take a few seconds. Please wait for a
moment....
-------------------------------------------------------------
 Lithium battery information of integrated power
-------------------------------------------------------------
Battery group information
```



```
  Battery status                          : Float charging
  Battery voltage(V)                      : 54.26
  Battery current(A)                      : 0.00
  Total battery capacity(Ah)                 : 200
  Available battery capacity(%)              : 100.00
  Battery temperature(degC)                  : 29.47
  Battery run time(h)                     : 256.00
  Number of connected ESMUs                     : 2

Battery 1 information
  Battery voltage(V)                      : 54.28
  Battery current(A)                      : 0.00
  Device address                          : 1
  Battery status                          : Charging
  Battery SOH(%)                             : 100.00
  Battery capacity(Ah)                       : 100
  Electrochemical cell package voltage(V)           : 50.99
  Maximum allowable current limiting coefficient(C10) :
0.30
  Electric core(1-16) voltage(V)                 :
     core[1-4]  :3.40 3.40 3.40 3.40
     core[5-8]  :3.40 3.40 3.40 3.40
     core[9-12] :3.38 3.40 3.40 3.40
     core[13-16]:3.40 3.40 3.40 3.40
  Electric core(1-16) degree(degC)               :
     core[1-4]  :29.00 29.00 29.00 29.00
     core[5-8]  :29.00 29.00 29.00 29.00
     core[9-12] :29.00 29.00 29.00 30.00
     core[13-16]:30.00 30.00 30.00 30.00
  SoftWare version                        : V116

Battery 2 information
  Battery voltage(V)                      : 54.25
  Battery current(A)                      : 0.00
  Device address                          : 2
  Battery status                          : Charging
  Battery SOH(%)                             : 100.00
  Battery capacity(Ah)                       : 100
  Electrochemical cell package voltage(V)           : 51.28
  Maximum allowable current limiting coefficient(C10) :
0.30
  Electric core(1-16) voltage(V)                 :
     core[1-4]  :3.42 3.42 3.41 3.42
     core[5-8]  :3.42 3.42 3.42 3.42
     core[9-12] :3.42 3.42 3.42 3.42
     core[13-16]:3.42 3.42 3.42 3.42
  Electric core(1-16) degree(degC)               :
     core[1-4]  :31.00 31.00 31.00 29.00
     core[5-8]  :29.00 29.00 29.00 29.00
     core[9-12] :29.00 29.00 29.00 30.00
     core[13-16]:30.00 30.00 30.00 30.00
  SoftWare version                        : V116
```

Table 3-3 Description of the **display battery information** command output

Item	Description
Lithium battery information of integrated power	Information about the integrated lithium battery system.
Battery group information	Battery group information.
Battery status	Battery status.
Battery voltage(V)	Battery voltage, in volts (V).

Item	Description
Battery current(A)	Battery current, in amperes (A).
Total battery capacity(Ah)	Total battery capacity, in Ah.
Available battery capacity(%)	Remaining battery capacity, in percentage.
Battery temperature(degC)	Battery temperature, in ºC.
Battery run time(h)	Battery backup time, in hours.
Number of connected ESMUs	Number of connected ESMUs.
Device address	Device address.
Battery SOH(%)	Battery string SOH, in percentage.
Battery capacity(Ah)	Battery capacity, in Ah.
Electrochemical cell package voltage(V)	Electrochemical cell package voltage, in volts (V).
Maximum allowable current limiting coefficient(C10)	Maximum allowable current limiting coefficient, in C10.
Electric core(1-16) voltage(V)	Voltage of electrochemical cells 1 to 16, in Volt (V).
Electric core(1-16) degree(degC)	Temperature of electrochemical cells 1 to 16, in degrees Celsius.
SoftWare version	Software version. The value is in ASCII format.

3.1.5 display chip-temperature

Function

The **display chip-temperature** command displays the temperature of chip.

Format

display chip-temperature { **all** | **slot** *slot-id* }

Parameters

Parameter	Description	Value
all	Displays the temperature of chip of all slots.	-

Parameter	Description	Value
slot *slot-id*	Displays the temperature of chip of a specified slot.	The value must be set according to the device configuration.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

A proper temperature range is the prerequisite for stable running of switches. If the temperature of chip is too high or too low, the hardware may be damaged.

Example

Display the temperature of chips of all slots. (The actual output information may differ from the following information.)

```
<HUAWEI> display chip-temperature all
-------------------------------------------------
 Slot       Chip       Status       Current(C)
-------------------------------------------------
 0          LSW        Normal       46
            CPU        Normal       60
            PHY        Normal       52
<HUAWEI> display chip-temperature all
-------------------------------------------------
 Slot       Chip       Status       Current(C)
-------------------------------------------------
 0          LSW1       Normal       46
            LSW2       Normal       50
            CPU        Normal       60
            PHY        Normal       52
```

Table 3-4 Description of the **display chip-temperature** command output

Item	Description
Slot	Slot ID.
Chip	Type of the chip. • CPU: indicates a CPU chip. • LSW: indicates a forwarding chip. If there are multiple chips, they are displayed as LSW1, LSW2, ..., and so on. • PHY: indicates a PHY chip on the backplane. • PHY1: indicates a PHY chip on a subcard.

Item	Description
Status	Temperature status. • Normal: The temperature is normal. • Abnormal: The temperature is abnormal or all interfaces on the device are down.
Current(C)	Current temperature of the chip, in the centigrade scale (°C). The temperature value is displayed as an integer, so there may be a maximum of 1°C error between the displayed value and actual temperature.

3.1.6 display compatible-information

Function

The **display compatible-information** command displays compatible information of a device.

Format

display compatible-information

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Generally, device versions have matching NMS software. The NMS software needs to apply to all the devices supported by matching versions. Otherwise, the NMS cannot manage devices. If the NMS version is an earlier version but the current device is running a later version that does not match the current NMS version, the NMS cannot manage the current device.

To decouple the NMS version and device version, a compatible device model developed based on an earlier version is defined for each device model. If the NMS cannot manage a device because of version mismatch, obtain information about the device compatible with the current device. The NMS can then use the obtained information to manage the current device.

For example:

S5720-SI_R10 is a device model newly available in V200R010. The NMS software version that matches the device software version is V200R010.

S5720-SI_R8 is a device model newly available in V200R008. The NMS software version that matches the device software version is V200R008.

When you use the NMS of V200R008 to manage S5720-SI_R10, the device cannot be managed because of version mismatch. The NMS then obtains compatibility information about S5720-SI_R10 and learns that it is compatible with S5720-SI_R8. Subsequently, the NMS uses information about S5720-SI_R8 to manage the current device.

If the device does not have a compatible version, the system will display a message, indicating that no compatible information exists after the **display compatible-information** command is executed.

Compatible information of stacked devices can also be displayed.

Example

Display compatible information of a device.

```
<HUAWEI> display compatible-information
SlotID              : 0
Compatible SysOids  : 1.3.6.1.4.1.2011.2.23.331
Compatible Version  : V200R008C00
ProductName         : S5720-52X-SI-AC
```

Table 3-5 Description of the display compatible-information command output

Item	Description
SlotID	The slot ID.
Compatible SysOids	System OID of an old device version.
Compatible Version	Old device version compatible with the current device version.
ProductName	Product name of new devices.

3.1.7 display cpu-usage

Function

The **display cpu-usage** command displays CPU usage statistics.

Format

display cpu-usage [**slave** | **slot** *slot-id*] [**vcpu** *vcpu-index*]

NOTE

The **slave** parameter is not supported if the switch does not support the stacking function or does not have the stacking function enabled.

Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S support the **vcpu** *vcpu-index* parameter.

Parameters

Parameter	Description	Value
slave	Displays the CPU usage of slave devices in a stack. This parameter is valid only in a stack system.	-
slot *slot-id*	Specifies a slot ID.	The value depends on the device configuration.
vcpu *vcpu-index*	Displays the usage of a specified virtual CPU.	Specify the *vcpu-index* parameter based on the hardware configuration.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

CPU usage is an important indicator to evaluate device performance. A high CPU usage will cause service faults, for example, BGP route flapping, frequent VRRP active/standby switchover, and even failed device login. You can use the **display cpu-usage** command to view CPU usage to check whether devices are working properly.

When the CPU usage is high, rectify the fault according to "Troubleshooting: High CPU" in ***Huawei S Series Campus Switches Troubleshooting Guide***.

Example

Display the CPU usage on the device.

```
<HUAWEI> display cpu-usage
CPU Usage Stat. Cycle: 60 (Second)
CPU Usage            : 20% Max: 99%
CPU Usage Stat. Time : 2019-10-23  10:04:45
CPU utilization for five seconds: 5%: one minute: 5%: five minutes: 5%
Max CPU Usage Stat. Time : 2019-10-21 16:14:00.

TaskName            CPU  Runtime(CPU Tick High/Tick Low)  Task Explanation
VIDL                80%        0/e3a150c0       DOPRA IDLE
```



```
OS              10%       0/ bfb0440      Operation System
1AGAGT           6%       0/      0      1AGAGT
AAA              2%       0/   1d4a      AAA  Authen Account Authorize
ACL              1%       0/  13362      ACL Access Control List
ADPT             1%       0/      0      ADPT Adapter
AGNT             0%       0/      0      AGNTSNMP agent task
AGT6             0%       0/      0      AGT6SNMP AGT6 task
ALM              0%       0/      0      ALM  Alarm Management
ALS              0%       0/ 527a3e      ALS  Loss of Signal
AM               0%       0/  232cf      AM   Address Management
APP              0%       0/      0      APP
ARP              0%       0/  36582      ARP
ASFI             0%       0/      0      ASFI
ASFM             0%       0/      0      ASFM
BATT             0%       0/      0      BATT Main Task
BFD              0%       0/ 100f36      BFD Bidirection Forwarding
                                         Detect
BFDA             0%       0/      0      BFDA BFD Adapter
BFDS             0%       0/   5825      BFDS
BOX              0%       0/ 1d0097      BOX Output
BPDU             0%       0/   1806      BPDU Adapter
BTRC             0%       0/     60e     BTRC
CDM              0%       0/   9b95      CDM
CFM              0%       0/   6f68      CFM Configuration file
                                         management
CLKI             0%       0/      0      CLKI
DEFD             0%       0/  22ebd      DEFD CPU Defend
DELM             0%       0/   355c      DELMAC FOR STP
DEV              0%       0/      0      DEV  Device Management
DHCP             0%       0/  12188      DHCP Dynamic Host Config
                                         Protocol
DLDP             0%       0/   dc0d      DLDP Protocol
EAP              0%       0/   38a9      EAP  Extensible Authen
                                         Protocol
EFMT             0%       0/  11c70      EFMTEST 802.3AH Test
EOAM             0%       0/   ea8f      EOAM1AG
ESAP             0%       0/      0      ESAP eSap Adapter
ETHA             0%       0/      0      ETHA
EZOP             0%       0/  506f4      EZOP EasyOperation
                                         application
EZPP             0%       0/ 1e41f8      EZPP EasyOperation packet
FCAT             0%       0/   6479      FCAT Catch Packets for
                                         debugging
FECD             0%       0/  11d8e      FECD Mod Manage Task
FIB              0%       0/   523b      FIB Forward Information Base
FIB6             0%       0/      0      FIB6IPv6 FIB
FLOW             0%       0/   ce76      FLOW SFLOW
FMAT             0%       0/   7f23      FMATFault Manage task
FTS              0%       0/ 125f35      FTS
GEM              0%       0/      0      GEM task
GEMR             0%       0/      0      GEMRun task
GRSA             0%       0/      0      GRSA
GVRP             0%       0/      0      GVRP Protocol
HACK             0%       0/      0      HACKtask for HA ACK
HOTT             0%       0/      0      HOTT
HS2M             0%       0/      0      HS2MHigh available task
HTTP             0%       0/  5d420      HTTP
IFLP             0%       0/   8611      IFLP
IFNT             0%       0/      0      IFNTIfnet task
IFPD             0%       0/ 2177f21     IFPD Ifnet Product Adapter
INFO             0%       0/  70409      INFOInformation center
IP               0%       0/   cb13      IP
IPCK             0%       0/      0      IPCKIPC task for ack message
IPCQ             0%       0/ 3c6ffd      IPCQIPC task for single queue
IPCR             0%       0/      0      IPCR IPC Receiver
JOB              0%       0/      0      JOB Schedule
L2               0%       0/  2a6b5      L2
L2IF             0%       0/  b7fbc      L2IF
L2_E             0%       0/  10088      L2_EOAM_Y1731
```

```
L2_P                0%        0/   58a50       L2_PR
L2_R                0%        0/  169c0c       L2_RING
L2_T                0%        0/    1724       L2_TRUNK
L3I4                0%        0/       0       L3I4 LPU Manage IPv4 unicast
                                               FDB
L3IO                0%        0/       0       L3IO LPU Process urpf, vrrp
                                               etc.
L3M4                0%        0/       0       L3M4 MPU Manage IPv4 unicast
                                               FDB
L3MB                0%        0/    4319       L3MB MPU Process urpf, vrrp
                                               etc.
LAGAGT              0%        0/   107dd       LAGAGT
LBDT                0%        0/  1bf810       LBDT Loopback Detect Mpu
LINK                0%        0/       0       LINK
LLDP                0%        0/   70921       LLDP Protocol
LNP                 0%        0/       0       LNP task
MAC                 0%        0/    564f       MAC Media Access Control
MACL                0%        0/   21954       MACL Access Control List
MAD                 0%        0/    dae7       MAD Task
MADP                0%        0/       0       MADP MAD proxy Task
MCSW                0%        0/   12624       MCSW Mulitcast Switch Adapter
MERX                0%        0/    8a774      MERX Meth Receive
METH                0%        0/    f0699      METH Metropolitan Ethernet
MFF                 0%        0/    b308       MFF MAC Forced Forwarding
MFIB                0%        0/     beb       MFIBMulticast forward info
MIRR                0%        0/       0       MIRR Capture Packet
MSYN                0%        0/    7245a      MSYN Mac Synchronization
Mirr                0%        0/    4107       Mirror
NDIO                0%        0/       0       NDIO LPU Manage IPv6 unicast
                                               FDB
NDMB                0%        0/       0       NDMB MPU Manage IPv6 unicast
                                               FDB
NFPT                0%        0/   d2dec       NFPTNFP timer task
NTPT                0%        0/       0       NTPT task
OAM1                0%        0/       0       OAM1 EOAM Adapter
PAT                 0%        0/       0       PAT
PNGI                0%        0/       0       PNGI
PNGM                0%        0/       0       PNGM MPU Process icmp reply
                                               fast
POE+                0%        0/       0       POE+ PPP Over Ethernet Plus
PPI                 0%        0/   58e46       PPI Product Process Interface
PTAL                0%        0/       0       PTAL Portal
RDS                 0%        0/       0       RDS  Radius
RMON                0%        0/   11240       RMONRemote monitoring
ROUT                0%        0/  6a6343       ROUTRoute task
RPCQ                0%        0/   22254       RPCQRemote procedure call
RTMR                0%        0/   ed870       RTMR
SAM                 0%        0/    2e2d       SAM  Service Agent Module
SAPP                0%        0/    758e       SAPP
SECE                0%        0/  2e6e82       SECE Security
SLAG                0%        0/       0       SLAG
SMAG                0%        0/       0       SMAG Smart Link Agent
SMLK                0%        0/   71827       SMLK Smart Link Protocol
SNPG                0%        0/   d97b7       SNPG Multicast Snooping
SOCK                0%        0/   4bdda       SOCKPacket schedule and
                                               process
SPM                 0%        0/   6a1ce       SPM  Smart Power Management
SRM                 0%        0/  6bb9b8       SRM  System Resource
                                               Management
SRMI                0%        0/       0       SRMI External Interrupt
SRMT                0%        0/  fe2a46       SRMT System Resource Manage
                                               Timer
STFW                0%        0/       0       STFW Super task forward
STND                0%        0/       0       STNDStandby task
STP                 0%        0/  79e590       STP
STRA                0%        0/   1c767       STRA Source Trail
TACH                0%        0/   9817e       TACHWTACACS
TARP                0%        0/       0       TARPING
TICK                0%        0/  7dbef6
```

```
TM                0%        0/       0       TM   Transmission Management
TNQA              0%        0/   83134       TNQAC
TRAP              0%        0/    14d7       TRAPSNMP trap task
TTNQ              0%        0/       0       TTNQAS
TUNL              0%        0/    5c17       TUNL
UCM               0%        0/    3e46       UCM  User Control Management
UTSK              0%        0/       0       UTSK
VCMP              0%        0/       0       VCMP task
VFS               0%        0/       0       VFS Virtual file system
VFSD              0%        0/       0       VFSDVFS flash task for delete
                                               file block
VMON              0%        0/    78d5       VMONSystem monitor
VMSH              0%        0/       0       VMSH
VP                0%        0/    5966       VP  Virtual path task
VPR               0%        0/       0       VPR  VP Receiver
VRPT              0%        0/    39fd       VRPT
VRRP              0%        0/  152ced       VRRP
VT                0%        0/       0       VT   Virtual Transfer
VT0               0%        0/  4909c5       VT0 Line user's task
VT1               0%        0/       0       VT1 Line user's task
VTYD              0%        0/    b3282      VTYDVirtual terminal
WEB               0%        0/    1295       WEB  Web
XMON              0%        0/       0       XMONVxworks system monitor
XQOS              0%        0/   12999       XQOS Quality of service
_EXC              0%        0/       0       Exception Agent Task
_TIL              0%        0/       0       Infinite loop event task
bcmCNTR.0         0%        0/  61077b       tS10
bcmCNTR.1         0%        0/  605691       tS11
bcmDPC            0%        0/   25d89       tS09
bcmL2X.0          0%        0/  b069d6       tS0c
bcmL2X.1          0%        0/  b2c5f2       tS0f
bcmRX             0%        0/  1df879       bcmRX
bcmTX             0%        0/    16f2       tS0a
frag_add          0%        0/  45ecce       tS0d
frag_del          0%        0/       0       tS0e
linkscan          0%        0/  ecce16       tS12
root              0%        0/       0       tS03
soft_learn        0%        0/    7812a      tS0b
tExcTask          0%        0/       0       tS00
tLogTask          0%        0/       0       tS01
tShell            0%        0/       0       tS02
```

Table 3-6 Description of the **display cpu-usage** command output

Item	Description
CPU Usage Stat. Cycle	Interval for collecting CPU usage statistics. The interval is 60 seconds and cannot be configured.
CPU Usage	Average CPU usage in the last 10 seconds.
Max	Highest CPU usage in history.
CPU Usage Stat. Time	Time when the latest CPU usage statistics are collected.
CPU utilization for five seconds	CPU usage in five seconds.
one minute	CPU usage in one minute.
five minutes	CPU usage in five minutes.
Max CPU Usage Stat. Time	Time when the highest CPU usage statistics are collected.

Item	Description
TaskName	Task that is being executed. For details about all the tasks and functions of the device, see "Troubleshooting: High CPU Usage - How to Locate the High CPU Usage Problem - Determining Fault Causes According to CPU Usages of Tasks (Fixed Switches)" and "Troubleshooting: High CPU Usage - Appendix - CPU-related Tasks and Functions for Fixed Switches" in ***Huawei S Series Campus Switches Troubleshooting Guide***.
CPU	Real-time CPU usage of each task.
Runtime(CPU Tick High/Tick Low)	System running time calculated based on CPU tick.
Task Explanation	Explanation to the task.

3.1.8 display cpu-usage configuration

Function

The **display cpu-usage configuration** command displays CPU usage configuration.

Format

display cpu-usage configuration [**slave** | **slot** *slot-id*]

NOTE

The **slave** parameter is not supported if the switch does not support the stacking function or does not have the stacking function enabled.

Parameters

Parameter	Description	Value
slave	Displays CPU usage configuration of standby switches in a stack.	-
slot *slot-id*	Displays device CPU usage configuration of a specified slot ID.	The value depends on the device configuration.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

This command displays the alarm threshold and recovery threshold.

- When CPU usage reaches the alarm threshold, the system generates a CPU usage alarm.
- When CPU usage falls within the recovery threshold, the system generates a clear alarm.

Example

Display CPU usage configuration.

```
<HUAWEI> display cpu-usage configuration
The CPU usage monitor is turned on.
The current monitor cycle is 60 seconds.
The current monitor warning threshold is 95%.
The current monitor restore threshold is 80%.
```

Table 3-7 Description of the **display cpu-usage configuration** command output

Item	Description
The CPU usage monitor	Whether the CPU usage monitoring function is enabled or disabled. To enable the CPU usage monitoring function, run the **cpu-usage monitor** command.
The current monitor cycle	CPU usage monitoring period, which cannot be configured.
The current monitor warning threshold	Alarm threshold. To set the CPU usage alarm threshold, run the **cpu-usage threshold** *threshold-value* [**restore** *restore-threshold-value*] [**slot** *slot-id*] command.
The current monitor restore threshold	Alarm recovery threshold. To set the CPU usage alarm recovery threshold, run the **cpu-usage threshold** *threshold-value* [**restore** *restore-threshold-value*] [**slot** *slot-id*] command.

3.1.9 display cpu-usage history

Function

The **display cpu-usage history** command displays CPU usage statistics within a period.

Format

display cpu-usage history [**1hour** | **24hour** | **72hour**] [**slave** | **slot** *slot-id*] [**vcpu** *vcpu-index*]

NOTE

The **slave** parameter is not supported if the switch does not support the stacking function or does not have the stacking function enabled.

Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S support the **vcpu** *vcpu-index* parameter.

Parameters

Parameter	Description	Value
1hour	Displays CPU usage statistics within the last one hour.	-
24hour	Displays CPU usage statistics within the last 24 hours.	-
72hour	Displays CPU usage statistics within the last 72 hours.	-
slave	Displays the CPU usage statistics of slave devices in a stack. This parameter is valid only in a stack system.	-
slot *slot-id*	Displays the CPU usage statistics of a specified slot ID.	The value varies with the device configuration.
vcpu *vcpu-index*	Displays the CPU usage statistics of a specified virtual CPU.	Specify the *vcpu-index* parameter based on the hardware configuration.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

The system collects CPU usage statistics at a specified interval (usually 60s) and saves them in the historical record table. To check CPU usage statistics within a period, run the **display cpu-usage history** command, and the command output helps you determine whether the CPU is working properly.

In the **display cpu-usage history** command output, the x-coordinate indicates the specified period, and the y-coordinate indicates the CPU usage.

Precautions

If CPU usage is constantly higher than the upper alarm threshold (95% by default) before the feature is deployed on a large scale, check the device to troubleshoot the fault.

Example

Display CPU usage statistics within the last one hour.

```
<HUAWEI> display cpu-usage history 1hour
100%|
 95%|
 90%|
 85%|
 80%|
 75%|
 70%|
 65%|
 60%|
 55%|
 50%|
 45%|
 40%|
 35%|               H
 30%|               H
 25%|               H
 20%|               H
 15%|               H
 10%|               H
  5%|HHHHHHHHHHHHHHHHHHHHHHHHHHHHHHHHHHHHHHHHHHHHHHHHHHHHHHHHHHHHHHHHHHHHHHH
    ---------+---------+---------+---------+---------+---------+>
             10        20        30        40        50        60
             System cpu-usage last 60 minutes(Per Min)
```

Display CPU usage statistics within the last 24 hours.

```
<HUAWEI> display cpu-usage history 24hour

100%|
 95%|
 90%|
 85%|
 80%|
 75%|*
 70%|*
 65%|*
 60%|*
```



```
55%|*
50%|*
45%|*
40%|*
35%|*                    **
30%|*                    **
25%|*                    **
20%|*                    **
15%|*                    **
10%|H                     **
 5%|HHHHHHHHHHHHHHHHHHHHHHHHHHHHHHHH
   ---------+---------+---------+---------+-------->
            10        20        30        40
     System cpu-usage last 24 hours(Per Halfhour)
    * = maximum cpu-usage    H = average cpu-usage
```

Display CPU usage statistics within the last 72 hours.

```
<HUAWEI> display cpu-usage history 72hour

100%|
 95%|
 90%|
 85%|
 80%|
 75%|*
 70%|*
 65%|*
 60%|*
 55%|*
 50%|*
 45%|*
 40%|*
 35%|*          *
 30%|*          *
 25%|*          *
 20%|*          *
 15%|*          *
 10%|*          *
  5%|HHHHHHHHHHHHHHH
   ---------+---------+---------+---------+---------+---------+---------+-->
            10        20        30        40        50        60        70
               System cpu-usage last 72 hours(Per Hour)
              * = maximum cpu-usage    H = average cpu-usage
```

Table 3-8 Description of the **display cpu-usage history** command output

Item	Description
System cpu-usage last 60 minutes(Per Min)	CPU usage statistics within the last one hour, with a step of one minute.
System cpu-usage last 24 hours(Per Halfhour)	CPU usage statistics within the last 24 hours, with a step of half an hour.
System cpu-usage last 72 hours(Per Hour)	CPU usage statistics within the last 72 hours, with a step of an hour.
* = maximum cpu-usage	Maximum CPU usage. For example, the maximum CPU usage in the first hour in the latest 72 hours is 75%.

Item	Description
H = average cpu-usage	Average CPU usage. For example, the average CPU usage in the first hour in the latest 72 hours is 5%.

3.1.10 display device

Function

The **display device** command displays the type and status of the components on a device.

Format

display device [**slot** *slot-id*]

Parameters

Parameter	Description	Value
slot *slot-id*	Specifies a slot ID.	The value depends on the device configuration.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

If you need to check whether a switch is working properly, run the **display device** command to view hardware information of the components and device registration status on the switch.

This command can also display the working status of the battery or redundant power supply (RPS) used for a device.

The following product models support the use of an RPS:

- S5720-LI series: S5720-28X-LI-AC, S5720-28X-LI-DC, S5720-28X-PWR-LI-AC, S5720-52X-LI-AC, S5720-52X-LI-DC, S5720-52X-PWR-LI-AC, S5720-28X-LI-24S-AC, S5720-28X-LI-24S-DC, S5720-28X-PWH-LI-AC, S5720-52X-PWR-LI-ACF, S5720-52X-LI-48S-AC, S5720-52X-LI-48S-AC1, S5720-52X-LI-48S-DC1, S5720-52X-LI-24S-AC1 S5720-28X-PWR-LI-ACF
- S5720S-LI series: S5720S-28X-LI-24S-AC and S5720S-52X-LI-24S-AC1

Example

Display information about the components on a device (with a built-in power supply unit or power module).

```
<<HUAWEI> display device
S5720-52P-LI-AC's Device status:
Slot Sub  Type             Online    Power     Register     Status   Role
--------------------------------------------------------------------------------
0    -    S5720-52P-LI       Present   PowerOn    Registered   Normal   Master
```

Display information about components on a device (connected to an RPS).

```
<HUAWEI> display device
S5720-28X-LI-AC's Device status:
Slot  Sub  Type             Online    Power     Register     Status   Role
--------------------------------------------------------------------------------
0     -     S5720-28X-LI       Present   PowerOn    Registered   Normal   Master
          RPS              Present   PowerOn    Registered   Self-powered
```

Display information about components on a device (where ports on the device panel and ports on subcards cannot be used together).

```
<HUAWEI> display device
S6720-32C-PWH-SI-AC's Device status:
Slot Sub  Type               Online    Power    Register     Status   Role
--------------------------------------------------------------------------------
0    -    S6720-32C-PWH-SI     Present   PowerOn  Registered   Normal
Master
     1    -                  Present   PowerOn  Unregistered -        NA
     PWR1 POWER              Present   PowerOn  Registered   Normal
NA
     FAN1 FAN                Present   PowerOn  Registered   Normal
NA
Info: Slot 0 is in the port-on-card disable mode, so subcard 1 is unavailable and unregistered.
```

Display information about the component in slot 0.

```
<HUAWEI> display device slot 0
*down: administratively down

S5720-52P-LI-AC's Device status:
Slot Sub  Type             Online    Power     Register     Status   Role
--------------------------------------------------------------------------------
0    -    S5720-52P-LI       Present   PowerOn    Registered   Normal   Master
--------------------------------------------------------------------------------
  Board Type        : S5720-52P-LI
  Board Description : 48 Ethernet 10/100/1000 ports,4 Gig SFP,AC 110/220V
--------------------------------------------------------------------------------
--------------------------------------------------------------------------------
Port      Port     Optic     MDI     Speed    Duplex  Flow-    Port   PoE
          Type     Status            (Mbps)           Ctrl     State  State
--------------------------------------------------------------------------------
0/0/1     GE(C)    Absent    Auto    1000     Full    Disable  Down   -
0/0/2     GE(C)    Absent    Auto    1000     Full    Disable  Up     -
0/0/3     GE(C)    Absent    Auto    1000     Full    Disable  Down   -
0/0/4     GE(C)    Absent    Auto    1000     Full    Disable  Down   -
0/0/5     GE(C)    Absent    Auto    1000     Full    Disable  Down   -
0/0/6     GE(C)    Absent    Auto    1000     Full    Disable  Down   -
0/0/7     GE(C)    Absent    Auto    1000     Full    Disable  Down   -
0/0/8     GE(C)    Absent    Auto    1000     Full    Disable  Down   -
0/0/9     GE(C)    Absent    Auto    1000     Full    Disable  Down   -
0/0/10    GE(C)    Absent    Auto    1000     Full    Disable  Down   -
0/0/11    GE(C)    Absent    Auto    1000     Full    Disable  Down   -
0/0/12    GE(C)    Absent    Auto    1000     Full    Disable  Down   -
0/0/13    GE(C)    Absent    Auto    1000     Full    Disable  Down   -
0/0/14    GE(C)    Absent    Auto    1000     Full    Disable  Down   -
0/0/15    GE(C)    Absent    Auto    1000     Full    Disable  Down   -
0/0/16    GE(C)    Absent    Auto    1000     Full    Disable  Down   -
0/0/17    GE(C)    Absent    Auto    1000     Full    Disable  Down   -
```



```
0/0/18   GE(C)   Absent   Auto   1000   Full   Disable  Down   -
0/0/19   GE(C)   Absent   Auto   1000   Full   Disable  Down   -
```

Table 3-9 Description of the display device command output

Item	Description
Slot	Slot ID.
Sub	Card ID. The value can be: ● –: indicates that the component is a device, not a card. ● n: indicates a card. *n* is a digit. ● FANn: indicates a fan module. *n* indicates the serial number of the fan module. ● PWRn: indicates a power module . *n* indicates the serial number of the power module.
Type	Component type. A component can be a device, RPS, or a card. Subcards are classified into the front subcard, rear subcard, power subcard and fan subcard. ● Front card: The command displays the PCB model of a front card. For card classification and details about different cards, see the *Hardware Description*. ● Rear card: The command displays the PCB model of a rear card. For card classification and details about different cards, see the *Hardware Description*. ● Fan subcards include FAN. ● Power subcard is POWER. ● Lead-acid battery board: PBB-12AHA Redundant power supply: RPS
Online	Whether a component is available. If the component is available, this field displays Present. If the component is unavailable, it is not displayed in the command output.
Power	Power supply status. The value can be: ● PowerOn ● PowerOff
Register	Whether the device is registered: ● Registered: indicates that the component is registered. ● Unregistered: indicates that the component is unregistered.

Item	Description
Status	Status of the component. The value can be: • Abnormal: indicates that the component is running abnormally or the component does not match the device model. • Normal: indicates that the component is running normally. • WarmingUp: indicates that a subcard is performing configuration restoration. If the device is connected to an RPS power supply, the following values may be displayed: • Non-powered: The RPS power supply is not supplying power to the local device. • Other-powered: The RPS power supply is supplying power to another device and cannot supply power to the local device. • Self-powered: The RPS power supply is supplying power to the local device. • –: The RPS power supply is initializing and has not registered.
Role	Role of a component. • In a stack, the value can be: Master: The component is the master switch. Standby: The component is the standby switch. Slave: The component is a slave switch. • On a standalone device, this field displays Master. • The value NA indicates a card.
Board Type	Device type.
Board Description	Device description.
Port	Number of an interface on a device.
Port Type	Type of an interface. • If the field value contains (C), this interface is an electrical interface. • If the field value contains (F), this interface is an optical interface.
Optic Status	Whether an optical module is available on an interface. • Present: An optical module is present on the interface. • Absent: No optical module is present on the interface. • -: Optical module information cannot be obtained.

Item	Description
MDI	Medium dependent interface (MDI) type, which can be any of the following: ● Auto ● Normal ● Across If this field displays -, the MDI type of the interface cannot be obtained.
Speed (Mbps)	Interface speed.
Duplex	Duplex mode of an interface. ● Half: The interface works in half-duplex mode. ● Full: The interface works in full-duplex mode. ● -: The interface duplex mode cannot be obtained. To set the duplex mode for an interface, run the **duplex** command.
Flow-Ctrl	Flow control status on an interface. ● Disable: The flow control and received flow control is disabled on the interface. ● Enable: The flow control function is enabled on the interface. ● Receive enable: The receive flow control is enabled on the interface. ● -: The flow control status cannot be obtained. To configure flow control, run the **flow-control** or **flow-control receive** command.
Port State	Status of an interface: ● down: The interface is physically Down. ● *down: The interface is manually shut down. ● up: The interface is in Up state.
PoE State	Status of the PoE function on an interface. ● Enable: The PoE function is enabled. ● Disable: The PoE function is disabled. ● -: PoE information cannot be obtained.

3.1.11 display device mac-number

Function

The **display device mac-number** command displays the number of MAC addresses of a switch.

Format

display device mac-number [**slot** *slot-id*]

Parameters

Parameter	Description	Value
slot *slot-id*	Specifies a device ID.	The value must be set according to the device configuration.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

One or more MAC addresses may be configured on a switch before delivery. To check the number of MAC addresses of a switch, run the **display device mac-number** command. If the switch has multiple MAC addresses configured, the MAC addresses of Layer 3 interfaces are different from the system MAC address. If the switch has only one MAC address configured, the MAC addresses of Layer 3 interfaces are the same as the system MAC address. On a switch with one or more MAC addresses configured, the MAC addresses of Layer 2 interfaces are the same as the system MAC address.

If **slot** *slot-id* is not specified in a stack, the **display device mac-number** command displays the number of MAC addresses of the master switch.

Example

Display the number of MAC addresses.

```
<HUAWEI> display device mac-number
The number of MAC address : 1
```

Table 3-10 Description of the **display device mac-number** command output

Item	Description
The number of MAC address	Number of MAC addresses.

3.1.12 display device manufacture-info

Function

The **display device manufacture-info** command displays manufacture information about the device.

Format

display device manufacture-info [**slot** *slot-id*]

Parameters

Parameter	Description	Value
slot *slot-id*	Specifies a slot ID.	The value depends on the device configuration.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display device manufacture-info** command to view manufacture information about the device, including the serial number and manufacture date. The command output contains information about only service subcards and does not contain information about fans and power modules.

Example

Display manufacture information about the device.

```
<HUAWEI> display device manufacture-info
Slot  Sub  Serial-number         Manu-date
- - - - - - - - - - - - - - - - - - - - - -
0     -    2102353169107C800132   2011-08-24
      1    021ESN1234567890       2000-01-01
```

Display manufacture information about devices in a stack.

```
<HUAWEI> display device manufacture-info
Slot  Sub  Serial-number         Manu-date
- - - - - - - - - - - - - - - - - - - - - -
0     -    2102353169107C800132   2011-08-24
      1    021ESN1234567890       2000-01-01
3     -    2102353170107C800132   2011-08-23
4     -    2102353170107C800132   2011-08-23
      1    020WYG1234567892       2010-12-02
8     -    2102353170107C800235   2000-01-01
```

Table 3-11 Description of the display device manufacture-info command output

Item	Description
slot	Slot ID.
Sub	Subcard number.
Serial-number	Serial number.
Manu-date	Manufacture date of the device.

3.1.13 display diagnostic-information

Function

The **display diagnostic-information** command collects and displays all the current diagnostic information or saves diagnostic information in a specified file.

Format

display diagnostic-information [**acl** | **ap** | **arp** | **bfd** | **cmng** | **decoding** | **defend** | **dhcp** | **engine** | **evpn** | **gpm** | **l2adp** | **l3adp** | **lbdt** | **lldp** | **mcast** | **mpls** | **qos** | **rrpp** | **rumng** | **sa** | **sdk** | **smlk** | **srm** | **sta** | **stack** | **stat** | **stp** | **ucm** | **vxlan**] [*file-name*]

NOTE

- Only the S5720I-SI, S500, S5735-S, S5735S-S, S5735-S-I, S5735S-H, S5736-S, S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6720S-S, S6730-H, S6730S-H, S6730-S, and S6730S-S support **bfd**.
- Only the S5731-H, S5731S-H, S5731-S, S5731S-S, S5732-H, S6720-EI, S6720S-EI, S6730S-H, S6730-S, S6730S-S, and S6730-H support **mpls**.
- Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S support **sdk**.
- The **stack** parameter is supported on a stack only.
- Only the S5731-H, S5731S-H, S5732-H, S6730S-H, and S6730-H support **ap** and **sta**.
- Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S support **vxlan** and **evpn**.

Parameters

Parameter	Description	Value
acl	Displays ACL information.	-
ap	Displays AP information.	-
arp	Displays ARP information.	-

Parameter	Description	Value
bfd	Displays BFD information.	-
cmng	Displays cloud-based management information.	-
defend	Displays attack defense information.	-
decoding	Displays decoding information.	-
dhcp	Displays DHCP information.	-
engine	Displays engine information.	-
evpn	Displays EVPN information.	-
gpm	Displays GPM information.	-
l2adp	Displays L2 information.	-
l3adp	Displays L3 information.	-
lbdt	Displays LBDT information.	-
lldp	Displays LLDP information.	-
mcast	Displays multicast information.	-
mpls	Displays MPLS information.	-
qos	Displays QoS information.	-
rrpp	Displays RRPP information.	-
sa	Displays SA information.	-
sdk	Displays sdk information.	-
smlk	Displays Smart Link information.	-
stack	Displays stack information.	-

Parameter	Description	Value
srm	Displays device information.	-
sta	Displays STA information.	-
stat	Displays basic statistic information.	-
stp	Displays STP information.	-
ucm	Displays UCM module information.	-
vxlan	Displays VXLAN module information.	-
file-name	Specifies the name of the file where diagnostic information is stored.	The value is a string of 5 to 64 characters. The file name extension must be .txt. The default directory where files are stored is flash:/.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

When a fault occurs in the system, you can use the **display diagnostic-information** command to collect diagnostic information for fault location.

The **display diagnostic-information** command output includes the output for multiple **display** commands, such as **display clock**, **display version**, and **display current-configuration**. Running the **display diagnostic-information** command is like running these **display** commands in batches.

Precautions

- If the *file-name* parameter is not specified, diagnostic information is only displayed on the screen. If the *file-name* parameter is specified, diagnostic information is only stored to a specified file but not displayed on the screen, and the command level is management level (3).
- The command output does not support split-screen display.

- If this command displays a long output, press **Ctrl+C** to abort this command.
- This command displays diagnostic information, which helps locate faults but may affect system performance. For example, CPU usage may become high. Therefore, do not use this command when the system is running properly.
- Running the **display diagnostic-information** command simultaneously on multiple terminals connected to the device is prohibited. This is because CPU usage of the device may obviously increase and the device performance may be degraded.
- When you run this command, the device obtains or uses some personal data of users, such as the STA MAC address. Delete the personal data immediately after the command is executed to ensure user data security.

Example

Display diagnostic information about the device.

```
<HUAWEI> display diagnostic-information
============================================================
  ==============display interface brief===============
============================================================
PHY: Physical
*down: administratively down
#down: LBDT down
(l): loopback
(s): spoofing
(E): E-Trunk down
(b): BFD down
(e): ETHOAM down
(dl): DLDP down
(lb): LBDT block
InUti/OutUti: input utility/output utility
Interface                   PHY   Protocol  InUti OutUti   inErrors  outErrors
Eth-Trunk5                  down  down        0%     0%          0          0
Eth-Trunk9                  down  down        0%     0%          0          0
GigabitEthernet0/0/1        *down down        0%     0%          0          0
GigabitEthernet0/0/2        *down down        0%     0%          0          0
GigabitEthernet0/0/3        *down down        0%     0%          0          0
GigabitEthernet0/0/4        *down down        0%     0%          0          0
GigabitEthernet0/0/5        up    up          0%     0%          0          0
GigabitEthernet0/0/6        *down down        0%     0%          0          0
GigabitEthernet0/0/7        down  down        0%     0%          0          0
GigabitEthernet0/0/8        *down down        0%     0%          0          0
GigabitEthernet0/0/9        down  down        0%     0%          0          0
GigabitEthernet0/0/10       down  down        0%     0%          0          0
GigabitEthernet0/0/11       up    up          0%     0%          0          0
GigabitEthernet0/0/12       down  down        0%     0%          0          0
GigabitEthernet0/0/13       down  down        0%     0%          0          0
GigabitEthernet0/0/14       down  down        0%     0%          0          0
GigabitEthernet0/0/15       down  down        0%     0%          0          0
GigabitEthernet0/0/16       down  down        0%     0%          0          0
GigabitEthernet0/0/17       down  down        0%     0%          0          0
GigabitEthernet0/0/18       down  down        0%     0%          0          0
GigabitEthernet0/0/19       down  down        0%     0%          0          0
GigabitEthernet0/0/20       *down down        0%     0%          0          0
GigabitEthernet0/0/21       down  down        0%     0%          0          0
GigabitEthernet0/0/22       *down down        0%     0%          0          0
GigabitEthernet0/0/23       down  down        0%     0%          0          0
GigabitEthernet0/0/24       up    up          0%     0%          0          0
......
```

Save diagnostic information to the file **aa.txt** in the flash memory.

```
<HUAWEI> display diagnostic-information aa.txt
Now saving the diagnostic information to the device
```



```
100%
Info: The diagnostic information was saved to the device successfully.
```

3.1.14 display elabel

Function

The **display elabel** command displays the electronic label of the device.

Format

display elabel [**slot** *slot-id* [*subcard-id*]]

Parameters

Parameter	Description	Value
slot *slot-id*	Specifies a slot ID.	The value depends on the device configuration.
subcard-id	Specifies the subcard ID the ID of power module.	The value must be set according to the device configuration.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Electronic labels identify the hardware. You can use the **display elabel** command to view the electronic label information.

No electronic label is displayed for an electrical interface or a combo interface working as an electrical interface.

NOTE

The electronic label version of devices delivered since V200R011 has been updated to version 4.0. This version adds the following fields compared to earlier versions:

- Model indicates the hardware external model of the device.
- ExInfo indicates the hardware extension information of the device. This field is not provided in electronic labels of optical modules.
- ElabelVersion indicates the version of the elabel.

Example

Display the electronic label of the slot 0.


```
<HUAWEI> display elabel slot 0
Warning: It may take a long time to excute this command. Continue? [Y/N]:y
Info: It is executing, please wait...
/$[System Integration Version]
/$SystemIntegrationVersion=3.0


[Slot_0]
/$[Board Integration Version]
/$BoardIntegrationVersion=3.0


[Main_Board]

/$[ArchivesInfo Version]
/$ArchivesInfoVersion=3.0


[Board Properties]
BoardType=S5720-28P-LI-AC
BarCode=2102353174107C800132
Item=02353174
Description=S5720-28P-LI-AC Mainframe (24 10/100/1000BASE-T, 4 100/1000BASE-X, AC 110/22
0V)
Manufactured=2011-08-22
VendorName=Huawei
IssueNumber=00
CLEICode=
BOM=




[Port_GigabitEthernet0/0/1]
/$[ArchivesInfo Version]
/$ArchivesInfoVersion=3.0


[Board Properties]
BoardType=
BarCode=
Item=
Description=
Manufactured=
/$VendorName=
IssueNumber=
CLEICode=
BOM=
```

Table 3-12 Description of the **display elabel** command output

Item	Description
BoardIntegrationVersion	Version of the board software integration format.
ArchivesInfoVersion	Electronic label information version.
SystemIntegrationVersion	Version of the host software integration format.
BoardType	Vendor's component model of the specified component.
BarCode	Bar code of the specified component.

Item	Description
Item	BOM code of the specified component.
Description	English description of the specified component.
Manufactured	Production date of the specified component.
VendorName	Vendor name of the specified component.
IssueNumber	Issuing number of the specified component.
CLEICode	CLEI code of the specified component.
BOM	Sales BOM code of the specified component, which is an item number.

3.1.15 display esn

Function

The **display esn** command displays the Equipment Serial Number (ESN) of a device.

Format

display esn

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

An ESN uniquely identifies a device.

In a stack, the **display esn** command displays the ESNs of all member devices.

Example

Display the ESN of the device.

```
<HUAWEI> display esn
ESN of slot 0: 21023586001xxxxxxx
```

Table 3-13 Description of the display esn command output

Item	Description
ESN of slot 0	SN of the device with the slot ID 0.

3.1.16 display fan

Function

The **display fan** command displays the fan status.

Format

display fan [**power**]

NOTE

Only the following models support the power parameter:
S5731-H, S5731S-H, S5732-H, S5735-L, S5735S-L, S5736-S, and S6730-H

Parameters

Parameter	Description	Value
power	Indicates the fan speed of the power module.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Devices can run properly when fans are working properly. If proper heat dissipation cannot be ensured for devices, devices may overheat, damaging the hardware. You can use the **display fan** command to view the fan status.

Different device models may support different numbers of fans.

Example

Display the fan status of the device.

```
<HUAWEI> display fan
-------------------------------------------------------------------------------------------
 Slot  FanID   Online    Status    Speed     Mode     Airflow         Auto Min-Speed
Name
-------------------------------------------------------------------------------------------
 2       1   Present   Normal     34%     Auto     Front-to-Back             -   FAN-031A-
B
 2       2   Present   Normal     34%     Auto     Front-to-Back             -   FAN-031A-B
```

Table 3-14 Description of the **display fan** command output

Item	Description
Slot	Slot ID.
FAN	Number of a fan.
Online	Whether a fan is available: ● Present: available ● Absent: unavailable
Status	Running status of a fan: ● Normal: The fan is running normally. ● Abnormal: The fan works abnormally. ● -: The fan is not present.
Speed	Percentage of the current fan speed to the full speed. If this field displays -, the fan is not present or the fan works abnormally.
Mode	Working mode of a fan: ● AUTO: The fan speed can be automatically adjusted. ● MANUAL: The fan works at a fixed speed. ● -: The fan is not present or the fan works abnormally.
Airflow	Airflow direction of a fan: ● Back-to-Side: Air flows from the rear to the left and right sides. ● Side-to-Back: Air flows from the left and right sides to the rear. ● Side-to-Side: Air flows from one side to the other side. ● Front-to-Back: Air flows from the front to the rear. ● -: The fan is not present.

Item	Description
Auto Min-Speed	Minimum fan speed in automatic fan speed adjustment mode. To configure the minimum fan speed in automatic fan speed adjustment mode, run the **set fan speed auto min-speed** command. If this field displays -, this command is not supported, or the fan is not present, or the fan works abnormally.
Name	Name of a fan: **NOTE** The information is displayed only for the S5731-H, S5732-H, and S6730-H.

Display the fan speed of the power module.

```
<HUAWEI> display fan power
-----------------------------------------
 Slot  FanID   Online     PowerSpeed
-----------------------------------------
 1        1   Absent           -
 1        2   Present        46%
```

Table 3-15 display fan power command output

Item	Description
Speed	Fan speed of the power module.

3.1.17 display integrated-power information

Function

The **display integrated-power information** command displays information about the built-in or external power supply of an extended-temperature switch.

NOTE

This command is available only on the following switch models:

S5735-S4T2X-IA150G1, S5735-S8P2X-IA200G1, S5735-S8P2X-IA200H1, S5735-L8P4X-IA1, S5735-L8T4X-IA1

Format

display integrated-power information

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run this command on an extended-temperature switch to check the version and working status of the built-in or external power supply.

Example

Display information about the built-in power supply of the S5735-S4T2X-IA150G1.

```
<HUAWEI> display integrated-power information
-------------------------------------------------------------
 Integrated power information
-------------------------------------------------------------
General information
  Software version            : 555
  Hardware version            : B
  Power supply mode           : Mains Power 500
  Total input power(W)        : 0.00
  AC input voltage status     : Normal
  12V DC output voltage status : Normal
  24V AC output voltage(V)    : 0.00
  24V AC output current(A)    : 0.00
  53V DC output voltage status : Normal
```

Table 3-16 Description of the **display integrated-power information** command output

Item	Description
Integrated power information	Information about the built-in power supply.
General information	Generic information about the built-in power supply.
Software version	Software version, in hexadecimal notation.
Hardware version	Hardware version, which is an ASCII value.
Power supply mode	Working mode of the built-in power supply.
Total input power(W)	Total input power, in Watt (W).
AC input voltage status	AC input voltage status: • Normal: The voltage is normal. • Abnormal: The voltage is abnormal.

Item	Description
12V DC output voltage status	12 V DC output voltage status: ● Normal: The voltage is normal. ● Abnormal: The voltage is abnormal.
24V AC output voltage(V)	24 V AC output voltage, in Volt (V).
24V AC output current(A)	24 V AC output current, in amperes (A).
53V DC output voltage status	53 V DC output voltage status: ● Normal: The voltage is normal. ● Abnormal: The voltage is abnormal.

Display information about the built-in power supply of the S5735-S8P2X-IA200H1.

```
<HUAWEI> display integrated-power information
Info: This operation may take a few seconds. Please wait for a
moment..
-------------------------------------------------------------
 Integrated power information
-------------------------------------------------------------
General information
   Hardware version             : A
   Software version(ASCII)      : V100R021C10SPC000
   Power supply mode            : Hybrid Power 500(B)
   Current power supply mode    : Mains
   Busbar voltage(V)            : 54.26
   AC voltage(V)                : 218.69
   SSU input voltage(V)         : 0.00
   SSU input current(A)         : 0.00
   Total load power(W)          : 0.00
   Total input power(W)         : 0.00
   12V DC output voltage status : Normal
   24V AC output voltage(V)     : 0.00
   24V AC output current(A)     : 0.00
   53V DC output voltage(V)     : 54.50
```

Table 3-17 Description of the **display integrated-power information** command output

Item	Description
Integrated power information	Information about the built-in power supply.
General information	Generic information about the built-in power supply.
Hardware version	Hardware version. The value is in hexadecimal notation.
Software version(ASCII)	Software version. The value is in ASCII format.

Item	Description
Current power supply mode	Working mode of the built-in power supply.
Busbar voltage(V)	Busbar voltage, in volts (V).
AC voltage(V)	AC voltage, in volts (V).
SSU input voltage(V)	Input voltage of the solar supply unit (SSU), in volts (V).
SSU input current(A)	Input current of the SSU, in amperes (A).
Total load power(W)	Total load power, in watts (W).
Total input power(W)	Total input power, in watts (W).
12V DC output voltage status	12 V DC output voltage status: ● Normal: The voltage is normal. ● Abnormal: The voltage is abnormal.
24V AC output voltage(V)	24 V AC output voltage, in volts (V).
24V AC output current(A)	24 V AC output current, in amperes (A).
53V DC output voltage(V)	53 V DC output voltage, in volts (V).
53V DC output current(A)	53 V DC output current, in amperes (A).
AC current(A)	AC current, in amperes (A).
Chip1 upgrade status	Upgrade status of chip 1: ● Normal: The voltage is normal. ● Abnormal: The voltage is abnormal.
Chip2 upgrade status	Upgrade status of chip 2: ● Normal: The voltage is normal. ● Abnormal: The voltage is abnormal.
Chip3 upgrade status	Upgrade status of chip 3: ● Normal: The voltage is normal. ● Abnormal: The voltage is abnormal.
Chip4 upgrade status	Upgrade status of chip 4: ● Normal: The voltage is normal. ● Abnormal: The voltage is abnormal.

Display information about the power supply connected to the S5735-L8P4X-IA1.

```
<HUAWEI> display integrated-power information
-------------------------------------------------------------
```



```
 Integrated power information
-------------------------------------------------------------
General information
  Hardware version          : B
  Software version          : V1.20
```

Table 3-18 Description of the **display integrated-power information** command output

Item	Description
Integrated power information	Information about the external power supply.
General information	Generic information about the built-in power supply.
Hardware version	Hardware version. The value is in hexadecimal notation.
Software version	Software version.

3.1.18 display memory-usage

Function

The **display memory-usage** command displays the memory usage of the device.

Format

display memory-usage [**slave** | **slot** *slot-id*] [**vcpu** *vcpu-index*]

NOTE

The **slave** parameter is not supported if the switch does not support the stacking function or does not have the stacking function enabled.

Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S support the **vcpu** *vcpu-index* parameter.

Parameters

Parameter	Description	Value
slave	Displays memory usage of a slave switch in a stack. This parameter is valid only when multiple switches form a stack.	-
slot *slot-id*	Displays memory usage of a slot ID.	The value depends on the device configuration.

Parameter	Description	Value
vcpu *vcpu-index*	Specifies the virtual CPU number.	Specify the *vcpu-index* parameter based on the hardware configuration.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Memory usage is an important index to evaluate device performance. A high memory usage will cause service faults. You can use the **display memory-usage** command to view memory usage to check whether devices are working properly.

The memory usage displayed using the **display memory-usage** command is based on the total available memory of a process.

Example

Display memory usage of the current device.

```
<HUAWEI> display memory-usage
 Memory utilization statistics at 2008-12-15 15:17:42+08:00
 System Total Memory Is: 394152720 bytes
 Total Memory Used Is: 130975664 bytes
 Memory Using Percentage Is: 33%
```

Display memory usage of the virtual CPU 1 in slot 0.

```
<HUAWEI> display memory-usage slot 0 vcpu 1
 Vcpu 1 Memory utilization Info:
 Memory utilization statistics at 2017-08-26 06:11:20+00:00
 System Total Memory Is: 30408904 bytes
 Total Memory Used Is: 22938332 bytes
 Memory Using Percentage Is: 75%
```

Table 3-19 Description of the **display memory-usage** command output

Item	Description
Memory utilization statistics at	Time when memory usage is collected.
System Total Memory	Total memory of the device network operating system.
Total Memory Used	Total used memory of the device network operating system.
Memory Using Percentage	Memory usage.

3.1.19 display memory-usage threshold

Function

The **display memory-usage threshold** command displays the memory usage threshold on the device.

Format

display memory-usage threshold [**slot** *slot-id*]

Parameters

Parameter	Description	Value
slot *slot-id*	Displays the memory usage threshold of a specified slot ID.	The value depends on the device configuration.

Views

All views

Default Level

2: Configuration level

Usage Guidelines

You can view the memory usage alarm threshold to learn about the conditions for triggering alarms.

- When memory usage reaches the alarm threshold, the system generates an alarm.
- When memory usage falls within the alarm threshold, the system generates a clear alarm.

Example

Display the memory usage threshold on the main control board.

```
<HUAWEI> display memory-usage threshold
 Current memory threshold of the main board is 95%.
```

Table 3-20 Description of the display memory-usage threshold command output

Item	Description
Current memory threshold of the main board is 95%.	The memory usage threshold of the main control board is 95%. To set the memory usage threshold of the main control board, use the **set memory-usage threshold** *threshold-value* command.

3.1.20 display power

Function

The **display power** command displays information about all power supplies on the device.

Format

display power

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can use this command to check the status of all power supplies, and their power.

No information is displayed for built-in power supplies.

Example

Display the current power supply status.

```
<HUAWEI> display power
-------------------------------------------------------------------------
 Slot    PowerID  Online   Mode   State      Power(W)  CurrentPower(W)
-------------------------------------------------------------------------
 0       PWRI     Present  AC     Supply     500.00         70.50
 0       PWRII    Absent   -      -          -              -
```

Table 3-21 Description of the **display power** command output

Item	Description
Slot	• Slot ID if stacking is not configured. The value is 0. • Stack ID if stacking is configured. The value must be set according to the device configuration.

Item	Description
PowerID	ID of a power supply slot: • PWRI: slot for a power module, or lead-acid battery board • PWRII: slot for a power module **NOTE** On the S5720I-SI, S5735-S, S500, S5735S-S, S5735-S-I, S5735S-H, S5736-S, S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6720S-S, S6730-H, S6730S-H, S6730-S, and S6730S-S series switches, the power supply slots are PWR1 and PWR2. If a device has only one power supply slot, only PWR1 is displayed.
Online	Whether a power supply is installed properly. • Present: indicates that the power supply is installed properly. • Absent: indicates that the power supply is not installed properly, or the power supply is a fixed power supply.
Mode	Type of the power module, or lead-acid battery board: • AC: AC power module • DC: DC power module • –: Power supply invalid or absent • PBB: Lead-acid battery board
State	Working status of a power module. • Supply: Current is output. • NotSupply: No current is output. • –: Invalid or absent
Power(W)	Rated power of a power supply. If this field displays –, the power supply is invalid or is not installed properly.
CurrentPower(W)	Real-time power of a power supply. If this field displays –, the power supply is not supported.

3.1.21 display system-software information

Function

The **display system-software information** command displays the software versions supported by the device.

NOTE

Only the S1730S-S1, S200, S2730S-S, S300, S500, S5731-H, S5731S-H, S5731-S, S5731S-S, S5732-H, S5735-L, S5735S-L, S5735-L1, S5735S-L1, S5735S-L-M, S5735-S, S5735-S-I, S5735S-S, S5735S-H, S5736-S, S6730-H, S6730-S, and S6735-S support this command.

Format

display system-software information

Parameters

None

Views

User views

Default Level

3: Management level

Usage Guidelines

Before upgrading a device, you can run this command to check the software versions supported by the device. This helps you select a software package supported by the device. Some models cannot be downgraded due to component upgrade. Before downgrading a device, run this command to check the software versions supported by the device.

Example

Display the software versions supported by the device.

```
<HUAWEI> display system-software information
Slot 0:
Device type       : S5735S-L48T4X-A
Supported versions : V200R021C00 and later versions
```

Table 3-22 Description of the **display system-software information** command output

Item	Description
Slot	Slot ID.
Device type	Device model.

Item	Description
Supported versions	Software versions to which the device can be upgraded.

3.1.22 display software information

Function

The **display software information** command displays information about the current system software package.

Format

display software information

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Before upgrading a device, you can run this command to check whether the current startup software package is supported by the device.

Example

Display the software version supported by the device.

```
<HUAWEI> display software information
Startup software name      : xxxx.cc
Startup software file name : xxxx.cc
```

Table 3-23 Description of the **display software information** command output

Item	Description
Startup software name	Name of the software package supported by the device.
Startup software file name	Name of the current startup software package.

3.1.23 display transceiver

Function

The **display transceiver** command displays information about the optical module on an interface.

NOTE

The command displays only information about optical interfaces.

Format

display transceiver [**interface** *interface-type interface-number* | **slot** *slot-id*] [**verbose**]

Parameters

Parameter	Description	Value
interface *interface-type interface-number*	Specifies the type and number of an interface. • *interface-type* specifies the interface type. • *interface-number* specifies the interface number.	-
slot *slot-id*	Specifies a slot ID.	The value depends on the device configuration.
verbose	Displays detailed information about the optical module on an interface, including the general information, manufacture information, alarm information, and diagnostic information.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run this command to view general information, manufacture information, and alarm information about an optical module. If you specify the **verbose** keyword, diagnostic information is also displayed in addition to the preceding information.

If a device does not support optical modules, a message will be displayed after you run this command.

Some parameters including the current and optical power will be displayed for each lane of the 40GE interfaces.

Example

Display general information, manufacture information, and alarm information about the optical module on a specified interface.

```
<HUAWEI> display transceiver interface gigabitethernet 0/0/1
GigabitEthernet0/0/1 transceiver information:
---------------------------------------------------------------
Common information:
  Transceiver Type              :1000_BASE_SX_SFP
  Connector Type                :LC
  Wavelength(nm)                :850
  Transfer Distance(m)          :0(9um),300(50um),150(62.5um)
  Digital Diagnostic Monitoring  :YES
  Vendor Name                   :HUAWEI
  Vendor Part Number            :02315204
  Ordering Name                 :
---------------------------------------------------------------
Manufacture information:
  Manu. Serial Number           :CD25HP12M
  Manufacturing Date            :2013-06-184
  Vendor Name                   :HUAWEI
---------------------------------------------------------------
```

Display general information, manufacture information, alarm information and diagnostic information about the optical module on a specified interface.

```
<HUAWEI> display transceiver interface gigabitethernet 0/0/3 verbose
GigabitEthernet0/0/3 transceiver information:
---------------------------------------------------------------
Common information:
  Transceiver Type              :GPS_SFP
  Connector Type                :SMA Coaxial Connector
  Wavelength(nm)                :-
  Transfer Distance(m)          :100(copper)
  Digital Diagnostic Monitoring  :NO
  Vendor Name                   :HUAWEI
  Vendor Part Number            :HUAWEI AE 905S A
  Ordering Name                 :
---------------------------------------------------------------
Manufacture information:
  Manu. Serial Number           :031TUX10HB000065
  Manufacturing Date            :2017-11-28
  Vendor Name                   :HUAWEI
---------------------------------------------------------------
Diagnostic information:
  Temperature(°C)               :26.00
  Temp High Threshold(°C)       :85.00
  Temp Low  Threshold(°C)       :-40.00
  Voltage(V)                    :3.29
  Volt High Threshold(V)        :3.64
  Volt Low  Threshold(V)        :2.95
  Bias Current(mA)              :4.57
```



```
  Bias High Threshold(mA)       :9.00
  Bias Low  Threshold(mA)       :2.00
  RX Power(dBM)                 :-40.00
  RX Power High Warning(dBM)    :-1.00
  RX Power Low  Warning(dBM)    :-15.80
  RX Power High Threshold(dBM)  :0.00
  RX Power Low  Threshold(dBM)  :-16.99
  TX Power(dBM)                 :-5.03
  TX Power High Warning(dBM)    :4.00
  TX Power Low  Warning(dBM)    :-4.70
  TX Power High Threshold(dBM)  :-2.22
  TX Power Low  Threshold(dBM)  :-6.99
  Transceiver phony alarm       :Yes
----------------------------------------------------------------------

<HUAWEI> display transceiver interface xgigabitethernet 0/0/4 verbose
XGigabitEthernet0/0/4 transceiver information:
----------------------------------------------------------------------
Common information:
  Transceiver Type              :GPS_SFP
  Connector Type                :SMA Coaxial Connector
  Wavelength(nm)                :-
  Transfer Distance(m)          :100(copper)
  Digital Diagnostic Monitoring  :NO
  Vendor Name                   :HUAWEI
  Vendor Part Number            :HUAWEI AE 905S A
  Ordering Name                 :
----------------------------------------------------------------------
Extended information:
  Longitude(° )                 :118.7662952
  Latitude(° )                  :31.9829019
  Altitude(mm)                  :75051
----------------------------------------------------------------------
Manufacture information:
  Manu. Serial Number           :031TUX10HB000065
  Manufacturing Date            :2017-11-28
  Vendor Name                   :HUAWEI
----------------------------------------------------------------------
Diagnostic information:
  Transceiver does not support diagnostic information.
----------------------------------------------------------------------
```

Table 3-24 Description of the **display transceiver** command output

Item	Description
Common information	Generic information about the optical module.
Transceiver Type	Type of the optical module.
Connector Type	Type of the fiber connector required by the optical module. The value depends on the protocol related to the optical module.
Wavelength (nm)	Wavelength of the optical module. If this field displays -, the optical module does not have wavelength information.

Item	Description
Transfer Distance (m)	Transmission distance of the optical module. 50 um and 62.5 um are fiber diameters. Fibers with a diameter of 50 um or 62.5 um are multimode fibers. Fibers with a diameter of 9 um are single-mode fibers. For a GPS module, this field indicates the maximum length of the antenna between the GPS module and signal receiver. **NOTE** Only the maximum transmission distance of the optical module is displayed if different optical fibers are used.
Digital Diagnostic Monitoring	Whether diagnostic information about the optical module is monitored.
Vendor Name	Vendor name of the optical module. If the system has not determined whether the optical module is a Huawei-customized one, this field displays Judging. If the vendor name of an optical module is not HUAWEI, check whether the optical module is a Huawei-certified optical module. For details, see "How Can I Determine Whether an Optical Module Is Huawei-Certified?" in the *S300, S500, S2700, S5700, and S6700 V200R023C00 Configuration Guide - Device Management – Device Status Query*.
Vendor Part Number	Vendor part number or product name. If the system has not determined whether the optical module is a Huawei-customized one, this field displays Judging.
Ordering Name	External name of the optical module. Currently, this field is not supported and is empty.
Extended information	GPS module information. Only the S5720I-SI and S5735-S-I support this item.
Longitude(°)	Longitude of the location of the GPS module. Only the S5720I-SI and S5735-S-I support this item.
Latitude(°)	Latitude of the location of the GPS module. Only the S5720I-SI and S5735-S-I support this item.
Altitude(mm)	Altitude of the location of the GPS module. Only the S5720I-SI and S5735-S-I support this item.
Manufacture information	Manufacture information of the optical module.
Manu. Serial Number	Vendor sequence number of the optical module.
Manufacturing Date	Manufacturing date of the optical module.

Item	Description
Diagnostic information	Diagnostic information about the optical module.
Temperature (°C)	Current temperature of the optical module.
Temp High Threshold (°C)	Upper temperature threshold for the optical module.
Temp Low Threshold (°C)	Lower temperature threshold for the optical module.
Voltage (V)	Current voltage of the optical module.
Volt High Threshold(V)	Upper voltage threshold for the optical module.
Volt Low Threshold(V)	Lower voltage threshold for the optical module.
Bias Current (mA)	Bias current of the optical module.
Bias High Threshold (mA)	Upper threshold for the bias current of the optical module.
Bias Low Threshold (mA)	Lower threshold for the bias current of the optical module.
RX Power (dBM)	Input power of the optical module. When the Input power is 0 W, **-Inf** is displayed.
RX Power High Warning(dBM)	Upper warning threshold for the receive power of the optical module.
RX Power Low Warning(dBM)	Lower warning threshold for the receive power of the optical module.
RX Power High Threshold (dBM)	Upper input power threshold for the optical module.
RX Power Low Threshold (dBM)	Lower input power threshold for the optical module.
TX Power (dBM)	Output power of the optical module. When the output power is 0 W, **-Inf** is displayed.
TX Power High Warning(dBM)	Upper warning threshold for the transmit power of the optical module.
TX Power Low Warning(dBM)	Lower warning threshold for the transmit power of the optical module.
TX Power High Threshold (dBM)	Upper output power threshold for the optical module.

Item	Description
TX Power Low Threshold (dBM)	Lower output power threshold for the optical module.
Transceiver phony alarm:Yes	The device has generated an alarm on an optical module not certified for Huawei switches. This field is displayed only when the following conditions are met: • The device is enabled to generate alarms on non-Huawei-customized optical modules. This alarm function is enabled by default. If it is disabled, you can run the **undo transceiver phony-alarm-disable** command to enable it. • This optical module is a non-Huawei-customized one.

3.1.24 display transceiver diagnosis interface

Function

The **display transceiver diagnosis interface** command displays the diagnosis parameters of an optical module.

Format

display transceiver diagnosis interface [*interface-type interface-number*]

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.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display transceiver diagnosis interface** command to view digital diagnostic monitoring (DDM) information about optical modules installed on all interfaces of a device.

If *interface-type interface-number* is specified, only diagnostic information about the optical module installed on the specified interface is displayed.

Example

Display the diagnosis parameters of the optical module installed in GigabitEthernet0/0/4.

```
<HUAWEI> display transceiver diagnosis interface gigabitethernet 0/0/4
Port GigabitEthernet0/0/4 transceiver diagnostic information:
-------------------------------------------------------------------------------
Item                Value   HighAlarm    HighWarn    LowAlarm     LowWarn    Status
-------------------------------------------------------------------------------
TxPower lane0(dBm)     0.23        7.00        4.00       -7.40       -4.40    Normal
TxPower lane1(dBm)    -1.56        7.00        4.00       -7.40       -4.40    Normal
RxPower lane0(dBm)     0.06        7.00        4.00      -11.20        -8.20    Normal
RxPower lane1(dBm)    -1.42        7.00        4.00      -11.20        -8.20    Normal
Current lane0(mA)      7.03       12.00       10.00        3.00        5.00    Normal
Current lane1(mA)      6.04       12.00       10.00        3.00        5.00    Normal
Temperature(C)        47.97       80.00       70.00      -10.00        0.00    Normal
Voltage(V)             3.35        3.63        3.46        2.97        3.13    Normal
LaserTemp(C)              -           -           -           -           -    -
TecCurrent(mA)            -           -           -           -           -    -
MediaSNR(dB)              -           -           -           -           -    -
-------------------------------------------------------------------------------

Versatile Diagnostics Monitoring:
-------------------------------------------------------------------
Item         Minimum     Maximum     Average     Current PriorPeriod
-------------------------------------------------------------------
Ber         5.56e-10    8.22e-10    6.75e-10    7.07e-10    0.00e+00
Fer         0.00e+00    0.00e+00    0.00e+00    0.00e+00    0.00e+00
-------------------------------------------------------------------
```

NOTE

If the parameter displays **-**, the parameter value cannot be obtained. If the **Status** field displays **-**, this parameter does not support diagnosis.

Table 3-25 Description of the **display transceiver diagnosis interface** command output

Item	Description
Item	Parameter type.
Value	Real-time value of a parameter.
HighAlarm	Upper alarm threshold.
HighWarn	Upper warning threshold.
LowAlarm	Lower alarm threshold.
LowWarn	Lower warning threshold.

Item	Description
Status	Parameter value status: • **Normal**: indicates that the current value is within the normal range, that is, the current value does not exceed the upper alarm threshold or fall below the lower upper alarm threshold. • **Abnormal**: indicates that the current value is not within the normal range.
TxPower lane0(dBm) TxPower lane1(dBm)	Transmit power of an optical module. lane*i* indicates a physical channel. If an optical module has multiple physical channels, this parameter is displayed multiple times.
RxPower lane0(dBm) RxPower lane1(dBm)	Indicates the receiving power of the optical module, in dBm.lane*i* indicates a physical channel. If an optical module has multiple physical channels, this parameter is displayed multiple times.
Current lane0(mA) Current lane1(mA)	Indicates the current of the optical module, in mA. lane*i* indicates a physical channel. If an optical module has multiple physical channels, this parameter is displayed multiple times.
Temperature(C)	Indicates the temperature of the optical module, in degree Celsius.
Voltage(V)	Indicates the voltage of the optical module, in V.
LaserTemp(C)	Laser temperature of an optical module. If an optical module has multiple channels, this parameter is displayed for multiple times for lane 0, lane 1, and so on.
TecCurrent(mA)	Indicates the tec current of the optical module.If an optical module has multiple channels, this parameter is displayed for multiple times for lane 0, lane 1, and so on.
MediaSNR(dB)	Indicates the media SNR of the optical module. If an optical module has multiple channels, this parameter is displayed for multiple times for lane 0, lane 1, and so on.
Ber	BER of an optical module. If an optical module has multiple channels, this parameter is displayed for multiple times for lane 0, lane 1, and so on.
Fer	FER of an optical module. If an optical module has multiple channels, this parameter is displayed for multiple times for lane 0, lane 1, and so on.
Minimum	Minimum BER and FER of an optical module.

Item	Description
Maximum	Maximum BER and FER of an optical module.
Average	Average BER and FER of an optical module.
Current	Real-time BER and FER of an optical module.
PriorPeriod	BER and FER of an optical module in the previous period.

3.1.25 display temperature

Function

The **display temperature** command displays the working status temperature information of the device's internal components.

Format

display temperature { **all** | **slot** *slot-id* }

Parameters

Parameter	Description	Value
all	Displays the working status temperature information of internal components in all slots on the device.	-
slot *slot-id*	Displays the working status temperature information of internal components on the specified slot.	The value depends on the device configuration.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

A high or low device temperature may damage the hardware. This command displays the working status temperature information of internal components instead of the operating temperature that indicates the temperature range of the surrounding environment. When the device temperature exceeds the upper threshold or falls below the lower threshold, the device generates an alarm to alert you that the device temperature is abnormal.

Example

Display the working status temperature information of internal components in all slots.

```
<HUAWEI> display temperature all
-------------------------------------------------------------------------------
 Slot  Card  Sensor Status    Current(C) Lower(C) Lower     Upper(C) Upper
                                        Resume(C)         Resume(C)
-------------------------------------------------------------------------------
 0     NA    NA     Normal          44       0       4        72       68
```

Table 3-26 Description of the **display temperature** command output

Item	Description
Slot	Slot ID.
Card	Subcard ID. This field is invalid on the device and displays NA.
Sensor	Number of a sensor on a card. This field is invalid on the device and displays NA.
Status	Temperature status of a device. ● Normal: The device temperature is within the normal range. ● Abnormal: The device temperature is out of the normal range.
Current(C)	Working status temperature information of internal components of a device, expressed in the centigrade scale (°C). The temperature value is displayed as an integer, so there may be a maximum of 1°C error between the displayed value and actual temperature. This field displays - when the sensor is abnormal or the obtained temperature is higher than 200°C or lower than 100°C.
Lower(C)	Low-temperature alarm threshold, expressed in the centigrade scale (°C). To set the low-temperature alarm threshold, run the **temperature threshold** command.
Lower Resume(C)	Low-temperature alarm clear threshold, expressed in the centigrade scale (°C). To set the low-temperature alarm clear threshold, run the **temperature threshold** command. The low-temperature alarm clear threshold is 4°C higher than the low-temperature alarm threshold.

Item	Description
Upper(C)	High-temperature alarm threshold, expressed in the centigrade scale (°C). To set the high-temperature alarm threshold, run the **temperature threshold** command. On the devices that support fan speed adjustment using the **set fan speed-adjust threshold minus** command, the default value of this field changes based on the PoE power load.
Upper Resume(C)	High-temperature alarm clear threshold, expressed in the centigrade scale (°C). To set the high-temperature alarm clear threshold, run the **temperature threshold** command. The high-temperature alarm clear threshold is 4°C lower than the high-temperature alarm threshold.

3.1.26 display version

Function

The **display version** command displays the device version.

Format

display version [**slot** *slot-id*]

Parameters

Parameter	Description	Value
slot *slot-id*	Specifies a slot ID.	The value depends on the device configuration.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can use the **display version** command to view the device version to determine whether the device needs to be upgraded.

Example

Display the device version.

```
<HUAWEI> display version
Huawei Versatile Routing Platform Software
VRP (R) software, Version 5.170 (S6720
V200R023C00)
Copyright (C) 2000-2020 HUAWEI TECH Co.,
Ltd.
HUAWEI S6720-54C-EI-48S-AC Routing Switch uptime is 0 week, 0 day, 0 hour, 5
minutes

ES5D2S50Q002 1(Master)  : uptime is 0 week, 0 day, 0 hour, 2
minutes
DDR             Memory Size : 2048  M bytes
FLASH Total     Memory Size : 512   M bytes
FLASH Available Memory Size : 446   M bytes
Pcb           Version   : VER.B
BootROM       Version   : 020b.0001
BootLoad      Version   : 020b.0001
CPLD          Version   : 0108
Software      Version   : VRP (R) Software, Version 5.170
(V200R023C00)
FLASH         Version   : 0000
CARD1 information
Pcb           Version   : ES5D21Q04Q01 VER.A
CPLD   Version          : 0105
PWR2 information
Pcb           Version   : PWR VER.A
FAN1 information
Pcb           Version   : NA
<HUAWEI> display version
Huawei Versatile Routing Platform Software
VRP (R) software, Version 5.170 (S5730 V200R023C00)
Copyright (C) 2000-2020 HUAWEI TECH Co., Ltd.
HUAWEI S5730-60C-HI-48S Routing Switch uptime is 0 week, 0 day, 13 hours, 49
minutes

ES5D2S52C004 1(Master)  : uptime is 0 week, 0 day, 13 hours, 47
minutes
DDR             Memory Size : 4096  M bytes
FLASH Total     Memory Size : 1024  M bytes
FLASH Available Memory Size : 842   M bytes
SSD             Memory Size : 223   G bytes
Pcb           Version   : VER.A
BootROM       Version   : 020d.0000
BootLoad      Version   : 020d.0000
CPLD          Version   : 0102
Software      Version   : VRP (R) Software, Version 5.170
(V200R023C00)
FLASH         Version   : 0000
CARD1 information
Pcb           Version   : ES5D21X08T00 VER.C
CPLD          Version   : 010c
PWR1 information
Pcb           Version   : PWR VER.A
FAN1 information
Pcb           Version   : NA
<HUAWEI> display version
Huawei Versatile Routing Platform Software
VRP (R) software, Version 5.170 (S5735 V200R023C00)
Copyright (C) 2000-2020 HUAWEI TECH Co., Ltd.
HUAWEI S5735-S8P2X-IA200G1 Routing Switch uptime is 0 week, 0 day, 0 hour, 0 minute

ES5D2V10S005 0(Master)  : uptime is 0 week, 0 day, 0 hour, 0 minute
DDR             Memory Size : 1024  M bytes
FLASH Total     Memory Size : 512   M bytes
FLASH Available Memory Size : 303   M bytes
```



```
Pcb          Version   : VER.A
BootROM      Version   : 0000.03e8
BootLoad     Version   : 0213.0000
CPLD         Version   : 0100
MCU          Version   : 1.9.10.1
Software     Version   : VRP (R) Software, Version 5.170 (V200R023C00)
FLASH        Version   : 0000.0000
Power        Version   : 0555
```

Table 3-27 Description of the display version command output

Item	Description
Huawei Versatile Routing Platform Software	-
VRP (R) software, Version	Versions of the VRP and the software of the device.
Copyright (C) 2000-2020 HUAWEI TECH Co., Ltd.	Huawei copyright.
Routing Switch uptime	System power-on time.
ES5D2S50Q002 1(Master) : uptime	Hardware type, role, and startup time of the device. **NOTE** The names in the instance are taken as an example.
DDR Memory Size	Device's physical memory capacity, which stores data when the program is running. The **System Total Memory** field value displayed using the **display memory-usage** command is part of the physical memory capacity and varies depending on the device model.
FLASH Total Memory Size	Total size of the flash memory.
FLASH Available Memory Size	Available flash memory size. This value is the **total** field value displayed using the **dir** command divided by 1024.
Pcb Version	Version of the printed circuit board (PCB).
MAB Version	MAB version information.
BootROM Version	Version of the BootROM software.
BootLoad Version	Version of the BootLoad software.
CPLD Version	Version of the complex programmable logic device (CPLD).

Item	Description
MCU Version	Micro Control Unit (MCU) version. **NOTE** The information is displayed only for the S5720I-6X-PWH-SI-AC, S5720I-10X-PWH-SI-AC, S5720-16X-PWH-LI-AC, S5720-28X-PWH-LI-AC, and the PoE devices of S5720I-SI, S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5735-S, S500, S5735S-S, S5735-S-I, S5731-H, S5731-S, S5731S-S, S5732-H, S5735S-H, and S5736-S.
Software Version	Versions of the VRP and the software of the device.
FLASH Version	Version of the flash memory.
Power Version	Firmware version of the power module. **NOTE** The information is displayed only for the PoE devices of S5735-S-I.
CARD1 information	Information about a front card. If no front card is available, this field is not displayed.
CARD2 information	Information about a rear card. If no rear card is available, this field is not displayed.
FAN1 information	Information about a pluggable fan module. If no pluggable fan module is available, this field is not displayed. If a pluggable fan module does not have an electronic label, its PCB version is displayed as NA.
PWR2 information	Information about a pluggable power module. If no pluggable power module is available, this field is not displayed. If a pluggable power module does not have an electronic label, its PCB version is displayed as NA.
RPS Version	RPS management software version. If the device does not support RPS, this information is not displayed.

3.2 Hardware Configuration Commands

3.2.1 Command Support

Commands provided in this section and all the parameters in the commands are supported by all switch models (except the S5731-L and S5731S-L), unless otherwise specified. For details, see specific commands.

3.2.2 assign resource-mode

Function

The **assign resource-mode** command configures the resource allocation mode of the device.

The **undo assign resource-mode** command restores the default resource allocation mode of the device.

By default, the resource allocation mode of the S5731-H, S5731S-H, S500, S5735-S, S300, S5735-L, S5735S-L, S5735-S-I, S5735S-L-M, S5735S-S, S5735-L-I, S5735-L1,S5735S-L1, S5732-H, S5731-S, S5731S-S, S6730-S, S6730S-S, S6730-H, S6730S-H, S6735-S, S6720-EI, and S6720S-EI is enhanced-arp.

NOTE

Only the S5731-H, S5731S-H, S5732-H, S5731-S, S5731S-S, S500, S5735-S, S300, S5735-L, S5735S-L, S5735-S-I, S5735S-L-M, S5735S-S, S5735-L-I, S5735-L1,S5735S-L1, S6730-S, S6730S-S, S6730-H, S6730S-H, S6735-S, S6720-EI, and S6720S-EI support this command.

Format

assign resource-mode { **enhanced-mac** | **enhanced-arp** | **enhanced-ipv4** | **ipv4-ipv6 6:1** | **super-arp** } [**slot** *slot-id* | **all**] (S6720-EI and S6720S-EI)

assign resource-mode { **enhanced-mac** | **enhanced-arp** | **enhanced-ipv4** | **super-arp** } [**slot** *slot-id* | **all**] (S6735-S)

assign resource-mode { **enhanced-arp** | **enhanced-sac** | **enhanced-sipfpm** | **eca** | **sac** } [**slot** *slot-id* | **all**] (S5731-H, S5731S-H, S5731-S, and S5731S-S)

assign resource-mode { **enhanced-arp** | **enhanced-sac** | **enhanced-sipfpm** | **sac** } [**slot** *slot-id* | **all**] (S6730-S, S6730S-S, and S5732-H)

assign resource-mode { **enhanced-mac** | **enhanced-arp** | **enhanced-fib** | **enhanced-sac** | **sac** | **enhanced-sipfpm** } [**slot** *slot-id* | **all**] (S6730-H and S6730S-H)

assign resource-mode { **enhanced-mac** | **enhanced-arp** } **global** (S500, S5735-S, S300, S5735-L, S5735S-L, S5735-S-I, S5735S-L-M, S5735S-S, S5735-L-I, S5735-L1,and S5735S-L1)

undo assign resource-mode global (S500, S5735-S, S300, S5735-L, S5735S-L, S5735-S-I, S5735S-L-M, S5735S-S, S5735-L-I, S5735-L1,and S5735S-L1)

undo assign resource-mode [**slot** *slot-id* | **all**]

Parameters

Parameter	Description	Value
enhanced-mac	Sets the resource allocation mode to enhanced-mac.	-

Parameter	Description	Value
enhanced-ipv4	Sets the resource allocation mode to enhanced-ipv4.	-
enhanced-ipv6	Sets the resource allocation mode to enhanced-ipv6.	-
enhanced-arp	Sets the resource allocation mode to enhanced-arp.	-
enhanced-fib	Sets the resource allocation mode to enhanced-fib.	-
enhanced-sac	Sets the resource allocation mode to enhanced-sac.	-
enhanced-sipfpm	Sets the resource allocation mode to enhanced-sipfpm.	-
ipv4-ipv6 6:1	Sets the resource allocation mode to ipv4-ipv6 6:1.	-
super-arp	Sets the resource allocation mode to super-arp.	-
eca	Sets the resource allocation mode to eca.	-
sac	Sets the resource allocation mode to sac.	-
slot *slot-id*	• Specifies a slot ID on a standalone switch where stacking is not enabled. • Specifies a stack ID in a stack.	In a stack, the value is an integer and must be set according to the configuration in the stack. On a standalone switch where stacking is not enabled, the default value is 0.
all	Configures a resource allocation mode for all devices that are present in slots.	-

Parameter	Description	Value
global	Configures the resource allocation mode of the system.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If a device's MAC address entries, FIB entries, or ARP entries are insufficient to meet service requirements, you can use this command to change the resource allocation mode so as to extend the entry space.

Precautions

- The configured resource allocation mode takes effect only after the configuration is saved and the device is restarted. To view the resource allocation modes that take effect currently and take effect after the device restarts, run the **display resource-mode configuration** command.
- The requirements for different entry spaces will change when service configuration is adjusted. In this case, you can change the resource allocation mode to meet the new service requirements. Subsequently, entry spaces in different resource allocation modes will change. Therefore, before changing the resource allocation mode, consider the benefit and loss that the new mode will bring.
- In versions earlier than V200R012C00, the resource allocation mode used by the device is recorded in only the flash memory but not the configuration file. In V200R012C00 and later versions, the resource allocation mode used by the device is recorded in both the flash memory and configuration file. If the resource allocation mode used by the device is not the default mode, and the **save** command is executed to save the configuration after the device is upgraded to V200R012C00 or later, the corresponding configuration is added to the configuration file.
- In a stack, member switches synchronize MAC addresses with each other. Therefore, the MAC address specifications of the stack are not the sum of MAC address specifications of multiple member switches.
  - If member switches have the same MAC address specifications, the MAC address specifications of the stack are those of any member switch.
  - If member switches have different MAC address specifications, when uplink and downlink traffic is forwarded by the same member switch, the MAC address specifications of the stack are those of the member switch. When uplink and downlink traffic is forwarded across member switches,

the MAC address specifications of the stack are those of the member switch with smaller MAC address specifications.

When the resource allocation mode of the following models is changed, the specifications of MAC, FIB, ARP, ND, or multicast entries will be modified.

Table 3-28 Number of entries supported in different resource allocation modes on the S5731-H and S5731S-H

Resource Allocation Mode	MAC	IPv4 FIB	IPv6 FIB	ARP	ND	Multicast IPv4	Multicast IPv6	Number of NAC Users
enhanced-arp	288K	512K(share)	64K(share)	128K(share)	64K(share)	16K(share)	16K(share)	10000
enhanced-sac	288K	512K(share)	64K(share)	128K(share)	64K(share)	16K(share)	16K(share)	10000
enhanced-sipfpm	288K	512K(share)	64K(share)	128K(share)	64K(share)	16K(share)	16K(share)	10000
eca	288K	512K(share)	64K(share)	128K(share)	64K(share)	16K(share)	16K(share)	10000
sac	288K	512K(share)	64K(share)	128K(share)	64K(share)	16K(share)	16K(share)	10000

NOTE

On the S5731-H and S5731S-H, when the resource allocation mode is set to **enhanced-sipfpm**, the specifications of MAC, FIB, ARP, ND, and multicast entries will not be modified, and NetStream aggregation flows cannot be configured.

Table 3-29 Number of entries supported in different resource allocation modes on the S5731-S and S5731-S-S

Resource Allocation Mode	MAC	IPv4 FIB	IPv6 FIB	ARP	ND	Multicast IPv4	Multicast IPv6	Number of NAC Users
enhanced-arp	64K	32K	8K	16K	8K	1K	1K	10000

Resource Allocation Mode	MAC	IPv4 FIB	IPv6 FIB	ARP	ND	Multicast IPv4	Multicast IPv6	Number of NAC Users
enhanced-sac	64K	32K	8K	16K	8K	1K	1K	10000
enhanced-sipfpm	64K	16K 32K	8K	16K	8K	1K	1K	10000
eca	64K	32K	8K	16K	8K	1K	1K	10000
sac	64K	32K	8K	16K	8K	1K	1K	10000

NOTE

On the S5731-S and S5731-S-S, when the resource allocation mode is set to **enhanced-sipfpm**, the specifications of MAC, FIB, ARP, ND, and multicast entries will not be modified, and NetStream aggregation flows cannot be configured.

Table 3-30 Number of entries supported in different resource allocation modes on the S5732-H

Resource Allocation Mode	MAC	IPv4 FIB	IPv6 FIB	ARP	ND	Multicast IPv4	Multicast IPv6	Number of NAC Users
enhanced-arp (default)	128K	192K (shared)	80K (shared)	140K (shared)	80K (shared)	64K-1 (shared)	4K	10000
sac	96K	192K (shared)	80K (shared)	96K (shared)	80K (shared)	64K-1 (shared)	4K	10000
enhanced-sac	96K	64K(Share)	24K(Share)	96K(Share)	80K(Share)	20(Share)	4K	10000

Resource Allocation Mode	MAC	IPv4 FIB	IPv6 FIB	ARP	ND	Multicast IPv4	Multicast IPv6	Number of NAC Users
enhanced-sipfpm	32K	128K(Share)	64K(Share)	128K(Share)	64K(Share)	4K(Share)	4K	10000

NOTE

On the S5732-H, IPv4 FIB, IPv6 FIB, ARP, ND, and Multicast IPv4 share hardware resources. The specifications listed in the preceding table indicate the maximum number of entries of a single type and cannot reach the maximum value simultaneously.

Table 3-31 Number of entries supported in different resource allocation modes on the S500, S5735-S, and S5735S-S

Resource Allocation Mode	MAC	IPv4 FIB	IPv6 FIB	ARP	ND	Multicast IPv4	Multicast IPv6	Number of NAC Users
enhanced-arp(Default)	16512	8192	3072	8180(share)	3072(share)	1500(Share)	1500(Share)	N/A
enhanced-mac	32896(Share)	128	64	128(share)	64(share)	128	64(Share with Multicast Ipv4)	N/A

Table 3-32 Number of entries supported in different resource allocation modes on the S300, S5735-L, S5735S-L, S5735-S-I, S5735S-L-M, S5735-L-I, S5735-L1,and S5735S-L1

Resource Allocation Mode	MAC	IPv4 FIB	IPv6 FIB	ARP	ND	Multicast IPv4	Multicast IPv6	Number of NAC Users
enhanced-arp(Default)	16512	4096	1024	4096	1024	1500	1500	N/A
enhanced-mac	32896(Share)	128	64	128(share)	64(share)	128	64(Share with Multicast Ipv4)	N/A

Table 3-33 Number of entries supported in different resource allocation modes on the S6720-EI and S6720S-EI

Resource Allocation Mode	MAC	IPv4 FIB	IPv6 FIB (0-64 Bits Mask)	IPv6 FIB (Over 64 Bits Mask)	ARP	ND	Multicast IPv4 &IPv6	Number of NAC Users
enhanced-arp (default)	160K	12K	6K (shared with IPv4 FIB)	1K	48K	44K (shared with ARP)	4000	2K
enhanced-mac	288K	12K	6K (shared with IPv4 FIB)	1K	16K	8K (shared with ARP)	4000	2K
enhanced-ipv4	32K	256000	128K (shared with IPv4 FIB)	0K	16K	8K (shared with ARP)	4000	2K
ipv4-ipv6 6:1	32K	64K	10K	10K	16K	8K (shared with ARP)	4000	2K

Resource Allocation Mode	MAC	IPv4 FIB	IPv6 FIB (0-64 Bits Mask)	IPv6 FIB (Over 64 Bits Mask)	ARP	ND	Multicast IPv4 &IPv6	Number of NAC Users
super-arp	96K	12K	6K (shared with IPv4 FIB)	1K	128K	48K (shared with ARP)	4000	2K

NOTE

- On the S6720-EI and S6720S-EI, ARP and ND share hardware resources. The value listed in the preceding table indicates the maximum number of entries of a single type. Numbers of the two types of entries cannot reach the maximum value simultaneously.
- When the S6720-EI and S6720S-EI work in enhanced-arp, enhanced-mac, enhanced-ipv4, or super-arp mode, IPv4 FIB and IPv6 FIB (0-64 bits mask) share hardware resources. The value listed in the preceding table indicates the maximum number of FIB entries of a single type. Numbers of the two types of FIB entries cannot reach the maximum value simultaneously.
- When the S6720-EI and S6720S-EI work in ipv4-ipv6 6:1 mode, IPv6 FIB (0-64 bits mask) and IPv6 FIB (over 64 bits mask) share hardware resources. The value listed in the preceding table indicates the maximum number of FIB entries of a single type. Numbers of the two types of FIB entries cannot reach the maximum value simultaneously.
- On the S6720-EI and S6720S-EI, if the **assign resource-mode** command sets the resource allocation mode to enhanced-ipv4 or ipv4-ipv6 6:1, and the **ipv4 destination-unreachable drop** or **ipv6 destination-unreachable drop** command has been executed, the function that dropping the packets that do not match routing entries does not take effect.
- On the S6720-EI and S6720S-EI, redirection to a low-priority next hop is not supported in enhanced-ipv4 or ipv4-ipv6 6:1 resource allocation mode.
- On the S6720-EI and S6720S-EI, MPLS and Layer 3 VXLAN Gateway are not supported in super-arp resource allocation mode.

Table 3-34 Number of entries supported in different resource allocation modes on the S6735-S

Resource Allocation Mode	MAC	IPv4 FIB	IPv6 FIB (0-64 Bits Mask)	IPv6 FIB (Over 64 Bits Mask)	ARP	ND	Multicast IPv4 &IPv6	Number of NAC Users
enhanced-arp (default)	160K	12K	6K (shared with IPv4 FIB)	1K	48K	44K (shared with ARP)	4000	2K

Resource Allocation Mode	MAC	IPv4 FIB	IPv6 FIB (0-64 Bits Mask)	IPv6 FIB (Over 64 Bits Mask)	ARP	ND	Multicast IPv4 &IPv6	Number of NAC Users
enhanced-mac	288K	12K	6K (shared with IPv4 FIB)	1K	16K	8K (shared with ARP)	4000	2K
enhanced-ipv4	32K	256000	128K (shared with IPv4 FIB)	0K	16K	8K (shared with ARP)	4000	2K
super-arp	96K	12K	6K (shared with IPv4 FIB)	1K	128K	48K (shared with ARP)	4000	2K

NOTE

- On the S6735-S, ARP and ND share hardware resources. The value listed in the preceding table indicates the maximum number of entries of a single type. Numbers of the two types of entries cannot reach the maximum value simultaneously.
- When the S6735-S works in enhanced-arp, enhanced-mac, enhanced-ipv4, or super-arp mode, IPv4 FIB and IPv6 FIB (0-64 bits mask) share hardware resources. The value listed in the preceding table indicates the maximum number of FIB entries of a single type. Numbers of the two types of FIB entries cannot reach the maximum value simultaneously.
- On the S6735-S, if the **assign resource-mode** command sets the resource allocation mode to enhanced-ipv4, and the **ipv4 destination-unreachable drop** or **ipv6 destination-unreachable drop** command has been executed, the function that dropping the packets that do not match routing entries does not take effect.
- On the S6735-S, redirection to a low-priority next hop is not supported in enhanced-ipv4 resource allocation mode.
- On the S6735-S, MPLS and Layer 3 VXLAN Gateway are not supported in super-arp resource allocation mode.

Table 3-35 Number of entries supported in different resource allocation modes on the S6730-S and S6730S-S

Resource Allocation Mode	MAC	IPv4 FIB	IPv6 FIB	ARP	ND	Multicast IPv4	Multicast IPv6	Number of NAC Users
enhanced-arp(Default)	64K	64K	32K	64K	32K	4K	4K	N/A
enhanced-sac	64K	64K	32K	64K	32K	4K	4K	N/A
enhanced-sipfpm	64K	64K	32K	64K	32K	4K	4K	N/A

NOTE

On the S6730-S and S6730S-S, when the resource allocation mode is set to **sac**, **enhanced-sipfpm**, or **enhanced-sac**, the specifications of MAC, FIB, ARP, ND, and multicast entries will not be modified.

Table 3-36 Number of entries supported in different resource allocation modes on the S6730-H and S6730S-H

Resource Allocation Mode	MAC	IPv4 FIB	IPv6 FIB	ARP	ND	Multicast IPv4	Multicast IPv6	Number of NAC Users
enhanced-arp (default)	128K	192K (shared)	80K (shared)	140K (shared)	80K (shared)	64K-1 (shared)	4K	10000
enhanced-mac	384K	32K	8K	32K (shared with FIBv4)	8K (shared with FIBv6)	4K	4K	8K
enhanced-fib	32K	256K (shared)	80K (shared)	128K (shared)	80K (shared)	4K	4K	8K

Resource Allocation Mode	MAC	IPv4 FIB	IPv6 FIB	ARP	ND	Multicast IPv4	Multicast IPv6	Number of NAC Users
enhanced-sac	96K	148K(Share)	80K(Share)	96K(Share)	80K(Share)	64K-1(Share)	4K	10000
sac	96K	192K (shared)	80K (shared)	96K (shared)	80K (shared)	64K-1 (shared)	4K	10000
enhanced-sipfpm	32K	128K(Share)	64K(Share)	128K(Share)	64K(Share)	4K	4K	8K

NOTE

On the S6730-H and S6730S-H, the value listed in the preceding table indicates the maximum number of entries of a single type. Numbers of the two types of entries cannot reach the maximum value simultaneously. For example, ARP and FIBv4 share hardware resources, while ND and FIBv6 share hardware resources.

Example

Set the resource allocation mode to enhanced-ipv4.

```
<HUAWEI> system-view
[HUAWEI] assign resource-mode enhanced-ipv4
Info: It is executing, please wait...
Info: The resource mode in slot 0 has been set to enhanced-ipv4
successfully.
Warning: It will take effect after rebooting this device.
```

3.2.3 backup elabel

Function

The **backup elabel** command backs up electronic labels of the device to the flash memory. The default file name format is elabel-slot*slotid*.fls, for example, elabel-slot0.fls.

The **backup elabel ftp** command backs up electronic labels of the device to a specified FTP server.

The **backup elabel sftp** command backs up electronic labels of the device to a specified SFTP server.

Format

backup elabel [**slot** *slot-id* [*subcard-id*]]

backup elabel ftp *ftp-server-address filename username password* [**slot** *slot-id* [*subcard-id*]]

backup elabel sftp *sftp-server-address filename username password* [**slot** *slot-id* [*subcard-id*]]

Parameters

Parameter	Description	Value
ftp-server-address	Specifies the IP address of the FTP server that stores electronic labels.	The value is in dotted decimal notation.
sftp-server-address	Specifies the IP address of the SFTP server that stores electronic labels.	The value is in dotted decimal notation.
filename	Specifies the name of the file that stores electronic labels.	The value is a string of 5 to 28 case-sensitive characters without spaces, in the format of elabel-slot*slotid*.fls, for example, elabel-slot0.fls.
username	Specifies the user name used to log in to the FTP or SFTP server.	The value is a string of 1 to 64 case-sensitive characters without spaces.
password	Specifies the password used to log in to the FTP or SFTP server.	The value is a string of 1 to 16 case-sensitive characters without spaces.
slot *slot-id*	Specifies the slot ID.	The value must be set according to the device configuration.
subcard-id	Specifies the subcard ID.	The value must be set according to the device configuration.

Views

User view

Default Level

3: Management level

Usage Guidelines

When electronic labels are stored on a device, run the **backup elabel** command to save electronic labels to a file. This file can be saved to the flash memory, to the

FTP or SFTP server using FTP or SFTP. FTP cannot ensure secure file transfer. SFTP is recommended on networks that require high security.

Example

Save electronic labels of the device to the **elabel-slot0.fls** file in the flash memory.

```
<HUAWEI> backup elabel slot 0
Info: Output information to file: flash:/elabel-slot0.fls. Please wait for a mom
ent...

Info: Put file to flash successfully.
```

Save electronic labels of the device to FTP server 192.168.12.91. Set the FTP user name to **user** and password to **123**. Save electronic labels in the **elabel-slot0.fls** file.

```
<HUAWEI> backup elabel ftp 192.168.12.91 elabel-slot0.fls user 123
Warning: FTP is not a secure protocol, and it is recommended to use SFTP.
Info: It is executing, please wait...

Info: Put file to FTP server successfully.
```

Save electronic labels of the device to SFTP server 192.168.12.91. Set the SFTP user name to **client001** and password to YsHsjx_202206. Save electronic labels in the **elabel-slot0.fls** file.

```
<HUAWEI> backup elabel sftp 192.168.12.91 elabel-slot0.fls client001 YsHsjx_202206
Info: It is executing, please wait...

Info: Put file to SFTP server successfully.
```

3.2.4 cpu-usage monitor

Function

The **cpu-usage monitor** command enables the CPU usage monitoring.

The **undo cpu-usage monitor** command disables the monitoring function.

By default, the CPU usage monitoring is enabled.

Format

cpu-usage monitor [{ **slot** *slot-id* } | **slave**]

undo cpu-usage monitor [{ **slot** *slot-id* } | **slave**]

NOTE

Devices that do not support the stack function or do not have the stack function enabled do not support the **slave** parameter.

Parameters

Parameter	Description	Value
slot *slot-id*	Specifies a slot ID.	The value depends on the device configuration.
slave	Indicates information about the CPU usage of the slave device. This Parameter is invalid.	-

Views

System view

Default Level

3: Management level

Usage Guidelines

If you want to check the status and performance of the device, run the **cpu-usage monitor** command to enable the CPU usage monitoring, and then run the **display cpu-usage** command to check information about the CPU usage.

Example

Enable the CPU usage monitoring.

```
<HUAWEI> system-view
[HUAWEI] cpu-usage monitor
```

3.2.5 cpu-usage threshold

Function

Using the **cpu-usage threshold** command, you can set the alarm threshold and alarm recovery threshold of CPU usage.

Using the **undo cpu-usage threshold** command, you can restore the alarm threshold and alarm recovery threshold of CPU usage.

By default, the alarm threshold of CPU usage is 95% and alarm recovery threshold is 80%.

Format

cpu-usage threshold *threshold-value* [**restore** *restore-threshold-value*] [**slot** *slot-id*]

undo cpu-usage threshold [*threshold-value* [**restore** [*restore-threshold-value*]]] [**slot** *slot-id*]

Parameters

Parameter	Description	Value
threshold *threshold-value*	Specifies the alarm threshold of CPU usage.	The value is an integer that ranges from 2 to 100. The default value is 95.
restore *restore-threshold-value*	Specifies the alarm recovery threshold of CPU usage.	The value is an integer that ranges from 1 to 99. The alarm recovery threshold must be smaller than the alarm threshold.
slot *slot-id*	Specifies a slot ID.	The value depends on the device configuration.

Views

System view

Default Level

3: Management level

Usage Guidelines

When the CPU usage exceeds the alarm threshold, a log is recorded. When the CPU usage reduces by equal to or smaller than 5% and exceeds the threshold again, no log is recorded. A log is recorded only when the CPU usage is reduced by greater than 5% and reaches the threshold again. Through log information, you can know the CPU usage more conveniently.

If **slot** *slot-id* is not configured, the alarm threshold and alarm recovery threshold of CPU usage are set. In addition, the system automatically synchronizes the threshold on the master switch with those on the member switches.

Example

Set the alarm threshold of CPU usage to 85% and alarm recovery threshold to 70% of the switch.

```
<HUAWEI> system-view
[HUAWEI] cpu-usage threshold 85 restore 70
```

3.2.6 clear battery-group esmu communication-failure

Function

The **clear battery-group esmu communication-failure** command clears alarms indicating that a battery module fails to communicate with its connected ESMUs.

NOTE

Only the S5735-S8P2X-IA200H1 supports this command.

Format

clear battery-group esmu communication-failure

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

An Energy Storage System Management Unit (ESMU) is a unit for monitoring lithium batteries. You can run this command to clear alarms indicating that a battery module fails to communicate with its connected ESMUs.

Example

Clear alarms indicating that a battery module fails to communicate with its connected ESMUs.

```
<HUAWEI> system-view
[HUAWEI] clear battery-group esmu communication-failure
```

3.2.7 clear battery-group module-missing alarm

Function

The **clear battery-group module-missing alarm** command clears alarms indicating that a lithium battery group module is lost.

NOTE

Only the S5735-S8P2X-IA200H1 supports this command.

Format

clear battery-group module-missing alarm

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

You can run this command to clear alarms indicating that a lithium battery group module is lost.

Example

Clear alarms indicating that a lithium battery group module is lost.

```
<HUAWEI> system-view
[HUAWEI] clear battery-group module-missing alarm
```

3.2.8 display device dc-output information

Function

The **display device dc-output information** command displays detailed information about DC output on the switch.

NOTE

Only the S5720I-10X-PWH-SI-AC supports this command.

Format

display device dc-output information

Parameters

None.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

When PDs require DC power supply, run the **display device dc-output information** command to view information about the switch output voltage, current, and power and determine whether the switch meets power supply requirements of PDs.

Example

Display detailed information about DC output on the switch.

```
<HUAWEI> display device dc-output information
-------------------------------------------------------
Output Line    Voltage(V)   Current(mA)   Power(mW)
-------------------------------------------------------
12V            12           147           1762
24V            24           0             0
-------------------------------------------------------
```

Table 3-37 Description of the **display device dc-output information** command output

Item	Description
Output Line	DC output line: • 12V: 12 V output line • 24V: 24 V output line
Voltage(V)	DC output voltage, in volts (V).
Current(mA)	DC output current, in milliamperes (mA).
Power(mW)	DC output power, in milliwatts (mW).

3.2.9 display device ac-output status

Function

The **display device ac-output status** command displays AC output status of the switch.

NOTE

Only the S5735-S8P2X-IA200H1, S5720I-6X-PWH-SI-AC, S5735-S4T2X-IA150G1, and S5735-S8P2X-IA200G1 support this command.

Format

display device ac-output status

Parameters

None.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

When PDs require AC power supply, check whether the AC output function has been enabled on the switch based on the device AC output status displayed using the **display device ac-output status** command.

Example

Display AC output status of the Switch.

```
<HUAWEI> display device ac-output status
-------------------------------------------------------
OutputLine      ConfiguredState      PowerStatus
-------------------------------------------------------
 24V            Enable               On
-------------------------------------------------------
```

Table 3-38 Description of the **display device ac-output status** command output

Item	Description
OutputLine	AC output line. 24V: 24 V AC output line.
ConfiguredState	AC output configuration: • Enable: AC output is enabled. • Disable: AC output is disabled. To enable AC output, run the **set device ac-output 24v enable** command.
PowerStatus	AC output power status: • On: Power is being supplied. • Off: No power is supplied.

3.2.10 display device dc-output status

Function

The **display device dc-output status** command displays DC output status of the switch.

NOTE

Only the S5720I-10X-PWH-SI-AC supports this command.

Format

display device dc-output status

Parameters

None.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

When PDs require DC power supply, check whether the DC output function has been enabled on the switch based on the device DC output status displayed using the **display device dc-output status** command.

Example

Display DC output status of the Switch.

```
<HUAWEI> display device dc-output status
-------------------------------------------------------
OutputLine       ConfiguredState       PowerStatus
-------------------------------------------------------
12V-line1        Enable                On
12V-line2        Disable               Off
24V              Disable               Off
-------------------------------------------------------
```

Table 3-39 Description of the **display device dc-output status** command output

Item	Description
OutputLine	DC output line: ● 12V-line1: 12 V line 1 DC output line ● 12V-line2: 12 V line 2 DC output line ● 24V: 24 V DC output line
ConfiguredState	DC output configuration: ● Enable: DC output is enabled. ● Disable: DC output is disabled. To enable DC output, run the **set device dc-output enable** command.
PowerStatus	DC output power status: ● On: Power is being supplied. ● Off: No power is supplied.

3.2.11 display device fault-light

Function

The **display device fault-light** command displays status of fault indicator on a device.

Format

display device fault-light

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After using the **display device fault-light** command to check the fault indicator status, you can determine whether to set the fault indicator on a device to indicate that the device is faulty using the **set device fault-light** command.

Example

Display the fault indicator status.

```
<HUAWEI> display device fault-light
-------------------------------------------------------------
Slot      Status      Keeptime(s)
-------------------------------------------------------------
0         UnderRepair    45
-------------------------------------------------------------
```

Table 3-40 Description of the display device fault-light command output

Item	Description
Slot	Slot ID.
Status	Status of the fault indicator. • Normal: Indicate that the device is running normally. • UnderRepair: Indicate that the device is faulty.

Item	Description
Keeptime(s)	Time during which the fault indicator indicates that the device is faulty. When the **Status** displays **Normal**, the value displays "--".

3.2.12 display fan speed-adjust threshold minus

Function

The **display fan speed-adjust threshold minus** command displays the temperature thresholds for fan speed adjustment.

Format

display fan speed-adjust threshold minus [**slot** *slot-id*]

NOTE

The following switches do not support this command:

- S2730S-S series
- S5720-LI series: S5720-12TP-LI-AC, S5720-12TP-PWR-LI-AC, S5720-28P-LI-AC, S5720-28TP-LI-AC, S5720-28TP-PWR-LI-AC, S5720-28X-LI-AC, S5720-28X-LI-DC, and S5720-16X-PWH-LI-AC
- S5735-L, S5735S-L, S5735-L1, S5735S-L1, and S5735S-L-M series: S5735-L12T4S-A, S5735-L24T4S-A, S5735-L24T4S-A1, S5735S-L24T4S-MA, S5735S-L24FT4S-A, S5735S-L12T4S-A, S5735S-L24T4S-A1, S5735-L8T4S-QA1, S5735-L24T4X-QA1, S5735-L24T4S-QA1, and S5735S-L24T4S-A
- S5720S-LI series: S5720S-12TP-LI-AC, S5720S-12TP-PWR-LI-AC, S5720S-28P-LI-AC, S5720SV2-28P-LI-AC, S5720S-28TP-PWR-LI-AC, and S5720S-28X-LI-AC
- S5720I-SI series: S5720I-6X-PWH-SI-AC, S5720I-10X-PWH-SI-AC, S5720I-12X-SI-AC, and S5720I-12X-PWH-SI-DC
- S5735-S-I series
- S5731-H series, S5731S-H series, S5731-S series, S5731S-S series, S5732-H series
- S6730-H series, S6730S-H series, S6730-S series, S6730S-S series
- S6735-S

If one of the preceding switches can set up a stack with other switch models that support this command, this switch also supports this command so that this command can be executed and delivered in the stack.

Parameters

Parameter	Description	Value
slot *slot-id*	Specifies a slot ID. If this parameter is not specified, the threshold settings in all slots are displayed.	The value depends on the device configuration.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

This command displays the temperature thresholds for fan speed adjustment, including the default values and current values.

In some situations, the higher the device temperature, the slower the fan speed may be. This is because the device temperature range when the fan speed increases overlaps with that when the fan speed decreases.

For example, if the threshold for fan speed adjustment is as follows:

- When the fan speed is 55%, the device temperature may be lower than or equal to 60°C.
- When the fan speed is 60%, the device temperature may be in the range from 55°C to 60°C.
- When the fan speed is 65%, the device temperature may be in the range from 56°C to 58°C.
- When the fan speed is 70%, the device temperature may be in the range from 54°C to 56°C.
- When the fan speed is 80%, the device temperature may be in the range from 52°C to 56°C.
- When the fan speed is 90%, the device temperature may be in the range from 53°C to 56°C.
- When the fan speed is 100%, the device temperature may be higher than 54°C.

The fan speed remains at 55% before the device temperature reaches 60°C from the startup temperature. If the temperature exceeds 60°C, the fan speed increases to 60%.

- If the temperature decreases to a value between 55°C and 60°C, the fan speed remains at 60%. If the temperature decreases to lower than 55°C, the fan speed reduces to 55% accordingly.

- If the temperature is still higher than 60°C, the fan speed increases to 65%.

The same rule applies to other temperatures.

Example

Display the temperature thresholds for fan speed adjustment.

```
<HUAWEI> display fan speed-adjust threshold minus
-------------------------------------------------------------
 Slot     Default Range  Current Range  Speed Rate Adjusted
-------------------------------------------------------------
 0         NA - 56        NA - 56        35%
           53 - 58        53 - 58        40%
           55 - 58        55 - 58        45%
           55 - 58        55 - 58        50%
           52 - 57        52 - 57        60%
           54 - 56        54 - 56        70%
           54 - 57        54 - 57        80%
           55 - 58        55 - 58        90%
           56 - NA        56 - NA        100%
```

Table 3-41 Description of the **display fan speed-adjust threshold minus** command output

Item	Description
Slot	Slot ID.
Default Range	Default temperature thresholds, which change based on the PoE power load.
Current Range	Current temperature thresholds. To set temperature thresholds, run the **set fan speed-adjust threshold minus** command. The new thresholds are the fixed temperature thresholds minus the configured value. After this command is executed, both the threshold for increasing the fan speed and the threshold for lowering the fan speed are reduced.
Speed Rate Adjusted	Fan speed adjustment range.

3.2.13 display flash threshold

Function

The **display flash threshold** command displays the alarm threshold for flash memory usage.

Format

display flash threshold

Parameters

None

Views

All views

Default Level

3: Management level

Usage Guidelines

To view the configured alarm threshold for flash memory usage, run the **display flash threshold** command.

Example

Display the alarm threshold for flash memory usage.

```
<HUAWEI> display flash threshold
Info: The current flash usage threshold is 80%.
```

3.2.14 display otdr capture history-record interface

Function

The **display otdr capture history-record interface** command displays historical Optical Time Domain Reflectometer (OTDR) test results on an interface.

Format

display otdr capture history-record interface *interface-type interface-number*

Parameters

Parameter	Description	Value
interface-type interface-number	Specifies the type and number of an interface.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After running the **otdr capture interface** command to perform an OTDR test on a specified interface, you can run the **display otdr capture history-record interface** command to view historical OTDR test results on the interface. Each test result displays reflection distances of 16 optical fibres, and the command output can display the latest 10 OTDR test results at most. If the reflection distance of an optical fiber is 0, the optical module connected to the optical fiber does not support OTDR testing.

After the device is restored to factory settings or the **reset otdr capture history-record** command is executed, historical OTDR test results are cleared and cannot be queried by running the **display otdr capture history-record interface** command.

Example

Display historical OTDR test results on GE0/0/1.

```
<HUAWEI> display otdr capture history-record interface gigabitethernet 0/0/1
-------------------------------------------------------------------------------------------------------
Index     Reflections Distance(m)                                                 Time
-------------------------------------------------------------------------------------------------------
 0        2027        0     0     0     0     0     0     0     2019-12-31
14:34:03
                     0     0     0     0     0     0     0     0
 1        2021        0     0     0     0     0     0     0     2019-12-26
20:14:05
                     0     0     0     0     0     0     0     0
 2        2019        0     0     0     0     0     0     0     2019-12-26
20:14:04
                     0     0     0     0     0     0     0     0
 3        2021        0     0     0     0     0     0     0     2019-12-26
20:14:03
                     0     0     0     0     0     0     0     0
 4        2021        0     0     0     0     0     0     0     2019-12-25
20:14:03
                     0     0     0     0     0     0     0     0
 5        2021        0     0     0     0     0     0     0     2019-12-24
17:15:08
                     0     0     0     0     0     0     0     0
 6        2021        0     0     0     0     0     0     0     2019-12-24
15:26:08
                     0     0     0     0     0     0     0     0
 7        2021        0     0     0     0     0     0     0     2019-12-23
11:22:38
                     0     0     0     0     0     0     0     0
 8        2021        0     0     0     0     0     0     0     2019-12-23
10:46:55
                     0     0     0     0     0     0     0     0
 9        2021        0     0     0     0     0     0     0     2019-12-23
09:33:48
                     0     0     0     0     0     0     0     0
```

Table 3-42 Description of the **display otdr capture history-record interface** command output

Item	Description
Index	Sequence number of an OTDR test result.

Item	Description
Reflections Distance(m)	Reflection distance, in meters.
Time	Time when an OTDR test is performed.

3.2.15 display otdr certificate interface

Function

The **display otdr certificate interface** command displays the OTDR test result which is configured as the OTDR birth certificate on an interface.

Format

display otdr certificate interface *interface-type interface-number*

Parameters

Parameter	Description	Value
interface-type interface-number	Specifies the type and number of an interface.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After you run the **otdr certificate interface** command to configure an OTDR test result as the OTDR birth certificate for an interface, you can run the **display otdr certificate interface** command to view the OTDR birth certificate.

After the device is restored to factory settings or the **reset otdr certificate** command is executed, OTDR birth certificates of interfaces are cleared and cannot be queried using the **display otdr certificate interface** command.

Example

Display the OTDR birth certificate on GE0/0/1.

```
<HUAWEI> display otdr certificate interface gigabitethernet 0/0/1
-------------------------------------------------------------------------------
Reflections     Distance(m)                                 Time
-------------------------------------------------------------------------------
```



```
    2021      0      0      0      0      0      0      0          2019-12-31
14:34:03
      0      0      0      0      0      0      0      0
```

Table 3-43 Description of the **display otdr certificate interface** command output

Item	Description
Reflections Distance(m)	Reflection distance, in meters.
Time	Time when an OTDR test is performed.

3.2.16 display resource-mode configuration

Function

The **display resource-mode configuration** command displays the resource allocation mode configuration on the device.

NOTE

Only the S5731-H, S5731S-H, S5732-H, S5731-S, S5731S-S, S500, S5735-S, S300, S5735-L, S5735S-L, S5735-S-I, S5735S-L-M, S5735S-S, S5735-L-I, S5735-L1,S5735S-L1, S6730-S, S6730S-S, S6730-H, S6730S-H, S6735-S, S6720-EI, and S6720S-EI support this command.

Format

display resource-mode configuration

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Before configuring or modifying the resource allocation mode, run the **display resource-mode configuration** command to check the resource allocation mode configuration.

Example

Display the resource allocation mode.


```
<HUAWEI> display resource-mode configuration
Slot      Current Mode    Next Mode
- - - - - - - - - - - - - - - - - - - - - - - -
0         enhanced-mac    enhanced-mac
```

Table 3-44 Description of the display resource-mode configuration command output

Item	Description
Slot	Slot ID.
Current Mode	Current resource allocation mode.
Next Mode	Resource allocation mode configured using the **assign resource-mode** command. **NOTE** If the Next Mode is different from the Current Mode, the device is not restarted after the resource allocation mode is modified.

3.2.17 display root-key configuration

Function

The **display root-key configuration** command displays information about the currently used root key.

Format

display root-key configuration

Parameters

None

Views

User view

Default Level

3: Management level

Usage Guidelines

You can use the **display root-key configuration** command to check information about the currently used root key.

Example

Display information about the currently used root key.


```
<HUAWEI> display root-key configuration
Master:
  Current root-key:  User-configured
  Next root-key:     System default
```

Table 3-45 Description of the **display root-key configuration** command output

Item	Specification
Current root-key	Information about the currently used root key: • User-configured: user-configured root key • System default: system default root key
Next root-key	Information about the root key used after the device restarts: • User-configured: user-configured root key • System default: system default root key To set the root key, run the **set root-key** command.

3.2.18 display service-mode configuration

Function

The **display service-mode configuration** command displays the working mode of the device.

NOTE

This command is supported only by S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S.

Format

display service-mode configuration

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

To view the working mode of the device, run the **display service-mode configuration** command.

Example

Display the working mode of the device.

```
<HUAWEI> display service-mode configuration
Service mode status: Normal
```

Display the working mode of the S6730-H.

```
<HUAWEI> display service-mode configuration
Service mode status: BFD-enhanced, OAM-normal, PTP-normal
```

Table 3-46 Description of the **display service-mode configuration** command output

Item	Description
Service mode status	Working mode of the device: • Normal • Enhanced • BFD-normal • BFD-enhanced • OAM-normal • OAM-enhanced • PTP-normal • PTP-enhanced To set the working mode, run the **set service-mode** command.

3.2.19 display switchover state

Function

The **display switchover state** command displays information about active/standby switchover, which helps check whether the stack meets switchover requirements.

Format

display switchover state

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

In a stack containing multiple switches, you can run the **display switchover state** command to view the status of master and standby switches to determine whether to perform an active/standby switchover. When performing active/standby switchover, ensure that the standby switch is in real-time backup state.

Example

Display information about active/standby switchover, which helps check whether the stack meets switchover requirements.

```
<HUAWEI> display switchover state
Slot 1 HA FSM State(master): waiting for the slave to be inserted.
```

Table 3-47 Description of the display switchover state command output

Item	Description
HA FSM State(master)	Master switch status: • The slave has been inserted: The slave switch has been inserted. • waiting for the slave to be inserted: The master switch is waiting for the slave switch to be inserted. • waiting the batch backup request from the slave: The master switch is waiting for the batch backup request from the slave switch. • batch global data: Backup global data in batch • batch backup: Backup data in batch • batch check: Check the backup data in batch • realtime or routine backup: Backup data periodically or promptly • data smooth: Synchronize data

Item	Description
HA FSM State(slave)	Standby switch status: • ready: The standby switch is started and ready for receiving the batch backup data. • receiving batch data: The standby switch is receiving the batch backup data. • receiving realtime or routine data: The standby switch is ready for receiving data in real time.

3.2.20 display system resource-template

Function

The **display system resource-template** command displays system resource template information.

NOTE

Only the S1720GW-E, S1720GWR-E, S5720I-SI, S5720-LI, S5720S-LI, S6735-S, S5735S-H, S5736-S, and S6720S-S support this command.

Format

display system resource-template [**slot** *slot-id*]

Parameters

Parameter	Description	Value
slot *slot-id*	• Specifies a slot ID on a standalone device. • Specifies the stack ID in a stack.	The value is an integer. In a stack, the value must be set according to the device configuration. On a standalone device, the default value is 0.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display system resource-template** command to view system resource template information, including the resource type, currently running resource template information and resource template for the next startup.

Example

Display information about the system resource template. For example, the S5720-LI.

```
<HUAWEI> display system resource-template
Resource Template Information:
-------------------------------------------------------------
 Slot    Type        RunningTemplate     NextTemplate
-------------------------------------------------------------
 0       acl-mode    dual-ipv4-ipv6      dual-ipv4-ipv6
-------------------------------------------------------------
```

Table 3-48 Description of the **display system resource-template** command output

Item	Description
Slot	Slot ID.
Type	Resource type. Currently, only one system resource template (acl-mode) is supported.
RunningTemplate	Currently running resource template information. To configure a resource template, run the **assign resource-template acl-mode** command.
NextTemplate	Resource template for the next startup.

3.2.21 display wavelength-map

Function

The **display wavelength-map** command displays the mapping between the wavelength channel, wavelength, and frequency.

Format

display wavelength-map

Parameters

None

Views

System view

Default Level

1: Monitoring level

Usage Guidelines

Before using the **wavelength-channel** command to add an optical module to a specific wavelength channel, run the **display wavelength-map** command to view the mapping between the wavelength channel, wavelength, and frequency.

Example

Display the mapping between the wavelength channel, wavelength, and frequency.

```
<HUAWEI> system-view
[HUAWEI] display wavelength-map
-----------------------------------------------
Channel     Frequency(THz)   Wavelength(nm)
-----------------------------------------------
1           192.10           1560.606
2           192.15           1560.200
3           192.20           1559.794
4           192.25           1559.389
5           192.30           1558.983
6           192.35           1558.578
7           192.40           1558.173
8           192.45           1557.768
9           192.50           1557.363
10          192.55           1556.959
11          192.60           1556.555
12          192.65           1556.151
13          192.70           1555.747
14          192.75           1555.344
15          192.80           1554.940
16          192.85           1554.537
17          192.90           1554.134
18          192.95           1553.731
19          193.00           1553.329
20          193.05           1552.927
21          193.10           1552.524
22          193.15           1552.122
23          193.20           1551.721
24          193.25           1551.319
25          193.30           1550.918
26          193.35           1550.517
27          193.40           1550.116
28          193.45           1549.715
29          193.50           1549.315
30          193.55           1548.915
31          193.60           1548.515
32          193.65           1548.115
33          193.70           1547.715
34          193.75           1547.316
35          193.80           1546.917
36          193.85           1546.518
37          193.90           1546.119
38          193.95           1545.720
39          194.00           1545.322
40          194.05           1544.924
```



```
41          194.10          1544.526
42          194.15          1544.128
43          194.20          1543.730
44          194.25          1543.333
45          194.30          1542.936
46          194.35          1542.539
47          194.40          1542.142
48          194.45          1541.746
49          194.50          1541.349
50          194.55          1540.953
51          194.60          1540.557
52          194.65          1540.162
53          194.70          1539.766
54          194.75          1539.371
55          194.80          1538.976
56          194.85          1538.581
57          194.90          1538.186
58          194.95          1537.792
59          195.00          1537.397
60          195.05          1537.003
61          195.10          1536.609
62          195.15          1536.216
63          195.20          1535.822
64          195.25          1535.429
65          195.30          1535.036
66          195.35          1534.643
67          195.40          1534.250
68          195.45          1533.858
69          195.50          1533.465
70          195.55          1533.073
71          195.60          1532.681
72          195.65          1532.290
73          195.70          1531.898
74          195.75          1531.507
75          195.80          1531.116
76          195.85          1530.725
77          195.90          1530.334
78          195.95          1529.944
79          196.00          1529.553
80          196.05          1529.163
--------------------------------------------
```

Table 3-49 Description of the **display wavelength-map** command output

Item	Description
Channel	Channel ID.
Frequency(THz)	Frequency, in THz.
Wavelength(nm)	Wavelength, in nm.

3.2.22 mib-data optical-module sample-interval

Function

The **mib-data optical-module sample-interval** command sets the sampling interval for optical module information in the MIB performance module.

The **undo mib-data optical-module sample-interval** command restores the default setting.

By default, the interval is 30 seconds.

Format

mib-data optical-module sample-interval *interval-value*

undo mib-data optical-module sample-interval

Parameters

Parameter	Description	Value
interval-value	Specifies a sampling interval for optical module information in the MIB performance module.	The value is an integer in the range from 10 to 300, in seconds.

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

It takes a long time for the NMS to query real-time optical module information on a device using hwOpticalModuleInfoTable in the MIB, especially when the device has a large number of optical modules installed. To solve this problem, you can configure devices to periodically sample optical module information. Then, the NMS can directly obtain sampling information about optical modules, which improves efficiency.

Precautions

- When you run the **mib-data optical-module sample-interval** command multiple times, only the latest configuration takes effect.
- The shorter the sampling interval, the higher the CPU usage.

Example

Set the sampling interval of optical module information in the MIB performance module to 35 seconds.

```
<HUAWEI> system-view
[HUAWEI] mib-data optical-module sample-interval 35
```


3.2.23 otdr capture interface

Function

The **otdr capture interface** command triggers an optical time domain reflectometer (OTDR) test on an interface.

Format

otdr capture interface *interface-type interface-number*

Parameters

Parameter	Description	Value
interface-type interface-number	Specifies the type and number of an interface.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

To perform an OTDR test to obtain reflection distances of optical fibers, run the **otdr capture interface** command. The reflection distances are used for fiber fault diagnosis. To query historical OTDR test results, run the **display otdr capture history-record interface** command.

To ensure that historical OTDR test results are not lost after the device is restarted, historical OTDR test results are recorded in the **flash:/otdr_capture.bin** file. This file is set as a system file and cannot be deleted. To clear historical OTDR test results, you need to run the **reset otdr capture history-record** command. After the **reset otdr capture history-record** command is executed and the device is restarted, historical OTDR test results are cleared and cannot be queried by running the **display otdr capture history-record interface** command.

Precautions

- The command can be run multiple times.
- This command can be configured only when a specific optical module is installed on an interface. For details about the optical module, contact Huawei technical support.

Example

Trigger an OTDR test on GE0/0/1.


```
<HUAWEI> otdr capture interface gigabitethernet 0/0/1
```

3.2.24 otdr certificate interface

Function

The **otdr certificate interface** command configures an OTDR test result as the OTDR birth certificate on an interface.

Format

otdr certificate interface *interface-type interface-number capture-number*

Parameters

Parameter	Description	Value
interface-type interface-number	Specifies the type and number of an interface.	-
capture-number	Specifies the sequence number of an OTDR test result.	The value is an integer ranging from 0 to 9.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

To configure an OTDR test result as the OTDR birth certificate, run the **otdr certificate interface** command. The OTDR birth certificate is used as a baseline for fault detection. You can run the **display otdr certificate interface** command to view the OTDR birth certificate. By comparing the fiber reflection distances in OTDR test results (in the **display otdr capture history-record interface** command output) and the OTDR birth certificate (in the **display otdr certificate interface** command output), you can determine whether a fault occurs on an optical fiber.

To ensure that birth certificates of interfaces are not lost after the device restarts, the birth certificates are recorded in the **flash:/otdr_certificate.bin** file. This file is set as a system file and cannot be deleted. To clear OTDR birth certificates of interfaces, you need to run the **reset otdr certificate** command. After the **reset otdr certificate** command is executed and the device is restarted, OTDR birth certificates of interfaces are cleared and cannot be queried by running the **display otdr certificate interface** command.

Precautions

- This command can be run multiple times, but the latest configuration takes effect.
- This command can be configured only when a specific optical module is installed on an interface. For details about the optical module, contact Huawei technical support.

Example

Configure the second OTDR test result as the OTDR birth certificate on GE0/0/1.

```
<HUAWEI> otdr certificate interface gigabitethernet 0/0/1 2
port_no=GigabitEthernet0/0/1
capture_no=2
```

3.2.25 reset battery esmu

Function

The **reset battery** command resets ESMUs that monitor a specific battery.

NOTE

Only the S5735-S8P2X-IA200H1 supports this command. This command takes effect only when the backup lithium battery is unavailable.

Format

reset battery *battery-id* **esmu**

Parameters

Parameter	Description	Value
battery-id	Specifies the battery number.	The value is an integer and must be set according to the device configuration.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

An ESMU is a unit for monitoring a lithium battery. You can run this command to reset ESMUs.

Example

Reset the ESMUs that monitor the battery whose number is 1.


```
<HUAWEI> system-view
[HUAWEI] reset battery 1 esmu
```

3.2.26 reset cpu-usage record

Function

The **reset cpu-usage record** command clears CPU usage records.

Format

reset cpu-usage record [**slot** *slot-id* | **slave** | **all**]

Parameters

Parameter	Description	Value
slot *slot-id*	Specifies the slot ID.	Set the value according to the device configuration.
slave	Clears CPU usage records on the slave switch.	-
all	Clears CPU usage records on all switches	-

Views

System view, User view

Default Level

3: Management level

Usage Guidelines

If the **slot** *slot-id* or **slave** parameter is not specified, CPU usage records of the master switch is cleared.

Example

Clear CPU usage records of the master switch.

```
<HUAWEI> system-view
[HUAWEI] reset cpu-usage record
Waiting for clearing . . . Done
```


3.2.27 reset integrated-power output

Function

The **reset integrated-power output** command resets the outputs of a PC510 power supply.

Format

reset integrated-power output

NOTE

This command is supported only by the S5735-L8P4X-IA1, S5735-L8T4X-IA1.

Parameters

None

Views

User view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After the switch is connected to a PC510 power supply through a network cable, the PC510 power supply can provide 12 V DC and 24 V AC outputs. When the power outputs are abnormal or the downstream devices of the switch need to be restarted, you can run this command on the switch to reset the PC510 power supply outputs.

Resetting the outputs of the PC510 power supply does not reset the output to the switch. Therefore, the switch does not restart.

Precautions

Before running this command, run the **set power protocol modbus** command on the switch to set up a connection with the PC510 power supply. If the connection fails to be set up, this command does not take effect.

Example

Reset the outputs of the PC510 power supply.

```
<HUAWEI> reset integrated-power output
```


3.2.28 reset power-detect status

Function

The **reset power-detect status** command restores the power supply to its factory defaults.

NOTE

Only the S5735-S8P2X-IA200H1 supports this command.

Format

reset power-detect status

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

You can run this command to restore the power supply to its factory defaults.

Example

Restore the power supply to its factory defaults.

```
<HUAWEI> system-view
[HUAWEI] reset power-detect status
```

3.2.29 reset otdr capture history-record

Function

The **reset otdr capture history-record** command clears historical OTDR test results on an interface.

Format

reset otdr capture history-record

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **otdr capture interface** command to obtain the fiber reflection distance for fiber fault diagnosis. You can run the **display otdr capture history-record interface** command to view historical OTDR test results.

To ensure that historical OTDR test results are not lost after the device is restarted, historical OTDR test results are recorded in the **flash:/otdr_capture.bin** file. This file is set as a system file and cannot be deleted. To clear historical OTDR test results, you need to run the **reset otdr capture history-record** command. After the **reset otdr capture history-record** command is executed and the device is restarted, historical OTDR test results are cleared and cannot be queried by running the **display otdr capture history-record interface** command.

Example

Clear historical OTDR test results on interfaces.

```
<HUAWEI> reset otdr capture history-record
```

3.2.30 reset otdr certificate

Function

The **reset otdr certificate** command clears the OTDR test results configured as birth certificates on interfaces.

Format

reset otdr certificate

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **otdr certificate interface** command to configure a historical OTDR test result as the OTDR birth certificate for an interface and run the **display**

otdr certificate interface command to view the OTDR birth certificate of an interface.

To ensure that birth certificates of interfaces are not lost after the device restarts, the birth certificates are recorded in the **flash:/otdr_certificate.bin** file. This file is set as a system file and cannot be deleted. To clear OTDR birth certificates of interfaces, you need to run the **reset otdr certificate** command. After the **reset otdr certificate** command is executed and the device is restarted, OTDR birth certificates of interfaces are cleared and cannot be queried by running the **display otdr certificate interface** command.

Example

Clear the OTDR test results used as birth certificates on interfaces.

```
<HUAWEI> reset otdr certificate
```

3.2.31 reset slot

Function

The **reset slot** command resets a device.

Format

reset slot *slot-id* [**cold**]

NOTE

Only the following devices support cold reset. Other devices that support the **cold** parameter do not support cold reset.

- S5735-S8P2X-IA200H1, S5735-L24P4S-A, S5735-L24P4S-A1, S5735S-L24P4S-A, S5735S-L24P4S-A1, S5735S-L24P4S-MA, S5735-L24P4X-A, S5735-L24P4X-A1, S5735S-L24P4X-A, S5735S-L24P4X-A1, S5735-S4T2X-IA150G1, S5735-S8P2X-IA200G1
- Devices that use a 300 W AC power module (PAC300S12-CL)
- Devices that use a 600 W AC power module (PAC600S12-CB, PAC600S12-EB, PAC600S12-DB, and PAC600S56-CB)
- Devices that use a 600 W AC PoE power module (PAC600S56-EB)
- Devices that use a 1000 W DC power module (PDC1000S12-DB)
- Devices that use a 1000 W DC Poe power module (PDC1000S56-CB and PDC1000S56-EB)
- Devices that use a 1000 W AC PoE power module (PAC1000S56-CB, PAC1000S56-EB, and PAC1000S56-DB)

The **cold** parameter is supported only in the user view.

Parameters

Parameter	Description	Value
slot-id	Specifies a slot ID.	The value must be set according to the device configuration.

Parameter	Description	Value
cold	Indicates cold reset.	-

Views

All views

Default Level

3: Management level

Usage Guidelines

Usage Scenario

In a stack, you can restart stack members. Restarting a stack member will interrupt services on this device, but the configuration of this device still exists.

Precautions

- Before commands have been executed, if a master/standby switchover occurs because the **reset slot** command is used to reset the master switch, you need to execute the commands that have not been executed on the new master switch again after the standby switch becomes the new master switch.
- For the S5735-S8P2X-IA200H1, after this command is run, the switch will not restart, but its output power supply will be reset.
- Due to the component upgrade of some device models, some devices cannot be downgraded. If the message "Error: The hardware version VER.B of slot %u does not support the configured system software package." (%u indicates the actual slot number) is displayed after the command is run, you can solve this problem by installing the patch that matches the version. For details about the first supported version of the device and matching patch version, see the device overview in the "Hardware Description"..

Example

Restart the switch with the slot ID 0.

```
<HUAWEI> reset slot 0
Warning: Confirm to reset slot 0? [Y/N]:y
Info: The board 0 is reset successfully.
```

Perform a cold reset on the switch with the slot ID 0.

```
<HUAWEI> reset slot 0 cold
Warning: The device in slot 0 will be cold reset. Ensure that the configuration has been saved. Otherwise, the configuration will be lost after cold restart. Continue? [Y/N]: y
Info: Succeeded in cold resetting the device in slot 0.
```


3.2.32 set battery-group

Function

The **set battery-group** command configures the float charging voltage or equalized charging voltage for the lithium battery group.

The **undo set battery-group** command restores the default float charging voltage or equalized charging voltage of the lithium battery group.

By default, the float charging voltage of the lithium battery group is 54.50 V, and the equalized charging voltage is 56.40 V.

NOTE

Only the S5735-S8P2X-IA200H1 supports this command.

Format

set battery-group { **equalized-charge-voltage** | **float-charge-voltage** } *value*

undo set battery-group { **equalized-charge-voltage** | **float-charge-voltage** }

Parameters

Parameter	Description	Value
equalized-charge-voltage	Configures the float charging voltage.	-
float-charge-voltage	Configures the equalized charging voltage.	-
value	Indicates the voltage value.	The value range is as follows: • **equalized-charge-voltage**: The value ranges from 43.20 to 56.40, in volts (V). • **float-charge-voltage**: The value ranges from 43.20 to 56.40, in volts (V). **NOTE** The equalized charging voltage must be greater than or equal to the float charging voltage.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

You can run this command to configure the float charging voltage or equalized charging voltage for the lithium battery group.

Example

Configure the float charging voltage of the lithium battery group to 55.11 V.

```
<HUAWEI> system-view
[HUAWEI] set battery-group equalized-charge-voltage 55.11
```

3.2.33 set battery-group charge current-limit

Function

The **set battery-group charge current-limit** command configures the charge current limiting coefficient for the lithium battery group.

The **undo set battery-group charge current-limit** command restores the default charge current limiting coefficient for the lithium battery group.

By default, the charge current limiting coefficient for the lithium battery group is 0.30.

NOTE

Only the S5735-S8P2X-IA200H1 supports this command.

Format

set battery-group charge current-limit *value*

undo set battery-group charge current-limit

Parameters

Parameter	Description	Value
value	Specifies the charge current limiting coefficient for the lithium battery group.	The value ranges from 0.05 to 1.00, in C10.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

You can run this command to configure the charge current limiting coefficient for the lithium battery group.

Example

Set the charge current limiting coefficient of the lithium battery group to 0.61.

```
<HUAWEI> system-view
[HUAWEI] set battery-group charge current-limit 0.61
```

3.2.34 set battery-group install date

Function

The **set battery-group install date** command sets the installation date of the lithium battery group.

The **undo set battery-group date** command restores the default installation date of the lithium battery group.

By default, the installation date of the lithium battery group is 2014-01-01.

NOTE

Only the S5735-S8P2X-IA200H1 supports this command.

Format

set battery-group install date *date-value*

undo set battery-group install date

Parameters

Parameter	Description	Value
date-value	Specifies the installation date of the lithium battery group.	The value is in YYYY-MM-DD format. It ranges from 2014-01-01 to 2037-12-31.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

You can run this command to record the installation date of the lithium battery group.

Example

Set the installation date of the lithium battery group to November 11, 2021.
<HUAWEI> **system-view**
[HUAWEI] **set battery-group install date 2021-11-11**

3.2.35 set device dc-output enable

Function

The **set device dc-output enable** command enables the DC output function on the switch.

The **undo set device dc-output enable** command disables the DC output function on the switch.

By default, the DC output function is enabled on a switch.

NOTE

Only the S5720I-10X-PWH-SI-AC supports this command.

Format

set device dc-output [**12V** [**line1** | **line2**] | **24V**] **enable**

undo set device dc-output [**12V** [**line1** | **line2**] | **24V**] **enable**

Parameters

Parameter	Description	Value
12V	Specifies the DC output voltage as 12 V.	-
line1	Configures DC output of 12 V line 1.	-
line2	Configures DC output of 12 V line 2.	-
24V	Specifies the DC output voltage as 24 V.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If PDs require DC power supply, enable DC output on the switch.

Precautions

If you run the **set device dc-output 12V** [**line1** | **line2**] **enable** command to enable the 12 V DC output function of the switch, and then run the **set device dc-output 24V enable** command to enable the 24 V DC output function of the switch, both the 12 V and 24 V DC output functions have been enabled on the switch. To determine the state of each DC output line, run the **display device dc-output status** command.

Example

Enable DC output of 12 V line 1 and set the DC output voltage to 12 V.

```
<HUAWEI> system-view
[HUAWEI] set device dc-output 12V line1 enable
Warning: The total PoE power and DC output power is 0mW, and the remaining power is 175000mW.
Continue? [Y/N]:Y
Warning: After the 12V line1 DC output is enabled, PoE power and DC output power may be disabled if the total PoE power and DC output power exceeds 175000mW. Continue? [Y/N]:Y
```

Enable DC output of all lines.

```
<HUAWEI> system-view
[HUAWEI] set device dc-output enable
Warning: The total PoE power and DC output power is 731mW, and the remaining power is 174269mW.
Continue? [Y/N]:Y
Warning: After all DC output is enabled, PoE power and DC output power may be disabled if the total PoE power and DC output power exceeds 175000mW. Continue? [Y/N]:Y
```

3.2.36 set device ac-output 24v enable

Function

The **set device ac-output 24v enable** command enables the 24 V AC output function on a switch.

The **undo set device ac-output 24v enable** command disables the 24 V AC output function on a switch.

By default, the 24 V AC output function is enabled on switches.

NOTE

Only the S5735-S8P2X-IA200H1, S5720I-6X-PWH-SI-AC, S5735-S4T2X-IA150G1, and S5735-S8P2X-IA200G1 support this command.

Format

set device ac-output 24v enable

undo set device ac-output 24v enable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If PDs require AC power supply, enable the AC output function on the switch.

Precautions

- For the S5720I-6X-PWH-SI-AC, when the sum of the PoE power, DC output power, and AC output power is greater than 150000 mW, the switch restarts.
- For the S5735-S4T2X-IA150G1 and S5735-S8P2X-IA200G1, when the sum of the PoE power, DC output power, and AC output power is greater than 160000 mW, the switch restarts.
- For the S5735-S8P2X-IA200H1, when the sum of the PoE power, DC output power, and AC output power is greater than 200000 mW, the switch restarts.

Example

Enable the 24 V AC output function on a switch.

```
<HUAWEI> system-view
[HUAWEI] set device ac-output 24v enable
Warning: After this command is excuted, the 24V AC output will be enabled. Continue? [Y/N]:y
Warning: After the 24V AC output is enabled, the switch will reboot if the total power of PoE power, DC output power and AC output power exceed 150000mW. Continue? [Y/N]:y
```

3.2.37 set device fault-light

Function

The **set device fault-light** command sets the fault indicator status on a device.

The **undo set device fault-light** command restores the default fault indicator status.

By default, the fault indicator status of the device is not set. The fault indicator status is displayed based on the current device running status.

Format

set device fault-light { **normal** | **under-repair** [**keeptime** *time*] } [**slot** *slot-id*]

undo set device fault-light [**slot** *slot-id*]

Parameters

Parameter	Description	Value
normal	Displays the fault indicator status based on the current device running status.	-
under-repair	Configures the fault indicator to indicate that the device is faulty.	-
keeptime *time*	Sets the time during which the fault indicator indicates that the device is faulty.	The value is an integer that ranges from 45 to 600, in seconds. The default value is 45.
slot *slot-id*	Specifies a slot ID. If not slot ID is specified in a stack, this command sets the fault indicator status of the stack master.	The value range depends on the device configuration.

Views

System view

Default Level

3: Management level

Usage Guidelines

If a switch is faulty, run the **set device fault-light** command to set the mode indicators or system indicator to the faulty state so that O&M personnel can find the faulty switch onsite.

- For the S500, S5735-S, S5735S-S, S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5731-H, S5731S-H, S5732-H, S5731-S, S5731S-S, S6730-H, S6730S-H, S6730-S, and S6730S-S

  When the **set device fault-light under-repair** command is executed, the ID indicator is steady blue and turns off after it is steady blue for the time specified by **keeptime** *time* (the default time is 45s if this parameter is not specified). The **set device fault-light normal** command and the **undo set device fault-light** command have the same functions. That is, after either of the two commands is executed, the ID indicator turns off.

- For the S5720I-6X-PWH-SI-AC and S5720I-10X-PWH-SI-AC

  The switch has only one fault indicator, WiFi indicator. When the **set device fault-light under-repair** command is executed, the WiFi indicator blinks red fast and turns off after it blinks red fast for the time specified by **keeptime**

time (the default time is 45s if this parameter is not specified). The **set device fault-light normal** and **undo set device fault-light** commands have the same functions. That is, after either of the two commands is executed, the WiFi indicator turns off.

- For the S5735-S-I

  The switch has only one fault indicator, SYS indicator. When the **set device fault-light under-repair** command is executed, the SYS indicator blinks red fast and returns to the previous state after it blinks red fast for the time specified by **keeptime** *time* (the default time is 45s if this parameter is not specified). The **set device fault-light normal** and **undo set device fault-light** commands have the same functions. That is, after either of the two commands is executed, the SYS indicator returns to the previous state.

- For other switches that support this command

  When the **set device fault-light under-repair** command is executed, the SYS indicator and mode indicators (STAT, SPED, PoE, and STCK) blink red fast. After these indicators blink red fast for the time specified by **keeptime** *time* (the default time is 45s if this parameter is not specified), the SYS indicator returns to the previous state, and the STAT indicator is steady on.

  The **set device fault-light normal** and **undo set device fault-light** commands have the same functions. That is, after either of the two commands is executed, the SYS indicator returns to the previous state, and the STAT indicator is steady on.

  If **slot** *slot-id* is not specified in a stack, the configuration takes effect on indicators on the master switch.

Example

Configure the fault indicator to indicate that the device is faulty.

```
<HUAWEI> system-view
[HUAWEI] set device fault-light under-repair
```

3.2.38 set fan speed auto min-speed

Function

The **set fan speed auto min-speed** command configures the minimum fan speed in automatic fan speed adjustment mode.

The **undo set fan speed auto min-speed** command restores the default minimum fan speed in automatic fan speed adjustment mode.

By default, the minimum fan speed in automatic fan speed adjustment mode is not configured.

NOTE

The following switches do not support this command:

- S2730S-S series
- S5720-LI series: S5720-12TP-LI-AC, S5720-12TP-PWR-LI-AC, S5720-28P-LI-AC, S5720-28TP-LI-AC, S5720-28TP-PWR-LI-AC, S5720-28X-LI-AC, S5720-28X-LI-DC, and S5720-16X-PWH-LI-AC
- S5735-L, S5735S-L, S5735-L1, S5735S-L1, and S5735S-L-M series: S5735-L12T4S-A, S5735-L24T4S-A, S5735-L24T4S-A1, S5735S-L24T4S-MA, S5735S-L24FT4S-A, S5735S-L12T4S-A, S5735S-L24T4S-A1, S5735-L8T4S-QA1, S5735-L24T4X-QA1, S5735-L24T4S-QA1, and S5735S-L24T4S-A
- S5720S-LI series: S5720S-12TP-LI-AC, S5720S-12TP-PWR-LI-AC, S5720S-28P-LI-AC, S5720SV2-28P-LI-AC, S5720S-28TP-PWR-LI-AC, and S5720S-28X-LI-AC
- S5720I-SI series: S5720I-6X-PWH-SI-AC, S5720I-10X-PWH-SI-AC, S5720I-12X-SI-AC, and S5720I-12X-PWH-SI-DC
- S5735-S-I series
- S5731-H series, S5731S-H series, S5731-S series, S5731S-S series, S5732-H series
- S6730-H series, S6730S-H series, S6730-S series, S6730S-S series
- S6735-S

If one of the preceding switches can set up a stack with other switch models that support this command, this switch also supports this command so that this command can be executed and delivered in the stack.

Format

set fan speed auto min-speed *value* [**slot** *slot-id* | **all**]

undo set fan speed auto min-speed [**slot** *slot-id* | **all**]

Parameters

Parameter	Description	Value
value	Sets the percentage of the minimum fan speed. For example, if this parameter is set to 35, the minimum fan speed in automatic fan speed adjustment mode is 35% of the full fan speed.	The value is an integer that ranges from 1 to 100.
slot *slot-id*	Specifies a slot ID. If this parameter is not specified, the minimum fan speed in automatic fan speed adjustment mode is configured for the fans on the master switch.	The value depends on the device configuration.
all	Specifies all slots.	-

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

The fan speed affects the device temperature. When the device temperature is high, increase the fan speed to lower the device temperature. When the device temperature is low, reduce the fan speed to save energy. A proper fan speed ensures stable device operation. By default, fans run in automatic fan speed adjustment mode. In this mode, the system adjusts the fan speed when detecting that the device temperature increases or decreases. To control the fan speed in a timely manner, run the **set fan speed auto min-speed** command to configure the minimum fan speed in automatic speed adjustment mode.

Precautions

- If the automatically calculated fan speed is lower than the configured minimum speed, the configured minimum speed takes effect. If the automatically calculated fan speed is greater than the configured minimum speed, the calculated fan speed takes effect. To obtain the minimum fan speed of a device, view the **Speed Rate Adjusted** field in the **display fan speed-adjust threshold minus** command output.
- To obtain the minimum fan speed in automatic fan speed adjustment mode on a device, view the **Auto Min-speed** field in the **display fan** command output.
- The following assumes that the device can set up a stack with other device models and has the minimum fan speed in automatic fan speed adjustment mode configured before the stack is set up. After the stack is set up, if this device functions as the master switch, the configured minimum fan speed still takes effect. If this device functions as the standby or slave switch, the configured minimum fan speed does not take effect.
- This configuration takes effect only when fan modules work in automatic speed adjustment mode. You can check the **Mode** field in the **display fan** command output to check the fan speed adjustment mode. If a fan module works at a fixed speed, run the **fan speed mandatory** command in the diagnostic view to configure the fan module to work in automatic speed adjustment mode.

Example

Set the minimum fan speed in automatic fan speed adjustment mode to 20% of the full fan speed.

```
<HUAWEI> system-view
[HUAWEI] set fan speed auto min-speed 20
Info: The configuration is successful and takes effect only when the specified value is greater than the value calculated based on the intelligent fan speed adjustment policy.
```


3.2.39 set fan speed-adjust threshold minus

Function

The **set fan speed-adjust threshold minus** command adjusts the temperature thresholds for fan speed adjustment.

The **undo set fan speed-adjust threshold minus** command restores the default temperature thresholds for fan speed adjustment.

The default temperature thresholds on different devices are different. You can get to run the **display fan speed-adjust threshold minus** command.

NOTE

The following switches do not support this command:

- S2730S-S series
- S5720-LI series: S5720-12TP-LI-AC, S5720-12TP-PWR-LI-AC, S5720-28P-LI-AC, S5720-28TP-LI-AC, S5720-28TP-PWR-LI-AC, S5720-28X-LI-AC, S5720-28X-LI-DC, and S5720-16X-PWH-LI-AC
- S5735-L, S5735S-L, S5735-L1, S5735S-L1, and S5735S-L-M series: S5735-L12T4S-A, S5735-L24T4S-A, S5735-L24T4S-A1, S5735S-L24T4S-MA, S5735S-L24FT4S-A, S5735S-L12T4S-A, S5735S-L24T4S-A1, S5735-L8T4S-QA1, S5735-L24T4X-QA1, S5735-L24T4S-QA1, and S5735S-L24T4S-A
- S5720S-LI series: S5720S-12TP-LI-AC, S5720S-12TP-PWR-LI-AC, S5720S-28P-LI-AC, S5720SV2-28P-LI-AC, S5720S-28TP-PWR-LI-AC, and S5720S-28X-LI-AC
- S5720I-SI series: S5720I-6X-PWH-SI-AC, S5720I-10X-PWH-SI-AC, S5720I-12X-SI-AC, and S5720I-12X-PWH-SI-DC
- S5735-S-I series
- S5731-H series, S5731S-H series, S5731-S series, S5731S-S series, S5732-H series
- S6730-H series, S6730S-H series, S6730-S series, S6730S-S series
- S6735-S

If one of the preceding switches can set up a stack with other switch models that support this command, this switch also supports this command so that this command can be executed and delivered in the stack.

Format

set fan speed-adjust threshold minus *threshold-value* [**slot** *slot-id*]

undo set fan speed-adjust threshold minus [**slot** *slot-id*]

Parameters

Parameter	Description	Value
threshold-value	Specifies the deduction to the temperature thresholds.	The value is an integer that ranges from 1 to 20.

Parameter	Description	Value
slot *slot-id*	Specifies a slot ID. If this parameter is not specified, the thresholds in all slots are set.	The value depends on the device configuration.

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

The device uses fixed temperature thresholds to increase and decrease the fan speed by default. The fan speed increases when the device temperature exceeds the upper threshold and decreases when the device temperature falls below the lower threshold. If you want to keep the device working at a lower temperature, you can set deduction for the fixed temperature thresholds. The adjusted temperature threshold is lower than the default temperature threshold.

Precautions

- The new thresholds are the fixed temperature thresholds minus *threshold-value*. After the **set fan speed-adjust threshold minus** command is executed, the thresholds for increasing and lowering the fan speed decrease.
- To view the fixed temperature thresholds, run the **display fan speed-adjust threshold minus** command.

NOTE

If a device uses intelligent fan control, this command reduces the temperature thresholds for starting and stopping the fans. Fans in intelligent heat dissipation mode can only start and stop rotating at a fixed speed that cannot be increased or reduced.

You can run the **display fan speed-adjust threshold minus** command to check temperature thresholds for fan speed adjustment of fans in intelligent heat dissipation mode. Assume you view that the current temperature threshold of the fans is 40-50, in which 40°C is the threshold for stopping the fans, and 50°C is the threshold for starting the fans. When the current device temperature is 45°C, you need to determine whether fans will rotate according to the fan temperature change:

- When the device temperature is increased to 45°C from a lower temperature (30°C for example), fans do not rotate because the device temperature does not reach the threshold for starting the fans.
- When the device temperature is reduced to 45°C from a higher temperature (65°C for example), fans keep rotating because the device temperature does not fall below the threshold for stopping the fans.

Example

Set the deduction to the temperature thresholds to 10.
<HUAWEI> **system-view**
[HUAWEI] **set fan speed-adjust threshold minus 10**
Info: Succeeded in setting the fan speed-adjust threshold.

3.2.40 set fan speed mandatory

Function

The **set fan speed mandatory** command sets a fixed speed for fans on a device.

The **undo set fan speed mandatory** command restores the automatic fan speed mode.

By default, the automatic fan speed mode is used.

Format

set fan speed mandatory { **minimal** | **middle** | **maximal** | **fixed40** | **fixed50** | **fixed60** | *speed* } [**slot** *slot-id*]

undo set fan speed mandatory { **minimal** | **middle** | **maximal** | **fixed40** | **fixed50** | **fixed60** | *speed* } [**slot** *slot-id*]

Parameters

Parameter	Description	Value
minimal	Sets the fan speed to the minimum speed of the device.	-
middle	Sets the fan speed to 70% of the full speed.	-
maximal	Sets the fan speed to the full speed.	-
fixed40	Sets the fan speed to 40% of the full speed.	-
fixed50	Sets the fan speed to 50% of the full speed.	-
fixed60	Sets the fan speed to 60% of the full speed.	-
speed	Specifies the percentage of the fan speed to the full speed.	The value is an integer from 20 to 100.

Parameter	Description	Value
slot *slot-id*	Specifies a slot ID.	The value depends on the device configuration.

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

The command for manually setting the fan speed is used only for fault locating. Generally, automatic fan speed adjustment is recommended.

Only devices installed with variable-speed fans support this command. Such fans support fan speed adjustment at two or multiple levels. The system can display the matching parameters according to the type of the fan installed on the device, and you do not need to know how many speed levels the fan supports.

Precautions

In a stack, the **set fan speed mandatory minimal** command will set the fan speed of each member switch to the minimum fan speed.

Example

Set the fan speed to 70% of the full speed.

```
<HUAWEI> system-view
[HUAWEI] set fan speed mandatory middle
```

3.2.41 set flash threshold

Function

The **set flash threshold** command sets the alarm threshold for flash memory usage.

The **undo set flash threshold** command restores the default alarm threshold for flash memory usage.

By default, the alarm threshold for flash memory usage is 80.

Format

set flash threshold *value*

undo set flash threshold *value*

Parameters

Parameter	Description	Value
value	Sets the alarm threshold for flash memory usage.	The value is an integer that ranges from 1 to 99.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

To ensure that the switch has sufficient flash memory, run the **set flash threshold** command to set the alarm threshold for flash memory usage. When flash memory of the switch is insufficient, the system prompts that flash memory is insufficient so that you can determine the flash memory usage.

Example

Set the alarm threshold for flash memory usage on an MPU to 50%.

```
<HUAWEI> system-view
[HUAWEI] set flash threshold 50
Info: Now the flash usage threshold is 50%.
```

3.2.42 set integrated-power

Function

The **set integrated-power** command configures a voltage threshold for the device.

The **undo set integrated-power** command restores the default voltage threshold of the device.

By default, the DC overvoltage threshold is 58.00 V, the DC undervoltage threshold is 50.00 V, the low-load voltage threshold is 49.00 V, and the 53 V DC output voltage threshold is 53.00 V.

NOTE

Only the S5735-S8P2X-IA200H1 supports this command.

Format

set integrated-power { **53v-dc output-voltage** | **dc-overvoltage** | **dc-undervoltage** | **low-load-voltage** } **threshold** *value*

undo set integrated-power { **53v-dc output-voltage** | **dc-overvoltage** | **dc-undervoltage** | **low-load-voltage** } **threshold**

Parameters

Parameter	Description	Value
53v-dc output-voltage	Configures a 53 V DC output voltage threshold.	-
dc-overvoltage	Configures a DC overvoltage threshold.	-
dc-undervoltage	Configures a DC undervoltage threshold.	-
low-load-voltage	Configures a low-load voltage threshold.	-
threshold *value*	Specifies a voltage threshold.	-
value	Specifies the threshold value.	The value range is as follows: • **53v-dc output-voltage**: The value ranges from 53 to 56.4, in volts (V). • **dc-overvoltage**: The value ranges from 53 to 60, in volts (V). • **dc-undervoltage**: The value ranges from 35 to 57, in volts (V). • **low-load-voltage**: The value ranges from 35 to 51.49, in volts (V).

Views

System view

Default Level

2: Configuration level

Usage Guidelines

You can run this command to configure a voltage threshold.

Example

Set the low-load voltage threshold to 39.11 V.


```
<HUAWEI> system-view
[HUAWEI] set integrated-power low-load-voltage threshold 39.11
```

3.2.43 set memory-usage threshold

Function

The **set memory-usage threshold** command sets the memory usage threshold.

The **undo set memory-usage threshold** command restores the default memory usage threshold.

By default, the following describes the memory usage alarm threshold on the S1720GFR:

- If the memory capacity on the device is lower than or equal to 256 MB, the memory usage alarm threshold is 85% and the memory usage alarm recovery threshold is 80%.
- If the memory capacity on the device is larger than 256 MB and smaller than or equal to 512 MB, the memory usage alarm threshold is 90% and the memory usage alarm recovery threshold is 85%.
- If the memory capacity on the device is higher than 512 MB, the memory usage alarm threshold is 95% and the memory usage alarm recovery threshold is 90%.

The following describes the memory usage alarm threshold on other switch models:

- If the memory capacity on the device is lower than or equal to 512 MB, the memory usage alarm threshold is 85% and the memory usage alarm recovery threshold is 80%.
- If the memory capacity on the device is larger than 512 MB and smaller than or equal to 1.5 GB, the memory usage alarm threshold is 90% and the memory usage alarm recovery threshold is 85%.
- If the memory capacity on the device is higher than 1.5 GB, the memory usage alarm threshold is 95% and the memory usage alarm recovery threshold is 90%.

Format

set memory-usage threshold *threshold-value* [**slot** *slot-id*]

undo set memory-usage threshold [*threshold-value*] [**slot** *slot-id*]

Parameters

Parameter	Description	Value
threshold-value	Specifies the memory usage threshold.	The value is an integer that ranges from 75 to 100.

Parameter	Description	Value
slot *slot-id*	Specifies the memory usage threshold of a specified slot ID.	The value depends on the device configuration.

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

You can use the **set memory-usage threshold** command to set the memory usage threshold. When memory usage exceeds the threshold, the system logs the event and generates an alarm. By viewing log information, you can learn about memory usage.

Precautions

You are advised to use the default threshold. If the memory usage threshold is set too low, the system frequently generates alarms. If the memory usage threshold is set too high, you cannot learn about memory usage in a timely manner.

Example

Set the memory usage threshold to 85%.

```
<HUAWEI> system-view
[HUAWEI] set memory-usage threshold 85
```

3.2.44 set power protocol modbus

Function

The **set power protocol modbus** command configures the IP address and port number of a PC510 power supply for the switch to connect to.

The **undo set protocol modbus** command deletes the configuration.

By default, the IP address and port number of a PC510 power supply for the switch to connect to are not configured.

NOTE

This command is supported only by the S5735-L8P4X-IA1, S5735-L8T4X-IA1.

Format

set power protocol modbus [**ip-address** *ip-address-value*] [**tcp-port** *port-value*]

undo set power protocol modbus

Parameters

Parameter	Description	Value
ip-address *ip-address-value*	Specifies the IP address of a PC510 power supply.	The value is in dotted decimal notation. The default value is 192.168.18.88.
tcp-port *port-value*	Specifies the port number of a PC510 power supply.	The value is an integer ranging from 0 to 65535. The default value is 502.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A PC510 power module provides multiple types of power outputs and can supply power to devices, such as switches and cameras, at the same time. To be powered by a PC510 power supply, the switch needs to set up a connection with the PC510 power supply using the Modbus TCP protocol. After connecting to a PC510 power supply, the switch can manage this power supply, for example, obtain its version information and restart it.

You need to run this command on the switch to configure the IP address and port number of the PC510 power supply so that the switch can set up a connection with it.

Precautions

- After running this command, to ensure that the switch can set up a connection with the power supply successfully, you need to create a VLANIF interface on the switch, configure an IP address on the same subnet as the power supply for the VLANIF interface, and add the interface connecting the switch to the power supply to the VLAN of the VLANIF interface.
- The IP address and port number of a PC510 power module are fixed at 192.168.18.88 and 502, respectively. Therefore, the IP address and port number configured using this command can only be 192.168.18.88 and 502.

Example

Configure the IP address and port number of a PC510 power supply for the switch to connect to.

```
<HUAWEI> system-view
[HUAWEI] set power protocol modbus ip-address 192.168.18.88 tcp-port 502
```

3.2.45 set root-key

Function

The **set root-key** command configures a root key for a switch.

The **undo set root-key** command restores the default root key of a switch.

By default, a switch uses the system default root key.

Format

set root-key [**auto**]

undo set root-key

Parameters

Parameter	Description	Value
auto	Automatically generates the root key of the device.	-

Views

User view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

A root key is located at the bottom of the key management infrastructure to protect confidentiality of upper-layer keys (such as key encryption key). Therefore, a root key is important to data security. A switch's root key is often stored in the system. If attackers illegally obtain the root key, encrypted data will become insecure. To improve data security and prevent attackers from obtaining encrypted packets, configure another root key on the switch. The configured root key will take effect after the switch restarts.

If the device has high security requirements and its configuration file needs to be prevented from being used by other devices, run the **set root-key auto** command to automatically generate a root key for the device. You can run this command to automatically generate a root key only for an unconfigured device.

Precautions

- The root key can only be configured when the switch has no service configuration. If service configuration has been performed on the switch, an error message will be displayed when you configure the root key.
- If you configure a password (not the administrator password) and key after configuring the root key, the password and key configuration will not be restored after the switch software version is changed to V200R009 or an earlier version.
- After the root key is configured and the device is restarted, run the **display root-key configuration** command to check whether the configuration takes effect. After the configuration takes effect on the device, if you export the device's configuration file and apply it to other devices, other devices cannot work properly.
- Do not run this command to set the root key to the weak password preset by running the **load security weak-password-dictionary** command.

Example

Set the root key that meets the length requirements, for example, 98765432109876543210abc. Set this parameter based on the site requirements.

```
<HUAWEI> set root-key
Warning: A new root key can take effect only after the device is restarted. Continue? [Y/N]:y
Please enter a new key of no more than 32 and no less than 20 characters:
Please enter the new key again:
Info: Succeed in setting next root-key on the master board.
```

Configure automatic root key generation.

```
<HUAWEI> set root-key auto
```

3.2.46 set rtc to power

Function

The **set rtc to power** command synchronizes the time of the power supply with the device time.

NOTE

Only the S5735-S8P2X-IA200H1 supports this command.

Format

set rtc to power

undo set rtc to power

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

You can run this command to synchronize the time of the power supply with the device time.

Example

Synchronize the time of the power supply with the device time.

```
<HUAWEI> system-view
[HUAWEI] set rtc to power
```

3.2.47 set service-mode

Function

The **set service-mode** command sets the working mode of the device to enhanced.

The **undo set service-mode** command restores the working mode of the device to normal.

By default, the working mode of the device is normal.

NOTE

This command is supported only by S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S.

Format

Command format on the S5732-H, S6730-S, S6730S-S, S6730S-H, and S6730-H:

set service-mode { **enhanced-bfd** | **enhanced-oam** | **enhanced-ptp** }

undo set service-mode { **enhanced-bfd** | **enhanced-oam** | **enhanced-ptp** }

Command format on other switches:

set service-mode enhanced

undo set service-mode enhanced

Parameters

Parameter	Description	Value
enhanced	Sets the working mode of the device to enhanced.	-

Parameter	Description	Value
enhanced-bfd	Sets the BFD working mode of the device to enhanced.	-
enhanced-oam	Sets the OAM working mode of the device to enhanced.	-
enhanced-ptp	Sets the PTP working mode of the device to enhanced.	-

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

In normal mode, the interval for receiving BFD packets must be more than or equal to 100 ms. If the interval cannot meet requirements, run the **set service-mode** command to change the working mode of the switch to enhanced or **enhanced-bfd** mode so that the switch supports a minimum of 3 ms interval.

To implement some OAM functions, you need to run the **set service-mode** command to change the working mode of the switch to enhanced or **enhanced-oam** mode. For more details, see the OAM description.

To configure PTP, you need to run the **set service-mode** command to change the working mode of the switch to enhanced **enhanced-ptp** mode.

Precautions

- Running the **set service-mode** command will reduce the device forwarding performance. Therefore, confirm the action before you use the command.
- If BFD has been enabled before this command is executed, disable BFD first.
- Before changing the working mode from enhanced to normal, disable the PTP function.
- On the S5732-H, S6730-S, S6730S-S, S6730S-H, and S6730-H, you can run the **set service-mode** command multiple times to set the working mode of BFD, PTP, and OAM to enhanced.

Example

Set the working mode of the device to enhanced.


```
<HUAWEI> system-view
[HUAWEI] set service-mode enhanced
Warning: This command will effect forward performance. Continue? [Y/N]:y
```

3.2.48 slave restart

Function

Using the **slave restart** command, you can reload the system software of the standby device and then restart it.

NOTE

This function is supported only on member devices in a stack.

Format

slave restart

Parameters

None

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

If the standby switch is not working normally, you can reset it to restore its functions without affecting existing services.

Precautions

Due to the component upgrade of some device models, the devices whose first supported version is V200R021C10 cannot be downgraded. If the message "Error: The hardware version VER.B of slot %u does not support the configured system software package." (%u indicates the actual slot number) is displayed after the command is run, you can solve this problem by installing the patch that matches the version. For details about the first supported version of the device and matching patch version, see the device overview in the "Hardware Description".

NOTICE

The command may interrupt services on the device. Therefore, exercise caution when using this command.

Example

Restart the standby device.

```
<HUAWEI> system-view
[HUAWEI] slave restart
```

3.2.49 slave switchover

Function

The **slave switchover** command performs an active/standby switchover.

NOTE

This function is supported only on member devices in a stack.

Format

slave switchover

Parameters

None

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

In a stack of multiple switches, you can manually perform an active/standby switchover on the master and standby switches during a software upgrade or system maintenance. After the active/standby switchover is complete, the original master switch restarts, becomes the new standby switch or a slave switch, and joins the stack, and the original standby switch becomes the new master switch.

Prerequisites

- The forcible active/standby switchover function has been enabled on devices.
- The **display switchover state** command output shows that system has met requirements for an active/standby switchover. The requirements for an active/standby switchover are met only when the value of **HA FSM State(master)** is **realtime or routine backup** and the value of **HA FSM State(slave)** is **receiving realtime or routine data**. This indicates that data is consistent on the master and standby switches.

Precautions

- You can run the **slave switchover** command to perform an active/standby switchover only in a stack of multiple switches.
- If an unregistered member switch exists in the stack, to prevent the stack from being split, do not run the **slave switchover** command to perform an active/standby switchover.
- If the **slave switchover** command is executed when other commands are being executed, you need to execute the commands that have not taken effect on the new master switch again after the original standby switch becomes the new master switch.
- Due to the component upgrade of some device models, some devices cannot be downgraded. If the message "Error: The hardware version VER.B of slot %u does not support the configured system software package." (%u indicates the actual slot number) is displayed after the command is run, you can solve this problem by installing the patch that matches the version. For details about the first supported version of the device and matching patch version, see the device overview in the "Hardware Description"..

Example

Perform an active/standby switchover.

```
<HUAWEI> system-view
[HUAWEI] slave switchover enable
[HUAWEI] slave switchover
Warning: This operation will switch the slave board to the master board. Continue? [Y/N]:y
```

3.2.50 slave switchover { disable | enable }

Function

The **slave switchover** { **disable** | **enable** } command enables or disables forcible master/slave switchover.

undo slave switchover disable command enables forcible master/slave switchover.

By default, master/slave switchover is enabled.

NOTE

This function is supported only on member devices in a stack.

Format

slave switchover { **disable** | **enable** }

undo slave switchover disable

Parameters

Parameter	Description	Value
disable	Disables forcible master/slave switchover.	-

Parameter	Description	Value
enable	Enables forcible master/slave switchover.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

The **slave switchover** command takes effect only after forcible master/slave switchover is enabled. If forcible master/slave switchover is disabled, the **slave switchover** command does not take effect.

Example

Disable forcible master/slave switchover.

```
<HUAWEI> system-view
[HUAWEI] slave switchover disable
```

3.2.51 system memory-usage monitor disable

Function

The **system memory-usage monitor disable** command disables the function of generating an alarm when the system memory usage reaches the threshold.

The **undo system memory-usage monitor disable** command enables the function of generating an alarm when the system memory usage reaches the threshold.

By default, the function of generating an alarm when the system memory usage reaches the threshold is enabled.

Format

system memory-usage monitor disable

undo system memory-usage monitor disable

Parameters

None

Views

System view

Default Level

3: Management level

Usage Guidelines

When the system memory is insufficient, services are abnormal. For example, configurations cannot be delivered or traffic cannot be forwarded. For the Linux operating system, when the system memory usage reaches 90%, the device reports an alarm indicating that the memory usage reaches the threshold by default.

If the memory is sufficient and the memory insufficiency alarm does not need to be reported, you can run this command to disable the function of reporting an alarm when the system memory usage reaches the threshold.

Example

Disable the function of generating an alarm when the system memory usage reaches the threshold.

```
<HUAWEI> system-view
[HUAWEI] system memory-usage monitor disable
```

3.2.52 temperature threshold

Function

The **temperature threshold** command sets the temperature alarm thresholds.

The **undo temperature threshold** command restores the default temperature alarm thresholds.

By default, the lower temperature threshold is -40°C on the S5720I-SI and S5735-S-I, and -3°C on the S5731-H, S5732-H, S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S500, S5735-S, S5735S-S, S5736-S, and S6730-H, and 0°C on other switch models, and the upper temperature threshold varies according to hardware of various models, ranging from 44°C to 88°C.

Format

temperature threshold slot { *slot-id* | **all** } **lower-limit** *min-temperature* **upper-limit** *max-temperature*

undo temperature threshold slot { *slot-id* | **all** }

Parameters

Parameter	Description	Value
slot *slot-id*	Specifies a slot ID.	The value depends on the device configuration.

Parameter	Description	Value
all	Sets the temperature alarm threshold for all member switches in a stack.	-
lower-limit *min-temperature*	Specifies the lower temperature alarm threshold.	The value is an integer that ranges from -40 to 88. *min-temperature* specifies the value of the temperature. The value of *min-temperature* varies according to device models. The minimum value of *min-temperature* is the default lower threshold. In a stack of multiple member switches, when **all** is specified in the **temperature threshold** command and the temperature alarm thresholds of all member switches are set, the *min-temperature* value is the largest value among the lower temperature alarm thresholds of the member switches.

Parameter	Description	Value
upper-limit *max-temperature*	Specifies the upper temperature alarm threshold.	The value is an integer that ranges from -40 to 88. *max-temperature* specifies the value of the temperature. The value of *max-temperature* varies according to device models. The maximum value of *max-temperature* is the default upper threshold. *max-temperature* must be at least 10 greater than *min-temperature*. In a stack of multiple member switches, when **all** is specified in the **temperature threshold** command and the temperature alarm thresholds of all member switches are set, the *max-temperature* value is the smallest value among the upper temperature alarm thresholds of the member switches.

Views

system view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

The device generates an alarm and records log information when the device temperature falls below the lower threshold or rises above the upper threshold.

Precautions

- If the configured threshold values are out of the allowed range, the configuration fails and the upper and lower thresholds are restored to the maximum values.

- Configuration commands are generated in a configuration file regardless of whether the configured threshold values are default values. These commands can be cleared only when the **undo temperature threshold** command is executed.

Example

Set the lower temperature alarm threshold to 20°C and upper temperature alarm threshold to 60°C.

```
<HUAWEI> system-view
[HUAWEI] temperature threshold slot all lower-limit 20 upper-limit 60
```

3.2.53 transceiver diagnosis threshold rx-power

Function

The **transceiver diagnosis threshold rx-power** command sets the upper and lower thresholds for the receive optical power of the optical transceiver installed in an interface.

The **undo transceiver diagnosis threshold rx-power** command restores the upper and lower thresholds to the default values for the receive optical power of the optical transceiver installed in an interface.

By default, the optical power upper and lower thresholds vary according to optical module vendors.

Format

transceiver diagnosis threshold rx-power { **default** | **low-alarm** *low-alarm* **high-alarm** *high-alarm* }

undo transceiver diagnosis threshold rx-power

Parameters

Parameter	Description	Value
default	Sets the upper and lower thresholds for the receive optical power of the optical transceiver installed in an interface to default values.	-
high-alarm *high-alarm*	Sets the upper threshold for the receive optical power of the optical transceiver installed in an interface.	The value varies according to the optical module vendor.

Parameter	Description	Value
low-alarm *low-alarm*	Sets the lower threshold for the receive optical power of the optical transceiver installed in an interface.	The value varies according to the optical module vendor.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

You can run the **transceiver diagnosis threshold rx-power** command to adjust the receive optical power of the optical transceiver.

Example

Set the upper and lower thresholds for the receive optical power of the optical transceiver installed in GigabitEthernet 0/0/2 to default values.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/2
[HUAWEI-GigabitEthernet0/0/2] transceiver diagnosis threshold rx-power default
```

3.2.54 transceiver diagnosis threshold tx-power

Function

The **transceiver diagnosis threshold tx-power** command sets the upper and lower thresholds for the transmit optical power of the optical transceiver installed in an interface.

The **undo transceiver diagnosis threshold tx-power** command restores the upper and lower thresholds for the transmit optical power of the optical transceiver installed in an interface to default values.

By default, the optical power upper and lower thresholds vary according to optical module vendors.

Format

transceiver diagnosis threshold tx-power { **default** | **low-alarm** *low-alarm* **high-alarm** *high-alarm* }

undo transceiver diagnosis threshold tx-power

Parameters

Parameter	Description	Value
default	Sets the upper and lower thresholds for the transmit optical power of the optical transceiver installed in an interface to default values.	-
high-alarm *high-alarm*	Sets the upper threshold for the transmit optical power of the optical transceiver installed in an interface.	The value varies according to the optical module vendor.
low-alarm *low-alarm*	Sets the lower threshold for the transmit optical power of the optical transceiver installed in an interface.	The value varies according to the optical module vendor.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

You can run the **transceiver diagnosis threshold tx-power** command to adjust the transmit optical power of the optical transceiver.

Example

Set the upper and lower thresholds for the transmit optical power of the optical transceiver installed in GigabitEthernet 0/0/2 to default values.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/2
[HUAWEI-GigabitEthernet0/0/2] transceiver diagnosis threshold tx-power default
```

3.2.55 transceiver phony-alarm-disable

Function

The **transceiver phony-alarm-disable** command disables the alarm function for non-Huawei-certified switch optical modules.

The **undo transceiver phony-alarm-disable** command enables the alarm function for non-Huawei-certified switch optical modules.

By default, the alarm function is enabled for non-Huawei-certified switch optical modules.

Format

transceiver phony-alarm-disable

undo transceiver phony-alarm-disable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Non-Huawei-certified switch optical modules may fail to work normally. If non-Huawei-certified switch optical modules are used on devices produced since July 1, 2013 (January 1, 2016 for QSFP+ 40GE optical modules), the devices generate a large number of alarms to prompt users to replace these optical modules with Huawei-certified switch optical modules. However, vendor information of optical modules early delivered from Huawei may not be recorded. Therefore, non-Huawei-certified switch optical module alarms are generated. These optical modules can still be used to protect customer investment. In this case, you can disable the alarm function for non-Huawei-certified switch optical modules.

Example

Disable the alarm function for non-Huawei-certified switch optical modules.

```
<HUAWEI> system-view
[HUAWEI] transceiver phony-alarm-disable
Info:Transceiver-phony-alarm disable.
```

Enable the alarm function for non-Huawei-certified switch optical modules.

```
<HUAWEI> system-view
[HUAWEI] undo transceiver phony-alarm-disable
Info:Transceiver-phony-alarm enable.
```

3.2.56 wavelength-channel

Function

The **wavelength-channel** command sets the wavelength channel of a wavelength-tunable optical module.

The **undo wavelength-channel** command restores the default wavelength channel of a wavelength-tunable optical module.

The default wavelength channel of a wavelength-tunable optical module is channel 1.

Format

wavelength-channel *channelnum*

undo wavelength-channel

Parameters

Parameter	Description	Value
channelnum	Specifies a wavelength channel number.	The value is an integer that ranges from 1 to 80.

Views

XGE interface view, 25GE interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To adjust the wavelength of a wavelength-tunable optical module on an interface, run the **wavelength-channel** *channelnum* command on this interface. This command will add the wavelength-tunable optical module to a specified wavelength channel. Each wavelength channel has a fixed center wavelength and frequency. To view the mapping between the wavelength channel, center wavelength, and frequency, run the **display wavelength-map** command.

You can also run the **wavelength-channel frequency** *frequency-value* and **wavelength-channel wavelength** *wavelength-value* commands to set the wavelength and frequency of a wavelength-tunable optical module.

Precautions

- When the **wavelength-channel** command configuration exists on the interface, after the interface has a wavelength-tunable optical module installed, this optical module will automatically adjust its wavelength to the configured wavelength. If a copper module is installed, the command configuration remains but does not take effect. If a non-wavelength-tunable optical module is installed, the command configuration will not take effect and the system displays an alarm.
- Running the **wavelength-channel** command will open and close the laser, resulting in interface flapping.
- The **wavelength-channel** *channelnum*, **wavelength-channel frequency** *frequency-value*, and **wavelength-channel wavelength** *wavelength-value*

commands are mutually exclusive with the **wavelength-channel trust sfp** command.

Example

Add a wavelength-tunable optical module to wavelength channel 20 on XGigabitEthernet0/0/2.

```
<HUAWEI> system-view
[HUAWEI] interface XGigabitEthernet 0/0/2
[HUAWEI-XGigabitEthernet0/0/2] wavelength-channel 20
```

3.2.57 wavelength-channel frequency

Function

The **wavelength-channel frequency** command sets the frequency of a wavelength-tunable optical module.

The **undo wavelength-channel frequency** command restores the default frequency of a wavelength-tunable optical module.

The default frequency of a wavelength-tunable optical module is the same as that of wavelength channel 1.

Format

wavelength-channel frequency *frequency-value*

undo wavelength-channel frequency

Parameters

Parameter	Description	Value
frequency-value	Specifies a frequency.	The value is an integer ranging from 0 to 4294967295, in MHz.

Views

XGE interface view, 25GE interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When two interfaces installed with optical modules are connected through optical fibers, the wavelengths of the two optical modules must match, and so do their

frequencies; otherwise, the interfaces cannot go Up or transmit traffic. When a wavelength-tunable optical module is connected to an optical module with a fixed wavelength and frequency, you need to change the wavelength and frequency of the wavelength-tunable optical module to match with those of its connected optical module, respectively.

You can run the **wavelength-channel frequency** *frequency-value* command to set the frequency of a wavelength-tunable optical module and run the **wavelength-channel wavelength** *wavelength-value* command to set the wavelength of a wavelength-tunable optical module. You can also run the **wavelength-channel** *channelnum* command to set the wavelength channel of a wavelength-tunable optical module. This changes its wavelength and frequency at the same time. To view the mapping between the wavelength channel, wavelength, and frequency, run the **display wavelength-map** command.

Precautions

- When the **wavelength-channel** command configuration exists on the interface, after the interface has a wavelength-tunable optical module installed, this optical module will automatically adjust its wavelength to the configured wavelength. If a copper module is installed, the command configuration remains but does not take effect. If a non-wavelength-tunable optical module is installed, the command configuration will not take effect and the system displays an alarm.
- Running the **wavelength-channel** command will open and close the laser, resulting in interface flapping.
- The **wavelength-channel** *channelnum*, **wavelength-channel frequency** *frequency-value*, and **wavelength-channel wavelength** *wavelength-value* commands are mutually exclusive with the **wavelength-channel trust sfp** command.

Example

Set the frequency of the wavelength-tunable optical module on XGigabitEthernet 0/0/2 to 192100000 MHz.

```
<HUAWEI> system-view
[HUAWEI] interface XGigabitEthernet 0/0/2
[HUAWEI-XGigabitEthernet0/0/2] wavelength-channel frequency 192100000
```

3.2.58 wavelength-channel wavelength

Function

The **wavelength-channel wavelength** command sets the wavelength of a wavelength-tunable optical module.

The **undo wavelength-channel wavelength** command restores the default wavelength of a wavelength-tunable optical module.

The default wavelength of a wavelength-tunable optical module is the same as that of wavelength channel 1.

Format

wavelength-channel wavelength *wavelength-value*

undo wavelength-channel wavelength

Parameters

Parameter	Description	Value
wavelength-value	Specifies a wavelength.	The value is an integer ranging from 0 to 4294967295, in pm.

Views

XGE interface view, 25GE interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When two interfaces installed with optical modules are connected through optical fibers, the wavelengths of the two optical modules must match, and so do their frequencies; otherwise, the interfaces cannot go Up or transmit traffic. When a wavelength-tunable optical module is connected to an optical module with a fixed wavelength and frequency, you need to change the wavelength and frequency of the wavelength-tunable optical module to match with those of its connected optical module, respectively.

You can run the **wavelength-channel frequency** *frequency-value* command to set the frequency of a wavelength-tunable optical module and run the **wavelength-channel wavelength** *wavelength-value* command to set the wavelength of a wavelength-tunable optical module. You can also run the **wavelength-channel** *channelnum* command to set the wavelength channel of a wavelength-tunable optical module. This changes its wavelength and frequency at the same time. To view the mapping between the wavelength channel, wavelength, and frequency, run the **display wavelength-map** command.

Precautions

- When the **wavelength-channel** command configuration exists on the interface, after the interface has a wavelength-tunable optical module installed, this optical module will automatically adjust its wavelength to the configured wavelength. If a copper module is installed, the command configuration remains but does not take effect. If a non-wavelength-tunable optical module is installed, the command configuration will not take effect and the system displays an alarm.
- Running the **wavelength-channel** command will open and close the laser, resulting in interface flapping.
- The **wavelength-channel** *channelnum*, **wavelength-channel frequency** *frequency-value*, and **wavelength-channel wavelength** *wavelength-value*

commands are mutually exclusive with the **wavelength-channel trust sfp** command.

Example

Set the wavelength of the wavelength-tunable optical module on XGigabitEthernet 0/0/2 to 1560606 pm.

```
<HUAWEI> system-view
[HUAWEI] interface XGigabitEthernet 0/0/2
[HUAWEI-XGigabitEthernet0/0/2] wavelength-channel wavelength 1560606
```

3.2.59 wavelength-channel trust sfp

Function

The **wavelength-channel trust sfp** command configures a device to trust the wavelength channel of an optical module.

The **undo wavelength-channel trust sfp** command deletes the configuration.

By default, a device does not trust the wavelength channel of an optical module.

Format

wavelength-channel trust sfp

undo wavelength-channel trust sfp

Parameters

None

Views

XGE interface view, 25GE interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When a wavelength-tunable optical module is installed on a device, the device forcibly sets the wavelength channel to the default value 1 or a value configured using the **wavelength-channel** *channelnum* command. This makes the wavelength channel on the local device be different from that of on the remote device. As a result, the two devices fail to communicate. In this case, you can run the **wavelength-channel trust sfp** command to configure the device to trust the wavelength channel of the optical module.

Precautions

The **wavelength-channel** *channelnum*, **wavelength-channel frequency** *frequency-value*, and **wavelength-channel wavelength** *wavelength-value* are mutually exclusive with the **wavelength-channel trust sfp** command. That is:

- After the **wavelength-channel** *channelnum*, **wavelength-channel frequency** *frequency-value*, or **wavelength-channel wavelength** *wavelength-value* command is configured, the **wavelength-channel trust sfp** command cannot be configured.
- After the **wavelength-channel trust sfp** command is configured, the **wavelength-channel** *channelnum*, **wavelength-channel frequency** *frequency-value*, or **wavelength-channel wavelength** *wavelength-value* command cannot be configured.

Example

Configure the device to trust the wavelength channel of the optical module on XGigabitEthernet0/0/2.

```
<HUAWEI> system-view
[HUAWEI] interface XGigabitEthernet 0/0/2
[HUAWEI-XGigabitEthernet0/0/2] wavelength-channel trust sfp
```

3.3 Stack Configuration Commands

3.3.1 Command Support

Table 3-50 Applicable product models and versions

Product	Software Version	Stack Connection Mode	Product Model
S200	Not supported	-	All S200 switches do not support stacking.
S300	V200R020C10, V200R021C00, V200R021C01, V200R021C10, V200R022C00, V200R022C10, V200R023C00	Service port connections using ordinary and dedicated cables	All S300 switches support stacking.
S300	V200R020C10, V200R021C00, V200R021C01, V200R021C10, V200R022C00, V200R022C10, V200R023C00	Service port connections using ordinary and dedicated cables	All S500 switches support stacking.

Product	Software Version	Stack Connection Mode	Product Model
S1720 and S1730	Not supported	-	All S1720 and S1730 switches do not support stacking.
S2700-SI	Not supported	-	All S2700-SI switches do not support stacking.
S2710-SI	V100R006(C03&C05)	Service port connection using ordinary cables	All S2710-SI switches support stacking.
S2700-EI	V100R005C01, V100R006(C00&C01&C03&C05)	Service port connection using ordinary cables	S2700-9TP-EI-AC, S2700-9TP-EI-DC, S2700-9TP-PWR-EI, S2700-18TP-EI-AC, S2700-26TP-EI-AC, S2700-26TP-EI-DC, and S2700-26TP-PWR-EI do not support stacking, whereas other models support.

Product	Software Version	Stack Connection Mode	Product Model
S2720-EI	Versions supporting service port connection using ordinary cables: V200R006C10, V200R009C00, V200R010C00, V200R011C10, V200R012C00, V200R013C00, V200R019C00, V200R019C10, V200R020C00, V200R020C10, V200R021C00, V200R021C10, V200R022C00 Versions supporting service port connection using dedicated cables: V200R011C10, V200R012C00, V200R013C00, V200R019C00, V200R019C10, V200R020C00, V200R020C10, V200R021C00, V200R021C10, V200R022C00	Service port connections using ordinary and dedicated cables	All S2720-EI switches support stacking.
S2730S-S	Versions supporting service port connection using ordinary cables: V200R020C10, V200R021C00, V200R021C10, V200R022C00, V200R022C10, V200R023C00	Service port connections using ordinary and dedicated cables	All S2730S-S switches support stacking.

Product	Software Version	Stack Connection Mode	Product Model
S2750-EI	Versions supporting service port connection using ordinary cables: V200R003C00, V200R005C00SPC300, V200R006C00, V200R007C00, V200R008C00, V200R009C00, V200R010C00, V200R011C00, V200R011C10, V200R012C00 Versions supporting service port connection using dedicated cables: V200R011C10 and V200R012C00	Service port connections using ordinary and dedicated cables	All S2750-EI switches support stacking.
S3700-SI	V100R005C01, V100R006(C00&C01&C03&C05)	Service port connection using ordinary cables	All S3700-SI switches support stacking.
S3700-EI	V100R005C01, V100R006(C00&C01&C03&C05)	Service port connection using ordinary cables	All S3700-EI switches support stacking.
S3700-HI	Not supported	-	All S3700-HI switches do not support stacking.
S5700-EI	V100R005C01, V100R006(C00&C01), V200R001(C00&C01), V200R002C00, V200R003C00, V200R005(C00&C01&C02&C03)	Stack card connection	All S5700-EI switches support stacking.
S5700-SI	V100R005C01, V100R006C00, V200R001C00, V200R002C00, V200R003C00, V200R005C00	Stack card connection	S5700-26X-SI-12S-AC does not support stacking, whereas other models support.

Product	Software Version	Stack Connection Mode	Product Model
S5700-HI	V200R003C00, V200R005C00	Service port connection using ordinary cables	All S5700-HI switches support stacking.
S5700-LI	Versions supporting service port connection using ordinary cables: V200R001C00, V200R002C00, V200R003(C00&C02&C10), V200R005C00SPC300, V200R006C00, V200R007C00, V200R008C00, V200R009C00, V200R010C00, V200R011C00, V200R011C10, V200R012C00 Versions supporting service port connection using dedicated cables: V200R011C10 and V200R012C00	Service port connections using ordinary and dedicated cables	S5700-10P-LI-AC, S5700-10P-PWR-LI-AC, S5700-28P-LI-BAT, and S5700-28P-LI-24S-BAT do not support stacking, whereas other models support.
S5700S-LI	Versions supporting service port connection using ordinary cables: V200R008C00, V200R009C00, V200R010C00, V200R011C00, V200R011C10, V200R012C00 Versions supporting service port connection using dedicated cables: V200R011C10 and V200R012C00	Service port connections using ordinary and dedicated cables	S5700S-28P-LI-AC and S5700S-52P-LI-AC do not support stacking, whereas other models support.
S5710-EI	V200R001C00, V200R002C00, V200R003C00, V200R005(C00&C02)	Service port connection using ordinary cables	All S5710-EI switches support stacking.

Product	Software Version	Stack Connection Mode	Product Model
S5710-HI	V200R005C03	Service port connection using ordinary cables	All S5710-HI switches support stacking.
S5710-C-LI	V200R001C00	Stack card connection	All S5710-C-LI switches support stacking.
S5710-X-LI	Versions supporting service port connection using ordinary cables: V200R008C00, V200R009C00, V200R010C00, V200R011C00, V200R011C10, V200R012C00 Versions supporting service port connection using dedicated cables: V200R011C10 and V200R012C00	Service port connections using ordinary and dedicated cables	All S5710-X-LI switches support stacking.

Product	Software Version	Stack Connection Mode	Product Model
S5720-LI and S5720S-LI	Versions supporting service port connection using ordinary cables: V200R010C00, V200R011C00, V200R011C10, V200R012(C00&C20), V200R013C00, V200R019C00, V200R019C10, V200R020C00, V200R020C10, V200R021C00, V200R021C10, V200R022C00, V200R022C10, V200R023C00 Versions supporting service port connection using dedicated cables: V200R011C10, V200R012C00, V200R013C00, V200R019C00, V200R019C10, V200R020C00, V200R020C10, V200R021C00, V200R021C10, V200R022C00, V200R022C10, V200R023C00	Service port connections using ordinary and dedicated cables	All S5720-LI and S5720S-LI switches support stacking.

Product	Software Version	Stack Connection Mode	Product Model
S5720-SI and S5720S-SI	Versions supporting service port connection using ordinary cables: V200R008C00, V200R009C00, V200R010C00, V200R011C00, V200R011C10, V200R012C00, V200R013C00, V200R019C00, V200R019C10 Versions supporting service port connection using dedicated cables: V200R011C10, V200R012C00, V200R013C00, V200R019C00, V200R019C10	Service port connections using ordinary and dedicated cables	All S5720-SI and S5720S-SI switches support stacking.
S5720I-SI	V200R012C00, V200R013C00, V200R019C00, V200R019C10	Service port connections using ordinary and dedicated cables	S5720I-6X-PWH-SI-AC and S5720I-10X-PWH-SI-AC do not support stacking, whereas other models support.

Product	Software Version	Stack Connection Mode	Product Model
S5720-EI	V200R007C00, V200R008C00, V200R009C00, V200R010C00, V200R011C00, V200R011C10, V200R012C00, V200R013C00, V200R019C00, V200R019C10	Service port connection using ordinary cables: S5720-C-EI, S5720-PC-EI Stack card connection: S5720-P-EI, S5720-C-EI, S5720-X-EI, S5720-PC-EI When using the stack card connection mode, note the following: • S5720-C-EI and S5720-PC-EI series switches use dedicated stack cards to set up stacks. • S5720-X-EI and S5720-P-EI series switches use stack ports fixed on cards to set up stacks.	All S5720-EI switches support stacking.

Product	Software Version	Stack Connection Mode	Product Model
S5720-HI	Versions supporting service port connection using ordinary cables: V200R009C00, V200R010C00, V200R011C00, V200R011C10, V200R012C00, V200R013C00, V200R019C00, V200R019C10 Versions supporting service port connection using dedicated cables: V200R011C10, V200R012C00, V200R013C00, V200R019C00, V200R019C10	Service port connections using ordinary and dedicated cables	All S5720-HI switches support stacking.
S5730-HI	V200R012C00, V200R013C00, V200R019C00, V200R019C10	Service port connections using ordinary and dedicated cables	All S5730-HI switches support stacking.
S5731-H	V200R013C02, V200R019C00, V200R019C10, V200R020C00, V200R020C10, V200R021C00, V200R021C01, V200R021C10, V200R022C00, V200R022C10, V200R023C00	Service port connections using ordinary and dedicated cables	All S5731-H switches support stacking.
S5731S-H	V200R019C00, V200R019C10, V200R020C00, V200R020C10, V200R021C00, V200R021C01, V200R021C10, V200R022C00, V200R022C10, V200R023C00	Service port connections using ordinary and dedicated cables	All S5731S-H switches support stacking.

Product	Software Version	Stack Connection Mode	Product Model
S5731-L and S5731S-L	Not supported	-	All S5731-L and S5731S-L switches do not support stacking.
S5731-S and S5731S-S	V200R019C00, V200R019C10, V200R020C00, V200R020C10, V200R021C00, V200R021C01, V200R021C10, V200R022C00, V200R022C10, V200R023C00	Service port connections using ordinary and dedicated cables	All S5731-S and S5731S-S switches support stacking.
S5732-H	Versions supporting service port connection using ordinary cables: V200R019C00, V200R019C10, V200R019C20, V200R020C00, V200R020C10, V200R021C00, V200R021C10, V200R022C00, V200R022C10, V200R023C00 Versions supporting service port connection using dedicated cables: V200R019C10, V200R020C00, V200R020C10, V200R021C00, V200R021C10, V200R022C00, V200R022C10, V200R023C00	Service port connections using ordinary and dedicated cables	All S5732-H switches support stacking.

Product	Software Version	Stack Connection Mode	Product Model
S5730-SI	Versions supporting service port connection using ordinary cables and dedicated cables: V200R011C10, V200R012C00, V200R013C00, V200R019C00, V200R019C10 Versions supporting stack card connection: V200R012C00, V200R013C00, V200R019C00, V200R019C10	Service port connections using ordinary and dedicated cables, and stack card connection	All S5730-SI switches support stacking.
S5730S-EI	Versions supporting service port connection using ordinary cables and dedicated cables: V200R011C10, V200R012C00, V200R013C00, V200R019C00, V200R019C10 Versions supporting stack card connection: V200R012C00, V200R013C00, V200R019C00, V200R019C10	Service port connections using ordinary and dedicated cables, and stack card connection	All S5730S-EI switches support stacking.
S5735-L, S5735S-L, and S5735S-L-M	V200R019C10, V200R020C00, V200R020C10, V200R021C00, V200R021C10, V200R022C00, V200R022C10, V200R023C00	Service port connections using ordinary and dedicated cables	All S5735-L, S5735S-L, and S5735S-L-M switches support stacking.
S5735-L-I	V200R021C00, V200R021C01, V200R021C10, V200R022C00, V200R022C10, V200R023C00	Service port connections using ordinary and dedicated cables	All S5735-L-I switches support stacking.

Product	Software Version	Stack Connection Mode	Product Model
S5735-L1 and S5735S-L1	V200R020C10, V200R021C00, V200R021C01, V200R021C10, V200R022C00, V200R022C10, V200R023C00	Service port connections using ordinary and dedicated cables	S5735-L8T4S-A1(98011284-001), S5735-L8P4S-A1(98011295-001), S5735-L24T4S-A1(98011306-001), and S5735-L24P4S-A1(98011321-001) do not support stacking, whereas other models support.
S5735-S and S5735S-S	V200R019C10, V200R020C00, V200R020C10, V200R021C00, V200R021C10, V200R022C00, V200R022C10, V200R023C00	Service port connections using ordinary and dedicated cables	All S5735-S and S5735S-S switches support stacking.
S5735-S-I	V200R020C00, V200R020C10, V200R021C00, V200R021C10, V200R022C00, V200R022C10, V200R023C00	Service port connections using ordinary and dedicated cables	Only the S5735-S24T4X-I switch supports stacking.
S5735S-H	V200R020C00, V200R020C10, V200R020C30, V200R021C00, V200R021C01, V200R021C10, V200R022C00, V200R022C10, V200R023C00	Service port connection using ordinary cables	All S5735S-H switches support stacking.
S5736-S	V200R020C00, V200R020C10, V200R020C30, V200R021C00, V200R021C01, V200R021C10, V200R022C00, V200R022C10, V200R023C00	Service port connection using ordinary cables	All S5736-S switches support stacking.

Product	Software Version	Stack Connection Mode	Product Model
S6700-EI	V100R006C00, V200R001(C00&C01), V200R002C00, V200R003C00, V200R005(C00&C01&C02)	Service port connection using ordinary cables	All S6700-EI switches support stacking.
S6720-EI	Versions supporting service port connection using ordinary cables: V200R008C00, V200R009C00, V200R010C00, V200R011C00, V200R011C10, V200R012C00, V200R013C00, V200R019C00, V200R019C10, V200R020C00, V200R020C10, V200R021C00, V200R021C10, V200R022C00, V200R022C10, V200R023C00 Versions supporting service port connection using dedicated cables: V200R011C10, V200R012C00, V200R013C00, V200R019C00, V200R019C10, V200R020C00, V200R020C10, V200R021C00, V200R021C10, V200R022C00, V200R022C10, V200R023C00	Service port connections using ordinary and dedicated cables	All S6720-EI switches support stacking.
S6720-HI	V200R012C00, V200R013C00, V200R019C00, V200R019C10	Service port connections using ordinary and dedicated cables	All S6720-HI switches support stacking.

Product	Software Version	Stack Connection Mode	Product Model
S6720S-EI	Versions supporting service port connection using ordinary cables: V200R009C00, V200R010C00, V200R011C00, V200R011C10, V200R012C00, V200R013C00, V200R019C00, V200R019C10, V200R020C00, V200R020C10, V200R021C00, V200R021C10, V200R022C00, V200R022C10, V200R023C00 Versions supporting service port connection using dedicated cables: V200R011C10, V200R012C00, V200R013C00, V200R019C00, V200R019C10, V200R020C00, V200R020C10, V200R021C00, V200R021C10, V200R022C00, V200R022C10, V200R023C00	Service port connections using ordinary and dedicated cables	All S6720S-EI switches support stacking.
S6720S-S	V200R020C00, V200R020C10, V200R020C30, V200R021C00, V200R021C01, V200R021C10, V200R022C00, V200R022C10, V200R023C00	Service port connection using ordinary cables	All S6720S-S switches support stacking.

Product	Software Version	Stack Connection Mode	Product Model
S6720-SI and S6720S-SI	Versions supporting service port connection using ordinary cables: V200R011C00, V200R011C10, V200R012C00, V200R013C00, V200R019C00, V200R019C10 Versions supporting service port connection using dedicated cables: V200R011C10, V200R012C00, V200R013C00, V200R019C00, V200R019C10	Service port connections using ordinary and dedicated cables	All S6720-SI and S6720S-SI switches support stacking.
S6720-LI and S6720S-LI	Versions supporting service port connection using ordinary cables: V200R011C00, V200R011C10, V200R012C00, V200R013C00, V200R019C00, V200R019C10 Versions supporting service port connection using dedicated cables: V200R011C10, V200R012C00, V200R013C00, V200R019C00, V200R019C10	Service port connections using ordinary and dedicated cables	All S6720-LI and S6720S-LI switches support stacking.
S6730-H	V200R013C02, V200R019C00, V200R019C10, V200R020C00, V200R020C10, V200R021C00, V200R021C10, V200R022C00, V200R022C10, V200R023C00	Service port connections using ordinary and dedicated cables	All S6730-H switches support stacking.

Product	Software Version	Stack Connection Mode	Product Model
S6730S-H	V200R019C10, V200R020C00, V200R020C10, V200R021C00, V200R021C10, V200R022C00, V200R022C10, V200R023C00	Service port connections using ordinary and dedicated cables	All S6730S-H switches support stacking.
S6730-S and S6730S-S	V200R019C00, V200R019C10, V200R020C00, V200R020C10, V200R021C00, V200R021C10, V200R022C00, V200R022C10, V200R023C00	Service port connections using ordinary and dedicated cables	All S6730-S and S6730S-S switches support stacking.
S6735-S	V200R021C00SPC600, V200R021C01, V200R021C10, V200R022C00, V200R022C10, V200R023C00	Service port connections using ordinary and dedicated cables	All S6735-S switches support stacking.

3.3.2 display mad

Function

The **display mad** command displays the multi-active detection (MAD) configuration.

Format

display mad [**proxy** | **verbose**]

Parameters

Parameter	Description	Value
proxy	Displays information about the proxy device.	-
verbose	Displays detailed MAD configuration.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

To check the MAD configuration, run the **display mad** command. If the **verbose** parameter is specified, detailed MAD configuration is displayed, including MAD-enabled interfaces and interfaces excluded from shutdown.

When MAD in relay mode is configured, you can run the **display mad proxy** command on the proxy device to check its MAD configuration.

Example

Display MAD configuration.

```
<HUAWEI> display mad
Current MAD domain: 0
MAD direct detection enabled: YES
MAD relay detection enabled: NO
```

Display detailed MAD configuration.

```
<HUAWEI> display mad verbose
Current MAD domain: 0
Current MAD status: Detect
Mad direct detect interfaces configured:
 GigabitEthernet2/0/8
 GigabitEthernet2/0/9
Mad relay detect interfaces configured:
Excluded ports(configurable):
 GigabitEthernet2/0/4
Excluded ports(can not be configured):
```

Display information about the specified proxy device.

```
<HUAWEI> display mad proxy
Mad relay interfaces configured:
 Eth-Trunk1
```

Table 3-51 Description of the **display mad** command output

Item	Description
Current MAD domain	MAD domain configured in the system. To configure this parameter, run the **mad domain** command.
MAD direct detection enabled	MAD in direct mode is configured. To configure MAD in direct mode, run the **mad detect mode direct** command.
MAD relay detection enabled	MAD in relay mode is configured. To configure MAD in relay mode, run the **mad detect mode relay** command.

Item	Description
Current MAD status	Current MAD status: • Detect: The stack is running properly. • Recovery: The switch that fails master switch election in a MAD scenario enters the Recovery state and blocks all of its service ports except those excluded from shutdown.
Mad direct detect interfaces configured	Interface on which MAD in direct mode is configured. To configure MAD in direct mode on an interface, run the **mad detect mode direct** command.
Mad relay detect interfaces configured	Interface on which MAD in relay mode is configured. To configure MAD in relay mode on an interface, run the **mad detect mode relay** command.
Excluded ports(configurable)	Interfaces excluded from shutdown. To configure interfaces excluded from shutdown, run the **mad exclude** command.
Excluded ports(can not be configured)	Interfaces that are excluded from shutdown in the system by default.
Mad relay interfaces configured	Interface on which the relay function is configured. To configure the relay function on an interface, run the **mad relay** command.

3.3.3 display stack

Function

The **display stack** command displays information about the member switches in a stack.

Format

display stack

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

To check stack information, including stack topology and stack member switches, run the **display stack** command.

This command can be used only after the stack function is enabled (default status).

Example

Display stack information.

```
<HUAWEI> display stack
Stack mode: Service-port
Stack topology type: Link
Stack system MAC: xxxx-xxxx-xxxx
MAC switch delay time: 10 min
Stack reserved VLAN: 4093
Slot of the active management port: 0
Slot    Role        MAC address       Priority   Device type
--------------------------------------------------------------
   0   Master      xxxx-xxxx-xxxx   200          S5720-28P-LI-AC
   1   Standby     xxxx-xxxx-xxxx   150          S5720-28P-LI-AC
```

Table 3-52 Description of the **display stack** command output

Item	Description
Stack mode	Stack connection mode supported by the switch: • Service-port: Service port connection • Card: Stack card connection
Stack topology type	Stack topology type: • Link: chain topology • Ring: ring topology
Stack system MAC	Stack system MAC address.
MAC switch delay time	Time after which the system MAC address of the stack is switched. To configure this parameter, run the **stack timer mac-address switch-delay** command.

Item	Description
Stack reserved VLAN	Stack reserved VLAN. To configure this parameter, run the **stack reserved-vlan** command.
Active management slot	Slot ID of the effective management interface in the stack. If no member switch in the stack has a management interface or all the management interfaces are Down, this field displays **--**. **NOTE** After a stack is set up, you can log in to the stack through any member switch's management interface or console interface. A stack can have only one effective management interface at a time.
Slot	Stack ID of the member switch.
Role	Member switch role: • Master • Standby • Slave
MAC address	MAC address of the member switch.
Priority	Stack priority. To configure this parameter, run the **stack slot priority** command.
Device Type	Device model of the member switch.

3.3.4 display stack peers

Function

The **display stack peers** command displays information about the neighbors of a member switch.

Format

display stack peers

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

To check information about the neighbors of a member switch, run the **display stack peers** command.

This command can be used only after the stack function is enabled (default status).

Example

Display information about the neighbors of a member switch.

```
<HUAWEI> display stack peers
(B): Block all
Slot      Port1               Peer1      Port2               Peer2
------------------------------------------------------------------------------
0         STACK 1               1        STACK 2             None
1         STACK 1             None       STACK 2               0
```

Table 3-53 Description of the **display stack peers** command output

Item	Description
(B): Block all	Indicates that the stack port is blocked.
Slot	Stack ID of a member switch.
Port1	Stack port 1.
Peer1	Stack ID of the switch to which stack port 1 connects. If this field displays **ID(B)**, stack port 1 is blocked. If this field displays **None**, there is no peer device.
Port2	Stack port 2.
Peer2	Stack ID of the switch to which stack port 2 connects. If this field displays **ID(B)**, stack port 2 is blocked. If this field displays **None**, there is no peer device.

3.3.5 display stack port

Function

The **display stack port** command displays information about stack ports.

Format

display stack port [**brief** | **slot** *slot-id*]

Parameters

Parameter	Description	Value
brief	Displays summary of stack ports.	-
slot *slot-id*	Displays configuration of stack ports on a specified switch. *slot-id* specifies the stack ID of a switch.	Set the value according to the device configuration.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display stack port** command to check summary and detailed information about stack ports.

Example

Display summary of stack ports on the S5720-LI (service port connection).

```
<HUAWEI> display stack port brief
PHY     :Physical state
Protocol:Stack link protocol state
*down   :administratively down
(r)     :Runts trigger error down
(c)     :CRC trigger error down
(l)     :Link-flapping trigger error down
(m)     :Media mismatch trigger error down
Stack Port              PHY    Protocol  InUti  OutUti    InErrors   OutErrors
--------------------------------------------------------------------------------
stack-port0/1           up     up        0.00%  0.00%     0          0
  XGigabitEthernet0/0/1 up     up        0.00%  0.00%     0          0
  XGigabitEthernet0/0/2 up     up        0.00%  0.00%     0          0
stack-port0/2           up     up        0.00%  0.00%     0          0
  XGigabitEthernet0/0/3 up     up        0.00%  0.00%     0          0
  XGigabitEthernet0/0/4 up     up        0.00%  0.00%     0          0
```

Display summary of stack ports on the S6720-EI (service port connection).

```
<HUAWEI> display stack port brief
PHY     :Physical state
Protocol:Stack link protocol state
*down   :administratively down
(r)     :Runts trigger error down
(c)     :CRC trigger error down
(l)     :Link-flapping trigger error down
(m)     :Media mismatch trigger error down
Stack Port              PHY    Protocol  InUti  OutUti    InErrors   OutErrors
--------------------------------------------------------------------------------
stack-port0/1
  XGigabitEthernet0/0/1 down   down      0.00%  0.00%     0
0
```

```
unAllocated
  XGigabitEthernet0/0/2  down  --      0.00%  0.00%        0        0
  XGigabitEthernet0/0/3  down  --      0.00%  0.00%        0        0
  XGigabitEthernet0/0/4  down  --      0.00%  0.00%        0        0
```

Table 3-54 Description of the **display stack port brief** command output

Item	Description
Stack Port	Number of a stack port. unAllocated indicates that a service port has become a stack member port but has not been bound to a logical stack port.
PHY	Physical status of an interface: ● down: The interface is physically disabled. ● up: The interface is physically enabled. ● *down: The interface is manually shut down. ● down(r): Runts error continuously occurs on a stack port. ● down(c): There are CRC error packets on a stack port. ● down(l): A stack port repeatedly alternates between Up and Down states. ● down(m): The rate of the optical module installed in a stack member port is not the rate required by the member port. ● down(s): A self-loop occurs on a stack port. **NOTE** Only the S5736-S, S5735-L, S5735S-L, S5735-L-I, S5735-L1,S5735S-L1, S5735S-L-M, S5735-S, S5735-S-I, S5735S-S, S5735S-H, and S6720S-S support this status.
Protocol	Link layer protocol status of the interface: ● down: A stack port does not receive stack link packets. ● up: A stack port can receive stack link detection packets.
InUti	Average inbound bandwidth usage of an interface within the last 300 seconds.
OutUti	Average outbound bandwidth usage within the last 300 seconds.
InErrors	Number of error packets received by an interface.
OutErrors	Number of error packets sent by an interface.

Display detailed information about stack ports (stack card connection).

```
<HUAWEI> display stack port
stack-port1/1:
--------------------------------------------
```



```
Current state : DOWN
Speed : NA

Input:  0 packets, 0 bytes
  Unicast:                0,  Multicast:                0
  Broadcast:              0,  Jumbo:                    0
  Discard:                0,  Frames:                   0

  Total Error:            0
  CRC:                    0,  Giants:                   0
  Jabbers:                0,  Fragments:                0
  Runts:                  0,  DropEvents:               0
  Alignments:             0,  Symbols:                  0
  Ignoreds:               0

Output:  0 packets, 0 bytes
  Unicast:                0,  Multicast:                0
  Broadcast:              0,  Jumbo:                    0
  Discard:                0

  Total Error:            0
  Collisions:             0,  ExcessiveCollisions:      0
  Late Collisions:        0,  Deferreds:                0
  Buffers Purged:         0


stack-port1/2:
-------------------------------------------
Current state : DOWN
Speed : NA

Input:  0 packets, 0 bytes
  Unicast:                0,  Multicast:                0
  Broadcast:              0,  Jumbo:                    0
  Discard:                0,  Frames:                   0

  Total Error:            0
  CRC:                    0,  Giants:                   0
  Jabbers:                0,  Fragments:                0
  Runts:                  0,  DropEvents:               0
  Alignments:             0,  Symbols:                  0
  Ignoreds:               0

Output:  0 packets, 0 bytes
  Unicast:                0,  Multicast:                0
  Broadcast:              0,  Jumbo:                    0
  Discard:                0

  Total Error:            0
  Collisions:             0,  ExcessiveCollisions:      0
  Late Collisions:        0,  Deferreds:                0
  Buffers Purged:         0
```

Table 3-55 Description of the **display stack port** command output (stack card connection)

Item	Description
stack-port1/1	Stack port 1 in slot 1.
Speed	Interface forwarding rate.
current state	Stack port status: • DOWN: The stack port is disabled. • UP: The stack port is enabled.

Item	Description
Input	Total number of packets received by the stack port.
Output	Total number of packets sent by the stack port.
Unicast	Number of unicast packets sent or received by the stack port.
Multicast	Number of multicast packets sent or received by the stack port.
Broadcast	Number of broadcast packets sent or received by the stack port.
Jumbo	Number of jumbo frames sent or received by the stack port.
Discard	Number of packets discarded by the stack port during physical layer detection.
Total Error	Total number of error packets found by the stack port during physical layer detection.
CRC	Number of CRC error packets received by the stack port.
Giants	Number of jumbo frames with correct FCS received by the stack port.
Jabbers	Number of jumbo frames with incorrect FCS received by the stack port.
Fragments	Number of undersized frames with incorrect FCS received by the stack port.
Runts	Number of undersized frames with correct FCS received by the stack port.
DropEvents	Number of received packets that are discarded because the GBP is full or there is back pressure.
Alignments	Number of frames with alignment errors received by the stack port.
Symbols	Number of coding error frames received by the stack port.
Ignoreds	Number of received MAC control frames whose OpCode is not PAUSE.
Frames	Number of packets with an incorrect 802.3 length received by the stack port.
Collisions	Number of packets that encountered 1 to 15 conflicts and sent by the stack port.
ExcessiveCollisions	Number of packets that encountered 16 conflicts and fail to be sent by the stack port.

Item	Description
Late Collisions	Number of packets sent by the stack port after a delay due to conflicts.
Deferreds	Number of packets sent by the stack port after a delay without any conflict.
Buffers Purged	Number of packets aged due to existence in the buffer for an extended time before being sent out by the stack port.

Display detailed information about stack ports (service port connection).

```
<HUAWEI> display stack port
*down : administratively down
Logic Port        Phy Port                  Online      Status
--------------------------------------------------------------------------------
stack-port0/1     XGigabitEthernet0/0/1       present     up
                  XGigabitEthernet0/0/2       present     down
                  XGigabitEthernet0/0/4       present     down
stack-port0/2     XGigabitEthernet0/0/3       present     up
stack-port3/1     XGigabitEthernet3/0/1       present     up
stack-port3/2     XGigabitEthernet3/0/3       present     up
stack-port4/1     XGigabitEthernet4/0/1       present     up
stack-port4/2     XGigabitEthernet4/0/3       present     up
stack-port8/1     XGigabitEthernet8/0/1       present     up
stack-port8/2     XGigabitEthernet8/0/3       present     up
```

Table 3-56 Description of the **display stack port** command output (service port connection)

Item	Description
Logic Port	Number of a stack port.
Phy Port	Type and number of a physical member port.
Online	Presence of a physical member port. • present: The current installed service card type is consistent with that configured on the switch. • absent: The current installed service card type is inconsistent with that configured on the switch.

Item	Description
Status	Physical status of an interface: • down: The interface is physically disabled. • up: The interface is physically enabled. • *down: The interface is manually shut down. • down(r): Runts error continuously occurs on a stack port. • down(c): There are CRC error packets on a stack port. • down(l): A stack port repeatedly alternates between Up and Down states. • down(m): The rate of the optical module installed in a stack member port is not the rate required by the member port. • down(s): A self-loop occurs on a stack port. **NOTE** Only the S5736-S, S5735-L, S5735S-L, S5735-L-I, S5735-L1,S5735S-L1, S5735S-L-M, S5735-S, S5735-S-I, S5735S-S, S5735S-H, and S6720S-S support this status.

3.3.6 display stack port auto-cable-info

Function

The **display stack port auto-cable-info** command displays information about dedicated stack cables.

Format

display stack port auto-cable-info slot *slot-id*

Parameters

Parameter	Description	Value
slot *slot-id*	Specifies the stack ID of a member switch.	The value range depends on the device.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display stack port auto-cable-info** command to check interfaces supporting dedicated stack cables and whether dedicated stack cables have been connected to interfaces.

Example

Display information about dedicated stack cables on the switch with the slot ID 0.

```
<HUAWEI> display stack port auto-cable-info slot 0
Logic Port       Phy Port                 Cable-role
------------------------------------------------------------
stack-port0/1    XGigabitEthernet0/0/1    Slave
stack-port0/1    XGigabitEthernet0/0/2    --
stack-port0/2    XGigabitEthernet0/0/3    --
stack-port0/2    XGigabitEthernet0/0/4    Master
```

Table 3-57 Description of the **display stack port auto-cable-info** command output

Item	Description
Logic Port	Logical stack port.
Phy Port	Physical member port.
Cable-role	Role of a dedicated stack cable: • Master: The installed dedicated stack cable is the master end. • Slave: The installed dedicated stack cable is the slave end. • --: No dedicated stack cable is connected to the current port.

3.3.7 display stack port speed

Function

The **display stack port speed** command displays the stack port working speed.

NOTE

Only the S5720-X-LI, S5720I-SI, S5732-H, and S5720S-X-LI support this command.

The S5720-P-LI does not support this command before the license is loaded and supports this command after the license is loaded and it restarts.

Format

display stack port speed

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display stack port speed** command to check the stack port's current working speed and working speed taking effect after a restart. To set the stack port working speed, run the **stack port speed** command.

Example

Display the stack port's current working speed and working speed taking effect after a restart.

```
<HUAWEI> display stack port speed
Stack Port                Current Speed    Next Speed
-------------------------------------------------------
stack-port2/1
  XGigabitEthernet2/0/1   10G              12G
stack-port2/2
  XGigabitEthernet2/0/4   10G              12G
stack-port3/1
  XGigabitEthernet3/0/1   10G              12G
  XGigabitEthernet3/0/3   10G              12G
stack-port3/2
  XGigabitEthernet3/0/28  10G              12G
  XGigabitEthernet3/0/30  10G              12G
```

Table 3-58 Description of the **display stack port speed** command output

Item	Description
Stack Port	Stack port.
Current Speed	Stack port's current working speed.
Next Speed	Stack port's working speed taking effect after a restart. To configure the parameter, run the **stack port speed** command.

3.3.8 display stack-port load-balance

Function

The **display stack-port load-balance** command displays the load balancing modes of stack ports.

NOTE

Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S support this command.

Format

display stack-port { **global load-balance** | **load-balance** [*slot-id*/*port-id*] }

Parameters

Parameter	Description	Value
slot-id	Specifies the stack ID of a member switch.	The value is an integer that ranges from 0 to 8.
port-id	Specifies the ID of a stack port.	The value is 1 or 2.
global	Displays the global load balancing mode. **NOTE** The S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S only support this parameter.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display stack-port load-balance** command to check the load balancing modes of stack ports and then locate data transmission failures between stack links.

Example

Display the load balancing modes of stack ports.


```
<HUAWEI> display stack-port load-balance
Global load balance mode: ENHANCED
Stack-port0/1 load balance mode: ENHANCED
Stack-port0/2 load balance mode: ENHANCED
Stack-port1/1 load balance mode: DST-MAC
Stack-port1/2 load balance mode: SRC-MAC
Stack-port2/1 load balance mode: DST-IP
Stack-port2/2 load balance mode: SRC-DST-IP
```

Table 3-59 Description of the **display stack-port load-balance** command output

Item	Description
Global load balance mode	Global load balancing mode: • DST-IP: performs load balancing based on destination IP addresses. • DST-MAC: performs load balancing based on destination MAC addresses. • SRC-IP: performs load balancing based on source IP addresses. • SRC-MAC: performs load balancing based on source MAC addresses. • SRC-DST-IP: performs load balancing based on the Exclusive-OR result of source and destination IP addresses. • SRC-DST-MAC: performs load balancing based on the Exclusive-OR result of source and destination MAC addresses. • ENHANCED: enhanced load balancing mode, that is, load balancing based on the Exclusive-OR result of the source and destination MAC addresses. To set the global load balancing mode, run the **stack-port load-balance mode** command in the system view.

Item	Description
Stack-port0/1 load balance mode Stack-port0/2 load balance mode Stack-port1/1 load balance mode Stack-port1/2 load balance mode Stack-port2/1 load balance mode Stack-port2/2 load balance mode	Load balancing mode of a stack port: • DST-IP: performs load balancing based on destination IP addresses. • DST-MAC: performs load balancing based on destination MAC addresses. • SRC-IP: performs load balancing based on source IP addresses. • SRC-MAC: performs load balancing based on source MAC addresses. • SRC-DST-IP: performs load balancing based on the Exclusive-OR result of source and destination IP addresses. • SRC-DST-MAC: performs load balancing based on the Exclusive-OR result of source and destination MAC addresses. • ENHANCED: enhanced load balancing mode, that is, load balancing based on the Exclusive-OR result of the source and destination MAC addresses. To set the load balancing mode for a stack port, run the **stack-port load-balance mode** command in the stack port view.

3.3.9 display stack configuration

Function

The **display stack configuration** command displays stack configuration commands configured in a stack.

Format

display stack configuration [**slot** *slot-id*]

Parameters

Parameter	Description	Value
slot *slot-id*	Displays the stack commands configured on a stack member switch. *slot-id* specifies the stack ID of the member switch.	The value range depends on the device configuration.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

Stack configuration will only be written to the flash memory instead of the configuration file. As a result, Stack configuration cannot be obtained through the configuration file. To view stack configuration, run the **display stack configuration** command.

Precautions

- This command is valid only when the stack function is enabled and has taken effect. By default, the stack function is enabled.
- This command displays only the stack commands that have been executed. The displayed command configuration is not necessarily the running stack configuration, because most stack configuration commands take effect after a system restart.

Example

Display the stack configuration commands that have been executed in a stack.

```
<HUAWEI> display stack configuration
*    : Invalid-configuration
#    : Unsaved configuration
---------------Configuration on slot 2
Begin---------------

stack enable
stack slot 0 renumber 2
stack slot 2 priority 150
stack reserved-vlan 4093
stack timer mac-address switch-delay 10

interface stack-port 2/1
 *port interface XGigabitEthernet2/0/1 enable

interface stack-port 2/2
 #port interface XGigabitEthernet2/0/4 enable
---------------Configuration on slot 2 End-----------------
```

- If a stack member port is marked with an asterisk (*), the current configuration does not take effect because of the following reasons:
  - The current configuration is the preconfiguration that has not taken effect.
  - Insert different types of subcards.
  - The stack member port is located on a subcard that is not available.
  - When ports on the device panel and ports on subcards cannot be used together, one of the two port types is configured as stack member ports but not configured as the ports that take effect on the device, and the device is restarted.
- If a stack member port is marked with a number sign (#), the current configuration is automatically generated for dedicated cable stacking but not

saved to the flash memory using the **save stack configuration** or **save** command.

- If a stack member port is marked with *#, the switch is using stack card stacking. In this case, the **display stack configuration** command displays the stack configuration that is automatically generated after dedicated stack cables are installed. To change stack card stacking to dedicated stack cable stacking, run the **save stack configuration** or **save** command to save the stack configuration to the flash memory and then restart the switch.

3.3.10 display stack channel

Function

The **display stack channel all** command displays stack link connections and status.

Format

display stack channel [**all** | **slot** *slot-id*]

Parameters

Parameter	Description	Value
all	Displays stack link connections and status of all the member switches.	-
slot *slot-id*	Displays stack link connections and status of the member switch with a specified stack ID.	The value range depends on the device configuration.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

To check stack link connections and status, run the **display stack channel all** command. If you do not specify **all** or **slot** *slot-id* in the command, this command displays the stack link connections and status of the master switch.

Example

Display stack link connections and status of all the member switches.

```
<HUAWEI> display stack channel all
!    : Port have received packets with CRC error.
L-Port: Logic stack port
```

```
P-Port: Physical port
Slot  L-Port  P-Port    Speed  State  ||  P-Port    Speed  State  L-Port  Slot
------------------------------------------------------------------------------
1     1/2     GE1/0/28  2.5G   UP         GE2/0/27  2.5G   UP     2/1     2
2     2/1     GE2/0/27  2.5G   UP         GE1/0/28  2.5G   UP     1/2     1
------------------------------------------------------------------------------
```

The following output information shows that the physical member port GE1/0/28 works at 2.5 Gbit/s and is in Up state; it is bound to stack port 1/2 and belongs to the member switch with stack ID 1; GE1/0/28 is connected to the physical member port GE2/0/27; GE2/0/27 works at 2.5 Gbit/s and is in Up state; It is bound to stack port 2/1 and belongs to member switch with stack ID 2.

```
1     1/2     GE1/0/28  2.5G   UP         GE2/0/27  2.5G   UP     2/1     2
```

Table 3-60 Description of the **display stack channel** command output

Item	Description
!	A physical member port has received CRC error packets. **NOTE** If a physical member port receives CRC error packets, its **Speed** field displays the speed value and an exclamation mark (!), for example, 2.5G!.
Slot	Stack ID of a device.
L-Port	Number of a stack port.
P-Port	Number of a physical member port.
Speed	Speed of a physical member port.
Status	Status of a physical member port.

3.3.11 display upgrade area

Function

The **display upgrade area** command displays area status and whether a smooth upgrade can start.

Format

display upgrade area

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

If the stack topology changes after the areas for smooth upgrade are divided, members in the active and backup areas may change, resulting in a smooth upgrade failure. To check whether a smooth upgrade can start in these areas, run the **display upgrade area** command.

If the areas fail the check, re-define the active and backup areas according to the current stack topology.

The active area contains the master switch.

Example

Display the current area status and whether a smooth upgrade can start.

```
<HUAWEI> display upgrade area
Slot      Area         Upgrade-Check
-------------------------------------
  0      backup        passed
  3      active        passed
  4      active        passed
  8      active        passed
```

Table 3-61 Description of the **display upgrade area** command output

Item	Description
Slot	Stack ID of a device.
Area	Area to which a device belongs. • active • backup • unknown: The device does not belong to any area.
Upgrade-Check	Upgrade check result. • passed • failed

3.3.12 display upgrade state

Function

The **display upgrade state** command displays the smooth upgrade status of member switches in a stack.

Format

display upgrade state [**slot** *slot-id*]

Parameters

Parameter	Description	Value
slot *slot-id*	Specifies the stack ID of a member switch.	The value is an integer that ranges from 0 to 8.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

To check the status of member switches in the active and backup areas before or after a smooth upgrade, run the **display upgrade state** command.

If you specify the **slot** *slot-id* parameter in the command, you can check whether the member switch with this slot ID has been upgraded successfully.

If the master switch of a stack restarts or experiences a master/standby switchover after a smooth upgrade, area information will be deleted from the master switch, and the **Area** field of the master switch will be displayed as **unknown**.

Example

Display the smooth upgrade status of member switches in a stack.

```
<HUAWEI> display upgrade state
Slot      Area         Status
-----------------------------
  0      backup       backup rebooting
  3      backup       backup rebooting
  4      active       backup rebooting
  8      active       backup rebooting
```

Display the smooth upgrade status of the member switch with stack ID 4.

```
<HUAWEI> display upgrade state slot 4
--------------------------------------
 Slot        : 4
 Area        : backup
 Status      : successful
 ErrorCode   : 0
 Description :
--------------------------------------
```

Table 3-62 Description of the **display upgrade state** command output

Item	Description
Slot	Stack ID of a device.

Item	Description
Area	Area to which a device belongs. • active • backup • unknown: The device does not belong to any area.
Status	Upgrade progress of a device. • idle: The upgrade has not been performed yet. • backup rebooting: The backup area is upgrading. • active rebooting: The active area is upgrading. • failed: The upgrade failed. • successful: The upgrade succeeded.
ErrorCode	Error code of an upgrade failure. For details, see **3.3.38 upgrade start**. The value 0 indicates that the upgrade succeeded.
Description	Description about the failure if an upgrade fails.

3.3.13 interface stack-port

Function

The **interface stack-port** command displays the stack port view.

NOTE

Only devices supporting service port stacking support this command.

Format

interface stack-port *member-id*/*port-id*

Parameters

Parameter	Description	Value
member-id	Specifies the stack ID of a member switch.	The value is an integer that ranges from 0 to 8.
port-id	Specifies a stack port number.	The value is 1 or 2.

Views

System view

Default Level

3: Management level

Usage Guidelines

Each member switch has two stack ports, which are named Stack-Port*n*/1 and Stack-Port*n*/2. *n* specifies the stack ID of a member switch. After you run the **interface stack-port** command to enter the view of a stack port, you can configure attributes for the stack port.

Example

Display the view of Stack-Port1/1.

```
<HUAWEI> system-view
[HUAWEI] interface stack-port 1/1
[HUAWEI-stack-port1/1]
```

3.3.14 mad backup ip address

Function

The **mad backup ip address** command configures a backup IP address for the management interface in a stack.

The **undo backup ip address** command deletes the backup IP address for the management interface in a stack.

By default, no backup IP address is configured for the management interface in a stack.

Format

mad backup ip address *ip-address* { *mask* | *mask-length* }

undo mad backup ip address

Parameters

Parameter	Description	Value
ip-address	Specifies the backup IP address for the management interface.	The value is in dotted decimal notation.
mask	Specifies the subnet mask of the backup IP address for the management interface.	The value is in dotted decimal notation.
mask-length	Specifies the mask length of the backup IP address for the management interface.	The value is an integer that ranges from 0 to 32.

Views

MEth0/0/1 management interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When MAD detects a stack split fault, all interfaces (including the management interface) of the member device that fails in the election are shut down to prevent network flapping caused by identical MAC and IP addresses, reducing the impact on the network. After the management interface of the member device is shut down, you cannot remotely log in to and manage the device, and can only log in to the device through the console interface, which is inconvenient for device maintenance.

To prevent this problem, you can configure a backup IP address for the management interface on the device. If the stack splits, the IP address of the management interface on the member device that fails in the election is set to the configured backup IP address. This prevents packet forwarding from being affected due to conflicting management IP addresses upon the stack split. In addition, you can remotely log in to and manage the device, which facilitates device maintenance.

If the stack splits after a backup IP address is configured for the management interface on the device, the management interface on the member device that fails in the election is not shut down, and only the backup IP address is configured as the IP address of the management interface. Other non-reserved service interfaces are still shut down.

Precautions

- This command does not take effect if the device does not have a management interface.
- The backup IP address cannot be on the same network segment as the IP addresses used by other interfaces on the device. Otherwise, the function does not take effect due to address conflicts.
- This command can only be used to configure the IP address of the management interface, regardless of the Up/Down status of the management interface. For example, if the management interface is shut down using a command or the management interface is not connected using a cable, the management interface is Down.

Example

Configure a backup IP address for the management interface in a stack.

```
<HUAWEI> system-view
[HUAWEI] interface meth 0/0/1
[HUAWEI-MEth0/0/1] mad backup ip address 10.1.1.1 24
```


3.3.15 mad detect mode direct

Function

The **mad detect mode direct** command configures multi-active detection (MAD) in direct mode on an interface.

The **undo mad detect** command cancels the configuration.

By default, MAD in direct mode is disabled on an interface.

Format

mad detect mode direct

undo mad detect [**mode direct**]

Parameters

None

Views

GE interface view, XGE interface view, 25GE interface view, 40GE interface view, port group view, MultiGE interface view, 100GE interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To ensure that only one switch becomes the master switch after a stack splits, thereby enhancing stack stability, run the **mad detect mode direct** command to configure MAD in direct mode on an interface.

Configuration Impact

Configuring MAD in direct mode on an interface blocks the interface. Disabling MAD in direct mode on an interface restores the forwarding function of the interface. If a loop exists on the network, a broadcast storm occurs.

Precautions

The **undo mad detect** command is not supported in the port group view. You can only run the **undo mad detect mode direct** command in the port group view to disable MAD in direct mode.

Example

Configure MAD in direct mode on GigabitEthernet0/0/1.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
```



```
[HUAWEI-GigabitEthernet0/0/1] mad detect mode direct
Warning: This command will block the port, and no other configuration running on this port is
recommended. Continue? [Y/N]:y
```

3.3.16 mad detect mode relay

Function

The **mad detect mode relay** command configures multi-active detection (MAD) in relay mode on an interface.

The **undo mad detect** command cancels the configuration.

By default, MAD in relay mode is disabled on an interface.

Format

mad detect mode relay

undo mad detect [**mode relay**]

Parameters

None

Views

Eth-Trunk interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To ensure that only one switch becomes the master switch after a stack splits, thereby enhancing stability of the stack, run the **mad detect mode relay** command to configure MAD in relay mode on an Eth-trunk.

Precautions

The **undo mad detect** command is not supported in the port group view. You can only run the **undo mad detect mode relay** command in the port group view to disable MAD in relay mode.

Example

Configure MAD in relay mode on Eth-Trunk 10.

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


3.3.17 mad domain

Function

The **mad domain** command sets a MAD domain ID for a stack.

The **undo mad domain** command restores the default MAD domain ID for a stack.

By default, the MAD domain ID of a stack is 0.

Format

mad domain *domain-id*

undo mad domain

Parameters

Parameter	Description	Value
domain-id	Specifies the MAD domain ID for a stack.	The value is an integer that ranges from 0 to 255.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

In most MAD scenarios, configuring a MAD domain ID for a stack is unnecessary. When two stack systems function as a proxy of each other to implement MAD, configure different MAD domain IDs for the stack systems.

Example

Set the MAD domain ID for a stack to 1.

```
<HUAWEI> system-view
[HUAWEI] mad domain 1
```

3.3.18 mad exclude

Function

The **mad exclude** command excludes specified interfaces of a stack from shutdown.

The **undo mad exclude** command cancels excluding specified interfaces of a stack from shutdown.

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

Format

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

undo mad 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

Usage Scenario

If MAD detects a stack split, all service ports of the member switch that fails master switch election must be shut down to prevent network flapping caused by MAC or IP address flapping. If some interfaces only transparently transmit packets, they do not affect network operation in a dual-active condition. You can run the **mad exclude** command to exclude these interfaces from shutdown before a stack split occurs.

Precautions

- After an interface is shut down because of MAD, it cannot be enabled if the **mad exclude** command is executed to exclude it from shutdown.
- When the **to** parameter is specified to exclude multiple ports from shutdown, these ports must reside on the same card and the port number following this parameter must be larger than the port number followed by this parameter.

Example

Exclude GigabitEthernet0/0/2 and GigabitEthernet0/0/3 from shutdown.


```
<HUAWEI> system-view
[HUAWEI] mad exclude interface gigabitethernet 0/0/2 to gigabitethernet 0/0/3
```

3.3.19 mad relay

Function

The **mad relay** command enables the relay function on an interface of a proxy device.

The **undo mad relay** command disables the relay function on an interface of a proxy device.

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

Format

mad relay

undo mad relay

Parameters

None

Views

Eth-Trunk interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

For MAD working in relay mode, run the **mad relay** command to configure the relay function on an Eth-Trunk interface of a proxy device. Member interfaces of the Eth-Trunk interface exchange MAD packets between member switches.

Example

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

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

3.3.20 mad restore

Function

The **mad restore** command restores all the blocked interfaces of a standby switch that enters the Recovery state after its stack splits.

Format

mad restore

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

When MAD detects a multi-active event, the member switch elected as the master switch remains in the Detect state. The elected standby switch enters the Recovery state, shuts down all its service ports except those excluded from shutdown, and stops forwarding service packets.

If the switch in the Detect state fails or is removed before the split stack is restored, run the **mad restore** command on the switch in the Recovery state to restore the interfaces in shutdown state. The switch in the Recovery state then goes to the Detect state. You can then restore the original switch in the Detect state and rectify the faulty stack links. After the faults are rectified, the two switches form a stack again.

Example

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

```
<HUAWEI> system-view
[HUAWEI] mad restore
```

3.3.21 port interface enable

Function

The **port interface enable** command configures a service interface as a physical member port and adds it to a stack port.

The **undo port interface enable** command restores a physical member port to being a service interface.

By default, service interfaces are not used as physical member ports of a stack port.

NOTE

Only the switches supporting service port stacking support this command.

Format

port interface { *interface-type interface-number1* [**to** *interface-type interface-number2*] } &<1-10> **enable**

undo port interface { *interface-type interface-number1* [**to** *interface-type interface-number2*] } &<1-10> **enable**

Parameters

Parameter	Description	Value
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

Stack interface view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

In service interface connection mode, run the **port interface enable** command to configure a service interface as a physical member port to implement the stack function.

Configuration Impact

A stack physical member port supports only stack-related functions, and other functions cannot be configured on the interface. All the commands irrelevant to the stack function are masked in the interface view, and only basic configuration commands, such as **description**, are retained.

After configuring a service port of a switch as a physical stack member port, you are advised to save the configuration if this service port has been referenced by other commands. Otherwise, the commands that reference this service port may be retained after the switch restarts.

On the S5720I-SI, S5735-S, S500, S5735S-S, S5735-S-I, S5735S-H, S5736-S, and S6720S-S the electrical or optical port stack configuration on the front panel is mutually exclusive with the SVF client mode configuration. If electrical or optical ports on the front panel have been configured as stack physical member ports,

SVF management VLAN cannot be configured. If an SVF management VLAN has been configured, electrical or optical ports on the front panel cannot be configured as stack physical member ports.

On the S6720-EI, S6735-S, and S6720S-EI, every four of XGE interfaces from the left are added to one group. For example, XGE interfaces numbered 1 to 4 can be added to one group, but XGE interfaces numbered 2 to 5 cannot. That is, the number of the last XGE interface in each group must be the multiple of 4. If you configure any interface in each group as a physical member port, configurations on the other three interfaces in the group will be lost and the three interfaces cannot be used as service ports.

Precautions

- The stack member ports of a logical stack port must be the same type.
- After a UCL group is created on the S5720I-SI, S5720-LI, S5720S-LI, or S5720-SI, using the **ucl-group** command, the **port interface enable** command cannot be used to configure a service interface as a stack member port.
- To restore a physical member port as a service interface, run the **shutdown interface** command in the stack port view and then run the **undo port interface enable** command.
- On the S5720I-SI, S5720-LI, S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5720S-LI, S5735-S, S500, S5735S-S, S5735-S-I, S5735S-H, S5736-S, and S6720S-S, after a service interface is configured as a stack member port, the following priority mapping rules apply to packets on this interface:
  - Packets sent to the CPU are mapped to queue 7.
  - Packets with priority 0 or 1 are mapped to queue 0.
  - Packets with priorities 2 to 7 are mapped to queues 1 to 6, respectively.
- If the switch functions as an AS in an SVF system and its downlink service ports have been configured as member ports of an uplink fabric port, all the downlink ports of the AS cannot be configured as stack member ports.

Example

Configure XGigabitEthernet0/0/28 as a physical member port and add it to stack port 0/1.

```
<HUAWEI> system-view
[HUAWEI] interface stack-port 0/1
[HUAWEI-stack-port0/1] port interface xgigabitethernet 0/0/28 enable
Warning: Enabling stack function may cause configuration loss on the interface. Continue? [Y/N]:y
Info: This operation may take a few seconds. Please wait....
```

On the S6720-EI, configure XGigabitEthernet0/0/15 as a physical member port and add it to stack port 0/1.

```
<HUAWEI> system-view
[HUAWEI] interface stack-port 0/1
[HUAWEI-stack-port0/1] port interface xgigabitethernet 0/0/15 enable
Warning: Enabling stack function may cause configuration loss on the interface XGigabitEthernet0/0/13 to XGigabitEthernet0/0/16. Continue? [Y/N]:y
Info: This operation may take a few seconds. Please wait....
Info: Ports XGigabitEthernet0/0/13 to XGigabitEthernet0/0/16 in a port group have been configured as physical stack ports.
```


3.3.22 reset stack configuration

Function

The **reset stack configuration** command clears all stack configuration. That is, this command restores the default stack configuration.

Format

reset stack configuration

Parameters

None

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

The cleared stack configuration includes: switch slot ID, stack priority, stack reserved VLAN, stack MAC address switching delay, stack port configuration, and stack port rate configuration. For example, when switches are stacked using dedicated stack cables, to ensure that slot IDs are automatically generated for the switches based on the sequence in which dedicated stack cables are connected, run the **reset stack configuration** command to clear all stack configuration.

Precautions

Running this command will cause the stack to split and member switches to restart.

Example

Clear all stack configuration.

```
<HUAWEI> system-view
[HUAWEI] reset stack configuration
Warning: This operation will clear all stack configurations and may lead to the loss of the slot ID configuration and cause the device to reset immediately. Are you sure you want to continue? [Y/N]:y
```

3.3.23 reset stack port statistics

Function

The **reset stack port statistics** command clears stack port statistics.

Format

reset stack port statistics [*slot-id*|*port-id*]

Parameters

Parameter	Description	Value
slot-id	Specifies the stack ID of a member switch.	The value is an integer that ranges from 0 to 8.
port-id	Specifies the number of a stack port.	The value is 1 or 2.

Views

User view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

Before collecting interface traffic statistics in a certain period of time, run the **reset stack port statistics** command to clear existing traffic statistics. If you do not specify the port number, statistics on all stack ports are cleared. If you specify the port number, only statistics on the specified port are cleared.

Precautions

The cleared statistics cannot be restored. Therefore, exercise caution when you run the **reset stack port statistics** command.

This command can be used only after the stack function is enabled (default status).

Example

Clear the statistics from all stack ports.

```
<HUAWEI> reset stack port statistics
```

3.3.24 save stack configuration

Function

The **save stack configuration** command saves the stack configuration automatically generated for dedicated cable stacking to the flash memory.

By default, the stack configuration automatically generated for dedicated cable stacking is not saved to the flash memory.

Format

save stack configuration

Parameters

None

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

After dedicated stack cables are connected to ports, stack configuration is automatically generated but not saved to the flash memory. If these cables are removed or other cables are connected, the stack configuration is automatically deleted. To ensure that the stack configuration still takes effect when these cables are removed or other cables are connected, run the **save stack configuration** command.

Precautions

- Removing dedicated stack cables from ports after this command is executed will cause these ports unable to automatically become service ports.
- No stack configurations can be manually modified before the stack configuration automatically generated for dedicated cable stacking is saved to the flash memory.

Example

Save the stack configuration that is automatically generated for dedicated cable stacking to the flash memory.

```
<HUAWEI> system-view
[HUAWEI] save stack configuration
Warning: This operation will save all stack configurations to flash. Are you sure you want to continue? [Y/N]:y
```

3.3.25 set l2-traffic fast-recover

Function

The **set l2-traffic fast-recover enable** command enables fast recovery of Layer 2 traffic.

The **undo set l2-traffic fast-recover enable** command disables fast recovery of Layer 2 traffic.

By default, fast recovery of Layer 2 traffic is disabled.

Format

set l2-traffic fast-recover enable

undo set l2-traffic fast-recover enable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

After fixed switches set up a stack and the standby switch starts, the standby switch restores configurations and then implements batch backup from the master switch.

By default, interfaces on the standby switch become Up when batch backup is complete. In this case, Layer 2 and Layer 3 traffic can be normally forwarded but there is a delay in Layer 2 traffic recovery. To enable fast recovery of Layer 2 traffic, run the **set l2-traffic fast-recover enable** command. Interfaces on the standby switch then immediately go Up when configuration restoration is complete. This way, however, cannot ensure Layer 3 traffic forwarding through the Up interfaces.

Example

Enable fast recovery of Layer 2 traffic.

```
<HUAWEI> system-view
[HUAWEI] set l2-traffic fast-recover enable
```

3.3.26 shutdown interface

Function

The **shutdown interface** command shuts down a physical member interface.

The **undo shutdown interface** command enables a physical member interface.

By default, a physical member interface is enabled after being configured.

NOTE

Only devices supporting service port stacking support this command.

Format

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

undo shutdown interface { *interface-type interface-number1* [**to** *interface-type interface-number2*] } &<1-10>

Parameters

Parameter	Description	Value
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

Stack interface view

Default Level

3: Management level

Usage Guidelines

To restore a physical member interface to being a service interface, run the **shutdown interface** command in the stack interface view and then run the **undo port interface enable** command.

If there is only one available link on a stack interface, running the **shutdown interface** command will change the stack status or split the stack. After you run the **undo shutdown interface** command on the stack interface, the stack will be set up again when a link on the stack interface becomes available.

Example

Shut down physical member interface XGigabitEthernet0/0/3.

```
<HUAWEI> system-view
[HUAWEI] interface stack-port 0/1
[HUAWEI-stack-port0/1] shutdown interface XGigabitEthernet0/0/3
Warning: Shutting down the last active stack-port will cause a topology change. Continue? [Y/N]:y
Info: This operation may take a few seconds. Please wait...succeeded.
```


3.3.27 stack authentication

Function

The **stack authentication** command configures the authentication mode and authentication information used when a switch needs to join a stack.

The **undo stack authentication** command deletes the authentication mode and authentication information used when a switch needs to join a stack.

By default, a switch does not need to be authenticated when joining a stack.

Format

stack authentication slot *slot-id* { **mac-address** *mac-address* | **esn** *esn-value* | **shared-key cipher** *shared-key* }

undo stack authentication slot *slot-id*

Parameters

Parameter	Description	Value
slot *slot-id*	Specifies the stack ID of a switch.	The value is an integer that ranges from 0 to 8.
mac-address *mac-address*	Configures MAC-based authentication.	The value is in H-H-H format, where H is a hexadecimal number of 1 to 4 digits.
esn *esn-value*	Configures ESN-based authentication.	The value is a string of 10 to 32 characters.
shared-key cipher *shared-key*	Configures shared key-based authentication.	The value is a string of case-sensitive characters without spaces. A plain text key contains 1 to 64 characters, and a cipher text key contains 48 to 108 characters. **NOTE** It is recommended that a shared key contains at least seven characters, including at least two types of lowercase letters, uppercase letters, digits, and special characters. The master switch and the specified slot must configure the same shared key. If a shared key is used for authentication, the master switch and the member switch specified in this command must be configured with the same shared key.

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

A switch can join a stack without being authenticated. In this situation, an attacker can add any switch to a stack to obtain the configuration file of the stack master switch, resulting in information leak. To solve this problem, configure authentication when a switch needs to join a stack. This configuration ensures that this switch joins the stack only when it is authenticated successfully.

A switch will be authenticated only when its stack ID is the same as that specified in the **stack authentication** command. Otherwise, this switch can join a stack without being authenticated. Therefore, before adding a switch to a stack, you are advised to change the slot ID of the switch to an unused stack ID in the stack and then configure an authentication mode for this stack ID.

Precautions

- This command can be executed only after the stacking function is enabled.
- Only one authentication mode can be configured for a stack ID, and the latest configuration takes effect.
- If a switch to join a stack fails the authentication, this switch will restart repeatedly.

Example

Configure MAC-based authentication to be used when a switch with the stack ID 4 needs to join a stack.

```
<HUAWEI> system-view
[HUAWEI] stack authentication slot 4 mac-address 3-3-3
```

3.3.28 stack led enable

Function

The **stack led enable** command enables a service port indicator to indicate the stack ID of a stack switch.

The **stack led disable** command disables a service port indicator from indicating the stack ID of a stack switch.

By default, a service port indicator does not indicate the stack ID of a stack switch.

NOTE

S6735-S does not support this command.

Format

stack led enable [**duration** *duration-value*]

stack led disable

Parameters

Parameter	Description	Value
duration *duration-value*	Specifies how long a service port indicator indicates the stack ID of a stack switch.	The value is an integer that ranges from 30 to 600, in seconds. By default, a stack ID indicator stays on for 45 seconds.

Views

All views

Default Level

2: Configuration level

Usage Guidelines

Stack IDs can be allocated by the master switch when a stack is set up, or you can configure them yourself. If stack IDs are allocated by the master switch, you cannot identify which ID a device maps to. To enable a service port indicator to indicate the stack ID of a stack switch, run the **stack led enable** command.

A service port indicator indicates the stack ID of a stack switch as follows:

- For a switch whose stack ID ranges from 1 to 8: Only the indicator whose serial number matches the stack ID is on. For example, if the stack ID is 1, the first indicator is on. If the stack ID is 2, the second indicator is on.
- For a switch whose stack ID is 0: If the stack contains *N* stack switches, the first *N* indicators are on. For example, if the stack contains 9 stack switches, the first 9 indicators are on, indicating the stack ID is 0.
- After service port indicators are configured to indicate the stack IDs, the service port indicator of the master switch blinks, and that of the slave switch is steady on.

The configuration of this command becomes invalid when port indicators show stack IDs of member switches for the specified time.

Example

Enable a service port indicator to indicate the stack ID of a stack device for a period of 30s.

```
<HUAWEI> stack led enable duration 30
```


3.3.29 stack-port load-balance mode

Function

The **stack-port load-balance mode** command sets a load balancing mode for the physical member ports of a stack port.

The **undo stack-port load-balance mode** command restores the default load balancing mode.

By default, the physical member ports of a stack port perform load balancing in enhanced mode, that is, load balancing based on the Exclusive-OR result of the source and destination MAC addresses.

NOTE

Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S support this command.

Format

stack-port load-balance mode { **dst-ip** | **dst-mac** | **src-dst-ip** | **src-dst-mac** | **src-ip** | **src-mac** }

undo stack-port load-balance mode

Parameters

Parameter	Description	Value
dst-ip	Performs load balancing based on destination IP addresses.	-
dst-mac	Performs load balancing based on destination MAC addresses.	-
src-dst-ip	Performs load balancing based on the Exclusive-OR result of the source and destination IP addresses.	-
src-dst-mac	Performs load balancing based on the Exclusive-OR result of the source and destination MAC addresses.	-
src-ip	Performs load balancing based on source IP addresses.	-

Parameter	Description	Value
src-mac	Performs load balancing based on source MAC addresses.	-

Views

System view

Logical stack port view (The S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S do not support the **stack-port load-balance mode** command in this view.)

Default Level

3: Management level

Usage Guidelines

Use Scenario

To transmit traffic from a stack port to a destination over different links, run the **stack-port load-balance mode** command to configure an appropriate load balancing mode for the physical member ports of the stack port. Outgoing traffic is then properly balanced among the physical links, preventing congestion on these links. If you run this command multiple times to set different load balancing modes, the last configuration takes effect. The load balancing mode configured in the system view takes effect globally, and the load balancing mode configured in a stack port view takes effect only on the specified stack port. You can run the **display stack-port** command to view the load balancing mode on a stack port.

Precautions

- If a non-default load balancing mode is configured on a stack port, the configured load balancing mode takes effect. If a stack port uses the default load balancing mode and the global load balancing mode is not the default one, the global load balancing mode takes effect.
- If the source MAC address-based load balancing mode is used, Layer 3 packets forwarded to a downstream device may fail to be balanced among the stack links because the source MAC address of the packets is the fixed system MAC address. If the traffic rate exceeds the bandwidth of a single stack link, some packets may be dropped.

Example

Set the global load balancing mode to **src-ip**.

```
<HUAWEI> system-view
[HUAWEI] stack-port load-balance mode src-ip
```

Set the load balancing mode on stack port 0/1 to **dst-ip**.


```
<HUAWEI> system-view
[HUAWEI] interface stack-port 0/1
[HUAWEI-stack-port0/1] stack-port load-balance mode dst-ip
```

3.3.30 stack port speed

Function

The **stack port speed** command sets the working speed for stack member ports.

The **undo stack port speed** command restores the working speed of stack member ports to the default value.

For the default working speeds of stack member ports on different switch models, see "Stack Support and Version Requirements" in Stack Configuration in the *S300, S500, S2700, S5700, and S6700 V200R023C00 Configuration Guide - Device Management*.

NOTE

Only the S5720-X-LI, S5720I-SI, S5732-H, and S5720S-X-LI support this command.

The S5720-P-LI does not support this command before the license is loaded and supports this command after the license is loaded and it restarts.

Format

stack port speed { **12G** | **2.5G** | **40GE** }

undo stack port speed

Parameters

Parameter	Description	Value
12G	Sets the working speed of stack member ports to 12 Gbit/s. This speed can be set only on the S5720-P-LI, S5720-X-LI, S5720I-SI, and S5720S-X-LI,.	-
2.5G	Sets the working speed of stack member ports to 2.5 Gbit/s. This speed can be set only on the S5720-P-LI, S5720-X-LI, and S5720S-X-LI.	-

Parameter	Description	Value
40GE	Sets the working speed of stack member ports to 40 Gbit/s. This speed can be set only on the S5732-H.	-

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

On the S5720-P-LI, S5720-X-LI, S5720I-SI, and S5720S-X-LI,, if optical ports are used as stack member ports and are connected using 1 m or 3 m SFP+ passive copper cables, you can use this command to increase their working speed from 10 Gbit/s to 12 Gbit/s, expanding the stack bandwidth. After their working speed is increased to 12 Gbit/s, switches using these ports cannot set up a stack with switches using ports with the working speed 10 Gbit/s.

If S5720-P-LI, S5720-X-LI, and S5720S-X-LI switches use XGE optical ports to stack with other switches that have GE optical ports, use this command to reduce the working speed of the XGE optical ports from 10 Gbit/s to 2.5 Gbit/s, so that the XGE optical ports can work with the remote GE optical ports.

On the S5732-H, if 100GE and 40GE ports need to be connected using 2 m QSFP28 dedicated stack cables for stack setup, run this command to reduce the working speed of the 100GE ports that function as stack member ports to 40 Gbit/s.

You can run the **display stack port speed** command to check the working speed of stack member ports.

Precautions

After changing the working speed of stack member ports, you need to restart the switch for the new speed to take effect.

Example

Set the working speed of stack member ports to 12 Gbit/s.

```
<HUAWEI> system-view
[HUAWEI] stack port speed 12G
```


3.3.31 stack port { crc | link-flap } trigger

Function

The **stack port { crc | link-flap } trigger** command sets the stack port error-down parameters.

The **undo stack port { crc | link-flap } trigger** command restores the default settings of the stack port error-down parameters.

By default, the stack port receives 20 CRC error packets (include Symbols error packets) per minute or alternates between Up and Down states 10 times per minute, the error-down check interval is 3 minutes, and the alarm clearance interval is 0 (not cleared automatically).

Format

stack port { **crc** | **link-flap** } **trigger** { **threshold** *threshold* | **interval** *interval* } *

undo stack port { **crc** | **link-flap** } **trigger** { **threshold** | **interval** }

stack port { **crc** | **link-flap** } **trigger error-down auto-recovery-interval** *auto-recovery-interval*

undo stack port { **crc** | **link-flap** } **trigger error-down auto-recovery-interval**

Parameters

Parameter	Description	Value
crc	Sets the parameters for stack port error-down alarms triggered by CRC error packets (include Symbols error packets).	-
link-flap	Sets the parameters for stack port error-down alarms triggered by port Up/Down transitions.	-
threshold *threshold*	Specifies the error-down alarm threshold.	The value is an integer. It ranges from 1 to 10000 for error-down alarms triggered by CRC error packets (include Symbols error packets) and ranges from 3 to 30 for error-down alarms triggered by port Up/Down transitions. The unit is times per minute.

Parameter	Description	Value
interval *interval*	Specifies the error-down check interval.	The value is an integer that ranges from 3 to 30, in minutes.
auto-recovery-interval *auto-recovery-interval*	Specifies the error-down alarm clearance interval.	The value is an integer that ranges from 3 to 30, in minutes.

Views

System view

Default Level

3: Management level

Usage Guidelines

After the stack port error-down function is enabled, you can run the **stack port { crc | link-flap } trigger** command to adjust the related parameters.

Example

Set the clearance interval of stack port error-down alarms triggered by CRC error packets (include Symbols error packets) to 3 minutes. That is, if the rate of received CRC error packets (include Symbols error packets) stays below the threshold for 3 minutes, the stack port changes to Up state and the error-down alarm is cleared.

```
<HUAWEI> system-view
[HUAWEI] stack port crc trigger error-down auto-recovery-interval 3
```

3.3.32 stack port { crc | link-flap } trigger error-down

Function

The **stack port { crc | link-flap } trigger error-down** command enables the stack port error-down function.

The **undo stack port { crc | link-flap } trigger error-down** command disables the stack port error-down function.

By default, the stack port error-down function is enabled.

Format

stack port { **crc** | **link-flap** } **trigger error-down**

undo stack port { **crc** | **link-flap** } **trigger error-down**

Parameters

Parameter	Description	Value
crc	Enables stack port error-down triggered by CRC error packets (include Symbols error packets).	-
link-flap	Enables stack port error-down triggered by port Up/Down transitions.	-

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

In a stack system, if a stack port continuously receives CRC error packets (include Symbols error packets) or flaps between Up and Down states, the corresponding stack link cannot forward traffic normally, thereby affecting network services. This command enables the stack port error-down function. This function can shut down a stack port and switch traffic to other stack links if the rate of received CRC error packets (include Symbols error packets) or the number of Up/Down transitions on the stack port reaches the specified threshold, reducing the impact on services. Additionally, the system generates stack port error-down alarms to help in fault location.

Follow-up Procedure

Run the **stack port { crc | link-flap } trigger** command to set stack port error-down parameters.

Precautions

- When one end is a stack port and the other end is a service port, the system does not set the stack port to error-down state or generate an error-down alarm even if this stack port continuously receives CRC error packets (include Symbols error packets).
- The stack port error-down alarm OID is 1.3.6.1.4.1.2011.5.25.183.1.22.59.
- The stack port error-down alarm clearance OID is 1.3.6.1.4.1.2011.5.25.183.1.22.60.

Example

Enable stack port error-down triggered by CRC error packets (include Symbols error packets).

```
<HUAWEI> system-view
[HUAWEI] stack port crc trigger error-down
```

3.3.33 stack reserved-vlan

Function

The **stack reserved-vlan** command configures a reserved VLAN for a stack.

By default, a stack uses VLAN 4093 as the reserved VLAN.

Format

stack reserved-vlan *vlan-id*

Parameters

Parameter	Description	Value
vlan-id	Specifies the ID of a reserved VLAN.	The value is an integer that ranges from 1 to 4094.

Views

System view

Default Level

3: Management level

Usage Guidelines

By default, a stack uses VLAN 4093 as the reserved VLAN. A reserved VLAN is used only to exchange stack protocol packets.

To deploy services in VLAN 4093, run the **stack reserved-vlan** command to change the reserved VLAN of the stack.

NOTICE

If the reserved VLAN is used for other services, the stack cannot be set up. You must specify an unused VLAN as the reserved VLAN for a stack.

Example

Configure VLAN 4000 as the reserved VLAN of a stack.

```
<HUAWEI> system-view
[HUAWEI] stack reserved-vlan 4000
Warning: Do not frequently modify the stack reserved VLAN because it will make the stack split. Continue?
[Y/N]:y
```

3.3.34 stack slot priority

Function

The **stack slot priority** command sets a stack priority for a member switch in a stack.

By default, the stack priority of a member switch is 100.

Format

stack slot *slot-id* **priority** *priority*

Parameters

Parameter	Description	Value
slot-id	Specifies the stack ID of a member switch.	The value is an integer that ranges from 0 to 8.
priority	Specifies a stack priority.	The value is an integer that ranges from 1 to 255.

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

To set a stack priority for a member switch in a stack, run the **stack slot priority** command. A larger priority indicates a higher priority, meaning that a switch is more likely to be selected as a master switch.

Example

Set the stack priority of the member switch with stack ID 4 to 150.


```
<HUAWEI> system-view
[HUAWEI] stack slot 4 priority 150
Warning: Do not frequently modify the priority because it will make the stack split. Continue? [Y/N]:y
```

3.3.35 stack slot renumber

Function

The **stack slot renumber** command changes the stack ID of a specified stack member switch.

Format

stack slot *slot-id* **renumber** *new-slot-id*

Parameters

Parameter	Description	Value
slot-id	Specifies the current stack ID.	The value is an integer that ranges from 0 to 8.
new-slot-id	Specifies a new stack ID.	The value is an integer that ranges from 0 to 8.

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

To change the stack ID of a stack member switch, run the **stack slot renumber** command.

Precautions

- After changing the stack ID of a switch, if you do not restart the switch, the switch continues to use the original stack ID, and all physical resources are identified by the original stack ID.
- After changing the stack ID of a switch, if you restarts the switch, the new stack ID takes effect and all physical resources are identified by the new stack ID. In the configuration file, only the global stack configuration and stack priority of the switch continue to take effect. All other configurations related to the old stack ID (such as interface configuration) become invalid and must be reconfigured.

- After a UCL group is created on the S5720I-SI, S5720-LI, S5720S-LI, or S5720-SI, using the **ucl-group** command, the **stack slot renumber** command cannot be used to change the stack ID of a specified stack member switch.

Example

Change the stack ID of a stack member switch from 4 to 5.

```
<HUAWEI> system-view
[HUAWEI] stack slot 4 renumber 5
Warning: All the configurations related to the slot ID will be lost after the slot ID is
modified.
Do not frequently modify the slot ID because it will make the stack split. Continue? [Y/
N]:y
Info: Stack configuration has been changed, and the device needs to restart to make the configuration
effective.
```

3.3.36 stack timer mac-address switch-delay

Function

The **stack timer mac-address switch-delay** command sets a period after which a stack changes its system MAC address.

The **undo stack timer mac-address switch-delay** command configures a stack to change the system MAC address immediately after the owner of the original system MAC address leaves the stack.

By default, a stack changes the system MAC address after 10 minutes.

NOTICE

When a stack is configured to switch the system MAC address immediately, the system begins using the MAC address of the new master switch the moment the previous master switch fails or leaves the stack. This may cause protocols such as LACP and STP to flap, thereby affecting services.

Format

stack timer mac-address switch-delay *delay-time*

undo stack timer mac-address switch-delay

Parameters

Parameter	Description	Value
delay-time	Specifies a period after which a stack changes the system MAC address.	The value ranges from 0 to 60, in minutes.

Views

System view

Default Level

3: Management level

Usage Guidelines

When a member switch leaves a stack, if you specify the MAC address of the leaving switch as the stack MAC address and it does not rejoin the stack within the time specified by *delay-time*, the master switch changes the stack MAC address to its own MAC address.

The stack MAC address switchover delay time of any member switch in a stack is the same as that of the master switch.

If the value of the MAC address switchover timer is set to 0, no stack MAC address switchover will be performed.

This command can be used only after the stack function is enabled (default status).

Example

Set the MAC address switchover delay of the local switch to 4 minutes.

```
<HUAWEI> system-view
[HUAWEI] stack timer mac-address switch-delay 4
Warning: Do not frequently modify the MAC switching time because it will make the stack split. Continue?
[Y/N]:y
```

3.3.37 upgrade backup-area slot

Function

The **upgrade backup-area slot** command defines the active and backup areas in a stack in preparation for a smooth upgrade.

Format

upgrade backup-area slot *slot-id* **to** *slot-id*

Parameters

Parameter	Description	Value
slot-id	Specifies the stack ID of a member switch.	The value is an integer that ranges from 0 to 8.

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

Before upgrading a reliable stack with uplinks and downlinks working in redundancy mode, you can divide the stack into an active area and a backup area for redundancy. After an upgrade is started, member switches in the two areas are upgraded in sequence, shortening the service interruption duration and reducing the impact of the upgrade on the network.

Precautions

- Member switches in the active and backup areas form the entire stack. When dividing active and backup areas, note that:
  - The active and backup areas cannot have the same member switch, and both areas must have at least one member switch.
  - The backup area cannot contain the master switch of the stack.
  - Member switches in each area must be directly connected.
- After this command is run, the member switches with specified stack IDs join the backup area. The other member switches automatically join the active area.
- To ensure mutual backup, it is recommended that the two areas have similar quantities of member switches.

Example

Add member switches with stack IDs 0 to 3 to the backup area.

```
<HUAWEI> system-view
[HUAWEI] upgrade backup-area slot 0 to 3
```

3.3.38 upgrade start

Function

The **upgrade start** command starts a smooth upgrade.

Format

upgrade start

Parameters

None

Views

System view

Default Level

3: Management level

Usage Guidelines

Before running this command, run the **upgrade backup-area slot** command to define the active and backup areas and ensure that all member switches in the stack are running the same system software and support smooth upgrades.

If an upgrade fails, error codes and displayed message help locate the cause. **Table 3-63** lists the error codes and displayed messages in different upgrade failure scenarios.

Table 3-63 Error codes and displayed messages in different upgrade failure scenarios

Upgrade Failure Scenario	Error Code	Displayed Message
Record in the backup area: The upgrade in the backup area times out and rolls back.	1	Rollback due to timeout.
Record in the active area: The upgrade in the backup area times out and rolls back.	2	
Record in the backup area: The upgrade in the active area times out and rolls back.	3	
Record in the active area: The upgrade in the active area times out and rolls back.	4	
Record in the backup area: Rollback occurs due to a topology change in the backup area.	257	Rollback due to topology changes.
Record in the active area: Rollback occurs due to a topology change in the backup area.	258	

Upgrade Failure Scenario	Error Code	Displayed Message
Record in the backup area: Rollback occurs due to a topology change in the active area.	259	
Record in the active area: Rollback occurs due to a topology change in the active area.	260	
A member switch records that the master switch is not upgraded.	512	Master is not upgraded.
During a backup area upgrade, the master switch instructs switches in the backup area to roll back (after the active area instructs the backup area to upgrade and switches in the backup area restart).	769	Master notifies others of rollback.
During a backup area upgrade, the master switch instructs switches in the backup area to roll back (after the active area instructs the backup area to upgrade and before switches in the backup area restart).	770	
During an active area upgrade, the master switch instructs switches in the active area to roll back (after the backup area instructs the active area to upgrade and before switches in the active area restart).	771	

Upgrade Failure Scenario	Error Code	Displayed Message
During an active area upgrade, the master switch instructs switches in the active area to roll back (after the backup area instructs the active area to upgrade and switches in the active area restart).	772	
During a backup area upgrade, the master switch in the active area instructs switches in the backup area to roll back (after switches in the backup area restart).	1025	Master of the active area notifies others of rollback.
During a backup area upgrade, the master switch in the active area instructs switches in the backup area to roll back (before switches in the backup area restart).	1026	
During an active area upgrade, the master switch in the active area instructs switches in the active area to roll back (before switches in the active area restart).	1027	
During an active area upgrade, the master switch in the active area instructs switches in the active area to roll back (after switches in the active area restart).	1028	
During a backup area upgrade, the master switch in the backup area instructs switches in the backup area to roll back (after switches in the backup area restart).	1281	Master of the backup area notifies others of rollback.

Upgrade Failure Scenario	Error Code	Displayed Message
During a backup area upgrade, the master switch in the backup area instructs switches in the backup area to roll back (before switches in the backup area restart).	1282	
During an active area upgrade, the master switch in the backup area instructs switches in the active area to roll back (before switches in the active area restart).	1283	
During an active area upgrade, the master switch in the backup area instructs switches in the active area to roll back (after switches in the active area restart).	1284	
A load event occurs, and switches in the backup area roll back.	1537	Rollback due to a load event.
A load event occurs, and switches in the active area roll back.	1549	
The system software package is incorrect in the active area.	5	Active startup file is incorrect.
The system software package is incorrect in the backup area.	6	Backup startup file is incorrect.

Example

Start a smooth upgrade.

```
<HUAWEI> system-view
[HUAWEI] upgrade start
Warning: Upgrade will begin. Continue? [Y/N]:y
```


3.4 Intelligent Simplified Campus Network Configuration Commands

3.4.1 Command Support

All commands in this chapter are run on a central switch. The following table lists the device models that can function as central switches.

Table 3-64 Device models that can function as central switches

Series	Sub-series or MPU
S12700E	MPUE, MPUEC
S12700	MPUD
S7700	SRUHX1, SRUE1, SRUH1, SRUHA1, MCUD, SRUHD, SRUED, SRUH, SRUE
S6700	S6730-H, S6730S-H, S6730-S, S6730S-S, S6735-S, S6720-EI, S6720S-EI, S6720S-S
S5700	S5732-H, S5731-H, S5731S-H, S5731-S, S5731S-S, S5736-S, S5736S-S, S5735S-H, S5735-S, S5735S-S, S5735-S-I, S5720I-SI, S5735-L, S5735S-L, S5735-L1, S5735S-L1, S5735-L-I, S5720-LI, S5720S-LI
S500, S300	-

3.4.2 bind interface

Function

The **bind interface** command binds an interface on the central switch to an RU for interconnection.

The **undo bind** command unbinds the interconnection interface from an RU.

By default, no interconnection interface is bound to an RU.

Format

bind interface *interface-type interface-number*

undo bind

Parameters

Parameter	Description	Value
interface-type interface-number	Specifies the type and number of an interface. The interface type and number can be closely next to each other or separated by a space character.	-

Views

remote-unit N view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To deliver configurations to an RU, you need to bind an interface on the central switch to the RU for interconnection. After interface binding, you can run the **remote-unit connect-interface** *interface-type interface-number* command on the central switch to enter the view of an RU by specifying an interconnection interface, and run the **display remote-unit connect-interface** *interface-type interface-number* command to view information about an RU bound to a specific interconnection interface.

Precautions

- An interface can be bound to only one RU.
- An Eth-Trunk physical member interface cannot be bound to an RU.

Example

Bind XGigabitEthernet0/0/1 to the RU 0.

```
<HUAWEI> system-view
[HUAWEI] remote-unit 0
[HUAWEI-remote-unit-0] bind interface XGigabitEthernet 0/0/1
```

3.4.3 commit (remote-unit N view)

Function

The **commit** command delivers configurations to a single RU.

Format

commit

Parameters

None

Views

remote-unit N view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

After configuring an RU by running commands on the central switch, such as configuring the port rate, port isolation, port shutdown, or port negotiation, you need to run the **commit** command to make the configuration take effect.

Precautions

A central switch does not deliver configurations to RUs that fail to be authenticated or are not authenticated.

RUs do not save their configurations. After the central switch or an RU is restarted and works normally, the central switch preferentially delivers the configuration in the single RU view. If no configuration is available in the single RU view, the central switch delivers the configuration in the global RU view.

Example

Deliver configurations to RU 0.

```
<HUAWEI> system-view
[HUAWEI] remote-unit 0
[HUAWEI-remote-unit-0] commit
```

3.4.4 commit (remote-unit view)

Function

The **commit** command delivers configurations to RUs.

Format

commit { **all** | **name** *remote-unit-name* | **interface** *interface-type interface-number* }

Parameters

Parameter	Description	Value
all	Commits configurations of all RUs.	-

Parameter	Description	Value
name *remote-unit-name*	Specifies the alias of an RU.	The value is a string of 1 to 32 case-sensitive characters without spaces.
interface *interface-type interface-number*	Specifies the type and number of an interface. The interface type and number can be closely next to each other or separated by a space character.	-

Views

remote-unit view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

After configuring an RU by running commands on the central switch, such as the port rate, port isolation, port shutdown, and port negotiation, you need to run the **commit** command to deliver the configurations to the RU for the configurations to take effect.

The **commit** command can be run to deliver configurations to offline RUs. After an offline RU goes online, the central switch automatically applies the committed configurations to this RU.

Precautions

A central switch does not deliver configurations to RUs that fail to be authenticated or are not authenticated.

RUs do not save their configurations. After the central switch or an RU is restarted and works normally, the central switch preferentially delivers the configuration in the single RU view. If no configuration is available in the single RU view, the central switch delivers the configuration in the global RU view.

Follow-up Procedure

Run the **display remote-unit commit configuration** command to check the configurations that are successfully delivered to RUs, and run the **display remote-unit commit result** command to check configuration delivery results of RUs.

Example

Deliver configurations to the RU connected to XGigabitEthernet0/0/1 on the central switch.


```
<HUAWEI> system-view
[HUAWEI] remote-unit
[HUAWEI-remote-unit] commit interface XGigabitEthernet 0/0/1
```

3.4.5 description (remote-unit N view)

Function

The **description** command sets a description for an RU.

The **undo description** command restores the default description of an RU.

By default, an RU has no description.

Format

description *description*

undo description

Parameters

Parameter	Description	Value
description	Specifies the description of an RU.	The value is a string of 1 to 64 case-sensitive characters, and can contain spaces.

Views

remote-unit N view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To facilitate management and maintenance of RUs, you can set descriptions for RUs to help you understand the usage of each RU.

Precautions

The description is displayed from the first non-space character.

Follow-up Procedure

Run the **display remote-unit commit configuration** command to check the configurations that are successfully delivered to RUs, and run the **display remote-unit commit result** command to check configuration delivery results of RUs.

Example

Set the description of an RU to **ru for office**.

```
<HUAWEI> system-view
[HUAWEI] remote-unit 0
[HUAWEI-remote-unit-0] description ru for office
```

3.4.6 display remote-unit

Function

The **display remote-unit** command displays RU information.

Format

display remote-unit [**connect-interface** *interface-type interface-number* | **name** *remote-unit-name*][**verbose**]

Parameters

Parameter	Description	Value
connect-interface *interface-type interface-number*	Specifies the type and number of an interface. The interface type and number can be closely next to each other or separated by a space character.	-
name *remote-unit-name*	Specifies the alias of an RU.	The value must be an existing RU alias.
verbose	Displays detailed RU information.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

You can run this command to view RU information, including the ESN, alias, MAC address, device type, online duration, and firmware version of an RU.

Precautions

The central switch does not maintain information about RUs that attempt to go online when the number of connected RUs has reached the upper limit.

The **display remote-unit** command output displays information only about online RUs. You can run the **display current-configuration configuration remote-unit** command to view global configurations of RUs, or run the **display current-configuration configuration remote-unit-n** command to view the configuration of a specific RU.

Example

Display RU information.

```
<HUAWEI> system-view
[HUAWEI] display remote-unit
-------------------------------------------------------------------------------------------------------------
ESN                 ID       Type              ConnectInterface  Status      VersionMatch  Name
-------------------------------------------------------------------------------------------------------------
219801176601XXXXXXXX  1        S5731-L8P2HT-RUA  XGE0/0/6          Normal      NO            RU1
219801176601XXXXXXXX  16777214 S5731-L8P2HT-RUA  XGE0/0/7          Normal      NO            RU2
-------------------------------------------------------------------------------------------------------------
Total: 2, printed: 2
```

Table 3-65 Description of the **display remote-unit** command output

Item	Description
ESN	ESN of an RU.
ID	ID of an RU. This field displays a hyphen (-) if an RU is not configured with an ID.
Type	Device type of an RU.
ConnectInterface	Interconnection interface.
Status	Status of an RU: • **Normal**: The RU is online. • **Upgrading**: The RU is being upgraded. • **Configuring**: The RU is being configured. • **Idle**: The RU is in the initialization state. • **Abnormal**: The link connecting the RU and central switch is faulty, or the RU is an excess one because the number of connected RUs has reached the upper limit.
Name	Alias of an RU. This field displays a hyphen (-) if an RU is not configured with an alias.

Item	Description
VersionMatch	Whether the firmware version of the RU matches that of the central switch. ● **YES**: The version matches. ● **NO**: The version does not match. ● **-**: The firmware version of the HUAWEI S5731-L16P2SR-RUA or S5731S-L16P2SR-RUA cannot be upgraded to that of the central switch or that of the patch.
Total: *m*, printed: *n*	Total number of RUs (*m*) and number of RUs whose information is displayed (*n*).

Display detailed RU information.

```
<HUAWEI> display remote-unit verbose
Total number: 2
--------------------------------------------------------------------------------
ESN               :219801177001xxxxxxxx
Name                :-
ID                :3
Device mac          :xxxx-xxxx-xxxx
Device type         :S5731-L8P2HT-RUA
Item              :98011770
Manufacture Date    :2021-12-17
Up time             :0 day, 6 hours, 25 minutes, 44 seconds
APP version         :220207016
POE version         :7812
BIOS version        :220225001
Connect interface   :Eth-Trunk100
Disk usage          :44%
Memory usage        :22%
Temperature         :37(Celsius)
Mac usage           :0%
Disk space(MB)      :16
Status              :Normal
VersionMatch        :YES
Version support     :YES
Authen Result       :Success
--------------------------------------------------------------------------------
ESN               :219801176801xxxxxxxx
Name                :-
ID                :2
Device mac          :xxxx-xxxx-xxxx
Device type         :S5731-L8P2HT-RUA
Item              :98011768
Manufacture Date    :2021-12-17
Up time             :0 day, 0 hour, 48 minutes, 39 seconds
APP version         :220123002
POE version         :7812
BIOS version        :220225001
Connect interface   :GigabitEthernet0/0/1
Disk usage          :44%
Memory usage        :22%
Temperature         :39(Celsius)
Mac usage           :0%
Disk space(MB)      :16
Status              :Normal
```



```
VersionMatch      :YES
Version support   :YES
Authen Result     :Success
------------------------------------------------------------------------------
```

Table 3-66 Description of the **display remote-unit verbose** command output

Item	Description
Total number	Total number of RUs.
ESN	ESN of an RU.
Name	Alias of an RU. This field displays a hyphen (-) if an RU is not configured with an alias.
ID	ID of an RU. If an RU is not configured with an ID, a hyphen (-) is displayed.
Device mac	System MAC address of an RU.
Device type	Device type of an RU.
Item	Code of an RU.
Manufacture Date	Manufacture date of an RU.
Up time	Online duration of an RU.
APP version	APP firmware version.
POE version	PoE firmware version.
BIOS version	BIOS firmware version.
Connect interface	Interface connecting the central switch to an RU. If the central switch uses a physical Eth-Trunk member interface to connect to an RU, this field displays the Eth-Trunk interface to which the member interface belongs.
Disk usage	Disk usage of an RU.
Memory usage	Memory usage of an RU.
Temperature	Current temperature of an RU. **NOTE** If the temperature value cannot be read properly, this field displays a hyphen (-). In this case, check whether the central switch receives an alarm from the RU, indicating that the IIC channel is faulty. For details, see the description of the hwRuIICFault alarm.
Mac usage	MAC address table usage of an RU.
Disk space(MB)	Disk size of an RU.

Item	Description
Status	Status of an RU: • **Unknown** • **Idle**: The RU is in the initialization state. • **Normal**: The RU is online. • **Upgrading**: The RU is being upgraded. • **Configuring**: The RU is being configured. • **Abnormal**: The link connecting the RU and central switch is faulty, or the RU is an excess one because the number of connected RUs has reached the upper limit. • **Offline**: The RU is offline.
VersionMatch	Whether the firmware version of the RU matches that of the central device. • **YES**: The version matches. • **NO**: The version does not match.
Version support	Whether the RU supports the firmware of the central switch: • YES: compatible • NO: incompatible
Authen Result	Authentication result of an RU: • **Success** • **Authenticating** • **Fail** • **-**: The RU is not authenticated.

3.4.7 display remote-unit commit configuration

Function

The **display remote-unit commit configuration** command displays the configurations successfully delivered to RUs.

Format

display remote-unit commit configuration

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

RUs do not support web-based management and cannot have commands run on them for configuration. All RU configurations are delivered by the central switch. You can run the **display remote-unit commit configuration** command on the central switch to view the configurations successfully delivered to RUs.

Example

Display the configurations successfully delivered to RUs.

```
<HUAWEI> display remote-unit commit configuration
#
remote-unit 3
 isolate disable
#
#
remote-unit 0
 isolate disable
 undo negotiation auto port 1
 speed 100 port 1
#
```

3.4.8 display remote-unit commit result

Function

The **display remote-unit commit result** command displays configuration delivery results of RUs.

Format

display remote-unit commit result

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

RUs do not support web-based management and cannot have commands run on them for configuration. All RU configurations are delivered by the central switch.

You can run the **display remote-unit commit result** command on the central switch to view configuration delivery results of RUs. A maximum of 500 result records are supported.

Example

Display configuration delivery results of RUs.

```
<HUAWEI> display remote-unit commit result
[HUAWEI-remote-unit-0] display remote-unit commit result
-------------------------------------------------------------------------------
StartTime           ConnectInterface       CfgType        Result   SendCnt
-------------------------------------------------------------------------------
2022/01/27 16:04:02   GE0/0/27               isolate        success  2
2022/01/27 16:04:02   GE0/0/27               shutdown       success  2
2022/01/27 16:04:02   GE0/0/27               negotiation    success  2
2022/01/27 16:04:02   GE0/0/27               speed          success  2
2022/01/27 16:04:02   XGE0/0/1               isolate        success  2
2022/01/27 16:04:02   XGE0/0/1               shutdown       success  2
2022/01/27 16:04:02   XGE0/0/1               negotiation    success  2
2022/01/27 16:04:02   XGE0/0/1               speed          success  2
```

Table 3-67 Description of the **display remote-unit commit result** command output

Item	Description
StartTime	Time when the configuration is delivered.
ConnectInterface	Interconnection interface.
CfgType	Configuration type.
Result	Delivery result: • **success** • **failed**
SendCnt	Number of times that the configurations of the same type are delivered to an RU.

3.4.9 display remote-unit connect record

Function

The **display remote-unit connect record** command displays onboarding and disconnection records of RUs.

Format

display remote-unit connect record

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

To view onboarding and disconnection records of RUs, you can run the **display remote-unit connect record** command. In the command output, you can check when an RU is onboarded or disconnected and the disconnection cause. A maximum of 1024 records are supported.

Example

Display onboarding and disconnection records of RUs.

```
<HUAWEI> system-view
[HUAWEI] display remote-unit connect record
-------------------------------------------------------------------------------------------------------
ESN                  ConnectInterface   Type    Offline Reason        Time
-------------------------------------------------------------------------------------------------------
219801177001XXXXXXXX      GE0/0/27        OnLine  -                2022-02-08/17:00:36
219801177601XXXXXXXX      GE0/0/25        OnLine  -                2022-02-08/17:00:39
219801177601XXXXXXXX      XGE0/0/1        OffLine Upgrade             2022-02-08/17:02:32
219801177001XXXXXXXX      GE0/0/27        OffLine Upgrade             2022-02-08/17:02:39
219801177601XXXXXXXX      XGE0/0/1        OnLine  -                2022-02-08/17:04:09
219801177001XXXXXXXX      GE0/0/27        OnLine  -                2022-02-08/17:04:33
219801177001XXXXXXXX      GE0/0/27        OffLine Port down           2022-02-09/11:43:06
-------------------------------------------------------------------------------------------------------
Total records: 7
```

Table 3-68 Description of the **display remote-unit record** command output

Item	Description
ESN	ESN of an RU.
ConnectInterface	Interface connecting the central switch to an RU.
Type	Record type: • **OnLine**: onboarding • **OffLine**: disconnection

Item	Description
Offline Reason	Disconnection cause: • **Upgrade**: The RU was upgraded and restarted. • **Manual**: The RU was manually restarted. • **No heartbeat**: The RU lost heartbeats and went offline. • **Port down**: The interconnection interface went Down. • **Multi-RU on port**: Multiple RUs were connected to the same interface. • **Abnormal temperature**: The RU goes offline due to abnormal temperature. • **Unknown**
Time	Time when an RU entered this state.
Total records	Total number of records.

3.4.10 display remote-unit poe

Function

The **display remote-unit poe** command displays the global PoE power supply status of an RU.

Format

display remote-unit poe [**connect-interface** *interface-type interface-number* | **name** *remote-unit-name*]

Parameters

Parameter	Description	Value
connect-interface *interface-type interface-number*	Specifies the type and number of an interface. The interface type and number can be closely next to each other or separated by a space character.	-

Parameter	Description	Value
name *remote-unit-name*	Specifies the alias of an RU.	The value must be an existing RU alias.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can use this command to view PoE power supply information about an RU, including the configured maximum power, current power consumption, peak power consumption, and PoE firmware status.

Example

Display the global PoE power supply information about the RU connected to XGigabitEthernet0/0/1.

```
<HUAWEI> display remote-unit poe connect-interface XGigabitEthernet 0/0/1
ESN               :21980117760123xxxxxxxx
Name              :-
Device type       :S5731-L8P2HT-RUA
Connect interface  :XGigabitEthernet0/0/1
------------------------------------------------------
PSE information    :
  PoE power supply(mW)                        :83000
  Total available power(mW)                   :83000
  Total power consumption(mW)                    :0
  Power peak value(mW)                        :0
  Power voltage(V)                         :54
  PSE reset times                        :0
  PoE failure                           :NO
------------------------------------------------------
```

Table 3-69 Description of the **display remote-unit poe** command output

Item	Description
ESN	ESN of an RU.
Name	Alias of an RU. This field displays a hyphen (-) if an RU is not configured with an alias.
Device type	Device type of an RU.
Connect interface	Interface connecting the central switch to an RU.
PoE power supply(mW)	Power supply.

Item	Description
Total available power(mW)	Total available power.
Total power consumption(mW)	Total output power.
Power peak value(mW)	Peak output power.
Power voltage(V)	Output voltage.
PSE reset times	Number of times that the PSE chip is reset.
PoE failure	Whether the PoE firmware is abnormal: • **NO**: normal • **YES**: abnormal

3.4.11 display remote-unit poe realtime

Function

The **display remote-unit poe realtime** command displays real-time PoE information about an RU.

Format

display remote-unit poe { **connect-interface** *interface-type interface-number* | **name** *remote-unit-name* } **realtime**

Parameters

Parameter	Description	Value
name *remote-unit-name*	Specifies the alias of an RU.	The value must be an existing RU alias.
interface *interface-type interface-number*	Specifies the type and number of an interface. The interface type and number can be closely next to each other or separated by a space character.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run this command to view real-time PoE information about an RU.

Example

Display real-time PoE information about all interfaces on the RU connected to GigabitEthernet0/0/19 on the central switch.

```
<HUAWEI> system-view
[HUAWEI] display remote-unit poe connect-interface GigabitEthernet 0/0/19 realtime
Info: This operation will take several seconds. Please wait....
ESN                :219801177601XXXXXXXX
Name               :-
Device type        :S5731-L8P2HT-RUA
Connect interface  :GigabitEthernet0/0/19
------------------------------------------------------
PSE information    :
  PoE power supply(mW)                          :83000
  Total available power(mW)                     :46100
  Total power consumption(mW)                       :36900
  Power peak value(mW)                          :50300
  Power voltage(V)                            :53
  PSE reset times                           :0
  PoE failure                             :NO
------------------------------------------------------
```

Table 3-70 Description of the **display remote-unit port poe** command output

Item	Description
ESN	ESN of an RU.
Name	Alias of an RU. This field displays a hyphen (-) if an RU is not configured with an alias.
Device type	Device type of an RU.
Connect interface	Interface connecting the central switch to an RU.
PoE power supply(mW)	Power supply.
Total available power(mW)	Total available power.
Total power consumption(mW)	Total output power.
Power peak value(mW)	Peak output power.
Power voltage(V)	Output voltage.
PSE reset times	Number of times that the PSE chip is reset.

Item	Description
PoE failure	Whether the PoE firmware is abnormal: • **NO**: normal • **YES**: abnormal

3.4.12 display remote-unit port brief

Function

The **display remote-unit port brief** command displays brief information about interfaces on an RU.

Format

display remote-unit port [**connect-interface** *interface-type interface-number* | **name** *remote-unit-name*] **brief**

Parameters

Parameter	Description	Value
connect-interface *interface-type interface-number*	Specifies the type and number of an interface. The interface type and number can be closely next to each other or separated by a space character.	-
name *remote-unit-name*	Specifies the alias of an RU.	The value must be an existing RU alias.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

To monitor interfaces on an RU or locate faults on interfaces, you can run the **display remote-unit port brief** command to view information about the interfaces, including the physical status, auto-negotiation status, working mode,

and rate. If no parameter is specified, brief information about interfaces on all RUs is displayed.

Precautions

- An uplink 2.5GE optical interface of an RU does not support a copper module, and supports only a GE or 2.5GE optical module. In V200R022C10 and earlier versions, the uplink interface configured with a GE optical module can connect to a central switch only when it works at the rate of 1 Gbit/s. In V200R023C00 and later versions, the uplink interface configured with a 2.5GE optical module can connect to a central switch when it works at the rate of 2.5 Gbit/s. After the rate of the uplink interface is changed, the RU automatically restarts for the change to take effect.
- An uplink 2.5GE hybrid optical-electrical interface of an RU does not support a copper module, and supports only a GE or 2.5GE optical or hybrid module. In V200R022C10 and earlier versions, the uplink interface configured with a GE optical or hybrid module can connect to a central switch only when it works at the rate of 1 Gbit/s. In V200R023C00 and later versions, the uplink interface configured with a 2.5GE optical or hybrid module can connect to a central switch when it works at the rate of 2.5 Gbit/s. After the rate of the uplink interface is changed, the RU automatically restarts for the change to take effect.

Example

Display brief information about interfaces on the RUs connected to Eth-Trunk 10 on the central switch.

```
<HUAWEI> display remote-unit port connect-interface Eth-Trunk 10 brief
ESN               :219801177801xxxxxxxx
Name              :-
Device type       :S5731-L8P2HT-RUA
Connect interface  :Eth-Trunk10
--------------------------------------------------------------------------------
Interface     PHY      Negotiation     Duplex    Mode      Speed(Mbps)   Neighbor-Interface
--------------------------------------------------------------------------------
GE1           Up       Enable          Full      Copper    1000          -
GE2           Down     Enable          Full      Copper    1000          -
GE3           Down     Enable          Full      Copper    1000          -
GE4           Down     Enable          Full      Copper    1000          -
GE5           Down     Enable          Full      Copper    1000          -
GE6           Down     Enable          Full      Copper    1000          -
GE7           Down     Enable          Full      Copper    1000          -
GE8           Up       Enable          Full      Copper    1000          -
GE9           Down     Enable          Full      Copper    1000          -
GE10          Up       Enable          Full      Fiber     1000          GE0/0/36
--------------------------------------------------------------------------------
```

Table 3-71 Description of the **display remote-unit port brief** command output

Item	Description
ESN	ESN of an RU.
Name	Alias of an RU. This field displays a hyphen (-) if an RU is not configured with an alias.
Device type	Device type of an RU.

Item	Description
Connect interface	Interconnection interface.
Interface	Interface on an RU.
PHY	Physical status of an RU interface: • **up**: The interface is Up. • **down**: The interface is Down.
Negotiation	Auto-negotiation status of an RU interface: • **Enable**: The interface works in auto-negotiation mode. • **Disable**: The interface works in non-auto negotiation mode.
Duplex	Duplex mode of an RU interface: • **Full**: The interface works in full-duplex mode. • **Half**: The interface works in half-duplex mode.
Mode	Working mode of an RU interface: • **Copper**: electrical mode • **Fiber**: optical mode
Speed(Mbps)	Rate at which an RU interface works.
Neighbor-Interface	Physical interface used by the central switch for connection with an RU.

3.4.13 display remote-unit port poe

Function

The **display remote-unit port poe** command displays PoE running information about an interface on an RU.

Format

display remote-unit port [*port-id*] **poe** [**connect-interface** *interface-type interface-number* | **name** *remote-unit-name*]

Parameters

Parameter	Description	Value
port-id	Specifies the index of an interface on an RU.	The value is an integer that ranges from 1 to 34.
connect-interface *interface-type interface-number*	Specifies the type and number of an interface connecting the central switch to an RU. The interface type and number can be closely next to each other or separated by a space character.	-
name *remote-unit-name*	Specifies the alias of an RU.	The value must be an existing RU alias.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

You can run the **display remote-unit port poe** command to view PoE running information about interfaces on an RU, including the current power, class of the power device (PD) connected to each interface, reference power of the PD, and power supply status.

If no parameter is specified, the PoE running information about all interfaces on all RUs is displayed.

Precautions

- An uplink 2.5GE optical interface of an RU does not support a copper module, and supports only a GE or 2.5GE optical module. In V200R022C10 and earlier versions, the uplink interface configured with a GE optical module can connect to a central switch only when it works at the rate of 1 Gbit/s. In V200R023C00 and later versions, the uplink interface configured with a 2.5GE optical module can connect to a central switch when it works at the rate of 2.5 Gbit/s. After the rate of the uplink interface is changed, the RU automatically restarts for the change to take effect.
- An uplink 2.5GE hybrid optical-electrical interface of an RU does not support a copper module, and supports only a GE or 2.5GE optical or hybrid module. In V200R022C10 and earlier versions, the uplink interface configured with a

GE optical or hybrid module can connect to a central switch only when it works at the rate of 1 Gbit/s. In V200R023C00 and later versions, the uplink interface configured with a 2.5GE optical or hybrid module can connect to a central switch when it works at the rate of 2.5 Gbit/s. After the rate of the uplink interface is changed, the RU automatically restarts for the change to take effect.

Example

Display the running PoE information about all interfaces on the RU connected to XGigabitEthernet0/0/1 on the central switch.

```
<HUAWEI> display remote-unit port poe connect-interface XGigabitEthernet0/0/1
ESN               :219801177601xxxxxxxx
Name              :-
Device type       :S5731-L4P2HW-RUA
Connect interface  :XGigabitEthernet0/0/1
------------------------------------------------------------
GE1 PoE information:
  PD class                  :-
  PD reference power(mW)      :-
  PD current power(mW)        :0
  PD peak power(mW)           :0
  PD average power(mW)        :0
  Power-up mode             :bt
  Force power               :Disable
  Power ON/OFF              :Off
  Power-on delay(s)         :0
  Power status              :Detecting
  Current(mA)               :0
  Voltage(V)                :0

GE2 PoE information:
  PD class                  :-
  PD reference power(mW)      :-
  PD current power(mW)        :0
  PD peak power(mW)           :0
  PD average power(mW)        :0
  Power-up mode             :bt
  Force power               :Disable
  Power ON/OFF              :Off
  Power-on delay(s)         :0
  Power status              :Detecting
  Current(mA)               :0
  Voltage(V)                :0

GE3 PoE information:
  PD class                  :0
  PD reference power(mW)      :15400
  PD current power(mW)        :4300
  PD peak power(mW)           :4500
  PD average power(mW)        :4120
  Power-up mode             :bt
  Force power               :Disable
  Power ON/OFF              :On
  Power-on delay(s)         :0
  Power status              :Powered
  Current(mA)               :80
  Voltage(V)                :52

GE4 PoE information:
  PD class                  :-
  PD reference power(mW)      :-
  PD current power(mW)        :0
  PD peak power(mW)           :0
  PD average power(mW)        :0
  Power-up mode             :bt
```



```
Force power              :Disable
Power ON/OFF               :Off
Power-on delay(s)          :0
Power status             :Detecting
Current(mA)               :0
Voltage(V)              :0

-------------------------------------------------------
```

Table 3-72 Description of the **display remote-unit port poe** command output

Item	Description
ESN	ESN of an RU.
Name	Alias of an RU. This field displays a hyphen (-) if an RU is not configured with an alias.
Device type	Device type of an RU.
Connect interface	Interface connecting the central switch to an RU.
PD class	Class of the PD connected to an interface. This field displays a hyphen (-) if **Power status** is **Detecting**.
PD reference power(mW)	Reference power of an interface. This field displays a hyphen (-) if **Power status** is **Detecting**.
PD current power(mW)	Current output power of an interface.
PD peak power(mW)	Peak output power of an interface.
PD average power(mW)	Average output power of an interface.
Power-up mode	Power supply mode of an interface.
Force power	Whether forcible PoE power supply is enabled on an interface. To configure this function, run the **poe force-power port** command.
Power ON/OFF	Whether the interface is supplying power: • **on**: The interface is supplying power. • **off**: The interface does not supply power.
Power-on delay(s)	Power supply delay of an interface, in seconds. The value 0 indicates no delay. To set this parameter, run the **poe power-on delay port** command.

Item	Description
Power status	Power supply status of an interface: • **Test mode**: indicates the testing state. • **Detecting**: indicates the detection state. • **Disabled**: indicates that PoE is disabled on the interface. • **Power-deny**: indicates that the reference power is greater than the maximum output power of the interface. • **Classification overcurrent**: indicates that the current of the PDs on the interface exceeds the threshold. • **Unknown**: indicates an unknown class. • **Power overcurrent**: indicates that the interface is in overcurrent condition. • **Power-on failed**: indicates that the interface fails to be powered on. • **Power-ready**: indicates that the interface is ready to be powered on. • **Powering**: indicates that the interface is being powered on. • **Powered**: indicates that the interface has been powered on. • **Overloaded**: indicates that the power is overloaded. • **Time-range power-off**: indicates that the interface is in the power-off time range. • **Unstable voltage**: indicates that the interface voltage is unstable. • **Legacy disable**: indicates that PD compatibility check is disabled on the interface. • **Class mismatch**: indicates that the interface does not support PD classification.
Current(mA)	Output current of an interface.
Voltage(V)	Output voltage of an interface.

3.4.14 display remote-unit port poe realtime

Function

The **display remote-unit port poe realtime** command displays real-time PoE information about an interface on an RU.

Format

display remote-unit port [*port-id*] **poe** { **connect-interface** *interface-type interface-number* | **name** *remote-unit-name* } **realtime**

Parameters

Parameter	Description	Value
port-id	Specifies the index of an interface on an RU.	The value is an integer that ranges from 1 to 34.
connect-interface *interface-type interface-number*	Specifies the type and number of an interface connecting the central switch to an RU. The interface type and number can be closely next to each other or separated by a space character.	-
name *remote-unit-name*	Specifies the alias of an RU.	The value must be an existing RU alias.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display remote-unit port poe realtime** command to view real-time power supply information about interfaces on an RU, such as the current power, class of the PD connected to the interface, reference power of the PD, and power supply status.

Example

Display the real-time running PoE information about all interfaces on the RU connected to XGigabitEthernet0/0/1 on the central switch.


```
<HUAWEI> display remote-unit port poe connect-interface XGigabitEthernet0/0/1 realtime
Info: This operation will take several seconds. Please wait.....
ESN                :219801177601xxxxxxxx
Name               :-
Device type        :S5731-L4P2HW-RUA
Connect interface  :XGigabitEthernet0/0/1
-------------------------------------------------------
GE1 PoE information:
  PD class                  :-
  PD reference power(mW)    :-
  PD current power(mW)      :0
  PD peak power(mW)         :0
  PD average power(mW)      :0
  Power-up mode             :bt
  Force power               :Disable
  Power ON/OFF              :Off
  Power-on delay(s)         :0
  Power status              :Detecting
  Current(mA)               :0
  Voltage(V)                :0
  Insertion and removal status :0

GE2 PoE information:
  PD class                  :-
  PD reference power(mW)    :-
  PD current power(mW)      :0
  PD peak power(mW)         :0
  PD average power(mW)      :0
  Power-up mode             :bt
  Force power               :Disable
  Power ON/OFF              :Off
  Power-on delay(s)         :0
  Power status              :Detecting
  Current(mA)               :0
  Voltage(V)                :0
  Insertion and removal status :0

GE3 PoE information:
  PD class                  :-
  PD reference power(mW)    :-
  PD current power(mW)      :4200
  PD peak power(mW)         :0
  PD average power(mW)      :0
  Power-up mode             :bt
  Force power               :Disable
  Power ON/OFF              :Off
  Power-on delay(s)         :0
  Power status              :Detecting
  Current(mA)               :83
  Voltage(V)                :52
  Insertion and removal status :0

GE4 PoE information:
  PD class                  :-
  PD reference power(mW)    :-
  PD current power(mW)      :0
  PD peak power(mW)         :0
  PD average power(mW)      :0
  Power-up mode             :bt
  Force power               :Disable
  Power ON/OFF              :Off
  Power-on delay(s)         :0
  Power status              :Detecting
  Current(mA)               :0
  Voltage(V)                :0
  Insertion and removal status :0

-------------------------------------------------------
```


Table 3-73 Description of the **display remote-unit port poe** command output

Item	Description
ESN	ESN of an RU.
Name	Alias of an RU. This field displays a hyphen (-) if an RU is not configured with an alias.
Device type	Device type of an RU.
Connect interface	Interconnection interface.
PD class	Class of the PD connected to an interface. This field displays a hyphen (-) if **Power status** is **Detecting**.
PD reference power(mW)	Reference power of an interface. This field displays a hyphen (-) if **Power status** is **Detecting**.
PD current power(mW)	Current output power of an interface.
PD peak power(mW)	Peak output power of an interface.
PD average power(mW)	Average output power of an interface.
Power-up mode	Power supply mode of an interface.
Force power	Whether forcible PoE power supply is enabled on an interface. To configure this function, run the **poe force-power port** command.
Power ON/OFF	Whether the interface is providing power: • **on**: The interface is supplying power. • **off**: The interface does not supply power.
Power-on delay(s)	Power supply delay of an interface, in seconds. The value 0 indicates no delay. To set this parameter, run the **poe power-on delay port** command.

Item	Description
Power status	Power supply status of an interface: • **Test mode**: indicates the testing state. • **Detecting**: indicates the detection state. • **Disabled**: indicates that PoE is disabled on the interface. • **Power-deny**: indicates that the reference power is greater than the maximum output power of the interface. • **Classification overcurrent**: indicates that the current of the PDs on the interface exceeds the threshold. • **Unknown**: indicates an unknown class. • **Power overcurrent**: indicates that the interface is in overcurrent condition. • **Power-on failed**: indicates that the interface fails to be powered on. • **Power-ready**: indicates that the interface is ready to be powered on. • **Powering**: indicates that the interface is being powered on. • **Powered**: indicates that the interface has been powered on. • **Overloaded**: indicates that the power is overloaded. • **Time-range power-off**: indicates that the interface is in the power-off time range. • **Unstable voltage**: indicates that the interface voltage is unstable. • **Legacy disable**: indicates that PD compatibility check is disabled on the interface. • **Class mismatch**: indicates that the interface does not support PD classification.
Current(mA)	Output current of an interface.
Voltage(V)	Output voltage of an interface.

Item	Description
Insertion and removal status	Whether the interface has PD removal and installation records. • **0**: initial value, which is meaningless. If an RU is started with a PD, this field displays **0**. • **1**: indicates that the interface has PD installation records. • **2**: indicates that the interface has PD removal records. • **3**: indicates that the interface has PD removal and installation records

3.4.15 display remote-unit port realtime

Function

The **display remote-unit port realtime** command displays real-time information about interfaces on an RU.

Format

display remote-unit port { **connect-interface** *interface-type interface-number* | **name** *remote-unit-name* } **realtime**

Parameters

Parameter	Description	Value
connect-interface *interface-type interface-number*	Specifies the type and number of an interface connecting the central switch to an RU. The interface type and number can be closely next to each other or separated by a space character.	-
name *remote-unit-name*	Specifies the alias of an RU.	The value must be an existing RU alias.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

To monitor interfaces on a specific RU or locate faults on interfaces, you can run the **display remote-unit port realtime** command to view real-time information about the interfaces, including the physical status, auto-negotiation status, working mode, and rate.

Precautions

- An uplink 2.5GE optical interface of an RU does not support a copper module, and supports only a GE or 2.5GE optical module. In V200R022C10 and earlier versions, the uplink interface configured with a GE optical module can connect to a central switch only when it works at the rate of 1 Gbit/s. In V200R023C00 and later versions, the uplink interface configured with a 2.5GE optical module can connect to a central switch when it works at the rate of 2.5 Gbit/s. After the rate of the uplink interface is changed, the RU automatically restarts for the change to take effect.
- An uplink 2.5GE hybrid optical-electrical interface of an RU does not support a copper module, and supports only a GE or 2.5GE optical or hybrid module. In V200R022C10 and earlier versions, the uplink interface configured with a GE optical or hybrid module can connect to a central switch only when it works at the rate of 1 Gbit/s. In V200R023C00 and later versions, the uplink interface configured with a 2.5GE optical or hybrid module can connect to a central switch when it works at the rate of 2.5 Gbit/s. After the rate of the uplink interface is changed, the RU automatically restarts for the change to take effect.

Example

Display information about all interfaces on the RUs connected to Eth-Trunk 10 on the central switch.

```
<HUAWEI> system-view
[HUAWEI] display remote-unit port connect-interface Eth-Trunk 10 realtime
Info: This operation will take several seconds. Please wait...
ESN               :219801177801xxxxxxxx
Name              :-
Device type       :S5731-L4P2HW-RUA
Connect interface  :Eth-Trunk10
--------------------------------------------------------------------------------
Interface     PHY      Negotiation     Duplex    Mode     Speed(Mbps)   Neighbor-Interface
--------------------------------------------------------------------------------
GE1           Up       Enable          Full      Copper    1000          -
GE2           Down      Enable          Full      Copper    1000          -
GE3           Down      Enable          Full      Copper    1000          -
GE4           Down      Enable          Full      Copper    1000          -
GE5           Down      Enable          Full      Copper    1000          -
GE6           Up       Enable          Full      Fiber     1000          GE0/0/36
--------------------------------------------------------------------------------
```

Table 3-74 Description of the **display remote-unit port brief** command output

Item	Description
ESN	ESN of an RU.

Item	Description
Name	Alias of an RU. This field displays a hyphen (-) if an RU is not configured with an alias.
Connect interface	Interface connecting the central switch to an RU.
Interface	Interface of an RU.
PHY	Status of an RU interface: • **up**: The interface is Up. • **down**: The interface is Down.
Negotiation	Auto-negotiation status of an RU interface: • **Enable**: The interface works in auto-negotiation mode. • **Disable**: The interface works in non-auto negotiation mode.
Duplex	Duplex mode of an RU interface: • **Full**: The interface works in full-duplex mode. • **Half**: The interface works in half-duplex mode.
Mode	Working mode of an RU interface: • **Copper**: electrical mode • **Fiber**: optical mode
Speed(Mbps)	Rate at which an RU interface works.
Neighbor-Interface	Physical interface used by the central switch for connection with an RU.

3.4.16 display remote-unit port statistics

Function

The **display remote-unit port statistics** command displays traffic statistics about an interface on an RU.

Format

display remote-unit port [*port-id*] **statistics** [**connect-interface** *interface-type interface-number* | **name** *remote-unit-name*]

Parameters

Parameter	Description	Value
port-id	Specifies the index of an interface on an RU.	The value is an integer that ranges from 1 to 34. If this parameter is not specified, statistics about all interfaces on the RU are displayed.
connect-interface *interface-type interface-number*	Specifies the type and number of an interface connecting the central switch to an RU. The interface type and number can be closely next to each other or separated by a space character.	-
name *remote-unit-name*	Specifies the alias of an RU.	The value must be an existing RU alias.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

You can run this command to view the status and statistics of interfaces on an RU, including the interface physical status, basic configuration, and packet forwarding information. The information is refreshed every 60 seconds. You can use this command to collect traffic statistics or locate faults on an interface. If no index of an RU interface is specified, traffic statistics about all interfaces on the RU are displayed.

Precautions

- An uplink 2.5GE optical interface of an RU does not support a copper module, and supports only a GE or 2.5GE optical module. In V200R022C10 and earlier versions, the uplink interface configured with a GE optical module can connect to a central switch only when it works at the rate of 1 Gbit/s. In V200R023C00 and later versions, the uplink interface configured with a 2.5GE optical module can connect to a central switch when it works at the rate of 2.5 Gbit/s. After the rate of the uplink interface is changed, the RU automatically restarts for the change to take effect.
- An uplink 2.5GE hybrid optical-electrical interface of an RU does not support a copper module, and supports only a GE or 2.5GE optical or hybrid module.

In V200R022C10 and earlier versions, the uplink interface configured with a GE optical or hybrid module can connect to a central switch only when it works at the rate of 1 Gbit/s. In V200R023C00 and later versions, the uplink interface configured with a 2.5GE optical or hybrid module can connect to a central switch when it works at the rate of 2.5 Gbit/s. After the rate of the uplink interface is changed, the RU automatically restarts for the change to take effect.

Example

Display traffic statistics on interface 1 of the RU connected to Eth-Trunk 10 on the central switch.

```
<HUAWEI> display remote-unit port 1 statistics connect-interface Eth-Trunk 10
ESN               :219801177601XXXXXXXX
Name              :S5731S-4P
Device type       :S5731-L8P2HT-RUA
Connect interface  :Eth-Trunk10
------------------------------------------------------------------------------
GE1 current state : DOWN
Speed: 1000,  Duplex: Full,  Negotiation: Enable,  Mode: Copper,  Congestion: No
Input rate 0 bits/sec, 0 packets/sec
Output rate 0 bits/sec, 0 packets/sec

Input: 0 packets, 0 bytes
  Unicast:                0,  Multicast:                0
  Broadcast:              0,  Jumbo:                    0
  Discard:                0,  Pause:                    0
  Frames:                 0

  Total Error:            0
  CRC:                    0,  Giants:                   0
  Runts:                  0,  DropEvents:               0
  Alignments:             0,  Symbols:                  0
  Ignoreds:               0

Output : 0 packets, 0 bytes
  Unicast:                0,  Multicast:                0
  Broadcast:              0,  Jumbo:                    0
  Discard:                0,  Pause:                    0

  Total Error:            0
  Collisions:             0,  Late Collisions:          0
  Deferreds:              0

    Input bandwidth utilization threshold : 80.00%
    Output bandwidth utilization threshold: 80.00%
    Last 60 seconds input utility rate : 0.00%
    Last 60 seconds output utility rate: 0.00%

------------------------------------------------------------------------------
```

Table 3-75 Description of the **display remote-unit port statistics** command output

Item	Description
ESN	ESN of an RU.
Name	Alias of an RU. This field displays a hyphen (-) if an RU is not configured with an alias.

Item	Description
Device type	Device type of an RU.
Connect interface	Interconnection interface.
GE*n* current state	Physical status of the GE*n* interface on an RU. • **DOWN**: indicates that a fault occurs at the physical layer of the interface. The possible cause can be that no terminal is connected to the interface or the interface is shut down. • **Up**: indicates that the interface is physically Up.
Speed	Current rate of an interface. • In auto-negotiation mode, this field displays the interface rate after auto-negotiation with terminals. • In non-auto-negotiation mode, you can run the **speed** command to configure an interface rate.
Duplex	Duplex mode of an interface: • **Full**: The interface works in full-duplex mode. • **Half**: The interface works in half-duplex mode.
Negotiation	Auto-negotiation status of an interface. To configure auto-negotiation for an interface, run the **negotiation auto** command. • **Enable**: The interface works in auto-negotiation mode. • **Disable**: The interface works in non-auto negotiation mode.
Mode	Working mode of an interface: • **Copper**: electrical mode • **Fiber**: optical mode
Congestion	Congestion status of an RU interface: • **YES**: The RU interface is congested. • **NO**: The RU interface is not congested.
Input rate 0 bits/sec, 0 packets/sec	Rate of incoming packets on an interface.

Item	Description
Output rate 0 bits/sec, 0 packets/sec	Rate of outgoing packets on an interface.
Input	Total number of received packets. **NOTE** • Packets that are longer than jumbo frames and have correct CRC values are counted in **Jumbo** statistics but not in **Input** statistics. • An RU can forward a packet with a maximum size of 10240 bytes.
Output	Total number of sent packets.
Unicast	Number of unicast packets received or sent by an interface.
Multicast	Number of multicast packets received or sent by an interface.
Broadcast	Number of broadcast packets that are received or sent by the interface.
Jumbo	Statistics about outgoing packets on an interface. The following packets are counted: • Ethernet frames longer than 1518 bytes and with correct FCS values Statistics about incoming packets on an interface. The following packets are counted: • Ethernet frames with the length greater than or equal to 1519 bytes and less than the maximum jumbo frame length and correct FCS values • VLAN frames with the length greater than or equal to 1519 bytes and less than the maximum jumbo frame length and correct FCS values • Packets with the length greater than the maximum jumbo frame length
Discard	Number of packets discarded by an interface during physical layer detection. A possible cause can be interface congestion. **NOTE** Currently, this item is not supported, and the value is displayed as 0.

Item	Description
Frames	Number of packets with the incorrect 802.3 length received by an interface.
Pause	Number of pause frames.
Total Error	Number of error frames found during physical layer detection.
CRC	Number of packets longer than 63 bytes and with incorrect FCS values.
Giants	Number of received packets with the length exceeding the maximum jumbo frame length. **NOTE** Currently, this item is not supported, and the value is displayed as 0. Such packets are counted in the **Jumbo** field.
Runts	Number of received undersized frames with correct CRC values. An undersized frame is a frame that is shorter than 64 bytes, in correct format, and contains a valid CRC field. **NOTE** Packets with incorrect CRC values and the length shorter than 64 bytes are also counted in **Runts**.
DropEvents	Number of received packets that are discarded due to GBP full or back pressure.
Alignments	Number of received frames with alignment errors. **NOTE** Currently, this item is not supported, and the value is displayed as 0.
Symbols	Number of received frames with coding errors.
Ignoreds	Number of received MAC control frames whose OpCode is not PAUSE. **NOTE** If an RU interface receives an **Ignoreds** packet, the packet is not only counted as an Ignoreds packet, but also is counted as a unicast, multicast, or a broadcast packet. The total number of incoming packets on an interface has excluded repeated counts. Therefore, the statistics are correct.

Item	Description
Collisions	Number of collision frames. A collision frame is a frame that is not sent due to a detected collision.
Late Collisions	Number of deferred collision frames. A deferred collision frame is a frame that is delayed to be sent because of a deferred collision detected after the frame's first 512 bits are sent.
Deferreds	Number of deferred packets. A deferred packet refers to a packet that is delayed due to a detected collision.
Input bandwidth utilization threshold	Threshold for inbound bandwidth usage.
Output bandwidth utilization threshold	Threshold for outbound bandwidth usage.
Last 60 seconds input utility rate	Inbound bandwidth usage within the last 60 seconds.
Last 60 seconds output utility rate	Outbound bandwidth usage within the last 60 seconds.

3.4.17 display remote-unit port statistics realtime

Function

The **display remote-unit port statistics realtime** command displays real-time traffic statistics about an interface on an RU.

Format

display remote-unit port [*port-id*] **statistics** { **connect-interface** *interface-type interface-number* | **name** *remote-unit-name* } **realtime**

Parameters

Parameter	Description	Value
port-id	Specifies the index of an interface on an RU.	The value is an integer that ranges from 1 to 34. If this parameter is not specified, statistics about all interfaces on the RU are displayed.

Parameter	Description	Value
connect-interface *interface-type interface-number*	Specifies the type and number of an interface. The interface type and number can be closely next to each other or separated by a space character.	-
name *remote-unit-name*	Specifies the alias of an RU.	The value must be an existing RU alias.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can view the status and statistics of interfaces on an RU, including the interface physical status, basic configuration, and packet forwarding information. You can run this command when you need to collect real-time traffic statistics or diagnose faults on an interface in real time, or when you cannot locate faults according to the information reported by RUs at an interval of 60s.

Example

Display real-time traffic statistics about interface 1 on the RU connected to XGigabitEthernet0/0/5 on the central switch

```
<HUAWEI> display remote-unit port 1 statistics  connect-interface XGigabitEthernet 0/0/5 realtime
ESN               :219801176601XXXXXXXX
Name              :-
Device type       :S5731-L8P2HT-RUA
Connect interface  :XGigabitEthernet 0/0/5
------------------------------------------------------------------------------
GE1 current state : UP
Speed: 1000,  Duplex: Full,  Negotiation: Enable,  Mode: Copper,  Congestion: No
Input rate 0 bits/sec, 0 packets/sec
Output rate 2294 bits/sec, 2 packets/sec

Input: 0 packets, 0 bytes
  Unicast:                0,  Multicast:                0
  Broadcast:              0,  Jumbo:                    0
  Discard:                0,  Pause:                    0
  Frames:                 0

  Total Error:            0
  CRC:                    0,  Giants:                   0
  Runts:                  0,  DropEvents:               0
  Alignments:             0,  Symbols:                  0
  Ignoreds:               0

Output : 2719354134 packets, 503308078504 bytes
  Unicast:                0,  Multicast:            50766
  Broadcast:        2719303368,  Jumbo:                 0
```



```
Discard:                0,  Pause:                0

Total Error:            0
Collisions:             0,  Late Collisions:      0
Deferreds:              0

  Input bandwidth utilization threshold : 80.00%
  Output bandwidth utilization threshold: 80.00%
  Last 60 seconds input utility rate : 0.00%
  Last 60 seconds output utility rate: 0.00%

--------------------------------------------------------------------------------
```

Table 3-76 Description of the **display remote-unit port statistics realtime** command output

Item	Description
ESN	ESN of an RU.
Name	Alias of an RU. This field displays a hyphen (-) if an RU is not configured with an alias.
Device type	Device type of an RU.
Connect interface	Interconnection interface.
GE*n* current state	Physical status of the GE*n* interface on an RU. • **DOWN**: indicates that a fault occurs at the physical layer of the interface. The possible cause can be that no terminal is connected to the interface or the interface is shut down. • **Up**: indicates that the interface is physically Up.
Speed	Current rate of an interface. • In auto-negotiation mode, this field displays the interface rate after auto-negotiation with terminals. • In non-auto-negotiation mode, you can run the **speed** command to configure an interface rate.
Duplex	Duplex mode of an interface: • **Full**: The interface works in full-duplex mode. • **Half**: The interface works in half-duplex mode.

Item	Description
Negotiation	Auto-negotiation status of an interface. To configure auto-negotiation for an interface, you can run the **negotiation auto** command. • **Enable**: The interface works in auto-negotiation mode. • **Disable**: The interface works in non-auto negotiation mode.
Mode	Working mode of an interface: • **Copper**: electrical mode • **Fiber**: optical mode
Congestion	Congestion status of an RU interface: • **YES**: The RU interface is congested. • **NO**: The RU interface is not congested.
Input rate 0 bits/sec, 0 packets/sec	Rate of incoming packets on an interface.
Output rate 0 bits/sec, 0 packets/sec	Rate of outgoing packets on an interface.
Input	Total number of received packets. **NOTE** • Packets that are longer than jumbo frames and have correct CRC values are counted in **Jumbo** statistics but not in **Input** statistics. • An RU can forward a packet with a maximum size of 10240 bytes.
Output	Total number of sent packets.
Unicast	Number of unicast packets received or sent by an interface.
Multicast	Number of multicast packets received or sent by an interface.
Broadcast	Number of broadcast packets that are received or sent by the interface.

Item	Description
Jumbo	Statistics about outgoing packets on an interface. The following packets are counted: • Ethernet frames longer than 1518 bytes and with correct FCS values Statistics about incoming packets on an interface. The following packets are counted: • Ethernet frames with the length greater than or equal to 1519 bytes and less than the maximum jumbo frame length and correct FCS values • VLAN frames with the length greater than or equal to 1519 bytes and less than the maximum jumbo frame length and correct FCS values • Packets with the length greater than the maximum jumbo frame length
Discard	Number of packets discarded by an interface during physical layer detection. A possible cause can be interface congestion. **NOTE** Currently, this item is not supported, and the value is displayed as 0.
Frames	Number of packets with the incorrect 802.3 length received by an interface.
Pause	Number of Pause frames.
Total Error	Number of error frames found during physical layer detection.
CRC	Number of packets longer than 63 bytes and with incorrect FCS values.
Giants	Number of received packets with the length exceeding the maximum jumbo frame length. **NOTE** Currently, this item is not supported, and the value is displayed as 0. Such packets are counted in the **Jumbo** field.

Item	Description
Runts	Number of received undersized frames with correct CRC values. An undersized frame is a frame that is shorter than 64 bytes, in correct format, and contains a valid CRC field. **NOTE** Packets with incorrect CRC values and the length shorter than 64 bytes are also counted in **Runts**.
DropEvents	Number of received packets that are discarded due to GBP full or back pressure.
Alignments	Number of received frames with alignment errors. **NOTE** Currently, this item is not supported, and the value is displayed as 0.
Symbols	Number of received frames with coding errors.
Ignoreds	Number of received MAC control frames whose OpCode is not PAUSE. **NOTE** If an RU interface receives an **Ignoreds** packet, the packet is not only counted as an Ignoreds packet, but also is counted as a unicast, multicast, or a broadcast packet. The total number of incoming packets on an interface has excluded repeated counts. Therefore, the statistics are correct.
Collisions	Number of collision frames. A collision frame is a packet that is not sent due to a detected collision.
Late Collisions	Number of deferred collision frames. A deferred collision frame is a frame that is delayed to be sent because of a deferred collision detected after the transmission of the frame first 512 bits.
Deferreds	Number of deferred packets. A deferred packet refers to a packet that is delayed due to a detected collision.
Input bandwidth utilization threshold	Threshold for the inbound bandwidth usage.
Output bandwidth utilization threshold	Threshold for the outbound bandwidth usage.

Item	Description
Last 60 seconds input utility rate	Inbound bandwidth usage within the last 60 seconds.
Last 60 seconds output utility rate	Outbound bandwidth usage within the last 60 seconds.

3.4.18 display remote-unit port transceiver

Function

The **display remote-unit port transceiver** command displays information about the optical module installed on an interface of an RU.

Format

display remote-unit port [*port-id*] **transceiver** [**connect-interface** *interface-type interface-number* | **name** *remote-unit-name*]

Parameters

Parameter	Description	Value
port-id	Specifies the index of an interface on an RU.	The value is an integer that ranges from 1 to 34. If this parameter is not specified, statistics about all interfaces on the RU are displayed.
connect-interface *interface-type interface-number*	Specifies the type and number of an interface. The interface type and number can be closely next to each other or separated by a space character.	-
name *remote-unit-name*	Specifies the alias of an RU.	The value must be an existing RU alias.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run this command to view general, manufacturing, and diagnostic information about the optical module installed on an interface of an RU.

Example

Display information about the optical module installed on the interface with index 6 of all RUs.

```
<HUAWEI> display remote-unit port 6 transceiver
ESN               :219801177001xxxxxxxx
Name              :-
Device type       :S5731-L4P2HW-RUA
Connect interface  :GigabitEthernet0/0/27
------------------------------------------------------------
GE6 transceiver information:
------------------------------------------------------------
Common information:
  Transceiver type                :1000_BASE_LX_SFP
  Transfer distance(m)            :10000(9um)
  Digital diagnostic monitoring    :YES
  Vendor name                     :WTD
------------------------------------------------------------
Manufacture information:
  Manu. serial Number             :MF213704450083
  Manufacturing date              :2021-10-22
  Vendor name                     :WTD
------------------------------------------------------------
Diagnostic information:
  Temperature(Celsius)            :57.04
  Temp high threshold(Celsius)     :95.00
  Temp low  threshold(Celsius)     :-50.00
  Voltage(V)                      :3.27
  Volt high threshold(V)           :3.63
  Volt low  threshold(V)           :2.97
  Bias current(mA)                :32.89
  Bias high threshold(mA)          :80.00
  Bias low threshold(mA)           :10.00
  RX power(dBM)                   :-5.52
  RX power high warning(dBM)       :-3.00
  RX power low warning(dBM)        :-19.00
  RX power high threshold(dBM)     :-1.00
  RX power low threshold(dBM)      :-21.02
  TX power(dBM)                   :-4.62
  TX power high warning(dBM)       :-3.00
  TX power low warning(dBM)        :-11.00
  TX power high threshold(dBM)     :-1.00
  TX power low threshold(dBM)      :-13.00


------------------------------------------------------------
ESN               :QU221A000285
Name              :-
Device type       :S5731-L8P2HT-RUA
Connect interface  :GigabitEthernet0/0/1
------------------------------------------------------------
GE10 transceiver information:
------------------------------------------------------------
Common information:
  Transceiver type                :1000_BASE_LX_SFP
  Transfer distance(m)            :10000(9um)
  Digital diagnostic monitoring    :YES
  Vendor name                     :WTD
------------------------------------------------------------
Manufacture information:
  Manu. serial Number             :MF213704450086
  Manufacturing date              :2021-10-22
```



```
  Vendor name                    :WTD
-------------------------------------------------------------
Diagnostic information:
  Temperature(Celsius)           :57.04
  Temp high threshold(Celsius)   :95.00
  Temp low  threshold(Celsius)   :-50.00
  Voltage(V)                     :3.27
  Volt high threshold(V)         :3.63
  Volt low  threshold(V)         :2.97
  Bias current(mA)               :32.64
  Bias high threshold(mA)        :80.00
  Bias low threshold(mA)         :10.00
  RX power(dBM)                  :-5.99
  RX power high warning(dBM)     :-3.00
  RX power low warning(dBM)      :-19.00
  RX power high threshold(dBM)   :-1.00
  RX power low threshold(dBM)    :-21.02
  TX power(dBM)                  :-4.62
  TX power high warning(dBM)     :-3.00
  TX power low warning(dBM)      :-11.00
  TX power high threshold(dBM)   :-1.00
  TX power low threshold(dBM)    :-13.00

-------------------------------------------------------------
```

Table 3-77 Description of the **display remote-unit port transceiver** command output

Item	Description
ESN	ESN of an RU.
Name	Alias of an RU. This field displays a hyphen (-) if an RU is not configured with an alias.
Device type	Device type of an RU.
Connect interface	Interconnection interface.
GE*n* transceiver information	Information about the optical module installed on the GE*n* interface of an RU.
Common information	General information.
Transceiver type	Type of an optical module.

Item	Description
Transfer distance(m)	Transmission distance of an optical module. • **OM1**: indicates traditional 62.5 μm/125 μm multimode fibers. • **OM2**: indicates traditional 50 μm/125 μm multimode fibers. • **OM3**: indicates next-generation multimode fibers, with longer transmission distances than OM1 and OM2 fibers. For a GPS optical module, this field indicates the maximum length of the antenna between the GPS optical module and signal receiver. **NOTE** The device displays only the maximum transmission distances supported by different optical fibers of an optical module.
Digital diagnostic monitoring	Whether diagnostic information about an optical module is monitored.
Vendor name	Vendor of an optical module.
Manufacture information	Manufacture information.
Manu. serial Number	Manufacturing sequence number of an optical module.
Manufacturing date	Manufacturing date of an optical module.
Diagnostic information	Diagnostic information.
Temperature(Celsius)	Current temperature of an optical module.
Temp high threshold(Celsius)	Upper temperature threshold of an optical module.
Temp low threshold(Celsius)	Lower temperature threshold of an optical module.
Voltage(V)	Current voltage of an optical module.
Volt high threshold(V)	Upper voltage threshold of an optical module.
Volt low threshold(V)	Lower voltage threshold of an optical module.
Bias current(mA)	Bias current of an optical module.

Item	Description
Bias high threshold(mA)	Upper threshold for the bias current of an optical module.
Bias low threshold(mA)	Lower threshold for the bias current of an optical module.
RX power(dBM)	Receive power of an optical module. When the receive power is 0 W, this field displays **-Inf**.
RX power high warning(dBM)	Upper warning threshold for the receive power of an optical module.
RX power low warning(dBM)	Lower warning threshold for the receive power of an optical module.
RX power high threshold(dBM)	Upper receive power threshold of an optical module.
RX power low threshold(dBM)	Lower receive power threshold of an optical module.
TX power(dBM)	Transmit power of an optical module. When the transmit power is 0 W, this field displays **-Inf**.
TX power high warning(dBM)	Upper warning threshold for the transmit power of an optical module.
TX power low warning(dBM)	Lower warning threshold for the transmit power of an optical module.
TX power high threshold(dBM)	Upper transmit power threshold of an optical module.
TX power low threshold(dBM)	Lower transmit power threshold of an optical module.

3.4.19 display remote-unit port transceiver realtime

Function

The **display remote-unit port transceiver** command displays real-time information about the optical module installed on an interface of an RU.

Format

display remote-unit port [*port-id*] **transceiver** { **connect-interface** *interface-type interface-number* | **name** *remote-unit-name* } **realtime**

Parameters

Parameter	Description	Value
port-id	Specifies the index of an interface on an RU.	The value is an integer that ranges from 1 to 34. If this parameter is not specified, statistics about all interfaces on the RU are displayed.
connect-interface *interface-type interface-number*	Specifies the type and number of an interface. The interface type and number can be closely next to each other or separated by a space character.	-
name *remote-unit-name*	Specifies the alias of an RU.	The value must be an existing RU alias.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run this command to view real-time information about the optical modules installed on an RU.

Example

Display real-time information about the optical module installed on the interface with index 6 of the RU connected to XGigabitEthernet 0/0/5 on the central switch.

```
<HUAWEI> display remote-unit port 6 transceiver connect-interface XGigabitEthernet 0/0/5 realtime
Info: This operation will take several seconds. Please wait.....
ESN                 :219801177002xxxxxxxx
Name                :-
Device type         :S5731-L8P2HT-RUA
Connect interface   :XGigabitEthernet0/0/5
------------------------------------------------------------
GE6 transceiver information:
------------------------------------------------------------
Common information:
  Transceiver type                :1000_BASE_SX_SFP
  Transfer distance(m)            :275(OM1),550(OM2),1000(OM3)
  Digital diagnostic monitoring   :YES
  Vendor name                     :WTD
------------------------------------------------------------
Manufacture information:
  Manu. serial Number             :EC184500011577
```



```
  Manufacturing date             :2018-11-06
  Vendor name                    :WTD
------------------------------------------------------------
Diagnostic information:
  Temperature(Celsius)           :57.04
  Temp high threshold(Celsius)   :95.00
  Temp low  threshold(Celsius)   :-50.00
  Voltage(V)                     :3.31
  Volt High Threshold(V)         :3.63
  Volt Low  Threshold(V)         :2.97
  Bias current(mA)               :2.78
  Bias high threshold(mA)        :40.00
  Bias low threshold(mA)         :0.00
  RX power(dBM)                  :-5.66
  RX power high warning(dBM)     :0.00
  RX power low warning(dBM)      :-17.01
  RX power high threshold(dBM)   :2.00
  RX power low threshold(dBM)    :-19.03
  TX power(dBM)                  :-5.77
  TX power high warning(dBM)     :0.00
  TX power low warning(dBM)      :-9.50
  TX power high threshold(dBM)   :2.00
  TX power low threshold(dBM)    :-11.51

------------------------------------------------------------
```

Table 3-78 Description of the **display remote-unit port transceiver realtime** command output

Item	Description
ESN	ESN of an RU.
Name	Alias of an RU. This field displays a hyphen (-) if an RU is not configured with an alias.
Connect interface	Interface connecting the central switch to an RU.
GE*n* transceiver information	Information about the optical module installed on the GE*n* interface of an RU.
Common information	General information.
Transceiver type	Type of an optical module.

Item	Description
Transfer distance(m)	Transmission distance of an optical module. • **OM1**: indicates traditional 62.5 μm/125 μm multimode fibers. • **OM2**: indicates traditional 50 μm/125 μm multimode fibers. • **OM3**: indicates next-generation multimode fibers, with longer transmission distances than OM1 and OM2 fibers. For a GPS optical module, this field indicates the maximum length of the antenna between the GPS optical module and signal receiver. **NOTE** The device displays only the maximum transmission distances supported by different optical fibers of an optical module.
Digital diagnostic monitoring	Whether diagnostic information about an optical module is monitored.
Vendor name	Vendor of an optical module.
Manufacture information	Manufacture information.
Manu. serial Number	Manufacturing sequence number of an optical module.
Manufacturing date	Manufacturing date of an optical module.
Vendor name	Vendor of an optical module.
Diagnostic information	Diagnostic information.
Temperature(Celsius)	Current temperature of an optical module.
Temp high threshold(Celsius)	Upper temperature threshold of an optical module.
Temp low threshold(Celsius)	Lower temperature threshold of an optical module.
Voltage(V)	Current voltage of an optical module.
Volt high threshold(V)	Upper voltage threshold of an optical module.
Volt low threshold(V)	Lower voltage threshold of an optical module.

Item	Description
Bias current(mA)	Bias current of an optical module.
Bias high threshold(mA)	Upper threshold for the bias current of an optical module.
Bias low threshold(mA)	Lower threshold for the bias current of an optical module.
RX power(dBM)	Receive power of an optical module. When the receive power is 0 W, this field displays **-Inf**.
RX power high warning(dBM)	Upper warning threshold for the receive power of an optical module.
RX power low warning(dBM)	Lower warning threshold for the receive power of an optical module.
RX power high threshold(dBM)	Upper receive power threshold of an optical module.
RX power low threshold(dBM)	Lower receive power threshold of an optical module.
TX power(dBM)	Transmit power of an optical module. When the transmit power is 0 W, this field displays **-Inf**.
TX power high warning(dBM)	Upper warning threshold for the transmit power of an optical module.
TX power low warning(dBM)	Lower warning threshold for the transmit power of an optical module.
TX power high threshold(dBM)	Upper transmit power threshold of an optical module.
TX power low threshold(dBM)	Lower transmit power threshold of an optical module.

3.4.20 display remote-unit upgrade

Function

The **display remote-unit upgrade** command displays RU upgrade information.

Format

display remote-unit upgrade { **record** | **information** }

Parameters

Parameter	Description	Value
record	Displays upgrade records of RUs.	-
information	Displays the upgrade information about the RUs that are being upgraded.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

An RU has three types of firmware: APP firmware (controlling the forwarding process, parsing XLDP packets, and processing configurations), PoE firmware, and BIOS firmware. The three types of firmware can all be upgraded. System software packages or patches (containing firmware) of the central switch can be used to upgrade RUs.

You can run this command to view the upgrade information about RUs. The information includes the firmware version of an RU connected to the central switch, information about the RUs that fail to be upgraded and enter the cooldown period, information about RUs which have the firmware package of the new version successfully pre-loaded and wait to be reset, information about RUs that are being upgraded, and the upgrade progress in percentage. After the upgrade is complete, you can run this command to check upgrade records.

If an RU fails to be upgraded, it enters the cooldown period. You can upgrade it again only after the cooldown period ends.

Example

Display RU upgrade information.

```
<HUAWEI> system-view
[HUAWEI] display remote-unit upgrade information
Firmware information:
--------------------------------------------------------------------------------
Type            Version               From              Note
--------------------------------------------------------------------------------
APP             220207016             Startup software  -
POE             -                     -                 -
BIOS            220207016             Startup software  -

Remote-unit during cooling down:
--------------------------------------------------------------------------------
Type            ConnectInterface      FailCnt           CoolDownInSeconds
--------------------------------------------------------------------------------

Waiting for restart to apply new firmware's remote-unit information:
--------------------------------------------------------------------------------
```



```
Type            ConnectInterface       NextVersion(APP/POE/BIOS)
--------------------------------------------------------------------------------

Upgrading remote-unit information:
--------------------------------------------------------------------------------
Type            ConnectInterface       Firmware          Percent
--------------------------------------------------------------------------------
S5731-L8P2HT-RUA  XGigabitEthernet0/0/1  APP               3%
```

Table 3-79 Description of the **display remote-unit upgrade information** command output

Item	Description
Firmware information	Firmware of the RU to be upgraded.
Type	Firmware type. The options include **APP**, **POE**, and **BIOS**.
Version	Firmware version. **NOTE** For an RU of the S5731-L16P2SR-RUA or S5731S-L16P2SR-RUA model, only the following firmware versions are supported: APP firmware: 221207011 PoE firmware: 7701 BIOS firmware: 220225001 The S5731-L8LP2ST-RUA supports only the following firmware versions: APP firmware: 230109001 and later
From	Source file used for upgrading the RU. It can be a patch or software package of the central switch.
Note	Whether the current firmware is successfully signed. • -: The signature is correct. • **Bad signature**: The firmware patch signature is incorrect. In this case, the firmware will not be upgraded. • **No signature**: The firmware patch does not have a digital signature. In this case, the firmware will not be upgraded.
Remote-unit during cooling down	RUs that fail to be upgraded and are in the cooldown period. You can end the cooldown period of an RU by resetting the RU.
Type	Device type of an RU.
ConnectInterface	Interconnection interface.
FailCnt	Number of upgrade failures.

Item	Description
CoolDownInSeconds	Remaining seconds in the cooldown period. When the value becomes 0, the RU can be upgraded again.
Waiting for restart to apply new firmware's remote-unit information	Information about the RUs that have new firmware successfully pre-loaded and wait to be reset. **NOTE** If the function of applying new functions after the upgrade at a specified time is enabled, the information about the RUs to be reset at a specified time is displayed. If this function is disabled and an RU cannot be reset in time, the information about the RU is displayed in this field for a short time. After the RU is reset, the corresponding information is automatically cleared.
NextVersion(APP/POE/BIOS)	Version number for the next startup. **NOTE** If the upgrade command is run in the remote-unit view, the version for the next RU startup is displayed. For the firmware not supported by the RU, a hyphen (-) is displayed. If the forcible upgrade command is run in the remote-unit N view, the version number only of the upgraded firmware is displayed. For the firmware not upgraded, a hyphen (-) is displayed.
Upgrading remote-unit information:	Information about the RUs that are being upgraded.
Firmware	Firmware type. The options include **APP**, **POE**, and **BIOS**.
Percent	Upgrade progress, in percentage.

Display upgrade records of RUs.

```
<HUAWEI> system-view
[HUAWEI] display remote-unit upgrade record
--------------------------------------------------------------------------------
StartTime           ConnectInterface        Firmware   UpdateResult
--------------------------------------------------------------------------------
2021/12/25 03:25:54 XGigabitEthernet0/0/1   APP        Success
2021/12/25 03:30:08 XGigabitEthernet0/0/1   APP        Success
```


Table 3-80 Description of the **display remote-unit upgrade record** command output

Item	Description
StartTime	Start time.
ConnectInterface	Interconnection interface.
Firmware	Firmware type. The options include **APP**, **POE**, and **BIOS**.
UpdateResult	Upgrade result. **Success** indicates that the upgrade is successful. Other values indicate that the upgrade fails.

3.4.21 display remote-unit verbose realtime

Function

The **display remote-unit** command displays detailed real-time information about an RU.

Format

display remote-unit { **connect-interface** *interface-type interface-number* | **name** *remote-unit-name* } **verbose realtime**

Parameters

Parameter	Description	Value
connect-interface *interface-type interface-number*	Specifies the type and number of the interface connecting the central switch to an RU. The interface type and number can be closely next to each other or separated by a space character.	-
name *remote-unit-name*	Specifies the alias of an RU.	The value is a string of 1 to 32 case-sensitive characters without spaces.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run this command to view detailed real-time information about an RU, including the ESN, name, MAC address, device type, online duration, and firmware version.

Example

Display detailed real-time information about the RU connected to Eth-Trunk 10 on the central switch.

```
<HUAWEI> system-view
[HUAWEI] display remote-unit connect-interface Eth-Trunk 10 verbose realtime
------------------------------------------------------------------------------
ESN               :219801177002xxxxxxxx
Name               :-
ID                :10
Device mac         :xxxx-xxxx-xxxx
Device type        :S5731-L4T2S-RUA
Item              :98011768
Manufacture Date   :2021-12-17
Up time            :0 day, 4 hours, 12 minutes, 20 seconds
APP version        :220123020
POE version        :-
BIOS version       :220207016
Connect interface  :Eth-Trunk10
Disk usage         :44%
Memory usage       :40%
Temperature        :34(Celsius)
Mac usage          :0%
Status            :Normal
Authen Result      :-
------------------------------------------------------------------------------
```

Table 3-81 Description of the **display remote-unit verbose realtime** command output

Item	Description
ESN	ESN of an RU.
Name	Alias of an RU. This field displays a hyphen (-) if an RU is not configured with an alias.
ID	ID of an RU.
Device mac	System MAC address of an RU.
Device type	Device type of an RU.
Item	Code of an RU.
Manufacture Date	Manufacture date of an RU.
Up time	Online duration of an RU.
APP version	APP firmware version.
POE version	PoE firmware version.
BIOS version	BIOS firmware version.

Item	Description
Connect interface	Interface connecting the central switch to an RU. If the central switch uses a physical Eth-Trunk member interface to connect to an RU, this field displays the corresponding Eth-Trunk interface.
Disk usage	Disk usage of an RU.
Memory usage	Memory usage of an RU.
Temperature	Current temperature of an RU.
Mac usage	MAC address table usage of an RU.
Disk space(MB)	Disk size of an RU.
Status	Status of an RU: • **Normal**: online • **Upgrading** • **Configuring**: the RU is being configured. • **Abnormal**: The link connecting the RU and central switch is faulty, or the RU is an excess one because the number of connected RUs has reached the upper limit. • **Idle**: the RU is in the initialization state.
Authen Result	Authentication result of an RU: • **Success** • **Fail** • **-**: the RU is not authenticated.

3.4.22 display remote-unit vlan

Function

The **display remote-unit vlan** command displays VLAN information about interfaces on an RU.

Format

display remote-unit vlan [**connect-interface** *interface-type interface-number* | **name** *remote-unit-name*]

display remote-unit vlan { **connect-interface** *interface-type interface-number* | **name** *remote-unit-name* } **vlan** *vlan-id*

Parameters

Parameter	Description	Value
connect-interface *interface-type interface-number*	Specifies the type and number of an interface. The interface type and number can be closely next to each other or separated by a space character.	-
name *remote-unit-name*	Specifies the alias of an RU.	The value must be an existing RU alias.
vlan *vlan-id*	Specifies a VLAN ID.	The value is an integer in the range from 1 to 4094.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

An RU supports interface-based VLAN configuration. After the central switch delivers a VLAN to an interface on an RU, you can run this command to view VLAN information about the interface.

Example

Display VLAN information about interfaces on the RU connected to XG0/0/6 of the central switch.

```
<HUAWEI> display remote-unit vlan connect-interface XGigabitEthernet0/0/6
--------------------------------------------------------------------------
U:Up           D:Down           TG:Tagged           UT:Untagged
--------------------------------------------------------------------------
ESN              :219801176601XXXXXXXX
Name             :-
Device type      :S5731-L4P2HW-RUA
Remote unit ID   :16777215
Connect interface  :XGigabitEthernet0/0/6
--------------------------------------------------------------------------
VlanID           Ports
--------------------------------------------------------------------------
1              UT:GE1(D)    GE2(D)    GE3(D)    GE4(D)
                 GE5(D)    GE6(U)    GE7(D)    GE8(D)
                 GE9(D)    UPLINK(U)
2              UT:UPLINK(U)
3              TG:GE1(D)    GE2(D)    GE3(D)    GE4(D)
                 UPLINK(U)
--------------------------------------------------------------------------
```


Display information about interfaces in VLAN 3 on the RU connected to XG0/0/6 of the central switch.

```
<HUAWEI> display remote-unit vlan connect-interface XGigabitEthernet0/0/6 vlan 3
--------------------------------------------------------------------------------
U:Up           D:Down           TG:Tagged           UT:Untagged
--------------------------------------------------------------------------------
ESN               :219801176601XXXXXXXX
Name              :-
Device type       :S5731-L4P2HW-RUA
Remote unit ID    :16777215
Connect interface  :XGigabitEthernet0/0/6
--------------------------------------------------------------------------------
VlanID           Ports
--------------------------------------------------------------------------------
3                TG:GE1(D)    GE2(D)    GE3(D)    GE4(D)
                   UPLINK(U)
--------------------------------------------------------------------------------
```

Table 3-82 Description of the **display remote-unit vlan** command output

Item	Description
ESN	ESN of an RU.
Name	Alias of an RU. This field displays a hyphen (-) if an RU is not configured with an alias.
Device type	Device type of an RU.
Remote unit ID	ID of an RU. This field displays a hyphen (-) if an RU is not configured with an ID.
ConnectInterface	Interconnection interface.
VlanID	VLAN ID.
Ports	Interface of an RU. GE*n*: downlink interface on the RU. *n* indicates the interface number on the panel of the RU. UPLINK: uplink interface of the RU

3.4.23 display xldp statistics

Function

The **display xldp statistics** command displays statistics about XLDP packets sent and received by a switch.

Format

display xldp statistics [**interface** *interface-type interface-number*]

Parameters

Parameter	Description	Value
interface *interface-type interface-number*	Displays statistics about XLDP packets sent and received by a specified interface. • *interface-type* specifies the interface type. • *interface-number* specifies the interface number. If no interface is specified, the command displays statistics about XLDP packets on all interfaces.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

To display the XLDP packet statistics within a specified period of time, you need to run the **reset xldp statistics** command to clear the existing statistics first, and then run the **display xldp statistics** command to view new statistics.

Example

Display statistics about XLDP packets sent and received by all interfaces on the central switch.

```
<HUAWEI> display xldp statistics
Statistics for GigabitEthernet0/0/1:
Transmitted frames total      : 27664
  Hello frames              : 27664
  Channel frames              : 0
Received frames total         : 0
  Hello frames              : 0
  Channel ACK frames          : 0
```


Table 3-83 Description of the **display xldp statistics** command output

Item	Description
Statistics for *x*	Statistics about XLDP packets received and sent by interface *x*.
Transmitted frames total	Number of sent XLDP packets.
Received frames total	Number of received XLDP packets.
Hello frames	Number of heartbeat packets.
Channel frames	Number of channel packets.
Channel ACK frames	Number of channel ACK packets.

3.4.24 isolate (remote-unit view)

Function

The **isolate enable** command enables interface isolation on RUs globally.

The **undo isolate enable** command disable interface isolation on RUs globally.

By default, interface isolation is disabled on RUs.

Format

isolate enable

undo isolate enable

Parameters

None

Views

remote-unit view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After an RU is delivered, its downlink interfaces are in the same broadcast domain and are not isolated by default. This allows users connected to the same RU to communicate with each other before being authenticated. To prevent this, you can configure interface isolation on RUs. To isolate downlink interfaces on all RUs, run the **isolate enable** command in the remote-unit view.

Follow-up Procedure

After running this command, run the **commit** command to make the configuration take effect.

Example

Configure interface isolation on all RUs.

```
<HUAWEI> system-view
[HUAWEI] remote-unit
[HUAWEI-remote-unit] isolate enable
```

3.4.25 isolate (remote-unit N view)

Function

The **isolate enable** command enables port isolation on an RU.

The **isolate disable** command disables port isolation on an RU.

The **undo isolate** command restores the default configuration.

By default, port isolation is disabled on an RU.

Format

isolate {enable | disable }

undo isolate

Parameters

Parameter	Description	Value
enable	Enables port isolation.	-
disable	Disables port isolation.	-

Views

remote-unit N view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After an RU is delivered, its downlink interfaces are in the same broadcast domain and are not isolated by default. This allows users connected to the same RU to communicate with each other before being authenticated. To prevent this, you can

configure port isolation on RUs. To isolate downlink interface on a single RU, run the **isolate enable** command in the view of the RU.

Precautions

The port isolation configuration specific to an RU has a higher priority than the global port isolation configuration.

Follow-up Procedure

After running this command, run the **commit** command to make the configuration take effect.

Example

Disable port isolation on an RU.

```
<HUAWEI> system-view
[HUAWEI] remote-unit 0
[HUAWEI-remote-unit-0] isolate disable
```

3.4.26 led off (remote-unit view)

Function

The **led off** command turns off indicators on RUs.

The **undo led off** command restores the default status of indicators on RUs.

By default, indicators on RUs are turned on.

Format

led off [**time-range** *time-name*]

undo led off

Parameters

Parameter	Description	Value
time-range *time-name*	Specifies the name of a time range. If no time range is specified, the configuration is always valid.	The specified time range must exist.

Views

remote-unit view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When RUs are deployed in places such as hotels and dormitories, the blinking of indicators on the RUs may affect users' rest at night. You can run the **led off** command to turn off indicators on RUs to reduce the impact on users, for example, to turn off the indicators from 8:00 p.m. every day to 7:00 a.m. the next day.

Follow-up Procedure

After you run this command to turn on or off indicators on RUs, you need to run the **commit** command to deliver the configuration to make the configuration take effect.

Precautions

If this command is configured in both the remote-unit view and remote-unit N view, the configuration in the remote-unit N view takes effect.

Example

Turn off indicators on all RUs from 8:00 p.m. every day to 7:00 a.m. the next day.

```
<HUAWEI> system-view
[HUAWEI] time-range test 20:00 to 00:00 daily
[HUAWEI] time-range test 00:00 to 07:00 daily
[HUAWEI] remote-unit
[HUAWEI-remote-unit] led off time-range test
[HUAWEI-remote-unit] commit
```

3.4.27 led (remote-unit N view)

Function

The **led** command sets the time period during which indicators on an RU are turned on or off.

The **undo led off** command restore the default status of indicators on an RU.

By default, indicators on RUs are turned on.

Format

led { **on** | **off** [**time-range** *time-name*] }

undo led off

Parameters

Parameter	Description	Value
time-range *time-name*	Specifies the name of a time range. If no time range is specified, the configuration is always valid.	The specified time range must exist.

Parameter	Description	Value
on	Turns on RU indicators.	-
off	Turns off RU indicators.	-

Views

remote-unit view, remote-unit N view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When RUs are deployed in places such as hotels and dormitories, the blinking of indicators on the RUs may affect users' rest at night. You can run the **led** command to set the time period during which indicators on an RU are turned on or off to reduce the impact on users, for example, to turn off the indicators from 8:00 p.m. every day to 7:00 a.m. the next day.

Follow-up Procedure

After you run this command to configure the time period during which indicators on an RU are turned on or off, you need to run the **commit** command to deliver the configuration to make the configuration take effect.

Precautions

If this command is configured in both the remote-unit view and remote-unit N view, the configuration in the remote-unit N view takes effect.

Example

Turns off indicators on RU 0 from 8:00 p.m. every day to 7:00 a.m. the next day.

```
<HUAWEI> system-view
[HUAWEI] time-range test 20:00 to 00:00 daily
[HUAWEI] time-range test 00:00 to 07:00 daily
[HUAWEI] remote-unit 0
[HUAWEI-remote-unit-0] led off time-range test
[HUAWEI-remote-unit-0] commit
```

3.4.28 loopbacktest internal port

Function

The **loopbacktest internal port** configures an interface on an RU to perform an internal loopback test.

By default, internal loopback testing is not configured for an RU interface.

Format

loopbacktest internal port *port-id*

Parameters

Parameter	Description	Value
port-id	Specifies the index of an interface on an RU.	The value is an integer that ranges from 1 to 32. If the specified interface index is larger than the largest one on the RU, the command is not issued to the RU.

Views

remote-unit N view

Default Level

3: Management level

Usage Guidelines

You can run this command to check whether the internal forwarding chip of an RU works properly.

Example

Configure internal loopback testing for interface 2 on RU 0.

```
<HUAWEI> system-view
[HUAWEI] remote-unit 0
[HUAWEI-remote-unit-0] loopbacktest internal port 2
```

3.4.29 name

Function

The **name** command configures an alias for an RU.

The **undo name** command deletes the alias of an RU.

By default, no alias is configured for an RU.

Format

name *remote-unit-name*

undo name

Parameters

Parameter	Description	Value
remote-unit-name	Specifies the alias of an RU.	The value is a string of 1 to 32 case-sensitive characters without spaces.

Views

remote-unit N view

Default Level

2: Configuration level

Usage Guidelines

If a central switch is connected to multiple RUs, you can configure an alias for each RU to facilitate management, since aliases are easier to remember than IDs. In addition, after specifying an alias for an RU, you can run the **remote-unit name** *remote-unit-name* command to enter the view of an RU by its alias directly.

Example

Set the alias of RU 0 to **access_1**.

```
<HUAWEI> system-view
[HUAWEI] remote-unit 0
[HUAWEI-remote-unit-0] name access_1
```

3.4.30 negotiation auto port

Function

The **negotiation auto port** command configures an interface on an RU to work in auto-negotiation mode.

The **undo negotiation auto port** command configures an interface on an RU to work in non-auto-negotiation mode.

By default, an interface on an RU works in auto-negotiation mode.

Format

negotiation auto port { *portid1* [**to** *portid2*] } &<1-32>

undo negotiation auto port { *portid1* [**to** *portid2*] } &<1-32>

Parameters

Parameter	Description	Value
portid1 [**to** *portid2*]	Specifies the index of an interface on an RU.	The value is an integer that ranges from 1 to 32. If the specified interface index is larger than the largest one on the RU, the command is not issued to the RU.

Views

remote-unit N view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

In auto-negotiation mode, interfaces on both ends of a link negotiate their operating parameters, including the duplex mode and rate. If the negotiation succeeds, the two interfaces work at the same operating parameters and the transmission capability can reach the maximum value supported by both ends.

Follow-up Procedure

After running this command, run the **commit** command to make the configuration take effect.

Example

Configure interface 8 on RU 0 to work in auto-negotiation mode.

```
<HUAWEI> system-view
[HUAWEI] remote-unit 0
[HUAWEI-remote-unit-0] negotiation auto port 8
```

3.4.31 poe anti-interference frequency

Function

The **poe anti-interference frequency** command configures the PoE anti-interference frequency for an RU.

The **undo poe anti-interference frequency** command restores the default configuration.

By default, the PoE anti-interference frequency of an RU is 50 Hz.

NOTE

Only PoE-capable RUs support this command.

Format

poe anti-interference frequency { **50** | **60** }

undo poe anti-interference frequency

Parameters

Parameter	Description	Value
50	Sets the anti-interference frequency to 50 Hz.	-
60	Sets the anti-interference frequency to 60 Hz.	-

Views

remote-unit view, remote-unit N view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

The mains frequency varies in different countries and regions. Some are 60 Hz and some are 50 Hz. When RUs provide PoE power supply, incorrect grounding may occur. As a result, industrial frequency interference is coupled to network cables, resulting in abnormal PoE detection classification. You can run the **poe anti-interference frequency** command to modify the filtering algorithm on the PoE port to make the PoE anti-interference frequency become the same as the mains frequency, reducing the impact of the mains frequency on PD detection.

Follow-up Procedure

After configuring the PoE anti-interference frequency for an RU, you need to run the **commit** command to make the configuration take effect.

Precautions

If this command is configured in both the remote-unit view and remote-unit N view, the configuration in the remote-unit N view takes effect.

Example

Set the PoE anti-interference frequency of RU 0 to 60 Hz.

```
<HUAWEI> system-view
[HUAWEI] remote-unit 0
[HUAWEI-remote-unit-0] poe anti-interference frequency 60
```


3.4.32 poe enable port

Function

The **poe enable port** command sets the power supply mode for an interface on an RU.

The **undo poe enable port** command restores the default power supply mode of a PoE interface on an RU.

By default, interfaces supporting the PoE++ mode provide power in that mode (also referred to as the **bt-inrush** mode). Interfaces that do not support the PoE++ mode provide power in **at-inrush** mode.

Format

poe { *at-inrush* | *af-inrush* } **enable port** *port-id*

undo poe { *at-inrush* | *af-inrush* } **enable port** *port-id*

NOTE

The following RUs work in PoE++ mode by default:

S5731-L4P2HW-RUA, S5731S-L4P2HW-RUA, S5731-L4P2S-RUA, S5731S-L4P2S-RUA, S5731-L4P2ST-RUA, S5731S-L4P2ST-RUA, S5731-L4P2HT-RUA, S5731S-L4P2HT-RUA

The following RUs work in PoE+ mode by default:

S5731-L8P2ST-RUA, S5731S-L8P2ST-RUA, S5731-L8P2HT-RUA, S5731S-L8P2HT-RUA, S5731-L8LP2ST-RUA

Parameters

Parameter	Description	Value
poe *at-inrush*	Sets an RU interface to work in PoE+ power supply mode.	-
poe *af-inrush*	Sets an RU interface to work in 802.3af power supply mode.	-
port-id	Specifies the index of an interface on an RU.	The value is an integer that ranges from 1 to 32. If the specified interface index is larger than the largest one on the RU, the command is not issued to the RU.

Views

remote-unit N view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

To power the PDs requiring the standard power supply mode, you can run the **poe at-inrush enable** command. This command configures PoE interfaces to work in PoE+ power supply mode. Some non-IEEE standard PDs do not support high-current power supply, and instead only support low-current power supply. To power on such non-standard PDs, you can run the **poe af-inrush enable** command to configure PoE interfaces on RUs to work in 802.3af power supply mode.

Follow-up procedure

After running this command, run the **commit** command to make the configuration take effect.

Precautions

Switching the PoE power supply mode of an RU interface between the at-inrush and bt-inrush modes will cause PDs to be powered off.

Example

Set interface 1 on RU 0 to work in PoE+ power supply mode.

```
<HUAWEI> system-view
[HUAWEI] remote-unit 0
[HUAWEI-remote-unit-0] poe at-inrush enable port 1
```

3.4.33 poe force-power port

Function

The **poe force-power port** command enables forcible PoE power supply for an interface on an RU.

The **undo poe force-power port** command disables forcible PoE power supply for an interface on an RU.

By default, forcible PoE power supply is disabled on interfaces of RUs.

Format

poe force-power port *port-id*

undo poe force-power port *port-id*

Parameters

Parameter	Description	Value
port-id	Specifies the index of an interface on an RU.	The value is an integer that ranges from 1 to 32. If the specified interface index is larger than the largest one on the RU, the command is not issued to the RU.

Views

remote-unit N view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

If the system power is sufficient, you can run this command to enable forcible power supply on RU interfaces connected to non-standard PDs when the RU, as the PSE, cannot detect the PDs.

Precautions

This command forcibly increases the power supplied by the RU. Ensure that the total power of PDs connected to the RU does not exceed the RU's available power.

Follow-up procedure

After running this command, run the **commit** command to make the configuration take effect.

Example

Enable forcible power supply on interface 1 of RU 0.

```
<HUAWEI> system-view
[HUAWEI] remote-unit 0
[HUAWEI-remote-unit-0] poe force-power port 1
```

3.4.34 poe power-on delay port

Function

The **poe power-on delay port** command sets the power supply delay for an interface on an RU.

The **undo poe power-on delay port** command restores the default power supply delay for an interface on an RU.

By default, the power supply delay for an interface on an RU is 0, which indicates no delay.

Format

poe power-on delay *delay-time* **port** *port-id*

undo poe power-on delay port *port-id*

Parameters

Parameter	Description	Value
delay-time	Specifies the power supply delay for an interface on an RU.	The value is an integer in the range from 1 to 60, in seconds. The default value is 0, indicating no delay.
port-id	Specifies the index of a downlink interface on an RU.	The value is an integer that ranges from 1 to 32. If some of the specified interface indexes are greater than the largest one on the RU, commands concerning these interfaces are not issued to the RU.

Views

remote-unit N view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

As the holding current of a non-standard PD is insufficient at the power-on moment, an RU assumes that the PD has been disconnected and powers it off.

To solve this problem, you can set the power supply delay for RU interfaces on the central switch. When the delay expires, the RUs detect the holding current to ensure that non-standard PDs can be properly powered on.

Follow-up procedure

After running this command, run the **commit** command to make the configuration take effect.

Precautions

If a PD is connected to an interface configured with a power supply delay, do not replace the PD within the delay. Otherwise, the new PD cannot work properly.

Example

Set the power supply delay to 5 seconds for interface 1 on RU 0.


```
<HUAWEI> system-view
[HUAWEI] remote-unit 0
[HUAWEI-remote-unit-0] poe power-on delay 5 port 1
```

3.4.35 poe xldp-proxy

Function

The **poe xldp-proxy** command binds an optical interface to a MultiGE electrical interface on the central switch.

The **undo poe xldp-proxy** command restores the default configuration.

By default, no optical interface is bound to a MultiGE electrical interface.

Format

poe xldp-proxy interface multige *interface-number*

undo poe xldp-proxy

NOTE

Only the S5732-H48XUM2CC supports this command.

Parameters

Parameter	Description	Value
interface multige *interface-number*	Specifies the number of a MultiGE electrical interface.	-

Views

XGE interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When an S5732-H48XUM2CC functions as a central switch and connects to RUs using first-generation hybrid copper-fiber cables (that is, electrical interfaces are used for power supply and optical interfaces are used for communication), the central switch needs to provide PoE power for RUs through its electrical interfaces. To implement this, run the **poe xldp-proxy** command to bind an optical interface to an electrical interface, so that the optical interface can function as a proxy for the electrical interface to provide PoE power for its connected RU.

If this command is not configured, the central switch provides 60 W power for RUs by default.

Precautions

XLDP has been enabled on a 10GE optical interface. By default, XLDP is enabled.

Example

Bind XGE0/0/1 optical interface to MultiGE0/0/1 electrical interface.

```
<HUAWEI> system-view
[HUAWEI] interface XGigabitEthernet 0/0/1
[HUAWEI-XGigabitEthernet0/0/1] poe xldp-proxy interface MultiGE 0/0/1
```

3.4.36 port default vlan (remote-unit N view)

Function

The **port default vlan** command configures the default VLAN for downlink interfaces on an RU.

The **undo port default vlan** command restores the default setting.

By default, a downlink interface on an RU uses VLAN 1 as its default VLAN.

Format

port { *portid1* [**to** *portid2*] } &<1-32> **default vlan** *vlanid*

undo port { *portid1* [**to** *portid2*] } &<1-32> **default vlan**

Parameters

Parameter	Description	Value
portid1 [**to** *portid2*]	Indicates numbers of downlink interfaces: *portid1* specifies the number of the first interface. **to** *portid2* specifies the number of the last interface. *portid2* must be greater than or equal to *portid1*.	*portid1* is an integer that ranges from 1 to 32. *portid2* is an integer that ranges from 1 to 32.
vlanid	Specifies the default VLAN ID for the downlink interfaces on the RU.	The value is an integer in the range from 1 to 4094.

Views

remote-unit N view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

An RU can connect to different types of terminals using its downlink interfaces and distinguish terminal services by joining its downlink interfaces to different VLANs. You can run the **port default vlan** command to configure a downlink interface on an RU as a hybrid interface and configure the default VLAN for the interface. As such, different VLANs can be configured for downlink interfaces of an RU to carry services of different terminals.

An RU saves the VLAN configuration delivered by the central switch to it in its flash memory and forwards traffic based on this VLAN configuration after being powered on. After the RU goes online on the central switch, the central switch synchronizes the latest VLAN configuration to the RU's flash memory.

Prerequisites

You have run the **vlan mode manual** command to configure the manual VLAN mode for the RU.

Follow-up Procedure

After you run the commands for configuring the VLAN mode for an RU and VLANs for RU interfaces, run the **commit** command to deliver the VLAN configuration to the RU or bring the RU offline and then online again for the configuration to take effect.

Run the **port uplink** { **tagged** | **untagged** } **vlan** *vlan-id1* command to configure the default VLAN of the downlink interfaces on an RU as an allowed VLAN for the RU's uplink interface.

Example

Configure VLAN 2 as the default VLAN for downlink interfaces 1 to 4 on RU 0.

```
<HUAWEI> system-view
[HUAWEI] remote-unit 0
[HUAWEI-remote-unit-0] port 1 to 4 default vlan 2
```

3.4.37 port uplink default vlan

Function

The **port uplink default vlan** command configures the default VLAN for the uplink interface on an RU.

The **undo port uplink default vlan** command restores the default setting.

By default, the uplink interface on an RU uses VLAN 1 as its default VLAN.

Format

port uplink default vlan *vlan-id*

undo port uplink default vlan

Parameters

Parameter	Description	Value
vlan-id	Specifies the default VLAN ID for the uplink interface on an RU.	The value is an integer in the range from 1 to 4094.

Views

remote-unit N view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If terminals connected to an RU run the same service, they can reside in the same service VLAN. In this situation, you can run the **port uplink default vlan** command to configure the service VLAN as the default VLAN for the uplink interface on the RU.

An RU saves the VLAN configuration delivered by the central switch to it in its flash memory and forwards traffic based on this VLAN configuration after being powered on. After the RU goes online on the central switch, the central switch synchronizes the latest VLAN configuration to the RU's flash memory.

Prerequisites

You have run the **vlan mode manual** command to configure the manual VLAN mode for the RU.

Follow-up Procedure

After you run the commands for configuring the VLAN mode for an RU and VLANs for RU interfaces, run the **commit** command to deliver the VLAN configuration to the RU or bring the RU offline and then online again for the configuration to take effect.

Run the **port uplink untagged vlan** command to configure the default VLAN as an allowed VLAN in untagged mode for the uplink interface.

Example

Set VLAN 10 as the default VLAN for the uplink interface on RU 0.

```
<HUAWEI> system-view
[HUAWEI] remote-unit 0
[HUAWEI-remote-unit-0] port uplink default vlan 10
```


3.4.38 port uplink vlan

Function

The **port uplink vlan** command configures allowed VLANs for the uplink interface on an RU.

The **undo port uplink vlan** command deletes the allowed VLAN configuration of the uplink interface on an RU.

By default, the uplink interface of an RU allows packets from VLAN 1 to pass through.

Format

port uplink { **tagged** | **untagged** } **vlan** { *vlan-id1* [**to** *vlan-id2*] } &<1-10>

undo port uplink { **tagged** | **untagged** } { **vlan** { *vlan-id1* [**to** *vlan-id2*] } &<1-10> | **all** }

Parameters

Parameter	Description	Value
vlan-id1 [**to** *vlan-id2*]	Specifies allowed VLANs: • *vlan-id1* specifies the first VLAN ID. • **to** *vlan-id2* specifies the last VLAN ID. *vlan-id2* must be greater than or equal to *vlan-id1*.	*vlan-id1* is an integer that ranges from 1 to 4094. *vlan-id2* is an integer that ranges from 1 to 4094.
tagged	Configures the uplink interface to forward packets of the specified VLAN in tagged mode.	-
untagged	Configures the uplink interface to forward packets of the specified VLAN in untagged mode.	-
all	Deletes all allowed VLANs from the uplink interface on the RU.	-

Views

remote-unit N view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If a downlink interface of an RU is configured with a default VLAN, the uplink interface must allow packets of this VLAN to pass through, so that service traffic can be forwarded normally.

An RU saves the VLAN configuration delivered by the central switch to it in its flash memory and forwards traffic based on this VLAN configuration after being powered on. After the RU goes online on the central switch, the central switch synchronizes the latest VLAN configuration to the RU's flash memory.

Prerequisites

You have run the **vlan mode manual** command to configure the manual VLAN mode for the RU.

Follow-up Procedure

After you run the commands for configuring the VLAN mode for an RU and VLANs for RU interfaces, run the **commit** command to deliver the VLAN configuration to the RU or bring the RU offline and then online again for the configuration to take effect.

Example

Configure the uplink interface on RU 0 to forward packets of VLAN 10 and VLAN 20 in tagged mode.

```
<HUAWEI> system-view
[HUAWEI] remote-unit 0
[HUAWEI-remote-unit-0] port uplink tagged vlan  10 20
```

3.4.39 port vlan

Function

The **port vlan** command configures allowed VLANs for downlink interfaces on an RU.

The **undo port vlan** command deletes the allowed VLAN configuration of downlink interfaces on an RU.

By default, a downlink interface of an RU allows packets from VLAN 1 to pass through.

Format

port { *portid1* [**to** *portid2*] } &<1-32> { **tagged** | **untagged** } **vlan** { *vlan-id1* [**to** *vlan-id2*] } &<1-10>

undo port { *portid1* [**to** *portid2*] } &<1-32> { **tagged** | **untagged** } { **vlan** { *vlan-id1* [**to** *vlan-id2*] } &<1-10> | **all** }

Parameters

Parameter	Description	Value
portid1 [**to** *portid2*]	Indicates numbers of downlink interfaces: *portid1* specifies the number of the first interface. **to** *portid2* specifies the number of the last interface. *portid2* must be greater than or equal to *portid1*.	*portid1* is an integer that ranges from 1 to 32. *portid2* is an integer that ranges from 1 to 32.
vlan-id1 [**to** *vlan-id2*]	Specifies allowed VLANs: • *vlan-id1* specifies the first VLAN ID. • **to** *vlan-id2* specifies the last VLAN ID. *vlan-id2* must be greater than or equal to *vlan-id1*.	*vlan-id1* is an integer that ranges from 1 to 4094. *vlan-id2* is an integer that ranges from 1 to 4094.
tagged	Configures the downlink interfaces to forward packets of the specified VLANs in tagged mode.	-
untagged	Configures the downlink interfaces to forward packets of the specified VLANs in untagged mode.	-
all	Deletes all allowed VLANs from the downlink interfaces on the RU.	-

Views

remote-unit N view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

An RU can connect to different types of terminals using its downlink interfaces and distinguish terminal services by joining its downlink interfaces to different VLANs. You can run the **port vlan** command to configure allowed VLANs for downlink interfaces on an RU, so that different service VLANs can be assigned to different terminals.

An RU saves the VLAN configuration delivered by the central switch to it in its flash memory and forwards traffic based on this VLAN configuration after being

powered on. After the RU goes online on the central switch, the central switch synchronizes the latest VLAN configuration to the RU's flash memory.

Prerequisites

You have run the **vlan mode manual** command to configure the manual VLAN mode for the RU.

Follow-up Procedure

After you run the commands for configuring the VLAN mode for an RU and VLANs for RU interfaces, run the **commit** command to deliver the VLAN configuration to the RU or bring the RU offline and then online again for the configuration to take effect.

Example

Configure downlink interfaces 1 to 4 on RU 0 to forward packets of VLAN 2 in tagged mode.

```
<HUAWEI> system-view
[HUAWEI] remote-unit 0
[HUAWEI-remote-unit-0] port 1 to 4 tagged vlan 2
```

3.4.40 reboot

Function

The **reboot** command resets an RU.

By default, an RU is not reset.

Format

reboot [**all**]

Parameters

Parameter	Description	Value
all	Resets all RUs.	This parameter is supported only in the remote-unit view.

Views

remote-unit view, remote-unit N view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

- You can run this command to reset a faulty RU.
- If an RU fails to be upgraded and enters the cooldown period, you can run the **reboot** command to end the cooldown period.

Precautions

- An RU that has no interconnection interface bound cannot be reset.
- An RU that fails to be authenticated or is not authenticated cannot be reset.
- An RU that encounters a communication error will fail to be reset.
- RUs do not save their configurations. After an RU starts, it goes online on the central switch. After the RU is authenticated successfully, the central switch delivers configurations to the RU for them to take effect. For example, port isolation is required on an RU. After you restart the RU, its downlink interfaces can communicate with each other. The interfaces are isolated after the central switch authenticates the RU successfully and delivers the port isolation configuration.

Example

Reset a single RU.

```
<HUAWEI> system-view
[HUAWEI] remote-unit 0
[HUAWEI-remote-unit-0] reboot
```

Reset all RUs.

```
<HUAWEI> system-view
[HUAWEI] remote-unit
[HUAWEI-remote-unit] reboot all
```

3.4.41 remote-unit

Function

The **remote-unit** command displays the remote-unit view.

Format

remote-unit

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

You can run this command to enter the global RU view to perform global configurations for RUs.

Example

Enter the remote-unit view.

```
<HUAWEI> system-view
[HUAWEI] remote-unit
```

3.4.42 remote-unit N

Function

The **remote-unit** command displays the view of an RU.

The **undo remote-unit** command deletes all configurations of an RU from the central switch.

Format

remote-unit { *id* | **connect-interface** *interface-type interface-number* | **name** *remote-unit-name* }

undo remote-unit *id*

Parameters

Parameter	Description	Value
id	ID of an RU, which is the RU index. The value range does not indicate the number of RUs that can be configured.	The value is an integer ranging from 0 to 16777215.
connect-interface *interface-type interface-number*	Specifies the type and number of an interface. The interface type and number can be closely next to each other or separated by a space character.	-
name *remote-unit-name*	Specifies the alias of an RU.	The value must be an existing RU alias.

Views

System view, remote-unit view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can configure or operate a single RU by running this command to enter the view of the specific RU.

Prerequisites

To enter the view of a specific RU by specifying the **name** parameter, ensure that you have configured an alias for this RU by running the **name** command. To enter the view of a specific RU by specifying the interconnection interface, ensure that you have bound an interconnection interface to this RU by running the **bind interface** command.

Example

Enter the view of an RU by specifying the ID of the RU.

```
<HUAWEI> system-view
[HUAWEI] remote-unit 0
```

Enter the view of an RU by specifying the interconnection interface.

```
<HUAWEI> system-view
[HUAWEI] remote-unit connect-interface XGigabitEthernet 0/0/1
```

Enter the view of an RU by specifying the RU alias.

```
<HUAWEI> system-view
[HUAWEI] remote-unit name test
```

3.4.43 remote-unit protect-action error-down

Function

The **remote-unit protect-action error-down enable** command enables RU protection by setting interfaces to the Error-Down state.

The **remote-unit protect-action error-down disable** command disables RU protection.

By default, this function is enabled.

Format

remote-unit protect-action error-down { **disable** | **enable** }

undo remote-unit protect-action error-down disable

Parameters

Parameter	Description	Value
disable	Disables RU protection.	-

Parameter	Description	Value
enable	Enables RU protection by setting interfaces to the Error-Down state.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

During RU deployment, a configuration error or link fault may occur (for details, see "Usage Guidelines" in **error-down auto-recovery cause remote-unit-link interval**). When the central switch detects the fault, it sets the interface connected to the RU to the Error-Down state.

Prerequisites

XLDP has been enabled on all interfaces of the central switch.

Precautions

The **undo remote-unit protect-action error-down disable** command is equivalent to the **remote-unit protect-action error-down enable** command.

Example

Enable RU protection by setting interfaces to the Error-Down state.

```
<HUAWEI> system-view
[HUAWEI] undo remote-unit protect-action error-down disable
```

3.4.44 remote-unit port default vlan

Function

The **remote-unit port default vlan** command configures the default VLAN for downlink interfaces on RUs in batches.

The **undo remote-unit port default vlan** command restores the default setting.

By default, a downlink interface on an RU uses VLAN 1 as its default VLAN.

Format

remote-unit { *ruid1* [**to** *ruid2*] } &<1-8> **port** { *portid1* [**to** *portid2*] } &<1-32> **default vlan** *vlanid*

undo remote-unit { *ruid1* [**to** *ruid2*] } &<1-8> **port** { *portid1* [**to** *portid2*] } &<1-32> **default vlan**

Parameters

Parameter	Description	Value
ruid1 [**to** *ruid2*]	Specifies IDs of RUs: *ruid1* specifies the ID of the first RU. **to** *ruid2* indicates the ID of the last RU. *ruid2* must be greater than or equal to *ruid1*.	*ruid1* is an integer that ranges from 0 to 16777215. *ruid2* is an integer that ranges from 0 to 16777215.
portid1 [**to** *portid2*]	Indicates numbers of downlink interfaces: *portid1* specifies the number of the first interface. **to** *portid2* specifies the number of the last interface. *portid2* must be greater than or equal to *portid1*.	*portid1* is an integer that ranges from 1 to 32. *portid2* is an integer that ranges from 1 to 32.
vlanid	Specifies the default VLAN ID for the downlink interfaces on the RUs.	The value is an integer in the range from 1 to 4094.

Views

remote-unit view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

An RU can connect to different types of terminals using its downlink interfaces and distinguish terminal services by joining its downlink interfaces to different VLANs. You can run the **remote-unit port default vlan** command to configure downlink interfaces on RUs as hybrid interfaces in batches and configure default VLANs for the interfaces, so that different VLANs can be configured to carry services of different terminals.

An RU saves the VLAN configuration delivered by the central switch to it in its flash memory and forwards traffic based on this VLAN configuration after being powered on. After the RU goes online on the central switch, the central switch synchronizes the latest VLAN configuration to the RU's flash memory.

Prerequisites

You have run the **vlan mode manual** command to configure the manual VLAN mode for the RU.

Follow-up Procedure

After you run the commands for configuring the VLAN mode for an RU and VLANs for RU interfaces, run the **commit** command to deliver the VLAN configuration to the RU or bring the RU offline and then online again for the configuration to take effect.

Run the **port uplink tagged vlan** command to configure the default VLAN of the downlink interfaces on the RUs as an allowed VLAN in tagged mode for the uplink interfaces on the RUs.

Example

Configure VLAN 2 as the default VLAN for downlink interfaces 1 to 4 on RUs 0 to 4.

```
<HUAWEI> system-view
[HUAWEI] remote-unit
[HUAWEI-remote-unit] remote-unit 0 to 4 port 1 to 4 default vlan 2
```

3.4.45 remote-unit port uplink default vlan

Function

The **remote-unit port uplink default vlan** command configures the default VLAN for uplink interfaces on RUs in batches.

The **undo remote-unit port uplink default vlan** command restores the default setting.

By default, an uplink interface on an RU uses VLAN 1 as its default VLAN.

Format

remote-unit { *ruid1* [**to** *ruid2*] } &<1-8> **port uplink default vlan** *vlanid*

undo remote-unit { *ruid1* [**to** *ruid2*] } &<1-8> **port uplink default vlan**

Parameters

Parameter	Description	Value
ruid1 [**to** *ruid2*]	Specifies IDs of RUs: *ruid1* indicates the ID of the first RU. **to** *ruid2* indicates the ID of the last RU. *ruid2* must be greater than or equal to *ruid1*.	*ruid1* is an integer that ranges from 0 to 16777215. *ruid2* is an integer that ranges from 0 to 16777215.
vlanid	Specifies the default VLAN for uplink interfaces on the RUs.	The value is an integer in the range from 1 to 4094.

Views

remote-unit view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If terminals connected to multiple RUs carry the same service and use the same service VLAN, you can run the **remote-unit port uplink default vlan** command to configure the service VLAN as the default VLAN for the uplink interfaces on the RUs in batches.

An RU saves the VLAN configuration delivered by the central switch to it in its flash memory and forwards traffic based on this VLAN configuration after being powered on. After the RU goes online on the central switch, the central switch synchronizes the latest VLAN configuration to the RU's flash memory.

Prerequisites

You have run the **vlan mode manual** command to configure the manual VLAN mode for the RU.

Follow-up procedure

After you run the commands for configuring the VLAN mode for an RU and VLANs for RU interfaces, run the **commit** command to deliver the VLAN configuration to the RU or bring the RU offline and then online again for the configuration to take effect.

Example

Set VLAN 10 as the default VLAN for the uplink interfaces on RUs 0 to 4.

```
<HUAWEI> system-view
[HUAWEI] remote-unit
[HUAWEI-remote-unit] remote-unit 0 to 4 port uplink default vlan 10
```

3.4.46 remote-unit port uplink vlan

Function

The **remote-unit port uplink vlan** command configures allowed VLANs for uplink interfaces on RUs in batches.

The **undo remote-unit port uplink vlan** command deletes the allowed VLAN configuration from uplink interfaces on RUs in batches.

By default, the uplink interface of an RU allows packets from VLAN 1 to pass through.

Format

remote-unit { *ruid1* [**to** *ruid2*] } &<1-8> **port uplink** { **tagged** | **untagged** } **vlan** { *vlan-id1* [**to** *vlan-id2*] } &<1-10>

undo remote-unit { *ruid1* [**to** *ruid2*] } &<1-8>] **port uplink** { **tagged** | **untagged** } { **vlan** { *vlan-id1* [**to** *vlan-id2*] } &<1-10> | **all** }

Parameters

Parameter	Description	Value
ruid1 [**to** *ruid2*]	Specifies IDs of RUs: *ruid1* indicates the ID of the first RU. **to** *ruid2* indicates the ID of the last RU. *ruid2* must be greater than or equal to *ruid1*.	*ruid1* is an integer that ranges from 0 to 16777215. *ruid2* is an integer that ranges from 0 to 16777215.
vlan-id1 [**to** *vlan-id2*]	Specifies allowed VLANs: *vlan-id1* specifies the first VLAN ID. **to** *vlan-id2* specifies the last VLAN ID. *vlan-id2* must be greater than or equal to *vlan-id1*.	*vlan-id1* is an integer that ranges from 1 to 4094. *vlan-id2* is an integer that ranges from 1 to 4094.
tagged	Configures the uplink interfaces to forward packets of the specified VLANs in tagged mode.	-
untagged	Configures the uplink interfaces to forward packets of the specified VLANs in untagged mode.	-
all	Deletes all allowed VLANs from the uplink interfaces on the specified RUs.	-

Views

remote-unit view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

An RU can connect to different types of terminals using its downlink interfaces and distinguish terminal services by joining its downlink interfaces to different VLANs. You can run the **remote-unit port uplink vlan** command to configure allowed VLANs for uplink interfaces on RUs in batches so that different service VLANs can be assigned to different terminals.

An RU saves the VLAN configuration delivered by the central switch to it in its flash memory and forwards traffic based on this VLAN configuration after being

powered on. After the RU goes online on the central switch, the central switch synchronizes the latest VLAN configuration to the RU's flash memory.

Prerequisites

You have run the **vlan mode manual** command to configure the manual VLAN mode for the RU.

Follow-up procedure

After you run the commands for configuring the VLAN mode for an RU and VLANs for RU interfaces, run the **commit** command to deliver the VLAN configuration to the RU or bring the RU offline and then online again for the configuration to take effect.

Example

Configure uplink interfaces on RUs 0 to 4 to forward packets of VLAN 2 in tagged mode.

```
<HUAWEI> system-view
[HUAWEI] remote-unit
[HUAWEI] remote-unit 0 to 4 port uplink tagged vlan 2
```

3.4.47 remote-unit port vlan

Function

The **remote-unit port vlan** command configures allowed VLANs for downlink interfaces on RUs in batches.

The **undo remote-unit port vlan** command deletes the allowed VLAN configuration from downlink interfaces on RUs.

By default, a downlink interface of an RU allows packets from VLAN 1 to pass through.

Format

remote-unit { *ruid1* [**to** *ruid2*] } &<1-8> **port** { *portid1* [**to** *portid2*] } &<1-32> { **tagged** | **untagged** } **vlan** { *vlan-id1* [**to** *vlan-id2*] } &<1-10>

undo remote-unit { *ruid1* [**to** *ruid2*] } &<1-8> **port** { *portid1* [**to** *portid2*] } &<1-32> { **tagged** | **untagged** } { **vlan** { *vlan-id1* [**to** *vlan-id2*] } &<1-10> | **all** }

Parameters

Parameter	Description	Value
ruid1 [**to** *ruid2*]	Specifies IDs of RUs: *ruid1* indicates the ID of the first RU. **to** *ruid2* indicates the ID of the last RU. *ruid2* must be greater than or equal to *ruid1*.	*ruid1* is an integer that ranges from 0 to 16777215. *ruid2* is an integer that ranges from 0 to 16777215.
portid1 [**to** *portid2*]	Indicates numbers of downlink interfaces: *portid1* specifies the number of the first interface. **to** *portid2* specifies the number of the last interface. *portid2* must be greater than or equal to *portid1*.	*portid1* is an integer that ranges from 1 to 32. *portid2* is an integer that ranges from 1 to 32.
vlan-id1 [**to** *vlan-id2*]	Specifies allowed VLANs: • *vlan-id1* specifies the first VLAN ID. • **to** *vlan-id2* specifies the last VLAN ID. *vlan-id2* must be greater than or equal to *vlan-id1*.	*vlan-id1* is an integer that ranges from 1 to 4094. *vlan-id2* is an integer that ranges from 1 to 4094.
tagged	Configures the downlink interfaces to forward packets of the specified VLANs in tagged mode.	-
untagged	Configures the downlink interfaces to forward packets of the specified VLANs in untagged mode.	-
all	Deletes all allowed VLANs from downlink interfaces on the specified RUs.	-

Views

remote-unit view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

An RU can connect to different types of terminals using its downlink interfaces and distinguish terminal services by joining its downlink interfaces to different VLANs. You can run the **remote-unit port vlan** command to configure allowed VLANs for downlink interfaces on RUs in batches so that different service VLANs can be assigned to different terminals.

An RU saves the VLAN configuration delivered by the central switch to it in its flash memory and forwards traffic based on this VLAN configuration after being powered on. After the RU goes online on the central switch, the central switch synchronizes the latest VLAN configuration to the RU's flash memory.

Prerequisites

You have run the **vlan mode manual** command to configure the manual VLAN mode for the RU.

Follow-up Procedure

After you run the commands for configuring the VLAN mode for an RU and VLANs for RU interfaces, run the **commit** command to deliver the VLAN configuration to the RU or bring the RU offline and then online again for the configuration to take effect.

Example

Configure downlink interfaces 1 to 4 on RUs 0 to 4 to forward packets of VLAN 2 in tagged mode.

```
<HUAWEI> system-view
[HUAWEI] remote-unit
[HUAWEI-remote-unit] remote-unit 0 to 4 port 1 to 4 tagged vlan 2
```

3.4.48 reset xldp statistics

Function

The **reset xldp statistics** command clears XLDP packet statistics on all interfaces or on a specified interface.

Format

reset xldp statistics [**interface** *interface-type interface-number*]

Parameters

Parameter	Description	Value
interface *interface-type interface-number*	Specifies the type and number of the interface where statistics need to be cleared. In the command: • *interface-type* specifies the interface type. • *interface-number* specifies the interface number. If no interface is specified, XLDP packet statistics on all interfaces are cleared.	-

Views

User view

Default Level

2: Configuration level

Usage Guidelines

To troubleshoot XLDP faults, you may need to view XLDP packet statistics within a certain period of time. In this case, you need to run this command to clear existing XLDP packet statistics, and run the **display xldp statistics** command to view new XLDP packet statistics.

Example

Clear XLDP packet statistics on all interfaces.

```
<HUAWEI> reset xldp statistics
```

Clear statistics about XLDP packets sent and received by GigabitEthernet0/0/1.

```
<HUAWEI> reset xldp statistics interface gigabitethernet 0/0/1
```

3.4.49 reset remote-unit commit result

Function

The **reset remote-unit commit result** command clears configuration delivery records of RUs.

Format

reset remote-unit commit result

Parameters

None

Views

User view

Default Level

3: Management level

Usage Guidelines

RUs do not support web-based management and cannot have commands run on them for configuration. All RU configurations are delivered by the central switch. You can run the **display remote-unit commit result** command on the central switch to view configuration delivery results. To clear configuration delivery records, you can run the **reset remote-unit commit result** command.

After this command is run, configuration delivery records of RUs are cleared and cannot be restored.

Example

Clear configuration delivery records of RUs.

```
<HUAWEI> reset remote-unit commit result
```

3.4.50 reset remote-unit connect record

Function

The **reset remote-unit connect record** command clears onboarding and disconnection records of RUs.

Format

reset remote-unit connect record

Parameters

None

Views

User view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

Before collecting onboarding and disconnection records of RUs, you can run this command to clear the existing records, and run the **display remote-unit connect record** command after a period of time to view new records.

Precautions

After this command is run, onboarding and disconnection records of RUs are cleared.

Example

Clear onboarding and disconnection records of RUs.

```
<HUAWEI> reset remote-unit connect record
```

3.4.51 reset remote-unit port statistics

Function

The **reset remote-unit port statistics** command clears the statistics on interfaces of an RU.

Format

reset remote-unit port [*port-id*] **statistics** [**connect-interface** *interface-type interface-number* | **name** *remote-unit-name*]

Parameters

Parameter	Description	Value
[*port-id*]	Specifies the index of an interface on an RU.	The value is an integer that ranges from 1 to 34.
connect-interface *interface-type interface-number*	Specifies the type and number of an interface. The interface type and number can be closely next to each other or separated by a space character.	-
name *remote-unit-name*	Specifies the alias of an RU.	The value must be an existing RU alias.

Views

User view

Default Level

3: Management level

Usage Guidelines

Before collecting traffic statistics on an RU interface within a period of time, run this command to clear the existing traffic statistics.

Example

Clear the statistics on all interfaces of an RU.

```
<HUAWEI> reset remote-unit port statistics
```

3.4.52 reset remote-unit upgrade record

Function

The **reset remote-unit upgrade record** command clears upgrade records of RUs.

Format

reset remote-unit upgrade record

Parameters

None

Views

User view

Default Level

3: Management level

Usage Guidelines

You can run this command to clear upgrade records of RUs.

Example

Clear upgrade records of RUs.

```
<HUAWEI> reset remote-unit upgrade record
```


3.4.53 restart port

Function

The **restart port** command restarts an interface on an RU.

By default, no interface on an RU will be restarted.

Format

restart port *port-id*

Parameters

Parameter	Description	Value
port-id	Specifies the index of an interface on an RU.	The value is an integer that ranges from 1 to 34. If the specified number is greater than the largest interface number on the RU, the RU will not execute this command.

Views

remote-unit N view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If an interface on an RU is faulty, you can run this command to restart the interface.

Precautions

- If an interface is disabled (in the shutdown state) before the restart, the interface is enabled automatically (in the undo shutdown state) after the restart.
- An RU that has no interconnection interface bound cannot be restarted.

Example

Restart interface 1 on the RU.

```
<HUAWEI> system-view
[HUAWEI] remote-unit 0
[HUAWEI-remote-unit-0] restart port 1
```


3.4.54 shutdown port

Function

The **shutdown port** command shuts down an interface on an RU.

The **undo shutdown port** command enables an interface on an RU.

By default, interfaces on an RU are enabled.

Format

shutdown port { *port-id*1 [**to** *port-id*2] } &<1-32>

undo shutdown port { *port-id*1 [**to** *port-id*2] } &<1-32>

Parameters

Parameter	Description	Value
port-id1 [**to** *port-id2*]	Specifies the index of an interface on an RU.	The value is an integer that ranges from 1 to 32. If the specified interface index is larger than the largest one on the RU, the command is not issued to the RU.

Views

remote-unit N view

Default Level

3: Management level

Usage Guidelines

When an interface on an RU is not connected to a cable or fiber, you can run the **shutdown** command to shut down the interface to prevent exceptions caused by interference.

Follow-up procedure

After running this command, run the **commit** command to make the configuration take effect.

Example

Shut down interface 8 on RU 0.

```
<HUAWEI> system-view
[HUAWEI] remote-unit 0
[HUAWEI-remote-unit-0] shutdown port 8
```


3.4.55 speed port

Function

The **speed port** command sets a fixed rate for an interface on an RU.

The **undo speed port** command restores the default rate of an interface on an RU.

By default, an interface on an RU works at the rate of 1000 Mbit/s.

Format

speed { **10** | **100** | **1000** } **port** { *portid1* [**to** *portid2*] } &<1-32>

undo speed { **10** | **100** | **1000** } **port** { *portid1* [**to** *portid2*] } &<1-32>

Parameters

Parameter	Description	Value
10	Sets the interface rate to 10 Mbit/s.	-
100	Sets the interface rate to 100 Mbit/s.	-
1000	Sets the interface rate to 1000 Mbit/s.	-
{ *portid1* [**to** *portid2*] }	Specifies the index of an interface on an RU.	The value is an integer that ranges from 1 to 32. If the specified interface index is larger than the largest one on the RU, the command is not issued to the RU.

Views

remote-unit N view

Default Level

3: Management level

Usage Guidelines

In non-auto negotiation mode, if interfaces on two connected devices work at different rates, the two devices cannot communicate with each other. In this case, you need to run this command to change the rates of the interfaces to be the same.

Prerequisites

The **undo negotiation auto port** command has been run to configure the interface to work in non-auto-negotiation mode.

Follow-up procedure

After running this command, run the **commit** command to make the configuration take effect.

Example

Configure interface 2 on RU 0 to work at the rate of 100 Mbit/s in non-auto-negotiation mode.

```
<HUAWEI> system-view
[HUAWEI] remote-unit 0
[HUAWEI-remote-unit-0] undo negotiation auto port 2
[HUAWEI-remote-unit-0] speed 100 port 2
```

3.4.56 upgrade cutoff-time

Function

The **upgrade cutoff-time** command sets the RU deployment end time. After this command is run, the firmware of the RUs that go online before the specified time will be automatically upgraded, and automatic RU firmware upgrade is disabled after the specified time.

The **undo upgrade cutoff-time** command deletes the configuration.

By default, no RU deployment end time is configured.

Format

upgrade cutoff-time *YYYY/MM/DD HH:MM:SS*

undo upgrade cutoff-time

Parameters

Parameter	Description	Value
YYYY/MM/DD	Specifies the date when RUs restart with firmware of the new version.	The value is in the 12-month format of YYYY/MM/DD. YYYY specifies the year, which ranges from 2000 to 2099. MM specifies the month, which ranges from 1 to 12. DD specifies the day, which ranges from 1 to 31.

Parameter	Description	Value
HH:MM:SS	Specifies the time when RUs restart with firmware of the new version.	The value is in the 24-hour format of HH:MM:SS. HH indicates hours, and its value is an integer ranging from 0 to 23; MM indicates minutes, and its value is an integer ranging from 0 to 59; SS indicates seconds, and its value is an integer ranging from 0 to 59.

Views

remote-unit view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

This command is applicable to the deployment scenario. The deployment process usually lasts for several days, during which RUs may be connected to the central switch successively. You can run this command to specify the deployment end time (based on the system time of the central switch), so that the firmware of all RUs is automatically upgraded when the specified time is reached. As such, you do not need to run the **upgrade right-now** command to upgrade RU firmware each time a new RU is connected to the central switch. After this command is run, the firmware of the RUs that go online before the specified time will be automatically upgraded, and automatic RU firmware upgrade is disabled after the specified time.

Precautions

After you run the **upgrade cutoff-time** command to configure the RU deployment time, other upgrade commands that have been configured are overwritten. That is, all RUs that go online before the specified deployment time will immediately restart with firmware of the new version.

Example

Set the time when RUs restart with firmware of the new version in the deployment scenario.

```
<HUAWEI> system-view
[HUAWEI] remote-unit
[HUAWEI-remote-unit] upgrade cutoff-time 2022/05/31 00:00:00
```

3.4.57 upgrade force

Function

The **upgrade force** command configures forcible firmware upgrade for RUs.

By default, the function of upgrading RU firmware is disabled.

Format

upgrade { **app** | **bios | poe** } **force**

Parameters

Parameter	Description	Value
app	Specifies the APP firmware of RUs.	-
bios	Specifies the BIOS firmware of RUs.	-
poe	Specifies the PoE firmware of RUs.	-

Views

remote-unit N view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If an RU fails to be upgraded, it enters the cooldown period and can be upgraded again only after the cooldown period ends. To upgrade the firmware of RUs in the cooldown period, you can run this command to configure forcible upgrade.

Precautions

During the BIOS firmware upgrade of RUs, do not power off or disconnect the RUs. Otherwise, the RUs cannot be started.

The **upgrade force** command upgrades firmware of an RU, regardless of whether the RU has the upgrade function enabled. After this command is run in the view of a single RU, the RU immediately restarts with firmware of the new version.

Example

Configure forcible APP firmware upgrade for RUs.

```
<HUAWEI> system-view
[HUAWEI] remote-unit 0
[HUAWEI-remote-unit-0] upgrade app force
```

3.4.58 upgrade right-now

Function

The **upgrade right-now** command upgrades the firmware of RUs immediately.

By default, the function of upgrading RU firmware is disabled.

Format

upgrade right-now

Parameters

None

Views

remote-unit view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If the firmware version of an RU is different from that in the system software package or patch package of the central switch, the central switch does not automatically upgrade the firmware version of the RU. You can run the **upgrade right-now** command to upgrade the firmware of all RUs. After the **upgrade right-now** command is run, the system checks whether the firmware version of an RU is the same as that in the system software package or patch package of the central switch. If not, the RU immediately loads the firmware package of the new version and restarts with new firmware.

Prerequisites

RUs are online and in the normal state.

Precautions

- RUs will restart after loading firmware packages, resulting in service interruption. To prevent this issue, upgrade RUs at a proper time.
- Do not power off RUs during the upgrade. Otherwise, RUs may fail to start.
- Only the firmware of the RUs that go online before the command is run is upgraded. To upgrade RUs that go online later, you need to run this command again.
- This command is executed only once and is not recorded in Buildrun information. You can run the **display remote-unit upgrade information** command to check whether an RU is being upgraded.
- After you run the **upgrade right-now** command, RUs are upgraded immediately. The **upgrade cutoff-time** and **upgrade start-time** upgrade commands that have been configured are overwritten.

Example

Enable RU firmware upgrade.


```
<HUAWEI> system-view
[HUAWEI] remote-unit
[HUAWEI-remote-unit] upgrade right-now
```

3.4.59 upgrade start-time

Function

The **upgrade start-time** command restarts RUs with firmware of the new version at a specified time.

The **undo upgrade start-time** command deletes the configuration.

By default, no time is set for RUs to restart with firmware of the new version.

Format

upgrade start-time *HH:MM:SS*

undo upgrade start-time

Parameters

Parameter	Description	Value
HH:MM:SS	Specifies the time when RUs restart with firmware of the new version.	The value is in the 24-hour format of HH:MM:SS. HH indicates hours, and its value is an integer ranging from 0 to 23; MM indicates minutes, and its value is an integer ranging from 0 to 59; SS indicates seconds, and its value is an integer ranging from 0 to 59.

Views

remote-unit view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The firmware upgrade of an RU consists of two steps:

1. The RU loads firmware of the new version. In this step, the central switch sends the firmware package of the new version to the RU.
2. The RU restarts to make firmware of the new version take effect.

You can run the **upgrade start-time** command to configure RUs to restart with firmware of the new version at a specified time. This command configures the restart time in step 2.

Precautions

During the BIOS firmware upgrade of RUs, do not power off or disconnect the RUs. Otherwise, the RUs cannot be started.

After you run the **upgrade start-time** command to configure RUs to restart with firmware of the new version at a specified time, other upgrade commands that have been configured are overwritten. That is, RUs will restart with firmware of the new version at the time specified by the **upgrade start-time** command.

Example

Configure RUs to restart with firmware of the new version at midnight.

```
<HUAWEI> system-view
[HUAWEI] remote-unit
[HUAWEI-remote-unit] upgrade start-time 00:00:00
```

3.4.60 vlan mode

Function

The **vlan mode** command configures the VLAN mode for an RU.

The **undo vlan mode** command restores the default VLAN mode for an RU.

By default, an RU uses the transparent VLAN mode.

Format

vlan mode { **manual** | **transparent** }

undo vlan mode

Parameters

Parameter	Description	Value
manual	Configures the manual VLAN mode. In manual mode, an interface uses VLAN 1 as its default VLAN and joins VLAN 1 in untagged mode.	-
transparent	Configures the transparent VLAN mode.	-

Views

remote-unit view, remote-unit N view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

An RU can connect to different types of terminals using its downlink interfaces and distinguish terminal services by joining its downlink interfaces to different VLANs. By default, all interfaces on an RU work in transparent VLAN mode. That is, the RU does not change the VLAN IDs of received packets. If services of downlink terminals connected to an RU need to be divided based on VLANs, you need to run the **vlan mode manual** command to configure the RU to work in manual VLAN mode, and then configure default and allowed VLANs for interfaces on the RU.

An RU saves the VLAN configuration delivered by the central switch to it in its flash memory and forwards traffic based on this VLAN configuration after being powered on. After the RU goes online on the central switch, the central switch synchronizes the latest VLAN configuration to the RU's flash memory.

Follow-up Procedure

- Configure default and allowed VLANs for interfaces on the RU.
- After you run the commands for configuring the VLAN mode for an RU and VLANs for RU interfaces, run the **commit** command to deliver the VLAN configuration to the RU or bring the RU offline and then online again for the configuration to take effect.

Precautions

You can configure the VLAN mode of an RU in the remote-unit view or remote-unit N view. If the VLAN mode is configured in both views, the configuration in the remote-unit N view takes effect. If no VLAN mode is configured in the remote-unit N view, the configuration in the remote-unit view takes effect.

Example

Configure all connected RUs to work in manual VLAN mode.

```
<HUAWEI> system-view
[HUAWEI] remote-unit
[HUAWEI-remote-unit] vlan mode manual
```

Configure the manual VLAN mode for the RU 0.

```
<HUAWEI> system-view
[HUAWEI] remote-unit 0
[HUAWEI-remote-unit-0] vlan mode manual
```

3.4.61 xldp enable (interface view)

Function

The **xldp enable** command enables XLDP on an interface.

The **xldp disable** command disables XLDP on an interface.

The **undo xldp disable** command restores the default configuration.

After XLDP is enabled in the system view, all interfaces are enabled with XLDP by default.

Format

xldp enable

xldp disable

undo xldp disable

Parameters

None

Views

Ethernet interface view, GE interface view, XGE interface view, 25GE interface view, MultiGE interface view, 40GE interface view, 100GE interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After XLDP is enabled on an interface, the interface exchanges XLDP packets with XLDP-enabled neighbors. The interface receives status information from the neighbors and sends the local status information to the neighbors. An intelligent simplified campus network runs based on the XLDP protocol.

Prerequisites

XLDP has been enabled globally using the **xldp enable** in the system view.

Precautions

- XLDP can be enabled in the system view and the interface view.
  - After XLDP is enabled in the system view, all interfaces are enabled with XLDP.
  - After XLDP is disabled in the system view, all XLDP settings are restored to the default settings except the setting of XLDP trap. Therefore, XLDP is also disabled on all interfaces.
  - An interface can send and receive XLDP packets only after XLDP is enabled in both the system view and the interface view.
  - After XLDP is disabled globally, the commands for enabling and disabling XLDP on an interface do not take effect.
  - If some interfaces need to have XLDP enabled but some need to have XLDP disabled, you can globally enable XLDP and run the **xldp disable** command in the interface view to disable XLDP for the required interfaces. To re-enable XLDP on these interfaces, run the **xldp enable** command in the views of these interfaces.
- The **xldp enable (interface view)** command can be run only on an Ethernet interface, regardless of whether it works at Layer 2 or Layer 3 mode, and cannot be run on a logical interface such as a VLANIF or Eth-Trunk interface.

For an Eth-Trunk interface, XLDP can only be enabled on its member interfaces. XLDP-enabled interfaces and XLDP-disabled interfaces can be added to the same Eth-Trunk.

- If a large number of XLDP packets are sent to attack an interface, disable XLDP on the interface so that the interface does not send XLDP packets to the CPU for processing.

Example

Disable XLDP on the Ethernet interface GigabitEthernet0/0/1.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] xldp disable
```

3.4.62 xldp enable (system view)

Function

The **xldp enable** command enables XLDP globally.

The **xldp disable** command disables XLDP globally.

The **undo xldp disable** command restores the default global XLDP configuration.

By default, XLDP is enabled globally.

Format

xldp enable

xldp disable

undo xldp disable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To view the status of Layer 2 links connecting the central switch and RUs for analyzing the network topology, you need to run this command to enable XLDP.

Configuration Impact

After XLDP is enabled globally, the device sends its own status information to XLDP-enabled neighbors and receives the status information from the neighbors.

Precautions

After global XLDP is disabled, the XLDP configuration is deleted from all interfaces.

XLDP can be enabled in the system view and the interface view.

- After XLDP is enabled in the system view, all interfaces are enabled with XLDP.
- After XLDP is disabled in the system view, all XLDP settings are restored to the default settings except the setting of XLDP trap. Therefore, XLDP is also disabled on all interfaces.
- An interface can send and receive XLDP packets only after XLDP is enabled in both the system view and the interface view.
- After XLDP is disabled globally, the commands for enabling and disabling XLDP on an interface do not take effect.

Example

Enable XLDP globally.

```
<HUAWEI> system-view
[HUAWEI] xldp enable
```

Disable XLDP globally.

```
<HUAWEI> system-view
[HUAWEI] xldp disable
```

3.5 SVF Configuration Commands

3.5.1 Command Support

NOTE

- When the parent version is earlier than V200R011C10, the AS version must be the same as the parent version. Otherwise, this AS cannot go online. For example, if the parent version is V200R010C00, the AS version must also be V200R010C00. When the parent version is V200R011C10 or later, the parent version and AS version can be different, but the parent version must be higher than or the same as the AS version and the AS version must also be V200R011C10 or later. **Table1** describes the version mapping between parent and AS. **Table2** describes supported Parent and AS switch models in different software versions.
- APs must use the software version matching that of the parent. For details, see "WLAN Service Configuration - Licensing Requirements and Limitations for WLAN" in the *Configuration Guide - WLAN-AC*.
- To check AP device types supported by the parent by default, run the **display ap-type all** command on the parent. The S6735-S, S6720-EI, S6720S-EI, S6720-SI, S6720S-SI, S6720S-S,S6730-S, or S6730S-S cannot manage APs when acting as a parent.

Table 3-84 Version mapping between parent and AS

Parent Version	Required AS Version
V200R007C00	V200R007C00
V200R008C00	V200R008C00
V200R009C00	V200R009C00
V200R010C00	V200R010C00
V200R011C00	V200R011C00
V200R011C10	V200R011C10
V200R012C00	V200R011C10, V200R012C00
V200R013C00	V200R011C10, V200R012C00, V200R013C00
V200R019C00	V200R012C00, V200R013C00, V200R019C00
V200R019C10	V200R012C00, V200R013C00, V200R019C00, V200R019C10
V200R020C00	V200R013C00, V200R019C00, V200R019C10, V200R020C00
V200R020C10	V200R013C00, V200R019C00, V200R019C10, V200R020C00, V200R020C10
V200R020C30	V200R013C00, V200R019C00, V200R019C10, V200R020C00, V200R020C10, V200R020C30
V200R021C00	V200R019C00, V200R019C10, V200R020C00, V200R020C10, V200R020C30, V200R021C00
V200R021C01	V200R019C00, V200R019C10, V200R020C00, V200R020C10, V200R020C30, V200R021C00, V200R021C01
V200R021C10	V200R019C00, V200R019C10, V200R020C00, V200R020C10, V200R020C30, V200R021C00, V200R021C01, V200R021C10
V200R022C00	V200R020C00, V200R020C10, V200R020C30, V200R021C00, V200R021C01, V200R021C10, V200R022C00
V200R022C10	V200R020C00, V200R020C10, V200R020C30, V200R021C00, V200R021C01, V200R021C10, V200R022C00, V200R022C10
V200R023C00	V200R021C00, V200R021C01, V200R021C10, V200R022C00, V200R022C10, V200R023C00

Table 3-85 Supported parent and AS switch models

Software Version	Supported Parent Switch Models	Supported AS Switch Models
V200R007C00	• S12708, S12712 • S7703, S7706, S7712 • S9703, S9706, S9712 • S5720-HI	S2750-EI, S5700-LI, S5700S-LI, S5720-EI
V200R008C00	• S12704, S12708, S12712 • S7703, S7706, S7712 • S9703, S9706, S9712 • S5720-HI	• S2750-EI, S5700-LI, S5700S-LI, S5710-X-LI, S5720-SI, S5720S-SI, S5720-EI • E600
V200R009C00	• S12704, S12708, S12712 • S7703, S7706, S7712 • S9703, S9706, S9712 • S5720-HI, S6720-EI, S6720S-EI	• S2720-EI, S2750-EI, S5700-LI, S5700S-LI, S5710-X-LI, S5720-SI, S5720S-SI, S5720-EI, S6720-EI, S6720S-EI • E600
V200R010C00	• S12704, S12708, S12710, S12712 • S7703, S7706, S7712 • S9703, S9706, S9712 • S5720-HI, S6720-EI, S6720S-EI	• S2720-EI, S2750-EI, S5700-LI, S5700S-LI, S5710-X-LI, S5720-LI, S5720S-LI, S5720-SI, S5720S-SI, S5720-EI, S6720-EI, S6720S-EI • E600 • S600-E
V200R011C00	S5720-HI, S6720-EI, S6720S-EI	• S2750-EI, S5700-LI, S5700S-LI, S5710-X-LI, S5720-LI, S5720S-LI, S5720-SI, S5720S-SI, S5720-EI, S6720-EI, S6720S-EI, S6720-LI, S6720S-LI, S6720-SI, S6720S-SI • E600 • S600-E
V200R011C10	• S12704, S12708, S12710, S12712 • S7703, S7706, S7712 • S9703, S9706, S9712 • S9303, S9306, S9310, S9312 • S5720-HI, S6720-EI, S6720S-EI, S6720-SI, S6720S-SI	• S2720-EI, S2750-EI, S5700-LI, S5700S-LI, S5710-X-LI, S5720-LI, S5720S-LI, S5720-SI, S5720S-SI, S5720-EI, S5730-SI, S5730S-EI, S6720-EI, S6720S-EI, S6720-LI, S6720S-LI, S6720-SI, S6720S-SI • E600 • S600-E

Software Version	Supported Parent Switch Models	Supported AS Switch Models
V200R012C00	• S12704, S12708, S12710, S12712 • S7703, S7706, S7712 • S9703, S9706, S9712 • S9303, S9306, S9310, S9312 • S5720-HI, S5730-HI, S6720-EI, S6720S-EI, S6720-SI, S6720S-SI, S6720-HI	• S2720-EI, S2750-EI, S5700-LI, S5700S-LI, S5710-X-LI, S5720-LI, S5720S-LI, S5720-SI, S5720S-SI, S5720I-SI, S5720-EI, S5730-SI, S5730S-EI, S5730-HI, S6720-EI, S6720S-EI, S6720-LI, S6720S-LI, S6720-SI, S6720S-SI • S600-E
V200R013C00	• S12704, S12708, S12710, S12712 • S7703, S7703 PoE, S7706, S7706 PoE, S7712 • S9703, S9706, S9712 • S9303, S9306, S9310, S9312 • S5720-HI, S5730-HI, S6720-EI, S6720S-EI, S6720-SI, S6720S-SI, S6720-HI	• S2720-EI, S5720-LI, S5720S-LI, S5720-SI, S5720S-SI, S5720I-SI, S5720-EI, S5730-SI, S5730S-EI, S5730-HI, S6720-EI, S6720S-EI, S6720-LI, S6720S-LI, S6720-SI, S6720S-SI • S600-E
V200R019C00	• S12704, S12708, S12710, S12712 • S12700E-4, S12700E-8, S12700E-12 • S7703, S7703 PoE, S7706, S7706 PoE, S7712 • S9303, S9306, S9310, S9312 • S5720-HI, S5730-HI, S5731-H, S5731S-H, S5732-H, S6720-EI, S6720S-EI, S6720-SI, S6720S-SI, S6720-HI, S6730-H, S6730-S, S6730S-S	• S2720-EI, S5720-LI, S5735-L, S5735S-L, S5735S-L-M, S5720S-LI, S5720-SI, S5735-S, S5735S-S, S5720S-SI, S5720I-SI, S5720-EI, S5730-SI, S5730S-EI, S5730-HI, S5731-H, S5731S-H, S5732-H, S5731-S, S5731S-S, S6730-H, S6730-S, S6730S-S, S6720-EI, S6720S-EI, S6720-LI, S6720S-LI, S6720-SI, S6720S-SI • S600-E
V200R019C10	• S12704, S12708, S12710, S12712 • S12700E-4, S12700E-8, S12700E-12 • S7703, S7703 PoE, S7706, S7706 PoE, S7712 • S9303, S9306, S9310, S9312 • S5720-HI, S5730-HI, S5731-H, S5731S-H, S5732-H, S6720-EI, S6720S-EI, S6720-SI, S6720S-SI, S6720-HI, S6730-H, S6730S-H, S6730-S, S6730S-S	• S2720-EI, S5720-LI, S5735-L, S5735S-L, S5735S-L-M, S5720S-LI, S5720-SI, S5735-S, S5735S-S, S5735-S-I, S5720S-SI, S5720I-SI, S5720-EI, S5730-SI, S5730S-EI, S5730-HI, S5731-H, S5731S-H, S5732-H, S5731-S, S5731S-S, S6730-H, S6730S-H, S6730-S, S6730S-S, S6720-EI, S6720S-EI, S6720-LI, S6720S-LI, S6720-SI, S6720S-SI • S600-E

Software Version	Supported Parent Switch Models	Supported AS Switch Models
V200R020C00	• S12704, S12708, S12710, S12712 • S12700E-4, S12700E-8, S12700E-12 • S7703, S7703 PoE, S7706, S7706 PoE, S7712 • S9303, S9306, S9310, S9312 • S5731-H, S5731S-H, S5732-H, S6720S-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, S6730S-S	• S2720-EI, S5720-LI, S5720S-LI, S5720I-SI, S5731-H, S5731S-H, S5732-H, S5731-S, S5731S-S, S5735-L, S5735S-L, S5735S-L-M, S5735-S, S5735S-S, S5735-S-I, S5735S-H, S5736-S, S6720S-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, S6730S-S • S600-E
V200R020C10	• S12704, S12708, S12710, S12712 • S12700E-4, S12700E-8, S12700E-12 • S7703, S7703 PoE, S7706, S7706 PoE, S7712 • S9303, S9306, S9310, S9312 • S5731-H, S5731S-H, S5732-H, S6720S-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, S6730S-S	• S2720-EI, S5720-LI, S5720S-LI, S5720I-SI, S5731-H, S5731S-H, S5732-H, S5731-S, S5731S-S, S2730S-S, S5735-L1, S300, S5735-L, S5735S-L1, S5735S-L, S5735S-L-M, S500, S5735-S, S5735S-S, S5735-S-I, S5735S-H, S5736-S, S6720S-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, S6730S-S • S600-E
V200R020C30	None	S5735-S8P2X-IA200H1, S5736-S48S4X-A, S5736-S48S4X-D
V200R021C00	• S12704, S12708, S12710, S12712 • S12700E-4, S12700E-8, S12700E-12 • S7703, S7703 PoE, S7706, S7706 PoE, S7712 • S9303, S9306, S9310, S9312 • S5731-H, S5731S-H, S5732-H, S6720S-S, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, S6730S-S	• S2720-EI, S5720-LI, S5720S-LI, S5720I-SI, S5731-H, S5731S-H, S5732-H, S5731-S, S5731S-S, S2730S-S, S5735-L1, S300, S5735-L, S5735-L-I, S5735S-L1, S5735S-L, S5735S-L-M, S500, S5735-S, S5735S-S, S5735-S-I, S5735S-H, S5736-S, S6720S-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, S6730S-S, S6735-S • S600-E

Software Version	Supported Parent Switch Models	Supported AS Switch Models
V200R021C01	• S12704, S12708, S12710, S12712 • S12700E-4, S12700E-8, S12700E-12 • S7703, S7703 PoE, S7706, S7706 PoE, S7712 • S9303, S9306, S9310, S9312 • S5731-H, S5731S-H, S5732-H, S6720S-S, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, S6730S-S	• S2720-EI, S5720-LI, S5720S-LI, S5720I-SI, S5731-H, S5731S-H, S5732-H, S5731-S, S5731S-S, S2730S-S, S5735-L1, S300, S5735-L, S5735-L-I, S5735S-L1, S5735S-L, S5735S-L-M, S500, S5735-S, S5735S-S, S5735-S-I, S5735S-H, S5736-S, S6720S-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, S6730S-S, S6735-S • S600-E
V200R021C10	• S12704, S12708, S12710, S12712 • S12700E-4, S12700E-8, S12700E-12 • S7703, S7703 PoE, S7706, S7706 PoE, S7712 • S9303, S9306, S9310, S9312 • S5731-H, S5731S-H, S5732-H, S6720S-S, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, S6730S-S	• S2720-EI, S5720-LI, S5720S-LI, S5720I-SI, S5731-H, S5731S-H, S5732-H, S5731-S, S5731S-S, S2730S-S, S5735-L1, S300, S5735-L, S5735-L-I, S5735S-L1, S5735S-L, S5735S-L-M, S500, S5735-S, S5735S-S, S5735-S-I, S5735S-H, S5736-S, S6720S-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, S6730S-S, S6735-S • S600-E
V200R022C00	• S12704, S12708, S12710, S12712 • S12700E-4, S12700E-8, S12700E-12 • S7703, S7703 PoE, S7706, S7706 PoE, S7712 • S9303, S9306, S9310, S9312 • S5731-H, S5731S-H, S5732-H, S6720S-S,S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, S6730S-S	• S2720-EI, S5720-LI, S5720S-LI, S5720I-SI, S5731-H, S5731S-H, S5732-H, S5731-S, S5731S-S, S2730S-S, S5735-L1, S300, S5735-L, S5735-L-I, S5735S-L1, S5735S-L, S5735S-L-M, S500, S5735-S, S5735S-S, S5735-S-I, S5735S-H, S5736-S, S6720S-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, S6730S-S, S6735-S • S600-E

Software Version	Supported Parent Switch Models	Supported AS Switch Models
V200R022C10	• S12704, S12708, S12712 • S12700E-4, S12700E-8, S12700E-12 • S7703, S7703 PoE, S7706, S7706 PoE, S7712 • S9303, S9306, S9310, S9312 • S5731-H, S5731S-H, S5732-H, S6720S-S, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, S6730S-S • S5531-H	• S2720-EI, S5720-LI, S5720S-LI, S5720I-SI, S5731-H, S5731S-H, S5732-H, S5731-S, S5731S-S, S2730S-S, S5735-L1, S300, S5735-L, S5735-L-I, S5735S-L1, S5735S-L, S5735S-L-M, S500, S5735-S, S5735S-S, S5735-S-I, S5735S-H, S5736-S, S6720S-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, S6730S-S, S6735-S • S5531-H, S5531-S
V200R023C00	• S12704, S12708, S12712 • S12700E-4, S12700E-8, S12700E-12 • S7703, S7703 PoE, S7706, S7706 PoE, S7712 • S9303, S9306, S9310, S9312 • S5731-H, S5731S-H, S5732-H, S6720S-S,S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, S6730S-S • S5531-H	• S2720-EI, S5720-LI, S5720S-LI, S5720I-SI, S5731-H, S5731S-H, S5732-H, S5731-S, S5731S-S, S2730S-S, S5735-L1, S300, S5735-L, S5735-L-I, S5735S-L1, S5735S-L, S5735S-L-M, S500, S5735-S, S5735S-S, S5735-S-I, S5735S-H, S5736-S, S6720S-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, S6730S-S, S6735-S • S5531-H, S5531-S

3.5.2 acl ipv6 number (AS administrator profile view)

Function

The **acl ipv6 number** command configures an IPv6 ACL rule number in an AS administrator profile.

The **undo acl ipv6 number** command deletes an IPv6 ACL rule number in an AS administrator profile.

By default, no IPv6 ACL rule number is configured in an AS administrator profile.

NOTE

This command can only be executed on a parent switch.

Format

acl ipv6 number { *acl-number* } &<1-16>

undo acl ipv6 number { *acl-number* } &<1-16>

Parameters

Parameter	Description	Value
acl-number	Specifies an ACL rule number.	The value is an integer in the range from 3000 to 3999.

Views

AS administrator profile view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

After creating an AS administrator profile, you can run the **acl ipv6 number** command to configure an IPv6 ACL rule number for an AS in the AS administrator profile. After the profile is bound to an AS, the following configuration is generated on the AS:

```
#
acl ipv6 number acl-number
 rule xxx
#
```

Precautions

- In SVF, only 5-tuple information (source IP address, destination IP address, source port, destination port, and protocol type) can be specified in ACL rules.
- The IPv6 ACL used in an AS administrator profile must have been created in the system view, and rules have been configured in the ACL view.
- A maximum of 64 IPv6 ACLs can be configured in an AS administrator profile, and a maximum of 1024 rules can be created in an ACL. The total number of IPv4 and IPv6 ACL rules cannot exceed 4096.

Example

Configure an IPv6 ACL rule number in an AS administrator profile.

```
<HUAWEI> system-view
[HUAWEI] uni-mng
[HUAWEI-um] as-admin-profile name profile_1
[HUAWEI-um-as-admin-profile_1] acl ipv6 number 3000 3002 3010 3011 3012
```

3.5.3 acl number (AS administrator profile view)

Function

The **acl number** command configures an ACL rule number in an AS administrator profile.

The **undo acl number** command deletes an ACL rule number in an AS administrator profile.

By default, no ACL rule number is configured in an AS administrator profile.

NOTE

This command can only be executed on a parent switch.

Format

acl number { *acl-number* } &<1-16>

undo acl number { *acl-number* } &<1-16>

Parameters

Parameter	Description	Value
acl-number	Specifies an ACL rule number.	The value is an integer in the range from 3000 to 3900.

Views

AS administrator profile view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

After creating an AS administrator profile, you can run the **acl number** command to configure an ACL rule number for an AS in the AS administrator profile. After the profile is bound to an AS, the following configuration is generated on the AS:

```
#
acl number acl-number
 rule xxx
#
```

Precautions

- In SVF, only 5-tuple information (source IP address, destination IP address, source port, destination port, and protocol type) can be specified in ACL rules.
- The ACL used in an AS administrator profile must have been created in the system view, and rules have been configured in the ACL view.
- A maximum of 64 ACLs can be configured in an AS administrator profile, and a maximum of 1024 rules can be created in an ACL. The total number of IPv4 and IPv6 ACL rules cannot exceed 4096.

Example

Configure an ACL rule number in an AS administrator profile.


```
<HUAWEI> system-view
[HUAWEI] uni-mng
[HUAWEI-um] as-admin-profile name profile_1
[HUAWEI-um-as-admin-profile_1] acl number 3000 3002 3010 3011 3012
```

3.5.4 arp anti-attack check user-bind enable (network enhanced profile view)

Function

The **arp anti-attack check user-bind enable** command configures dynamic ARP inspection (DAI) in a network enhanced profile.

The **undo arp anti-attack check user-bind enable** command disables DAI in a network enhanced profile.

By default, DAI is not configured in a network enhanced profile.

NOTE

This command can only be executed on a parent switch.

Format

arp anti-attack check user-bind enable

undo arp anti-attack check user-bind enable

Parameters

None

Views

Network enhanced profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After creating a network enhanced profile, you can configure DAI in the profile. After the profile is bound to an AS port, DAI is automatically enabled on the port. The following configuration is generated on the AS port:

```
#
 arp anti-attack rate-limit enable
 arp anti-attack rate-limit packet 5 interval 1
 arp anti-attack check user-bind enable
 arp anti-attack check user-bind alarm enable
#
```

You can configure DAI to prevent Man in The Middle (MITM) attacks and theft on authorized user information. When a device receives an ARP packet, it compares the source IP address, source MAC address, interface number, and VLAN ID of the

ARP packet with DHCP snooping binding entries. If the ARP packet matches a binding entry, the device allows the packet to pass through. If the ARP packet does not match any binding entry, the device discards the packet.

Prerequisites

DHCP snooping has been enabled in the network enhanced profile using the **dhcp snooping enable** command.

Example

Enable DAI in a network enhanced profile.

```
<HUAWEI> system-view
[HUAWEI] uni-mng
[HUAWEI-um] network-enhanced-profile name profile_1
[HUAWEI-um-net-enhanced-profile_1] dhcp snooping enable
[HUAWEI-um-net-enhanced-profile_1] arp anti-attack check user-bind enable
```

3.5.5 as-admin-profile (AS group view)

Function

The **as-admin-profile** command binds an AS administrator profile to an AS group.

The **undo as-admin-profile** command unbinds an AS administrator profile from an AS group.

By default, no AS administrator profile is bound to an AS group.

NOTE

This command can only be executed on a parent switch.

Format

as-admin-profile *profile-name*

undo as-admin-profile

Parameters

Parameter	Description	Value
profile-name	Specifies the name of an AS administrator profile.	The value must have an existing AS administrator profile name.

Views

AS group view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

You can bind an AS administrator profile to an AS group to deliver the configurations in the profile to all the member ASs in the AS group.

Prerequisites

The AS administrator profile has been created.

Precautions

AS groups can only be bound to AS administrator profiles. Each AS group can be bound to only one AS administrator profile.

Example

Bind an AS administrator profile to an AS group.

```
<HUAWEI> system-view
[HUAWEI] uni-mng
[HUAWEI-um] as-admin-profile name profile_1
[HUAWEI-um-as-admin-profile_1] quit
[HUAWEI-um] as-group name group_1
[HUAWEI-um-as-group-group_1] as-admin-profile profile_1
```

3.5.6 as-admin-profile name

Function

The **as-admin-profile name** command creates an AS administrator profile.

The **undo as-admin-profile name** command deletes an AS administrator profile.

By default, no AS administrator profile is configured.

NOTE

This command can only be executed on a parent switch.

Format

as-admin-profile name *profile-name*

undo as-admin-profile name *profile-name*

Parameters

Parameter	Description	Value
profile-name	Specifies the name of an AS administrator profile.	The value is a string of 1 to 31 case-sensitive characters without spaces. The value can contain letters, digits, and underscores (_).

Views

uni-mng view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

In an AS administrator profile, you can configure AS administrator information and the rate limit for outgoing ARP and DHCP packets on an uplink fabric port.

Precautions

You can create a maximum of 16 AS administrator profiles.

Example

Create an AS administrator profile.

```
<HUAWEI> system-view
[HUAWEI] uni-mng
[HUAWEI-um] as-admin-profile name profile_1
```

3.5.7 as authentication configuration revert disable

Function

The **as authentication configuration revert disable** command enables the function of retaining the authentication configuration after an AS goes offline.

The **undo as authentication configuration revert disable** command disables the function of retaining the authentication configuration after an AS goes offline.

By default, the authentication configuration is cleared after an AS goes offline.

NOTE

This command can only be executed on a parent switch.

Format

as authentication configuration revert disable

undo as authentication configuration revert disable

Parameters

None

Views

uni-mng view

Default Level

3: Management level

Usage Guidelines

When an AS goes offline, it automatically clears its authentication configuration to ensure connectivity in the local area network (LAN) connected to it in case of an AS authentication failure. However, clearing the authentication configuration when the AS goes offline will lengthen the time taken for the AS to go online again. If the AS is not connected to a LAN or if the time taken for the AS to go online again needs to be shortened, enable the function of retaining the authentication configuration after the AS goes offline on the parent to shorten the time taken for the AS to go online again.

Example

Enable the function of retaining the authentication configuration after an AS goes offline.

```
<HUAWEI> system-view
[HUAWEI] uni-mng
[HUAWEI-um] as authentication configuration revert disable
```

3.5.8 as-auth

Function

The **as-auth** command displays the AS authentication view.

NOTE

This command can only be executed on a parent switch.

Format

as-auth

Parameters

None

Views

System view

Default Level

3: Management level

Usage Guidelines

After entering the AS authentication view, you can configure the AS authentication mode, blacklist, and whitelist.

Example

Enter the AS authentication view.

```
<HUAWEI> system-view
[HUAWEI] as-auth
```

3.5.9 as-group name

Function

The **as-group name** command creates an AS group or displays the AS group view.

The **undo as-group name** command deletes an AS group.

By default, no AS group is created.

NOTE

This command can only be executed on a parent switch.

Format

as-group name *group-name*

undo as-group name *group-name*

Parameters

Parameter	Description	Value
group-name	Specifies the name of an AS group.	The value is a string of 1 to 31 case-sensitive characters without spaces. The value can contain letters, digits, and underscores (_).

Views

uni-mng view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

An AS group contains one or more ASs, which facilitates AS batch configuration.

Follow-up Procedure

Run the **as name** *as-name* or **as name-include** *string* command to add ASs to an AS group.

Precautions

You can create a maximum of 16 AS groups.

AS groups can only be bound to AS administrator profiles. Each AS group can be bound to only one AS administrator profile.

Example

Create an AS group.

```
<HUAWEI> system-view
[HUAWEI] uni-mng
[HUAWEI-um] as-group name group_1
```

3.5.10 as access dtls psk

Function

The **as access dtls psk** command configures a pre-shared key for Datagram Transport Layer Security (DTLS) encryption on an access switch (AS).

The **undo as access dtls psk** command deletes a pre-shared key used for DTLS encryption.

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.

NOTE

This command can only be executed on an AS.

Format

as access dtls psk *psk-value*

undo as access dtls psk

Parameters

Parameter	Description	Value
psk-value	Specifies a pre-shared key.	The value is a string of 6 to 32 case-sensitive characters without spaces. The pre-shared key must be in plain text and contain at least two of the following: letters, digits, and special characters.

Views

User view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

To encrypt CAPWAP-encapsulated packets between the parent and an AS, configure the same pre-shared key on the parent and AS. You can run the **as access dtls psk** command to configure a pre-shared key for DTLS encryption on the AS.

Precautions

- The default pre-shared key has security risks. You are advised to change the pre-shared key.
- After an AS has connected to an SVF system, configuring or deleting the pre-shared key for DTLS encryption is not allowed on the AS.

Example

Set the pre-shared key for DTLS encryption to **test@1234**.

```
<HUAWEI> as access dtls psk test@1234
```

3.5.11 as access manage-mac

Function

The **as access manage-mac** command configures the management MAC address of an AS.

The **undo as access manage-mac** command restores the default management MAC address of an AS.

By default, an AS uses the system MAC address as the management MAC address.

NOTE

This command can only be executed on an AS.

Format

as access manage-mac *mac-address*

undo as access manage-mac

Parameters

Parameter	Description	Value
mac-address	Specifies the management MAC address of an AS.	The value is in H-H-H format, where H is a hexadecimal number of 1 to 4 digits. The value cannot be all 0s, all Fs, or a multicast MAC address.

Views

User view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

In a Super Virtual Fabric (SVF) system, each AS has a unique management MAC address to identify itself. By default, an AS uses its system MAC address as the management MAC address to connect to an SVF system. When the management MAC address of an AS conflicts with that of another AS, you can run the **as access manage-mac** command to change the management MAC address so as to prevent MAC address conflicts.

Precautions

- Use of this command is not recommended when no MAC address conflict occurs, as an improper management MAC address may affect service operations.
- This command can be used only before an AS connects an SVF system. If an AS has connected to an SVF system, use of this command is not allowed.
- Before using this command to change the management MAC address of an AS, you must run the **undo as access manage-mac** command to delete the existing management MAC address.

Example

Configure the management MAC address of an AS.

```
<HUAWEI> as access manage-mac 00e0-fc91-52a0
```

3.5.12 as auto-replace enable

Function

The **as auto-replace enable** command enables AS automatic replacement.

The **undo as auto-replace enable** command disables AS automatic replacement.

By default, AS automatic replacement is disabled.

NOTE

This command can only be executed on a parent switch.

Format

as auto-replace enable

undo as auto-replace enable

Parameters

None

Views

uni-mng view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

In an SVF system, each AS is identified by its MAC address by default. When a new device is used to replace an AS, the SVF system considers the new device as a new AS because their MAC addresses are different. As a result, the new AS does not inherit services from the previous AS.

You can enable AS automatic replacement to solve this problem. When an AS is replaced by a new device connected to the same fabric port, the SVF system replaces the AS MAC address with the MAC address of the new device in the configuration. Consequently, the new device can inherit services from the AS.

Precautions

- An AS can only be replaced by a device of the same model. If the new device is a different model, the SVF system considers it as a new AS, which then cannot inherit services from the previous AS.
- Only a standalone AS can be replaced. If an AS is a stack, it cannot be replaced.
- AS automatic replacement is not supported when an AS connects to the parent through a network.
- To ensure that a replacement AS can be successfully authenticated, run the **auth-mode none** command to set the AS authentication mode to none, or run the **whitelist mac-address** command to add the management MAC address of the replacement AS to the whitelist. If the replacement AS has no management MAC address configured, its system MAC address is used as the management MAC address.

Example

Enable AS automatic replacement.

```
<HUAWEI> system-view
[HUAWEI] uni-mng
[HUAWEI-um] as auto-replace enable
```


3.5.13 as-mode disable

Function

The **as-mode disable** command changes the switch working mode to the parent mode.

The **undo as-mode disable** command restores the switch working mode to the AS mode.

Swich models supporting this command and the default working mode of them are as follows:

- S5731-H (excluding S5731-H24HB4XZ, S5731-H48HB4XZ), S5731S-H (excluding S5731S-H24HB4XZ-A, S5731S-H48HB4XZ-A), S5732-H24S6Q, S5732-H48S6Q, S6730S-H, S6730-H: Parent mode
- S5531-H48HB4XZ, S5731-H24HB4XZ, S5731-H48HB4XZ, S5731S-H24HB4XZ-A, S5731S-H48HB4XZ-A, S5732-H24UM2CC, S5732-H48UM2CC, S5732-H48XUM2CC, S6730-S, S6730S-S, S6720-SI, S6720S-S, S6720S-SI, S6720-EI, S6720S-EI, S6735-S: AS mode

Format

as-mode disable

undo as-mode disable

Parameters

None

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

Switch models supporting this command can function as the parent or AS in an SVF system.

Precautions

- After the working mode of a switch is changed, the switch restarts for the new working mode to take effect, and does not use any configuration file at the next startup. As such, the switch restarts without any configuration file. In this case, you are advised to back up the configuration file of the switch before it restarts.
- By default, the following switches work in AS mode: S5732-H24UM2CC, S5732-H48UM2CC, S5732-H48XUM2CC. To enable these switches to

automatically change the working mode to parent during unconfigured device deployment, run the **option 148 ascii** *ascii-string* command to configure Option 148 of the DHCP server. The format of *ascii-string* is svfmode=uc.

Example

Change the switch working mode to the parent mode.

```
<HUAWEI> system-view
[HUAWEI] as-mode disable
Warning: Switching the AS mode will clear current configuration and reboot the system. Continue? [Y/N]:y
```

3.5.14 as all (AS group view)

Function

The **as all** command adds all ASs to an AS group.

The **undo as all** command deletes all ASs from an AS group.

By default, no AS is added to an AS group.

NOTE

This command can only be executed on a parent switch.

Format

as all

undo as all

Parameters

None

Views

AS group view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

After creating an AS group, you need to add the ASs that require the same configuration to the AS group. This command adds all ASs to the same AS group.

Precautions

An AS can be added to only one AS group. For example, if you run the **as all** command in group_1 and then in group_2, the system displays a message, saying that the ASs need to be deleted from the previous AS group before they can be added to the new AS group.

Example

Add all ASs to the AS group group_1.

```
<HUAWEI> system-view
[HUAWEI] uni-mng
[HUAWEI-um] as-group name group_1
[HUAWEI-um-as-group-group_1] as all
```

3.5.15 as name (AS group view)

Function

The **as name** command adds an AS with a specified name to an AS group.

The **as name-include** command adds an AS of which the name contains a specified string to an AS group.

The **undo as name** command deletes an AS with a specified name from an AS group.

The **undo as name-include** command deletes an AS of which the name contains a specified string from an AS group.

By default, no AS is added to an AS group.

NOTE

This command can only be executed on a parent switch.

Format

as name *as-name*

as name-include *string*

undo as name *as-name*

undo as name-include *string*

Parameters

Parameter	Description	Value
as-name	Specifies the name of an AS.	The value must have an existing AS name.
string	Specifies the string contained in an AS name.	The value is a string of 1 to 31 case-insensitive characters without spaces.

Views

AS group view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

After creating an AS group, add the ASs that need to be configured in a batch to the AS group. You can only add created ASs to an AS group.

Precautions

An AS can be added to only one AS group.

After an AS is added to an AS group, to change the AS group, run the **as name** command to add the AS to another AS group.

Example

Add the AS **as_1** to the AS group **group_1**.

```
<HUAWEI> system-view
[HUAWEI] uni-mng
[HUAWEI-um] as-group name group_1
[HUAWEI-um-as-group-group_1] as name as_1
```

3.5.16 as name interface (port group view)

Function

The **as name interface** command adds ports on the AS with a specified name to a port group.

The **as name-include interface** command adds ports on the AS of which the name contains a specified string to a port group.

The **undo as name interface** command deletes ports on the AS with a specified name from a port group.

The **undo as name-include interface** command deletes ports on the AS of which the name contains a specified string from a port group.

By default, no ports on an AS are added to a port group.

NOTE

This command can only be executed on a parent switch.

Format

as name *as-name* **interface** { { *interface-type interface-number1* [**to** *interface-number2*] } &<1-10> | **all** }

as name-include *string* **interface all**

undo as name *as-name* **interface** { { *interface-type interface-number1* [**to** *interface-number2*] } &<1-10> | **all** }

undo as name-include *string* **interface all**

Parameters

Parameter	Description	Value
as-name	Specifies the name of an AS.	The value must have an existing AS name.
string	Specifies the string contained in an AS name.	The value is a string of 1 to 31 case-insensitive characters without spaces.
interface-type interface-number1 [**to** *interface-number2*]	Specifies the type and number of AS interfaces. • *interface-type* specifies the interface type. • *interface-number1* specifies the first interface number. • *interface-number2* specifies the last interface number.	The following ports cannot be added to a port group: • Fabric port • Eth-Trunk member interface • Uplink port on an AS. You can run the **display port connection-type access all** command to view all downlink ports of the device. The ports that are not displayed in the command output are uplink ports. Note that an uplink port still cannot be added to a port group after it is configured as a downlink port using the **port connection-type access** command.
all	Indicates all downlink ports on an AS.	-

Views

Port group view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

After creating a port group, add the AS ports that need to be configured in a batch to the port group.

Precautions

A port can be added to only one port group.

After ports on an AS are added to a port group, to change the port group, run the **as name interface** command to add the ports to another port group.

A fabric port in a port group takes effect only for a network QoS profile but not for any network basic profile, network enhanced profile, traffic policy profile, or user access profile.

Example

Add ports on the AS **as1** to the port group **group_1**.

```
<HUAWEI> system-view
[HUAWEI] uni-mng
[HUAWEI-um] port-group name group_1
[HUAWEI-um-portgroup-group_1] as name as1 interface gigabitethernet 0/0/1 to 0/0/5
```

3.5.17 as name (uni-mng view)

Function

The **as name** command configures an AS name or displays the AS view.

The **undo as name** command deletes an AS.

By default, system default name-device MAC address is used as the AS name, for example, **huawei-000a-123d-2200**.

NOTE

This command can only be executed on a parent switch.

Format

as name *as-name* [**model** *as-model* **mac-address** *mac-address*]

undo as { **all** | **name** *as-name* }

Parameters

Parameter	Description	Value
as-name	Specifies the name of an AS.	The value is a string of 1 to 31 case-insensitive characters without spaces.
model *as-model*	Specifies the device model of an AS.	The value is of enumerated type. You can enter a question mark (?) and select a value from the displayed value range.
mac-address *mac-address*	Specifies the management MAC address of an AS.	The value is in H-H-H format, where H is a hexadecimal number of 1 to 4 digits. The value cannot be all 0s, all Fs, or a multicast MAC address.

Parameter	Description	Value
all	Deletes all ASs.	-

Views

uni-mng view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

You can configure a name for an AS and use the name to uniquely identify the AS. This configuration facilitates AS identification and management.

If no AS name is configured, system default name-device MAC address is used as the AS name after the AS connects to an SVF system.

You can change the name of an AS that has connected to an SVF system when the following conditions are met:

1. The AS is not bound to any service profile.
2. The AS is not added to any AS group.
3. Ports of the AS are not added to any port group.

Precautions

- If the **model** *as-model* **mac-address** *mac-address* parameter is not specified, the AS view is displayed. You can enter the view of an AS only when the AS has been created.
- If an AS has connected to an SVF system, the AS leaves the SVF system and restarts after being deleted.
- If the message "A port instance in the AS (xxx) has been added to the PM. Please delete the configuration first." is displayed when you delete an AS, run the **undo binding** command in the PM statistics task view to delete the configuration. This command ensures that the AS can be deleted successfully.

Example

Configure an AS name.

```
<HUAWEI> system-view
[HUAWEI] uni-mng
[HUAWEI-um] as name as1 model S5720-28P-LI-AC mac-address xxxx-xxxx-xxxx
```

3.5.18 as reset

Function

The **as reset** command restarts an AS.

NOTE

This command can only be executed on a parent switch.

Format

as reset { **all** | **name** *as-name* }

Parameters

Parameter	Description	Value
all	Restarts all ASs.	-
name *as-name*	Restarts an AS with a specified name.	The value must have an existing AS name.

Views

uni-mng view

Default Level

3: Management level

Usage Guidelines

When an AS is upgraded or working abnormally, you can restart the AS.

Example

Restart the AS **as1**.

```
<HUAWEI> system-view
[HUAWEI] uni-mng
[HUAWEI-um] as reset name as1
```

3.5.19 as service-vlan igmp-snooping

Function

The **as service-vlan igmp-snooping** command enables IGMP snooping for a service VLAN on an AS.

The **undo as service-vlan igmp-snooping** command disables IGMP snooping for a service VLAN on an AS.

By default, IGMP snooping is disabled for service VLANs on an AS.

NOTE

This command can only be executed on a parent switch.

Format

as service-vlan igmp-snooping { *vlan-id1* [**to** *vlan-id2*] } &<1-16>

undo as service-vlan igmp-snooping { *vlan-id1* [**to** *vlan-id2*] } &<1-16>

Parameters

Parameter	Description	Value
vlan-id1 [**to** *vlan-id2*]	Specifies range of service VLANs: • *vlan-id1* specifies the start VLAN ID. • *vlan-id2* specifies the end VLAN ID. *vlan-id2* must be greater than or equal to *vlan-id1*. *vlan-id1* and *vlan-id2* define a range together. • If the parameter **to** *vlan-id2* is not specified, only the VLAN specified by *vlan-id1* is a service VLAN ID.	The *vlan-id1* and *vlan-id2* are integers ranging from 1 to 4094.

Views

uni-mng view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

By default, IGMP snooping is disabled for service VLANs on an AS. If IGMP snooping needs to be enabled on an AS, run the **as service-vlan igmp-snooping** command to deliver the configuration to the AS. After the configuration is delivered successfully, the igmp-snooping enable configuration will be generated in the corresponding VLAN view of the AS.

Precautions

This VLAN cannot be a stack reserved VLAN, SVF management VLAN, super VLAN, or RRPP/SEP/ERPS control VLAN.

Example

Enable IGMP snooping for the service VLAN 10 on an AS.

```
<HUAWEI> system-view
[HUAWEI] uni-mng
[HUAWEI-um] as service-vlan igmp-snooping 10
```


3.5.20 as service-vlan authorization

Function

The **as service-vlan authorization** command creates service VLANs on ASs.

The **undo as service-vlan authorization** command deletes service VLANs on ASs.

By default, all interfaces on an AS belong to the default VLAN, that is, VLAN 1.

NOTE

This command can only be executed on a parent switch.

Format

as service-vlan authorization { *vlan-id1* [**to** *vlan-id2*] } &<1-16>

undo as service-vlan authorization { *vlan-id1* [**to** *vlan-id2*] } &<1-16>

Parameters

Parameter	Description	Value
vlan-id1 [**to** *vlan-id2*]	Specifies service VLAN IDs in a batch: • *vlan-id1* specifies the first VLAN ID. • *vlan-id2* specifies the last VLAN ID. *vlan-id2* must be greater than or equal to *vlan-id1*. *vlan-id1* and *vlan-id2* together determine a VLAN range. • If you do not specify **to** *vlan-id2*, only one service VLAN is specified by *vlan-id1*.	Values of *vlan-id1* and *vlan-id2* are integers in a range of 1 to 4094.

Views

uni-mng view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

You can run the **as service-vlan authorization** command to deliver service VLANs to ASs in a batch. After these service VLANs are delivered successfully, corresponding VLANs are created on these ASs.

Precautions

This VLAN cannot be a stack reserved VLAN, SVF management VLAN, super VLAN, or RRPP/SEP/ERPS control VLAN.

In versions earlier than V200R019, a maximum of 32 service VLANs can be created. In V200R019 and later versions, a maximum of 1024 service VLANs can be created.

Example

Create the service VLAN 10 for ASs.

```
<HUAWEI> system-view
[HUAWEI] uni-mng
[HUAWEI-um] as service-vlan authorization 10
```

3.5.21 as type

Function

The **as type** command specifies the file to be loaded during the upgrade of an AS of a specified device type.

The **undo as type** command deletes the file to be loaded during the upgrade of an AS of a specified device type.

By default, the file to be loaded is not specified during the upgrade of an AS of a specified device type.

NOTE

This command can only be executed on a parent switch.

Format

as type *as-type* { **system-software** *system-software* | **patch** *patch* } *

undo as type *as-type* [**system-software** | **patch**]

Parameters

Parameter	Description	Value
as-type	Specifies the device type of an AS.	The value is an enumerated type. You can enter a question mark (?) and select a value from the displayed value range.
system-software *system-software*	Specifies the name of the system software file to be loaded on an AS.	The value is a string of 4 to 48 case-insensitive characters without spaces or special characters, including ~ * : ' " ? < > | [ ] % \ /.
patch *patch*	Specifies the name of the patch file to be loaded on an AS.	The value is a string of 5 to 48 case-insensitive characters without spaces or special characters, including ~ * : ' " ? < > | [ ] % \ /.

Views

uni-mng view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

When an AS is automatically upgraded after going online, the AS is upgraded using the file specified by the **as type** command.

Precautions

You can run the **as type** command multiple times to specify different files for different types of ASs.

If the system software file is not specified and only the patch file is specified during a patch upgrade, the patch upgrade fails if the patch file does not match the system software.

Follow-up Procedure

Run the **upgrade as** command to upgrade the AS.

Example

Specify the file to be loaded on the AS of the S5720-P-LI type.

```
<HUAWEI> system-view
[HUAWEI] uni-mng
[HUAWEI-um] as type s5720-p-li system-software S5720-P-LI-V200R022C00SPC500.cc
```

3.5.22 attach as

Function

The **attach as** command allows you to log in to an AS from the parent.

NOTE

This command can only be executed on a parent switch.

Format

attach as name *as-name*

Parameters

Parameter	Description	Value
name *as-name*	Specifies the name of an AS for login.	The value must have an existing AS name.

Views

uni-mng view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

In addition to local login through a console port, you can log in to an AS from the parent. This login mode is supported in two service configuration modes: centralized mode and independent mode.

After you log in to an AS in centralized mode, you can configure only commands related to file management and service diagnosis for fault location.

After you log in to an AS in independent mode, you can use more commands to configure services on the AS.

Prerequisites

In centralized mode, an AS administrator profile has been bound to the AS, and an AS user name and password have been configured.

In independent mode, an AS user name and password have been configured in the uni-mng view using the **independent-as-admin** command.

Precautions

After an AS user name and password are configured, you need to enter the correct user name and password when logging in to an AS through the console port. When you log in to an AS from the parent using the **attach as** command, you can log in to the AS without entering the user name or password.

In versions earlier than V200R011C10, at most one VTY user can log in to an AS at a time. In V200R011C10 and later versions, at most four VTY users can log in to an AS at a time.

Example

In centralized mode, log in to the AS **as1** from the parent.

```
<HUAWEI> system-view
[HUAWEI] uni-mng
[HUAWEI-um] as-admin-profile name profile_1
[HUAWEI-um-as-admin-profile_1] user asuser password YsHsjx_202206
[HUAWEI-um-as-admin-profile_1] quit
```



```
[HUAWEI-um] as-group name group_1
[HUAWEI-um-as-group-group_1] as name as1
[HUAWEI-um-as-group-group_1] as-admin-profile profile_1
[HUAWEI-um-as-group-group_1] quit
[HUAWEI-um] commit as all
Info: Commiting the configuration will take a long time. Are you sure you want to commit the configuration? [Y/N]: y
[HUAWEI-um] attach as name as1
```

In independent mode, log in to the AS **as1** from the parent. Before the login, the independent mode needs to be enabled on the fabric-port connected to the AS **as1**. The following uses a level-1 AS as the AS **as1**.

```
<HUAWEI> system-view
[HUAWEI] uni-mng
[HUAWEI-um] independent-as-admin user asuser password YsHsjx_202206
[HUAWEI-um] interface fabric-port 1
[HUAWEI-um-fabric-port-1] port connect independent-as
[HUAWEI-um-fabric-port-1] quit
[HUAWEI-um] attach as name as1
```

3.5.23 authentication access-user maximum (user access profile view)

Function

The **authentication access-user maximum** command configures the maximum number of access users in a user access profile.

The **undo authentication access-user maximum** command deletes the maximum number of access users in a user access profile.

By default, the maximum number of access users is not configured in a user access profile.

NOTE

This command can only be executed on a parent switch.

Format

authentication access-user maximum *max-num*

undo authentication access-user maximum

Parameters

Parameter	Description	Value
max-num	Specifies the maximum number of access users in a user access profile.	The value is an integer that ranges from 1 to 1024. After the value is delivered to an AS, the effective value depends on the AS specifications. For details, see **authentication access-point max-user**.

Views

User access profile view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

After creating a user access profile, you can configure the maximum number of access users in the profile. When the profile is bound an AS port, the maximum number of access users is automatically configured for the port. The following configuration is generated on the AS port:

```
#
 authentication access-point max-user max-num
#
```

Precautions

The **authentication access-user maximum** command configuration takes effect only for new users.

Example

Set the maximum number of access users to 100 in the user access profile **profile_1**.

```
<HUAWEI> system-view
[HUAWEI] uni-mng
[HUAWEI-um] user-access-profile name profile_1
[HUAWEI-um-user-access-profile_1] authentication access-user maximum 100
```

3.5.24 auth-mode none

Function

The **auth-mode none** command sets the AS authentication mode to no authentication.

The **undo auth-mode** command restores the default AS authentication mode.

By default, authentication is required when an AS connects to an SVF system.

NOTE

This command can only be executed on a parent switch.

Format

auth-mode none

undo auth-mode

Parameters

None

Views

AS authentication view

Default Level

3: Management level

Usage Guidelines

By default, an AS needs to be authenticated using a blacklist or whitelist before connecting to an SVF system. You can also configure no authentication for ASs. In no authentication mode, an AS can connect to an SVF system regardless of whether it is in a blacklist or whitelist.

NOTE

Non-authentication has security risks. Therefore, authentication is recommended.

Example

Configure no authentication for ASs to connect to an SVF system.

```
<HUAWEI> system-view
[HUAWEI] as-auth
[HUAWEI-as-auth] auth-mode none
```

3.5.25 authentication-profile (user access profile view)

Function

The **authentication-profile** command binds an authentication profile to a user access profile.

The **undo authentication-profile** command deletes the authentication profile bound to a user access profile.

By default, no authentication profile is bound to a user access profile.

NOTE

This command can only be executed on a parent switch.

Format

authentication-profile *authentication-profile-name*

undo authentication-profile

Parameters

Parameter	Description	Value
authentication-profile-name	Specifies the name of an authentication profile.	The value is a string of 1-31 case-sensitive characters, which cannot be configured to - and --. It cannot contain spaces and the following symbols: / \ : * ? " < > | @ ' %.

Views

User access profile view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

After creating a user access profile, you can bind an authentication profile to the user access profile. When the user access profile is bound to an AS port, the user access authentication mode specified in the authentication profile is automatically configured on the AS port.

NAC provides three user authentication modes: 802.1X authentication, MAC address authentication, and Portal authentication. To implement user access authentication, run the **dot1x-access-profile name** *access-profile-name*, **mac-access-profile name** *access-profile-name*, and **portal-access-profile name** *access-profile-name* commands in the system view to create an access profile, bind one or multiple of the three user authentication modes to the authentication profile, and then bind the authentication profile to the user access profile in an SVF system.

Precautions

- If Portal authentication is deployed in an SVF system, you must run the **web-auth-server** *server-name* command to specify the Portal server template used in Portal authentication in the Portal access profile view. Additionally, only one Portal server template can be configured in a Portal access profile.
- If the Portal authentication mode has been set to **layer3** in the portal-access-profile bound to the authentication profile, it is not allowed to bind this authentication profile to the user access profile. If an authentication profile has been bound to the user access profile, it is now allowed to set the Portal authentication mode to **layer3**.
- In versions earlier than V200R019C10, user access profiles must be bound to the same authentication profile at any time. In V200R019C10 and later versions, user access profiles can be bound to different authentication profiles. However, if these user access profiles are bound to ASs on the same cascade port, the authentication profiles must be the same.

- The **authentication-profile** and **mac-limit maximum** *max-num* as well as **authentication-profile** and **traffic-limit inbound** { **arp** | **dhcp** } **cir** *cir-value* commands are mutually exclusive and cannot be configured together in a user access profile.
- If many users are connected to the port to which a user access profile is bound, the authentication configuration in the profile may need to take a certain period of time to complete.
- Before changing the authentication profile on the parent, run the **undo authentication-profile** command to delete the existing authentication profile and then run the **commit as** { **name** *as-name* | **all** } command to commit the configuration. You can then create a new authentication profile on the parent.
- After bidirectional flow control is configured in an authentication profile using the **authentication control-direction all** command, this authentication profile cannot be bound to a user access profile.
- In SVF of a version earlier than V200R019, access authentication is not supported for IPv6 users. In SVF of V200R019 or a later version, access authentication is supported for IPv6 users.
- In V200R019 and later versions, the **authentication ipv6-control enable** command configured in an authentication profile can be delivered to ASs. This command can take effect only in the following situations:
  - The parent is S6735-S, S6720-EI, or S6720S-EI, and ASs are S5720-LI, S5720S-LI, S5720I-SI, S5735-S, S5735S-S, S5735S-H, S5736-S, S6735-S, S6720-EI, S6720S-S, or S6720S-EI.
  - The parent is a modular switch and the parent's port to which the authentication profile is bound is not located on the ES0D0G24SA00, ES0D0G24CA00, LE0MG24CA, LE0MG24SA, LE1D2S04SEC0, LE1D2X32SEC0, LE1D2H02QEC0, or X series cards, and ASs are S5720-LI, S5720S-LI, S5720I-SI, S5735-S, S5735S-S, S5735S-H, S5736-S, S6735-S, S6720-EI, S6720S-S, or S6720S-EI.
- In V200R019 and later versions, the **authentication single-stack-control enable** command configured in an authentication profile can be delivered to ASs. This command can take effect only in the following situations:
  - The parent is S5531-H, S5731-H, S5731S-H, S5732-H, S6730-S, S6730S-S, S6730S-H, or S6730-H, and ASs are S5531-H, S5531-S, S5731-H, S5731S-H, S5732-H, S5731-S, S5731S-S, S6730-S, S6730S-S, S6730S-H, or S6730-H.
  - The parent is a modular switch and the parent's port to which the authentication profile is bound is located on the LE1D2S04SEC0, LE1D2X32SEC0, LE1D2H02QEC0, or X series cards, and ASs are S5731-H, S5731S-H, S5732-H, S5731-S, S5731S-S, S6730-S, S6730S-S, S6730S-H, or S6730-H.
- If an interface needs to be unbound from an authentication profile and there are many users on the interface, it takes a long time to unbind the interface from the authentication profile. To shorten the time, run the **authentication speed-limit max-num** command to increase the rate at which a specified AS sends user disassociation request messages.

Example

Bind an authentication profile to the user access profile.

```
<HUAWEI> system-view
[HUAWEI] mac-access-profile name 1
[HUAWEI-mac-access-profile-1] quit
[HUAWEI] authentication-profile name test
[HUAWEI-authen-profile-test] mac-access-profile 1
[HUAWEI-authen-profile-test] quit
[HUAWEI] uni-mng
[HUAWEI-um] user-access-profile name profile_1
[HUAWEI-um-user-access-profile_1] authentication-profile test
```

3.5.26 blacklist mac-address

Function

The **blacklist mac-address** command adds a specified MAC address to the blacklist.

The **undo blacklist mac-address** command deletes a MAC address from the blacklist.

By default, no MAC address is added to the blacklist. A maximum of 128 MAC addresses can be added to the blacklist.

NOTE

This command can only be executed on a parent switch.

Format

blacklist mac-address *mac-address1* [**to** *mac-address2*]

undo blacklist mac-address { *mac-address1* [**to** *mac-address2*] | **all** }

Parameters

Parameter	Description	Value
mac-address1 [**to** *mac-address2*]	Specifies the MAC address to be added to the blacklist.	The value is in H-H-H format, where H is a hexadecimal number of 1 to 4 digits. The value cannot be all 0s, all Fs, or a multicast MAC address.
all	Deletes all the MAC addresses in the blacklist.	-

Views

AS authentication view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

When an SVF system needs to authenticate an AS, the SVF system allows the AS to connect to if the MAC address of the AS is in the whitelist and disallows the AS to connect to if the MAC address is in the blacklist.

Precautions

- A MAC address cannot exist in both the whitelist and blacklist.
- By default, if the MAC address of an AS is neither in the whitelist nor in the blacklist, the AS fails the authentication. You can run the **confirm** { **all** | **mac-address** *mac-address* } command to allow all ASs or a specified AS to pass the authentication.
- If the MAC address of an AS that has connected to an SVF system is added to the blacklist, the AS restarts and exits from the SVF system.

Example

Add the MAC address 00e0-fc12-3456 to the blacklist.

```
<HUAWEI> system-view
[HUAWEI] as-auth
[HUAWEI-as-auth] blacklist mac-address 00e0-fc12-3456
```

3.5.27 broadcast-suppression (network enhanced profile view)

Function

The **broadcast-suppression** command configures broadcast traffic suppression in a network enhanced profile.

The **undo broadcast-suppression** command cancels broadcast traffic suppression in a network enhanced profile.

By default, broadcast traffic suppression is not configured in a network enhanced profile. By default, the percentage of broadcast traffic that can pass through an AS port is 50%.

NOTE

This command can only be executed on a parent switch.

Format

broadcast-suppression packets *packets-per-second*

undo broadcast-suppression

Parameters

Parameter	Description	Value
packets *packets-per-second*	Specifies the packet rate of an interface.	The value is an integer that ranges from 0 to 14881000, in packets per second (PPS). If the configured packet rate on the parent switch is larger than the maximum value on the AS port, the maximum value takes effect on the AS port.

Views

Network enhanced profile view

Default Level

3: Management level

Usage Guidelines

After creating a network enhanced profile, you can configure broadcast traffic suppression in the profile. After the profile is bound to an AS port, broadcast traffic suppression is automatically configured on the port. The following configuration is generated on the AS port:

```
#
 broadcast-suppression packets packets-per-second
#
```

To prevent broadcast storms, you can run the **broadcast-suppression** command to configure the maximum number of broadcast packets that can pass through a port. When the broadcast traffic rate reaches the maximum value, the system discards excess broadcast packets to control the traffic volume within a proper range.

Example

Configure broadcast traffic suppression in a network enhanced profile.

```
<HUAWEI> system-view
[HUAWEI] uni-mng
[HUAWEI-um] network-enhanced-profile name profile_1
[HUAWEI-um-net-enhanced-profile_1] broadcast-suppression packets 148810
```

3.5.28 clear direct-command

Function

The **clear direct-command** command deletes commands to be directly delivered to an AS from the parent.

NOTE

This command can only be executed on a parent switch.

Format

clear direct-command [**slot** *slot-id*]

Parameters

Parameter	Description	Value
slot *slot-id*	Specifies the stack ID of a member device in an AS.	The value is an integer that ranges from 0 to 4.

Views

AS view

Default Level

3: Management level

Usage Guidelines

After you run the **direct-command** command to directly deliver commands to an AS, you can run the **clear direct-command** command to delete the commands from the parent.

You can delete directly delivered commands only when the AS is offline. Do not run the **clear direct-command** command when the parent is delivering the commands to an AS.

Example

Delete the commands to be directly delivered to AS1 from the parent.

```
<HUAWEI> system-view
[HUAWEI] uni-mng
[HUAWEI-um] as name as1
[HUAWEI-um-as-as1] clear direct-command
```

3.5.29 commit as

Function

The **commit as** command delivers the service configuration to ASs.

NOTE

This command can only be executed on a parent switch.

Format

commit as { **name** *as-name* | **all** }

Parameters

Parameter	Description	Value
name *as-name*	Delivers the service configuration to an AS with a specified name.	The value must have an existing AS name.
all	Delivers the service configuration to all ASs.	-

Views

uni-mng view

Default Level

3: Management level

Usage Guidelines

After configuring or changing services (including service profiles and user authentication-free rules) on the parent, you need to run the **commit as** command to deliver the configuration to ASs to make the configuration take effect.

In versions earlier than V200R020C00, you do not need to configure an AS administrator before configuring an AS in centralized mode. However, in V200R020C00 and later versions, before configuring an AS in centralized mode, you have to configure an AS administrator and deliver it to the AS. Otherwise, the AS configuration will fail to be delivered. For details about how to configure an AS administrator, see Configuring Services for ASs Using an AS Administrator Profile.

Example

Deliver the service configuration to all ASs.

```
<HUAWEI> system-view
[HUAWEI] uni-mng
[HUAWEI-um] commit as all
```

3.5.30 confirm

Function

The **confirm** command confirms that unauthenticated ASs pass the authentication.

NOTE

This command can only be executed on a parent switch.

Format

confirm { **all** | **mac-address** *mac-address* }

Parameters

Parameter	Description	Value
all	Confirms that all ASs pass the authentication.	-
mac-address *mac-address*	Confirms that an AS with a specified MAC address passes the authentication.	The value is in H-H-H format, where H is a hexadecimal number of 1 to 4 digits. The value cannot be all 0s, all Fs, or a multicast MAC address.

Views

AS authentication view

Default Level

3: Management level

Usage Guidelines

When an AS needs to be authenticated before connecting to an SVF system, the AS fails the authentication if its MAC address is neither in the whitelist nor in the blacklist. You can run the **confirm** command to allow all ASs or a specified AS to pass the authentication.

You can run the **display as unauthorized record** command to check information about the ASs that fail the authentication.

Example

Confirm that the AS with the MAC address 00e0-fc12-3456 passes the authentication.

```
<HUAWEI> system-view
[HUAWEI] as-auth
[HUAWEI-as-auth] confirm mac-address 00e0-fc12-3456
```

3.5.31 description (Fabric-port view)

Function

The **description** command configures the description of a fabric port.

The **undo description** command deletes the description of a fabric port.

By default, no description is configured for a fabric port.

NOTE

This command can only be executed on a parent switch.

Format

description *description*

undo description

Parameters

Parameter	Description	Value
description	Specifies the description.	The value is a string of 1 to 64 case-sensitive characters with spaces supported.

Views

Fabric-port view

Default Level

2: Configuration level

Usage Guidelines

To facilitate fabric port management and identification, you can configure descriptions for fabric ports. For example, you can describe the name of an AS that connects to a fabric port.

Example

Configure the description of a fabric port.

```
<HUAWEI> system-view
[HUAWEI] uni-mng
[HUAWEI-um] interface fabric-port 1
[HUAWEI-um-fabric-port-1] description To_as1
```

3.5.32 description (port group view)

Function

The **description** command configures the description of a port group.

The **undo description** command deletes the description of a port group.

By default, a port group does not have a description.

NOTE

This command can only be executed on a parent switch.

Format

description *description*

undo description

Parameters

Parameter	Description	Value
description	Specifies the description.	The value is a string of 1 to 15 case-sensitive characters with spaces supported.

Views

Port group view

Default Level

2: Configuration level

Usage Guidelines

To facilitate identification and management of terminals connected to a port group in the web system, configure the description of the port group.

Example

Configure the description of a specified port group.

```
<HUAWEI> system-view
[HUAWEI] uni-mng
[HUAWEI-um] port-group name 1
[HUAWEI-um-portgroup-1] description switch
```

3.5.33 dhcp snooping enable (network enhanced profile view)

Function

The **dhcp snooping enable** command configures DHCP snooping in a network enhanced profile.

The **undo dhcp snooping enable** command cancels DHCP snooping in a network enhanced profile.

By default, DHCP snooping is not configured in a network enhanced profile.

NOTE

This command can only be executed on a parent switch.

Format

dhcp snooping enable

undo dhcp snooping enable

Parameters

None

Views

Network enhanced profile view

Default Level

3: Management level

Usage Guidelines

After creating a network enhanced profile, you can configure DHCP snooping in the profile. After the profile is bound to an AS port, DHCP snooping is automatically enabled on the AS and AS port. The following configuration is generated on the AS:

```
#
dhcp enable
#
dhcp snooping enable
#
interface GigabitEthernet0/0/1
 dhcp snooping enable
#
```

In the preceding configuration, GigabitEthernet0/0/1 is used for reference only. The actual configuration depends on the profile configuration.

You can run the **dhcp snooping enable** command to enable DHCP snooping on a port so as to improve DHCP security.

Precautions

Before running the **undo dhcp snooping enable** command, ensure that the network enhanced profile view is not configured with IPSG or DAI. To disable IPSG and DAI, run the **undo ip source check user-bind enable (network enhanced profile view)** and **undo arp anti-attack check user-bind enable (network enhanced profile view)** commands respectively.

The **dhcp snooping enable** command configured in the network enhanced profile can only configure a DHCP dynamic binding table but not a DHCP static binding table.

Example

Configure DHCP snooping in a network enhanced profile.

```
<HUAWEI> system-view
[HUAWEI] uni-mng
[HUAWEI-um] network-enhanced-profile name profile_1
[HUAWEI-um-net-enhanced-profile_1] dhcp snooping enable
```

3.5.34 direct-command

Function

The **direct-command** command configures ASs on the parent. The parent directly delivers the configuration to the ASs, and you do not need to run the **commit as** command.

The **undo direct-command** command cancels the configuration for ASs on the parent.

The following table lists the service configurations that can be delivered using the **direct-command** command. If no configuration dependency and restriction are provided for a command, see the details in the command reference.

NOTE

This command can only be executed on a parent switch.

Format

direct-command view { **system** | **eth-trunk** *trunk-id* | *interface-type interface-number* | **stack-port** *member-id/port-id* } **command** *command-text*

undo direct-command view { **system** | **eth-trunk** *trunk-id* | *interface-type interface-number* | **stack-port** *member-id/port-id* } **command** *command-text*

Parameters

Parameter	Description	Value
view { **system** | **eth-trunk** *trunk-id* | *interface-type interface-number* | **stack-port** *member-id/port-id* }	Specifies the view in which a command is executed. • **system**: system view • *interface-type interface-number*: interface view • **stack-port** *member-id/port-id*: stack port view • **eth-trunk** *trunk-id*: Eth-Trunk interface view	-
command *command-text*	Specifies the command to be delivered to ASs.	The value is a string of 1 to 128 characters. This command does not support auto-completion of keywords by pressing Tab.

Views

AS view

Default Level

3: Management level

Usage Guidelines

- When you configure a directly delivered command on the parent, enter the complete and correct command instead of the abbreviated form. No info message is displayed for confirming your input.
- A directly delivered command supports the help and typeahead functions but not real-time check during input. The system checks the input only after you complete typing a command and press **Enter**. No detailed description is provided in help information. If you fail to configure a command for an AS, an info message is displayed.
- When you configure a directly delivered command, the AS to which the command is to be delivered must be online. If you need to specify a port or *slot-id* in a command, the corresponding member device must be available. If the AS is offline, run the **clear direct-command** command to delete the completed configuration on the parent.
- If a port has the configuration directly delivered using commands, the port cannot be configured as a member port of the Eth-Trunk to which a fabric port is bound. If a port has been configured as a member port of the Eth-Trunk to which a fabric port is bound, the configuration cannot be directly delivered to the port using commands.
- Directly delivering configuration using commands and delivering configuration using service profiles are mutually exclusive and cannot be performed simultaneously.
- In versions earlier than V200R019C00, a maximum of 4096 commands can be configured. In V200R019C00 and later versions, a maximum of 8192 commands can be configured.
- In versions earlier than V200R020C00, you do not need to configure an AS administrator before configuring an AS in centralized mode. However, in V200R020C00 and later versions, before configuring an AS in centralized mode, you have to configure an AS administrator and deliver it to the AS. Otherwise, the AS configuration will fail to be delivered. For details about how to configure an AS administrator, see Configuring Services for ASs Using an AS Administrator Profile.
- The following lists the commands that can be directly delivered to ASs. You can run the **undo direct-command view** { **system** | *interface-type interface-number* } **command** *command-text* command to cancel the configuration or restore default settings. The *command-text* parameter specifies the commands listed in the following table.

Service Category	Format	View	Function	Configuration Dependency and Restriction
Energy-saving management	**port-auto-sleep enable**	Interface view	Enables the port sleeping function on an electrical interface.	Currently, this command can be used on electrical interfaces (excluding MultiGE interfaces) and combo interfaces working as electrical interfaces.
PoE	**poe force-power**	Interface view	Enables forcible PoE power supply on an interface.	-
	poe legacy enable	Interface view	Enables an interface to check compatibility of PDs.	-
	poe priority { **critical** | **high** | **low** }	Interface view	Sets the power supply priority of a PoE interface.	-
	poe af-inrush enable slot *slot-id*	System view	Configures the IEEE 802.3at-compliant device to provide power in accordance with IEEE 802.3af.	-

Service Category	Format	View	Function	Configuration Dependency and Restriction
	poe high-inrush enable slot *slot-id*	System view	Configures a device to allow high inrush current during power-on.	-
	undo poe enable (supported in V200R011C10 and later versions)	Interface view	Disables the PoE function on an interface.	-
Ethernet interfaces	**undo negotiation auto**	Interface view	Configures an interface to work in non-auto negotiation mode. After you run the **undo direct-command** command, the interface works in auto negotiation mode.	• This command cannot be configured on combo interfaces. • Do not cancel the **undo negotiation auto** command when **speed** or **duplex** is specified.
	speed { **10** | **100** | **1000** | **2500** | **5000** | **10000** }	Interface view	Sets the rate in non-auto negotiation mode.	• This command cannot be configured on combo interfaces. • Ensure that the interface works in non-auto negotiation mode before configuring this command.

Service Category	Format	View	Function	Configuration Dependency and Restriction
	speed auto-negotiation	Interface view	Enables auto-negotiation on a GE optical interface.	• Support for this command varies depending on switch models. For details, see the **speed auto-negotiation** command in the *Command Reference - Interface Management Commands - Ethernet Interface Configuration Commands*. • Ensure that the interface works in auto-negotiation mode before configuring this command.

Service Category	Format	View	Function	Configuration Dependency and Restriction
	duplex { **full** | **half** }	Interface view	Sets the duplex mode for an electrical interface in non-auto negotiation mode.	• This command cannot be configured on combo interfaces. • Ensure that the interface works in non-auto negotiation mode before configuring this command. • When the working rate of a GE electrical interface is 1000 Mbit/s, the interface supports only the full duplex mode.
	loopback internal	Interface view	Configures a loopback detection mode on an interface.	-

Service Category	Format	View	Function	Configuration Dependency and Restriction
	description *description* (supported in V200R011C10 and later versions)	Interface view	Configures the description for an interface.	The description contains a maximum of 52 characters in V200R011C10, and the description contains a maximum of 116 characters in V200R012C00 and later versions.
Eth-Trunk interface	**description** *description* (supported in V200R019C00 and later versions)	Eth-Trunk interface view	Configures the description for an Eth-Trunk interface.	The description contains a maximum of 116 characters. The description can be configured for a service Eth-Trunk interface or an Eth-Trunk interface used in an SVF system to connect upstream and downstream devices. The description cannot be configured for Eth-Trunk0.

Service Category	Format	View	Function	Configuration Dependency and Restriction
Port bridge	**port bridge enable**	Interface view	Enables the bridging function on an interface.	-

Service Category	Format	View	Function	Configuration Dependency and Restriction
Port Security (supported in V200R019C00 and later versions)	**port-security max-mac-num** *max-number*	Interface view	Sets the maximum number of secure MAC addresses that can be learned on an interface.	• The **port-security max-mac-num** *max-number* command in direct configuration mode is mutually exclusive with the **mac-limit maximum** *max-num* command configured in a user access profile and cannot be both configured. • Port security (and sticky MAC if needed) must be enabled in a network enhanced profile, and then run the **direct-command** command to deliver this command.

Service Category	Format	View	Function	Configuration Dependency and Restriction
	port-security mac-address sticky *mac-address* **vlan** *vlan-id*	Interface view	Configures a sticky MAC address entry.	Port security and sticky MAC must be enabled in a network enhanced profile, and then run the **direct-command** command to deliver this command.
	save sticky-mac configuration	System view	Saves the sticky MAC addresses on an AS to a file named unimng-xxxx.ztbl. *xxxx* in the file name represents the management MAC address of the AS.	-
Voice VLAN	**voice-vlan mac-address** *mac-address* **mask** *mask* (supported in V200R011C10 and later versions)	System view	Configures the OUI address of the voice VLAN.	-
LBDT	**loopback-detect enable**	Interface view	Enables loopback detection on an interface.	-

Service Category	Format	View	Function	Configuration Dependency and Restriction
	loopback-detect packet vlan *vlan-id*	Interface view	Enables loopback detection for a specified VLAN.	If you configure this command multiple times, loopback detection is enabled for multiple VLANs.

Service Category	Format	View	Function	Configuration Dependency and Restriction
ARP rate limiting	**arp speed-limit source-mac maximum** *maximum*	System view	Configures ARP rate limiting based on source MAC addresses.	• Only some models support this command. For details, see the **arp speed-limit source-mac** command in the *Command Reference - Security Commands - ARP Security Configuration Commands*. • The value of **maximum** *maximum* ranges from 0 to 256. • This function takes effect only for the ARP packets sent to the CPU.

Service Category	Format	View	Function	Configuration Dependency and Restriction
	arp speed-limit source-ip maximum *maximum*	System view	Configures ARP rate limiting based on source IP addresses.	• The value of **maximum** *maximum* ranges from 0 to 256. • This function takes effect only for the ARP packets sent to the CPU.
Stack	**port interface** { *interface-type interface-number1* [**to** *interface-type interface-number2*] } **enable** (supported in V200R010 and later versions)	Stack interface view: **stack-port** *member-id/port-id*	Configures a service interface as a stack member port and adds it to a stack port.	Before restoring the stack member ports that are added to a stack port in direct configuration mode as common service interfaces, you do not need to run the **shutdown interface** command in the stack interface view.
	stack slot *slot-id* **priority** *priority* (supported in V200R010 and later versions)	System view	Sets a stack priority for a member switch in a stack.	-

Service Category	Format	View	Function	Configuration Dependency and Restriction
	stack slot *slot-id* **renumber** *new-slot-id* (supported in V200R011C10 and later versions)	System view	Changes the stack ID of a specified member switch in a stack. **NOTICE** If there are services running, delivering this command may cause service interruptions and configuration loss. Therefore, you are advised to deliver this command when an AS is unconfigured.	A stack ID cannot be changed in the following situations: ● The switch is a standalone switch that does not join any stack. ● The newly configured stack ID is an existing stack ID of a specified member switch in a stack. ● Ports with the specified *slot-id* have been configured as member ports of an uplink fabric port. ● Ports with the specified *slot-id* have been configured as member ports of a downlink

Service Category	Format	View	Function	Configuration Dependency and Restriction
				fabric port.

Service Category	Format	View	Function	Configuration Dependency and Restriction
User Access and Authentication (supported in V200R012C00 and later versions)	**access-user arp-detect vlan** *vlan-id* **ip-address** *ip-address* **mac-address** *mac-address*	System view	Sets the source IP address and source MAC address of offline detection packets in a VLAN.	• In other V200R012C00 versions except V200R012C00SPC710, this command can be configured only one. If you want to modify the configuration, delete the existing configuration and then perform the configuration again. • In V200R012C00SPC710 and V200R013C00, when **vlan**, **ip-address**, and **mac-address** are all different, multiple configurations of this command can be generated.

Service Category	Format	View	Function	Configuration Dependency and Restriction
				If any one of **vlan**, **ip-address**, and **mac-address** has been configured, delete the existing configuration before reconfiguring them. ● In V200R019 and later versions, multiple configurations of this command can be generated regardless of whether the VLAN, IP address, and MAC address are the same. You do not need to delete the existing configuration. If the newly configured VLAN is the same as the

Service Category	Format	View	Function	Configuration Dependency and Restriction
				existing one, the IP address and MAC address in the original configuration are replaced with the newly configured IP address and MAC address. If the newly configured VLAN is different from the existing one, a new configuration is generated.
	access-user arp-detect default ip-address *ip-address*	System view	Sets the default source IP address of offline detection packets.	-
	undo user-detect	System view	Disables the online user detection function.	-

Service Category	Format	View	Function	Configuration Dependency and Restriction
	authentication speed-limit max-num *max-num-value* **interval** *interval-value* (supported in V200R013C00 and later versions)	System view	Configures the rate limit for an access device to send user association and disassociation request messages.	-
	access-user arp-detect fallback ip-address *mask-length* (supported in V200R013C00 and later versions)	System view	Configures an IP address required for calculating the source address of offline detection packets.	If you run this command multiple times, only the latest configuration takes effect.
	access-user arp-detect delay *delay* (supported in V200R013C00 and later versions)	System view	Configures the delay for sending offline detection packets.	-
	static-user *start-ip-address* [*end-ip-address*] [**mac-address** *mac-address* | **vlan** *vlan-id*] (supported in V200R019C00 and later versions)	System view	Configures a static user.	If the IP address of a static user is set to an IP address range, any IP address in this address range cannot be modified or deleted.

Example

Configure the parent to deliver the **loopback-detect enable** command to GigabitEthernet0/0/1 on **as1** to enable loopback detection on GigabitEthernet0/0/1.

```
<HUAWEI> system-view
[HUAWEI] uni-mng
```



```
[HUAWEI-um] as name as1
[HUAWEI-um-as-as1] direct-command view gigabitethernet 0/0/1 command loopback-detect enable
```

3.5.35 display as

Function

The **display as** command displays information about access switches (ASs).

NOTE

This command can only be executed on a parent switch.

Format

display as { **all** | **name** *as-name* | **mac-address** *mac-address* | **vpn-instance information** }

Parameters

Parameter	Description	Value
all	Displays information about all ASs.	-
name *as-name*	Specifies the name of an AS.	The value must have an existing AS name.
mac-address *mac-address*	Specifies the MAC address of an AS.	The value is in H-H-H format, where H is a hexadecimal number of 1 to 4 digits. The value cannot be all 0s, all Fs, or a multicast MAC address.
vpn-instance information	Displays VPN instance information.	The value must be an existing VPN instance name.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display as** command to view information about ASs in an SVF system, including the AS device type, VPN instance information, and access status.

Example

Display information about all ASs.

```
<HUAWEI> display as all
Total: 1, Normal: 1, Fault: 0, Idle: 0, Version mismatch: 0
--------------------------------------------------------------------------------
No.  Type          MAC            IP              State       Name
--------------------------------------------------------------------------------
0    S5720-P-LI    00e0-fcbb-cc92 192.168.11.254  normal      as1
--------------------------------------------------------------------------------
```

Table 3-86 Description of the **display as all** command output

Item	Description
Total	Total number of ASs.
Normal	Number of ASs that are running normally.
Fault	Number of ASs in abnormal running status.
Idle	Number of ASs that have been configured but no gone online.
Version mismatch	Number of ASs of which the software versions do not match the software version of the parent.
No.	Sequence number.
Type	Device type of an AS.
MAC	Management MAC address of an AS.
IP	IP address of an AS.
State	Status of an AS: • idle: The AS is in initial state. • normal: The AS has gone online and connected to an SVF system. • fault: The AS does not connect to an SVF system. • version mismatch: The V, R, or C versions of the AS and parent are inconsistent.
Name	Name of an AS.

Display information about the AS **as1**.

```
<HUAWEI> display as name as1
--------------------------------------------------------------------------------
Management MAC       : 00e0-fcbb-cc92
System MAC           : 00e0-fcbb-cc92
```



```
ESN                 : 210235317310xxxxxxxx
Name                  : as1
Model               : S5720-28P-LI-AC
Device type           : S5720-P-LI
State               : normal
Mode                  : centralized
Slot                : 0
AS group              : group1
Port group            : group2
------------------------------------------------------------------------------
```

Table 3-87 Description of the **display as name** command output

Item	Description
Management MAC	Management MAC address of an AS. In a Super Virtual Fabric (SVF) system, each AS has a unique management MAC address to identify itself. To set a management MAC address for an AS, run the **as access manage-mac** command. If no management MAC address is configured for an AS, the system MAC address of the AS is used as the management MAC address.
System MAC	System MAC address of an AS, which is the physical MAC address of this AS.
ESN	Sequence number of an AS.
Name	Name of an AS.
Model	Device model of an AS.
Device type	Device type of an AS.
State	Status of an AS: • idle: The AS is in initial state. • normal: The AS has gone online and connected to an SVF system. • fault: The AS does not connect to an SVF system. • version mismatch: The V, R, or C versions of the AS and parent are inconsistent.
Mode	Service configuration mode of an AS: • centralized: indicates the centralized mode. • independent: indicates the independent mode.
Slot	Stack ID of an AS in a stack.
AS group	AS group to which an AS belongs.

Item	Description
Port group	Port group to which an AS port belongs.

Display VPN instance information of ASs.

```
<HUAWEI> display as vpn-instance information
Total: 5
------------------------------------------------------------------------------
No.  VPN-Instance                AS Name
------------------------------------------------------------------------------
0    VPN1                        e-10005(1-1)
1    --                         t-10018(2-2)
2    VPN2                        s-10021(1-1)
3    --                         6-10023(2-1)
4    --                         11-t-16(x-s)
------------------------------------------------------------------------------
```

Table 3-88 Description of the **display as vpn-instance information** command output

Item	Description
Total	Number of ASs.
No.	AS number.
VPN-Instance	VPN instance name.
AS Name	AS name.

3.5.36 display as access configuration

Function

The **display as access configuration** command displays the access configuration of ASs.

NOTE

Only the switches that function as ASs support this command.

Format

display as access configuration

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display as access configuration** command on an AS to check the access configuration of the AS.

Example

Display the access configuration of an AS.

```
<HUAWEI> display as access configuration
  AS mode                          : centralized
  Access interface                 : vlanif11
  Access controller configuration  : --
  Current connected access controller : 192.168.11.1(dynamic)
  Access management MAC            : xxxx-xxxx-xxxx
  Access system MAC                : xxxx-xxxx-xxxx
  Current connected state          : normal
```

Table 3-89 Description of the **display as access configuration** command output

Item	Description
AS mode	AS mode: • disable: The device works in parent mode. To change the device working mode, run the **as-mode disable** command. • enable: The device works in AS mode, but it does not have the SVF function enabled using the **uni-mng** command. • centralized: The device works in AS mode and the service configuration mode is centralized mode. • independent: The device works in AS mode and the service configuration mode is independent mode.
Access interface	VLANIF interface for the management VLAN of an AS.
Access controller configuration	Parent IP address configured using the **as access controller ip-address** command. If this IP address is configured, the **Current connected access controller** field value contains configured.

Item	Description
Current connected access controller	IP address of the parent to which an AS is connected. If this field contains dynamic, the IP address is obtained through DHCP or in broadcast mode. If this field contains configured, the IP address is statically configured. If an AS does not go online, this field displays --.
Access management MAC	Configured management MAC address of an AS.
Access system MAC	System MAC address of an AS.
Current connected state	Connection status of an AS: ● idle: The AS is in initial state. ● normal: The AS has gone online and connected to an SVF system. ● fault: The AS does not connect to an SVF system. ● version mismatch: The V, R, or C versions of the AS and parent are inconsistent.

3.5.37 display as blacklist

Function

The **display as blacklist** command displays blacklist information of an AS.

NOTE

This command can only be executed on a parent switch.

Format

display as blacklist

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display as blacklist** command to check blacklist information of an AS.

Example

Display blacklist information of an AS.

```
<HUAWEI> display as blacklist
--------------------------------------------------------------------------------
ID     MAC
--------------------------------------------------------------------------------
0      xxxx-xxxx-xxxx
--------------------------------------------------------------------------------
Total: 1
```

Table 3-90 Description of the **display as blacklist** command output

Item	Description
ID	ID of a blacklist.
MAC	MAC address added to the blacklist. To add a MAC address to a blacklist, run the **blacklist mac-address** command. If no MAC address is specified, no information is displayed.

3.5.38 display as run-info

Function

The **display as run-info** command displays running status information of an AS.

NOTE

This command can only be executed on a parent switch.

Format

display as { **name** *as-name* | **mac-address** *mac-address* } **run-info**

Parameters

Parameter	Description	Value
name *as-name*	Specifies the name of an AS.	The value must have an existing AS name.

Parameter	Description	Value
mac-address *mac-address*	Specifies the MAC address of an AS.	The value is in H-H-H format, where H is a hexadecimal number of 1 to 4 digits. The value cannot be all 0s, all Fs, or a multicast MAC address.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display as run-info** command to check running status information of an AS, including the AS access status, CPU usage, and memory usage.

Example

Display running status information of an AS.

```
<HUAWEI> display as name as1 run-info
Info: This operation may take a few seconds. Please wait...
------------------------------------------------------------------------------
Software version     : Version 5.170 V200R023C00
Hardware version     : VER.A
Patch version        : --
Patch state          : running
IP address           : 192.168.1.154
IP mask              : 255.255.255.0
Gateway              : 192.168.1.1
VPN-Instance         : --
State                : normal
Online time          : 1 day, 18 hours, 40 minutes, 0 second
CPU usage            : 12%
Memory usage         : 52%
Slot 0               : present
------------------------------------------------------------------------------
```

Table 3-91 Description of the **display as run-info** command output

Item	Description
Software version	Software version running on an AS.
Hardware version	Hardware version running on an AS.
Patch version	Patch version. This field displays-- when the patch package is not installed.

Item	Description
Patch state	Patch status. • Running: The patch is running. • not running: The patch is not running.
IP address	IP address of an AS.
IP mask	Subnet mask.
Gateway	Gateway of an AS.
VPN-Instance	Name of a VPN instance.
State	Status of an AS: • idle: The AS is in initial state. • normal: The AS has gone online and connected to an SVF system. • fault: The AS does not connect to an SVF system. • version mismatch: The V, R, or C versions of the AS and parent are inconsistent.
Online time	Online time of an AS.
CPU usage	CPU usage of an AS.
Memory usage	Memory usage of an AS.
Slot 0	Whether an AS member device is present: • present • absent

3.5.39 display as unauthorized record

Function

The **display as unauthorized record** command displays information about the ASs that fail the authentication.

NOTE

This command can only be executed on a parent switch.

Format

display as unauthorized record

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display as unauthorized record** command to check information about the ASs that fail the authentication.

Example

Display information about the ASs that fail the authentication.

```
<HUAWEI> display as unauthorized record
Unauthorized AS record:
--------------------------------------------------------------------------------
AS type        : S5720-SI
Host name      : host
AS MAC address : xxxx-xxxx-xxxx
AS IP address  : 192.168.1.253
Record time    : 2023-02-20 16:06:10 DST
--------------------------------------------------------------------------------
Total: 1
```

Table 3-92 Description of the **display as unauthorized record** command output

Item	Description
AS type	Device type of an AS.
Host name	Name of the AS.
AS MAC address	MAC address of the AS.
AS IP address	IP address of the AS.
Record time	Time when the AS is authenticated.

3.5.40 display as whitelist

Function

The **display as whitelist** command displays whitelist information of an AS.

NOTE

This command can only be executed on a parent switch.

Format

display as whitelist

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display as whitelist** command to check whitelist information of an AS.

Example

Display whitelist information of an AS.

```
<HUAWEI> display as whitelist
--------------------------------------------------------------------------------
ID     MAC
--------------------------------------------------------------------------------
0      00e0-fc07-8282
--------------------------------------------------------------------------------
Total: 1
```

Table 3-93 Description of the **display as whitelist** command output

Item	Description
ID	ID of a whitelist.
MAC	MAC address added to the whitelist.

3.5.41 display uni-mng as-discover packet statistics

Function

The **display uni-mng as-discover packet statistics** command displays AS Discovery packet statistics on a fabric port.

NOTE

This command can be used on the parent or an AS. After running this command, you can check AS Discovery packet statistics on a fabric port of the local device.

Format

display uni-mng as-discover packet statistics interface fabric-port *port-id*

Parameters

Parameter	Description	Value
interface fabric-port *port-id*	Specifies the number of a fabric port.	The value is an integer that ranges from 0 to 63 on an AS and the value range on the parent varies depending on the switch model: • S12700/S12700E: 0 to 255 • MCUD/SRUK/MFUX/MPUE/SRUE/SRUHA1/SRUHX1/SRUH: 0 to 255 • Other switch models: 0 to 63

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display uni-mng as-discover packet statistics** command to check AS Discovery packet statistics on a fabric port.

Example

Display AS Discovery packet statistics on a fabric port.

```
<HUAWEI> display uni-mng as-discover packet statistics interface fabric-port 1
The statistics of AS Discover packet on Fabric-port1:

PortName     Packet-type                 Receive        Send
--------------------------------------------------------------------------------
GE2/0/23     AS Discover Request           0              3
             AS Discover ACK              3              0
             AS Discover ParaSyn Req      0              3
             AS Discover ParaSyn ACK      3              0
             AS Discover HeartBeat Req    0              11238
             AS Discover HeartBeat ACK    11238          0
             AS Discover NAK              0              0
             AS Discover FabricCfg Req    0              0
             AS Discover FabricCfg ACK    0              0
             AS Discover NotifyOffline Req  0            0
             AS Discover NotifyOffline ACK  0            0
--------------------------------------------------------------------------------
```


Table 3-94 Description of the **display uni-mng as-discover packet statistics** command output

Item	Description
PortName	Name of a member port in a fabric port.
Packet-type	Packet type: • AS Discover Request: neighbor discovery request packet • AS Discover Request: neighbor discovery request packet • AS Discover ParaSyn Req: neighbor discovery parameter synchronization packet • AS Discover ParaSyn ACK: neighbor discovery parameter synchronization response packet • AS Discover HeartBeat Req: neighbor discovery heart packet • AS Discover HeartBeat ACK: neighbor discovery heart response packet • AS Discover NAK: neighbor discovery error packet • AS Discover FabricCfg Req: neighbor discovery AS fabric port configuration packet • AS Discover FabricCfg ACK: neighbor discovery AS fabric port configuration response packet • AS Discover NotifyOffline Req: request packet that notifies AS offline • AS Discover NotifyOffline ACK: response packet of the request that notifies AS offline
Receive	Statistics about received packets. Statistics about AS Discover HeartBeat Req and AS Discover HeartBeat ACK packets will be cleared and start from 0 after an active/standby switchover is performed on the device.

Item	Description
Send	Statistics about sent packets. Statistics about AS Discover HeartBeat Req and AS Discover HeartBeat ACK packets will be cleared and start from 0 after an active/standby switchover is performed on the device.

3.5.42 display uni-mng as-group

Function

The **display uni-mng as-group** command displays information about AS groups.

NOTE

This command can only be executed on a parent switch.

Format

display uni-mng as-group [**name** *group-name* | **verbose**]

Parameters

Parameter	Description	Value
name *group-name*	Specifies the name of an AS group.	The value must be an existing an AS group name.
verbose	Displays detailed information about an AS group.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display uni-mng as-group** command to check information about created AS groups.

Example

Display brief information about all AS groups.

```
<HUAWEI> display uni-mng as-group

------------------------------------------------------------------------------
 Number                    AS-group Name
------------------------------------------------------------------------------
 1                         asgroup
------------------------------------------------------------------------------
```

Table 3-95 Description of the **display uni-mng as-group** command output

Item	Description
Number	Sequence number.
AS-group Name	AS group name.

Display detailed information about all AS groups.

```
<HUAWEI> display uni-mng as-group verbose

AS-group name: asgroup
------------------------------------------------------------------------------
AS name list: (Total number = 1)
 as1
------------------------------------------------------------------------------
AS-admin profile name: admin
------------------------------------------------------------------------------
```

Table 3-96 Description of the **display uni-mng as-group verbose** command output

Item	Description
AS-group name	AS group name.
AS name list	List of ASs added to an AS group.
AS-admin profile name	Name of the bound AS administrator profile.

3.5.43 display uni-mng as index

Function

The **display uni-mng as index** command displays the index of an AS.

NOTE

This command can only be executed on a parent switch.

Format

display uni-mng as index

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display uni-mng as index** command to check the index, management MAC address, and name of an AS.

Example

Display the index of an AS.

```
<HUAWEI> display uni-mng as index
Total number : 1
-------------------------------------------------------------------------------
Index     MAC-Current         MAC-Saved         Name
-------------------------------------------------------------------------------
1         00e0-fc12-3456      00e0-fc12-3456    as1
-------------------------------------------------------------------------------
```

Table 3-97 Description of the **display uni-mng as index** command output

Item	Description
Index	Index of an AS.
MAC-Current	Management MAC address.

Item	Description
MAC-Saved	MAC address saved in the flash memory. This field indicates the MAC address saved in the flash memory using the **save** command after an AS goes online or the **as name (uni-mng view)** command is configured. • If this field displays --, the **save** command is not executed after an AS goes online or the **as name (uni-mng view)** command is configured. • When **MAC-Current** and **MAC-Saved** are inconsistent, the **save** command is not executed after an AS is replaced or the **as name (uni-mng view)** command is configured.
Name	Name of an AS.

3.5.44 display uni-mng as interface brief

Function

The **display uni-mng as interface brief** command displays brief information about AS ports.

NOTE

This command can only be executed on a parent switch.

Format

display uni-mng as name *as-name* **interface brief**

Parameters

Parameter	Description	Value
name *as-name*	Specifies the name of an AS.	The value must have an existing AS name.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display uni-mng as interface brief** command to check brief information about AS ports.

When an AS is offline or its version is inconsistent with the parent version, this command displays default attributes of ports on this AS.

Example

Display brief information about AS ports.

```
<HUAWEI> display uni-mng as name as1 interface brief
PHY: Physical
*down      : administratively down
*Stack Port: inactive stack port
--------------------------------------------------------------------------------
Interface                Type           PHY      Online       MSTP state
--------------------------------------------------------------------------------
Eth-Trunk1               Fabric Port    up       present      forwarding
Eth-Trunk40              Service Port   down     present      discarding
GigabitEthernet0/0/1     Service Port   down     present      discarding
GigabitEthernet0/0/2     Service Port   up       present      forwarding
GigabitEthernet0/0/3     Service Port   down     present      discarding
GigabitEthernet0/0/4     Service Port   down     present      discarding
GigabitEthernet0/0/5     Service Port   down     present      discarding
GigabitEthernet0/0/6     Service Port   down     present      discarding
GigabitEthernet0/0/7     Service Port   down     present      discarding
GigabitEthernet0/0/8     Service Port   down     present      discarding
GigabitEthernet0/0/9     Service Port   down     present      discarding
GigabitEthernet0/0/10    Service Port   down     present      discarding
GigabitEthernet0/0/11    Service Port   down     present      discarding
GigabitEthernet0/0/12    Service Port   down     present      discarding
GigabitEthernet0/0/13    Service Port   down     present      discarding
GigabitEthernet0/0/14    Service Port   down     present      discarding
GigabitEthernet0/0/15    Service Port   down     present      discarding
GigabitEthernet0/0/16    Service Port   down     present      discarding
GigabitEthernet0/0/17    Service Port   down     present      discarding
GigabitEthernet0/0/18    Service Port   down     present      discarding
GigabitEthernet0/0/19    Service Port   down     present      discarding
GigabitEthernet0/0/20    Service Port   down     present      discarding
GigabitEthernet0/0/21    Service Port   down     present      discarding
GigabitEthernet0/0/22    Service Port   down     present      discarding
GigabitEthernet0/0/23    Service Port   down     present      discarding
GigabitEthernet0/0/24    Service Port   down     present      discarding
GigabitEthernet0/0/25    Fabric Port    down     present      discarding
GigabitEthernet0/0/26    Fabric Port    up       present      forwarding
GigabitEthernet0/0/27    Fabric Port    down     present      discarding
GigabitEthernet0/0/28    Fabric Port    up       present      discarding
--------------------------------------------------------------------------------
```

Table 3-98 Description of the **display uni-mng as interface brief** command output

Item	Description
Interface	Interface number.

Item	Description
Type	Interface type: • Service Port: indicates a service port. • Stack Port: indicates a physical stack member port. • Fabric Port: indicates a member port of a fabric port. • *Stack Port: indicates a stack member port that does not take effect.
PHY	Interface status: • up: The interface is Up. • down: The interface is Down. • *down: The administrator shuts down the interface.
Online	Whether the card where the interface resides is present: • present • absent
MSTP state	STP forwarding status of the interface: • disabled • discarding • learning • forwarding • --: The interface is absent or a physical stack member port. If the interface is an Eth-Trunk member port, this field displays the forwarding state of the Eth-Trunk.

3.5.45 display uni-mng as interface eth-trunk

Function

The **display uni-mng as interface eth-trunk** command displays information about an Eth-Trunk interface of an AS.

NOTE

This command can only be executed on a parent switch.

Format

display uni-mng as name *as-name* **interface eth-trunk** *eth-trunk-id*

Parameters

Parameter	Description	Value
name *as-name*	Specifies the name of an AS.	The value must have an existing AS name.
eth-trunk-id	Specifies the ID of an Eth-Trunk.	The value range varies depending on the device.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After you use the **uni eth-trunk** command to create an Eth-Trunk on an AS, you can run the **display uni-mng as interface eth-trunk** command to view information including the Eth-Trunk working mode, member interface, and member interface status.

Example

Display information about Eth-Trunk 40 on AS as1.

```
<HUAWEI> display uni-mng as name as1 interface eth-trunk 40
Eth-Trunk40's state information is:
WorkingMode: NORMAL
Operate status: down
--------------------------------------------------------------------------------
PortName                Status
GigabitEthernet0/0/10   down
GigabitEthernet0/0/11   down
--------------------------------------------------------------------------------
The Number of Ports in Trunk : 2
The Number of UP Ports in Trunk : 0
```

Table 3-99 Description of the **display uni-mng as interface eth-trunk** command output

Item	Description
Eth-Trunk40's state information is	State information of Eth-Trunk 40.

Item	Description
WorkingMode	Working mode of the Eth-Trunk interface: ● NORMAL: manual mode ● LACP: LACP mode. To set the LACP mode, specify the **mode lacp** parameter when running the **uni eth-trunk** command to create an Eth-Trunk.
Operate status	Status of the Eth-Trunk interface: ● down: The interface is Down. ● up: The interface is Up.
PortName	Eth-Trunk member interface name. To add or delete an Eth-Trunk member interface, run the **port eth-trunk trunkmember** command.
Status	Eth-Trunk member interface status: ● down: The member interface is Down. ● up: The member interface is Up.
The Number of Ports in Trunk	Number of Eth-Trunk member interfaces.
The Number of UP Ports in Trunk	Number of Eth-Trunk member interfaces in Up state.

3.5.46 display uni-mng authen-user

Function

The **display uni-mng authen-user** command displays authenticated user information on an AS.

NOTE

This command can be used on the parent or an AS.

Format

display uni-mng authen-user [**as name** *as-name*]

Parameters

Parameter	Description	Value
as name *as-name*	Specifies the name of an AS. **NOTE** This parameter can be specified only when the command is run on the parent.	The value must be the name of an online AS.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display uni-mng authen-user** command to view authenticated user information on an AS.

Example

Display authenticated user information on the AS named **test1**.

```
<HUAWEI> display uni-mng authen-user as name test1
Total: 5
--------------------------------------------------------------------------------
MAC Address      VLAN  IP              Interface    AS Name
--------------------------------------------------------------------------------
xxxx-xxxx-xxx1   212   1.1.1.1         Ge1/0/1      test1
xxxx-xxxx-xxx2   212   1.1.1.2         Ge1/0/1      test1
xxxx-xxxx-xxx3   212   1.1.1.3         Ge1/0/1      test1
xxxx-xxxx-xxx4   212   1.1.1.4         Ge1/0/1      test1
xxxx-xxxx-xxx5   212   1.1.1.5         Ge1/0/1      test1
--------------------------------------------------------------------------------
```

Table 3-100 Description of the **display uni-mng authen-user** command output

Item	Description
Total	Total number of authenticated users on an AS.
MAC Address	MAC address of an authenticated user.
VLAN	VLAN that an authenticated user belongs to.
IP	IP address of an authenticated user. **NOTE** If this command is run on an AS, this field is displayed as **--**.

Item	Description
Interface	Interface to which an authenticated user is connected.
AS Name	Name of an AS.

3.5.47 display uni-mng commit-result

Function

The **display uni-mng commit-result** command displays the configuration delivery result.

NOTE

This command can only be executed on a parent switch.

Format

display uni-mng commit-result { **profile** | **free-rule** | **as-direct-config** }

Parameters

Parameter	Description	Value
profile	Displays the delivery result of the service profile configuration.	-
free-rule	Displays the delivery result of user authenticate-free rules.	-
as-direct-config	Displays the direct configuration recovery result after an AS goes online.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display uni-mng commit-result** command to check the result of delivering the configuration to an AS, including the service profiles configured on the parent, user authentication-free rules, and configurations directly delivered to ASs. This command displays only the latest result but not historical information.

Example

Display the result of delivering the service profile configuration to an AS.

```
<HUAWEI> display uni-mng commit-result profile
Result of profile:
--------------------------------------------------------------------------------
 AS Name                 Commit Time           Commit/Execute Result
--------------------------------------------------------------------------------
 as1                     2014-09-16 14:38:03   Success/Success
--------------------------------------------------------------------------------
```

Table 3-101 Description of the **display uni-mng commit-result profile** command output

Item	Description
AS Name	Name of an AS.
Commit Time	Time when the configuration is delivered.
Commit/Execute Result	Commit Result indicates the configuration delivery result: • Success: The configuration is delivered successfully. • Failed: The configuration fails to be delivered. • Committing: The configuration is being delivered. Execute Result indicates the execution result of the delivered configuration: • Success: The configuration is executed successfully. • Failed: The configuration fails to be executed. • Executing: The configuration is being executed.

3.5.48 display uni-mng global

Function

The **display uni-mng global** command displays the global configuration of SVF.

NOTE

This command can only be executed on a parent switch.

Format

display uni-mng global

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display uni-mng global** command to view the globally configured service functions of SVF.

Example

Display the global configuration of SVF.

```
<HUAWEI> display uni-mng global
Forward-mode : Centralized
Portal url encode : Disable
IGMP snooping VLAN : 10
Authorization VLAN : 23
Authentication configuration revert : Disabled
```

Table 3-102 Description of the **display uni-mng global** command output

Item	Description
Forward-mode	SVF forwarding mode: • Distributed: distributed forwarding. In distributed forwarding, local traffic of an AS can be forwarded from the AS, and traffic between ASs is sent to the parent for forwarding. • Centralized: centralized forwarding. In centralized forwarding mode, both traffic forwarded by the local AS and traffic forwarded between ASs are sent to the parent for forwarding.
Portal url encode	Whether URL encoding is enabled: • Disable: URL encoding is disabled. • Enable: URL encoding is enabled. To disable URL encoding, run the **portal url-encode disable** command.

Item	Description
IGMP snooping VLAN	Service VLAN in which IGMP snooping is enabled. To configure a service VLAN in which IGMP snooping is enabled, run the **as service-vlan igmp-snooping** command. If no service VLAN is configured, this field is not displayed.
Authorization VLAN	Create the service VLAN for ASs. To create the service VLAN, run **as service-vlan authorization** command.
Authentication configuration revert	Whether the function retaining the authentication configuration after an AS goes offline is enabled. To disable the function, run the **as authentication configuration revert disable** command.

3.5.49 display uni-mng indirect configuration

Function

The **display uni-mng indirect configuration** command displays the indirect connection configuration on ASs.

NOTE

This command can only be executed on an AS.

Format

display uni-mng indirect configuration

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display uni-mng indirect configuration** command on an AS to check the indirect connection configuration on the AS.

Example

Display the SVF indirect connection configuration on an AS.

```
<HUAWEI> display uni-mng indirect configuration
Uni-mng configuration information:
 Current uni-mng status      : disable
 Next uni-mng status         : enable
 Current management VLAN     : --
 Next management VLAN        : 100
 Current fabric-port members :
 Next fabric-port members    :
  GigabitEthernet0/0/9
```

Table 3-103 Description of the **display uni-mng indirect configuration** command output

Item	Description
Current uni-mng status	Current manually configured client mode.
Next uni-mng status	Next startup manually configured client mode. To configure the client mode and management VLAN, run the **uni-mng indirect mng-vlan** command.
Current management VLAN	Current management VLAN. To configure the client mode and management VLAN, run the **uni-mng indirect mng-vlan** command.
Next management VLAN	Next startup management VLAN.
Current fabric-port members	Current member port configuration in a fabric port. To configure member ports for a fabric port, run the **uni-mng indirect fabric-port** command.
Next fabric-port members	Next startup member port configuration in a fabric port.

3.5.50 display uni-mng execute-failed-record

Function

The **display uni-mng execute-failed-record** command displays execution failure records after the configuration is delivered to an AS.

NOTE

This command can only be executed on a parent switch.

Format

display uni-mng execute-failed-record { **profile** | **as-direct-config** } **as name** *as-name*

Parameters

Parameter	Description	Value
profile	Displays records of configurations delivered through profiles.	-
as-direct-config	Displays records of configurations directly delivered through commands.	-
as name *as-name*	Specifies the name of an AS.	The value must have an existing AS name.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display uni-mng execute-failed-record** command to check execution failure records after the configuration is delivered to an AS.

Example

Display execution failure records after the configuration is delivered to an AS.

```
<HUAWEI> display uni-mng execute-failed-record as-direct-config as name as1
Info: This operation may take a few seconds. Please wait....done.
------------------------------------------------------------------------------
View name     : system
Command       : arp speed-limit source-mac maximum
1
Execute time  : 2015-01-19 15:09:23 DST
Failed reason : This device does not support this
command.
------------------------------------------------------------------------------
```


Table 3-104 Description of the **display uni-mng execute-failed-record as-direct-config** command output

Item	Description
View name	View in which the configuration is executed.
Command	Command that failed to be executed.
Execute Time	Time the configuration is executed.
Failed reason	Cause of the execution failure.

3.5.51 display uni-mng interface fabric-port configuration

Function

The **display uni-mng interface fabric-port configuration** command displays the fabric port configuration.

NOTE

This command can only be executed on a parent switch.

Format

display uni-mng interface fabric-port configuration [**parent** | **as name** *as-name*]

Parameters

Parameter	Description	Value
parent	Display the parent-side fabric port configuration.	-
as name *as-name*	Display the AS-side fabric port configuration. If **parent** and *as-name* are not specified, the configurations of all the fabric ports in an SVF system are displayed.	The value must have an existing AS name.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display uni-mng interface fabric-port configuration** command to check the fabric port configuration.

Example

Display the fabric port configuration.

```
<HUAWEI> display uni-mng interface fabric-port configuration
Interface      Direction  Connect-type  Member-name
Location
--------------------------------------------------------------------------------
Fabric-port0   Down       Direct        Eth-Trunk0   Parent
Fabric-port1   Down       Direct        Eth-Trunk1   Parent
Fabric-port3   Down       Direct        Eth-Trunk3   Parent
Fabric-port5   Down       Direct        Eth-Trunk5   Parent
Fabric-port6   Down       Direct        Eth-Trunk6   Parent
Fabric-port7   Down       Direct        Eth-Trunk7   Parent
Fabric-port8   Down       Direct        Eth-Trunk8   Parent
Fabric-port9   Down       Indirect      Eth-Trunk9   Parent
Fabric-port10  Down       Indirect      Eth-Trunk10  Parent
Fabric-port11  Down       Direct        Eth-Trunk11  Parent
Fabric-port15  Down       Direct        Eth-Trunk15  Parent
--------------------------------------------------------------------------------
Total : 11
```

Table 3-105 Description of the **display uni-mng interface fabric-port configuration** command output

Item	Description
Interface	Fabric port name.
Direction	Direction of a fabric port. Down indicates downlink and Up indicates uplink.
Connect-type	Connection mode of a fabric port. Direct indicates the direct connection mode, whereas Indirect indicates the indirect connection mode (connection through an intermediate network).
Member-name	Eth-Trunk to which a fabric port is bound.
Location	Device where a fabric port resides.

3.5.52 display uni-mng interface fabric-port state

Function

The **display uni-mng interface fabric-port state** command displays the fabric port status.

NOTE

This command can be used on the parent or an AS. After running this command, you can check the fabric port status on the local device.

Format

display uni-mng interface fabric-port [*port-id*] **state**

Parameters

Parameter	Description	Value
port-id	Specifies the number of a fabric port. If this parameter is not specified, the status of all fabric ports is displayed.	The value is an integer and must be set according to the device configuration.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display uni-mng interface fabric-port state** command to check the fabric port status.

- If an AS connects to the parent through an intermediate network, peer fabric port information cannot be obtained and displays --.
- If a fabric port is incorrectly connected, the system displays an error summary message to provide the cause of the error.

Example

Display the fabric port status on the parent.

```
<HUAWEI> display uni-mng interface fabric-port state
--------------------------------------------------------------------------------
Fabric-port name             : Fabric-port1
Fabric-port direction        : Down
Fabric-port member name      : Eth-Trunk1

Peer MAC                     : xxxx-xxxx-xxxx
Peer AS name                 : as1
Peer fabric-port member name : Eth-Trunk0

Physical member number       : 1
Local-port    Peer-port     State     Detail                    Exptime(s)
XGE6/0/3      XGE0/0/1      Connected None                          32
--------------------------------------------------------------------------------
```


Table 3-106 Description of the **display uni-mng interface fabric-port state** command output

Item	Description
Fabric-port name	Fabric port name.
Fabric-port direction	Direction of a fabric port. Down indicates downlink and Up indicates uplink.
Fabric-port member name	Eth-Trunk to which a fabric port is bound.
Peer MAC	MAC address of the peer device.
Peer AS name	Name of the peer device.
Peer fabric-port member name	Eth-Trunk to which the peer fabric port is bound.
Physical member number	Number of member ports in a fabric port.
Local-port	Local member port.
Peer-port	Peer member port.
State	Port connection status: • Init: initialization state • Config: negotiation state • Error: negotiation error state • Connected: connected state • unknown: unknown state
Detail	Detailed information when the port connection state is Error. For error reasons and solutions, see **Table 3-107**.
Exptime(s)	Timeout period of link heartbeat packets, in seconds.

Table 3-107 Error reasons indicated by the **Detail** field and solutions

Detail Field	Meaning	Solution
Startup cfg file exists	The AS has a startup configuration file.	Clear the startup configuration file and restart the AS.

Detail Field	Meaning	Solution
Console input exists	Input exists on the console interface of an AS.	Restart the AS and do not log in to the console interface immediately after the AS is restarted.
VLAN for VCMP exists	The VLAN for VCMP exists on the AS.	Run the **reset vcmp** command on the AS to restart the AS.
Port not supported	The AS attempts to connect to the parent through an unsupported port.	Connect the AS to the parent through an uplink port or subcard port.
Fabric-port linked to multi-AS	Member ports of the same downlink fabric port connect to two ASs.	Member ports of a downlink fabric port can connect to only one AS, and different ASs must connect to different fabric ports.
Parent exists already	The AS connects to two parent switches.	Disconnect the AS from one parent switch.
Linked to multi fabric-port	The uplink port of the AS connects to multiple fabric ports of the parent.	Ensure that the AS connects to only one fabric port of the parent and disconnect the AS from other fabric ports.
Level-1 AS linked to level-1 AS	The downlink fabric port of a level-1 AS connects to another level-1 AS.	Disconnect the two level-1 ASs from each other.
Parent linked to level-2 AS	The parent directly connects to a level-2 AS.	Disconnect the parent from the level-2 AS.
Downstream fabric-port linked	A downlink fabric port of an AS connects to the parent.	Disconnect the fabric port of the AS from the parent.
No response received	The parent does not receive any response packet.	• Ensure that the parent is a Huawei switch that supports the SVF function. • Ensure that the AS starts without configuration. • Ensure that physical ports that connect the AS to the parent are of the same type.

Detail Field	Meaning	Solution
Failed to create Eth-Trunk	Failed to create an Eth-Trunk on an AS.	Disconnect the AS from the parent and then reconnect them.
Failed to bind trunk	Failed to add ports of an AS to an Eth-Trunk.	Disconnect the AS from the parent and then reconnect them.
Force Uni-mng mode	An AS has been configured to work in client mode.	On the parent, configure the indirect connection mode for the fabric port that connects to the AS. Alternative, run the **undo uni-mng enable** command on the AS and restart the AS to enable it exit from the client mode.
Parent linked to parent	The fabric port of the parent connects to another parent.	Disconnect the fabric port from the remote parent.
System is busy on AS	The system is busy on the AS.	Wait until the AS is idle.
Linked to AS with IPv4-hardware	When an S5700-10P-LI, S5700-10P-PWR-LI-AC, or S2750-EI functions as an AS, Layer 3 hardware forwarding for IPv4 packets has been enabled using the **assign forward-mode ipv4-hardware** command.	Disable Layer 3 hardware forwarding for IPv4 packets.
Configurations exist on port	Configurations exist on the port of an AS.	Delete the configurations of the port.
Invalid stack config exists	Downlink service port of AS is configured as a stack port.	Clear the stack configuration of the downlink service port.

3.5.53 display uni-mng port-group

Function

The **display uni-mng port-group** command displays information about port groups.

NOTE

This command can only be executed on a parent switch.

Format

display uni-mng port-group [**name** *group-name* | **verbose**]

Parameters

Parameter	Description	Value
name *group-name*	Specifies the name of a port group.	The value must be an existing a port group name.
verbose	Displays detailed information about a port group.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display uni-mng port-group** command to check information about created port groups.

Example

Display brief information about all port groups.

```
<HUAWEI> display uni-mng port-group

-------------------------------------------------------------------------------
 Number            Port-group Name                Port-group Type
-------------------------------------------------------------------------------
 1                 group1                      connect to user
 2                 ap_group1                     connect to AP
-------------------------------------------------------------------------------
```

Table 3-108 Description of the **display uni-mng port-group** command output

Item	Description
Number	Sequence number.
Port-group Name	Port group name.

Item	Description
Port-group Type	Port group type: • connect to user: port connected to a terminal user • connect to AP: port connected to an AP

Display detailed information about all port groups.

```
<HUAWEI> display uni-mng port-group verbose

------------------------------------------------------------------------------
Port-group name                  : ap
Port-group type                 : connect to AP
Interface list                  :
 AS name as1 interface Eth-trunk 5 GigabitEthernet 0/0/2
Network-basic profile            : qos
Network-enhanced profile         : net
Network-qos profile              : test
Traffic-policy profile          : test(inbound)
User-access profile              : access_profile
------------------------------------------------------------------------------
Port-group name                  : group_2
Port-group type                 : connect to user
Interface list                  :
 AS name as1 interface Eth-trunk 4 GigabitEthernet 0/0/10
Network-basic profile            : --
Network-enhanced profile         : --
Network-qos profile              : --
Traffic-policy profile          : --

User-access profile              : --
------------------------------------------------------------------------------
```

Table 3-109 Description of the **display uni-mng port-group verbose** command output

Item	Description
Port-group name	Port group name.
Port-group type	Port group type: • connect to user: port connected to a terminal user • connect to AP: port connected to an AP
Interface list	List of member ports added to a port group.
Network-basic profile	Name of the network basic profile bound to the port group. When no network basic profile is bound to the port group, this field displays --.

Item	Description
Network-enhanced profile	Name of the network enhanced profile bound to the port group. When no network enhanced profile is bound to the port group, this field displays --.
Network-qos profile	Name of the network QoS profile bound to the port group. When no network QoS profile is bound to the port group, this field displays --.
Traffic-policy profile	Name of the traffic policy profile bound to the port group. When no traffic policy profile is bound to the port group, this field displays --.
User-access profile	Name of the user access profile bound to the port group. When no user access profile is bound to the port group, this field displays --.

3.5.54 display uni-mng profile

Function

The **display uni-mng profile** command displays service profile information.

NOTE

This command can only be executed on a parent switch.

Format

display uni-mng profile [{ **as-admin** | **network-basic** | **network-enhanced** | **user-access** | **network-qos** | **traffic-policy** } [**name** *profile-name*]]

Parameters

Parameter	Description	Value
as-admin	Displays information about AS administrator profiles.	-
network-basic	Displays information about network basic profiles.	-
network-enhanced	Displays information about network enhanced profiles.	-

Parameter	Description	Value
user-access	Displays information about user access profiles.	-
network-qos	Displays information about network qos profiles.	-
traffic-policy	Displays information about traffic policy profiles.	-
name *profile-name*	Specifies the name of a service profile. If this parameter is specified, you can check information about services configured in a specified profile.	The profile must have an existing profile name.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display uni-mng profile** command to check information about created service profiles.

Example

Display brief information about all service profiles.

```
<HUAWEI> display uni-mng profile

AS-admin profile:
------------------------------------------------------------------------------
 Number                 Profile Name
------------------------------------------------------------------------------
 1                      hehe
 2                      profile_1
------------------------------------------------------------------------------

Network-basic profile:
------------------------------------------------------------------------------
 Number                 Profile Name
------------------------------------------------------------------------------
 1                      b_pro
 2                      p
------------------------------------------------------------------------------

Network-enhanced profile:
------------------------------------------------------------------------------
 Number                 Profile Name
------------------------------------------------------------------------------
 1                      enp
```



```
------------------------------------------------------------------------------

Network-qos profile:
------------------------------------------------------------------------------
Number                  Profile Name
------------------------------------------------------------------------------
1                       test
------------------------------------------------------------------------------

Traffic-policy profile:
------------------------------------------------------------------------------
Number                  Profile Name
------------------------------------------------------------------------------
1                       12341
2                       123410
3                       123411
------------------------------------------------------------------------------

User-access profile:
------------------------------------------------------------------------------
Number                  Profile Name
------------------------------------------------------------------------------
1                       u_pro
------------------------------------------------------------------------------
```

Table 3-110 Description of the **display uni-mng profile** command output

Item	Description
Number	Sequence number.
Profile Name	Name of each profile type.
AS-admin profile	AS administrator profile created using the **as-admin-profile name** command.
Network-basic profile	Network basic profile created using the **network-basic-profile name** command.
Network-enhanced profile	Network enhanced profile created using the **network-enhanced-profile name** command.
Network-qos profile	Network qos profile created using the **network-qos-profile name** command.
Traffic-policy profile	Traffic policy profile created using the **traffic-policy-profile name** command.
User-access profile	User access profile created using the **user-access-profile name** command.

Display information about the service profile with a specified name.

```
<HUAWEI> display uni-mng profile network-basic name basic

------------------------------------------------------------------------------
Profile name: basic
 User-vlan              : 110
```



```
Voice-vlan          : 114
Pass-vlan           : 1 112 to 113
------------------------------------------------------------------------------
```

Table 3-111 Description of the **display uni-mng profile network-basic name** command output

Item	Description
Profile name	Name of a service profile.
User-vlan	Default VLAN configured in a service profile. To configure a default VLAN, run the **user-vlan** command. By default, VLAN 1 is a default VLAN.
Voice-vlan	Voice VLAN configured in a service profile. To configure a voice VLAN, run the **voice-vlan** command. If no voice VLAN is configured, this field displays --.
Pass-vlan	Allowed VLAN configured in a service profile. To configure an allowed VLAN, run the **pass-vlan** command. By default, only VLAN 1 is allowed.

3.5.55 display uni-mng profile as

Function

The **display uni-mng profile as** command displays the configuration generated after an AS is bound to service profiles.

NOTE

This command can only be executed on a parent switch.

Format

display uni-mng profile as name *as-name* [**interface** *interface-type interface-number*]

Parameters

Parameter	Description	Value
name *as-name*	Specifies the name of an AS.	The value must have an existing AS name.
interface *interface-type interface-number*	Displays the configuration of a specified interface: • *interface-type* specifies the interface type. The interface type can be a physical interface, an Eth-Trunk, or a fabric port. • *interface-number* specifies the interface number. If this parameter is not specified, the configurations of all the service interfaces on an AS are displayed.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display uni-mng profile as** command to check the configuration generated after an AS is bound to service profiles.

If a fabric port is specified, this command displays only the network QoS profile configuration.

Example

Display the configuration generated on an AS.

```
<HUAWEI> display uni-mng profile as name as1

Global
------------------------------------------------------------------------------
 Centralized forward mode: disable
------------------------------------------------------------------------------
 Portal url-encode: enable
------------------------------------------------------------------------------
 Igmp-vlan                    : --
------------------------------------------------------------------------------
 Authorization-vlan           : --
------------------------------------------------------------------------------
AS-group name: xy
 Username: admin
  Privilege-level   : 3
```



```
  Service-type      : terminal ssh
  Bpdu-protection   : --
  Ipv6              : --
  Acl number        : 3000 3002 3011 3012 3013 3014 3015 3016 3017 3018
 Traffic-limit outbound ARP(Kbps)  : 512
 Traffic-limit outbound DHCP(Kbps) : 128
------------------------------------------------------------------------------

Interface fabric-port 0
------------------------------------------------------------------------------
Port-group name: --
 Trust Flag                    : --
 Scheduling Profile            : --
 Scheduling Mode               : --
  Weight of Queue 0            : --
  Weight of Queue 1            : --
  Weight of Queue 2            : --
  Weight of Queue 3            : --
  Weight of Queue 4            : --
  Weight of Queue 5            : --
  Weight of Queue 6            : --
  Weight of Queue 7            : --
------------------------------------------------------------------------------

Interface GigabitEthernet0/0/1
------------------------------------------------------------------------------
Port-group name: --
 User-vlan                     : --
 Voice-vlan                    : --
 Pass-vlan                     : --

 Priority-trust                : disable
 User-access-port              : disable
 DHCP snooping                 : disable
 IP source check               : disable
 ARP anti-attack check         : disable
 Unicast-suppression(pps)      : --
 Multicast-suppression(pps)    : --
 Broadcast-suppression(pps)    : --
 Rate-limit(Kbps)              : --
 Port-security                 : disable
 Mac-address sticky            : disable
 Port-security aging-time      : --

 Trust Flag                    : dscp
 Scheduling Profile            : qos
 Scheduling Mode               : wrr
  Weight of Queue 0            : --
  Weight of Queue 1            : 6
  Weight of Queue 2            : --
  Weight of Queue 3            : --
  Weight of Queue 4            : --
  Weight of Queue 5            : --
  Weight of Queue 6            : --
  Weight of Queue 7            : --

 Authentication                : --
 Authentication maximum user-num  : --
 MAC-limit                     : --
 Traffic-limit inbound ARP(Kbps)  : --
 Traffic-limit inbound DHCP(Kbps) : --

 Traffic policy profile        : --
------------------------------------------------------------------------------

Interface GigabitEthernet0/0/2
------------------------------------------------------------------------------
Port-group name: --
 User-vlan                     : --
```



```
Voice-vlan                    : --
Pass-vlan                     : --

Priority-trust                : disable
User-access-port              : disable
DHCP snooping                 : disable
IP source check               : disable
ARP anti-attack check         : disable
Unicast-suppression(pps)      : --
Multicast-suppression(pps)    : --
Broadcast-suppression(pps)    : --
Rate-limit(Kbps)              : --
Port-security                 : disable
Mac-address sticky            : disable
Port-security aging-time      : --

Trust Flag                    : dscp
Scheduling Profile            : qos
Scheduling Mode               : wrr
 Weight of Queue 0            : --
 Weight of Queue 1            : 6
 Weight of Queue 2            : --
 Weight of Queue 3            : --
 Weight of Queue 4            : --
 Weight of Queue 5            : --
 Weight of Queue 6            : --
 Weight of Queue 7            : --

Authentication                : --
Authentication maximum user-num  : --
MAC-limit                     : --
Traffic-limit inbound ARP(Kbps)  : --
Traffic-limit inbound DHCP(Kbps) : --

Traffic policy profile        : --
------------------------------------------------------------------------------
.....
```

Table 3-112 Description of the **display uni-mng profile as** command output

Item	Description
Global	Global AS configuration.
Centralized forward mode	Whether centralized forwarding is enabled: ● disable: Centralized forwarding is disabled, and distributed forwarding is used currently. ● enable: Centralized forwarding is enabled. To configure centralized forwarding, run the **forward-mode centralized** command. By default, distributed forwarding is used.

Item	Description
Portal url-encode	Whether URL encoding is enabled for an AS: • disable: URL encoding is disabled for the AS. • enable: URL encoding is enabled for the AS. To disable URL encoding for an AS, run the **portal url-encode disable** command. By default, URL encoding is enabled for an AS.
Igmp-vlan	VLAN in which IGMP Snooping is enabled. If no VLAN is configured, this field displays --. To configure the VLAN, run the **as service-vlan igmp-snooping** command.
Authorization-vlan	Service VLAN created on an AS. If no VLAN is configured, this field displays --. To configure the service VLAN, run the **as service-vlan authorization** command.
AS-group name	Name of the AS group to which an AS belongs.
Username	AS administrator user name. If no AS administrator user name is configured, this field displays --. AS administrator user name configured in the AS administrator profile bound to an AS group. To configure an AS administrator user name, run the **user password** command.
Privilege-level	User level. The value is 3 and cannot be changed.
Service-type	User access type. The value is terminal ssh and cannot be changed.
Bpdu-protection	BPDU protection status of an AS. If BPDU protection is not configured, this field displays --.
Ipv6	Whether IPv6 is enabled on an AS.
Acl number	ACL number created on an AS.

Item	Description
Traffic-limit outbound ARP(Kbps)	Outbound ARP packet rate limit of the uplink fabric port of an AS, in kbit/s. To set the outbound ARP packet rate limit, run the **traffic-limit outbound** command.
Traffic-limit outbound DHCP(Kbps)	Outbound DHCP packet rate limit of the uplink fabric port of an AS, in kbit/s. To set the outbound ARP packet rate limit, run the **traffic-limit outbound** command.
Interface GigabitEthernet0/0/1 Interface GigabitEthernet0/0/2 Interface fabric-port 0	Interface name.
Port-group name	Name of the port group to which an interface belongs. If an interface is not added to any port group, this field displays -- or disable.
User-vlan	Default VLAN. To configure a default VLAN, run the **user-vlan** command.
Voice-vlan	Voice VLAN. To configure a voice VLAN, run the **voice-vlan** command.
Pass-vlan	Allowed VLAN. To configure an allowed VLAN, run the **pass-vlan** command.
Priority-trust	Whether the priority trust function is enabled: ● disable: The priority trust function is disabled in a network enhanced profile. ● enable: The priority trust function is enabled in a network enhanced profile.

Item	Description
User-access-port	Whether the edge port function is enabled: ● disable: The edge port function is disabled in a network enhanced profile. ● enable: The edge port function is enabled in a network enhanced profile. To enable the edge port function, run the **user-access-port enable** command.
DHCP snooping	Whether DHCP snooping is enabled: ● disable: DHCP snooping is disabled in a network enhanced profile. ● enable: DHCP snooping is enabled in a network enhanced profile. To enable DHCP snooping, run the **dhcp snooping enable** command.
IP source check	Whether the IP packet check function is enabled: ● disable: IP packet check is disabled in a network enhanced profile. ● enable: IP packet check is enabled in a network enhanced profile. To enable IP packet check, run the **ip source check user-bind enable** command.
ARP anti-attack check	Whether the dynamic ARP inspection function is enabled: ● disable: The dynamic ARP inspection function is disabled in a network enhanced profile. ● enable: The dynamic ARP inspection function is enabled in a network enhanced profile. To enable the dynamic ARP inspection function, run the **arp anti-attack check user-bind enable** command.
Unicast-suppression(pps)	Rate limit for unknown unicast traffic, in pps. To set the rate limit for unknown unicast traffic, run the **unicast-suppression** command.

Item	Description
Multicast-suppression(pps)	Rate limit for multicast traffic, in pps. To set the rate limit for multicast traffic, run the **multicast-suppression** command.
Broadcast-suppression(pps)	Rate limit for broadcast traffic, in pps. To set the rate limit for broadcast traffic, run the **broadcast-suppression** command.
Rate-limit(Kbps)	Traffic rate limit, in kbit/s. To set the traffic rate limit, run the **rate-limit** command.
Port-security	Whether port security is enabled. To enable the port security function, run the **port-security enable** command.
Mac-address sticky	Whether the sticky MAC function is enabled on an interface. To enable the sticky MAC function on an interface, run the **port-security mac-address sticky** command.
Port-security aging-time	Aging time of secure dynamic MAC addresses on an interface. To set this parameter, run the **port-security aging-time** command.
Trust Flag	Packet priority mapping flag. To configure priority mapping, run the **trust dscp** command.
Scheduling Profile	Name of a network QoS profile.
Scheduling Mode	Queue scheduling mode. To configure the queue scheduling mode, run the **qos { pq | wrr | drr }** command.

Item	Description
Weight of Queue 0 Weight of Queue 1 Weight of Queue 2 Weight of Queue 3 Weight of Queue 4 Weight of Queue 5 Weight of Queue 6 Weight of Queue 7	Queue scheduling weight. To configure the queue scheduling weight, run the **qos queue** command.
Authentication	User authentication profile created using the **authentication-profile** command.
Authentication maximum user-num	Maximum number of access users configured in a user access profile. To set this parameter, run the **authentication access-user maximum** command.
MAC-limit	MAC address learning limit. To set the MAC address learning limit, run the **mac-limit** command.
Traffic-limit inbound ARP(Kbps)	Inbound ARP packet rate limit of an AS port, in kbit/s. To set the inbound ARP packet rate limit, run the **traffic-limit inbound** command.
Traffic-limit inbound DHCP(Kbps)	Inbound DHCP packet rate limit of an AS port, in kbit/s. To set the inbound ARP packet rate limit, run the **traffic-limit inbound** command.
Traffic policy profile	Name of the traffic policy profile bound to an AS.

3.5.56 display uni-mng topology configuration

Function

The **display uni-mng topology configuration** command displays the SVF network topology collection configuration.

NOTE

This command can only be executed on a parent switch.

Format

display uni-mng topology configuration

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display uni-mng topology configuration** command to check the SVF network topology collection configuration.

Example

Display the SVF network topology collection configuration.

```
<HUAWEI> display uni-mng topology configuration
Explore timer: 10 minutes
Last collection time: 10:03:58 UTC+00:00 2014/09/11
Total time for last collection: 9 ms
```

Table 3-113 Description of the **display uni-mng topology configuration** command output

Item	Description
Explore timer	Network topology collection interval. To set the network topology collection interval, run the **topology explore** command.
Last collection time	Last time the SVF network topology is collected.
Total time for last collection	Time taken to collect the SVF network topology.

3.5.57 display uni-mng topology information

Function

The **display uni-mng topology information** command displays SVF network topology information.

NOTE

This command can only be executed on a parent switch.

Format

display uni-mng topology information [**by-name**]

Parameters

Parameter	Description	Value
by-name	Displays SVF network topology information based on the device name. If this parameter is not specified, SVF network topology information is displayed based on the MAC address.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display uni-mng topology information** command to check SVF network topology information.

Example

Display SVF network topology information.

```
<HUAWEI> display uni-mng topology information
The topology information of uni-mng network:
<-->: direct link        <??>: indirect link
T: Trunk ID               *: independent AS
--------------------------------------------------------------------------------
 Local MAC       Hop  Local Port      T  ||  T   Peer Port      Peer MAC
--------------------------------------------------------------------------------
 00e0-fc12-7890  0    GE6/1/0         11 <-->0   GE0/0/26       00e0-fc12-0008 *
 00e0-fc12-0008  1    GE0/0/2         -- <-->--  GE0/0/0        00e0-fc12-0005
--------------------------------------------------------------------------------
Total items displayed : 2
```

Display SVF network topology information based on the device name.

```
<HUAWEI> display uni-mng topology information by-name
The topology information of uni-mng network:
<-->: direct link        <??>: indirect link
T: Trunk ID              *: independent AS
-------------------------------------------------------------------------------------------------------
 Local Dev                    Hop  Local Port      T  ||  T   Peer Port      Peer Dev
-------------------------------------------------------------------------------------------------------
 100-S1                       0    GE6/1/0         1  <-->0   GE0/0/26       as1 *
```



```
as1                          1    GE0/0/2        -- <-->--  GE0/0/0       ap-1
------------------------------------------------------------------------------------------------------------------
Total items displayed : 2
```

Table 3-114 Description of the **display uni-mng topology information** command output

Item	Description
Local MAC	MAC address of the local device. If **by-name** is specified, this field displays **Local Dev**, indicating the device name.
Hop	Hierarchy of a device on the SVF network: ● 0: the parent ● 1: level-1 AS ● 2: level-2 AS
Local Port	Local physical port. When two devices are indirectly connected, port information cannot be displayed because ports are not indirectly connected.
T	ID of the Eth-Trunk to which a physical port belongs.
||	Whether two devices are directly connected: ● <-->: indicates that two devices are directly connected. ● <??>: indicates that two devices are indirectly connected. For example, two devices are connected through other networks.
Peer Port	Peer physical port. When two devices are indirectly connected, port information cannot be displayed because ports are not indirectly connected.
Peer MAC	MAC address of the peer device. If **by-name** is specified, this field displays **Peer Dev**, indicating the device name. If * is displayed, the AS is configured in the independent mode.
Local Dev	Local device name.

Item	Description
Peer Dev	Peer device name. If * is displayed, the AS is configured in the independent mode.

3.5.58 display uni-mng unauthen-user

Function

The **display uni-mng unauthen-user** command displays information about non-authenticated users on an AS.

NOTE

This command can be used on the parent or an AS.

Format

display uni-mng unauthen-user [**as name** *as-name* | **mac-address** *mac-address*]

Parameters

Parameter	Description	Value
as name *as-name*	Specifies the name of an AS. **NOTE** This parameter is supported only on the parent.	The value is a string of 1 to 31 case-insensitive characters without spaces.
mac-address *mac-address*	Specifies the MAC address of an AS.	The value is in H-H-H format, where H is a hexadecimal number of 1 to 4 digits. The value cannot be all 0s, all Fs, or a multicast MAC address.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

To view information about non-authenticated users on an AS, run the **display uni-mng unauthen-user** command.

Example

Display information about non-authenticated users on the AS **test1**.

```
<HUAWEI> display uni-mng unauthen-user as name test1
Total: 5
--------------------------------------------------------------------------------
MAC Address      VLAN  IP              Interface    AS Name
--------------------------------------------------------------------------------
xxxx-xxxx-xxx2   212   1.1.1.1         Ge1/0/1      test1
xxxx-xxxx-xxx3   212   1.1.1.2         Ge1/0/1      test1
xxxx-xxxx-xxx4   212   1.1.1.3         Ge1/0/1      test1
xxxx-xxxx-xxx5   212   1.1.1.4         Ge1/0/1      test1
xxxx-xxxx-xxx6   212   1.1.1.5         Ge1/0/1      test1
--------------------------------------------------------------------------------
```

Table 3-115 Description of the **display uni-mng unauthen-user** command output

Item	Description
Total	Number of non-authenticated users on an AS.
MAC Address	MAC address of a non-authenticated user.
VLAN	VLAN to which a non-authenticated user belongs.
IP	IP address of a non-authenticated user. **NOTE** When this command is run on the AS, this field is displayed as --.
Interface	Access interface of a non-authenticated user.
AS Name	Name of an AS.

3.5.59 display uni-mng unauthen-user offline-record

Function

The **display uni-mng unauthen-user offline-record** command displays offline records of non-authenticated users on an AS.

NOTE

This command can only be executed on a parent switch.

Format

display uni-mng unauthen-user offline-record [**as name** *as-name* | **mac-address** *mac-address*]

Parameters

Parameter	Description	Value
as name *as-name*	Specifies the name of an AS.	The value is a string of 1 to 31 case-insensitive characters without spaces.
mac-address *mac-address*	Specifies the MAC address of an AS.	The value is in H-H-H format, where H is a hexadecimal number of 1 to 4 digits. The value cannot be all 0s, all Fs, or a multicast MAC address.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

To view offline records of non-authenticated users on an AS, run the **display uni-mng unauthen-user offline-record** command.

Example

Display offline records of non-authenticated users on the AS **test1**.

```
<HUAWEI> display uni-mng unauthen-user offline-record as name test1
Total: 2
--------------------------------------------------------------------------------
  AS name              : test1
  User MAC             : 00e0-fc46-b67c
  User VLAN            : 212
  User access interface : Ge1/0/2
  User IP address      : 192.168.1.1
  User offline time    : 2016/01/21 04:59:43
  User offline reason  : As offline
--------------------------------------------------------------------------------
  AS name              : test1
  User MAC             : 00e0-fc46-b67d
  User VLAN            : 212
  User access interface : Ge1/0/3
  User IP address      : 192.168.1.2
  User offline time    : 2016/01/21 05:59:43
  User offline reason  : User offline
--------------------------------------------------------------------------------
```


Table 3-116 Description of the **display uni-mng unauthen-user offline-record** command output

Item	Description
Total	Number of offline records of non-authenticated users on an AS.
AS name	Name of an AS.
User MAC	MAC address of a non-authenticated user.
User VLAN	VLAN to which a non-authenticated user belongs.
User access interface	Access interface of a non-authenticated user.
User IP address	IP address of a non-authenticated user.
User offline time	Time when a non-authenticated user goes offline.
User offline reason	Reason that a non-authenticated user goes offline. • User offline: The user goes offline. • AS offline: The AS is offline.

3.5.60 display uni-mng upgrade-info

Function

The **display uni-mng upgrade-info** command displays AS version upgrade information.

NOTE

This command can only be executed on a parent switch.

Format

display uni-mng upgrade-info [**as name** *as-name* | **verbose**]

Parameters

Parameter	Description	Value
as name *as-name*	Specifies the name of an AS.	The value must have an existing AS name.

Parameter	Description	Value
verbose	Displays detailed version upgrade information.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display uni-mng upgrade-info** command to check AS version upgrade information.

Example

Display AS version upgrade information.

```
<HUAWEI> display uni-mng upgrade-info
The total number of AS is : 1
------------------------------------------------------------------------------
Name                        Method      Phase      Status      Result
------------------------------------------------------------------------------
as1                         --          --         NO-UPGRADE  --
------------------------------------------------------------------------------
```

Table 3-117 Description of the **display uni-mng upgrade-info** command output

Item	Description
Name	Name of an AS.
Method	AS upgrade mode: ● --: The upgrade task is not started. ● ver-sync: The AS is automatically upgraded when going online. ● upgrade: The AS is manually upgraded after going online.

Item	Description
Phase	Upgrade phase: ● --: The upgrade task is not started. ● sys-file: The system is determining whether to download the system software or is downloading the system software from the parent. ● patch-file: The system is determining whether to download the patch file or is downloading the patch file from the parent. ● waiting: The AS is waiting for activation. ● activating: The AS is being activated. ● rebooting: The AS is restarting.
Status	Whether the AS is being upgraded: ● NO-UPGRADE: The AS is not upgraded. ● UPGRADING: The AS is being upgraded.
Result	Upgrade result: ● --: The upgrade task is not started. ● successful: The upgrade is successful. ● failed: The upgrade fails.

Display detailed AS version upgrade information.

```
<HUAWEI> display uni-mng upgrade-info verbose
The total number of AS is : 1
------------------------------------------------------------------------------
 AS name                      : as1
 Work status                  : UPGRADING
 Startup system-software      : flash:/s5720-p-li-v200r021c00.cc
 Startup version              : V200R013C00
 Startup patch                : --
 Next startup system-software : flash:/s5720-p-li-v200r022c00spc500.cc
 Next startup patch           : --
 Download system-software     : s5720-p-li-v200r022c00spc500.cc
 Download version             : --
 Download patch               : --
 Activating file time         : immediately
 Activating file method       : reload
 Method                       : upgrade
 Upgrading phase              : sys-file
 Last operation result        : --
 Error reason                 : --
 Last operation time          : --
------------------------------------------------------------------------------
```


Display detailed information after an AS version upgrade is complete.

```
<HUAWEI> display uni-mng upgrade-info verbose
The total number of AS is : 1
------------------------------------------------------------------------------
 AS name                      : as1
 Work status                  : NO-UPGRADE
 Startup system-software      : flash:/s5720-p-li-v200r022c00spc500.cc
 Startup version              : V200R022C00SPC500
 Startup patch                : --
 Next startup system-software : --
 Next startup patch           : --
 Download system-software     : --
 Download version             : --
 Download patch               : --
 Method                       : --
 Upgrading phase              : --
 Last operation result        : failed
 Error reason                 : The local file server has not been configured.
 Last operation time          : 2019-10-04  15:51:05
------------------------------------------------------------------------------
```

Table 3-118 Description of the **display uni-mng upgrade-info verbose** command output

Item	Description
AS name	Name of an AS.
Work status	Whether the AS is being upgraded: ● NO-UPGRADE: The AS is not upgraded. ● UPGRADING: The AS is being upgraded.
Startup system-software	Running system software.
Startup version	Current software version.
Startup patch	Running patch file. If this field displays --, no patch file is running.
Next startup system-software	System software that is configured for the next startup. If this field displays --, no system software is configured for the next startup.
Next startup patch	Patch package file that is configured for the next startup. If this field displays --, no patch package file is configured for the next startup.
Download system-software	Downloaded system software. If this field displays --, the upgrade task is not started.
Download version	Downloaded system software version. If this field displays --, the upgrade task is not started.

Item	Description
Download patch	Downloaded patch file. If this field displays --, the upgrade task is not started.
Activating file time	Activation time after the AS system software is downloaded. ● at **xxx**: The downloaded AS system software is activated at the specified time. ● delay **xxx**: The downloaded AS system software is activated after the specified delay time. ● immediately: The AS system software is activated immediately after being downloaded.
Activating file method	Mode in which the AS system software is activated: ● reload: The AS system software is activated by restarting the AS. ● default: The AS system software is activated without restarting the AS.
Method	AS upgrade mode: ● --: The upgrade task is not started. ● ver-sync: The AS is automatically upgraded when going online. ● upgrade: The AS is manually upgraded after going online.
Upgrading phase	Upgrade phase: ● --: The upgrade task is not started. ● sys-file: The system is determining whether to download the system software or is downloading the system software from the parent. ● patch-file: The system is determining whether to download the patch file or is downloading the patch file from the parent. ● waiting: The AS is waiting for activation. ● activating: The AS is being activated. ● rebooting: The AS is restarting.

Item	Description
Last operation result	Upgrade result: • --: The upgrade task is not started. • successful: The upgrade is successful. • failed: The upgrade fails.
Error reason	Upgrade failure reason.
Last operation time	Last time the AS is upgraded.

3.5.61 display uni-mng up-direction fabric-port

Function

The **display uni-mng up-direction fabric-port** command displays information about AS service ports added to an uplink fabric port.

NOTE

This command can only be executed on an AS.

Format

display uni-mng up-direction fabric-port

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display uni-mng up-direction fabric-port** command to check the current and next startup configurations of AS service ports added to an uplink fabric port.

Example

Display information about AS service ports added to an uplink fabric port.

```
<HUAWEI> display uni-mng up-direction fabric-port
Uni-mng up-direction fabric-port configuration:
```



```
Current fabric-port members :
GigabitEthernet0/0/1
GigabitEthernet0/0/2
GigabitEthernet0/0/3
GigabitEthernet0/0/4
Next fabric-port members    :
GigabitEthernet0/0/1
GigabitEthernet0/0/2
GigabitEthernet0/0/3
GigabitEthernet0/0/4
```

Table 3-119 Description of the **display uni-mng up-direction fabric-port** command output

Item	Description
Uni-mng up-direction fabric-port configuration	Configuration of an uplink fabric port.
Current fabric-port members	Effective member interfaces of the uplink fabric port.
Next fabric-port members	Effective member interfaces of the uplink fabric port after the device's next startup.

3.5.62 down-direction fabric-port

Function

The **down-direction fabric-port** command configures the fabric port that connects a level-1 AS to a level-2 AS.

The **undo down-direction fabric-port** command deletes the fabric port that connects a level-1 AS to a level-2 AS.

By default, no fabric port that connects a level-1 AS to a level-2 AS is configured.

NOTE

This command can only be executed on a parent switch.

Format

down-direction fabric-port *port-id* **member-group interface eth-trunk** *trunk-id*

undo down-direction fabric-port *port-id* **member-group**

Parameters

Parameter	Description	Value
port-id	Specifies the number of a fabric port.	The value is an integer and must be set according to the device configuration.
member-group interface	Specifies the Eth-Trunk to which a fabric port is bound.	-
eth-trunk *trunk-id*	Specifies the ID of an Eth-Trunk.	The value is an integer that ranges from 1 to 63. **NOTE** If an Eth-Trunk has been created and configured on an AS in independent mode, the **eth-trunk** *trunk-id* parameter cannot be the same as the existing Eth-Trunk ID of this AS. Otherwise, this command cannot be delivered.

Views

AS view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

When a level-1 AS needs to connect to a level-2 AS, you need to configure a fabric port on the level-1 AS to connect to the level-2 AS. A downlink port of a level-1 AS becomes Up only after the parent finishes delivering the configuration. A level-2 AS begins to go online only after the downlink port of the level-1 AS becomes Up.

Follow-up Procedure

Run the **port eth-trunk** *trunk-id* **trunkmember interface** *interface-type interface-number1* [**to** *interface-number2*] command to add member ports to the bound Eth-Trunk.

Example

Configure the fabric port that connects a level-1 AS to a level-2 AS.

```
<HUAWEI> system-view
[HUAWEI] uni-mng
[HUAWEI-um] as name as1
[HUAWEI-um-as-as1] down-direction fabric-port 1 member-group interface eth-trunk 1
```


3.5.63 down-direction fabric-port connect independent-as

Function

The **down-direction fabric-port connect independent-as** command enables the independent mode on the fabric port that connects a level-1 AS to a level-2 AS.

The **undo down-direction fabric-port** command restores the default mode of the fabric port that connects a level-1 AS to a level-2 AS.

By default, the service configuration mode of the fabric port that connects a level-1 AS to a level-2 AS is centralized mode.

NOTE

This command can only be executed on a parent switch.

Format

down-direction fabric-port *port-id* **connect independent-as**

undo down-direction fabric-port *port-id* **connect**

Parameters

Parameter	Description	Value
port-id	Specifies the number of a fabric port.	The value is an integer and must be set according to the device configuration.

Views

AS view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

In independent mode, you can log in to an AS to configure this AS using commands. After the independent mode is enabled on the fabric port that connects a level-1 AS to a level-2 AS, the level-2 AS can be configured independently.

Prerequisites

The fabric port used to connect a level-1 AS to a level-2 AS has been created using the **down-direction fabric-port** *port-id* **member-group interface eth-trunk** *trunk-id* command in the AS view.

Precautions

Before enabling the independent mode, run the **independent-as-admin** command in the uni-mng view to configure an administrator for AS login. If no administrator is created, you can only log in to an AS through a console port.

If service configurations have been delivered in centralized mode to a level-1 AS port before this port is changed to the independent mode, this port cannot be configured as a fabric port that connects to a level-2 AS. To do so, restore the level-1 AS to the centralized mode and cancel the service configurations of this port on the parent.

In independent mode, when an AS goes offline, traffic on the network attached to an AS port cannot be forwarded if the port has authentication configurations. To enable the traffic to be forwarded normally, manually delete the authentication configurations from the port.

Example

Enable the independent mode on the fabric port that connects a level-1 AS to a level-2 AS.

```
<HUAWEI> system-view
[HUAWEI] uni-mng
[HUAWEI-um] as name as1
[HUAWEI-um-as-as1] down-direction fabric-port 1 member-group interface eth-trunk 1
[HUAWEI-um-as-as1] down-direction fabric-port 1 connect independent-as
```

3.5.64 forward-mode centralized

Function

The **forward-mode centralized** command sets the forwarding mode of an SVF system to centralized forwarding.

The **undo forward-mode** command restores the default forwarding mode of an SVF system.

By default, the forwarding mode of an SVF system is distributed forwarding.

NOTE

This command can only be executed on a parent switch.

Format

forward-mode centralized

undo forward-mode

Parameters

None

Views

uni-mng view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

An SVF system uses the distributed forwarding mode by default. You can change the forwarding mode to centralized mode.

- In centralized forwarding mode, traffic forwarded by the local AS and forwarded between ASs is sent to the parent for forwarding.
- In distributed forwarding mode, an AS directly forwards local traffic and the parent forwards traffic between ASs.

Precautions

- After changing the SVF forwarding mode, you must run the **commit as** { **name** *as-name* | **all** } command to commit the configuration so that the device can deliver it to ASs.
- In centralized forwarding mode, ports of the ASs connected to the same fabric port of the parent are isolated and so cannot communicate at Layer 2, and need to have proxy ARP in the corresponding VLAN configured using the **arp-proxy inner-sub-vlan-proxy enable** command to communicate at Layer 3.
- In centralized forwarding mode, after an AS goes offline, traffic of its attached network cannot be forwarded by the parent and will be interrupted.
- In distributed forwarding mode, after an AS goes offline, in versions earlier than V200R012C00, downlink ports of the AS are automatically error down. As a result, traffic of the AS attached network will be interrupted. In V200R012C00 and later versions, downlink ports of the AS will not be error down, and traffic of the AS attached network will be forwarded as usual.

Example

Set the SVF forwarding mode to centralized forwarding.

```
<HUAWEI> system-view
[HUAWEI] uni-mng
[HUAWEI-um] forward-mode centralized
```

3.5.65 independent-as-admin

Function

The **independent-as-admin** command creates an administrator for AS login in independent mode.

The **undo independent-as-admin** command deletes the administrator for AS login in independent mode.

By default, no administrator is created for AS login in independent mode.

NOTE

This command can only be executed on a parent switch.

Format

independent-as-admin user *user-name* **password** *password*

undo independent-as-admin user

Parameters

Parameter	Description	Value

user *user-name*	Specifies a user name.	The value is a string of 1 to 64 characters. It cannot contain spaces, asterisk, double quotation mark and question mark.
		NOTE
		• During local authentication or authorization, run the **authentication-mode** { **local** | **local-case** } or **authorization-mode** { **local** | **local-case** } command to configure case sensitivity for user names. If the parameter is set to **local**, user names are case-insensitive. If the parameter is set to **local-case**, user names are case-sensitive.
		• Note the following when configuring case sensitivity for user names:
		  • Only the user name is case-sensitive and the domain name is case-insensitive.
		  • For user security purposes, you cannot configure multiple local users with the user names that differ only in uppercase or lowercase. For example, after configuring ABC, you cannot configure Abc or abc as the user name.
		  • When a device is upgraded from V200R011C10 or an earlier version to a version later than V200R011C10, all local user names in the original configuration file are saved in lowercase. When a configuration file that is manually configured or generated using the third-party tool is used for configuration restoration, local user names that differ only in uppercase or lowercase are considered as one user name and the first one among these local user names is used.

Parameter	Description	Value
password *password*	Specifies the password.	The value is a string of case-sensitive characters without spaces. A password in plain text is a string of 8 to 128 characters. A password in cipher text is a string of 48 to 188 characters and cannot be generated using the irreversible algorithm. The password is displayed in cipher text in the configuration file regardless of whether the password is input in plain or cipher text. Do not set this password to the weak password preset by running the **load security weak-password-dictionary** command.

Views

uni-mng view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

If the AS service configuration mode is set to independent mode, you need to use this command to configure the administrator account used to log in to ASs. After the configuration is complete, the user name and password used for login are automatically configured on the AS. The following configuration is generated on the AS:

```
#
aaa
 local-user user-name password irreversible-cipher password
 local-user user-name privilege level 3
 local-user user-name service-type terminal ssh
#
```

After an AS user name and password are configured, you need to enter the correct user name and password when logging in to an AS through the console port. When you log in to an AS from the parent using the **attach as name** *as-name* command, you can log in to the AS without entering the user name or password.

Precautions

The user name and password configured using this command take effect after the configuration is generated on ASs. It takes about 5 minutes for the configuration to take effect after you run the command. Do not log in to an AS within this period; otherwise, the configuration may take effect after a longer period of time.

Example

Create an AS administrator user name and password in independent mode.

```
<HUAWEI> system-view
[HUAWEI] uni-mng
[HUAWEI-um] independent-as-admin user test password YsHsjx_202206
```

3.5.66 interface fabric-port

Function

The **interface fabric-port** command creates a fabric port and displays the fabric port view.

The **undo interface fabric-port** command deletes a fabric port.

By default, no fabric port exists in the system.

NOTE

This command can only be executed on a parent switch.

Format

interface fabric-port *port-id*

undo interface fabric-port *port-id*

Parameters

Parameter	Description	Value
port-id	Specifies the number of a fabric port.	The value range on the parent varies depending on the switch model: • S12700/S12700E: 0 to 255 • MCUD/SRUK/MFUX/MPUE/SRUE/SRUHA1/SRUHX1/SRUH: 0 to 255 • Other switch models: 0 to 63

Views

uni-mng view

Default Level

3: Management level

Usage Guidelines

To set up an SVF system, create fabric ports on the parent switches to allow ASs to connect to the parent switches.

Example

Create a fabric port and enter the fabric port view.

```
<HUAWEI> system-view
[HUAWEI] uni-mng
[HUAWEI-um] interface fabric-port 1
```

3.5.67 ip source check user-bind enable (network enhanced profile view)

Function

The **ip source check user-bind enable** command configures IP packet checking in a network enhanced profile.

The **undo ip source check user-bind enable** command cancels IP packet checking in a network enhanced profile.

By default, IP packet checking is not configured in a network enhanced profile.

NOTE

This command can only be executed on a parent switch.

Format

ip source check user-bind enable

undo ip source check user-bind enable

Parameters

None

Views

Network enhanced profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After creating a network enhanced profile, you can configure IP packet checking in the profile. After the profile is bound to the port of an AS, IP packet checking is automatically enabled on the port. The following configuration is generated on the AS port:

```
#
 ip source check user-bind enable
 ip source check user-bind alarm enable
#
```


When attackers steal authorized users' IP addresses or MAC addresses to send packets to access or attack networks, authorized users cannot obtain stable and secure network services. After configuring IP packet checking on a device, the device checks received IP packets against the binding table to prevent such attacks.

Prerequisites

DHCP snooping has been enabled in the network enhanced profile using the **dhcp snooping enable** command.

Precautions

When an AS is an S2750-EI, S5700-10P-LI, or S5700-10P-PWR-LI and works in Layer 3 hardware forwarding mode, the **ip source check user-bind enable** command does not take effect on the AS. Because an AS performs only Layer 2 forwarding in an SVF system, you are advised to run the **undo assign forward-mode** command to cancel the Layer 3 hardware forwarding mode and then connect the AS to the SVF system.

Example

Configure IP packet checking in a network enhanced profile.

```
<HUAWEI> system-view
[HUAWEI] uni-mng
[HUAWEI-um] network-enhanced-profile name profile_1
[HUAWEI-um-net-enhanced-profile_1] dhcp snooping enable
[HUAWEI-um-net-enhanced-profile_1] ip source check user-bind enable
```

3.5.68 ipv6 (AS administrator profile view)

Function

The **ipv6** command enables IPv6 in an AS administrator profile.

The **undo ipv6** command disables IPv6 in an AS administrator profile.

By default, IPv6 is disabled in an AS administrator profile.

NOTE

This command can only be executed on a parent switch.

Format

ipv6

undo ipv6

Parameters

None

Views

AS administrator profile view

Default Level

3: Management level

Usage Guidelines

After creating an AS administrator profile, you can run the **ipv6** command to enable IPv6 for ASs in the profile. After an AS administrator profile is bound to an AS, the following configurations are generated globally on the AS:

```
#
ipv6
#
```

Example

Enable IPv6 in the AS administrator profile.

```
<HUAWEI> system-view
[HUAWEI] uni-mng
[HUAWEI-um] as-admin-profile name profile_1
[HUAWEI-um-as-admin-profile_1] ipv6
```

3.5.69 mac-address flapping action (network enhanced profile view)

Function

The **mac-address flapping action** command configures the action taken on an interface in case of MAC address flapping in a network enhanced profile.

The **undo mac-address flapping action** command deletes the action taken on an interface in case of MAC address flapping in a network enhanced profile.

By default, in a network enhanced profile, the system does not perform any action when detecting MAC address flapping on an interface.

NOTE

This command can only be executed on a parent switch.

Format

mac-address flapping action error-down

undo mac-address flapping action error-down

Parameters

Parameter	Description	Value
error-down	Configures the system to set an interface to the Error-Down state when detecting MAC address flapping on this interface.	-

Views

Network enhanced profile view

Default Level

3: Management level

Usage Guidelines

After creating a network enhanced profile, you can configure the action taken on an interface when MAC address flapping occurs on the interface in the profile. After the profile is bound to an AS port, the configuration is automatically delivered to the AS port. The following configuration is generated on the AS:

```
#
interface GigabitEthernet0/0/1
 mac-address flapping action error-down
#
```

In the preceding configuration, GigabitEthernet0/0/1 is used for reference only. The actual configuration is determined by the profile configuration.

Example

Configure the system to set an interface to the Error-Down state when detecting MAC address flapping on this interface.

```
<HUAWEI> system-view
[HUAWEI] uni-mng
[HUAWEI-um] network-enhanced-profile name profile_1
[HUAWEI-um-net-enhanced-profile_1] mac-address flapping action error-down
```

3.5.70 mac-address trap notification (network enhanced profile view)

Function

The **mac-address trap notification** command configures the alarm function for MAC address learning and aging in a network enhanced profile.

The **undo mac-address trap notification** command deletes the alarm function of MAC address learning and aging in a network enhanced profile.

By default, the alarm function for MAC address learning and aging is not configured in a network enhanced profile.

NOTE

This command can only be executed on a parent switch.

Format

mac-address trap notification all

undo mac-address trap notification

Parameters

Parameter	Description	Value
all	Indicates the alarm function for MAC address learning and aging.	-

Views

Network enhanced profile view

Default Level

3: Management level

Usage Guidelines

After creating a network enhanced profile, you can configure the alarm function for MAC address learning and aging in the profile. After the profile is bound to an AS port, the configuration is automatically delivered to the AS port. The following configuration is generated on the AS:

```
#
interface GigabitEthernet0/0/1
 mac-address trap notification all
#
```

In the preceding configuration, GigabitEthernet0/0/1 is used for reference only. The actual configuration is determined by the profile configuration.

Example

Configure the alarm function for MAC address learning and aging.

```
<HUAWEI> system-view
[HUAWEI] uni-mng
[HUAWEI-um] network-enhanced-profile name profile_1
[HUAWEI-um-net-enhanced-profile_1] mac-address trap notification all
```

3.5.71 mac-limit (user access profile view)

Function

The **mac-limit** command configures MAC address learning limiting in a user access profile.

The **undo mac-limit** command cancels MAC address learning limiting in a user access profile.

By default, MAC address learning limiting is not configured in a user access profile.

NOTE

This command can only be executed on a parent switch.

Format

mac-limit maximum *max-num*

undo mac-limit

Parameters

Parameter	Description	Value
maximum *max-num*	Specifies the maximum number of MAC addresses that can be learned on an interface.	The value is an integer that ranges from 0 to 4096. The value 0 indicates that the maximum number of MAC addresses that can be learned is not limited.

Views

User access profile view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

After creating a user access profile, you can configure MAC address learning limiting in the profile. When the profile is bound an AS port, MAC address learning limiting is automatically configured on the port. The following configuration is generated on the AS port:

```
#
 mac-limit maximum max-num
#
```

To control the number of access users and protect the MAC address table against attacks, you can limit the maximum number of MAC addresses that can be learned on an interface.

Precautions

The **mac-limit** and **authentication** commands are mutually exclusive and cannot be configured together in a user access profile.

Example

Configure MAC address learning limiting in a user access profile.

```
<HUAWEI> system-view
[HUAWEI] uni-mng
[HUAWEI-um] user-access-profile name profile_1
[HUAWEI-um-user-access-profile_1] mac-limit maximum 1024
```


3.5.72 multicast-suppression (network enhanced profile view)

Function

The **multicast-suppression** command configures unknown multicast traffic suppression in a network enhanced profile.

The **undo multicast-suppression** command cancels unknown multicast traffic suppression in a network enhanced profile.

By default, unknown multicast traffic suppression is not configured in a network enhanced profile.

NOTE

This command can only be executed on a parent switch.

Format

multicast-suppression packets *packets-per-second*

undo multicast-suppression

Parameters

Parameter	Description	Value
packets *packets-per-second*	Specifies the packet rate of an interface.	The value is an integer that ranges from 0 to 14881000, in packets per second (PPS). If the configured packet rate on the parent switch is larger than the maximum value on the AS port, the maximum value takes effect on the AS port.

Views

Network enhanced profile view

Default Level

3: Management level

Usage Guidelines

After creating a network enhanced profile, you can configure unknown multicast traffic suppression in the profile. After the profile is bound to an AS port, unknown multicast traffic suppression is automatically configured on the port. The following configuration is generated on the AS port:

```
#
 multicast-suppression packets packets-per-second
#
```

To prevent broadcast storms, you can run the **multicast-suppression** command to configure the maximum number of unknown multicast packets that can pass

through a port. When the unknown multicast traffic rate reaches the maximum value, the system discards excess unknown multicast packets to control the traffic volume within a proper range.

Example

Configure unknown multicast traffic suppression in a network enhanced profile.

```
<HUAWEI> system-view
[HUAWEI] uni-mng
[HUAWEI-um] network-enhanced-profile name profile_1
[HUAWEI-um-net-enhanced-profile_1] multicast-suppression packets 148810
```

3.5.73 network-basic-profile name

Function

The **network-basic-profile name** command creates a network basic profile.

The **undo network-basic-profile name** command deletes a network basic profile.

By default, no network basic profile is created.

NOTE

This command can only be executed on a parent switch.

Format

network-basic-profile name *profile-name*

undo network-basic-profile name *profile-name*

Parameters

Parameter	Description	Value
profile-name	Specifies the name of a network basic profile.	The value is a string of 1 to 31 case-sensitive characters without spaces. The value can contain letters, digits, and underscores (_).

Views

uni-mng view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

You can configure basic user services in a network basic profile, including the default VLAN, allowed VLAN, and voice VLAN of a port.

Precautions

You can create a maximum of 256 network basic profiles in a version earlier than V200R011C10.

You can create a maximum of 512 network basic profiles in V200R011C10 and later versions.

Example

Create a network basic profile.

```
<HUAWEI> system-view
[HUAWEI] uni-mng
[HUAWEI-um] network-basic-profile name profile_1
```

3.5.74 network-basic-profile (port group view)

Function

The **network-basic-profile** command binds a network basic profile to a port group.

The **undo network-basic-profile** command unbinds a network basic profile from a port group.

By default, no network basic profile is bound to a port group.

NOTE

This command can only be executed on a parent switch.

Format

network-basic-profile *profile-name*

undo network-basic-profile

Parameters

Parameter	Description	Value
profile-name	Specifies the name of a network basic profile.	The value must have an existing network basic profile name.

Views

Port group view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

You can bind a network basic profile to a port group to deliver the configurations in the profile to all the member ports in the port group.

Prerequisites

The network basic profile has been created.

Precautions

A port group can be bound to only one network basic profile.

Example

Bind a network basic profile to a port group.

```
<HUAWEI> system-view
[HUAWEI] uni-mng
[HUAWEI-um] network-basic-profile name profile_1
[HUAWEI-um-net-basic-profile_1] quit
[HUAWEI-um] port-group name group_1
[HUAWEI-um-portgroup-group_1] network-basic-profile profile_1
```

3.5.75 network-enhanced-profile name

Function

The **network-enhanced-profile name** command creates a network enhanced profile.

The **undo network-enhanced-profile name** command deletes a network enhanced profile.

By default, no network enhanced profile is created.

NOTE

This command can only be executed on a parent switch.

Format

network-enhanced-profile name *profile-name*

undo network-enhanced-profile name *profile-name*

Parameters

Parameter	Description	Value
profile-name	Specifies the name of a network enhanced profile.	The value is a string of 1 to 31 case-sensitive characters without spaces. The value can contain letters, digits, and underscores (_).

Views

uni-mng view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

You can configure value-added services in a network enhanced profile, such as network security and QoS.

Precautions

- You can create a maximum of 16 network enhanced profiles.
- A network enhanced profile can be bound to only an AS port group but not an AP port group.

Example

Create a network enhanced profile.

```
<HUAWEI> system-view
[HUAWEI] uni-mng
[HUAWEI-um] network-enhanced-profile name profile_1
```

3.5.76 network-enhanced-profile (port group view)

Function

The **network-enhanced-profile** command binds a network enhanced profile to a port group.

The **undo network-enhanced-profile** command unbinds a network enhanced profile from a port group.

By default, no network enhanced profile is bound to a port group.

NOTE

This command can only be executed on a parent switch.

Format

network-enhanced-profile *profile-name*

undo network-enhanced-profile

Parameters

Parameter	Description	Value
profile-name	Specifies the name of a network enhanced profile.	The value must have an existing network enhanced profile name.

Views

Port group view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

You can bind a network enhanced profile to a port group to deliver the configurations in the profile to all the member ports in the port group.

Prerequisites

The network enhanced profile has been created.

Precautions

- A network enhanced profile can be bound to only an AS port group but not an AP port group.
- A port group can be bound to only one network enhanced profile.

Example

Bind a network enhanced profile to a port group.

```
<HUAWEI> system-view
[HUAWEI] uni-mng
[HUAWEI-um] network-enhanced-profile name profile_1
[HUAWEI-um-net-enhanced-profile_1] quit
[HUAWEI-um] port-group name group_1
[HUAWEI-um-portgroup-group_1] network-enhanced-profile profile_1
```

3.5.77 network-qos-profile name

Function

The **network-qos-profile name** command creates a network QoS profile and displays the network QoS profile view.

The **undo network-qos-profile name** command deletes a network QoS profile.

By default, no network QoS profile is created.

NOTE

This command can only be executed on a parent switch.

Format

network-qos-profile name *profile-name*

undo network-qos-profile name *profile-name*

Parameters

Parameter	Description	Value
profile-name	Specifies the name of a network QoS profile.	The value is a string of 1 to 31 case-sensitive characters without spaces. The value can contain letters, digits, and underscores (_).

Views

uni-mng view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

A network QoS profile is used to configure QoS services for ASs on the parent, including the packet priority mapping mode, queue scheduling mode, and queue scheduling weight.

Precautions

- A maximum of 32 network QoS profiles can be created on the parent.
- A maximum of six network QoS profiles can be created on an AS.

Example

Create a network QoS profile.

```
<HUAWEI> system-view
[HUAWEI] uni-mng
[HUAWEI-um] network-qos-profile name test
[HUAWEI-um-net-qos-test]
```

3.5.78 network-qos-profile (port group view)

Function

The **network-qos-profile** command binds a network QoS profile to a port group.

The **undo network-qos-profile** command unbinds a network QoS profile from a port group.

By default, no network QoS profile is bound to a port group.

NOTE

This command can only be executed on a parent switch.

Format

network-qos-profile *profile-name*

undo network-qos-profile

Parameters

Parameter	Description	Value
profile-name	Specifies the name of a network QoS profile.	The value must be an existing network QoS profile name.

Views

Port group view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

You can bind a network QoS profile to a port group to deliver the configurations in the profile to all the member ports in the port group in a batch.

Prerequisites

The network QoS profile has been created before being bound to a port group.

Precautions

- A network QoS profile can be bound to only an AS port group but not an AP port group.
- A port group can be bound to only one network QoS profile.

Example

Bind a network QoS profile to a port group.

```
<HUAWEI> system-view
[HUAWEI] uni-mng
[HUAWEI-um] network-qos-profile name test
[HUAWEI-um-net-qos-test] trust dscp
[HUAWEI-um-net-qos-test] quit
```



```
[HUAWEI-um] port-group name group_1
[HUAWEI-um-portgroup-group_1] network-qos-profile test
```

3.5.79 pass-vlan (network basic profile view)

Function

The **pass-vlan** command configures allowed VLANs in a network basic profile.

The **undo pass-vlan** command deletes allowed VLANs in a network basic profile.

By default, no allowed VLANs are configured in a network basic profile, and downlink ports of an AS allow packets from VLAN 1 to pass through.

NOTE

This command can only be executed on a parent switch.

Format

pass-vlan { *vlan-id1* [**to** *vlan-id2*] } &<1-10>

undo pass-vlan { *vlan-id1* [**to** *vlan-id2*] } &<1-10>

Parameters

Parameter	Description	Value
vlan-id1 [**to** *vlan-id2*]	Specifies IDs of VLANs from which packets are allowed to pass through.	The value is an integer that ranges from 1 to 4094. The value cannot be the ID of an SVF management VLAN, a stack management VLAN, an ERPS control VLAN, an RRPP control VLAN, an SEP control VLAN, or a super VLAN.

Views

Network basic profile view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

After creating a network basic profile, you can configure allowed VLANs in the profile. After the profile is bound to an AS port, the port allows packets from these VLANs to pass through. The following configuration is generated on the AS port:

```
#
 port link-type hybrid
```



```
 port hybrid tagged vlan vlan-id1 to vlan-id2
#
```

Precautions

- The default VLAN, allowed VLANs, and voice VLAN in a network basic profile must be different.
- You can configure a maximum of 32 allowed VLANs in a network basic profile.

Example

Configured allowed VLANs in a network basic profile.

```
<HUAWEI> system-view
[HUAWEI] uni-mng
[HUAWEI-um] network-basic-profile name profile_1
[HUAWEI-um-net-basic-profile_1] pass-vlan 10 to 12
```

3.5.80 patch delete as

Function

The **patch delete as** command deletes patches on a specified online AS.

NOTE

This command can only be executed on a parent switch.

Format

patch delete as { **all** | **name** *patch-name* | **name-include** *string* }

Parameters

Parameter	Description	Value
all	Indicates all online ASs.	-
name *patch-name*	Specifies the name of an AS.	The value is a string of 1 to 31 case-insensitive characters without spaces.
name-include *string*	Specifies the string contained in an AS name.	The value is a string of 1 to 31 case-insensitive characters without spaces.

Views

uni-mng view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

If you find errors in the patches loaded to an AS, run this command to delete the patches to prevent system operation failures.

If non-incremental patches need to be loaded to an AS, you need to run the **patch delete as** command to delete the existing patches on the AS first. Otherwise, non-incremental patches will fail to be loaded.

Precautions

If the patch file to be loaded to an AS type has been specified using the **as type** command, patches on this AS type cannot be deleted.

Example

Delete the patches on as1.

```
<HUAWEI> system-view
[HUAWEI] uni-mng
[HUAWEI-um] patch delete as name as1
Warning: This command will start to delete the patch of AS. Continue?[Y/N]:y
Info: This operation will take several seconds, please wait...
```

3.5.81 policy (traffic policy profile view)

Function

The **policy** command configures a traffic policy in a traffic policy profile.

The **undo policy** command deletes a traffic policy in a traffic policy profile.

By default, no traffic policy is configured in a traffic policy profile.

NOTE

This command can only be executed on a parent switch.

Format

policy *policy-name* **remark** { **8021p** { *8021p-value* | **inner-8021p** } | **cvlan-id** *cvlan-id* | **dscp** { *dscp-value* | *dscp-name* } | **ip-precedence** *ip-precedence* | **local-precedence** { *local-precedence-value* | *local-precedence-name* } [**green** | **yellow** | **red**] | **vlan-id** *vlan-id* | **flow-id** *flow-id* | **destination-mac** *mac-address* }* **if-match acl** *acl-number*

undo policy *policy-name*

Parameters

Parameter	Description	Value
policy-name	Specifies the name of a traffic policy.	The value is a string of 1 to 64 case-sensitive characters without spaces. If the string is enclosed in double quotation marks (" "), the string can contain spaces.
remark	Specifies re-marking information.	-
8021p	Specifies the 802.1p priority of packets.	-
8021p-value	Specifies the 802.1p priority value of packets.	The value is an integer in the range from 0 to 7. A larger value indicates a higher priority.
inner-8021p	Inherits the 802.1p priority in the inner tag.	-
cvlan-id *cvlan-id*	Re-marks the inner VLAN tag in QinQ packets.	The value is an integer in the range from 1 to 4094.
dscp	Specifies the DSCP priority of packets.	-
dscp-value	Specifies the DSCP priority value of packets.	The value is an integer in the range from 0 to 63. A larger value indicates a higher priority.
dscp-name	Specifies the DSCP priority name of packets.	The value can be: **ef**, **af11**, **af12**, **af13**, **af21**, **af22**, **af23**, **af31**, **af32**, **af33**, **af41**, **af42**, **af43**, **cs1**, **cs2**, **cs3**, **cs4**, **cs5**, **cs6**, **cs7**, or **default**.
ip-precedence *ip-precedence*	Specifies the IP precedence.	The value is an integer in the range from 0 to 7. A larger value indicates a higher priority.
local-precedence	Specifies the local priority of packets.	-

Parameter	Description	Value
local-precedence-value	Specifies the local priority value.	The value is an integer in the range from 0 to 7. A larger value indicates a higher priority.
local-precedence-name	Specifies the local priority name.	The value can be: **af1**, **af2**, **af3**, **af4**, **be**, **cs6**, **cs7**, or **ef**.
green	Indicates that the packet color corresponding to the local priority is green.	-
yellow	Indicates that the packet color corresponding to the local priority is yellow.	-
red	Indicates that the packet color corresponding to the local priority is red.	-
vlan-id *vlan-id*	Re-marks a VLAN ID in packets.	The value is an integer in the range from 1 to 4094.
flow-id *flow-id*	Specifies the value of a flow ID.	The value is an integer in the range from 1 to 8.
destination-mac *mac-address*	Re-marks the destination MAC address in packets.	The value is in the format of H-H-H, in which H is a hexadecimal number of 1 to 4 digits.
if-match	Specifies an ACL rule for matching packets.	-
acl *acl-number*	Specifies an ACL rule number.	The value is an integer in the range from 3000 to 3900.

Views

Traffic policy profile view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

After creating a traffic policy profile, you can configure traffic behaviors and traffic classifiers in the profile. After the profile is bound to an AS port, the traffic behaviors and traffic classifiers are automatically configured on the port.

The following global configuration is generated on the AS:

```
#
traffic classifier classifier-name operator or
 if-match acl-number
#
traffic behavior behavior-name
 remark xxxx
#
```

The following configuration is generated on the AS port:

```
#
 traffic-policy profile-name inbound
#
```

Or:

```
#
 traffic-policy profile-name outbound
#
```

Precautions

- A maximum of 64 traffic policies can be created in a traffic policy profile.
- **remark 8021p** and **remark local-precedence** cannot be configured in the same traffic policy.
- **remark dsc** and **remark ip-precedence** cannot be configured in the same traffic policy.

Example

Configured allowed VLANs in a traffic policy profile.

```
<HUAWEI> system-view
[HUAWEI] uni-mng
[HUAWEI-um] traffic-policy-profile name profile_1
[HUAWEI-um-traffic-policy-profile_1] policy a remark 8021p 2 if-match acl 3456
```

3.5.82 port connect independent-as

Function

The **port connect independent-as** command enables the independent mode on the fabric port that connects the parent to a level-1 AS.

The **undo port connect** command restores the default mode of the fabric port that connects the parent to a level-1 AS.

By default, the service configuration mode of the fabric port that connects the parent to a level-1 AS is centralized mode.

NOTE

This command can only be executed on a parent switch.

Format

port connect independent-as

undo port connect

Parameters

None

Views

Fabric-port view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

In independent mode, you can log in to an AS to configure this AS using commands. After the independent mode is enabled on the fabric port that connects the parent to a level-1 AS, the level-1 AS can be configured independently.

Precautions

- Before enabling the independent mode, run the **independent-as-admin** command in the uni-mng view to configure an administrator for AS login.
- If the AS connected to a fabric port is online, running the **undo port connect** command on the fabric port for mode switching will cause the AS to automatically restart and register with the parent again. Switching from the centralized mode to the independent mode does not cause the AS to restart.
- During mode switching on a fabric port, the parent and AS exchange packets for multiple times. In this process, if faults occur, for example, link or device faults, mode switching may fail. An error message will be displayed on the parent, indicating that mode switching fails. Additionally, the AS may restart and then registers with the parent again. In this situation, run commands on the fabric port again to change the mode after the AS has registered with the parent.
- In independent mode, when an AS goes offline, traffic on the network attached to an AS port cannot be forwarded if the port has authentication configurations. To enable the traffic to be forwarded normally, manually delete the authentication configurations from the port.
- When the service configuration mode of an AS is independent mode, configuring the following commands on the Eth-Trunk bound to or on the member port of a fabric port connected to the AS may cause this AS to go offline.

Table 3-120 Commands that may cause an AS to go offline

Command
loopback internal

Command
traffic-policy
traffic-filter
speed
negotiation
port media-type
port split
training disable
wavelength-channel
undo port hybrid tagged vlan
undo port trunk allow-pass vlan
storm-control action
mac-address flapping action
port-security protect-action

- If the Eth-Trunk bound to a fabric port has other configurations in addition to the following **Table 2** and **Table 3**, you need to manually delete the other configurations before running the **undo port connect** command on this fabric port for mode switching. Otherwise, an error message will be displayed to indicate that mode switching fails.

  Table 3-121 Commands that can not be manually deleted in an Eth-Trunk

Command
port link-type hybrid
port hybrid tagged vlan

  Table 3-122 Commands that do not need to be manually deleted in an Eth-Trunk

Command
undo port hybrid vlan
stp root-protection
stp edged-port disable
loop-detection disable

Command
mode lacp
mad relay
trust 8021p
authentication-profile
authentication control-point

Example

Enable the independent mode on the fabric port that connects the parent to a level-1 AS.

```
<HUAWEI> system-view
[HUAWEI] uni-mng
[HUAWEI-um] interface fabric-port 1
[HUAWEI-um-fabric-port-1] port connect independent-as
```

3.5.83 port connect-type indirect

Function

The **port connect-type indirect** command configures the indirect connection mode for a fabric port.

The **undo port connect-type** command restores the default connection mode for a fabric port.

The default connection mode of a fabric port is direct connection.

NOTE

This command can only be executed on a parent switch.

Format

port connect-type indirect

undo port connect-type

Parameters

None

Views

Fabric-port view

Default Level

3: Management level

Usage Guidelines

When the parent connects to an AS across a network, you need to run the **port connect-type indirect** command to configure the indirect connection mode for the fabric port that connects the parent to the AS.

Prerequisites

No Eth-Trunk is bound to the fabric port.

Follow-up Procedure

Run the **port member-group interface** command to bind an Eth-Trunk to the fabric port.

Example

Configure the indirect connection mode for a fabric port.

```
<HUAWEI> system-view
[HUAWEI] uni-mng
[HUAWEI-um] interface fabric-port 1
[HUAWEI-um-fabric-port-1] port connect-type indirect
```

3.5.84 port-group name

Function

The **port-group name** command creates an AS port group.

The **port-group connect-ap name** command creates an AP port group.

The **undo port-group name** command deletes an AS port group.

The **undo port-group connect-ap name** command deletes an AP port group.

By default, no AS port group is created.

NOTE

This command can be executed only on a parent switch of models except the S6735-S, S6720-EI, S6720S-EI, S6720-SI, S6720S-SI, S6720S-S,S6730-S, or S6730S-S.

Format

port-group name *group-name*

port-group connect-ap name *group-name*

undo port-group name *group-name*

undo port-group connect-ap name *group-name*

Parameters

Parameter	Description	Value
group-name	Specifies the name of a port group.	The value is a string of 1 to 31 case-sensitive characters without spaces. The value can contain letters, digits, and underscores (_).

Views

uni-mng view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

A port group is a set of AS ports. The purpose of a port group is to facilitate batch configuration of AS ports.

Port groups are classified into AS port groups and AP port groups.

- Ports in an AS port group are used to connect an AS to a user terminal. An AS port group can be bound to four types of service profiles (network basic profile, network enhanced profile, user access profile, traffic policy profile, and network qos profile), but only one profile of the same type can be bound.
- Ports in an AP port group are used to connect an AS to an AP. To connect an AP to an AS, you need to add the port that connects the AS to the AP to an AP port group. An AP port group can be bound to only a network basic profile, and only the **pass-vlan** { *vlan-id1* [**to** *vlan-id2*] } &<1-10> command configured in the profile takes effect.

Follow-up Procedure

Run the **as name** *as-name* or **as name-include** *string* **interface all** command to add AS ports to a port group.

Precautions

- You can create a maximum of 256 AS port groups in a version earlier than V200R011C10.

  You can create a maximum of 512 AS port groups in V200R011C10 and later versions.
- You can create a maximum of 1 AP port group.

Example

Create a port group.


```
<HUAWEI> system-view
[HUAWEI] uni-mng
[HUAWEI-um] port-group name group_1
```

3.5.85 port eth-trunk trunkmember

Function

The **port eth-trunk trunkmember** command adds member ports to the Eth-Trunk.

The **undo port eth-trunk trunkmember** command deletes member ports from an Eth-Trunk.

By default, no member ports are added to the Eth-Trunk.

NOTE

This command can only be executed on a parent switch.

Format

port eth-trunk *trunk-id* **trunkmember interface** *interface-type interface-number1* [**to** *interface-number2*]

undo port eth-trunk *trunk-id* **trunkmember interface** *interface-type interface-number1* [**to** *interface-number2*]

Parameters

Parameter	Description	Value
trunk-id	Specifies the ID of an Eth-Trunk.	The value is an integer and the minimum value is 1. The maximum value varies according to the switch model. For a specific switch model, the maximum value is the same as that described in **interface eth-trunk**.
interface *interface-type interface-number1* [**to** *interface-number2*]	Specifies the type and number of the interface added to an Eth-Trunk: • *interface-type* specifies the interface type. • *interface-number1* specifies the first interface number. • *interface-number2* specifies the last interface number.	-

Views

AS view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

After a downlink fabric port of a level-1 AS is configured using the **down-direction fabric-port** *port-id* **member-group interface eth-trunk** *trunk-id* command, you need to add member ports to the Eth-Trunk to which the fabric port is bound.

When an Eth-Trunk has been created for an AS using the **uni eth-trunk** command, you can run the **port eth-trunk trunkmember** command to add member ports to this Eth-Trunk.

Precautions

AS uplink ports can be used to connect to the parent or level-1 AS or set up a stack and be configured as downlink fabric ports to connect to other ASs.

On the S6720-EI and S6720S-EI, 40GE ports and 10GE ports split from 40GE ports cannot be configured as downlink fabric ports.

Example

Add member ports to the Eth-Trunk to which a fabric port is bound.

```
<HUAWEI> system-view
[HUAWEI] uni-mng
[HUAWEI-um] as name as1
[HUAWEI-um-as-as1] down-direction fabric-port 1 member-group interface eth-trunk 1
[HUAWEI-um-as-as1] port eth-trunk 1 trunkmember interface gigabitethernet 0/0/16
```

Add member ports to the Eth-Trunk configured on the specified AS.

```
<HUAWEI> system-view
[HUAWEI] uni-mng
[HUAWEI-um] as name as1
[HUAWEI-um-as-as1] uni eth-trunk 40
[HUAWEI-um-as-as1] port eth-trunk 40 trunkmember interface GigabitEthernet 0/0/10
```

3.5.86 port member-group interface

Function

The **port member-group interface** command binds a fabric port to an Eth-Trunk.

The **undo port member-group** command unbinds a fabric port from an Eth-Trunk.

By default, no fabric port is bound to an Eth-Trunk.

NOTE

This command can only be executed on a parent switch.

Format

port member-group interface eth-trunk *trunk-id*

undo port member-group

Parameters

Parameter	Description	Value
eth-trunk *trunk-id*	Specifies the ID of the Eth-Trunk to which a fabric port is bound.	The value is an integer that ranges from 0 to 127.

Views

Fabric-port view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

After creating a fabric port using the **interface fabric-port** *port-id* command, bind the fabric port to an Eth-Trunk.

Follow-up Procedure

Run the **eth-trunk** *trunk-id* command in the interface view to add interfaces to the bound Eth-Trunk.

Precautions

- After the **port connect independent-as** command is executed to enable the independent configuration mode, you need to run the **undo port connect** command to restore to the centralized configuration mode before unbinding a fabric port from an Eth-Trunk.
- A created Eth-Trunk cannot be bound to a fabric port. When a fabric port is bound to an Eth-Trunk, the system creates the Eth-Trunk.
- You can run the **interface eth-trunk** command to enter the view of the Eth-Trunk to which a fabric port is bound and configure services. Currently, the following commands can be executed in the view of the Eth-Trunk to which a fabric port is bound: **authentication open ucl-policy enable**, **mac-address multiport**, **quit**, and all display commands.
- If physical member interfaces have been added to the Eth-Trunk bound to a fabric port, the **undo port member-group** command cannot be used to unbind the fabric port from the Eth-Trunk.

- Running the **undo port member-group** command will delete the configuration in the Eth-Trunk interface view and delete the Eth-Trunk.
- When a fabric port is bound to an Eth-Trunk, the system creates the Eth-Trunk and performs some service configurations on the Eth-Trunk, for example, the **stp root-protection** and **mad relay** command configurations.

Example

Bind a fabric port to an Eth-Trunk.

```
<HUAWEI> system-view
[HUAWEI] uni-mng
[HUAWEI-um] interface fabric-port 1
[HUAWEI-um-fabric-port-1] port member-group interface eth-trunk 11
```

3.5.87 port-security aging-time (network enhanced profile view)

Function

The **port-security aging-time** command sets the aging time of secure dynamic MAC addresses on an interface in a network enhanced profile.

The **undo port-security aging-time** command cancels the configuration.

By default, the aging time of secure dynamic MAC addresses is not configured in a network enhanced profile, that is, secure dynamic MAC addresses will not be aged out.

NOTE

This command can only be executed on a parent switch.

Format

port-security aging-time *time*

undo port-security aging-time

Parameters

Parameter	Description	Value
time	Specifies the aging time of secure dynamic MAC address entries.	The value is an integer ranging from 1 to 1440, in minutes.

Views

Network enhanced profile view

Default Level

3: Management level

Usage Guidelines

Application scenario

After creating a network enhanced profile, you can set the aging time of secure dynamic MAC addresses in the profile. After the profile is bound to an AS port, the configuration is automatically delivered to the AS port. The following configuration is generated on the AS:

```
#
interface GigabitEthernet0/0/1
 port-security enable
 port-security aging-time 10
#
```

In the preceding configuration, GigabitEthernet0/0/1 is used for reference only. The actual configuration depends on the profile.

Prerequisites

Before setting the aging time of secure dynamic MAC addresses in a network enhanced profile, ensure that port security is enabled in the profile.

Example

Set the aging time of secure dynamic MAC addresses on an interface to 10 minutes.

```
<HUAWEI> system-view
[HUAWEI] uni-mng
[HUAWEI-um] network-enhanced-profile name profile_1
[HUAWEI-um-net-enhanced-profile_1] port-security enable
[HUAWEI-um-net-enhanced-profile_1] port-security aging-time 10
```

3.5.88 port-security enable (network enhanced profile view)

Function

The **port-security enable** command enables port security in a network enhanced profile.

The **undo port-security enable** command disables port security in a network enhanced profile.

By default, port security is disabled in a network enhanced profile.

NOTE

This command can only be executed on a parent switch.

Format

port-security enable

undo port-security enable

Parameters

None

Views

Network enhanced profile view

Default Level

3: Management level

Usage Guidelines

Application scenario

After creating a network enhanced profile, you can enable port security in the profile. After the profile is bound to an AS port, the configuration is automatically delivered to the AS port. The following configuration is generated on the AS:

```
#
interface GigabitEthernet0/0/1
 port-security enable
#
```

In the preceding configuration, GigabitEthernet0/0/1 is used for reference only. The actual configuration depends on the profile.

Prerequisites

- If the **mac-limit** command is configured in the user access profile view on an AS port bound to a network enhanced profile, the port security function cannot be enabled on the AS port.
- The port security function cannot be disabled in a network enhanced profile if other port security configurations exist in the profile.

Example

Enable port security in a network enhanced profile.

```
<HUAWEI> system-view
[HUAWEI] uni-mng
[HUAWEI-um] network-enhanced-profile name profile_1
[HUAWEI-um-net-enhanced-profile_1] port-security enable
```

3.5.89 port-security mac-address sticky (network enhanced profile view)

Function

The **port-security mac-address sticky** command enables the sticky MAC address function in a network enhanced profile.

The **undo port-security mac-address sticky** command disables the sticky MAC address function in a network enhanced profile.

By default, the sticky MAC address function is disabled in a network enhanced profile.

NOTE

This command can only be executed on a parent switch.

Format

port-security mac-address sticky

undo port-security mac-address sticky

Parameters

None

Views

Network enhanced profile view

Default Level

3: Management level

Usage Guidelines

Application scenario

After creating a network enhanced profile, you can enable the sticky MAC address function in the profile. After the profile is bound to an AS port, the configuration is automatically delivered to the AS port. The following configuration is generated on the AS:

```
#
interface GigabitEthernet0/0/1
 port-security enable
 port-security mac-address sticky
#
```

In the preceding configuration, GigabitEthernet0/0/1 is used for reference only. The actual configuration depends on the profile.

Prerequisites

Before enabling the sticky MAC address function in a network enhanced profile, ensure that port security has been enabled in the profile.

Example

Configure the system to set an interface to the Error-Down state when detecting MAC address flapping on the interface.

```
<HUAWEI> system-view
[HUAWEI] uni-mng
[HUAWEI-um] network-enhanced-profile name profile_1
[HUAWEI-um-net-enhanced-profile_1] port-security enable
[HUAWEI-um-net-enhanced-profile_1] port-security mac-address sticky
```

3.5.90 portal url-encode disable

Function

The **portal url-encode disable** command disables the URL encoding function of ASs.

The **undo portal url-encode disable** command enables the URL encoding function of ASs.

By default, the URL encoding function of AS is enabled.

NOTE

This command can only be executed on a parent switch.

Format

portal url-encode disable

undo portal url-encode disable

Parameters

None

Views

uni-mng view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

To improve web application security, data from untrustworthy sources must be encoded before being sent to clients. URL encoding is most commonly used in web applications. After URL encoding is enabled for ASs, special characters in redirect URLs are converted to secure formats, preventing clients from mistaking them for syntax signs or instructions and unexpectedly modifying the original syntax. In this way, cross-site scripting attacks and injection attacks are prevented. By default, URL encoding is enabled in ASs. This function can be disabled using the **portal url-encode disable** command.

Precautions

If the system software is upgraded from a version earlier than V200R009C00SPC500 to V200R009C00SPC500 or a later version, the switch automatically runs the **portal url-encode disable** command to disable URL encoding and decoding.

Example

Disable URL encoding.

```
<HUAWEI> system-view
[HUAWEI] uni-mng
[HUAWEI-um] portal url-encode disable
```

3.5.91 qos { pq | wrr | drr } (network QoS profile view)

Function

The **qos** { **pq** | **wrr** | **drr** } command configures the queue scheduling mode for an AS port.

The **undo qos** { **pq** | **wrr** | **drr** } command restores the default queue scheduling mode of an AS port.

By default, no interface queue scheduling mode is configured in the network QoS profile view.

NOTE

This command can only be executed on a parent switch.

Format

qos { **pq** | **wrr** | **drr** }

undo qos { **pq** | **wrr** | **drr** }

Parameters

Parameter	Description	Value
pq	Indicates the PQ scheduling mode.	-
wrr	Indicates the WRR scheduling mode.	-
drr	Indicates the WDRR scheduling mode.	-

Views

Network QoS profile view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

When congestion occurs on a network, configure the interface queue scheduling mode to balance between the delay and jitter of various service packets. In this way, packets of delay-sensitive services, such as voice and video services, can be processed preferentially. Among delay-insensitive services, such as the email service, the packets with the same priority are processed equally and the packets with different priorities are processed based on their weights.

In an SVF system, to change the queue scheduling mode of an AS port, run the **qos** { **pq** | **wrr** | **drr** } command in the network QoS profile view and then bind the profile to the AS port.

Precautions

If the queue scheduling weight has been configured using the **qos queue** command before the queue scheduling mode is configured, delete the configured queue scheduling weight first.

Example

Set the queue scheduling mode of an AS port to WDRR.

```
<HUAWEI> system-view
[HUAWEI] uni-mng
[HUAWEI-um] network-qos-profile name test
[HUAWEI-um-net-qos-test] qos drr
```

3.5.92 qos queue (network QoS profile view)

Function

The **qos queue** command configures a queue scheduling weight for an AS.

The **undo qos queue** command restores the default queue scheduling weight of an AS.

By default, the queue scheduling weight is 1.

NOTE

This command can only be executed on a parent switch.

Format

qos queue *queue-index* { **drr** | **wrr** } **weight** *weight*

undo qos queue *queue-index* { **drr** | **wrr** }

Parameters

Parameter	Description	Value
queue-index	Specifies the index of a queue.	The value is an integer that ranges from 0 to 7.
drr	Specifies the WDRR scheduling weight.	-
wrr	Specifies the WRR scheduling weight.	-
weight *weight*	Specifies the scheduling weight.	The value is an integer that ranges from 0 to 127.

Views

Network QoS profile view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

If congestion occurs during queue scheduling, to ensure that each queue can be scheduled, configure a scheduling weight for each queue so that the device schedules each queue based on the configured scheduling weights.

In an SVF system, to change the queue scheduling weight of an AS port, run the **qos queue** command in the network QoS profile view and then bind the profile to the AS port.

Prerequisites

The queue scheduling mode of an AS port has been set to WRR or WDRR using the **qos { pq | wrr | drr }** command.

Example

Set the WDRR scheduling weight of queue 4 in a network QoS profile to 6.

```
<HUAWEI> system-view
[HUAWEI] uni-mng
[HUAWEI-um] network-qos-profile name test
[HUAWEI-um-net-qos-test] qos drr
[HUAWEI-um-net-qos-test] qos queue 4 drr weight 6
```

3.5.93 rate-limit (network enhanced profile view)

Function

The **rate-limit** command configures traffic rate limiting in a network enhanced profile.

The **undo rate-limit** command cancels traffic rate limiting in a network enhanced profile.

By default, traffic rate limiting is not configured in a network enhanced profile.

NOTE

This command can only be executed on a parent switch.

Format

rate-limit *cir-value*

undo rate-limit

Parameters

Parameter	Description	Value
cir-value	Specifies the committed information rate (CIR), which is the allowed rate at which traffic can pass through.	The value is an integer that ranges from 64 to 1000000, in kbit/s. The packet rate range of an interface depends on the interface bandwidth,If the configured packet rate is larger than the maximum value, the maximum value takes effect.

Views

Network enhanced profile view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

After creating a network enhanced profile, you can configure traffic rate limiting in the profile. After the profile is bound to an AS port, traffic rate limiting is automatically configured on the port. The following configuration is generated on the AS port:

```
#
 qos lr inbound cir cir-value cbs 125*cir-value
#
```

If user traffic is not limited, continuous burst data from numerous users can make the network congested. You can configure traffic rate limiting in inbound direction on an interface to limit traffic entering from the interface within a specified range.

Precautions

When an AS is an S2750-EI, S5700-10P-LI, or S5700-10P-PWR-LI switch and works in Layer 3 hardware forwarding mode, the **rate-limit** *cir-value* command does not take effect on the AS. Because an AS performs only Layer 2 forwarding in an SVF system, you are advised to run the **undo assign forward-mode** command to cancel the Layer 3 hardware forwarding mode and then connect the AS to the SVF system.

Example

Configure traffic rate limiting in a network enhanced profile.

```
<HUAWEI> system-view
[HUAWEI] uni-mng
[HUAWEI-um] network-enhanced-profile name profile_1
[HUAWEI-um-net-enhanced-profile_1] rate-limit 100000
```


3.5.94 reboot uni-mng

Function

The **reboot uni-mng** command restarts an SVF system.

NOTE

This command can only be executed on a parent switch.

Format

reboot uni-mng

Parameters

None

Views

User view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

When upgrading or troubleshooting an SVF system, you can restart the SVF system, including the parent and all ASs.

Precautions

- This command can be used only after the SVF function is enabled.
- The next startup software version of the AS must be V200R011C10 or later, and the next startup software version of the parent cannot be earlier than that of the AS.
- Before running this command to restart an SVF system, you must save the configuration of the parent. If an AS is configured in independent mode, you also need to save the configuration of the AS.

Example

Restart an SVF system.

```
<HUAWEI> reboot uni-mng
```

3.5.95 reset uni-mng as-discover packet statistics

Function

The **reset uni-mng as-discover packet statistics** command clears AS Discovery packet statistics on a fabric port.

NOTE

This command can be used on the parent or an AS. After running this command, you can clear AS Discovery packet statistics on a fabric port of the local device.

Format

reset uni-mng as-discover packet statistics interface fabric-port *port-id*

Parameters

Parameter	Description	Value
interface fabric-port *port-id*	Specifies the number of a fabric port.	The value is an integer that ranges from 0 to 63 on an AS and the value range on the parent varies depending on the switch model: • S12700/S12700E: 0 to 255 • MCUD/SRUK/MFUX/MPUE/SRUE/SRUHA1/SRUHX1/SRUH: 0 to 255 • Other switch models: 0 to 63

Views

User view

Default Level

3: Management level

Usage Guidelines

Before collecting statistics about AS Discovery packets on a fabric port, clear the existing statistics.

Example

Clear AS Discovery packet statistics on a fabric port.

```
<HUAWEI> reset uni-mng as-discover packet statistics interface fabric-port 1
```


3.5.96 shutdown interface

Function

The **shutdown interface** command disables an AS port.

The **undo shutdown interface** command enables an AS port.

By default, an interface is enabled.

NOTE

This command can only be executed on a parent switch.

Format

shutdown interface *interface-type interface-number*

undo shutdown interface *interface-type interface-number*

Parameters

Parameter	Description	Value
interface-type interface-number	Specifies the interface type and number. • *interface-type* specifies the interface type. The interface type cannot be an Eth-Trunk interface. • *interface-number* specifies the interface number.	-

Views

AS view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

You can run the **shutdown interface** command to disable an AS port.

Precautions

Running this command can disable only an AS downlink port but not an AS uplink port. If an uplink port has been configured as a downlink fabric port, this port can be disabled.

If the version of an AS is inconsistent with that of the parent, the **shutdown interface** and **undo shutdown interface** commands do not take effect on the ports of this AS.

If an AS is configured in the independent mode, the **shutdown interface** and **undo shutdown interface** commands do not take effect on the ports of this AS.

Example

Disable an AS port.

```
<HUAWEI> system-view
[HUAWEI] uni-mng
[HUAWEI-um] as name as1
[HUAWEI-um-as-as1] shutdown interface gigabitethernet 0/0/1
```

3.5.97 slot

Function

The **slot** command pre-configures a stack ID or changes the pre-configured device model.

The **undo slot** command deletes the pre-configured stack ID or changes the pre-configured device model.

By default, the pre-configured stack ID is 0.

NOTE

This command can only be executed on a parent switch.

Format

slot *slot-id1* **replace-model** *model-name*

undo slot *slot-id1* **replace-model**

slot *slot-id2* [**to** *slot-id3*] [**replace-model** *model-name*]

undo slot *slot-id2* [**to** *slot-id3*] [**replace-model**]

Parameters

Parameter	Description	Value
slot-id1	Specifies the pre-configured stack ID.	The value is 0.
slot-id2 [**to** *slot-id3*]	Specifies the pre-configured stack ID. *slot-id3* must be larger than *slot-id2*.	The value is an integer that ranging from 1 to 4.
replace-model *model-name*	Specifies the device model of which the stack ID needs to be pre-configured.	The value range depends on the device configuration.

Views

AS view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

When an AS is a stack of multiple member switches, the system pre-configures only stack ID 0 by default. You can only pre-configure services for the member switch with stack ID 0. Before pre-configuring services for another member switch, pre-configure a stack ID for the member switch.

The pre-configured stack ID does not affect the actual stack ID. For example, the pre-configured stack ID is 0 (default value), but the actual stack IDs are 0 and 2. The actual stack IDs remain 0 and 2 except that no services are configured on the device with stack ID 2.

An AS can be a stack of the same device series but different device models. If the stack contains different device models, you need to specify the **replace-model** parameter to change the device model that is different from the other device models in the stack to the actual access device model. If you do not specify the device model of a specified member, by default, the device model of this member is consistent with the pre-configured AS type.

Precautions

If the AS does not support stacking, the **slot** *slot-id* command configuration takes effect on the parent only when slot 0 is configured as the stack ID.

Changing the device models of online devices in a stack is not allowed.

Example

Pre-configure a stack ID.

```
<HUAWEI> system-view
[HUAWEI] uni-mng
[HUAWEI-um] as name as1
[HUAWEI-um-as-as1] slot 1 to 4
```

Change the device model of the switch with stack ID 2 in the AS **as1** to S5720-28X-SI-AC.

```
<HUAWEI> system-view
[HUAWEI] uni-mng
[HUAWEI-um] as name as1
[HUAWEI-um-as-as1] slot 2 replace-model S5720-28X-SI-AC
```

3.5.98 stp bpdu-protection (AS administrator profile)

Function

The **stp bpdu-protection** command configures BPDU protection for ASs in an AS administrator profile.

The **undo stp bpdu-protection** command cancels BPDU protection of ASs in an AS administrator profile.

By default, BPDU protection is not configured for ASs in an AS administrator profile.

NOTE

This command can only be executed on a parent switch.

Format

stp bpdu-protection

undo stp bpdu-protection

Parameters

None

Views

AS administrator profile view

Default Level

3: Management level

Usage Guidelines

After creating an AS administrator profile, run the **stp bpdu-protection** command to configure BPDU protection for ASs in the profile. After the profile is bound to an AS, the following configuration is generated on the AS:

```
#
stp bpdu-protection
#
```

Example

Configure BPDU protection for ASs in an AS administrator profile.

```
<HUAWEI> system-view
[HUAWEI] uni-mng
[HUAWEI-um] as-admin-profile name profile_1
[HUAWEI-um-as-admin-profile_1] stp bpdu-protection
```

3.5.99 traffic-limit inbound (user access profile view)

Function

The **traffic-limit inbound** command configures the rate limit for incoming ARP and DHCP packets on an AS port.

The **undo traffic-limit inbound** command restores the default rate limit for incoming ARP and DHCP packets on an AS port.

By default, the forwarding rate of incoming ARP and DHCP packets on an AS port is not limited.

NOTE

This command can only be executed on a parent switch.

Format

traffic-limit inbound { **arp** | **dhcp** } **cir** *cir-value*

undo traffic-limit inbound { **arp** | **dhcp** }

Parameters

Parameter	Description	Value
arp	Specifies the ARP packet.	-
dhcp	Specifies the DHCP packet.	-
cir *cir-value*	Specifies the committed information rate (CIR), which is the allowed average rate of traffic that can pass through.	The value is an integer that ranges from 8 to 128, in kbit/s.

Views

User access profile view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

After a user access profile is created, you can configure the rate limit for incoming ARP and DHCP packets on an AS port. After the user access profile is bound to the AS port, the following configuration is generated on the AS port:

```
#
 traffic-limit inbound acl 4999 cir cir-value pir pir-value cbs cbs-value pbs pbs-value
 traffic-statistic inbound acl 4999
 traffic-limit inbound acl 3999 cir cir-value pir pir-value cbs cbs-value pbs pbs-value
 traffic-statistic inbound acl 3999
#
```

Precautions

- This command and the **authentication** command cannot be both run in the user access profile view.
- Do not run the **traffic-limit inbound dhcp** and **dhcp snooping enable (network enhanced profile view)** commands simultaneously on the same port; otherwise, the **traffic-limit inbound dhcp** command does not take

effect. On an AS of the S2750-EI, S5700-LI, S5700S-LI, S5720S-LI, S5720-LI, S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5735-S, S500, S5735S-S, S5735-S-I, S5720I-SI, S5710-X-LI, S5735S-H, S5736-S, S6720S-S, or S600-E model, running the **dhcp snooping enable (network enhanced profile view)** command on any port may cause the **traffic-limit inbound dhcp** command unable to take effect on all ports. You are advised to shut down the attacked port after detecting DoS attacks.

- Do not run the **traffic-limit inbound arp** and **arp anti-attack check user-bind enable (network enhanced profile view)** commands simultaneously on the same port. Otherwise, the **traffic-limit inbound arp** command may not take effect. On an AS of the S2750-EI, S5700-LI, S5700S-LI, S5720S-LI, S5720-LI, S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5735-S, S500, S5735S-S, S5735-S-I, S5720I-SI, S5710-X-LI, S5735S-H, S5736-S, S6720S-S, or S600-E model, running the **arp anti-attack check user-bind enable (network enhanced profile view)** command on any port may cause the **traffic-limit inbound arp** command unable to take effect on all ports. You are advised to shut down the attacked port after detecting DoS attacks.

Example

Set the rate limit for incoming ARP packets to 64 on an AS port.

```
<HUAWEI> system-view
[HUAWEI] uni-mng
[HUAWEI-um] user-access-profile name profile_1
[HUAWEI-um-user-access-profile_1] traffic-limit inbound arp cir 64
```

3.5.100 traffic-limit outbound (AS administrator profile view)

Function

The **traffic-limit outbound** command configures the rate limit for outgoing ARP and DHCP packets on an AS uplink fabric port.

The **undo traffic-limit outbound** command restores the default rate limit for outgoing ARP and DHCP packets on an AS uplink fabric port.

By default, the rate limits for outgoing ARP packets and DHCP packets are 32 kbit/s and 128 kbit/s respectively on an AS uplink fabric port.

NOTE

This command can only be executed on a parent switch.

Format

traffic-limit outbound { **arp** | **dhcp** } **cir** *cir-value*

undo traffic-limit outbound { **arp** | **dhcp** }

Parameters

Parameter	Description	Value
arp	Specifies the ARP packet.	-
dhcp	Specifies the DHCP packet.	-
cir *cir-value*	Specifies the committed information rate (CIR), which is the allowed average rate of traffic that can pass through.	The value is an integer that ranges from 8 to 512, in kbit/s.

Views

AS administrator profile view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

After an AS administrator profile is created, you can configure the rate limit for outgoing ARP and DHCP packets on an AS uplink fabric port. After the AS goes online, the following configuration is generated in the AS Eth-Trunk 0 view and system view, regardless of whether the AS administrator profile is bound to the AS:

```
#
acl number 3999
 rule 5 permit udp destination-port eq bootps
#
acl number 4998
 rule 5 permit vlan-id management-vlan
acl number 4999
 rule 5 permit l2-protocol arp destination-mac ffff-ffff-ffff
 rule 10 permit l2-protocol arp
#
interface Eth-Trunk0
 traffic-filter outbound acl 4998
 traffic-statistic outbound acl 3999
 traffic-limit outbound acl 3999 cir cir-value pir pir-value cbs cbs-value pbs pbs-value
 traffic-statistic outbound acl 4999
 traffic-limit outbound acl 4999 cir cir-value pir pir-value cbs cbs-value pbs pbs-value
#
```

Example

Set the rate limit for outgoing ARP packets to 64 on an uplink fabric port.

```
<HUAWEI> system-view
[HUAWEI] uni-mng
[HUAWEI-um] as-admin-profile name profile_1
[HUAWEI-um-as-admin-profile_1] traffic-limit outbound arp cir 64
```


3.5.101 traffic-policy-profile (port group view)

Function

The **traffic-policy-profile** command binds a traffic policy profile to a port group.

The **undo traffic-policy-profile** command unbinds a traffic policy profile from a port group.

By default, no traffic policy profile is bound to a port group.

NOTE

This command can only be executed on a parent switch.

Format

traffic-policy-profile *profile-name* { **inbound** | **outbound** }

undo traffic-policy-profile { **inbound** | **outbound** }

Parameters

Parameter	Description	Value
profile-name	Specifies the name of a traffic policy profile.	The profile must have been created.
inbound	Applies a traffic policy profile to the inbound direction of an interface.	-
outbound	Applies a traffic policy profile to the outbound direction of an interface.	-

Views

Port group view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

You can bind a traffic policy profile to a port group to deliver the configurations in the profile to all the member ports in the port group in a batch.

Prerequisites

The traffic policy profile has been created before being bound to a port group.

Precautions

- A traffic policy profile can be bound to only an AS port group but not an AP port group.
- A port group can be bound to only one traffic policy profile.

Example

Bind a traffic policy profile to a port group.

```
<HUAWEI> system-view
[HUAWEI] uni-mng
[HUAWEI-um] traffic-policy-profile name profile_1
[HUAWEI-um-traffic-policy-profile_1] quit
[HUAWEI-um] port-group name group_1
[HUAWEI-um-portgroup-group_1] traffic-policy-profile profile_1 inbound
```

3.5.102 traffic-policy-profile name

Function

The **traffic-policy-profile name** command creates a traffic policy profile.

The **undo traffic-policy-profile name** command deletes a traffic policy profile.

By default, no traffic policy profile is configured.

NOTE

This command can only be executed on a parent switch.

Format

traffic-policy-profile name *profile-name*

undo traffic-policy-profile name *profile-name*

Parameters

Parameter	Description	Value
profile-name	Specifies the name of a traffic policy profile.	The value is a string of 1 to 31 case-sensitive characters without spaces. The value can contain letters, digits, and underscores (_).

Views

uni-mng view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

A traffic policy profile is used to configure traffic policy functions for ASs, including the packet re-marking function.

Precautions

You can create at most 32 traffic policy profiles.

Example

Create a traffic policy profile.

```
<HUAWEI> system-view
[HUAWEI] uni-mng
[HUAWEI-um] traffic-policy-profile name profile_1
```

3.5.103 trust dscp (network QoS profile view)

Function

The **trust dscp** command configures an AS to perform priority mapping on packets based on DSCP priorities.

The **undo trust dscp** command cancels configuring an AS to perform priority mapping on packets based on DSCP priorities.

By default, an AS performs priority mapping on packets based on 802.1p priorities.

NOTE

This command can only be executed on a parent switch.

Format

trust dscp

undo trust dscp

Parameters

None

Views

Network QoS profile view

Default Level

3: Management level

Usage Guidelines

By default, a device performs priority mapping on packets based on 802.1p priorities. If packets have the same 802.1p priority, the device cannot provide differentiated services to packets. To solve this problem, configure the device to perform priority mapping on packets based on DSCP priorities. After the **trust dscp** command is configured, the device searches for the priority mapping table

based on DSCP priorities and assigns an internal priority to packets so that packets are placed in their corresponding queues.

In an SVF system, you can configure an AS to perform priority mapping on packets based on DSCP priorities by running the **trust dscp** command in the network QoS profile view and then binding the profile to an AS port.

Example

In a network QoS profile, configure an AS to perform priority mapping on packets based on DSCP priorities.

```
<HUAWEI> system-view
[HUAWEI] uni-mng
[HUAWEI-um] network-qos-profile name test
[HUAWEI-um-net-qos-test] trust dscp
```

3.5.104 topology explore

Function

The **topology explore** command triggers SVF network topology collection immediately.

The **topology explore interval** command sets the interval for collecting SVF network topology information.

The **undo topology explore interval** command restores the default interval for collecting SVF network topology information.

By default, the interval for collecting SVF network topology information is 10 minutes.

NOTE

This command can only be executed on a parent switch.

Format

topology explore [**interval** *interval*]

undo topology explore interval

Parameters

Parameter	Description	Value
interval	Specifies the interval for collecting SVF network topology information.	The value is an integer that ranges from 0 to 1440, in minutes. The value 0 indicates that SVF network topology information is not automatically collected.

Views

uni-mng view

Default Level

3: Management level

Usage Guidelines

You can adjust the interval for collecting SVF network topology information based on SVF network stability. When the network topology is stable, you can increase the interval or disable periodic topology information collection. When the network topology is unstable, you can shorten the interval.

You can also run the **topology explore** command to trigger SVF network topology collection immediately.

Example

Set the SVF network topology collection interval to 30 minutes.

```
<HUAWEI> system-view
[HUAWEI] uni-mng
[HUAWEI-um] topology explore interval 30
```

3.5.105 undo uni-mng enable

Function

The **undo uni-mng enable** command changes an AS from the client mode to the standalone mode.

NOTE

This command can only be executed on an AS. After this command is executed, the AS restarts.

Format

undo uni-mng enable

Parameters

None

Views

User view

Default Level

3: Management level

Usage Guidelines

You can run the **undo uni-mng enable** command to change an AS from the client mode to the standalone mode.

Example

Change an AS from the client mode to the standalone mode.

```
<HUAWEI> undo uni-mng enable
```

3.5.106 uni eth-trunk

Function

The **uni eth-trunk** command creates an Eth-Trunk interface for an AS.

The **undo uni eth-trunk** command deletes an Eth-Trunk interface of an AS.

By default, no Eth-Trunk interface is created on an AS.

NOTE

This command can only be executed on the parent.

Format

uni eth-trunk *trunk-id* [**mode lacp**]

undo uni eth-trunk *trunk-id* [**mode lacp**]

Parameters

Parameter	Description	Value
trunk-id	Specifies the ID of an Eth-Trunk interface.	The value is an integer and the minimum value is 1. The maximum value varies according to the switch model. For a specific switch model, the maximum value is the same as that described in **interface eth-trunk**.
mode lacp	Sets the working mode of an Eth-Trunk interface to LACP mode. If this parameter is not specified, the working mode of an Eth-Trunk interface is manual mode.	-

Views

AS view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

When an AP with two network interfaces connects to an SVF system through an AS or to improve access user bandwidth and reliability, you can create an Eth-Trunk interface for this AS.

Precautions

- An Eth-Trunk interface can be created for an AS only when this AS is in centralized mode.
- When an AS works in independent mode and its Eth-Trunk interface needs to be deleted, you need to run the **undo uni eth-trunk** *trunk-id* command in the AS view of the parent and log in to this AS to delete this Eth-Trunk interface.
- To delete an Eth-Trunk interface, ensure that it does not contain member interfaces.
- After an Eth-Trunk interface is created and its working mode is set to LACP, running the **uni eth-trunk** *trunk-id* command will not change the working mode of the Eth-Trunk interface. To change the working mode to manual mode, run the **undo uni eth-trunk** *trunk-id* **mode lacp** command.
- Running the **undo uni eth-trunk** *trunk-id* **mode lacp** command only changes the working mode of an Eth-Trunk interface and will not delete the Eth-Trunk interface. To delete an Eth-Trunk interface, run the **undo uni eth-trunk** *trunk-id* command.
- The Eth-Trunk interface of an AS and Eth-Trunk interfaces bound to fabric ports share the Eth-Trunk interface specifications.
- An Eth-Trunk interface contains a maximum of eight member interfaces.
- An Eth-Trunk interface cannot be created across ASs.

Follow-up Procedure

Run the **port eth-trunk trunkmember** command to add member interfaces to the Eth-Trunk interface.

Example

Create Eth-Trunk 2 in LACP mode for the AS **test**.

```
<HUAWEI> system-view
[HUAWEI] uni-mng
[HUAWEI-um] as name test
[HUAWEI-um-as-test] uni eth-trunk 2 mode lacp
```


3.5.107 uni eth-trunk lacp timeout

Function

The **uni eth-trunk lacp timeout** command configures the LACP timeout time for an Eth-Trunk interface on an AS.

The **undo uni eth-trunk lacp timeout** command restores the default LACP timeout time of an Eth-Trunk interface on an AS.

By default, the LACP timeout time of an Eth-Trunk interface on an AS is 90 seconds.

NOTE

This command can only be executed on a parent switch.

Format

uni eth-trunk *trunk-id* **lacp timeout fast** [**user-defined** *user-defined-timeout*]

undo uni eth-trunk *trunk-id* **lacp timeout**

Parameters

Parameter	Description	Value
trunk-id	Specifies an Eth-Trunk ID.	The value must be an Eth-Trunk ID that has been created using the **uni eth-trunk** command.
fast	Sets the LACP timeout time of an Eth-Trunk interface to 3 seconds. In this situation, the interval at which the remote end sends LACP PDUs is 1 second.	-
user-defined *user-defined-timeout*	Indicates the user-defined LACP timeout time of an Eth-Trunk interface.	The value is an integer that ranges from 3 to 90, in seconds.

Views

AS view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

By default, if a member interface of the remote Eth-Trunk interface is faulty, it takes 90 seconds for the local Eth-Trunk interface to detect the remote member interface status change. This results in data traffic loss because the local interface continues to forward data traffic to the faulty remote member interface within 90 seconds. To enable the local interface to detect the remote member interface status change in a timely manner, run the **uni eth-trunk lacp timeout** command to reduce the LACP timeout time.

Prerequisites

The **uni eth-trunk lacp timeout** command can be configured only when the **uni eth-trunk** command has been configured to create an Eth-Trunk interface and set its working mode to LACP mode.

Precautions

The **uni eth-trunk lacp timeout** command is deleted when the **undo uni eth-trunk** command is configured to delete the Eth-Trunk interface.

Example

Set the LACP timeout time of Eth-Trunk 2 on the AS **test** to 3 seconds.

```
<HUAWEI> system-view
[HUAWEI] uni-mng
[HUAWEI-um] as name test
[HUAWEI-um-as-test] uni eth-trunk 2 mode lacp
[HUAWEI-um-as-test] uni eth-trunk 2 lacp timeout fast
```

3.5.108 uni-mng

Function

The **uni-mng** command enables SVF or displays the uni-mng view.

The **undo uni-mng** command disables SVF.

By default, SVF is disabled.

NOTE

This command can only be executed on a parent switch.

Format

uni-mng

undo uni-mng

Parameters

None

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

When SVF is disabled, the **uni-mng** command enables SVF and displays the uni-mng view. When SVF has been enabled, this command displays the uni-mng view.

Prerequisites

- A source interface used to set up a CAPWAP link has been specified using the **capwap source interface vlanif** *vlan-id* command.
- The STP working mode must be STP or RSTP. If the current working mode is not STP or RSTP, run the **stp mode** { **rstp** | **stp** } command to set the STP working mode to STP or RSTP before enabling SVF. By default, the STP working mode is MSTP. You can run the **display stp** command to check the current STP working mode.
- The default STP/RSTP port path cost algorithm must be used. If the current port path cost algorithm is not the default one, run the **undo stp pathcost-standard** command to restore the default port path cost algorithm before enabling SVF. The default STP/RSTP port path cost algorithm is IEEE 802.1t (**dot1t**). You can run the **display stp** command to check the current port path cost algorithm.
- The default Eth-Trunk specifications are used. If the current Eth-Trunk specifications are not the default value on S5531-H, S5531-S, S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, S6730S-S, S6735-S, S6720-EI, or S6720S-EI, run the **undo assign trunk** command to restore the default Eth-Trunk specifications before enabling SVF. You can run the **display trunk configuration** command to check the default and configured Eth-Trunk specifications.
- The NAC configuration mode must be the unified mode. If the current mode is not the unified mode, run the **authentication unified-mode** command to set the NAC configuration mode to unified mode. The default NAC configuration mode is unified mode. You can run the **display authentication mode** command to check the current NAC configuration mode.
- Remote authorization is not configured in the system. If remote authorization has been configured, run the **undo remote-authorize** command to disable remote authorization before enabling SVF. By default, remote authorization is not configured in the system. You can run the **display current-configuration** command to check whether remote authorization is configured.

Precautions

- When SVF is enabled on the parent, LLDP is automatically enabled on the parent if LLDP is disabled. When SVF is disabled on the parent, LLDP is not automatically disabled on the parent.

- When SVF is disabled on the parent, the STP priorities of ports change, and STP recalculates the port role and changes the interface status.
- After SVF is enabled on a switch used as the parent, the **stack timer mac-address switch-delay** value changes to 0 (not changing system MAC address) and cannot be changed. After SVF is disabled on this switch, this delay time is still 0, but you can manually change it.

Example

Enable SVF (default Eth-Trunk specifications and default NAC configuration mode).

```
<HUAWEI> system-view
[HUAWEI] vlan batch 11
[HUAWEI] interface Vlanif 11
[HUAWEI-Vlanif11] ip address 192.168.11.1 24
[HUAWEI-Vlanif11] quit
[HUAWEI] capwap source interface vlanif 11
[HUAWEI] stp mode stp
[HUAWEI] uni-mng
Warning: This operation will enable the uni-mng mode and disconnect all ASs. STP calculation may be triggered and service traffic will be affected. Continue? [Y/N]:y
```

3.5.109 uni-mng indirect fabric-port

Function

The **uni-mng indirect fabric-port** command configures a member port for an uplink fabric port that connects an AS to the parent through a network.

The **undo uni-mng indirect fabric-port** command deletes a member port of an uplink fabric port that connects an AS to the parent through a network.

By default, no member port is configured for an uplink fabric port that connects an AS to the parent through a network.

NOTE

This command can only be executed on an AS.

Format

uni-mng indirect fabric-port member interface *interface-type interface-number*

undo uni-mng indirect fabric-port member interface *interface-type interface-number*

Parameters

Parameter	Description	Value
member interface *interface-type interface-number*	Specifies the type and number of member ports of a fabric port.	-

Views

User view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

When an AS connects to the parent through a network, you must run the **uni-mng indirect fabric-port** command to configure a member port for an uplink fabric port of the AS. You can run this command multiple times to add multiple member ports to the fabric port.

Prerequisites

The **uni-mng indirect mng-vlan** command has been executed to configure the device to work in client mode and configure a management VLAN.

Precautions

- Only AS uplink ports or subcard ports can be added to an uplink fabric port. If you have to add AS downlink ports to uplink fabric ports, run the **uni-mng up-direction fabric-port member interface** *interface-type interface-number* [**to** *interface-number*] command.
- A maximum of eight member ports can be added to a fabric port.
- Ports used to set up a stack cannot be configured as member ports of a fabric port.
- The command that configures the stack ID is mutually exclusive with the command that configures a member port for a fabric port:
  - After the **stack slot** *slot-id* **renumber** *new-slot-id* command is executed in a specified slot, the port in the slot cannot be configured as a member port of a fabric port.
  - After a port in a slot is configured as a member port of a fabric port, the stack ID of the slot cannot be configured using the **stack slot** *slot-id* **renumber** *new-slot-id* command.
- You need to configure a member port of a fabric port according to the network configuration. A member port needs to be reconfigured if the stack ID changes because the stack changes, for example, the stacking function is disabled, or existing stack IDs conflict after member devices are added to the stack.

Example

Configure member ports for an uplink fabric port that connects an AS to the parent through a network.

```
<HUAWEI> uni-mng indirect fabric-port member interface gigabitethernet 0/0/27
<HUAWEI> uni-mng indirect fabric-port member interface gigabitethernet 0/0/28
```


3.5.110 uni-mng indirect mng-vlan

Function

The **uni-mng indirect mng-vlan** command configures a device to work in client mode and configures a management VLAN.

NOTE

This command can only be executed on an AS.

Format

uni-mng indirect mng-vlan *vlan-id*

Parameters

Parameter	Description	Value
vlan-id	Specifies a management VLAN. The VLAN must be consistent with the management VLAN configured on a parent.	The value is an integer that ranges from 2 to 4094. The VLAN cannot be the reserved VLAN (The default is VLAN 4093) of a stack.

Views

User view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

When an AS connects to the parent through a network, you must run the **uni-mng indirect mng-vlan** command to configure the AS to work in client mode and configures a management VLAN.

Precautions

- The VCMP role switching command is mutually exclusive with the command that configures a device to work in client mode. If the current device is not a silent switch in a VCMP domain, the device cannot be configured to work in client mode. You must run the **vcmp role silent** command in the system view to set the VCMP role of the device to silent. After a device is configured to work in client mode, the VCMP role switching command cannot be executed. That is, the device cannot change from the silent role to another role.
- After running the **uni-mng indirect mng-vlan** *vlan-id* command on the device in standalone mode, you must delete the configuration file of the device and restart the device to make the configuration take effect.

- If the device has been configured to work in client mode but has not gone online, you can run the **uni-mng indirect mng-vlan** *vlan-id* command multiple times to change the management VLAN, and the configuration takes effect immediately.
- If the device has been configured to work in client mode and has gone online, the **uni-mng indirect mng-vlan** *vlan-id* command cannot be executed.
- When an AS is an S5700-10P-LI, S5700-10P-PWR-LI-AC, or S2750-EI and Layer 3 hardware forwarding for IPv4 packets has been enabled using the **assign forward-mode ipv4-hardware** command in the system view, the management VLAN cannot be configured. To solve this problem, start the AS in standalone mode and run the **undo assign forward-mode** command in the system view to disable Layer 3 hardware forwarding for IPv4 packets.
- On the S5720-SI, S5735-S, S500, S5735S-S, S5720I-SI, S5735S-H, S5736-S, S6720S-S, or S600-E, the electrical port stack configuration on the front panel is mutually exclusive with the client mode configuration. If electrical ports on the front panel have been configured as stack physical member ports, no management VLAN cannot be configured. If a management VLAN has been configured, electrical ports on the front panel cannot be configured as stack physical member ports.
- If an AS is configured in the independent mode, its management VLAN cannot be configured using this command.
- The slot ID of an AS cannot be greater than or equal to 5. Otherwise, the management VLAN cannot be configured for the AS using the **uni-mng indirect mng-vlan** command.
- The command that changes a stack ID and the command that configures a management VLAN are mutually exclusive.
  - The management VLAN cannot be configured for an AS after the slot ID of the AS is changed using the **stack slot** *slot-id* **renumber** *new-slot-id* command.
  - The slot ID of an AS cannot be changed using the **stack slot** *slot-id* **renumber** *new-slot-id* command after a management VLAN is configured for the AS using the **uni-mng indirect mng-vlan** command.

Example

Configure the device to work in client mode and configure a management VLAN 100.

```
<HUAWEI> uni-mng indirect mng-vlan 100
```

3.5.111 uni-mng up-direction fabric-port

Function

The **uni-mng up-direction fabric-port** command configures AS service ports as an uplink fabric port's members.

The **undo uni-mng up-direction fabric-port** command cancels the configuration.

By default, AS service ports are not configured as members of uplink fabric ports.

NOTE

This command can only be executed on an AS.

Format

uni-mng up-direction fabric-port member interface *interface-type interface-number* [**to** *interface-number*]

undo uni-mng up-direction fabric-port member interface *interface-type interface-number* [**to** *interface-number*]

undo uni-mng up-direction fabric-port member all

Parameters

Parameter	Description	Value
member interface *interface-type interface-number*	Specifies the type and number of an AS service port to be configured as a member of an uplink fabric port.	-
all	Specifies all AS service ports.	-

Views

User view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

To configure AS service ports as an uplink fabric port's members, run the **uni-mng up-direction fabric-port** command.

Precautions

- A maximum of eight interfaces can be configured as a fabric port's members on an AS.
- Stack ports cannot be configured as members of fabric ports. Similarly, fabric member ports cannot be configured as stack ports.
- After the **uni-mng up-direction fabric-port** command is run on an AS, you must restart the AS to make the configuration take effect. If the AS is a stack, you need to restart all stack members. If a configuration conflicting with this command exists on the parent, the AS may fail to go online.
- The command for configuring a stack ID and the command for configuring a fabric member port are mutually exclusive. Specifically:

  - If you have run the **stack slot** *slot-id* **renumber** *new-slot-id* command in a slot, you are not allowed to configure the service port of this slot as a member of an uplink fabric port.
  - If you have configured a service port of a slot as a member of an uplink fabric port, you are not allowed to run the **stack slot** *slot-id* **renumber** *new-slot-id* command to configure a stack ID in this slot.
- When configuring a service port as a member of a fabric port, pay attention to the stacking configuration. A member port needs to be reconfigured if stack IDs change because the stack changes, for example, the stacking function is disabled, or existing stack IDs conflict after member switches are added to the stack.
- If a downlink service interface of an AS is incorrectly configured as a stack port, other interfaces on the AS cannot be configured as uplink interfaces. In this case, delete the stack port configuration from the downlink service interface.

Example

Configure an AS service port as a member of an uplink fabric port.

```
<HUAWEI> uni-mng up-direction fabric-port member interface gigabitethernet 0/0/3
Warning: After a service port on an AS is configured as an uplink port, the AS needs to be restarted to
make the configuration take effect.
 If the parent has a configuration conflict with the AS, the AS may fail to go online. Continue? [Y/N]:y
```

3.5.112 unicast-suppression (network enhanced profile view)

Function

The **unicast-suppression** command configures unknown unicast traffic suppression in a network enhanced profile.

The **undo unicast-suppression** command cancels unknown unicast traffic suppression in a network enhanced profile.

By default, unknown unicast traffic suppression is not configured in a network enhanced profile.

NOTE

This command can only be executed on a parent switch.

Format

unicast-suppression packets *packets-per-second*

undo unicast-suppression

Parameters

Parameter	Description	Value
packets *packets-per-second*	Specifies the packet rate of an interface.	The value is an integer that ranges from 0 to 14881000, in packets per second (PPS). If the configured packet rate on the parent switch is larger than the maximum value on the AS port, the maximum value takes effect on the AS port.

Views

Network enhanced profile view

Default Level

3: Management level

Usage Guidelines

After creating a network enhanced profile, you can configure unknown unicast traffic suppression in the profile. After the profile is bound to an AS port, unknown unicast traffic suppression is automatically configured on the port. The following configuration is generated on the AS port:

```
#
 unicast-suppression packets packets-per-second
#
```

To prevent broadcast storms, you can run the **unicast-suppression** command to configure the maximum number of unknown unicast packets that can pass through a port. When the unknown unicast traffic rate reaches the rate limit, the system discards excess unknown unicast packets to control the traffic volume within a proper range.

Example

Configure unknown unicast traffic suppression in a network enhanced profile.

```
<HUAWEI> system-view
[HUAWEI] uni-mng
[HUAWEI-um] network-enhanced-profile name profile_1
[HUAWEI-um-net-enhanced-profile_1] unicast-suppression packets 148810
```

3.5.113 upgrade as

Function

The **upgrade as name** command upgrades an AS with a specified name.

The **upgrade as name-include** command upgrades ASs of which the name contains a specified string.

The **upgrade as type** command upgrades ASs of a specified type.

The **upgrade as all** command upgrades all ASs.

undo upgrade as command rolls back ASs to the previous version.

NOTE

This command can only be executed on a parent switch.

Format

upgrade as name *as-name* [**reload** [**at** *time*]]

upgrade as name-include *string* [**reload** [**at** *time*]]

upgrade as type *as-type* [**reload** [**at** *time*]]

upgrade as all [**reload** [**at** *time*]]

undo upgrade as { **all** | **name** *as-name* | **name-include** *string* | **type** *as-type* }

Parameters

Parameter	Description	Value
as-name	Upgrades an AS with a specified name.	The value must have an existing AS name.
string	Upgrades all the ASs of which the name contains a specified string.	The value is a string of 1 to 31 case-insensitive characters without spaces.
as-type	Upgrades ASs of a specified type.	The value is an enumerated type. You can enter a question mark (?) and select a value from the displayed value range.
reload	Configures an AS to restart after upgrade files are downloaded.	-
at *time*	Specifies the AS restart time. If **reload** is specified but *time* is not specified, an AS restarts immediately after loading files. If *time* is specified, the AS restarts at the specified time.	The value is a string of characters in the HH:MM format, where HH:MM indicates the hour and minute. HH ranges from 0 to 23, and MM ranges from 0 to 59.

Views

uni-mng view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

You can run the **upgrade as** command to upgrade online ASs. You can upgrade one AS, ASs of a specified type, or all ASs.

After performing upgrade configuration on an AS, the patch and system software files for the next startup will be the specified ones. You can run the **undo upgrade as** command to cancel the configuration as long as the AS is not restarted. After this command is executed, the patch and system software files for the next startup are consistent with the currently running ones. If the patch has taken effect after upgrade configuration is performed, the patch cannot be rolled back to the previous version.

Precautions

- The patch and system software files used to upgrade ASs are specified in the **as type** command. If no system software file is not specified using the **as type** command, an AS automatically uses the system software of the same version as the parent during an upgrade. If the system software of the same version as the parent does not exist, the AS continues to use the previous system software.
- The **upgrade as** command cannot upgrade an AS if the software file name or patch file name specified in the **as type** command is the same as the current or next startup software file name or patch file name of the AS.
- The **upgrade as** command cannot upgrade an AS if the software file name specified in the **as type** command does not exist.
- When you upgrade an AS using the **upgrade as** command without specifying **reload**:
  - If you specify **patch** *patch* but not **system-software** *system-software* in the **as type** command, the patch file is activated online immediately.
  - If you specify both **patch** *patch* and **system-software** *system-software* in the **as type** command and the specified system software file version is the version running on the AS, the patch file is activated online immediately.
  - If you specify both **patch***patch* and **system-software***system-software* in the **as type** command and the specified system software file version is earlier or later than the version running on the AS, the specified system software file and patch file will be set as next startup files.

Example

Perform an in-service upgrade on an AS of the S5720-P-LI type.

```
<HUAWEI> system-view
[HUAWEI] uni-mng
[HUAWEI-um] upgrade as type s5720-p-li reload
```


3.5.114 upgrade { local-ftp-server | local-sftp-server }

Function

The **upgrade** { **local-ftp-server** | **local-sftp-server** } command configures a local file server.

The **undo upgrade** { **local-ftp-server** | **local-sftp-server** } command deletes a local file server.

By default, no local file server is configured.

NOTE

This command can only be executed on a parent switch.

Format

upgrade { **local-ftp-server** | **local-sftp-server** } **username** *username* **password** *password*

undo upgrade { **local-ftp-server** | **local-sftp-server** }

Parameters

Parameter	Description	Value
local-ftp-server	Specifies the file server type as FTP server.	-
local-sftp-server	Specifies the file server type as SFTP server.	-

Parameter	Description	Value

username *username*	Specifies the user name for accessing the file server.	The value is a string of 1 to 64 characters. It cannot contain spaces, asterisk, double quotation mark and question mark.
		NOTE
		• During local authentication or authorization, run the **authentication-mode** { **local** | **local-case** } or **authorization-mode** { **local** | **local-case** } command to configure case sensitivity for user names. If the parameter is set to **local**, user names are case-insensitive. If the parameter is set to **local-case**, user names are case-sensitive.
		• Note the following when configuring case sensitivity for user names:
		  • Only the user name is case-sensitive and the domain name is case-insensitive.
		  • For user security purposes, you cannot configure multiple local users with the user names that differ only in uppercase or lowercase. For example, after configuring ABC, you cannot configure Abc or abc as the user name.
		  • When a device is upgraded from V200R011C10 or an earlier version to a version later than V200R011C10, all local user names in the original configuration file are saved in lowercase. When a configuration file that is manually configured or generated using the third-party tool is used for configuration restoration, local user names that differ only in uppercase or lowercase are considered as one user name and the first one among these local user names is used.

password *password*	Specifies the password for accessing the file server.	The value is a string of case-sensitive characters without spaces. By default, the value is a string of 8 to 128 characters or 48 to 188 characters. You can enter a password in plain text or cipher text. The password is displayed in cipher text in the configuration file regardless of whether the password is input in plain or cipher text. • The password in plain text is a string of 8 to 128 characters. • The password in cipher text is a string of 48 to 188 characters. The password in cipher text cannot be generated using the irreversible algorithm.

Views

uni-mng view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

In an AS automatic upgrade or in-service AS batch upgrade, you need to download the version file or patch file from the parent. Before the upgrade, you need to configure the parent as an FTP/SFTP server. The AS then can work as a client to download files from the FTP/SFTP server.

Precautions

- The files used to upgrade an AS are often saved in the root directory unimng/ of the parent. These files can also be saved on an AS when the AS is upgraded or downgraded to the software version that is consistent with that of the parent.
- FTP has potential security risks, and so SFTP is recommended. If you want to use FTP, you are advised to configure ACLs to improve security. For details, see Configure the FTP ACL in "File Management" in the *S300, S500, S2700, S5700, and S6700 V200R023C00 Configuration Guide - Basic Configuration*.
- When the file server is an FTP server, the parent automatically enables the FTP service and creates an FTP user. You only need to run the ftp server-source command to specify the source IP address of the FTP server.
- When the file server type is set to SFTP, the SFTP service is not automatically enabled and no SFTP user is created on the parent. You need to manually pre-configure SFTP on the parent.
- After the **upgrade** { **local-ftp-server** | **local-sftp-server** } command is executed, the same user name and password configuration is also generated in the AAA view. If you modify the configured local user information (the user password for example) in AAA view, the version management function does not take effect.
- If information about a user already exists in the AAA view, you cannot run this command to configure the same user name.
- Running this command multiple times to create new users will delete previous user information. Previous user information can be deleted only when the user level of the user running this command is higher or equal to the user level configured in the AAA view. Otherwise, the command does not take effect.
- If a remote authentication server is used for AAA authentication, the user name and password configured using this command must also be configured on the remote authentication server.
- If a remote authentication server is used for AAA authentication and the remote authentication server does not support FTP or SFTP, ASs will fail to be authenticated. In this case, run the **authentication-scheme** *authentication-scheme-name* command in the AAA view to create an authentication scheme and run the **authentication-mode local** command in the authentication scheme view to set the authentication mode to local authentication. Then, run the **domain** command in the AAA view to create a domain and run the **authentication-scheme** *authentication-scheme-name* command in the AAA

domain view to apply the created authentication scheme to the domain. ASs can be authenticated when they use the newly created domain for local authentication.

Example

Set the local file server type to FTP server.

```
<HUAWEI> system-view
[HUAWEI] uni-mng
[HUAWEI-um] upgrade local-ftp-server username test password Pwd@12345
```

3.5.115 upload config

Function

The **upload config** command saves the AS configuration to the flash memory of an AS and uploads the configuration file of the AS to the parent.

NOTE

This command can only be executed on an AS.

Format

upload config

Parameters

None

Views

User view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

In independent mode, after services are configured on an AS using commands, you can run the **upload config** command to save the service configuration and upload the configuration file to the parent.

Precautions

- After this command is executed, the AS configuration file uploaded to the parent will be saved to the **flash:/unimng/ind-cfg** directory or the **cfcard:/unimng/ind-cfg** directory on some parent switch models. If the file name format is unimng-xxxx-xxxx-xxxx.zip (xxxx-xxxx-xxxx indicates the management MAC address of an AS), and the service configuration mode of this AS is independent mode, it is not allowed to delete this configuration file.

- After the **upload config** command is executed, the AS configuration file may fail to be uploaded to the parent. The possible causes include insufficient storage space on the parent and a fault of the link between the AS and parent.
- To prevent services from being affected, it is recommended not to delete the configuration file saved on the AS.
- The AS configuration file saved on the parent can ensure configuration integrity for the AS. For example, after an AS goes online again or is replaced, the AS will compare its saved configuration file with that saved on the parent. If the two files are inconsistent, the configuration file saved on the parent will replace the configuration file saved on the AS and take effect after the AS restarts.

Example

Save the AS configuration to the flash memory of the AS and upload the configuration file of the AS to the parent.

```
<HUAWEI> upload config
```

3.5.116 user-access-port enable (network enhanced profile view)

Function

The **user-access-port enable** command configures the edge port function in a network enhanced profile.

The **undo user-access-port enable** command cancels the edge port function in a network enhanced profile.

By default, the edge port function is not configured in a network enhanced profile.

NOTE

This command can only be executed on a parent switch.

Format

user-access-port enable

undo user-access-port enable

Parameters

None

Views

Network enhanced profile view

Default Level

3: Management level

Usage Guidelines

After creating a network enhanced profile, you can configure the edge port function in the profile. After the profile is bound to an AS port, the port becomes an edge port. The following configuration is generated on the AS port:

```
#
 stp edged-port enable
#
```

Ports connected to a Layer 2 STP network do not need to participate in spanning tree calculation. If these ports participate in the calculation, the network topology convergence speed is affected and the status changes of these ports may cause network flapping. After these ports are configured as edge ports, they do not participate in spanning tree calculation. This configuration speeds up network topology convergence and enhances network stability.

Example

Enable the edge port function in a network enhanced profile.

```
<HUAWEI> system-view
[HUAWEI] uni-mng
[HUAWEI-um] network-enhanced-profile name profile_1
[HUAWEI-um-net-enhanced-profile_1] user-access-port enable
```

3.5.117 user-access-profile name

Function

The **user-access-profile name** command creates a user access profile.

The **undo user-access-profile name** command deletes a user access profile.

By default, no user access profile is configured.

NOTE

This command can only be executed on a parent switch.

Format

user-access-profile name *profile-name*

undo user-access-profile name *profile-name*

Parameters

Parameter	Description	Value
profile-name	Specifies the name of a user access profile.	The value is a string of 1 to 31 case-sensitive characters without spaces. The value can contain letters, digits, and underscores (_).

Views

uni-mng view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

In a user access profile, you can configure authentication services for user access (for example, the authentication mode), MAC address learning limiting, and the rate limit for incoming ARP and DHCP packets on an AS port.

Precautions

You can create a maximum of 16 user access profiles.

Example

Create a user access profile.

```
<HUAWEI> system-view
[HUAWEI] uni-mng
[HUAWEI-um] user-access-profile name profile_1
```

3.5.118 user-access-profile (port group view)

Function

The **user-access-profile** command binds a user access profile to a port group.

The **undo user-access-profile** command unbinds a user access profile from a port group.

By default, no user access profile is bound to a port group.

NOTE

This command can only be executed on a parent switch.

Format

user-access-profile *profile-name*

undo user-access-profile

Parameters

Parameter	Description	Value
profile-name	Specifies the name of a user access profile.	The value must have an existing user access profile name.

Views

Port group view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

You can bind a user access profile to a port group to deliver the configurations in the profile to all the member ports in the port group.

Prerequisites

The user access profile has been created.

Precautions

- A user access profile can be bound to only an AS port group but not an AP port group.
- A port group can be bound to only one user access profile.

Example

Bind a user access profile to a port group.

```
<HUAWEI> system-view
[HUAWEI] uni-mng
[HUAWEI-um] user-access-profile name profile_1
[HUAWEI-um-user-access-profile_1] quit
[HUAWEI-um] port-group name group_1
[HUAWEI-um-portgroup-group_1] user-access-profile profile_1
```

3.5.119 user-vlan (network basic profile view)

Function

The **user-vlan** command configures the default VLAN in a network basic profile.

The **undo user-vlan** command deletes the default VLAN in a network basic profile.

By default, no default VLAN is configured in a network basic profile, and downlink ports of an AS use VLAN 1 as the default VLAN.

NOTE

This command can only be executed on a parent switch.

Format

user-vlan *vlan-id*

undo user-vlan

Parameters

Parameter	Description	Value
vlan-id	Specifies a VLAN ID.	The value is an integer that ranges from 1 to 4094. The value cannot be the ID of an SVF management VLAN, a stack management VLAN, an ERPS control VLAN, an RRPP control VLAN, an SEP control VLAN, or a super VLAN.

Views

Network basic profile view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

After creating a network basic profile, you can configure the default VLAN in the profile. After the profile is bound to an AS port, the default VLAN is automatically configured on the port. The following configuration is generated on the AS port:

```
#
 port link-type hybrid
 port hybrid pvid vlan vlan-id
 port hybrid tagged vlan 1
 port hybrid untagged vlan vlan-id
#
```

The **user-vlan** command can only configure the default VLAN for a port. To enable this port to allow packets of multiple VLANs to pass through, run the **pass-vlan** command in a network basic profile.

Precautions

The default VLAN, allowed VLANs, and voice VLAN in a network basic profile must be different.

Example

Configure the default VLAN in a network basic profile.

```
<HUAWEI> system-view
[HUAWEI] uni-mng
[HUAWEI-um] network-basic-profile name profile_1
[HUAWEI-um-net-basic-profile_1] user-vlan 10
```


3.5.120 user password (AS administrator profile view)

Function

The **user password** command configures an AS administrator in an AS administrator profile.

The **undo user** command deletes an AS administrator in an AS administrator profile.

By default, no AS administrator is configured in an AS administrator profile.

NOTE

This command can only be executed on a parent switch.

Format

user *user-name* **password** *password*

undo user *user-name*

Parameters

Parameter	Description	Value

user-name	Specifies a user name.	The value is a string of 1 to 64 characters. It cannot contain spaces, asterisk, double quotation mark and question mark.
		NOTE
		• During local authentication or authorization, run the **authentication-mode** { **local** | **local-case** } or **authorization-mode** { **local** | **local-case** } command to configure case sensitivity for user names. If the parameter is set to **local**, user names are case-insensitive. If the parameter is set to **local-case**, user names are case-sensitive.
		• Note the following when configuring case sensitivity for user names:
		  • Only the user name is case-sensitive and the domain name is case-insensitive.
		  • For user security purposes, you cannot configure multiple local users with the user names that differ only in uppercase or lowercase. For example, after configuring ABC, you cannot configure Abc or abc as the user name.
		  • When a device is upgraded from V200R011C10 or an earlier version to a version later than V200R011C10, all local user names in the original configuration file are saved in lowercase. When a configuration file that is manually configured or generated using the third-party tool is used for configuration restoration, local user names that differ only in uppercase or lowercase are considered as one user name and the first one among these local user names is used.

Parameter	Description	Value
password	Specifies the password.	The value is a string of case-sensitive characters without spaces. By default, the value is a string of 8 to 128 characters or 48 to 188 characters. You can enter a password in plain text or cipher text. The password is displayed in cipher text in the configuration file regardless of whether the password is input in plain or cipher text. • The password in plain text is a string of 8 to 128 characters. • The password in cipher text is a string of 48 to 188 characters. The password in cipher text cannot be generated using the irreversible algorithm. Do not set this password to the weak password preset by running the **load security weak-password-dictionary** command.

Views

AS administrator profile view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

After creating an AS administrator profile, you can configure an AS administrator in the profile, including the user name and password. After the profile is bound to an AS, the user name and password for login are automatically configured on the AS. The following configuration is generated on the AS:

```
#
aaa
 local-user user-name password irreversible-cipher password
 local-user user-name privilege level 3
 local-user user-name service-type terminal ssh
#
```

After an AS user name and password are configured, you need to enter the correct user name and password when logging in to an AS through the console port. When you log in to an AS from the parent using the **attach as name** *as-name* command, you can log in to the AS without entering the user name or password.

Precautions

In versions earlier than V200R020C00, when no AS user name and password are configured, you need to enter the default username and password when logging in to an AS through the console port. However, in V200R020C00 and later versions, there is no preset password for logging in to an AS through the console

port, therefore, you must configure an AS user name and password before logging in to the AS through the console port.

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.

Example

Configure the user name and password for an AS administrator.

```
<HUAWEI> system-view
[HUAWEI] uni-mng
[HUAWEI-um] as-admin-profile name profile_1
[HUAWEI-um-as-admin-profile_1] user test password YsHsjx_202206
```

3.5.121 voice-vlan (network basic profile view)

Function

The **voice-vlan** command configures a voice VLAN in a network basic profile.

The **undo voice-vlan** command deletes the voice VLAN in a network basic profile.

By default, no voice VLAN is configured in a network basic profile.

NOTE

This command can only be executed on a parent switch.

Format

voice-vlan *vlan-id* [**include-untagged**]

undo voice-vlan

Parameters

Parameter	Description	Value
vlan-id	Specifies a VLAN ID.	The value is an integer that ranges from 2 to 4094. The value cannot be the ID of an SVF management VLAN, a stack management VLAN, an ERPS control VLAN, an RRPP control VLAN, an SEP control VLAN, or a super VLAN.
include-untagged	Adds voice VLAN IDs to untagged packets.	-

Views

Network basic profile view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

After creating a network basic profile, you can configure a voice VLAN in the profile. After the profile is bound to an AS port, the voice VLAN is automatically configured on the port. The following configuration is generated on the AS port:

- The **include-untagged** parameter is not specified:

```
#
 port link-type hybrid
 port hybrid tagged vlan vlan-id
 lldp tlv-enable med-tlv network-policy voice-vlan vlan vlan-id
 lldp compliance cdp txrx
#
```

- The **include-untagged** parameter is specified (S6735-S, S6720-EI, and S6720S-EI):

```
#
 port link-type hybrid
 port hybrid untagged vlan vlan-id
 voice-vlan vlan-id enable include-untagged include-tag0
 undo lldp tlv-enable med-tlv network-policy
#
```

- The **include-untagged** parameter is specified (except S6735-S, S6720-EI, and S6720S-EI):

```
#
 port link-type hybrid
 port hybrid untagged vlan vlan-id
 voice-vlan vlan-id enable include-untagged
 undo lldp tlv-enable med-tlv network-policy
#
```

Precautions

The default VLAN, allowed VLANs, and voice VLAN in a network basic profile must be different.

When configuring a voice VLAN on an AS port, ensure that IP phones connected to the AS port support LLDP and have LLDP enabled.

Example

Configure a voice VLAN in a network basic profile.

```
<HUAWEI> system-view
[HUAWEI] uni-mng
[HUAWEI-um] network-basic-profile name profile_1
[HUAWEI-um-net-basic-profile_1] voice-vlan 10
```


3.5.122 whitelist mac-address

Function

The **whitelist mac-address** command adds a specified MAC address to the whitelist.

The **undo whitelist mac-address** command deletes a MAC address from the whitelist.

By default, no MAC address is added to the whitelist. A maximum of 512 MAC addresses can be added to the whitelist.

NOTE

This command can only be executed on a parent switch.

Format

whitelist mac-address *mac-address1* [**to** *mac-address2*]

undo whitelist mac-address { *mac-address1* [**to** *mac-address2*] | **all** }

Parameters

Parameter	Description	Value
mac-address1 [**to** *mac-address2*]	Specifies MAC addresses to be added to a whitelist.	The value is in H-H-H format, where H is a hexadecimal number of 1 to 4 digits. The value cannot be all 0s, all Fs, or a multicast MAC address.
all	Deletes all the MAC addresses in a whitelist.	-

Views

AS authentication view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

When an SVF system needs to authenticate an AS, the SVF system allows the AS to connect to if the MAC address of the AS is in the whitelist and disallows the AS to connect to if the MAC address is in the blacklist.

Precautions

- A MAC address cannot exist in both the whitelist and blacklist.
- By default, if the MAC address of an AS is neither in the whitelist nor in the blacklist, the AS fails the authentication. You can run the **confirm** { **all** | **mac-address** *mac-address* } command to allow all ASs or a specified AS to pass the authentication.

Example

Add the MAC address xxxx-xxxx-xxxx to the whitelist.

```
<HUAWEI> system-view
[HUAWEI] as-auth
[HUAWEI-as-auth] whitelist mac-address xxxx-xxxx-xxxx
```

3.6 PoE Configuration Commands

3.6.1 Command Support

NOTE

Whether switches support PoE depends on the hardware. Non-PoE switches cannot be changed to PoE switches through software upgrades. A switch that meets any of the following conditions is a PoE switch:

- The device name contains PWR or PWH.
- The switch is released in V200R013C02 or later versions and provides new downlink interface types XUM, UM, P or U.

Only the following switch models support the PoE function:

S1720GW-E, S1720GWR-E, S5720-LI, S5720S-LI, S5720I-SI, S5731-H, S5731-S, S5731S-S, S5732-H, S2730S-S, S5735-L1, S300, S5735-L, S5735-L-I, S5735S-L1, S5735S-L, S5735S-L-M, S500, S5735-S, S5735S-H, S5735S-S, S5735-S-I, S5736-S

3.6.2 display poe device

Function

The **display poe device** command displays information about the device supporting Power over Ethernet (PoE).

Format

display poe device

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Before using the PoE function, run the **display poe device** command to check whether the device supports the PoE function. If the command output is displayed, the device supports the PoE function.

Example

Display information about the device supporting PoE.

```
<HUAWEI> display poe device
slot 0   : PoE
```

Table 3-123 Description of the display poe device command output

Item	Description
Slot 0	The device supports PoE.

3.6.3 display poe information

Function

The **display poe information** command displays PoE running information about the device.

Format

display poe information [**slot** *slot-id*]

Parameters

Parameter	Description	Value
slot *slot-id*	Displays the PoE running information in a specified slot ID. If this parameter is not specified, the PoE information about all device is displayed.	The value depends on the device configuration.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

This command displays information including the maximum output power set by the user, current power consumption, peak power consumption, and power management mode.

Example

Display the PoE running information about the device. (The actual output information may differ from the following information.)

```
<HUAWEI> display poe information
PSE Information of slot 0:
   User Set Max Power(mW)     : 739200
   PoE Power Supply(mW)       : 369600
   Available Total Power(mW)  : 369600
   Total Power Consumption(mW): 0
   Power Peak Value(mW)       : 0
   Power-Management Mode      : auto
   Power High Inrush          : disable
<HUAWEI> display poe information
PSE Information of slot 0:
MCU 1:
   User Set Max Power(mW)     : 739200
   PoE Power Supply(mW)       : 369600
   Available Total Power(mW)  : 369600
   Total Power Consumption(mW): 0
   Power Peak Value(mW)       : 0
   Power-Management Mode      : auto
   Power High Inrush          : disable
MCU 2:
   User Set Max Power(mW)     : 739200
   PoE Power Supply(mW)       : 369600
   Available Total Power(mW)  : 369600
   Total Power Consumption(mW): 0
   Power Peak Value(mW)       : 0
   Power-Management Mode      : auto
   Power High Inrush          : disable
```

Table 3-124 Description of the **display poe information** command output

Item	Description
User Set Max Power(mW)	Maximum output power set by the user. To set the value, run the **poe max-power** command. When the value is not set using the command, this field displays the maximum output power that can be provided by the device.

Item	Description
PoE Power Supply(mW)	PoE total power supply, which is determined by the PoE power module configured on the device. **NOTE** On the S5720I-6X-PWH-SI-AC switch, the total available power includes the power of two 12 V DC outputs and one 24 V AC output. No command is available to view the 12 V DC and 24 V AC output power. On the S5720I-10X-PWH-SI-AC switch, the total available power includes the power of two 12 V DC outputs and one 24 V AC output. To view the DC output power, run the **display device dc-output information** command.
Available Total Power(mW)	Remaining available power
Total Power Consumption(mW)	Total output power.
Power Peak Value(mW)	Peak value of the output power.
Power-Management Mode	Power management mode, including auto and manual modes. To set the mode, run the **poe power-management** command.
Power High Inrush	State of power high inrush function, including enabled and disabled state. By default, the power high inrush function is in disabled state. To set the state, run the **poe high-inrush enable** command.

3.6.4 display poe power

Function

The **display poe power** command displays current power information on interfaces.

Format

display poe power [**slot** *slot-id* | **interface** *interface-type interface-number*]

Parameters

Parameter	Description	Value
slot *slot-id*	Displays the PoE power information in a specified slot ID. If this parameter is not specified, the PoE power information of all devices in a stack system or the PoE power information of the device in a non-stack system is displayed.	The value depends on the device configuration.
interface *interface-type interface-number*	Displays the PoE power information about a specified interface. ● *interface-type* specifies the interface type. ● *interface-number* specifies the interface number. If this parameter is not specified, the output power of all interfaces on the device is displayed.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

The **display poe power** command displays information including the current actual power, maximum output power set for an interface, and class, reference power, and average power of PDs on the interface.

If this parameter is not specified, the output power of all interfaces on the device is displayed.

An interface provides 15400 mW power to PDs based on the power class 0 if non-standard PDs are connected to the interface or forcible power supply is configured on the interface of the switches except the S5720-16X-PWH-LI-AC, S5720-28X-

PWH-LI-AC, S5720I-SI, S2730S-S, S5735-L-I, S5735-L1, S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5735-S, S500, S5735-S-I, S5735S-H, S5736-S, S5731-H, S5731-S, S5731S-S, and S5732-H. If you run the **display poe power** command to check the interface power, the PD class is displayed as 0.

Example

Display the power information of interfaces on the device whose ID is 0.

```
<HUAWEI> display poe power slot 0
Codes: REFPW(Reference power), USMPW(User set max power),
       CURPW(Current power), PKPW(Peak power), AVGPW(Average power)

PortName             Class  REFPW(mW) USMPW(mW) CURPW(mW) PKPW(mW)  AVGPW(mW)
------------------------------------------------------------------------------
GigabitEthernet0/0/1   -      -        15400     0         0         0
GigabitEthernet0/0/2   -      -        15400     0         0         0
GigabitEthernet0/0/3   -      -        15400     0         0         0
GigabitEthernet0/0/4   -      -        15400     0         0         0
GigabitEthernet0/0/5   -      -        15400     0         0         0
GigabitEthernet0/0/6   -      -        15400     0         0         0
GigabitEthernet0/0/7   -      -        15400     0         0         0
GigabitEthernet0/0/8   -      -        15400     0         0         0
GigabitEthernet0/0/9   -      -        15400     0         0         0
GigabitEthernet0/0/10  -      -        15400     0         0         0
GigabitEthernet0/0/11  2      7000     15400     3710      3816      3487
GigabitEthernet0/0/12  2      7000     15400     2968      3180      2960
GigabitEthernet0/0/13  -      -        15400     0         0         0
GigabitEthernet0/0/14  -      -        15400     0         0         0
GigabitEthernet0/0/15  -      -        15400     0         0         0
GigabitEthernet0/0/16  -      -        15400     0         0         0
GigabitEthernet0/0/17  -      -        15400     0         0         0
GigabitEthernet0/0/18  -      -        15400     0         0         0
GigabitEthernet0/0/19  -      -        15400     0         0         0
GigabitEthernet0/0/20  -      -        15400     0         0         0
GigabitEthernet0/0/21  -      -        15400     0         0         0
GigabitEthernet0/0/22  -      -        15400     0         0         0
GigabitEthernet0/0/23  -      -        15400     0         0         0
GigabitEthernet0/0/24  -      -        15400     0         0         0
```

Table 3-125 Description of the display poe power slot command output

Item	Description
PortName	Name of an interface.
Class	Class of a PD on an interface. The system classifies PDs into nine classes, namely, class 0 to class 8, according to their maximum power. If no PD is connected to interface, "-" is displayed.
REFPW(mW)	Reference power of a PD. The system can identify the reference power of each PD. The value varies according to types of PDs.
USMPW(mW)	Maximum output power set for an interface. To set the value, run the **poe power** command.
CURPW(mW)	Current power of the PDs on an interface.

Item	Description
PKPW(mW)	Peak power of the PDs on an interface. The value is a statistical value, which equals the current maximum power consumption of the PDs on the interface.
AVGPW(mW)	Average power of the PDs on an interface. The value is a statistical value, which equals the average power consumption from the power-on of the interface till now.

Display the power of interface GigabitEthernet0/0/3.

```
<HUAWEI> display poe power interface gigabitethernet 0/0/3
PD power(mW)          : 3710
PD class              : 2
PD reference power(mW) : 7000
user set max power(mW) : 15400
PD peak power(mW)      : 3816
PD average power(mW)   : 3487
```

Table 3-126 Description of the display poe power interface command output

Item	Description
PD power(mW)	Output power of an interface.
PD class	Class of a PD on an interface. The system classifies PDs into nine classes, namely, class 0 to class 8, according to their maximum power.
PD reference power(mW)	Reference power of a PD. The system can identify the reference power of each PD. The value varies according to types of PDs.
user set max power(mW)	Maximum output power set for an interface. To set the value, run the **poe power** command.
PD peak power(mW)	Peak power of the PDs on an interface. The value is a statistical value, which equals the current maximum power consumption of the PDs on the interface.
PD average power(mW)	Average power of the PDs on an interface. The value is a statistical value, which equals the average power consumption from the power-on of the interface till now.

3.6.5 display poe power-state

Function

The **display poe power-state** command displays the PoE power supply status of a device.

Format

display poe power-state [**slot** *slot-id* | **interface** *interface-type interface-number*]

Parameters

Parameter	Description	Value
slot *slot-id*	Displays the PoE power supply status of a specified slot ID. If the parameter is not specified, the PoE power supply status of all devices in a stack system or the PoE power supply status of a device in a non-stack system is displayed.	The value range depends on the device configuration.
interface *interface-type interface-number*	Displays the PoE power supply status of a specified interface. • *interface-type* specifies the interface type. • *interface-number* specifies the interface number. If this parameter is not specified, the PoE power supply status of all interfaces on the device is displayed.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

The **display poe power-state** command displays information including whether an interface is enabled to check compatibility of non-standard PDs, power supply status on of an interface, class of PDs on an interface, power supply priority, and maximum output power of an interface.

Example

Display the PoE power supply status of GigabitEthernet 0/0/3.

```
<HUAWEI> display poe power-state interface gigabitethernet 0/0/3
Legacy detect           : disable
Power enable state      : enable
Power fast-on state     : -
Single-class state      : disable
Power-up mode           : at
Power-on delay(s)       : 0
PD power auto-neg state : enable
PD power-up mode        : at
PD support mode         : af at
Power ON/OFF            : on
Power status            : Powered
PD class                : 4
Reference power(mW)     : 30000
Power priority          : Low
Max power(mW)           : 30000
Current power(mW)       : 8910
Peak power(mW)          : 10725
Average power(mW)       : 8779
Current(mA)             : 162
Voltage(V)              : 55
```

Table 3-127 Description of the **display poe power-state interface** command output

Item	Description
Legacy detect	Whether an interface is enabled to check compatibility of non-standard PDs. To enable an interface to check compatibility of non-standard PDs, run the **poe legacy enable** command.
Power enable state	Whether PoE is enabled on an interface. To enable PoE on an interface, run the **poe enable** command.
Power fast-on state	Whether PoE fast power-on is enabled on an interface. To enable PoE fast power-on on an interface, run the **poe fast-on enable** command. If this field displays -, the device does not support the **poe fast-on enable** command.
Single-class state	Single-class power supply mode of an interface: ● disable: standard power supply mode ● enable: single-class power supply To set this parameter, run the **poe single-class enable** command.

Item	Description
Power-up mode	Power supply mode of an interface. To set the power supply mode for an interface, run the **poe { at-inrush | pre-bt-inrush | bt-inrush } enable** command. If this field displays -, this interface does not support this configuration.
Power-on delay(s)	Power supply delay of an interface, in seconds. The value 0 indicates that power supply is not delayed. To set the power supply delay, run the **poe power-on delay** command.
PD power auto-neg state	Whether power auto-negotiation is enabled for interfaces. To enable power auto-negotiation for interfaces, run the **poe power auto-neg enable** command. **NOTE** The S5731-H(except S5731-H48HB4XZ and S5731-H24HB4XZ), S5731-S, S5731S-S, S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5735-S, S500, S5735-S-I, S5720-12TP-PWR-LI-AC, S5720-28TP-PWR-LI-AC, S5720-28TP-PWR-LI-ACL, S5720-28P-PWR-LI-AC, S5720-52P-PWR-LI-AC, S5720-28X-PWR-LI-AC, S5720-28X-PWR-LI-ACF, S5720-52X-PWR-LI-AC, S5720-52X-PWR-LI-ACF, S5720S-12TP-PWR-LI-AC, S5720S-28TP-PWR-LI-ACL, S5720S-28P-PWR-LI-AC, S5720S-52P-PWR-LI-AC, S5720S-28X-PWR-LI-AC, and S5720S-52X-PWR-LI-AC support this field.
PD power-up mode	Current power supply standards of the PD connected to an interface: ● af: IEEE 802.3af ● at: IEEE 802.3at **NOTE** The S5731-H(except S5731-H48HB4XZ and S5731-H24HB4XZ), S5731-S, S5731S-S, S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5735-S, S500, S5735-S-I, S5720-12TP-PWR-LI-AC, S5720-28TP-PWR-LI-AC, S5720-28TP-PWR-LI-ACL, S5720-28P-PWR-LI-AC, S5720-52P-PWR-LI-AC, S5720-28X-PWR-LI-AC, S5720-28X-PWR-LI-ACF, S5720-52X-PWR-LI-AC, S5720-52X-PWR-LI-ACF, S5720S-12TP-PWR-LI-AC, S5720S-28TP-PWR-LI-ACL, S5720S-28P-PWR-LI-AC, S5720S-52P-PWR-LI-AC, S5720S-28X-PWR-LI-AC, and S5720S-52X-PWR-LI-AC support this field.

Item	Description
PD support mode	Power supply standards supported by the PD connected to an interface: ● af: IEEE 802.3af ● at: IEEE 802.3at ● af at: both IEEE 802.3af and 802.3at **NOTE** The S5731-H(except S5731-H48HB4XZ and S5731-H24HB4XZ), S5731-S, S5731S-S, S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5735-S, S500, S5735-S-I, S5720-12TP-PWR-LI-AC, S5720-28TP-PWR-LI-AC, S5720-28TP-PWR-LI-ACL, S5720-28P-PWR-LI-AC, S5720-52P-PWR-LI-AC, S5720-28X-PWR-LI-AC, S5720-28X-PWR-LI-ACF, S5720-52X-PWR-LI-AC, S5720-52X-PWR-LI-ACF, S5720S-12TP-PWR-LI-AC, S5720S-28TP-PWR-LI-ACL, S5720S-28P-PWR-LI-AC, S5720S-52P-PWR-LI-AC, S5720S-28X-PWR-LI-AC, and S5720S-52X-PWR-LI-AC support this field.
Power ON/OFF	Whether the interface is providing power: ● on: The interface is providing power. ● off: The interface is not providing power.

Item	Description
Power status	Power supply status of an interface: ● Test mode: indicates the testing state. ● Detecting: indicates the detection state. ● Disabled: indicates that PoE is disabled on the interface. ● Power-deny: indicates that the reference power is greater than the maximum output power of an interface. ● Classification overcurrent: indicates that the current of the PD connected to the interface exceeds the threshold. ● Unknown: indicates that the class of the PD is unknown. ● Power overcurrent: indicates that the current of the PD connected to the interface exceeds the maximum current of the interface. ● Power-on failed: indicates that the interface fails to provide power. ● Power-ready: indicates that the interface is ready to provide power. ● Powering: indicates that the PSE starts to power on the interface. ● Powered: indicates that the interface is providing power. ● Overloaded: indicates that the power is overloaded. ● Time-range power-off: indicates that the interface is in the power-off time range. ● Unstable voltage: indicates that the interface voltage is unstable. ● Legacy disable: indicates that the PSE does not check the capability of PDs. ● Class mismatch: indicates that the interface works in standard hierarchical power supply mode.
PD class	Class of a PD connected to an interface. The system classifies PDs into nine classes, namely, class 0 to class 8, according to their maximum power.
Reference power(mW)	Reference power of an interface. The system can identify the maximum power of a PD, classify the PD into a certain level, and define the reference power of each level.

Item	Description
Power priority	Power supply priority of an interface: ● Critical: indicates the highest priority. ● High: indicates the second highest priority. ● Low: indicates the lowest priority. To set the priority, run the **poe priority** command.
Max power(mW)	Maximum output power of an interface. A maximum output power of 15400 mW indicates that the device complies with IEEE 802.3af. A maximum output power of 30000 mW indicates that the device complies with IEEE 802.3at. To set the value, run the **poe power** command.
Current power(mW)	Current output power of an interface.
Peak power(mW)	Peak output power of an interface.
Average power(mW)	Average output power of an interface.
Current(mA)	Output current of an interface.
Voltage(V)	Output voltage of an interface.

Display the PoE power supply status of the device.

```
<HUAWEI> display poe power-state slot 0
PORTNAME            POWERON/OFF  ENABLED  FAST-ON  PRIORITY STATUS
--------------------------------------------------------------------------------
GigabitEthernet0/0/1     off     enable   disable  Low      Detecting
GigabitEthernet0/0/2     off     enable   disable  Low      Detecting
GigabitEthernet0/0/3     off     enable   disable  Low      Detecting
GigabitEthernet0/0/4     off     enable   disable  Low      Detecting
GigabitEthernet0/0/5     off     enable   disable  Low      Detecting
GigabitEthernet0/0/6     off     enable   disable  Low      Detecting
GigabitEthernet0/0/7     off     enable   disable  Low      Detecting
GigabitEthernet0/0/8     off     enable   disable  Low      Detecting
GigabitEthernet0/0/9     off     enable   disable  Low      Detecting
GigabitEthernet0/0/10    off     enable   disable  Low      Detecting
GigabitEthernet0/0/11    off     enable   disable  Low      Detecting
GigabitEthernet0/0/12    off     enable   disable  Low      Legacy disable
```

Table 3-128 Description of the display poe power-state slot command output

Item	Description
PORTNAME	Name of an interface.
POWERON/OFF	Whether the interface is providing power: ● On: The interface is providing power. ● Off: The interface is not providing power.

Item	Description
ENABLED	Whether PoE is enabled on an interface. To enable PoE on an interface, run the **poe enable** command.
FAST-ON	Whether PoE fast power-on is enabled on an interface. To enable PoE fast power-on on an interface, run the **poe fast-on enable** command.
PRIORITY	Power supply priority of an interface: ● Critical: indicates the highest priority. ● High: indicates the second highest priority. ● Low: indicates the lowest priority. To set the priority, run the **poe priority** command.

Item	Description
STATUS	Power supply status of an interface: • Test mode: indicates the testing state. • Detecting: indicates the detection state. • Disabled: indicates that PoE is disabled on the interface. • Power-deny: indicates that the reference power is greater than the maximum output power of an interface. • Classification overcurrent: indicates that the current of the PD connected to the interface exceeds the threshold. • Unknown: indicates that the class of the PD is unknown. • Power overcurrent: indicates that the current of the PD connected to the interface exceeds the maximum current of the interface. • Power-on failed: indicates that the interface fails to provide power. • Power-ready: indicates that the interface is ready to provide power. • Powering: indicates that the PSE starts to power on the interface. • Powered: indicates that the interface is providing power. • Overloaded: indicates that the power is overloaded. • Time-range power-off: indicates that the interface is in the power-off time range. • Unstable voltage: indicates that the interface voltage is unstable. • Legacy disable: indicates that the PSE does not check the capability of PDs. • Class mismatch: indicates that the interface works in standard hierarchical power supply mode.

3.6.6 display poe-power

Function

The **display poe-power** command displays information about the PoE power supply.

Format

display poe-power [**slot** *slot-id*]

Parameters

Parameter	Description	Value
slot *slot-id*	Specifies a slot ID.	The value depends on the device configuration.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

The **display poe-power** displays information including the available total PoE power, percentage of the reserved power, power alarm threshold, and PoE power module.

If the stack ID is not specified, information about the PoE power supply of all the stack devices is displayed.

Example

Display information about the PoE power supply of a switch (except S5720I-28X-PWH-SI-AC).

```
<HUAWEI> display poe-power
Slot 0
Total Available PoE Power(mW)  : 246400
Reserved PoE Power Percent     : 20 %
PoE Power Threshold Percent    : 90 %
   PoE Power 1
   Power Value(mW)          : 123200
   Type                  : PSA250-A2
   Supported Mode           : Redundancy, Balance
   PoE Power 2
   Power Value(mW)          : 123200
   Type                  : PSA250-A2
   Supported Mode           : Redundancy, Balance

Slot 1
Total Available PoE Power(mW) : 492800
Reserved PoE Power Percent    : 20 %
PoE Power Threshold Percent   : 90 %
   PoE Power 1
   Power Value(mW)          : 123200
   Type                  : PSA250-A2
   Supported Mode           : Redundancy, Balance
   PoE Power 2
   Power Value(mW)          : 369600
   Type                  : PSA500-A1
   Supported Mode           : Redundancy, Balance

Slot 2
Total Available PoE Power(mW) : 739200
Reserved PoE Power Percent    : 20 %
PoE Power Threshold Percent   : 90 %
```



```
  PoE Power 1
  Power Value(mW)          : 369600
  Type                  : PSA500-A1
  Supported Mode           : Redundancy, Balance
  PoE Power 2
  Power Value(mW)          : 369600
  Type                  : PSA500-A1
  Supported Mode           : Redundancy, Balance
```

Display information about the PoE power supply of S5720I-28X-PWH-SI-AC.

```
<HUAWEI> display poe-power
Slot 0
Total Available PoE Power(mW) : 369600
Power backup-mode             : 2+0
MCU 1:
Reserved PoE Power Percent    : 20 %
PoE Power Threshold Percent   : 90 %
MCU 2:
Reserved PoE Power Percent    : 20 %
PoE Power Threshold Percent   : 90 %

  PoE Power 1
  Power Value(mW)          : 369600
  PoE Power 2
  Power Value(mW)          : -
```

Table 3-129 Description of the display poe-power command output

Item	Description
Total Available PoE Power(mW)	Total power that can be provided for PDs.
Power backup-mode	PoE power supply backup mode: ● 2+0: high power mode ● 1+1: backup mode
MCU 1/MCU 2	MCU ID.
PoE Power 1/PoE Power 2	PoE Power ID.
Reserved PoE Power Percent	Percentage of the reserved power to the total power. To set the percentage, run the **poe power-reserved** command.
PoE Power Threshold Percent	Alarm threshold of the power consumption percentage. To set the threshold, run the **poe power-threshold** command.
Power Value(mW)	Power of a PoE power supply.

Item	Description
Type	Type of a PoE power supply. The value can be: • PSA250-A1: 250 W non-current-balance power supply • PSA250-A2: 250 W current balance power supply • PSA500-A1: 500 W current balance power supply • PAC1000S56-CB: 1000W AC power supply • PAC1000S56-DB: 1000W AC power supply • PDC1000S56-CB: 1000W DC power supply • PAC600S56-CB: 600W AC & 240V DC power module • PAC600S56-EB: 600W AC & 240V DC power module • PAC1000S56-EB: 1000W AC & 240V DC power module • PDC1000S56-EB: 1000W DC power module
Supported Mode	Supported PoE power supply mode. The value can be: • Redundancy: redundancy backup mode • Balance: current balance mode

3.6.7 poe af-inrush enable

Function

The **poe af-inrush enable** command configures the power supply standards of interfaces as 802.3af.

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

By default, interfaces on the devices supporting PoE++ comply with 802.3bt, the other interfaces comply with 802.3at.

Format

poe af-inrush enable

undo poe af-inrush enable

Parameters

None

Views

Interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Switches that comply with 802.3at or 802.3bt cannot power some non-standard PDs that do not support inrush current. To power these PDs, configure the power supply standards of interfaces as 802.3af.

Precautions

- The **poe af-inrush enable** command applies to the scenario where some non-standard PDs cannot be powered on. After this command is executed, some PDs requiring high current may be unable to be powered on.
- After running the **poe af-inrush enable** command, remove non-standard PDs and then install them so that they can be powered on.
- On the S5720-16X-PWH-LI-AC, S5720-28X-PWH-LI-AC, S5720I-SI, S2730S-S, S5735-L-I, S5735-L1, S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5735-S, S500, S5735-S-I, S5735S-H, S5736-S, S5731-H, S5731-S, S5731S-S, and S5732-H, the **poe af-inrush enable** and **poe single-class enable** commands are mutually exclusive and cannot be configured on the same interface.
- In an upgrade to V200R011C10 or later, if the **poe af-inrush enable** command is configured in the system view before the upgrade, the **poe af-inrush enable** command configuration is automatically generated on all interfaces after the upgrade.

Example

Configures the power supply standards of interfaces as 802.3af.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] poe af-inrush enable
Warning: This operation will cause PD to be powered off. Continue?[Y/N]:y
```

3.6.8 poe anti-interference frequency

Function

The **poe anti-interference frequency** command configures the PoE anti-interference frequency of the device.

The **undo poe anti-interference frequency** command restores the default configuration.

By default, the PoE anti-interference frequency of a device is 50 Hz.

NOTE

PoE models in the S5720-LI, S5720S-LI, and S5720I-SI series do not support this command. PoE models in other series support this command.

Format

poe anti-interference frequency { **50** | **60** }

undo poe anti-interference frequency

Parameters

Parameter	Description	Value
50	Sets the anti-interference frequency to 50 Hz.	-
60	Sets the anti-interference frequency to 60 Hz.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

The mains frequency varies in different countries and regions. Some are 60 Hz and some are 50 Hz. When a device provide PoE power supply, incorrect grounding may occur. As a result, industrial frequency interference is coupled to network cables, resulting in abnormal PoE detection classification. You can run the **poe anti-interference frequency** command to modify the PoE anti-interference frequency on the device to make that become the same as the mains frequency, reducing the impact of the mains frequency on PoE detection.

Example

Set the PoE anti-interference frequency of a device to 60 Hz.

```
<HUAWEI> system-view
[HUAWEI] poe anti-interference frequency 60
```

3.6.9 poe { at-inrush | pre-bt-inrush | bt-inrush } enable

Function

The **poe { at-inrush | pre-bt-inrush | bt-inrush } enable** command changes the power supply mode of interfaces supporting the PoE++ mode.

The **undo poe { at-inrush | pre-bt-inrush | bt-inrush } enable** command restores the default power supply mode of PoE interfaces.

By default, interfaces supporting the PoE++ mode on devices provide power in PoE ++ mode. That is, the power supply mode is **bt-inrush**, interfaces not supporting the PoE++ mode on devices provide power in **at-inrush** mode.

NOTE

Only the MultiGE interface of an S5720-28X-PWH-LI-AC, the first 12 electrical interfaces of an S5720-16X-PWH-LI-AC, the first 8 electrical interfaces of an S5720I-28X-PWH-SI-AC, and electrical interfaces of the S5720I-6X-PWH-SI-AC, S5720I-10X-PWH-SI-AC, S5720I-12X-PWH-SI-DC, S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5735-S, S500, S5735-S-I, S5731-H, S5731S-H, S5731-S, S5731S-S, and S5732-H support this command.

Format

poe { **at-inrush** | **pre-bt-inrush** | **bt-inrush** } **enable**

undo poe { **at-inrush** | **pre-bt-inrush** | **bt-inrush** } **enable**

Parameters

Parameter	Description	Value
at-inrush	Sets the power supply mode to PoE+.	-
pre-bt-inrush	Sets the power supply mode to PoE++ compatible. That is, except that the PoE power is 60000 mW, interfaces comply with 802.3at. **NOTE** The S2730S-S, S5735-L-I, S5735-L1, S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5735-S, S500, S5735-S-I, S5731-H, S5731S-H, S5731-S, and S5731S-S do not support the **pre-bt-inrush**.	-
bt-inrush	Sets the power supply mode to PoE++. **NOTE** The S2730S-S, S5735-L-I, S5735-L1, S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5735-S, S500, S5735-S-I, S5731-H, S5731S-H, S5731-S, and S5731S-S do not support the **bt-inrush**.	-

Views

Interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To power the PDs requiring the standard power supply mode, run the **poe at-inrush enable** command. This command changes the power supply mode of the PoE interface to the PoE+ mode. If most of the parameters supported by the PDs requiring high power comply with 802.3at, run the **poe pre-bt-inrush enable**

command to change the power supply mode of these interfaces to PoE++ compatible.

Precautions

- When the **poe bt-inrush enable** command is configured after the **poe af-inrush enable** command is configured in the interface, the **poe af-inrush enable** command configuration is automatically overwritten.
- The **poe { pre-bt-inrush | bt-inrush } enable** and **poe single-class enable** commands are mutually exclusive and cannot be configured on the same interface.
- Changing the power supply mode of a PoE interface will power off the PD connected to this PoE interface.
- After the power supply mode of an interface is set to **bt-inrush**, forcible PoE power supply and PD compatibility check configured on this interface using the **poe force-power** and **poe legacy enable** commands respectively do not take effect on this interface.
- After the power supply mode of an interface is set to **bt-inrush**, and the interface detects that it connects to a non-standard PD, confirm whether this interface is connected to a PD. If so, run the **poe pre-bt-inrush enable** command and the **poe legacy enable** or **poe force-power** command to provide power to this PD.

Example

Set the power supply mode of GE0/0/1 to PoE+.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] poe at-inrush enable
Warning: This operation will cause the PD to be powered off. Continue?[Y/N]:y
```

Set the power supply mode of GE0/0/1 to PoE++ compatible.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] poe pre-bt-inrush enable
Warning: This operation will cause the PD to be powered off. Continue?[Y/N]:y
```

3.6.10 poe enable

Function

The **poe enable** command enables the PoE function on an interface.

The **undo poe enable** command disables the PoE function on an interface.

By default, the PoE function is enabled on an interface.

Format

poe enable

undo poe enable

Parameters

None

Views

Interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenarios

Before providing power for the PD connected to an interface, ensure that the PoE function has been enabled on the interface. If the PoE function is not enabled on the interface, run the **poe enable** command to enable the PoE function on the interface.

In automatic mode, PD power-on and power-off on interfaces are determined by the PoE power and interface power priority. When the PoE power is sufficient, the device does not power off the PD connected to any interface. To stop providing power for a PD, run the **undo poe enable** command on the interface to which the PD is connected.

Precautions

The device only supports PoE power supply on downlink interfaces and does not support PoE power supply on uplink interfaces.

Example

Disable the PoE function on GigabitEthernet0/0/3.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/3
[HUAWEI-GigabitEthernet0/0/3] undo poe enable
```

3.6.11 poe fast-on enable

Function

The **poe fast-on enable** command enables fast power-on for a PoE interface.

The **undo poe fast-on enable** command disables fast power-on for a PoE interface.

By default, fast power-on is disabled on a PoE interface.

NOTE

Only the S5720-28X-PWH-LI-AC, S5720-16X-PWH-LI-AC, S5720I-12X-PWH-SI-DC, S5735S-H, S5736-S, S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5735-S, S500, S5731-H, S5731S-H, S5731-S, S5731S-S, and S5732-H support this command.

Format

poe fast-on enable

undo poe fast-on enable

Parameters

None

Views

Interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After a PoE switch is powered off and then restarts, interfaces on this device can be powered on again only after a certain period. As a result, PDs connected to these interfaces are powered off within this period. To shorten the time during which the PDs are powered off, you can run the **poe fast-on enable** command on the PoE switch. After the PoE switch is powered off and then restarts, PoE interfaces can rapidly resume power supply to PDs.

Precautions

- This command takes effect only during cold startup of the device.
- The **poe fast-on enable** command does not generate any configuration but always takes effect after being executed until the **undo poe fast-on enable** command is executed. To determine whether the fast power-on configuration takes effect, run the **display poe power-state** command to check the **fast-on** field.

Example

Enable fast power-on for GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] poe fast-on enable
Warning: This configuration takes effect only after a cold restart. Continue?[Y/N]:y
Warning: Ensure that the power required by the connected PD does not exceed the rated PoE power provided by the device. Otherwie, the device may not start normally. Continue?[Y/N]:y
```

Disable fast power-on for GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo poe fast-on enable
Warning: This configuration takes effect only after a cold restart. Continue?[Y/N]:y
```


3.6.12 poe force-power

Function

The **poe force-power** command enables forcible powering on a PoE interface.

The **undo poe force-power** command disables forcible powering on a PoE interface.

By default, forcible powering is disabled on a PoE interface.

Format

poe force-power

undo poe force-power

Parameters

None

Views

Interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If the power of the system is sufficient, you can run the **poe force-power** command on the interface connected to PDs when the PSE cannot detect the PDs.

Precautions

After the power supply mode of an interface is set to PoE++ using the **poe bt-inrush enable** command, the **poe force-power** command does not take effect on this interface.

The **poe force-power** command and the **poe legacy enable** command are mutually exclusive. When configured on the same interface, the later configured command takes effect and the earlier configured command is cleared.

If the interface connects to a non-PD device, configuring forcible powering on the interface may damage the non-PD device. Exercise caution when using the **poe force-power** command. After forcible powering is configured on a PoE switch, you must delete the forcible powering configuration from the switch if you need to remove the switch from the current networking environment and deploy it in a new networking environment.

Example

Enable forcible powering on GigabitEthernet0/0/1.


```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] poe force-power
Warning: Is there a valid PD connected to this interface? Yes or No?[Y/N]:y
```

3.6.13 poe group management enable

Function

The **poe group management enable** command enables a PoE device's group management of PDs.

The **undo poe group management enable** command disables a PoE device's group management of PDs.

By default, a PoE device's group management of PDs is disabled.

NOTE

Among PoE models, the S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5735-S, S500, S5735-S-I, S5731-H, S5731-S, S5731-S24UN4X2Q, S5731-S8UM16UN2Q, S5731S-S24UN4X2Q-A, S5731S-S8UM16UN2Q-A, S5736-S24UM4XC, and S5731S-S do not support this command.

Format

poe group management enable

undo poe group management enable

Parameters

None

Views

Interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Powering on some PDs may affect other PDs, causing other PDs unable to be detected by a PoE device. After group management of PDs is enabled, a PoE device can detect PDs on a per-group basis and power on these PDs in a batch.

Precautions

- To support a PoE device's group management of PDs, every four interfaces on the left are added to one group. For example, interfaces numbered 1 to 4 or numbered 5 to 8 can be added to one group, but interfaces numbered 2 to 5 cannot. That is, the number of the last interface in each group must be the multiple of 4. If the **poe group management enable** command is configured

on any interface in a group, this command is also delivered to the other three interfaces in the same group.

- After group management of PDs is configured on an interface, the other interfaces in the same group use the same power supply priority as this interface and this priority is lower than that of other interfaces that are not added to any group. If some interfaces have this group management function configured, the PoE interface power supply priority configured using the **poe priority** command does not take effect on these interfaces.

Example

Enable group management of PDs on PoE interfaces GE0/0/1 through GE0/0/4.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] poe group management enable
Info: 'Poe group management enable' will be executed on interface GigabitEthernet0/0/1 to
GigabitEthernet0/0/4. Continue?[Y/N]: y
```

3.6.14 poe high-inrush enable

Function

The **poe high-inrush enable** command configures an interface to allow generation of the high pulse current during power-on.

The **undo poe high-inrush enable** command configures an interface not to allow generation of the high pulse current during power-on.

By default, interfaces do not allow generation of the high pulse current during power-on.

Format

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

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

Parameters

Parameter	Description	Value
slot *slot-id*	Specifies a slot ID.	The value range depends on the device configuration.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

High inrush current is generated when a non-standard PD is powered on. In this case, the PSE cuts off the power of the PD to protect itself. If the PSE is required to provide power for the PD, the PSE must allow high inrush current. The high inrush current may damage device components.

Example

Enable the device to allow generation of the high pulse current during power-on.

```
<HUAWEI> system-view
[HUAWEI] poe high-inrush enable
```

3.6.15 poe { power-off | power-on } interface

Function

The **poe** { **power-off** | **power-on** } **interface** command manually powers on or powers off the PD of an interface.

NOTE

Among PoE models, the S5720-16X-PWH-LI-AC, S5720-28X-PWH-LI-AC, S5720I-SI, S2730S-S, S5735-L-I, S5735-L1, S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5735-S, S500, S5735-S-I, S5735S-H, S5736-S, S5731-H, S5731-S, S5731S-S, and S5732-H do not support this command.

Format

poe { **power-off** | **power-on** } **interface** *interface-type interface-number*

Parameters

Parameter	Description	Value
power-off	Powers off an interface.	-
power-on	Powers on an interface.	-
interface-type interface-number	Specifies the type and number of the interface that needs to be powered on or powered off manually.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenarios

By default, a PoE device works in automatic power management mode. After a PD is connected to a PoE device, the PoE device automatically provides power for the PD.

After you run the **poe power-management** command to configure the power management mode of a PoE device to manual, the PoE device does not automatically provide power for PDs when PDs are connected to the PoE device. You need to run the **poe power-on interface** command to manually power on the interfaces of the PoE device. Check whether the interface is powered on based on the Power ON/OFF field in the **display poe power-state** command.

Precautions

When the available power of the device is insufficient and the device cannot provide power for a new PD, the **poe power-on interface** command is invalid.

Pre-configuration Tasks

Before powering on or powering off an interface, ensure that:

- The power management mode has been in manual mode through running the **poe power-management** command.
- PDs have been connected to the interface.
- The PoE function of the interface has been enabled.
- The classification of the PDs connected to the interface has finished and the PDs have been ready for being powered on.

Example

Manually power on PDs connected to GigabitEthernet 0/0/1.

```
<HUAWEI> system-view
[HUAWEI] poe power-management manual
[HUAWEI] poe power-on interface gigabitethernet 0/0/1
```

3.6.16 poe legacy enable

Function

The **poe legacy enable** command enables the power sourcing equipment (PSE) to check the compatibility of power devices (PDs).

The **undo poe legacy enable** command disables the PSE from checking the compatibility of PDs.

By default, the PSE does not check the capability of PDs.

Format

poe legacy enable

undo poe legacy enable

Parameters

None

Views

Interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After the switch is enabled to check the compatibility of PDs, the switch can detect and provide power to the PDs that do not comply with the 802.3af or 802.3at standard or the standard PDs that are detected as non-standard PDs because of the external environment. If compatibility check is disabled, the switch cannot provide power to the non-standard PDs.

After interfaces are enabled to check the compatibility of PDs, the interfaces can provide power to both standard and non-standard PDs. This configuration does not affect the power supply of standard PDs. That is, the interfaces can still provide power to standard PDs after the **poe legacy enable** command is configured.

Precautions

After the power supply mode of an interface is set to PoE++ using the **poe bt-inrush enable** command, the **poe legacy enable** command does not take effect on this interface.

The **poe force-power** command and the **poe legacy enable** command are mutually exclusive. When configured on the same interface, the later configured command takes effect and the earlier configured command is cleared.

If the interface is connected to a non-PD device, enabling PD compatibility check may damage this non-PD device. Exercise caution when you use this command. After enabling PD compatibility check on a PoE switch, you need to manually disable this function if you need to remove the switch from the current networking environment and deploy it in a new networking environment.

Example

Enable GigabitEthernet0/0/1 to check the compatibility of the PD.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] poe legacy enable
```


3.6.17 poe lldp-proxy

Function

The **poe lldp-proxy** command configures a 10GE optical port as a proxy for a MultiGE electrical port to perform LLDP negotiation.

The **undo poe lldp-proxy** command restores the default configuration.

By default, a 10GE optical port does not act as a proxy for a MultiGE electrical port to perform LLDP negotiation.

NOTE

Only the S5732-H48XUM2CC supports this command.

Format

poe lldp-proxy interface multige *interface-number*

undo poe lldp-proxy

Parameters

Parameter	Description	Value
interface multige *interface-number*	Specifies the number of a MultiGE electrical port.	It must be a MultiGE electrical port on the panel of an S5732-H48XUM2CC switch.

Views

XGE interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Hybrid optical/electrical cables integrate optical fibers and electrical cables and are used to connect S5732-H48XUM2CC switches to APs. Hybrid optical/electrical cables are often used in the following scenarios:

- One end of the RJ45 cable in a hybrid optical/electrical cable is connected to a MultiGE electrical port of a switch, and the other end is connected to the RJ45 power receiving port of an AP. The RJ45 cable is used only for the switch to provide PoE power supply for the AP and does not transmit data.
- One end of the optical fiber in a hybrid optical/electrical cable is connected to a 10GE optical port on a switch, and the other end is connected to an uplink

10GE optical port on an AP. The optical fiber is used for data transmission between the switch and AP.

Since the MultiGE electrical port connected to a hybrid optical/electrical cable stays in the **down** state, to use LLDP to negotiate the power supply capability, you must run the **poe lldp-proxy** command to configure the 10GE optical port on the switch connected to the hybrid optical/electrical cable as a proxy for the MultiGE electrical port to perform LLDP negotiation.

Precautions

- LLDP must be enabled on the 10GE optical port connected to a hybrid optical/electrical cable. This function is enabled by default.
- If an AP requires PoE++ power supply, run the **poe legacy enable** command on the 10GE optical port connected to a hybrid optical/electrical cable to enable compatibility check.

Example

Configure the 10GE 0/0/1 optical port as a proxy for the MultiGE 0/0/1 electrical port to perform LLDP negotiation.

```
<HUAWEI> system-view
[HUAWEI] interface XGigabitEthernet 0/0/1
[HUAWEI-XGigabitEthernet0/0/1] poe lldp-proxy interface MultiGE 0/0/1
```

3.6.18 poe max-power

Function

The **poe max-power** command sets the maximum output power of the device.

The **undo poe max-power** command restores the default maximum output power of the device.

By default, the maximum output power of a device is the power actually provided by the device. Therefore, the configured maximum output power must be lower than or equal to the total power of PoE power modules. On the S5720I-12X-PWH-SI-DC, the default maximum output power is 220000 mW, and the supported maximum output power is 240000 mW. On the S5720I-10X-PWH-SI-AC, the default maximum output power is 175000 mW. When the 110 V voltage is input, the maximum output power is 175000 mW. When the input voltage is 220 V, the maximum output power is 200000 mW.

Format

poe max-power *max-power* [**slot** *slot-id* [**mcu** *mcu-id*]]

undo poe max-power *max-power* **slot** *slot-id*

undo poe max-power [**slot** *slot-id* [**mcu** *mcu-id*]]

NOTE

Only the S5720I-28X-PWH-SI-AC supports the **mcu** *mcu-id* parameter.

Parameters

Parameter	Description	Value
max-power	Specifies the maximum output power.	The value is an integer that ranges from 15400 to 2880000, in mW.
slot *slot-id*	Specifies a slot ID.	The value depends on the device configuration.
mcu *mcu-id*	Specifies an MCU ID.	The value is 1 or 2.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In a stack, if no stack ID is added to the **poe max-power** command, this command sets the maximum output power of all stack member switches.

Precautions

- If the configured maximum output power is lower than the total power required by PDs, lower-priority PDs will be powered off or cannot be powered on manually.
- The configured maximum output power of the device must be lower than the remaining PoE power of the device. Otherwise, the configuration does not take effect.

Example

Set the maximum output power of the device with the ID 0 to 45000 mW.

```
<HUAWEI> system-view
[HUAWEI] poe max-power 45000 slot 0
```

3.6.19 poe power

Function

The **poe power** command sets the maximum output power of an interface.

The **undo poe power** command restores the default maximum output power of an interface.

This default value varies depending on interfaces of switches:

- The electrical interface of an S5731-S24UN4X2Q, S5731-S8UM16UN2Q, S5731S-S24UN4X2Q-A, S5731S-S8UM16UN2Q-A, S5736-S24UM4XC, S5736-S24U4XC, S5736-S48U4XC, S5735S-H24U4XC-A, or S5735S-H48U4XC-A: 90000 mW
- The MultiGE interface of an S5720-28X-PWH-LI-AC: 60000 mW; Other electrical interface of an S5720-28X-PWH-LI-AC: 30000 mW
- First 8 electrical interfaces of an S5720I-28X-PWH-SI-AC: 60000 mW; last 16 electrical interfaces of an S5720I-28X-PWH-SI-AC: 30000 mW
- The electrical interface of an S5720I-6X-PWH-SI-AC, S5720I-10X-PWH-SI-AC, S5720I-12X-PWH-SI-DC, S5720-16X-PWH-LI-AC, or S5732-H: 60000 mW
- The electrical interface of other PoE devices: 30000 mW

Format

poe power *port-max-power*

undo poe power

Parameters

Parameter	Description	Value
port-max-power	Specifies the maximum output power of an interface.	The value is an integer, in mW. ● For a electrical interface of S5731-S24UN4X2Q, S5731-S8UM16UN2Q, S5731S-S24UN4X2Q-A, S5731S-S8UM16UN2Q-A, S5736-S24UM4XC, S5736-S24U4XC, S5736-S48U4XC, S5735S-H24U4XC-A, or S5735S-H48U4XC-A, the value ranges from 0 to 90000. ● For a MultiGE interface of S5720-28X-PWH-LI-AC, the value ranges from 0 to 60000. For other an electrical interface of S5720-28X-PWH-LI-AC, the value ranges from 0 to 30000. ● For the first 8 electrical interfaces of an S5720I-28X-PWH-SI-AC, the value ranges from 0 to 60000. For the last 16 electrical interfaces of an S5720I-28X-PWH-SI-AC, the value ranges from 0 to 30000. ● For an electrical interface of S5720I-6X-PWH-SI-AC, S5720I-10X-PWH-SI-AC, S5720I-12X-PWH-SI-DC, S5720-16X-PWH-LI-AC, S5732-H, or the value ranges from 0 to 60000.

Parameter	Description	Value
		• For electrical interfaces of other PoE devices, the value ranges from 0 to 30000.

Views

Interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenarios

The PD negotiation power may be different from the power required by some non-standard PDs or PDs that cannot be classified. You can run the **poe power** command to set the maximum output power of the interface, which prevents power overload for PDs and saves energy.

Prerequisites

The PoE function has been enabled on the interface using the **poe enable** command.

Example

Set the maximum output power on GigabitEthernet0/0/1 to 15400 mW.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] poe power 15400
```

3.6.20 poe power auto-neg enable

Function

The **poe power auto-neg enable** command enables power auto-negotiation for interfaces.

The **undo poe power auto-neg enable** command disables power auto-negotiation for interfaces.

By default, power auto-negotiation is disabled for interfaces.

NOTE

Among PoE models, only the S5731-H(except S5731-H48HB4XZ and S5731-H24HB4XZ), S5731-S, S5731S-S, S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5735-S, S500, S5735-S-I, S5720-12TP-PWR-LI-AC, S5720-28TP-PWR-LI-AC, S5720-28TP-PWR-LI-ACL, S5720-28P-PWR-LI-AC, S5720-52P-PWR-LI-AC, S5720-28X-PWR-LI-AC, S5720-28X-PWR-LI-ACF, S5720-52X-PWR-LI-AC, S5720-52X-PWR-LI-ACF, S5720S-12TP-PWR-LI-AC, S5720S-28TP-PWR-LI-ACL, S5720S-28P-PWR-LI-AC, S5720S-52P-PWR-LI-AC, S5720S-28X-PWR-LI-AC, and S5720S-52X-PWR-LI-AC support this command.

Format

poe power auto-neg enable

undo poe power auto-neg enable

Parameters

None

Views

Interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

By default, the switch supplies power to the APs connected to interfaces in compliance with IEEE 802.3at (the maximum output power is 30 W). Some APs support both IEEE 802.3at and 802.3af. The switch can supply power to these APs in accordance with IEEE 802.3af (the maximum output power is 15.4 W). When the APs connected to the switch support both IEEE 802.3at and 802.3af, enable power auto-negotiation on the interfaces connected to these APs. When the total available power of the switch is less than 30 W and the switch detects that the current power supply standards of an AP are IEEE 802.3at, the switch can send an LLDP packet to the AP to enable the AP to set its power supply standards to IEEE 802.3af. Power auto-negotiation changes only the power supply standards of APs but not the interfaces to which the APs are connected.

Enabling power auto-negotiation on interfaces will change the power supply standards of the APs connected to the interfaces, reduce the power consumption of the APs, and enable the switch to supply power to more APs when the rated output power of the switch is fixed.

Precautions

- The **poe power auto-neg enable** command is mutually exclusive with the **lldp dot3-tlv power 802.1ab force** and **lldp dot3-tlv power 802.3at** commands and cannot be configured together.
- When the total available power of the switch is less than 30 W, the power supply standards of all the APs connected to the interfaces that have power

auto-negotiation enabled will be set to IEEE 802.3af. When the total available power of the switch is more than the larger value of 60 W and reserved power, the power supply standards of the APs connected to the interfaces will be restored to IEEE 802.3at based on the power supply priority configured on the interfaces. That is, the power supply standards of the AP connected to the interface with a higher priority are restored to IEEE 802.3at. If the power supply priority of these interfaces is the same, the power supply standards of the AP connected to the interface with a smaller interface number are restored to IEEE 802.3at first.

- Disabling power auto-negotiation on an interface will restore the power supply standards of the AP connected to the interface to IEEE 802.3at. This operation will power off the APs connected to some interfaces if the total power of the switch is insufficient.

Example

Enable power auto-negotiation on GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] poe power auto-neg enable
Warning: This operation will enable PoE power auto-negotiation of the port, which will change the power-up mode of the PD connected to the port from AT to AF in case of insufficient power. Continue?[Y/N]:y
```

3.6.21 poe power-management

Function

The **poe power-management** command sets the power management mode of the device.

The **undo poe power-management** command restores the default power management mode of the device.

By default, the device uses the automatic power management mode.

NOTE

Among PoE models, the S5720-16X-PWH-LI-AC, S5720-28X-PWH-LI-AC, S5720I-SI, S2730S-S, S5735-L-I, S5735-L1, S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5735-S, S500, S5735-S-I, S5735S-H, S5736-S, S5731-H, S5731-S, S5731S-S, and S5732-H do not support this command.

Format

poe power-management { **auto** | **manual** } [**slot** *slot-id*]

undo poe power-management { **auto** | **manual** } **slot** *slot-id*

undo poe power-management [**slot** *slot-id*]

Parameters

Parameter	Description	Value
auto	Specifies the power management mode to automatic mode.	-
manual	Specifies the power management mode to manual mode.	-
slot *slot-id*	Specifies the slot ID.	The value range depends on the device configuration.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenarios

In automatic power management mode, the device first provides power for the interfaces with higher priority and powers off the interfaces of lower priority when the power is insufficient. When the power is sufficient, all interfaces connected to PDs are powered on. To stop providing power for some interfaces, run the **undo poe enable** command to disable the PoE function on the interfaces. If the PoE function is enabled and disabled frequently, faults may occur on the interfaces. To prevent the faults, you can set the power management mode to manual mode. In manual mode, the power-on and power-off of an interface are controlled manually and not affected by the interface power priority.

Precautions

- If all the interfaces are of the same priority, the power supply priority of the interface with a smaller interface number is higher in automatic mode.
- You can view the power management mode by running the **display poe information** command.

Follow-up Procedures

After setting the power management mode to manual, you need to run the **poe { power-off | power-on } interface** command to manually power on or off the PDs connected to interfaces of the device. If the device restarts after being powered off, you need to run the **power-on** command on the interfaces again to power on the PDs connected to the interfaces. If the device restarts without being powered off, you do not need to run the **power-on** command on the interfaces again to power on the PDs.

Example

Set the power management mode of a device to automatic mode.
<HUAWEI> **system-view**
[HUAWEI] **poe power-management auto slot 0**

3.6.22 poe power-off time-range

Function

The **poe power-off time-range** command makes a configured PoE power-off time range effective on an interface.

The **undo poe power-off time-range** command cancels the configuration.

By default, a device is not configured with PoE power-off time range.

Format

poe power-off time-range *time-range-name*

undo poe power-off time-range

Parameters

Parameter	Description	Value
time-range-name	Specifies a name for a PoE power-off time range.	The value is a string of 1 to 32 case-sensitive characters and must begin with a letter. In addition, the word all cannot be specified as a time range name.

Views

Interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **poe power-off time-range** command makes a PoE power-off time range set in the system view effective on an interface. If the current time is within the specified time range, the PD connected to the interface cannot be powered on.

The **undo poe power-off time-range** command cancels the configuration. The time range does not take effect on the PD connected to the interface; however, the configuration of the time range is still saved.

Pre-configuration Tasks

Before running the **poe power-off time-range** command, you must ensure a PoE power-off time range has been configured through running the **time-range** command in the system view.

Example

Configure a PoE power-off time range from 10:00 to 11:00 for PDs connected to GigabitEthernet0/0/1.

```
<HUAWEI> system-view
[HUAWEI] time-range PoE 10:00 to 11:00 daily
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] poe power-off time-range PoE
```

3.6.23 poe power-on delay

Function

The **poe power-on delay** command sets the PoE power supply delay on an interface.

The **undo poe power-on delay** command restores the default PoE power supply delay on an interface.

By default, the PoE power supply delay is 0. That is, the PoE power supply is not delayed.

Format

poe power-on delay *delay-time*

undo poe power-on delay

Parameters

Parameter	Description	Value
delay-time	Specifies the PoE power supply delay.	The value is an integer that ranges from 1 to 60, in seconds.

Views

Interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The maintain current of the used PD is insufficient at the power-on moment, so the PoE switch considers that the PD has been disconnected and powers it off.

IEEE standards require that a PD must maintain a current value of more than 10 mA for at least 75 ms in each 325 ms duration. Otherwise, the PoE switch considers that the PD has left and powers off the PD.

To enable the PoE switch to power these non-standard PDs, set the PoE power supply delay on the appropriate interfaces of the switch so that the switch detects the maintain power of the PDs after the specified delay.

Precautions

After the PoE power supply delay is configured on an interface, do not replace the PD connected to this interface within the delay. Otherwise, the new PD cannot work properly.

Example

Set the PoE power supply delay to 5 seconds on GigabitEthernet0/0/1.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] poe power-on delay 5
```

3.6.24 poe power-reserved

Function

The **poe power-reserved** command sets the percentage of the reserved PoE power against the total PoE power.

The **undo poe power-reserved** command restores the default percentage of the reserved PoE power against the total PoE power.

By default, the percentage of the reserved PoE power against the total PoE power is 20%.

Format

poe power-reserved *power-reserved* [**slot** *slot-id* [**mcu** *mcu-id*]]

undo poe power-reserved *power-reserved* **slot** *slot-id*

undo poe power-reserved [**slot** *slot-id* [**mcu** *mcu-id*]]

NOTE

Only the S5720I-28X-PWH-SI-AC supports the **mcu** *mcu-id* parameter.

Parameters

Parameter	Description	Value
power-reserved	Specifies the percentage of the reserved PoE power against the total PoE power.	The value is an integer that ranges from 0 to 100, in percentage. The default value is 20.

Parameter	Description	Value
slot *slot-id*	Specifies a slot ID.	The value depends on the device configuration.
mcu *mcu-id*	Specifies an MCU ID.	The value is 1 or 2.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenarios

The device can dynamically allocate power to each interface according to the power consumption of each interface. The power consumption of a PD keeps changing when the PD is running. The system periodically calculates the total power consumption of all the PDs. If the total power consumption exceeds the upper threshold of the device, the system powers off the PDs on the interfaces of low priority. If interfaces have the same priority, the system powers off the PD on the interface with a larger port number.

Sometimes, however, the power consumption increases sharply and the available power of the system cannot support the burst increase of power. At this time, the system has not calculated and found that the total power consumption exceeded the upper threshold; therefore, the system does not cut off power low-priority interfaces in time. As a result, the PoE power supply is shut down for overload protection, and all PDs are powered off.

This problem can be solved by running the **poe power-reserved** command to set proper reserved power. When there is a burst increase in power consumption, the reserved power can support the system running. Then the system has time to power off interfaces of low priority to ensure stable running of other PDs.

Precautions

- The reserved power should not be set greater than 20%. If the reserved PoE power is greater than 20% of the total PoE power, the power capacity of the device is affected.
- To set the maximum output power of a device, run the **poe max-power** command. In this case, the device calculates the reserved power based on the set maximum output power. If the maximum output power is not set, the available PoE power is the power provided by the PoE power module.

Example

Set the percentage of reserved PoE power to the total PoE power to 30%.


```
<HUAWEI> system-view
[HUAWEI] poe power-reserved 30
Warning: The power for new PDs connected to slot 0 may be insufficient after this operation is performed.
Continue?[Y/N]:y
```

3.6.25 poe power-threshold

Function

The **poe power-threshold** command sets the alarm threshold of the PoE power consumption percentage.

The **undo poe power-threshold** command restores the default alarm threshold of the PoE power consumption percentage.

By default, the alarm threshold is 90%. That is, an alarm is generated when the consumed power accounts for 90% of the total power.

Format

poe power-threshold *threshold-value* [**slot** *slot-id* [**mcu** *mcu-id*]]

undo poe power-threshold *threshold-value* **slot** *slot-id*

undo poe power-threshold [**slot** *slot-id* [**mcu** *mcu-id*]]

NOTE

Only the S5720I-28X-PWH-SI-AC supports the **mcu** *mcu-id* parameter.

Parameters

Parameter	Description	Value
threshold-value	Specifies the alarm threshold of the PoE power consumption percentage. When the power consumption reaches this value, a PoE power alarm is generated.	The value is an integer that ranges from 0 to 100, in percentage. The default value is 90.
slot *slot-id*	Specifies a slot ID.	The value depends on the device configuration.
mcu *mcu-id*	MCU ID	The value is an integer ranging from 1 to 2.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

The **poe power-threshold** command sets the alarm threshold of the PoE power consumption percentage. If the total PoE power is 369.6 W and the alarm threshold is 90%, an alarm is generated when the power consumption is greater than 332.64 W. When the power consumption falls below 332.64 W, the alarm is cleared.

Example

Set the alarm threshold of the PoE power consumption percentage to 80%.

```
<HUAWEI> system-view
[HUAWEI] poe power-threshold 80
```

3.6.26 poe priority

Function

The **poe priority** command sets the power priority of a PoE interface.

The **undo poe priority** command restores the default power priority of a PoE interface.

By default, the power supply priority of an interface is **low**.

Format

poe priority { **critical** | **high** | **low** }

undo poe priority

Parameters

Parameter	Description	Value
critical	Indicates the highest priority.	-
high	Indicates the second highest priority.	-
low	Indicates the lowest priority.	-

Views

Interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

When the output power of a device is insufficient, the device in automatic power management mode provides power for the interfaces of the higher power supply priorities first and cuts off power of the interfaces of the lower power supply priorities. PoE switches provide power to PDs connected to the interfaces in the sequence in which PDs are connected to them.

Example

Set the power supply priority of GigabitEthernet0/0/1 to critical.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] poe priority critical
```

3.6.27 poe-power backup-mode

Function

The **poe-power backup-mode** command sets the PoE power supply mode to the backup mode.

The **undo poe-power backup-mode** command restores the PoE power supply mode to the high-power mode.

By default, the PoE power supply mode is the high-power mode.

NOTE

Only the S5720I-28X-PWH-SI-AC supports this command.

Format

poe-power backup-mode *backup-mode* [**slot** *slot-id*]

undo poe-power backup-mode [**slot** *slot-id*]

Parameters

Description	Description	Value
backup-mode	Specifies the backup mode of PoE power supplies.	The value can only be 1.

Description	Description	Value
slot *slot-id*	Specifies a slot ID. If this parameter is not specified in Stack, only the PoE power supply mode of the master switch is modified.	The value must be set according to the device configuration.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The S5720I-28X-PWH-SI-AC has two built-in power modules, which support two PoE power supply modes:

- High-power mode (default): When two power modules are used, they provide 369.6 W PoE power for the first 8 electrical ports and last 16 electrical ports respectively, and the system provides 739.2 W PoE power. If one of the two power modules is faulty, the first 8 electrical interfaces provide power normally, but the PDs connected to the last 16 electrical ports are powered off and the PoE function becomes unavailable on the last 16 electrical ports. When only one power module is used, only the first 8 electrical interfaces can provide PoE power.
- PoE backup mode: The PoE power supply mode can be manually set to the backup mode using the **poe-power backup-mode** command. The backup mode provides 1+1 redundancy. In backup mode, the system provides 369.6 W PoE power, regardless of whether one or two power modules are used. The 369.6 W PoE power is shared by 24 electrical ports. Setting the PoE power supply mode to the backup mode can improve system stability.

Precautions

Changing the PoE power supply mode will power off the PDs connected to all ports.

Example

Set the PoE power supply mode to the backup mode.

```
<HUAWEI> system-view
[HUAWEI] poe-power backup-mode 1
```


3.6.28 poe single-class enable

Function

The **poe single-class enable** command configures the single-class power supply mode for an interface.

The **undo poe single-class enable** command restores the standard hierarchical power supply mode for an interface.

By default, an interface works in standard hierarchical power supply mode.

NOTE

Format

poe single-class enable

undo poe single-class enable

Parameters

None

Views

Interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

By default, a PoE interface works in standard hierarchical power supply mode. If PoE interfaces provide power to non-standard PDs in standard hierarchical power supply mode, these PDs cannot initiate power requests using LLDP or CDP and can only obtain a low power. As a result, these PDs cannot work normally. To address this issue, run the **poe single-class enable** command to configure the single-class power supply mode for PoE interfaces. These non-standard PDs can then initiate power requests and obtain the standard power supply to work normally.

Precautions

- If a standard PD is connected to the interface, this PD may be unable to work normally after the **poe single-class enable** command is run.
- On the S5720-16X-PWH-LI-AC, S5720-28X-PWH-LI-AC, S5720I-SI, S2730S-S, S5735-L-I, S5735-L1, S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5735-S, S500, S5735-S-I, S5735S-H, S5736-S, S5731-H, S5731-S, S5731S-S, and S5732-H, the **poe af-inrush enable** and **poe single-class enable** commands are mutually exclusive and cannot be configured on the same interface.

Example

Configure the single-class power supply mode for GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] poe single-class enable
```

3.6.29 reset poe slot

Function

The **reset poe slot** command resets the PoE chip in a specified slot.

NOTE

Only the S5720-LI, S5731-H, S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5720S-LI, S5735-S-I, S500, and S5735-S support this command.

Format

reset poe { **all chips** | **chip** *chip-id* } **slot** *slot-id*

Parameters

Parameter	Description	Value
all chips	Specifies all PoE chips.	-
chip *chip-id*	Specifies a chip ID.	The value must be set according to the device configuration.
slot-id	Specifies a slot ID.	The value must be set according to the device configuration.

Views

All views

Default Level

3: Management level

Usage Guidelines

If one or multiple PoE chips of a PSE are suspended, the port connected to a PD cannot detect the suspension and fails power the PD. In this case, you can run the **reset poe** { **all chips** | **chip** *chip-id* } **slot** *slot-id* command to reset the PoE chip.

Example

Reset PoE chip 0 in slot 1.


```
<HUAWEI> reset poe chip 0 slot 1
Warning: This command will cause power cycling for the PD connected to port 1,2,3,4. Continue? [Y/N]:y
```

3.7 Monitoring Interface Configuration Commands

3.7.1 Command Support

Only the following switch models support monitoring interfaces:

S5720I-SI (excluding the S5720I-6X-PWH-SI-AC and S5720I-10X-PWH-SI-AC), S5735-S-I

3.7.2 display monitor input

Function

The **display monitor input** command displays the status of an input line connected to a monitoring interface.

NOTE

Only the S5735-S-I supports this command.

Format

display monitor input { *line-id* | **all** } [**slot** *slot-id*]

Parameters

Parameter	Description	Value
line-id	Displays the status of the specified input line.	The value is an integer that ranges from 1 to 2.
all	Displays the status of all input lines.	-
slot *slot-id*	Specifies the stack ID if stacking is configured.	The value is determined based on the device configuration.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display monitor input** command to check the status of an input line connected to a monitoring interface, including the name, the normal level,

and the current status of the input line, and whether the monitoring function is enabled.

Example

Display the current status of all input lines.

```
<HUAWEI> display monitor input all

-------------------------------------------------------------------------------
LineID  LineName                  Enable  NormalStatus  CurrentStatus
-------------------------------------------------------------------------------
1       Input1                    enable  low-level     abnormal
2       Input2                    enable  high-level    normal
-------------------------------------------------------------------------------
```

Table 3-130 Description of the display monitor input command output

Item	Description
LineID	ID of the input line connected to a monitoring interface.
LineName	Name of the input line connected to a monitoring interface. To set the name, run the **monitor input** command.
Enable	Whether an input line connected to a monitoring interface is enabled. To set the parameter, run the **monitor input enable** command.
NormalStatus	Normal level of an input line connected to a monitoring interface: ● low-level: The normal level is low level. ● high-level: The normal level is high level. To set the normal level, run the **monitor input** command.
CurrentStatus	Current status of an input line connected to a monitoring interface: ● normal: The input line is in normal state. ● abnormal: The input line is abnormal state.

3.7.3 display monitor output

Function

The **display monitor output** command displays the status of an output line connected to a monitoring interface.

NOTE

Only the S5735-S-I supports this command.

Format

display monitor output { *line-id* | **all** }

Parameters

Parameter	Description	Value
line-id	Displays the status of a specified output line.	The value is 1.
all	Displays the status of all output lines.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After running the **monitor output enable** or **undo monitor output enable** command, you can run the **display monitor output** command to check the status of an output line connected to a monitoring interface, including line ID, the initial status of the monitoring function on the output line, and the current status of the monitoring function on the output line. If the initial status of the monitoring function on the output line is the same as the current status, the maintenance compartment door is closed. If they are inconsistent, the maintenance compartment door is opened.

Example

Display the status of all output lines.

```
<HUAWEI> display monitor output all
-----------------------------------
LineID  Config  Current Keeptime(s)
-----------------------------------
1       enable  enable  3
-----------------------------------
```

Table 3-131 Description of the **display monitor output** command output

Item	Description
LineID	ID of the output line connected to a monitoring interface.

Item	Description
Config	Initial status of the monitoring function on the output line. • enable: The **monitor output enable** command is run. • disable: The **undo monitor output enable** command is run.
Current	Current status of the monitoring function on the output line. If the value of this field is the same as that of **Config**, the maintenance compartment door is closed. If they are inconsistent, the maintenance compartment door is opened.
Keeptime(s)	Hold time of the signals indicating the maintenance compartment door is open or closed when the monitoring function on the output line connecting to a monitoring interface is enabled. The unit is second.

3.7.4 monitor input

Function

The **monitor input** command configures the name and normal level of the input lines connected to a monitoring interface.

The **undo monitor input** command restores the name and normal level of the input lines connected to a monitoring interface to default value.

By default, the name of a monitored input line is **Input1** or **Input2**. The normal level is **low-level**.

NOTE

Only the S5735-S-I supports this command.

Format

monitor input *line-id* **name** *line-name* **normal-state** { **low-level** | **high-level** } [**slot** *slot-id*]

undo monitor input *line-id* [**slot** *slot-id*]

Parameters

Parameter	Description	Value
line-id	Specifies the ID of an input line.	The value is an integer that ranges from 1 to 2.
name *line-name*	Specifies the name of an input line.	The name is a string of 1 to 31 case-sensitive characters without spaces.
normal-state { **low-level** | **high-level** }	Specifies the normal level of input lines connected to a monitoring interface. • **low-level**: indicates that the normal level is low level. • **high-level**: indicates that the normal level is high level.	-
slot *slot-id*	Specifies the stack ID if stacking is configured.	The value is determined based on the device configuration.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

You can run the **monitor input** command to configure the name and normal level of the input lines connected to a monitoring interface. When the level of the input line changes, the device generates an alarm.

Example

Configure the name of input line 1 as line1 and normal level as **high-level**.

```
<HUAWEI> system-view
[HUAWEI] monitor input 1 name line1 normal-state high-level
```

3.7.5 monitor input enable

Function

The **monitor input enable** command enables the monitoring function on an input line.

The undo monitor input enable command disables the monitoring function on an input line.

By default, the monitoring function on an input line is disabled.

NOTE

Only the S5735-S-I supports this command.

Format

monitor input *line-id* **enable** [**slot** *slot-id*]

undo monitor input *line-id* **enable** [**slot** *slot-id*]

Parameters

Parameter	Description	Value
line-id	Specifies the ID of an input line.	The value is an integer that ranges from 1 to 2.
slot *slot-id*	Specifies the stack ID if stacking is configured.	The value is determined based on the device configuration.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

You can run the **monitor input enable** command to enable the monitoring function on an input line so that you can monitor the application environment of the device.

Example

Enable the monitoring function on input line 1.

```
<HUAWEI> system-view
[HUAWEI] monitor input 1 enable
```

3.7.6 monitor output enable

Function

The **monitor output enable** command configures the initial status of the monitoring function on an output line connected to a monitoring interface to enabled.

The **undo monitor output enable** command configures the initial status of the monitoring function on an output line connected to a monitoring interface to disabled.

By default, the initial status of the monitoring function on an output line is not configured.

NOTE

Only the S5735-S-I supports this command.

Format

monitor output *line-id* **enable slot** *slot-id*

undo monitor output *line-id* **enable slot** *slot-id*

Parameters

Parameter	Description	Value
line-id	Specifies the ID of an output line.	The value is 1.
slot *slot-id*	Specifies the slot ID.	The value must be set according to the device configuration.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

After the **monitor output enable** command is run, the initial status of the monitoring function on an output line (DOUT status for short) is configured to enabled. If the maintenance compartment door is opened, the DOUT status changes to disabled. If the maintenance compartment door is closed, the DOUT status changes to enabled. You can monitor whether the maintenance compartment door is opened based on the DOUT status.

Similarly, after the **undo monitor output enable** command is run, the initial DOUT status is configured to disabled. If the maintenance compartment door is opened, the DOUT status changes to enabled. If the maintenance compartment door is closed, the DOUT status changes to disabled.

Example

Configure the initial status of the monitoring function on output line 1 to enabled.


```
<HUAWEI> system-view
[HUAWEI] monitor output 1 enable slot 0
```

3.7.7 monitor output keeptime

Function

The **monitor output keeptime** command sets the hold time of the signals indicating the maintenance compartment door on a device is open or closed when the monitoring function on the output line connecting to a monitoring interface is enabled.

The **undo monitor output keeptime** command restores the default setting.

By default, the hold time of the signals indicating the maintenance compartment door on a device is open or closed is 3 seconds.

NOTE

Only the S5735-S-I supports this command.

Format

monitor output keeptime *time* **slot** *slot-id*

undo monitor output keeptime slot *slot-id*

Parameters

Parameter	Description	Value
time	Specifies the hold time.	The value is an integer ranging from 1 to 3600, in seconds.
slot *slot-id*	Specifies the slot ID.	The value must be set according to the device configuration.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

By default, the hold time of the signals indicating the maintenance compartment door on a device is open or closed is three seconds. That is, a camera keeps monitoring the device maintenance compartment door for 3 seconds and then turns to another direction. You can run the **monitor output keeptime** command to change the hold time based on the actual situation of the camera.

Example

Set the hold time to 10 seconds.

```
<HUAWEI> system-view
[HUAWEI] monitor output keeptime 10 slot 0
```

3.8 OPS Configuration Commands

3.8.1 Command Support

Commands provided in this section and all the parameters in the commands are supported by all switch models (except the S5731-L and S5731S-L), unless otherwise specified. For details, see specific commands.

3.8.2 assistant scheduler suspend

Function

The **assistant scheduler suspend** command disables the OPS maintenance assistant function.

The **undo assistant scheduler suspend** command enables the OPS maintenance assistant function.

By default, the OPS maintenance assistant function is enabled.

Format

assistant scheduler suspend

undo assistant scheduler suspend

Parameters

None

Views

OPS view

Default Level

3: Management level

Usage Guidelines

If the OPS maintenance assistant function is no longer needed, the **assistant scheduler suspend** command applies to the following scenarios:

- Before deleting configured Python script assistants one by one, you can run this command to disable the OPS maintenance assistant function to prevent the assistants from running.

- During system maintenance, you can run this command to disable the OPS maintenance assistant function temporarily.

After you run the **assistant scheduler suspend** command to disable the OPS maintenance assistant function, none of Python script assistants will run again.

Example

Disable the OPS maintenance assistant function.

```
<HUAWEI> system-view
[HUAWEI] ops
[HUAWEI-ops] assistant scheduler suspend
```

3.8.3 display ops assistant

Function

The **display ops assistant** command displays information about Python script assistants.

Format

display ops assistant { **current** [**verbose**] | **history** } [**name** *assistant-name*]

Parameters

Parameter	Description	Value
current	Displays brief information about the current status of Python script assistants.	-
verbose	Displays detailed information about the current status of Python script assistants.	-
history	Displays historical operation records of Python script assistants.	-
name *assistant-name*	Specifies the name of a Python script assistant, namely, a Python script name for a script assistant.	The value must be the name of a script file for which the script assistant has been configured.

Views

All views

Default Level

3: Management level

Usage Guidelines

You can use this command to check the current status and historical operation record of a Python script assistant, including the Python script assistant name, running status, and execution result. The command can display a maximum of 100 latest Python script assistant records.

Example

Display brief information about the current status of Python script assistants.

```
<HUAWEI> display ops assistant current
-------------------------------------------------------
Assistant                State          Condition
-------------------------------------------------------
subscribe_cli_sync_1.py      ready          cli
user-correlat-10.py          ready          multi
-------------------------------------------------------
```

Table 3-132 Description of the **display ops assistant current** command output

Item	Description
Assistant	Name of a Python script assistant.
State	Current status of the Python script assistant. • ready: The Python script assistant is waiting to be triggered. • pending: The Python script assistant is waiting to run. • waiting: A resident script is waiting to be triggered the second time. • running: The Python script assistant is running. • shutdown: The Python script assistant stops. • suspend: The OPS maintenance assistant function is disabled.

Item	Description
Condition	Triggering condition for a Python script assistant. ● cli: command line event ● device: stack status change event ● iclog: log event ● ifm: interface statistics collection event event ● lldp: LLDP neighbor change event ● multi: complex event ● timer: timer event ● trap: trap event ● URM: routing event

Display detailed information about the current status of Python script assistants.

```
<HUAWEI> display ops assistant current verbose
Assistant information
  Name                    :user-correlat-10.py
  State                   :ready
Running statistics
  Running times             :0
  Queue size/(free)         :5/(5)
  Skip for queue full       :0
  Skip for delay            :0
  Skip for suppression      :0
Condition information
  Condition tag             :cli1
    Condition type          :multi
    Threshold               :1
    Period (s)              :0
    Hits in period          :0
  Condition tag             :cli2
    Condition type          :multi
    Threshold               :1
    Period (s)              :0
    Hits in period          :0
  Condition tag             :cli3
    Condition type          :multi
    Threshold               :1
    Period (s)              :0
    Hits in period          :0
  Condition tag             :cli4
    Condition type          :multi
    Threshold               :1
    Period (s)              :0
    Hits in period          :0
  Correlate expression      :((cli1 andnot cli2) and (cli3 andnot cli4))
  Trigger control
    Threshold               :1
    Period (s)              :30
    Delay (s)               :0
    Suppress max            :0
    Hits in period          :0
```


Table 3-133 Description of the **display ops assistant current verbose** command output

Item	Description
Assistant information	Information about a Python script assistant.
Name	Name of a Python script assistant.
State	Current status of a Python script assistant. • ready: The Python script assistant is waiting to be triggered. • pending: The Python script assistant is waiting to run. • waiting: A resident script is waiting to be triggered the second time. • running: The Python script assistant is running. • shutdown: The Python script assistant stops. • suspend: The OPS maintenance assistant function is disabled.
Running statistics	Detailed running information about a Python script assistant.
Running times	Number of running times.
Queue size/(free)	Number of buffered Python script assistants. If the number of buffered Python script assistants reaches the maximum value, excessive assistants will be discarded.
Skip for queue full	Number of tasks discarded because the queue is full.
Skip for delay	Number of tasks discarded within the delay.
Skip for suppression	Number of times the triggering of the assistant is suppressed.
Condition information	Condition information about a Python script assistant. The **Condition information** field is displayed only for a complex event script.
Condition tag	Condition name.
Condition type	Type of triggering condition. The value is **multi**.

Item	Description
Threshold	Maximum number of times that tasks are executed. The default value is 1.
Period (s)	Detection period, in seconds. The default value is 30.
Hits in period	Number of times the triggering condition is met in the detection period.
Correlate expression	Condition combination mode.
Trigger control	Trigger control.
Delay (s)	Delay in triggering a working task. The default value is 0 seconds.
Suppress max	Maximum number of times working tasks are triggered within the delay. The default value is 0, indicating that working tasks will not be suppressed.

Display historical operation records of Python script assistants.

```
<HUAWEI> display ops assistant history
Assistant history information
  Name                    :subscribe_cli_sync_1.py
  Running information
    Trigger condition       :cli
    Trigger event name      :cli1
    Trigger time            :2017-03-25 19:48:51
    Execute start time      :2017-03-25 19:48:51
    Execute end time        :2017-03-25 19:48:53
    Execute result          :normal
```

Table 3-134 Description of the **display ops assistant history** command output

Item	Description
Assistant history information	Historical information about a Python script assistant.
Name	Name of a Python script assistant.
Running information	Running information about a Python script assistant.

Item	Description
Trigger condition	Triggering condition for a Python script assistant. • cli: command line event • device: stack status change event • iclog: log event • ifm: interface statistics collection event event • lldp: LLDP neighbor change event • multi: complex event • timer: timer event • trap: trap event • URM: routing event
Trigger event name	Trigger event name for a Python script assistant.
Trigger time	Triggering time of a Python script assistant.
Execute start time	Execution time of a Python script assistant.
Execute end time	End time of a Python script assistant.
Execute result	Execution result of a Python script assistant. • normal: The script assistant ends normally. • abnormal: An exception occurs in the script. • userCancel: A user stops the script. • duplicate: The script file name conflicts with the database file name. • os: The system kills the script process due to a script exception.

3.8.4 display ops environment

Function

The **display ops environment** command displays information about user-defined environment variables.

Format

display ops environment

Parameters

None

Views

All views

Default Level

3: Management level

Usage Guidelines

You can run the **display ops environment** command to check information about user-defined environment variables after user-defined environment variables are configured using the **environment** command.

Example

Display user-defined environment variables.

```
<HUAWEI> display ops environment
No.  Name                    Value
1    user                    admin
```

Table 3-135 Description of the **display ops environment** command output

Item	Description
No.	User-defined environment variable number. The value ranges from 1 to 100.
Name	Name of a user-defined environment variable. To configure this parameter, run the **environment** command.
Value	Value of a user-defined environment variable. To configure this parameter, run the **environment** command.

3.8.5 display ops error

Function

The **display ops error** command displays script execution errors.

Format

display ops error [**name** *assistant-name*]

Parameters

Parameter	Description	Value
name *assistant-name*	Specifies the name of a Python script assistant, namely, a Python script name for a script assistant.	The value must be the name of a script file for which the script assistant has been configured.

Views

All views

Default Level

3: Management level

Usage Guidelines

You can run this command to view execution errors of all scripts or a specified script. According to the errors in the command output, you can modify the script.

Example

Display execution errors of all scripts.

```
<HUAWEI> display ops error
---------------------------------------------------------------------------
test12.py:
Traceback (most recent call last):
  File ".lib/frame.py", line 114, in <module>
    ret = m.ops_execute(ops)
  File "flash:$_user/test12.py", line 7, in ops_execute
    status, err_context = ops.context.save(varName, value)
NameError: global name 'varName' is not defined

---------------------------------------------------------------------------
test13.py:
Traceback (most recent call last):
  File ".lib/frame.py", line 114, in <module>
    ret = m.ops_execute(ops)
  File "flash:$_user/test13.py", line 6, in ops_execute
    status, err_log = ops.syslog("Syslog: Hello, World..", ops.CRITICAL, "syslog
")
```



```
AttributeError: 'module' object has no attribute 'syslog'

------------------------------------------------------------------------------
```

Table 3-136 Description of the **display ops error** command output

Item	Description
test12.py	Python script file name.
Traceback (most recent call last)	Last call error.
File ".lib/frame.py", line 114, in <module>	Stack where an error occurs.
File "flash:$_user/test12.py", line 7, in ops_execute	Information about location where an error occurs, including the Python script name, number of line, and phase when the error occurs.
status, err_context = ops.context.save(varName, value)	Invalid contents.
NameError	A variable error. The system is attempting to access a variable that is not declared.
AttributeError	An attribute error. The system is attempting to access an unknown object attribute.

3.8.6 display ops system-script

Function

The **display ops system-script** command displays system built-in OPS scripts.

Format

display ops system-script

Parameters

None

Views

All views

Default Level

3: Management level

Usage Guidelines

Usage Scenario

When associating OIDS with OPS, you need to use OPS scripts to subscribe to OIDS events. The device provides built-in OPS scripts, which removing the need to make scripts or download scripts from websites and import the scripts to the device. To view system built-in OPS scripts, run the **display ops system-script** command.

Precautions

The system built-in OPS scripts are not installed by default.

Example

Display system built-in OPS scripts.

```
<HUAWEI> display ops system-script
ScriptName                Description
------------------------------------------------------------------------------
oids.py                     The OIDS sample script describes the subscriptio
                          n process. The execution result of the script ha
                          s been recorded to OIDS. You can refer to this s
                          cript to implement the OIDS script process.
```

Table 3-137 Description of the **display ops system-script** command output

Item	Description
ScriptName	Name of a script.
Description	Description of the script.

3.8.7 environment

Function

The **environment** command configures a user-defined environment variable.

The **undo environment** command deletes a user-defined environment variable.

By default, no user-defined environment variable is configured.

Format

environment *variable-name variable-value*

undo environment *variable-name*

Parameters

Parameter	Description	Value
variable-name	Specifies the name of a user-defined environment variable.	The value is a string of 1 to 31 case-sensitive characters without spaces. It starts with a letter and contains only letters, digits, and underscores (_).
variable-value	Specifies the value of a user-defined environment variable.	The value is a string of 1 to 64 case-sensitive characters without spaces. If the string is enclosed in double quotation marks (""), the string can contain spaces.

Views

OPS view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

An environment variable consists of a name and a value. In a Python script, you can input an environment variable name in the location where a parameter needs to be input to indicate that an environment variable value needs to be referenced. When the system is running a Python script, it replaces an environment variable name with an environment variable value. To change the value, you can directly change it on the device without having to change and install the Python script. You can define and use user-defined environment variables to simplify the configuration and improve flexibility and feasibility of the Python script.

Precautions

If *variable-name* is specified multiple times, the system will prompt that the configured user-defined environment variable already exists. You can choose whether to overwrite the existing variable value. After overwriting the existing variable value, you need to run the **undo script-assistant python** command to delete the Python script assistant that uses the environment variable and then run the **script-assistant python** command to re-configure the Python script assistant.

A maximum of 100 environment variables can be configured on the device.

To check configured user-defined environment variables, run the **display ops environment** command.

Example

Set the value of the user-defined environment variable **user** to **admin**.

```
<HUAWEI> system-view
[HUAWEI] ops
[HUAWEI-ops] environment user admin
```

3.8.8 ops

Function

The **ops** command displays the OPS view.

Format

ops

Parameters

None

Views

System view

Default Level

3: Management level

Usage Guidelines

You can configure the Python script assistant in the OPS view.

Example

Display the OPS view.

```
<HUAWEI> system-view
[HUAWEI] ops
[HUAWEI-ops]
```

3.8.9 ops abort

Function

The **ops abort** command stops all OPS Python scripts.

Format

ops abort

Parameters

None

Views

All views

Default Level

3: Management level

Usage Guidelines

Usage Scenario

If commands cannot be entered on the switch due to OPS Python script exceptions, run the **ops abort** command to stop all OPS Python scripts to make the switch work properly.

Prerequisites

Running the **ops abort** command on the master switch will not be captured by the CLI event subscription API (ops.cli.subscribe), but running this command on the standby switch will be captured by this API.

Follow-up Procedure

To restore the OPS function, perform the following operations:

1. Run the **system-view** command to enter the system view.
2. Run the **ops** command to enter the OPS view.
3. Run the **undo script-assistant python** *script-name* command to delete the assistant of the abnormal Python script.
4. Run the **return** command to return to the user view.
5. Run the **ops uninstall file** *script-name* command to uninstall the abnormal Python script.
6. Run the **system-view** command to enter the system view.
7. Run the **ops** command to enter the OPS view.
8. Run the **undo assistant scheduler suspend** command to enable the OPS assistant to restore the OPS function.

Example

Stop all OPS Python scripts.

```
<HUAWEI> ops abort
```

3.8.10 ops install file

Function

The **ops install file** command installs a Python script.

Format

ops install file *file-name* [**destination** *directory*]

Parameters

Parameter	Description	Value
file-name	Specifies the directory and file name of the Python script to be installed. • To install a Python script stored in the root directory of the device, you can directly specify the file name of the script. • To install a Python script that is stored a non-root directory, you need to specify both the directory and file name of the script.	The value is a string of 4 to 64 case-insensitive characters. Spaces and special characters |, ;, &, $, >, <, `, \, !, \n, and \0 are not allowed. The file name extension of a Python script file is .py.

Parameter	Description	Value
		NOTE *file-name* cannot be set to the name of a built-in Python script file, including ConfigParser.py, copy_reg.py, locale.py, sre.py, Queue.py, decimal.py, macurl2path.py, sre_compile.py, StringIO.py, dis.py, modulefinder.py, sre_constants.py, UserDict.py, dummy_thread.py, ntpath.py, sre_parse.py, UserList.py, dummy_threading.py, nturl2path.py, stat.py, UserString.py, filecmp.py, numbers.py, string.py, __future__.py, fileinput.py, opcode.py, stringold.py, _abcoll.py, fnmatch.py, os.py, struct.py, _pyio.py, formatter.py, os2emxpath.py, subprocess.py, _strptime.py, fractions.py, pickle.py, sysconfig.py, _threading_local.py, functools.py, pkgutil.py, textwrap.py, _weakrefset.py, genericpath.py, platform.py, threading.py, abc.py, getopt.py, posixpath.py, token.py, argparse.py, getpass.py, pprint.py, tokenize.py, atexit.py, gettext.py, re.py, trace.py, base64.py, glob.py, repr.py, traceback.py, bisect.py, heapq.py, runpy.py, types.py, calendar.py, imputil.py, sched.py, user.py, codecs.py, inspect.py, sets.py, warnings.py, collections.py, io.py, shutil.py, weakref.py, contextlib.py, keyword.py, site.py, xmllib.py, copy.py, linecache.py, socket.py, _cli.py, _device.py, _frame.py, _route.py, _timer.py, _common.py, _environment.py, _iclog.py, _snmp.py, _trap.py, _context.py, _farg.py, _lldp.py, _terminal.py, and ops.py.

Parameter	Description	Value
destination *directory*	Specifies the installation directory of a script.	The value is a string of 1 to 64 case-insensitive characters without any spaces. If this parameter is not specified, the script will be installed in $_user. If this parameter is specified, the script will be installed in $_user/*directory*. If the directory name does not exist, a directory will be created. **NOTE** The total length of *file-name* and the installation directory of the script cannot exceed 118. The total length refers to the storage path + $_user + directory name + file name. The installation directory of the script cannot be huawei_pys. The depth of the path specified by *directory* cannot exceed three levels.

Views

User view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

OPS allows you to run the scripts you make. A script can be executed after the script assistant is configured. Before configuring a script assistant, install the script.

To check information about the scripts installed in $_user, run the **dir (user view)** command.

Precautions

- Before installing a script, upload the script to the root directory of flash: on the device.

- Ensure that the device has sufficient storage space when the script is installed. Otherwise, the script fails to be installed.
- If the specified installation directory does not exist, a directory will be created. A maximum of seven levels of subdirectories can be created in $_user.
- The name of the script to be installed cannot be the same as an existing directory name on the device. After scripts are installed successfully, you cannot create a directory whose name is the same as that of an installed script.
- To install scripts in $_user, you can only run the **ops install file** command. The scripts installed in this directory will be automatically backed up to the standby switch when a stack is configured.
- To modify a script that has been installed, run the **ops uninstall file** command to uninstall the script and the **delete (user view)** command to delete the script file. After modifying the script, upload and reinstalling the script file.
- It is recommended that the total size of files installed in $_user be smaller than 100 MB. If the total size of files exceeds 100 MB, performance of data synchronization between the active and standby cards may deteriorate.

Example

Install the script file config.py in the flash: root directory to the default flash:/$_user.

```
<HUAWEI> ops install file config.py
```

Install the script file config.py in the flash: root directory to the specified flash:/$_user/user.

```
<HUAWEI> ops install file config.py destination user
```

Install the script file config.py in the flash:/admin directory to the default flash:/$_user.

```
<HUAWEI> ops install file admin/config.py
```

3.8.11 ops uninstall file

Function

The **ops uninstall file** command uninstalls a Python script.

Format

ops uninstall file *file-name*

Parameters

Parameter	Description	Value
file-name	Specifies the name of the script file to be uninstalled.	The value must be the name of a script file that has been installed. If a script in a specified installation directory *directory*/*file-name* needs to be deleted, *directory* specifies the installation directory of the script. **NOTE** The total length of *file-name* and the installation directory of the script cannot exceed 118. The total length refers to the storage path + $_user + directory name + file name.

Views

User view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

You can uninstall unnecessary scripts to release storage space on a device. If an installed script needs to be updated, uninstall it first, and reinstall it after the update.

Precautions

This command cannot uninstall a script for which a script assistant has been configured. To uninstall the script, delete the script assistant first.

If the script for which a script assistant has configured invokes another script, the called script can be uninstalled using this command. Therefore, it is recommended that you use one script to implement required functions.

Example

Uninstall the script file config.py in the default directory flash:/$_user.

```
<HUAWEI> ops uninstall file config.py
```


Uninstall the script file config.py in the specified directory flash:/$_user/user.

```
<HUAWEI> ops uninstall file user/config.py
```

3.8.12 script-assistant python

Function

The **script-assistant python** command configures a Python script assistant.

The **undo script-assistant python** command deletes a Python script assistant.

By default, no Python script assistant is configured.

Format

script-assistant python *script-name*

undo script-assistant python *script-name*

Parameters

Parameter	Description	Value
script-name	Specifies the name of a Python script assistant, namely, a Python script name for a script assistant.	The value must be the name of a script file that has been installed.

Parameter	Description	Value
		NOTE *script-name* cannot be set to the file name of a built-in Python script, including ConfigParser.py, copy_reg.py, locale.py, sre.py, Queue.py, decimal.py, macurl2path.py, sre_compile.py, StringIO.py, dis.py, modulefinder.py, sre_constants.py, UserDict.py, dummy_thread.py, ntpath.py, sre_parse.py, UserList.py, dummy_threading.py, nturl2path.py, stat.py, UserString.py, filecmp.py, numbers.py, string.py, __future__.py, fileinput.py, opcode.py, stringold.py, _abcoll.py, fnmatch.py, os.py, struct.py, _pyio.py, formatter.py, os2emxpath.py, subprocess.py, _strptime.py, fractions.py, pickle.py, sysconfig.py, _threading_local.py, functools.py, pkgutil.py, textwrap.py, _weakrefset.py, genericpath.py, platform.py, threading.py, abc.py, getopt.py, posixpath.py, token.py, argparse.py, getpass.py, pprint.py, tokenize.py, atexit.py, gettext.py, re.py, trace.py, base64.py, glob.py, repr.py, traceback.py, bisect.py, heapq.py, runpy.py, types.py, calendar.py, imputil.py, sched.py, user.py, codecs.py, inspect.py, sets.py, warnings.py, collections.py, io.py, shutil.py, weakref.py, contextlib.py, keyword.py, site.py, xmllib.py, copy.py, linecache.py, socket.py, _cli.py, _device.py, _frame.py, _route.py, _timer.py, _common.py, _environment.py, _iclog.py, _snmp.py, _trap.py, _context.py, _farg.py, _lldp.py, _terminal.py, and ops.py.

Views

OPS view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

As networks are developing rapidly, existing network devices provide only limited functions and predefined services, failing to meet the requirements for diversified services. You can run the script using OPS to implement customized functions.

The device supports a built-in Python script interpreter. You can run the **script-assistant python** command to run a Python script and register the events defined in the script.

Prerequisites

The script has been uploaded to the device and installed using the **ops install file** command in the user view.

Precautions

Only one assistant can be configured for a Python script. A maximum of 100 Python script assistants can be configured on the device.

The system does not check correctness of the Python script.

If you run the **undo script-assistant python** command to uninstall the script assistant, the corresponding Python script will be terminated.

Example

Configure a script assistant for the script config.py.

```
<HUAWEI> ops install file config.py
<HUAWEI> system-view
[HUAWEI] ops
[HUAWEI-ops] script-assistant python config.py
```

3.8.13 shutdown script-assistant

Function

The **shutdown script-assistant** command stops a Python script assistant.

The **undo shutdown script-assistant** command starts a Python script assistant.

By default, the Python script assistant is started.

Format

shutdown script-assistant *script-name*

undo shutdown script-assistant *script-name*

Parameters

Parameter	Description	Value
script-name	Specifies the name of a Python script assistant, namely, a Python script name for a script assistant.	The value must be the name of a script file for which the script assistant has been configured.

Views

OPS view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

To prevent a Python script of an assistant from running, run the **shutdown script-assistant** command to stop the Python script assistant.

Precautions

Stopping a running assistant interrupts the task of the assistant. Exercise caution when you perform this operation.

Example

Stop a script assistant for the script config.py.

```
<HUAWEI> system-view
[HUAWEI] ops
[HUAWEI-ops] shutdown script-assistant config.py
Info: Succeeded in stopping script assistant config.py.
```

3.9 Energy-saving Configuration Commands

3.9.1 Command Support

Commands provided in this section and all the parameters in the commands are supported by all switch models (except the S5731-L and S5731S-L), unless otherwise specified. For details, see specific commands.

3.9.2 als enable

Function

The **als enable** command enables ALS on an interface.

The **undo als enable** command disables ALS on an interface.

By default, ALS is disabled on an interface.

Format

als enable

undo als enable

Parameters

None

Views

Interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

The constraints on ALS are as follows:

- Only optical interfaces support ALS. Electrical interfaces and combo interface do not support ALS.
- When optical interfaces transmit services unidirectionally, they do not support ALS.
- When the copper cable, copper module, or GPON optical module is used on the optical port, the ALS function is not supported. In addition, after the copper cable or GPON optical module is inserted, all the ALS-related commands configured on this interface are cleared.
- When you run the display elabel command to view electronic label information of a port and the command output shows that the component vendor is FCBN410QB1C10-HW, this port does not support ALS.

Example

Enable ALS on GigabitEthernet0/0/1.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] als enable
```


3.9.3 als restart

Function

The **als restart** command manually restarts the laser of an interface.

Format

als restart

Parameters

None

Views

Interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can run this command to manually restart the laser of an optical module. After the optical link recovers, the laser is started after a certain interval if the restart mode is automatic restart. To start the laser immediately after the optical link recovers, set the restart mode of the laser to manual restart and run the **als restart** command. If this command is not executed, the laser automatically sends a pulse after receiving a pulse from the remote end.

Prerequisites

ALS has been enabled on the interface using the **als enable** command and the restart mode of the laser has been set to manual restart mode using the **als restart mode manual** command.

Precautions

This command cannot be executed on an interface if the interface has been added to an interface protection group and is in **Protect** state.

Example

Restart lasers on GigabitEthernet0/0/1 manually.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] als enable
[HUAWEI-GigabitEthernet0/0/1] als restart mode manual
[HUAWEI-GigabitEthernet0/0/1] als restart
```


3.9.4 als restart mode manual

Function

The **als restart mode manual** command sets the mode of restarting the laser of the optical module to manual.

The **undo als restart mode manual** command restores the mode of restarting the laser of the optical module to automatic.

By default, a laser works in automatic restart mode.

Format

als restart mode manual

undo als restart mode manual

Parameters

None

Views

Interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

The laser of an optical module works in automatic restart mode or manual restart mode.

- In automatic restart mode, the laser sends pulses at the interval set using the **als restart pulse-interval** command to detect whether the link is recovered. The pulse width is set through the **als restart pulse-width** command.
- In manual restart mode, you must manually start the laser using the **als restart** command so that the laser can send a pulse. The ALS pulse width is set using the **als restart pulse-width** command.

If the fiber link recovery is detected in time, you can use the manual restart mode so that the laser can send pulses immediately. Therefore, data communication can be recovered rapidly.

Example

Configure lasers on GigabitEthernet0/0/1 to work in manual restart mode.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] als restart mode manual
```


3.9.5 als restart pulse-interval

Function

The **als restart pulse-interval** command sets the ALS pulse interval for the laser of an optical module.

The **undo als restart pulse-interval** command restores the default ALS pulse interval of the laser of an optical module.

By default, the ALS pulse interval of the laser is 100s.

Format

als restart pulse-interval *pulse-interval*

undo als restart pulse-interval

Parameters

Parameter	Description	Value
pulse-interval	Specifies the ALS pulse interval of the laser.	The value is an integer that ranges from 100 to 20000, in seconds.

Views

Interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

In automatic restart mode, the ALS pulse interval affects the frequency of detecting the LOS on the interface. A long ALS pulse interval is beneficial for energy saving, but the fiber link recovery cannot be detected in a timely manner. In contrary, a short ALS pulse interval wastes power but the fiber link recovery can be detected immediately.

Example

Set the ALS pulse interval of lasers on GigabitEthernet0/0/1 to 150s.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] als restart pulse-interval 150
```


3.9.6 als restart pulse-width

Function

The **als restart pulse-width** command sets the ALS pulse width for the laser of an optical module.

The **undo als restart pulse-width** command restores the default ALS pulse width for the laser of an optical module.

By default, the ALS pulse width of the laser is 2s.

Format

als restart pulse-width *pulse-width*

undo als restart pulse-width

Parameters

Parameter	Description	Value
pulse-width	Specifies the ALS pulse width of the laser.	The value is an integer that ranges from 2 to 200, in seconds.

Views

Interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

The ALS pulse width refers to the period between rising edges of pulses. A short ALS pulse width is beneficial for energy saving, but the fiber link recovery cannot be detected immediately. In contrary, a long ALS pulse width consumes more power but the fiber link recovery can be detected immediately.

Example

Set the ALS pulse width on GigabitEthernet0/0/1 to 3s.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] als restart pulse-width 3
```

3.9.7 display als configuration

Function

The **display als configuration** command displays ALS configuration.

Format

display als configuration slot *slot-id*

display als configuration interface *interface-type interface-number*

Parameters

Parameter	Description	Value
slot *slot-id*	Displays ALS configuration in a slot with a specified slot ID.	The value depends on the device configuration.
interface *interface-type interface-number*	Displays ALS configuration on a specified interface. • *interface-type* specifies the interface type. • *interface-number* specifies the interface number.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

If an optical interface connects to a high-speed cable, this command does not have command output.

Example

Display ALS configuration on GigabitEthernet0/0/1.

```
<HUAWEI> display als configuration interface gigabitethernet 0/0/1
--------------------------------------------------------------------------------
Interface              ALS       Laser     Restart    Interval(s)   Width(s)
                     Status    Status    Mode
--------------------------------------------------------------------------------
GigabitEthernet0/0/1   Disable   On        Auto       100           2
--------------------------------------------------------------------------------
```

Table 3-138 Description of the **display als configuration** command output

Item	Description
Interface	Interface type and number.

Item	Description
ALS Status	Whether ALS is enabled. ● Enable: ALS is enabled. ● Disable: ALS is disabled. ALS is enabled using the **als enable** command.
Laser Status	Status of the laser on the interface. The value can be: ● Off: The laser is shut down. ● On: The laser is turned on. ● --: No optical module is present on the interface.
Restart Mode	ALS restart mode. ● Auto: automatic restart mode. ● Manual: manual restart mode. The ALS restart mode is set to manual using the **als restart mode manual** command.
Interval(s)	ALS pulse interval, expressed in seconds. The ALS pulse interval is set using the **als restart pulse-interval** command.
Width(s)	ALS pulse width, expressed in seconds. The ALS pulse width is set using the **als restart pulse-width** command.

3.9.8 display power manage cycle

Function

The **display power manage cycle** command displays the interval for updating power consumption data.

Format

display power manage cycle

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

The average power consumption of a device is the average power consumption within a period of time. You can use the **display power manage cycle** command to view the interval for calculating the average power consumption.

Example

Display the interval for updating power consumption data.

```
<HUAWEI> display power manage cycle
 3 : 1 hour
```

Table 3-139 Description of the display power manage cycle command output

Item	Description
3 (1 hour)	The interval for updating power consumption data is 1 hour. You can set the interval to the following values: ● 1 : 15 minutes ● 2 : 30 minutes ● 3 : 1 hour ● 4 : 1 day ● 5 : 1 week ● 6 : 1 month (30 days) To set the interval for updating power consumption data, use the **set power manage cycle** command.

3.9.9 display power manage mode

Function

The **display power manage mode** command displays the energy-saving mode of the device.

Format

display power manage mode

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display power manage mode** command to check the currently configured energy-saving mode of the device.

Example

Display the energy-saving mode of the device.

```
<HUAWEI> display power manage mode
2 (Standard mode)
```

Table 3-140 Description of the display power manage mode command output

Item	Description
2 (Standard mode)	Standard energy-saving mode. The device supports the following energy-saving modes: • 1. User-defined mode: user-defined energy-saving mode. • 2. Standard mode: standard energy-saving mode • 3. Basic mode: basic energy-saving mode • 4. Deep mode: depth energy-saving mode • 5. Standby mode. **NOTE** The device does not support the user-defined mode. Only the S5720-16X-PWH-LI supports the standby mode. You can set the energy-saving mode using the **set power manage mode** command.

3.9.10 display power manage power-information

Function

The **display power manage power-information** command displays the power consumption information of a device.

Format

display power manage power-information

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

The **display power manage power-information** command enables you to check the system power consumption information, including the accumulative power consumption, average power, real-time power, rated power, and power threshold of the device.

Example

Display the system power consumption information.

```
<HUAWEI> display power manage power-information
The information of net element power:
 ----------------------------------------------------
 The total power consumption (Joule) : 3702200060
 The average power consumption (mW)  : 67050
 The current power consumption (mW)  : 65750
 The inbound interface power (mW)    : 81750
 The rated power (mW)                : 229000
 The threshold of power (mW)         : 600000
 The typical power (mW)              : 126000
 ----------------------------------------------------
```

Table 3-141 Description of the display power manage power-information command output

Item	Description
The information of net element power	System power consumption information.

Item	Description
The total power consumption (Joule)	Accumulative power consumption, in Joule. This field displays NA for PoE-incapable models, including the SS1720GW-E, S1720GWR-E, S5720I-SI, S5720-LI, S5720S-LI, S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5735-S, S500, S5735S-S, and S5735-S-I. This field displays NA when the device uses the PDC180S12-CR, PDC260S12-DL, PAC60S12-AR or PAC150S12-R power module of which power information cannot be obtained. **NOTE** The accumulative power consumption is stored in the device memory and will not be lost when the device is powered off. When the device is running, power consumption is accumulated once every 15 minutes. The accumulated power consumption and accumulative power consumption in the memory are added and recorded in the memory once every 24 hours. If there is no accumulative power consumption in the memory, this field displays 0. If the device is powered off within 24 hours after starting, the power consumption accumulated within 24 hours is not added to the accumulative power consumption in the memory.
The average power consumption (mW)	The average power consumption of a device is the average power consumption within a period of time, including the PoE power, in mW. This field displays NA for PoE-incapable models, including the SS1720GW-E, S1720GWR-E, S5720I-SI, S5720-LI, S5720S-LI, S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5735-S, S500, S5735S-S, and S5735-S-I. This field displays NA when the device uses the PDC180S12-CR, PDC260S12-DL, PAC60S12-AR or PAC150S12-R power module of which power information cannot be obtained.
The current power consumption (mW)	The output power of the system, including the PoE power, in mW. This field displays NA for PoE-incapable models, including the SS1720GW-E, S1720GWR-E, S5720I-SI, S5720-LI, S5720S-LI, S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5735-S, S500, S5735S-S, and S5735-S-I. This field displays NA when the device uses the PDC180S12-CR, PDC260S12-DL, PAC60S12-AR or PAC150S12-R power module of which power information cannot be obtained.

Item	Description
The inbound interface power (mW)	The input power of the system, including the PoE power, in mW. This field displays NA for PoE-incapable models, including the SS1720GW-E, S1720GWR-E, S5720I-SI, S5720-LI, S5720S-LI, S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5735-S, S500, S5735S-S, and S5735-S-I. This field displays NA when the device uses the PDC180S12-CR, PDC260S12-DL, PAC60S12-AR or PAC150S12-R power module of which power information cannot be obtained.
The rated power (mW)	Rated power of the system, excluding the PoE power, in mW. For a stack, the value of this parameter indicates the maximum power consumption of the stack.
The threshold of power (mW)	Power threshold of the power supply unit, in mW. The value is the rated power of the power supply unit used on the device. ● When there are two power supply units on the device, they work in redundancy mode to supply power to the system. The supplied power is not the accumulated power of the two power supply units. When the rated power of both power supply units can be obtained, this field displays the smaller rated power. If the rated power of one power supply unit cannot be obtained, this field displays the obtained rated power. If the rated power of both power supply units cannot be obtained, this field displays the system rated power. ● If a built-in power supply is used, the value is the rated power of the system.
The typical power (mW)	Power of the device when 30% of the line rate is used, excluding the PoE power. The unit is mW.

3.9.11 display power manage sleep configuration

Function

The **display power manage sleep configuration** command displays device dormancy information.

NOTE

Only the S500, S5735-S, S5735-S-I, S5735S-S, S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5735S-H, and S5736-S series switches support the sleep mode.

Format

display power manage sleep configuration

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

The **display power manage sleep configuration** command shows device dormancy information, including the time range, period during which the awakening port status is detected continuously, awakening mode, and non-awakening ports.

Example

Display the device dormancy configuration.

```
<HUAWEI> display power manage sleep configuration
The device sleep function status: enable
The device sleep time-range: night-time
-------------------------------------------------
Current time is 16:19:45 5-14-2012 Monday

Time-range: night-time ( Inactive )
20:00 to 00:00 working-day
00:00 to 08:00 working-day
-------------------------------------------------
The awaken port state check interval (minutes): 20(default)
The configuration of non-awaken port:
-------------------------------------------------
 GigabitEthernet0/0/1     GigabitEthernet0/0/2
 GigabitEthernet0/0/3     GigabitEthernet0/0/4
 GigabitEthernet0/0/5     GigabitEthernet0/0/6
 GigabitEthernet0/0/7     GigabitEthernet0/0/8
 GigabitEthernet0/0/9     GigabitEthernet0/0/10
-------------------------------------------------
```


Table 3-142 Description of the display power manage sleep configuration command output

Item	Description
The device sleep function status	Device dormancy mode. • disable: The device dormancy function is disabled. That is, the device energy-saving mode configured using the **set power manage mode** command is not 4. • enable: The device dormancy function is enabled. That is, the device energy-saving mode configured using the **set power manage mode** command is 4.
The device sleep time-range	Dormancy time range name. If no dormancy time range is specified, the whole day takes effect by default. To set a dormancy time range, run the **sleep time-range** command.
Time-range	Dormancy time range. • If the field value contains (Inactive), the current time is not within the dormancy time range. • If the field value contains (Active), the current time is within the dormancy time range.
The awaken port state check interval (minutes)	Period during which the awakening port status is detected continuously. To set the period, run the **set power manage interval** command.
The configuration of non-awaken port	Configured non-awakening ports. To configure non-awakening ports, run the **set power manage non-awaken-port** command.

3.9.12 energy-efficient-ethernet enable

Function

The **energy-efficient-ethernet enable** command enables the Energy Efficient Ethernet (EEE) function on an electrical interface.

The **undo energy-efficient-ethernet enable** command disables the EEE function on an electrical interface.

By default, EEE is disabled on an electrical interface.

Format

energy-efficient-ethernet enable

undo energy-efficient-ethernet enable

Parameters

None

Views

GE interface view, port group view, MultiGE interface view, XGE interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The system provides power for each interface. Even though an interface is idle, it consumes the same power as working interfaces. The **energy-efficient-ethernet enable** command enables the system to reduce the power on an interface when the interface is idle and restore the power when the interface starts to transmit data. This reduces system power consumption.

Prerequisites

If an electrical interface works in non-auto negotiation mode, run the **negotiation auto** command to enable auto-negotiation.

Precautions

- The EEE function can be configured only on electrical interfaces (including combo electrical interfaces). Optical interfaces do not support the EEE function.
- If an electrical interface works at 10 Mbit/s after auto-negotiation, the EEE function does not take effect.
- The S5731-H, S5731-S (except S5731-S32ST4X-A, S5731-S32ST4X-D, S5731-S24N4X2Q-A, S5731-S24UN4X2Q, S5731-S8UM16UN2Q, and S5731-S32ST4X), S5731S-H, S5731S-S (except S5731S-S32ST4X-A, S5731S-S24N4X2Q-A1, S5731S-S24UN4X2Q-A, S5731S-S8UM16UN2Q-A, and S5731S-S32ST4X-A1), S6735-S, S6720-EI, and S6720S-EI do not support the EEE function.
- For the S5732-H48XUM2CC, S5732-H24UM2CC and S5732-H48UM2CC, MultiGE interfaces working at 2.5 Gbit/s or 5 Gbit/s do not support the EEE function.
- Enabling or disabling EEE on an interface will trigger re-negotiation. During the negotiation, the interface may change to Down state, which causes short service interruption. Therefore, determine whether the operation is allowed before you run this command.
- If auto-negotiation is disabled on an interface, the EEE configuration is automatically deleted.

Example

Enable the EEE function on electrical interface GE0/0/1.


```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] energy-efficient-ethernet enable
```

3.9.13 port-auto-sleep enable

Function

The **port-auto-sleep enable** command enables the port dormancy function on an Ethernet electrical port to save energy.

The **undo port-auto-sleep enable** command disables the port dormancy function on an Ethernet electrical port.

By default, the port dormancy function is disabled on an Ethernet electrical port.

Format

port-auto-sleep enable

undo port-auto-sleep enable

Parameters

None

Views

Interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

The **port-auto-sleep enable** command enables electrical port dormancy. If this function is enabled on a port, the port enters the energy-saving mode when no carrier wave signals are transmitted on the port. When carrier wave signals are transmitted on the port, the port exits the energy-saving mode. Port sleep does not affect functioning of the port.

NOTE

Currently, this command can be used on electrical interfaces (excluding MultiGE interfaces) and combo interfaces working as electrical interfaces.

The port sleeping function is enabled by default on the ES5D21X08T00 electrical sub-card supported by the S5731-H, and S5731S-H, and cannot be disabled.

Example

Enable the port dormancy function on GigabitEthernet0/0/1.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] port-auto-sleep enable
```

3.9.14 set power manage cycle

Function

The **set power manage cycle** command sets the interval for updating power consumption data.

The **undo set power manage cycle** command restores the default interval for updating power consumption data.

By default, the interval for updating power consumption data is 1 hour.

Format

set power manage cycle *cycle-id*

undo set power manage cycle

Parameters

Parameter	Description	Value
cycle-id	Sets the interval for updating power consumption data.	The value is an integer that ranges from 1 to 6. ● 1: 15 minutes ● 2: 30 minutes ● 3: 1 hour ● 4: 1 day ● 5: 1 week ● 6: 30 days

Views

System view

Default Level

3: Management level

Usage Guidelines

The average power consumption of a device is the average power consumption within a period of time. You can use the **set power manage cycle** command to set the interval for calculating the average power consumption. To obtain real-time power consumption, set a short interval.

Example

Set the interval for updating power consumption data to 15 minutes.


```
<HUAWEI> system-view
[HUAWEI] set power manage cycle 1
```

3.9.15 set power manage interval

Function

The **set power manage interval** command sets the period during which the awakening port status is probed continuously.

The **undo set power manage interval** command restores the default period during which the awakening port status is probed continuously.

By default, the period is 20 minutes.

NOTE

Only the S500, S5735-S, S5735-S-I, S5735S-S, S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5735S-H, and S5736-S series switches support the sleep mode.

Format

set power manage interval *interval-time*

undo set power manage interval

Parameters

Parameter	Description	Value
interval-time	Specifies the period during which the awakening port status is probed continuously.	The value is an integer ranging from 5 to 60, in minutes.

Views

System view

Default Level

3: Management level

Usage Guidelines

When the device does not enter the dormancy state in the specified time range, the device continuously probes the status of all awakening ports. The device enters the dormancy state when the device does not probe any awakening port in Up state within the default 20 minutes. Otherwise, the device continues to probe the awakening ports status.

If no time range is applied to the device, the device probes the status of all awakening ports all round the clock. By default, the device enters the dormancy

state when the device does not probe any awakening port in Up state within 20 minutes.

NOTE

In a stack, the **set power manage interval** command cannot set the period during which the awakening port status is detected continuously. However, you can use the **undo set power manage interval** command to delete the configuration in standalone mode.

Example

Set the period during which the awakening port status is probed continuously to 10 minutes.

```
<HUAWEI> system-view
[HUAWEI] set power manage interval 10
[HUAWEI] quit
<HUAWEI> save
```

3.9.16 set power manage mode

Function

The **set power manage mode** command sets the energy-saving mode of the device.

The **undo set power manage mode** command restores the default energy-saving mode of the device.

By default, the standard energy-saving mode is used.

Format

set power manage mode *mode-id*

undo set power manage mode

Parameters

Parameter	Description	Value
mode-id	Specifies the energy-saving mode of the device.	The value is an integer that ranges from 1 to 5: • 1: indicates the user-defined energy-saving mode. This mode is not supported currently. • 2: indicates the standard energy-saving mode. • 3: indicates the basic energy-saving mode. • 4: indicates the deep energy-saving mode. • 5: indicates the standby energy-saving mode. **NOTE** Only the S5720-16X-PWH-LI supports the standby energy-saving mode.

Views

System view

Default Level

3: Management level

Usage Guidelines

The **set power manage mode** command sets the energy-saving mode of the device.

The device can run in the following energy-saving modes:

- Standard mode

  Factory mode and default power saving mode.

- Basic mode

  Components not in use are shut down or switched to the sleep mode when no services are configured or users are not online.

- Deep mode

  Power consumption is dynamically adjusted for running services, and components not in use are shut down or switched to the sleep mode according to service requirements.

- Standby mode

  The device enters the low power consumption mode when it does not need to provide PoE power to PDs and shuts down all the interfaces except GE0/0/13 and GE0/0/14.

NOTE

- The ALS, EEE, and port dormancy functions are disabled in standard mode by default. However, the port dormancy function is enabled by default on the ES5D21X08T00 electrical sub-card supported by the S5731-H, and S5731S-H, and cannot be disabled.
- The ALS, EEE, and port dormancy functions are enabled by default in basic or deep mode.
- The deep mode adds the device dormancy function based on functions of the basic mode.
- Only the S5720-16X-PWH-LI supports the standby mode. The interfaces that have been shut down in standby mode cannot be enabled manually using a command. To enable these interfaces manually, ensure that the switch exits the standby mode.
- Before entering the standby mode, the system forcibly saves the configuration to the configuration file that is being used by the device.
- The configuration restoration function is not configured in the standby mode. That is, after the device restarts, the currently configured standby mode of an interface is automatically restored to the default standard mode.
- On the S5720-16X-PWH-LI XGE0/0/1 and XGE0/0/2, installing optical modules and configuring the standby mode are mutually exclusive. That is, the two interfaces cannot have the standby mode configured after they have optical modules installed. When they work in standby mode, installing optical modules into them will restore them to the default standard mode or may even restart the device.
- The minimum interval between configuring and disabling the standby mode is 15s.
- The standby mode cannot be configured in a stack.
- When the device is switched from the basic or deep mode to the standby mode, disabling the EEE function may cause interface flapping. Similarly, when the device is switched from the standby mode to the basic or deep mode, enabling the EEE function may cause interface flapping.

After the energy-saving mode is set to basic or deep mode, loopback test on interfaces is disabled. Therefore, before performing a loopback test, set the energy-saving mode to standard mode.

Example

Set the energy-saving mode of the device to basic mode.

```
<HUAWEI> system-view
[HUAWEI] set power manage mode 3
Warning: Performance of ALS, EEE, Auto sleep will be enabled, and the EEE function may lead to port flapping. Continue?[Y/N]:y
Info: It will take a few seconds. Please wait...
```

3.9.17 set power manage non-awaken-port

Function

The **set power manage non-awaken-port** command configures a port as a non-awakening port.

The **undo set power manage non-awaken-port** command restores a non-awakening port to be an awakening port.

By default, all ports are awakening ports.

NOTE

Only the S500, S5735-S, S5735-S-I, S5735S-S, S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5735S-H, and S5736-S series switches support the sleep mode.

Format

set power manage non-awaken-port interface { *interface-type interface-number1* [**to** *interface-type interface-number2*] } &<1-10>

undo set power manage non-awaken-port 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.	-

Views

System view

Default Level

3: Management level

Usage Guidelines

You can use the **set power manage non-awaken-port** command to configure some ports as non-awakening ports so that these ports do not affect device dormancy and awakening. This is because device dormancy and awakening depend on the awakening port status.

NOTE

In a stack, the **set power manage non-awaken-port** command cannot configure a port as a non-awakening port. However, you can use the **undo set power manage non-awaken-port** command to delete the configuration in standalone mode.

Example

Configure interfaces GigabitEthernet0/0/1 to GigabitEthernet0/0/5 as non-awakening interfaces.

```
<HUAWEI> system-view
[HUAWEI] set power manage non-awaken-port interface gigabitethernet 0/0/1 to gigabitethernet
0/0/5
Info: Succeeded in setting the configuration.
[HUAWEI] quit
<HUAWEI> save
```

3.9.18 sleep time-range

Function

The **sleep time-range** command applies a time range to the device in dormancy state.

The **undo sleep time-range** command deletes the time range.

By default, no time range is applied to the device.

NOTE

Only the S500, S5735-S, S5735-S-I, S5735S-S, S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5735S-H, and S5736-S series switches support the sleep mode.

Format

sleep time-range *timerange-name*

undo sleep time-range *timerange-name*

Parameters

Parameter	Description	Value
timerange-name	Specifies the name of a time range that applies to the device.	The value is a string of 1 to 32 case-sensitive characters without spaces and must start with an uppercase or lowercase.

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

A device on an enterprise network is not used at certain time. You can apply a time range to the device in dormancy mode to save power. When dormancy conditions are met, the device automatically enters the dormancy state during the time range. When the time range expires, the device is awakened.

When an awakening interface detects a user, the device in dormancy mode is awakened. User services on the device are not affected.

The device enters the sleeping mode when the following conditions are met:

- The device works in deep mode. By default, the standard energy-saving mode is used.
- A time range applies to the device in sleeping mode.
- During the period for continuously detecting awakening port status, the terminals (switches or PCs) connected to awakening ports are shut down.

  NOTE

  If the terminal is a PC, the device can enter the dormancy state only when the PC is shut down and its network adapter is powered off (this can be set in the power management module of BIOS).

The device is awakened when either of the following conditions is met:

- A user logs in to the device through the serial port and presses Ctrl+W.
- The terminals (switches or PCs) connected to awakening ports are started up.
- The sleeping time range expires (if a time range is configured).
- A user presses the mode switching button.

Prerequisites

- The energy-saving mode of the device has been set to deep mode using the **set power manage mode** command.
- A time range has been specified using the **time-range** command.

NOTE

In a stack, the **sleep time-range** command cannot apply a time range to the device in dormancy state. However, you can use the **undo sleep time-range** command to delete the configuration in standalone mode.

Example

Apply the time range 1:00 to 6:00 am to the device.

```
<HUAWEI> system-view
[HUAWEI] set power manage mode 4
[HUAWEI] time-range test 1:00 to 6:00 daily
[HUAWEI] sleep time-range test
[HUAWEI] quit
<HUAWEI> save
```

3.10 Information Center Configuration Commands

3.10.1 Command Support

Commands provided in this section and all the parameters in the commands are supported by all switch models (except the S5731-L and S5731S-L), unless otherwise specified. For details, see specific commands.

3.10.2 display buffer

Function

The **display buffer** command displays statistics about logs cached in the buffer.

Format

display buffer [*feature-name* [*buffer-name*]]

Parameters

Parameter	Description	Value
feature-name	Specifies the name of the buffer dedicated to caching logs of a specific feature.	-
buffer-name	Specifies the name of the buffer.	-

Views

All views

Default Level

3: Management level

Usage Guidelines

On the device, service modules generate logs and control the log volume. The information center processes the received logs.

When the number of logs that are generated within a specified period (T) exceeds the threshold, the service module, with the buffer mechanism, saves extra logs to the buffer and does not send them to the information center.

You can run the **display buffer** command to view statistics about log information in the buffer.

Example

Display statistics about logs cached in the buffer on the service module **L2IF**.

```
<HUAWEI> display buffer L2IF
Feature name : L2IF
Buffer number : 1
Buffer name : CALLBACKFAIL
  Buffer ID                 : 35
```



```
Max length of message        : 256
Max number of message        : 5
Time threshold(s)            : 3600
Store lastest message number : 0
Total receive number         : 76
Total process number         : 5
Max rate record              : 0 / 3600(s)
Max rate timestamp           : 0-00-00 00:00:00
```

Table 3-143 Description of the **display buffer** command output

Item	Description
Feature name	Feature name.
Buffer number	Buffer number.
Buffer name	Buffer name.
Buffer ID	Buffer ID.
Max length of message	Maximum length of a message.
Max number of message	Maximum number of messages.
Time threshold(s)	Time threshold.
Store lastest message number	Number of messages saved to non-volatile memory.
Total receive number	Total receive number
Total process number	Total process number
Max rate record	Maximum rate record.
Max rate timestamp	Maximum rate timestamp.

3.10.3 display channel

Function

The **display channel** command displays the channel configuration.

Format

display channel [*channel-number* | *channel-name*]

Parameters

Parameter	Description	Value
channel-number	Specifies the number of a channel.	The value is an integer that ranges from 0 to 9. That is, the system has 10 channels. Channels 0 to 5 have default names and the six channels map to six different output directions. **Table 3-144** shows the relationship between channels and output directions.
channel-name	Specifies the name of a channel.	The value is a string of 1 to 30 case-insensitive characters. The value consists of letters or numbers and must start with a letter.

Table 3-144 Relationship between channel and output directions

Channel Number	Default Channel Name	Output Direction	Description
0	console	console	Console that can receive logs, traps, and debugging messages.
1	monitor	monitor	VTY terminal that can receive logs, traps, and debugging messages, which facilitates remote maintenance.
2	loghost	loghost	Log host that can receive logs, traps, and debugging messages. By default, information is saved on the log host in file format for easy reference.
3	trapbuffer	trapbuffer	Trap buffer that can receive traps.
4	logbuffer	logbuffer	Log buffer that can receive logs.
5	snmpagent	snmpagent	SNMP agent that can receive traps.
6	channel6	Unspecified	Reserved. You can specify to which destination this channel can output information.
7	channel7	Unspecified	Reserved. You can specify to which destination this channel can output information.
8	channel8	Unspecified	Reserved. You can specify to which destination this channel can output information.

Channel Number	Default Channel Name	Output Direction	Description
9	channel9	Unspecified	Reserved. You can specify to which destination this channel can output information.

Views

All views

Default Level

3: Management level

Usage Guidelines

The **display channel** command displays the channel configuration.

When using this command, note the following points:

- When *channel-number* or *channel-name* is specified, the **display channel** command displays the specified channel that information passes through and information severity.
- When *channel-number* or *channel-name* is not specified, the **display channel** command displays all the channels that information passes through and information severity.

Example

Display the configuration of channel 0.

```
<HUAWEI> display channel 0
channel number:0, channel name:console
MODU_ID  NAME     ENABLE LOG_LEVEL     ENABLE TRAP_LEVEL    ENABLE DEBUG_LEVEL
ffff0000 default  Y      warning       Y      debugging     Y      debugging
```

Display the configuration of all channels.

```
<HUAWEI> display channel
channel number:0, channel name:console
MODU_ID  NAME     ENABLE LOG_LEVEL     ENABLE TRAP_LEVEL    ENABLE DEBUG_LEVEL
ffff0000 default  Y      warning       Y      debugging     Y      debugging

channel number:1, channel name:monitor
MODU_ID  NAME     ENABLE LOG_LEVEL     ENABLE TRAP_LEVEL    ENABLE DEBUG_LEVEL
ffff0000 default  Y      warning       Y      debugging     Y      debugging

channel number:2, channel name:loghost
MODU_ID  NAME     ENABLE LOG_LEVEL     ENABLE TRAP_LEVEL    ENABLE DEBUG_LEVEL
ffff0000 default  Y      informational Y      debugging     N      debugging

channel number:3, channel name:trapbuffer
MODU_ID  NAME     ENABLE LOG_LEVEL     ENABLE TRAP_LEVEL    ENABLE DEBUG_LEVEL
ffff0000 default  N      informational Y      debugging     N      debugging
```



```
channel number:4, channel name:logbuffer
MODU_ID  NAME     ENABLE LOG_LEVEL     ENABLE TRAP_LEVEL    ENABLE DEBUG_LEVEL
ffff0000 default  Y      warning       N      debugging     N      debugging

channel number:5, channel name:snmpagent
MODU_ID  NAME     ENABLE LOG_LEVEL     ENABLE TRAP_LEVEL    ENABLE DEBUG_LEVEL
ffff0000 default  N      debugging     Y      debugging     N      debugging

channel number:6, channel name:channel6
MODU_ID  NAME     ENABLE LOG_LEVEL     ENABLE TRAP_LEVEL    ENABLE DEBUG_LEVEL
ffff0000 default  Y      debugging     Y      debugging     N      debugging

channel number:7, channel name:channel7
MODU_ID  NAME     ENABLE LOG_LEVEL     ENABLE TRAP_LEVEL    ENABLE DEBUG_LEVEL
ffff0000 default  Y      debugging     Y      debugging     N      debugging

channel number:8, channel name:channel8
MODU_ID  NAME     ENABLE LOG_LEVEL     ENABLE TRAP_LEVEL    ENABLE DEBUG_LEVEL
ffff0000 default  Y      debugging     Y      debugging     N      debugging

channel number:9, channel name:channel9
MODU_ID  NAME     ENABLE LOG_LEVEL     ENABLE TRAP_LEVEL    ENABLE DEBUG_LEVEL
ffff0000 default  Y      debugging     Y      debugging     N      debugging
```

Table 3-145 Description of the display channel command output

Item	Description
channel number	Channel number, which ranges from 0 to 9.
channel name	Channel name. **Table 3-144** lists default channel names. To set the channel name, run the **info-center channel name** command.
MODU_ID	Module ID. The default value is ffff0000.
NAME	Module name. The default value is **default**. To set the module name, run the **info-center source channel** command.
ENABLE	Whether logs/traps/debugging messages are allowed to pass through a channel: • Y • N To specify the channel, run the **info-center source channel** command.

Item	Description
LOG_LEVEL/ TRAP_LEVEL/ DEBUG_LEVEL	Lowest severity of output logs/traps/debugging messages. The following severities are listed in descending order of priority: • emergencies • alert • critical • error • warning • notification • informational • debugging To set the lowest severity of output logs, run the **info-center source channel** command.

3.10.4 display debugging

Function

The **display debugging** command displays debugging messages allowed to be sent by the device.

Format

display debugging [**interface** *interface-type interface-number*] [*module-name*]

display debugging interface all

display debugging slot *slot-id* **vcpu** *vcpu-index*

NOTE

Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S support **vcpu** *vcpu-index* parameter.

Parameters

Parameter	Description	Value
interface *interface-type interface-number*	Specifies the interface type and number.	-
all	Display debugging information on all interfaces.	-

Parameter	Description	Value
module-name	Displays debugging messages sent by a specified module such as the DHCP module. If this parameter is not specified, all debugging messages allowed to be sent are displayed.	Enumerated type. The value depends on the registered module.
slot *slot-id*	Specifies a slot ID.	The value is an integer, and the value range depends on the device configuration.
vcpu *vcpu-index*	Specifies the virtual CPU number.	Specify the *vcpu-index* parameter based on the hardware configuration.

Views

All views

Default Level

3: Management level

Usage Guidelines

Usage Scenario

Using the **display debugging** command, you can display the enabled debugging. If no parameters are specified, the **display debugging** command displays global debugging information.

Debugging affects device performance. The **display debugging** command displays debugging messages allowed to be sent by the Switch.

Prerequisites

By default, sending debugging messages is prohibited. The debugging of a specified module has been enabled.

Example

Display debugging messages allowed to be sent by the Switch.

```
<HUAWEI> debugging acl4 all
<HUAWEI> display debugging
ACL4 event debugging switch is on
ACL4 packet debugging switch is on
```


Table 3-146 Description of the **display debugging** command output

Item	Description
ACL4 event debugging switch is on	Event debugging is enabled for the ACL4 module.
ACL4 packet debugging switch is on	Packet debugging is enabled for the ACL4 module.

3.10.5 display info-center

Function

The **display info-center** command displays the output configuration of the information center.

Format

display info-center

Parameters

None

Views

All views

Default Level

3: Management level

Usage Guidelines

You can run the **display info-center** command to display all information recorded in the information center.

When a module is specified, you can view all information about the module recorded in the information center.

Example

Display output configuration of the information center.

```
<HUAWEI> display info-center
Information Center:enabled
Log host:
       10.1.1.1, channel number 2, channel name loghost,
language English , host facility local7
Console:
```

```
      channel number : 0, channel name : console
Monitor:
      channel number : 1, channel name : monitor
SNMP Agent:
      channel number : 5, channel name : snmpagent
Log buffer:
      enabled,max buffer size 1024, current buffer size 512,
current messages 512, channel number : 4, channel name : logbuffer
dropped messages 0, overwritten messages 53
Trap buffer:
      enabled,max buffer size 1024, current buffer size 256,
current messages 256, channel number:3, channel name:trapbuffer
dropped messages 0, overwritten messages 6229
Information timestamp setting:
      log - date, trap - date, debug - date millisecond

 Sent messages = 270090, Received messages = 281030

 IO Reg messages = 2 IO Sent messages = 10940
```

Table 3-147 Description of the display info-center command output

Item	Description
Information Center	Information center status: • enabled • disabled To enable the information center, run the **info-center enable** command.
Log host	Log host configuration.
10.1.1.1	Log host IP address. To set the log host IP address, run the **info-center loghost** command.
channel number	Number of a channel used to output information. To set the number of a channel used to output information, run the **info-center channel** command.
channel name	Name of a channel used to output information. To set the name of a channel used to output information, run the **info-center channel name** command.
language	Language mode in which information is output to a log host. To set the language mode in which information is output to a log host, run the **info-center loghost** command.
host facility	Logging tool. To configure the logging tool, run the **info-center loghost** command.
Console	Console configuration.
Monitor	Remote terminal configuration.
SNMP Agent	SNMP agent configuration.

Item	Description
Log buffer	Log buffer configuration.
enabled	Whether the Switch is enabled to send logs/traps to the log/trap buffer. • enabled • disabled To enable the Switch to send logs/traps to the log/trap buffer, run the **info-center logbuffer** or **info-center trapbuffer** command.
max buffer size	Maximum number of logs/traps in the log/trap buffer.
current buffer size	Maximum number of logs/traps in the current log/trap buffer. To set the maximum number of logs/traps in the current log/trap buffer, run the **info-center logbuffer size** or **info-center trapbuffer size** command.
current messages	Number of messages recorded in the log/trap buffer.
dropped messages	Number of messages discarded by the log/trap buffer.
overwritten messages	Number of overwritten messages in the log/trap buffer.
Trap buffer	Trap buffer configuration.
Information timestamp setting	Timestamp format of logs, traps, and debugging messages: • boot: indicates that the timestamp is expressed in the format of relative time, a period of time since system start. • date: indicates the current system date and time. It is expressed in mm dd yyyy hh:mm:ss format. • short-date: indicates the short date. This timestamp differs from **date** is that the year is not displayed. • format-date: indicates that the timestamp is expressed in YYYY-MM-DD hh:mm:ss format. • none: indicates that the output information does not contain the timestamp. To configure the timestamp format, run the **info-center timestamp** command.
Sent messages	Number of sent messages output by information center modules.
Received messages	Number of messages sent to information center modules.
IO Reg messages	Number of receive messages by switch.
IO Sent messages	Number of sent messages by switch.

3.10.6 display info-center filter-id

Function

The **display info-center filter-id** command displays information filtered by the information center.

Format

display info-center filter-id [*id* | **bymodule-alias** *modname alias*]

Parameters

Parameter	Description	Value
id	Displays filtered information with the specified ID.	The value is in hexadecimal notation and is a string of 8 digits. The value can contain 0-9, a-f, and A-F.
bymodule-alias *modname alias*	Displays filtered information with the specified module name and mnemonic symbol. • *modname*: specifies the module name. • *alias* specifies the mnemonic symbol.	Enumerated type. Set the value according to the device configuration.

Views

All views

Default Level

3: Management level

Usage Guidelines

ID identifies each function module for log registration. An ID filter list is the aggregation of the shielded IDs.

If *id* or **bymodule-alias** is not specified, all information is filtered.

If you do not want to output a specific log to the log file or log buffer, you can find the ID of the log in the data dictionary and run the **info-center filter-id** command to inject the ID into the filter list. Then, you can run the **display info-center filter-id** command to check whether the ID has become the one to be filtered.

Example

Display all the IDs in the filter list.

```
<HUAWEI> display info-center filter-id
ID              : 0x40394017
Module          : SHELL
Alias           : CMDRECORD
Content         : Recorded command information. (Task=[string], Ip=[string], VpnName=[STRING],
User=[string], AthenticationMethod="[STRING]",
Command="[string]")
Filtered Number : 2

ID              : 0x40394018
Module          : SHELL
Alias           : DISPLAY_CMDRECORD
Content         : Recorded display command information. (Task=[string], Ip=[string], VpnName=[string],
User=[string], AuthenticationMethod="[string]",
Command="[string]")
Filtered Number : 1
```

Table 3-148 Description of the display info-center filter-id command output

Item	Description
ID	Identifier to which each log corresponds. To configure the Switch to filter a log or trap with a specified ID, run the **info-center filter-id** *id* command.
Module	Module name. To configure the Switch to filter a log or trap with a specified module name or alias name, run the **info-center filter-id bymodule-alias** *modname alias* command.
Alias	Alias name. To configure the Switch to filter a log or trap with a specified module name or alias name, run the **info-center filter-id bymodule-alias** *modname alias* command.
Content	Log message to which each log ID corresponds.
Filtered Number	Number of times that the log to which the log ID corresponds is filtered.

3.10.7 display info-center rate-limit record

Function

The **display info-center rate-limit record** command displays the suppression of the log processing rate in the information center.

Format

display info-center rate-limit record

Parameters

None

Views

All views

Default Level

3: Management level

Usage Guidelines

You can run the **display info-center rate-limit record** command to check suppression information of the log processing rate. Then you can determine whether service logs are suppressed because there are many logs.

Example

Display the suppression of the log processing rate in the information center.

```
<HUAWEI> display info-center rate-limit record
Record No.1
 InfoID              : 417d5000
 Module              : 6OVER4
 Alias               : DESTFAIL
 Rate limit threshold : 50
 Total receive number : 1872
 Total drop number    : 922
 Total send number    : 950
 Begin timestamp      : 2009-12-21 11:41:28
```

Table 3-149 Description of the **display info-center rate-limit record** command output

Item	Description
InfoID	Log ID.
Module	Log module name.
Alias	Log mnemonic name.
Rate limit threshold	Maximum number of logs set for the information center to process every second.
Total receive number	Total number of logs that are generated during the latest suppression period.
Total drop number	Total number of logs that are discarded during the latest suppression period.

Item	Description
Total send number	Total number of logs that the information center process during the latest suppression period.
Begin timestamp	Timestamp signifying when the suppression function is enabled for the last time.

3.10.8 display info-center rate-limit threshold

Function

The **display info-center rate-limit threshold** command displays the threshold of the log processing rate (maximum number of logs that the information center can process every second). The threshold information includes the default threshold contained in the released version, the default threshold for the specified log ID, and the threshold set through the command lines after the system startup.

Format

display info-center rate-limit threshold

Parameters

None

Views

All views

Default Level

3: Management level

Usage Guidelines

You can run the **display info-center rate-limit threshold** command to check the log processing rate threshold of each module and then adjust the threshold based on service requirements.

Example

Display the threshold of the log processing rate set for the information center.

```
<HUAWEI> display info-center rate-limit threshold
Rate limit threshold(per second):
 Module          Alias                          Default  Config
 default                                        30       30
 IPC             IPCFRGTOOLARGE                  5        5
 IPC             IPCDUMPMEM                      5        5
 IPC             ALLOCINDEXERR                   5        5
 IPC             DRVNOTSTABLE                    2        2
```

```
IPC          NOTIMODFALNOREASM                2       2
IPC          SYNRPCGETSMFAL                   5       5
IPC          SYNRPCMODUNREG                   5       5
IPC          SYNRPCRETNULL                    5       5
IPC          MODULENOTREG                     5       5
IPC          SENDRETURN                       5       5
IPC          GETMTUFAL                        5       5
IPC          ALLOCIPCFRGFAL                   5       5
IPC          RECVINVALIDMSG                   5       5
IPC          RCVNOTIQUEERR                    5       5
IPC          NOTIFYQUEERR                     5       5
IPC          SENDFINISHRETURN                 5       5
IPC          RECVINVALIDMSGTYPE               5       5
SOURCE       UMSGGETSRCOBJFAL                 1       1
```

Table 3-150 Description of the **display info-center rate-limit threshold** command output

Item	Description
Module	Log module name.
Alias	Log mnemonic name.
Default	The default threshold of the log processing rate.
Config	The threshold of the log processing rate set for the information center.

3.10.9 display info-center session log status

Function

The **display info-center session log status** command displays the status of the user session logging function.

Format

display info-center session log status

Parameters

None

Views

All views

Level

3: Management level

Usage Guidelines

If no session log file is generated in a VTY window, you can run the **display info-center session log status** command to view the status of the user session logging function and status of the online user session logging function.

Example

Display the status of the user session logging function.

```
<HUAWEI> display info-center session log status
Info-center Session Log Status:
------------------------------
Global Status: On
------------------------------
User-Interface    Status
VTY 0             Off
VTY 1             On
VTY 2             On
VTY 3             On
CON 0              On
```

Table 3-151 Description of the **display info-center session log status** command output

Item	Description
Info-center Session Log Status	Status of the user session logging function.
Global Status	Status of the user session logging function: • On: Recording session logs is enabled. • Off: Recording session logs is disabled. This function can be configured using the **info-center session log disable** command in the system view.
User-Interface	User UI identifier: • VTY/CON: indicates the user type. • 0/1/2/3: indicates online users.
Status	Status of the online user session logging function: • On: The function is enabled. • Off: The function is disabled. The online user session logging function is disabled after the **info-center session log disable** command is executed to disable the user session logging function. The online user session logging function is enabled after the **undo info-center session log disable** command is executed to enable the user session logging function.

3.10.10 display info-center statistics

Function

The **display info-center statistics** command displays statistics on the information center.

Format

display info-center statistics

Parameters

None

Views

All views

Default Level

3: Management level

Usage Guidelines

You can run the **display info-center statistics** command to view statistics on the information center, including logs, traps, and debugging messages of each module.

Example

Display statistics on the information center.

```
<HUAWEI> display info-center statistics
Information statistics data:
ModuleID    ModuleName       LogSend   LogDrop   DiagSend  DiagDrop  TrapSend
TrapDrop  DebugSend DebugDrop
0x417d0000  6OVER4            0        0        0        0        0
0        0        0
0x41470000  AAA              0        0        0        0        0
0        0        0
0x406c0000  ACL              0        0        0        0        0
0        0        0
0x40ef0000  ACL6             0        0        0        0        0
0        0        0
0xff060000  ACLE             1        0        0        0        0
0        0        0
0xff380000  ADA_BFD           0        0        0        0        0
0        0        0
0x40e70000  ADDR             0        0        0        0        0
0        0        0
0xff2f0000  ADP_RRPP         0        0        114      18       0
0        0        0
0xff950000  ADPIPV4          0        0        253      393      0
0        0        0
  ---- More ----
```


Table 3-152 Description of the display info-center statistics command output

Item	Description
ModuleID	Registered ID of the module.
ModuleName	Name of the module that generates logs.
LogSend	Number of sent logs.
LogDrop	Number of discarded logs.
DiagSend	Number of sent diagnostic messages.
DiagDrop	Number of discarded diagnostic messages.
TrapSend	Number of sent traps.
TrapDrop	Number of discarded traps.
DebugSend	Number of sent debugging messages.
DebugDrop	Number of discarded debugging messages.

3.10.11 display logbuffer

Function

The **display logbuffer** command displays information recorded in the log buffer.

Format

display logbuffer [**size** *size* | **slot** *slot-id* | **module** *module-name* | **security** | **level** { *severity* | *level* }] *

display logbuffer summary [**level** *severity* | **slot** *slot-id*] *

display logbuffer order by module

Parameters

Parameter	Description	Value
size *size*	Displays the specified number of logs recently generated in the log buffer.	The value is an integer that ranges from 1 to 1024.
module *module-name*	Displays logs of a specified module in the log buffer.	Enumerated type. The value depends on the registered module.

Parameter	Description	Value
security	Specifies the security logs.	-
slot *slot-id*	Displays logs in a specified slot.	The value must be set according to the device configuration.
level { *severity* | *level* }	Displays logs of specified severity name or ID. ● *severity* specifies the severity ID. ● *level* specifies the severity name.	The value of *severity* is an integer that ranges from 0 to 7. ● 0: Emergencies ● 1: Alert ● 2: Critical ● 3: Error ● 4: Warning ● 5: Notification ● 6: Informational ● 7: Debugging The value of *level* is the enumerated type: ● emergencies ● alert ● critical ● error ● warning ● notification ● informational ● debugging
summary	Displays the summary of logs in the log buffer.	-

Parameter	Description	Value
order by module	Displays logs in the order of the modules to which they belong to. **NOTE** • Logs in the log buffer are classified and displayed by the modules they belong to. • Modules are displayed by the time that the module's first log is generated in the log buffer in descending order. • Logs in each module are displayed by the time they are generated in descending order.	-

Views

All views

Default Level

3: Management level

Usage Guidelines

The **display logbuffer** command displays the information of recent logs. If the actual number of logs is smaller than the value specified by *size*, the system displays logs of the actual number.

Example

Display all the logs in the log buffer.

```
<HUAWEI> display logbuffer
Logging buffer configuration and contents : enabled
Allowed max buffer size : 1024
Actual buffer size : 512
Channel number : 4 , Channel name : logbuffer
Dropped messages : 0
Overwritten messages : 0
Current messages : 43

Oct 16 2013 06:06:48 HUAWEI %%01VFS/4/DISKSPACE_NOT_ENOUGH(l)[3]:Disk space is
insufficient. The system begins to delete unused log files.
Oct 10 2013 19:06:48 HUAWEI %%01VFS/4/DISKSPACE_NOT_ENOUGH(l)[4]:Disk space is
insufficient. The system begins to delete unused log files.
Oct  7 2013 16:36:48 HUAWEI %%01VFS/4/DISKSPACE_NOT_ENOUGH(l)[5]:Disk space is
insufficient. The system begins to delete unused log files.
```



```
Oct  5 2013 09:12:22 HUAWEI %%01EZOP/3/PROCESS_STOP(l)[6]:Easy-operation upgrad
e process has been stopped. (Reason=There is a configuration file in this device)
Oct  5 2013 09:09:29 HUAWEI %%01IFNET/4/IF_ENABLE(l)[7]:Interface XGigabitEther
net0/0/4 has been available.
Oct  5 2013 09:09:29 HUAWEI %%01IFNET/4/IF_ENABLE(l)[8]:Interface XGigabitEther
net0/0/3 has been available.
Oct  5 2013 09:09:29 HUAWEI %%01IFNET/4/IF_ENABLE(l)[9]:Interface XGigabitEther
net0/0/2 has been available.
Oct  5 2013 09:09:29 HUAWEI %%01IFNET/4/IF_ENABLE(l)[10]:Interface XGigabitEthe
rnet0/0/1 has been available.
Oct  5 2013 09:09:29 HUAWEI %%01IFNET/4/CARD_ENABLE(l)[11]:Board 0 card 1 has b
een available.
Oct  5 2013 09:09:24 HUAWEI %%01ALML/4/ENT_PLUG_IN(l)[12]:LS51S24CA frame[1] bo
ard[0]'s card[1] was plugged in.
Oct  5 2013 09:09:22 HUAWEI %%01IFNET/4/IF_ENABLE(l)[13]:Interface GigabitEther
net0/0/24 has been available.
Oct  5 2013 09:09:22 HUAWEI %%01IFNET/4/IF_ENABLE(l)[14]:Interface GigabitEther
net0/0/23 has been available.
Oct  5 2013 09:09:21 HUAWEI %%01IFNET/4/IF_ENABLE(l)[15]:Interface GigabitEther
net0/0/22 has been available.
Oct  5 2013 09:09:21 HUAWEI %%01IFNET/4/IF_ENABLE(l)[16]:Interface GigabitEther
net0/0/21 has been available.
Oct  5 2013 09:09:20 HUAWEI %%01IFNET/4/IF_ENABLE(l)[17]:Interface GigabitEther
net0/0/20 has been available.
Oct  5 2013 09:09:20 HUAWEI %%01IFNET/4/IF_ENABLE(l)[18]:Interface GigabitEther
net0/0/19 has been available.
Oct  5 2013 09:09:20 HUAWEI %%01IFNET/4/IF_ENABLE(l)[19]:Interface GigabitEther
net0/0/18 has been available.
Oct  5 2013 09:09:19 HUAWEI %%01IFNET/4/IF_ENABLE(l)[20]:Interface GigabitEther
net0/0/17 has been available.
Oct  5 2013 09:09:19 HUAWEI %%01IFNET/4/IF_ENABLE(l)[21]:Interface GigabitEther
net0/0/16 has been available.
Oct  5 2013 09:09:18 HUAWEI %%01IFNET/4/IF_ENABLE(l)[22]:Interface GigabitEther
net0/0/15 has been available.
Oct  5 2013 09:09:18 HUAWEI %%01IFNET/4/IF_ENABLE(l)[23]:Interface GigabitEther
net0/0/14 has been available.
  ---- More ----
```

Display logs in the order of the modules they belong to.

```
<HUAWEI> display logbuffer order by module
Logging buffer configuration and contents : enabled
Allowed max buffer size : 1024
Actual buffer size : 512
Channel number : 4 , Channel name : logbuffer
Dropped messages : 0
Overwritten messages : 0
Current messages : 113

Nov 10 2010 16:16:53 HUAWEI %%01DHCP/4/DHCP_INFO_LOG_DHCP_REMOTEBACKUP_FAILED(l)
[0]:Saving the dynamic binding table to a remot
e server failed. Ensure that the FTP/SFTP server address is reachable and the FTP/SFTP user name and
password and the file path are
correct.
Nov 10 2010 10:38:23 HUAWEI %%01INFO/4/SUPPRESS_LOG(l)[1]:Last message repeated 1 times.
(InfoID=1077493787, ModuleName=SHELL, I
nfoAlias=LOGINFAILED)
Nov 10 2010 10:19:42 HUAWEI %%01SHELL/4/LOGINFAILED(s)[2]:Failed to login. (Ip=10.134.27.157,
UserName=**, Times=3, AccessType=
TELNET, VpnName=)
Nov 10 2010 10:19:42 HUAWEI %%01SHELL/4/LOGIN_FAIL_FOR_INPUT_TIMEOUT(s)[3]:Failed to log in due
to timeout.(Ip=10.134.27.157, U
serName=**, Times=3, AccessType=TELNET,
VpnName=)
Nov 10 2010 10:18:02 HUAWEI %%01SHELL/4/LOGINFAILED(s)[4]:Failed to login. (Ip=10.134.27.157,
UserName=**, Times=2, AccessType=
TELNET, VpnName=)
Nov 10 2010 10:18:02 HUAWEI %%01SHELL/4/LOGIN_FAIL_FOR_INPUT_TIMEOUT(s)[5]:Failed to log in due
to timeout.(Ip=10.134.27.157, U
serName=**, Times=2, AccessType=TELNET,
VpnName=)
```



```
Nov 10 2010 10:16:27 HUAWEI %%01SHELL/4/LOGINFAILED(s)[6]:Failed to login. (Ip=10.134.27.157,
UserName=**, Times=1, AccessType=
TELNET, VpnName=)
Nov 10 2010 10:16:27 HUAWEI %%01SHELL/4/LOGIN_FAIL_FOR_INPUT_TIMEOUT(s)[7]:Failed to log in due
to timeout.(Ip=10.134.27.157, U
serName=**, Times=1, AccessType=TELNET,
VpnName=)
Nov  9 2010 19:51:57 HUAWEI %%01SHELL/4/LOGINFAILED(s)[8]:Failed to login. (Ip=10.134.27.157,
UserName=**, Times=1, AccessType=
TELNET, VpnName=)
```

Table 3-153 Description of the display logbuffer command output

Item	Description
Logging buffer configuration and contents	Whether the device is enabled to output logs to the log buffer: • enabled • disabled To configure the device to output logs to the log buffer, run the **info-center logbuffer** command.
Allowed max buffer size	Maximum size of the log buffer.
Actual buffer size	Actual size of the log buffer. To set the log buffer size, run the **info-center logbuffer size** command.
Channel number	Number of the channel used to send logs to the log buffer. To configure the number of a channel used to send logs to the log buffer, run the **info-center channel** command.
Channel name	Name of the channel used to send logs to the log buffer. To configure the name of a channel used to send logs to the log buffer, run the **info-center channel name** command.
Dropped messages	Number of dropped messages.
Overwritten messages	Number of overwritten messages.
Current messages	Number of current messages.

Display the summary of information in the log buffer.

```
<HUAWEI> display logbuffer summary
    SLOT EMERG ALERT  CRIT ERROR  WARN NOTIF  INFO DEBUG
      0     0     0     0    36   476     0     0     0
```


Table 3-154 Description of the display logbuffer summary command output

Item	Description
SLOT	ID of the slot where logs are generated.
EMERG	Number of logs of emergency.
ALERT	Number of logs of alert.
CRIT	Number of logs of critical.
ERROR	Number of logs of error.
WARN	Number of logs of warning.
NOTIF	Number of logs of notification.
INFO	Number of logs of informational.
DEBUG	Number of logs of debugging.

3.10.12 display logfile

Function

The **display logfile** command displays information about a log file.

Format

display logfile *file-name* [*offset* | **hex**] *

Parameters

Parameter	Description	Value
file-name	Specifies the log file name, which can contain the drive and path.	The value is a string of case-insensitive characters, spaces not supported. If the parameter value does not contain any path, it is a string of 1 to 64 bytes. Otherwise, it is a string of 1 to 160 bytes.
offset	Displays the log file with the specified offset or byte.	The value is an integer that ranges from 0 to 2147483647.

Parameter	Description	Value
hex	Displays the log file in hexadecimal notation. If the parameter is not specified, the log file is displayed in text format.	-

Views

All views

Default Level

3: Management level

Usage Guidelines

When encountering problems, you can query log information to know about what happened during device operation. This is helpful for fault location.

The file name is generated automatically by the system. The file name extension of the log file is *.log or *.dblg. When the current log file size reaches the specified upper limit, the system compresses the file into a *.log.zip or *.dblg.zip file.

You can view the *.log files or *.log.zip files. When viewing a *.log.zip file, you can press **Ctrl+C** to abort command execution.

When viewing the *.log.zip file, it is recommended that the length of the file name (including the driver and path) not exceed 62 bytes. Otherwise, the content of the file may fail to be viewed.

If the files you filter based on the pipe character are large and no qualified log file is displayed, the command fails to display any output for a long period of time until the command execution finishes.

For details about the log format, see "Log Message Format Description" in the *S300, S500, S2700, S5700, and S6700 V200R023C00 Log Reference - Introduction*.

Example

Display log information saved in the log file in a specified path.

```
<HUAWEI> display logfile logfile/log.log
######################################################################
#     This logfile is generated at slot 0
######################################################################

Aug 30 2013 16:18:58-05:13 HUAWEI FSP/4/STANDBY_CHANGE:OID 1.3.6.1.4.1.2011.5.25.183.1.22.3 Slot 2
is designated as standby.
Aug 30 2013 16:19:40-05:13 HUAWEI SNMP/4/WARMSTART:OID 1.3.6.1.6.3.1.1.5.2
warmStart
Aug 30 2013 16:19:15-05:13 HUAWEI %%01ACL/6/INIT_OK(l)[6]:Succeed in mqc
initializtion.
Aug 30 2013 16:19:41-05:13 HUAWEI %%01SHELL/5/CMDRECORD(s)[7]:Record command information.
(Task=CFM, Ip=**, User=**, Command="vlan
batch 4090", Result=Success)
```



```
Aug 30 2013 16:19:41-05:13 HUAWEI %%01SHELL/5/CMDRECORD(s)[8]:Record command information.
(Task=CFM, Ip=**, User=**, Command="inter
face Vlanif4090", Result=Success)
Aug 30 2013 16:19:43-05:13 HUAWEI %%01SHELL/5/CMDRECORD(s)[9]:Record command information.
(Task=CFM, Ip=**, User=**, Command="inter
face Eth-Trunk10", Result=Success)
Aug 30 2013 16:19:43-05:13 HUAWEI %%01SHELL/5/CMDRECORD(s)[10]:Record command information.
(Task=CFM, Ip=**, User=**, Command="inte
rface Eth-Trunk20", Result=Success)
Aug 30 2013 16:19:44-05:13 HUAWEI %%01SHELL/5/CMDRECORD(s)[11]:Record command information.
(Task=CFM, Ip=**, User=**, Command="inte
rface Eth-Trunk30", Result=Success)
Aug 30 2013 16:19:44-05:13 HUAWEI %%01SHELL/5/CMDRECORD(s)[12]:Record command information.
(Task=CFM, Ip=**, User=**, Command="inte
rface GigabitEthernet0/0/1", Result=Success)
Aug 30 2013 16:19:44-05:13 HUAWEI %%01SHELL/5/CMDRECORD(s)[13]:Record command information.
(Task=CFM, Ip=**, User=**, Command="inte
rface GigabitEthernet0/0/2", Result=Success)
Aug 30 2013 16:19:44-05:13 HUAWEI %%01SHELL/5/CMDRECORD(s)[14]:Record command information.
(Task=CFM, Ip=**, User=**, Command="inte
rface GigabitEthernet0/0/3", Result=Success)
```

3.10.13 display log restrain all

Function

The **display log restrain all** command displays all log suppression configurations.

Format

display log restrain all

Parameters

None

Views

All views

Default Level

3: Management level

Usage Guidelines

To check configurations of the log suppression function, run this command.

Example

Display all log suppression configurations.

```
<HUAWEI> display log restrain all
Log restrain                        : enable
Check interval in seconds           : 60
The maximum number of a log per minute : 200

------------------------------------------------------------------------
Description                 InfoId              MaxCount
------------------------------------------------------------------------
```



```
RecordCommand(*)              40394017            NotLimit
RecordCommandResult(*)        40394025            NotLimit
```

Table 3-155 Description of the **display log restrain all** command output

Item	Description
Log restrain	Whether log suppression is enabled.
Check interval in seconds	Statistical period, in seconds.
The maximum number of a log per minute	Maximum number of logs that can be generated every minute.
Description	Description.
InfoId	Log ID.
MaxCount	Maximum number of logs with a specific log ID that can be generated per minutes.

3.10.14 display log restrain statistics

Function

The **display log restrain statistics** command displays all log suppression statistics.

Format

display log restrain statistics

Parameters

None

Views

All views

Default Level

3: Management level

Usage Guidelines

To view all log suppression statistics, run this command.

Example

Display all log suppression statistics.

```
<HUAWEI> display log restrain statistics
Total number of logs              : 56477
```



```
Average number of logs per minute      : 6
Maximum number of logs per minute      : 1796
Minimum number of logs per minute      : 0
Number of log types in the last minute : 0

------------------------------------------------------------------
InfoId                    TotalDiscard          MaxCount
------------------------------------------------------------------
ff51502a                  29                    229
ffd35005                  124                   324
```

Table 3-156 Description of the **display log restrain statistics** command output

Item	Description
Total number of logs	Total number of logs.
Average number of logs per minute	Average number of logs generated per minute.
Maximum number of logs per minute	Maximum number of logs generated per minute.
Minimum number of logs per minute	Minimum number of logs generated per minute.
Number of log types in the last minute	Number of types of the logs generated in the last minute.
InfoId	Log ID.
TotalDiscard	Total number of discarded logs.
MaxCount	Maximum number of logs with a specific log ID generated per minutes.

3.10.15 display trapbuffer

Function

The **display trapbuffer** command displays information recorded in the trap buffer.

Format

display trapbuffer [**size** *value* | **slot** *slot-id* | **module** *module-name* | **level** { *severity* | *level* }] *

display trapbuffer order by module

Parameters

Parameter	Description	Value
size *value*	Displays the specified number of traps recently generated in the trap buffer. If this parameter is not specified, all traps are displayed.	The value is an integer that ranges from 1 to 1024.
module *module-name*	Displays traps of a specified module in the trap buffer.	Enumerated type. The value depends on the registered module.
slot *slot-id*	Displays traps in a specified slot.	The value must be set according to the device configuration.
level { *severity* | *level* }	Displays traps of specified severity name or ID. ● *severity* specifies the severity ID. ● *level* specifies the severity name.	The value of *severity* is an integer that ranges from 0 to 7. ● 0: Emergencies ● 1: Alert ● 2: Critical ● 3: Error ● 4: Warning ● 5: Notification ● 6: Informational ● 7: Debugging The value of *level* is the enumerated type: ● emergencies ● alert ● critical ● error ● warning ● notification ● informational ● debugging

Parameter	Description	Value
order by module	Displays alarms in the order of the modules they belong to. **NOTE** • Alarms in the alarm buffer are classified and displayed by the modules they belong to. • Modules are displayed by the time that the module's first alarm is generated in the alarm buffer in descending order. • Alarms in each module are displayed by the time they are generated in descending order.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

The **display trapbuffer** command displays the information of recent traps. If the number of traps in the trap buffer is smaller than *value*, traps of the actual number are displayed.

Example

Display all traps in the trap buffer.

```
<HUAWEI> display trapbuffer
Trapping buffer configuration and contents : enabled
Allowed max buffer size : 1024
Actual buffer size : 256
Channel number : 3 , Channel name : trapbuffer
Dropped messages : 0
Overwritten messages : 6248
Current messages : 256

#Sep 19 2012 04:38:03+08:00 HUAWEI DS/4/DATASYNC_CFGCHANGE:OID 1.3.6.1.4.1.2011
.5.25.191.3.1 configurations have been changed. The current change number is 8,
the change loop count is 0, and the maximum number of records is 4095.
#Sep 19 2012 04:37:39+08:00 HUAWEI LINE/5/VTYUSERLOGIN:OID 1.3.6.1.4.1.2011.5.2
5.207.2.2 A user login. (UserIndex=34, UserName=VTY, UserIP=10.135.18.114, UserC
hannel=VTY0)
#Sep 19 2012 04:35:48+08:00 HUAWEI LINE/5/VTYUSERLOGOUT:OID 1.3.6.1.4.1.2011.5.
25.207.2.4 A user logout. (UserIndex=34, UserName=VTY, UserIP=10.135.18.143, Use
rChannel=VTY0)
#Sep 19 2012 04:20:54+08:00 HUAWEI LINE/5/VTYUSERLOGIN:OID 1.3.6.1.4.1.2011.5.2
5.207.2.2 A user login. (UserIndex=34, UserName=VTY, UserIP=10.135.18.143, UserC
hannel=VTY0)
#Sep 19 2012 04:08:03+08:00 HUAWEI LINE/5/VTYUSERLOGOUT:OID 1.3.6.1.4.1.2011.5.
25.207.2.4 A user logout. (UserIndex=34, UserName=VTY, UserIP=10.135.18.143, Use
rChannel=VTY0)
```



```
#Sep 19 2012 03:54:27+08:00 HUAWEI LINE/5/VTYUSERLOGIN:OID 1.3.6.1.4.1.2011.5.2
5.207.2.2 A user login. (UserIndex=34, UserName=VTY, UserIP=10.135.18.143, UserC
hannel=VTY0)
#Sep 19 2012 03:54:18+08:00 HUAWEI LINE/5/VTYUSERLOGINFAIL:OID 1.3.6.1.4.1.2011
.5.25.207.2.3 A user login fail. (UserIndex=34, UserName=VTY, UserIP=10.135.18.1
43, UserChannel=VTY0)
#Sep 19 2012 02:51:03+08:00 HUAWEI LINE/5/VTYUSERLOGOUT:OID 1.3.6.1.4.1.2011.5.
25.207.2.4 A user logout. (UserIndex=34, UserName=VTY, UserIP=10.135.18.57, User
Channel=VTY0)
#Sep 19 2012 02:50:24+08:00 HUAWEI LINE/5/VTYUSERLOGOUT:OID 1.3.6.1.4.1.2011.5.
25.207.2.4 A user logout. (UserIndex=35, UserName=VTY, UserIP=10.135.18.164, Use
rChannel=VTY1)
#Sep 19 2012 02:40:19+08:00 HUAWEI LINE/5/VTYUSERLOGIN:OID 1.3.6.1.4.1.2011.5.2
5.207.2.2 A user login. (UserIndex=35, UserName=VTY, UserIP=10.135.18.164, UserC
hannel=VTY1)
#Sep 19 2012 02:35:23+08:00 HUAWEI LINE/5/VTYUSERLOGIN:OID 1.3.6.1.4.1.2011.5.2
5.207.2.2 A user login. (UserIndex=34, UserName=VTY, UserIP=10.135.18.57, UserCh
annel=VTY0)
......
```

Display alarms in the order of the modules they belong to.

```
<HUAWEI> display trapbuffer order by module
Trapping buffer configuration and contents : enabled
Allowed max buffer size : 1024
Actual buffer size : 256
Channel number : 3 , Channel name : trapbuffer
Dropped messages : 0
Overwritten messages : 0
Current messages : 79

#Nov 11 2010 11:51:24 HUAWEI LINE/5/VTYUSERLOGIN:OID 1.3.6.1.4.1.2011.5.25.207.2.2 A user login.
(UserIndex=36, UserName=**, Us
erIP=10.135.19.152, UserChannel=VTY2)
#Nov 10 2010 18:54:06 HUAWEI LINE/5/VTYUSERLOGIN:OID 1.3.6.1.4.1.2011.5.25.207.2.2 A user login.
(UserIndex=35, UserName=**, Us
erIP=10.135.186.212, UserChannel=VTY1)
#Nov 10 2010 12:07:44 HUAWEI LINE/5/VTYUSERLOGIN:OID 1.3.6.1.4.1.2011.5.25.207.2.2 A user login.
(UserIndex=34, UserName=**, Us
erIP=10.135.19.157, UserChannel=VTY0)
#Nov 10 2010 11:19:23 HUAWEI LINE/5/VTYUSERLOGOUT:OID 1.3.6.1.4.1.2011.5.25.207.2.4 A user logout.
(UserIndex=34, UserName=**,
UserIP=10.134.27.157, UserChannel=VTY0)
#Nov 10 2010 10:48:57 HUAWEI LINE/5/VTYUSERLOGIN:OID 1.3.6.1.4.1.2011.5.25.207.2.2 A user login.
(UserIndex=34, UserName=**, Us
erIP=10.134.27.157, UserChannel=VTY0)
#Nov 10 2010 10:48:48 HUAWEI LINE/5/VTYUSERLOGOUT:OID 1.3.6.1.4.1.2011.5.25.207.2.4 A user logout.
(UserIndex=34, UserName=**,
UserIP=10.134.27.157, UserChannel=VTY0)
#Nov 10 2010 10:38:23 HUAWEI LINE/5/VTYUSERLOGIN:OID 1.3.6.1.4.1.2011.5.25.207.2.2 A user login.
(UserIndex=34, UserName=**, Us
erIP=10.134.27.157, UserChannel=VTY0)
```

Table 3-157 Description of the display trapbuffer command output

Item	Description
Trapping buffer configuration and contents	Whether the device is enabled to output traps to the trap buffer: ● enabled ● disabled To enable the device to output traps to the trap buffer, run the **info-center trapbuffer** command.

Item	Description
Allowed max buffer size	Maximum size of the trap buffer.
Actual buffer size	Actual size of the trap buffer. To set the size of the trap buffer, run the **info-center trapbuffer size** command.
Channel number	Number of the channel used to send traps to the trap buffer. To set the channel number, run the **info-center channel** command.
Channel name	Name of the channel used to send traps to the trap buffer. To set the channel name, run the **info-center channel name** command.
Dropped messages	Number of dropped messages.
Overwritten messages	Number of overwritten messages.
Current messages	Number of current messages.

3.10.16 info-center channel

Function

The **info-center channel** command configures channels for outputting information in various directions.

The **undo info-center channel** command restores the default settings.

By default, the system outputs information in various directions through channels listed in the table below.

Table 3-158 Default association between the channel number, channel name, and output direction of information channels

Channel Number	Channel Name	Output Direction
0	console	Console
1	monitor	User terminal
2	loghost	Log host
3	trapbuffer	Trap buffer
4	logbuffer	Log buffer

Channel Number	Channel Name	Output Direction
5	snmpagent	SNMP agent
6	channel6	Unspecified
7	channel7	Unspecified
8	channel8	Unspecified
9	channel9	Log file

Format

info-center { **console** | **logbuffer** | **logfile** | **monitor** | **snmp** | **trapbuffer** } **channel** { *channel-number* | *channel-name* }

undo info-center { { **console** | **monitor** | **snmp** | **logfile** } **channel** | { **logbuffer** | **trapbuffer** } **channel** [*channel-number* | *channel-name*] }

Parameters

Parameter	Description	Value
console	Specifies the channel used to output information to the console.	-
logbuffer	Specifies the channel used to output information to the log buffer.	-
logfile	Specifies the channel used to output information to the log file.	-
monitor	Specifies the channel used to output information to the user terminal.	-
snmp	Specifies the channel used to output information to the SNMP agent.	-
trapbuffer	Specifies the channel used to output information to the trap buffer.	-
channel-number	Specifies the channel number.	The value is an integer ranging from 0 to 9.
channel-name	Specifies the name of a channel, which can be the default channel name or a user-defined name.	The value is a string of 1 to 30 case-insensitive characters. The value consists of letters or numbers and must start with a letter.

Views

System view

Default Level

3: Management level

Usage Guidelines

You can run the **info-center channel** command in the following scenarios: The same information is sent to different directions. For example, the log file and log host record the same content or the trap buffer and the SNMP agent record the same content.

NOTE

The channels should not have the same name.

For details on how to configure a channel for outputting information to a log host, see **info-center loghost**.

The **info-center channel** command takes effect only after the information center function has been enabled using the **info-center enable** command.

Example

Configure the channel used to output information to a console.

```
<HUAWEI> system-view
[HUAWEI] info-center console channel console
```

Configure the channel used to output information to the log buffer.

```
<HUAWEI> system-view
[HUAWEI] info-center logbuffer channel logbuffer
```

Configure the channel used to output information to the user terminal.

```
<HUAWEI> system-view
[HUAWEI] info-center monitor channel monitor
```

Configure the channel used to output information to an SNMP agent.

```
<HUAWEI> system-view
[HUAWEI] info-center snmp channel 5
```

Configure the channel used to output information to the trap buffer.

```
<HUAWEI> system-view
[HUAWEI] info-center trapbuffer channel trapbuffer
```

3.10.17 info-center channel name

Function

The **info-center channel name** command names a channel with a specified number.

The **undo info-center channel** command restores the default channel name.

The following lists default channel names.

Table 3-159 Default channel names

Channel Number	Default Channel Name
0	console
1	monitor
2	loghost
3	trapbuffer
4	logbuffer
5	snmpagent
6	channel6
7	channel7
8	channel8
9	channel9

Format

info-center channel *channel-number* **name** *channel-name*

undo info-center channel *channel-number*

Parameters

Parameter	Description	Value
channel-number	Specifies the number of a channel.	The value is an integer that ranges from 0 to 9. That is, the system has 10 channels.
channel-name	Specifies the name of a channel.	The value is a string of 1 to 30 case-insensitive characters. The value consists of letters or numbers and must start with a letter.

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

You can rename channels, which facilitates memorization and usage.

Precautions

Channel names must be unique. It is recommended that channel names represent channel functions.

Example

Name channel 0 execconsole.

```
<HUAWEI> system-view
[HUAWEI] info-center channel 0 name execconsole
```

3.10.18 info-center enable

Function

The **info-center enable** command enables the information center.

The **undo info-center enable** command disables the information center.

The **info-center disable** command disables the information center.

By default, the information center is enabled.

Format

info-center enable

undo info-center enable

info-center disable

Parameters

None

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

During device running, the information center records device operation. The system outputs system information to destinations such as the log host and the console only after the information center is enabled. Network administrators can store and query output information to monitor device running and locate faults.

Precautions

After the **undo info-center enable** or **info-center disable** command is executed, only logfile, logbuffer, and user session record logs, the other channel no longer records logs.

Follow-up Procedure

Configure a rule for outputting information to the terminal or remote server.

Example

Enable the information center.

```
<HUAWEI> system-view
[HUAWEI] info-center enable
Info: Information center is enabled.
```

3.10.19 info-center filter-id

Function

The **info-center filter-id** command configures the Switch to filter a specified log or trap.

The **undo info-center filter-id** command disables the Switch from filtering a specified log or trap.

By default, no log or trap is filtered.

Format

info-center filter-id { *id* | **bymodule-alias** *modname alias* } &<1-50>

info-center filter-id { *id* | **bymodule-alias** *modname alias* } [**bytime** *interval* | **bynumber** *number*]

undo info-center filter-id all

undo info-center filter-id { *id* | **bymodule-alias** *modname alias* } &<1-50>

undo info-center filter-id { *id* | **bymodule-alias** *modname alias* } [**bytime** *interval* | **bynumber** *number*]

Parameters

Parameter	Description	Value
id	Specifies the ID of the log or trap to be filtered. **NOTE** This parameter indicates the ID of a log. If this parameter fails to be configured, the log specified by this ID does not exist.	The value is in hexadecimal notation and contains 8 digits. The value contains 0-9, a-f, and A-F.
bymodule-alias *modname alias*	Specifies the module name and alias name corresponding to the log or trap to be filtered.	Enumerated type. Set the value according to the device configuration.

Parameter	Description	Value
all	Filters all logs or traps.	-
bytime *interval*	Specifies the interval at which logs are sent.	The value is an integer that ranges from 1 to 86400, in seconds.
bynumber *number*	Specifies the number of logs that are discarded between two received logs.	The value is an integer that ranges from 1 to 1000.

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

If some logs or traps are unnecessary, configure the Switch not to output the logs and traps. When the filtering function is enabled, the information center does not send the traps with a specified ID that satisfy the filtering condition to any channel. As a result, the trap buffer, console, terminal, or SNMP agent cannot receive the traps with the specified ID.

Precautions

- Currently, the Switch can filter traps with a maximum of 50 IDs. If there are more than 50 log IDs, the system displays a message indicating that the filtering table is full. To configure the filtering function, run the **undo info-center filter-id** { *id* | **bymodule-alias** *modname alias* } &<1-50> [**bytime** *interval* | **bynumber** *number*], or the **undo info-center filter-id all** command to delete original IDs and reconfigure the log ID.
- When both the **bytime** *interval* and **bynumber** *number* parameters are not specified, all the logs with the specified ID will be discarded.
- When the **bytime** *interval* parameter is specified, the interval for sending two allowed logs must be at least the configured time.
- When the **bynumber** *number* parameter is specified, the configured number of logs between two allowed logs must be discarded.
- To add multiple IDs at a time, use a space to separate every two IDs. The result of adding each ID is displayed.
- You cannot add the same ID or alias name repeatedly.
- When you add an unregistered or nonexistent ID or alias name, the system displays a message indicating that the system fails to filter the log or trap with the specified ID or alias name.

- During a software upgrade, if the information filtering function is configured in the old version, but the new version does not support the specified log module and alias, the information filtering configuration of the specified log module and alias will be automatically cleared after the upgrade.
- You are advised to use the module name and alias to filter specified log information. The *id* parameter can be obtained by running the **display info-center register-info** [**module** *module-name*] **log** command in the diagnostic view, and the *modname* and *alias* parameters can be obtained through the command association function.

Example

Filter information by module names and alias names.
<HUAWEI> **system-view**
[HUAWEI] **info-center filter-id bymodule-alias CMD CMD_PRI_REARRG**

Cancel filtering for all logs.
<HUAWEI> **system-view**
[HUAWEI] **undo info-center filter-id all**

Filter the log with the ID of 40394017.
<HUAWEI> **system-view**
[HUAWEI] **info-center filter-id 40394017**

3.10.20 info-center local log-counter disable

Function

The **info-center local log-counter disable** command disables the local log from carrying the sequence number.

The **undo info-center local log-counter disable** command enables the local log to carry the sequence number.

By default, the local log carries the sequence number.

Format

info-center local log-counter disable

undo info-center local log-counter disable

Parameters

None

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

If the device keeps running for a long time, a large number of logs may be generated.

- You can run the **info-center local log-counter disable** command to disable logs sent to the log buffer, log file, console, or terminal from carrying the sequence number, and run the **undo info-centerlocal log-counter disable** command to enable these logs to carry the sequence number.
- You can run the **undo info-center local log-counter disable** command to enable logs to carry the incremental sequence number, checking whether all logs have been sent to the log buffer, log file, console, or terminal.

NOTE

- Logs sent to the console log file, or terminal are counted separately and therefore carry different sequence numbers in ascending order. The sequence number of the earliest log is 0.
- Logs sent to the log buffer carry sequence numbers in descending order. The sequence number of the latest log is 0.

Example

Disable local logs from carrying the sequence number.

```
<HUAWEI> system-view
[HUAWEI] info-center local log-counter disable
```

Enable local logs to carry the sequence number.

```
<HUAWEI> system-view
[HUAWEI] undo info-center local log-counter disable
```

3.10.21 info-center logbuffer

Function

The **info-center logbuffer** command enables the Switch to send logs to the log buffer.

The **undo info-center logbuffer** command disables the Switch from sending logs to the log buffer.

By default, the Switch is enabled to send logs to the log buffer.

Format

info-center logbuffer

undo info-center logbuffer

Parameters

None

Views

System view

Default Level

3: Management level

Usage Guidelines

To log in to a device and check the faults or problems during operation, run the **info-center logbuffer** command to enable the function to output logs to the log buffer. Then, you can view log information in the log buffer.

By configuring the size of the log buffer using the **info-center logbuffer size** *buffersize* command, you can view information about specified logs.

By configuring the number or name of a channel through which a device sends logs to the log buffer using the **info-center logbuffer channel** { *channel-number* | *channel-name* } command, you can send log information through a specified channel to the log buffer.

Example

Enable the Switch to send logs to the log buffer.

```
<HUAWEI> system-view
[HUAWEI] info-center logbuffer
```

3.10.22 info-center logbuffer size

Function

The **info-center logbuffer size** command sets the maximum number of logs in the log buffer.

The **undo info-center logbuffer size** command restores the default maximum number of logs in the log buffer.

By default, a log buffer can store a maximum of 512 logs.

Format

info-center logbuffer size *logbuffer-size*

undo info-center logbuffer size [*logbuffer-size*]

Parameters

Parameter	Description	Value
logbuffer-size	Specifies the maximum number of logs in the log buffer.	The value is an integer that ranges from 0 to 1024. If *logbuffer-size* is 0, logs are not displayed.

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

If the number of logs in the log buffer reaches the maximum value, new logs will replace the existing logs that were placed earlier in the log buffer until all the new logs are stored.

Precautions

When you run the **info-center logbuffer size** command multiple times, only the latest configuration takes effect.

The **info-center logbuffer size** command takes effect only after the information center function has been enabled using the **info-center enable** command.

Example

Set the maximum number of logs in the log buffer to 50.

```
<HUAWEI> system-view
[HUAWEI] info-center logbuffer size 50
```

3.10.23 info-center logfile size

Function

The **info-center logfile size** command sets the log file size.

The **undo info-center logfile size** command restores the default log file size.

By default, the log file size is 8 MB.

Format

info-center logfile size *size*

undo info-center logfile size

Parameters

Parameter	Description	Value
size	Specifies the log file size.	The value is an integer that is 4, 8, 16, or 32, in MB. The default value is 8 MB.

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

To configure the Switch to export information to a log file, run the **info-center logfile size** command to set the log file size.

Precautions

If you configure the device to export information to a log file, exported information is saved in the **log.log** or **log.dblg** file. When the **log.log** or **log.dblg** file exceeds the specified size, the system compresses the file in to a zip package and names the compressed file *date time*.log.zip or *date time*.dblg.zip.

The **info-center logfile size** command takes effect only after the information center function has been enabled using the **info-center enable** command.

Example

Set the log file size to 32 MB.

```
<HUAWEI> system-view
[HUAWEI] info-center logfile size 32
```

3.10.24 info-center loghost

Function

The **info-center loghost** command configures the device to output information to a log host.

The **undo info-center loghost** command disables the device from outputting information to a log host.

By default, no information is output to the log host.

Format

info-center loghost *ip-address* [**channel** { *channel-number* | *channel-name* } | **facility** *local-number* | **language** *language-name* | { **vpn-instance** *vpn-instance-name* | **public-net** } | **local-time** | **log-counter** { **disable** | **enable** } | **port** *port* | **security-log** | **operation-log** | { **source-ip** *source-ip-address* } | **transport** { **udp** | **tcp ssl-policy** *policy-name* [**verify-dns-name** *verify-dns-name*] }] *

info-center loghost ipv6 *ipv6-address* [**channel** { *channel-number* | *channel-name* } | **facility** *local-number* | **language** *language-name* | **local-time** | **log-counter** { **disable** | **enable** } | **port** *port* | **security-log** | **operation-log** | **transport** { **udp** | **tcp ssl-policy** *policy-name* [**verify-dns-name** *verify-dns-name*] }] *

undo info-center loghost *ip-address* [**vpn-instance** *vpn-instance-name*]

undo info-center loghost ipv6 *ipv6-address*

info-center loghost domain *domain-name* [**vpn-instance** *vpn-instance-name*] [**channel** { *channel-number* | *channel-name* } | **facility** *local-number* | **language** *language-name* | **log-counter** { **disable** | **enable** } | **local-time** | **port** *port* | **security-log** | **operation-log** | **transport** { **udp** | **tcp ssl-policy** *policy-name* [**verify-dns-name** *verify-dns-name*] }] *

undo info-center loghost domain *domain-name* [**vpn-instance** *vpn-instance-name*]

Parameters

Parameter	Description	Value
ip-address	Specifies the IPv4 address of the log host.	The value is in dotted decimal notation.
channel { *channel-number* | *channel-name* }	Specifies the channel used to send information to a log host. • *channel-number*: specifies the number of a channel. • *channel-name*: specifies the name of a channel. The name can be the default or user-defined channel name.	The value of *channel-number* is an integer that ranges from 0 to 9. The value of *channel-name* is a string of 1 to 30 case-insensitive characters. The value consists of letters or numbers and must start with a letter.
facility *local-number*	Specifies a syslog server facility that is used to identify the log information source. You can use this parameter to plan a local value for the log information of a specified device, so that the syslog server can handle received log information based on the parameter.	The value ranges from local0 to local7. The default value is local7.
language *language-name*	Displays the language in which logs are recorded.	Currently, the value can only be English.

Parameter	Description	Value
vpn-instance *vpn-instance-name*	VPN instance.	The value must be an existing VPN instance name. **NOTE** _public_ cannot be specified as a VPN instance name.If the VPN instance is not created, the command does not take effect.
public-net	Indicates that the log host is connected in the public network.	-
local-time	Indicates the local time when logs are sent to the log host.	-
log-counter { **disable** | **enable** }	Disables or enables the log counter function.	-
port *port*	Specifies the port number of a log host.	The value is an integer that ranges from 1 to 65535. By default, when the transport mode is UDP, the port number of the log host is 514; when the transport mode is TCP, the port number of the log host is 6514.
security-log	Configures a device to send security logs to a specified log host.	-
operation-log	Configures a device to send operation logs to a specified log host.	-
source-ip *source-ip-address*	Specifies the source IP address used to send information to the log host.	The value is in dotted decimal notation.
transport	Indicates the information transport mode.	-

Parameter	Description	Value
udp	Indicates the UDP transport mode. **NOTE** The default transport mode is UDP if no transport mode is specified.	-
tcp	Indicates the TCP transport mode. **NOTE** The default transport mode is UDP if no transport mode is specified.	-
ssl-policy *policy-name*	Specifies a Secure Sockets Layer (SSL) policy in the TCP transport mode. This parameter is recommended to improve log transmission security.	The value is a string of 1 to 23 case-insensitive characters without spaces.
verify-dns-name *verify-dns-name*	Verify DNS identifier name.	The value is a string of 1 to 255 case-insensitive characters without spaces.
ipv6 *ipv6-address*	Specifies the IPv6 address of the log host.	The value is a 32-digit hexadecimal number.
domain *domain-name*	Specifies a DNS domain name of a log host.	The value is a string of 1 to 255 case-sensitive characters, spaces not supported.

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

To query information generated on the Switch deployed remotely, configure the Switch to export information to a log host so that you can view device information on the log host. Run the **info-center loghost** command to configure the Switch to export information to a log host.

To configure the Switch to output information to different log hosts using different channels, specify the channels used to send information to the log hosts. For example, you can configure the Switch to output information to log hosts at 192.168.0.1 and 192.168.0.2 using channels 7 and 8 respectively.

Precautions

The Switch can output information to eight log hosts including IPv4 and IPv6 hosts to implement backup among log hosts.

To transfer logs to the log hosts using TCP and encrypt logs using SSL, create an SSL policy first.

If the **set net-manager vpn-instance** command is run to configure the NMS to manage network elements through a VPN instance, either of the following situations occurs.

- If **vpn-instance** is configured, the system accesses the log host in the VPN instance.
- If **public-net** is configured, the system accesses the log host on the public network.

If the **transport tcp ssl-policy** *policy-name* parameters are specified to enable logs to be transmitted in TCP mode through SSL encryption, perform the following operations:

- Run the **ssl-policy** *policy-name* command to configure an SSL policy and enter the SSL policy view.
- Run the **trusted-ca load** command to load trusted-CA files (**cacert** and **rootcert** files) of the SSL client.
- On the log server, load trusted-CA files (**serverkey** and **servercert** files) of the SSL server.
- Run the **display tcp status** command to check that the TCP connection status of port 6514 is **Established**.

Example

Configure a device to use channel 6 to output information to the log host at 10.1.1.1.

```
<HUAWEI> system-view
[HUAWEI] info-center loghost 10.1.1.1 channel channel6
```

Configure the source IP address used to send information to the log host is Loopback1.

```
<HUAWEI> system-view
[HUAWEI] info-center  loghost source LoopBack1
```

Configure the Switch to send information to the log host at FC00:0:0:3001::1/64.

```
<HUAWEI> system-view
[HUAWEI] info-center loghost ipv6 fc00:0:0:3001::1
```

Configure the Switch to send information to the host with the IPv4 address 192.168.2.2 and VPN instance name **vpn1**.

```
<HUAWEI> system-view
[HUAWEI] info-center loghost 192.168.2.2 vpn-instance vpn1
```


Configure a device to send information to a log host with the domain name set to **www.test.com**.
```
<HUAWEI> system-view
[HUAWEI] info-center loghost domain www.test.com
```

Configure a device to send information to the log host at 192.168.2.2 in TCP mode, using the SSL policy **YsHsjx_202206** that has been created in the system.
```
<HUAWEI> system-view
[HUAWEI] ssl policy YsHsjx_202206
[HUAWEI-ssl-policy-ftps_der] trusted-ca load pem-ca 1_cacert_pem_rsa.pem
[HUAWEI-ssl-policy-ftps_der] trusted-ca load pem-ca 1_rootcert_pem_rsa.pem
[HUAWEI-ssl-policy-ftps_der] quit
```

3.10.25 info-center loghost source

Function

The **info-center loghost source** command configures the source interface used by the Switch to send information to a log host.

The **undo info-center loghost source** command restores the default source interface used by the Switch to send information to a log host.

By default, the source interface for a device to send logs to a log host is the actual interface that sends the logs.

Format

info-center loghost source *interface-type interface-number*

undo info-center loghost source

Parameters

Parameter	Description	Value
interface-type interface-number	Specifies the type and number of an interface.	-

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

If multiple devices send log messages to the same log host, you can identify the devices by setting different source interfaces so as to index the received log messages.

The source interface specified in the **info-center loghost source** command for a device to send logs to a log host is not necessarily the actual interface that sends the logs, but the IP address of the specified source interface is carried in logs.

Prerequisites

There is a reachable route between the source interface and the log host.

Example

Specify Loopback0 IP address as the source interface address to send information to a log host.

```
<HUAWEI> system-view
[HUAWEI] interface loopback 0
[HUAWEI-LoopBack0] ip address 10.1.1.1 255.255.255.0
[HUAWEI-LoopBack0] quit
[HUAWEI] info-center loghost source loopback 0
```

3.10.26 info-center loghost source-port

Function

The **info-center loghost source-port** command configures a source interface through which the device sends information to the log host.

The **undo info-center loghost source-port** command restores the default source interface through which the device sends information to the log host.

By default, the source interface number is 38514.

Format

info-center loghost source-port *source-port*

undo info-center loghost source-port

Parameters

Parameter	Description	Value
source-port	Specifies the number of the source interface through which the device sends information to the log host.	The value is an integer ranging from 1025 to 65535.

Views

System view

Default Level

3: Management level

Usage Guidelines

If the device uses the default source interface to send information to the log host, attackers may keep accessing this interface. As a result, the log host cannot send

information. To improve system security, you can run the **info-center loghost source-port** *source-port* command to change the source interface through which the device sends information to the log host so that attackers cannot obtain the new source interface.

Example

Change the number of the source interface through which the device sends information to the log host to 1026.

```
<HUAWEI> system-view
[HUAWEI] info-center loghost source-port 1026
```

3.10.27 info-center max-logfile-number

Function

The **info-center max-logfile-number** command sets the maximum number of log files to be saved.

The **undo info-center max-logfile-number** command restores the default maximum number of log files to be saved.

By default, a maximum of 500 log files can be stored on the S5732-H, S6730-H, S6730-S, S6730S-S, and S6730S-H, and a maximum of 200 log files can be stored on other models.

Format

info-center max-logfile-number *filenumbers*

undo info-center max-logfile-number

Parameters

Parameter	Description	Value
filenumbers	Specifies the maximum number of log files that can be saved.	The value is an integer that ranges from 3 to 500.

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

If too many log files are saved on the Switch, many disk space resources are occupied. To view log files generated recently, run the **info-center max-logfile-number** command to set the maximum number of log files that can be saved.

Precautions

If the number of log files generated on the Switch exceeds the limit, the system deletes the oldest log file so that the number of log files is not larger than the maximum value.

NOTICE

If the number of saved log files is greater than the default value, more system resources are consumed. The default value is recommended. Excess log files can be deleted automatically. When the system deletes excess log files, high CPU usage may last for a short period.

Example

Set the maximum number of log files to be saved to 100.

```
<HUAWEI> system-view
[HUAWEI] info-center max-logfile-number 100
```

3.10.28 info-center rate-limit except

Function

The **info-center rate-limit except** command cancels the log processing rate limit for logs.

The **undo info-center rate-limit except** command deletes the preceding configuration.

Format

info-center rate-limit except { **byinfoid** *infoID* | **bymodule-alias** *modname alias* }

undo info-center rate-limit except { **byinfoid** *infoID* | **bymodule-alias** *modname alias* }

Parameters

Parameter	Description	Value
byinfoid *infoID*	Specifies the log ID in hexadecimal notation.	The value is a 32-digit hexadecimal number in the format XXXXXXXX. It ranges from 0 to ffffffff.
bymodule-alias *modname*	Specifies the log module name.	The value is a string of 1 to 24 case-insensitive characters without spaces.

Parameter	Description	Value
alias	Specifies the log mnemonic name.	The value is a string of 1 to 64 case-insensitive characters without spaces.

Views

System view

Default Level

3: Management level

Usage Guidelines

When too many logs will never be generated under a specified ID, you can run the **info-center rate-limit except** command to avoid the impact of the suppression of the log processing rate. After this command is run, the configured log processing rate limit will not be effective for logs with the specified ID or module name.

During a software upgrade, if the function that prevents logs from being suppressed by the information center is configured in the old version, but the new version does not support the specified log module and alias, the function configuration of the specified log module and alias will be automatically cleared after the upgrade.

Example

Prevent logs specified by the module name and mnemonic from being suppressed by the information center.

```
<HUAWEI> system-view
[HUAWEI] info-center rate-limit except bymodule-alias AAA AUTHEN_ERR_EVENT
```

Prevent logs specified by the log ID from being suppressed by the information center.

```
<HUAWEI> system-view
[HUAWEI] info-center rate-limit except byinfoid ff011015
```

Prevent logs with a specified log ID from being suppressed by the information center.

```
<HUAWEI> system-view
[HUAWEI] undo info-center rate-limit except bymodule-alias AAA AUTHEN_ERR_EVENT
```

3.10.29 info-center rate-limit global-threshold

Function

The **info-center rate-limit global-threshold** command sets the total number of logs that the information center can process every second.

The **undo info-center rate-limit global-threshold** command restores the default value.

By default, the information center processes a maximum of 400 logs in every second.

Format

info-center rate-limit global-threshold *value*

undo info-center rate-limit global-threshold

Parameters

Parameter	Description	Value
value	Specifies the maximum number of logs that the information center can process every second.	The value is an integer that ranges from 100 to 1000.

Views

System view

Default Level

3: Management level

Usage Guidelines

You can run the **info-center rate-limit global-threshold** command to adjust the processing capability of the information center. If the number of logs to be processed exceeds the processing capability of the information center, the extra logs are discarded.

NOTE

- If the threshold is too low, some logs may be discarded.
- If the threshold is too high, the information center cannot identify the log ID under which too many logs are generated. The number of logs to be processed depends on the current processing capacity of the information center.

Example

Set the number of logs that the information center can process every second to 300.

```
<HUAWEI> system-view
[HUAWEI] info-center rate-limit global-threshold 300
```

3.10.30 info-center rate-limit monitor-period

Function

The **info-center rate-limit monitor-period** command sets the monitoring period for the information center to suppress the log processing rate.

The **undo info-center rate-limit monitor-period** command restores the default value.

By default, the monitoring period is 3 seconds.

Format

info-center rate-limit monitor-period *value*

undo info-center rate-limit monitor-period

Parameters

Parameter	Description	Value
value	Specifies the monitoring period for the information center to suppress the log processing rate.	The value is an integer ranging from 1 to 60, in seconds.

Views

System view

Default Level

3: Management level

Usage Guidelines

In the monitoring period specified by *value*, if the rate of sending a single log every second exceeds the threshold configured using the **info-center rate-limit threshold** command, the information center will limit the log processing rate. In this situation, the information center discards logs exceeding the threshold.

In the monitoring period that is five times *value*, if the number of a single type of logs that are sent every second is smaller than the threshold configured using the **info-center rate-limit threshold** command, the information center does not limit the log processing rate.

Example

Set the monitoring period for the information center to suppress the log processing rate to 5 seconds.

```
<HUAWEI> system-view
[HUAWEI] info-center rate-limit monitor-period 5
```

3.10.31 info-center rate-limit threshold

Function

The **info-center rate-limit threshold** command sets the maximum number of logs with the same log ID that the information center can process every second.

The **undo info-center rate-limit threshold** command restores the default setting.

By default, the information center processes a maximum of 30 logs with the same log ID in every second.

Format

info-center rate-limit threshold *value* [**byinfoid** *infoID* | **bymodule-alias** *modname alias*]

undo info-center rate-limit threshold [*value*] [**byinfoid** *infoID* | **bymodule-alias** *modname alias*]

Parameters

Parameter	Description	Value
value	Specifies the maximum number of logs with the same log ID that the information center can process every second.	The value is an integer that ranges from 1 to 500.
byinfoid *infoID*	Specifies the log ID.	The value is a 32-digit hexadecimal number in the format XXXXXXXX. It ranges from 0 to ffffffff.
bymodule-alias *modname*	Specifies the log of the module name.	The value is a string of 1 to 24 case-insensitive characters without spaces.
alias	Specifies the log of the mnemonic name.	The value is a string of 1 to 64 case-insensitive characters without spaces.

Views

System view

Default Level

3: Management level

Usage Guidelines

You can run the **info-center rate-limit threshold** command to set the maximum number of logs with the same log ID that the information center can process every second. The information center monitors the number of logs that are generated every second under the same log ID. When the number of logs that are generated every second under the same log ID exceeds the threshold in the monitoring period, the information center decides that too many logs are generated and suppresses its log processing rate by processing only the conforming traffic (logs within the threshold) and discarding the non-conforming traffic (logs exceeding the threshold). When the number of logs that are generated every second under the same log ID falls below the threshold and remains below the threshold for five monitoring periods, the information center removes the suppression.

By default, the information center processes a maximum of 30 logs with the same log ID in every second. In certain application scenarios, by default, the information

center needs to process more than 50 logs with the same log ID in every second. You can set thresholds for logs with different log IDs. Generally, the default threshold is recommended.

- If the threshold is too low, some logs may be discarded.
- If the threshold is too high, the information center cannot identify the log ID under which too many logs are generated.

NOTE

- If the threshold *value1* specified by the parameter **byinfoid** *infoID* or **bymodule-alias** *modname alias* differs from the threshold *value0* specified globally, *value1* takes effect.
- During a software upgrade, if the threshold is configured in the old version, but the new version does not support the specified log module and alias, the threshold configuration of the specified log module and alias will be automatically cleared after the upgrade.

Example

Set the maximum number of logs that the information center can process every second to 60.

```
<HUAWEI> system-view
[HUAWEI] info-center rate-limit threshold 60
```

Set the maximum number of logs identified by the same module name and mnemonic that the information center can process every second to 30.

```
<HUAWEI> system-view
[HUAWEI] info-center rate-limit threshold 30 bymodule-alias AAA AUTHEN_ERR_EVENT
```

Set the maximum number of logs with the same log ID that the information center can process every second to 20.

```
<HUAWEI> system-view
[HUAWEI] info-center rate-limit threshold 20 byinfoid ff011015
```

Restore the maximum number of logs that the information center can process every second to the default value.

```
<HUAWEI> system-view
[HUAWEI] undo info-center rate-limit threshold
```

Cancel the restriction on the maximum number of logs with a specified log ID that the information center can process every second.

```
<HUAWEI> system-view
[HUAWEI] undo info-center rate-limit threshold bymodule-alias AAA AUTHEN_ERR_EVENT
```

3.10.32 info-center session log disable

Function

The **info-center session log disable** command disables the user session logging function.

The **undo info-center session log disable** command enables the user session logging function.

By default, the user session logging function is enabled.

Format

info-center session log disable

undo info-center session log disable

Parameters

None

Views

System view

Level

3: Management level

Usage Guidelines

Usage Scenario

The user session logging function saves the user input, device screen output, and time when the device executes the commands entered by users to a session log file. If the device becomes faulty or services become abnormal, you can obtain the user operation records from the saved session log file for fault location.

A session log file is generated in each VTY window and named cli_channel name.log, for example: **cli_vty1.log**. The generated session log files are stored in the sessionlog directory. The file size cannot exceed 1 MB.

If the number of session log files exceed the maximum value 20 (cannot be changed), the system compresses the files into .zip files. The compressed file is named cli_slot ID_timestamp_channel name_host name.log.zip, for example: **cli_11_20171129081148_vty1_huawei.log.zip**.

If the remaining device space is less than 30 MB, the system deletes the earliest log files until the remaining device space is more than 30 MB.

Precautions

Using the **undo info-center enable** or **info-center disable** command disables the information center will not affect the user session logging function. This function can only be enabled or disabled using the **undo info-center session log disable** or **info-center session log disable** command.

Example

Disable the user session logging function.

```
<HUAWEI> system-view
[HUAWEI] info-center session log disable
```

3.10.33 info-center source channel

Function

The **info-center source channel** command configures a rule for outputting information to a channel.

The **undo info-center source channel** command deletes the rules for outputting information to a channel.

The following lists the default rule for outputting information to a channel.

Table 3-160 Default rule for outputting information to a channel

Output Channel	Module Enabled to Output Information	Log		Trap		Debugging Message	
		Status	Lowest Output Severity	Status	Lowest Output Severity	Status	Lowest Output Severity
0 (console)	default	on	warning	on	debugging	on	debugging
1 (remote terminal)	default	on	warning	on	debugging	on	debugging
2 (log host)	default	on	informational	on	debugging	off	debugging
3 (trap buffer)	default	off	informational	on	debugging	off	debugging
4 (log buffer)	default	on	warning	off	debugging	off	debugging
5 (SNMP agent)	default	Not supported	Not supported	on	debugging	Not supported	Not supported
6 (channel 6)	default	on	debugging	on	debugging	off	debugging
7 (channel 7)	default	on	debugging	on	debugging	off	debugging
8 (channel 8)	default	on	debugging	on	debugging	off	debugging
9 (channel 9)	default	on	debugging	on	debugging	off	debugging

Format

info-center source { *module-name* | **default** } **channel** { *channel-number* | *channel-name* } [**log** { **state** { **off** | **on** } | **level** *severity* } * | **trap** { **state** { **off** | **on** } | **level** *severity* } * | **debug** { **state** { **off** | **on** } | **level** *severity* } *] *

undo info-center source { *module-name* | **default** } **channel** { *channel-number* | *channel-name* }

Parameters

Parameter	Description	Value
module-name	Specifies the module name.	Enumerated type. The value depends on the registered module.
default	Indicates the default module.	-
channel-number	Specifies the number of a channel.	The value is an integer that ranges from 0 to 9.
channel-name	Specifies the name of a channel.	The value is a string of 1 to 30 case-insensitive characters. The value consists of letters or numbers and must start with a letter.
log { **state** { **off** | **on** } }	Specifies the log status. • **off**: Logs are not sent. • **on**: Logs are sent. **NOTE** This field does not take effect for diagnostic logs.	-

Parameter	Description	Value
log { **level** *severity* }	Specifies the lowest severity of output logs. **NOTE** This field does not take effect for diagnostic logs.	Logs are classified into eight severities. The following severities are listed in descending order of priority: ● emergencies ● alert ● critical ● error ● warning ● notification ● informational ● debugging
trap { **state** { **off** | **on** } }	Specifies the trap status: ● **off**: Traps are not sent. ● **on**: Traps are sent.	-
trap { **level** *severity* }	Specifies the lowest severity of output traps.	Traps are classified into eight severities. The following severities are listed in descending order of priority: ● emergencies ● alert ● critical ● error ● warning ● notification ● informational ● debugging
debug { **state** { **off** | **on** } }	Specifies the debugging message status. ● **off**: Debugging messages are not sent. ● **on**: Debugging messages are sent.	-

Parameter	Description	Value
debug { **level** *severity* }	Specifies the lowest severity of output debugging messages.	Debugs are classified into eight severities. The following severities are listed in descending order of priority: • emergencies • alert • critical • error • warning • notification • informational • debugging

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

To collect and query information generated on the Switch, define severities for various types of information that is output to different channels. You can run the **info-center source channel** command to configure a rule for outputting information to a channel.

The following lists information severities.

Table 3-161 Information severities

Value	Severity	Description
0	emergencies	A fault causes the device to fail to run normally unless it is restarted. For example, the device is restarted because of program exceptions or a memory error is detected.
1	alert	A fault needs to be rectified immediately. For example, memory usage of the system reaches the upper limit.

Value	Severity	Description
2	critical	A fault needs to be analyzed and processed. For example, the memory usage falls below the lower threshold; temperature falls below the alarm threshold; BFD detects that a device is unreachable or detects locally generated error messages.
3	error	An improper operation is performed or exceptions occur during service processing. The fault does not affect services but needs to be analyzed. For example, users enter incorrect commands or passwords; error protocol packets are received from other devices.
4	warning	Some events or operations may affect device running or cause service processing faults, which requires full attention. For example, a routing process is disabled; BFD detects packet loss; error protocol packets are detected.
5	notification	A key operation is performed to keep the device running normally. For example, the **shutdown** command is run; a neighbor is discovered; protocol status changes.
6	informational	A normal operation is performed. For example, a **display** command is run.
7	debugging	A normal operation is performed, which requires no attention.

Precautions

Each information channel has a default record with the module name **default**. The default configuration for logs, traps, and debugging messages in different channels may differ.

If a module generates a large number of logs, traps, or debugging messages in a short time, use the following methods to suppress this information:

- Specify **level** *severity* to adjust the channel level. Information with lower severity will be filtered.
- Specify **state off** to disable information sent by a specified module.

NOTICE

After the lowest severity of output information is specified, information lower than the severity will be filtered.

Example

Enable the device to send debugging messages of the CFM module through the log host channel, and set the lowest severity of output debugging messages to warning.

```
<HUAWEI> system-view
[HUAWEI] info-center source CFM channel loghost debug level warning
```

3.10.34 info-center statistic-suppress enable

Function

The **info-center statistic-suppress enable** command enables suppression of statistics about consecutive repeated logs.

The **undo info-center statistic-suppress enable** command disables suppression of statistics about consecutive repeated logs.

The **info-center statistic-suppress disable** command disables suppression of statistics about consecutive repeated logs.

By default, suppression of statistics about consecutive repeated logs is enabled.

Format

info-center statistic-suppress enable

undo info-center statistic-suppress enable

info-center statistic-suppress disable

Parameters

None

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

In the system, service modules generate logs and control the volume of generated logs. The information center processes the received logs.

A large number of repeated logs are generated in a short time in some scenarios, for example, when ARP and VRRP are enabled. This wastes both the storage space and CPU resources. Generally, users do not want to view the repeated logs. You can run the **info-center statistic-suppress enable** command to suppress statistics on consecutive repeated logs so that the system can still record other logs.

NOTE

Logs that are generated consecutively and with the identical log ID and parameters can be regarded as repeatedly generated logs.

Precautions

Statistics about repeatedly generated logs are first output at the 30th seconds from the time the first log is output, and then statistics about repeatedly generated logs are output at the 120th seconds. After being output two times, statistics about repeatedly generated logs are output every 600 seconds.

By default, once receiving a log, the information center outputs the log. If the information center receives repeatedly generated logs within a period, it outputs the number of these logs and will output logs only when it receives a new log (a log with a different log ID). For example, a module sends logs to the information center in the sequence of A1(T1) A2(T2) A3(T2) B1(T3) B2(T4) B3(T4) C1(T5) C2(T6) A4(T7) B4(T8) B5(T8) B5(T8) B7(T9) A5(T9) B8(T10) D1(T11) A6(T11) A7(T12) A8(T12) A9(T13) A10(T14) A11(T15) A12(T16) A13(T17) A14(T18) B9(T18). A1 to A14 are the same; B1 to B9 are the same; C1, C2 and D1 are different from others; T1 to T18 are sequence numbers. The log information output by the information center is as follows:

```
T1:A1
T3(1): last message repeated 2 times
T3:B1
T5: last message repeated 2 times
T5:C1
T6:C2
T7:A4
T8:B4
T9(1): last message repeated 3 times
T9:A5
T10:B8
T11:D1
T11:A6
T13(2): last message repeated 3 times
T18(2): last message repeated 5 times
T18:B9
```

Logs of the service module received by the information center show that:

- Statistics about repeatedly generated logs are output when either of the following conditions is met:
  - The next log is a different log, as shown in **(1)**.
  - The time period (every 30 seconds, 120 seconds, and 600 seconds) for outputting log statistics expires, as shown in **(2)**.
- Each time the statistics are output, the service module clears the count and starts counting again. For example, during the period from T11 to T18, log A is generated 9 times.
- The information center outputs logs in the same sequence the logs are generated, making the trace of information and scenario easy.

NOTE

Logs with the sequence being A B A B A B A B are alternate logs; therefore, the **info-center statistic-suppress enable** command is unable to suppression the statistics about these logs.

Example

Disable suppression of statistics about consecutive repeated logs.

```
<HUAWEI> system-view
[HUAWEI] undo info-center statistic-suppress enable
```

3.10.35 info-center timestamp

Function

The **info-center timestamp** command sets the timestamp format of logs, traps, and debugging messages.

The **undo info-center timestamp** command restores the default timestamp format of logs, traps, and debugging messages.

By default, the **date** timestamp is used in traps, logs and debugging messages. Debugging messages are accurate to milliseconds, and traps and logs are accurate to seconds.

Format

info-center timestamp { **debugging** | **log** | **trap** } { { **date** | **format-date** | **short-date** } [**precision-time** { **second** | **tenth-second** | **millisecond** }] | **boot** } [**without-timezone**]

undo info-center timestamp { **debugging** | **trap** | **log** }

Parameters

Parameter	Description	Value
debugging	Indicates debugging messages.	-
log	Indicates logs.	-
trap	Indicates traps.	-
boot	Indicates that the timestamp is expressed in the format of relative time, a period of time since the start of the system. The format is xxxxxx.yyyyyy. xxxxxx is the higher order 32 bits of the milliseconds elapsed since the start of the system; yyyyyy is the lower order 32 bits of the milliseconds elapsed since the start of the system.	-
date	Specifies the current date and time. It is expressed in mm dd yyyy hh:mm:ss format.	-
short-date	Indicates the short date. This timestamp differs from **date** is that the year is not displayed.	-
format-date	Indicates that the timestamp is expressed in YYYY-MM-DD hh:mm:ss format.	-
precision-time	Specifies the precision.	-

Parameter	Description	Value
second	Indicates that the precision is accurate to seconds.	-
tenth-second	Indicates that the precision is accurate to 0.1 second.	-
millisecond	Indicates that the precision is accurate to milliseconds.	-
without-timezone	Specifies a timestamp to filter timezone information. **NOTE** If **without-timezone** is configured for logs, traps, or debug information, the log, trap, or debugging information sent to the log host does not carry time zone or DST information.	-

Views

System view

Default Level

3: Management level

Usage Guidelines

The **info-center timestamp** command sets the timestamp format of logs, traps, and debugging messages.

The following describes the timestamp in **date** format.

Table 3-162 Description of fields of the timestamp in **date** format

Field	Description	Value
mm	Month	The value can be Jan, Feb, Mar, Apr, May, Jun, Jul, Aug, Sep, Oct, Nov, or Dec.
dd	Date	1-31. If the date is smaller than 10, add a space in front of the date, For example, " 7".
yyyy	Year	4 digits
hh:mm:ss	Local time	hh ranges from 00 to 23, and mm or ss ranges from 00 to 59.

When the precision of the timestamp is accurate to 0.1 second or milliseconds, the system adds identifiers to the logs generated at the same time based on the sequence.

Prerequisites

The information center has been enabled by using the **info-center enable** command.

Example

Set the timestamp format of traps to **boot**.

```
<HUAWEI> system-view
[HUAWEI] info-center timestamp trap boot
```

Set the timestamp precision of logs, traps, and debugging messages.

```
<HUAWEI> system-view
[HUAWEI] info-center timestamp log date precision-time millisecond
[HUAWEI] info-center timestamp debugging date precision-time tenth-second
[HUAWEI] info-center timestamp trap date precision-time millisecond
```

3.10.36 info-center trapbuffer

Function

The **info-center trapbuffer** command enables the Switch to send traps to the trap buffer.

The **undo info-center trapbuffer** command disables the Switch from sending traps to the trap buffer.

By default, the Switch is enabled to send traps to the trap buffer.

Format

info-center trapbuffer

undo info-center trapbuffer

Parameters

None

Views

System view

Default Level

3: Management level

Usage Guidelines

To view traps in the trap buffer, run the **info-center trapbuffer** command to enable the Switch to send traps to the trap buffer.

The **info-center trapbuffer** command takes effect only after the information center function has been enabled using the **info-center enable** command.

Example

Enable the Switch to send traps to the trap buffer.

```
<HUAWEI> system-view
[HUAWEI] info-center trapbuffer
```


3.10.37 info-center trapbuffer size

Function

The **info-center trapbuffer size** command sets the maximum number of traps in the trap buffer.

The **undo info-center trapbuffer size** command restores the default maximum number of traps in the trap buffer.

By default, a trap buffer allows a maximum of 256 traps.

Format

info-center trapbuffer size *trapbuffer-size*

undo info-center trapbuffer size [*trapbuffer-size*]

Parameters

Parameter	Description	Value
trapbuffer-size	Specifies the maximum number of traps in the trap buffer.	The value is an integer that ranges from 0 to 1024. If *trapbuffer-size* is 0, traps are not displayed.

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

The **info-center trapbuffer size** command sets the maximum number of traps in the trap buffer.

Prerequisites

The Switch has been enabled to output traps to the trap buffer by using the **info-center trapbuffer** command.

Precautions

When you run the **info-center trapbuffer size** command multiple times, only the latest configuration takes effect.

If a small value of *trapbuffer-size* is used, some traps may be not displayed. If a large value of *trapbuffer-size* is used, repeated traps may be displayed. The default value of *trapbuffer-size* is recommended.

Example

Set the maximum number of traps in the trap buffer to 30.

```
<HUAWEI> system-view
[HUAWEI] info-center trapbuffer size 30
```

3.10.38 log restrain disable

Function

The **log restrain disable** command disables log restrainion.

The **undo log restrain disable** command enables log restrainion.

By default, log restrainion is enabled.

Format

log restrain disable

undo log restrain disable

Parameters

None

Views

System view

Default Level

3: Management level

Usage Guidelines

When a large number of logs are generated, device resources are wasted, affecting system performance. To prevent this problem, enable log restrainion.

Example

Disable log restrainion.

```
<HUAWEI> system-view
[HUAWEI] log restrain disable
```

3.10.39 log restrain threshold

Function

The **log restrain threshold** command sets the maximum number of logs that can be generated per minute.

The **undo log restrain threshold** command restores the default setting.

By default, a maximum of 200 logs can be generated per minute.

Format

log restrain threshold *threshold-value* [**infoid** *infoid-value* **description** *description-str*]

undo log restrain threshold [**infoid** *infoid-value*]

Parameters

Parameter	Description	Value
threshold-value	Specifies the maximum number of logs that can be generated per minute.	The value is an integer that ranges from 10 to 50000.
infoid *infoid-value*	Specifies a log ID. If this parameter is specified, *threshold-value* specifies the maximum number of logs with the specified ID that can be generated per minute. If this parameter is not specified, *threshold-value* specifies the maximum number of logs that can be generated globally on the device per minute.	The value is a 32-digit hexadecimal number in the format XXXXXXXX. It ranges from 0 to ffffffff.
description *description-str*	Specifies the description of the log with the sepecified ID.	The value is a string of 1 to 32 case-insensitive characters without spaces.

Views

System view

Default Level

3: Management level

Usage Guidelines

After log restrainion is enabled, if the number of logs generated per minute exceeds the specified threshold, excess logs are discarded.

You can run the **display log restrain all** command to check the configuration of the log suppression function. If the value of **MaxCount** in the command output is **NotLimit**, the log of the corresponding ID is not suppressed.

Example

Set the maximum number of logs that can be generated globally on the device per minute to 100.

```
<HUAWEI> system-view
[HUAWEI] log restrain threshold 100
```

3.10.40 reset info-center statistics

Function

The **reset info-center statistics** command clears statistics on each module.

Format

reset info-center statistics

Parameters

None

Views

User view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

To re-collect statistics on each module, run the **reset info-center statistics** command to clear all historical statistics.

Precautions

The cleared statistics cannot be restored. Exercise caution when you run the **reset info-center statistics** command.

Example

Clear statistics on each module.

```
<HUAWEI> reset info-center statistics
```

3.10.41 reset logbuffer

Function

The **reset logbuffer** command clears logs in the log buffer.

Format

reset logbuffer

Parameters

None

Views

User view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

To record logs in the log buffer again, run the **reset logbuffer** command to clear all the information in the log buffer.

Precautions

Statistics cannot be restored after being cleared. Exercise caution when you run the **reset logbuffer** command.

Example

Clear information in the log buffer.

```
<HUAWEI> reset logbuffer
Warning: This command will reset the log buffer. Logs in the buffer will be lost. Continue? [Y/N]:y
```

3.10.42 reset log restrain statistics

Function

The **reset log restrain statistics** command clears all log suppression statistics.

Format

reset log restrain statistics

Parameters

None

Views

All views

Default Level

3: Management level

Usage Guidelines

To clear all log suppression statistics, run this command.

Example

Clear all log suppression statistics.

```
<HUAWEI> reset log restrain statistics
```

3.10.43 reset trapbuffer

Function

The **reset trapbuffer** command clears Trap information in the trap buffer.

Format

reset trapbuffer

Parameters

None

Views

User view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

To record traps in the trap buffer again, run the **reset trapbuffer** command to clear all the information in the trap buffer.

Precautions

Statistics cannot be restored after being cleared. Exercise caution when you run the **reset trapbuffer** command.

Example

Clear information in the trap buffer.

```
<HUAWEI> reset trapbuffer
```


3.10.44 save logfile

Function

The **save logfile** command saves logs in the user log file buffer to a user log file.

Format

save logfile

Parameters

None

Views

User view

Default Level

3: Management level

Usage Guidelines

The system periodically saves log information in the user log buffer to a user log file. If the log buffer becomes full within the log saving interval, the system immediately saves logs to the user log file. To view the current logs, run the **save logfile** command to save the logs to the user log file.

When you run this command, the device obtains or uses some personal data of users, such as the STA MAC address. Delete the personal data immediately after the command is executed to ensure user data security.

Example

Save logs in the user log file buffer to the user log file.

```
<HUAWEI> save logfile
Info: Save logfile successfully.
```

3.10.45 save logfile all

Function

The **save logfile all** command saves the logs in the user log buffer area and diagnostic log buffer area to the user log file and diagnostic log file, respectively.

Format

save logfile all

Parameters

None

Views

User view

Default Level

3: Management level

Usage Guidelines

The logs in the user log buffer area and diagnostic log buffer area are periodically saved to the user log file and diagnostic log file, respectively. The log saving interval varies with the product. To save the logs in the user log buffer area and diagnostic log buffer area to the user log file and diagnostic log file, respectively, run the **save logfile all** command.

A user log file is saved in a log directory (for example, the **log** or **logfile** directory) and named in the **log.log** format.

A diagnostic log file is saved in a log directory (for example, the **log** or **logfile** directory) and named in the **log.dblg** format.

Example

Save the logs in the user log buffer area and diagnostic log buffer area to the user log file and diagnostic log file, respectively.

```
<HUAWEI> save logfile all
Info: Save logfile successfully.
Info: Save diagnostic logfile successfully.
```

3.10.46 terminal debugging

Function

The **terminal debugging** command enables debugging message display on the user terminal.

The **undo terminal debugging** command disables debugging message display on the user terminal.

By default, debugging message display is disabled on the user terminal.

Format

terminal debugging

undo terminal debugging

Parameters

None

Views

User view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

You can run the **terminal debugging** command to enable debugging message display on the user terminal to view system debugging message and locate faults.

Prerequisites

The **terminal monitor** command has been executed to enable display of logs, traps, and debugging message output on the user terminal.

Example

Enable debugging message display on the user terminal.

```
<HUAWEI> terminal debugging
Info: Current terminal debugging is on.
```

3.10.47 terminal echo synchronous

Function

The **terminal echo synchronous** command enables a terminal to display debugging, log, or trap information synchronously.

The **undo terminal echo synchronous** command disables a terminal from displaying debugging, log, or trap information synchronously.

By default, a terminal displays debugging, log, and trap information asynchronously.

Format

terminal echo synchronous [**level** { *severity* | **all** } | **size** *size-number*] *

undo terminal echo synchronous

Parameters

Parameter	Description	Value
level *severity*	Specifies an information severity.	The value is an integer ranging from 0 to 7. The default value is **0**. The information center classifies information into the following severities: • 0: emergency • 1: alert • 2: critical • 3: error • 4: warning • 5: notice • 6: informational • 7: debug A smaller value indicates a higher severity. The information with a severity higher than a specified severity is displayed asynchronously.
all	Displays information of all severities.	–
size *size-number*	Specifies the total number of debugging, log, and trap records.	The value is an integer ranging from 1 to 1024. The default value is **512**.

Views

User view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

When a device generates debugging, log, or trap information, the information queues in the device process and is sent to a terminal sequentially. This output is called a synchronous output.

A synchronous output provides effectively organized output information, improving user experience. In asynchronous output mode, multiple types of

information interlaces, which brings poor readability. An asynchronous output allows you to promptly obtain debugging and diagnosis information and therefore applies to debugging and diagnosis scenarios.

You can run the **terminal echo synchronous** command to enable a synchronous output on a terminal, facilitating subsequent operations.

- When you enter a command, the entered command content is displayed after debugging, log, or trap information is displayed. This function is enabled by default. After a synchronous output is disabled, this function is still supported.
- When no command is entered, the command prompt is displayed after debugging, log, or trap information is displayed. This function is enabled by default. After a synchronous output is disabled, this function is still supported.
- When a command is being run, no debugging, log, or trap information is displayed. After the command is run, debugging, log, or trap information is displayed.
- When you enter **Y** for the message "Are you sure to continue?[Y/N]," the **[Y/N]:** prompt is displayed after debugging, log, or trap information is displayed.
- When you enter the More phase, the **More** prompt is displayed after debugging, log, or trap information is displayed.
- If you run a command, for example, for decompressing or saving a file, the terminal does not display output information until the operation is complete. This process ensures monitoring continuity.

Prerequisites

- Terminal display has been enabled using the **terminal monitor** command.
- The terminal has been enabled to display debugging, log, or trap information using the **terminal debugging**, **terminal logging**, or **terminal trapping** command.

Example

Enable a terminal to display debugging information synchronously.

```
<HUAWEI> terminal monitor
Info: Current terminal monitor is on.
<HUAWEI> terminal debugging
Info: Current terminal debugging is on.
<HUAWEI> terminal echo synchronous
Info: Current terminal synchronization is on.
<HUAWEI> save
The current configuration will be written to the device.
Are you sure to continue?[Y/N]:
Aug 23 2012 12:04:37.790.2 huawei VTY/7/Debug_Stat:
 (0)VTY ACCEPT BEGIN !
Aug 23 2012 12:04:37.790.3 huawei VTY/7/Debug_Stat:
 (1)SOCKET ACCEPT OK !
Aug 23 2012 12:04:37.790.4 huawei VTY/7/Debug_Stat:
 (2)FIND LINE INDEX OK !
[Y/N]:
```


3.10.48 terminal logging

Function

The **terminal logging** command enables log display on the user terminal.

The **undo terminal logging** command disables log display on the user terminal.

By default, log display is enabled on the user terminal.

Format

terminal logging

undo terminal logging

Parameters

None

Views

User view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

To view logs on a terminal, run the **terminal logging** command to enable log display on the user terminal.

Prerequisites

The **terminal monitor** command has been executed to enable display of logs, traps, and debugging message output on the user terminal.

Example

Disable log display on the user terminal.

```
<HUAWEI> undo terminal logging
Info: Current terminal logging is off.
```

3.10.49 terminal monitor

Function

The **terminal monitor** command enables display of logs, traps, and debugging message output by the information center on the user terminal.

The **undo terminal monitor** command disables display of logs, traps, and debugging message output by the information center on the user terminal.

By default, console display is enabled and terminal display is disabled.

Format

terminal monitor

undo terminal monitor

Parameters

None

Views

User view

Default Level

3: Management level

Usage Guidelines

Prerequisites

The information center has been enabled by using the **info-center enable** command.

Follow-up Procedure

Run the **terminal debugging**/**undo terminal debugging**, **terminal logging**/**undo terminal logging**, **terminal trapping**/**undo terminal trapping**/ command to enable or disable terminal debugging message, log, or trap display.

Precautions

Logs, traps, and debugging message are sent to the current terminal only when the **terminal monitor** command is used.

Running the **undo terminal monitor** command is equivalent to running the **undo terminal debugging**, **undo terminal logging**, **undo terminal trapping** command.

Example

Disable display of logs, traps, and debugging message output by the information center on the user terminal.

```
<HUAWEI> undo terminal monitor
Info: Current terminal monitor is off.
```

3.10.50 terminal session-log disable

Function

The **terminal session-log disable** command disables the session logging function for an online user.

The **undo terminal session-log disable** command enables the session logging function for an online user.

By default, the session logging function for an online user is enabled.

Format

terminal session-log disable

undo terminal session-log disable

Parameters

None

Views

User view

Level

1: Monitoring level

Usage Guidelines

Usage Scenario

The session logging function for an online user stores the user input, device output, and time when the device executes user-issued commands to a session log file.

Prerequisites

The session logging function has been enabled globally.

Example

Enable the session logging function for an online user.

```
<HUAWEI> undo terminal session-log disable
```

3.10.51 terminal trapping

Function

The **terminal trapping** command enables trap display on the user terminal.

The **undo terminal trapping** command disables trap display on the user terminal.

By default, trap display is enabled on the user terminal.

Format

terminal trapping

undo terminal trapping

Parameters

None

Views

User view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

To view traps on a terminal, run the **terminal trapping** command to enable trap display on the user terminal.

Prerequisites

The **terminal monitor** command has been executed to enable display of logs, traps, and debugging message output on the user terminal.

Example

Disable trap display on the user terminal.

```
<HUAWEI> undo terminal trapping
Info: Current terminal trapping is off.
```

3.11 Fault Management Commands

3.11.1 Command Support

Commands provided in this section and all the parameters in the commands are supported by all switch models (except the S5731-L and S5731S-L), unless otherwise specified. For details, see specific commands.

3.11.2 alarm (system view)

Function

Using the **alarm** command, you can enter the alarm view.

Format

alarm

Parameters

None

Views

System view

Default Level

3: Management level

Usage Guidelines

After running the **alarm** command to enter the alarm view, you can configuration alarm management functions.

Example

Enter the alarm view.

```
<HUAWEI> system-view
[HUAWEI] alarm
[HUAWEI-alarm]
```

3.11.3 alarm-name severity

Function

The **alarm-name severity** command sets the severity for an alarm.

The **undo alarm-name severity** command restores the default setting.

By default, each alarm has a default severity.

Format

alarm-name *alarm-name* **severity** *severity*

undo alarm-name *alarm-name* **severity**

Parameters

Parameter	Description	Value
alarm-name	Specifies the registered alarm name.	The value is a string and varies according to the registered device type. To view registered alarm information, run the **display alarm information** command.

Parameter	Description	Value
severity *severity*	Specifies the alarm severity.	The value is of enumerated type. Alarms are classified into the following severities: • **critical**: indicates that a fault affecting services has occurred and it must be rectified immediately. • **major**: indicates that services are being affected and related measures need to be taken urgently. • **minor**: indicates that a fault occurs but does not affect services. To avoid more serious faults that affect services, related measures must be taken. • **warning**: indicates that a potential or impending service-affecting fault is detected before any significant effect has been felt. Take corrective actions to diagnose and rectify the fault. • **indeterminate**: indicates that the alarm severity cannot be determined. • **cleared**: indicates one or more previous alarm conditions have been cleared.

Views

Alarm view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

You can run the **alarm-name severity** command to raise or lower the level of an alarm based on the severity and emergency of the alarm. However, the level of a clear alarm cannot be changed unless during the configuration restoration period. You can configure filtering conditions to allow the NMS to receive only alarms of specified alarm severity.

Precautions

The default severity of each alarm is different. To view the default severity of an alarm, run the **undo alarm-name severity** and **display alarm information** commands in sequence.

Example

Set the severity of the hwSysSlaveHDError alarm to warning.

```
<HUAWEI> system-view
[HUAWEI] alarm
[HUAWEI-alarm] alarm-name hwSysSlaveHDError severity warning
```

3.11.4 clear alarm active

Function

The **clear alarm active** command clears active alarms.

Format

clear alarm active { **all** | **sequence-number** *sequence-number* }

Parameters

Parameter	Description	Value
all	Clears all active alarms.	-
sequence-number *sequence-number*	Specifies the sequence number of an active alarm.	The value is an integer ranging from 1 to 2147483647.

Views

Alarm view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

Before collecting statistics on alarms generated on the device again, run the **clear alarm active** to clear active alarms.

Precautions

After the **clear alarm active** command is used, all active alarms on the device are deleted and cannot be restored.

Example

Clear all active alarms on the device.

```
<HUAWEI> system-view
[HUAWEI] alarm
[HUAWEI-alarm] clear alarm active all
```

3.11.5 clear alarm manual-clear

Function

The **clear alarm manual-clear** command clears the active alarms that are not reported repeatedly so that these active alarms can be reported again.

Format

clear alarm manual-clear { **all** | **sequence-number** *sequence-number* }

Parameters

Parameter	Description	Value
all	Specifies all the active alarms that are not reported repeatedly.	-
sequence-number *sequence-number*	Specifies the sequence number of the active alarm that is not reported repeatedly. You can run **display alarm manual-clear** get the sequence number of the active alarm.	The value is an integer that ranges from 1 to 2147483647.

Views

Alarm management view

Default Level

3: Management level

Usage Guidelines

After the **mask manual-clear alarm** command is executed to prevent manually cleared active alarms from being reported repeatedly and then the **clear alarm**

active command or MIB table hwAlarmActiveTable is used to manually clear active alarms, active alarms will not be reported repeatedly. To view the active alarms that are not reported repeatedly, run the **clear alarm manual-clear** command.

To ensure that the active alarms that are not reported repeatedly can be reported again, run the **clear alarm manual-clear** command. After the **clear alarm manual-clear** command is executed, running the **display alarm manual-clear** command does not display corresponding alarm information.

Example

Clear the active alarms that are not reported repeatedly.

```
<HUAWEI> system-view
[HUAWEI] alarm
[HUAWEI-alarm] clear alarm manual-clear all
```

3.11.6 clear event all

Function

The **clear event all** command clears events on the device.

Format

clear event all

Parameters

None

Views

Event view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

Before collecting statistics on events generated on the device again, run the **clear event all** to clear events.

Precautions

NOTICE

The **clear event all** command clears events on the device and cleared events cannot be restored.

Example

Clear events on the device.

```
<HUAWEI> system-view
[HUAWEI] event
[HUAWEI-event] clear event all
```

3.11.7 clear record device-alarm

Function

The **clear record device-alarm** command clears hardware alarms.

Format

clear record device-alarm [**all** | **slot** *slot-id*]

Parameters

Parameter	Description	Value
all	Clears all hardware alarms of the device.	-
slot *slot-id*	Specifies a slot ID.	The value depends on the device configuration.

Views

User view

Default Level

3: Management level

Usage Guidelines

When current hardware alarms are not required on the device, use the **clear record** command to clear the hardware alarms of the device.

Example

Clear all hardware alarms of the device.

```
<HUAWEI> clear record device-alarm all
```

3.11.8 delay-suppression enable

Function

The **delay-suppression enable** command enables delayed alarm or event reporting.

The **undo delay-suppression enable** command disables delayed alarm or event reporting.

By default, delayed reporting is enabled.

NOTE

Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S support this command.

Format

delay-suppression enable

undo delay-suppression enable

Parameters

None

Views

Alarm view or event view

Default Level

3: Management level

Usage Guidelines

In the event that an alarm or an event is repeatedly generated, you can enable delayed reporting to prevent a large number of repeated alarms or events from being reported to the NMS. You can choose to enable or disable delayed reporting:

- Run the **delay-suppression enable** command to enable delayed reporting.
- Run the **undo delay-suppression enable** command to disable delayed reporting.

Run the **delay-suppression enable** command in the alarm view to enable delayed alarm reporting. Run the **delay-suppression enable** command in the event view to enable delayed event reporting.

Example

Enable delayed alarm reporting.

```
<HUAWEI> system-view
[HUAWEI] alarm
[HUAWEI-alarm] delay-suppression enable
```

3.11.9 display alarm active

Function

The **display alarm active** command displays active alarms on the device.

Format

display alarm active

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display alarm active** command to view active alarms on the device to locate faults.

Example

Display active alarms on the device.

```
<HUAWEI> display alarm active
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)

  92/Independent/2019-08-09 10:44:58/-/0x502001/linkDown/Critical/Start/OID 1.3.6.1.6.3.1.1.5.3 Interface
58 turned into DOWN state.
(AdminStatus=1,OperStatus=2,InterfaceName=40GE0/0/5)
```

Table 3-163 Description of the display alarm active command output

Item	Description
A/B/C/D/E/F/G/H/I/J	Alarm display format
A=Sequence	Sequence number
B=RootKindFlag(Independent|RootCause|nonRootCause)	Flag indicating a root-cause alarm or a non-root-cause alarm: • Independent: indicates an alarm for which alarm correlation analysis is not performed. • RootCause: indicates a root-cause alarm. • nonRootCause: indicates a non-root-cause alarm.

Item	Description
C=Generating time	Time when an alarm is generated
D=Clearing time	Time when an alarm is cleared
E=ID	Alarm ID
F=Name	Alarm name
G=Level	Alarm severity level You can run the **alarm-name severity** command to set this parameter.
H=State	Alarm status: • Start • End
I=Description information for locating(Para info, Reason info)	Alarm description including alarm parameters and causes for triggering alarms
J=RootCause alarm sequence(Only for nonRootCause alarm)	Sequence number of the root-cause alarm (for non-root-cause alarms only)

3.11.10 display alarm history

Function

The **display alarm history** command displays historical alarms on the device.

Format

display alarm history

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display alarm history** command to view the alarms that are cleared or generated on the device. The **display alarm history** command displays a maximum of 300 alarm history records.

Example

Display historical alarms on the device.

```
<HUAWEI> display alarm history
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)

  3/Independent/2010-07-14 09:40:20-08:00/2010-07-14 09:40:23-08:00/0x502001/linkDown/
Critical/End/OID 1.3.6.1.6.3.1.1.5.3 Interface 5 turned into DOWN state.
```

Table 3-164 Description of the display alarm history command output

Item	Description
A/B/C/D/E/F/G/H/I/J	Alarm display format
A=Sequence	Sequence number
B=RootKindFlag(Independent|RootCause|nonRootCause)	Flag indicating a root-cause alarm or a non-root-cause alarm: • Independent: indicates an alarm for which alarm correlation analysis is not performed. • RootCause: indicates a root-cause alarm. • nonRootCause: indicates a non-root-cause alarm.
C=Generating time	Time when an alarm is generated
D=Clearing time	Time when an alarm is cleared
E=ID	E=ID
F=Name	Alarm ID
G=Level	Alarm severity level You can run the **alarm-name severity** command to set this parameter.

Item	Description
H=State	Alarm status: • Start • End
I=Description information for locating(Para info, Reason info)	Alarm description including alarm parameters and causes for triggering alarms
J=RootCause alarm sequence(Only for nonRootCause alarm)	Sequence number of the root-cause alarm

3.11.11 display alarm information

Function

The **display alarm information** command displays alarm configurations.

Format

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

Parameters

Parameter	Description	Value
name *alarm-name*	Displays the configuration of a specified alarm. If this parameter is not set, configurations of all alarms are displayed.	The value is a string and varies according to the registered device type.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

To view alarm configurations on the device, run the **display alarm information** command.

If no alarm name is specified, information about all alarms in the system will be displayed.

In addition, to change the severity level of an alarm, you can run the **alarm-name** *alarm-name* **severity** *severity* command.

Example

Display the configuration of the alarm named linkUp.

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

Table 3-165 Description of the display alarm information command output

Item	Description
AlarmName	Name of an alarm.
AlarmType	Alarm type: • Alarm: indicates a fault occurs. • Resume Alarm: indicates a fault is rectified.
AlarmLevel	Alarm severity. To set this parameter, run the **alarm-name severity** command.
Suppress Period	Alarm reporting delay. To set this parameter, run the **suppression alarm-name** command. If this field displays **NA**, this alarm does not support the delayed alarm reporting function.
CauseAlarmName	Name of the root-cause alarm. Name of the root-cause alarm, namely, paired alarm name.
Match VB Name	Matching content of paired alarms.

3.11.12 display alarm manual-clear

Function

The **display alarm manual-clear** command displays the alarms that are not reported repeatedly after being cleared.

Format

display alarm manual-clear

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After the **mask manual-clear alarm** command is executed to prevent manually cleared active alarms from being reported repeatedly and then the **clear alarm active** command or MIB table hwAlarmActiveTable is used to manually clear active alarms, you can run the **display alarm manual-clear** command to view the active alarms that are not reported repeatedly after being cleared.

Example

Display the alarms that are not reported repeatedly after being cleared.

```
<HUAWEI> display alarm manual-clear
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)

  2/Independent/2016-05-04 10:38:46-08:00/-/0xff14280c/hwEntityOffline/Major/Start/ OID 1
.3.6.1.4.1.2011.5.25.129.2.1.13 Physical entity changed to the offline state. (E
ntityPhysicalIndex=16842752, BaseTrapSeverity=5, BaseTrapProbableCause=69120, Ba
seTrapEventType=5, EntPhysicalContainedIn=16777216, EntPhysicalName="LPU slot 1"
, RelativeResource="", ReasonDescription="Because of get offline message, the en
tity of SLOT1 changed to offline state")
```

Table 3-166 Description of the **display alarm manual-clear** command output

Item	Description
A/B/C/D/E/F/G/H/I/J	Alarm display format
A=Sequence	Alarm sequence number.

Item	Description
B=RootKindFlag(Independent|RootCause|nonRootCause)	Flag indicating a root-cause alarm or a non-root-cause alarm: • Independent: indicates an alarm for which alarm correlation analysis is not performed. • RootCause: indicates a root-cause alarm. • nonRootCause: indicates a non-root-cause alarm.
C=Generating time	Time when an alarm is generated.
D=Clearing time	Time when an alarm is cleared.
E=ID	Alarm ID.
F=Name	Alarm name.
G=Level	Alarm severity. To set this parameter, run the **alarm-name severity** command.
H=State	Alarm status: • Start • End
I=Description information for locating(Para info, Reason info)	Alarm description.
J=RootCause alarm sequence(Only for nonRootCause alarm)	Sequence number of a root-cause alarm (for non-root-cause alarms only)

3.11.13 display alarm urgent

Function

Using the **display alarm urgent** command, you can view hardware alarms on the device.

Format

display alarm urgent [**slot** *slot-id* | **time** *interval*]

Parameters

Parameter	Description	Value
slot *slot-id*	Specifies a slot ID.	The value depends on the device configuration.
time *interval*	Displays hardware alarms generated in the last period of time. *interval* specifies the period.	The value is an integer that ranges from 1 to 10000, in minutes.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can use the command to view hardware alarms, including alarms about the abnormality of the temperature, the fan, and the chip.

If no parameter is specified, the command displays all the hardware alarms.

Example

Display hardware alarms of the device.

```
<HUAWEI> display alarm urgent
 Alarm:

Alarm                 Slot     Date       Time(DST)     Location
------------------------------------------------------------------------------
Temp normal             1        2000/04/09  04:52:47     Slot 1
Temp low              1        2000/04/09  04:52:14     Slot 1
Temp normal             1        2000/04/09  04:39:05     Slot 1
Temp high             1        2000/04/09  04:37:23     Slot 1
Temp normal             2        2000/04/10  07:13:16     Slot 2
Temp high             2        2000/04/10  07:11:22     Slot 2
```


Table 3-167 Description of the display alarm urgent command output

Item	Description
Alarm	Details about an alarm. ● Fan pulled out: A fan module is removed. ● Fan plugged in: A fan module is installed. ● Fan abnormal: A fan module is not working properly. ● Fan normal: A fan module is working properly. ● Fan unmatched: A fan module does not match the device model. ● Fan matched: A fan module matches the device model. ● Power pulled out: A power module is removed. ● Power plugged in: A power module is installed. ● Power abnormal: A power module is not working properly. ● Power normal: A power module is working properly. ● PWR Input Vol Low: A power module is in an input power outage or undervoltage condition. ● PWR Input Vol Low Resume: A power module recovers from an input power outage or undervoltage condition. ● Built-in power Off: A built-in power module does not provide power. ● Built-in power On: A built-in power module provides power normally. ● Temp high: The temperature is too high. ● Temp low: The temperature is too low. ● Temp normal: The temperature returns to the normal range. ● Temp chip abnormal: A temperature sensor is faulty. ● Temp chip normal: A temperature sensor recovers from a failure. ● storage abnormal: The storage utilization exceeded 85%.
Slot	Slot ID of the device where alarms are generated.
Date	Date when alarms are generated.
Time(DST)	Time when alarms are generated.
Location	Position where alarms are generated.

3.11.14 display event

Function

The **display event** command displays events on the device.

Format

display event

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

To obtain the contents of events in the system, you can run the display event command.

Example

Display events on the device.

```
<HUAWEI> display event
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/2008-10-12 22:42:28-08:00/-/0x40812000/warmStart/Warning/Start/O
ID 1.3.6.1.6.3.1.1.5.2 warmStart
  2/Independent/2008-10-12 22:42:28-08:00/-/0x41132002/hgmpMemberStatusChange/Wa
rning/Start/OID:1.3.6.1.4.1.2011.6.7.1.0.3, DeviceID:0018-8201-0987, Role:17.
  3/Independent/2008-10-16 17:50:32-08:00/-/0x41b82000/hwCfgChgNotify/Warning/St
art/OID 1.3.6.1.4.1.2011.5.25.191.3.1 configurations have been changed. The curr
ent change number is 2, the change loop count is 0, and the maximum number of re
cords is 4095.
```

Table 3-168 Description of the display event command output

Item	Description
A/B/C/D/E/F/G/H/I/J	Event display format
A=Sequence	Sequence number of an event

Item	Description
B=RootKindFlag(Independent| RootCause| nonRootCause)	Flag indicating a root-cause alarm or a non-root-cause alarm (The value of this field is **Independent** for any event.)
C=Generating time	Time when the event is generated
D=Clearing time	Time when the event is cleared (for non-root-cause alarms only)
E=ID	Event ID
F=Name	Event name
G=Level	Event level
H=State	Event status: • Start • End
I=Description information for locating(Para info, Reason info)	Description of an event, including parameters of the event and the reason why the event was triggered.
J=RootCause alarm sequence(Only for nonRootCause alarm)	This parameter is valid only for alarms.

3.11.15 display event information

Function

The **display event information** command displays event configurations.

Format

display event information [**name** *event-name*]

Parameters

Parameter	Description	Value
name *event-name*	Displays the configuration of a specified event. If this parameter is not set, configurations of all events are displayed.	The value is a string and varies according to the registered device type.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

To view event configurations on the device, run the **display event information** command.

If no event name is specified, information about all events in the system will be displayed.

Example

Display registration information about the hwCfgManEventlog event.

```
<HUAWEI> display event information name hwCfgManEventlog
**********************************
  EventName: hwCfgManEventlog
  EventType: Critical Event
  EventLevel: Warning
  Suppress Period: NA
  Match VB Name: hwCfgLogSrcCmd hwCfgLogSrcData hwCfgLogDesData
**********************************
```

Table 3-169 Description of the display event information command output

Item	Description
EventName	Event name.
EventType	Event type.
EventLevel	Event level, which cannot be configured.
Suppress Period	Event report delay period. To set this parameter, run the **suppression event-name** command. If this field displays **NA**, this event does not support the delayed event reporting function.
Match VB Name	Matching content of repeated events.

3.11.16 event

Function

Using the **event** command, you can enter the event view.

Format

event

Parameters

None

Views

System view

Default Level

3: Management level

Usage Guidelines

After running the **event** command to enter the event view, you can configure event management functions.

Example

Enter the event view.

```
<HUAWEI> system-view
[HUAWEI] event
[HUAWEI-event]
```

3.11.17 mask manual-clear alarm

Function

The **mask manual-clear alarm** command prevents manually cleared active alarms from being reported repeatedly.

The **undo mask manual-clear alarm** command restores the default configuration.

By default, active alarms are reported repeatedly after being manually cleared.

Format

mask manual-clear alarm

undo mask manual-clear alarm

Parameters

None

Views

Alarm management view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

By default, after the **clear alarm active** command or MIB table hwAlarmActiveTable is used to manually clear active alarms, active alarms are reported repeatedly when being generated again. To prevent manually cleared active alarms from being reported repeatedly, run the **mask manual-clear alarm** command.

After the **mask manual-clear alarm** command is executed and then the **clear alarm active** command or MIB table hwAlarmActiveTable is used, cleared active alarms will not be reported repeatedly before clear alarms of active alarms are reported. To view all the active alarms that are not reported repeatedly, run the **display alarm manual-clear** command.

Precautions

Before the **mask manual-clear alarm** command is executed, the active alarms manually cleared using the **clear alarm active** command or MIB table hwAlarmActiveTable will be reported repeatedly.

Example

Prevent manually cleared active alarms from being reported repeatedly.

```
<HUAWEI> system-view
[HUAWEI] alarm
[HUAWEI-alarm] mask manual-clear alarm
```

3.11.18 reset alarm urgent

Function

The **reset alarm urgent** command clears all alarm messages.

Format

reset alarm urgent slot *slot-id*

Parameters

Parameter	Description	Value
slot *slot-id*	Specifies a slot ID.	The value depends on the device configuration.

Views

System view

Default Level

3: Management level

Usage Guidelines

You can run the **reset alarm urgent** command to clear all alarm messages. Confirm the action before you run this command.

Example

Clear all alarm messages of the device that slot id is 0.

```
<HUAWEI> system-view
[HUAWEI] reset alarm urgent slot 0
```

3.11.19 set alarm resend interval

Function

The **set alarm resend interval** command set the alarm reporting interval.

The **undo set alarm resend interval** command restores the default alarm reporting interval.

By default, the alarm interval is 10 minutes.

Format

set alarm resend interval *interval-value*

undo set alarm resend interval

Parameters

Parameter	Description	Value
interval-value	Specifies the alarm interval.	The value is an integer that ranges from 0 to 65535, in minutes.

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

The **set alarm resend interval** command sets the interval at which alarms are generated. If the periodic alarm reporting function is not required, set the interval to 0.

Precautions

If the alarm reporting interval is set to 0, the system does not report alarms periodically.

Example

Set the alarm reporting interval to 4 minutes.

```
<HUAWEI> system-view
[HUAWEI] set alarm resend interval 4
```

3.11.20 suppression alarm-name

Function

The **suppression alarm-name** command modifies a delay period after which a generated alarm is reported.

The **undo suppression alarm-name** command restores the configured delay period after which a generated alarm is reported.

By default, the system defines a delay period after which a generated alarm is reported. To view this default delay period, run the **undo suppression alarm-name** command and then the **display alarm information** command. If the **Suppress Period** field displays NA for an alarm, this alarm does not support the delayed alarm reporting function.

NOTE

Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S support this command.

Format

suppression alarm-name *alarm-name* { **cause-period** *cause-seconds* | **clear-period** *clear-seconds* }

undo suppression alarm-name *alarm-name* { **cause-period** | **clear-period** }

Parameters

Parameter	Description	Value
alarm-name	Specifies the name of an alarm for which the delay period is set.	The value cannot be the alarm name of which the **Suppress Period** field in the **display alarm information** command output displays NA.
cause-period *cause-seconds*	Specifies the period after which a generated alarm is reported.	The value is an integer ranging from 0 to 600, in seconds. If the value is set to 0s, the alarm management module sends the alarm to the NMS without any delay.
clear-period *clear-seconds*	Specifies the period after which a generated clear alarm is reported.	The value is an integer ranging from 0 to 600, in seconds. If the value is set to 0s, the alarm management module sends the alarm to the NMS without any delay.

Views

Alarm view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

If a certain alarm is repeatedly generated, you can enable delayed alarm reporting and set a period after which the alarm is reported to prevent the alarm from being reported during this period.

After the period is set for a certain alarm:

- If no clear alarm is generated during the period, the alarm is not reported to the NMS until the period expires.
- If a clear alarm is generated during this period, the alarm and its clear alarm are both deleted from the alarm queue and will not be reported to the NMS.

If the delay period is too short, alarm reporting is not efficiently delayed. If the delay period is too long, alarm reporting is postponed and the time when the fault occurs cannot be correctly obtained. For most alarms, the default delay period is recommended. For common alarms, such as alarms about hardware and environment, delayed alarm reporting is not recommended.

The value of **cause-period** *cause-seconds* is irrelevant to the value of **clear-period** *clear-seconds*. The delay in reporting an alarm and the delay in reporting a clear alarm can be configured separately.

Prerequisites

Before running the **suppression alarm-name** command, ensure that delayed alarm reporting has been enabled using the **delay-suppression enable** command.

Precautions

- If the delay period is changed when an alarm is being sent, the changed delay period takes effect on the next alarm to be sent.
- If *alarm-name* specifies an alarm, you can configure only **cause-period** *cause-seconds*. If it specifies a clear alarm, you can configured only **clear-period** *clear-seconds*.

Example

Set the hwsysmasterhderror alarm to be reported 5s after it is generated.

```
<HUAWEI> system-view
[HUAWEI] alarm
[HUAWEI-alarm] delay-suppression enable
[HUAWEI-alarm] suppression alarm-name hwsysmasterhderror cause-period 5
```

3.11.21 suppression event-name

Function

The **suppression event-name** command modifies a delay period after which a generated event is reported.

The **undo suppression event-name** command restores the configured delay period after which a generated event is reported.

By default, the system defines a delay period after which a generated event is reported. To view this default delay period, run the **undo suppression event-name** command and then the **display event information** command. If the **Suppress Period** field displays NA for an alarm, this alarm does not support the delayed alarm reporting function.

NOTE

Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S support this command.

Format

suppression event-name *event-name* **period** *seconds*

undo suppression event-name *event-name* **period**

Parameters

Parameter	Description	Value
event-name	Specifies the name of an event for which the delay period is set.	The value cannot be the event name of which the **Suppress Period** field in the **display event information** command output displays NA.
period *seconds*	Specifies the period after which a generated event is reported.	The value is an integer ranging from 0 to 600, in seconds. If the value is set to 0s, the alarm management module sends the event to the NMS without any delay.

Views

Event view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

In the case where a certain event is repeatedly generated, you can enable delayed event reporting and set a period after which a generated event is reported.

After the delay period is set for a certain event, if an event is generated several times during the delay period, the system reports only the first one to the NMS when the delay period expires and discards the following ones.

Prerequisites

Before running the **suppression event-name** command, ensure that delayed alarm reporting has been enabled using the **delay-suppression enable** command.

Precautions

If the delay period is changed when an event is being sent, the changed delay period takes effect on the next event to be sent.

Example

Set the delay period to 5s after which a generated hwFlhSyncFailNotification event is reported.

```
<HUAWEI> system-view
[HUAWEI] event
[HUAWEI-event] delay-suppression enable
[HUAWEI-event] suppression event-name hwFlhSyncFailNotification period 5
```


3.12 SAID Configuration Commands

3.12.1 Command Support

Commands provided in this section and all the parameters in the commands are supported by all switch models (except the S5731-L and S5731S-L), unless otherwise specified. For details, see specific commands.

3.12.2 display said-node brief

Function

The **display said-node brief** command displays brief information about SAID nodes.

Format

display said-node { **all** | *said-name* } **brief** [**slot** *slot-id*]

Parameters

Parameter	Description	Value
all	Indicates all SAID nodes.	-
said-name	Specifies an SAID node.	The value depends on the device configuration.
slot *slot-id*	Specifies a slot ID. If no slot ID is specified, this command displays brief information about SAID nodes on the active MPU.	The value depends on the device configuration.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display said-node brief** command to view brief information about all supported SAID nodes for fault location.

Example

Display brief information about the SAID node named **mac** in slot 2.

```
<HUAWEI> display said-node mac brief slot 2
-------------------------------------------------------------------------------
Node  Node            Type    Cycle  Enable   Active      Inactive Reason
ID    Name                    (s)    Status   Status
-------------------------------------------------------------------------------
2     mac             Restore 1      Enable   Active      -
-------------------------------------------------------------------------------
```

Table 3-170 Description of the **display said-node brief** command output

Item	Description
Node ID	ID of an SAID node.
Node Name	Name of the SAID node.
Type	Type of the SAID node: ● Detect: diagnostic node ● Restore: self-healing node
Cycle(s)	Detection period of the SAID node, in seconds.
Enable Status	Whether the SAID node is enabled: ● Enable: The SAID node is enabled. ● Disable: The SAID node is disabled.
Active Status	Running status of the SAID node: ● Active: The SAID node is running. ● Inactive: The SAID node is not running.
Inactive Reason	Whether the SAID node is activated: ● -: The SAID node is enabled and activated. ● Node disabled: The SAID node is not activated.

3.12.3 set said-node disable

Function

The **set said-node disable** command disables SAID nodes.

The **undo set said-node disable** command enables SAID nodes.

By default, all SAID nodes are enabled.

Format

set said-node { **all** | *said-name* &<1-6> } **disable**

undo set said-node { **all** | *said-name* &<1-6> } **disable**

Parameters

Parameter	Description	Value
all	Indicates all SAID nodes.	-
said-name	Specifies an SAID node.	The value depends on the device configuration. A maximum of six SAID nodes can be configured at a time. If you need to configure more than six SAID nodes, run the **set said-node disable** command multiple times.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The System of Active Immunization and Diagnosis (SAID) is an intelligent fault diagnosis system that automatically diagnoses and rectifies some faults by simulating human operations in troubleshooting. The SAID system has multiple SAID nodes, which detect, diagnose, and rectify faults of multiple modules. However, if a node processes a large number of services, the processing efficiency of other nodes is affected. In this case, run this command disable this node.

Currently, the switch supports the following SAID nodes listed in **Table 3-171**.

Table 3-171 Supported SAID nodes

Node Name	Node Type
FLASH-WRITE	Diagnostic node
MAC	Self-healing node
STG	Self-healing node

Node Name	Node Type
PORT	Self-healing node
VLAN	Self-healing node
SE-REG **NOTE** Only the S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5735-S, S500, S5735-S-I, and S5735S-S support this node.	Self-healing node
SE-TABLE **NOTE** Only the S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5735-S, S500, S5735-S-I, and S5735S-S support this node.	Self-healing node
CONFD-MEMORY	Self-healing node
PING	Diagnostic node After this node is enabled, the device periodically sends ICMP ping packets.

Precautions

If some cards do not support a specific SAID node and no cards that support this SAID node are installed on the device, the device displays a message, indicating that the device does not support this SAID node.

Example

Disable the SAID nodes **mac** and **stg**.

```
<HUAWEI> system-view
[HUAWEI] set said-node mac stg disable
```

Disable all SAID nodes.

```
<HUAWEI> system-view
[HUAWEI] set said-node all disable
```

3.13 NTP Configuration Commands

3.13.1 Command Support

Commands provided in this section and all the parameters in the commands are supported by all switch models (except the S5731-L and S5731S-L), unless otherwise specified. For details, see specific commands.

3.13.2 display ntp-service event clock-unsync

Function

The **display ntp-service event clock-unsync** command displays the last 10 clock unsynchronization reasons.

Format

display ntp-service event clock-unsync

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display ntp-service event clock-unsync** command to view information about the last 10 clock unsynchronization reasons in the current system.

Example

Display the last 10 clock unsynchronization reasons.

```
<HUAWEI> display ntp-service event clock-unsync
 1. Clock source   :  10.1.1.1(vrf1)
    Session type   :  client, configured
    Unsync reason  :  Peer reachability lost
    Unsync time    :  2012-07-30 12:24:44+00:00

 2. Clock source   :  10.2.1.1(vrf2)
    Session type   :  bdcast client (Interface: GE0/0/1), dynamic
    Unsync reason  :  Authentication failure
    Unsync time    :  2011-06-15 11:24:44+00:0
```

Display the clock unsynchronization reasons.

Table 3-172 Description of the **display ntp-service event clock-unsync** command output

Item	Description
Clock source	Indicates the IP address of the server clock.

Item	Description
Session type	Indicates the session type of the server clock.
Unsync reason	Indicates the unsynchronization reasons.
Unsync time	Indicates the unsynchronization time.

3.13.3 display ntp-service sessions

Function

The **display ntp-service sessions** command displays all session information maintained by NTP on the local end.

Format

display ntp-service sessions [**verbose**]

Parameters

Parameter	Description	Value
verbose	Displays detailed information about an NTP session. If **verbose** is not specified, only summary information about the NTP session is displayed.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

To monitor or locate faults on NTP sessions, run the **display ntp-service sessions** command to obtain status information about NTP sessions so that the fault can be located efficiently.

Precautions

- If **verbose** is not specified, summary information about NTP sessions is displayed.

- If **verbose** is specified, detailed information about NTP sessions is displayed.

Example

Display NTP session information of the local device.

```
<HUAWEI> display ntp-service sessions
 clock source: 224.0.1.1
 clock stratum: 1
 clock status: configured, insane, valid, unsynced
 reference clock ID: LOCAL(0)
 reach: 0
 current poll: 64
 now: 9
 offset: 0.0000 ms
 delay: 0.00 ms
 disper: 0.00 ms
```

Table 3-173 Description of the display ntp-service sessions command output

Item	Description
clock source	Address of the clock source.
clock stratum	Stratum of the clock source. The clock stratum determines the precision of the clock, and its value ranges from 1 to 16. The higher the stratum value, the lower the clock precision. The value 1 indicates the highest precision, and the value 16 indicates the lowest precision. The clock with stratum 16 is in the unsynchronized status, and cannot be used as a reference clock.

Item	Description
clock status	Status of a clock, where ● configured: indicates that the session is set up by a configuration command. ● master: indicates that the clock source corresponding to the session is the primary clock source of the current system. ● selected: indicates that the clock source corresponding to the session passes the clock selecting algorithm. ● candidate: indicates that the clock source corresponding to the session is a candidate clock source. ● sane: indicates that the clock source corresponding to the session passes the saneness test. ● insane: indicates that the clock source corresponding to the session does not pass the saneness test. ● valid: indicates that the clock source corresponding to the session is valid. The clock source corresponding to the session passes the test, is in a synchronized status and is of an effective stratum. The root delay and the root dispersion are within the normal range. ● invalid: indicates that the clock source corresponding to the session is invalid. ● unsynced: indicates that the clock source corresponding to the session is not yet synchronized or the stratum is invalid.
reference clock ID	When the local system has been synchronized to a remote NTP server or a clock source, the address of the remote server or the identifier of the clock source is displayed.
reach	Reachability count of the clock source. The value 0 indicates that the clock source is unreachable.
current poll	Poll interval of NTP packets. The interval for sending two successive NTP packets, in seconds. To set the poll interval, run the **ntp-service discard min-interval** command.
now	Interval between the last synchronization and the current time.
offset	Offset to the superior clock source.
delay	Delay to the superior clock source.
disper	Dispersion to the superior clock source.

Display detailed information about NTP sessions on the local device.

```
<HUAWEI> display ntp-service sessions verbose
 clock source: 172.16.12.1
 clock stratum: 1
 clock status: configured, insane, valid, unsynced
 reference clock ID: LOCAL(0)
 local mode: client, local poll: 64, current poll: 64
 peer mode: server, peer poll: 64, now: 21
 offset: -3.2385 ms,delay: 26.97 ms,  disper: 14.85 ms
 root delay: 0.00 ms, root disper: 10.94 ms
 reach: 255, sync dist: 0.058, sync state: 4
 precision: 2^18, version: 3, peer interface: wildcard
 reftime: 10:01:38.546 UTC Sep 5 2005(C6C69602.8C00DA1A)
 orgtime: 10:01:43.463 UTC Sep 5 2005(C6C69607.76ACC921)
 rcvtime: 10:01:43.480 UTC Sep 5 2005(C6C69607.7AF4ADBC)
 xmttime: 10:01:43.452 UTC Sep 5 2005(C6C69607.73F1E8E6)
 filter delay :  0.03   0.02   0.03   0.02   0.02   0.02   0.04   0.02
 filter offset:  0.00  -0.01   0.00   0.01   0.00   0.00   0.00   0.00
 filter disper:  0.03   0.02   0.00   0.11   0.09   0.08   0.06   0.05
 reference clock status: normal
```

Table 3-174 Description of the display ntp-service sessions verbose command output

Item	Description
clock source	Address of the clock source.
clock stratum	NTP stratum on which the local system is located.

Item	Description
clock status	Status of a clock, where ● configured: indicates that the session is set up by a configuration command. ● master: indicates that the clock source corresponding to the session is the primary clock source of the current system. ● selected: indicates that the clock source corresponding to the session passes the clock selecting algorithm. ● candidate: indicates that the clock source corresponding to the session is a candidate clock source. ● sane: indicates that the clock source corresponding to the session passes the saneness test. ● insane: indicates that the clock source corresponding to the session does not pass the saneness test. ● valid: indicates that the clock source corresponding to the session is valid. The clock source corresponding to the session passes the test, is in a synchronized status and is of an effective stratum. The root delay and the root dispersion are within the normal range. ● invalid: indicates that the clock source corresponding to the session is invalid. ● unsynced: indicates that the clock source corresponding to the session is not yet synchronized or the stratum is invalid.
reference clock ID	When the local system has been synchronized to a remote NTP server or a clock source, the address of the remote server or the identifier of the clock source is displayed. When the server is located on a certain VPN, the name of the VPN instance is displayed.
local mode	Local system mode.
peer mode	Peer system mode.
local poll	Local polling mode.
peer poll	Peer polling mode.
offset	Offset to the superior clock source.
delay	Delay to the superior clock source.
disper	Dispersion to the superior clock source.

Item	Description
root delay	Total system delay between the local end and the master reference clock. The default value is 0. If the value of root delay or root disper is large, clock synchronization may fail. A larger value indicates that the packet takes a longer time to reach the local device from the master reference clock. Therefore, the local device cannot determine whether the time in the packet is correct.
root disper	System dispersion of the local end to the master reference clock. The default value is 0. If the value of root delay or root disper is large, clock synchronization may fail. A larger value indicates that the packet takes a longer time to reach the local device from the master reference clock. Therefore, the local device cannot determine whether the time in the packet is correct.
reach	Reachability mark, indicating the reachability to the clock source.
sync dist	Synchronization distance to the superior clock source. This parameter evaluates and describes the clock source, and NTP chooses the clock source with the shortest synchronization distance.
sync state	Synchronization state: ● 0: The clock has never been synchronized. ● 1: Frequency information is obtained from configuration information. ● 2: The clock is set. ● 3: The clock is set, but the frequency is not yet determined. ● 4: The clock is synchronized. ● 5: An error is found.
precision	Precision of a peer clock.
version	NTP version.
peer interface	Peer interface.
reftime	Reference timestamp.
orgtime	Time when an NTP packet is sent for the last time.
rcvtime	Time when an NTP packet is received for the last time.
xmttime	Time when an NTP packet is forwarded for the last time.
filter delay	Filter delays of the 8 packets received for the last time.

Item	Description
filter offset	Filter offsets of the 8 packets received for the last time.
filter disper	Filter dispersions of the 8 packets received for the last time.
reference clock status	The status of the reference clock, including: • normal: indicates that the peer clock is reachable. • abnormal: indicates that the peer clock is unreachable.

3.13.4 display ntp-service statistics packet

Function

The **display ntp-service statistics packet** command displays statistics on NTP packets.

Format

display ntp-service statistics packet [**ipv6** | **peer** [*ip-address* [**vpn-instance** *vpn-instance-name*] | **ipv6** [*ipv6-address* [**vpn-instance** *vpn-instance-name*]]]]

Parameters

Parameter	Description	Value
ipv6	Displays statistics about global IPv6 NTP packets.	-
peer	Displays statistics on an NTP symmetric peer.	-
ip-address	Specifies the IP address of an NTP symmetric peer.	-
vpn-instance *vpn-instance-name*	Specifies a VPN instance related to an NTP symmetric peer.	The value must be an existing VPN instance name.
ipv6	Displays the packet statistics on IPv6 peers.	-
ipv6-address	Displays the NTP packet statistics on the specified IPv6 peer.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

The **display ntp-service statistics packet** command output includes the following information, and can help you to debug NTP packets.

- Number of packets sent and received by an interface
- Number of packets failing authentication
- Number of dropped packets
- Reason for dropping an NTP packet last time

Example

Display the statistics on NTP packets.

```
<HUAWEI> display ntp-service statistics packet
 NTP IPv4 Packet Statistical Information
 ----------------------------------------
 Sent                                : 100
   Send failures                     : 10
 Received                            : 1000
   Processed                         : 800
   Dropped                           : 200
     Validity test failures          : 50
       Authentication failures       : 20
     Invalid packets                 : 50
     Access denied                   : 50
     Rate-limited                    : 0
     Processing delay                : 50
     Interface disabled              : 0
     Max dynamic association reached : 0
     Server disabled                 : 0
     Others                          : 0
Last 2 packets drop reasons:
  [2011-11-24 12:19:26-08:00] Global drop: NTP service disabled for interface.
  [2011-11-24 12:20:30-08:00] Global drop: NTP service disabled for interface.
```

Table 3-175 Description of the **display ntp-service statistics packet** command output

Item	Description
NTP IPv4 Packet Statistical Information	Statistics on IPv4 NTP packets.
Sent	Number of packets sent.
Send failures	Number of failures in sending packets.
Received	Number of received packets.
Processed	Number of processed packets.
Dropped	Number of dropped packets.

Item	Description
Validity test failures	Number of packets dropped because the packets fail to pass the validity test.
Authentication failures	Number of packets dropped because the packets fail to pass the authentication.
Invalid packets	Number of packets dropped because the packets are invalid.
Access denied	Number of packets dropped for lack of access control authority.
Rate-limited	Number of packets dropped due to rate limit.
Processing delay	Number of packets dropped because processing of the packets is delayed.
Interface disabled	Number of packets dropped because the interface is disabled.
Max dynamic association reached	Number of packets dropped because the maximum number of dynamic sessions is reached.
Server disabled	Indicates the number of packets dropped as server disabled.
Others	Number of packets dropped for other reasons.
Last 2 packets drop reasons	Reason for dropping the last n packets, where the maximum value of n can be 10.

3.13.5 display ntp-service status

Function

The **display ntp-service status** command displays the status of NTP.

Format

display ntp-service status

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

To monitor or locate faults on the NTP service, run the **display ntp-service status** command to obtain status information about the NTP service, such as the synchronization status of the local clock and the stratum of the clock.

Example

Display the status of the NTP service.

```
<HUAWEI> display ntp-service status
clock status: synchronized
clock stratum: 2
reference clock ID: LOCAL(0)
nominal frequency: 60.0002 Hz
actual frequency: 60.0002 Hz
clock precision: 2^18
clock offset: 0.0000 ms
root delay: 0.00 ms
root dispersion: 0.00 ms
peer dispersion: 10.00 ms
reference time: 15:51:36.259 UTC Apr 25 2012(C6179088.426490A3)
synchronization state: spike (clock will be set in 1010 secs)
```

Table 3-176 Description of the display ntp-service status command output

Item	Description
clock status	Indicates the clock status. • synchronized: indicates that the local clock has been synchronized with an NTP server or the reference clock. • unsynchronized: indicates that the local clock has not been synchronized with any NTP server.
clock stratum	Indicates the stratum of the reference clock. The value ranges from 1 to 15. A lower the clock stratum indicates higher clock precision. When the client gets synchronized to a session, its stratum is the session stratum plus 1.
reference clock ID	Indicates ID of the reference clock. • When the local clock has been synchronized with the remote NTP server, ID of the reference clock shows IP address of the remote server. • When the local clock has been synchronized with the reference clock, it shows ID of the reference clock. • If the local clock is the reference clock, it shows "Local".
nominal frequency	Indicates the nominal frequency of the local clock, in Hz.
actual frequency	Indicates the actual frequency of the local clock, in Hz.
clock precision	Indicates the precision of the local clock.
clock offset	Indicates the offset between the local clock and the NTP server, in ms.

Item	Description
root delay	Indicates the delay between the local clock and the master reference clock, in ms.
root dispersion	Indicates the dispersion between the local clock and the master reference clock, in ms.
peer dispersion	Indicates the dispersion between the local clock and the peer clock, in ms.
reference time	Indicates reference timestamp.
synchronization state	Indicates the synchronization status of the local clock: • **clock not set**: Indicates the clock is not updated. • **frequency set by configuration**: Indicates the clock frequency is set by NTP configuration. • **clock set**: Indicates the clock is set. • **clock set but frequency not determined:** Indicates the clock is set but the frequency is not determined. • **clock synchronized**: Indicates that the clock is synchronized. • **spike (clock will be set in XXX secs)**: Indicates a time difference of more than 128 milliseconds is detected between NTP server and client clock. The clock change will take effect in XXX seconds.

3.13.6 display ntp-service trace

Function

The **display ntp-service trace** command displays the system to trace the path of reference clock source from the local device.

Format

display ntp-service trace

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

When you run the **display ntp-service trace** command, summary information of NTP servers for synchronizing time on the link from the local device to the reference clock source can be displayed.

Example

Display the summary of each passing NTP server when you trace the reference clock source from the local device.

```
<HUAWEI> display ntp-service trace
server 127.0.0.1,stratum 5, offset 0.024099 s, synch distance 0.06337
server 192.168.1.2,stratum 4, offset 0.028786 s, synch distance 0.04575
server 192.168.2.2,stratum 3, offset 0.035199 s, synch distance 0.03075
server 192.168.10.1,stratum 2, offset 0.039855 s, synch distance 0.01096
refid 127.127.1.0
```

Table 3-177 Description of the display ntp-service trace command output

Item	Description
server	IP address of the NTP server.
stratum	Stratum of the clock on the NTP server.
offset	Offset to the superior reference clock.
synch distance	Synchronization distance to the superior reference clock. This parameter evaluates and describes the reference clock and NTP chooses the reference clock with the shortest synchronization distance.
refid	Reference clock source.

3.13.7 display snmp-agent trap feature-name ntp all

Function

The **display snmp-agent trap feature-name ntp all** command displays the status of NTP traps.

Format

display snmp-agent trap feature-name ntp all

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display snmp-agent trap feature-name ntp all** command to check status of NTP traps. This status can be configured using the **snmp-agent trap enable feature-name ntp** command.

Example

Display the status of NTP traps.

```
<HUAWEI> display snmp-agent trap feature-name ntp all
------------------------------------------------------------------------------
Feature name: NTP
Trap number : 1
------------------------------------------------------------------------------
Trap name                Default switch status   Current switch status
hwNtpStateChangeTrap           on                      on
```

Table 3-178 Description of the **display snmp-agent trap feature-name ntp all** command output

Item	Description
Feature name	Name of the module where the trap is generated.
Trap number	Number of traps.
Trap name	Name of a trap.
Default switch status	Default status of a trap: ● on: The trap function is enabled. ● off: The trap function is disabled.
Current switch status	Current status of a trap: ● on: The trap function is enabled. ● off: The trap function is disabled. This status can be configured using the **snmp-agent trap enable feature-name ntp** command.

3.13.8 ntp-service

Function

The **ntp-service** command configures the maximum polling interval, the timestamp difference between packets sent by the clock server and received by the client, the maximum interval at which the clock of the client is synchronized.

The **undo ntp-service** command restores the default value.

By default, the maximum polling interval is 2^{17}s, the timestamp difference between packets sent by the clock server and received by the client is 128 ms, the maximum interval at which the clock of the client is synchronized is 600 seconds.

Format

ntp-service { **max-sys-poll** *max-sys-poll-value* | **spike-offset** *spike-offset-value* | **sync-interval** *interval* } *

undo ntp-service { **max-sys-poll** | **spike-offset** | **sync-interval** } *

NOTE

Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S support **max-sys-poll** *max-sys-poll-value* and **spike-offset** *spike-offset-value* parameters.

Parameters

Parameter	Description	Value
max-sys-poll *max-sys-poll-value*	Specifies the maximum polling rate.	The value is an integer ranging from 6 to 17.
spike-offset *spike-offset-value*	Specifies the timestamp difference between packets sent by the clock server and received by the client.	The value is an integer ranging from 32 to 128, in milliseconds.
sync-interval *interval*	Sets the maximum interval for clock synchronization.	The value is an integer, in seconds. The value ranges from 180 to 600.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The NTP polling interval is expressed in nth power of 2 (n is an integer). For example, run the **ntp-service max-sys-poll 6** command, the system sends polling packets every 64s. In other words, the device monitors the clock change on the server every 64s.

To decrease the timestamp difference between packets sent by the clock server and received by the client, run the **ntp-service spike-offset** command. If the time

offset of the server is greater than the configured timestamp difference, NTP sets the system clock after the interval for time synchronization elapses.

When the clock of the server changes, the clock of the client is required to be synchronized with the clock of the server. If the clock of the server is unstable, you can run the **ntp-service sync-interval** command on the client to reduce the interval.

The **ntp-service max-distance** command is applied to only the NTP client. The NTP client calculates the distance with each NTP server, and compares the calculated distance with the distance threshold configured using the **ntp-service max-distance** command. If the calculated distance is longer than the threshold, the NTP client does not synchronize the clock from this NTP server.

Precautions

The NTP poll interval must be an integer power of 2; therefore, the interval for the client synchronization is configured as a value closest to the integer power of 2. For example, if the interval configured by the user is 180 seconds, the client is synchronized at any time after 128 seconds.

If you run the **ntp-service** command repeatedly, the latest configuration overrides the previous configurations.

Example

Set the maximum interval to 200 seconds for clock synchronization.

```
<HUAWEI> system-view
[HUAWEI] ntp-service sync-interval 200
```

3.13.9 ntp-service access

Function

The **ntp-service access** command sets the access control authority of the local NTP.

The **undo ntp-service access** command cancels the configured access control authority.

By default, no access control authority is set.

Format

ntp-service access { **peer** | **query** | **server** | **synchronization** | **limited** } { *acl-number* | **ipv6** *acl6-number* } *

undo ntp-service access { **peer** | **query** | **server** | **synchronization** | **limited** } [**ipv6** | **all**]

undo ntp-service access { **peer** | **query** | **server** | **synchronization** | **limited** } [*acl-number* | **ipv6** *acl6-number*] *

Parameters

Parameter	Description	Value
peer	Indicates maximum access authority. Both time request and control query can be performed on the local NTP service, and the local clock can be synchronized to the remote server.	-
query	Indicates minimum access. Only control query can be performed on the local NTP service.	-
server	Indicates that server access and query are permitted. Both time request and control query can be performed on the local NTP service, but the local clock cannot be synchronized to the remote server.	-
synchronization	Indicates that only server access is permitted. Only time request can be performed on the local NTP service.	-
limited	When the rate of NTP packets exceeds the upper limit, the incoming NTP packets are discarded.	-
acl-number	Indicates the number of a basic ACL with IPv4 address specified.	The value is an integer that ranges from 2000 to 2999.
ipv6 *acl6-number*	Indicates the number of an ACL with IPv6 address specified.	The value is an integer that ranges from 2000 to 2999.
all	Indicates all access control authority.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Compared with NTP authentication, **ntp-service access** is simpler to ensure the network security. When an access request reaches the local end, the access request is successively matched with the access authority from the highest one to the

lowest one. The first successfully matched access authority takes effect. The matching order is: **peer**, **server**, **synchronization**, **query** and **limited**.

Depending on the access authority to be limited, run the command on different devices accordingly. For details, see the following table.

Table 3-179 Configuration of the NTP access control authority

NTP Operating Mode	Usage Scenario	Device Configured
Unicast NTP server/ client mode	The client is restricted from being synchronized to a server, so that the client will not be synchronized to an unreliable unicast NTP server on the network.	Client
Unicast NTP server/ client mode	The server is restricted from processing the synchronization time request of the client, so that the synchronization range of the server is controlled.	Server
NTP symmetric peer mode	The two ends are restricted from being synchronized with each other to prevent an unreliable symmetric passive peer on the network from synchronizing the client.	Symmetric active peer
NTP symmetric peer mode	The symmetric passive peer is restricted from processing the time request, so that the synchronization range of the symmetric passive peer is controlled.	Symmetric passive peer
NTP multicast mode	The client is restricted from synchronizing to the server to prevent an unreliable multicast NTP server from synchronizing the client.	NTP multicast client
NTP broadcast mode	The client is restricted from being synchronized to a server, so that the client will not be synchronized to an unreliable broadcast NTP server on the network.	NTP broadcast client
NTP manycast client mode	The client is restricted from being synchronized to a server.	NTP manycast client
NTP manycast server mode	The server is restricted from processing the clock synchronization request sent by the client.	NTP manycast server

The **ntp-service access** command ensures the security to the minimal extent. A safer method is to perform identity authentication. See the **ntp-service authentication enable** command for relevant configuration.

Precautions

Before configuring access control authority in ACL, check ACL rule configurations as follows:

- If the ACL rule is set to **permit** or empty, a permit action will be performed.
- If the ACL rule is set to **deny** or the associated peer is not bound to the ACL rule, a deny action will be performed.

Example

Enable the peer matching ACL 2000 to perform time request, query control and time synchronization on the local device.

```
<HUAWEI> system-view
[HUAWEI] ntp-service access peer 2000
```

Enable the server matching ACL 2002 to perform time request and query control on the local device.

```
<HUAWEI> system-view
[HUAWEI] ntp-service access server 2002
```

3.13.10 ntp-service authentication enable

Function

The **ntp-service authentication enable** command enables identity authentication for NTP.

The **undo ntp-service authentication enable** command disables the identity authentication.

By default, identity authentication is disabled.

Format

ntp-service authentication enable

undo ntp-service authentication enable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

On networks requiring high security, authentication must be enabled for NTP. The NTP client authenticates NTP servers using a password and synchronizes time with only the authenticated server. This improves network security.

Example

Enable identity authentication for NTP.

```
<HUAWEI> system-view
[HUAWEI] ntp-service authentication enable
```

3.13.11 ntp-service authentication-keyid

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** } [**cipher**] *password*

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.	-
cipher	Indicates that the configured password is displayed in cipher text.	-

Parameter	Description	Value
password	Specifies the authentication password in plain text or in cipher text.	The keyword is a string of case sensitive characters, spaces supported. • 1 to 255 characters in plain text. • 20 to 392 characters in cipher text. When quotation marks are used around the string, spaces are allowed in the string. **NOTE** To improve password security, the password must be a combination of at least two of the following: digits, letters, and special characters, and the password length must be equal to or larger than 8. If a password contains a space, the password must be placed into a pair of double quotation marks. Only one pair of double quotation marks can be used for each password.

Views

System view

Default Level

2: Configuration 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 the HMAC-SHA256 identity authentication key. The key ID number is 10, and the key is **Betterkey**.

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

Set authentication text to **xyz123** in HMAC-SHA256 authentication with cipher option.

```
<HUAWEI> system-view
[HUAWEI] ntp-service authentication-keyid 10 authentication-mode hmac-sha256 cipher xyz123
```

3.13.12 ntp-service broadcast-client

Function

The **ntp-service broadcast-client** command configures the device to work in NTP broadcast client mode.

The **undo ntp-service broadcast-client** command removes the device from the NTP broadcast client mode.

By default, the device is not configured in the NTP broadcast client mode.

Format

ntp-service broadcast-client

undo ntp-service broadcast-client

Parameters

None

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

On a synchronization subnet, when the IP address of a server or a symmetric peer is not determined, or when the clocks on a large number of devices need to be synchronized on the network, you can implement clock synchronization by configuring the broadcast mode.

On a specified interface on the broadcast client, run the **ntp-service broadcast-client** command to configure an interface on the local device to receive NTP broadcast packets. When the local device automatically runs in the broadcast client mode, the device can receive the synchronization packets sent by a broadcast server. For the configuration of the broadcast server, see the **ntp-service broadcast-server** command.

When the configuration is complete, you can run the **display ntp-service sessions** command to obtain information about sessions between the broadcast server and the local device.

Example

Enable VLANIF100 to receive NTP broadcast messages.

```
<HUAWEI> system-view
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] ip address 10.1.1.1 24
[HUAWEI-Vlanif100] ntp-service broadcast-client
```

Enable GigabitEthernet0/0/1 to receive NTP broadcast messages.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] ntp-service broadcast-client
```

3.13.13 ntp-service broadcast-server

Function

The **ntp-service broadcast-server** command configures the local device to work in NTP broadcast server mode.

The **undo ntp-service broadcast-server** command removes the device from the NTP broadcast server mode.

By default, the broadcast server mode is not configured.

Format

ntp-service broadcast-server [**version** *number* | **authentication-keyid** *key-id* | **port** *port-number* | **subnet-broadcast**] *

undo ntp-service broadcast-server [**version** *number* | **authentication-keyid** *key-id* | **port** *port-number* | **subnet-broadcast**] *

Parameters

Parameter	Description	Value
version *number*	Indicates the NTP version number. If this parameter is not specified, the version number is a default value.	The value is an integer that ranges from 1 to 4. The default value is 3.
authentication-keyid *key-id*	Indicates the authentication key number used to transmit a message to broadcast clients. If this parameter is not specified, authentication is not performed.	For NTPv1, NTPv2, and NTPv3, the value is an integer ranging from 1 to 4294967295. For NTPv4, the value is an integer ranging from 1 to 65535.
port *port-number*	Specifies the port number to transmit NTP broadcast message.	The value is 123 or an integer ranging from 1025 to 65535. The default value is 123.
subnet-broadcast	Specifies the subnet broadcast mode for NTP broadcast server.	-

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

On a synchronization subnet, when the IP address of a server or a symmetric peer is not determined, or when the clocks on a large number of devices need to be synchronized on the network, you can implement clock synchronization by configuring the broadcast mode. On a specified interface on the broadcast server, run the **ntp-service broadcast-server** command to configure an interface on the local device to send NTP broadcast packets. When the local device automatically runs in the broadcast server mode, the device can send synchronization packets to a broadcast client. For the configuration of the broadcast client, see the **ntp-service broadcast-client** command.

- Full broadcast mode: The broadcast server sends NTP packets to the broadcast address 255.255.255.255 periodically.

- Subnet broadcast mode: The broadcast server sends NTP packets to the broadcast address of the network segment to which the interface IP address belongs periodically.

Precautions

The full broadcast mode and subnet broadcast mode cannot be specified at the same time. After configuring either of the two modes, you must run the **undo ntp-service broadcast-server** command to cancel the current mode before configuring the other mode.

Follow-up Procedure

When the configuration is complete, you can run the **display ntp-service sessions** command to obtain information about sessions between the broadcast server and the client.

Example

Enable VLANIF100 to send NTP broadcast packets, with the NTP version as 2 and the key number as 4.

```
<HUAWEI> system-view
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] ip address 10.1.1.1 24
[HUAWEI-Vlanif100] ntp-service broadcast-server version 2 authentication-keyid 4
```

Enable GigabitEthernet0/0/1 to send NTP broadcast packets, with the NTP version as 3 and the key number as 100.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] ntp-service broadcast-server version 3 authentication-keyid 100
```

3.13.14 ntp-service disable

Function

The **ntp-service disable** command disables the IPv4 and IPv6 NTP function.

The **undo ntp-service disable** command enables the IPv4 and IPv6 NTP function.

By default, the NTP function is enabled.

Format

ntp-service [**ipv6**] **disable**

undo ntp-service [**ipv6**] **disable**

Parameters

Parameter	Description	Value
ipv6	Indicates IPv6 NTP services.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Run the **ntp-service disable** or **ntp-service ipv6 disable** command in the system view to disable the IPv4 or IPv6 NTP service function.

You can run the **ntp-service disable** command in either of the following situations:

- The device does not need to synchronize clock with IPv4 or IPv6 external servers or peers.
- The device does not need to provide reference clock source for IPv4 or IPv6 external clients.

Precautions

Disabling of NTP service will not delete the existing configurations.

After the NTP service is enabled, the system listens to IP address 0.0.0.0 by default. That is, the system listens to all IP addresses, which is prone to security issues. It is recommended that you run the **ntp-service access** { **peer** | **query** | **server** | **synchronization** | **limited** } { *acl-number* | **ipv6** *acl6-number* } * command to configure access control permission on the local NTP service. You can also run the **ntp-service authentication enable** command to configure NTP identify authentication.

Example

Disable the IPv4 NTP service.

```
<HUAWEI> system-view
[HUAWEI] ntp-service disable
```

Disable the IPv6 NTP service.

```
<HUAWEI> system-view
[HUAWEI] ntp-service ipv6 disable
```

3.13.15 ntp-service discard

Function

The **ntp-service discard** command sets the minimum inter-packet interval and the average inter-packet interval of NTP.

The **undo ntp-service discard** command cancels the minimum inter-packet interval and the average inter-packet interval of NTP.

By default, the minimum inter-packet interval is set to the first power of 2 in seconds, namely, 2 seconds, and the average inter-packet interval is set to the fifth power of 2 in seconds, namely, 32 seconds.

Format

ntp-service discard { **min-interval** *min-interval-val* | **avg-interval** *avg-interval-val* } *

undo ntp-service discard

Parameters

Parameter	Description	Value
min-interval *min-interval-val*	Specifies the minimum inter-packet interval of NTP. The actual value of the minimum inter-packet interval of NTP is the value obtained by raising 2 to the power of *min-interval-val*, expressed in seconds.	The value of *min-interval-val* is an integer that ranges from 1 to 8.
avg-interval *avg-interval-val*	Specifies the average inter-packet interval of NTP. The actual value of the average inter-packet interval of NTP is the value obtained by raising 2 to the power of *avg-interval-val*, expressed in seconds.	The value of *avg-interval-val* is an integer that ranges from 1 to 8.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

The minimum inter-packet interval and the average inter-packet interval of NTP are set using the **ntp-service discard** command. To generate kiss code RATE, we need to set the minimum inter-packet interval and the average inter-packet interval of NTP.

Example

Set both the minimum inter-packet interval and the average inter-packet interval of NTP to the fourth power of 2, expressed in seconds, namely, 16 seconds.


```
<HUAWEI> system-view
[HUAWEI] ntp-service discard min-interval 4 avg-interval 4
```

3.13.16 ntp-service in-interface disable

Function

The **ntp-service in-interface disable** command disables an interface from receiving NTP packets.

The **undo ntp-service in-interface disable** command enables an interface to receive NTP packets.

By default, an interface is enabled to receive NTP packets.

Format

ntp-service [**ipv6**] **in-interface disable**

undo ntp-service [**ipv6**] **in-interface disable**

Parameters

Parameter	Description	Value
ipv6	Indicates IPv6 NTP services.	-

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **undo ntp-service** [**ipv6**] **in-interface disable** command provides a method for access control.

You can disable the interface connected to external devices from receiving NTP packets in either of the following situations:

- An unreliable clock server exists on the interface. By default, all the interfaces can receive NTP packets after NTP is enabled on the device. However, an unreliable clock source makes NTP clock data inaccurate.
- The NTP clock data is modified when the interface is attacked maliciously.

Prerequisites

Before an interface is disabled from receiving IPv6 NTP packets, the IPv6 function must be enabled on the interface.

Example

Disable VLANIF100 from receiving NTP packets.

```
<HUAWEI> system-view
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] ntp-service in-interface disable
```

Disable GigabitEthernet0/0/1 from receiving NTP packets.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] ntp-service in-interface disable
```

3.13.17 ntp-service kod-enable

Function

The **ntp-service kod-enable** command enables the KOD function.

The **undo ntp-service kod-enable** command disables the KOD functions.

By default, the KOD function is disabled.

Format

ntp-service kod-enable

undo ntp-service kod-enable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The Kiss-o'-Death (KOD) is a brand new access control technology put forward by NTPv4, and the KOD is mainly used for a server to provide information, such as a status report and access control, for a client. After the KOD function is enabled on the server, the server sends the kiss code DENY or RATE to the client according to the operating status of the system.

When the kiss code is generated in a specific situation, run the **ntp-service kod-enable** command.

Follow-up Procedure

After the KOD function is enabled on the server, you can run the **ntp-service access limited** command to enable control on the rate of incoming NTP packets. When the rate of incoming NTP packets reaches the upper threshold, the server sends the kiss code.

Example

Enable the KOD function.

```
<HUAWEI> system-view
[HUAWEI] ntp-service kod-enable
```

3.13.18 ntp-service manycast-client

Function

The **ntp-service manycast-client** command configures the NTP manycast client mode.

The **undo ntp-service manycast-client** command cancels the NTP manycast client mode.

By default, the NTP manycast client mode is disabled.

Format

ntp-service manycast-client [*ip-address* | **ipv6** [*ipv6-address*]] [**authentication-keyid** *key-id* | **ttl** *ttl-number* | **port** *port-number*] *

undo ntp-service manycast-client [*ip-address* | **ipv6** [*ipv6-address*]] [**authentication-keyid** *key-id* | **ttl** *ttl-number* | **port** *port-number*] *

Parameters

Parameter	Description	Value
ip-address	Specifies a manycast IPv4 address, which is a class D address.	The default IPv4 address is 224.0.1.1.
ipv6 [*ipv6-address*]	Specifies a manycast IPv6 address.	The default IPv6 address is FF0E::0101.
authentication-keyid *key-id*	Specifies the ID of the authentication key used for sending packets to a manycast server.	The value is an integer that ranges from 1 to 65535.
ttl *ttl-number*	Specifies the TTL value of a manycast packet.	The value is an integer ranges from 1 to 255.

Parameter	Description	Value
port *port-number*	Specifies the port number to transmit NTP manycast message.	The value is 123 or an integer ranging from 1025 to 65535. The default value is 123.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

The local device runs in the manycast client mode, and periodically sends manycast packets to manycast servers. After the local device receives the reply packet sent by a manycast server, the local device establishes dynamic C/S association with the server.

NOTE

In the configuration of the manycast client, if the server address is not specified, 224.0.1.1 or FF0E::0101 is adopted as the server address by default.

Example

Configure VLANIF100 to receive NTP manycast packets.

```
<HUAWEI> system-view
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] ip address 10.1.1.1 24
[HUAWEI-Vlanif100] ntp-service manycast-client
```

Configure GigabitEthernet0/0/1 to receive NTP manycast packets.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] ntp-service manycast-client
```

3.13.19 ntp-service manycast-server

Function

The **ntp-service manycast-server** command configures the NTP manycast server mode.

The **undo ntp-service manycast-server** command cancels the NTP manycast server mode.

By default, the NTP manycast server mode is not configured.

Format

ntp-service manycast-server [*ip-address* | **ipv6** [*ipv6-address*]]

undo ntp-service manycast-server [*ip-address* | **ipv6** [*ipv6-address*]]

Parameters

Parameter	Description	Value
ip-address	Specifies a manycast IPv4 address, which is a class D address.	The default IPv4 address is 224.0.1.1.
ipv6 [*ipv6-address*]	Specifies a manycast IPv6 address.	The default IPv6 address is FF0E::0101.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The manycast server responds to the manycast packets sent by the client. After the manycast client receives the reply packet, the manycast client establishes temporary association with the server and enters C/S mode.

Precautions

If the manycast IP address is not specified when the **undo ntp-service manycast-server** command is run, the local device searches for the default IP address. In IPv4 networks, the default IP address of the manycast server is 224.0.1.1. In IPv6 networks, the default IP address of the manycast server is FF0E::0101. If the local device finds the default IP address, the **undo ntp-service manycast-server** command takes effect; otherwise, the **undo ntp-service manycast-server** does not take effect.

Example

Configure VLANIF100 as an interface of the server. The interface is used for responding to the manycast client request from a manycast address.

```
<HUAWEI> system-view
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] ip address 10.1.1.1 24
[HUAWEI-Vlanif100] ntp-service manycast-server
```

Configure GigabitEthernet0/0/1 as an interface of the server. The interface is used for responding to the manycast client request from a manycast address.


```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] ntp-service manycast-server
```

3.13.20 ntp-service max-distance

Function

The **ntp-service max-distance** command configures the maximum distance threshold value.

The **undo ntp-service max-distance** command restores the default value.

By default, the maximum distance threshold value is 1.

Format

ntp-service max-distance *max-distance-value*

undo ntp-service max-distance

Parameters

Parameter	Description	Value
max-distance-value	Indicates the maximum distance threshold value in seconds.	The value is an integer and ranges from 1 to 16, in seconds. The default value is 1.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

ntp-service max-distance command is used at the client side. At the client side, NTP will calculate synchronization distance for each server and compare it with synchronization distance threshold value. If the synchronization distance exceeds synchronization distance threshold value, the client will not consider that server for clock synchronization. This command is used in the calculation of synchronization distance threshold value.

Example

Set the NTP maximum distance to 16s.

```
<HUAWEI> system-view
[HUAWEI] ntp-service max-distance 16
```


3.13.21 ntp-service max-dynamic-sessions

Function

The **ntp-service max-dynamic-sessions** command sets the maximum dynamic NTP sessions that can be set up.

The **undo ntp-service max-dynamic-sessions** command restores the maximum dynamic NTP sessions to the default value.

By default, a maximum of 100 NTP dynamic sessions can be set up.

Format

ntp-service max-dynamic-sessions *number*

undo ntp-service max-dynamic-sessions

Parameters

Parameter	Description	Value
number	Specifies the number of dynamic sessions that can be set up.	The value is an integer that ranges from 0 to 100, and the default value is 100.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A maximum of 128 sessions can be established on the same device running the NTP service in the same period, including static and dynamic sessions. In both unicast server/client mode and symmetric peer mode, command lines are used to establish static sessions. The dynamic sessions are established in broadcast mode or multicast mode.

Excessive dynamic sessions directly affect the establishment of static sessions. A user can limit the number of local dynamic sessions solve this problem.

Precautions

When the number of local dynamic sessions on the device is limited:

- This command limits the number of only dynamic sessions, not static sessions.
- NTP dynamic sessions established are not affected. That is, when the number of the dynamic sessions exceeds the limit, the dynamic sessions established are not deleted, but a new dynamic session cannot be established.

- The limit on the number of local dynamic sessions allowed should be configured on the client because the server does not record the number of the established NTP sessions.

Example

Set the maximum number of NTP dynamic sessions that can be set up to 50.

```
<HUAWEI> system-view
[HUAWEI] ntp-service max-dynamic-sessions 50
```

3.13.22 ntp-service multicast-client

Function

The **ntp-service multicast-client** command configures the local device to work in NTP multicast client mode.

The **undo ntp-service multicast-client** command cancels the NTP multicast client mode.

By default, the NTP multicast client mode is not configured.

Format

ntp-service multicast-client [*ip-address* | **ipv6** [*ipv6-address*]]

undo ntp-service multicast-client [*ip-address* | **ipv6** [*ipv6-address*]]

Parameters

Parameter	Description	Value
ip-address	Indicates the multicast IP address.	The default IP address is 224.0.1.1.
ipv6 [*ipv6-address*]	Indicates the multicast IPv6 address.	The default IPv6 address is FF0E::0101.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To perform clock synchronization in multicast mode, you can use the **ntp-service multicast-client** command to specify the current interface on the local device to receive NTP multicast packets. The local device runs in the multicast client mode.

If the valid multicast server is configured, the local device gets synchronized with the multicast server. The local device time is updated with the time of the server.

Follow-up Procedure

When the configuration is complete, run the **display ntp-service sessions** command to obtain session information about the multicast server and the local device.

NOTE

You can configure more than one multicast client with different multicast IP address on the same interface. When multiple multicast clients are configured, the device selects the optimal clock source by selecting a preferred clock.

You can configure a maximum of 1024 multicast clients on the local device, but a maximum of 128 multicast clients can work simultaneously.

Example

Configure VLANIF100 to receive NTP multicast packets. The multicast address of the multicast packets is 224.0.1.2.

```
<HUAWEI> system-view
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] ip address 10.1.1.1 24
[HUAWEI-Vlanif100] ntp-service multicast-client 224.0.1.2
```

Configure GigabitEthernet0/0/1 to receive NTP multicast packets. The multicast address of the multicast packets is 224.0.1.1.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] ntp-service multicast-client 224.0.1.1
```

3.13.23 ntp-service multicast-server

Function

The **ntp-service multicast-server** command specifies an interface on the local device to send NTP multicast packets. The local device runs in the multicast server mode.

The **undo ntp-service multicast-server** command cancels the NTP multicast server mode.

By default, the multicast server mode is not configured.

Format

ntp-service multicast-server [*ip-address*] [**version** *number* | **authentication-keyid** *key-id* | **ttl** *ttl-number* | **port** *port-number*] *

ntp-service multicast-server ipv6 [*ipv6-address*] [**authentication-keyid** *key-id* | **ttl** *ttl-number* | **port** *port-number*] *

undo ntp-service multicast-server [*ip-address*] [**version** *number* | **authentication-keyid** *key-id* | **ttl** *ttl-number* | **port** *port-number*] *

undo ntp-service multicast-server ipv6 [*ipv6-address*] [**authentication-keyid** *key-id* | **ttl** *ttl-number* | **port** *port-number*] *

Parameters

Parameter	Description	Value
ip-address	Indicates the multicast IP address.	The default address is 224.0.1.1.
ipv6 [*ipv6-address*]	Indicates the multicast IPv6 address.	The default IPv6 address is FF0E::0101.
version *number*	Indicates the NTP version number. If this parameter is not specified, the version number is a default value.	The value is an integer that ranges from 1 to 4. The default value is 3.
authentication-keyid *key-id*	Indicates the authentication key ID used when sending messages to the multicast clients. If this parameter is not specified, authentication is not performed.	The value is an integer. It ranges from 1 to 4294967295 when the NTP version number is 1, 2, or 3, and ranges from 1 to 65535 when the version number is 4 or the specified remote server uses an IPv6 address.
ttl *ttl-number*	Indicates the life span of the multicast packet. If this parameter is not specified, the life span of the multicast packet is a default value.	The ttl number is an integer that ranges from 1 to 255. The default value is 255.
port *port-number*	Specifies the port number to transmit NTP multicast message.	The value is 123 or an integer ranging from 1025 to 65535. The default value is 123.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To perform clock synchronization in the multicast mode, run the **ntp-service multicast-server** command to specify the current interface on the local device to send NTP multicast packets. The local device runs in the multicast server mode, and functions as the multicast server to periodically send multicast packets to the multicast client.

Follow-up Procedure

When the configuration is complete, run the **display ntp-service sessions** command to obtain session information about the multicast server and the local device.

NOTE

You can configure a maximum of 128 multicast servers on the local device.

Example

Configure VLANIF100 to send NTP multicast packets. The multicast IPv4 address is 224.0.1.1, the authentication key ID is 4 and the NTP version number is 3.

```
<HUAWEI> system-view
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] ip address 10.1.1.1 24
[HUAWEI-Vlanif100] ntp-service multicast-server 224.0.1.1 authentication-keyid 4 version 3
```

Configure GigabitEthernet0/0/1 to send NTP multicast packets. The multicast IPv4 address is 224.0.1.1, the authentication key ID is 4 and the NTP version number is 3.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] ntp-service multicast-server 224.0.1.1 authentication-keyid 4 version 3
```

3.13.24 ntp-service port

Function

The **ntp-service port** command changes the number of the port that sends NTP packets.

The **undo ntp-service port** command restores the default port number.

By default, port 123 sends NTP packets.

Format

ntp-service port *port-value*

undo ntp-service port

Parameters

Parameter	Description	Value
port-value	Specifies the number of the port that sends NTP packets.	The value is an integer ranging from 1025 to 65535. **NOTE** The *port-value* can be set to the default port 123.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

To improve security of network packets, run the **ntp-service port** command to configure the number of the port that sends NTP packets. Therefore, the user firewall filters packets based on the port number.

Example

Set the number of the port that sends NTP packets to 5000.

```
<HUAWEI> system-view
[HUAWEI] ntp-service port 5000
```

3.13.25 ntp-service refclock-master

Function

The **ntp-service refclock-master** command sets the local clock to be the NTP primary clock that provides the synchronizing time for other devices.

The **undo ntp-service refclock-master** command cancels the configuration of the NTP primary clock.

By default, no NTP primary clock is specified.

Format

ntp-service refclock-master [*ip-address*] [*stratum*]

undo ntp-service refclock-master [*ip-address*] [*stratum*]

Parameters

Parameter	Description	Value
ip-address	Specifies the IP address of the local reference clock. When no IP address is assigned, the local clock whose IP address is 127.127.1.0 is set as the default NTP primary clock.	The value of *ip-address* is 127.127.1.u, and **u** ranges from 0 to 3, which represents the number of the selected local clock.
stratum	Specifies the stratum of the NTP primary clock. If this parameter is not specified, the stratum is a default value.	The value of the stratum is an integer that ranges from 1 to 15. The default value is 8. Timer is accurate if the stratum value is small.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The local clock is the clock of the device itself. Run the **ntp-service refclock-master** command to set the local clock as the NTP primary clock that provides the synchronization time for other devices.

In NTP, the time synchronization in an NTP synchronization subnet is performed from a smaller level to a larger level, that is, from the 1st level to the 15th level. An authoritative clock is used as a reference time source for the synchronization subnet, and is located at the top of the synchronization subnet. The authoritative clock is stratum0. The current authoritative clock is mostly a Radio Clock or the Global Positioning System. The time of the authoritative clock is synchronized through the broadcast UTC time code other than NTP.

Precautions

A device on the network can perform clock synchronization in the following manners.

- Synchronizing with the local clock: The local clock is used as the reference clock.
- Synchronizing with another device on the network: This device is used as an NTP clock server to provide a reference clock for the local end.

If both manners are configured, the device selects an optimal clock source through selecting a preferred clock. That is, clocks determined in the two manners are

compared to determine which clock is a lower stratum. The clock of a lower stratum is the preferred clock source.

Example

Set the local clock to be the NTP primary clock, the stratum of which set to 3.

```
<HUAWEI> system-view
[HUAWEI] ntp-service refclock-master 3
```

3.13.26 ntp-service reliable authentication-keyid

Function

The **ntp-service reliable authentication-keyid** command specifies the authentication key to be reliable.

The **undo ntp-service reliable authentication-keyid** command cancels the current setting.

By default, no authentication key is specified to be reliable.

Format

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

undo ntp-service reliable 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.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

If the identity authentication is enabled, this command is used to specify that one or more keys are reliable. That is, the client can only be synchronized with the server that provides the reliable key. The client cannot be synchronized with the server that provides unreliable keys.

Example

Enable the identity authentication in NTP and adopt the HMAC-SHA256 encryption mode with key number as 37 and the key as BetterKey. Specify the key to be reliable.

```
<HUAWEI> system-view
[HUAWEI] ntp-service authentication enable
[HUAWEI] ntp-service authentication-keyid 37 authentication-mode hmac-sha256 cipher BetterKey
[HUAWEI] ntp-service reliable authentication-keyid 37
```

3.13.27 ntp-service server disable

Function

The **ntp-service server disable** command disables NTP server function.

The **undo ntp-service server disable** command enables NTP server function.

By default, NTP server function is disabled.

Format

ntp-service [**ipv6**] **server disable**

undo ntp-service [**ipv6**] **server disable**

Parameters

Parameter	Description	Value
ipv6	Indicates IPv6 NTP services.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

For the security purpose, NTP server function can be disabled when the device does not need to act as a server.

By default, NTP server functionality is disabled. To enable NTP server functionality, first configure other NTP functions, such as a clock source, and then run the **undo ntp-service server disable** command to make the NTP server function take effect. If you run the **undo ntp-service** [**ipv6**] **server disable** command alone, the NTP server function cannot take effect.

Example

Disable IPv4 NTP server function.


```
<HUAWEI> system-view
[HUAWEI] ntp-service server disable
```

Disable IPv6 NTP server function.

```
<HUAWEI> system-view
[HUAWEI] ntp-service ipv6 server disable
```

3.13.28 ntp-service source-interface

Function

The **ntp-service source-interface** command specifies the local source interface that sends NTP packets.

The **undo ntp-service source-interface** command cancels the current setting.

By default, the local source interface is not specified for sending NTP packets. The local source interface is automatically determined based on routes.

Format

ntp-service [**ipv6**] **source-interface** *interface-type interface-number* [**vpn-instance** *vpn-instance-name*]

undo ntp-service [**ipv6**] **source-interface** [*interface-type interface-number*] [**vpn-instance** *vpn-instance-name*]

Parameters

Parameter	Description	Value
ipv6	Indicates that the network type of the local source interface is IPv6.	-
interface-type interface-number	Indicates the local interface that sends NTP packets.	-
vpn-instance *vpn-instance-name*	Indicates the name of a VPN instance.	The value must be an existing VPN instance name.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Configure the local source interface for sending and receiving NTP packets to prevent other interfaces on the device from receiving NTP response packets. This configuration is convenient for a user to subsequently deploy a flow control policy. If no interface is specified, the source IP address of NTP packets is selected according to routes.

If you have specified **vpn-instance** when configuring a source IP address using this command, the source IP address can only be used by the NTP client bound to the specified VPN instance and cannot be used by NTP clients bound to other VPN instances or not bound to any VPN instance.

Precautions

- In broadcast, multicast, and manycast modes, NTP is implemented on a specific interface, and this interface is the source interface. Therefore, the **ntp-service source-interface** command is invalid in broadcast, multicast, and manycast modes.
- This command applies only to the NTP client, but not the NTP server.

Example

Specify VLANIF100 as the source interface to send all NTP packets.

```
<HUAWEI> system-view
[HUAWEI] ntp-service source-interface vlanif 100
```

3.13.29 ntp-service unicast-peer

Function

The **ntp-service unicast-peer** command configures NTP peer mode.

The **undo ntp-service unicast-peer** command cancels the NTP peer mode.

By default, the NTP peer mode is not configured.

Format

ntp-service unicast-peer *ip-address* [**version** *number* | **authentication-keyid** *key-id* | **source-interface** *interface-type interface-number* | **preference** | **vpn-instance** *vpn-instance-name* | **maxpoll** *max-number* | **minpoll** *min-number* | **preempt** | **port** *port-number*] *

ntp-service unicast-peer ipv6 *ipv6-address* [**authentication-keyid** *key-id* | **source-interface** *interface-type interface-number* | **preference** | **vpn-instance** *vpn-instance-name* | **maxpoll** *max-number* | **minpoll** *min-number* | **preempt** | **port** *port-number*] *

undo ntp-service unicast-peer { *ip-address* | **ipv6** *ipv6-address* } [**vpn-instance** *vpn-instance-name*]

Parameters

Parameter	Description	Value
ip-address	Indicates the IPv4 address of the remote peer.	The parameter *ip-address* is a host address and cannot be the broadcast address, the multicast address or the IP address of a reference clock.
ipv6 *ipv6-address*	Indicates the IPv6 address of the remote server.	The value of *ipv6-address* is a unicast address, but cannot be a broadcast address, multicast address, or reference clock's IP address.
version *number*	Indicates the NTP version number. If this parameter is not specified, the default version number is used.	The version number is an integer that ranges from 1 to 4. By default, it is 3.
authentication-keyid *key-id*	Indicates the authentication key ID used when transmitting messages to the remote peer. If this parameter is not specified, authentication is not performed.	The key ID is an integer that ranges from 1 to 4294967295 when the NTP version number is from 1 to 3. When the NTP version number is 4, the key ID is integer that ranges from 1 to 65535. When the remote server address is an IPv6 address, the key ID is an integer that ranges from 1 to 65535.
maxpoll *max-number*	Indicates the maximum NTP poll interval.	The value is an integer that ranges from 10 to 17.
minpoll *min-number*	Indicates the minimum NTP poll interval.	The value is an integer that ranges from 3 to 6.

Parameter	Description	Value
source-interface *interface-type interface-number*	Indicates the source interface from which the symmetric active end sends NTP packets to the symmetric passive end. The source IP address of the NTP packets is the IP address of this interface.	-
vpn-instance *vpn-instance-name*	Specifies the VPN instance name.	The value must be an existing VPN instance name.
preference	Indicates the remote peer as the preferred one. By default, the remote peer is not preferred. **NOTE** If you run the **ntp-service unicast-peer** command multiple times to configure multiple remote peers, you can specify the **preference** parameter to configure a peer as the preferred one. This prevents the local device from frequently switching connections with remote peers and prevents frequent time changes and a large number of logs generated on the local device.	-
preempt	Indicates that the symmetric peer is in preemption mode. If any error, for example, an authentication failure, is detected on the association, the symmetric peer in preemption mode is marked as unavailable for selection. However, when no other symmetric peers are available for selection, this symmetric peer is marked as available.	-
port *port-number*	Specifies the port number to transmit NTP unicast message.	The value is 123 or an integer ranging from 1025 to 65535. The default value is 123.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When the clock of a device on the network needs to be synchronized in symmetric peer mode, you can run the **ntp-service unicast-peer** command to configure a remote node as the symmetric peer of the device. The local device runs in symmetric active peer mode. In this mode, the device and the remote peer can synchronize clock with each other.

Precautions

- If the same server is specified in at least two commands that are run in sequence to configure the NTP server mode, during the configuration restoration, the last run command takes effect. For example, the **ntp-service unicast-peer 10.10.1.1 source-interface vlanif 10** command and **ntp-service unicast-peer 10.10.1.1** command are run in sequence. During the configuration restoration, only the **ntp-service unicast-peer 10.10.1.1** command takes effect.
- A maximum of 128 peers can be configured for the local device. The optimal symmetric peer is selected as the synchronization source.
- When a PE is synchronized to another PE or CE in a VPN, the parameter **vpn-instance** *vpn-instance-name* needs to be specified.
- When you run the **undo ntp-service unicast-peer** command with a specified **vpn-instance** *vpn-instance-name*, the configuration of the NTP symmetric passive peer with the IP address *ip-address* on the VPN is canceled. If **vpn-instance** *vpn-instance-name* is not specified, the configuration of the NTP symmetric passive peer with the IP address *ip-address* on the public network.

Example

Configure the peer 10.10.1.1 to provide the synchronizing time for the local device. The local device can also provide synchronizing time for the peer. The version number is 3. The IP address of the NTP packets is the address of VLANIF100.

```
<HUAWEI> system-view
[HUAWEI] ntp-service unicast-peer 10.10.1.1 version 3 source-interface vlanif 100
```

3.13.30 ntp-service unicast-server

Function

The **ntp-service unicast-server** command configures the NTP server mode.

The **undo ntp-service unicast-server** command cancels the NTP server mode.

By default, the NTP server mode is not configured.

Format

ntp-service unicast-server *ip-address* [**version** *number* | **authentication-keyid** *key-id* | **source-interface** *interface-type interface-number* | **preference** | **vpn-instance** *vpn-instance-name* | **maxpoll** *max-number* | **minpoll** *min-number* | **burst** | **iburst** | **preempt** | **port** *port-number*] *

ntp-service unicast-server ipv6 *ipv6-address* [**authentication-keyid** *key-id* | **source-interface** *interface-type interface-number* | **preference** | **vpn-instance** *vpn-instance-name* | **maxpoll** *max-number* | **minpoll** *min-number* | **burst** | **iburst** | **preempt** | **port** *port-number*] *

undo ntp-service unicast-server { *ip-address* | **ipv6** *ipv6-address* } [**vpn-instance** *vpn-instance-name*]

Parameters

Parameter	Description	Value
ip-address	Indicates the IPv4 address of the remote server.	The value of *ip-address* must be an IP address of a host, but cannot be a broadcast address, multicast address, or reference clock's IP address.
version *number*	Indicates the NTP version number. If this parameter is not specified, the default version number is used.	The version number is an integer that ranges from 1 to 4. By default, the version number is 3.
authentication-keyid *key-id*	Indicates the authentication key ID used when messages are transmitted to the remote server. If this parameter is not specified, authentication is not performed.	The key ID is an integer that ranges from 1 to 4294967295 when the NTP version number is from 1 to 3. When the NTP version number is 4, the key ID is integer that ranges from 1 to 65535. When the remote server address is an IPv6 address, the key ID is an integer that ranges from 1 to 65535.

Parameter	Description	Value
maxpoll *max-number*	Specifies the NTP maximum poll interval. The NTP poll interval of the system floats between the minimum value and maximum value.	It is an integer ranging from 10 to 17, in seconds. The default value is 10 seconds in NTPv1, NTPv2, NTPv3, and NTPv4.
minpoll *min-number*	Specifies NTP minimum poll interval. The NTP poll interval of the system floats between the minimum value and maximum value.	It is an integer ranging from 3 to 6, in seconds. The default value is 6 seconds.
source-interface *interface-type interface-number*	Indicates the source interface from which the unicast client sends NTP packets to the unicast server. The source IP address of the NTP packets is the IP address of this interface.	-
vpn-instance *vpn-instance-name*	Specifies the VPN instance name.	The value must be an existing VPN instance name.
preference	Indicates the remote server as the preferred one. By default, the remote server is not preferred. **NOTE** If you run the **ntp-service unicast-server** command multiple times to configure multiple remote servers, you can specify the **preference** parameter to configure a server as the preferred one. This prevents the local device from frequently switching connections with remote servers and prevents frequent time changes and a large number of logs generated on the local device.	-
burst	Indicates that a burst of packets is sent within a fixed poll period. When the poll interval is long, this method helps measure the time jitter.	-

Parameter	Description	Value
iburst	Indicates that the device sends a burst of packets when receiving a response of an unreachable server. This parameter can be used to accelerate synchronization.	-
preempt	Indicates that the server is in preemption mode. If any error, for example, an authentication failure, is detected on the association, the server marked as "preempt" is marked as unavailable for selection. However, the server is marked as available for selection when no other servers are available for selection on the network and no error occurs on the association of the server.	-
port *port-number*	Specifies the port number to transmit NTP unicast message.	The value is 123 or an integer ranging from 1025 to 65535. The default value is 123.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When the clock of a device on the network needs to be synchronized in unicast server/client mode, the command can be run, and the remote server specified by *ip-address* or *ipv6-address* is used as the local clock server. The local device runs in client mode. In this mode, the local client can be synchronized to the remote server, but the remote server cannot be synchronized to the local client.

When the **ntp-service unicast-server** command is run, you can also configure the mode used for the remote server, such as the NTP version, authentication key, and the polling interval.

Precautions

- A maximum of 128 servers can be configured for the local device. The optimal symmetric peer is selected as the synchronization source.

- If the local device works in the client mode, the local device can only be synchronized with the remote server but the remote server cannot be synchronized with the local device.
- When a PE is synchronized to another PE or CE in a VPN, the parameter **vpn-instance** *vpn-instance-name* needs to be specified.
- When the **undo ntp-service unicast-server** command is run, if the parameter **vpn-instance** *vpn-instance-name* is specified, cancel the configuration of the NTP server with the IP address *ip-address* or *ipv6-address* in the VPN. If the parameter **vpn-instance** *vpn-instance-name* is not specified, cancel the configuration of the NTP server with the IP address *ip-address* or *ipv6-address* in the public network.
- Before deleting a VPN instance, check whether the VPN instance is bound to the NTP server. This confirmation is to ensure that the changed configuration meets users' requirements. For example:
  a. Specify an NTP server and bind a VPN instance to the NTP server. You can view the following configurations:
  ```
  <HUAWEI> display current-configuration | begin ntp
  ntp-service unicast-server 10.1.1.1 vpn-instance vpn2
  ntp-service refclock-master
  ```
  b. If the VPN instance named vpn2 is deleted, the VPN instance bound to the NTP server is also deleted.
  ```
  <HUAWEI> display current-configuration | be ntp
  ntp-service unicast-server 10.1.1.1
  ntp-service refclock-master
  ```

Example

Configure the server 10.10.1.1 to provide the synchronizing time for the local device. The NTP version number is 3.

```
<HUAWEI> system-view
[HUAWEI] ntp-service unicast-server 10.10.1.1 version 3
```

Configure the server 10.10.1.1 with VPN instance "abc" to provide the synchronizing time for the local device.

```
<HUAWEI> system-view
[HUAWEI] ntp-service unicast-server 10.10.1.1 vpn-instance abc
```

3.13.31 reset ntp-service statistics packet

Function

The **reset ntp-service statistics packet** command clears statistics on NTP packets.

Format

reset ntp-service statistics packet [**ipv6** | **peer** [*ip-address* [**vpn-instance** *vpn-instance-name*] | **ipv6** [*ipv6-address* [**vpn-instance** *vpn-instance-name*]]]]

Parameters

Parameter	Description	Value
ipv6	Clears the statistics about global IPv6 NTP packets.	-
peer	Clears statistics related to NTP peers.	-
ip-address	Specifies the IP address of an NTP peer.	-
vpn-instance *vpn-instance-name*	Specifies the VPN instance bound to an NTP peer.	The value must be an existing VPN instance name.
ipv6	Clears the packet statistics on IPv6 peers.	-
ipv6-address	Clears the NTP packet statistics on the specified IPv6 peer.	-

Views

User view

Default Level

3: Management level

Usage Guidelines

When debugging NTP, you can use this command to clear the statistics on NTP.

NOTICE

The statistics on NTP cannot be recovered after being cleared. Confirm before you delete the statistics.

Example

Clear statistics on NTP packets.

```
<HUAWEI> reset ntp-service statistics packet
```

Clear statistics on NTP peers.

```
<HUAWEI> reset ntp-service statistics packet peer
```

3.13.32 snmp-agent trap enable feature-name ntp

Function

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

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

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

Format

snmp-agent trap enable feature-name ntp [**trap-name hwntpstatechangetrap**]

undo snmp-agent trap enable feature-name ntp [**trap-name hwntpstatechangetrap**]

Parameters

Parameter	Description	Value
trap-name hwntpstatechangetrap	Indicates that NTP synchronization status changed.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

To enable the NMS to easily manage the NTP module of the device, run the **snmp-agent trap enable feature-name ntp** command to enable the trap function for the NTP module. The command configuration ensures that the traps generated during the device operation are sent to the NMS. Otherwise, NTP traps are not sent to the NMS.

You can run the **snmp-agent trap enable feature-name ntp** command to check the configuration result.

Example

Enable the **hwntpstatechangetrap** trap.

```
<HUAWEI> system-view
[HUAWEI] snmp-agent trap enable feature-name ntp trap-name hwntpstatechangetrap
```

3.14 PTP Configuration Commands

3.14.1 Command Support

Model	Supported Part Number	Unsupported Part Number
S6730-H24X6C	• 02352FSG, 02352FSG-001, 02352FSG-003, 02352FSG-005, 02352FSG-006 • 02353GFC, 02353GFC-001, 02353GFC-003	• 02352FSG-007, 02352FSG-008 • 02353GFC-004
S6730-H48X6C	• 02352FSF, 02352FSF-003, 02352FSF-005, 02352FSF-007, 02352FSF-008, 02352FSF-011 • 02353FWL, 02353FWL-003, 02353FWL-005	• 02352FSF-009, 02352FSF-010 • 02353FWL-006
S6730-H24X4Y4C	None	No part number supports this model.
S6730-H28Y4C	None	No part number supports this model.
S6730S-H24X6C-A	• 02353HVK, 02353HVK-001, 02353HVK-003	02353HVK-004

3.14.2 display ptp

Function

The **display ptp** command displays information about the Precision Time Protocol (PTP).

Format

display ptp all [**config** | **state**] [**slot** *slot-id*]

display ptp interface *interface-type interface-number*

Parameters

Parameter	Description	Value
all	Displays all the statistics of a PTP device, such as the global configuration parameters, interface where the clock source resides, time trace status, and interface running status.	-

Parameter	Description	Value
config	Displays configurations of all the modules related to PTP on the device.	-
state	Displays the running status of the protocol on all the modules related to PTP on the device.	-
slot *slot-id*	Displays the status information of the protocol on all the modules related to PTP based on a slot ID.	The value must be set according to the device configuration.
interface *interface-type interface-number*	Displays the BMC running status and the number of sent and received PTP packets on a specified interface. • *interface-type* specifies the type of an interface. • *interface-number* specifies the number of an interface.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

Using the **display ptp** command, you can view the running status of PTP and statistics information about the global configuration parameters, interface where the clock source resides, and clock lock status. In addition, the command also displays the grandmaster clock ID, receiver number, parent clock ID, parent port number, statistics, and status of interfaces or role list.

Precautions

The **display ptp** displays the configuration on the interface only when PTP is enabled globally and in the interface view.

Example

Display the status and statistics of all the modules related to PTP.

```
<HUAWEI> display ptp all slot 0
 Device config info
```



```
--------------------------------------------------------------------------------
PTP state          :enabled    Domain  value      :0
Slave only         :no         Device type        :E2ETCOC
Set port state     :no         Local clock ID     :e468a3fffe552a30
Virtual clock ID   :no         Time lock success  :no
PTP profile        :IEEE1588V2

BMC run info
--------------------------------------------------------------------------------
Grand clock ID     :9c8fd0fffecf3c87
Receive number     :XGigabitEthernet0/0/3
Parent clock ID    :9c8fd0fffecf3c87
Parent portnumber :256
Priority1          :1          Priority2          :1
Step removed       :0          Clock accuracy     :0x21
Clock class        :6          Time Source        :0xa0
UTC Offset         :35         UTC Offset Valid   :False
Timescale          :PTP        Time Traceable     :False
Leap               :None       Frequence Traceable:True
Offset scaled      :0xffff


Clock source info
Clock Pri1 Pri2 Accuracy Class TimeSrc Signal Switch Direction In-Status
--------------------------------------------------------------------------------
local 128  128  0x31     187   0xa0     -      -      -         -
```

Display PTP interface status and packet statistics of XGigabitEthernet0/0/3.

```
<HUAWEI> display ptp interface xgigabitethernet 0/0/3
  Port State :faulty
  Port Number :3

  Recv Packet Statistics
  --------------------------------------------------------------------------------
  Announce               :0          Sync                    :0
  Req                    :0          Resp                    :0
  Followup               :0          Pdelay_resp_followup    :0

  Send Packet Statistics
  --------------------------------------------------------------------------------
  Announce               :0          Sync                    :0
  Req                    :0          Resp                    :0
  Followup               :0          Pdelay_resp_followup    :0

  Discard Packet Statistics
  --------------------------------------------------------------------------------
  Announce               :0          Sync                    :0
  Delayreq               :0          Pdelayreq               :0
  Resp                   :0          Pdelayresp              :0
  Followup               :0          Pdelay_resp_followup    :0
```

Table 3-180 Description of the **display ptp** command output

Item	Description
Device config info	
PTP state	Whether PTP is enabled. The value is set through the **ptp enable** command.
Domain value	Domain that the PTP clock belongs to. The value is set through the **ptp domain** command.

Item	Description
Slave only	Whether the **slave only** mode is adopted. The value is set through the **ptp slaveonly** command.
Device-type	Type of the PTP device. The value is set through the **ptp device-type** command.
Set port state	Whether to manually enable tracing for a clock source.
Virtual clock ID	Whether a virtual clock ID is configured.
Time lock success	Whether the device time is locked.
PTP profile	PTP profile the device is using.
Local clock ID	ID of the local clock. The value is set through the **ptp virtual-clock-id** command.
BMC run info	
Grand clock ID	ID of the grandmaster clock.
Receive number	Interface that receives signals of the clock source.
Parent clock ID	ID of the parent clock.
Parent portnumber	Interface that sends signals of the parent clock source.
Priority1	Priority1 of the clock source obtained from the master clock.
Priority2	Priority2 of the clock source obtained from the master clock.
Step removed	Number of communication channels between the local clock and the grandmaster clock, that is, number of BC devices.
Clock-accuracy	Accuracy of the clock source, which is obtained from the master clock.
Clock-class	Class of the clock source, which is obtained from the master clock.
Time Source	Time source of the clock source, which is obtained from the master clock.

Item	Description
UTC Offset	Offset between the Universal Time Coordinated (UTC) and International Atomic Time (TAI).
UTC Offset Valid	Whether the UTC offset takes effect.
Timescale	Time scale used by the PTP clock. The PTP protocol supports two types of time scales: • ARB • PTP
Time Traceable	Whether the time can be traced.
Frequence Traceable	Whether the clock frequency can be traced.
Source port	Clock source of the master clock.
Port info	
Name	Name of the interface enabled with PTP.
State	Status of the interface enabled with PTP: • Faulty: indicates that the interface is faulty. • Listening: indicates that the interface is being monitored. • Master: indicates that the interface is a master interface. • Passive: indicates that the interface is a passive port. • Premaster: indicates that the interface is a standby master interface. • Slave: indicates that the interface is a slave interface.
Delay-mech	Delay measurement mechanism used on an interface. The value is set through the **ptp delay-mechanism** command.
Ann-timeout	Timeout interval for waiting the Announce message. The value is set through the **ptp announce receipt-timeout** command.
Type	Type of an interface, which is usually the same as the type of the device. If the device type is TCandBC, the value is set through the **ptp port-type** command.

Item	Description
Domain	The clock domain of an interface should be the same as the device type. If the device type is TCandBC, the clock domain of the interface is set by the **ptp domain** command.
Clock source info	
Clock	Clock source.
Pri1	Priority1 of the clock source. The value is set through the **ptp clock-source** command.
Pri2	Priority2 of the clock source. The value is set through the **ptp clock-source** command.
Accuracy	Accuracy of the clock source. The value is set through the **ptp clock-source** command.
Class	Class of the clock source. The value is set through the **ptp clock-source** command.
TimeSrc	Time source of the clock source. The value is set through the **ptp clock-source** command.
In-Status	Whether the clock source is normal.
Port State	Port state.
Port Number	Port number of the clock source.
Recv Packet Statistics	Received packet statistics.
Send Packet Statistics	Sent packet statistics.
Discard Packet Statistics	Discarded packet statistics.

3.14.3 display ptp utc

Function

The **display ptp utc** command displays the Universal Time Coordinated (UTC) time.

Format

display ptp utc [**slot** *slot-id*]

Parameters

Parameter	Description	Value
slot *slot-id*	Displays the UTC time based on a slot ID.	The value range depends on the device configuration.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

UTC is also called the Greenwich Mean Time (GMT). The time displayed on the PTP device must be the UTC time.

The command is used to view the synchronization status of the UTC time. After two devices are synchronized, the UTC time should be the same.

The PTP supports two types of time scales: ARB and PTP.

- When the ARB time scale is used, the time can start from any time point and be reset by the management process. The slave clock obtains only the offset between the UTC time and TAI time in seconds. Therefore, the ARB time scale is used only to transmit the offset of the PTP time.
- When the PTP time scale is used, the system time is the UTC time adjusted according to *utc-offset*.

  The origin of the PTP time scale is 00:00:00 of January 1, 1970. The formula for converting the TAI time to the UTC time is: UTC = TAI - *utc-offset*. The *utc-offset* parameter indicates the accumulated offset between the current UTC and the TAI.

Example

Display the UTC time.

```
<HUAWEI> display ptp utc
Non-UTC Time:2009-12-30  20:43:39
```

Table 3-181 Description of the display ptp utc command output

Item	Description
Non-UTC Time	Non-standard UTC time converted according to the ARB time.

3.14.4 ptp announce-drop enable

Function

The **ptp announce-drop enable** command configures the interface of the PTP device to discard Announce messages.

The **undo ptp announce-drop enable** command restores the default mode of processing Announce messages on the interface of the PTP device.

By default, Announce messages are not discarded.

Format

ptp announce-drop enable

undo ptp announce-drop enable

Parameters

None.

Views

XGE interface view, 25GE interface view, 40GE interface view, 100GE interface view

Default Level

2: Configuration level

Usage Guidelines

Announce messages are advertisement messages in PTP, which are used to establish the master-slave hierarchy between devices. If the interface discards Announce messages, the device where the interface resides cannot receive clock synchronization information from other PTP devices. Usually, the **ptp announce-drop enable** command is configured on the interface at the user side to prevent the interface from receiving and processing Announce messages. This saves system resources.

Example

Configure the mode of processing Announce messages on XGigabitEthernet1/0/1 of the PTP device to **discard**.

```
<HUAWEI> system-view
[HUAWEI] interface xgigabitethernet 1/0/1
[HUAWEI-XGigabitEthernet1/0/1] ptp announce-drop enable
```

3.14.5 ptp announce-interval

Function

The **ptp announce-interval** command sets the interval for sending Announce packets on an interface of the PTP device.

The **undo ptp announce-interval** command restores the default interval for sending Announce packets on the interface of the PTP device.

By default, the interval for sending Announce packets is 128 ms.

Format

ptp announce-interval *announce-interval*

undo ptp announce-interval

Parameters

Parameter	Description	Value
announce-interval	Indicates that the interval for sending Announce packets on the interface is set to the *n*th power of 2 in milliseconds, where *n* is specified by *announce-interval*.	The value is an integer that ranges from 0 to 20. By default, the interval is 7 (128 ms).

Views

XGE interface view, 25GE interface view, 40GE interface view, 100GE interface view

Default Level

2: Configuration level

Usage Guidelines

Announce messages are advertisement messages in PTP, which are used to establish the master-slave hierarchy between devices. Announce packets ensure the exchange of clock synchronization information between PTP devices. If the value of the *announce-interval* is too small, devices frequently exchange PTP packets, which consume excessive bandwidth; if the value of the *announce-interval* is too great, the clock synchronization accuracy cannot be guaranteed. Therefore, while the clock synchronization accuracy is ensured, you should set the *announce-interval* to a larger value.

Example

Set the interval for sending Announce packets on XGigabitEthernet0/0/1 of the PTP device to 256 ms.

```
<HUAWEI> system-view
[HUAWEI] interface xgigabitethernet 0/0/1
[HUAWEI-XGigabitEthernet0/0/1] ptp announce-interval 8
```


3.14.6 ptp announce receipt-timeout

Function

The **ptp announce receipt-timeout** command configures the maximum timeout times of receiving Announce messages on an interface.

The **undo ptp announce receipt-timeout** command restores the default maximum timeout times of receiving Announce messages on an interface.

By default, the maximum timeout times of receiving Announce messages is 3.

Format

ptp announce receipt-timeout *timeout-value*

undo ptp announce receipt-timeout

Parameters

Parameter	Description	Value
timeout-value	Specifies the maximum timeout times of receiving Announce messages.	The value is an integer that ranges from 2 to 255. The default value is **3**.

Views

XGE interface view, 25GE interface view, 40GE interface view, 100GE interface view

Default Level

2: Configuration level

Usage Guidelines

Announce messages are advertisement messages in PTP, which are used to establish the master-slave hierarchy between devices. When the maximum timeout times of receiving Announce messages on an interface exceeds the specified threshold:

- In dynamic clock source selection: The local device configures the status of the 1588v2 interface as non-slave. That is, the 1588v2 interface does not synchronize the time with other devices.
- In static clock source selection: The 1588v2 interface status remains unchanged.

Timeout interval for receiving Announce messages on the local interface = Maximum timeout times of receiving Announce messages on the local interface (receipt-timeout) x Interval for sending Announce messages to the peer device (announce-interval) The interval for sending Announce messages to the peer

device (announce-interval) is set using the **ptp announce-interval** *announce-interval* command.

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

Example

Set the maximum timeout times of receiving Announce messages on XGigabitEthernet0/0/1 of the PTP device to 4.

```
<HUAWEI> system-view
[HUAWEI] interface xgigabitethernet 0/0/1
[HUAWEI-XGigabitEthernet0/0/1] ptp announce receipt-timeout 4
```

3.14.7 ptp asymmetry-correction

Function

The **ptp asymmetry-correction** command sets the delay offset value to ensure accurate time synchronization.

The **undo ptp asymmetry-correction** command restores the default delay offset.

By default, the asymmetry correction value of the PTP packet sent from the interface is not configured.

Format

ptp asymmetry-correction { **positive** | **negative** } *asymmetry-correction*

undo ptp asymmetry-correction

Parameters

Parameter	Description	Value
positive *asymmetry-correction*	Indicates the positive asymmetry correction value.	The value is an integer that ranges from 0 to 2000000, in ns. The default value is 0.
negative *asymmetry-correction*	Indicates the negative asymmetry correction value.	The value is an integer that ranges from 0 to 2000000, in ns. The default value is 0.

Views

XGE interface view, 25GE interface view, 40GE interface view, 100GE interface view

Default Level

2: Configuration level

Usage Guidelines

In case of path delay calculation, PTP measures the packet sending path only and considers the delays for sending and receiving packets as the same by default.

If the two delays are different or asymmetric, you need to configure an asymmetry correction value. In this case, the device automatically considers the asymmetry correction value in the path delay calculation complying with the Pdelay or Delay measurement mechanism.

Example

Set the delay offset value to 1 ns on XGigabitEthernet 0/0/1.

```
<HUAWEI> system-view
[HUAWEI] interface xgigabitethernet 0/0/1
[HUAWEI-XGigabitEthernet0/0/1] ptp asymmetry-correction positive 1
```

3.14.8 ptp clock-source

Function

The **ptp clock-source** command sets the attributes of the clock source and time source.

The **undo ptp clock-source** command cancels the settings.

For default values of the parameters, see the parameter description.

Format

ptp clock-source local { **clock-accuracy** *clock-accuracy* | **clock-class** *clock-class* | **priority1** *priority1* | **priority2** *priority2* | **time-source** *time-source* } **slot** *slot-id*

undo ptp clock-source local { **clock-accuracy** | **clock-class** | **priority1** | **priority2** | **time-source** } **slot** *slot-id*

NOTE

After G.8275.1 is enabled, only the **priority2** *priority2* and **time-source** *time-source* parameters are supported.

Parameters

Parameter	Description	Value
local	Indicates the local clock.	-

Parameter	Description	Value
clock-accuracy *clock-accuracy*	Specifies an attribute defining the accuracy of a clock.	The value of *clock-accuracy* is a hexadecimal number that is in the range of 0 to FF. You can set the value to 20-31 or 80-FD. The default accuracy of the local clock is 31. The accuracy values mapping the values of *clock-accuracy-value* are as follows: • 20: The time is accurate to within 25 ns. • 21: The time is accurate to within 100 ns. • 22: The time is accurate to within 250 ns. • 23: The time is accurate to within 1 us. • 24: The time is accurate to within 2.5 us. • 25: The time is accurate to within 10 us. • 26: The time is accurate to within 25 us. • 27: The time is accurate to within 100 us. • 28: The time is accurate to within 250 us. • 29: The time is accurate to within 1 ms. • 2A: The time is accurate to within 2.5 ms.

Parameter	Description	Value
		• 2B: The time is accurate to within 10 ms. • 2C: The time is accurate to within 25 ms. • 2D: The time is accurate to within 100 ms. • 2E: The time is accurate to within 250 ms. • 2F: The time is accurate to within 1s. • 30: The time is accurate to within 10s. • 31: The time is accurate to more than 10s. • 80 to FD: reserved for PTP features.

Parameter	Description	Value
clock-class *clock-class*	Specifies the attribute of an ordinary or boundary clock denotes the traceability of the time or frequency distributed by the grandmaster clock, that is the capability to trace the International Atomic Time (TAI).	The value of *clock-class* is an integer that ranges from 0 to 255. The default value of the local clock is 187. The capabilities to trace the TAI mapping the values of *clock-class-value* are as follows: • 0, 9, and 10: reserved to enable compatibility with future versions. • 1-5, 8, 11-12, 15-51, 53-57, 59-67, 123-127, 128-132, 171-186, 188-192, 194-215, 233-247, 249-250, 252-254: reserved. • 68-122, 133-170, 216-232: used by alternate PTP profiles. • 6: a clock that is synchronized to a primary reference time source. The timescale distributed is PTP. A clock of class 6 cannot be a slave to another clock in the domain. • 7: a clock that has previously been designated as class 6 but that has lost the capability to synchronize to a primary reference time source. The PTP system enters the holdover state and does not perform best clock source selection. The timescale distributed is PTP. A clock of class 7 cannot be a slave to

Parameter	Description	Value
		another clock in the domain. ● 13: a clock that is synchronized to an application specific source of time. The timescale distributed is ARB. A clock of class 13 cannot be a slave to another clock in the domain. ● 14: a clock that has previously been designated as class 13 but that has lost the capability to synchronize to an application specific source of time. The clock is in holdover mode and within holdover specifications. The timescale distributed is ARB. A clock of class 14 cannot be a slave to another clock in the domain. ● 52: Degradation alternative A for a clock of class 7 that is not within holdover specification. A clock of class 52 cannot be a slave to another clock in the domain. ● 58: Degradation alternative A for a clock of class 14 that is not within holdover specification. A clock of class 58 cannot be a slave to another clock in the domain. ● 187: Degradation alternative B for a clock of class 7 that is not within holdover specification. A clock

Parameter	Description	Value
		of class 187 can be a slave to another clock in the domain. • 193: Degradation alternative B for a clock of class 14 that is not within holdover specification. A clock of class 193 can be a slave to another clock in the domain. • 248: This clock class is used if none of the other clock class definitions apply. • 251: Reserved for version 1 compatibility. • 255: clock class of a slave-only clock.
priority1 *priority1*	Specifies a user configurable designation that a clock belongs to an ordered set of clocks from which a master is selected. The attribute priority1 is used in the execution of the best master clock algorithm.	The value of *priority1* is an integer that ranges from 0 to 255. The default value is 128. Lower values take precedence.
priority2 *priority2*	Specifies a user configurable designation that provides finer grained ordering among otherwise equivalent clocks. The attribute priority2 is used in the execution of the best master clock algorithm.	The value of *priority2* is an integer that ranges from 0 to 255. The default value is 128. Lower values take precedence.

Parameter	Description	Value
time-source *time-source*	Specifies the source of time used by the grandmaster clock.	The value of *time-source* is an integer that ranges from 1 to 8. The default value of the local clock is 8 (INTERNAL_OSCILLATOR). The attributes mapping the values of *time-source-value* are as follows: • 1: (0x10) ATOMIC_CLOCK • 2: (0x20) GPS • 3: (0x30) TERRESTRIAL_RADIO • 4: (0x40) PTP • 5: (0x50) NTP • 6: (0x60) HAND_SET • 7: (0x90) OTHER • 8: (0xa0) INTERNAL_OSCILLATOR
slot *slot-id*	Specifies the slot ID.	The value range depends on the device configuration.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

The **time-source** parameter specifies the clock source attribute used by the grandmaster clock device and the value is set according to the clock source connected to the device.

When the BMC algorithm is used by the PTP device for master clock selection, **priority1** > **clock-class** > **clock-accuracy** > **priority2** of each candidate time source is compared first. If the **priority1** of candidate time sources is the same, **clock-class** is compared, **clock-accuracy** and **priority2**. The time source with the highest priority is selected as the master clock.

A smaller *clock-class* value indicates a higher clock class. When the *clock-class* of a device is smaller than 128, the device cannot function as a slave clock. Therefore, do not set a high *clock-class* for a slave clock. Otherwise, the PTP interface of the slave clock cannot enter the slave state, and the device cannot synchronize with the master clock.

Example

Configure the time source of the local clock to ATOMIC_CLOCK.

```
<HUAWEI> system-view
[HUAWEI] ptp clock-source local time-source 1 slot 0
```

Set priority 1 of the local clock to 1.

```
<HUAWEI> system-view
[HUAWEI] ptp clock-source local priority1 1 slot 0
```

Set priority 2 of the local clock to 1.

```
<HUAWEI> system-view
[HUAWEI] ptp clock-source local priority2 1 slot 0
```

Set the class of the local clock to 10.

```
<HUAWEI> system-view
[HUAWEI] ptp clock-source local clock-class 10 slot 0
```

Set the accuracy of the local clock to 31 (accurate to >10s).

```
<HUAWEI> system-view
[HUAWEI] ptp clock-source local clock-accuracy 31 slot 0
```

3.14.9 ptp clock-source local local-priority

Function

The **ptp clock-source local local-priority** command sets the local priority for a local PTP clock source or an external clock source.

The **undo ptp clock-source local local-priority** command restores the default local priority of a local or external clock source.

By default, the local priority of a local PTP clock source or an external clock source is 128.

Format

ptp clock-source local local-priority *local-priority-value* **slot** *slot-id*

undo ptp clock-source local local-priority slot *slot-id*

Parameters

Parameter	Description	Value
local-priority *local-priority-value*	Specifies a local priority.	The value is an integer that ranges from 1 to 255.

Parameter	Description	Value
slot *slot-id*	Specifies the slot ID.	The value range depends on the device configuration.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenarios

According to the BMC algorithm in G.8275.1, when the local or external clock source competes with a line clock source and other attributes are the same, the two clock sources are compared against the local priority. The clock source with a lower local priority is preferentially selected.

Example

Set the local priority of a local PTP clock source to 120.

```
<HUAWEI> system-view
[HUAWEI] ptp clock-source local local-priority 120 slot 0
```

3.14.10 ptp clock-step

Function

The **ptp clock-step** command specifies the mode in which PTP packets that are used by PTP devices to perform time synchronization are timestamped.

The **undo ptp clock-step** command resets the mode in which PTP packets that are used by PTP devices to perform time synchronization are timestamped.

By default, the mode in which PTP packets are timestamped is **one-step**.

Format

ptp clock-step { **one-step** | **two-step** }

undo ptp clock-step

Parameters

Parameter	Description	Value
one-step	Indicates the one-step clock mode. In one-step clock mode, Sync messages in Delay mode and Pdelay_Resp messages in Pdelay mode are stamped with the time when they are sent.	-
two-step	Indicates the two-step clock mode. In two-step clock mode, Sync messages in Delay mode and Pdelay_Resp messages in Pdelay mode only record the time when they are generated, but carry no timestamps. The timestamps are carried in subsequent messages, that is, Follow_Up or Pdelay_Resp_Follow_Up messages.	-

Views

XGE interface view, 25GE interface view, 40GE interface view, 100GE interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The device adopts the one-step mode to timestamp outgoing PTP messages to communicate with other devices, and identify received Follow_Up messages in **two-step** mode. In this way, an interface in one-step clock mode can communicate with another interface in two-step clock mode.

Precautions

After the PTP device type is set to **e2etc**, **e2etcoc**, **p2ptc**, or **p2ptcoc** using the **ptp device-type**, the mode in which PTP messages are timestamped cannot be changed to **two-step** using the **ptp clock-step** command.

Example

Configure the two-step clock mode on XGigabitEthernet0/0/1.

```
<HUAWEI> system-view
[HUAWEI] interface xgigabitethernet 0/0/1
[HUAWEI-XGigabitEthernet0/0/1] ptp clock-step two-step
```


3.14.11 ptp delay-mechanism

Function

The **ptp delay-mechanism** command configures the delay measurement mechanism applied on the interface of a PTP device.

The **undo ptp delay-mechanism** command deletes the delay measurement mechanism applied on the interface of the PTP device.

By default, the delay measurement mechanism is only configured on the P2P transparent clock (P2PTC), E2E transparent clock (E2ETC), P2P transparent clock and ordinary clock (P2PTCOC), and E2E transparent clock and ordinary clock (E2ETCOC).

Format

ptp delay-mechanism { **delay** | **pdelay** }

undo ptp delay-mechanism

Parameters

Parameter	Description	Value
delay	Indicates that the delay measurement mechanism applied on the interface is in Delay mode.	-
pdelay	Indicates that the delay measurement mechanism applied on the interface is in Pdelay mode.	-

Views

XGE interface view, 25GE interface view, 40GE interface view, 100GE interface view

Default Level

2: Configuration level

Usage Guidelines

Usage scenario

PTP supports two delay measurement mechanisms:

- Delay request-response end to end (E2E) mechanism: calculates the time difference based on the total delay of the link between the master and slave clocks.
- Peer delay peer to peer (P2P) mechanism: calculates the time difference based on the delay of each link between the master and slave clocks.

In the P2P mechanism, the link delay of each interface must be measured separately. Different from the E2E mechanism, the P2P mechanism calculates and accumulates the forwarding delay and link delay to ensure accurate clock synchronization. If the master and slave clocks are far from each other and there are many TCs, the P2P mechanism will greatly reduce the clock synchronization efficiency and affect the clock synchronization effect. Therefore, when there is only one or two TCs, the P2P mechanism is recommended. When there are three or more TCs, the E2E mechanism is recommended.

Precautions

- OC and BC interfaces must be configured with the delay measurement mechanism before PTP is enabled.
- If the delay measurement mechanism is configured on an interface, to configure another delay measurement mechanism, you need to cancel the original configuration first.
- The corresponding delay measurement mechanism is applied on the E2ETC, E2ETCOC, P2PTC, P2PTCOC by default and cannot be modified; therefore, PTP can be directly enabled on interfaces of these devices.

Example

Configure the mode of the delay measurement mechanism of XGigabitEthernet0/0/1 on the PTP device as Delay.

```
<HUAWEI> system-view
[HUAWEI] ptp device-type bc
[HUAWEI] interface xgigabitethernet 0/0/1
[HUAWEI-XGigabitEthernet0/0/1] ptp delay-mechanism delay
```

3.14.12 ptp device-type

Function

The **ptp device-type** command configures the device type of a PTP device.

The **undo ptp device-type** command cancels the setting of the device type of a PTP device.

By default, the device type is not configured on a PTP device.

Format

ptp device-type { **bc** | **oc** | **e2etc** | **e2etcoc** | **p2ptc** | **p2ptcoc** | **tcandbc** | **t-bc** } **slot** *slot-id*

undo ptp device-type slot *slot-id*

NOTE

After G.8275.1 is enabled, only the **t-bc** parameter is supported.

Parameters

Parameter	Description	Value
oc	Indicates the ordinary clock (OC). An OC device has only one interface in the PTP domain, through which the local clock synchronizes with the upstream clock or advertises the time to the downstream clock.	-
bc	Indicates the boundary clock (BC). A BC device has multiple interfaces in the PTP domain. One of these interfaces synchronizes time from the upstream device, and the other interfaces advertise the time to the downstream device.	-
e2etc	Indicates the end to end transparent clock (E2ETC). A TC device does not participate in the calculation of the PTP clock and only transparently transmits PTP packets.	-
p2ptc	Indicates that the peer to peer transparent clock (P2PTC).	-
e2etcoc	Indicates the end to end transparent ordinary clock (E2ETCOC). A TCOC device is a special TC node. It synchronizes time in the same way as a TC device and can synchronize the clock frequency with the upstream device according to PTP packets.	-
p2ptcoc	Indicates the peer to peer transparent ordinary clock (P2PTCOC).	-
tcandbc	Indicates the transparent boundary clock.	-
t-bc	Indicates the telecom boundary clock.	-
slot *slot-id*	Specifies the ID of the slot where the PTP device resides.	The value range depends on the device configuration.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Each device can be configured with only one device type.

The PTP functions and parameters are not affected when you change the device type of the device. The device supports the following functions to simplify the configuration:

- Conversion between the BC, OC, and TCandBC modes
- Conversion between the E2ETC, P2PTC, E2ETCOC, and P2PTCOC modes

The PTP functions and parameters are not affected when you change the device type of the device. Before changing the device type, make sure that the conditions of the new device type are met. For example:

- To change the device type from BC or TCandBC to OC, make sure that the conditions of the OC are met, that is, PTP is enabled on only one interface. Otherwise, the following error information is displayed:
- To change the device type from OC to BC, make sure that the device is not in slave-only state. Otherwise, the following error information is displayed:
- To change the device type from E2ETCOC or P2PTCOC to E2ETC or P2PTC, make sure that no PTP-related configuration exists on the OC interface of the TCOC device. Otherwise, the following error information exists:
- If the original device type is TCandBC and the type of an interface is set to TC, when you switch the device type to OC or BC, the following error information is displayed:
- If the original device type is E2ETC or P2PTC, you can switch the device type to only E2ETCOC, or P2PTCOC. Otherwise, the following error information is displayed:

You set the device type of the PTP device and enable PTP on the device in a random sequence.

Precautions

- Running the **undo ptp device-type** command will clear the PTP configuration in the interface view. If the PTP device type is OC and the **ptp slaveonly slot** *slot-id* command is configured, running the **undo ptp device-type** command will also clear the **ptp slaveonly slot** *slot-id* command configuration. Exercise caution when running the **undo ptp device-type** command.
- When the device type of the device is set to TC, TCOC, or TCandBC (the interface type is TC):
  - Ensure that PTP packets are forwarded at the service layer. For example, on a ring network, you need to use ring network protocols to remove loops at the service layer.
  - On the TC device, the interfaces for receiving and sending PTP packets must be enabled with PTP. Otherwise, the resident time of the device cannot be calculated correctly. In this case, only packets are forwarded.
  - To ensure PTP time synchronization, ensure that PTP packets are first forwarded when the interface reaches the maximum rate.
- After the mode in which PTP messages are timestamped is changed to **two-step** using the **ptp clock-step** command, the **ptp device-type** command

cannot be used to configure the PTP device type to **e2etc**, **e2etcoc**, **p2ptc**, or **p2ptcoc**.

Example

Set the PTP device type to OC.

```
<HUAWEI> system-view
[HUAWEI] ptp device-type oc
```

3.14.13 ptp domain

Function

The **ptp domain** command configures the domain where the PTP device resides.

The **undo ptp domain** command restores the domain where the PTP device resides to the default value.

By default, the domain where the PTP device resides is PTP domain 0.

Format

ptp domain *domain-value*

undo ptp domain

Parameters

Parameter	Description	Value
domain-value	Specifies the domain that the clock source belongs to.	The value is an integer that ranges from 0 to 255.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

A physical time synchronization network can be logically divided into multiple clock domains. Each clock domain has a synchronization time, to which all devices in the domain are synchronized. Different clock domains have their own synchronization time, which is independent from each other.

Example

Set the value of the domain where the PTP device resides to 4.


```
<HUAWEI> system-view
[HUAWEI] ptp domain 4
```

3.14.14 ptp enable (interface view)

Function

The **ptp enable** command enables PTP on a certain interface of the device.

The **undo ptp enable** command disables PTP on a certain interface of the device.

By default, PTP is not enabled on the interface of the device.

Format

ptp enable

undo ptp enable

Parameters

None

Views

XGE interface view, 25GE interface view, 40GE interface view, 100GE interface view

Default Level

2: Configuration level

Usage Guidelines

Usage scenario

After PTP is enabled globally, enable PTP on an interface so that PTP can take effect.

Precautions

- Before enabling PTP, ensure that the interface supports PTP.
- The management interface and the sub interface cannot be enabled with PTP.

Pre-configuration tasks

- Before enabling PTP on an interface, you must run the **ptp device-type** command in the system view to set the device type.
- You must use the **ptp port-type** command to configure the clock mode of an interface on the TCandBC device.
- On the OC device, only one interface can be enabled with PTP.
- On the OC or BC device, you must use the **ptp delay-mechanism** command to configure the delay mechanism before enabling PTP.

Example

Enable PTP on XGigabitEthernet 0/0/1.

```
<HUAWEI> system-view
[HUAWEI] ptp device-type bc slot 0
[HUAWEI] interface xgigabitethernet 0/0/1
[HUAWEI-XGigabitEthernet0/0/1] ptp delay-mechanism delay
[HUAWEI-XGigabitEthernet0/0/1] ptp enable
```

3.14.15 ptp enable (system view)

Function

The **ptp enable** command enables PTP on the device.

The **undo ptp enable** command disables PTP on the device.

By default, PTP is disabled globally.

Format

ptp enable

undo ptp enable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Before using PTP, run the **ptp enable** command in the system view to enable PTP globally.

The **undo ptp enable** command will disable PTP and make all the PTP configuration become ineffective. To use PTP, reconfigure PTP.

Example

Enable PTP globally.

```
<HUAWEI> system-view
[HUAWEI] ptp enable
```


3.14.16 ptp local-priority

Function

The **ptp local-priority** command configures the local priority of a G.8275.1 interface.

The **undo ptp local-priority** command restores the default local priority of a G.8275.1 interface.

By default, the local priority of a G.8275.1 interface is 128.

Format

ptp local-priority *local-priority-value*

undo ptp local-priority [*local-priority-value*]

Parameters

Parameter	Description	Value
local-priority-value	Specifies the local priority of a G.8275.1 interface.	The value is an integer that ranges from 1 to 255.

Views

XGE interface view, 25GE interface view, 40GE interface view, 100GE interface view

Default Level

2: Configuration level

Usage Guidelines

According to the BMC algorithm in G.8275.1:

- When two line clock sources are compared and other attributes the same, the interface with a lower local priority is preferentially selected.
- When the local or external clock source competes with a line clock source and other attributes are the same, the two clock sources are compared against the local priority. The clock source with a lower local priority is preferentially selected.

Example

Set the local priority of a local G.8275.1 clock source to 120.

```
<HUAWEI> system-view
[HUAWEI] interface xgigabitethernet 0/0/1
[HUAWEI-XGigabitEthernet0/0/1] ptp local-priority 120
```


3.14.17 ptp mac-egress

Function

The **ptp mac-egress** command configures the MAC encapsulation mode for the PTP packets.

The **undo ptp mac-egress** command restores the default MAC encapsulation mode.

By default, PTP packets are encapsulated in MAC multicast mode and do not carry any VLAN tag.

Format

ptp mac-egress { **destination-mac** *destination-mac* | **vlan** *vlan-id* [**priority** *priority-value*] }

undo ptp mac-egress { **destination-mac** | **vlan** [**priority**] }

NOTE

In G.8275.1 mode, only the **destination-mac** *destination-mac* parameter is supported.

Parameters

Parameter	Description	Value
destination-mac *destination-mac*	Indicates the destination MAC address of the PTP packet. If the destination MAC address is not configured, the PTP packet is encapsulated in multicast mode by default and does not carry any VLAN tag.	The value is in the format of H-H-H. An H contains one to four hexadecimal numbers.
vlan *vlan-id*	Specifies the VLAN ID of PTP messages.	The value is an integer that ranges from 1 to 4094.
priority *priority-value*	Specifies the priority of VLAN packets.	The value is an integer that ranges from 0 to 7. The default value is 7, indicating the highest priority.

Views

XGE interface view, 25GE interface view, 40GE interface view, 100GE interface view

Default Level

2: Configuration level

Usage Guidelines

Usage scenario

You can configure the encapsulation mode for packets based on the Layer 2 network types of devices. If a device resides on a Layer 2 unicast network, configure a MAC address for the device. If a device resides on a multicast network, no MAC address needs to be configured for the device because a default multicast MAC address is defined.

Table 3-182 Default multicast MAC address for delay and Pdelay measurement mechanisms

Packet Type	MAC Address
All except peer delay measurement mechanisms	011B-1900-0000
Peer delay measurement mechanism	0180-C200-000E

Precautions

- This command is invalid for transparently transmitted packets.
- The MAC address cannot be 0000-0000-0000.
- Before configuring MAC encapsulation, delete the UDP encapsulation configuration if UDP encapsulation has been configured.
- MAC encapsulation is required when the VLAN ID to be encapsulated to sent or received packets is configured.
- After G.8275.1 is configured, only the default multicast MAC addresses 011B-1900-0000 and 0180-C200-000E can be configured.

Example

Configure the unicast MAC encapsulation for the PTP packet.

```
<HUAWEI> system-view
[HUAWEI] interface xgigabitethernet 0/0/1
[HUAWEI-XGigabitEthernet0/0/1] ptp mac-egress destination-mac 001B-1911-1100
```

Configure the multicast MAC encapsulation for the PTP packet.

```
<HUAWEI> system-view
[HUAWEI] interface xgigabitethernet 0/0/1
[HUAWEI-XGigabitEthernet0/0/1] ptp mac-egress vlan 2 priority 2
```


3.14.18 ptp min-delayreq-interval

Function

The **ptp min-delayreq-interval** command sets the minimum interval for sending Delay_Req messages on a 1588v2 interface.

The **undo ptp min-delayreq-interval** command restores the default minimum interval for sending Delay_Req messages on a 1588v2 interface.

By default, the minimum interval for sending 1588v2 Delay_Req messages on a 1588v2 interface is 128 ms, and the minimum interval for sending G.8275.1 Delay_Req messages on a 1588v2 interface is 64 ms.

Format

ptp min-delayreq-interval *min-delayreq-interval*

undo ptp min-delayreq-interval

Parameters

Parameter	Description	Value
min-delayreq-interval	Specifies that the minimum interval for sending Delay_Req messages on a 1588v2 interface is set to the min-pdelayreq-intervalth power of 2, in milliseconds.	The value is an integer that ranges from 0 to 20. In 1588v2 mode, the default value is 7, namely, 128 ms. In G.8275.1 mode, the default value is 6, namely, 64 ms. **Table 3-183** shows the mapping between the *min-delayreq-interval* value and the actual sending interval.

Table 3-183 Mapping between the *min-delayreq-interval* value and the actual sending interval

Value of min-delayreq-interval	Actual Interval
0	1 ms
1	2 ms
2	4 ms
3	8 ms
4	16 ms
5	32 ms
6	64 ms
7	128 ms
8	256 ms

Value of min-delayreq-interval	Actual Interval
9	512 ms
10	1s
11	2s
12	4s
13	8s
14	16s
15	32s
16	64s
17	128s
18	256s
19	512s
20	1024s

Views

XGE interface view, 25GE interface view, 40GE interface view, 100GE interface view

Default Level

2: Configuration level

Usage Guidelines

During 1588v2 clock synchronization, an Announce message is sent to determine the master-slave hierarchy, where the upstream node that advertises the synchronization time is the master device and the downstream node that receives the synchronization time is called the slave device. The master device sends Sync messages to the slave device to transmit performance parameters of time signals. In addition, the delay measurement mechanism can be implemented to ensure the accuracy of time signals.

Because the delay varies according to the network link, the 1588v2 time signals may be inaccurate. During 1588v2 clock synchronization, delay and Pdelay messages are transmitted to measure link delay, and time signals can be corrected based on the link delay. During the delay measurement request process, the local device sends a Delay_Req message and the peer device replies with a Delay_Resp message. There are two types of delay measurement mechanism.

- **delay**: specifies a delay request-response mechanism, in which information about the clock and time is calculated according to the delay of the entire link between the PTP device and the clock source. In this mode, the slave device sends a Delay_Req message to the master device, and the slave device

corrects time signals based on the Delay_Resp message replied by the master device.

- **pdelay**: specifies a peer delay mechanism, in which information about the time and clock is calculated according to the delay of each segment of the link between the PTP device and the clock source. In this mode, the slave device and master device exchange Pdelay_Req messages and time signals are corrected based on the Pdelay_Resq messages replied.

If *min-delayreq-interval* is set to a small value, PTP devices frequently exchange Delay_Req messages, occupying many bandwidth resources. If *min-delayreq-interval* is set to a large value, high-precision clock synchronization cannot be guaranteed. If the required clock synchronization accuracy is guaranteed, set *min-delayreq-interval* to a large value.

Example

Set the minimum interval for sending Delay_Req messages on the 1588v2 interface XGigabitEthernet 0/0/1 to 256 ms.

```
<HUAWEI> system-view
[HUAWEI] interface xgigabitethernet 0/0/1
[HUAWEI-XGigabitEthernet0/0/1] ptp min-delayreq-interval 8
```

3.14.19 ptp min-pdelayreq-interval

Function

The **ptp min-pdelayreq-interval** command configures the minimum interval for sending Pdelay_Req messages on a 1588v2 interface.

The **undo ptp min-pdelayreq-interval** command restores the default minimum interval for sending Pdelay_Req messages on a 1588v2 interface.

By default, the minimum interval for sending Pdelay_Req message is 128 ms.

Format

ptp min-pdelayreq-interval *min-pdelayreq-interval*

undo ptp min-pdelayreq-interval

Parameters

Parameter	Description	Value
min-pdelayreq-interval	Specifies that the minimum interval for sending Pdelay_Req messages on a 1588v2 interface is set to the **min-pdelayreq-interval** power of 2, in milliseconds.	The value is an integer that ranges from 0 to 20. The default value is 7, that is, 128 milliseconds. **Table 3-184** lists the mapping between the **min-pdelayreq-interval** value and the actual sending interval.

Table 3-184 Mapping between the **min-pdelayreq-interval** value and the actual sending interval

Value of min-pdelayreq-interval	Actual Interval
0	1 ms
1	2 ms
2	4 ms
3	8 ms
4	16 ms
5	32 ms
6	64 ms
7	128 ms
8	256 ms
9	512 ms
10	1s
11	2s
12	4s
13	8s
14	16s
15	32s
16	64s
17	128s
18	256s
19	512s
20	1024s

Views

XGE interface view, 25GE interface view, 40GE interface view, 100GE interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

During 1588v2 clock synchronization, an Announce message is sent to determine the master-slave hierarchy, where the upstream node that advertises the synchronization time is the master device and the downstream node that receives the synchronization time is called the slave device. The master device sends Sync messages to the slave device to transmit performance parameters of time signals. In addition, the delay measurement mechanism can be implemented to ensure the accuracy of time signals.

Because the delay varies according to the network link, the 1588v2 time signals may be inaccurate. During 1588v2 clock synchronization, delay and Pdelay messages are transmitted to measure link delay, and time signals can be corrected based on the link delay. During the delay measurement request process, the local device sends a Delay_Req message and the peer device replies with a Delay_Resp message. There are two types of delay measurement mechanism.

- **delay**: specifies a delay request-response mechanism, in which information about the clock and time is calculated according to the delay of the entire link between the PTP device and the clock source. In this mode, the slave device sends a Delay_Req message to the master device, and the slave device corrects time signals based on the Delay_Resp message replied by the master device.
- **pdelay**: specifies a peer delay mechanism, in which information about the time and clock is calculated according to the delay of each segment of the link between the PTP device and the clock source. In this mode, the slave device and master device exchange Pdelay_Req messages and time signals are corrected based on the Pdelay_Resq messages replied.

If *min-pdelayreq-interval* is set to a small value, PTP devices frequently exchange Pdelay_Req messages, occupying many bandwidth resources. If *min-pdelayreq-interval* is set to a large value, high-precision clock synchronization cannot be guaranteed. If the required clock synchronization accuracy is guaranteed, set *min-pdelayreq-interval* to a large value.

Example

Set the minimum interval for sending Pdelay_Req messages on the 1588v2 interface XGigabitEthernet 0/0/1 to 128 ms.

```
<HUAWEI> system-view
[HUAWEI] interface xgigabitethernet 0/0/1
[HUAWEI-XGigabitEthernet0/0/1] ptp min-pdelayreq-interval 7
```

3.14.20 ptp notslave disable

Function

The **ptp notslave disable** command configures the notslave attribute of a G.8275.1 interface as false.

The **undo ptp notslave disable** command restores the default notslave attribute of a G.8275.1 interface as true.

By default, the notslave attribute of a G.8275.1 interface is set to true.

Format

ptp notslave disable

undo ptp notslave disable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

To change the notslave attribute of a G.8275.1 interface, run the **ptp notslave disable** command. If the notslave attribute of a G.8275.1 interface is true, the G.8275.1 interface will never work in the slave state. If the notslave attribute of a G.8275.1 interface is false, the G.8275.1 interface can be in the slave state.

Prerequisites

The PTP device complies with the G.8275.1 profile.

Example

Set the nontslave attribute of a G.8275.1 interface to false.

```
<HUAWEI> system-view
[HUAWEI] ptp notslave disable
```

3.14.21 ptp port-state

Function

The **ptp port-state** command statically configures the status of a PTP interface.

The **undo ptp port-state** command restores the default status of a PTP interface.

By default, a statically specified PTPT interface is in the initializing state.

Format

ptp port-state { **slave** | **passive** | **master** | **premaster** | **listening** | **faulty** | **disabled** | **initializing** }

undo ptp port-state

Parameters

Parameter	Description	Value
slave	Configures the PTP interface status as slave. A slave interface traces external time information. A PTP device can be configured with only one slave interface.	-
passive	Configures the PTP interface status as passive. A passive PTP interface neither traces external time information nor advertises time information. A passive interface can send Pdelay_Req, Pdelay_Resp, delay_Resp_Follow_Up, and signaling messages as well as respond to management messages. If multiple PTP interfaces are detected as master devices in a domain, the PTP interface with the highest priority is selected as the master device and the local interface connected to this PTP interface is in the slave state. In this case, other local interfaces are in the passive state and back up the slave interface.	-
master	Configures the PTP interface status as master. A master PTP interface advertises time information to other devices.	-
premaster	Configures the PTP interface status as premaster. A premaster PTP interface neither traces external time information nor advertises time information. A premaster interface can send Pdelay_Req, Pdelay_Resp, delay_Resp_Follow_Up, and signaling messages as well as respond to management messages.	-
listening	Configures the PTP interface status as listening. A listening PTP interface neither traces external time information nor advertises time information. If a device originally functioning as a master clock is configured to be an OC working in slaveonly mode, or if the device becomes faulty, the status of the PTP interface on the device changes from master to listening.	-
faulty	Configures the PTP interface status as faulty. A faulty interface can only respond to some management messages on a link, instead of sending other PTP messages.	-
disabled	Configures the PTP interface status as disabled. A disabled PTP interface cannot send PTP messages, and discards all PTP messages except for management messages. The disabled status of a PTP interface equals to disabling the PTP function from the interface using the **undo ptp enable** command in the interface view.	-
initializing	Configures the PTP interface status as initializing. An initializing PTP interface initializes the data set, hardware information, and communication device information. In case of an initializing PTP interface, all interfaces on the clock node are prohibited from sending PTP messages.	-

Views

XGE interface view, 25GE interface view, 40GE interface view, 100GE interface view

Default Level

2: Configuration level

Usage Guidelines

Static clock source selection and dynamic BMC clock source selection are two independent sets of clock source selection mechanism. The priority of static clock source selection is higher than that of dynamic BMC clock source selection. You can fix the master-slave relationship between clock nodes within a network by statically configuring the status of PTP interfaces on them. In this way, the reference clock source is not selected through BMC algorithm.

Example

Configure the PTP interface to be in the slave state.

```
<HUAWEI> system-view
[HUAWEI] ptp set-port-state enable
[HUAWEI] interface xgigabitethernet 0/0/1
[HUAWEI-XGigabitEthernet0/0/1] ptp port-state slave
```

3.14.22 ptp port-type

Function

The **ptp port-type** command configures the clock mode of an interface on a TCandBC device.

The **undo ptp port-type** command deletes the clock mode configured on the interface on a TCandBC device.

By default, the PTP clock mode is not configured on the interface.

Format

ptp port-type { **bc** | **tc** }

undo ptp port-type

Parameters

Parameter	Description	Value
bc	Indicates that the clock mode configured on the interface of the TCandBC is BC.	-

Parameter	Description	Value
tc	Indicates that the clock mode configured on the interface of the TCandBC is TC.	-

Views

XGE interface view, 25GE interface view, 40GE interface view, 100GE interface view

Default Level

2: Configuration level

Usage Guidelines

Usage scenario

The device supports the TCandBC clock mode. In this case, you can configure the clock mode of the interface to TC or BC. If the original clock mode of the interface is BC or OC, and the interface is enabled with PTP, the clock mode of the interface changes to BC after the device clock mode is changed to TC and BC mode.

Precautions

- This command is invalid when G.8275.1 is enabled.
- If the interface is enabled with PTP, the **ptp port-type** command is invalid.
- Before delete the clock mode of the interface of the TCandBC device, you must first clear the clock domain of the interface, if the clock mode is TC and the clock domain of the interface is configured.

Example

Configure the clock mode of XGigabitEthernet0/0/1 interface on the TCandBC device to BC.

```
<HUAWEI> system-view
[HUAWEI] ptp device-type tcandbc
[HUAWEI] interface xgigabitethernet 0/0/1
[HUAWEI-XGigabitEthernet0/0/1] ptp port-type bc
```

3.14.23 ptp profile g-8275-1 enable

Function

The **ptp profile g-8275-1 enable** command configures PTP to comply with ITU-T G.8275.1.

The **undo ptp profile g-8275-1 enable** command cancels configuring PTP to comply with ITU-T G.8275.1. That is, PTP complies with IEEE 1588v2.

By default, PTP complies with IEEE 1588v2.

Format

ptp profile g-8275-1 enable

undo ptp profile g-8275-1 enable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

ITU-T G.8275.1 is a new PTP protocol designed for the telecom domain. To switch the 1588v2 profile to the G.8275.1 profile, run the **ptp profile g-8275-1 enable** command. To switch the G.8275.1 profile to the 1588v2 profile, run the **undo ptp profile g-8275-1 enable** command.

Configuration Impact

After the ITU-T G.8275.1 profile is configured, all the configurations related to IEEE 1588v2 in the system view and interface view are deleted, and the PTP configurations are restored to the default values. In addition, the default values of value ranges of the **domain**, **sync-interval**, and **delayreq-interval** parameters are changed. However, the function to globally enable PTP (using the **ptp enable** command) is not affected.

Example

Configure the ITU-T G.8275.1 profile.

```
<HUAWEI> system-view
[HUAWEI] ptp profile g-8275-1 enable
```

3.14.24 ptp set-port-state enable

Function

The **ptp set-port-state enable** command enables the function to statically specify the interface status.

The **undo ptp set-port-state enable** command disables the function to statically specify the interface status.

By default, the function to statically specify the interface status is disabled.

Format

ptp set-port-state enable slot *slot-id*

undo ptp set-port-state enable slot *slot-id*

Parameters

Parameter	Description	Value
slot *slot-id*	Specifies a slot ID.	The value depends on the device configuration.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

In a 1588v2/G.8275.1 clock synchronization network, all clock nodes work in the master-slave relationship. By default, the master-slave relationship between clock nodes is calculated through the BMC algorithm. To fix the master-slave relationship between clock nodes within a network, run the **ptp set-port-state enable** command to enable the function to statically specify the 1588v2/G.8275.1 interface status and then run the **ptp port-state** command to specify the clock synchronization status of all interfaces (except for the TC interface). After the **ptp set-port-state enable** command is run in the system view, all 1588v2/G.8275.1 interfaces are in the initializing state by default.

The following considerations apply when statically configuring the 1588v2 interface status:

- The status of a TC interface is fixed to be premaster. Therefore, you cannot change the status of TC interfaces, including all the 1588v2 interfaces on the E2ETC and P2PTC devices and TC interfaces on the E2ETCOC and P2PTCOC devices using commands.
- If the status of a 1588v2 interface has been specified and the device mode needs to be switched to E2ETC, P2PTC, E2ETCOC, or 2PTCOC, delete the 1588v2 interface status configuration.
- A 1588v2 device can be configured with only one slave interface.

Ensure that a G.8275.1 device is configured with only one slave interface.

Example

Enable the function to statically specify the interface status.

```
<HUAWEI> system-view
[HUAWEI] ptp set-port-state enable slot 0
```


3.14.25 ptp slaveonly

Function

The **ptp slaveonly** command sets the attribute of the clock source interface of the OC to slave-only.

The **undo ptp slaveonly** command restores the default status of the PTP interface of the OC.

By default, the clock source interface can be a master interface or a slave interface.

Format

ptp slaveonly slot *slot-id*

undo ptp slaveonly slot *slot-id*

Parameters

Parameter	Description	Value
slot *slot-id*	Specifies the ID of the slot where the OC with the PTP interface in the slave state resides.	The value range depends on the device configuration.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage scenario

When an OC functions as the last clock node, the OC receives clock signals from an upstream device and sends the clock signals to clients. To prevent clock signals of clients from affecting the PTP system, configure the interface status of the OC to slave-only. This configuration ensures that the OC does not synchronize the clock signals of clients.

The OC in a domain has only one PTP interface. If the interface status of the OC is set to slave-only, no interface can switch to the master.

Example

Set the attribute of the clock source interface to slave-only on the OC.


```
<HUAWEI> system-view
[HUAWEI] ptp device-type oc slot 0
[HUAWEI] ptp slaveonly slot 0
```

3.14.26 ptp sync-interval

Function

The **ptp sync-interval** command sets the interval for sending Sync packets from an interface.

The **undo ptp sync-interval** command restores the default interval for sending Sync packets from an interface.

By default, the interval for sending 1588v2 Sync packets is 8 ms, the interval for sending G.8275.1 Sync packets is 64 ms.

Format

ptp sync-interval *sync-interval*

undo ptp sync-interval

Parameters

Parameter	Description	Value
sync-interval	Indicates that the interval for sending Sync packets on an interface is set to the *n*th power of 2 in milliseconds, where *n* is specified by *sync-interval*.	The value is an integer that ranges from 0 to 20. In 1588v2 mode, the default value is 3. That is, the interval is 8 ms. In G.8275.1 mode, the default value is 6. That is, the interval is 64 ms.

Views

XGE interface view, 25GE interface view, 40GE interface view, 100GE interface view

Default Level

2: Configuration level

Usage Guidelines

Usage scenario

Sync packets are used to generate timestamps when the delay mechanism is used. Based on the generated timestamps, PTP calculates the link delay and implements clock synchronization. The interval for sending Sync packets affects the clock synchronization accuracy. A higher interval indicates a higher clock synchronization accuracy. However, a high packet sending interval will increase the

network load. Therefore, configure the interval for sending Sync packets according to networking requirements.

Example

Set the interval for sending Sync packets to 128 ms on XGigabitEthernet0/0/1.

```
<HUAWEI> system-view
[HUAWEI] interface xgigabitethernet 0/0/1
[HUAWEI-XGigabitEthernet0/0/1] ptp sync-interval 7
```

3.14.27 ptp tcoc-clock-id

Function

The **ptp tcoc-clock-id** command, you can specify a clock source for an OC interface on the TCOC device to synchronize.

The **undo ptp tcoc-clock-id** command cancels the previous setting.

By default, no clock source is specified for a TCOC device to synchronize.

Format

ptp tcoc-clock-id *clock-source-id* **port-num** *port-num*

undo ptp tcoc-clock-id

Parameters

Parameter	Description	Value
clock-source-id	Specifies the ID of the peer clock source (ID of the static clock source).	The format is HHHHHHHH. H is a two-digit hexadecimal number, such as E0 and FC.

Parameter	Description	Value
port-num *port-num*	Indicates the number of the interface where the peer master clock is located. The value is converted from the x/y/z format of the interface number. x stands for the slot number, y stands for the sub-card number, and z stands for the interface number. To convert the port number from the x/y/z format into an integer, you need to first convert x into a 6-bit binary number; y into a 2-bit binary number; z into an 8-bit binary number. Then, rank these binary numbers in the format of x/y/z to obtain a 16-bit binary number. Convert the 16-bit binary number into a decimal number, which is the *port-num* value. For example, port number 2/0/1 on the master clock is converted into 2049.	The value is an integer that ranges from 0 to 65535.

Views

XGE interface view, 25GE interface view, 40GE interface view, 100GE interface view

Default Level

2: Configuration level

Usage Guidelines

Usage scenario

The **ptp tcoc-clock-id** command specifies the interface from which the local device synchronizes the clock frequency. The *clock-source-id* and *port-num* parameter of the command specify the port identify. The local device accepts only the PTP packets with specified clock ID and port number.

Precautions

- A TCOC device cannot synchronize the time. It can synchronize only the frequency; therefore, it can be configured with only one interface.
- *clock-source-id* specifies the clock ID of the peer master clock source device and *port-num* specifies the number of the peer master clock interface. If the values of *clock-source-id* and *port-num* are incorrect or the specified master clock source is faulty, synchronization cannot be performed.

Example

Set ID of the clock source for XGigabitEthernet0/0/1 on the TCOC device to 122323FFFE122110.

```
<HUAWEI> system-view
[HUAWEI] ptp device-type e2etcoc slot 0
[HUAWEI] interface xgigabitethernet 0/0/1
[HUAWEI-XGigabitEthernet0/0/1] ptp tcoc-clock-id 122323FFFE122110 port-num 1
```

3.14.28 ptp udp-egress

Function

The **ptp udp-egress** command sets the UDP encapsulation mode for PTP packets.

The **undo ptp udp-egress source-ip** command restores the encapsulation mode for PTP packets to MAC encapsulation mode.

Using the **undo ptp udp-egress** { **destination-ip** | **destination-mac** | **dscp** | **vlan** | **priority** } command, you can restore the default configuration of the UDP encapsulation mode.

By default, PTP packets are encapsulated in MAC multicast mode. If UDP encapsulation is configured, multicast UDP encapsulation is used by default.

Format

ptp udp-egress source-ip *source-ip* [**destination-ip** *destination-ip*] [**dscp** *dscp*] [**vlan** *vlan-id* [**priority** *priority*]]

ptp udp-egress destination-mac *destination-mac*

undo ptp udp-egress { **source-ip** | **destination-ip** | **destination-mac** | **dscp** | **vlan** | **priority** }

Parameters

Parameter	Description	Value
source-ip *source-ip*	Indicates the source IP address of the UDP-encapsulated PTP packets.	The value is in dotted decimal notation.
destination-ip *destination-ip*	Indicates the destination IP address of the UDP-encapsulated PTP packets.	The value is in dotted decimal notation.

Parameter	Description	Value
destination-mac *destination-mac*	Indicates the destination MAC address of the UDP-encapsulated PTP packets.	The value is in the format of H-H-H. An H contains one to four hexadecimal numbers.
dscp *dscp*	Indicates the Differentiated Service Code Point (DSCP) priority carried in the UDP-encapsulated PTP packets.	The value is an integer that ranges from 0 to 63. The default value is 56.
vlan *vlan-id*	Indicates the VLAN ID encapsulated in the PTP packets.	The value is an integer that ranges from 1 to 4094.
priority *priority*	Indicates the 802.1p priority carried in the VLAN-encapsulated packet.	The value is an integer that ranges from 0 to 7. The default value is 7, indicating the highest priority.

Views

XGE interface view, 25GE interface view, 40GE interface view, 100GE interface view

Default Level

2: Configuration level

Usage Guidelines

Usage scenario

By default, PTP packets are encapsulated in multicast MAC mode. You can use the **ptp udp-egress** command to change the encapsulation mode to UDP encapsulation to implement Layer 3 encapsulation.

UDP encapsulation is further classified into unicast UDP encapsulation and multicast UDP encapsulation.

- Unicast encapsulation

  In this encapsulation mode, you need to set the unicast destination IP address of PTP packets.
- Multicast encapsulation

  Table 3-185 shows destination IP addresses that can be used only in the multicast UDP encapsulation.

Table 3-185 Default multicast IP address for delay and Pdelay measurement mechanisms

Delay Mechanism	IP Address
All except peer delay	224.0.1.129
Peer delay	224.0.0.107

In multicast UDP encapsulation mode, you do not need to set the destination IP address.

Precautions

Before using the **ptp udp-egress destination-mac** *destination-mac* command to configure the destination MAC address for UDP encapsulation, configure the source IP address for UDP encapsulation. The destination MAC address cannot be all 0s or a multicast address.

Example

Configure the PTP packet to be encapsulated in UDP unicast mode. Set the source IP address of the PTP packet to 192.168.2.2 and the destination IP address to 192.168.1.1.

```
<HUAWEI> system-view
[HUAWEI] interface xgigabitethernet 0/0/1
[HUAWEI-XGigabitEthernet0/0/1] ptp udp-egress source-ip 192.168.2.2 destination-ip 192.168.1.1
```

3.14.29 ptp virtual-clock-id

Function

The **ptp virtual-clock-id** command configures the virtual clock ID on the PTP device.

The **undo ptp virtual-clock-id** command restores the automatically generated clock ID on the PTP device.

By default, no virtual clock ID is configured on the PTP device. The clock ID is generated by padding fffe to the middle of the system bridge MAC address. For example, if the system bridge MAC address is 111122223333, the default clock ID is 111122fffe223333.

Format

ptp virtual-clock-id *clock-id-value* **slot** *slot-id*

undo ptp virtual-clock-id slot *slot-id*

Parameters

Parameter	Description	Value
clock-id-value	Specifies the lower four bytes of a virtual clock ID. The lower four bytes of the virtual clock ID are configurable, whereas the higher four bytes are automatically allocated by the system. The value of the higher four bytes automatically allocated by the system is 0x00259e32.	The value range is 00000001-ffffffff in the form of a hexadecimal number.
slot *slot-id*	Specifies the ID of the slot where the involved PTP device resides.	The value range depends on the device configuration.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

The 8-byte clock ID uniquely identifies a PTP device in the PTP domain. When a PTP device performs the master-slave switchover, the clock ID of the PTP device changes along with the system bridge MAC address. As a result, the clock ID may not uniquely identify the PTP device.

By using the **ptp virtual-clock-id** command, you can specify the clock ID of a PTP device. The specified clock ID does not change in the case of the master-slave switchover, and can therefore uniquely identify the PTP device. The lower four bytes of the virtual clock ID are configurable, whereas the higher four bytes are automatically allocated by the system.

Example

Set the lower four bytes of the virtual clock ID on the PTP device to **00000123**.

```
<HUAWEI> system-view
[HUAWEI] ptp virtual-clock-id 00000123 slot 0
```


3.14.30 reset ptp statistics

Function

The **reset ptp statistics** command clears statistics on PTP packets on the interface of a device.

Format

reset ptp statistics { **all** [**slot** *slot-id*] | **interface** *interface-type interface-number* }

Parameters

Parameter	Description	Value
all	Clears statistics on the received PTP packets of all interfaces.	-
interface *interface-type interface-number*	Clears statistics on the received PTP packets of a specified interface. • *interface-type* specifies the type of an interface. • *interface-number* specifies the number of an interface.	-
slot *slot-id*	Clears statistics on the received PTP packets of all interface with a specified slot ID.	The value range depends on the device configuration.

Views

User view

Default Level

2: Configuration level

Usage Guidelines

You can use the **reset ptp statistics** command to clear the statistics on the received PTP packets of a specified interface or all interfaces by restoring the counter.

Example

Clear the statistics on PTP packets on XGigabitEthernet0/0/1.

```
<HUAWEI> reset ptp statistics interface xgigabitethernet 0/0/1
```

3.15 Clock Synchronization Commands

3.15.1 Command Support

Only the following models support synchronous Ethernet:

Model	Supported Part Number	Unsupported Part Number
S6730-H24X6C	• 02352FSG, 02352FSG-001, 02352FSG-003, 02352FSG-005, 02352FSG-006 • 02353GFC, 02353GFC-001, 02353GFC-003	• 02352FSG-007, 02352FSG-008 • 02353GFC-004
S6730-H48X6C	• 02352FSF, 02352FSF-003, 02352FSF-005, 02352FSF-007, 02352FSF-008, 02352FSF-011 • 02353FWL, 02353FWL-003, 02353FWL-005	• 02352FSF-009, 02352FSF-010 • 02353FWL-006
S6730-H24X4Y4C	None	No part number supports this model.
S6730-H28Y4C	None	No part number supports this model.
S6730S-H24X6C-A	• 02353HVK, 02353HVK-001, 02353HVK-003	02353HVK-004

3.15.2 clock alarm-threshold frequency-offset

Function

The **clock alarm-threshold frequency-offset** command configures an alarm threshold for frequency offset.

The **undo clock alarm-threshold frequency-offset** command restores the default alarm threshold of frequency offset.

By default, the alarm threshold of frequency offset is 9200 ppb.

Format

clock alarm-threshold frequency-offset *frequency-offset-value*

undo clock alarm-threshold frequency-offset [*frequency-offset-value*]

Parameters

Parameter	Description	Value
frequency-offset-value	Specifies the alarm threshold of frequency offset.	The value is an integer that ranges from 10 to 92, in 100 ppb. The default value is 92.

Views

System view

Default Level

3: Management level

Usage Guidelines

Frequency offset can be performed on a list of clock sources. If the frequency offset value of a clock source exceeds the specified threshold, the clock source is abnormal and does not participate in clock source selection. To configure an alarm threshold for frequency offset, run the **clock alarm-threshold frequency-offset** command.

Example

Configure the alarm threshold of frequency offset as 6000 ppb.

```
<HUAWEI> system-view
[HUAWEI] clock alarm-threshold frequency-offset 60
```

3.15.3 clock clear

Function

The **clock clear** command restores the automatic clock source selection mode.

Format

clock clear slot *slot-id*

Parameters

Parameter	Description	Value
slot *slot-id*	Specifies a slot ID.	The value range depends on the device configuration.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

To clear configurations of the manual or forcible clock source selection mode and restore the automatic clock source selection mode, run the **clock clear** command.

Example

Restore the automatic clock source selection mode for the clock source in slot 0.

```
<HUAWEI> system-view
[HUAWEI] clock clear slot 0
```

3.15.4 clock ethernet-synchronization enable

Function

The **clock ethernet-synchronization enable** command enables synchronous Ethernet.

The **undo clock ethernet-synchronization enable** command disables synchronous Ethernet.

By default, synchronous Ethernet is not enabled.

Format

clock ethernet-synchronization enable

undo clock ethernet-synchronization enable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

To enable synchronous Ethernet, run the **clock ethernet-synchronization enable** command. After synchronous Ethernet is enabled on a switch, the switch selects the clock signal sent through Ethernet interfaces as the clock source.

The synchronous Ethernet function of an interface needs to be enabled both globally and on this interface. If the global synchronous Ethernet configuration is disabled, the synchronous Ethernet configuration on the interface is not deleted, but this function becomes unavailable.

Example

Enable synchronous Ethernet on a switch.

```
<HUAWEI> system-view
[HUAWEI] clock ethernet-synchronization enable
```

3.15.5 clock freq-deviation-detect enable

Function

The **clock freq-deviation-detect enable** command enables frequency offset check on clock signals.

The **undo clock freq-deviation-detect enable** command disables frequency offset check on clock signals.

By default, frequency offset check on clock signals is not enabled.

Format

clock freq-deviation-detect enable

undo clock freq-deviation-detect enable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

If the clock synchronization network has high requirements for frequency offset of clock signals, run the **clock freq-deviation-detect enable** command to enable frequency offset check. After this function is enabled, the system performs frequency offset check on clock signals. If the frequency offset value exceeds the specified threshold, the system considers that the clock source is unreliable and triggers another automatic clock source selection.

Frequency offset check on a clock source helps determine whether the quality of the clock source is good or not. If the frequency offset value of a clock source exceeds the specified threshold, the system clock does not trace this clock source any more. To configure the range of frequency offset check, run the **clock alarm-threshold frequency-offset** *frequency-offset-value* command.

Example

Enable frequency offset check on clock signals.


```
<HUAWEI> system-view
[HUAWEI] clock freq-deviation-detect enable
```

3.15.6 clock map unk

Function

The **clock map unk** command maps a clock source with the SSM quality level of UNK to a new SSM quality level.

Format

clock map unk { **prc** | **ssua** | **ssub** | **sec** | **dnu** }

Parameters

Parameter	Description	Value
prc	Indicates G.811 clock signals with the SSM quality level of PRC.	-
ssua	Indicates G.812 transit node clock signals with the SSM quality level of SSUA.	-
ssub	Indicates G.812 local node clock signals with the SSM quality level of SSUB.	-
sec	Indicates SDH clock source signals with the SSM quality level of SEC.	-
dnu	Indicates that the clock with the SSM quality level of DNU cannot function as a clock source.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

If the SSM quality level of an upstream clock source is UNK, to allow switches to trace this clock source, run the **clock map unk** command to map the upstream clock source to a new SSM quality level. By default, a clock source with the SSM quality level of UNK is mapped to the SSM quality level of DNU. In this case, if SSM control is enabled also, the clock source does not participate in clock source selection.

By default, when SSM control is enabled, the clock source with the SSM quality level of UNK does not participate in clock source selection.

Example

Map the clock source with the SSM quality level of UNK to the SSM quality level of PRC.

```
<HUAWEI> system-view
[HUAWEI] clock map unk prc
```

3.15.7 clock priority (interface view)

Function

The **clock priority** command sets the priority of a clock source.

The **undo clock priority** command restores the default priority of a clock source.

By default, the priority of a clock source is 0.

Format

clock priority *priority-value*

undo clock priority

Parameters

Parameter	Description	Value
priority-value	Specifies the priority of a clock source.	The value is an integer that ranges from 1 to 255. A smaller value indicates a higher priority.

Views

XGE interface view, 25GE interface view, 40GE interface view, 100GE interface view

Default Level

2: Configuration level

Usage Guidelines

By default, the priority of a clock source is 0, indicating that the clock source does not participate in clock source selection.

In automatic clock source selection mode, a clock source can participate in clock source selection only when a priority is configured. In manual and forcible clock source selection modes, clock source switching can be performed regardless of the clock source priority. In this case, whether a priority is configured does not affect the switching result. To set the priority of a clock source, run the **clock priority** command.

Example

Set the priority of the clock source on the interface XGE0/0/1 to 10.


```
<HUAWEI> system-view
[HUAWEI] interface xgigabitethernet 0/0/1
[HUAWEI-XGigabitEthernet0/0/1] clock priority 10
```

3.15.8 clock source ptp priority (system view)

Function

The **clock source ptp priority** command sets the priority of a ptp clock source.

The **undo clock source ptp priority** command restores the default priority of a ptp clock source.

The default priority of a ptp clock source is 0.

Format

clock source ptp priority *priority-value* **slot** *slot-id*

undo clock source ptp priority slot *slot-id*

Parameters

Parameter	Description	Value
priority-value	Specifies the priority of a clock source.	The value is an integer that ranges from 1 to 255. The default value is 0. A smaller value indicates a higher priority.
slot *slot-id*	Specifies a slot ID.	The value range depends on the device configuration.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

When PTP is enabled and the PTP clock is a slave clock, the frequency of the PTP clock can be used as a line clock to participate in clock source selection.

In automatic clock source selection mode, a clock source can participate in clock source selection only when a priority is configured. In manual and forcible clock source selection modes, clock source switching can be performed regardless of the clock source priority. In this case, whether a priority is configured does not affect the switching result. To set the priority of a clock source, run the **clock source priority** command.

Example

Set the priority of the PTP clock source in slot 0 to 15.


```
<HUAWEI> system-view
[HUAWEI] clock source ptp priority 15 slot 0
```

3.15.9 clock run-mode

Function

The **clock run-mode** command configures a clock node to work in free, hold, or normal mode.

By default, a clock node works in normal mode.

Format

clock run-mode { **free** | **hold** | **normal** } **slot** *slot-id*

Parameters

Parameter	Description	Value
free	Indicates that a clock node works in free mode.	-
hold	Indicates that a clock node works in hold mode.	-
normal	Indicates that a clock node works in normal mode.	-
slot *slot-id*	Specifies a slot ID.	The value range depends on the device configuration.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

To configure the working mode of a clock node, run the **clock run-mode** command.

- In free mode, a clock node does not select a clock source using the clock source selection algorithm.
- In hold mode, a clock node retains the locked frequency.
- In normal mode, a clock node selects a clock source using the clock source selection algorithm. If no clock source is available, the clock node automatically enters the free or hold mode.

A clock node working in free mode cannot enter the hold mode using this command.

Example

Configure the clock node in slot 0 to work in free mode.

```
<HUAWEI> system-view
[HUAWEI] clock run-mode free slot 0
```

3.15.10 clock source

Function

The **clock source** command sets the clock source selection mode to manual or forcible and specifies the master clock source.

By default, the automatic clock source selection mode is used.

Format

clock { **manual** | **force** } **source** { **ptp slot** *slot-id* | **interface** *interface-type interface-number* }

Parameters

Parameter	Description	Value
manual	Indicates that the manual clock source selection mode is used.	-
force	Indicates that the forcible clock source selection mode is used.	-
ptp	Indicates that an PTP clock source is used as the clock source.	-
interface *interface-type interface-number*	Specifies the input interface of the clock source. • *interface-type*: specifies the interface type. • *interface-number*: specifies the interface number.	-
slot *slot-id*	Specifies the slot ID of the master clock source.	The value range depends on the device configuration.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

To configure the clock source selection mode as manual or forcible, run the **clock source** command. In manual clock source selection mode, a clock source can be switched to a clock source with a higher SSM quality level, regardless of the clock source priority. In forcible clock source selection mode, a clock can be selected regardless of the SSM quality level and priority.

Precautions

In manual clock source selection mode, a clock source takes effect only when the following conditions are met:

- The synchronous Ethernet function is enabled.
- The SSM quality level is the highest and not DNU.
- The status of the selected clock source is not abnormal or initial.

In forcible clock source selection mode, a clock source takes effect only when the following conditions are met:

- The synchronous Ethernet function is enabled.

If a clock source in manual clock source selection mode does not meet conditions, the clock source automatically switches to the automatic clock source selection mode. If a clock source in forcible clock source selection mode does not meet conditions, for example, the clock source is abnormal, the clock source automatically switches to the hold mode. After the clock source is restored, it is automatically selected again.

A manually selected clock source is used temporarily and no configuration file is generated. To permanently use a clock source, use the forcible clock source selection mode.

The latest configuration of manual clock source selection overrides the previous configuration of manual clock source selection but not forcible clock source selection. The latest configuration of forcible clock source selection overrides the previous configuration of manual or forcible clock source selection.

Example

Set the clock source selection mode to manual and specify the input interface of the master clock source as XGE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] clock manual source interface xgigabitethernet 0/0/1
```

3.15.11 clock source-lost holdoff-time

Function

The **clock source-lost holdoff-time** command configures the holdoff time for the system to consider a clock source lost.

By default, the holdoff time for the system to consider a clock source lost is 1000 ms.

Format

clock source-lost holdoff-time *value*

Parameters

Parameter	Description	Value
value	Specifies the holdoff time for the system to consider a clock source lost.	The value is an integer that ranges from 300 to 1800, in milliseconds.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

The system considers a clock source lost after a specified holdoff time. Within this period, the system considers that the clock source exists. Setting the holdoff time can avoid some mistakes in determining the clock source caused by occasional signal jitter on the network. To set the holdoff time for the system to consider a clock source lost, run the **clock source-lost holdoff-time** command.

If clock source switching needs to be implemented as soon as possible, set **holdoff-time** to a small value. To prevent frequent clock source switching, set **holdoff-time** to a large value.

Example

Set the holdoff time for the system to consider a clock source lost to 400 ms.

```
<HUAWEI> system-view
[HUAWEI] clock source-lost holdoff-time 400
```

3.15.12 clock source ptp ssm (system view)

Function

The **clock source ptp ssm** command configures the SSM quality level of a clock source.

The **undo clock source ptp ssm** command restores the default SSM quality level of a clock source.

By default, the SSM quality level of a clock source is unknown.

Format

clock source ptp ssm { **unk** | **prc** | **ssua** | **ssub** | **sec** | **dnu** } **slot** *slot-id*

undo clock source ptp ssm slot *slot-id*

Parameters

Parameter	Description	Value
ptp	Indicates a PTP clock source.	-
dnu	Indicates that the clock source is unavailable.	-
prc	Indicates G.811 clock signals with the SSM quality level of PRC.	-
sec	Indicates SDH clock source signals with the SSM quality level of SEC.	-
ssua	Indicates G.812 transit node clock signals with the SSM quality level of SSUA.	-
ssub	Indicates G.812 local node clock signals with the SSM quality level of SSUB.	-
unk	Indicates clock signals with unknown synchronization quality.	-
slot *slot-id*	Specifies a slot ID.	The value range depends on the device configuration.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

When SSM control is enabled using the **clock ssm-control on** command, an SSM quality level needs to be specified for the clock source on an interface. To set the SSM quality level of a clock source, run the **clock source ptp ssm** command.

In switch stacking scenarios, each switch independently runs synchronous Ethernet and PTP. Therefore, this command needs to be configured for the stacked switch in each slot.

Example

Set the SSM quality level of a clock source to PRC.

```
<HUAWEI> system-view
[HUAWEI] clock source ptp ssm prc slot 0
```

3.15.13 clock ssm (interface view)

Function

The **clock ssm** command sets the SSM quality level of a clock source.

The **undo clock ssm** command cancels the configured SSM priority level of a clock source.

By default, no SSM quality level is configured for a clock source. The SSM quality level of a line clock source is transmitted from the peer device.

Format

clock ssm { **unk** | **prc** | **ssua** | **ssub** | **sec** | **dnu** }

undo clock ssm

Parameters

Parameter	Description	Value
dnu	Indicates that the clock source is unavailable.	-
prc	Indicates G.811 clock signals with the SSM quality level of PRC.	-
sec	Indicates SDH clock source signals with the SSM quality level of SEC.	-
ssua	Indicates G.812 transit node clock signals with the SSM quality level of SSUA.	-
ssub	Indicates G.812 local node clock signals with the SSM quality level of SSUB.	-
unk	Indicates clock signals with unknown synchronization quality.	-

Views

XGE interface view, 25GE interface view, 40GE interface view, 100GE interface view

Default Level

2: Configuration level

Usage Guidelines

When SSM control is enabled on a clock source using the **clock ssm-control on** command in the system view, an SSM quality level needs to be specified for the clock source on an interface. To set the SSM quality level of a clock source, run the **clock ssm** command. In switch stacking scenarios, each switch independently runs synchronous Ethernet and PTP. Therefore, this command needs to be configured for the stacked switch in each slot.

Example

Set the SSM quality level of the clock source on the interface XGE0/0/1 as PRC.

```
<HUAWEI> system-view
[HUAWEI] interface xgigabitethernet 0/0/1
[HUAWEI-XGigabitEthernet0/0/1] clock ssm prc
```

3.15.14 clock ssm-control

Function

The **clock ssm-control** command enables or disables SSM quality levels are used for automatic clock source selection.

By default, SSM quality levels are used for clock source selection.

Format

clock ssm-control { **on** | **off** }

Parameters

Parameter	Description	Value
on	Enables SSM control.	-
off	Disables SSM control.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

When the system clock works in automatic clock source selection mode, if SSM control is enabled, the system clock selects the clock source to trace based on SSM quality levels and then the priorities. If SSM control is disabled, the system clock selects the clock source to trace based on priorities. To configure SSM control, run the **clock ssm-control** command.

Example

Enable SSM control.

```
<HUAWEI> system-view
[HUAWEI] clock ssm-control on
```

3.15.15 clock switch

Function

The **clock switch** command configures the recovery mode of a clock node.

By default, clock nodes work in revertive mode.

Format

clock switch { **revertive** | **non-revertive** }

Parameters

Parameter	Description	Value
revertive	Indicates the revertive mode.	-
non-revertive	Indicates the non-revertive mode.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

To configure a clock source to work in revertive or non-revertive mode, run the **clock switch** command.

- Revertive mode: Switching is performed if the new clock source has a higher SSM quality level. If the new clock source has the same SSM quality level but a higher priority than the old clock source, switching is also performed. In other situations, switching is not performed.
- Non-revertive mode: Switching is performed if the new clock source has a higher SSM quality level. If the new clock source has the same SSM quality level but a higher priority than the old clock source, switching is not performed. In other situations, switching is not performed.

Example

Configure a clock node to work in revertive mode.

```
<HUAWEI> system-view
[HUAWEI] clock switch revertive
```


3.15.16 clock synchronization enable

Function

The **clock synchronization enable** command enables clock synchronization.

The **undo clock synchronization enable** command disables clock synchronization.

By default, clock synchronization is not enabled.

Format

clock synchronization enable

undo clock synchronization enable

Parameters

None

Views

XGE interface view, 25GE interface view, 40GE interface view, 100GE interface view

Default Level

2: Configuration level

Usage Guidelines

An interface can participate in clock source selection only after clock synchronization is enabled.

Example

Enable clock synchronization on the interface XGE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] interface xgigabitethernet 0/0/1
[HUAWEI-XGigabitEthernet0/0/1] clock synchronization enable
```

3.15.17 clock source ptp synchronization enable

Function

The **clock source ptp synchronization enable** command enables clock synchronization of a PTP clock source.

The **undo clock source ptp synchronization enable** command disables clock synchronization from a PTP clock source.

By default, clock synchronization is not enabled for a PTP clock source.

Format

clock source ptp synchronization enable slot *slot-id*

undo clock source ptp synchronization enable slot *slot-id*

Parameters

Parameter	Description	Value
slot *slot-id*	Specifies a slot ID.	The value depends on the device configuration.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

To enable clock synchronization for a PTP clock source, run the **clock source ptp synchronization enable** command. If a PTP clock source with clock synchronization enabled is selected as the clock source, frequency is transmitted through PTP messages.

An interface can participate in clock source selection after it is enabled with clock synchronization using the **clock synchronization enable** command.

Example

Enable clock synchronization for a PTP clock source.

```
<HUAWEI> system-view
[HUAWEI] clock source ptp synchronization enable slot 0
```

3.15.18 clock wtr

Function

The **clock wtr** command sets the wait-to-restore (WTR) time for a clock source.

By default, the WTR time of a clock source is 5 minutes.

Format

clock wtr *wtr-time*

Parameters

Parameter	Description	Value
wtr-time	Specifies the WTR time of a clock source.	The value is an integer that ranges from 0 to 12, in minutes.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

When a lost clock source is restored, the system waits for a period of 0 to 12 minutes before considering the clock source available. During this period, the system considers the clock source lost.

Setting the WTR time can avoid some mistakes in determining the clock source caused by occasional signal jitter on the network.

The default WTR time of a clock source is 5 minutes. Generally, you do not need to change the default value. If you want to view the clock source switching result during debugging, set the WTR time to 0.

Example

Set the WTR time to 0.

```
<HUAWEI> system-view
[HUAWEI] clock wtr 0
```

3.15.19 display clock

Function

The **display clock** command displays synchronous Ethernet configurations or the attributes of a PTP clock source.

Format

display clock { **config** | **source** [**ptp**] } [**slot** *slot-id*]

Parameters

Parameter	Description	Value
config	Displays the current clock configurations.	-
source	Displays the attributes of all clock sources.	-

Parameter	Description	Value
ptp	Displays the attributes of a PTP clock source.	-
slot *slot-id*	Displays configurations based on a slot ID.	The value range depends on the device configuration.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After a clock source is configured, run the **display clock config** command to view clock configurations. During routing maintenance, run the **display clock source** command to view attributes of the clock source being traced or all clock sources.

Example

Display synchronous Ethernet configurations on a switch.

```
<HUAWEI> display clock config
 ethernet synchronization   :enable
 clock freq deviation detect:disable
 clock unk map              :dnu
 system pll run mode        :normal

 switch config
   sys pll              :auto mode
   SSM control          :on
   switch mode          :revertive
   wtr                  :5min
   holdoff time         :1000ms

 source config
 ptp
   Sync enable
   Pri(sys)             :1
   SSM                  :unk
 XGigabitEthernet0/0/4
   Sync enable
   Pri(sys)             :10
   SSM                  :sec
```

Table 3-186 Description of the **display clock config** command output

Item	Description
ethernet synchronization	Whether synchronous Ethernet is enabled globally

Item	Description
clock freq deviation detect	Whether frequency offset check is enabled
clock unk map	SSM quality level mapped to the clock source with the SSM quality level of UNK
system pll run mode	PLL running mode
switch config	Switching configuration
sys pll	Clock source selection mode of the system phase-locked loop
SSM control	Whether the SSM quality level is used in clock source selection
switch mode	Switching mode
wtr	WTR time
holdoff time	Holdoff time
source config	Clock source configuration
ptp	PTP clock source
XGigabitEthernet0/0/4	Line clock source
Sync enable	Whether clock synchronization is enabled
Pri(sys)	Priority
SSM	SSM quality level

3.15.20 display clock source freq-deviation

Function

The **display clock source freq-deviation** command displays the frequency offset value of a clock source.

Format

display clock source freq-deviation [**slot** *slot-id*]

Parameters

Parameter	Description	Value
slot *slot-id*	Specifies a slot ID.	The value depends on the device configuration.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

To view the frequency offset value of a clock source, run the **display clock source freq-deviation** command. If the frequency offset value is greater than or equal to the specified threshold, the frequency offset is abnormal. If the frequency offset value is less than the threshold, the frequency offset is normal.

Precautions

- If frequency offset check is not enabled, this command also displays the frequency offset check result of the clock source. The check result, however, is not used for clock source selection.
- A clock source that does not pass the frequency offset check is tagged "--".

Example

Display the frequency offset result of the clock source in slot 2.

```
<HUAWEI> display clock source freq-deviation slot 2
 Frequence deviation detect:     enable
  Source                        Freq-deviation-value
 ------------------------------------------------------------
   XGE2/0/4                      -0.05ppm(normal)
```

Table 3-187 Description of the **display clock source freq-deviation** command output

Item	Description
Source	Interface clock source or PTP clock source with synchronous Ethernet enabled
Freq-deviation-value	Frequency offset value, which is in the format of symbol (negative sign only) + frequency offset value + unit (ppm) + frequency offset status. If the value is "---", the frequency offset check cannot be performed on the clock source.

