3 Device Management Commands

About This Chapter

3.1 Device Status Checking Commands

3.2 Hardware Configuration Commands

3.3 Information Center Configuration Commands

3.4 Fault Management Commands

3.5 NTP Configuration Commands

3.6 Energy-saving Configuration Commands

3.7 PoE Configuration Commands

3.8 Stack Configuration Commands

3.9 SVF Configuration Commands

3.10 Cloud-based Management Configuration Commands

3.1 Device Status Checking Commands

3.1.1 Command Support

3.1.2 display compatible-information

3.1.3 display cpu-usage

3.1.4 display cpu-usage configuration

3.1.5 display cpu-usage history

3.1.6 display device

3.1.7 display device capability

3.1.8 display device manufacture-info

3.1.9 display diagnostic-information

3.1.10 display elabel

3.1.11 display esn

3.1.12 display fan

3.1.13 display memory-usage

3.1.14 display memory-usage threshold

3.1.15 display power

3.1.16 display transceiver

3.1.17 display transceiver diagnosis interface

3.1.18 display temperature

3.1.19 display version

3.1.1 Command Support

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

3.1.2 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:

S5700LI_R7 is a device model newly available in V200R007. The NMS software version that matches the device software version is V200R007.

S5700LI_R5 is a device model newly available in V200R005. The NMS software version that matches the device software version is V200R005.

When you use the NMS of V200R005 to manage S5700LI_R7, the device cannot be managed because of version mismatch. The NMS then obtains compatibility information about S5700LI_R7 and learns that it is compatible with S5700LI_R5. Subsequently, the NMS uses information about S5700LI_R5 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
Compatible SysOids  : 1.3.6.1.4.1.2011.2.23.117
Compatible Version  : V200R003C00
ProductName         : S2750-28TP-EI-AC
```

Table 3-1 Description of the display compatible-information command output

Item	Description
Compatible SysOids	System OID of an old device version.
Compatible Version	Old device version compatible with the current device version.
ProductName	Product name of a new device.

3.1.3 display cpu-usage

Function

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

Format

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

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 S5720HI supports the **vcpu** *vcpu* 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 the slot ID if stacking is not configured. ● Specifies the stack ID if stacking is configured.	The value is 0 if stacking is not configured. The value range depends on the stack configuration if stacking is configured.
vcpu *vcpu*	Displays the usage of a specified virtual CPU.	Specify the *vcpu* 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 : 2013-10-23  10:04:45
CPU utilization for five seconds: 5%: one minute: 5%: five minutes: 5%
Max CPU Usage Stat. Time : 2013-10-21 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 3-2 Description of the **display cpu-usage** command output

Item	Description
CPU Usage Stat. Cycle	Interval for collecting CPU usage statistics. The default interval is 60 seconds.
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.

Item	Description
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.
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.

3.1.4 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. This parameter is valid only when multiple switches form stack.	-
slot *slot-id*	Displays device CPU usage configuration. *slot-id* specifies the stack ID.	The value is 0 if stacking is not configured. The value ranges from 0 to 8 if stacking is configured.

Views

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 3-3 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.

Item	Description
The current monitor warning threshold	Alarm threshold. To set the CPU usage alarm threshold, run the **3.2.5 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 **3.2.5 cpu-usage threshold** *threshold-value* [**restore** *restore-threshold-value*] [**slot** *slot-id*] command.

Related Topics

3.2.5 cpu-usage threshold

3.1.5 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*]

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 S5720HI supports the **vcpu** *vcpu* 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.	-

Parameter	Description	Value
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*	Displays the CPU usage statistics of a specified virtual CPU.	Specify the *vcpu* 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%|HHHHHHHHHHHHHHHHHHHHHHHHHHHHHHHHHHHHHHHHHHHHHHHHHHHHHHHHHHHHH
     ---------+---------+---------+---------+---------+---------+>
              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%|HHHHHHHHHHHHHHHHHHHHHHHHHHHHHH
     ---------+---------+---------+---------+-------->
              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%|HHHHHHHHHHHHHH
     ---------+---------+---------+---------+---------+---------+---------+-->
              10        20        30        40        50        60        70
                  System cpu-usage last 72 hours(Per Hour)
                 * = maximum cpu-usage    H = average cpu-usage
```

Table 3-4 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
H = average cpu-usage	Average CPU usage

3.1.6 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*	● On a non-stacked device, the value indicates the slot ID. ● On a stacked device, the value indicates the stack ID.	The value is an integer, and the value must be set according to the device configuration if stacking is configured. The value is 0 if stacking is not configured.

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:

- S5720S-SI: S5720S-28P-SI-AC, S5720S-52X-SI-AC, S5720S-28X-SI-AC, S5720S-52P-SI-AC, S5720S-28X-SI-DC, S5720S-52X-SI-DC
- S5720SI: S5720-28X-SI-24S-AC, S5720-28X-SI-24S-DC
- S5720EI series: S5720-32X-EI-24S-AC, S5720-50X-EI-46S-AC, S5720-32X-EI-AC, S5720-52X-EI-AC, S5720-50X-EI-AC, S5720-32P-EI-AC, S5720-52P-EI-AC, S5720-32X-EI-DC, S5720-50X-EI-DC, S5720-32X-EI-24S-DC, S5720-50X-EI-46S-DC
- S5700LI series: all models except S5700-10P-LI-AC, S5700-28P-LI-BAT, S5700-28P-LI-24S-BAT, and S5700-10P-PWR-LI-AC
- S5700S-LI series: all models
- S5710-X-LI series: all models
- S5720LI 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
- S5720S-LI series: S5720S-28X-LI-24S-AC
- S6720LI series: all models
- S6720S-LI series: all models

The following product models support the use of a battery: S5700-28P-LI-BAT, S5700-28P-LI-24S-BAT.

Example

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

```
<HUAWEI> display device
S5700-52P-LI-AC's Device status:
Slot Sub  Type              Online    Power     Register     Status   Role
-------------------------------------------------------------------------------
0    -    S5700-52P-LI      Present   PowerOn   Registered   Normal   Master
```

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

```
<HUAWEI> display device
S5700-28X-LI-AC's Device status:
Slot  Sub  Type             Online    Power     Register     Status   Role
-------------------------------------------------------------------------------
0     -    S5700-28X-LI     Present   PowerOn   Registered   Normal   Master
           RPS              Present   PowerOn   Registered   Self-powered
```

# Display information about components on a device (with a battery installed).

```
<HUAWEI> display device
S5700-28P-LI-24S-BAT's Device status:
Slot Sub  Type              Online    Power      Register     Status   Role
-------------------------------------------------------------------------------
0    -    S5700-28P-LI-24S    Present   PowerOn    Registered   Normal   Master
     5    BAT-4AHA             Present   PowerOn    Registered   Normal   NA
```

# 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

S5700-52P-LI-AC's Device status:
Slot Sub  Type              Online    Power      Register     Status   Role
-------------------------------------------------------------------------------
0    -    S5700-52P-LI        Present   PowerOn    Registered   Normal   Master
-------------------------------------------------------------------------------
  Board Type        : S5700-52P-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 3-5 Description of the display device command output

Item	Description
Slot	● On a standalone device, this field indicates a slot ID. ● In a stack, this field indicates a stack ID, and the value must be set according to the device configuration.

Item	Description
Sub	Card ID. The value can be: ● –: The component is a device, not a card. ● 1: front card. ● 2: rear card. ● 3: fan module. ● 4 and 5: power module, lithium battery or lead-acid battery board.
Type	Component type. A component can be a device, RPS, or a card. The device types are displayed as S5700-52P-LI. The **-AC** or **-DC** field is not displayed. 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. ● Lithium battery: BAT-4AHA or BAT-8AHA ● 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.

Item	Description
Power	Power supply status. The value can be: ● PowerOn ● PowerOff If the device has a battery installed, the following values may be displayed: ● Lithium battery PowerOn: A lithium battery is installed. ● Lead-acid battery PowerOn: A lead-acid battery board is installed and a lead-acid battery is connected to it. PowerOff: A lead-acid battery board is installed but no lead-acid battery is connected to it. If no lithium battery or lead-acid battery board is installed, the command does not display the preceding information. You can also check the power supply status of a lithium battery or lead-acid battery using the **display power** command.
Register	Whether the device is registered: ● Registered: indicates that the component is registered. ● Unregistered: indicates that the component is unregistered.
Status	Status of the component. The value can be: ● Abnormal: indicates that the component is running abnormally. ● Normal: indicates that the component is running normally. 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.

Item	Description
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.
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.

Item	Description
Flow-Ctrl	Flow control status on an interface. ● Disable: The flow control function is disabled on the interface. ● Enable: The flow control function is enabled on the interface. ● -: The flow control status cannot be obtained. To configure flow control, run the **flow-control** 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.

3.1.7 display device capability

Function

The **display device capability** command displays the hardware and software capabilities of a device.

NOTE

Only the S5720EI supports this command.

Format

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

Parameters

Parameter	Description	Value
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 value is fixed as 0.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

Whether a device supports a function depends on whether the hardware has the capability of the function and whether the running system software provides this function. You can use this command to check the hardware and software support for a function and determine whether you need to update the system software or use other methods to obtain the function.

Precautions

Currently, this command can only display the hardware and software support for the MPLS feature.

Example

# Display the hardware and software capabilities of a device.

```
<HUAWEI> display device capability
Slot  Feature  Hardware  Software
--------------------------------------------------------
0     MPLS     NO        YES
--------------------------------------------------------
```

Table 3-6 Description of the **display device capability** command output

Item	Description
Slot	Slot ID.
Feature	Name of a feature. Currently, the feature name can only be **MPLS**.
Hardware	Hardware support for the feature.
Software	Software support for the feature.

3.1.8 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 the slot ID when no stack is configured. - Specifies the stack ID when a stack is configured.	- The value is 0 when no stack is configured. - The value ranges from 0 to 8 when a stack is configured.

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 3-7 Description of the display device manufacture-info command output

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

3.1.9 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** | **defend** | **dhcp** | **l2adp** | **l3adp** | **lbdt** | **lldp** | **mcast** | **mpls** | **qos** | **rrpp** | **sdk** | **smlk** | **srm** | **sta** | **stack** | **stat** | **stp** | **ucm**] [*file-name*]

NOTE

- The S1720 does not support **defend**.
- Only the S5720S-SI, S5720SI, S5720EI, S5720HI, S5730SI, S5730S-EI, S6720SI, S6720S-SI, S6720S-EI, and S6720EI support **bfd**.
- Only the S5720EI, S5720HI, S6720S-EI, and S6720EI support **mpls**.
- Among S5720EI switches running V200R009C00 and later versions, only some switches support the MPLS feature. Run the **display device capability** command on the switch to check the switch's software and hardware capabilities. The switch supports the MPLS feature only when chips also support the MPLS feature.
- Only the S5720EI, S5720HI, S6720S-EI, and S6720EI support **sdk**.
- The **stack** parameter is supported on a stack only.
- Only the S5720HI supports **ap** and **sta**.

Parameters

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

Parameter	Description	Value
bfd	Displays BFD information.	-
defend	Displays attack defense information.	-
dhcp	Displays DHCP 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.	-
sdk	Displays sdk information.	-
smlk	Displays Smart Link information.	-
stack	Displays stack information.	-
srm	Displays device information.	-
sta	Displays STA information.	-
stat	Displays basic statistic information.	-
stp	Displays STP information.	-
ucm	Displays UCM module information.	-

Parameter	Description	Value
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 **2.4.6 display clock**, **3.1.19 display version**, and **2.8.13 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).
- 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.
```

Related Topics

3.1.19 display version

2.4.6 display clock

2.8.13 display current-configuration

3.1.10 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 or the number of a fan module or power module.	The value depends on the device configuration.
subcard-id	Specifies the subcard ID. This parameter can be specified if any subcard is used on the device.	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

For a new device delivered since V200R011, its electronic label version has been updated to version 4.0, which has the following changes compared to earlier versions:

- The Model field is added to indicate the hardware external model of the device.
- The ExInfo field is added to indicate the hardware extension information of the device. This field does not exist in electronic labels of optical modules.
- The ElabelVersion is added to indicate the version of the elabel.

Example

# Display the electronic label of the device with stack ID 0.

```
<HUAWEI> display elabel slot 0
/$[System Integration Version]
/$SystemIntegrationVersion=3.0


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


[Main_Board]

/$[ArchivesInfo Version]
/$ArchivesInfoVersion=3.0
```

```


[Board Properties]
BoardType=S5752S-LI
BarCode=2102353174107C800132
Item=
Description=S5752S-LI Mainframe(48 10/100/1000 BASE-T ports  and 4 SFP GE (100/1
000 BASE-X) ports (SFP Req.) and DC -48V)
Manufactured=2011-08-22
VendorName=Huawei
IssueNumber=
CLEICode=
BOM=




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


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

Table 3-8 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	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.

Item	Description
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.

Related Topics

3.2.3 backup elabel

3.1.11 display esn

Function

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

NOTE

The S2750EI, S5700LI, S5700S-LI, and S5720EI do not support this command.

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: 21023586001234567890
```

Table 3-9 Description of the display esn command output

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

3.1.12 display fan

Function

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

Format

display fan

Parameters

None

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 number of fans.

Example

# Display the fan status of the device.

```
<HUAWEI> display fan
-------------------------------------------------------------------------
 Slot  FanID   Online    Status    Speed     Mode     Airflow
-------------------------------------------------------------------------
 0     1       Absent    -         -         -
 0     2       Present   Normal    100%      AUTO     Side-to-Side
 0     3       Absent    -         -         -
```

Table 3-10 Description of the **display fan** command output

Item	Description
Slot	● On a standalone device, this field indicates a slot ID. ● In a stack, this field indicates the stack ID of the local device.
FAN	Number of a fan.
Online	Check 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.
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.
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. ● -: The fan is not present.

3.1.13 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*]

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 S5720HI supports the **vcpu** *vcpu* 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*	● Specifies the slot ID if stacking is not configured. ● Specifies the stack ID if stacking is configured.	The value ranges from 0 to 8 if stacking is configured. The value is 0 if stacking is not configured.
vcpu *vcpu*	Specifies the virtual CPU number.	Specify the *vcpu* 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.

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%
```

Table 3-11 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.

3.1.14 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 in a specified slot ID.	The value is 0 if stacking is not configured; the value ranges from 0 to 8 if stacking is configured.

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 3-12 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.

Related Topics

3.2.28 set memory-usage threshold

3.1.15 display power

Function

The **display power** command displays the information of all power supply units and battery 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 supply units and battery, and their power. The following product models support the use of a battery: S5700-28P-LI-BAT, S5700-28P-LI-24S-BAT.

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)
-------------------------------------------------------------
 0       PWRI     Present  AC     Supply     500.00
 0       PWRII    Absent   -      -          -
```

# Display the status of the battery used on the device.

```
<HUAWEI> display power
-------------------------------------------------------------
 Slot    PowerID  Online   Mode   State      Power(W)
-------------------------------------------------------------
 0       PWRI     Present  BAT    Charge     80.00
```

Table 3-13 Description of the display power command output

Item	Description
Slot	● Specifies the slot ID if stacking is not configured, and the value is 0. ● Specifies the stack ID if stacking is configured, and the value must be set according to the device configuration.
PowerID	ID of a power supply slot: ● PWRI: slot for a power module, lithium battery, or lead-acid battery board ● PWRII: slot for a power module On the S5720S-SI, S5720SI, S5720EI, S5720HI, S5730SI, S5730S-EI, S6720SI, S6720S-SI, S6720S-EI, and S6720EI series switches, the power supply slots are PWR1 and PWR2.
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.

Item	Description
Mode	Type of the power module, lithium battery, or lead-acid battery board: ● AC: AC power module ● DC: DC power module ● –: power supply invalid or absent ● BAT: lithium battery ● PBB: lead-acid battery board
State	Working status of a power module or battery. ● For a power module, the value can be: Supply: current is output. NotSupply: no current is output. –: invalid or absent ● For a lithium battery, the value can be: Charge: The battery is charging. Discharge: The battery is discharging. Full: The battery is in full power state. ● For a lead-acid battery, the value can be: Charge: The battery is charging. Discharge: The battery is discharging. Full: The battery is in full power state. Abnormal: The battery is not working properly. For example, the lead-acid battery board is installed but no lead-acid battery is connected to it; alternatively, the lead-acid battery is reversely connected.
Power(W)	Rated power of a power supply. – indicates that the power supply is invalid or is not installed properly.

3.1.16 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 the slot ID on a standalone switch. ● Specifies the stack ID in a stack.	The value range depends on the actual configuration if stacking is configured. The value is 0 if stacking is not configured.
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            :02318169
  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(¡ãC)              :26.00
  Temp High Threshold(¡ãC)      :85.00
  Temp Low  Threshold(¡ãC)      :-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 Threshold(dBM)  :0.00
 RX Power Low  Threshold(dBM)  :-16.99
 TX Power(dBM)                 :-5.03
 TX Power High Threshold(dBM)  :-2.22
 TX Power Low  Threshold(dBM)  :-6.99
 Transceiver phony alarm       :Yes
-------------------------------------------------------------
```

Table 3-14 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.
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.
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 a Huawei-Certified Optical Module?" in the *S1720, S2700, S5700, and S6720 V200R011C10 Configuration Guide - Device Management – Device Status Query*.
Vendor Part Number	The 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.
Manufacture information	Manufacture information of the optical module.

Item	Description
Manu. Serial Number	Vendor sequence number of the optical module.
Manufacturing Date	Manufacturing date of the optical module.
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.

Item	Description
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.
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.

3.1.17 display transceiver diagnosis interface

Function

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

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 check the digital diagnostic monitoring (DMM) information about an optical module.

Example

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

```
<HUAWEI> display transceiver diagnosis interface gigabitethernet 0/0/4
Port GigabitEthernet0/0/4 transceiver diagnostic information:
Parameter        Current     Low Alarm    High Alarm
  Type           Value      Threshold    Threshold    Status
-------------   ---------    ---------    ----------   --------
TxPower(dBm)     -4.64        0.00         0.00         abnormal
RxPower(dBm)     -4.37        33.00        0.00         abnormal
Current(mA)      7.42         0.00         0.00         abnormal
Temp.(°C)        30.00        0.00         0.00         abnormal
Voltage(V)       3.28         0.00         8.19         normal
```

Table 3-15 Description of the **display transceiver diagnosis interface** command output

Item	Description
Parameter Type	Parameter type: - TxPower(dBm): indicates the transmission power of the optical transceiver, in dBm. - RxPower(dBm): indicates the receiving power of the optical transceiver, in dBm. - Current(mA): indicates the current of the optical transceiver, in mA. - Temp.(°C): indicates the temperature of the optical transceiver, in degree Celsius. - Voltage(V): indicates the voltage of the optical transceiver, in V.
Current Value	Current value of a parameter.
Low Alarm Threshold	Lower alarm threshold of a parameter.
High Alarm Threshold	Upper alarm threshold of a parameter.
Status	Status of the optical transceiver: - Normal: The value is within the normal range. - Abnormal: The value is not within the normal range.

3.1.18 display temperature

Function

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

Format

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

Parameters

Parameter	Description	Value
all	Displays temperature of all slots on the device.	-
slot *slot-id*	Displays temperature of the specified slot.	The value is an integer, and the value must be set according to the device configuration if stacking is configured. The value is 0 if stacking is not configured.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

A high or low device temperature may damage the hardware. This command displays the current device temperature 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 temperature of 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 3-16 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)	Current temperature 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.
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.

Item	Description
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.

3.1.19 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 the slot ID if stacking is not configured. ● Specifies the stack ID if stacking is configured.	The value range depends on the actual configuration if stacking is configured. The value is 0 if stacking is not configured.

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
V200R011C10)
Copyright (C) 2000-2017 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
(V200R011C10)
CARD1 information
Pcb           Version   : ES5D21Q04Q01 VER.A
CPLD   Version          : 0105
PWR2 information
Pcb           Version   : PWR VER.A
FAN1 information
Pcb           Version   : NA
```

Table 3-17 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) 2000-2017 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.

Item	Description
Pcb Version	Version of the printed circuit board (PCB).
BootROM Version	Version of the BootROM software.
BootLoad Version	Version of the BootLoad software. **NOTE** This field can be not displayed on S1720GFR, S2750, S5700S-LI (except S5700S-28X-LI-AC and S5700S-52X-LI-AC), and S5700LI.
CPLD Version	Version of the complex programmable logic device (CPLD).
MCU Version	Micro Control Unit (MCU) version. **NOTE** The information is displayed only for the S5720-16X-PWH-LI-AC, S5720-28X-PWH-LI-AC, and the PoE devices of S5730SI, S5730S-EI, and S6720SI.
Software Version	Versions of the VRP and the software of the device.
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 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

3.2.2 assign resource-mode

3.2.3 backup elabel

3.2.4 cpu-usage monitor

3.2.5 cpu-usage threshold

3.2.6 display device battery

3.2.7 display device battery lifetime threshold

3.2.8 display device fault-light

3.2.9 display fan speed-adjust threshold minus

3.2.10 display resource-mode configuration

3.2.11 display root-key configuration

3.2.12 display service-mode configuration

3.2.13 display switchover state

3.2.14 display system resource-template

3.2.15 display snmp-agent trap feature-name entityexttrap all

3.2.16 display snmp-agent trap feature-name entitymib all

3.2.17 display snmp-agent trap feature-name entitytrap all

3.2.18 display snmp-agent trap feature-name srmtrap all

3.2.19 display snmp-agent trap feature-name swithsrvres all

3.2.20 display snmp-agent trap feature-name system all

3.2.21 display wavelength-map

3.2.22 reset cpu-usage record

3.2.23 reset slot

3.2.24 set device battery lifetime

3.2.25 set device battery off

3.2.26 set device fault-light

3.2.27 set fan speed-adjust threshold minus

3.2.28 set memory-usage threshold

3.2.29 set root-key

3.2.30 set service-mode

3.2.31 slave restart

3.2.32 slave switchover

3.2.33 slave switchover { disable | enable }

3.2.34 snmp-agent trap enable feature-name entityexttrap

3.2.35 snmp-agent trap enable feature-name entitymib

3.2.36 snmp-agent trap enable feature-name entitytrap

3.2.37 snmp-agent trap enable feature-name srmtrap

3.2.38 snmp-agent trap enable feature-name swithsrvres

3.2.39 snmp-agent trap enable feature-name system

3.2.40 temperature threshold

3.2.41 transceiver diagnosis threshold rx-power

3.2.42 transceiver diagnosis threshold tx-power

3.2.43 transceiver phony-alarm-disable

3.2.44 wavelength-channel

3.2.1 Command Support

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

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 S5720EI is enhanced-mac and that of the S6720EI and S6720S-EI is enhanced-arp.

NOTE

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

Format

assign resource-mode { **enhanced-mac** | **enhanced-ipv4** | **enhanced-ipv6** } [**slot** *slot-id* | **all**] (S5720EI)

assign resource-mode { **enhanced-mac** | **enhanced-arp** | **enhanced-ipv4** | **ipv4-ipv6 6:1** | **96k-arp** } [**slot** *slot-id* | **all**] (S6720EI, S6720S-EI)

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

Parameters

Parameter	Description	Value
enhanced-mac	Sets the resource allocation mode to enhanced-mac.	-
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.	-
ipv4-ipv6 6:1	Sets the resource allocation mode to ipv4-ipv6 6:1.	-
96k-arp	Sets the resource allocation mode to 96k-arp.	-
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 value is fixed as 0.
all	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.

Table 3-18 Number of entries supported in different resource allocation modes on the S5720EI

Resource Allocation Mode	MAC	IPv4 FIB	IPv6 FIB (0-64 Bits Mask)	IPv6 FIB (Over 64 Bits Mask)	ARP	ND	Multicast IPv4& IPv6
enhanced-mac	64K	12K	6K	1K	16K	8K	2000
enhanced-ipv4	32K	16K	8K	0K	16K	8K	2000
enhanced-ipv6	32K	8K	4K	2K	16K	8K	2000

NOTE

On the S5720EI, IPv4 FIB and IPv6 FIB (0-64 bits mask) share hardware resources. The specifications listed in the preceding table indicate 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 S5720EI, 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.

Table 3-19 Number of entries supported in different resource allocation modes on the S6720EI 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
enhanced-arp	96K	12K	6K	1K	48K	44K	4000
enhanced-mac	288K	12K	6K	1K	16K	8K	4000
enhanced-ipv4	32K	128K	80K	0K	16K	8K	4000
ipv4-ipv6 6:1	32K	64K	10K	10K	16K	8K	4000

Resource Allocation Mode	MAC	IPv4 FIB	IPv6 FIB (0-64 Bits Mask)	IPv6 FIB (Over 64 Bits Mask)	ARP	ND	Multicast IPv4& IPv6
96k-arp	96K	12K	6K	1K	96000	44K	4000

NOTE

On the S6720EI 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 S6720EI and S6720S-EI work in enhanced-arp, enhanced-mac, enhanced-ipv4, or 96k-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 S6720EI 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.

Precautions

The configured resource allocation mode takes effect only after the device is restarted.

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.

On the S6720EI and S6720S-EI, if the **3.2.2 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 S6720EI 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 S6720EI and S6720S-EI, MPLS is not supported in 96k-arp resource allocation mode.

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.
```

Related Topics

3.2.10 display resource-mode configuration

3.2.3 backup elabel

Function

The **backup elabel** command backs up electronic labels of the device to the flash memory. The default name of the saved file is **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.
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.

Parameter	Description	Value
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 FTPor 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 **Huawei@1234**. Save electronic labels in the **elabel-slot0.fls** file.

```
<HUAWEI> backup elabel sftp 192.168.12.91 elabel-slot0.fls client001 Huawei@1234
Info: It is executing, please wait...

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

Related Topics

3.1.10 display elabel

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 the slot ID if stacking is not configured. ● Specifies the stack ID if stacking is configured.	The value is 0 if stacking is not configured; the value is an integer that ranges from 0 to 8 if stacking is configured.
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
```

Related Topics

3.1.3 display cpu-usage

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 recover threshold must be smaller than the alarm threshold.
slot *slot-id*	● Specifies the slot ID if stacking is not configured. ● Specifies the stack ID if stacking is configured.	The value is 0 if stacking is not configured; the value ranges from 0 to 8 if stacking is configured.

Views

System view

Default Level

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 thresholds on the master switch with those on other 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
```

Related Topics

3.1.4 display cpu-usage configuration

3.2.6 display device battery

Function

The **display device battery** command displays the battery status on a device.

NOTE

Only the S5700-28P-LI-BAT and S5700-28P-LI-24S-BAT support this command.

Format

display device battery

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can use this command to check the real-time status of the battery. When the battery is working normally, it can supply power to the device in case the external power supply encounters a power failure.

Example

# Display the battery status.

```
<HUAWEI> display device battery
--------------------------------------------------------------------------------
 SlotID  Type      State     Temperature(L/H)  Remain  Remain-Time  Charge-Times
                               (c)         (%)      (mins)
--------------------------------------------------------------------------------
 0       BAT-4AHA  Charge    29/31           22      54           2
```

Table 3-20 Description of the display device battery command output

Item	Description
SlotID	Slot ID of the battery.
Type	Type of the battery or battery board. The value can be: ● BAT-4AHA: lithium battery with a rated capacity of 4 Ah. ● BAT-8AHA: lithium battery with a rated capacity of 8 Ah. ● PBB: lead-acid battery board.
State	Power supply status of the battery. ● For a lithium battery, the value can be: Charge: The battery is charging. Discharge: The battery is discharging. Full: The battery is in full power state. ● For a lead-acid battery, the value can be: Charge: The battery is charging. Discharge: The battery is discharging. Full: The battery is in full power state. Abnormal: The battery is not working properly. For example, the lead-acid battery board is installed but no lead-acid battery is connected to it; alternatively, the lead-acid battery is reversely connected.
Temperature(L/H)	● When a lithium battery is installed, this field indicates the highest and lowest temperature of the lithium battery's electrochemical cell. The temperature is expressed in °C. ● When a lead-acid battery is installed, this field displays N/A.
Remain	● When a lithium battery is installed, this field indicates the available power of the lithium battery. The value is a percentage to the full power. ● When a lead-acid battery is installed, this field displays N/A.

Item	Description
Remain-Time	● When a lithium battery is installed, this field indicates the power supply time of the lithium battery. The time is expressed in minutes. ● When a lead-acid battery is installed, this field displays N/A.
Charge-Times	● When a lithium battery is installed, this field indicates the number of charge and discharge events. ● When a lead-acid battery is installed, this field displays N/A.

3.2.7 display device battery lifetime threshold

Function

The **display device battery lifetime threshold** command displays the lifetime expiration alarm threshold for a lithium battery.

NOTE

Only the S5700-28P-LI-BAT and S5700-28P-LI-24S-BAT that have a lithium battery installed support this command.

Format

display device battery lifetime threshold [**slot** *slot-id*]

Parameters

Parameter	Description	Value
slot *slot-id*	Specifies the slot ID of the lithium battery.	The value is fixed as 0 currently.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Use Scenario

If a lithium battery discharges too fast, its lifetime is about to expire. During a discharge, if the time taken to consume 10% of the total power is shorter than the alarm threshold, the lifetime of the lithium battery is about to expire. When this occurs, the device generates an alarm. When receiving this alarm, replace the lithium battery to ensure normal operation of the device in the case of a mains power outage. You can set the lifetime expiration alarm threshold for a lithium battery using the **set device battery lifetime threshold** *threshold* [**slot** *slot-id*] command.

You can use the **display device battery lifetime threshold** command to check the lifetime expiration alarm threshold and determine whether the threshold needs to be changed.

Precautions

When the S5700-28P-LI-BAT and S5700-28P-LI-24S-BAT have no battery or a lead-acid battery installed, the system displays a message indicating that this command is not supported.

Example

# Display the lifetime expiration alarm threshold for the lithium battery.

```
<HUAWEI> display device battery lifetime threshold
--------------------------------------------
 Slot    Type   Threshold(mins)
--------------------------------------------
 0       BAT     20
```

Table 3-21 Description of the display device battery lifetime threshold command output

Item	Description
Slot	Slot ID of the battery.
Type	Battery type. The value is BAT, indicating a lithium battery.
Threshold(mins)	Lifetime expiration alarm threshold for the lithium battery. The unit is minute. By default, the lifetime expiration alarm threshold for a lithium battery is 20 minutes. To set the lifetime expiration alarm threshold for a lithium battery, run the **set device battery lifetime** command.

Related Topics

3.2.24 set device battery lifetime

3.2.8 display device fault-light

Function

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

NOTE

Only the S1720GW, S1720GWR, S1720X, S1720GW-E, S1720GWR-E, S1720X-E, S2720EI, S5700S-LI (only the S5700S-28X-LI-AC and S5700S-52X-LI-AC), S5710-X-LI, S5720LI, S5720S-LI, S5720S-SI, S5720SI, S5720EI, S5730SI, S5730S-EI, S6720LI, S6720S-LI, S6720SI, S6720S-SI, S6720S-EI, and S6720EI support this command.

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 3-22 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 "--".

Related Topics

3.2.26 set device fault-light

3.2.9 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:

- S1720GW series
- S1720GW-E series
- S1720GWR series: S1720-28GWR-4P, S1720-28GWR-4X, and S1720-28GWR-PWR-4TP
- S1720GWR-E series: S1720-28GWR-4P-E, S1720-28GWR-4X-E, and S1720-28GWR-PWR-4TP-E
- S1720GFR series
- S2720EI series: S2720-12TP-EI, S2720-12TP-PWR-EI, S2720-28TP-EI, S2720-28TP-PWR-EI-L
- S2750EI series: S2750-28TP-EI-AC and S2751-28TP-PWR-EI-AC
- S5700LI series: S5700-28TP-LI-AC, S5700-28P-LI-AC, S5700-28P-LI-DC, S5700-10P-LI-AC, and S5700-10P-PWR-LI-AC
- S5700S-LI series: S5700S-28P-LI-AC
- S5710-X-LI series: S5710-28X-LI-AC
- S5720LI 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
- S5720S-LI series: S5720S-12TP-LI-AC, S5720S-12TP-PWR-LI-AC, S5720S-28P-LI-AC, S5720S-28TP-PWR-LI-AC, and S5720S-28X-LI-AC
- S5720S-SI series: S5720S-28P-SI-AC, S5720S-28X-SI-AC, and S5720S-28X-SI-DC

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 the slot ID when stack is not configured. ● Specifies the stack ID when a stack is configured. If this parameter is not specified, the threshold settings in all slots are displayed.	● The value is 0 when stack is not configured. ● The value can be set according to the device configuration when stack is configured.

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.

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 3-23 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.

Item	Description
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.

Related Topics

3.2.27 set fan speed-adjust threshold minus

3.2.10 display resource-mode configuration

Function

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

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 3-24 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.

Related Topics

3.2.2 assign resource-mode

3.2.11 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 3-25 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.

Related Topics

3.2.29 set root-key

3.2.12 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 S5720HI.

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
```

Table 3-26 Description of the **display service-mode configuration** command output

Item	Description
Service mode status	Working mode of the device: ● Normal ● Enhanced To set the working mode, run the **set service-mode** command.

Related Topics

3.2.30 set service-mode

3.2.13 display switchover state

Function

The **display switchover state** command displays information about active and 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 and 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 3-27 Description of the display switchover state command output

Item	Description
HA FSM State(master)	Master switch status: ● waiting for the slave to be inserted: There is only the master switch but not the standby switch. ● waiting batch backup request from slave: The master switch is waiting for the batch backup request from the standby switch. ● realtime or routine backup: The master switch is in real-time backup state. ● data smooth: The master switch is in data smoothing state.
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.

Related Topics

3.2.32 slave switchover

3.2.33 slave switchover { disable | enable }

3.2.14 display system resource-template

Function

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

NOTE

Only the S5720HI supports 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 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.

```
<HUAWEI> display system resource-template
Resource Template Information:
------------------------------------------------------------
 Slot    Type        RunningTemplate      NextTemplate
```

```
-----------------------------------------------------------------
0      acl-mode    dual-ipv4-ipv6      dual-ipv4-ipv6
-----------------------------------------------------------------
```

Table 3-28 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.

Related Topics

14.1.7 assign resource-template acl-mode

3.2.15 display snmp-agent trap feature-name entityexttrap all

Function

The **display snmp-agent trap feature-name entityexttrap all** command displays the status of all traps of the ENTITYEXTTRAP module.

Format

display snmp-agent trap feature-name entityexttrap all

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

After the trap function of a specified feature is enabled, to check the status of all traps of the ENTITYEXTTRAP module, run the **display snmp-agent trap feature-name entityexttrap all** command. To enable the trap function for the ENTITYEXTTRAP module, run the **snmp-agent trap enable feature-name entityexttrap** command.

Prerequisites

SNMP has been enabled using the **snmp-agent** command.

Example

# Display the status of all traps of the ENTITYEXTTRAP module.

```
<HUAWEI> display snmp-agent trap feature-name entityexttrap all
------------------------------------------------------------------------------
Feature name: ENTITYEXTTRAP
Trap number : 9
------------------------------------------------------------------------------
Trap name                     Default switch status   Current switch status
hwEntityInputRateThresholdAlarm
                              on                      on
hwEntityInputRateThresholdAlarmResume
                              on                      on
hwEntityOutputRateThresholdAlarm
                              on                      on
hwEntityOutputRateThresholdAlarmResume
                              on                      on
hwEntityHigErrorPacketThresholdAlarm
                              on                      on
hwEntityHigStateChangeNotify    on                      on
hwEntityHigStateDownNotify      on                      on
hwEntityRuntPacketCheckNotify   on                      on
hwBoardDropRuntPacketNotify     on                      on
```

Table 3-29 Description of the **display snmp-agent trap feature-name entityexttrap all** command output

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

Item	Description
Trap name	Names of a trap. Traps of the ENTITYEXTTRAP module include: ● hwEntityInputRateThresholdAlarm: The bandwidth usage of incoming traffic exceeds the threshold. ● hwEntityInputRateThresholdAlarmResume: The bandwidth usage of incoming traffic falls below the threshold. ● hwEntityOutputRateThresholdAlarm: The bandwidth usage of outgoing traffic exceeds the threshold. ● hwEntityOutputRateThresholdAlarmResume: The bandwidth usage of outgoing traffic falls below the threshold. ● hwEntityHigErrorPacketThresholdAlarm: Incoming packets are discarded because an error is detected during physical layer detection. ● hwEntityHigStateChangeNotify: The Higig port status changes. ● hwEntityHigStateDownNotify: The Higig port status remains Down. ● hwEntityRuntPacketCheckNotify: The number of packet fault recoveries detected on a port exceeds 5000. ● hwBoardDropRuntPacketNotify: Some packets of 64 to 86 bytes or 145 to 193 bytes are discarded.
Default switch status	Default status of the trap function: ● on: indicates that the trap function is enabled by default. ● off: indicates that the trap function is disabled by default.
Current switch status	Trap function status: ● on: The trap function is enabled. ● off: The trap function is disabled.

Related Topics

3.2.34 snmp-agent trap enable feature-name entityexttrap

3.2.16 display snmp-agent trap feature-name entitymib all

Function

display snmp-agent trap feature-name entitymib all command displays the status of all traps on the ENTITYMIB module.

Format

display snmp-agent trap feature-name entitymib all

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

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

Prerequisites

SNMP has been enabled. For details, see **snmp-agent**.

Example

# Display all the traps of the ENTITYMIB module.

```
<HUAWEI>display snmp-agent trap feature-name entitymib all
------------------------------------------------------------------------------
Feature name: ENTITYMIB
Trap number : 1
------------------------------------------------------------------------------
Trap name                     Default switch status   Current switch status
entConfigChange                 on                     on
```

Table 3-30 Description of the display snmp-agent trap feature-name entitymib all command output

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

Item	Specification
Trap name	Trap name. Traps of the ENTITYMIB module include: ● entConfigChange: The entity MIB changes.
Default switch status	Default status of the trap function: ● on: indicates that the trap function is enabled by default. ● off: indicates that the trap function is disabled by default.
Current switch status	Status of the trap function: ● on: indicates that the trap function is enabled. ● off: indicates that the trap function is disabled.

Related Topics

3.2.35 snmp-agent trap enable feature-name entitymib

3.2.17 display snmp-agent trap feature-name entitytrap all

Function

display snmp-agent trap feature-name entitytrap all command displays the status of all traps on the ENTITYTRAP module.

Format

display snmp-agent trap feature-name entitytrap all

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

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

Prerequisites

SNMP has been enabled. For details, see **snmp-agent**.

Example

# Display all the traps of the ENTITYTRAP module.

```
<HUAWEI>display snmp-agent trap feature-name entitytrap all
------------------------------------------------------------------------------
Feature name: ENTITYTRAP
Trap number : 79
------------------------------------------------------------------------------
Trap name                          Default switch status   Current switch status
hwChassisRemove                    on                      on
hwChassisInsert                    on                      on
hwChassisFail                      on                      on
hwChassisFailResume                on                      on
hwChassisInvalid                   on                      on
hwChassisInvalidResume             on                      on
hwChassisLeaveMaster               on                      on
hwChassisBecomeMaster              on                      on
hwBoardRemove                      on                      on
hwBoardInsert                      on                      on
hwBoardFail                        on                      on
hwBoardFailResume                  on                      on
hwBoardInvalid                     on                      on
hwBoardInvalidResume               on                      on
hwBoardLeaveMaster                 on                      on
hwBoardBecomeMaster                on                      on
hwCardRemove                       on                      on
hwCardInsert                       on                      on
hwCardFail                         on                      on
hwCardFailResume                   on                      on
hwCardInvalid                      on                      on
hwCardInvalidResume                on                      on
hwOpticalRemove                    on                      on
hwOpticalInsert                    on                      on
hwOpticalFail                      on                      on
hwOpticalFailResume                on                      on
hwOpticalInvalid                   on                      on
hwOpticalInvalidResume             on                      on
hwOpticalTunableNotMatch           off                     on
hwOpticalTunableNotMatchResume     off                     on
hwPowerRemove                      on                      on
hwPowerInsert                      on                      on
hwPowerFail                        on                      on
hwPowerFailResume                  on                      on
hwPowerInvalid                     on                      on
hwPowerInvalidResume               on                      on
hwPowerUnusable                    on                      on
hwPowerUnusableResume              on                      on
hwFanRemove                        on                      on
hwFanInsert                        on                      on
hwFanFail                          on                      on
hwFanFailResume                    on                      on
hwFanInvalid                       on                      on
hwFanInvalidResume                 on                      on
hwFanUnusable                      on                      on
hwFanUnusableResume                on                      on
hwLCDRemove                        on                      on
hwLCDInsert                        on                      on
hwLCDInvalid                       on                      on
hwLCDInvalidResume                 on                      on
hwLCDUnusable                      on                      on
hwLCDUnusableResume                on                      on
hwCMURemove                        on                      on
hwCMUInsert                        on                      on
```

```
hwCMUInvalid                on                  on
hwCMUInvalidResume          on                  on
hwCMUUnusable               on                  on
hwCMUUnusableResume         on                  on
hwCommunicateError          on                  on
hwCommunicateResume         on                  on
hwHumidityAlarm             on                  on
hwHumidityResume            on                  on
hwVoltAlarm                 on                  on
hwVoltResume                on                  on
hwGateAlarm                 on                  on
hwGateResume                on                  on
hwFogAlarm                  on                  on
hwFogResume                 on                  on
hwUnstableAlarm             on                  on
hwUnstableResume            on                  on
hwBrdTempAlarm              on                  on
hwBrdTempResume             on                  on
hwCPUUtilizationRising      on                  on
hwCPUUtilizationResume      on                  on
hwMemUtilizationRising      on                  on
hwMemUtilizationResume      on                  on
hwBatteryFull               on                  on
hwOpticalMayInvalid         on                  on
hwOpticalMayInvalidResume   on                  on
```

Table 3-31 Description of the display snmp-agent trap feature-name entitytrap all command output

Item	Specification
Feature name	Name of the module that the trap belongs to.
Trap number	Number of traps.
Trap name	Trap name.
Default switch status	Default status of the trap function: ● on: indicates that the trap function is enabled by default. ● off: indicates that the trap function is disabled by default.
Current switch status	Status of the trap function: ● on: indicates that the trap function is enabled. ● off: indicates that the trap function is disabled.

Related Topics

3.2.36 snmp-agent trap enable feature-name entitytrap

3.2.18 display snmp-agent trap feature-name srmtrap all

Function

display snmp-agent trap feature-name srmtrap all command displays the status of all traps on the SRMTRAP module.

Format

display snmp-agent trap feature-name srmtrap all

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

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

Prerequisites

SNMP has been enabled. For details, see **snmp-agent**.

Example

# Display all the traps of the SRMTRAP module.

```
<HUAWEI>display snmp-agent trap feature-name srmtrap all
------------------------------------------------------------------------------
Feature name: SRMTRAP
Trap number : 68
------------------------------------------------------------------------------
Trap name                     Default switch status   Current switch status
hwPortPhysicalAutoNegotiateFail
                              on                      on
hwPortPhysicalEthHalfDuplexAlarm
                              on                      on
hwPortPhysicalAutoNegotiateClear
                              on                      on
hwPortPhysicalEthFullDuplexClear
                              on                      on
hwfanOffline                  on                      on
hwfanOnline                   on                      on
hwTempRisingAlarm             on                      on
hwTempRisingResume            on                      on
hwTempFallingAlarm            on                      on
hwTempFallingResume           on                      on
hwtempchipexcption            on                      on
hwtempchipexcptionresume      on                      on
hwfanfault                    on                      on
hwfanfaultresume              on                      on
hwphychipabnormal             on                      on
hwPHYfaultresume              on                      on
hwtxpowerexceedminor          on                      on
hwtxpowerresume               on                      on
hwrxpowerexceedminor          on                      on
```

```
hwrxpowerresume                 on                  on
hwPortPhysicalPortTypeChange    on                  on
hwPowerabsent                   on                  on
hwPowerabsentresume             on                  on
hwPowerfault                    on                  on
hwPowerfaultresume              on                  on
hwTXPowerExceedMajor            on                  on
hwRXPowerExceedMajor            on                  on
hwBIASExceedMajor               on                  on
hwBIASExceedMinor               on                  on
hwBIASResume                    on                  on
hwPHYfault                      on                  on
hwPCIfault                      on                  on
hwPCIfaultResume                on                  on
hwXAUIREFClockFault             on                  on
hwXAUIREFClockFaultResume       on                  on
hwCPICoreClockFault             on                  on
hwCPICoreClockFaultResume       on                  on
hwLanSwitchFault                on                  on
hwLanSwitchFaultResume          on                  on
hwCLPDCheckFault                on                  on
hwCLPDCheckFaultResume          on                  on
hwFPGACheckFault                on                  on
hwFPGACheckFaultResume          on                  on
hwEEPROMCheckFault              on                  on
hwEEPROMCheckFaultResume        on                  on
hwLightFault                    on                  on
hwLightFaultResume              on                  on
hwPOEFault                      on                  on
hwPOEFaultResume                on                  on
hwUSBFault                      on                  on
hwUSBFaultResume                on                  on
hwUSBPlugIn                     on                  on
hwUSBPlugOut                    on                  on
hwUSBPowerFault                 on                  on
hwUSBPowerFaultResume           on                  on
hwI2CFault                      on                  on
hwI2CFaultResume                on                  on
hwSubcardPullOut                on                  on
hwSubcardPlugIn                 on                  on
hwRTCfault                      on                  on
hwRTCfaultresume                on                  on
hwWriteFlashError               on                  on
hwWriteFlashErrorResume         on                  on
hwOpticalPowerAbnormal          on                  on
hwOpticalPowerResume            on                  on
hwEntityHeartbeatTrap           on                  on
hwPoeChipFault                  on                  on
hwPoeChipResume                 on                  on
```

Table 3-32 Description of the display snmp-agent trap feature-name srmtrap all command output

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

Item	Specification
Trap name	Trap name. Traps of the SRMTRAP module include: ● hwbiasexceedmajor: The bias current exceeds the upper threshold. ● hwbiasexceedmajor: The bias current falls below the lower threshold. ● hwbiasresume: The bias current restores to the normal range. ● hwclpdcheckfault: CPLD check fails. ● hwclpdcheckfaultresume: CPLD check succeeds. ● hwcpicoreclockfault: CPI kernel clock becomes faulty. ● hwcpicoreclockfaultresume: CPI kernel clock recovers from a fault. ● hweepromcheckfault: EEPROM check fails. ● hweepromcheckfaultresume: EEPROM check succeeds. ● hwentityheartbeattrap: The device sends a heartbeat notification. ● hwfanfault: A fan module becomes faulty. ● hwfanfaultresume: A fan module recovers from a fault. ● hwfanoffline: A fan module is unavailable. ● hwfanonline: A fan module becomes available. ● hwfpgacheckfault: FPGA check fails. ● hwfpgacheckfaultresume: FPGA check succeeds. ● hwi2cfault: An I2C fault occurs. ● hwi2cfaultresume: An I2C fault is rectified. ● hwlanswitchfault: An LSW chip becomes faulty. ● hwlanswitchfaultresume: An LSW chip recovers from a fault. ● hwlightfault: An indicator becomes faulty. ● hwlightfaultresume: An indicator recovers from a fault. ● hwopticalpowerabnormal: The optical module power is out of the normal range. ● hwopticalpowerresume: The optical module power restores to the normal range. ● hwpcifault: A PCI fault occurs. ● hwpcifaultresume: A PCI fault is rectified. ● hwphychipabnormal: A PHY chip is faulty. ● hwphyfault: A PHY fault occurs. ● hwphyfaultresume: A PHY fault is rectified.

Item	Specification
	- hwpoechipfault: A PoE chip is faulty. - hwpoechipresume: A PoE chip recovers from a fault. - hwpoefault: The PoE function is unavailable. - hwpoefaultresume: A PoE function becomes available. - hwportphysicalautonegotiateclear: Port auto-negotiation succeeds. - hwportphysicalautonegotiatefail: Port auto-negotiation fails. - hwportphysicalethfullduplexclea: A port is in full-duplex mode. - hwportphysicalethhalfduplexalarm: A port is in half-duplex mode. - hwportphysicalporttypechange: The port type changes. - hwpowerabsent: A power module is unavailable. - hwpowerabsentresume: A power module becomes available. - hwpowerfault: A power module is faulty. - hwphyfaultresume: A power module recovers from a fault. - hwrtcfault: A real-time clock (RTC) is faulty. - hwrtcfaultresume: A real-time clock (RTC) recovers from a fault. - hwrxpowerexceedmajor: The Rx power exceeds the upper threshold. - hwrxpowerexceedminor: The Rx power falls below the lower threshold. - hwrxpowerresume: The Rx power restores to the normal range. - hwsubcardplugin: A subcard is installed. - hwsubcardpullout: A subcard is removed. - hwtempchipexcption: A temperature sensor chip is faulty. - hwtempchipexcptionresume: A temperature sensor chip recovers from a fault. - hwtempfallingalarm: The device temperature is too low. - hwtempfallingresume: The device temperature restores to the normal range. - hwtemprisingalarm: The device temperature is too high.

Item	Specification
	● hwtemprisingresume: The device temperature restores to the normal range. ● hwtxpowerexceedmajor: The Tx power exceeds the upper threshold. ● hwtxpowerexceedminor: The Tx power falls below the lower threshold. ● hwtxpowerresume: The Tx power restores to the normal range. ● hwusbfault: A USB flash drive is faulty. ● hwusbfaultresume: A USB flash drive recovers from a fault. ● hwusbplugin: A USB flash drive is installed. ● hwusbplugout: A USB flash drive is removed. ● hwusbpowerfault: A USB 5V power module is faulty. ● hwusbpowerfaultresume: A USB 5V power module recovers from a fault. ● hwwriteflasherror: An error occurs when data is written to the flash memory. ● hwwriteflasherrorresume: An error that occurs when data is written to the flash memory is resolved. ● hwxauirefclockfault: An XAUIREF clock is faulty. ● hwxauirefclockfaultresume: An XAUIREF clock recovers from a fault.
Default switch status	Default status of the trap function: ● on: indicates that the trap function is enabled by default. ● off: indicates that the trap function is disabled by default.
Current switch status	Status of the trap function: ● on: indicates that the trap function is enabled. ● off: indicates that the trap function is disabled.

Related Topics

3.2.37 snmp-agent trap enable feature-name srmtrap

3.2.19 display snmp-agent trap feature-name swithsrvres all

Function

display snmp-agent trap feature-name swithsrvres all command displays the status of all traps on the SWITHSRVRES module.

Format

display snmp-agent trap feature-name swithsrvres all

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

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

Prerequisites

SNMP has been enabled. For details, see **snmp-agent**.

Example

# Display all the traps of the SWITHSRVRES module.

```
<HUAWEI>display snmp-agent trap feature-name swithsrvres all
------------------------------------------------------------------------------
Feature name: SWITHSRVRES
Trap number : 3
------------------------------------------------------------------------------
Trap name                       Default switch status   Current switch status
hwSrvServiceExceedThreshould    on                      on
hwSrvServiceExceedThreshouldResume
                                on                      on
hwSrvServiceConfigFailed        on                      on
```

Table 3-33 Description of the display snmp-agent trap feature-name swithsrvres all command output

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

Item	Specification
Trap name	Trap name. Traps of the SWITHSRVRES module include: ● hwSrvServiceExceedThreshould: The service configurations exceed the recommended threshold. ● hwSrvServiceExceedThreshouldResume: The service configurations fall below the recommended threshold. ● hwSrvServiceConfigFailed: The service configurations fail.
Default switch status	Default status of the trap function: ● on: indicates that the trap function is enabled by default. ● off: indicates that the trap function is disabled by default.
Current switch status	Status of the trap function: ● on: indicates that the trap function is enabled. ● off: indicates that the trap function is disabled.

Related Topics

3.2.38 snmp-agent trap enable feature-name swithsrvres

3.2.20 display snmp-agent trap feature-name system all

Function

The **display snmp-agent trap feature-name system all** command displays the status of all the traps of the SYSTEM module.

Format

display snmp-agent trap feature-name system all

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display snmp-agent trap feature-name system all** command to check status of all SYSTEM traps. This status can be configured using the **3.2.39 snmp-agent trap enable feature-name system** command.

Example

# Display the status of all the traps of the SYSTEM module.

```
<HUAWEI> display snmp-agent trap feature-name system all
------------------------------------------------------------------------------
Feature name: SYSTEM
Trap number : 8
------------------------------------------------------------------------------
Trap name                       Default switch status   Current switch status
hwSysReloadNotification          off                     off
hwSysClockChangedNotification    off                     off
hwPatchErrorTrap                 off                     off
hwPatchActiveOverTimeTrap        off                     off
hwPatchMalfunctionComebackTrap   off                     off
hwSysSlaveSwitchFailNotification
                                 off                     off
hwSysSlaveSwitchSuccessNotification
                                 off                     off
hwSysIssuNotification            off                     off
```

Table 3-34 Description of the display snmp-agent trap feature-name system 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 **3.2.39 snmp-agent trap enable feature-name system** command.

Related Topics

3.2.39 snmp-agent trap enable feature-name system

3.2.21 display wavelength-map

Function

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

NOTE

This command is not supported by S1720GFR, S2750, S5700LI, and S5700S-LI.

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 3-35 Description of the **display wavelength-map** command output

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

Related Topics

3.2.44 wavelength-channel

3.2.22 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
```

3.2.23 reset slot

Function

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

Format

reset slot *slot-id*

Parameters

Parameter	Description	Value
slot-id	Specifies the stack ID of the device that needs to be restarted.	The value must be set according to the device configuration.

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/slave 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.

Example

# Restart stack member with stack ID 1.

```
<HUAWEI> reset slot 1
Warning: Confirm to reset slot 1? [Y/N]:y
Info: The board 1 is reset successfully.
```

3.2.24 set device battery lifetime

Function

The **set device battery lifetime** command sets the lifetime expiration alarm threshold for a lithium battery.

By default, the lifetime expiration alarm threshold for a lithium battery is 20 minutes.

NOTE

Only the S5700-28P-LI-BAT and S5700-28P-LI-24S-BAT that have a lithium battery installed support this command.

Format

set device battery lifetime threshold *threshold* [**slot** *slot-id*]

Parameters

Parameter	Description	Value
threshold *threshold*	Sets the lifetime expiration alarm threshold for a lithium battery.	The value is an integer that ranges from 10 to 60, in minutes.
slot *slot-id*	Specifies the slot ID of the lithium battery.	The value is fixed as 0 currently.

Views

System view

Default Level

3: Management level

Usage Guidelines

Use Scenario

If a lithium battery discharges too fast, its lifetime is about to expire. During a discharge, if the time taken to consume 10% of the total power is shorter than the configured alarm threshold, the lifetime of the lithium battery is about to expire. When this occurs, the device generates an alarm. When receiving this alarm, replace the lithium battery to ensure normal operation of the device in the case of a mains power outage.

Precautions

When the S5700-28P-LI-BAT and S5700-28P-LI-24S-BAT have no battery or a lead-acid battery installed, the system displays a message indicating that this command is not supported.

Example

# Set the lifetime expiration alarm threshold for the lithium battery to 50 minutes.

```
<HUAWEI> system-view
[HUAWEI] set device battery lifetime threshold 50
```

Related Topics

3.2.7 display device battery lifetime threshold

3.2.25 set device battery off

Function

The **set device battery off** command turns off the lithium battery on a device so that the battery no longer supplies power to the device.

NOTE

Only the S5700-28P-LI-BAT and S5700-28P-LI-24S-BAT that have a lithium battery installed support this command.

Format

set device battery off [**slot** *slot-id*]

Parameters

Parameter	Description	Value
slot *slot-id*	Specifies the slot ID of the lithium battery.	The value is fixed as 0 currently.

Views

System view

Default Level

3: Management level

Usage Guidelines

Use Scenario

If a device has a lithium battery installed, the lithium battery can supply power to the device after the power supply of the device is turned off. To power off the device, turn off the lithium battery after powering off the power supply.

Precautions

This command can be executed only if a lithium battery is available and the power supply of the device has been turned off. If no lithium battery is available or the power supply of the device is on, the system displays a message indicating that the command cannot be executed.

Example

# Turn off the lithium battery.

```
<HUAWEI> system-view
[HUAWEI] set device battery off
Info: The system is now comparing the configuration, please wait.
Warning: The configuration has been modified, and it will be saved to the next startup saved-configuration
file flash:/vrpcfg.zip. Continue? [Y/N]:N
Warning:The battery in slot 0 will be turned off and the device will be powered off. Continue? (Y/N): Y
```

3.2.26 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.

NOTE

Only the S1720GW, S1720GWR, S1720X, S1720GW-E, S1720GWR-E, S1720X-E, S2720EI, S5700S-LI (only the S5700S-28X-LI-AC and S5700S-52X-LI-AC), S5710-X-LI, S5720LI, S5720S-LI, S5720S-SI, S5720SI, S5720EI, S5730SI, S5730S-EI, S6720LI, S6720S-LI, S6720SI, S6720S-SI, S6720S-EI, and S6720EI support this command.

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.	-

Parameter	Description	Value
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.	The value range depends on the device configuration.

Views

System view

Default Level

3: Management level

Usage Guidelines

Use Scenario

The fault indicator status of the device is indicated by mode indicators and the system indicator. When a device becomes faulty, you can configure mode indicators and the system indicator on the device to blink red fast so that maintenance personnel can quickly find this device on site.

Precautions

Mode indicators include the STAT indicator, SPED indicator, PoE indicator (supported only on PoE switches) and STCK indicator. The system indicator is the SYS indicator, which indicates the system running status.

When the **set device fault-light under-repair** command is executed, the system indicator and all mode indicators blink red fast. After these indicators blink red fast for the time specified by **keeptime** *time*, the following situations occur:

- The system indicator restores to the previous status.
- The STAT indicator is steady on.
- When the stack function is enabled, the STCK indicator on the master switch blinks slowly, while the STCK indicators on the other member devices are off.
- When the stack function is disabled, the STCK indicator is off.
- Other mode indicators are off.

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 following situations occur:

- The system indicator restores to the previous status.
- The STAT indicator is steady on.
- When the stack function is enabled, the STCK indicator on the master switch blinks slowly, while the STCK indicators on the other member devices are off.

- When the stack function is disabled, the STCK indicator is off.
- Other mode indicators are off

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
```

Related Topics

3.2.8 display device fault-light

3.2.27 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.

NOTE

The following switches do not support this command:

- S1720GW series
- S1720GW-E series
- S1720GWR series: S1720-28GWR-4P, S1720-28GWR-4X, and S1720-28GWR-PWR-4TP
- S1720GWR-E series: S1720-28GWR-4P-E, S1720-28GWR-4X-E, and S1720-28GWR-PWR-4TP-E
- S1720GFR series
- S2720EI series: S2720-12TP-EI, S2720-12TP-PWR-EI, S2720-28TP-EI, S2720-28TP-PWR-EI-L
- S2750EI series: S2750-28TP-EI-AC and S2751-28TP-PWR-EI-AC
- S5700LI series: S5700-28TP-LI-AC, S5700-28P-LI-AC, S5700-28P-LI-DC, S5700-10P-LI-AC, and S5700-10P-PWR-LI-AC
- S5700S-LI series: S5700S-28P-LI-AC
- S5710-X-LI series: S5710-28X-LI-AC
- S5720LI 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
- S5720S-LI series: S5720S-12TP-LI-AC, S5720S-12TP-PWR-LI-AC, S5720S-28P-LI-AC, S5720S-28TP-PWR-LI-AC, and S5720S-28X-LI-AC
- S5720S-SI series: S5720S-28P-SI-AC, S5720S-28X-SI-AC, and S5720S-28X-SI-DC

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.
slot *slot-id*	● Specifies the slot ID when stack is not configured. ● Specifies the stack ID when a stack is configured. If this parameter is not specified, the thresholds in all slots are set.	The value is an integer that ranges from 0 to 8.

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 temperature threshold after modification is lower than the default temperature threshold.

Precautions

- The new thresholds are the fixed temperature thresholds minus *threshold-value*. After this command is executed, both the threshold for increasing the fan speed and the threshold for lowering the fan speed are reduced.
- 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.
```

Related Topics

3.2.9 display fan speed-adjust threshold minus

3.2.28 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 memory usage alarm threshold is 90% and the memory usage alarm recovery threshold is 85% on the S5720EI. On the S1720GFR, S2750EI, S5700LI and S5700S-LI , The following describes the memory usage alarm threshold :

- 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 *threshold-value*	Specifies the memory usage threshold.	The value is an integer that ranges from 75 to 100.
slot *slot-id*	Specifies the memory usage threshold of the device. *slot-id* specifies the stack ID.	The value is an integer that ranges from 1 to 8.

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
```

Related Topics

3.1.14 display memory-usage threshold

3.2.29 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

undo set root-key

Parameters

None

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.

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, the configuration file of the switch cannot be exported and used on other devices.

Example

# Set the root key to **huawei**.

```
<HUAWEI> set root-key
Warning: A new root key can take effect only after the device is restarted. Are you sure you want to
configure it. Continue? [Y/N]:y
Please enter a new key of no more than 32 characters:huawei
Please enter the new key again:huawei
Info: Successed in setting next root-key on the master board.
```

3.2.30 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 S5720HI.

Format

set service-mode enhanced

undo set service-mode enhanced

Parameters

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

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

By default, S5720HIs work in normal mode, requiring the interval for receiving BFD packets to be longer than or equal to 100 ms. If the interval cannot meet requirements, run the **set service-mode** command to change the working mode of an S5720HI to enhanced so that the S5720HI supports a minimum of 3 ms interval.

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.

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
```

Related Topics

3.2.12 display service-mode configuration

3.2.31 slave restart

Function

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

NOTE

Devices that do not support the stack function or do not have the stack function enabled do not support this function.

Format

slave restart

Parameters

None

Views

System view

Default Level

3: Management level

Usage Guidelines

To upgrade the system software in-service, first upgrade the software on the standby device when the master device works normally, and then restart the standby device. After the standby device is ready, perform active/standby switchover and upgrade the software on the master device.

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
```

3.2.32 slave switchover

Function

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

NOTE

Devices that do not support the stack function or do not have the stack function enabled do not support this function.

Format

slave switchover

Parameters

None

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

In a stack containing multiple switches, you can manually switch the master and standby switches during software upgrade or system maintenance. After the active/standby switchover is complete, the original master switch joins the stack after restarting, and the original switch becomes the new master switch.

Prerequisites

- The forcible active/standby switchover has been enabled on devices.
- The **3.2.13 display switchover state** command output shows that system has met requirements for 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 active and standby MPUsmaster and standby switches.

Precautions

You can run the **slave switchover** command to perform an active/standby switchover only in a stack containing multiple switches.

Before commands have been executed, if the **slave switchover** command is executed to perform an active/standby switchover, 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.

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
```

Related Topics

3.2.13 display switchover state

3.2.33 slave switchover { disable | enable }

3.2.33 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

Devices that do not support the stack function or do not have the stack function enabled do not support this function.

Format

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

undo slave switchover disable

Parameters

Parameter	Description	Value
disable	Disables forcible master/slave switchover.	-
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 **3.2.32 slave switchover** command does not take effect.

Example

# Disable forcible master/slave switchover.

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

Related Topics

3.2.13 display switchover state

3.2.32 slave switchover

3.2.34 snmp-agent trap enable feature-name entityexttrap

Function

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

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

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

Format

snmp-agent trap enable feature-name entityexttrap [**trap-name** *trap-name*]

undo snmp-agent trap enable feature-name entityexttrap [**trap-name** *trap-name*]

Parameters

Parameter	Description	Value
trap-name *trap-name*	Enables or disables the trap function of the specified event for the ENTITYEXTTRAP module.	The value is a trap name. Traps of the ENTITYEXTTRAP module include: ● hwentityinputratethresholdalarm: The bandwidth usage of incoming traffic exceeds the threshold. ● hwentityinputratethresholdalarmresume: The bandwidth usage of incoming traffic falls below the threshold. ● hwentityoutputratethresholdalarm: The bandwidth usage of outgoing traffic exceeds the threshold. ● hwentityoutputratethresholdalarmresume: The bandwidth usage of outgoing traffic falls below the threshold. ● hwentityhigerrorpacketthresholdalarm: Incoming packets are discarded because an error is detected during physical layer detection. ● hwentityhigstatechangenotify: The Higig port status changes. ● hwentityhigstatedownnotify: The Higig port status remains Down. ● hwentityruntpacketchecknotify: The number of packet fault recoveries detected on a port exceeds 5000.

Parameter	Description	Value
		- hwboarddroprunt-packetnotify: Some packets of 64 to 86 bytes or 145 to 193 bytes are discarded.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

After the trap function is enabled on a switch, the switch will generate traps during operation and send the traps to the NMS through the SNMP module. If the trap function is disabled on the switch, the switch will not generate traps and not send traps to the NMS through the SNMP module.

You can specify the parameter **trap-name** to enable one or more event traps.

Example

# Enable the hwboardsoftwareversionincompatible trap for the ENTITYEXTTRAP module.

```
<HUAWEI> system-view
[HUAWEI] snmp-agent trap enable feature-name entityexttrap trap-name
hwboardsoftwareversionincompatible
```

Related Topics

3.2.15 display snmp-agent trap feature-name entityexttrap all

3.2.35 snmp-agent trap enable feature-name entitymib

Function

snmp-agent trap enable feature-name entitymib command enables the trap function for the ENTITYMIB module.

undo snmp-agent trap enable feature-name entitymib command disables the trap function for the ENTITYMIB module.

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

Format

snmp-agent trap enable feature-name entitymib [**trap-name entconfigchange**]

undo snmp-agent trap enable feature-name entitymib [**trap-name entconfigchange**]

Parameters

Parameter	Description	Value
trap-name	Enables or disables the trap function for the specified event.	-
entconfigchange	Enables the trap function when the entity MIB changes.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

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

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

Example

# Enable the entconfigchange trap of the ENTITYMIB module.

```
<HUAWEI> system-view
[HUAWEI] snmp-agent trap enable feature-name entitymib trap-name entconfigchange
```

Related Topics

3.2.16 display snmp-agent trap feature-name entitymib all

3.2.36 snmp-agent trap enable feature-name entitytrap

Function

snmp-agent trap enable feature-name entitytrap command enables the trap function for the ENTITYTRAP module.

undo snmp-agent trap enable feature-name entitytrap command disables the trap function for the ENTITYTRAP module.

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

Format

snmp-agent trap enable feature-name entitytrap [**trap-name** *trap-name*]

undo snmp-agent trap enable feature-name entitytrap [**trap-name** *trap-name*]

Parameters

Parameter	Description	Value
trap-name *trap-name*	Specifies the trap for an event of the ENTITYTRAP module.	The value is an enumerated value and must be set as prompted by the device.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

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

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

Example

# Enable the hwentitytrapconflictdetect trap of the ENTITYTRAP module.

```
<HUAWEI> system-view
[HUAWEI] snmp-agent trap enable feature-name entitytrap trap-name hwpowerfail
```

Related Topics

3.2.17 display snmp-agent trap feature-name entitytrap all

3.2.37 snmp-agent trap enable feature-name srmtrap

Function

snmp-agent trap enable feature-name srmtrap command enables the trap function for the SRMTRAP module.

undo snmp-agent trap enable feature-name srmtrap command disables the trap function for the SRMTRAP module.

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

Format

snmp-agent trap enable feature-name srmtrap [**trap-name** *trap-name*]

undo snmp-agent trap enable feature-name srmtrap [**trap-name** *trap-name*]

Parameters

Parameter	Description	Value
trap-name *trap-name*	Specifies the trap for an event of the SRMTRAP module.	● hwbiasexceedmajor: The bias current exceeds the upper threshold. ● hwbiasexceedmajor: The bias current falls below the lower threshold. ● hwbiasresume: The bias current restores to the normal range. ● hwclpdcheckfault: CPLD check fails. ● hwclpdcheckfaultresume: CPLD check succeeds. ● hwcpicoreclockfault: CPI kernel clock becomes faulty. ● hwcpicoreclockfaultresume: CPI kernel clock recovers from a fault. ● hweepromcheckfault: EEPROM check fails. ● hweepromcheckfaultresume: EEPROM check succeeds. ● hwentityheartbeattrap: The device sends a heartbeat notification. ● hwfanfault: A fan module becomes faulty. ● hwfanfaultresume: A fan module recovers from a fault. ● hwfanoffline: A fan module is unavailable. ● hwfanonline: A fan module becomes available. ● hwfpgacheckfault: FPGA check fails.

Parameter	Description	Value
		● hwfpgacheckfaultresume: FPGA check succeeds. ● hwi2cfault: An I2C fault occurs. ● hwi2cfaultresume: An I2C fault is rectified. ● hwlanswitchfault: An LSW chip becomes faulty. ● hwlanswitchfaultresume: An LSW chip recovers from a fault. ● hwlightfault: An indicator becomes faulty. ● hwlightfaultresume: An indicator recovers from a fault. ● hwopticalpowerabnormal: The optical module power is out of the normal range. ● hwopticalpowerresume: The optical module power restores to the normal range. ● hwpcifault: A PCI fault occurs. ● hwpcifaultresume: A PCI fault is rectified. ● hwphychipabnormal: A PHY chip is faulty. ● hwphyfault: A PHY fault occurs. ● hwphyfaultresume: A PHY fault is rectified. ● hwpoechipfault: A PoE chip is faulty. ● hwpoechipresume: A PoE chip recovers from a fault. ● hwpoefault: The PoE function is unavailable.

Parameter	Description	Value
		● hwpoefaultresume: A PoE function becomes available. ● hwportphysicalauto-negotiateclear: Port auto-negotiation succeeds. ● hwportphysicalauto-negotiatefail: Port auto-negotiation fails. ● hwportphysicalethfull-duplexclea: A port is in full-duplex mode. ● hwportphysicaleth-halfduplexalarm: A port is in half-duplex mode. ● hwportphysicalporttypechange: The port type changes. ● hwpowerabsent: A power module is unavailable. ● hwpowerabsentresume: A power module becomes available. ● hwpowerfault: A power module is faulty. ● hwphyfaultresume: A power module recovers from a fault. ● hwrtcfault: A real-time clock (RTC) is faulty. ● hwrtcfaultresume: A real-time clock (RTC) recovers from a fault. ● hwrxpowerexceedmajor: The Rx power exceeds the upper threshold. ● hwrxpowerexceedminor: The Rx power falls below the lower threshold.

Parameter	Description	Value
		● hwrxpowerresume: The Rx power restores to the normal range. ● hwsubcardplugin: A subcard is installed. ● hwsubcardpullout: A subcard is removed. ● hwtempchipexcption: A temperature sensor chip is faulty. ● hwtempchipexcption-resume: A temperature sensor chip recovers from a fault. ● hwtempfallingalarm: The device temperature is too low. ● hwtempfallingresume: The device temperature restores to the normal range. ● hwtemprisingalarm: The device temperature is too high. ● hwtemprisingresume: The device temperature restores to the normal range. ● hwtxpowerexceedmajor: The Tx power exceeds the upper threshold. ● hwtxpowerexceedminor: The Tx power falls below the lower threshold. ● hwtxpowerresume: The Tx power restores to the normal range. ● hwusbfault: A USB flash drive is faulty. ● hwusbfaultresume: A USB flash drive recovers from a fault.

Parameter	Description	Value
		● hwusbplugin: A USB flash drive is installed. ● hwusbplugout: A USB flash drive is removed. ● hwusbpowerfault: A USB 5V power module is faulty. ● hwusbpowerfaultresume: A USB 5V power module recovers from a fault. ● hwwriteflasherror: An error occurs when data is written to the flash memory. ● hwwriteflasherrorresume: An error that occurs when data is written to the flash memory is resolved. ● hwxauirefclockfault: An XAUIREF clock is faulty. ● hwxauirefclockfaultresume: An XAUIREF clock recovers from a fault.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

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

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

Example

# Enable the hwclpdcheckfault trap of the SRMTRAP module.

```
<HUAWEI> system-view
[HUAWEI] snmp-agent trap enable feature-name srmtrap trap-name hwclpdcheckfault
```

Related Topics

3.2.18 display snmp-agent trap feature-name srmtrap all

3.2.38 snmp-agent trap enable feature-name swithsrvres

Function

snmp-agent trap enable feature-name swithsrvres command enables the trap function for the SWITHSRVRES module.

undo snmp-agent trap enable feature-name swithsrvres command disables the trap function for the SWITHSRVRES module.

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

Format

snmp-agent trap enable feature-name swithsrvres [**trap-name** { **hwsrvserviceconfigfailed** | **hwsrvserviceexceedthreshould** | **hwsrvserviceexceedthreshouldresume** }]

undo snmp-agent trap enable feature-name swithsrvres [**trap-name** { **hwsrvserviceconfigfailed** | **hwsrvserviceexceedthreshould** | **hwsrvserviceexceedthreshouldresume** }]

Parameters

Parameter	Description	Value
trap-name	Enables or disables the trap function for the specified event.	-
hwsrvserviceconfig-failed	Enables the trap function when the service configurations fail.	-
hwsrvserviceexceed-threshould	Enables the trap function when the service configurations exceed the recommended threshold.	-
hwsrvserviceexceed-threshouldresume	Enables the trap function when the service configurations fall below the recommended threshold.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

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

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

Example

# Enable the hwsrvserviceconfigfailed trap of the SWITHSRVRES module.

```
<HUAWEI> system-view
[HUAWEI] snmp-agent trap enable feature-name swithsrvres trap-name hwsrvserviceconfigfailed
```

Related Topics

3.2.19 display snmp-agent trap feature-name swithsrvres all

3.2.39 snmp-agent trap enable feature-name system

Function

The **snmp-agent trap enable feature-name system** command enables an SYSTEM trap.

The **undo snmp-agent trap enable feature-name system** command disables an SYSTEM trap.

Format

snmp-agent trap enable feature-name system [**trap-name** *trap-name*]

undo snmp-agent trap enable feature-name system [**trap-name** *trap-name*]

Parameters

Parameter	Description	Value
trap-name *trap-name*	Specifies the name of a trap.	The value is an enumerated value and must be set as prompted by the device.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

To enable the NMS to easily manage the SYSTEM module of the device, you can run the **snmp-agent trap enable feature-name system** command to enables an SYSTEM trap. The command configuration ensures that the traps generated during the device operation are sent to the NMS. Otherwise, SYSTEM traps are not sent to the NMS.

You can run the **3.2.20 display snmp-agent trap feature-name system all** command to check the configuration result.

Example

# Enable the hwSysReloadNotification trap.

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

Related Topics

3.2.20 display snmp-agent trap feature-name system all

3.2.40 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 0°C, and the upper temperature threshold varies according to hardware of various models, ranging from 44°C to 74°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 the slot ID if stacking is not configured. - Specifies the stack ID if stacking is configured.	The value is integer that is 0 if stacking is not configured; and ranges from 0 to 8 if stacking is configured.
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 0 to 74. *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 0 to 74. *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 for all member switches in a stack.

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

Related Topics

3.1.18 display temperature

3.2.41 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

GE interface view, XGE interface view, 40GE 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
```

3.2.42 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

GE interface view, XGE interface view, 40GE 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
```

3.2.43 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.
```

3.2.44 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.

NOTE

This command is not supported by S1720GFR, S2750, S5700LI, and S5700S-LI.

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

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** 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.

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 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.

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
```

Related Topics

3.2.21 display wavelength-map

3.3 Information Center Configuration Commands

3.3.1 Command Support

3.3.2 display buffer

3.3.3 display channel

3.3.4 display debugging

3.3.5 display info-center

3.3.6 display info-center filter-id

3.3.7 display info-center rate-limit record

3.3.8 display info-center rate-limit threshold

3.3.9 display info-center statistics

3.3.10 display logbuffer

3.3.11 display logfile

3.3.12 display snmp-agent trap feature-name info all

3.3.13 display trapbuffer

3.3.14 info-center channel

3.3.15 info-center channel name

3.3.16 info-center enable

3.3.17 info-center filter-id

3.3.18 info-center local log-counter disable

3.3.19 info-center logbuffer

3.3.20 info-center logbuffer size

3.3.21 info-center logfile size

3.3.22 info-center loghost

3.3.23 info-center loghost source

3.3.24 info-center loghost source-port

3.3.25 info-center max-logfile-number

3.3.26 info-center rate-limit except

3.3.27 info-center rate-limit global-threshold

3.3.28 info-center rate-limit monitor-period

3.3.29 info-center rate-limit threshold

3.3.30 info-center source channel

3.3.31 info-center statistic-suppress enable

3.3.32 info-center timestamp

3.3.33 info-center trapbuffer

3.3.34 info-center trapbuffer size

3.3.35 reset info-center statistics

3.3.36 reset logbuffer

3.3.37 reset trapbuffer

3.3.38 save logfile

3.3.39 save logfile all

3.3.40 snmp-agent trap enable feature-name info

3.3.41 terminal debugging

3.3.42 terminal echo synchronous

3.3.43 terminal logging

3.3.44 terminal monitor

3.3.45 terminal trapping

3.3.1 Command Support

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

3.3.2 display buffer

Function

The **display buffer** command displays the statistics about logs cached in the buffer.

Format

display buffer [*feature-name* [*buffer-name*]]

Parameters

Parameter	Description	Value
feature-name	Name of the buffer dedicated to caching logs of a specific feature	-
buffer-name	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 volumes. 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 the statistics about log information in the buffer.

Example

# View the 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 3-36 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

Item	Description
Max length of message	Max length of message
Max number of message	Max number of message
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	Max rate record
Max rate timestamp	Max rate timestamp

3.3.3 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 than 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 3-37** 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 3-37 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 . 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.
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 3-38 Description of the display channel command output

Item	Description
channel number	Channel number, which ranges from 0 to 9.

Item	Description
channel name	Channel name. **Table 3-37** lists default channel names. To set the channel name, run the **3.3.15 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 **3.3.30 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 **3.3.30 info-center source channel** command.
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 **3.3.30 info-center source channel** command.

Related Topics

3.3.14 info-center channel

3.3.15 info-center channel name

3.3.16 info-center enable

3.3.30 info-center source channel

3.3.4 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*

NOTE

Only the S5720HI supports the **vcpu** *vcpu* parameter.

Parameters

Parameter	Description	Value
interface *interface-type interface-number*	Specifies the interface type and number.	-
all	Display debugging information on all interfaces.	-
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*	Specifies the virtual CPU number.	Specify the *vcpu* 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 3-39 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.

Related Topics

3.3.16 info-center enable

3.3.30 info-center source channel

3.3.41 terminal debugging

3.3.44 terminal monitor

3.3.5 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 3-40 Description of the display info-center command output

Item	Description
Information Center	Information center status: ● enabled ● disabled To enable the information center, run the **3.3.16 info-center enable** command.
Log host	Log host configuration.

Item	Description
10.1.1.1	Log host IP address. To set the log host IP address, run the **3.3.22 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 **3.3.14 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 **3.3.15 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 **3.3.22 info-center loghost** command.
host facility	Logging tool. To configure the logging tool, run the **3.3.22 info-center loghost** command.
Console	Console configuration.
Monitor	Remote terminal configuration.
SNMP Agent	SNMP agent configuration.
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 **3.3.19 info-center logbuffer** or **3.3.33 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 **3.3.20 info-center logbuffer size** or **3.3.34 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.

Item	Description
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 **3.3.32 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.

Related Topics

3.3.14 info-center channel

3.3.15 info-center channel name

3.3.16 info-center enable

3.3.19 info-center logbuffer

3.3.20 info-center logbuffer size

3.3.22 info-center loghost

3.3.32 info-center timestamp

3.3.33 info-center trapbuffer

3.3.34 info-center trapbuffer size

3.3.6 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 **3.3.17 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 3-41 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 **3.3.17 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 **3.3.17 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 **3.3.17 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.

Related Topics

3.3.17 info-center filter-id

3.3.7 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 3-42 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.

Related Topics

3.3.29 info-center rate-limit threshold

3.3.8 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 3-43 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.

Related Topics

3.3.29 info-center rate-limit threshold

3.3.9 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 3-44 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.

Item	Description
DebugSend	Number of sent debugging messages.
DebugDrop	Number of discarded debugging messages.

Related Topics

3.3.5 display info-center

3.3.16 info-center enable

3.3.30 info-center source channel

3.3.10 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.
security	Specifies the security logs.	-
slot *slot-id*	Displays logs in a specified slot.	The value must be set according to the device configuration.

Parameter	Description	Value
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.	-
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 3-45 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 **3.3.19 info-center logbuffer** command.
Allowed max buffer size	Maximum size of the log buffer.

Item	Description
Actual buffer size	Actual size of the log buffer. To set the log buffer size, run the **3.3.20 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 **3.3.14 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 **3.3.15 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 3-46 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.

Related Topics

3.3.5 display info-center

3.3.14 info-center channel

3.3.15 info-center channel name

3.3.16 info-center enable

3.3.19 info-center logbuffer

3.3.20 info-center logbuffer size

3.3.36 reset logbuffer

3.3.11 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.
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 *S1720, S2700, S5700, and S6720 V200R011C10 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)
```

Related Topics

3.3.16 info-center enable

3.3.38 save logfile

3.3.12 display snmp-agent trap feature-name info all

Function

display snmp-agent trap feature-name info all command displays all trap messages of the Information Center module.

Format

display snmp-agent trap feature-name info all

Parameters

None

Views

All views

Default Level

3: Management level

Usage Guidelines

The **display snmp-agent trap feature-name info all** command displays whether all trap functions of the Information Center module are enabled.

Example

# Display all trap messages of the Information Center module.

```
<HUAWEI> display snmp-agent trap feature-name info all
------------------------------------------------------------------------------
Feature name: INFO
Trap number : 2
------------------------------------------------------------------------------
Trap name                    Default switch status   Current switch status
hwICLogFileAging                on                      on
hwICLogBufferLose               on                      on
```

Table 3-47 Description of the **display snmp-agent trap feature-name info all** command output

Item	Description
Feature name	Name of the module to which a trap message belongs.
Trap number	Number of trap messages.

Item	Description
Trap name	Name of a trap message of the Information Center module: ● hwICLogFileAging: indicates that a log file aged and then was deleted. ● hwICLogBufferLose: indicates that some logs in the log buffer were lost because of storage space insufficiency.
Default switch status	Status of the default trap switch: ● on: indicates that the trap function is enabled. ● off: indicates that the trap function is disabled.
Current switch status	Status of the current trap switch: ● on: indicates that the trap function is enabled. ● off: indicates that the trap function is disabled.

Related Topics

3.3.40 snmp-agent trap enable feature-name info

3.3.13 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.

Parameter	Description	Value
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
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 3-48 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 **3.3.33 info-center trapbuffer** command.
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 **3.3.34 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 **3.3.14 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 **3.3.15 info-center channel name** command.
Dropped messages	Number of dropped messages.
Overwritten messages	Number of overwritten messages.

Item	Description
Current messages	Number of current messages.

Related Topics

3.3.5 display info-center

3.3.14 info-center channel

3.3.15 info-center channel name

3.3.16 info-center enable

3.3.33 info-center trapbuffer

3.3.34 info-center trapbuffer size

3.3.37 reset trapbuffer

3.3.14 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 3-49 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
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 **3.3.22 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
```

Related Topics

3.3.3 display channel

3.3.5 display info-center

3.3.15 info-center channel name

3.3.16 info-center enable

3.3.19 info-center logbuffer

3.3.22 info-center loghost

3.3.30 info-center source channel

3.3.33 info-center trapbuffer

3.3.15 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 3-50 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
```

Related Topics

3.3.3 display channel

3.3.5 display info-center

3.3.16 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 and logbuffer record logs, the other channel no longer records.

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.
```

Related Topics

3.3.5 display info-center

3.3.10 display logbuffer

3.3.13 display trapbuffer

3.3.14 info-center channel

3.3.15 info-center channel name

3.3.19 info-center logbuffer

3.3.30 info-center source channel

3.3.33 info-center trapbuffer

3.3.17 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.
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 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
```

Related Topics

3.3.16 info-center enable

3.3.6 display info-center filter-id

3.3.18 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 log file, console, or terminalconsole 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
```

3.3.19 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
```

Related Topics

3.3.5 display info-center

3.3.10 display logbuffer

3.3.14 info-center channel

3.3.15 info-center channel name

3.3.16 info-center enable

3.3.20 info-center logbuffer size

3.3.36 reset logbuffer

3.3.20 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
```

Related Topics

3.3.5 display info-center

3.3.10 display logbuffer

3.3.14 info-center channel

3.3.15 info-center channel name

3.3.16 info-center enable

3.3.19 info-center logbuffer

3.3.36 reset logbuffer

3.3.21 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
```

Related Topics

3.3.5 display info-center

3.3.11 display logfile

3.3.38 save logfile

3.3.22 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* | { **source-ip** *source-ip-address* } | **transport** { **udp** | **tcp ssl-policy** *policy-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* | **transport** { **udp** | **tcp ssl-policy** *policy-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* | **transport** { **udp** | **tcp ssl-policy** *policy-name* }] *

undo info-center loghost domain *domain-name* [**vpn-instance** *vpn-instance-name*]

NOTE

Only the S6720EI, S6720S-EI, S5720HI, S5720EI, S6720SI, S6720S-SI, S5730SI, S5730S-EI, S5720SI, S5720S-SI, S5720LI, S5720S-LI, S6720LI, S6720S-LI, S2720EI, S1720X-E, S1720GW-E, S1720GWR-E, S1720X, S1720GW, S1720GWR support the **vpn-instance** *vpn-instance-name* parameter.

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 the tool used by the log host to record information.	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.
vpn-instance *vpn-instance-name*	VPN instance.	The value must be an existing VPN instance name.
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
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.
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 TC 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 **huawei123** that has been created in the system.

```
<HUAWEI> system-view
[HUAWEI] ssl policy huawei123
[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
```

Related Topics

3.3.5 display info-center

3.3.14 info-center channel

3.3.15 info-center channel name

3.3.16 info-center enable

3.3.23 info-center loghost source

3.3.23 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
```

Related Topics

3.3.5 display info-center

3.3.14 info-center channel

3.3.15 info-center channel name

3.3.16 info-center enable

3.3.22 info-center loghost

3.3.24 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
```

3.3.25 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 200 log files can be saved.

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 manually or 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
```

Related Topics

3.3.5 display info-center

3.3.21 info-center logfile size

3.3.11 display logfile

3.3.38 save logfile

3.3.26 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.
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
```

Related Topics

3.3.8 display info-center rate-limit threshold

3.3.7 display info-center rate-limit record

3.3.27 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
```

Related Topics

3.3.8 display info-center rate-limit threshold

3.3.7 display info-center rate-limit record

3.3.28 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
```

Related Topics

3.3.8 display info-center rate-limit threshold

3.3.7 display info-center rate-limit record

3.3.29 info-center rate-limit threshold

3.3.29 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.

Parameter	Description	Value
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
```

Related Topics

3.3.8 display info-center rate-limit threshold

3.3.7 display info-center rate-limit record

3.3.30 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 3-51 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

Output Channel	Module Enabled to Output Information	Log		Trap		Debugging Message	
		Status	Lowest Output Severity	Status	Lowest Output Severity	Status	Lowest Output Severity
3 (trap buffer)	default	off	informational	on	debugging	off	debugging
4 (log buffer)	default	on	warning	off	debugging	off	debugging
5 (SNMP agent)	default	off	debugging	on	debugging	off	debugging
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.	-

Parameter	Description	Value
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.	-
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.	Logs are classified into eight severities. The following severities are listed in descending order of priority: ● emergencies ● alert ● critical ● error ● warning ● notification ● informational ● debugging

Parameter	Description	Value
debug { **state** { **off** | **on** } }	Specifies the debugging message status. - **off**: Debugging messages are not sent. - **on**: Debugging messages are sent.	-
debug { **level** *severity* }	Specifies the lowest severity of output debugging messages.	Logs 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 type 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 3-52 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.

Value	Severity	Description
1	alert	A fault needs to be rectified immediately. For example, memory usage of the system reaches the upper limit.
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 settings 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

# Configure the device to send logs higher than or equal to warning of the CFM module.

```
<HUAWEI> system-view
[HUAWEI] info-center source CFM channel snmpagent log level warning
```

Related Topics

3.3.3 display channel

3.3.5 display info-center

3.3.14 info-center channel

3.3.15 info-center channel name

3.3.16 info-center enable

3.3.19 info-center logbuffer

3.3.22 info-center loghost

3.3.33 info-center trapbuffer

3.3.41 terminal debugging

3.3.43 terminal logging

3.3.44 terminal monitor

3.3.45 terminal trapping

3.3.31 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
```

3.3.32 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.	-

Parameter	Description	Value
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.	-
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 3-53 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.

Field	Description	Value
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 **3.3.16 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
```

Related Topics

3.3.5 display info-center

3.3.33 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
```

Related Topics

3.3.5 display info-center

3.3.13 display trapbuffer

3.3.14 info-center channel

3.3.15 info-center channel name

3.3.16 info-center enable

3.3.34 info-center trapbuffer size

3.3.37 reset trapbuffer

3.3.34 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 **3.3.33 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
```

Related Topics

3.3.5 display info-center

3.3.13 display trapbuffer

3.3.14 info-center channel

3.3.15 info-center channel name

3.3.16 info-center enable

3.3.33 info-center trapbuffer

3.3.37 reset trapbuffer

3.3.35 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 recollect 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
```

Related Topics

3.3.5 display info-center

3.3.9 display info-center statistics

3.3.36 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
```

Related Topics

3.3.10 display logbuffer

3.3.37 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
```

Related Topics

3.3.13 display trapbuffer

3.3.38 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

0: Visit 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.
```

Related Topics

3.3.5 display info-center

3.3.21 info-center logfile size

3.3.11 display logfile

3.3.25 info-center max-logfile-number

3.3.39 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.
```

3.3.40 snmp-agent trap enable feature-name info

Function

snmp-agent trap enable feature-name info command enables the trap function of the Information Center module.

undo snmp-agent trap enable feature-name info command disables the trap function of the Information Center module.

By default, the trap function of the Information Center module is enabled.

Format

snmp-agent trap enable feature-name info [**trap-name** { **hwiclogbufferlose** | **hwiclogfileaging** }]

undo snmp-agent trap enable feature-name info [**trap-name** { **hwiclogbufferlose** | **hwiclogfileaging** }]

Parameters

Parameter	Description	Value
trap-name	Indicates the trap of a specified event type of the information center module. If the trap-name parameter is not specified, all the traps of the information center module are enabled.	-
hwiclogbufferlose	Enables or disables the trap generated when some logs in the log buffer were lost because of storage space insufficiency.	-
hwiclogfileaging	Enables or disables the trap generated when a log file aged and then was deleted.	-

Views

System view

Default Level

3: Management level

Usage Guidelines

After the trap function is enabled, the trap about the Information Center module generated when the device is running will be sent to the NMS. Otherwise, the trap about the Information Center module will not be sent to the NMS. If you want to enable a specific trap or several traps, choose the **trap-name** parameter.

Example

# Enables hwiclogfileaging for the Information Center module.

```
<HUAWEI> system-view
[HUAWEI] snmp-agent trap enable feature-name info trap-name hwiclogfileaging
```

Related Topics

3.3.12 display snmp-agent trap feature-name info all

3.3.41 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 **3.3.44 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.
```

Related Topics

3.3.16 info-center enable

3.3.30 info-center source channel

3.3.44 terminal monitor

3.3.42 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 **3.3.44 terminal monitor** command.
- The terminal has been enabled to display debugging, log, or trap information using the **3.3.41 terminal debugging**, **3.3.43 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]:
```

Related Topics

3.3.44 terminal monitor

3.3.41 terminal debugging

3.3.43 terminal logging

3.3.45 terminal trapping

3.3.43 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 **3.3.44 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.
```

Related Topics

3.3.16 info-center enable

3.3.30 info-center source channel

3.3.44 terminal monitor

3.3.44 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 **3.3.16 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.
```

Related Topics

3.3.16 info-center enable

3.3.30 info-center source channel

3.3.41 terminal debugging

3.3.43 terminal logging

3.3.45 terminal trapping

3.3.45 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 **3.3.44 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.
```

Related Topics

3.3.16 info-center enable

3.3.30 info-center source channel

3.3.44 terminal monitor

3.4 Fault Management Commands

3.4.1 Command Support

3.4.2 alarm (system view)

3.4.3 alarm-name severity

3.4.4 clear alarm active

3.4.5 clear alarm manual-clear

3.4.6 clear event all

3.4.7 clear record device-alarm

3.4.8 delay-suppression enable

3.4.9 display alarm active

3.4.10 display alarm history

3.4.11 display alarm information

3.4.12 display alarm manual-clear

3.4.13 display alarm urgent

3.4.14 display event

3.4.15 display event information

3.4.16 display snmp-agent trap feature-name fm all

3.4.17 event

3.4.18 mask manual-clear alarm

3.4.19 reset alarm urgent

3.4.20 set alarm resend interval

3.4.21 snmp-agent trap enable feature-name fm

3.4.22 suppression alarm-name

3.4.23 suppression event-name

3.4.1 Command Support

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

3.4.2 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]
```

Related Topics

3.4.3 alarm-name severity

3.4.4 clear alarm active

3.4.3 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 **3.4.11 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 **3.4.11 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
```

Related Topics

3.4.2 alarm (system view)

3.4.11 display alarm information

3.4.4 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
```

Related Topics

3.4.2 alarm (system view)

3.4.9 display alarm active

3.4.5 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 **3.4.12 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
```

Related Topics

3.4.4 clear alarm active

3.4.12 display alarm manual-clear

3.4.18 mask manual-clear alarm

3.4.6 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
```

Related Topics

3.4.17 event

3.4.7 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 the slot ID if stacking is not configured. • Specifies the stack ID if stacking is configured.	The value is 0 if stacking is not configured; the value ranges from 0 to 8 if stacking is configured.

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
```

Related Topics

3.4.13 display alarm urgent

3.4.8 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 S5720EI, S5720HI, S6720EI, and S6720S-EI 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
```

Related Topics

3.4.2 alarm (system view)

3.4.17 event

3.4.22 suppression alarm-name

3.4.23 suppression event-name

3.4.9 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)

  1/Independent/2015-09-01 09:18:25-05:13/-/0x40c12004/hwEntityInvalid/Critical/
Start/OID 1.3.6.1.4.1.2011.5.25.129.2.1.9 Power is abnormal. (EntityPhysicalInde
x=67108873, BaseTrapSeverity=3, BaseTrapProbableCause=67966, BaseTrapEventType=5
, EntPhysicalContainedIn=5, EntPhysicalName=MPU Board 0, RelativeResource=PWR2 P
OWER, ReasonDescription=PWR2 POWER is abnormal)
```

Table 3-54 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.
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 **3.4.3 alarm-name severity** command to set this parameter.
H=State	Alarm status: ● Start ● End

Item	Description
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)

Related Topics

3.4.2 alarm (system view)

3.4.3 alarm-name severity

3.4.4 clear alarm active

3.4.10 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 1024 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 3-55 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 **3.4.3 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

Item	Description
J=RootCause alarm sequence(Only for nonRootCause alarm)	Sequence number of the root-cause alarm

Related Topics

3.4.2 alarm (system view)

3.4.9 display alarm active

3.4.3 alarm-name severity

3.4.11 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 3-56 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 **3.4.3 alarm-name severity** command.
Suppress Period	Alarm reporting delay. To set this parameter, run the **3.4.22 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.

Related Topics

3.4.2 alarm (system view)

3.4.3 alarm-name severity

3.4.12 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 3-57 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 **3.4.3 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)

Related Topics

3.4.4 clear alarm active

3.4.5 clear alarm manual-clear

3.4.18 mask manual-clear alarm

3.4.13 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 the slot ID if stacking is not configured. ● Specifies the stack ID if stacking is configured.	The value is 0 if stacking is not configured; the value ranges from 0 to 8 if stacking is configured.
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
------------------------------------------------------------------------
Power abnormal          1        2015/10/16  18:22:17      Slot 1
PWR Input Vol Low        1        2015/10/16  18:22:17      Slot 1
PWR2
Power abnormal          1        2015/10/16  18:19:11      Slot 1
PWR Input Vol Low        1        2015/10/16  18:19:11      Slot 1
PWR2
Power abnormal          1        2015/10/16  18:10:29      Slot 1
PWR Input Vol Low        1        2015/10/16  18:10:29      Slot 1
PWR2
Power abnormal          1        2015/10/16  09:35:05      Slot 1
PWR Input Vol Low        1        2015/10/16  09:35:05      Slot 1
```

```
PWR2
Power abnormal          8         2015/10/16  10:19:18      Slot 8
PWR Input Vol Low        8         2015/10/16  10:19:18      Slot 8
PWR2
Power abnormal          8         2015/10/16  10:04:48      Slot 8
PWR Input Vol Low        8         2015/10/16  10:04:48      Slot 8
PWR2
Power abnormal          8         2015/10/16  10:01:45      Slot 8
PWR Input Vol Low        8         2015/10/16  10:01:45      Slot 8
PWR2
Power abnormal          8         2015/10/16  09:58:53      Slot 8
PWR Input Vol Low        8         2015/10/16  09:58:53      Slot 8
PWR2
Power abnormal          8         2015/10/16  09:56:00      Slot 8
PWR Input Vol Low        8         2015/10/16  09:56:00      Slot 8
PWR2
Power abnormal          1         2015/10/16  09:41:40      Slot 1
PWR Input Vol Low        1         2015/10/16  09:41:40      Slot 1 PWR2
```

Table 3-58 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. ● Bat temperature low: The lithium battery temperature is too low. ● Bat temperature normal: The lithium battery temperature returns to the normal range. ● Bat temperature high: The lithium battery temperature is too high. ● Bat temperature normal: The lithium battery temperature returns to the normal range. ● Bat invalid: A lithium battery is unavailable. ● Battery's life end: The lifetime of a lithium battery has expired. ● Bat supplytime short: The power supply time of a lithium battery is less than the threshold.

Item	Description
	- Bat supptime short clear: The power supply time of a lithium battery is longer than the threshold. - Bat Voltage Low: A lithium battery is in an undervoltage condition. - Bat Voltage Low resume: A lithium battery recovers from an undervoltage condition. - Bat Current high: A lithium battery is in an overcurrent condition.
Slot	Stack 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.

Related Topics

3.4.7 clear record device-alarm

3.4.14 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 3-59 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
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.

Item	Description
J=RootCause alarm sequence(Only for nonRootCause alarm)	This parameter is valid only for alarms.

Related Topics

3.4.6 clear event all

3.4.15 display event information

3.4.17 event

3.4.15 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 3-60 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 **3.4.23 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.

3.4.16 display snmp-agent trap feature-name fm all

Function

The **display snmp-agent trap feature-name fm all** command displays the status of all traps of the fault management module.

Format

display snmp-agent trap feature-name fm all

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

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

The **display snmp-agent trap feature-name fm all** command displays whether all trap functions of the FM module are enabled.

Example

# Display all trap messages of the fault management module.

```
<HUAWEI>display snmp-agent trap feature-name fm all
------------------------------------------------------------------------------
Feature name: FM
Trap number : 2
------------------------------------------------------------------------------
Trap name                    Default switch status   Current switch status
hwAlarmTargetHostDel              on                      on
hwAlarmStorm                      on                      on
```

Table 3-61 Description of the **display snmp-agent trap feature-name fm all** command output

Item	Description
Feature name	Name of the module to which a trap message belongs
Trap number	Number of trap messages
Trap name	Names of the trap messages of the fault management module, including: ● **hwAlarmTargetHostDel**: generated when the configuration of a target host is deleted ● **hwAlarmStorm**: generated when an alarm storm occurs
Default switch status	Default status of the trap function: ● on: the trap function is enabled. ● off: the trap function is disabled.
Current switch status	Current status of the trap function: ● on: the trap function is enabled. ● off: the trap function is disabled.

Related Topics

3.4.21 snmp-agent trap enable feature-name fm

3.4.17 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]
```

Related Topics

3.4.14 display event

3.4.15 display event information

3.4.18 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 setting.

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
```

Related Topics

3.4.4 clear alarm active

3.4.12 display alarm manual-clear

3.4.5 clear alarm manual-clear

3.4.19 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 the slot ID if stacking is not configured. - Specifies the stack ID if stacking is configured.	The value is an integer that is 0 if stacking is not configured. The value ranges from 0 to 8 if stacking is configured.

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
```

3.4.20 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
```

3.4.21 snmp-agent trap enable feature-name fm

Function

The **snmp-agent trap enable feature-name fm** command enables the trap function of the fault management module.

The **undo snmp-agent trap enable feature-name fm** command disables the trap function of the fault management module.

By default, the trap function is enabled for the fault management module.

Format

snmp-agent trap enable feature-name fm [**trap-name** { **hwalarmtargethostdel** | **hwalarmstorm** }]

undo snmp-agent trap enable feature-name fm [**trap-name** { **hwalarmtargethostdel** | **hwalarmstorm** }]

Parameters

Parameter	Description	Value
trap-name	Enables the trap of a specified event. If this parameter is not specified, all traps of the fault management module are enabled.	-
hwalarmtargethostdel	Indicates that the configuration of a target host is deleted.	-
hwalarmstorm	Indicates that a trap alarm occurs.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

The traps of the fault management module generated in the running process of a device are reported to the NMS only when the trap function is enabled. To enable the trap function for one or more specific events, configure **trap-name** in the command.

Example

# Enable all traps of the fault management module.

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

3.4.22 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 S5720EI, S5720HI, S6720EI, and S6720S-EI 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
```

Related Topics

3.4.2 alarm (system view)

3.4.8 delay-suppression enable

3.4.23 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 S5720EI, S5720HI, S6720EI, and S6720S-EI 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
```

Related Topics

3.4.17 event

3.4.8 delay-suppression enable

3.5 NTP Configuration Commands

3.5.1 Command Support
3.5.2 display ntp-service event clock-unsync
3.5.3 display ntp-service sessions
3.5.4 display ntp-service statistics packet
3.5.5 display ntp-service status
3.5.6 display ntp-service trace
3.5.7 ntp-service
3.5.8 ntp-service access
3.5.9 ntp-service authentication enable
3.5.10 ntp-service authentication-keyid
3.5.11 ntp-service broadcast-client
3.5.12 ntp-service broadcast-server
3.5.13 ntp-service disable
3.5.14 ntp-service discard
3.5.15 ntp-service in-interface disable
3.5.16 ntp-service kod-enable
3.5.17 ntp-service manycast-client
3.5.18 ntp-service manycast-server
3.5.19 ntp-service max-distance
3.5.20 ntp-service max-dynamic-sessions
3.5.21 ntp-service multicast-client
3.5.22 ntp-service multicast-server
3.5.23 ntp-service port
3.5.24 ntp-service refclock-master
3.5.25 ntp-service reliable authentication-keyid
3.5.26 ntp-service server disable
3.5.27 ntp-service source-interface
3.5.28 ntp-service unicast-peer
3.5.29 ntp-service unicast-server
3.5.30 reset ntp-service statistics packet

3.5.1 Command Support

Only the S6720EI, S6720S-EI, S5720HI, S5720EI, S6720SI, S6720S-SI, S5730SI, S5730S-EI, S5720SI, S5720S-SI, S5720LI, S5720S-LI, S6720LI, S6720S-LI, S2720EI, S1720X-E, S1720GW-E, S1720GWR-E, S1720X, S1720GW, S1720GWR support the **vpn-instance** *vpn-instance-name* parameter.

3.5.2 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 3-62 Description of the **display ntp-service event clock-unsync** command output

Item	Description
Clock source	Indicates the IP address of the server clock.
Session type	Indicates the session type of the server clock.
Unsync reason	Indicates the unsynchronous reasons.
Unsync time	Indicates the unsynchronous time.

3.5.3 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 3-63 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 3-64 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.

Related Topics

3.5.28 ntp-service unicast-peer

3.5.29 ntp-service unicast-server

3.5.11 ntp-service broadcast-client

3.5.12 ntp-service broadcast-server

3.5.21 ntp-service multicast-client

3.5.22 ntp-service multicast-server

3.5.4 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.	-

Parameter	Description	Value
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 3-65 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.
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.

3.5.5 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 3-66 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 clock stratum indicates higher clock precision. When the client gets synchronized to a session, it is stratum becomes session stratum + 1.

Item	Description
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.
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.

3.5.6 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 3-67 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.

3.5.7 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 128ms, 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 S5720EI, S5720HI, S6720EI, and S6720S-EI 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

# Sets the maximum interval to 200 seconds for clock synchronization.

```
<HUAWEI> system-view
[HUAWEI] ntp-service sync-interval 200
```

3.5.8 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 3-68 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
```

Related Topics

3.5.9 ntp-service authentication enable

3.5.9 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
```

Related Topics

3.5.10 ntp-service authentication-keyid

3.5.25 ntp-service reliable authentication-keyid

3.5.10 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.	-

Parameter	Description	Value
cipher	Indicates that the configured password is displayed in cipher text.	-
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 6. 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
```

Related Topics

3.5.9 ntp-service authentication enable

3.5.25 ntp-service reliable authentication-keyid

3.5.11 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
```

Related Topics

3.5.12 ntp-service broadcast-server

3.5.12 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*] *

undo ntp-service broadcast-server [**version** *number* | **authentication-keyid** *key-id* | **port** *port-number*] *

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 number of the port that transmits NTP broadcast packets.	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

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.

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
```

Related Topics

3.5.11 ntp-service broadcast-client

3.5.13 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
```

3.5.14 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
```

3.5.15 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
```

3.5.16 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
```

3.5.17 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.
port *port-number*	Specifies the number of the port that transmits NTP manycast packets.	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
```

Related Topics

3.5.22 ntp-service multicast-server

3.5.18 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.

Parameter	Description	Value
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
```

Related Topics

3.5.17 ntp-service manycast-client

3.5.19 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
```

3.5.20 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, up to 100 NTP dynamic sessions are allowed to be set up.

Format

ntp-service max-dynamic-sessions *number*

undo ntp-service max-dynamic-sessions

Parameters

Parameter	Description	Value
number	Indicates the number of dynamic sessions allowed to be set up.	The number of dynamic NTP sessions is an integer that ranges from 0 to 100.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 NTP dynamic sessions allowed to be set up to 50.

```
<HUAWEI> system-view
[HUAWEI] ntp-service max-dynamic-sessions 50
```

3.5.21 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
```

Related Topics

3.5.22 ntp-service multicast-server

3.5.3 display ntp-service sessions

3.5.22 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 NIP 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 number of port that transmits NTP multicast packets.	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
```

Related Topics

3.5.21 ntp-service multicast-client

3.5.3 display ntp-service sessions

3.5.23 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
```

3.5.24 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
```

3.5.25 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
```

Related Topics

3.5.9 ntp-service authentication enable

3.5.10 ntp-service authentication-keyid

3.5.26 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
```

3.5.27 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 the route.

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 the NTP packets.	-
vpn-instance *vpn-instance-name*	Indicates the name of the 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/receiving NTP packets, so that the another interface on the device cannot receive the NTP response packets, which is convenient for a user to subsequently deploy a flow control policy. If the interface is not specified, the source IP address of the NTP packets is selected according to the route.

If you have specified **vpn-instance** when configuring a source IP address with this command, the source IP address can be used only by the NTP server mapping the specified VPN instance instead of other VPN instances or NTP servers that do not have VPN instances specified.

Precautions

For broadcast, multicast, and manycast modes, NTP service is implemented on the specified interface, and this interface is the source interface. Therefore, the **ntp-service source-interface** command is invalid for broadcast, multicast, and manycast modes.

Example

# Specify VLANIF100 as the source interface to send all the NTP packets.

```
<HUAWEI> system-view
[HUAWEI] ntp-service source-interface vlanif 100
```

3.5.28 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. The default value 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.
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.

Parameter	Description	Value
preference	Indicates the remote peer as the preferred one. By default, the remote peer is not preferred.	-
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 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
```

3.5.29 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.

Parameter	Description	Value
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 an 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.
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.	-
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
```

3.5.30 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
```

3.6 Energy-saving Configuration Commands

3.6.1 Command Support

3.6.2 als enable

3.6.3 als restart

3.6.4 als restart mode manual

3.6.5 als restart pulse-interval

3.6.6 als restart pulse-width

3.6.7 display als configuration

3.6.8 display power manage cycle

3.6.9 display power manage mode

3.6.10 display power manage power-information

3.6.11 display power manage sleep configuration

3.6.12 display snmp-agent trap feature-name spmtrap all

3.6.13 energy-efficient-ethernet enable

3.6.14 port-auto-sleep enable

3.6.15 set power manage awaken-mode fast

3.6.16 set power manage cycle

3.6.17 set power manage interval

3.6.18 set power manage mode

3.6.19 set power manage non-awaken-port

3.6.20 sleep time-range

3.6.21 snmp-agent trap enable feature-name spmtrap

3.6.1 Command Support

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

3.6.2 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

GE interface view, XGE interface view, 40GE 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 do not support ALS.
- When optical interfaces transmit services unidirectionally, they do not support ALS.
- When the copper cable or copper module is used on the optical port, the ALS function is not supported. In addition, after the copper cable is inserted, all the ALS-related commands configured on this interface are cleared.

Example

# Enable ALS on GigabitEthernet0/0/1.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] als enable
```

Related Topics

3.6.7 display als configuration

3.6.3 als restart

Function

The **als restart** command manually restarts the laser of an interface.

Format

als restart

Parameters

None

Views

GE interface view, XGE interface view, 40GE 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 **3.6.2 als enable** command and the restart mode of the laser has been set to manual restart mode using the **3.6.4 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
```

Related Topics

3.6.2 als enable

3.6.4 als restart mode manual

3.6.4 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

GE interface view, XGE interface view, 40GE 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 **3.6.5 als restart pulse-interval** command to detect whether the link is recovered. The pulse width is set through the **3.6.6 als restart pulse-width** command.
- In manual restart mode, you must manually start the laser using the **3.6.3 als restart** command so that the laser can send a pulse. The ALS pulse width is set using the **3.6.6 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
```

Related Topics

3.6.2 als enable

3.6.3 als restart

3.6.5 als restart pulse-interval

3.6.6 als restart pulse-width

3.6.7 display als configuration

3.6.5 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

GE interface view, XGE interface view, 40GE 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
```

Related Topics

3.6.2 als enable

3.6.7 display als configuration

3.6.6 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

GE interface view, XGE interface view, 40GE 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
```

Related Topics

3.6.2 als enable

3.6.7 display als configuration

3.6.7 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*	Specifies the slot ID if stacking is not configured. Specifies the stack ID if stacking is configured.	The value is 0 if stacking is not configured; the value ranges from 0 to 8 if stacking is configured.
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 3-69 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 **3.6.2 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 **3.6.4 als restart mode manual** command.
Interval(s)	ALS pulse interval, expressed in seconds. The ALS pulse interval is set using the **3.6.5 als restart pulse-interval** command.
Width(s)	ALS pulse width, expressed in seconds. The ALS pulse width is set using the **3.6.6 als restart pulse-width** command.

Related Topics

3.6.2 als enable

3.6.4 als restart mode manual

3.6.5 als restart pulse-interval

3.6.6 als restart pulse-width

3.6.8 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 3-70 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 **3.6.16 set power manage cycle** command.

Related Topics

3.6.16 set power manage cycle

3.6.9 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 3-71 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 **3.6.18 set power manage mode** command.

Related Topics

3.6.18 set power manage mode

3.6.10 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) : 1000
 The average power consumption (mW)  : 20000
 The current power consumption (mW)  : 20000
 The rated power (mW)                : 433000
 The threshold of power (mW)         : 433000
 --------------------------------------------------
```

Table 3-72 Description of the display power manage power-information command output

Item	Description
The information of net element power	System power consumption information.
The total power consumption (Joule)	Accumulative power consumption, in Joule. This field displays NA when the device type is S1720GFR, S1720GW, S1720GWR, S1720X, S1720GW-E, S1720GWR-E, S1720X-E, S2720EI, S2750EI, S5700LI, S5700S-LI, S5720LI, S5720S-LI, S5710-X-LI, S5720S-SI and S5720SI. **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)	Average power of the system, in mW. This field displays NA when the device type is S1720GFR, S1720GW, S1720GWR, S1720X, S1720GW-E, S1720GWR-E, S1720X-E, S2720EI, S2750EI, S5700LI, S5700S-LI, S5720LI, S5720S-LI, S5710-X-LI, S5720S-SI and S5720SI.

Item	Description
The current power consumption (mW)	Real-time power of the system, in mW. This field displays NA when the device type is S1720GFR, S1720GW, S1720GWR, S1720X, S1720GW-E, S1720GWR-E, S1720X-E, S2720EI, S2750EI, S5700LI, S5700S-LI, S5720LI, S5720S-LI, S5710-X-LI, S5720S-SI and S5720SI.
The rated power (mW)	Rated power of the system, in mW.
The threshold of power (mW)	Power threshold of the power supply unit, in mW. The value is the rated power supplied to the device by power supply units. 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.

3.6.11 display power manage sleep configuration

Function

The **display power manage sleep configuration** command displays device dormancy information.

NOTE

The following product models support the sleep mode:

- S5710-X-LI
- S5700S-LI: S5700S-28P-LI-AC, S5700S-52P-LI-AC, S5700S-28X-LI-AC, and S5700S-52X-LI-AC
- S5700LI: S5700-28P-LI-AC, S5700-28TP-LI-AC, S5700-28P-LI-DC, S5700-52P-LI-AC, S5700-52P-LI-DC, S5700-28X-LI-AC, S5700-28X-LI-DC, S5700-52X-LI-AC, S5700-52X-LI-DC, and S5701-28X-LI-AC
- S5720SI: S5720-28P-SI-AC, S5720-28X-SI-AC, S5720-28X-SI-DC, S5720-52P-SI-AC, S5720-52X-SI-DC, and S5720-52X-SI-AC
- S5720S-SI: S5720S-28P-SI-AC, S5720S-28X-SI-AC, S5720S-28X-SI-DC, S5720S-52P-SI-AC, S5720S-52X-SI-DC, and S5720S-52X-SI-AC

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 awaken mode: normal
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 3-73 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.

Item	Description
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 awaken mode	Configured awakening mode. - normal: Traffic forwarding does not resume quickly after the device exits the device dormancy mode. - fast: Traffic forwarding resumes quickly after the device exits the device dormancy mode. To enable the fast awakening mode, run the **set power manage awaken-mode fast** 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.

Related Topics

3.6.17 set power manage interval

3.6.15 set power manage awaken-mode fast

3.6.19 set power manage non-awaken-port

3.6.12 display snmp-agent trap feature-name spmtrap all

Function

display snmp-agent trap feature-name spmtrap all command displays the status of all traps on the SPMTRAP module.

NOTE

The following product models support the sleep mode:

- S5710-X-LI
- S5700S-LI: S5700S-28P-LI-AC, S5700S-52P-LI-AC, S5700S-28X-LI-AC, and S5700S-52X-LI-AC
- S5700LI: S5700-28P-LI-AC, S5700-28TP-LI-AC, S5700-28P-LI-DC, S5700-52P-LI-AC, S5700-52P-LI-DC, S5700-28X-LI-AC, S5700-28X-LI-DC, S5700-52X-LI-AC, S5700-52X-LI-DC, and S5701-28X-LI-AC
- S5720SI: S5720-28P-SI-AC, S5720-28X-SI-AC, S5720-28X-SI-DC, S5720-52P-SI-AC, S5720-52X-SI-DC, and S5720-52X-SI-AC
- S5720S-SI: S5720S-28P-SI-AC, S5720S-28X-SI-AC, S5720S-28X-SI-DC, S5720S-52P-SI-AC, S5720S-52X-SI-DC, and S5720S-52X-SI-AC

Format

display snmp-agent trap feature-name spmtrap all

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

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

Prerequisites

SNMP has been enabled. For details, see **snmp-agent**.

Example

# Display all the traps of the SPMTRAP module.

```
<HUAWEI>display snmp-agent trap feature-name spmtrap all
------------------------------------------------------------------------------
Feature name: SPMTRAP
Trap number : 1
------------------------------------------------------------------------------
Trap name                   Default switch status   Current switch status
hwEnergyDevChangeToSleep        on                      on
```

Table 3-74 Description of the display snmp-agent trap feature-name spmtrap all command output

Item	Specification
Feature name	Name of the module that the trap belongs to.
Trap number	Number of traps.
Trap name	Trap name. Traps of the SPMTRAP module include: ● hwEnergyDevChangeToSleep: The device enters the sleeping mode.
Default switch status	Default status of the trap function: ● on: indicates that the trap function is enabled by default. ● off: indicates that the trap function is disabled by default.
Current switch status	Status of the trap function: ● on: indicates that the trap function is enabled. ● off: indicates that the trap function is disabled.

Related Topics

3.6.21 snmp-agent trap enable feature-name spmtrap

3.6.13 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. S2750EI does 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 S6720EI and S6720S-EI 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.

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
```

Related Topics

4.2.4 auto speed

4.2.38 negotiation auto

3.6.14 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

GE interface view, port group view, Ethernet interface 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

This command can be used on electrical interfaces and combo interfaces working as electrical interfaces.

The port sleeping function is enabled by default on the 2*10GE electrical sub-card supported by the S5720EI 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
```

3.6.15 set power manage awaken-mode fast

Function

The **set power manage awaken-mode fast** command enables the fast awaking mode to allow the device to restore Layer 2 traffic quickly after exiting the device sleeping mode.

The **undo set power manage awaken-mode fast** command disables the fast awaking mode.

By default, a device cannot restore services quickly after exiting the device sleeping mode.

NOTE

Only S5700S-28P-LI-AC and S5700S-52P-LI-AC in the S5700S-LI series and S5700-28P-LI-AC, S5700-28P-LI-DC, S5700-52P-LI-AC, S5700-52P-LI-DC in the S5700LI series support this command.

Format

set power manage awaken-mode fast

undo set power manage awaken-mode fast

Parameters

None

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

A device can wake from the deep sleeping state in any of the following conditions:

- A user logs in to the device through the serial port and presses **Ctrl+W**.
- A user logs in from the awakening port.
- The sleeping time range expires (if a time range is configured).
- A user clicks the mode switching button.

The awaking process takes a relatively long time, and services cannot be restored quickly. To shorten the awaking time, you can use the **set power manage awaken-mode** command to enable the fast awaking mode. This mode enables a device to restore fast Layer 2 traffic after exiting the device sleeping mode.

Precautions

Before using the **set power manage awaken-mode** command, run the **stp disable** command in the system view to disable STP globally and run the **save** command to save the configuration. Loops may occur when STP is disabled; therefore, monitor the network status to check for loops when using the fast awaking function.

In a stack, the **set power manage awaken-mode fast** command cannot enable a device to fast restore Layer 2 traffic after exiting the device sleeping mode. However, you can use the **undo set power manage awaken-mode fast** command to delete the configuration in standalone mode.

Example

# Enable the fast awaking mode.

```
<HUAWEI> system-view
[HUAWEI] set power manage awaken-mode fast
Warning: This command will take effect only after disable stp and saving the c
onfiguration. Some service would be affected with this awaken mode after the dev
ice restored from sleep. Continue?[Y/N]:y
Info: Succeeded in setting the configuration.
```

3.6.16 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
```

Related Topics

3.6.8 display power manage cycle

3.6.17 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

The following product models support the sleep mode:

- S5710-X-LI
- S5700S-LI: S5700S-28P-LI-AC, S5700S-52P-LI-AC, S5700S-28X-LI-AC, and S5700S-52X-LI-AC
- S5700LI: S5700-28P-LI-AC, S5700-28TP-LI-AC, S5700-28P-LI-DC, S5700-52P-LI-AC, S5700-52P-LI-DC, S5700-28X-LI-AC, S5700-28X-LI-DC, S5700-52X-LI-AC, S5700-52X-LI-DC, and S5701-28X-LI-AC
- S5720SI: S5720-28P-SI-AC, S5720-28X-SI-AC, S5720-28X-SI-DC, S5720-52P-SI-AC, S5720-52X-SI-DC, and S5720-52X-SI-AC
- S5720S-SI: S5720S-28P-SI-AC, S5720S-28X-SI-AC, S5720S-28X-SI-DC, S5720S-52P-SI-AC, S5720S-52X-SI-DC, and S5720S-52X-SI-AC

Format

set power manage interval *interval-time*

undo set power manage interval

Parameters

Parameter	Description	Value
interval *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.

NOTICE

A device enters the dormancy state when the conditions for device dormancy are met. On the S5700S-28P-LI-AC and S5700S-52P-LI-AC in the S5700S-LI series and S5700-28P-LI-AC, S5700-28P-LI-DC, S5700-52P-LI-AC, S5700-52P-LI-DC in the S5700LI series, save the configuration immediately after you run this command.

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
```

Related Topics

3.6.11 display power manage sleep configuration

3.6.18 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 2*10GE electrical sub-card supported by the S5720EI 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.

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.

NOTE

- 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.
- 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.

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...
```

# Set the energy-saving mode of the device to deep mode.

```
<HUAWEI> system-view
[HUAWEI] set power manage mode 4
Warning: Performance of ALS, EEE, Auto sleep will be enabled, and the EEE function may lead to port
flapping. Continue?[Y/N]:y
Warning: This command will enable the device sleep function. The device will enter in sleep mode under
the conditon specified, and all of service will not be provided. Continue? [Y/N]:y
Info: It will take a few seconds. Please wait...
Info: Succeeded in setting the configuration.
Info: The system is now comparing the configuration, please wait.
Warning: The configuration has been modified, and it will be saved to the next startup saved-configuration
file flash:/s249.cfg. Continue? [Y/N]:y
Now saving the current configuration to the slot 0....
Save the configuration successfully.
```

# Set the energy-saving mode of the device to standby mode.

```
<HUAWEI> system-view
[HUAWEI] set power manage mode 5
Warning: When the device enters the standby mode, some ports will enter the power down mode and
become unavailable. Installing the optical module to a switch in standby mode will cause the switch to
restart. Continue?[Y/N]:y
Info: It will take a few seconds. Please wait...
```

Related Topics

3.6.9 display power manage mode

3.6.19 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

The following product models support the sleep mode:

- S5710-X-LI
- S5700S-LI: S5700S-28P-LI-AC, S5700S-52P-LI-AC, S5700S-28X-LI-AC, and S5700S-52X-LI-AC
- S5700LI: S5700-28P-LI-AC, S5700-28TP-LI-AC, S5700-28P-LI-DC, S5700-52P-LI-AC, S5700-52P-LI-DC, S5700-28X-LI-AC, S5700-28X-LI-DC, S5700-52X-LI-AC, S5700-52X-LI-DC, and S5701-28X-LI-AC
- S5720SI: S5720-28P-SI-AC, S5720-28X-SI-AC, S5720-28X-SI-DC, S5720-52P-SI-AC, S5720-52X-SI-DC, and S5720-52X-SI-AC
- S5720S-SI: S5720S-28P-SI-AC, S5720S-28X-SI-AC, S5720S-28X-SI-DC, S5720S-52P-SI-AC, S5720S-52X-SI-DC, and S5720S-52X-SI-AC

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.

NOTICE

A device enters the dormancy state when the conditions for device dormancy are met. On the S5700S-28P-LI-AC and S5700S-52P-LI-AC in the S5700S-LI series and S5700-28P-LI-AC, S5700-28P-LI-DC, S5700-52P-LI-AC, S5700-52P-LI-DC in the S5700LI series, save the configuration immediately after you run this command.

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
```

Related Topics

3.6.11 display power manage sleep configuration

3.6.20 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

The following product models support the sleep mode:

- S5710-X-LI
- S5700S-LI: S5700S-28P-LI-AC, S5700S-52P-LI-AC, S5700S-28X-LI-AC, and S5700S-52X-LI-AC
- S5700LI: S5700-28P-LI-AC, S5700-28TP-LI-AC, S5700-28P-LI-DC, S5700-52P-LI-AC, S5700-52P-LI-DC, S5700-28X-LI-AC, S5700-28X-LI-DC, S5700-52X-LI-AC, S5700-52X-LI-DC, and S5701-28X-LI-AC
- S5720SI: S5720-28P-SI-AC, S5720-28X-SI-AC, S5720-28X-SI-DC, S5720-52P-SI-AC, S5720-52X-SI-DC, and S5720-52X-SI-AC
- S5720S-SI: S5720S-28P-SI-AC, S5720S-28X-SI-AC, S5720S-28X-SI-DC, S5720S-52P-SI-AC, S5720S-52X-SI-DC, and S5720S-52X-SI-AC

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 **3.6.18 set power manage mode** command.
- A time range has been specified using the **14.1.26 time-range** command.

NOTICE

A device enters the dormancy state when the conditions for device dormancy are met. On the S5700S-28P-LI-AC and S5700S-52P-LI-AC in the S5700S-LI series and S5700-28P-LI-AC, S5700-28P-LI-DC, S5700-52P-LI-AC, S5700-52P-LI-DC in the S5700LI series, save the configuration immediately after you run this 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
```

Related Topics

3.6.18 set power manage mode

14.1.26 time-range

3.6.21 snmp-agent trap enable feature-name spmtrap

Function

snmp-agent trap enable feature-name spmtrap command enables the trap function for the SPMTRAP module.

undo snmp-agent trap enable feature-name spmtrap command disables the trap function for the SPMTRAP module.

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

NOTE

The following product models support the sleep mode:

- S5710-X-LI
- S5700S-LI: S5700S-28P-LI-AC, S5700S-52P-LI-AC, S5700S-28X-LI-AC, and S5700S-52X-LI-AC
- S5700LI: S5700-28P-LI-AC, S5700-28TP-LI-AC, S5700-28P-LI-DC, S5700-52P-LI-AC, S5700-52P-LI-DC, S5700-28X-LI-AC, S5700-28X-LI-DC, S5700-52X-LI-AC, S5700-52X-LI-DC, and S5701-28X-LI-AC
- S5720SI: S5720-28P-SI-AC, S5720-28X-SI-AC, S5720-28X-SI-DC, S5720-52P-SI-AC, S5720-52X-SI-DC, and S5720-52X-SI-AC
- S5720S-SI: S5720S-28P-SI-AC, S5720S-28X-SI-AC, S5720S-28X-SI-DC, S5720S-52P-SI-AC, S5720S-52X-SI-DC, and S5720S-52X-SI-AC

Format

snmp-agent trap enable feature-name spmtrap [**trap-name hwenergydevchangetosleep**]

undo snmp-agent trap enable feature-name spmtrap [**trap-name hwenergydevchangetosleep**]

Parameters

Parameter	Description	Value
trap-name	Enables or disables the trap function for the specified event.	-
hwenergydevchangeto-sleep	Enables the trap function when the device enters the sleeping mode.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

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

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

Example

# Enable the hwenergydevchangetosleep trap of the SPMTRAP module.

```
<HUAWEI> system-view
[HUAWEI] snmp-agent trap enable feature-name spmtrap trap-name hwenergydevchangetosleep
```

Related Topics

3.6.12 display snmp-agent trap feature-name spmtrap all

3.7 PoE Configuration Commands

3.7.1 Command Support

3.7.2 display poe device

3.7.3 display poe information

3.7.4 display poe power

3.7.5 display poe power-state

3.7.6 display poe-power

3.7.7 display snmp-agent trap feature-name poetrap all

3.7.8 poe af-inrush enable

3.7.9 poe { at-inrush | pre-bt-inrush | bt-inrush } enable

3.7.10 poe enable

3.7.11 poe fast-on enable

3.7.12 poe force-power

3.7.13 poe group management enable

3.7.14 poe high-inrush enable

3.7.15 poe { power-off | power-on } interface

3.7.16 poe legacy enable

3.7.17 poe max-power

3.7.18 poe power

3.7.19 poe power-management

3.7.20 poe power-off time-range

3.7.21 poe power-on delay

3.7.22 poe power-policy port-index-priority disable

3.7.23 poe power-reserved

3.7.24 poe power-threshold

3.7.25 poe priority

3.7.26 poe single-class enable

3.7.27 rps cold-backup

3.7.28 snmp-agent trap enable feature-name poetrap

3.7.1 Command Support

Only electrical interfaces of switch models with PWR or PWH in the device names support the PoE function.

3.7.2 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 3-75 Description of the display poe device command output

Item	Description
Slot 0	The device supports PoE.

3.7.3 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 state information about a specified stack device. If this parameter is not specified, the PoE information about all device is displayed.	The value is 0 if stacking is not configured; the value ranges from 0 to 8 if stacking is configured.

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.

```
<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
    Port Index Priority         : enable
```

Table 3-76 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 **3.7.17 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.
PoE Power Supply(mW)	PoE power supply, which is determined by the PoE power module configured on the device.
Available Total Power(mW)	Total 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 **3.7.19 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 **3.7.14 poe high-inrush enable** command.
Port Index Priority	Whether the device is enabled to power on or off PDs connected to interfaces based on the interface numbers. By default, a device powers on or off PDs connected to interfaces based on the interface numbers. To configure this parameter, run the **poe power-policy port-index-priority disable** command.

Related Topics

3.7.17 poe max-power

3.7.19 poe power-management

3.7.14 poe high-inrush enable

3.7.4 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 about a specified stack device. 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 is an integer, and the value ranges from 0 to 8 if stacking is configured. The value is 0 if stacking is not configured.
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 S5730SI, S5730S-EI, S5720-16X-PWH-LI-AC, S5720-28X-PWH-LI-AC, and S6720SI. 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 3-77 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. The mapping between PD classes and the reference power is as follows: ● 0: reference power 15.4 W ● 1: reference power 4 W ● 2: reference power 7 W ● 3: reference power 15.4 W ● 4: reference power 30 W
USMPW(mW)	Maximum output power set for an interface. To set the value, run the **3.7.18 poe power** command.
CURPW(mW)	Current power of the PDs on an interface.
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 3-78 Description of the display poe power interface command output

Item	Description
PD power(mW)	Output power of an interface.

Item	Description
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. The mapping between PD classes and the reference power is as follows: ● 0: reference power 15.4 W ● 1: reference power 4 W ● 2: reference power 7 W ● 3: reference power 15.4 W ● 4: reference power 30 W
user set max power(mW)	Maximum output power set for an interface. To set the value, run the **3.7.18 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.

Related Topics

3.7.2 display poe device

3.7.18 poe power

3.7.10 poe enable

3.7.5 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 stack device. 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 ranges from 0 to 8 if stacking is configured. The value is 0 if stacking is not configured.
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     : disable
Single-class state      : disable
Power-up mode           : at
Power-on delay(s)       : 5
Power ON/OFF            : off
Power status            : Detecting
PD class                : -
Reference power(mW)     : -
Power priority          : Low
Max power(mW)           : 60000
Current power(mW)       : 0
Peak power(mW)          : 0
Average power(mW)       : 0
Current(mA)             : 0
Voltage(V)              : 0
```

Table 3-79 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-on is enabled on an interface. To enable PoE fast-on on an interface, run 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.
Power-up mode	Power supply mode of an interface. To set the power supply mode for an interface, run the **3.7.9 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.
Power ON/OFF	Whether the interface is powered on. ● On: indicates that the interface is powered on. ● Off: indicates that the interface is powered off.

Item	Description
Power status	Power supply status of an interface. The status can be: ● 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 nterface 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. The priority is as follows: ● Critical: indicates the highest priority. ● High: indicates the second highest priority. ● Low: indicates the lowest priority. To set the priority, run the **3.7.25 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 802.3af. A maximum output power of 30000 mW indicates that the device complies with 802.3at. To set the value, run the **3.7.18 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 3-80 Description of the display poe power-state slot command output

Item	Description
PORTNAME	Name of an interface.
POWERON/OFF	Whether the interface is powered on. ● On: indicates that the interface is powered on. ● Off: indicates that the interface is powered off.

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-on is enabled on an interface. To enable PoE on an interface, run the **poe fast-on enable** command.
PRIORITY	Power supply priority of an interface. The priority is as follows: ● Critical: indicates the highest priority. ● High: indicates the second highest priority. ● Low: indicates the lowest priority. To set the priority, run the **3.7.25 poe priority** command.

Item	Description
STATUS	Power supply status of an interface. The status is classified into following types: ● 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 nterface works in standard hierarchical power supply mode.

Related Topics

3.7.16 poe legacy enable

3.7.10 poe enable

3.7.25 poe priority

3.7.18 poe power

3.7.6 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 the stack ID of a device.	The value is 0 if stacking is not configured. The value ranges from 0 to 8 if stacking is configured.

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 all the stack member switches.

```
<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
```

Table 3-81 Description of the display poe-power command output

Item	Description
Total Available PoE Power(mW)	Total power that can be provided for PDs.
Reserved PoE Power Percent	Percentage of the reserved power to the total power. To set the percentage, run the **3.7.23 poe power-reserved** command.
PoE Power Threshold Percent	Alarm threshold of the power consumption percentage. To set the threshold, run the **3.7.24 poe power-threshold** command.
PoE Power 1	PoE power supply 1.
PoE Power 2	PoE power supply 2.
Power Value(mW)	Power of a PoE power supply.
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 ● W2PSA0580: 580W current balance power supply ● PDC-650WA-BE: 650W current balance power supply ● W2PSA1150: 1150W current balance power supply
Supported Mode	Supported PoE power supply mode. The value can be: ● Redundancy: redundancy backup mode ● Balance: current balance mode

Related Topics

3.7.23 poe power-reserved

3.7.24 poe power-threshold

3.7.7 display snmp-agent trap feature-name poetrap all

Function

display snmp-agent trap feature-name poetrap all command displays the status of all traps on the POETRAP module.

Format

display snmp-agent trap feature-name poetrap all

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

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

Prerequisites

SNMP has been enabled. For details, see **snmp-agent**.

Example

# Display all the traps of the POETRAP module.

```
<HUAWEI>display snmp-agent trap feature-name poetrap all
------------------------------------------------------------------------------
Feature name: POETRAP
Trap number : 16
------------------------------------------------------------------------------
Trap name                    Default switch status   Current switch status
hwPoePdConnected                  on                      on
hwPoePdDisconnected               on                      on
```

```
hwPoePdClassInvalid           on                    on
hwPoePdClassOvercurrent         on                    on
hwPoePowerOff                 on                    on
hwPoePowerOn                  on                    on
hwPoePdPriorityDifferent        on                    on
hwPoePowerOverUtilizationThreshold
                              on                    on
hwPoePowerOverUtilizationThresholdResume
                              on                    on
hwPoePowerAbsent              on                    on
hwPoePowerAbsentResume          on                    on
hwPoeRpsPowerOutputAlarm        on                    on
hwPoeRpsPowerOutputAlarmResume  on
on
hwPoeCardAbsent               on                    on
hwPoePortFail                 on                    on
hwPoePortFailResume           on                    on
```

Table 3-82 Description of the display snmp-agent trap feature-name poetrap all command output

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

Item	Specification
Trap name	Trap name: ● hwPoePdConnected: A PD is connected to a port. ● hwPoePdDisconnected: A PD is disconnected from a port. ● hwPoePdClassInvalid: The system detects that the PD class is invalid. ● hwPoePdClassOvercurrent: The system detects that a PD is in overcurrent condition during PD classification. ● hwPoePowerOff: A PD connected to a port is powered off. ● hwPoePowerOn: A port meets power supply requirements. ● hwPoePdPriorityDifferent: The port priority is inconsistent with the PD priority. ● hwPoePowerOverUtilizationThreshold: The total PoE power consumption is larger than or equal to the alarm threshold. ● hwPoePowerOverUtilizationThresholdResume: The total PoE power consumption is less than the alarm threshold. ● hwPoePowerAbsent: No PoE power module on a PoE device is working properly. ● hwPoePowerAbsentResume: There are PoE power modules working properly on a PoE device. ● hwPoeRpsPowerOutputAlarm: An RPS power module fails to provide full power for the connected PoE device. ● hwPoeRpsPowerOutputAlarmResume: An RPS power module can provide the full power for the connected PoE device. ● hwPoeCardAbsent: A PoE card is not properly installed. ● hwPoePortFail: A PoE port is faulty. ● hwPoePortFailResume: A PoE port recovers from a failure.
Default switch status	Default status of the trap function: ● on: indicates that the trap function is enabled by default. ● off: indicates that the trap function is disabled by default.

Item	Specification
Current switch status	Status of the trap function: ● on: indicates that the trap function is enabled. ● off: indicates that the trap function is disabled.

Related Topics

3.7.28 snmp-agent trap enable feature-name poetrap

3.7.8 poe af-inrush enable

Function

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

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

By default, interfaces comply with 802.3at.

Format

poe af-inrush enable

undo poe af-inrush enable

Parameters

None

Views

Ethernet interface view, GE interface view, MultiGE interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Switches that comply with 802.3at cannot power some non-standard PDs that do not support inrush current. To power these PDs, change the power supply standards of interfaces from 802.3at to 802.3af.

Precautions

- The **poe af-inrush enable** command does not take effect on an interface if the **poe force-power** command has been executed on the interface.

- 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 S5730SI, S5730S-EI, S5720-16X-PWH-LI-AC, S5720-28X-PWH-LI-AC, and S6720SI, 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 may cause PD to work abnormally. Continue?[Y/N]:y
```

3.7.9 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**.

NOTE

Only the GE interfaces of S5730SI and S5730S-EI, the GE0/0/1 to GE0/0/12 of S5720-16X-PWH-LI-AC, the MultiGE interfaces of S5720-28X-PWH-LI-AC, and S6720SI 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+.	-

Parameter	Description	Value
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.	-
bt-inrush	Sets the power supply mode to PoE++.	-

Views

MultiGE interface view, GE interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

By default, on the S5720-16X-PWH-LI-AC, S5720-28X-PWH-LI-AC, and S6720SI, interfaces supporting the PoE++ mode provide power in PoE+ mode. 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 may cause 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 may cause PD to be powered off. Continue?[Y/N]:y
```

3.7.10 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

Ethernet interface view, GE interface view, port group view, MultiGE interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenarios

Before providing power for the PD connected to the interface, ensure the PoE function on the interface is enabled. IF the PoE function is not enabled, run the **poe enable** command to enable the PoE function on the interface.

In automatic mode, the power-on and power-off of interfaces are determined by the PoE power and interface power priority. When the PoE power is sufficient, the device does not power off one interface. To stop providing power for one PD, run the **undo poe enable** command.

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
```

Related Topics

3.7.5 display poe power-state

3.7.11 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.

NOTE

Only the S5720-28X-PWH-LI-AC, S5720-16X-PWH-LI-AC, S5730SI, S5730S-EI, and S6720SI support this command.

Format

poe fast-on enable

undo poe fast-on enable

Parameters

None

Views

MultiGE interface view, GE 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
```

# 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
```

3.7.12 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

Ethernet interface view, GE interface view, port group view, MultiGE interface 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.

NOTICE

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
```

3.7.13 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.

Format

poe group management enable

undo poe group management enable

Parameters

None

Views

Ethernet interface view, GE interface view, port group view, MultiGE interface 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 **3.7.25 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
```

3.7.14 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 the stack ID of a device.	The value ranges from 0 to 8 if stacking is configured. The value is 0 if stacking is not configured.

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
```

Related Topics

3.7.3 display poe information

3.7.15 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 S5730SI, S5730S-EI, S5720-16X-PWH-LI-AC, S5720-28X-PWH-LI-AC, and S6720SI 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**3.7.19 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 **poepower-oninterface** 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**3.7.5 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 **3.7.19 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
```

Related Topics

3.7.19 poe power-management

3.7.5 display poe power-state

3.7.4 display poe power

3.7.16 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

Ethernet interface view, GE interface view, port group view, MultiGE interface 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.

NOTICE

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
```

Related Topics

3.7.5 display poe power-state

3.7.17 poe max-power

Function

The **poe max-power** command sets the maximum output power of a device.

The **undo poe max-power** command restores the maximum output power of a device to the default value.

By default, the maximum output power of the device is the total power that the PoE power supply provides for PDs. Therefore, the configured maximum output power must be smaller than the total power that the PoE power supply provides for PDs.

Format

poe max-power *max-power* [**slot** *slot-id*]

undo poe max-power [[*max-power*] **slot** *slot-id*]

Parameters

Parameter	Description	Value
max-power	Specifies the maximum output power of a device.	The value is an integer ranging from 15400 to 1570800. The unit is mW.
slot *slot-id*	Specifies the stack ID.	The value is 0 if stacking is not configured. The value ranges from 0 to 8 if stacking is configured.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenarios

When the stacking function is enabled, if the stack ID is not specified, the **poe max-power** command is used to set the maximum output power of all member switches of a stack.

Precautions

- If the maximum output power that you set is smaller than the total power required by PDs, PDs with lower priority are powered off or cannot be powered on manually.
- The maximum output power of the device you configured should be smaller than the remaining power of the device. Otherwise, the configuration may be invalid.

Example

# Set the maximum output power of the device to 45000 mW.

```
<HUAWEI> system-view
[HUAWEI] poe max-power 45000 slot 0
```

Related Topics

3.7.6 display poe-power

3.7.18 poe power

3.7.18 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.

By default, the maximum power of each interface is 30000 mW , except for the following exceptions: each MultiGE interface of the S5720-14X-PWH-SI-AC provides a maximum of 90000 mW power; each MultiGE interface of S5720-28X-PWH-LI-AC, interfaces GE0/0/1 to GE0/0/12 of the S5720-16X-PWH-LI-AC, and S6720SI provide a maximum of 60000 mW power.

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 that ranges from 0 to 30000 mW , except for the following exceptions: each MultiGE interface of the S5720-14X-PWH-SI-AC ranges from 0 to 90000 mW; each MultiGE interface of S5720-28X-PWH-LI-AC, interfaces GE0/0/1 to GE0/0/12 of the S5720-16X-PWH-LI-AC, and S6720SI ranges from 0 to 60000 mW power.

Views

Ethernet interface view, GE interface view, port group view, MultiGE interface 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 **3.7.10 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
```

Related Topics

3.7.5 display poe power-state

3.7.17 poe max-power

3.7.19 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 S5730SI, S5730S-EI, S5720-16X-PWH-LI-AC, S5720-28X-PWH-LI-AC, and S6720SI 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.	-

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

Views

System view

Default Level

2: Configuration level

Usage Guidelines

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
```

Related Topics

3.7.3 display poe information

3.7.20 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

Ethernet interface view, GE interface view, port group view, MultiGE interface 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
```

Related Topics

14.1.26 time-range

3.7.21 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 10, in seconds.

Views

Ethernet interface view, GE interface view, port group view, MultiGE interface 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
```

3.7.22 poe power-policy port-index-priority disable

Function

The **poe power-policy port-index-priority disable** command disables the device from powering on or off PDs connected to interfaces based on the interface numbers.

The **undo poe power-policy port-index-priority disable** command enables the device to power on or off PDs connected to interfaces based on the interface numbers.

By default, a device powers on or off PDs connected to interfaces based on the interface numbers.

NOTE

Only the S2750EI, S5700LI, S5700S-LI, S5720EI, and S5720HI support this function.

Format

poe power-policy port-index-priority disable [**slot** *slot-id*]

undo poe power-policy port-index-priority disable [**slot** *slot-id*]

Parameters

Parameter	Description	Value
slot *slot-id*	Specifies a device ID.	The value is an integer, and the value range depends on the hardware configuration of the switch.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

In automatic power supply management mode, a PoE switch provides power to PDs connected to interfaces according to the following rules:

1. Preferentially provides power to PDs connected to the interface with a higher power supply priority.
2. Preferentially provides power to PDs connected to the interface with a smaller interface number if interfaces have the same power supply priority.

According to the rules, when the PoE power of a device is insufficient and interfaces connected to PDs have the same power supply priority, the device may power off PDs connected to the interface with a larger interface number to power on PDs connected to the interface with a smaller interface number even if these PDs are connected to the device last.

To prevent this problem, you can run the **poe power-policy port-index-priority disable** command to disable the device from powering on PDs connected to interfaces based on the interface numbers. Subsequently, when the PoE power is insufficient, the device does not power on the PDs that are connected later regardless of which interface they are connected to and does not power off the PDs that have been powered on.

Example

# Disable the device from powering on or off PDs connected to interfaces based on the port numbers.

```
<HUAWEI> system-view
[HUAWEI] poe power-policy port-index-priority disable
```

3.7.23 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*]

undo poe power-reserved *power-reserved* **slot** *slot-id*

undo poe power-reserved [**slot** *slot-id*]

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

Views

System view

Default Level

2: Configuration level

Usage Guidelines

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 cuts off the power of the PDs on the interfaces of low priority to ensure that other PDs can run normally.

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 **3.7.17 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: This operation may power off some PDs of slot 0.Continue?[Y/N]:y
```

Related Topics

3.7.17 poe max-power

3.7.6 display poe-power

3.7.24 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*]

undo poe power-threshold *threshold-value* **slot** *slot-id*

undo poe power-threshold [**slot** *slot-id*]

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 the stack ID.	The value is 0 if stacking is not configured. The value ranges from 0 to 8 if stacking is configured.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

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
```

Related Topics

3.7.23 poe power-reserved

3.7.25 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

Ethernet interface view, GE interface view, port group view, MultiGE interface 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. the S2750EI, S5700LI, S5700S-LI, S5720EI, and S5720HI provide power to PDs connected to the interfaces in ascending order of interface numbers. Other series of 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
```

Related Topics

3.7.19 poe power-management

3.7.26 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.

Format

poe single-class enable

undo poe single-class enable

Parameters

None

Views

Ethernet interface view, GE interface view, port group view, MultiGE interface 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 S5730SI, S5730S-EI, S5720-16X-PWH-LI-AC, S5720-28X-PWH-LI-AC, and S6720SI, 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
```

3.7.27 rps cold-backup

Function

The **rps cold-backup** command configures the RPS as the backup power module.

The **undo rps cold-backup** command restores the RPS power module for the PoE device.

By default, if a PoE switch connects to an RPS, the RPS and power modules of the switch supply power to the switch simultaneously.

NOTE

Only the S5700-28P-PWR-LI-AC, S5700-28TP-PWR-LI-AC, S5700-28X-PWR-LI-AC, S5700-52P-PWR-LI-AC, S5700-52X-PWR-LI-AC, and S5701-28TP-PWR-LI-AC support the command.

Format

rps cold-backup [**slot** *slot-id*]

undo rps cold-backup [**slot** *slot-id*]

Parameters

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

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenarios

S5700LI can use an RPS and its own power modules for power supply. By default, if a PoE switch connects to an RPS, the RPS and power modules of the switch supply power to the switch simultaneously. The switch provides 800 W of PoE power. You can configure the RPS as a backup power supply using the **rps cold-backup** command. After you run this command, the switch uses its own power modules for PoE power supply. If the total power consumption of all PDs connected to the switch is low, the RPS can be configured as a backup power supply to save power.

Precautions

- The command is valid only when the RPS has been correctly connected to the switch and powered on.
- When the AC input voltage is 220 V, the RPS that has one 870 W PoE power module can provide 800 W PoE power for only one PoE switch. The RPS can have at most two 870 W PoE power modules configured to provide PoE power for two PoE switches, 800 W PoE power for each switch.
- When the AC input voltage is 110 V, each 870 W PoE power module can provide only 400 W PoE power. If you need to use the RPS to provide PoE power, the RPS must have two 870 W PoE power modules configured and it can provide only one port to provide 800 W PoE power for one PoE switch.
- If an RPS is not used as a backup power supply, it can provide PoE power supply to a maximum of two S5700LI switches at the same time.
- When an RPS is configured as a backup power supply, it can provide power redundancy for a maximum of six switches. If the power modules of a switch fail, the RPS can provide power supply to the switch immediately to ensure uninterrupted services. The RPS can ensure seamless power supply switchover for one switch at a time.
- Switches connected to the same RPS must have the same configuration.

Example

# Set the RPS to the backup PoE power module.

```
<HUAWEI> system-view
[HUAWEI] rps cold-backup
Warning: The RPS power will change the supply mode! Continue? [Y/N]:y
Info: Succeeded in setting the configuration. This command will take effect only after
RPS has capability for power suppply.
```

3.7.28 snmp-agent trap enable feature-name poetrap

Function

snmp-agent trap enable feature-name poetrap command enables the trap function for the POETRAP module.

undo snmp-agent trap enable feature-name poetrap command disables the trap function for the POETRAP module.

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

Format

snmp-agent trap enable feature-name poetrap [**trap-name** *trap-name*]

undo snmp-agent trap enable feature-name poetrap [**trap-name** *trap-name*]

Parameters

Parameter	Description	Value
trap-name *trap-name*	Specifies the trap for an event of the POETRAP module.	The value is an enumerated value and must be set as prompted by the device.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

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

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

Example

# Enable the hwpoepdconnected trap of the POETRAP module.

```
<HUAWEI> system-view
[HUAWEI] snmp-agent trap enable feature-name poetrap trap-name hwpoepdconnected
```

Related Topics

3.7.7 display snmp-agent trap feature-name poetrap all

3.8 Stack Configuration Commands

3.8.1 Command Support

3.8.2 display mad

3.8.3 display snmp-agent trap feature-name stack all

3.8.4 display snmp-agent trap feature-name mad all

3.8.5 display stack

3.8.6 display stack peers

3.8.7 display stack port

3.8.8 display stack port auto-cable-info

3.8.9 display stack port speed

3.8.10 display stack-port load-balance

3.8.11 display stack configuration

3.8.12 display stack channel

3.8.13 display upgrade area

3.8.14 display upgrade state

3.8.15 interface stack-port

3.8.16 mad detect mode direct

3.8.17 mad detect mode relay

3.8.18 mad domain

3.8.19 mad exclude

3.8.20 mad relay

3.8.21 mad restore

3.8.22 port interface enable

3.8.23 reset stack configuration

3.8.24 reset stack port statistics

3.8.25 reset stack-port configuration

3.8.26 save stack configuration

3.8.27 set l2-traffic fast-recover

3.8.28 shutdown interface

3.8.29 stack authentication

3.8.30 stack led enable

3.8.31 stack-port load-balance mode

3.8.32 stack port speed

3.8.33 stack port { crc | link-flap } trigger

3.8.34 stack port { crc | link-flap } trigger error-down

3.8.35 stack reserved-vlan

3.8.36 stack slot priority

3.8.37 stack slot renumber

3.8.38 stack timer mac-address switch-delay

3.8.39 snmp-agent trap enable feature-name stack

3.8.40 snmp-agent trap enable feature-name mad

3.8.41 upgrade backup-area slot

3.8.42 upgrade start

3.8.1 Command Support

Table 3-83 Applicable product models and versions

Product	Software Version	Stack Connection Mode
S1720	Not supported	-
S2700SI	Not supported	-
S2710SI	V100R006(C03&C05)	Service port connection using ordinary cables
S2700EI	V100R005C01, V100R006(C00&C01&C03&C05)	Service port connection using ordinary cables
S2720EI	Versions supporting service port connection using ordinary cables: V200R006C10, V200R009C00, V200R010C00, V200R011C10 Versions supporting service port connection using dedicated cables: V200R011C10	Service port connections using ordinary and dedicated cables
S2750EI	Versions supporting service port connection using ordinary cables: V200R003C00, V200R005C00SPC300, V200R006C00, V200R007C00, V200R008C00, V200R009C00, V200R010C00, V200R011C00, V200R011C10 Versions supporting service port connection using dedicated cables: V200R011C10	Service port connections using ordinary and dedicated cables
S3700SI	V100R005C01, V100R006(C00&C01&C03&C05)	Service port connection using ordinary cables
S3700EI	V100R005C01, V100R006(C00&C01&C03&C05)	Service port connection using ordinary cables
S3700HI	Not supported	-

Product	Software Version	Stack Connection Mode
S5700EI	V100R005C01, V100R006(C00&C01), V200R001(C00&C01), V200R002C00, V200R003C00, V200R005(C00&C01&C02&C03)	Stack card connection
S5700SI	V100R005C01, V100R006C00, V200R001C00, V200R002C00, V200R003C00, V200R005C00	Stack card connection
S5700HI	V200R003C00, V200R005C00	Service port connection using ordinary cables
S5700LI	Versions supporting service port connection using ordinary cables: V200R001C00, V200R002C00, V200R003(C00&C02&C10), V200R005C00SPC300, V200R006C00, V200R007C00, V200R008C00, V200R009C00, V200R010C00, V200R011C00, V200R011C10 Versions supporting service port connection using dedicated cables: V200R011C10	Service port connections using ordinary and dedicated cables
S5700S-LI	Versions supporting service port connection using ordinary cables: V200R008C00, V200R009C00, V200R010C00, V200R011C00, V200R011C10 Versions supporting service port connection using dedicated cables: V200R011C10	Service port connections using ordinary and dedicated cables
S5710EI	V200R001C00, V200R002C00, V200R003C00, V200R005(C00&C02)	Service port connection using ordinary cables
S5710HI	V200R005C03	Service port connection using ordinary cables
S5710-C-LI	V200R001C00	Stack card connection

Product	Software Version	Stack Connection Mode
S5710-X-LI	Versions supporting service port connection using ordinary cables: V200R008C00, V200R009C00, V200R010C00, V200R011C00, V200R011C10 Versions supporting service port connection using dedicated cables: V200R011C10	Service port connections using ordinary and dedicated cables
S5720LI and S5720S-LI	Versions supporting service port connection using ordinary cables: V200R010C00, V200R011C00, V200R011C10 Versions supporting service port connection using dedicated cables: V200R011C10	Service port connections using ordinary and dedicated cables
S5720SI and S5720S-SI	Versions supporting service port connection using ordinary cables: V200R008C00, V200R009C00, V200R010C00, V200R011C00, V200R011C10 Versions supporting service port connection using dedicated cables: V200R011C10	Service port connections using ordinary and dedicated cables

Product	Software Version	Stack Connection Mode
S5720EI	V200R007C00, V200R008C00, V200R009C00, V200R010C00, V200R011C00, V200R011C10	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.
S5720HI	Versions supporting service port connection using ordinary cables: V200R009C00, V200R010C00, V200R011C00, V200R011C10 Versions supporting service port connection using dedicated cables: V200R011C10	Service port connections using ordinary and dedicated cables
S5730SI	V200R011C10	Service port connections using ordinary and dedicated cables
S5730S-EI	V200R011C10	Service port connections using ordinary and dedicated cables
S6700EI	V100R006C00, V200R001(C00&C01), V200R002C00, V200R003C00, V200R005(C00&C01&C02)	Service port connection using ordinary cables

Product	Software Version	Stack Connection Mode
S6720EI	Versions supporting service port connection using ordinary cables: V200R008C00, V200R009C00, V200R010C00, V200R011C00, V200R011C10 Versions supporting service port connection using dedicated cables: V200R011C10	Service port connections using ordinary and dedicated cables
S6720S-EI	Versions supporting service port connection using ordinary cables: V200R009C00, V200R010C00, V200R011C00, V200R011C10 Versions supporting service port connection using dedicated cables: V200R011C10	Service port connections using ordinary and dedicated cables
S6720SI and S6720S-SI	Versions supporting service port connection using ordinary cables: V200R011C00, V200R011C10 Versions supporting service port connection using dedicated cables: V200R011C10	Service port connections using ordinary and dedicated cables
S6720LI and S6720S-LI	Versions supporting service port connection using ordinary cables: V200R011C00, V200R011C10 Versions supporting service port connection using dedicated cables: V200R011C10	Service port connections using ordinary and dedicated cables

3.8.2 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 3-84 Description of the **display mad** command output

Item	Description
Current MAD domain	MAD domain configured in the system. To configure this parameter, run the **3.8.18 mad domain** command.
MAD direct detection enabled	MAD in direct mode is configured. To configure MAD in direct mode, run the **3.8.16 mad detect mode direct** command.
MAD relay detection enabled	MAD in relay mode is configured. To configure MAD in relay mode, run the **3.8.17 mad detect mode relay** command.
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 **3.8.16 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 **3.8.17 mad detect mode relay** command.
Excluded ports(configurable)	Interfaces excluded from shutdown. To configure interfaces excluded from shutdown, run the **3.8.19 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 **3.8.20 mad relay** command.

Related Topics

3.8.16 mad detect mode direct

3.8.17 mad detect mode relay

3.8.19 mad exclude

3.8.20 mad relay

3.8.3 display snmp-agent trap feature-name stack all

Function

The **display snmp-agent trap feature-name stack all** command displays the status of all stack traps.

Format

display snmp-agent trap feature-name stack all

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can use this command to check the status of all stack traps. These traps can be enabled or disabled using the **3.8.39 snmp-agent trap enable feature-name stack** command.

Example

# Display the status of all stack traps.

```
<HUAWEI> display snmp-agent trap feature-name stack all
------------------------------------------------------------------------------
Feature name: stack
Trap number : 21
------------------------------------------------------------------------------
Trap name                        Default switch status   Current switch status
hwStackLinkUp                      on                      on
hwStackLinkDown                    on                      on
hwStackStandbyChange               on                      on
hwStackSwitchOver                  on                      on
hwStackSystemRestart               on                      on
hwStackStackMemberAdd              on                      on
hwStackStackMemberLeave            on                      on
hwStackStackMacChange              on                      on
hwStackLogicStackPortLinkErr       on                      on
hwStackPhyStackPortLinkErr         on                      on
hwPhyStackPortIsDown               on                      on
```

```
hwPhyStackPortIsUp              on                     on
hwStackPortConfigureFailed      on                     on
hwStackMemberExceedSpec         on                     on
hwPhyStackPortErrorDown         on                     on
hwPhyStackPortErrorDownRecover  on                     on
hwPhyStackVlanConflict          on                     on
hwStackPortErrorDown            on                     on
hwStackPortErrorDownRecovery    on                     on
hwStackSetUpFailure             on                     on
hwStackAutoConfigFailed         on                     on
```

Table 3-85 Description of the **display snmp-agent trap feature-name stack all** command output

Item	Description
Feature name	Name of the feature for which the traps are defined.
Trap number	Number of traps.

Item	Description
Trap name	Name of a trap: ● hwStackLinkUp: A stack port was Up. ● hwStackLinkDown: A stack port was Down. ● hwStackStandbyChange: A slave switch was elected as the standby switch. ● hwStackSwitchOver: The standby switch became the master switch. ● hwStackSystemRestart: A stack restarted, and the original master switch was no longer the master after master preemption. ● hwStackStackMemberAdd: A new member switch joined the stack. ● hwStackStackMemberLeave: A member switch left the stack. ● hwStackStackMacChange: The stack MAC address changed. ● hwStackLogicStackPortLinkErr: A logical stack port was incorrectly connected. ● hwStackPhyStackPortLinkErr: A physical member port was incorrectly connected. ● hwPhyStackPortIsDown: The physical member port was Down. ● hwPhyStackPortIsUp: The physical member port was Up. ● hwStackPortConfigureFailed: The stack port configuration was incorrect. ● hwStackMemberExceedSpec: The number of member switches reached the maximum value. ● hwPhyStackPortErrorDown: An Error-down event occurred on a physical member port that was added to a logical stack port. ● hwPhyStackPortErrorDownRecover: The physical member port that was added to a logical stack port recovered from the Error-down state. ● hwPhyStackVlanConflict: The service VLAN conflicted with the stack reserved VLAN. ● hwStackPortErrorDown: The stack port entered the Error-down state. ● hwStackPortErrorDownRecovery: The stack port recovered from the Error-down state. ● hwStackSetUpFailure: The stack failed to be set up.

Item	Description
	- hwStackAutoConfigFailed: After a dedicated stack cable was connected, the interface did not automatically become a stack port.
Default switch status	Default status of a trap: - on: The trap is enabled by default. - off: The trap is disabled by default.
Current switch status	Current status of a trap: - on: The trap is enabled. - off: The trap is disabled. A trap can be enabled or disabled using the **3.8.39 snmp-agent trap enable feature-name stack** command.

Related Topics

3.8.39 snmp-agent trap enable feature-name stack

3.8.4 display snmp-agent trap feature-name mad all

Function

display snmp-agent trap feature-name mad all command displays the status of all traps in the MAD module.

Format

display snmp-agent trap feature-name mad all

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

After the trap function of the MAD module is enabled using the **snmp-agent trap enable feature-name mad** command, you can run the **display snmp-agent trap**

feature-name mad all command to check the status of all traps in the MAD module.

Prerequisites

SNMP has been enabled using the **snmp-agent** command.

Example

# Display the status of all the traps in the MAD module.

```
<HUAWEI>display snmp-agent trap feature-name mad all
------------------------------------------------------------------------------
Feature name: MAD
Trap number : 2
------------------------------------------------------------------------------
Trap name                    Default switch status   Current switch status
hwMadConflictDetect              on                     on
hwMadConflictResume              on                     on
```

Table 3-86 Description of the **display snmp-agent trap feature-name mad all** command output

Item	Specification
Feature name	Name of the module that the trap belongs to.
Trap number	Number of traps.
Trap name	Trap name: ● hwMadConflictDetect: A MAD conflict is detected. ● hwMadConflictResume: Existing stacks are merged.
Default switch status	Default status of the trap function: ● on: The trap function is enabled by default. ● off: The trap function is disabled by default.
Current switch status	Status of the trap function: ● on: The trap function is enabled. ● off: The trap function is disabled.

Related Topics

3.8.40 snmp-agent trap enable feature-name mad

3.8.5 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: 0018-82b1-6eb4
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      0018-82b1-6eb4   200          S5700-28P-LI-AC
   1   Standby     0018-82b1-6eba   150          S5700-28P-LI-AC
```

Table 3-87 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.

Item	Description
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.
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.

3.8.6 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
Slot      Port1                  Peer1       Port2                  Peer2
-------------------------------------------------------------------------
0         STACK 1                1           STACK 2                None
1         STACK 1                None        STACK 2                0
```

Table 3-88 Description of the **display stack peers** command output

Item	Description
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.

3.8.7 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 S5720EI (stack card 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
Stack Port           PHY  Protocol  InUti OutUti  InErrors          OutErrors
-------------------------------------------------------------------------------
stack-port0/1          up   up        0%    0%            0           0
stack-port0/2          up   up        0%    0%            0           0
```

# Display summary of stack ports on the S5720LI (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
Stack Port              PHY  Protocol  InUti OutUti  InErrors          OutErrors
--------------------------------------------------------------------------------
stack-port0/1           up   up        0%    0%           0          0
  XGigabitEthernet0/0/1  up   up        0%    0%           0          0
  XGigabitEthernet0/0/2  up   up        0%    0%           0          0
stack-port0/2           up   up        0%    0%           0          0
  XGigabitEthernet0/0/3  up   up        0%    0%           0          0
  XGigabitEthernet0/0/4  up   up        0%    0%           0          0
```

# Display summary of stack ports on the S6720EI (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
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 0
```

Table 3-89 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.
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.

Item	Description
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 3-90 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.
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.

Item	Description
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.
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 3-91 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.
Status	Status of a physical member port.

3.8.8 display stack port auto-cable-info

Function

The **display stack port auto-cable-info** command displays information about dedicated stack cables.

NOTE

S1720 and S5720EI do not support this command.

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 3-92 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.

3.8.9 display stack port speed

Function

The **display stack port speed** command displays the stack port working speed.

NOTE

- Only the S5710-X-LI, S5700S-X-LI, S5720SI, S5720S-SI, S5720-X-LI, S5720S-X-LI, S5730SI, S5730S-EI, S6720LI, S6720S-LI, S6720SI, and S6720S-SI 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 3-93 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.

3.8.10 display stack-port load-balance

Function

The **display stack-port load-balance** command displays the load balancing modes of stack ports.

NOTE

Only the S5720HI, S6720EI, and S6720S-EI 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.

Parameter	Description	Value
port-id	Specifies the ID of a stack port.	The value is 1 or 2.
global	Displays the global load balancing mode. **NOTE** The S5720HI 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
Interface stack-port0/1 load balance mode: ENHANCED
Interface stack-port0/2 load balance mode: ENHANCED
Interface stack-port1/1 load balance mode: DST-MAC
Interface stack-port1/2 load balance mode: SRC-MAC
Interface stack-port2/1 load balance mode: DST-IP
Interface stack-port2/2 load balance mode: SRC-DST-IP
```

Table 3-94 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. To set the global load balancing mode, run the **stack-port load-balance mode** command in the system view.
Interface stack-port0/1 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. To set the load balancing mode for a stack port, run the **stack-port load-balance mode** command in the stack port view.

3.8.11 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

When a new device joins a stack, you can run this command to check which stack commands have been configured in the stack. You can then modify parameter settings in these commands and issue these commands to the new device in sequence. During command execution, you may need to restart the device or confirm your operation as prompted.

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.
  - 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.

3.8.12 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 3-95 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.

3.8.13 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 3-96 Description of the **display upgrade area** 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.
Upgrade-Check	Upgrade check result. ● passed ● failed

3.8.14 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   : -
 Description : -
--------------------------------------
```

Table 3-97 Description of the **display upgrade state** 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.
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.
Description	Description about the failure if an upgrade fails.

3.8.15 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]
```

3.8.16 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, 40GE interface view, port group view, MultiGE 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
```

Related Topics

3.8.2 display mad

3.8.17 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
```

Related Topics

3.8.2 display mad

3.8.18 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
```

Related Topics

3.8.2 display mad

3.8.19 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
```

Related Topics

3.8.2 display mad

3.8.20 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
```

3.8.21 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
```

3.8.22 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 **4.1.4 description (interface view)**, 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 S5720SI, S5720S-SI, S5730SI, S5730S-EI, S6720LI, S6720S-LI, S6720SI, and S6720S-SI, 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 S6720EI 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

- To restore a physical member port as a service interface, run the **3.8.28 shutdown interface** command in the stack port view and then run the **undo port interface enable** command.
- On the S2720EI, S2750EI, S5700S-LI, S5700LI, S5710-X-LI, S5720LI, S5720S-LI, S5720S-SI, S5720SI, S5730SI, S5730S-EI, S6720LI, S6720S-LI, S6720SI, and S6720S-SI, 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 S6720EI, 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: Port groups XGigabitEthernet0/0/13 to XGigabitEthernet0/0/16 have been configured as physical stack-
ports.
```

Related Topics

3.8.15 interface stack-port

3.8.23 reset stack configuration

Function

The **reset stack configuration** command clears all stack configuration. That is, this command restores the default stack configuration.

NOTE

S1720 and S5720EI do not support this command.

Format

reset stack configuration

Parameters

None

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

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.

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.

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
```

3.8.24 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
```

3.8.25 reset stack-port configuration

Function

The **reset stack-port configuration** command clears the service port stack configuration.

NOTE

Only the S5720EI supports this command.

Format

reset stack-port configuration [**slot** *slot-id*]

Parameters

Parameter	Description	Value
slot *slot-id*	Specifies a 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

- When the current stack connection mode is service port connection, you must run the **reset stack-port configuration** command to clear the existing service port stack configuration before changing the stack connection mode to stack card connection. After the configuration is cleared, restart the stack and then the stack card connection mode takes effect.
- If the current stack connection mode is stack card connection, you can run the **reset stack-port configuration** command to clear the service port stack configuration if such configuration already exists. You can run the **3.8.11 display stack configuration** command to check the existing service port stack configuration.

Precautions

- In service port connection mode, after clearing the service port stack configuration of a member switch, restart the switch to make the configuration take effect. If you perform the service port stack configuration on the member switch before restarting, the service port stack configuration on the member switch is not cleared.
- When the stack is changed from service port connection to stack card connection, remove the cables connected to service ports to prevent potential loops.

Example

# Clear the service port stack configuration.

```
<HUAWEI> system-view
[HUAWEI] reset stack-port configuration
```

Related Topics

3.8.11 display stack configuration

3.8.26 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.

NOTE

S1720 and S5720EI do not support this command.

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
```

3.8.27 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
```

3.8.28 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
Info: This operation may take a few seconds. Please wait...succeeded.
```

3.8.29 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** *mac-address* | **esn** *esn-value* }

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 *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.

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
```

3.8.30 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.

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
```

3.8.31 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 load balancing of stack member ports is performed in enhanced mode based on the source MAC address, destination MAC address, source IP address, destination IP address, and port number.

NOTE

Only the S5720HI, S6720EI, and S6720S-EI 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 S5720HI does 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
```

3.8.32 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 "Stacking Support and Version Requirements " in Stack Configuration in the *S1720, S2700, S5700, and S6720 V200R011C10 Configuration Guide - Device Management*.

NOTE

- Only the S5710-X-LI, S5700S-X-LI, S5720SI, S5720S-SI, S5720-X-LI, S5720S-X-LI, S5730SI, S5730S-EI, S6720LI, S6720S-LI, S6720SI, and S6720S-SI 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 { **48G** | **12G** | **2.5G** }

undo stack port speed

Parameters

Parameter	Description	Value
48G	Sets the working speed of stack member ports to 48 Gbit/s. This speed can be set only on the S5730SI, S5730S-EI, S6720LI, S6720S-LI, S6720SI, and S6720S-SI.	-
12G	Sets the working speed of stack member ports to 12 Gbit/s. This speed can be set only on the S5710-X-LI, S5700S-X-LI, S5720SI, S5720S-SI, S5720-P-LI, S5720-X-LI, and S5720S-X-LI.	-

Parameter	Description	Value
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.	-

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

On the S5710-X-LI, S5700S-X-LI, S5720SI, S5720S-SI, S5720-P-LI, S5720-X-LI, 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.

On the S5730SI, S5730S-EI, S6720LI, S6720S-LI, S6720SI, and S6720S-SI, if 40GE optical ports are used as stack member ports and are connected using 1 m, 3 m or 5m QSFP+ passive copper cables, you can use this command to increase their working speed from 40 Gbit/s to 48 Gbit/s, expanding the stack bandwidth. After their working speed is increased to 48 Gbit/s, switches using these ports cannot set up a stack with switches using ports with the working speed 40 Gbit/s.

On the S6720SI, only the rate of 40GE interfaces on the front panel can be increased to 48 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.

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
```

3.8.33 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 error-down alarm threshold is 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 errors.	-
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 errors and ranges from 3 to 30 for error-down alarms triggered by port Up/Down transitions. The unit is times per minute.
interval *interval*	Specifies the error-down check interval.	The value is an integer that ranges from 3 to 30, in minutes.

Parameter	Description	Value
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 errors to 3 minutes. That is, if the rate of received CRC 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
```

3.8.34 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 errors.	-
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 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 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.
- 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 errors.

```
<HUAWEI> system-view
[HUAWEI] stack port crc trigger error-down
```

3.8.35 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
```

3.8.36 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: Please do not frequently modify Priority because it will make the stack split. Continue? [Y/N]:y
```

Related Topics

3.8.5 display stack

3.8.37 stack slot renumber

Function

The **stack slot renumber** command changes the stack ID of a specified member switch in a stack.

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 member switch in a stack, run the **stack slot renumber** command.

NOTE

- 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 save the current configuration and 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.

Example

# Change the stack ID of a 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.
Please do not frequently modify 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.
```

Related Topics

3.8.5 display stack

3.8.38 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: Please do not frequently modify MAC switch time because it will make the stack split. Continue?
[Y/N]:y
```

3.8.39 snmp-agent trap enable feature-name stack

Function

The **snmp-agent trap enable feature-name stack** command enables a specified stack trap or all stack traps.

The **undo snmp-agent trap enable feature-name stack** command disables a specified stack trap or all stack traps.

By default, all stack traps are enabled.

Format

snmp-agent trap enable feature-name stack [**trap-name** *trap-name*]

undo snmp-agent trap enable feature-name stack [**trap-name** *trap-name*]

Parameters

Parameter	Description	Value
trap-name *trap-name*	Specifies the name of a trap.	This parameter has enumerated values: ● hwphystackporterrordown: An Error-down event occurred on a physical member port that was added to a logical stack port. ● hwphystackporterrordownrecover: The physical member port that was added to a logical stack port recovered from the Error-down state. ● hwphystackportisdown: The physical member port was Down. ● hwphystackportisup: The physical member port was Down. ● hwphystackvlanconflict: The service VLAN conflicted with the stack reserved VLAN. ● hwstackautoconfigfailed: After a dedicated stack cable was connected, the interface did not automatically become a stack port. ● hwstacklinkdown: A stack port was Down. ● hwstacklinkup: A stack port was Up. ● hwstacklogicstackportlinkerr: A logical stack port was incorrectly connected. ● hwstackmemberexceedspec: The number of member switches reached the maximum value. ● hwstackphystackportlinkerr: A physical member port was incorrectly connected. ● hwstackportconfigurefailed: The stack port configuration was incorrect. ● hwstackporterrordown: The stack port entered the Error-down state. ● hwstackporterrordownrecovery: The stack port recovered from the Error-down state. ● hwstacksetupfailure: The stack failed to be set up. ● hwstackstackmacchange: The stack MAC address changed. ● hwstackstackmemberadd: A new member switch joined the stack. ● hwstackstackmemberleave: A new member switch left the stack. ● hwstackstandbychange: A slave switch was elected as the standby switch. ● hwstackswitchover: The standby switch became the master switch.

Parameter	Description	Value
		- hwstacksystemrestart: A stack restarted, and the original master switch was no longer the master after master preemption.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

By default, all stack traps are enabled. You can learn about stack status changes from these traps. If you disable a type of stack trap, the switch no longer sends this trap. Disabling the stack traps is not recommended.

Example

# Enable the hwstackswitchover trap.

```
<HUAWEI> system-view
[HUAWEI] snmp-agent trap enable feature-name stack trap-name hwstackswitchover
```

Related Topics

3.8.3 display snmp-agent trap feature-name stack all

3.8.40 snmp-agent trap enable feature-name mad

Function

snmp-agent trap enable feature-name mad command enables the trap function for the MAD module.

undo snmp-agent trap enable feature-name mad command disables the trap function of the MAD module.

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

Format

snmp-agent trap enable feature-name mad [**trap-name** { **hwmadconflictdetect** | **hwmadconflictresume** }]

undo snmp-agent trap enable feature-name mad [**trap-name** { **hwmadconflictdetect** | **hwmadconflictresume** }]

Parameters

Parameter	Description	Value
trap-name	Enables or disables the trap function for a specified event.	-
hwmadconflictdetect	Enables or disables the trap function when a MAD conflict is detected.	-
hwmadconflictresume	Enables or disables the trap function when existing stacks are merged.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

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

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

Example

# Enable the hwmadconflictdetect trap function of the MAD module.

```
<HUAWEI> system-view
[HUAWEI] snmp-agent trap enable feature-name mad trap-name hwmadconflictdetect
```

Related Topics

3.8.4 display snmp-agent trap feature-name mad all

3.8.41 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. Member switches in the two areas can then be upgraded in turns. When member switches in one area are being upgraded, traffic is transmitted to member switches in the other area.

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
```

3.8.42 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 **3.8.41 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 3-98** lists the error codes and displayed messages in different upgrade failure scenarios.

Table 3-98 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	

Upgrade Failure Scenario	Error Code	Displayed Message
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	
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	

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 before switches in the active area restart).	771	
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	

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 (after switches in the backup area restart).	1281	Master of the backup area notifies others of rollback.
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
```

3.9 SVF Configuration Commands

3.9.1 Command Support

3.9.2 arp anti-attack check user-bind enable (network enhanced profile view)

3.9.3 as-admin-profile (AS group view)

3.9.4 as-admin-profile name

3.9.5 as-auth

3.9.6 as-group name

3.9.7 as access dtls psk

3.9.8 as access manage-mac

3.9.9 as auto-replace enable

3.9.10 as-mode disable

3.9.11 as all (AS group view)

3.9.12 as name (AS group view)

3.9.13 as name interface (port group view)

3.9.14 as name (uni-mng view)

3.9.15 as reset

3.9.16 as service-vlan igmp-snooping

3.9.17 as service-vlan authorization

3.9.18 as type

3.9.19 attach as

3.9.20 authentication access-user maximum (user access profile view)

3.9.21 auth-mode none

3.9.22 authentication-profile (user access profile view)

3.9.23 blacklist mac-address

3.9.24 broadcast-suppression (network enhanced profile view)

3.9.25 clear direct-command

3.9.26 commit as

3.9.27 confirm

3.9.28 description (Fabric-port view)

3.9.29 description (port group view)

3.9.30 dhcp snooping enable (network enhanced profile view)

3.9.31 direct-command

3.9.32 display as

3.9.33 display as access configuration

3.9.34 display as blacklist

3.9.35 display as run-info

3.9.36 display as unauthorized record

3.9.37 display as whitelist

3.9.38 display snmp-agent trap feature-name asmngtrap all

3.9.39 display snmp-agent trap feature-name unimbrtrap all

3.9.40 display snmp-agent trap feature-name uni-topomng all

3.9.41 display snmp-agent trap feature-name uni-tplm all

3.9.42 display snmp-agent trap feature-name uni-vermng all

3.9.43 display uni-mng as-discover packet statistics

3.9.44 display uni-mng as-group

3.9.45 display uni-mng as index

3.9.46 display uni-mng as interface brief

3.9.47 display uni-mng as interface eth-trunk

3.9.48 display uni-mng commit-result

3.9.49 display uni-mng global

3.9.50 display uni-mng indirect configuration

3.9.51 display uni-mng execute-failed-record

3.9.52 display uni-mng interface fabric-port configuration

3.9.53 display uni-mng interface fabric-port state

3.9.54 display uni-mng patch-delete info

3.9.55 display uni-mng port-group

3.9.56 display uni-mng profile

3.9.57 display uni-mng profile as

3.9.58 display uni-mng topology configuration

3.9.59 display uni-mng topology information

3.9.60 display uni-mng unauthen-user

3.9.61 display uni-mng unauthen-user offline-record

3.9.62 display uni-mng upgrade-info

3.9.63 display uni-mng up-direction fabric-port

3.9.64 down-direction fabric-port

3.9.65 down-direction fabric-port connect independent-as

3.9.66 forward-mode centralized

3.9.67 independent-as-admin

3.9.68 interface fabric-port

3.9.69 ip source check user-bind enable (network enhanced profile view)

3.9.70 mac-limit (user access profile view)

3.9.71 multicast-suppression (network enhanced profile view)

3.9.72 network-basic-profile name

3.9.73 network-basic-profile (port group view)

3.9.74 network-enhanced-profile name

3.9.75 network-enhanced-profile (port group view)

3.9.76 pass-vlan (network basic profile view)

3.9.77 patch delete as

3.9.78 port connect independent-as

3.9.79 port connect-type indirect

3.9.80 port-group name

3.9.81 port eth-trunk trunkmember

3.9.82 port member-group interface

3.9.83 portal url-encode disable

3.9.84 rate-limit (network enhanced profile view)

3.9.85 reboot uni-mng

3.9.86 reset uni-mng as-discover packet statistics

3.9.87 shutdown interface

3.9.88 slot

3.9.89 snmp-agent trap enable feature-name asmngtrap

3.9.90 snmp-agent trap enable feature-name unimbrtrap

3.9.91 snmp-agent trap enable feature-name uni-topomng

3.9.92 snmp-agent trap enable feature-name uni-tplm

3.9.93 snmp-agent trap enable feature-name uni-vermng

3.9.94 traffic-limit inbound (user access profile view)

3.9.95 traffic-limit outbound (AS administrator profile view)

3.9.96 topology explore

3.9.97 undo uni-mng enable

3.9.98 uni eth-trunk

3.9.99 uni-mng

3.9.100 uni-mng indirect fabric-port

3.9.101 uni-mng indirect mng-vlan

3.9.102 uni-mng up-direction fabric-port

3.9.103 unicast-suppression (network enhanced profile view)

3.9.104 upgrade as

3.9.105 upgrade { local-ftp-server | local-sftp-server }

3.9.106 upload config

3.9.107 user-access-port enable (network enhanced profile view)

3.9.108 user-access-profile name

3.9.109 user-access-profile (port group view)

3.9.110 user-vlan (network basic profile view)

3.9.111 user password (AS administrator profile view)

3.9.112 voice-vlan (network basic profile view)

3.9.113 whitelist mac-address

3.9.1 Command Support

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

3.9.2 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
```

Related Topics

3.9.74 network-enhanced-profile name

3.9.3 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
```

Related Topics

3.9.4 as-admin-profile name

3.9.6 as-group name

3.9.4 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
```

Related Topics

3.9.111 user password (AS administrator profile view)

3.9.5 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
```

3.9.6 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
```

Related Topics

3.9.12 as name (AS group view)

3.9.3 as-admin-profile (AS group view)

3.9.7 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
```

3.9.8 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 4cb1-6c91-52a0
```

3.9.9 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 on 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 on 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 on the previous AS.
- Only a standalone AS can be replaced, and a stacked AS 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
```

Related Topics

3.9.99 uni-mng

3.9.10 as-mode disable

Function

The **as-mode disable** command changes the device working mode to the parent mode.

The **undo as-mode disable** command restores the device working mode to the AS mode.

By default, the device works in AS mode.

NOTE

This command is only supported by S6720SI, S6720S-SI, S6720EI, and S6720S-EI.

Format

as-mode disable

undo as-mode disable

Parameters

None

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

The S6720SI, S6720S-SI, S6720EI, and S6720S-EI can function as the parent or AS in an SVF system. By default, the device works in AS mode and functions only as an AS. To use the device as the parent, run the **as-mode disable** command. This command will change the device working mode to the parent mode.

Precautions

After the working mode of a device is changed, the device does not use any configuration file at the next startup.

Example

# Change the device 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 s
ystem. Continue? [Y/N]:y
```

3.9.11 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
```

Related Topics

3.9.6 as-group name

3.9.12 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 one only 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
```

Related Topics

3.9.6 as-group name

3.9.13 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. The interface type can be Eth-Trunk interface. ● *interface-number1* specifies the first interface number. ● *interface-number2* specifies the last interface number.	-
all	Indicates all downlink service 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.

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
```

Related Topics

3.9.80 port-group name

3.9.14 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 an 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.
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.

Example

# Configure an AS name.

```
<HUAWEI> system-view
[HUAWEI] uni-mng
[HUAWEI-um] as name as1 model S5700-28P-LI-AC mac-address 0200-0000-0022
```

Related Topics

3.9.99 uni-mng

3.9.15 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
```

Related Topics

3.9.99 uni-mng

3.9.16 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
```

3.9.17 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 larger 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.

Example

# Create the service VLAN 10 for ASs.

```
<HUAWEI> system-view
[HUAWEI] uni-mng
[HUAWEI-um] as service-vlan authorization 10
```

3.9.18 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 using the **as type** command. If no file is specified, the system searches the root directory unimng/ of the parent for a system software file applicable to the AS.

Precautions

You can run the **as type** command multiple times to specify different files for different types of ASs.

Example

# Specify the file to be loaded on the AS of the S5700-P-LI type.

```
<HUAWEI> system-view
[HUAWEI] uni-mng
[HUAWEI-um] as type s5700-p-li system-software s5700-p-li-v200r011c10.cc
```

Related Topics

3.9.99 uni-mng

3.9.19 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 Pwd@123456
[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 Pwd@123456
[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
```

3.9.20 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 512. After the value is delivered to an AS, the effective value depends on the AS specifications. For details, see **13.6.5 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
```

Related Topics

3.9.108 user-access-profile name

3.9.21 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.

Example

# Configure no authentication for ASs to connect to an SVF system.

```
<HUAWEI> system-view
[HUAWEI] as-auth
[HUAWEI-as-auth] auth-mode none
```

Related Topics

3.9.5 as-auth

3.9.22 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 profile used in Portal authentication in the Portal access profile view. Additionally, only one Portal server profile 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**.
- Different user access profiles must be bound to the same authentication profile.
- 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.

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 huawei
[HUAWEI-um-user-access-huawei] authentication-profile test
```

Related Topics

3.9.108 user-access-profile name

3.9.23 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 0025-9e07-8281 to the blacklist.

```
<HUAWEI> system-view
[HUAWEI] as-auth
[HUAWEI-as-auth] blacklist mac-address 0025-9e07-8281
```

Related Topics

3.9.5 as-auth

3.9.24 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
```

Related Topics

3.9.74 network-enhanced-profile name

3.9.25 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
```

Related Topics

3.9.31 direct-command

3.9.26 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.

Example

# Deliver the service configuration to all ASs.

```
<HUAWEI> system-view
[HUAWEI] uni-mng
[HUAWEI-um] commit as all
```

Related Topics

3.9.48 display uni-mng commit-result

3.9.27 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 **3.9.36 display as unauthorized record** command to check information about the ASs that fail the authentication.

Example

# Confirm that the AS with the MAC address 0025-9e07-8280 passes the authentication.

```
<HUAWEI> system-view
[HUAWEI] as-auth
[HUAWEI-as-auth] confirm mac-address 0025-9e07-8280
```

Related Topics

3.9.5 as-auth

3.9.36 display as unauthorized record

3.9.28 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
```

Related Topics

3.9.68 interface fabric-port

3.9.29 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
```

Related Topics

3.9.80 port-group name

3.9.30 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
```

Related Topics

3.9.74 network-enhanced-profile name

3.9.31 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 service configurations that can be delivered using this 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** | *interface-type interface-number* | **stack-port** *member-id/port-id* } **command** *command-text*

undo direct-command view { **system** | *interface-type interface-number* | **stack-port** *member-id/port-id* } **command** *command-text*

Parameters

Parameter	Description	Value
view { **system** | *interface-type interface-number* }	Specifies the view in which a command is executed. ● **system**: system view ● *interface-type interface-number*: interface view. It cannot be an Eth-Trunk interface view. ● **stack-port** *member-id/port-id*: stack interface view	-
command *command-text*	Specifies the command to be delivered to ASs.	The value is a string of 1 to 64 characters.

Views

AS view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

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.	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** { **10** | **100** | **1000** } or **duplex** { **full** | **half** } is specified.

Service Category	Format	View	Function	Configuration Dependency and Restriction
	speed { **10** | **100** | **1000** }	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.	-
	description *description* (supported in V200R011C10 and later versions)	Interface view	Configures the description for an interface.	The description contains a maximum of 52 characters.

Service Category	Format	View	Function	Configuration Dependency and Restriction
Port bridge	**port bridge enable**	Interface view	Enables the bridging function on an interface.	-
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.	-
	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 the S5720EI, S6720S-EI, and S6720EI support this command. ● The value of **maximum** *maximum* ranges from 0 to 256. ● This function takes effect only for the ARP packets sent to the CPU.
	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.

Service Category	Format	View	Function	Configuration Dependency and Restriction
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 physical member port and adds it to a stack port.	Before restoring the physical 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.

Precautions

- 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.
- A maximum of 4096 commands can be configured.

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
```

Related Topics

3.9.25 clear direct-command

3.9.32 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    S5700-P-LI     aaaa-bbbb-cc92 192.168.11.254  normal       as1
-------------------------------------------------------------------------------
```

Table 3-99 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       : aaaa-bbbb-cc92
System MAC           : aaaa-bbbb-cc92
ESN                  : 2102353173107C800132
Name                 : as1
Model                : S5700-28P-LI-AC
Device type          : S5700-P-LI
State                : normal
Mode                 : centralized
Slot                 : 0
AS group             : group1
```

```
Port group          : group2
--------------------------------------------------------------------------------
```

Table 3-100 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.
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 3-101 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.

3.9.33 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                : 0200-0000-0022
   Access system MAC                    : 0200-0000-0022
   Current connected state              : normal
```

Table 3-102 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. This field is only supported on S6720SI, S6720S-SI, S6720EI, and S6720S-EI. ● 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.
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.
Access management MAC	Configured management MAC address of an AS.
Access system MAC	System MAC address of an AS.

Item	Description
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.

3.9.34 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     0025-9e07-8281
```

```
--------------------------------------------------------------------------------
Total: 1
```

Table 3-103 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.

3.9.35 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.
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 5.160 V200R011C10
Hardware version     : VER.A
Patch version        : V200R011SPH001
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 3-104 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.
Patch state	Patch status. ● Running: The patch is running. ● not running: The patch is not running. This field displays**--** when the **Patch version** field displays **--**.
IP address	IP address of an AS.
IP mask	Subnet mask.
Gateway	Gateway of an AS.
VPN-Instance	Name of a VPN instance.

Item	Description
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

3.9.36 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      : huawei-000b-0987-d5aa
AS MAC address : 000b-0987-d5aa
AS IP address  : 192.168.1.253
Record time    : 2015-05-20 16:06:10 DST
-------------------------------------------------------------------------------
Total: 1
```

Table 3-105 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.

3.9.37 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      0025-9e07-8282
--------------------------------------------------------------------------------
Total: 1
```

Table 3-106 Description of the **display as whitelist** command output

Item	Description
ID	ID of a whitelist.
MAC	MAC address added to the whitelist.

3.9.38 display snmp-agent trap feature-name asmngtrap all

Function

display snmp-agent trap feature-name asmngtrap all command displays the status of all traps for the ASMNGTRAP module.

NOTE

This command can only be executed on a parent switch.

Format

display snmp-agent trap feature-name asmngtrap all

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

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

Prerequisites

SNMP has been enabled. For details, see **snmp-agent**.

Example

# Display all the traps of the ASMNGTRAP module.

```
<HUAWEI>display snmp-agent trap feature-name asmngtrap all
------------------------------------------------------------------------------
Feature name: ASMNGTRAP
Trap number : 23
------------------------------------------------------------------------------
Trap name                     Default switch status   Current switch status
hwAsFaultNotify                   on                      on
hwAsNormalNotify                  on                      on
hwAsAddOffLineNotify              on                      on
hwAsDelOffLineNotify              on                      on
hwAsPortStateChangeToDownNotify
                                  on                      on
hwAsPortStateChangeToUpNotify     on                      on
hwAsModelNotMatchNotify           on                      on
hwAsVersionNotMatchNotify         on                      on
hwAsNameConflictNotify            on                      on
hwAsSlotModelNotMatchNotify       on                      on
hwAsFullNotify                    on                      on
hwUnimngModelNotMatchNotify       on                      on
hwAsBoardAdd                      on                      on
hwAsBoardDelete                   on                      on
hwAsBoardPlugIn                   on                      on
hwAsBoardPlugOut                  on                      on
hwAsInBlacklist                   on                      on
hwAsUnconfirmed                   on                      on
hwAsComboPortTypeChange           on                      on
hwAsOnlineFailNotify              on                      on
hwAsSlotIdInvalidNotify           on                      on
hwAsSysmacSwitchCfgErrNotify      on                      on
hwAsSlotOnlineFailNotify          on                      on
```

Table 3-107 Description of the **display snmp-agent trap feature-name asmngtrap all** command output

Item	Description
Feature name	Name of the module that the trap belongs to.

Item	Description
Trap number	Number of traps.
Trap name	Trap name of the module: ● hwAsFaultNotify: An AS goes offline. ● hwAsNormalNotify: An AS goes online. ● hwAsAddOffLineNotify: An AS has been added offline. ● hwAsDelOffLineNotify: An AS has been deleted offline. ● hwAsPortStateChangeToDownNotify: An AS port goes Down. ● hwAsPortStateChangeToUpNotify: An AS port goes Up. ● hwAsModelNotMatchNotify: The actual AS model does not match the configured one. ● hwAsVersionNotMatchNotify: The AS version does not match. ● hwAsNameConflictNotify: The AS name conflicts. ● hwAsSlotModelNotMatchNotify: An AS has a different SVF enabling status than the parent. ● hwAsFullNotify: The number of ASs reaches the maximum value. ● hwUnimngModelNotMatchNotify: The model of a new device in the AS stack system differs from the configured model. ● hwAsBoardAdd: An AS slot has been added. ● hwAsBoardDelete: An AS slot has been deleted. ● hwAsBoardPlugIn: A new member has joined an AS stack system. ● hwAsBoardPlugOut: A member has left an AS stack system. ● hwAsInBlacklist: An AS is in the blacklist. ● hwAsUnconfirmed: An AS fails authentication. ● hwAsComboPortTypeChange: The AS interface type has changed. ● hwAsOnlineFailNotify: An AS fails to go online. ● hwAsSlotIdInvalidNotify: An AS slot ID is invalid. ● hwAsSysmacSwitchCfgErrNotify: The MAC address switching mode of the AS stack system is not set to non-switching. ● hwAsSlotOnlineFailNotify: When an AS is a stack, some member switches in the stack fail to go online.
Default switch status	Default status of the trap function: ● on: The trap function is enabled. ● off: The trap function is disabled.
Current switch status	Status of the trap function: ● on: The trap function is enabled. ● off: The trap function is disabled.

Related Topics

3.9.89 snmp-agent trap enable feature-name asmngtrap

3.9.39 display snmp-agent trap feature-name unimbrtrap all

Function

display snmp-agent trap feature-name unimbrtrap all command displays the status of all traps on the UNIMBRTRAP module.

NOTE

This command can only be executed on a parent switch.

Format

display snmp-agent trap feature-name unimbrtrap all

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

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

Prerequisites

SNMP has been enabled. For details, see **snmp-agent**.

Example

# Display all the traps of the UNIMBRTRAP module.

```
<HUAWEI>display snmp-agent trap feature-name unimbrtrap all
------------------------------------------------------------------------------
Feature name: UNIMBRTRAP
Trap number : 30
------------------------------------------------------------------------------
```

```
Trap name                      Default switch status   Current switch status
hwASBrdTempAlarm                    on                   on
hwASBrdTempResume                     on                   on
hwASBoardFail                    on                   on
hwASBoardFailResume                  on                   on
hwASBoardInvalid                  on                   on
hwASBoardInvalidResume                on                   on
hwASOpticalInvalid                on                   on
hwASOpticalInvalidResum               on                   on
hwASPowerRemove                      on                   on
hwASPowerInsert                   on                   on
hwASPowerInvalid                  on                   on
hwASPowerInvalidResum                 on                   on
hwASFanRemove                       on                   on
hwASFanInsert                    on                   on
hwASFanInvalid                   on                   on
hwASFanInvalidResume                 on                   on
hwASCommunicateError                  on                   on
hwASCommunicateResume                    on                   on
hwASCPUUtilizationRising             on                   on
hwASCPUUtilizationResume               on                   on
hwASMemUtilizationRising              on                   on
hwASMemUtilizationResume                on                   on
hwASMadConflictDetect                on                   on
hwASMadConflictResume                  on                   on
hwUniMbrLinkStateChange                on                   on
hwUniMbrASDiscoverAttack               on                   on
hwUniMbrConnectError                 on                   on
hwUniMbrIllegalFabricConfig           on                   on
hwUniMbrFabricPortMemberDelete  on                   on
hwUniMbrAsServiceAbnormal               on                   on
```

Table 3-108 Description of the display snmp-agent trap feature-name unimbrtrap all command output

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

Item	Specification
Trap name	Trap name. Traps of the UNIMBRTRAP module include: ● hwASBoardFail: An AS becomes unavailable partially. ● hwASBoardFailResume: An AS becomes available. ● hwASBoardInvalid: An AS is invalid. ● hwASBoardInvalidResume: An AS is valid. ● hwASBrdTempAlarm: The AS temperature is out of the normal range. ● hwASBrdTempResume: The AS temperature restores to the normal range. ● hwASCommunicateError: A communication fault occurs. ● hwASCommunicateResume: A communication fault is rectified. ● hwASCPUUtilizationResume: The AS CPU usage falls below the threshold. ● hwASCPUUtilizationRising: The AS CPU usage exceeds the threshold. ● hwASFanInsert: An AS fan module is installed. ● hwASFanInvalid: An AS fan module becomes unavailable completely. ● hwASFanInvalidResume: An AS fan module becomes available. ● hwASFanRemove: An AS fan module is removed. ● hwASMadConflictDetect: A MAD conflict is detected. ● hwASMadConflictResume: A MAD conflict is resolved. ● hwASMemUtilizationResume: The AS memory usage restores to the normal range. ● hwASMemUtilizationRising: The AS memory usage exceeds the threshold. ● hwASOpticalInvalid: The AS optical module is invalid. ● hwASOpticalInvalidResum: The AS optical module is valid. ● hwASPowerInsert: An AS power module is installed. ● hwASPowerInvalid: An AS power module is invalid. ● hwASPowerInvalidResum: An AS power module is valid.

Item	Specification
	● hwASPowerRemove: An AS power module is removed. ● hwUniMbrASDiscoverAttack: An AS discovers attacks. ● hwUniMbrConnectError: Cable connection of a fabric port is incorrect. ● hwUniMbrFabricPortMemberDelete: A member port of a fabric port is removed. ● hwUniMbrIllegalFabricConfig: The fabric port configuration is invalid. ● hwUniMbrLinkStateChange: The connection status changes. ● hwUniMbrAsServiceAbnormal: Services on an AS become abnormal.
Default switch status	Default status of the trap function: ● on: indicates that the trap function is enabled by default. ● off: indicates that the trap function is disabled by default.
Current switch status	Status of the trap function: ● on: indicates that the trap function is enabled. ● off: indicates that the trap function is disabled.

Related Topics

3.9.90 snmp-agent trap enable feature-name unimbrtrap

3.9.40 display snmp-agent trap feature-name uni-topomng all

Function

display snmp-agent trap feature-name uni-topomng all command displays the status of all traps on the UNI-TOPOMNG module.

NOTE

This command can only be executed on a parent switch.

Format

display snmp-agent trap feature-name uni-topomng all

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

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

Prerequisites

SNMP has been enabled. For details, see **snmp-agent**.

Example

# Display all the traps of the UNI-TOPOMNG module.

```
<HUAWEI>display snmp-agent trap feature-name uni-topomng all
------------------------------------------------------------------------------
Feature name: uni-topomng
Trap number : 2
------------------------------------------------------------------------------
Trap name                       Default switch status   Current switch status
hwTopomngLinkNormal                  on                      on
hwTopomngLinkAbnormal                 on                      on
```

Table 3-109 Description of the display snmp-agent trap feature-name uni-topomng all command output

Item	Specification
Feature name	Name of the module that the trap belongs to.
Trap number	Number of traps.
Trap name	Trap name. Traps of the UNI-TOPOMNG module include: ● hwTopomngLinkNormal: The connection status becomes normal. ● hwTopomngLinkAbnormal: A connection fault occurs.
Default switch status	Default status of the trap function: ● on: indicates that the trap function is enabled by default. ● off: indicates that the trap function is disabled by default.

Item	Specification
Current switch status	Status of the trap function: ● on: indicates that the trap function is enabled. ● off: indicates that the trap function is disabled.

Related Topics

3.9.91 snmp-agent trap enable feature-name uni-topomng

3.9.41 display snmp-agent trap feature-name uni-tplm all

Function

display snmp-agent trap feature-name uni-tplm all command displays the status of all traps on the UNI-TPLM module.

NOTE

This command can only be executed on a parent switch.

Format

display snmp-agent trap feature-name uni-tplm all

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

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

Prerequisites

SNMP has been enabled. For details, see **snmp-agent**.

Example

# Display all the traps of the UNI-TPLM module.

```
<HUAWEI>display snmp-agent trap feature-name uni-tplm all
------------------------------------------------------------------------------
Feature name: uni-tplm
Trap number : 3
------------------------------------------------------------------------------
Trap name                        Default switch status   Current switch status
hwTplmCmdExecuteFailedNotify     on                      on
hwTplmCmdExecuteSuccessfulNotify
                                 on                      on
hwTplmDirectCmdRecoverFail       on                      on
```

Table 3-110 Description of the display snmp-agent trap feature-name uni-tplm all command output

Item	Specification
Feature name	Name of the module that the trap belongs to.
Trap number	Number of traps.
Trap name	Trap name. Traps of the UNI-TPLM module include: ● hwTplmCmdExecuteFailedNotify: The command fails to be executed on the AS. ● hwTplmCmdExecuteSuccessfulNotify: The command is executed successfully on the AS. ● hwTplmDirectCmdRecoverFail: Configurations of the commands directly configured on the parent for the AS fail to be restored.
Default switch status	Default status of the trap function: ● on: indicates that the trap function is enabled by default. ● off: indicates that the trap function is disabled by default.
Current switch status	Status of the trap function: ● on: indicates that the trap function is enabled. ● off: indicates that the trap function is disabled.

Related Topics

3.9.92 snmp-agent trap enable feature-name uni-tplm

3.9.42 display snmp-agent trap feature-name uni-vermng all

Function

display snmp-agent trap feature-name uni-vermng all command displays the status of all traps on the UNI-VERMNG module.

NOTE

This command can only be executed on a parent switch.

Format

display snmp-agent trap feature-name uni-vermng all

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

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

Prerequisites

SNMP has been enabled. For details, see **snmp-agent**.

Example

# Display all the traps of the UNI-VERMNG module.

```
<HUAWEI>display snmp-agent trap feature-name uni-vermng all
------------------------------------------------------------------------------
Feature name: uni-vermng
Trap number : 1
------------------------------------------------------------------------------
Trap name                     Default switch status   Current switch status
hwVermngUpgradeFail                on                      on
```

Table 3-111 Description of the display snmp-agent trap feature-name uni-vermng all command output

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

Item	Specification
Trap name	Trap name. Traps of the UNI-VERMNG module include: ● hwVermngUpgradeFail: An AS fails to be upgraded.
Default switch status	Default status of the trap function: ● on: indicates that the trap function is enabled by default. ● off: indicates that the trap function is disabled by default.
Current switch status	Status of the trap function: ● on: indicates that the trap function is enabled. ● off: indicates that the trap function is disabled.

Related Topics

3.9.93 snmp-agent trap enable feature-name uni-vermng

3.9.43 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: 0 to 255 ● S7712 (SRUE/SRUH)/S7706 (SRUE/SRUH): 0 to 255 ● S9312 (SRUE/SRUH)/S9310/S9306(SRUE/SRUH)/S9310X: 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
-------------------------------------------------------------------------------
GE9/0/19     AS Discover Request          0              2
             AS Discover ACK              1              0
             AS Discover ParaSyn Req      0              1
             AS Discover ParaSyn ACK      1              0
             AS Discover HeartBeat Req    0              210
             AS Discover HeartBeat ACK    210            0
             AS Discover NAK              0              0
             AS Discover FabricCfg Req    0              0
             AS Discover FabricCfg ACK    0              0
-------------------------------------------------------------------------------
```

Table 3-112 Description of the **display uni-mng as-discover packet statistics** command output

Item	Description
PortName	Name of a member port in a fabric port.

Item	Description
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
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.
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.

Related Topics

3.9.86 reset uni-mng as-discover packet statistics

3.9.44 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 3-113 Description of the **display uni-mng as-group** command output

Item	Description
Number	Sequence number.

Item	Description
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 3-114 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.

3.9.45 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
-------------------------------------------------------------------------------
Index     MAC-Current          MAC-Saved          Name
-------------------------------------------------------------------------------
1         aaaa-bbbb-cc92       aaaa-bbbb-cc92     as1
-------------------------------------------------------------------------------
Total: 1
```

Table 3-115 Description of the **display uni-mng as index** command output

Item	Description
Index	Index of an AS.
MAC-Current	Management MAC address.
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.

3.9.46 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
------------------------------------------------------------------------------
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 3-116 Description of the **display uni-mng as interface brief** command output

Item	Description
Interface	Interface number.
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.
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

Item	Description
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.

3.9.47 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 3-117 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.
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.

Item	Description
The Number of UP Ports in Trunk	Number of Eth-Trunk member interfaces in Up state.

3.9.48 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 3-118 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.

3.9.49 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
```

Table 3-119 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.

3.9.50 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 3-120 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.

3.9.51 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 3-121 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.

3.9.52 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 3-122 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.

3.9.53 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                      : 0000-1382-4569
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 3-123 Description of the **display uni-mng interface fabric-port state** command output

Item	Description
Fabric-port name	Fabric port name.

Item	Description
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 3-124**.
Exptime(s)	Timeout period of link heartbeat packets, in seconds.

Table 3-124 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.
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.

Detail Field	Meaning	Solution
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.
Failed to create Eth-Trunk	Failed to create an Eth-Trunk on an AS.	Disconnect the AS from the parent and then reconnect them.

Detail Field	Meaning	Solution
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 S2750EI 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.

3.9.54 display uni-mng patch-delete info

Function

The **display uni-mng patch-delete info** command displays information about the operation of deleting patches on ASs.

NOTE

This command can only be executed on a parent switch.

Format

display uni-mng patch-delete info

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After patches on a specified AS are deleted using the **patch delete as** command, you can use the **display uni-mng patch-delete info** command to view information about the operation of deleting the patches.

Example

# Display information about the operation of deleting patches on ASs.

```
<HUAWEI> display uni-mng patch-delete info
Total: 7
-------------------------------------------------------------------------------
AS Name                          Result          Time
-------------------------------------------------------------------------------
e-10005(1-1)                      successful      2014-09-04  15:51:05 DST
t-10021(1-s)                     failed          2014-09-04  15:51:05
m-10018(x-1)                      deleting        2014-09-04  15:51:05
p-10017(2-2)                      expired         2014-09-04  15:51:05
6-10016(2-1)                      successful      2014-09-04  15:51:05
7-10015(2-2)                      successful      2014-09-04  15:51:05
2-10011(2-1)                      --              --
-------------------------------------------------------------------------------
```

Table 3-125 Description of the **display uni-mng patch-delete info** command output

Item	Description
Total	Number of ASs.
AS Name	Name of an AS.

Item	Description
Result	Result of the operation of deleting patches: ● successful: Patches are deleted successfully. ● failed: Patches fail to be deleted. ● deleting: Patches are being deleted. ● expired: Deleting patches expires. After the operation of deleting patches is delivered, if no operation result is received within 2 minutes, the **Result** field displays **expired**. ● --: No records of the deletion operation are available.
Time	Time for the last operation.

Related Topics

3.9.77 patch delete as

3.9.55 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 3-126 Description of the **display uni-mng port-group** command output

Item	Description
Number	Sequence number.
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

# 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       : --
-------------------------------------------------------------------------------
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    : --
```

```
User-access profile        : --
-------------------------------------------------------------------------------
```

Table 3-127 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 --.
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 --.
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 --.

3.9.56 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** } [**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.	-
user-access	Displays information about user access 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
--------------------------------------------------------------------------------

User-access profile:
--------------------------------------------------------------------------------
 Number                        Profile Name
--------------------------------------------------------------------------------
 1                         u_pro
--------------------------------------------------------------------------------
```

Table 3-128 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.
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 3-129 Description of the **display uni-mng profile network-basic name** command output

Item	Description
Profile Name	Name of a service profile.

Item	Description
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.

3.9.57 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.

Parameter	Description	Value
interface *interface-type interface-number*	Displays the configuration of a specified interface: ● *interface-type* specifies the interface type. The interface type can be Eth-Trunk interface. ● *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.

Example

# Display the configuration generated on an AS.

```
<HUAWEI> display uni-mng profile as name as1

Global
-------------------------------------------------------------------------------
Centralized forward mode: disable
-------------------------------------------------------------------------------
Portal url-encode: disable
-------------------------------------------------------------------------------
AS-group name: xy
 Username: admin
  Privilege-level   : 3
  Service-type      : terminal ssh
 Traffic-limit outbound ARP(Kbps)  : 512
 Traffic-limit outbound DHCP(Kbps) : 128
-------------------------------------------------------------------------------

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)                 : --

 Authentication                   : --
 Authentication maximum user-num  : --
 MAC-limit                        : --
 Traffic-limit inbound ARP(Kbps)  : --
 Traffic-limit inbound DHCP(Kbps) : --
-------------------------------------------------------------------------------

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)                 : --

 Authentication                   : --
 Authentication maximum user-num  : --
 MAC-limit                        : --
 Traffic-limit inbound ARP(Kbps)  : --
 Traffic-limit inbound DHCP(Kbps) : --
-------------------------------------------------------------------------------
......
```

Table 3-130 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.
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.
Service-type	User access type. The value is terminal ssh and cannot be changed.
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 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.

Item	Description
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.
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.

Item	Description
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 detection function is enabled: ● disable: The dynamic ARP detection function is disabled in a network enhanced profile. ● enable: The dynamic ARP detection function is enabled in a network enhanced profile. To enable the dynamic ARP detection 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.
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.
Authentication	User authentication profile created using the **authentication-profile** command.

Item	Description
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.

3.9.58 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 3-131 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.

3.9.59 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
-----------------------------------------------------------------------------
 00e0-0987-7890  0    GE6/1/0         11 <-->0   GE0/0/26       00e0-0001-0008*
 00e0-0001-0008  1    GE0/0/2         -- <-->--  GE0/0/0        00e0-0001-0005
-----------------------------------------------------------------------------
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 3-132 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.
Peer Dev	Peer device name. If * is displayed, the AS is configured in the independent mode.

3.9.60 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
-------------------------------------------------------------------------------
0001-c002-c302    212   1.1.1.1         Ge1/0/1      test1
000b-099a-8a3d    212   1.1.1.2         Ge1/0/1      test1
0010-0020-0004    212   1.1.1.3         Ge1/0/1      test1
0200-0000-0000    212   1.1.1.4         Ge1/0/1      test1
4cb1-6c91-52a1    212   1.1.1.5         Ge1/0/1      test1
-------------------------------------------------------------------------------
```

Table 3-133 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.

3.9.61 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             : 0021-9746-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             : 0021-9746-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 3-134 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.

Item	Description
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.

3.9.62 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.
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 3-135 Description of the **display uni-mng upgrade-info** command output

Item	Description
Name	Name of an AS.
Method	Upgrade mode of the AS: ● --: 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.
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
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 succeeds. ● 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                    : NO-UPGRADE
 Startup system-software        : flash:/s5700-p-li-v200r011c10.cc
 Startup version                : V200R011C10
 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            : 2016-07-04  15:51:05
--------------------------------------------------------------------------------
```

Table 3-136 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 software software.
Startup version	Current software version.
Startup patch	Running patch file. If this field displays --, no patch file is running.

Item	Description
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.
Download patch	Downloaded patch file. If this field displays --, the upgrade task is not started.
Method	Upgrade mode of the AS: ● --: 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.
Last operation result	Upgrade result: ● --: The upgrade task is not started. ● successful: The upgrade succeeds. ● failed: The upgrade fails.

Item	Description
Error reason	Upgrade failure reason.
Last operation time	Last time the AS is upgraded.

3.9.63 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 3-137 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.

3.9.64 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.	-

Parameter	Description	Value
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
```

Related Topics

3.9.14 as name (uni-mng view)

3.9.99 uni-mng

3.9.81 port eth-trunk trunkmember

3.9.65 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 and need to enter the default password. 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. The default password has security risks. You are advised to change the login password.

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.

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
```

3.9.66 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.
- After an AS goes offline, downlink ports of the AS are automatically shut down. As a result, traffic of the AS attached network will be interrupted.

Example

# Set the SVF forwarding mode to centralized forwarding.

```
<HUAWEI> system-view
[HUAWEI] uni-mng
[HUAWEI-um] forward-mode centralized
```

Related Topics

3.9.99 uni-mng

3.9.67 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-name	Specifies a user name.	The value is a string of 1 to 64 case-insensitive characters. It cannot contain spaces, asterisk, double quotation mark and question mark.
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. The newly configured password cannot be the default password of local users.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.

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 Pwd@123456
```

3.9.68 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.	● When the S12700 functions as a parent switch, the value ranges from 0 to 255. ● When the S9300X functions as a parent switch, the value ranges from 0 to 255. ● When the S9700 functions as a parent switch, the value ranges from 0 to 63. ● When the S7700 functions as a parent switch, the value ranges from 0 to 255 when it uses SRUE or SRUH or ranges from 0 to 63 when it uses other cards. ● When the S9300 functions as a parent switch, the value ranges from 0 to 255 when it uses SRUE, SRUH or SRUK or ranges from 0 to 63 when it uses other cards. ● When the S9300E functions as a parent switch, the value ranges from 0 to 63. ● When the S5720HI, S6720EI and S6720S-EI function as parent switches, the value ranges from 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
```

Related Topics

3.9.82 port member-group interface

3.9.69 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 S2750EI, 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
```

Related Topics

3.9.74 network-enhanced-profile name

3.9.70 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
```

Related Topics

3.9.108 user-access-profile name

3.9.71 multicast-suppression (network enhanced profile view)

Function

The **multicast-suppression** command configures multicast traffic suppression in a network enhanced profile.

The **undo multicast-suppression** command cancels multicast traffic suppression in a network enhanced profile.

By default, 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 multicast traffic suppression in the profile. After the profile is bound to an AS port, 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 multicast packets that can pass through a port. When the multicast traffic rate reaches the maximum value, the system discards excess multicast packets to control the traffic volume within a proper range.

Example

# Configure 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
```

Related Topics

3.9.74 network-enhanced-profile name

3.9.72 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
```

Related Topics

3.9.110 user-vlan (network basic profile view)

3.9.76 pass-vlan (network basic profile view)

3.9.112 voice-vlan (network basic profile view)

3.9.73 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
```

Related Topics

3.9.72 network-basic-profile name

3.9.80 port-group name

3.9.74 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
```

Related Topics

3.9.24 broadcast-suppression (network enhanced profile view)

3.9.71 multicast-suppression (network enhanced profile view)

3.9.103 unicast-suppression (network enhanced profile view)

3.9.30 dhcp snooping enable (network enhanced profile view)

3.9.69 ip source check user-bind enable (network enhanced profile view)

3.9.2 arp anti-attack check user-bind enable (network enhanced profile view)

3.9.84 rate-limit (network enhanced profile view)

3.9.107 user-access-port enable (network enhanced profile view)

3.9.75 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
```

Related Topics

3.9.74 network-enhanced-profile name

3.9.80 port-group name

3.9.76 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
```

Related Topics

3.9.72 network-basic-profile name

3.9.77 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
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...
```

Related Topics

3.9.54 display uni-mng patch-delete info

3.9.78 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.
- 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.
- 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 3-138 Commands that may cause an AS to go offline

Command
loopback internal
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
port-security enable

- 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 3-139 Commands that can not be manually deleted in an Eth-Trunk

Command
port link-type hybrid
port hybrid tagged vlan

Table 3-140 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
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
```

Related Topics

3.9.68 interface fabric-port

3.9.79 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 **3.9.82 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
```

Related Topics

3.9.68 interface fabric-port

3.9.80 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 S6720EI, S6720S-EI, S6720SI, and S6720S-SI.

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 three types of service profiles (network basic profile, network enhanced profile, and user access 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 groups.

Example

# Create a port group.

```
<HUAWEI> system-view
[HUAWEI] uni-mng
[HUAWEI-um] port-group name group_1
```

Related Topics

3.9.13 as name interface (port group view)

3.9.73 network-basic-profile (port group view)

3.9.75 network-enhanced-profile (port group view)

3.9.109 user-access-profile (port group view)

3.9.81 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 S6720EI 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
```

Related Topics

3.9.14 as name (uni-mng view)

3.9.64 down-direction fabric-port

3.9.99 uni-mng

3.9.82 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

- 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
```

Related Topics

3.9.99 uni-mng

3.9.68 interface fabric-port

3.9.83 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 redirected 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
```

3.9.84 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: ● Ethernet interface: 64 to 100000 ● GE interface: 64 to 1000000 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 S2750EI, 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
```

Related Topics

3.9.74 network-enhanced-profile name

3.9.85 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
```

3.9.86 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: 0 to 255 ● S7712 (SRUE/SRUH)/S7706 (SRUE/SRUH): 0 to 255 ● S9312 (SRUE/SRUH)/S9310/S9306(SRUE/SRUH)/S9310X: 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
```

Related Topics

3.9.43 display uni-mng as-discover packet statistics

3.9.87 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
```

Related Topics

3.9.99 uni-mng

3.9.14 as name (uni-mng view)

3.9.88 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
```

Related Topics

3.9.99 uni-mng

3.9.14 as name (uni-mng view)

3.9.89 snmp-agent trap enable feature-name asmngtrap

Function

snmp-agent trap enable feature-name asmngtrap command enables the trap function for the ASMNGTRAP module.

undo snmp-agent trap enable feature-name asmngtrap command disables the trap function for the ASMNGTRAP module.

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

NOTE

This command can only be executed on a parent switch.

Format

snmp-agent trap enable feature-name asmngtrap [**trap-name** *trap-name*]

undo snmp-agent trap enable feature-name asmngtrap [**trap-name** *trap-name*]

Parameters

Parameter	Description	Value
trap-name	Enables or disables the trap function for a specified event.	● **hwasaddofflinenotify**: the trap for the event that an AS is added offline. ● **hwasboardadd**: the trap for the event that an AS slot is added. ● **hwasboarddelete**: the trap for the event that an AS slot is deleted. ● **hwasboardplugin**: the trap for the event that a new member joins an AS stack system. ● **hwasboardplugout**: the trap for the event that a member leaves an AS stack system. ● **hwascomboporttypechange**: the trap for the event that the AS interface type changes. ● **hwasdelofflinenotify**: the trap for the event that an AS is deleted offline. ● **hwasfaultnotify**: the trap for the event that an AS goes offline. ● **hwasfullnotify**: the trap for the event that the number of ASs reaches the maximum value. ● **hwasinblacklist**: the trap for the event that an AS is in the blacklist. ● **hwasmodelnotmatchnotify**: the trap for the event that the actual AS model does not match the configured one. ● **hwasnameconflictnotify**: the trap for the event that the AS name conflicts. ● **hwasnormalnotify**: the trap for the event that an AS goes online. ● **hwasonlinefailnotify**: the trap for the event that an AS fails to go online. ● **hwasportstatechangetodownnotify**: the trap for the event that an AS port goes Down. ● **hwasportstatechangetoupnotify**: the trap for the event that an AS port goes Up. ● **hwasslotidinvalidnotify**: the trap for the event that an AS slot ID is invalid. ● **hwasslotmodelnotmatchnotify**: the trap for the event that the model of a new device in the AS stack system differs from the configured model. ● **hwassysmacswitchcfgerrnotify**: the trap for the event that the MAC address switching

Parameter	Description	Value
		mode of the AS stack system is not set to non-switching. - **hwasunconfirmed**: the trap for the event that an AS fails authentication. - **hwasversionnotmatchnotify**: the trap for the event that the AS version does not match. - **hwunimngmodelnotmatchnotify**: the trap for the event that an AS has a different SVF enabling status than the parent. - **hwasslotonlinefailnotify**: the trap for the event that some member switches in a stack fail to go online when this stack is an AS.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

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

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

Example

# Enable the hwasaddofflinenotify trap of the ASMNGTRAP module.

```
<HUAWEI> system-view
[HUAWEI] snmp-agent trap enable feature-name asmngtrap trap-name hwasaddofflinenotify
```

Related Topics

3.9.38 display snmp-agent trap feature-name asmngtrap all

3.9.90 snmp-agent trap enable feature-name unimbrtrap

Function

snmp-agent trap enable feature-name unimbrtrap command enables the trap function for the UNIMBRTRAP module.

undo snmp-agent trap enable feature-name unimbrtrap command disables the trap function for the UNIMBRTRAP module.

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

NOTE

This command can only be executed on a parent switch.

Format

snmp-agent trap enable feature-name unimbrtrap [**trap-name** { **hwasboardfail** | **hwasboardfailresume** | **hwasboardinvalid** | **hwasboardinvalidresume** | **hwasbrdtempalarm** | **hwasbrdtempresume** | **hwascommunicateerror** | **hwascommunicateresume** | **hwascpuutilizationresume** | **hwascpuutilizationrising** | **hwasfaninsert** | **hwasfaninvalid** | **hwasfaninvalidresume** | **hwasfanremove** | **hwasmadconflictdetect** | **hwasmadconflictresume** | **hwasmemutilizationresume** | **hwasmemutilizationrising** | **hwasopticalinvalid** | **hwasopticalinvalidresum** | **hwaspowerinsert** | **hwaspowerinvalid** | **hwaspowerinvalidresum** | **hwaspowerremove** | **hwunimbrasdiscoverattack** | **hwunimbrconnecterror** | **hwunimbrfabricportmemberdelete** | **hwunimbrillegalfabricconfig** | **hwunimbrlinkstatechange** | **hwunimbrasserviceabnormal** }]

undo snmp-agent trap enable feature-name unimbrtrap [**trap-name** { **hwasboardfail** | **hwasboardfailresume** | **hwasboardinvalid** | **hwasboardinvalidresume** | **hwasbrdtempalarm** | **hwasbrdtempresume** | **hwascommunicateerror** | **hwascommunicateresume** | **hwascpuutilizationresume** | **hwascpuutilizationrising** | **hwasfaninsert** | **hwasfaninvalid** | **hwasfaninvalidresume** | **hwasfanremove** | **hwasmadconflictdetect** | **hwasmadconflictresume** | **hwasmemutilizationresume** | **hwasmemutilizationrising** | **hwasopticalinvalid** | **hwasopticalinvalidresum** | **hwaspowerinsert** | **hwaspowerinvalid** | **hwaspowerinvalidresum** | **hwaspowerremove** | **hwunimbrasdiscoverattack** | **hwunimbrconnecterror** | **hwunimbrfabricportmemberdelete** | **hwunimbrillegalfabricconfig** | **hwunimbrlinkstatechange** | **hwunimbrasserviceabnormal** }]

Parameters

Parameter	Description	Value
trap-name	Enables or disables the trap function for the specified event.	-
hwasboardfail	Enables the trap function when an AS becomes unavailable partially.	-
hwasboardfailresume	Enables the trap function when an AS becomes available.	-

Parameter	Description	Value
hwasboardinvalid	Enables the trap function when an AS is invalid.	-
hwasboardinvalidresume	Enables the trap function when an AS is valid.	-
hwasbrdtempalarm	Enables the trap function when the AS temperature is out of the normal range.	-
hwasbrdtempresume	Enables the trap function when the AS temperature restores to the normal range.	-
hwascommunicateerror	Enables the trap function when a communication fault occurs.	-
hwascommunicateresume	Enables the trap function when a communication fault is rectified.	-
hwascpuutilizationresume	Enables the trap function when the AS CPU usage falls below the threshold.	-
hwascpuutilizationrising	Enables the trap function when the AS CPU usage exceeds the threshold.	-
hwasfaninsert	Enables the trap function when an AS fan module is installed.	-
hwasfaninvalid	Enables the trap function when an AS fan module becomes unavailable completely.	-
hwasfaninvalidresume	Enables the trap function when an AS fan module becomes available.	-
hwasfanremove	Enables the trap function when an AS fan module is removed.	-
hwasmadconflictdetect	Enables the trap function when a MAD conflict is detected.	-

Parameter	Description	Value
hwasmadconflictresume	Enables the trap function when a MAD conflict is resolved.	-
hwasmemutilizationresume	Enables the trap function when the AS memory usage restores to the normal range.	-
hwasmemutilizationrising	Enables the trap function when the AS memory usage exceeds the threshold.	-
hwasopticalinvalid	Enables the trap function when the AS optical module is invalid.	-
hwasopticalinvalidresum	Enables the trap function when the AS optical module is valid.	-
hwaspowerinsert	Enables the trap function when an AS power module is installed.	-
hwaspowerinvalid	Enables the trap function when an AS power module is invalid.	-
hwaspowerinvalidresum	Enables the trap function when an AS power module is valid.	-
hwaspowerremove	Enables the trap function when an AS power module is removed.	-
hwunimbrasdiscoverattack	Enables the trap function when an AS discovers attacks.	-
hwunimbrconnecterror	Enables the trap function when cable connection of a fabric port is incorrect.	-
hwunimbrfabricport-memberdelete	Enables the trap function when a member port of a fabric port is removed.	-
hwunimbrillegalfabric-config	Enables the trap function when the fabric port configuration is invalid.	-

Parameter	Description	Value
hwunimbrlinkstate-change	Enables the trap function when the connection status changes.	-
hwunimbrasserviceab-normal	Enables the trap function when services on an AS become abnormal.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

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

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

Example

# Enable the hwasboardfail trap of the UNIMBRTRAP module.

```
<HUAWEI> system-view
[HUAWEI] snmp-agent trap enable feature-name unimbrtrap trap-name hwasboardfail
```

Related Topics

3.9.39 display snmp-agent trap feature-name unimbrtrap all

3.9.91 snmp-agent trap enable feature-name uni-topomng

Function

snmp-agent trap enable feature-name uni-topomng command enables the trap function for the UNI-TOPOMNG module.

undo snmp-agent trap enable feature-name uni-topomng command disables the trap function for the UNI-TOPOMNG module.

By default, the trap function is enabled for the UNI-TOPOMNG module.

NOTE

This command can only be executed on a parent switch.

Format

snmp-agent trap enable feature-name uni-topomng [**trap-name** { **hwtopomnglinkabnormal** | **hwtopomnglinknormal** }]

undo snmp-agent trap enable feature-name uni-topomng [**trap-name** { **hwtopomnglinkabnormal** | **hwtopomnglinknormal** }]

Parameters

Parameter	Description	Value
trap-name	Enables or disables the trap function for the specified event.	-
hwtopomnglinkabnormal	Enables the trap function when a connection fault occurs.	-
hwtopomnglinknormal	Enables the trap function when the connection status becomes normal.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

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

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

Example

# Enable the hwtopomnglinkabnormal trap of the UNI-TOPOMNG module.

```
<HUAWEI> system-view
[HUAWEI] snmp-agent trap enable feature-name uni-topomng trap-name hwtopomnglinkabnormal
```

Related Topics

3.9.40 display snmp-agent trap feature-name uni-topomng all

3.9.92 snmp-agent trap enable feature-name uni-tplm

Function

snmp-agent trap enable feature-name uni-tplm command enables the trap function for the UNI-TPLM module.

undo snmp-agent trap enable feature-name uni-tplm command disables the trap function for the UNI-TPLM module.

By default, the trap function is enabled for the UNI-TPLM module.

NOTE

This command can only be executed on a parent switch.

Format

snmp-agent trap enable feature-name uni-tplm [**trap-name** { **hwtplmcmdexecutefailednotify** | **hwtplmcmdexecutesuccessfulnotify** | **hwtplmdirectcmdrecoverfail** }]

undo snmp-agent trap enable feature-name uni-tplm [**trap-name** { **hwtplmcmdexecutefailednotify** | **hwtplmcmdexecutesuccessfulnotify** | **hwtplmdirectcmdrecoverfail** }]

Parameters

Parameter	Description	Value
trap-name	Enables or disables the trap function for the specified event.	-
hwtplmcmdexecutefailednotify	Enables the trap function when the command fails to be executed on the AS.	-
hwtplmcmdexecutesuccessfulnotify	Enables the trap function when the command is executed successfully on the AS.	-
hwtplmdirectcmdrecoverfail	Enables the trap function when configurations of the commands directly configured on the parent for the AS fail to be restored.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

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

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

Example

# Enable the hwtplmcmdexecutefailednotify trap of the UNI-TPLM module.

```
<HUAWEI> system-view
[HUAWEI] snmp-agent trap enable feature-name uni-tplm trap-name hwtplmcmdexecutefailednotify
```

Related Topics

3.9.41 display snmp-agent trap feature-name uni-tplm all

3.9.93 snmp-agent trap enable feature-name uni-vermng

Function

snmp-agent trap enable feature-name uni-vermng command enables the trap function for the UNI-VERMNG module.

undo snmp-agent trap enable feature-name uni-vermng command disables the trap function for the UNI-VERMNG module.

By default, the trap function is enabled for the UNI-VERMNG module.

NOTE

This command can only be executed on a parent switch.

Format

snmp-agent trap enable feature-name uni-vermng [**trap-name hwvermngupgradefail**]

undo snmp-agent trap enable feature-name uni-vermng [**trap-name hwvermngupgradefail**]

Parameters

Parameter	Description	Value
trap-name	Enables or disables the trap function for the specified event.	-

Parameter	Description	Value
hwvermngupgradefail	Enables the trap function when an AS fails to be upgraded.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

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

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

Example

# Enable the hwvermngupgradefail trap of the UNI-VERMNG module.

```
<HUAWEI> system-view
[HUAWEI] snmp-agent trap enable feature-name uni-vermng trap-name hwvermngupgradefail
```

Related Topics

3.9.42 display snmp-agent trap feature-name uni-vermng all

3.9.94 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 S2720EI, S2750EI, S5700LI, S5700S-LI, S5720S-LI, S5720LI, S5720SI, S5720S-SI, S5710-X-LI, S5730SI, S5730S-EI, S6720LI, S6720S-LI, S6720SI, S6720S-SI, 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 S2720EI, S2750EI, S5700LI, S5700S-LI, S5720S-LI, S5720LI, S5720SI, S5720S-SI, S5710-X-LI, S5730SI, S5730S-EI, S6720LI, S6720S-LI, S6720SI, S6720S-SI, 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
```

Related Topics

3.9.108 user-access-profile name

3.9.95 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
```

Related Topics

3.9.4 as-admin-profile name

3.9.96 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
```

Related Topics

3.9.99 uni-mng

3.9.97 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
```

3.9.98 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.

- 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
```

Related Topics

3.9.13 as name interface (port group view)

3.9.47 display uni-mng as interface eth-trunk

3.9.55 display uni-mng port-group

3.9.99 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 S6720EI 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 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 switch to the uni-mng system and disconnect all online ASs. Continue? [Y/N]:y
```

Related Topics

13.4.38 authentication unified-mode

11.1.67 capwap source interface

5.12.47 stp mode (system view)

5.12.49 stp pathcost-standard

3.9.100 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 **3.9.101 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
```

3.9.101 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 (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 S2750EI 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 S5720SI, S5720S-SI, S5730SI, S5730S-EI, S6720LI, S6720S-LI, S6720SI, S6720S-SI, 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.

Example

# Configure the device to work in client mode and configure a management VLAN 100.

```
<HUAWEI> uni-mng indirect mng-vlan 100
```

3.9.102 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
```

3.9.103 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
```

Related Topics

3.9.74 network-enhanced-profile name

3.9.104 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** [**in** *time*]]

upgrade as name-include *string* [**reload** [**in** *time*]]

upgrade as type *as-type* [**reload** [**in** *time*]]

upgrade as all [**reload** [**in** *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.	-
in *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.
- The system software file name or patch file name specified using the **as type** command cannot be the same as the current or next startup system software file or patch file of an AS. Otherwise, the AS cannot be upgraded using the **upgrade as** command.
- 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 S5700-P-LI type.

```
<HUAWEI> system-view
[HUAWEI] uni-mng
[HUAWEI-um] upgrade as type s5700-p-li reload
```

Related Topics

3.9.99 uni-mng

3.9.105 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.	-
username *username*	Specifies the user name for accessing the file server.	The value is a string of 1 to 64 case-insensitive characters. It cannot contain spaces, asterisk, double quotation mark and question mark.
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. The newly configured password cannot be the default password of local users.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.

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 *S1720, S2700, S5700, and S6720 V200R011C10 Configuration Guide - Basic Configuration*.
- When the file server is an FTP server, the FTP service is automatically enabled and an FTP user is created on the parent, removing the need to perform the FTP configuration.
- 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, running this command to create the same user will change the user password in the AAA view to the configured password and change the user level to level 3. Changing the user password is allowed 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.
- 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 **13.1.20 authentication-scheme (AAA view)** 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 **13.1.47 domain (AAA view)** command in the AAA view to create a domain and run the **13.1.19 authentication-scheme (AAA domain view)** 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
```

3.9.106 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 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
```

3.9.107 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
```

Related Topics

3.9.74 network-enhanced-profile name

3.9.108 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
```

Related Topics

3.9.22 authentication-profile (user access profile view)

3.9.70 mac-limit (user access profile view)

3.9.109 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
```

Related Topics

3.9.108 user-access-profile name

3.9.80 port-group name

3.9.110 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
```

Related Topics

3.9.72 network-basic-profile name

3.9.111 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 case-insensitive characters. It cannot contain spaces, asterisk, double quotation mark and question mark.

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. The newly configured password cannot be the default password of local users.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.

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

When no AS user name and password are configured, you need to enter the default user name and password when logging in to an 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.

NOTE

The default password has security risks. You are advised to change the login password.

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 Pwd@123456
```

Related Topics

3.9.4 as-admin-profile name

3.9.112 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 (S5720EI, S6720EI, 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 S5720EI, S6720EI, 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
```

Related Topics

3.9.72 network-basic-profile name

3.9.113 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 0025-9e07-8280 to the whitelist.

```
<HUAWEI> system-view
[HUAWEI] as-auth
[HUAWEI-as-auth] whitelist mac-address 0025-9e07-8280
```

Related Topics

3.9.5 as-auth

3.10 Cloud-based Management Configuration Commands

3.10.1 Command Support

3.10.2 cloud-mng controller ip-address

3.10.3 cloud-mng controller url

3.10.4 cloud-mng management-vlan

3.10.5 cloud-mng redirected-controller ip-address

3.10.6 display cloud-mng connect-attribute

3.10.7 display cloud-mng configuration

3.10.8 display cloud-mng register-fail-record

3.10.9 display cloud-mng register-status

3.10.10 display linux network status

3.10.11 display work-mode

3.10.12 work-mode cloud-mng

3.10.13 reset cloud-mng db-configuration

3.10.14 reset cloud-mng register-fail-record

3.10.1 Command Support

Cloud-based management can be configured only on the S5720LI, S5720S-LI, S5720SI, and S5720S-SI.

3.10.2 cloud-mng controller ip-address

Function

The **cloud-mng controller ip-address** command configures an IP address for the cloud management platform.

The **undo cloud-mng controller ip-address** command deletes the IP address configured for the cloud management platform.

By default, no IP address is configured for the cloud management platform.

Format

cloud-mng controller ip-address *ip-address* **port** *port-number*

undo cloud-mng controller ip-address

NOTE

This command is supported only after the switch is changed to the cloud-based management mode.

Parameters

Parameter	Description	Value
ip-address	Specifies an IP address for the cloud management platform.	The value is in dotted decimal notation.
port-number	Specifies a port number.	The value is an integer that ranges from 0 to 65535.

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

After the switch is changed to the cloud-based management mode, it needs to register with the cloud management platform for authentication. Before registration authentication, the switch needs to obtain the cloud management platform's IP address. The switch can obtain the IP address using DHCP, the registration query center, or the **cloud-mng controller ip-address** command.

Precautions

- If the switch is configured to obtain the cloud management platform's IP address using DHCP, the registration query center, and commands, the three methods are used in descending order of priority: DHCP, commands, and the registration query center.
- If you run this command multiple times, only the latest configuration takes effect.
- When both the **cloud-mng controller ip-address** and **cloud-mng controller url** commands are configured on the switch, only the latest configured one takes effect. That is, the switch registers with the cloud management platform using either the cloud management platform's IP address or URL-resolved IP address.
- The configuration of this command is saved in the flash memory and therefore cannot be cleared by running the **reset cloud-mng db-configuration** command. To clear the configuration of this command, run the **undo cloud-mng controller ip-address** command.

Example

# Configure an IP address for the cloud management platform.

```
<HUAWEI> system-view
[HUAWEI] cloud-mng controller ip-address 10.1.1.1 port 10020
```

3.10.3 cloud-mng controller url

Function

The **cloud-mng controller url** command configures a URL for the cloud management platform.

The **undo cloud-mng controller url** command deletes the URL configured for the cloud management platform.

By default, no URL is configured for the cloud management platform.

Format

cloud-mng controller url *url-string* **port** *port-number*

undo cloud-mng controller url

NOTE

This command is supported only after the switch is changed to the cloud-based management mode.

Parameters

Parameter	Description	Value
url-string	Specifies a URL for the cloud management platform.	The value is a string of 3 to 128 case-sensitive characters. If you need to set one or more consecutive spaces, enclose the spaces in double quotation marks (").
port-number	Specifies a port number.	The value is an integer that ranges from 0 to 65535.

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

After the switch is changed to the cloud-based management mode, it needs to register with the cloud management platform for authentication. Before registration authentication, the switch needs to obtain the cloud management platform's IP address. The switch can obtain the IP address using DHCP or the registration query center or obtain the IP address resolved from the URL configured using the **cloud-mng controller url** command.

Precautions

- If the switch is configured to obtain the cloud management platform's URL using DHCP, the registration query center, and commands, the three methods are used in descending order of priority: DHCP, commands, and the registration query center.
- If you run this command multiple times, only the latest configuration takes effect.
- When both the **cloud-mng controller ip-address** and **cloud-mng controller url** commands are configured on the switch, only the latest configured one takes effect. That is, the switch registers with the cloud management platform using either the cloud management platform's IP address or URL-resolved IP address.
- The configuration of this command is saved in the flash memory and therefore cannot be cleared by running the **reset cloud-mng db-configuration** command. To clear the configuration of this command, run the **undo cloud-mng controller url** command.

Example

# Configure a URL for the cloud management platform.

```
<HUAWEI> system-view
[HUAWEI] cloud-mng controller url controller.huawei.com port 10020
```

3.10.4 cloud-mng management-vlan

Function

The **cloud-mng management-vlan** command records the VLAN used by the switch to communicate with a DHCP server.

By default, the switch uses VLAN 1 to communicate with a DHCP server.

Format

cloud-mng management-vlan *vlan-id*

NOTE

This command cannot be configured on the switch and can only be configured through the cloud management platform.

Parameters

Parameter	Description	Value
vlan-id	Specifies the ID of the VLAN used by the switch to communicate with a DHCP server.	The value is an integer that ranges from 1 to 4094.

Views

System view

Default Level

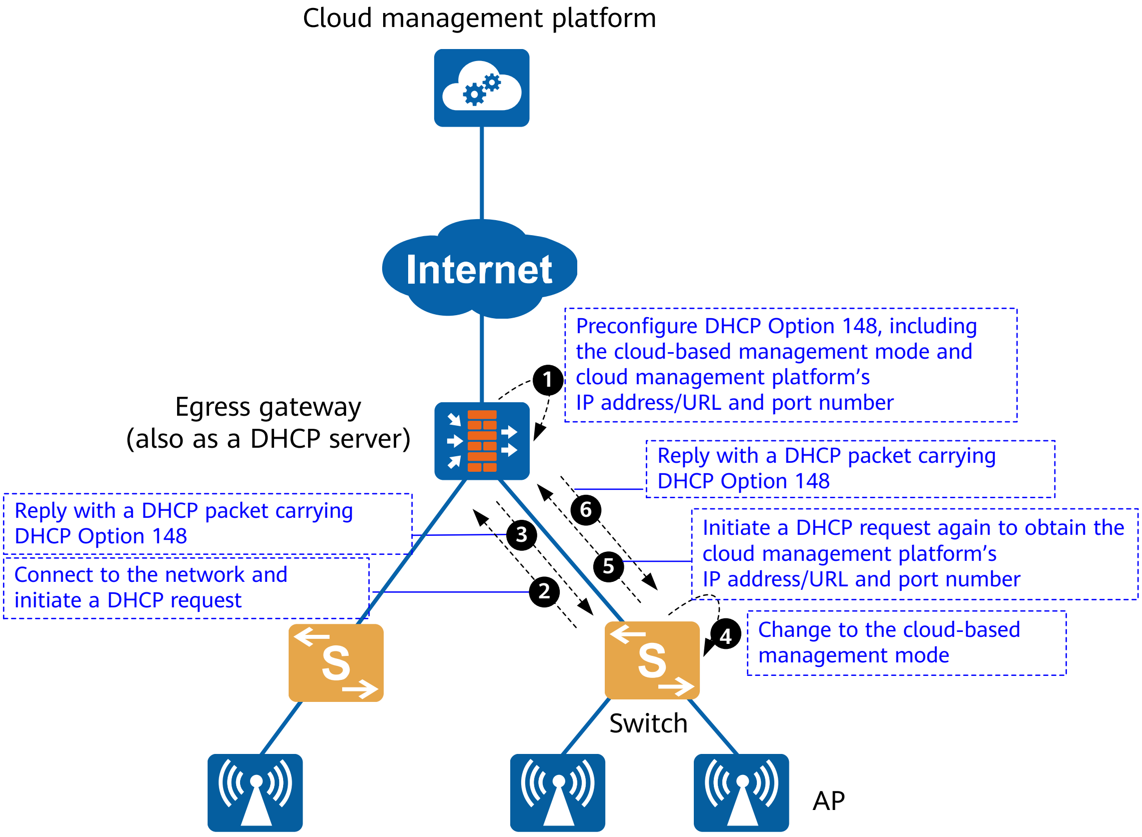
3: Management level

Usage Guidelines

Usage Scenario

After the switch is changed to the cloud-based management mode, it can obtain the cloud management platform's address information using DHCP. As shown in **Figure 3-1**, the switch obtains the cloud management platform's address information through the DHCP server in step 2. The DHCP request initiated by the switch is transmitted over VLAN 1. After the switch passes registration authentication, the controller of the cloud management platform reconfigures the VLAN used by the switch to communicate with the DHCP server. After the switch restarts, to ensure that it continues to use the reconfigured VLAN to communicate with the DHCP server, it records the management VLAN configured by the controller for communication between the switch and DHCP server into its configuration file. During the restart of the switch, the management VLAN can take effect through configuration restoration.

Figure 3-1 Changing the device management mode and obtaining the cloud management platform's address information through a DHCP server


Cloud management platform
Internet
Preconfigure DHCP Option 148, including the cloud-based management mode and cloud management platform's IP address/URL and port number
1
Egress gateway (also as a DHCP server)
Reply with a DHCP packet carrying DHCP Option 148
6
Reply with a DHCP packet carrying DHCP Option 148
3
Initiate a DHCP request again to obtain the cloud management platform's IP address/URL and port number
5
Connect to the network and initiate a DHCP request
2
4
Change to the cloud-based management mode
S
S
Switch
AP

Precautions

This command cannot be configured on the switch and can only be modified through the controller.

3.10.5 cloud-mng redirected-controller ip-address

Function

The **cloud-mng redirected-controller ip-address** command records the redirected IP address and port number of the cloud management platform.

By default, the switch does not record the redirected IP address and port number of the cloud management platform.

Format

cloud-mng redirected-controller ip-address *ip-address* **port** *port-number*

NOTE

This command cannot be configured on the switch and can only be configured through the cloud management platform.

Parameters

Parameter	Description	Value
ip-address	Specifies the redirected IP address.	The value is in dotted decimal notation.
port *port-number*	Specifies the redirected port number.	The value is an integer that ranges from 0 to 65535.

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

After the switch is changed to the cloud-based management mode and passes registration authentication with the cloud management platform, the IP address and port number of the cloud management platform are redirected on the controller of the cloud management platform.

After the switch restarts, to ensure that it continues to use the redirected cloud management platform on the controller, it records the redirected IP address and port number of the cloud management platform into its configuration file. During the restart of the switch, the redirected IP address and port number can take effect through configuration restoration.

Precautions

The switch can obtain the cloud management platform's address information using different methods (listed in descending order of priority): obtain the cloud management platform's redirection information recorded in its configuration file, use DHCP, use commands, and obtain the information from the registration query center.

3.10.6 display cloud-mng connect-attribute

Function

The **display cloud-mng connect-attribute** command displays information about the connection between a switch and the cloud management platform.

Format

display cloud-mng connect-attribute

NOTE

This command is supported only after the switch is changed to the cloud-based management mode.

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

This command can display information about the connection between a switch and the cloud management platform, including the cloud management platform's URL and port number.

Example

# Display information about the connection between a switch and the cloud management platform.

```
<HUAWEI> display cloud-mng connect-attribute
------------------------------------------------------------------------------
Controller address source  : Allocated by Register Center
Controller URL             : device_naas.huawei.com
Controller IP address      : -
Controller port            : 10020
Management VLAN            : 1
Management IP address      : 10.10.10.1
------------------------------------------------------------------------------
```

Table 3-141 Description of the **display cloud-mng connect-attribute** command output

Item	Description
Controller address source	How the cloud management platform's IP address is obtained: ● User-defined configuration: indicates that the IP address is the user-defined configuration. ● Allocated by Register Center: indicates that the IP address is obtained through the registration query center. ● Allocated by DHCP: indicates that the IP address is obtained through DHCP. ● Allocated by controller: indicates that the IP address is obtained through the cloud management platform. ● -: indicates that no IP address is obtained.
Controller URL	URL of the cloud management platform. To configure the cloud management platform's URL, run the **cloud-mng controller url** command. If no URL is configured or obtained, this field displays -.
Controller IP address	IP address of the cloud management platform. To configure the cloud management platform's IP address, run the **cloud-mng controller ip-address** command. If no IP address is configured or obtained, this field displays -.
Controller port	Port number of the cloud management platform. To configure the cloud management platform's IP address, run the **cloud-mng controller ip-address** command. If no IP address is configured or obtained, this field displays -.

Item	Description
Management VLAN	Management VLAN ID used when the switch communicates with the cloud management platform. The default value is 1. You can configure the management VLAN ID through the controller on the cloud management platform. Then the switch records the configured VLAN ID in the configuration file using the **cloud-mng management-vlan** command.
Management IP address	IP address of the VLANIF interface for the management VLAN used when the switch communicates with the cloud management platform. This IP address can be dynamically allocated by the DHCP server or use the IP address configured on the VLANIF interface for the management VLAN. If no IP address is dynamically allocated or configured on the VLANIF interface, this field displays -.

3.10.7 display cloud-mng configuration

Function

The **display cloud-mng configuration** command displays cloud management platform information.

Format

display cloud-mng configuration

NOTE

This command is supported only after the switch is changed to the cloud-based management mode.

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

To view cloud management platform information (such as an IP address), run the **display cloud-mng configuration** command.

This command cannot display cloud management platform information that is obtained through DHCP or the registration query center.

Example

# Display cloud management platform information.

```
<HUAWEI> display cloud-mng configuration
--------------- Cloud-mng configuration begin---------------
cloud-mng controller ip-address 10.1.1.1 port 10020
cloud-mng controller ip-address 192.168.2.2 port 10020 (redirected)
--------------- Cloud-mng configuration end-----------------
```

Table 3-142 Description of the **display cloud-mng configuration** command output

Item	Description
cloud-mng controller ip-address 10.1.1.1 port 10020	The configured IP address and port number of the cloud management platform are 10.1.1.1 and 10020. If the information is marked **redirected**, the switch has been redirected from the cloud management platform with which it just registers to another cloud management platform for management.

3.10.8 display cloud-mng register-fail-record

Function

The **display cloud-mng register-fail-record** command displays records about failures to register with the cloud management platform.

Format

display cloud-mng register-fail-record

NOTE

This command is supported only after the switch is changed to the cloud-based management mode.

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After this command is executed, a maximum of five registration failure records can be displayed.

Example

# Display records about failures to register with the cloud management platform.

```
<HUAWEI> display cloud-mng register-fail-record
-----------------------------------------------------------------------------
Time                    Error Info
-----------------------------------------------------------------------------
2016/02/09 22:21:02        Failed to apply IP address
2016/02/09 23:12:13        Failed to create TCP link to controller (192.168.1.1)
-----------------------------------------------------------------------------
```

Table 3-143 Description of the **display cloud-mng register-fail-record** command output

Item	Description
Time	Registration failure time.

Item	Description
Error Info	Registration failure reason. The IP address in this field is the IP address of the cloud management platform with which the switch failed to register. Possible reasons include: ● Manage VLAN is physical down ● Change to tradition work mode failed ● Failed to apply IP address ● No DNS information in DHCP options ● No controller IP or URL information ● Failed to get IP address of controller ● Failed to create TCP link to controller ● Failed to get register result from controller ● Controller certificate authentication failed ● Controller ESN check failed ● Device is not authorized ● Device type and ESN does not match ● Failed to connect registration query center ● Others

3.10.9 display cloud-mng register-status

Function

The **display cloud-mng register-status** command displays the status of registration with the cloud management platform.

Format

display cloud-mng register-status

NOTE

This command is supported only after the switch is changed to the cloud-based management mode.

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display cloud-mng register-status** command to check the current registration status and registration phase.

Example

# Display the status of registration with the cloud management platform.

```
<HUAWEI> display cloud-mng register-status
------------------------------------------------------------------------------
Register status        : unregistered
Register phase          : DHCP
------------------------------------------------------------------------------
```

Table 3-144 Description of the **display cloud-mng register-status** command output

Item	Description
Register status	Current registration status of the device. **NOTE** If the TCP connection between the switch and cloud management platform is disconnected, the switch changes from **registered** to **unregistered** state after detecting the disconnection within 3 minutes.
Register phase	Current registration phase of the device. ● DHCP: The switch requests an IP address from a DHCP server. ● registering: The switch has obtained an IP address from a DHCP server and is registering with the cloud management platform. ● registered: The switch has registered with the cloud management platform successfully.

3.10.10 display linux network status

Function

The **display linux network status** command displays information of transport layer connections.

Format

display linux network status

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display network status** command to view which transport-layer ports are in use. However, this command does not display the transport-layer ports used in NETCONF connections set up between the switch and remote device. To view these ports, run the **display linux network status** command.

Example

# Display information of transport layer connections.

```
<HUAWEI> display linux network status
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 192.168.20.102:55800    192.168.10.7:55804      ESTABLISHED
tcp        0      0 192.168.20.103:55801    192.168.10.8:55805      ESTABLISHED
tcp        0      0 192.168.20.104:55803    192.168.10.9:55806      ESTABLISHED
```

Table 3-145 Description of the **display linux network status** command output

Item	Description
Active Internet connections (servers and established)	Information of transport layer connections.
Proto	Transport layer protocol: ● tcp ● udp
Recv-Q	The count of bytes not copied by the user program connected to this socket.
Send-Q	The count of bytes not acknowledged by the remote host.
Local Address	IP address and TCP port used by the switch to set up a connection with the remote end.

Item	Description
Foreign Address	IP address and TCP port used by the remote end to set up a connection with the switch.
State	status of the connection: ● ESTABLISHED: The socket has an established connection. ● SYN_SENT: The socket is actively attempting to establish a connection. ● SYN_RECV: A connection request has been received from the network. ● FIN_WAIT1: The socket is closed, and the connection is shutting down. ● FIN_WAIT2: Connection is closed, and the socket is waiting for a shutdown from the remote end. ● TIME_WAIT: The socket is waiting after close to handle packets still in the network. ● CLOSE_WAIT: The remote end has shut down, waiting for the socket to close. ● LAST_ACK: The remote end has shut down, and the socket is closed. Waiting for acknowledgement. ● LISTEN: The socket is listening for incoming connections. ● CLOSING: Both sockets are shut down but we still don't have all our data sent. ● CLOSED: The socket is not being used.

3.10.11 display work-mode

Function

The **display work-mode** command displays the working mode of the current device.

Format

display work-mode

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

To check whether the current device works in cloud-based management mode, run the **display work-mode** command.

Example

# Display the working mode of the current device.

```
<HUAWEI> display work-mode
Current work-mode: cloud-mng
```

Table 3-146 Description of the **display work-mode** command output

Item	Description
Current work-mode	Working mode of the current device: ● cloud-mng: cloud-based management mode ● tradition: traditional management mode

3.10.12 work-mode cloud-mng

Function

The **work-mode cloud-mng** command sets the device management mode of a switch to the cloud-based management mode.

The **undo work-mode** command restores the default device management mode of a switch.

By default, the device management mode of a switch is the traditional management mode.

Format

work-mode cloud-mng (Supported when the switch is the traditional management mode)

undo work-mode (Supported when the switch is the cloud-based management mode.)

Parameters

None

Views

User view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

To perform cloud-based management on a switch, you must first change the switch to the cloud-based management mode. You can enable the switch to automatically change to the cloud-based management mode through DHCP or the registration query center. However, the two methods have some limitations. For example, the DHCP-based method requires that the switch should be unconfigured and have no input on the console port, and the registration query center-based method requires that the registration query center should have imported device ESNs and corresponding cloud management platform's address information. If switches do not meet these conditions, run the **work-mode cloud-mng** command to manually change their device management mode.

Precautions

If the switch works in AS mode, it cannot change to the cloud-based management mode using the **work-mode cloud-mng** command.

After this command is executed, the system asks whether you want to clear all the configuration and restart the switch. Confirm the action.

After the switch works in cloud-based management mode, pay attention to the following points:

- The switch supports only some commands supported in traditional management mode. These commands are mainly used for fault location, including commands used to configure the mirroring function and packet header obtaining function. For details about these commands, see "Commands supported in cloud-based management mode" in the *Licensing Requirements and Limitations for Cloud-based Management - Feature Limitations*.
- The management interface of the switch will generate an IP address 192.168.1.253/24 so that you can log in to the switch through the web system, Telnet, or FTP. To log in to the switch through the web system, hold down the **MODE** button for 6s or longer.

Example

# Set the device management mode of a switch to the cloud-based management mode.

```
<HUAWEI> work-mode cloud-mng
Warning:This command will clear current startup configuration and reboot, the unsaved configuration will
be lost. Continue? [Y/N]: y
```

3.10.13 reset cloud-mng db-configuration

Function

The **reset cloud-mng db-configuration** command clears the database configuration.

Format

reset cloud-mng db-configuration

Parameters

None

Views

System view

Default Level

3: Management level

Usage Guidelines

To stop providing network services, run the **reset cloud-mng db-configuration** command to clear all the database configuration.

NOTICE

After the **reset cloud-mng db-configuration** command is executed, the system asks whether you want to restart the switch. If you enter **Y**, the switch restarts and clears all thedatabase configuration. Confirm your action.

Example

# Clear the database configuration.

```
<HUAWEI> system-view
[HUAWEI] reset cloud-mng db-configuration
Warning: This operation will clear the database configuration and saved configuration file and restart the
device. Continue? [Y/N]:
```

3.10.14 reset cloud-mng register-fail-record

Function

The **reset cloud-mng register-fail-record** command clears records about failures to register with the cloud management platform.

Format

reset cloud-mng register-fail-record

NOTE

This command is supported only after the switch is changed to the cloud-based management mode.

Parameters

None

Views

All views

Default Level

3: Management level

Usage Guidelines

You can run the **reset cloud-mng register-fail-record** command to clear records about failures to register with the cloud management platform. Confirm the action before running this command.

Example

# Clear records about failures to register with the cloud management platform.

```
<HUAWEI> reset cloud-mng register-fail-record
Warning: This command will clear the registration failures. Continue? [Y/N]: y
```