4 Interface Management Commands

About This Chapter

4.1 Basic Interface Configuration Commands

4.1.1 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.

4.1.2 collect counters top

Function

The **collect counters top** command sets the parameters for top N interface traffic statistics and enables the function to generate top N interface traffic statistics reports.

Format

collect counters top [*number*] **interface** { *interface-type* | **all** | **layer-2** | **layer-3** } [**sort-by** *statistics-type* | **interval** *interval-value*] *

Parameters

Parameter	Description	Value
number	Specifies the number of busiest interfaces for which traffic statistics reports are to be generated. For example, if the value is 10, a traffic statistics report about top 10 busiest interfaces is generated. If you do not specify this parameter, a traffic statistics report about top 20 busiest interfaces is generated.	The value is an integer ranging from 1 to 50000.

Parameter	Description	Value
interface { *interface-type* | **all** | **layer-2** | **layer-3** }	Specifies the type of the interfaces for which a top N traffic statistics report is to be generated: - *interface-type*: indicates a specific type of interface. - **all**: indicates all interfaces. - **layer-2**: indicates Layer 2 interfaces. - **layer-3**: indicates Layer 3 interfaces.	The specified interfaces must be Ethernet physical interfaces or Eth-Trunk interfaces.
sort-by *statistics-type*	Specifies the statistics type by which ports are determined to be the busiest. If you do not specify **sort-by** *statistics-type*, statistics are sorted by the total number of bytes in descending order.	The value can be: - **utilization**: indicates to sort statistics by bandwidth utilization. - **bytes**: indicates to sort statistics by the total number of bytes. - **packets**: indicates to sort statistics by the total number of packets. - **multicast**: indicates to sort statistics by the total number of multicast packets. - **broadcast**: indicates to sort statistics by the total number of broadcast packets. - **errors**: indicates to sort statistics by the total number of error packets. - **discards**: indicates to sort statistics by the total number of dropped packets.
interval *interval-value*	Specifies the interval at which statistics are collected.	The value is an integer ranging from 1 to 999, in seconds. The default value is 30.

Views

All views

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The display command allows you to view statistics about the traffic sent and received by each interface on a device, but cannot sort these statistics by traffic volume in descending order. The **display counters top interface** command allows you to view top N interface traffic statistics reports, facilitating interface monitoring. Before you view a top N interface traffic statistics report, run the **collect counters top** command to generate your desired top N interface traffic statistics report. For example, configure the device to generate a top N statistics report about packets dropped on Layer 2 interfaces within 50s.

The top N interface traffic statistics function sorts statistics about inbound and outbound traffic processed by interfaces within a collection interval in descending order and generates a top N interface traffic statistics report. The device stops collecting interface traffic statistics after the collection interval ends. To generate another top N interface traffic statistics report, run the **collect counters top** command again.

Configuration Impact

- After the **collect counters top** command is run, the device collects interface traffic statistics and generates a top N interface traffic statistics report based on the set parameters.
- The **collect counters top** command configuration is not saved in the configuration file.

Follow-up Procedure

To view a top N interface traffic statistics report, run the **display counters top interface** command.

Precautions

- When the master switch in a stack containing multiple member switches is faulty, the top N interface traffic statistics function takes effect only on a master switch. If the master switch encounters a fault and switches to the backup state, run the **collect counters top** command on the new master switch again.
- The **collect counters top** command can be run multiple times in succession with different parameters specified. For example, you can configure a device to generate a top N statistics report about interface multicast packets when the device is still generating a top N statistics report about interface broadcast packets.
- The top N interface traffic statistics function allows a device to generate a maximum of five top N interface traffic statistics reports. If you want the device to generate new top N interface traffic statistics reports when five top N interface traffic statistics reports already exist, run the **reset counters top interface** command to clear existing ones.

Example

# Configure a device to generate a statistics report about top 10 Layer 2 interfaces in terms of the number of packets dropped within 40s.

```
<HUAWEI> collect counters top 10 interface layer-2 sort-by discards interval 40
```

Related Topics

4.1.9 display counters top interface

4.1.21 reset counters top interface

4.1.3 bandwidth (Interface view)

Function

The **bandwidth** command sets the interface bandwidth obtained by the NMS from the MIB.

The **undo bandwidth** command restores the default configuration.

By default, the interface bandwidth obtained by the NMS from the MIB depends on the interface type. For example, the bandwidth of a GE interface is 1000 Mbit/s.

NOTE

Only the S2750EI, S5720EI, S5720HI, S6720EI and S6720S-EI support this command.

Format

bandwidth *bandwidth*

undo bandwidth

Parameters

Parameter	Description	Value
bandwidth	Specifies the bandwidth of an interface.	The value is an integer ranging from 1 to 1000000, and the unit is Mbit/s.

Views

Ethernet interface view, GE interface view, XGE interface view, 40GE interface view, Tunnel interface view, Eth-Trunk interface view, VLANIF interface view, VE interface view, VE sub-interface view

Default Level

2: Configuration level

Usage Guidelines

Running the **bandwidth** command sets an interface bandwidth obtained by the NMS from the MIB and does not change an interface actual bandwidth. The NMS can check the interface bandwidth through the two objects **ifSpeed** and **ifHighSpeed** in **IF-MIB**.

- If the configured bandwidth is smaller than 4000 Mbit/s, **ifSpeed** and **ifHighSpeed** are respectively displayed as *bandwidth* x 1000 x 1000 and *bandwidth*.
- If the configured bandwidth is equal to or larger than 4000 Mbit/s, **ifSpeed** and **ifHighSpeed** are respectively displayed as 4294967295 (0XFFFFFFFF) and *bandwidth*.

Example

# Set the bandwidth of GE0/0/1 to 100 Mbit/s.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet0/0/1
[HUAWEI-gigabitethernet0/0/1] bandwidth 100
```

4.1.4 description (interface view)

Function

The **description** command configures the description for an interface.

The **undo description** command restores the default description of an interface.

By default, the description of an interface is null.

Format

description *description*

undo description

Parameters

Parameter	Description	Value
description	Specifies the interface description.	The value is a string of 1 to 242 characters. The character string is case sensitive. It can contain blanks but cannot contain the question mark (?).

Views

Interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To facilitate switch management and maintenance, you can configure interface descriptions. An interface description can contain:

Precautions

The interface description is displayed from the first non-space character.

Example

# Configure the description of GE0/0/1 as To-[DeviceB]GE-0/0/1, indicating that this device is connected to device B through GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] description To-[DeviceB]GE-0/0/1
```

Related Topics

4.1.12 display interface description

4.1.5 display counters

Function

The **display counters** command displays traffic statistics on an interface.

Format

display counters [**inbound** | **outbound**] [**interface** *interface-type* [*interface-number*]] [**nonzero**]

Parameters

Parameter	Description	Value
inbound	Displays incoming traffic statistics on an interface.	-
outbound	Displays outgoing traffic statistics on an interface.	-
interface *interface-type* [*interface-number*]	Displays traffic statistics on a specified interface. - *interface-type* specifies the interface type. - *interface-number* specifies the interface number. If the interface number is not specified, traffic statistics on all the interfaces of the specified type are displayed.	-
nonzero	Displays statistics about interface traffic. If the numbers of bytes, octets packets, unicast packets, multicast packets, and broadcast packets on an interface are all 0s, traffic statistics on this interface are not displayed.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

You can run the **display counters** command to view incoming or outgoing traffic statistics based on the interface type for fault location.

Precautions

Only the S6720EI, S6720S-EI, S5720HI and S5720EI support sub-interfaces.

When a device has a large number of interfaces, you are advertised to specify the interface type in the **display counters** command to view only desired information. If you do not specify those parameters, the following faults will occur:

- The displayed information is repeatedly refreshed, causing desired information unable to be obtained.
- The system does not respond because of long-time information traversing and searching.

Example

# Display traffic statistics on GE0/0/1.

```
<HUAWEI> display counters interface gigabitethernet 0/0/1
Inbound
Interface         Octets(bytes) Unicast(pkts) Multicast(pkts) Broadcast(pkts)
GE0/0/1             754918035105    1408179641        15018056      9668635374
Outbound
Interface         Octets(bytes) Unicast(pkts) Multicast(pkts) Broadcast(pkts)
GE0/0/1             764800451602    1148151623        15086605      9957268821
```

# Display traffic statistics on interfaces with at least one of the numbers of bytes, unicast packets, multicast packets, and broadcast packets not 0.

```
<HUAWEI> display counters nonzero
Info: This operation may take a few seconds. Please wait for a moment...
Inbound
Interface         Octets(bytes) Unicast(pkts) Multicast(pkts) Broadcast(pkts)
GE0/0/1                1467604             0           2902              0
Outbound
Interface         Octets(bytes) Unicast(pkts) Multicast(pkts) Broadcast(pkts)
GE0/0/1                2703904             0          13750              1
```

Table 4-1 Description of the **display counters** command output

Item	Description
Inbound	Incoming traffic statistics on an interface.
Interface	Interface name.
Octets(bytes)	Total number of incoming or outgoing bytes.

Item	Description
Unicast(pkts)	Number of incoming or outgoing unicast packets.
Multicast(pkts)	Number of incoming or outgoing multicast packets.
Broadcast(pkts)	Number of incoming or outgoing broadcast packets.
Outbound	Outgoing traffic statistics on an interface.

Related Topics

4.1.8 display counters rate

4.1.7 display counters interface

4.1.6 display counters error

Function

The **display counters error** command displays error packet statistics.

Format

display counters error [**inbound** | **outbound**] [**interface** *interface-type* [*interface-number*]]

Parameters

Parameter	Description	Value
inbound	Displays inbound error packet statistics.	-
outbound	Displays outbound error packet statistics.	-
interface *interface-type* [*interface-number*]	Displays error packet statistics on the specified interface. ● *interface-type* specifies the interface type. ● *interface-number* specifies the interface number. If interface type and interface number are not specified, the statistics of error packets on all interfaces are displayed.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display counters error** command to view detailed error packet statistics on all types of interfaces, which facilitates maintenance when there is a large number of error packets.

Example

# Check all error packet statistics on the device.

```
<HUAWEI> display counters error
Inbound
Interface         Total        CRC        Giants       Fragments
GE0/0/1              0          0            0             0
GE0/0/2              0          0            0             0
GE0/0/3              0          0            0             0
GE0/0/4              0          0            0             0
GE0/0/5              0          0            0             0
Interface         Runts    DropEvents    Alignments        Symbols
GE0/0/1              0          0            0             0
GE0/0/2              0          0            0             0
GE0/0/3              0          0            0             0
GE0/0/4              0          0            0             0
GE0/0/5              0          0            0             0
Outbound
Interface         Total    Collisions    Excess-Col  Late Collisions
GE0/0/1              0          0            0             0
GE0/0/2              0          0            0             0
GE0/0/3              0          0            0             0
GE0/0/4              0          0            0             0
GE0/0/5              0          0            0             0
```

Table 4-2 Description of the **display counters error** command output

Item	Description
Inbound	Inbound error packet statistics.
Outbound	Outbound error packet statistics.
Interface	Interface name.
Total	Total number of inbound and outbound error packets.
CRC	Number of packets shorter than 1518 bytes and with incorrect FCS values. For the S5720SI, S5720S-SI, S5710X-LI, S5720HI, S5730SI, S5730S-EI, S6720SI, and S6720S-SI, the value of this field includes the number of received packets longer than the maximum jumbo frame length and with incorrect FCS values. For switches excluding the S5720EI, the value of this field contains the number of received packets with length ranging from 1518 bytes to the jumbo frame size configured on the interface and incorrect FCS values.
Giants	Number of received packets with length exceeding the maximum jumbo frame size.

Item	Description
Fragments	Number of fragmented packets received by the interface. A fragmented packet is a packet with length less than 64 bytes and incorrect CRC values. On the S5720SI, S5720S-SI, S5710-X-LI, S5730SI, S5730S-EI, S6720SI, S6720S-SI, S6720S-EI, and S6720EI, the command output does not contain the Fragments field to display statistics about received fragmented packets.
Runts	Number of received undersized frames with correct CRC values. An undersized frame is a frame that is shorter than 64 bytes, in correct format, and contains a valid CRC field. For the S5720SI, S5720S-SI, S5710-X-LI, S5730SI, S5730S-EI, S6720SI, S6720S-SI, S6720S-EI, and S6720EI, the value of this field includes the number of received fragmented packets shorter than 64 bytes and with incorrect CRC values.
DropEvents	Number of received packets that are discarded due to GBP full or back pressure.
Alignments	Number of received frames with alignment error.
Symbols	Number of received frames with coding error.
Collisions	Number of packets with 1 to 15 collisions during packet forwarding. For the S5720SI, S5720S-SI, S5710-X-LI, S5730SI, S5730S-EI, S6720SI, S6720S-SI, S6720S-EI, and S6720EI, the value of this field contains the number of frames that are not sent due to 16 consecutive collisions.
Excess-Col	After sixteen successive collisions, the system will take it as excessive collision statistics when another collision occurs. Frames that are not sent due to excessive collisions are counted in this field. On the S5720SI, S5720S-SI, S5710-X-LI, S5730SI, S5730S-EI, S6720SI, S6720S-SI, S6720S-EI, and S6720EI, the command output does not contain the Excess-Col field to display statistics about frames that are not sent due to 16 consecutive collisions.
Late Collisions	Number of delay collision frames. A delay collision frame is a frame that is delayed because a collision is detected when the first 512 bits of the frame are sent.

4.1.7 display counters interface

Function

The **display counters interface** command displays traffic statistics on an interface, including typical packet statistics and number of packets discarded in queues.

Format

display counters interface [*interface-type interface-number*] [**verbose** | **nonzero**]

display counters interface verbose [**nonzero**]

Parameters

Parameter	Description	Value
interface-type interface-number	Specifies the interface type and number. ● *interface-type* specifies the interface type. ● *interface-number* specifies the interface number.	-
verbose	Displays detailed traffic statistics on an interface, including typical packet statistics and number of packets discarded in queues.	-
nonzero	Displays non-zero traffic statistics on an interface, including typical packet statistics and number of packets discarded in queues.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

When diagnosing faults on an interface, run the **display counters interface** [*interface-type interface-number*] [**verbose** | **nonzero**] command to view detailed information about packets received and sent by the interface to determine whether the interface works properly. You can also run this command to view detailed traffic statistics on an interface, including typical packet statistics and number of packets discarded in queues. You can also run this command to view non-zero traffic statistics on an interface, including typical packet statistics and number of packets discarded in queues.

Follow-up Procedure

If you want to collect new traffic statistics, run the **reset counters interface** command to clear the current statistics.

Example

# Display traffic statistics on an interface, including typical packet statistics and number of packets discarded in queues. (The following uses a S5720EI as an example.)

```
<HUAWEI> display counters interface gigabitethernet 0/0/1 verbose
GigabitEthernet0/0/1
InPackets                 :                 0
InOctets                  :                 0
InUcastPkts               :                 0
InMcastPkts               :                 0
InBcastPkts               :                 0
OutPackets                :                 0
OutOctets                 :                 0
OutUcastPkts              :                 0
OutMcastPkts              :                 0
OutBcastPkts              :                 0
InJumbo                   :                 0
InPause                   :                 0
Frames                    :                 0
OutJumbo                  :                 0
OutPause                  :                 0
InDiscards                :                 0
OutDiscards               :                 0
InErrors                  :                 0
OutErrors                 :                 0
CRC                       :                 0
Giants                    :                 0
Jabbers                   :                 0
Fragments                 :                 0
Runts                     :                 0
DropEvents                :                 0
Alignments                :                 0
Symbols                   :                 0
Ignoreds                  :                 0
Collisions                :                 0
ExcessiveCollisions       :                 0
Late Collisions           :                 0
Deferreds                 :                 0
Buffers purged            :                 0
InPkts64Octets            :                 0
InPkts65to127Octets       :                 0
InPkts128to255Octets      :                 0
InPkts256to511Octets      :                 0
InPkts512to1023Octets     :                 0
```

```
InPkts1024to1518Octets   :              0
OutPkts64Octets          :              0
OutPkts65to127Octets     :              0
OutPkts128to255Octets    :              0
OutPkts256to511Octets    :              0
OutPkts512to1023Octets   :              0
OutPkts1024to1518Octets  :              0
Queue0lostPkts           :              0
Queue1lostPkts           :              0
Queue2lostPkts           :              0
Queue3lostPkts           :              0
Queue4lostPkts           :              0
Queue5lostPkts           :              0
Queue6lostPkts           :              0
Queue7lostPkts           :              0
```

Table 4-3 Description of the **display counters interface** command output

Item	Description
GigabitEthernet0/0/1	The interface type and number.
InPackets	Total number of packets received by the interface.
InOctets	Total number of bytes in packets received by the interface.
InUcastPkts	Number of unicast packets received by the interface.
InMcastPkts	Number of multicast packets received by the interface.
InBcastPkts	Number of broadcast packets received by the interface.
OutPackets	Total number of packets sent by the interface.
OutOctets	Total number of bytes in packets sent by the interface.
OutUcastPkts	Number of unicast packets sent by the interface.
OutMcastPkts	Number of multicast packets sent by the interface.
OutBcastPkts	Number of broadcast packets sent by the interface.
InJumbo	Number of Ethernet frames with length ranging from 1518 bytes to the maximum jumbo frame size and correct FCS values received by the interface, or number of VLAN frames with length ranging from 1522 bytes to the maximum jumbo frame size and correct FCS values received or sent by the interface.
InPause	Number of pause frames received by the interface.
Frames	Number of packets in which the 802.3 length field does not match the actual length received by the interface.
OutJumbo	Number of Ethernet frames with length ranging from 1518 bytes to the maximum jumbo frame size and correct FCS values sent by the interface, or number of VLAN frames with length ranging from 1522 bytes to the maximum jumbo frame size and correct FCS values received or sent by the interface.

Item	Description
OutPause	Number of pause frames sent by the interface.
InDiscards	Number of incoming packets discarded by the interface. The number is detected during physical layer detection.
OutDiscards	Number of outgoing packets discarded by the interface. The number is detected during physical layer detection.
InErrors	Number of incoming error packets on the interface. The number is detected during physical layer detection.
OutErrors	Number of outgoing error packets on the interface. The number is detected during physical layer detection.
CRC	Number of packets shorter than 1518 bytes and with incorrect FCS values. For the S5720LI, S5720SI, S5720S-SI, S5710X-LI, S5720HI, S5730SI, S5730S-EI, S6720SI, and S6720S-SI, the value of this field includes the number of received packets longer than the maximum jumbo frame length and with incorrect FCS values. For switches excluding the S5720EI, the value of this field contains the number of received packets with length ranging from 1518 bytes to the jumbo frame size configured on the interface and incorrect FCS values.
Giants	Number of received packets with length exceeding the maximum jumbo frame size. ● On a 10000M interface, the number of bytes for Giants packets is calculated according to the actual packet length. ● On a 1000M interface, the number of bytes for Giants packets is calculated according to the maximum jumbo frame size. To set the maximum jumbo frame size, run the **jumboframe enable** command.
Jabbers	Number of received packets with length ranging from 1518 bytes to the maximum jumbo frame size and incorrect FCS values on the S5720EI. The S2720EI, S5720LI, S5720SI, S5720S-SI, S5710-X-LI, S5730SI, S5730S-EI, S6720SI, S6720S-SI, S6720S-EI, and S6720EI do not have the Jabbers field. On the other product models, this field indicates the number of received packets with length exceeding the maximum jumbo frame size and incorrect FCS values.

Item	Description
Fragments	Number of received fragmented packets. A fragmented packet is a packet shorter than 64 bytes and with incorrect CRC values. For the S5720HI, the value of this field contains the number of undersized frames with the correct CRC values received is displayed. On the S2720EI, S5720LI, S5720SI, S5720S-SI, S5710-X-LI, S5730SI, S5730S-EI, S6720SI, S6720S-SI, S6720S-EI, and S6720EI, the command output does not contain the Fragments field to display statistics about received fragmented packets.
Runts	Number of undersized frames with correct CRC values received by the interface. For the S5720LI, S5720SI, S5720S-SI, S5710-X-LI, S5730SI, S5730S-EI, S6720SI, S6720S-SI, S6720S-EI, and S6720EI, the value of this field includes the number of received fragmented packets shorter than 64 bytes and with incorrect CRC values.
DropEvents	Number of received packets that are discarded due to GBP full or back pressure.
Alignments	Number of received frames with alignment errors.
Symbols	Number of received frames with coding errors.
Ignoreds	Number of received MAC control frames whose OpCode is not PAUSE.
Collisions	Number of packets with 1 to 15 collisions during packet forwarding. For the S5720SI, S5720S-SI, S5710-X-LI, S5730SI, S5730S-EI, S6720SI, S6720S-SI, S6720S-EI, and S6720EI, the value of this field contains the number of frames that are not sent due to 16 consecutive collisions.
ExcessiveCollisions	Number of packets with 16 collisions and fail to be sent. On the S2720EI, S5720SI, S5720S-SI, S5710-X-LI, S5730SI, S5730S-EI, S6720SI, S6720S-SI, S6720S-EI, and S6720EI, the command output does not contain the ExcessiveCollisions field to display statistics about frames that are not sent due to 16 consecutive collisions.
Late Collisions	Number of packets with conflict and delayed.
Deferreds	Number of delayed packets without conflict.
Buffers Purged	Number of packets aged in the cache.

Item	Description
InOutPkts64Octets	Number of packets shorter than 64 bytes received and sent by the interface.
InOutPkts65to127Octets	Number of packets with length ranging from 65 bytes to 127 bytes received and sent by the interface.
InOutPkts128to255Octets	Number of packets with length ranging from 128 bytes to 255 bytes received and sent by the interface.
InOutPkts256to511Octets	Number of packets with length ranging from 256 bytes to 511 bytes received and sent by the interface.
InOutPkts512to1023Octets	Number of packets with length ranging from 512 bytes to 1023 bytes received and sent by the interface.
InOutPkts1024toMaxOctets	Number of packets with length exceeding 1024 bytes received and sent by the interface.
InPkts64Octets	Number of packets shorter than 64 bytes received by the interface.
InPkts65to127Octets	Number of packets with length ranging from 65 bytes to 127 bytes received by the interface.
InPkts128to255Octets	Number of packets with length ranging from 128 bytes to 255 bytes received by the interface.
InPkts256to511Octets	Number of packets with length ranging from 256 bytes to 511 bytes received by the interface.
InPkts512to1023Octets	Number of packets with length ranging from 512 bytes to 1023 bytes received by the interface.
InPkts1024to1518Octets	Number of packets with length ranging from 1024 bytes to 1518 bytes received by the interface.
OutPkts64Octets	Number of packets shorter than 64 bytes sent by the interface. The value **NA** indicates that the interface does not support this field.
OutPkts65to127Octets	Number of packets with length ranging from 65 bytes to 127 bytes sent by the interface. The value **NA** indicates that the interface does not support this field.
OutPkts128to255Octets	Number of packets with length ranging from 128 bytes to 255 bytes sent by the interface. The value **NA** indicates that the interface does not support this field.

Item	Description
OutPkts256to511Octets	Number of packets with length ranging from 256 bytes to 511 bytes sent by the interface. The value **NA** indicates that the interface does not support this field.
OutPkts512to1023Octets	Number of packets with length ranging from 512 bytes to 1023 bytes sent by the interface. The value **NA** indicates that the interface does not support this field.
OutPkts1024to1518Octets	Number of packets with length ranging from 1024 bytes to 1518 bytes sent by the interface. The value **NA** indicates that the interface does not support this field.
Queue0lostPkts	Number of packets discarded in queue 0.
Queue1lostPkts	Number of packets discarded in queue 1.
Queue2lostPkts	Number of packets discarded in queue 2.
Queue3lostPkts	Number of packets discarded in queue 3.
Queue4lostPkts	Number of packets discarded in queue 4.
Queue5lostPkts	Number of packets discarded in queue 5.
Queue6lostPkts	Number of packets discarded in queue 6.
Queue7lostPkts	Number of packets discarded in queue 7.

NOTE

The number (InPkts) of packets received by the interface and the number (OutPkts) of packets sent by the interface can be displayed separately only on the S5720HI, S5720EI, S6720S-EI, and S6720EI. The S5720SI, S5720S-SI, S5700S-LI, S5700LI, S5720LI, S5720S-LI, S5710-X-LI, S1720GFR, S1720GW, S1720GWR, S1720X, S1720GW-E, S1720GWR-E, S1720X-E, S2720EI, S2750EI, S5730SI, S5730S-EI, S6720SI, S6720S-SI, S6720LI and S6720S-LI display only the total number (InOutPkts) of packets received and sent by the interface.

Related Topics

4.1.10 display interface

4.1.11 display interface brief

4.1.5 display counters

4.1.8 display counters rate

Function

The **display counters rate** command displays the incoming or outgoing traffic rate of an interface.

Format

display counters rate [**inbound** | **outbound**] [**interface** *interface-type* [*interface-number*]] [**nonzero**]

Parameters

Parameter	Description	Value
inbound	Displays the incoming traffic rate of an interface.	-
outbound	Displays the outgoing traffic rate of an interface.	-
interface *interface-type* [*interface-number*]	Displays the traffic rate of a specified interface. ● *interface-type* specifies the interface type. ● *interface-number* specifies the interface number. If the interface number is not specified, the traffic rates of all the interfaces of the specified type are displayed.	-
nonzero	Displays the traffic rate of an interface. If the numbers of bytes, Octets packets, unicast packets, multicast packets, and broadcast packets on an interface are all 0s, the traffic rate of this interface is not displayed.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

You can run the **display counters rate** command to view the incoming or outgoing traffic rate based on the interface type for fault location.

Precautions

After the system is started, in the case of the first query or when the interval with the last query is longer than 600s, the system re-initiates rate statistics collection. In this case, you need to wait until the rate statistics collection result is displayed.

The minimum statistics collection interval is 5 seconds. If the interval is less than 5 seconds, the data collected last time is displayed.

When a device has a large number of interfaces, you are advertised to specify the interface type in the **display counters rate** command to view only desired information. If you do not specify those parameters, the following faults will occur:

- The displayed information is repeatedly refreshed, causing desired information unable to be obtained.
- The system does not respond because of long-time information traversing and searching.

Example

# Display the traffic rate of GE0/0/1.

```
<HUAWEI> display counters rate interface gigabitethernet 0/0/1
Inbound
Interface   Octets(bytes/s) Unicast(pkts/s) Multicast(pkts/s) Broadcast(pkts/s)
GE0/0/1                 18              0                 0                 0
Outbound
Interface   Octets(bytes/s) Unicast(pkts/s) Multicast(pkts/s) Broadcast(pkts/s)
GE0/0/1                 61              0                 0                 0
```

# Display the traffic rate of interfaces with at least one of the numbers of bytes, unicast packets, multicast packets, and broadcast packets not 0.

```
<HUAWEI> display counters rate nonzero
Info: This operation may take a few seconds. Please wait for a moment...
Inbound
Interface   Octets(bytes/s) Unicast(pkts/s) Multicast(pkts/s) Broadcast(pkts/s)
GE0/0/1                 82              1                 0                 0
Outbound
Interface   Octets(bytes/s) Unicast(pkts/s) Multicast(pkts/s) Broadcast(pkts/s)
GE0/0/1                224              2                 0                 0
```

Table 4-4 Description of the **display counters rate** command output

Item	Description
Inbound	Incoming traffic rate.
Outbound	Outgoing traffic rate.
Interface	Interface name.
Octets(bytes/s)	Total incoming or outgoing traffic rate, in bytes/s.
Unicast(pkts/s)	Incoming or outgoing rate of unicast packets, in pkts/s.
Multicast(pkts/s)	Incoming or outgoing rate of multicast packets, in pkts/s.
Broadcast(pkts/s)	Incoming or outgoing rate of broadcast packets, in pkts/s.

4.1.9 display counters top interface

Function

The **display counters top interface** command displays top N interface traffic statistics reports.

Format

display counters top interface report [*report-number*]

Parameters

Parameter	Description	Value
report [*report-number*]	Specifies the number of a top N interface traffic statistics report. If you do not specify this parameter, the command output displays the summary information about all top N interface traffic statistics reports.	The value is an integer ranging from 1 to 5.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

The **collect counters top** command generates top N interface traffic statistics reports, but does not display these reports. To view the generated reports, run the **display counters top interface report** [*report-number*] command.

Precautions

Before you run the **display counters top interface report** [*report-number*] command, ensure that a top N interface traffic statistics report has been generated using the **collect counters top** command. Otherwise, the "There is no TOPN interface counters report." message is displayed after you run the **display counters top interface report** [*report-number*] command.

Example

# Display the summary information about all top N interface traffic statistics reports.

```
<HUAWEI> display counters top interface report
Id Start Time                Interval Number Sort-By   Status Interface-Type
------------------------------------------------------------------------------
1  2012-09-05 09:03:13-08:00    30       20     bytes     doing  GigabitEthernet
```

Table 4-5 Description of the **display counters top interface report** command output

Item	Description
Id	Indicates the number of a top N interface traffic statistics report.
Start Time	Indicates the start time of statistics collection.
Interval	Indicates the statistics collection interval.
Number	Indicates the number of busiest interfaces for which interface statistics reports are to be generated.
Sort By	Indicates the statistics type by which ports are determined to be the busiest, which can be: ● utilization: indicates to sort statistics by bandwidth utilization. ● bytes: indicates to sort statistics by the total number of bytes. ● packets: indicates to sort statistics by the total number of packets. ● multicast: indicates to sort statistics by the total number of multicast packets. ● broadcast: indicates to sort statistics by the total number of broadcast packets. ● errors: indicates to sort statistics by the total number of error packets. ● discards: indicates to sort statistics by the total number of dropped packets.
Status	Indicates the generation status of a top N interface traffic statistics report, which can be: ● doing: The report is being generated. ● done: The report has been generated.
Interface-Type	Indicates the type of interfaces for which the top N interface traffic statistics report is generated, which can be: ● all: indicates all interfaces. ● layer-2: indicates Layer 2 interfaces. ● layer-3: indicates Layer 3 interfaces. ● Specified interface type: indicates Ethernet physical interfaces or Eth-Trunk interfaces.

# Display the detailed information about the top N interface traffic statistics report numbered 1.

```
<HUAWEI> display counters top interface report 1
Owner           : RT1(10.1.1.1)
```

```
Start Time        : 2012-09-17 13:26:06
End Time          : 2012-09-17 13:26:36
Interface Type    : GigabitEthernet
Sort By           : bytes
Interval          : 30 seconds


Port    Band  Util  Bytes      Packets    Multicast  Broadcast  Error  Discards
        width       (In + Out) (In + Out) (In + Out) (In + Out)
-------------------------------------------------------------------------------

GE0/0/1 1000  0.21% 537592     6892       0          54         0      0
```

Table 4-6 Description of the **display counters top interface report 1** command output

Item	Description
Owner	Indicates the device on which the top N interface traffic statistics report is generated.
Start Time	Indicates the start time of statistics collection.
End Time	Indicates the end time of statistics collection.
Interface Type	Indicates the type of interfaces for which the top N interface traffic statistics report is generated, which can be: ● all: indicates all interfaces. ● layer-2: indicates Layer 2 interfaces. ● layer-3: indicates Layer 3 interfaces. ● Specified interface type: indicates Ethernet physical interfaces or Eth-Trunk interfaces.
Sort-By	Indicates the statistics type by which ports are determined to be the busiest, which can be: ● utilization: indicates to sort statistics by bandwidth utilization. ● bytes: indicates to sort statistics by the total number of bytes. ● packets: indicates to sort statistics by the total number of packets. ● multicast: indicates to sort statistics by the total number of multicast packets. ● broadcast: indicates to sort statistics by the total number of broadcast packets. ● errors: indicates to sort statistics by the total number of error packets. ● discards: indicates to sort statistics by the total number of dropped packets.
Interval	Indicates the statistics collection interval.
Port	Indicates the interface name.

Item	Description
Band width	Indicates interface bandwidth.
Util	Indicates bandwidth utilization.
Bytes	Indicates the total number of sent and received bytes.
Packets	Indicates the total number of sent and received packets.
Multicast	Indicates the total number of sent and received multicast packets.
Broadcast	Indicates the total number of sent and received broadcast packets.
Error	Indicates the total number of error packets.
Discards	Indicates the total number of dropped packets.

4.1.10 display interface

Function

The **display interface** command displays the interface running status and statistics.

Format

display interface [*interface-type* [*interface-number* [.*subinterface-number*] | **main**] | **main**]

display interface slot *slot-id* [**main**]

Parameters

Parameter	Description	Value
interface-type [*interface-number*]	Displays the running status of an interface. ● *interface-type* specifies the interface type. ● *interface-number* specifies the interface number. If the interface type is specified but no interface number is specified, the running status of all the interfaces of this type is displayed.	-
subinterface-number	Displays the running status of a sub-interface.	The value is an integer that ranges from 1 to 4096.
main	Displays running status and traffic statistics about an interface. ● If an interface has no sub-interfaces, status and traffic statistics about the interface are displayed whether you specify the **main** parameter or not. ● If an interface has sub-interfaces, status and traffic statistics about the interface and sub-interfaces are displayed if you do not specify the **main** parameter.	-
slot *slot-id*	Specifies the slot ID.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

The running status and statistics of an interface includes the physical status, basic configuration, and packet forwarding of the interface. You can use the **display interface** command to collect traffic statistics or locate faults on an interface.

Precautions

If no interface type is specified, the running status and statistics of all the interfaces is displayed. If the interface type is specified but no interface number is specified, the running status of all the interfaces of this type is displayed.

Only the S6720EI, S6720S-EI, S5720HI and S5720EI support sub-interfaces.

Example

# Display the running status, basic configuration, and packet forwarding statistics on GE0/0/1.

```
<HUAWEI> display interface gigabitethernet 0/0/1
GigabitEthernet 0/0/1 current state : UP
Line protocol current state : UP
Description:
Switch Port,Link-type : access(negotiated),
 PVID :    1, TPID : 8100(Hex), The Maximum Frame Length is 9216
IP Sending Frames' Format is PKTFMT_ETHNT_2, Hardware address is 0025-9ef4-abcd
Last physical up time   : -
Last physical down time : 2015-12-21 16:12:29 UTC+08:00
Current system time: 2012-06-05 18:56:41
Port Mode: COMMON FIBER, Transceiver: 1000_BASE_SX_SFP
Speed : 1000,   Loopback: NONE
Duplex: FULL,   Negotiation: ENABLE
Mdi   : -, Flow-control: DISABLE
Last 300 seconds input rate 0 bits/sec, 0 packets/sec
Last 300 seconds output rate 0 bits/sec, 0 packets/sec
Input peak rate 0 bits/sec, Record time: -
Output peak rate 0 bits/sec, Record time: -

Input:  0 packets, 0 bytes
  Unicast:                     0,  Multicast:                    0
  Broadcast:                   0,  Jumbo:                        0
  Discard:                     0,  Pause:                        0
  Frames:                      0

  Total Error:                 0
  CRC:                         0,  Giants:                       0
  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,  Pause:                        0

  Total Error:                 0
  Collisions:                  0,  ExcessiveCollisions:          0
  Late Collisions:             0,  Deferreds:                    0
  Buffers Purged:              0

    Input bandwidth utilization threshold : 80.00%
    Output bandwidth utilization threshold: 80.00%
    Input bandwidth utilization  :     0%
    Output bandwidth utilization :     0%
```

# Display the running status, basic configuration, and packet forwarding on GE0/0/1 of the S5720HI.

```
<HUAWEI> display interface gigabitethernet 0/0/1
GigabitEthernet 0/0/1 current state : UP
Line protocol current state : UP
Description:
Switch Port, Link-type : access(negotiated),
PVID :    1, TPID : 8100(Hex), The Maximum Frame Length is 9216
IP Sending Frames' Format is PKTFMT_ETHNT_2, Hardware address is 000b-09a9-c9d7
Last physical up time   : -
Last physical down time : 2015-12-21 16:12:29 UTC+08:00
Current system time: 2009-03-31 11:51:03
Port Mode: COMMON COPPER
Speed : 1000,    Loopback: NONE
Duplex: FULL,   Negotiation: ENABLE
Mdi   : AUTO,   Flow-control: DISABLE
Last 300 seconds input rate 176 bits/sec, 0 packets/sec
Last 300 seconds output rate 440 bits/sec, 0 packets/sec
Input peak rate 7032 bits/sec, Record time: 2009-03-30 19:12:09
Output peak rate 38624 bits/sec, Record time: 2009-03-30 20:41:44

Input:  7650 packets, 1327062 bytes
  Unicast:                         0,  Multicast:                        7650
  Broadcast:                       0,  Jumbo:                               0
  Discard:                         0,  Pause:                               0

  Total Error:                     0
  CRC:                             0,  Giants:                              0
  Runts:                           0,  Fragments:                           0
  Alignments:                      0,  Symbols:                             0

Output:  38348 packets, 3683776 bytes
  Unicast:                         0,  Multicast:                       32314
  Broadcast:                    6034,  Discard:                             0
  Pause:                           0

    Input bandwidth utilization threshold : 80.00%
    Output bandwidth utilization threshold: 80.00%
    Input bandwidth utilization  :     0%
    Output bandwidth utilization :     0%
```

Table 4-7 Description of the **display interface** command output

Item	Description
current state	Current status of the interface: ● UP: indicates that the interface is physically Up. ● DOWN: indicates that the interface is physically Down. Protected port indicates that an interface is added to an interface protection group and set to be a protected interface. To add an interface to an interface protection group and set the interface to be a protected interface, run the **port protect-group** and **protect-group member** commands. ● Administratively down: indicates that the administrator has run the **shutdown** command on the interface. ● TRIGGER DOWN (BFD): When BFD detects a fault, the physical status of the interface becomes Down according to the OAM association. ● TRIGGER DOWN (3AH): When 3AH detects a fault, the physical status of the interface becomes Down according to the OAM association. ● TRIGGER DOWN (1AG): When 1AG detects a fault, the physical status of the interface becomes Down according to the OAM association. ● ERROR DOWN(auto-defend): When the interface receives packets from an attack source, the physical status of the interface becomes Down. ● ERROR DOWN(efm-threshold-event): When the number of error frames, error codes, or error frame seconds of EFM OAM detected by the interface reaches or exceeds the threshold within a set period, the physical status of the interface becomes Down according to the OAM association. ● ERROR DOWN(efm-remote-failure): When EFM detects a remote failure, the physical status of the interface becomes Down according to the OAM association. ● ERROR DOWN(bpdu-protection): If an edge interface receives RST BPDUs after BPDU protection is enabled, the physical status of the edge interface becomes Down. ● ERROR DOWN(error-statistics): If the system detects that the number of error packets received by the interface exceeds the threshold, the physical status of the interface becomes Down. ● ERROR DOWN(runts-error-statistics): When the number of Runts error packets received by the

Item	Description
	interface reaches the alarm threshold, the physical status of the interface becomes Down. ● ERROR DOWN(transceiver-power-low): If the system detects that the optical power of the interface falls below the configured lower alarm threshold, the physical status of the interface becomes Down. ● ERROR DOWN(port-security): When the number of learned MAC address entries reaches the threshold, the interface goes Down. ● ERROR DOWN(mac-address-flapping): When the learned MAC address flaps, the interface goes Down. ● ERROR DOWN(dhcp-packet-overspeed): When the DHCP packet rate of the interface exceeds the threshold, the physical status of the associated interface becomes Down. ● ERROR DOWN(link-flap): When the link flaps, the physical status of the associated interface becomes Down. ● ERROR DOWN(data-integrity-error): The chip memory identifier has a data integrity error and the physical status of the interface becomes Down. ● LOOPBACK-DETECT DOWN: The interface goes Down due to loopback detection. ● UP(E-TRUNK-DOWN): The Eth-Trunk interface goes Down because of E-Trunk negotiation. **NOTE** There is a delay before the interface state is reported, so an interface undergoes a short-time intermediate state before it transitions to the ERROR DOWN state. The intermediate state is ERROR DOWN (ERROR DOWN reason), up. This state does not affect functioning of the interface. When the physical status of the interface is ERROR DOWN(data-integrity-error), perform the following operations: 1. Check whether the **error-down auto-recovery cause data-integrity-error interval** *interval-value* command has been configured on the switch. If the command has been configured, go to step 2. Otherwise, go to step 3. 2. Check whether the interface restores to Up state after the time specified by *interval-value* expires. If the interface does not restore to Up state, go to step 3. 3. Run the **undo shutdown** command in the interface view to enable the interface and check whether the interface restores to Up state. If the interface does not restore to Up state, go to step 4. 4. Run the **reset slot** command to restart the switch. After the switch restarts, check whether the interface restores to Up state. If the interface does not restore to Up state, go to step 5. 5. Replace the switch.

Item	Description
Line protocol current state	Link layer protocol status of the interface: - UP: indicates that the link layer protocol of the interface is working properly. - UP (BFD status down): indicates that BFD associated with the interface is Down. - UP (Main BFD status down): indicates that the BFD session associated with the main interface becomes Down and is associated with the sub-interface status. This state is displayed only for sub-interfaces. - UP (spoofing): indicates that the link layer protocol of the interface is always Up with the spoofing feature enabled. - DOWN: indicates that the link-layer protocol status of the interface is Down or no IP address is assigned to the interface. For example, if no IP address is assigned to an IP service-capable interface, its protocol status is Down. - DOWN (CFM down): indicates that CFM detects a fault or receives a fault notification message from its associated module. In this case, the link layer protocol of the interface becomes CFM Down. - DOWN (EFM down): indicates that EFM detects a fault or receives a fault notification message from its associated module. In this case, the link layer protocol of the interface becomes EFM Down. - DOWN (DLDP down): indicates that DLDP detects a fault or receives a fault notification message from its associated module. In this case, the link layer protocol of the interface becomes DLDP Down. - DOWN (MACsec down): indicates that MACsec is not enabled on the peer interface. In this case, the link layer protocol of the interface becomes MACsec Down. **NOTE** DOWN (MACsec down) is displayed only after the MACsec plug-in is installed. Only the S5720SI, S5720S-SI, S6720SI, S5720EI, and S5720HI support MACsec.
Description	Interface description. To configure the description for an interface, run the **description** command.

Item	Description
Switch Port	A Layer 2 interface. To switch an interface to the Layer 3 mode, run the **undo portswitch** command. If the interface is a Layer 3 interface, **Route Port** is displayed here.
PVID	Default VLAN ID of the interface.
Link-type	Link type of an interface, which is displayed only when the interface works in Layer 2 mode: ● access(configured): The interface is manually configured as the access type. ● hybrid: The interface is manually configured as the hybrid type. ● trunk(configured): The interface is manually configured as the trunk type. ● dot1q-tunnel: The interface is manually configured as the dot1q-tunnel type. ● access(negotiated): The interface is automatically negotiated as the access type. ● trunk(negotiated): The interface is automatically negotiated as the trunk type. To set the link type for an interface, run the **5.3.34 port link-type** command.
The Maximum Frame Length	Maximum frame length allowed by the interface. To set the maximum frame length, run the **jumboframe enable** command.
TPID	Type of frames that are supported on the interface. By default, this field displays 0x8100, indicating an 802.1Q frame. This field is displayed only for a Layer 2 interface.
IP Sending Frames' Format	Format of frames sent by the IP protocol, including PKTFMT_ETHNT_2, Ethernet_802.3, and Ethernet_SNAP.
Hardware address	MAC address of the interface.

Item	Description
Port Mode	Working mode of the interface: - COMMON COPPER: The interface works as an electrical interface. - COMMON FIBER: The interface works as an optical interface. If the interface is a combo interface: - COMBO AUTO: The combo interface automatically selects the working mode. - FORCE FIBER: The combo interface is configured as an optical interface. - FORCE COPPER: The combo interface is configured as an electrical interface. To configure the working mode for an interface, run the **combo-port** command.
Transceiver	Type of the optical module. - This field is not displayed for electrical interfaces. - If an optical or copper module is inserted into the optical interface, the field indicates the model of the optical or copper module. - If an optical or copper module is not inserted into the optical interface, the field is not displayed. - If the optical interface is connected to the high-speed cable, the field indicates the type of the cable.
Last physical up time	Last time the interface went Up physically. If this field displays "-", the physical status of the interface does not change. If the system is configured with a time zone and is in the daylight saving time, the time is displayed in the format of YYYY-MM-DD HH:MM:SS UTC±HH:MM DST.
Last physical down time	Last time the interface went Down physically. If this field displays "-", the physical status of the interface does not change. If the system is configured with a time zone and is in the summer daylight saving time, the time is displayed in the format of YYYY-MM-DD HH:MM:SS UTC±HH:MM DST.
Current system time	Current system time. If the time zone is configured and the daylight saving time is used, the time is in YYYY-MM-DD HH:MM:SS ±HH:MM format.

Item	Description
Speed	Current rate of the interface. ● In auto-negotiation mode, the **auto speed** command configures the rate of an interface. ● In non-auto negotiation mode, the **speed** command configures the rate of an interface.
Loopback	Loopback configuration of the interface. To configure loopback on an interface, run the **loopback** command.
Duplex	Duplex mode of the interface: ● FULL: The interface works in full-duplex mode. ● HALF: The interface works in half-duplex mode. ● In auto-negotiation mode, the **auto duplex** command configures the duplex mode of an interface. ● In non-auto negotiation mode, the **duplex** command configures the duplex mode of an interface.
Negotiation	Auto-negotiation mode of the interface: ● ENABLE: The interface works in auto-negotiation mode. ● DISABLE: The interface works in non-auto negotiation mode. To configure the auto-negotiation mode for an interface, run the **negotiation auto** command.
Mdi	Network cable type of the interface. To configure the network cable type of an interface, run the **mdi** command. The Mdi field displays - for an optical interface.
Flow-control	Whether flow control is enabled: ● ENABLE: Flow control is enabled on the interface. ● DISABLE: Flow control is disabled on the interface. **NOTE** If the **flow-control** command has been executed to enable flow control on an Ethernet interface, this field displays **DISABLE** in the following situations: ● The interface is in Down state. ● The interface works in half-duplex mode.
Last 300 seconds input rate	Incoming packet rate (bits per second and packets per second) within the last 300 seconds.
Last 300 seconds output rate	Outgoing packet rate (bits per second and packets per second) within the last 300 seconds.

Item	Description
Input peak rate 0 bits/sec,Record time	Maximum rate of incoming packets and time when the maximum rate is reached.
Output peak rate 0 bits/sec,Record time	Maximum rate of outgoing packets and time when the maximum rate is reached.
Input	Total number of received packets.
Output	Total number of sent packets.
Unicast	Number of unicast packets that are received or sent by the interface.
Multicast	Number of multicast packets that are received or sent by the interface. For the S5720HI, the value of this field contains the number of pause frames.
Broadcast	Number of broadcast packets that are received or sent by the interface.
Jumbo	Number of received packets with length ranging from 1518 bytes to the maximum jumbo frame length and correct FCS values. Number of sent packets with lengths of over 1518 bytes and correct FCS. For the S5720HI, the value of this field contains the number of received packets with length ranging from 1518 bytes to the jumbo frame length configured on the interface and correct CRC values. To set the maximum jumbo frame length, run the **jumboframe enable** command. **NOTE** Only S6720EI, S6720S-EI, S5720HI and S5720EI support statistics on Jumbo frames.
Discard	Number of packets discarded by the interface during physical layer detection. On the S1720GFR, S1720GW, S1720GWR, S1720X, S1720GW-E, S1720GWR-E, S1720X-E, S2720EI, S2750EI, S5700LI, S5720LI, S5720S-LI, S5700S-LI, S5720SI, S5720S-SI, S5710-X-LI, S5730SI, S5730S-EI, S6720SI, S6720S-SI, S6720LI, and S6720S-LI, after you run the **reset qos queue statistics** command, the number of packets discarded by the interface is cleared.
Total Error	Number of error frames found during physical layer detection.

Item	Description
CRC	Number of packets shorter than 1519 bytes and with incorrect FCS values. For the S5720LI, S5720SI, S5720S-SI, S5710-X-LI, S5720HI, S5730SI, S5730S-EI, S6720SI, and S6720S-SI, the value of this field includes the number of received packets longer than the maximum jumbo frame length and with incorrect FCS values. For switches excluding the S5720EI, the value of this field contains the number of received packets with length ranging from 1518 bytes to the jumbo frame size configured on the interface and incorrect FCS values.
Giants	Number of received frames with length exceeding the maximum jumbo frame length.
Jabbers	Number of received packets with length ranging from 1518 bytes to the maximum jumbo frame length and incorrect FCS values on the S5720EI. The S2720EI, S5720LI, 720S-SI, S5710-X-LI, S5730SI, S5730S-EI, S6720SI, S6720S-SI, S6720S-EI, and S6720EI do not have the Jabbers field. On the other product models, this field indicates the number of received packets with length exceeding the maximum jumbo frame length and incorrect FCS values.
Fragments	Number of received fragmented packets. A fragmented packet is a packet shorter than 64 bytes and with incorrect CRC values. For the S5720HI, the value of this field contains the number of undersized frames with the correct CRC values received is displayed. On the S2720EI, S5720LI, S5720SI, S5720S-SI, S5710-X-LI, S5730SI, S5730S-EI, S6720SI, S6720S-SI, S6720S-EI, and S6720EI, the command output does not contain the Fragments field to display statistics about received fragmented packets.
Runts	Number of received undersized frames with correct CRC values. For the S5720LI, S5720SI, S5720S-SI, S5710-X-LI, S5730SI, S5730S-EI, S6720SI, S6720S-SI, S6720S-EI, and S6720EI, the value of this field includes the number of received fragmented packets shorter than 64 bytes and with incorrect CRC values.
DropEvents	Number of received packets that are discarded due to GBP full or back pressure.
Alignments	Number of received frames with alignment errors.
Symbols	Number of received frames with coding errors.

Item	Description
Ignoreds	Number of received MAC control frames whose OpCode is not PAUSE.
Frames	Number of packets with incorrect 802.3 length.
Collisions	Number of packets with 1 to 15 collisions during packet forwarding. For the S5720SI, S5720S-SI, S5710-X-LI, S5730SI, S5730S-EI, S6720SI, and S6720S-SI, the value of this field contains the number of frames that are not sent due to 16 consecutive collisions.
ExcessiveCollisions	Number of packets with 16 collisions and fail to be sent. On the S2720EI, S5720SI, S5720S-SI, S5710-X-LI, S5730SI, S5730S-EI, S6720SI, and S6720S-SI, the command output does not contain the ExcessiveCollisions field to display statistics about frames that are not sent due to 16 consecutive collisions.
Late Collisions	Number of packets with conflict and delayed.
Deferreds	Number of delayed packets without conflict.
Buffers Purged	Number of packets aged in the cache. The S5720SI, S5720S-SI, S5710X-LI, S6720S-EI, and S6720EI do not have the Buffers Purged field. On other models, the value of this field is always 0.
Input bandwidth utilization threshold	Threshold for inbound bandwidth usage.
Output bandwidth utilization threshold	Threshold for outbound bandwidth usage.
Input bandwidth utilization	Inbound bandwidth usage. For the S1720GFR, S1720GW, S1720GWR, S1720X, S1720GW-E, S1720GWR-E, S1720X-E, S2720EI, S2750EI, S5720SI, S5720S-SI, S5710-X-LI, S5700LI, S5720LI, S5720S-LI, S5700S-LI, S5730SI, S5730S-EI, S6720SI, S6720S-SI, S6720LI, and S6720S-LI, the bandwidth usage of Giants packets is calculated based on the configured jumbo frame length. To set the maximum jumbo frame length, run the **jumboframe enable** command.

Item	Description
Output bandwidth utilization	Outbound bandwidth usage. For the S1720GFR, S1720GW, S1720GWR, S1720X, S1720GW-E, S1720GWR-E, S1720X-E, S2720EI, S2750EI, S5720SI, S5720S-SI, S5710-X-LI, S5700LI, S5720LI, S5720S-LI, S5700S-LI, S5730SI, S5730S-EI, S6720SI, S6720S-SI, S6720LI, and S6720S-LI, the bandwidth usage of Giants packets is calculated based on the configured jumbo frame length. To set the maximum jumbo frame length, run the **jumboframe enable** command.

Related Topics

4.1.4 description (interface view)

4.1.24 shutdown (interface view)

4.1.11 display interface brief

Function

The **display interface brief** command displays brief information about the status and configuration of interfaces.

Format

display interface brief [**main**]

Parameters

Parameter	Description	Value
main	Displays brief information about an Ethernet main interface.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

The **display interface brief** command displays brief information about interfaces, including the physical status, link layer protocol status, inbound and outbound bandwidth usage within a certain period, and numbers of sent and received error packets. This information helps locate faults on interfaces.

Precautions

To clear statistics on an interface, run the **reset counters interface** command.

Example

# Display brief information about the status and configuration of interfaces.

```
<HUAWEI> 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
(ms): MACsec down
InUti/OutUti: input utility/output utility
Interface                   PHY   Protocol InUti OutUti   inErrors  outErrors
GigabitEthernet0/0/1        up    up       0.06%   100%          0   21217388
GigabitEthernet0/0/2        up    up        100%   100%          0          0
GigabitEthernet0/0/3        up    up          0%   100%          0          0
GigabitEthernet0/0/4        up    up        100%   100%          0          0
GigabitEthernet0/0/5        up    up         99%   100%          0          0
GigabitEthernet0/0/6        down  down        0%     0%         10          0
GigabitEthernet0/0/7        down  down        0%     0%         12          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       down  down        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       down  down        0%     0%          0          0
MEth0/0/1                   down  down        0%     0%          0          0
NULL0                       up    up(s)       0%     0%          0          0
```

Table 4-8 Description of the **display interface brief** command output

Item	Description
Interface	Type and number of an interface.

Item	Description
PHY	Physical status of an interface: ● up: indicates that the interface is working properly. ● down: indicates that the physical layer of the interface fails. ● *down: Administratively Down, indicating that the administrator has run the **shutdown** command on the interface. ● ^down: indicates that the interface is a backup interface. ● #down: LBDT down, indicating that loop detection is enabled on the interface. The interface is shut down when the device detects a loop on the downstream network or between interfaces. ● (l): indicates that the loopback function is enabled on the interface. ● (b): indicates that the physical layer of the interface is in BFD down state.
Protocol	Link layer protocol status of the interface: ● up: indicates that the interface is working properly. ● down: indicates that the link layer protocol fails. ● (s): indicates that the spoofing function is enabled on the interface. ● (E): indicating that the Eth-Trunk goes down because of the E-Trunk negotiation failure. ● (b): indicates that the link layer of the interface is in BFD down state. ● (e): indicates that the link layer of the interface is in ETHOAM down state. ● (dl): indicates that the link layer of the interface is in DLDP down state. ● (lb): indicates that the interface is blocked due to loops on the downstream network or between interfaces. ● (ms): indicates that the link layer of the interface is in MACsec down state because MACsec is not enabled on the peer interface. **NOTE** (ms): MACsec down is displayed only after the MACsec plug-in is installed. Only the S5720SI, S5720S-SI, S6720SI, S5720EI, and S5720HI support MACsec.

Item	Description
InUti	Average inbound bandwidth usage of an interface within the last 300 seconds. Average inbound bandwidth usage within the last 300 seconds = Average inbound traffic rate within the last 300 seconds/Interface bandwidth When the average bandwidth usage is smaller than 0.005% and greater than 0, the value 0 is displayed. When the average bandwidth usage is smaller than 0.01% and greater than 0.005%, the value 0.01% is displayed. When the interface bandwidth becomes lower, for example, the **speed** command is executed to reduce the bandwidth of an Ethernet interface, the bandwidth usage be displayed as 100% because the traffic volume is not adjusted in time. "--" indicates that an interface does not support the display of bandwidth usage.
OutUti	Average outbound bandwidth usage within the last 300 seconds. Average outbound bandwidth usage within the last 300 seconds = Average outbound traffic rate within the last 300 seconds/Interface bandwidth When the average bandwidth usage is smaller than 0.005% and greater than 0, the value 0 is displayed. When the average bandwidth usage is smaller than 0.01% and greater than 0.005%, the value 0.01% is displayed. When the interface bandwidth becomes lower, for example, the **speed** command is executed to reduce the bandwidth of an Ethernet interface, the bandwidth usage may be displayed as 100% because the traffic volume is not adjusted in time. "--" indicates that an interface does not support the display of bandwidth usage.
inErrors	The number of error packets received by an interface. The value ranges from 0 to 4294967295. The count restarts after the value exceeds the upper limit. The value becomes 0 when you run the **reset counters interface** command in the user view or when the number of received packets reaches the maximum value 0xFFFFFFFF.
outErrors	The number of error packets sent by an interface. The value ranges from 0 to 4294967295. The count restarts after the value exceeds the upper limit. The value becomes 0 when you run the **reset counters interface** command in the user view or when the number of sent packets reaches the maximum value 0xFFFFFFFF.

Related Topics

4.1.10 display interface

4.1.20 reset counters interface

4.1.12 display interface description

Function

The **display interface description** command displays the description of an interface.

Format

display interface description [*interface-type* [*interface-number*]]

display interface description [*interface-type*] **main**

Parameters

Parameter	Description	Value
interface-type [*interface-number*]	Displays the description of a specified interface. If an interface type is specified but no interface number is specified, the description of all interfaces of the specified type is displayed.	-
main	Displays the description of the main interface. ● If an interface has no sub-interfaces, description about the interface is displayed whether you specify the **main** parameter or not. ● If an interface has sub-interfaces, description about the interface and sub-interfaces is displayed if you do not specify the **main** parameter.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

The **display interface** command can also display the description of an interface. To quickly view the description of an interface, you are advised to use the **display interface description** command.

Precautions

If no interface type is specified, the description of all interfaces is displayed. If an interface type is specified but no interface number is specified, the description of all interfaces of the specified type is displayed.

If there is a great deal of statistics about traffic on Eth-Trunk interfaces, you are recommended to specify *trunk-id* to filter output information. Otherwise, a problem may occur due to excessive output information: The displayed information is repeatedly refreshed, and therefore required information cannot be located.

Only the S6720EI, S6720S-EI, S5720HI and S5720EI support sub-interfaces.

Example

# Display the description of GE0/0/1.

```
<HUAWEI> display interface description gigabitethernet 0/0/1
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
(ms): MACsec down
Interface                    PHY     Protocol Description
GE0/0/1                       down    down
```

Table 4-9 Description of the **display interface description** command output

Item	Description
Interface	Type and number of an interface. If the bandwidth of an interface exceeds 1 GB, the bandwidth value is displayed following the interface name.

Item	Description
PHY	Physical status of an interface: - up: indicates that the interface is working properly. - down: indicates that the physical layer of the interface fails. - *down: administratively down, indicating that the administrator has run the **shutdown** command on the interface. - #down: LBDT down, indicating that loopback detection is enabled on the interface. The interface is shut down when the device detects a loop on the downstream network or between interfaces. - (l): loopback, indicating that the loopback function is enabled on the interface. - (b): BFD down, indicating that the physical layer of the interface is in BFD Down state.
Protocol	Link layer protocol status of the interface: - up: indicates that the interface is working properly. - down: indicates that the link layer protocol of the interface fails. - (s): spoofing, indicating that the spoofing function is enabled on the interface. - (E): E-Trunk down, indicating that the interface goes down because of the E-Trunk negotiation failure. - (b): indicates that the link layer of the interface is in BFD down state. - (e): ETHOAM down, indicating that the link layer protocol of the interface is in ETHOAM down state. - (dl): DLDP down, indicating that the link layer protocol of the interface is in DLDP down state. - (lb): indicates that the interface is blocked due to loops on the downstream network or between interfaces. - (ms): MACsec down, indicating that the interface is Down because MACsec is not enabled on the peer interface. **NOTE** (ms): MACsec down is displayed only after the MACsec plug-in is installed. Only the S5720SI, S5720S-SI, S6720SI, S5720EI, and S5720HI support MACsec.
Description	Interface description.

Related Topics

4.1.4 description (interface view)

4.1.13 display ip interface

Function

The **display ip interface** command displays the IP configuration and statistics on interfaces. The statistics include the number of packets and bytes received and sent by interfaces, number of multicast packets sent and received by interfaces, and number of broadcast packets received, sent, forwarded, and discarded by interfaces.

The **display ip interface brief** command displays brief information about interface IP addresses, including the IP address, subnet mask, physical status, link-layer protocol status, and number of interfaces in different states.

Format

display ip interface [*interface-type interface-number*]

display ip interface brief [*interface-type* [*interface-number*] | **slot** *slot-id* [**card** *card-number*]]

display ip interface brief [*interface-type*] &<1-8>

Parameters

Parameter	Description	Value
interface-type interface-number	Specifies the type and number of an interface. If no interface is specified, IP configuration and statistics about all interfaces are displayed.	-
brief	Displays brief information, including the IP address, subnet mask, physical status, link-layer protocol status, and number of interfaces in different states.	-
slot *slot-id*	Displays the IP configuration and statistics of interfaces on the specified slot. If the slot number is not specified, brief information related to the IP addresses of the interfaces on all interface boards and main control boards is displayed.	-
card *card-number*	Displays the IP configuration and statistics of interfaces on specified card.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display ip interface brief** command to view the following information:

- IP configurations of all interfaces
- IP configurations of interfaces of the specified type and a specified interface
- IP configurations of interfaces that have IP addresses

This command, however, cannot display the IP configurations of Layer 2 interfaces or Eth-Trunk member interfaces.

NOTE

- You can run the **display interface description** command to view the interface description.
- You can run the **display interface** command to view detailed information about the running status and statistics on the interface.
- Only the S6720EI, S6720S-EI, S5720HI and S5720EI support sub-interfaces.

Example

# Display IP information about VLANIF15.

```
<HUAWEI> display ip interface vlanif 15
Vlanif15 current state : UP
Line protocol current state : UP
The Maximum Transmit Unit : 1500 bytes
input packets : 766390, bytes : 41540847, multicasts : 681817
output packets : 242239, bytes : 14679482, multicasts : 172333
Directed-broadcast packets:
 received packets:            0, sent packets:            0
 forwarded packets:           0, dropped packets:           0
Internet Address is 10.1.1.119/24
Broadcast address : 10.1.1.255
TTL being 1 packet number:    164035
TTL invalid packet number:         0
ICMP packet input number:          0
  Echo reply:                      0
  Unreachable:                     0
  Source quench:                   0
  Routing redirect:                0
  Echo request:                    0
  Router advert:                   0
  Router solicit:                  0
  Time exceed:                     0
  IP header bad:                   0
  Timestamp request:               0
  Timestamp reply:                 0
  Information request:             0
  Information reply:               0
  Netmask request:                 0
  Netmask reply:                   0
  Unknown type:                    0
```

Table 4-10 Description of the **display ip interface** command output

Item	Description
Vlanif15 current state	Physical status of the interface: - UP: indicates that the interface is physically Up. - DOWN: indicates that the interface is physically Down. - Administratively down: indicates that the administrator has run the **shutdown** command on the interface.
Line protocol current state	Link layer protocol status of the interface: - UP: The link layer protocol of the interface is running properly. - DOWN: The link layer protocol of the interface is Down or no IP address is configured on the interface.
The Maximum Transmit Unit	MTU of the interface. The default MTU of an Ethernet interface or a serial interface is 1500 bytes. Packets longer than the MTU are fragmented before being transmitted. If fragmentation is not allowed, the packets are discarded.
input packets : 766390, bytes : 41540847, multicasts : 681817	Total number of packets, bytes, and multicast packets received by the interface.
output packets : 242239, bytes : 14679482, multicasts : 172333	Total number of packets, bytes, and multicast packets sent by the interface.
Directed-broadcast packets	Number of packets broadcast on the interface directly.
received packets	Total number of received packets.
sent packets	Total number of sent packets.
forwarded packets	Total number of forwarded packets.
dropped packets	Total number of discarded packets.
Internet Address is	IP address assigned to the interface and mask length.
Broadcast address	Broadcast address of the interface.
TTL being 1 packet number	Number of packets with TTL 1.
TTL invalid packet number	Number of packets with invalid TTL.
ICMP packet input number	Number of received ICMP packets.

Item	Description
Echo reply	Number of Echo Reply packets.
Unreachable	Number of Destination Unreachable packets.
Source quench	Number of Source Quench packets.
Routing redirect	Number of Redirect packets.
Echo request	Number of Echo Request packets.
Router advert	Number of Router Advertisement packets.
Router solicit	Number of Router Solicitation packets.
Time exceed	Number of Time Exceeded packets.
IP header bad	Number of IP header error packets.
Timestamp request	Number of Timestamp Request packets.
Timestamp reply	Number of Timestamp Reply packets.
Information request	Number of Information Request packets.
Information reply	Number of Information Reply packets.
Netmask request	Number of Address Mask Request packets.
Netmask reply	Number of Address Mask Reply packets.
Unknown type	Number of unknown packets.

# Display brief IP information about VLANIF15.

```
<HUAWEI> display ip interface brief vlanif 15
*down: administratively down
^down: standby
(l): loopback
(s): spoofing
(E): E-Trunk down
Interface                         IP Address/Mask      Physical   Protocol
Vlanif15                          10.1.1.119/24        up         up
```

Table 4-11 Description of the **display ip interface brief** command output

Item	Description
*down:	Reason why an interface is physically Down. Administratively down indicates that the administrator has run the **shutdown** command on the interface.
^down	^down: indicates that the interface is a backup interface.
(l): loopback	The letter "l" refers to loopback.

Item	Description
(s): spoofing	The letter "s" refers to spoofing.
(E): E-Trunk down	Indicates that the Eth-Trunk is Down because of the protocol negotiation on the E-Trunk.
Interface	Interface type and number.
IP Address/Mask	IP address and mask of an interface.
Physical	Physical status of an interface: ● Up: indicates that the interface is physically Up. (l) indicates that the loopback function is configured on the interface. ● Down: indicates that the interface becomes faulty. ● *down: indicates that the administrator has run the **shutdown (interface view)** command on the interface. (l) indicates that the loopback function is configured on the interface. ● !down: indicates that the FIB module is suspended. In this case, the link protocol status of the interface is Down.
Protocol	Link protocol status of the interface: ● Up: indicates that the link protocol of the interface is running properly. (s) indicates that the link protocol status of the interface is Up when this interface is created and has no IP address configured. This is an inherent attribute of an interface. When this interface is configured with an IP address, (s) is still displayed. ● Down: indicates that the link protocol of the interface fails or no IP address is configured on the interface. (l) indicates that the loopback function is configured on the interface.

Related Topics

4.1.10 display interface

4.1.14 display ip interface description

Function

The **display ip interface description** command displays IP-related information (such as the IP address, subnet mask, physical layer status, link layer protocol status, and number of interfaces in different states) and description of an interface.

Format

display ip interface description [*interface-type* [*interface-number*] | *interface-type* &<1-8> | **slot** *slot-number* [**card** *card-number*]]

Parameters

Parameter	Description	Value
interface-type	Indicates the interface type. If no interface type is specified, IP-related configurations and statistics of all interfaces are displayed.	-
interface-number	Indicates the interface number, which is used together with *interface-type* to identify an interface. If no interface number is specified, IP-related configurations and statistics of interfaces in the same type are displayed.	-
interface-type	Indicates that the command can display IP-related information about interfaces of multiple types. The command can display IP-related information about interfaces in a maximum of eight types.	-
slot *slot-number*	Specifies the interface board number.	-
card *card-number*	Indicates the card number. If no card number is specified, IP-related information about all interfaces on all cards in a specified slot is displayed.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

Instead of running the **display ip interface brief** and **display interface description** commands, you can run the **display ip interface description** command to view both IP-related information and description of an interface, which facilitates the user operation.

The **display ip interface description** command cannot display information about Layer 2 interfaces. When it runs on an Eth-Trunk interface, it displays the status and description of Eth-Trunk member interfaces.

Example

# View IP-related information and description of a specified interface.

```
<HUAWEI> display ip interface description
Codes:
    Ana(Analogmodem),       Asy(Async),             Cell(Cellular),
    Dia(Dialer),            Eth(Ethernet)           GE(GigabitEthernet),
    H(Hssi),                Ima(Ima-group),         Loop(LoopBack),
    MTun(MTunnel),          S(Serial),              Tun(Tunnel),
    VE(Virtual-Ethernet),   VT(Virtual-Template)

    d(dampened),            D(down),                *D(administratively down)
    ^D(standby),            l(loopback),            s(spoofing),
    U(up)                   E(E-Trunk down)


------------------------------------------------------------------------------
Number of interfaces whose physical status is Up: 9
Number of interfaces whose physical status is Down: 1
Number of interfaces whose protocol status is Up: 9
Number of interfaces whose protocol status is Down: 1

Interface                   IP Address/Mask    Phy  Prot Description
Loop0                       10.3.0.2/32        U    U(s)
Loop1                       unassigned         U    U(s)
MEth0/0/1                   192.168.150.143/24 U    U
NULL0                       unassigned         U    U(s)
Tun1                        unassigned         U    D
Vlanif10                    unassigned         D    D
Vlanif20                    10.1.2.2/24        D    D
Vlanif30                    10.1.1.1/24        D    D
Vlanif100                   unassigned         *D   D
```

Table 4-12 Description of the **display ip interface description** command output

Item	Description
Codes:	The following information provides the full spelling and explanation of the abbreviated interface names, physical status, and link layer protocols. Full spelling of the abbreviated interface names is as follows: ● Ana: Analogmodem interfaces ● Asy: Async interfaces ● Cell: Cellular interfaces ● Dia: Dialer interfaces ● Eth: Ethernet interfaces ● GE: GigabitEthernet interfaces ● H: Hssi interfaces ● Ima: IMA-Group interfaces ● Loop: Loopback interfaces ● MTun: MTunnel interfaces ● S: Serial interfaces ● Tun: Tunnel interfaces ● VE: Virtual-Ethernet interfaces ● VT: Virtual-Template interfaces Explanation of the abbreviated physical status of the interface is as follows: ● U: indicates that the physical status of the interface is Up. U(l) indicates that the interface is enabled with the loopback function. ● d: indicates that the physical status of the interface is Down. ● *D: indicates that the network administrator has run the **shutdown** command on the interface. ● ^D: indicates that the FIB module is in the standby state. ● s: indicates that the interface is in spoofing status. ● E: indicates that the Eth-Trunk goes Down because of E-Trunk negotiation. Explanation of the abbreviated link layer protocol status is as follows: ● U: indicates that the status of the link layer protocol on the interface is Up. U(s)

Item	Description
	indicates that the link layer protocol of the interface is Up even though the interface is not configured with an IP address. (s) is an inherent attribute of the interface and will be displayed when the interface is configured with an IP address. (d) indicates that the protocol module of the interface is dampened. ● D: indicates that the link layer protocol of the interface is Down or no IP address is assigned to the interface.
Number of interfaces whose physical status is Up:	Indicates the number of interfaces whose physical status is Up.
Number of interfaces whose physical status is Down:	Indicates the number of interfaces whose physical status is Down.
Number of interfaces whose protocol status is Up:	Indicates the number of interfaces whose link layer protocol is Up.
Number of interfaces whose protocol status is Down:	Indicates the number of interfaces whose link layer protocol is Down.
Interface	Indicates the name and number of an interface.
IP Address/Mask	Indicates the IP address and subnet mask of an interface.
Phy	Indicates the physical status of an interface.
Prot	Indicates the link layer protocol status of an interface.
Description	Indicates the description of an interface, expressed in characters. A maximum of 20 characters can be displayed. When the length of the description is greater than 20 characters, only the first 16 characters are displayed and the last 3 characters are replaced by ellipsis (...). If the description of an interface is the default setting, no information is displayed.

Related Topics

4.1.10 display interface

4.1.15 display this interface

Function

The **display this interface** command displays interface information in the current interface view.

Format

display this interface

Parameters

None

Views

Interface view

Default Level

1: Monitoring level

Usage Guidelines

In the interface view, you can run the **display this interface** command to rapidly view the status of the interface and packet statistics on the interface.

Example

# Display information about GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] display this interface
GigabitEthernet0/0/1 current state : UP
Line protocol current state : UP
Description:
Switch Port,Link-type : access(negotiated),
 PVID :    1, TPID : 8100(Hex), The Maximum Frame Length is 9216
IP Sending Frames' Format is PKTFMT_ETHNT_2, Hardware address is 0025-9ef4-abcd
Last physical up time   : -
Last physical down time : 2000-04-01 23:55:43
Current system time: 2012-08-24 00:41:35+08:00
Port Mode: COMMON FIBER, Transceiver: 1000_BASE_SX_SFP
Speed : 1000,  Loopback: NONE
Duplex: FULL,  Negotiation: ENABLE
Mdi   : -, Flow-control: DISABLE
Last 300 seconds input rate 0 bits/sec, 0 packets/sec
Last 300 seconds output rate 0 bits/sec, 0 packets/sec
Input peak rate 0 bits/sec, Record time: 2007-12-26 07:23:14
Output peak rate 0 bits/sec, Record time: 2007-12-26 07:23:14

Input:  0 packets, 0 bytes
  Unicast:                      0,  Multicast:                     0
  Broadcast:                    0,  Jumbo:                         0
  Discard:                      0,  Pause:                         0
  Frames:                       0
  Total Error:                  0
  CRC:                          0,  Giants:                       0
  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,  Pause:                        0

  Total Error:                  0
  Collisions:                   0,  ExcessiveCollisions:          0
  Late Collisions:              0,  Deferreds:                    0
  Buffers Purged:               0

    Input bandwidth utilization threshold : 80.00%
    Output bandwidth utilization threshold: 80.00%
    Input bandwidth utilization  :    0%
    Output bandwidth utilization :    0%
```

Table 4-13 Description of the **display this interface** command output

Item	Description
current state	Current status of the interface: ● UP: indicates that the interface is physically Up. ● DOWN: indicates that the interface is physically Down. Protected port indicates that an interface is added to an interface protection group and set to be a protected interface. To add an interface to an interface protection group and set the interface to be a protected interface, run the **port protect-group** and **protect-group member** commands. ● Administratively down: indicates that the administrator has run the **shutdown** command on the interface. ● TRIGGER DOWN (BFD): When BFD detects a fault, the physical status of the interface becomes Down according to the OAM association. ● TRIGGER DOWN (3AH): When 3AH detects a fault, the physical status of the interface becomes Down according to the OAM association. ● TRIGGER DOWN (1AG): When 1AG detects a fault, the physical status of the interface becomes Down according to the OAM association. ● ERROR DOWN(auto-defend): When the interface receives packets from an attack source, the physical status of the interface becomes Down. ● ERROR DOWN(efm-threshold-event): When the number of error frames, error codes, or error frame seconds of EFM OAM detected by the interface reaches or exceeds the threshold within a set period, the physical status of the interface becomes Down according to the OAM association. ● ERROR DOWN(efm-remote-failure): When EFM detects a remote failure, the physical status of the interface becomes Down according to the OAM association. ● ERROR DOWN(bpdu-protection): If an edge interface receives RST BPDUs after BPDU protection is enabled, the physical status of the edge interface becomes Down. ● ERROR DOWN(error-statistics): If the system detects that the number of error packets received by the interface exceeds the threshold, the physical status of the interface becomes Down. ● ERROR DOWN(runts-error-statistics): When the number of Runts error packets received by the

Item	Description
	interface reaches the alarm threshold, the physical status of the interface becomes Down. ● ERROR DOWN(transceiver-power-low): If the system detects that the optical power of the interface falls below the configured lower alarm threshold, the physical status of the interface becomes Down. ● ERROR DOWN(port-security): When the number of learned MAC address entries reaches the threshold, the interface goes Down. ● ERROR DOWN(mac-address-flapping): When the learned MAC address flaps, the interface goes Down. ● ERROR DOWN(dhcp-packet-overspeed): When the DHCP packet rate of the interface exceeds the threshold, the physical status of the associated interface becomes Down. ● ERROR DOWN(link-flap): When the link flaps, the physical status of the associated interface becomes Down. ● ERROR DOWN(data-integrity-error): The chip memory identifier has a data integrity error and the physical status of the interface becomes Down. ● UP(E-TRUNK-DOWN): The Eth-Trunk interface goes Down because of E-Trunk negotiation. **NOTE** There is a delay before the interface state is reported, so an interface undergoes a short-time intermediate state before it transitions to the ERROR DOWN state. The intermediate state is ERROR DOWN (ERROR DOWN reason), up. This state does not affect functioning of the interface. When the physical status of the interface is ERROR DOWN(data-integrity-error), perform the following operations: 1. Check whether the **error-down auto-recovery cause data-integrity-error interval** *interval-value* command has been configured on the switch. If the command has been configured, go to step 2. Otherwise, go to step 3. 2. Check whether the interface restores to Up state after the time specified by *interval-value* expires. If the interface does not restore to Up state, go to step 3. 3. Run the **undo shutdown** command in the interface view to enable the interface and check whether the interface restores to Up state. If the interface does not restore to Up state, go to step 4. 4. Run the **reset slot** command to restart the switch. After the switch restarts, check whether the interface restores to Up state. If the interface does not restore to Up state, go to step 5. 5. Replace the switch.

Item	Description
Line protocol current state	Link layer protocol status of the interface: ● UP: indicates that the link layer protocol of the interface is working properly. ● UP (BFD status down): indicates that BFD associated with the interface is Down. ● UP (Main BFD status down): indicates that the BFD session associated with the main interface becomes Down and is associated with the sub-interface status. This state is displayed only for sub-interfaces. ● UP (spoofing): indicates that the link layer protocol of the interface is always Up with the spoofing feature enabled. ● DOWN: indicates that the link-layer protocol status of the interface is Down or no IP address is assigned to the interface. For example, if no IP address is assigned to an IP service-capable interface, its protocol status is Down. ● DOWN (CFM down): indicates that CFM detects a fault or receives a fault notification message from its associated module. In this case, the link layer protocol of the interface becomes CFM Down. ● DOWN (EFM down): indicates that EFM detects a fault or receives a fault notification message from its associated module. In this case, the link layer protocol of the interface becomes EFM Down. ● DOWN (DLDP down): indicates that DLDP detects a fault or receives a fault notification message from its associated module. In this case, the link layer protocol of the interface becomes DLDP Down. ● DOWN (MACsec down): indicates that MACsec is not enabled on the peer interface. In this case, the link layer protocol of the interface becomes MACsec Down. **NOTE** DOWN (MACsec down) is displayed only after the MACsec plug-in is installed. Only the S5720SI, S5720S-SI, S6720SI, S5720EI, and S5720HI support MACsec.
Description	Interface description. To configure the description for an interface, run the **description** command.

Item	Description
Switch Port	A Layer 2 interface. To switch an interface to the Layer 3 mode, run the **undo portswitch** command. If the interface is a Layer 3 interface, **Route Port** is displayed here.
PVID	Default VLAN ID of the interface.
Link-type	Link type of an interface, which is displayed only when the interface works in Layer 2 mode: ● access(configured): The interface is manually configured as the access type. ● hybrid: The interface is manually configured as the hybrid type. ● trunk(configured): The interface is manually configured as the trunk type. ● dot1q-tunnel: The interface is manually configured as the dot1q-tunnel type. ● access(negotiated): The interface is automatically negotiated as the access type. ● trunk(negotiated): The interface is automatically negotiated as the trunk type. To set the link type for an interface, run the **5.3.34 port link-type** command.
The Maximum Frame Length	Maximum frame length allowed by the interface. To set the maximum frame length, run the **jumboframe enable** command.
TPID	Type of frames that are supported on the interface. By default, this field displays 0x8100, indicating an 802.1Q frame. This field is displayed only for a Layer 2 interface.
IP Sending Frames' Format	Format of frames sent by the IP protocol, including PKTFMT_ETHNT_2, Ethernet_802.3, and Ethernet_SNAP.
Hardware address	MAC address of the interface.

Item	Description
Port Mode	Working mode of the interface: ● COMMON COPPER: The interface works as an electrical interface. ● COMMON FIBER: The interface works as an optical interface. If the interface is a combo interface: ● COMBO AUTO: The combo interface automatically selects the working mode. ● FORCE FIBER: The combo interface is configured as an optical interface. ● FORCE COPPER: The combo interface is configured as an electrical interface. To configure the working mode for an interface, run the **combo-port** command.
Transceiver	Type of the optical module. ● This field is not displayed for electrical interfaces. ● If an optical or copper module is inserted into the optical interface, the field indicates the model of the optical or copper module. ● If an optical or copper module is not inserted into the optical interface, the field is not displayed. ● If the optical interface is connected to the high-speed cable, the field indicates the type of the cable. ● For the S5720SI and S5720LI, if an H87MMA5671A2 GPON optical module or a faulty optical module is inserted into an optical interface, the value of this field is ONLINE within about 1 minute. After 1 minute, the value of this field becomes the type of the GPON optical module or becomes empty for the faulty optical module accordingly.
Last physical up time	Last time the interface went Up physically. If this field displays "-", the physical status of the interface does not change. If the system is configured with a time zone and is in the daylight saving time, the time is displayed in the format of YYYY-MM-DD HH:MM:SS UTC±HH:MM DST.
Last physical down time	Last time the interface went Down physically. If this field displays "-", the physical status of the interface does not change. If the system is configured with a time zone and is in the summer daylight saving time, the time is displayed in the format of YYYY-MM-DD HH:MM:SS UTC±HH:MM DST.

Item	Description
Current system time	Current system time. If the time zone is configured and the daylight saving time is used, the time is in YYYY-MM-DD HH:MM:SS ±HH:MM format.
Speed	Current rate of the interface. ● In auto-negotiation mode, the **auto speed** command configures the rate of an interface. ● In non-auto negotiation mode, the **speed** command configures the rate of an interface.
Loopback	Loopback configuration of the interface. To configure loopback on an interface, run the **loopback** command.
Duplex	Duplex mode of the interface: ● FULL: The interface works in full-duplex mode. ● HALF: The interface works in half-duplex mode. ● In auto-negotiation mode, the **auto duplex** command configures the duplex mode of an interface. ● In non-auto negotiation mode, the **duplex** command configures the duplex mode of an interface.
Negotiation	Auto-negotiation mode of the interface: ● ENABLE: The interface works in auto-negotiation mode. ● DISABLE: The interface works in non-auto negotiation mode. To configure the auto-negotiation mode for an interface, run the **negotiation auto** command.
Mdi	Network cable type of the interface. To configure the network cable type of an interface, run the **mdi** command. The Mdi field displays - for an optical interface.
Flow-control	Whether flow control is enabled: ● ENABLE: Flow control is enabled on the interface. ● DISABLE: Flow control is disabled on the interface. **NOTE** If the **flow-control** command has been executed to enable flow control on an Ethernet interface, this field displays **DISABLE** in the following situations: ● The interface is in Down state. ● The interface works in half-duplex mode.

Item	Description
Last 300 seconds input rate	Incoming packet rate (bits per second and packets per second) within the last 300 seconds.
Last 300 seconds output rate	Outgoing packet rate (bits per second and packets per second) within the last 300 seconds.
Input peak rate 0 bits/sec,Record time	Maximum rate of incoming packets and time when the maximum rate is reached.
Output peak rate 0 bits/sec,Record time	Maximum rate of outgoing packets and time when the maximum rate is reached.
Input	Total number of received packets.
Output	Total number of sent packets.
Unicast	Number of unicast packets that are received or sent by the interface.
Multicast	Number of multicast packets that are received or sent by the interface. For the S5720HI, the value of this field contains the number of pause frames.
Broadcast	Number of broadcast packets that are received or sent by the interface.
Jumbo	Number of received packets with length ranging from 1518 bytes to the maximum jumbo frame length and correct FCS values. Number of sent packets with lengths of over 1518 bytes and correct FCS. For the S5720HI, the value of this field contains the number of received packets with length ranging from 1518 bytes to the jumbo frame length configured on the interface and correct CRC values. To set the maximum jumbo frame length, run the **jumboframe enable** command. **NOTE** Only S6720EI, S6720S-EI, S5720HI and S5720EI support statistics on Jumbo frames.
Discard	Number of packets discarded by the interface during physical layer detection. On the S1720GFR, S1720GW, S1720GWR, S1720X, S1720GW-E, S1720GWR-E, S1720X-E, S2720EI, S2750, S5700LI, S5720LI, S5720S-LI, S5700S-LI, S5720SI, S5720S-SI, S5710–X-LI, S5730SI, S5730S-EI, S6720SI, S6720S-SI, S6720LI and S6720S-LI, after you run the **reset qos queue statistics** command, the number of packets discarded by the interface is cleared.

Item	Description
Total Error	Number of error frames found during physical layer detection.
CRC	Number of packets shorter than 1519 bytes and with incorrect FCS values. For the S5720LI, S5720SI, S5720S-SI, S5710X-LI, S5720HI, S5730SI, S5730S-EI, S6720SI, and S6720S-SI, the value of this field includes the number of received packets longer than the maximum jumbo frame length and with incorrect FCS values. For switches excluding the S5720EI, the value of this field contains the number of received packets with length ranging from 1518 bytes to the jumbo frame size configured on the interface and incorrect FCS values.
Giants	Number of received frames with length exceeding the maximum jumbo frame length.
Jabbers	Number of received packets with length ranging from 1518 bytes to the maximum jumbo frame length and incorrect FCS values on the S5720EI. The S5720LI, S5720SI, S5720S-SI, S5710X-LI, S5730SI, S5730S-EI, S6720SI, S6720S-SI, S6720S-EI, and S6720EI do not have the Jabbers field. On the other product models, this field indicates the number of received packets with length exceeding the maximum jumbo frame length and incorrect FCS values.
Fragments	Number of received fragmented packets. A fragmented packet is a packet shorter than 64 bytes and with incorrect CRC values. For the S5720HI, the value of this field contains the number of undersized frames with the correct CRC values received is displayed. On the S5720LI, S5720SI, S5720S-SI, S5710X-LI, S5730SI, S5730S-EI, S6720SI, S6720S-SI, S6720S-EI, and S6720EI, the command output does not contain the Fragments field to display statistics about received fragmented packets.
Runts	Number of received undersized frames with correct CRC values. For the S5720LI, S5720SI, S5720S-SI, S5710X-LI, S5730SI, S5730S-EI, S6720SI, S6720S-SI, S6720S-EI, and S6720EI, the value of this field includes the number of received fragmented packets shorter than 64 bytes and with incorrect CRC values.
DropEvents	Number of received packets that are discarded due to GBP full or back pressure.

Item	Description
Alignments	Number of received frames with alignment errors.
Symbols	Number of received frames with coding errors.
Ignoreds	Number of received MAC control frames whose OpCode is not PAUSE.
Frames	Number of packets with incorrect 802.3 length.
Collisions	Number of packets with 1 to 15 collisions during packet forwarding. For the S5720SI, S5720S-SI, S5710X-LI, S5730SI, S5730S-EI, S6720SI, S6720S-SI, S6720S-EI, and S6720EI, the value of this field contains the number of frames that are not sent due to 16 consecutive collisions.
ExcessiveCollisions	Number of packets with 16 collisions and fail to be sent. On the S5720SI, S5720S-SI, S5710X-LI, S5730SI, S5730S-EI, S6720SI, S6720S-SI, S6720S-EI, and S6720EI, the command output does not contain the ExcessiveCollisions field to display statistics about frames that are not sent due to 16 consecutive collisions.
Late Collisions	Number of packets with conflict and delayed.
Deferreds	Number of delayed packets without conflict.
Buffers Purged	Number of packets aged in the cache.
Input bandwidth utilization threshold	Threshold for inbound bandwidth usage.
Output bandwidth utilization threshold	Threshold for outbound bandwidth usage.
Input bandwidth utilization	Inbound bandwidth usage. For the S1720GFR, S1720GW, S1720GWR, S1720X, S1720GW-E, S1720GWR-E, S1720X-E, S2720EI, S2750EI, S5720SI, S5720S-SI, S5710-X-LI, S5700LI, S5720LI, S5720S-LI, S5700S-LI, S5730SI, S5730S-EI, S6720SI, S6720S-SI, S6720LI, and S6720S-LI, the bandwidth usage of Giants packets is calculated based on the configured jumbo frame length. To set the maximum jumbo frame length, run the **jumboframe enable** command.

Item	Description
Output bandwidth utilization	Outbound bandwidth usage. For the S1720GFR, S1720GW, S1720GWR, S1720X, S1720GW-E, S1720GWR-E, S1720X-E, S2720EI, S2750EI, S5720SI, S5720S-SI, S5710-X-LI, S5700LI, S5720LI, S5720S-LI, S5700S-LI, S5730SI, S5730S-EI, S6720SI, S6720S-SI, S6720LI, and S6720S-LI, the bandwidth usage of Giants packets is calculated based on the configured jumbo frame length. To set the maximum jumbo frame length, run the **jumboframe enable** command.

Related Topics

4.1.10 display interface

4.1.11 display interface brief

4.1.16 interface

Function

The **interface** command displays the interface view or sub-interface view.

The **undo interface** command deletes a sub-interface.

Format

interface *interface-type interface-number*

undo interface *interface-type interface-number*

Parameters

Parameter	Description	Value
interface-type interface-number	Specifies the type and number of an interface. The interface type and number can be closely next to each other or separated by a space character. To create a sub-interface, enter the sub-interface view, or delete a sub-interface, specify *interface-number* in the format of main interface number.sub-interface number. For example, the number of sub-interface 1 on GE0/0/1 is GE0/0/1.1.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After the specified interface view is displayed, you can set attributes for the interface.

Precautions

- Physical interfaces cannot be created or deleted. You can only run the **interface** *interface-type interface-number* command to enter the view of an existing physical interface.
- You need to set the interface type before creating a sub-interface. Only hybrid and trunk interfaces on the preceding series of cards support Ethernet sub-interface configuration.
- Sub-interfaces can be created. Run the **interface** *interface-type interface-number* command to create a sub-interface and enter the sub-interface view.
- Sub-interfaces can be deleted. Run the **undo interface** *interface-type interface-number* command to delete a sub-interface.
- Only the S6720EI, S6720S-EI, S5720HI and S5720EI support sub-interfaces.

Example

# Display the view of GE0/0/1.

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

# Create sub-interface GE0/0/1.1.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] port link-type hybrid
[HUAWEI-GigabitEthernet0/0/1] quit
[HUAWEI] interface gigabitethernet 0/0/1.1
```

# Delete sub-interface GE0/0/1.1.

```
<HUAWEI> system-view
[HUAWEI] undo interface gigabitethernet 0/0/1.1
```

Related Topics

4.1.10 display interface

5.2.31 interface eth-trunk

4.1.17 mtu (Interface view)

Function

Using the **mtu** command, you can set the maximum transmission unit (MTU) of an interface.

Using the **undo mtu** command, you can restore the default MTU of an interface.

By default, the MTU of an interface is 1500 bytes.

Format

mtu *mtu*

undo mtu

Parameters

Parameter	Description	Value
mtu	Specifies the MTU of an interface.	● For a physical interface , a VLANIF interface , an Eth-Trunk interface , a physical sub-interface and an Eth-Trunk sub-interface , the value is an integer that ranges from 128 to 9216, in bytes. ● For a VE sub-interface, the value is an integer that ranges from 46 to 1500, in bytes. ● For a VBDIF interface, the value is an integer that ranges from 46 to 1560, in bytes. ● For a tunnel interface, the value is an integer. For the S5720EI, S5720HI, S6720EI, and S6720S-EI, the value ranges from 128 to 9216, in bytes. For other switch models, the value ranges from 128 to 1530, in bytes.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The maximum transmission unit (MTU) determines the maximum number of bytes in IP packets each time a sender can send. The MTU of an IP packet refers to the number of bytes from the IP header of the packet to the data.

The size of data frames is limited at the network layer. Any time the IP layer receives an IP packet to be sent, it checks to which local interface the packet needs to be sent and obtains the MTU configured on the interface. Then the IP layer compares the MTU with the packet length. If the packet length is longer than the MTU, the IP layer fragments the packet into smaller packets, which are shorter than or equal to the MTU. If unfragmentation is configured, some packets may be discarded during data transmission at the IP layer. To ensure jumbo packets are not dropped during transmission, you need to configure forcible fragmentation. In this case, you can run the **mtu** command to set the size of a fragment.

Therefore, a proper MTU is a prerequisite for normal communication on a network.

- If the configured MTU is excessively small and the packet size is larger, packets are discarded when being forwarded through the forwarding chip; packets are broken into a great number of fragments when being forwarded through the CPU, affecting proper data transmission.
- If the size of packets exceeds the MTU supported by a transit node or a receiver, the transit node or receiver fragments the packets or even discards them, aggravating the network transmission load.

The default MTU is recommended. When the size of packets to be transmitted or the device that receives packets changes, you can change the MTU based on the actual network.

NOTE

The configured MTU takes effect for data packets on the control plane.

For S5720HI, the configured MTU takes effect for data packets on the forwarding plane after you run the **ipv4 fragment enable** command to enable packet fragmentation. The configured MTU takes effect for GRE packets on the forwarding plane without the need to execute the **ipv4 fragment enable** command.

For other devices, the configured MTU does not take effect for data packets on the forwarding plane.

Prerequisites

Run **undo portswitch** command to change the working mode of Ethernet interfaces from Layer 2 mode to Layer 3 mode.

Precautions

- After changing the maximum transmission unit (MTU) using the **mtu** command on an interface, you need to restart the interface to make the new MTU take effect. To restart the interface, run the **shutdown** command and then the **undo shutdown** command, or run the **restart** command in the interface view.
- If IPv6 is run on a tunnel interface and the MTU set using the **mtu** command on the interface is smaller than 1280, IPv6 works abnormally on this interface.

To prevent this problem, set the MTU of a tunnel interface to a value greater than or equal to 1280 if IPv6 runs on the tunnel interface.

- Configuring the MTU of an interface affects the maximum number of bytes for IP packets to be sent by the interface at a time. This configuration also affects the maximum frame length of sent Ethernet packets. The Ethernet packet size cannot exceed the maximum frame length allowed by the peer interface, which can be set using the **jumboframe enable** command.

Example

# Set the MTU of GE0/0/1 to 1200 bytes.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] mtu 1200
[HUAWEI-GigabitEthernet0/0/1] restart
```

# Set the MTU of the VLANIF interface to 1492 bytes.

```
<HUAWEI> system-view
[HUAWEI] interface Vlanif 100
[HUAWEI-Vlanif100] mtu 1492
[HUAWEI-Vlanif100] restart
```

# Set the MTU of Tunnel 1 to 1492.

```
<HUAWEI> system-view
[HUAWEI] interface tunnel 1
[HUAWEI-Tunnel1] mtu 1492
[HUAWEI-Tunnel1] shutdown
[HUAWEI-Tunnel1] undo shutdown
```

Related Topics

5.3.44 shutdown (VLANIF interface view)

10.1.4 display interface tunnel

18.1.11 display interface vbdif

4.1.18 port description

Function

The **port description** command configures description about the device type connected to an interface.

The **undo port description** command restores the default setting.

By default, no description about the device type connected to an interface is configured.

Format

port description { **router** | **switch** | **phone** | **desktop** }

undo port description

Parameters

Parameter	Description	Value
router	Indicates that the interface is connected to a router.	-
switch	Indicates that the interface is connected to a switch.	-
phone	Indicates that the interface is connected to an IP phone.	-
desktop	Indicates that the interface is connected to a desktop terminal, such as a PC.	-

Views

Ethernet interface view, GE interface view, XGE interface view, MultiGE interface view, 40GE interface view, Eth-Trunk interface view , port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can run this command to configure description about the device type connected to an interface to facilitate device management and maintenance. For example, you can run **port description router** command to indicate that the interface is connected to a router.

Precautions

After you configure this command on an interface, the interface can still switch between Layer 2 and Layer 3 modes.

Example

# Specify description of the Ethernet interface GE0/0/1 to **router** to indicate that the interface is connected to a router.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] port description router
```

4.1.19 reset counters if-mib interface

Function

The **reset counters if-mib interface** command clears interface traffic statistics in the Network Management System (NMS).

Format

reset counters if-mib interface [*interface-type* [*interface-number*]]

Parameters

Parameter	Description	Value
interface-type [*interface-number*]	Clears traffic statistics on a specified interface in the NMS. ● *interface-type* specifies the interface type. ● *interface-number* specifies the interface number. If an interface type is specified but no interface number is specified, traffic statistics on all interfaces of the specified type are cleared.	-

Views

User view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

Before collecting traffic statistics on a specific interface within a period in the NMS, clear existing traffic statistics on this interface in the NMS.

NOTE

For details on how to view interface traffic statistics in the NMS, see the NMS documentation.

Precautions

- If no interface type and number are specified, traffic statistics of all interfaces in the NMS are cleared.
- After you run the **reset counters if-mib interface** command, traffic statistics on all interfaces in the NMS are cleared. Therefore, confirm the action before you run this command.

- Running the **reset counters if-mib interface** command does not affect the interface traffic statistics displayed by the **display interface** command. To clear the interface traffic statistics displayed by the **display interface** command, run the **reset counters interface** command.

Example

# Clear traffic statistics on GE0/0/1 in the NMS.

```
<HUAWEI> reset counters if-mib interface gigabitethernet 0/0/1
```

Related Topics

4.1.20 reset counters interface

4.1.20 reset counters interface

Function

The **reset counters interface** command clears traffic statistics about a specified interface.

Format

reset counters interface [*interface-type* [*interface-number*]]

Parameters

Parameter	Description	Value
interface-type [*interface-number*]	Clears traffic statistics on a specified interface. ● *interface-type* specifies the interface type. ● *interface-number* specifies the interface number. If an interface type is specified but no interface number is specified, traffic statistics on all interfaces of the specified type are cleared.	-

Views

User view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

Before collecting traffic statistics on an interface within a certain period, run the **reset counters interface** command to clear existing traffic statistics.

Precautions

- Statistics cannot be restored after being cleared. Therefore, exercise caution before clearing the statistics.
- Traffic accounting is based on the packet statistics on an interface. The clearing of the packet statistics on an interface by using the **reset counters interface** command affects the traffic accounting result. Therefore, do not randomly clear the packet statistics on an interface in a normal application environment.
- If no interface type is specified, traffic statistics on all types of interfaces are cleared. If an interface type is specified but no interface number is specified, traffic statistics on all interfaces of the specified type are cleared.
- Running the **reset counters interface** command clears the last part of the **display interface** command output. That is, statistics about received and transmitted packets on the interface are cleared.

Example

# Clear traffic statistics on all interfaces.

```
<HUAWEI> reset counters interface
```

# Clear traffic statistics on VLANIF10.

```
<HUAWEI> reset counters interface vlanif 10
```

Related Topics

4.1.10 display interface

4.1.11 display interface brief

4.1.21 reset counters top interface

Function

The **reset counters top interface** command clears top N interface traffic statistics reports.

Format

reset counters top interface report [*report-number*]

Parameters

Parameter	Description	Value
report-number	Specifies the number of the top N interface traffic statistics report to be deleted. If you do not specify this parameter, the command clears all top N interface traffic statistics reports.	The value is an integer ranging from 1 to 5.

Views

User view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

The top N interface traffic statistics function allows a device to generate a maximum of five top N interface traffic statistics reports. If you want to generate new top N interface traffic statistics reports when five top N interface traffic statistics reports already exist, run the **reset counters top interface report** [*report-number*] command to clear existing ones.

Precautions

- After you run the **reset counters top interface report** *report-number* command to clear a specified top N interface traffic statistics report, the numbers of other top N interface traffic statistics reports remain unchanged.
- You can run the **reset counters top interface report** [*report-number*] command even if less than five top N interface traffic statistics reports exist.

Example

# Clear all top N interface traffic statistics reports.

```
<HUAWEI> reset counters top interface report
```

# Clear the top N interface traffic statistics report numbered 1.

```
<HUAWEI> reset counters top interface report 1
```

4.1.22 restart (interface view)

Function

The **restart** command restarts an interface.

Format

restart

Parameters

None

Views

Ethernet interface view, GE interface view, XGE interface view, MultiGE interface view, 40GE interface view, Eth-Trunk interface view, VLANIF interface view, Sub-interface view, Tunnel interface view, VE interface view, VE sub-interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After modifying parameters of an interface, run the **restart** command to make the modification take effect.

Precautions

- Restarting an interface during data transmission will cause data frame loss or service interruption. Exercise caution when you use the **restart** command.
- Running the **restart** command is equivalent to running the **shutdown** command and the **undo shutdown** command in sequence.
- Only the S6720EI, S6720S-EI, S5720HI and S5720EI support sub-interfaces.

Example

# Restart GE0/0/1.

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

Related Topics

4.1.24 shutdown (interface view)

4.1.23 set flow-stat interval

Function

The **set flow-stat interval** command sets the interval for collecting the traffic statistics on interfaces.

The **undo set flow-stat interval** command restores the default interval for collecting traffic statistics on interfaces.

By default, the interval for collecting traffic statistics on interfaces is 300 seconds.

Format

set flow-stat interval *interval-time*

undo set flow-stat interval

Parameters

Parameter	Description	Value
interval-time	Specifies the interval for collecting traffic statistics on interfaces.	The value is an integer that ranges from 10 to 600, in seconds. In addition, the value must be a multiple of 10. The default value is 300s.

Views

System view, Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

By using the **set flow-stat interval** command to set the interval for collecting traffic statistics on interfaces, you can collect and analyze traffic statistics according to your needs. You can also take traffic control measures based on the traffic statistics to prevent network congestion and service interruption.

- When congestion occurs, set the interval for collecting traffic statistics on an interface to less than 300 seconds, or 30 seconds if congestion worsens. Then observe the traffic distribution on the interface within a short period of time. If data packets cause congestion, take proper measures to control the rate of the packets.
- When the network bandwidth is sufficient and services are running properly, set the interval for collecting traffic statistics on an interface to more than 300 seconds. If the value of any traffic parameter is not within the specified range, change the interval for collecting traffic statistics to observe the traffic volume in real time.

Precautions

- The interval configured in the system view takes effect on all the interfaces that use the default interval.
- The interval configured in the interface view takes effect only on the current interface.
- The interval configured in the interface view takes precedence over the interval configured in the system view.

Example

# Set the interval for collecting traffic statistics on GE0/0/1 to 400s.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] set flow-stat interval 400
```

Related Topics

4.1.10 display interface

4.1.20 reset counters interface

4.1.20 reset counters interface

4.1.24 shutdown (interface view)

Function

The **shutdown** command disables an interface.

The **undo shutdown** command enables an interface.

By default, interfaces are enabled.

Format

shutdown

undo shutdown

Parameters

None

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After modifying parameters of an interface, run the **shutdown** and **undo shutdown** commands to make the modification take effect.

When an interface is not connected to a cable or fiber, you can use the **shutdown** command to disable the interface to prevent exceptions caused by interference.

Precautions

- When the device supports the autocomplete function, you must enter at least the characters **shut** before the device can automatically complete the **shutdown** command.

- Disabling an interface during data transmission will cause data frame loss or service interruption. Exercise caution when you use the **shutdown** command.
- Some logical interfaces, such as loopback, and null interfaces, do not support the **shutdown** and **undo shutdown** commands.
- If you run the **shutdown** command in the Eth-Trunk interface view, all Eth-Trunk member interfaces are disabled.
- Running the **shutdown** and **undo shutdown** commands is equivalent to running the **restart** command.

Example

# Shut down GE0/0/1.

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

Related Topics

4.1.10 display interface

5.2.25 eth-trunk

4.1.22 restart (interface view)

4.2 Ethernet Interface Configuration Commands

4.2.1 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.

4.2.2 am isolate

Function

The **am isolate** command isolates the current interface from a specified interface unidirectionally.

The **undo am isolate** command cancels unidirectional isolation between the current interface and a specified interface. If no interface is specified, unidirectional isolation between the current interface and all the other interfaces is canceled.

By default, no unidirectional isolation is configured between the current interface and a specified interface.

Format

am isolate { *interface-type interface-number* }&<1-8>

undo am isolate [*interface-type interface-number*]&<1-8>

am isolate *interface-type interface-number1* [**to** *interface-number2*]

undo am isolate [*interface-type interface-number1* [**to** *interface-number2*]]

Parameters

Parameter	Description	Value
interface-type interface-number	Specifies the type and number of the interface from which the current interface is isolated unidirectionally. ● *interface-type* specifies the type of the interface. ● *interface-number* specifies the number of the interface.	-
interface-type interface-number1 [**to** *interface-number2*]	Specifies the type and number of the interface from which the current interface is isolated unidirectionally. **to** specifies an interface range, indicating all the interfaces numbered between *interface-number1* and *interface-number2*.	*interface-number2* must be greater than *interface-number1*.

Views

Ethernet interface view, GE interface view, XGE interface view, MultiGE interface view, 40GE interface view, Eth-Trunk interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **am isolate** command isolates interfaces unidirectionally. For example, if interface A is isolated from interface B unidirectionally, packets sent from interface A cannot reach interface B, but packets sent from interface B can reach interface A. Unidirectional isolation needs to be configured in the following scenarios:

- When multiple hosts connect to different interfaces of a device and a host sends many broadcast packets to the other hosts, isolate the interface connected to the host from other interfaces unidirectionally. Then the other hosts do not receive packets from the host.
- Interfaces in a port isolation group are isolated from each other, but interfaces in different port isolation groups can communicate. To isolate interfaces in different port isolation groups, configure unidirectional isolation between these interfaces.

By default, only Layer 2 packets of the current interface are isolated from a specified interface, but Layer 3 packets are not isolated. To isolate both Layer 2 and Layer 3 packets on interfaces unidirectionally, run the **port-isolate mode all** command.

Precautions

An interface can be unidirectionally isolated from another type of interface. However, an interface cannot be unidirectionally isolated from itself or from the management interface. In addition, an Eth-Trunk cannot be unidirectionally isolated from its member interfaces.

NOTE

An interface can be isolated from a maximum of 128 interfaces unidirectionally.

Example

# Isolate GE0/0/1 from GE0/0/2 unidirectionally.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] am isolate gigabitethernet 0/0/2
```

4.2.3 auto duplex

Function

The **auto duplex** command configures the duplex mode on an Ethernet electrical interface in auto-negotiation mode.

The **undo auto duplex** command restores the default duplex mode on an Ethernet electrical interface in auto-negotiation mode.

By default, the duplex mode on an Ethernet electrical interface is negotiated with the peer interface.

Format

auto duplex { **half** | **full** }*

undo auto duplex

Parameters

Parameter	Description	Value
half	Sets the duplex mode on an Ethernet electrical interface in auto-negotiation mode to half-duplex.	-
full	Sets the duplex mode on an Ethernet electrical interface in auto-negotiation mode to full-duplex.	-

Views

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

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In auto-negotiation mode, interfaces on both ends of a link negotiate their duplex mode. If the negotiated duplex mode is not the required one, you can run the **auto duplex** command to set the required duplex mode in auto-negotiation mode.

- If service traffic volume of enterprise users is high, interfaces at both ends of a link must work in full-duplex mode. Otherwise, packet loss occurs. You can run the **auto duplex** **full** command to set the duplex mode to full-duplex. After the auto-negotiation succeeds, the interfaces work in full-duplex mode.
- If service traffic volume of enterprise users is low, interfaces at both ends of a link can meet data transmission requirements when they work in half-duplex mode. You can run the **auto duplex** **half** command to set the duplex mode to half-duplex. After the auto-negotiation succeeds, the interfaces work in half-duplex mode.

Prerequisites

Run the **negotiation auto** command to configure Ethernet interface to work in auto-negotiation mode.

Precautions

- In auto-negotiation mode, an FE electrical interface negotiates the duplex mode with the peer device on the link.

- In auto-negotiation mode, a GE electrical interface that works at a rate of 1000 Mbit/s only supports the full-duplex mode. If the duplex mode is changed to half-duplex, the GE electrical interface works at a maximum rate of 100 Mbit/s.
- The GE optical interfaces support the duplex mode configuration when they are equipped with GE copper modules.
- The interfaces on both ends of a link must have the same duplex mode.

Example

# Configure Ethernet electrical interface GE0/0/1 in auto-negotiation mode to work in half-duplex mode.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] negotiation auto
[HUAWEI-GigabitEthernet0/0/1] auto duplex half
```

Related Topics

4.2.38 negotiation auto

4.2.4 auto speed

Function

The **auto speed** command configures the auto-negotiation rate of an Ethernet electrical interface.

The **undo auto speed** command restores the default auto-negotiation rate of an Ethernet electrical interface.

By default, Ethernet electrical interfaces on both ends can negotiate to any rate they support.

Format

auto speed { **10** | **100** | **1000** | **2500** | **5000** | **10000** } *

undo auto speed

Parameters

Parameter	Description	Value
10	Sets the auto-negotiation rate of an Ethernet electrical interface to 10 Mbit/s.	-
100	Sets the auto-negotiation rate of an Ethernet electrical interface to 100 Mbit/s.	-

Parameter	Description	Value
1000	Sets the auto-negotiation rate of an Ethernet electrical interface to 1000 Mbit/s. **NOTE** FE electrical interfaces do not support this parameter. When an XGE interface has a GE copper module installed, the rate of the interface can only be negotiated to 1000 Mbit/s or 100 Mbit/s. Only the rate of XGE interfaces on the S6720LI, S6720S-LI, S6720SI, S6720S-SI, S6720EI and S6720S-EI can be negotiated to 100 Mbit/s.	-
2500	Sets the auto-negotiation rate of an Ethernet electrical interface to 2500 Mbit/s. **NOTE** Only MultiGE interfaces support this parameter.	-
5000	Sets the auto-negotiation rate of an Ethernet electrical interface to 5000 Mbit/s. **NOTE** Only MultiGE interfaces support this parameter.	-
10000	Sets the auto-negotiation rate of an Ethernet electrical interface to 10000 Mbit/s. **NOTE** Only MultiGE interfaces support this parameter.	-

Views

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

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In auto-negotiation mode, interfaces on both ends of a link negotiate their rate. If the negotiated rate is not the required one, run the **auto speed** command to set the auto-negotiation rate range to limit the negotiated rate.

For example, the network adapter speeds on Server1, Server2, and Server3 that form a server cluster are all 1000 Mbit/s, and the speed of the outbound interface GE0/0/4 connecting the device to external networks is also 1000 Mbit/s. The servers connect to GE0/0/1, GE0/0/2, and GE0/0/3 respectively. If the auto-negotiation speed is not specified on the device, the speeds negotiated by GE0/0/1, GE0/0/2, and GE0/0/3 with their connected servers are all 1000 Mbit/s. When the servers send data at the speed of 1000 Mbit/s concurrently, the outbound interface GE0/0/4 will be blocked. In this case, you can run the **auto speed 100 100** command to configure the auto-negotiation speed to 100 Mbit/s for GE0/0/1, GE0/0/2, and GE0/0/3, preventing the outbound interface from being blocked.

Prerequisites

Run the **negotiation auto** command to configure the Ethernet interface to work in auto-negotiation mode.

Example

# Configure Ethernet electrical interface GE0/0/1 to work at a rate of 100 Mbit/s in auto-negotiation mode.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] negotiation auto
[HUAWEI-GigabitEthernet0/0/1] auto speed 100
```

Related Topics

4.2.38 negotiation auto

4.2.5 cable-snr-test

Function

The **cable-snr-test** command checks the network cable quality and displays the check result.

NOTE

Only MultiGE electrical interfaces on the S6720-52X-PWH-SI, S6720-56C-PWH-SI-AC, S6720-56C-PWH-SI, S5720-28X-PWH-LI-AC, S6720-32C-SI-AC, S6720-32C-SI-DC, S6720-32C-PWH-SI-AC, and S6720-32C-PWH-SI support this command.

Format

cable-snr-test

Parameters

None

Views

MultiGE interface view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

You can check the quality of the network cable on a MultiGE electrical interface to determine whether the network cable quality meets communication requirements.

Precautions

- This command checks real-time quality of the network cable on an interface, and the network cable quality changes with the external environment.
- A MultiGE electrical interface supports accurate network cable quality check only when it works at the rate of 2.5 Gbit/s or higher.
- An interface does not support the network cable quality check when it is Down or in loopback detection mode.

Example

# Check the network cable quality on MultiGE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] interface MultiGE 0/0/1
[HUAWEI-MultiGE0/0/1] cable-snr-test
Info: The current network cable is of good quality.
```

4.2.6 carrier

Function

The **carrier** command configures the delay in reporting an interface status change event.

The **undo carrier** command restores the default delay in reporting an interface status change event.

By default, the delay in reporting an interface Up event is 2000 milliseconds, and the delay in reporting an interface Down event is 0 milliseconds.

Format

carrier { **up-hold-time** | **down-hold-time** } *interval*

undo carrier { **up-hold-time** | **down-hold-time** }

Parameters

Parameter	Description	Value
up-hold-time *interval*	Specifies the delay in reporting an interface Up event.	The value is 0 or an integer that ranges from 50 to 50000, in milliseconds.
down-hold-time *interval*	Specifies the delay in reporting an interface Down event.	The value is 0 or an integer that ranges from 1000 to 50000, in milliseconds.

Views

Ethernet interface view, GE interface view, XGE interface view, MultiGE interface view, 40GE interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The physical status of an Ethernet interface can be Up or Down. When the physical status changes, the system notifies upper-layer protocol modules (such as the routing and forwarding modules) of the change to direct packet receiving and forwarding. The system also automatically generates traps and logs to remind users to perform corresponding operations on physical links. For example, when the physical status of the active interface in an interface protection group changes from Up to Down, the system immediately instructs the upper-layer service forwarding protocol to send service packets from the standby interface.

If frequent physical status changes are reported to the system, extra system costs are generated. You can configure the delay in reporting physical status changes to solve the problem. The system is unaware of the physical status changes on interfaces within the configured delay. If the interface physical status is not recovered after the delay expires, the physical status changes are reported to the system.

You can configure the delay in reporting physical status changes based on the network connection status.

- Setting a long delay

  For example, an interface frequently alternates between Up and Down states at an interval shorter than the IP route convergence time. In this case, the upper-layer protocol does not need to sense the physical status changes. You can set a long delay in reporting physical status changes to avoid unnecessary routing entry refreshing caused by frequent physical status changes.

- Setting a short delay

  For example, when the physical status of the active interface in an interface protection group changes from Up to Down, the system needs to immediately instruct the upper-layer service forwarding protocol to send service packets from the standby interface. In this case, you can set a short delay in reporting physical status changes to ensure real-time service switchover.

Precautions

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

Example

# Set the delay in reporting an interface Up event to 1000 milliseconds on GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] carrier up-hold-time 1000
```

4.2.7 clear configuration port-isolate

Function

The **clear configuration port-isolate** command clears all the interface isolation configurations on the device.

By default, interface isolation configurations on the device are not cleared.

Format

clear configuration port-isolate

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

To clear all the interface isolation configurations on the device, you need to delete the configurations one by one. If a large number of configurations exist on the device, deleting the configurations takes much time and increases the maintenance workload. To reduce the maintenance workload and operation complexity, run the **clear configuration port-isolate** command in the system view to clear all the interface isolation configurations on the device. The configurations involve the port isolation group, unidirectional port isolation, and isolation mode.

Example

# Clear all the interface isolation configurations on the device.

```
<HUAWEI> system-view
[HUAWEI] clear configuration port-isolate
Warning: The port isolate will be cancelled. Continue?[Y/N]:y
Info: This operation may take a few seconds. Please wait for a moment...done.
```

4.2.8 combo-port

Function

The **combo-port** command configures the working mode of a combo interface.

The **undo combo-port** command restores the default setting.

By default, a combo interface works in auto mode. That is, the combo interface automatically switches between the electrical mode and optical mode.

NOTE

The following models support combo interfaces:

- S2720EI: S2720-12TP-EI, S2720-12TP-PWR-EI, S2720-28TP-EI, S2720-28TP-PWR-EI, S2720-28TP-PWR-EI-L
- S2750EI: S2750-28TP-EI-AC, S2750-20TP-PWR-EI-AC, S2750-28TP-PWR-EI-AC, S2751-28TP-PWR-EI-AC
- S5700LI: S5700-28TP-LI-AC, S5700-28TP-PWR-LI-AC, S5701-28TP-PWR-LI-AC, S5700-28X-LI-24S-AC, S5700-28X-LI-24S-DC, S5701-28X-LI-24S-AC, S5700-52X-LI-48CS-AC
- S5700S-LI: S5700S-28P-PWR-LI-AC
- S5700-LI-BAT: S5700-28P-LI-24S-BAT
- S5720LI: S5720-12TP-LI-AC, S5720-12TP-PWR-LI-AC, S5720-28TP-LI-AC, S5720-28TP-PWR-LI-AC, S5720-28TP-PWR-LI-ACL, S5720-28X-LI-24S-AC, S5720-28X-LI-24S-DC
- S5720S-LI: S5720S-12TP-LI-AC, S5720S-12TP-PWR-LI-AC, S5720S-28TP-PWR-LI-ACL, S5720S-28X-LI-24S-AC
- S5720SI: S5720-28P-SI-AC, S5720-28X-SI-AC, S5720-28X-SI-DC, S5720-28X-PWR-SI-AC, S5720-28X-PWR-SI-DC, S5720-28X-SI-24S-AC, S5720-28X-SI-24S-DC, S5721-28X-SI-24S-AC
- S5720EI: S5720-36C-EI-AC, S5720-36C-EI-DC, S5720-36C-EI-28S-AC, S5720-36C-EI-28S-DC, S5720-36C-PWR-EI-AC, S5720-36C-PWR-EI-DC, S5720-36PC-EI-AC
- S5720HI: S5720-32C-HI-24S-AC

Format

combo-port { **auto** | **copper** | **fiber** }

undo combo-port

Parameters

Parameter	Description	Value
auto	Allows a combo interface to automatically select the working mode. The combo interface checks whether an optical module has been installed: ● When a cable is not connected and an optical module is installed, the combo interface works in optical mode. ● When a cable is connected, the interface is in Up state, and an optical module is installed, the combo interface works in electrical mode. After the device restarts, the combo interface works in optical mode. ● When a cable is connected, the interface is in Down state, and an optical module is installed, the combo interface works in optical mode. In summary, when an optical module is installed on the combo optical interface, the combo interface works in optical mode after the device restarts.	-
copper	Configures a combo interface to work in electrical mode so that data is transmitted through network cables.	-

Parameter	Description	Value
fiber	Configures a combo interface to work in optical mode so that data is transmitted through optical fibers.	-

Views

GE interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A combo interface consists of a GE electrical interface and a GE optical interface on the panel. The multiplexed electrical and optical interfaces share one internal forwarding interface and cannot work at the same time. When one interface works, the other interface is disabled. You can use the electrical or optical interface based on the remote interface type. The electrical and optical interfaces share one interface view. When you enable the electrical or optical interface, configure the interface attributes (such as the rate and duplex mode) in the same interface view.

Precautions

This command takes effect only on combo interfaces.

If a combo interface is configured to work in a different mode from the remote interface, the two interfaces cannot communicate.

The electrical interface is used with the optical interface as a combo interface. Combo optical interface does not support GE copper module.

Example

# Configure GE0/0/1 to work in electrical mode.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] combo-port copper
```

Related Topics

4.1.15 display this interface

4.2.9 display counters protocol

Function

The **display counters protocol** command displays IPv4 and IPv6 packet statistics on an interface.

NOTE

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

Format

display counters [**interface** *interface-type interface-number*] **protocol** [**rate**]

Parameters

Parameter	Description	Value
interface *interface-type interface-number*	Specifies the interface type and number.	-
rate	Displays packet rate information.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After enabling IPv4 or IPv6 packet statistics collection on an interface, you can run this command to view packet statistics, facilitating fault location and troubleshooting.

Example

# Display IPv4 and IPv6 packet statistics on interfaces.

```
<HUAWEI> display counters protocol
-: Statistic not enable
Inbound
Interface      IPv4(bytes)    IPv4(pkts)    IPv6(bytes)    IPv6(pkts)
GE0/0/20                 0             0              0             0
GE0/0/21                 -             -             0             0
Outbound
Interface      IPv4(bytes)    IPv4(pkts)    IPv6(bytes)    IPv6(pkts)
GE0/0/20                 0             0              0             0
GE0/0/21                 -             -             0             0
```

# Display IPv4 and IPv6 packet rate information on interfaces.

```
<HUAWEI> display counters protocol rate
-: Statistic not enable
Inbound
Interface      IPv4(bytes/s)   IPv4(pkts/s)   IPv6(bytes/s)   IPv6(pkts/s)
GE0/0/20                 0             0             0             0
GE0/0/21                 -             -             0             0
Outbound
Interface      IPv4(bytes/s)   IPv4(pkts/s)   IPv6(bytes/s)   IPv6(pkts/s)
GE0/0/20                 0             0             0             0
GE0/0/21                 -             -             0             0
```

Table 4-14 Description of the **display counters protocol** command output

Item	Description
-: Statistic not enable	If a field of an interface displays **-**, traffic statistics collection about the corresponding type of packets is disabled.
Inbound	Packet statistics in the inbound direction of an interface.
Outbound	Packet statistics in the outbound direction of an interface.
Interface	Interface name.
IPv4(bytes)	Number of bytes in IPv4 packets.
IPv4(pkts)	Number of IPv4 packets.
IPv6(bytes)	Number of bytes in IPv6 packets.
IPv6(pkts)	Number of IPv6 packets.
IPv4(bytes/s)	Rate of bytes in IPv4 packets.
IPv4(pkts/s)	Rate of IPv4 packets.
IPv6(bytes/s)	Rate of bytes in IPv6 packets.
IPv6(pkts/s)	Rate of IPv6 packets.

Related Topics

4.2.67 statistic enable (interface view)

4.2.10 display device port-on-card status

Function

The **display device port-on-card status** command displays information about the card interface working mode.

NOTE

Only S6720-C-SI series switches support this command.

Format

display device port-on-card status [**slot** *slot-id*]

Parameters

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

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run this command to view information about the card interface working mode.

Example

# Display information about the card interface working mode.

```
<HUAWEI> display device port-on-card status
Slot ID        Port-on-card status
------------------------------------
0             enable
1             enable
------------------------------------
```

Table 4-15 Description of the **display device port-on-card status** command output

Item	Description
Slot ID	Slot ID.
Port-on-card status	Whether the switch works in the card interface working mode: ● enable: The switch works in the card interface working mode. ● disable: The switch works in the panel interface working mode. ● NA: The card interface working mode cannot be configured on the member switch in a stack.

Related Topics

4.2.56 set device port-on-card enable

4.2.11 display error-down recovery

Function

The **display error-down recovery** command displays information about the port in Error-Down state, including the interface name, cause of the Error-Down event, delay for the interface to change from Down to Up, and remaining time for the Up event.

NOTE

An interface enters the error-down state after being shut down due to an error. Currently, errors include the auto-defend protection, threshold crossing event, remote failure event, MAC address flapping, link flapping, low optical power, error packets exceeding the alarm threshold, and BPDU protection.

Format

display error-down recovery [**interface** *interface-type interface-number*]

Parameters

Parameter	Description	Value
interface *interface-type interface-number*	Displays the specified port in Error-Down state. ● *interface-type* specifies the interface type. ● *interface-number* specifies the interface number.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

The auto recovery function is configured and the delay for an interface to change from Down to Up is set using the **error-down auto-recovery** command. If the interface is in the Error-Down state, you can run the **display error-down recovery** command to view the remaining time for the Up event.

Prerequisites

The auto recovery function has been configured on an interface using the **error-down auto-recovery** command.

Precautions

If **interface** is not specified in this command, the system displays information about all interfaces in error-down state.

Example

# Display the delay for the interface to change from Down to Up and the remaining time for the Up event.

```
<HUAWEI> display error-down recovery
interface                error-down cause        recovery   remainder
                                                 time(sec)  time(sec)
-------------------------------------------------------------------------
GigabitEthernet0/0/1        bpdu-protection          30         10
```

Table 4-16 Description of the **display error-down recovery** command output

Item	Description
interface	Interface name.
error-down cause	Cause of the Error-Down event, including: ● as-not-ready: An AS is not in service. ● auto-defend ● efm-threshold-event ● efm-remote-failure ● bpdu-protection ● data-integrity-error ● error-statistics ● storm-control ● port-security ● mac-address-flapping ● transceiver-power-low ● link-flap
recovery time(sec)	Delay for the interface to change from Down to Up, in seconds. If no automatic recovery time is configured, you need to run the **undo shutdown (interface view)** command to make the interface go Up and the recovery time is displayed as **--**.
remainder time(sec)	Remaining time for the Up event, in seconds. If no automatic recovery time is configured, you need to run the **undo shutdown (interface view)** command to make the interface go Up and the remaining time is displayed as **--**.

Related Topics

4.2.22 error-down auto-recovery

4.2.12 display interface ethernet brief

Function

The **display interface ethernet brief** command displays brief information about Ethernet interfaces.

Format

display interface ethernet brief [**main**]

Parameters

Parameter	Description	Value
main	Displays brief information about Ethernet main interfaces.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

You can use the **display interface ethernet brief** command to view brief information about Ethernet interfaces, including the physical status, auto-negotiation mode, duplex mode, rate, and average inbound and outbound bandwidth usages within the last period of time. This information helps you locate and rectify faults.

Precautions

To clear statistics on an interface, run the **reset counters interface** command.

Example

# Display brief information about Ethernet interfaces.

```
<HUAWEI> display interface ethernet brief
PHY: Physical
*down: administratively down
#down: LBDT down
(l): loopback
```

```
(b): BFD down
InUti/OutUti: input utility/output utility
Interface                  PHY   Auto-Neg Duplex Bandwidth  InUti OutUti Trunk
GigabitEthernet0/0/1       up    enable   half      100M  0.06%   100%    --
GigabitEthernet0/0/2       up    enable   full     1000M   100%   100%    --
GigabitEthernet0/0/3       up    enable   full     1000M     0%   100%    --
GigabitEthernet0/0/4       up    enable   full     1000M   100%   100%     1
GigabitEthernet0/0/5       up    enable   full     1000M    99%   100%    --
GigabitEthernet0/0/6       down  enable   half     1000M     0%     0%    --
GigabitEthernet0/0/7       down  enable   half     1000M     0%     0%    --
GigabitEthernet0/0/8       down  enable   full     1000M     0%     0%    --
GigabitEthernet0/0/9       down  enable   full     1000M     0%     0%    --
GigabitEthernet0/0/10      down  enable   full     1000M     0%     0%    --
GigabitEthernet0/0/11      down  enable   full     1000M     0%     0%    --
GigabitEthernet0/0/12      down  enable   full     1000M     0%     0%    --
GigabitEthernet0/0/13      down  enable   full     1000M     0%     0%    --
GigabitEthernet0/0/14      down  enable   full     1000M     0%     0%    --
GigabitEthernet0/0/15      down  enable   full     1000M     0%     0%    --
GigabitEthernet0/0/16      down  enable   full     1000M     0%     0%    --
GigabitEthernet0/0/17      down  enable   full     1000M     0%     0%    --
GigabitEthernet0/0/18      down  enable   full     1000M     0%     0%    --
GigabitEthernet0/0/19      down  enable   full     1000M     0%     0%    --
GigabitEthernet0/0/20      down  enable   full     1000M     0%     0%    --
GigabitEthernet0/0/21      down  enable   full     1000M     0%     0%    --
GigabitEthernet0/0/22      down  enable   full     1000M     0%     0%    --
GigabitEthernet0/0/23      down  enable   full     1000M     0%     0%    --
GigabitEthernet0/0/24      down  enable   full     1000M     0%     0%    --
MEth0/0/1                  down  enable   half      100M     0%     0%    --
```

Table 4-17 Description of the **display interface ethernet brief** command output

Item	Description
Interface	Type and number of an interface. All interfaces are displayed in alphabetical order. Information about the following interfaces can be displayed: ● MEth0/0/1 interface ● FE interface ● GE interface ● XGE interface ● MultiGE interface ● 40GE interface
PHY	Physical status of an interface: ● up: indicates that the interface works properly. ● down: indicates that the physical layer of the interface fails. ● *down: refers to administratively down, indicating that the administrator has run the **shutdown (interface view)** command on the interface. ● #down: LBDT down, indicating that loop detection is enabled on the interface. The interface is shut down when the device detects a loop on the downstream network or between interfaces. ● (l): refers to loopback, indicating that the loopback function is enabled on the interface. ● (b): indicates that the physical layer of the interface is in BFD down state.

Item	Description
Auto-Neg	Whether auto-negotiation is enabled on an interface: ● enable: indicates that auto-negotiation is enabled on the interface. ● disable: indicates that auto-negotiation is disabled on the interface. To configure the auto-negotiation mode for an interface, run the **negotiation auto** command.
Duplex	Duplex mode of an interface: ● full: indicates the full-duplex mode. ● half: indicates the half-duplex mode. ● In auto-negotiation mode, use the **auto duplex** command to configure the duplex mode of an interface. ● In non-auto negotiation mode, use the **duplex** command to configure the duplex mode of an interface.
Bandwidth	Bandwidth on the interface.
InUti	Average inbound bandwidth usage within the last 5 minutes. Average inbound bandwidth usage = Average inbound rate within the last 5 minutes/Interface bandwidth When the average bandwidth usage is smaller than 0.01% and greater than 0.005%, the value 0.01% is displayed. When the average bandwidth usage is smaller than 0.005% and greater than 0, the value 0 is displayed. When the interface bandwidth becomes smaller, for example, the bandwidth is changed using the **4.2.65 speed** command, or when an Eth-Trunk member interface becomes Down or is removed from the Eth-Trunk, the bandwidth usage be displayed as 100% because the communication traffic is not adjusted in time.
OutUti	Average outbound bandwidth usage within the last 5 minutes. Average outbound bandwidth usage = Average outbound rate within the last 5 minutes/Interface bandwidth When the average bandwidth usage is smaller than 0.01% and greater than 0.005%, the value 0.01% is displayed. When the average bandwidth usage is smaller than 0.005% and greater than 0, the value 0 is displayed. When the interface bandwidth becomes smaller, for example, the bandwidth is changed using the **4.2.65 speed** command, or when an Eth-Trunk member interface becomes Down or is removed from the Eth-Trunk, the bandwidth usage be displayed as 100% because the communication traffic is not adjusted in time.
Trunk	Number of the Eth-Trunk to which an interface is added.

Related Topics

4.1.10 display interface

4.1.20 reset counters interface

4.2.13 display port-group

Function

The **display port-group** command displays information about permanent port groups and interfaces in these groups.

Format

display port-group [**all** | *port-group-name*]

Parameters

Parameter	Description	Value
all	Displays information about all permanent port groups and interfaces in these groups.	-
port-group-name	Displays information about a specified permanent port group and interfaces in the group.	The value is the name of an existing port group.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

When using the **display port-group** command, note that:

- If no parameter is configured, names of all permanent port groups are displayed.
- If **all** is configured, information about all permanent port groups and interfaces in these groups is displayed.
- If *port-group-name* is configured, information about a specified permanent port group and interfaces in the group is displayed.

Example

# Display information about all port groups and interfaces in these groups.

```
<HUAWEI> display port-group all
Portgroup: 1
GigabitEthernet0/0/1
GigabitEthernet0/0/2
GigabitEthernet0/0/3
```

Table 4-18 Description of the **display port-group** command output

Item	Description
Portgroup	Name of a permanent port group.

Related Topics

4.2.43 port-group

4.2.27 group-member

4.2.14 display port-isolate group

Function

The **display port-isolate group** command displays the configuration of a port isolation group.

Format

display port-isolate group { *group-id* | **all** }

Parameters

Parameter	Description	Value
group-id	Displays the configuration of a specified port isolation group.	The value is an integer that ranges from 1 to 64.
all	Displays the configurations of all port isolation groups.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

The port isolation feature isolates interfaces in a VLAN. Run **port-isolate enable** [**group** *group-id*] command to add interfaces to a port isolation group, you can implement Layer 2 isolation between these interfaces. To view the configuration of the port isolation group, run the **display port-isolate group** command.

Example

# Display the configurations of all port isolation groups.

```
<HUAWEI> display port-isolate group all
  The ports in isolate group 3:
GigabitEthernet0/0/1
GigabitEthernet0/0/2
  The ports in isolate group 4:
GigabitEthernet0/0/3
GigabitEthernet0/0/4
```

Related Topics

4.2.45 port-isolate enable

4.2.15 display port protect-group

Function

The **display port protect-group** command displays information about member interfaces in an interface protection group.

Format

display port protect-group { **all** | *protect-group-index* }

Parameters

Parameter	Description	Value
all	Displays information about all interface protection groups and their member interfaces.	-
protect-group-index	Displays information about member interfaces in the specified interface protection group.	The value is an integer that ranges from 0 to 63.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Hosts are usually connected to an external network through a default gateway. If the outbound interface of the default gateway fails, the hosts cannot communicate with the external network, interrupting normal service transmission and degrading device reliability. The port protection function solves this problem. Without changing the networking, you can add two interfaces on the device to a port protection group to implement interface backup in active/standby mode. When the active interface fails, services are immediately switched to the standby interface, ensuring non-stop service transmission.

The **display port protect-group** command displays information about member interfaces in an interface protection group.

Example

# Display information about interface protection group 1 and its member interfaces.

```
<HUAWEI> display port protect-group 1
  Group ID : 1
-----------------------------------------------
  Protect-group member        Role      State
-----------------------------------------------
  GigabitEthernet0/0/1        Master    Work
  GigabitEthernet0/0/2        Standby   Protect
```

Table 4-19 Description of the display port protect-group command output

Item	Description
Group ID	ID of the interface protection group.
Protect-group member	Member name of the interface protection group.
Role	Interface role: ● Master: working interface ● Standby: protected interface
State	Interface status: ● Work: working state ● Protect: protection state ● Down: the interface is physically down

Related Topics

4.2.50 port protect-group

4.2.47 protect-group member

4.2.16 display port split

Function

The **display port split** command displays the current status of a split or merged interface.

Format

display port split [**slot** *slot-id*]

Parameters

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

Views

User view, system view

Default Level

1: Monitoring level

Usage Guidelines

After interfaces are split, you can run this command to view the current status of the split and merged interface.

Example

# Display the current status of a split or merged interface .

```
<HUAWEI> display port split
*enable  : Will be enabled after board reset
*disable : Will be disabled after board reset

 Port          Status     Split Port
----------------------------------------------------
 40GE0/0/1     enable     XGigabitEthernet0/0/49
                          XGigabitEthernet0/0/50
                          XGigabitEthernet0/0/51
                          XGigabitEthernet0/0/52
 40GE0/0/2     enable     XGigabitEthernet0/0/53
                          XGigabitEthernet0/0/54
                          XGigabitEthernet0/0/55
                          XGigabitEthernet0/0/56
 40GE0/1/1     disable    -
 40GE0/1/2     enable     XGigabitEthernet0/1/5
                          XGigabitEthernet0/1/6
                          XGigabitEthernet0/1/7
```

```
                  XGigabitEthernet0/1/8
40GE0/1/3     disable    -
40GE0/1/4     disable    -
```

Table 4-20 Description of the display port split command output

Item	Description
Port	Port that can be split or merged.
Status	Current status of a split or merged interface: ● enable: Interface split is enabled. ● disable: Interface split is disabled. ● *enable: Interface split is enabled after the device is reset. ● *disable: Interface merge is enabled after the device is reset.
Split Port	Interfaces that have been split. If an interface is not split, this field displays as **-**. If an interface is split, converted interfaces are displayed.

4.2.17 display snmp-agent trap feature-name ifnet all

Function

The **display snmp-agent trap feature-name ifnet all** command displays all trap messages of the IFNET module.

Format

display snmp-agent trap feature-name ifnet 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 ifnet all** command displays whether all trap functions of the IFNET module are enabled.

Example

# Display all trap messages of the IFNET module.

```
<HUAWEI> display snmp-agent trap feature-name ifnet all
------------------------------------------------------------------------------
Feature name: IFNET
Trap number : 15
------------------------------------------------------------------------------
Trap name                      Default switch status   Current switch status
hwIfMonitorCrcErrorRising       off                     on
hwIfMonitorCrcErrorResume       off                     off
hwIfFlowDown                    off                     off
hwIfFlowUp                      off                     off
hwIfNameChange                  off                     off
hwIfNameChangeResume            off                     off
hwIfMonitorInputRateRising      off                     off
hwIfMonitorInputRateResume      off                     off
hwIfMonitorOutputRateRising     off                     off
hwIfMonitorOutputRateResume     off                     off
hwEntityExtCfmOverSlot          off                     on
hwEntityExtCfmOverCard          off                     off
linkDown                        off                     off
linkUp                          off                     off
hwExtInterfaceDelete            off                     off
```

Table 4-21 Description of the display snmp-agent trap feature-name ifnet 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 IFNET module: ● hwIfMonitorCrcErrorRising: The number of CRC errors occurring within a certain period exceeds the configured threshold. ● hwIfMonitorCrcErrorResume: The number of CRC errors occurring within a certain period falls below the configured threshold. ● hwIfFlowDown: Traffic is interrupted. ● hwIfFlowUp: Traffic is restored. ● hwIfNameChange: Interface information changes when the single-chassis system is expanded to multi-chassis system. ● hwIfNameChangeResume: Interface information changes when the multi-chassis system is rolled back to the single-chassis system. ● hwIfMonitorInputRateRising: The percentage of incoming traffic on an interface to the total interface bandwidth exceeds the configured threshold. ● hwIfMonitorInputRateResume: The percentage of incoming traffic on an interface to the total interface bandwidth falls below the configured threshold. ● hwIfMonitorOutputRateRising: The percentage of outgoing traffic on an interface to the total interface bandwidth exceeds the configured threshold. ● hwIfMonitorOutputRateResume: The percentage of outgoing traffic on an interface to the total interface bandwidth falls below the configured threshold. ● hwEntityExtCfmOverSlot: The slot configuration has been restored. ● hwEntityExtCfmOverCard: The interface card configuration has been restored. ● linkDown: The link protocol status of an interface becomes Down. ● linkUp: The link protocol status of an interface becomes Up. ● hwExtInterfaceDelete: An interface is deleted.
Default switch status	Status of the default trap function: ● on: indicates that the trap function is enabled. ● off: indicates that the trap function is disabled.

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

Related Topics

4.2.62 snmp-agent trap enable feature-name ifnet

4.2.18 display snmp-agent trap feature-name ifpdt all

Function

The **display snmp-agent trap feature-name ifpdt all** command displays all trap messages of the IFPDT module.

Format

display snmp-agent trap feature-name ifpdt 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 ifpdt all** command displays whether all trap functions of the IFPDT module are enabled.

Example

# Display all trap messages of the IFPDT module.

```
<HUAWEI> display snmp-agent trap feature-name ifpdt all
-------------------------------------------------------------------------------
```

```
Feature name: IFPDT
Trap number : 12
------------------------------------------------------------------------------
Trap name                          Default switch status   Current switch status
hwPortNoSupportOETrap              on                      on
hwTrunkMemSpeedDifferentAlarm      off                     on
hwTrunkMemSpeedDifferentResume     off                     on
hwPortErrorRateExceed              on                      on
hwPhysicalPortInBroadcastRapidChange
                                   on                      on
hwSubIfNumExceededSpecAlarm        on                      on
hwSubIfNumExceededSpecAlarmResume
                                   on                      on
hwInputRateChangeOverThresholdNotice
                                   on                      on
hwOutputRateChangeOverThresholdNotice
                                   on                      on
hwPortProtectGroupUnavailable      on                      on
hwPortProtectGroupAvailable        on                      on
hwPortProtectGroupDelete           on                      on
hwCableSnrAbnormal                 on                      on
hwCableSnrNormal                   on                      on
hwCableSnrDetectNotSupport         on                      on
```

Table 4-22 Description of the **display snmp-agent trap feature-name ifpdt 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 IFPDT module: ● hwPortNoSupportOETrap: The stack interface is connected to the copper transceiver module or GE optical module. ● hwTrunkMemSpeedDifferentAlarm: The rates of active interfaces of the Eth-Trunk are different. ● hwTrunkMemSpeedDifferentResume: The rates of active interfaces of the Eth-Trunk are changed to be the same. ● hwPortErrorRateExceed: The rate of CRC, Giants, and Runts error packets received by an interface is greater than or equal to 1000 packets per second. **NOTE** Only the S5720EI supports this field. ● hwPhysicalPortInBroadcastRapidChange: The rapid-change-ratio of inputbroadcast exceeded the threshold. ● hwSubIfNumExceededSpecAlarm: The number of sub-interfaces on the switch exceeds the maximum value. **NOTE** Only the S6720EI, S6720S-EI, S5720HI, and S5720EI support this field. ● hwSubIfNumExceededSpecAlarmResume: The number of sub-interfaces on the switch is within the normal range. **NOTE** Only the S6720EI, S6720S-EI, S5720HI, and S5720EI support this field. ● hwInputRateChangeOverThresholdNotice: The sudden traffic volume change in the inbound direction of interfaces. ● hwOutputRateChangeOverThresholdNotice: The sudden traffic volume change in the outbound direction of interfaces. ● hwPortProtectGroupUnavailable: The port protection group function becomes unavailable. ● hwPortProtectGroupAvailable: The port protection group function becomes available. ● hwPortProtectGroupDelete: The port protection group is deleted. ● hwCableSnrAbnormal: The network cable quality is abnormal. ● hwCableSnrNormal: The network cable quality is normal.

Item	Description
	● hwCableSnrDetectNotSupport: The network cable quality cannot be checked. ● hwVxlanTrunkHashNotSupport: This object indicates that the IP address-based load balancing mode configured on an Eth-Trunk does not take effect for VXLAN packets when the Eth-Trunk functions as the outbound interface of VXLAN packets.
Default switch status	Status of the default trap function: ● on: indicates that the trap function is enabled. ● off: indicates that the trap function is disabled.
Current switch status	Status of the current trap function: ● on: indicates that the trap function is enabled. ● off: indicates that the trap function is disabled.

Related Topics

4.2.63 snmp-agent trap enable feature-name ifpdt

4.2.19 display snmp-agent trap feature-name error-down all

Function

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

Format

display snmp-agent trap feature-name error-down all

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

The Simple Network Management Protocol (SNMP) is a network management standard widely used on the TCP/IP network. It uses a central computer (a network management station) that runs network management software to manage network elements. The SNMP agent reports trap messages to the network management station so that the network management station can obtain the network status in a timely manner, and the network administrator can take measures accordingly.

The **display snmp-agent trap feature-name error-down all** command displays the following information:

- Trap names supported by the error-down module. The trap names are the same as the trap names specified by the **snmp-agent trap enable feature-name error-down trap-name** *trap-name* command. Each trap name corresponds to a network element abnormality.
- Trap status of the error-down module. You can check whether the trap is reported based on the trap name.

Prerequisites

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

Example

# Display all traps of the error-down module.

```
<HUAWEI>display snmp-agent trap feature-name error-down all
------------------------------------------------------------------------------
Feature name: ERROR-DOWN
Trap number : 2
------------------------------------------------------------------------------
Trap name                      Default switch status   Current switch status
hwErrordown                      on                    on
hwErrordownRecovery                on                    on
```

Table 4-23 Description of the display snmp-agent trap feature-name error-down all command output

Item	Description
Feature name	Name of the module that the trap belongs to.
Trap number	Number of traps.
Trap name	Name of the trap: ● hwErrordown: indicates an error-down alarm. ● hwErrordownRecovery: indicates an error-down clear alarm.
Default switch status	Default status of the trap function: ● on: indicates that the trap function is enabled. ● off: indicates that the trap function is disabled.
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

4.2.64 snmp-agent trap enable feature-name error-down

4.2.20 display virtual-cable-test

Function

The **display virtual-cable-test** command displays the last cable test result on an Ethernet electrical interface.

Format

display virtual-cable-test *interface-type interface-number*

Parameters

Parameter	Description	Value
interface-type interface-number	Displays the cable test result on a specified interface. This Parameter can be an GE optical interface that has a GE copper module installed. This Parameter can be an XGE optical interface that has a GE copper module installed.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

A cable test detects faults on the cable connected to an interface. If the cable is working properly, the test result displays the total length of the cable. If the cable cannot work properly, the test result displays the distance between the interface and the failure point.

NOTE

The test result is only for reference and may be inaccurate for cables of some vendors.

Example

# Display the cable test result on Ethernet electrical interface GE0/0/1.

```
<HUAWEI> display virtual-cable-test gigabitethernet 0/0/1
VCT test last ran on: 2013-07-12 21:25:13
Pair A length: 189meter(s)
Pair B length: 189meter(s)
Pair C length: 189meter(s)
Pair D length: 189meter(s)
Pair A state: Ok
Pair B state: Ok
Pair C state: Ok
Pair D state: Ok
Info: The test result is only for reference.
```

Table 4-24 Description of the display virtual-cable-test command output

Item	Description
VCT test last ran on	Time when the last VCT test was performed on the interface. **NOTE** ● When the daylight saving time (DST) is not used, the system displays the following information: VCT test last ran on: 2013-07-12 21:25:13. ● When the DST is used, the system displays the following information: VCT test last ran on: 2013-07-12 21:25:13 DST.
Pair A length	Length of a network cable. ● The length is the distance between the interface and the faulty point if a fault occurs. ● The length is the actual length of the cable when the cable works properly. ● The length is the default length 0 m if the interface is not connected to any network cable. **NOTE** If the cable length is displayed as Unknown, the cable status is OK, but the cable length test result cannot be used.

Item	Description
Pair A state	Status of a circuit pair of the cable: - Ok: indicates that the circuit pair is terminated normally. - Open: indicates that the circuit pair is not terminated. - Short: indicates that the circuit pair is short-circuited. - Crosstalk: indicates that the circuit pairs interfere with each other. - Unknown: indicates that the circuit pair has an unknown fault.

NOTE

Pairs A, B, C, and D are the four pairs in a cable.

Related Topics

4.2.73 virtual-cable-test

4.2.21 duplex

Function

The **duplex** command sets the duplex mode for an Ethernet electrical interface in non-auto-negotiation mode.

The **undo duplex** command restores the default duplex mode for an Ethernet electrical interface in non-auto-negotiation mode.

By default, the duplex mode of an Ethernet electrical interface is full duplex when the interface works in non-auto-negotiation mode.

Format

duplex { **full** | **half** }

undo duplex

Parameters

Parameter	Description	Value
full	Sets the duplex mode to full duplex for an Ethernet electrical interface in non-auto-negotiation mode.	-

Parameter	Description	Value
half	Sets the duplex mode to half duplex for an Ethernet electrical interface in non-auto-negotiation mode.	-

Views

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

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Interfaces can work in the following two duplex modes:

- Half-duplex mode: An interface in this mode only receives or sends data at a time within a specified transmission distance.
- Full-duplex mode: An interface in this mode receives and sends data at the same time. The maximum throughput in full-duplex mode is double that in half-duplex mode, and the transmission distance is not limited.

If the peer device does not support auto-negotiation, you can run this command to manually set the duplex mode for the local interface in non-auto-negotiation mode to ensure that the interface works in the same duplex mode as the peer interface.

Prerequisites

The Ethernet interface has been set to work in non-auto-negotiation mode by running the **undo negotiation auto** command.

Precautions

- When the working rate of a GE electrical interface is 1000 Mbit/s, the interface supports only the full duplex mode and does not need to negotiate the duplex mode with the peer interface.
- When an interface works in half-duplex mode, flow control does not take effect on the interface.
- Interfaces on both ends of a link must have the same duplex mode.
- Physical service interfaces of the S5720HI, S5720EI, S6720S-EI, and S6720EI do not support the half duplex mode.

Example

# Set the duplex mode to half duplex for Ethernet electrical interface GE0/0/1 in non-auto-negotiation mode.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo negotiation auto
[HUAWEI-GigabitEthernet0/0/1] speed 100
[HUAWEI-GigabitEthernet0/0/1] duplex half
```

Related Topics

4.1.10 display interface

4.2.34 loopback

4.2.36 mdi

4.2.38 negotiation auto

4.2.65 speed

4.2.22 error-down auto-recovery

Function

The **error-down auto-recovery** command enables an interface in Error-Down state to go Up and sets the auto recovery delay.

The **undo error-down auto-recovery** command disables an interface in Error-Down state from going Up automatically.

By default, an interface in Error-Down state is not enabled to go Up.

NOTE

An interface enters the Error-Down state after being shut down due to an error. Currently, errors include the auto-defend protection, threshold crossing event, remote failure event, MAC address flapping, link flapping, low optical power, error packets exceeding the alarm threshold, and BPDU protection.

Format

error-down auto-recovery cause { **as-not-ready** | **auto-defend** | **bpdu-protection** | **efm-remote-failure** | **efm-threshold-event** | **error-statistics** | **runts-error-statistics** | **link-flap** | **mac-address-flapping** | **port-security** | **transceiver-power-low** | **storm-control** | **data-integrity-error** } **interval** *interval-value*

undo error-down auto-recovery cause { **auto-defend** | **bpdu-protection** | **efm-remote-failure** | **efm-threshold-event** | **error-statistics** | **runts-error-statistics** | **link-flap** | **mac-address-flapping** | **port-security** | **transceiver-power-low** | **storm-control** | **data-integrity-error** }

NOTE

The S1720GFR does not support the **as-not-ready** parameter.

efm-threshold-event does not take effect on the S1720GFR.

Parameters

Parameter	Description	Value
cause	Indicates the cause for an interface in Error-Down state.	-
as-not-ready	Indicates that the AS where the interface resides is not in service.	-
auto-defend	Indicates that the auto-defend function is enabled.	-
bpdu-protection	Indicates that STP BPDU protection is enabled.	-
efm-remote-failure	Indicates that an EFM remote failure event occurs.	-
efm-threshold-event	Indicates that a threshold crossing event occurs.	-
error-statistics	Indicates that the number of error packets exceeds the alarm threshold.	-
runts-error-statistics	Indicates that the number of received Runts error packets reaches the alarm threshold. **NOTE** Only interfaces on the S5720EI can be in this Error-Down state.	-
link-flap	Indicates that link flapping occurs.	-
storm-control	Indicates that storm control is enabled.	-
port-security	Indicates that the number of learned secure MAC addresses exceeds the upper limit or static MAC address flapping is detected.	-
mac-address-flapping	Indicates that MAC address flapping occurs.	-
transceiver-power-low	Indicates that the optical power is too low.	-
data-integrity-error	Indicates that the chip memory identifier has a data integrity error.	-

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

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

An interface enters the Error-Down state in the following scenarios.

Cause for an Interface in Error-Down State	Scenario	Remarks
as-not-ready	When the device negotiates to the AS mode, its port status becomes Down and then becomes Up after services in the service profiles have been delivered.	-
auto-defend	After the **auto-defend action** command is used to configure actions against attack sources, the interface that receives attack packets is shut down to prevent the device from attacks.	-
bpdu-protection	On an STP-enabled network where BPDU protection is configured on an edge port, if malicious attackers send bogus BPDUs to attack the switching device, the switching device sets the edge port to Down immediately after the edge port receives BPDUs. As a result, all services on the edge port are interrupted.	For details, see **stp bpdu-protection**.

Cause for an Interface in Error-Down State	Scenario	Remarks
efm-remote-failure	The **efm trigger error-down** command associates an error event with an interface. When EFM detects **critical-event**, **dying-gasp**, **link-fault**, or **timeout** faults, the protocol status of the interface becomes Down and all services on the interface are interrupted.	-
efm-threshold-event	When link monitoring is configured for an interface on a link, the link is considered unavailable, if the number of errored frames, errored codes, or errored frame seconds detected by the interface reaches or exceeds the threshold within a period. You can associate an EFM crossing event with an interface. Then the system sets the administrative status of the interface to Down. In this manner, all services on the interface are interrupted.	-
error-statistics	When an Ethernet interface configured with a backup link receives error packets, faults such as packet loss occur. To ensure nonstop service transmission, when the number of received error packets reaches the alarm threshold, the interface is shut down and services are switched to the backup link.	For details, see **trap-threshold error-statistics** and **error-statistics threshold-event trigger error-down**.

Cause for an Interface in Error-Down State	Scenario	Remarks
runts-error-statistics	An interface receives Runts error packets if the optical fiber, network cable, or optical module is removed and reinstalled, the **shutdown** or **undo shutdown** command is executed, or Runts packets are forwarded on the network. To avoid worse impact on the device or services, the device counts the number of Runts error packets received by an interface within one minute, and shuts down the interface if the number reaches the alarm threshold 5.	-
link-flap	Network cable faults or active/standby switchovers may cause an interface to alternate between Up and Down. You can configure link flapping protection. When the device receives an interface Up/Down message, it checks the interface flapping count and link flapping detection interval. If the interface flapping count reaches the limit within the specified period, the device shuts down interface.	For details, see **port link-flap protection enable**.

Cause for an Interface in Error-Down State	Scenario	Remarks
storm-control	After the storm control action is configured as error-down on an interface, the interface is shut down when the average rate of receiving broadcast, multicast, and unknown unicast packets is larger than the specified limit within the interval for detecting storms.	For details, see **storm-control action**.
port-security	After port security is enabled on an interface, MAC addresses learned by the interface change to secure dynamic MAC addresses. If the **port-security protect-action** command sets the security protection action to **shutdown**, the interface is shut down when the number of learned MAC addresses on the interface exceeds the upper limit or static MAC address flapping is detected.	For details, see **port-security protect-action** and **port-security enable**.
mac-address-flapping	If the user network where the device is deployed does not support loop prevention protocols, configure a loop prevention action for the device to perform when the device detects MAC address flapping. The device shuts down an interface when detecting MAC address flapping on the interface.	For details, see **mac-address flapping detection** and **mac-address flapping action**.

Cause for an Interface in Error-Down State	Scenario	Remarks
transceiver-power-low	When the optical power of an Ethernet optical interface configured with a backup link is reduced, faults such as packet loss occur. When the optical power is lower than the lower alarm threshold, the interface is triggered to be in Error-Down state and services are switched immediately.	For details, see **transceiver power low trigger error-down**.
data-integrity-error	After the switch runs for a long time, the chip memory identifier has a data integrity error.	-

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

The restored interface is shut down again if the interface receives BPDUs again or the link is considered unavailable in a specified time.

Precautions

The **error-down auto-recovery** command is invalid for the interface that has been in Error-Down state. It takes effect for only the interface that enters the Error-Down state after the **error-down auto-recovery** command is executed.

BPDU protection has been enabled using the **stp bpdu-protection** command in the system view.

A threshold crossing event has been associated with an interface using the **efm threshold-event trigger error-down** command in the interface view.

An error event has been associated with an interface using the **efm trigger error-down** command in the interface view.

Example

# Set the delay for an interface changes from Down to Up to 50s after the edge port is enabled with BPDU protection on an STP-enabled network.

```
<HUAWEI> system-view
[HUAWEI] error-down auto-recovery cause bpdu-protection interval 50
```

# Set the auto recovery delay to 50s after an EFM threshold crossing event is associated with an interface.

```
<HUAWEI> system-view
[HUAWEI] error-down auto-recovery cause efm-threshold-event interval 50
```

# Set the auto recovery delay to 50s after an EFM remote failure event is associated with an interface.

```
<HUAWEI> system-view
[HUAWEI] error-down auto-recovery cause efm-remote-failure interval 50
```

Related Topics

4.2.11 display error-down recovery

5.12.33 stp bpdu-protection

4.2.41 port link-flap protection enable

5.1.23 mac-address flapping action

4.2.72 trap-threshold error-statistics

4.2.24 error-statistics threshold-event trigger error-down

4.2.70 transceiver power low trigger error-down

4.2.23 error-down-threshold error-statistics

Function

The **error-down-threshold error-statistics** command configures the alarm threshold for error packets causing an interface status to change to Error-Down and interval for receiving error packets.

The **undo error-down-threshold error-statistics** command restores the default value of the alarm threshold and the alarm interval for error packets that cause the interface status to change to Error-Down.

By default, the alarm threshold for error packets is 3 and the alarm interval is 10 seconds.

Format

error-down-threshold error-statistics *threshold-value* **interval** *interval-value*

undo error-down-threshold error-statistics

Parameters

Parameter	Description	Value
threshold-value	Specifies the alarm threshold for error packets that cause the interface status to change to Error-Down.	The value is an integer that ranges from 1 to 65535. **NOTE** The threshold is greater than or equal to the alarm threshold for error packets configured by the **trap-threshold error-statistics** command.

Parameter	Description	Value
interval *interval-value*	Specifies the alarm interval for error packets that cause the interface status to change to Error-Down.	The value is an integer that ranges from 10 to 65535, in seconds.

Views

Ethernet interface view, GE interface view, XGE interface view, MultiGE interface view, 40GE interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After an interface is configured to transit to the Error-Down state when the number of received error packets exceeds the threshold using the **error-statistics threshold-event trigger error-down** command, the interface transits to the Error-Down state when the number of received error packets exceeds the threshold within the specified interval. By default, an interface transits to the Error-Down state when the number of received error packets exceeds 3 within 10 seconds. Run the **error-down-threshold error-statistics** command to configure the interval and the threshold for received error packets.

Precautions

This command is not supported on the stack interface.

On a switch running a version earlier than V200R009C00, if the alarm threshold has been set to *n* and alarm interval to *m* seconds using the **trap-threshold error-statistics** *threshold-value* **interval** *interval-value* command, the **error-down-threshold error-statistics** *n* **interval** *m* configuration is automatically generated after the system software version is upgraded to V200R009C00 or a later version.

On a switch running a version earlier than V200R009C00, if the **error-down-threshold error-statistics** configuration exists on the switch, the configuration remains unchanged after the system software version is upgraded to V200R009C00 or a later version.

Example

By default, the alarm threshold of error packets that cause the interface status to change to Error-Down is 10 and the alarm interval is 30 seconds.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] error-down-threshold error-statistics 10 interval 30
```

4.2.24 error-statistics threshold-event trigger error-down

Function

The **error-statistics threshold-event trigger error-down** command configures an interface to transit to the error-down state when the number of error packets received on the interface reaches the threshold.

The **undo error-statistics threshold-event trigger error-down** command restores the default setting.

By default, an interface does not transit to the error-down state when the number of error packets received on the interface reaches the threshold.

Format

error-statistics threshold-event trigger error-down

undo error-statistics threshold-event trigger error-down

Parameters

None

Views

Ethernet interface view, GE interface view, XGE interface view, MultiGE interface view, 40GE interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When an Ethernet interface receives excessive error packets, faults such as packet loss will occur. Because the interface is still in Up state, traffic is still transmitted on the interface even if a backup link is configured. To avoid impact on services, you can configure the interface to change to the Error-down state when it receives excessive error packets. When the number of received error packets on the interface exceeds the threshold, the system disables the interface and records the interface status as **ERROR DOWN(error-statistics)** state (indicating that the interface is Down because of excessive error packets). Services are then switched to the backup link immediately.

Follow-up Procedure

An interface in Error-down state can be recovered using either of the following methods:

- Manual recovery: If a few interfaces need to be recovered forcibly, run the **shutdown** and **undo shutdown** commands in the interface view. Alternatively, run the **restart** command in the interface view to restart the interfaces.

- Automatic recovery: If a large number of interfaces need to be recovered, manual recovery is time consuming and some interfaces may be omitted. You can run the **error-down auto-recovery** **cause error-statistics interval** *interval-value* command in the system view to enable automatic interface recovery and set the recovery delay time. An interface in Error-down state automatically recovers when the specified delay time expires.

Example

# Configure GE0/0/1 to transit to the error-down state when the number of error packets received on the interface reaches the threshold.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] error-statistics threshold-event trigger error-down
```

Related Topics

4.2.72 trap-threshold error-statistics

4.2.22 error-down auto-recovery

4.2.25 flow-control (interface view)

Function

The **flow-control** command enables flow control on an Ethernet interface.

The **undo flow-control** command disables flow control on an Ethernet interface.

By default, flow control is disabled on an Ethernet interface.

Format

flow-control

undo flow-control

Parameters

None

Views

Ethernet interface view, GE interface view, XGE interface view, MultiGE interface view, 40GE interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Flow control prevents packet loss caused by network congestion. If network congestion occurs on the local device after flow control is configured, the local device sends a message to the remote device, requesting the remote device to temporarily stop sending packets. After receiving the message, the remote device temporarily stops sending packets to the local device regardless of the interface working rate.

Precautions

- If flow control is enabled on an interface, it must also be enabled on the peer interface.
- Flow control and flow control auto-negotiation can be configured on Ethernet interfaces, but they cannot be configured concurrently.
- XGE interfaces on the S5720-32C-HI-24S-AC, and XGE interfaces and the last eight GE interfaces on the S5720-56C-HI-AC, S5720-56C-PWR-HI-AC, and S5720-56C-PWR-HI-AC1 do not support flow control.
- When an interface works in half-duplex mode, flow control does not take effect on the interface.
- In a scenario where Layer 3 services are deployed, enabling flow control may affect the IP traffic forwarding on the interface. As a result, the interface becomes unavailable. You can run the **undo flow-control** command in the interface view to disable flow control to recover the interface.

Example

# Enable flow control on GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] flow-control
```

Related Topics

4.2.26 flow-control negotiation

4.2.26 flow-control negotiation

Function

The **flow-control negotiation** command enables flow control auto-negotiation on an Ethernet interface.

The **undo flow-control negotiation** command disables flow control auto-negotiation on an Ethernet interface.

By default, flow control auto-negotiation is disabled on an Ethernet interface.

Format

flow-control negotiation

undo flow-control negotiation

Parameters

None

Views

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

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Network congestion causes packet loss. Flow control can prevent packet loss. If congestion occurs on a device, the device sends a message to request the peer device to stop sending packets, which prevents packet loss. Flow control auto-negotiation enables a device to determine whether to enable flow control by negotiating with the peer device.

Prerequisites

Run the **negotiation auto** command to configure the Ethernet interface to work in auto negotiation mode.

Precautions

- Electrical interfaces support flow control auto-negotiation.
- If flow control auto-negotiation is enabled on an interface, it must also be enabled on the peer interface.
- If flow control has been enabled on an Ethernet interface using the **flow-control** command, run the **undo flow-control** command to disable flow control before running the **flow-control negotiation** command. Otherwise, the **flow-control negotiation** command fails to be executed.
- XGE interfaces on the S5720-32C-HI-24S-AC, and XGE interfaces and the last eight GE interfaces on the S5720-56C-HI-AC, S5720-56C-PWR-HI-AC, and S5720-56C-PWR-HI-AC1 do not support flow control auto-negotiation.
- This command can be used on an XGE optical interface that has a GE copper module installed.
- This command can be used on a GE optical interface that has a GE optical module or GE copper module installed.
- In a scenario where Layer 3 services are deployed, configuring flow control auto-negotiation on an Ethernet interface may affect the IP traffic forwarding on the interface. As a result, the interface becomes unavailable. You can run the **undo flow-control negotiation** command in the interface view to disable flow control auto-negotiation to recover the interface.

NOTE

On the S2720-52TP-EI, S5700-52P-LI-AC, S5720-52P-LI-AC, S5700-52P-LI-DC, if interfaces 0 to 23 work as inbound interfaces (or outbound interfaces) and interfaces 24 to 47 work as outbound interfaces (or inbound interfaces), flow control auto-negotiation does not take effect on these interfaces.

Example

# Enable flow control auto-negotiation on GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] negotiation auto
[HUAWEI-GigabitEthernet0/0/1] flow-control negotiation
```

Related Topics

4.2.25 flow-control (interface view)

4.2.38 negotiation auto

4.2.27 group-member

Function

The **group-member** command adds specified Ethernet interfaces to a permanent port group.

The **undo group-member** command deletes specified Ethernet interfaces from a permanent port group.

By default, no Ethernet interface is added to a permanent port group.

Format

group-member { *interface-type interface-number1* [**to** *interface-type interface-number2*] } &<1-10>

undo group-member { *interface-type interface-number1* [**to** *interface-type interface-number2*] } &<1-10>

undo group-member all-unavailable-interface

Parameters

Parameter	Description	Value
interface-type interface-number1 **to** *interface-type interface-number2*	Adds an Ethernet interface to a permanent port group. **to** indicates an interface range. All interfaces numbered between *interface-number1* and *interface-number2* are added to the temporary port group.	*interface-number2* must be greater than *interface-number1*.
all-unavailable-interface	Delete all unavailable interfaces from this port-group.	-

Views

Permanent port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If you need to perform the same operations on multiple Ethernet interfaces, configuring each interface one by one easily causes incorrect configurations and is labor-intensive.

The port group function easily solves the problem. You can add all the Ethernet interfaces to the same port group. After you run a configuration command once in the port group view, the configuration takes effect on all the Ethernet interfaces in the port group, reducing the configuration workload.

Prerequisite

Prior to running this command, run the **port-group** command in the system view to create a permanent interface group.

Configuration Impact

If the **group-member** command is run more than once, all configurations take effect.

Precautions

- Both physical and logical interfaces can be added to a permanent port group.
- This command has the same function as the **port-group group-member** command that is used in the system view. You can also run the **port-group group-member** command to add interfaces to a temporary port group to configure the interfaces in batches.
- When you specify the keyword **to** in the **group-member** command:
  - The interfaces specified before and after the keyword **to** must have the same attribute. For example, both of them are main interfaces or sub-interfaces. If they are sub-interfaces, they must belong to the same main interface.
  - If **to** is not used, these limitations do not apply.
  - Only the S6720EI, S6720S-EI, S5720HI and S5720EI support sub-interfaces.

Example

# Add GE0/0/1 and GE0/0/2 to port group **portgroup1**.

```
<HUAWEI> system-view
[HUAWEI] port-group portgroup1
[HUAWEI-port-group-portgroup1] group-member gigabitethernet 0/0/1 to gigabitethernet 0/0/2
```

Related Topics

4.2.43 port-group

4.2.13 display port-group

4.2.28 interface (Ethernet interface)

Function

The **interface** command displays the specified interface view or sub-interface view.

The **undo interface** command deletes a sub-interface.

Format

interface { **ethernet** | **gigabitethernet** | **multige** | **xgigabitethernet** | **40ge** } *interface-number*[.*subinterface-number*] [**mode l2**]

undo interface { **ethernet** | **gigabitethernet** | **multige** | **xgigabitethernet** | **40ge** } *interface-number*[.*subinterface-number*]

Parameters

Parameter	Description	Value
gigabitethernet	Displays the view of a GE interface.	-
multige	Displays the view of a MultiGE interface. **NOTE** Only the S5720-14X-PWH-SI-AC, S5720-28X-PWH-LI-AC, S6720-32C-SI-AC , S6720-32C-SI-DC , S6720-32C-PWH-SI-AC, S6720-52X-PWH-SI, S6720-56C-PWH-SI-AC, S6720-56C-PWH-SI, and S6720-32C-PWH-SI support MultiGE interfaces.	-
xgigabitethernet	Displays the view of an XGE interface.	-
ethernet	Displays the view of an FE interface.	-
40ge	Displays the view of a 40GE interface.	-
interface-number	Specifies the number of an interface.	The value depends on the interface type and slot ID.
subinterface-number	Specifies the number of a sub-interface.	The value is an integer that ranges from 1 to 4096.

Parameter	Description	Value
mode l2	Configures a sub-interface to work in Layer 2 mode for the VXLAN service. **NOTE** Only the S6720EI, S6720S-EI, and S5720HI support this parameter.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

After entering the specified Ethernet interface view, you can set attributes for the Ethernet interface.

NOTE

- Only the S6720EI, S6720S-EI, S5720HI, and S5720EI support Ethernet sub-interfaces.
- Only hybrid and trunk interfaces on the preceding switches support Ethernet sub-interface configuration.
- After you run the **undo portswitch** command to switch Layer 2 interfaces on the preceding series of switches into Layer 3 interfaces, you can configure Ethernet sub-interfaces on the interfaces.
- After an interface is added to an Eth-Trunk, sub-interfaces cannot be configured on the interface.
- VLAN termination sub-interfaces cannot be created on a VCMP client.

Example

# Enter the view of GE0/0/1.

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

Related Topics

4.1.10 display interface

4.2.29 interface range

Function

The **interface range** command creates a temporary interface group and adds specified interfaces to this temporary interface group. Commands configured for a temporary interface group then automatically run on all member interfaces.

By default, no temporary interface group is created.

Format

interface range { *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 Ethernet interfaces to be added to a temporary port group. **to** indicates an interface range. All interfaces numbered between *interface-number1* and *interface-number2* are added to the temporary port group.	The value of *interface-number2* must be larger than the value of *interface-number1*. A maximum of 48 temporary port groups can be created on a device.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If you need to perform the same operations on multiple Ethernet interfaces, configuring each interface one by one easily causes incorrect configurations and is labor-intensive.

The port group function easily solves the problem. You can add all the Ethernet interfaces to the same port group. After you run a configuration command once in the port group view, the configuration takes effect on all the Ethernet interfaces in the port group, reducing the configuration workload.

Configuration Impact

If the **interface range** command is run more than once, all configurations take effect.

Precautions

- The **interface range** and **port-group group-member** commands have the same functions. Therefore, use either of the commands for configuration. After exiting from the temporary port group view, the system deletes the temporary port group.
- The **interface range** command is equivalent to the **group-member** command executed in the permanent port group view. Multiple interfaces can be added to a permanent port group in batches using the **group-member** command.
- When you specify the keyword **to** in the **interface range** command:
  - The interfaces specified by *interface-number1* and *interface-number2* must reside on the same member switch. To add contiguous interfaces on different member switches to the same port group, run this command several times or use the keyword **to** several times.
  - The interfaces specified by *interface-number1* and *interface-number2* must be of the same type, for example, both of the interfaces are GE interfaces.
  - The interfaces specified before and after the keyword **to** must have the same attribute. For example, both of them are main interfaces or sub-interfaces. If they are sub-interfaces, they must belong to the same main interface.
  - If **to** is not specified, the preceding limitations do not apply.
  - Only the S6720EI, S6720S-EI, S5720HI and S5720EI support sub-interfaces.

Example

# Add GE0/0/1, 0/0/2, and 0/0/3 to a temporary port group.

```
<HUAWEI> system-view
[HUAWEI] interface range gigabitethernet 0/0/1 to gigabitethernet 0/0/3
[HUAWEI-port-group]
```

Related Topics

4.2.43 port-group

4.2.44 port-group group-member

4.2.30 ifg

Function

The **ifg** command configures the inter-frame gap (IFG).

The **undo ifg** command restores the default IFG.

By default, the IFG is 12 bytes.

Format

ifg *ifg-value*

undo ifg [*ifg-value*]

Parameters

Parameter	Description	Value
ifg-value	Specifies the IFG.	The value is an integer that ranges from 9 to 12, in bytes.

Views

GE interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The IFG is used to differentiate two data packets. You can run the **ifg** command to configure the IFG to improve data packet forwarding efficiency.

The packet forwarding rate, also called throughput, refers to the data forwarding capability on an interface and is measured in packet per second (pps). The packet forwarding rate is calculated based on the number of 64-byte data packets transmitted in a period. The lengths of preamble and IFG affect the packet forwarding rate.

The default IFG is the maximum value of 12 bytes and is recommended. If you set the IFG to a small value, the device will not have enough time to receive the next frame after receiving one data frame. The packets then cannot be processed in real time, which results in packet loss.

NOTE

Only the S5700-X-LI and S1720GFR support the IFG configuration.

Example

# Set the IFG of GE0/0/1 to 10 bytes.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] ifg 10
```

4.2.31 jumboframe enable

Function

The **jumboframe enable** command sets the maximum frame length allowed by an interface.

The **undo jumboframe enable** command restores the default maximum frame length allowed by an interface.

By default, the maximum frame length allowed by interfaces of other switches is 9216 bytes.

Format

jumboframe enable [*value*]

undo jumboframe enable

Parameters

Parameter	Description	Value
value	Specifies the maximum frame length allowed by an Ethernet interface.	● On the S1720GFR, S1720GW, S1720GWR, S1720X, S1720GW-E, S1720GWR-E, S1720X-E, S2720EI, S2750, S5700LI, S5720LI, S5720S-LI, S5710-X-LI, S5700S-LI, S5720SI, S5720S-SI, S5730SI, S5730S-EI, S6720SI, S6720S-SI, S6720LI, and S6720S-LI, the value is an integer that ranges from 1536 to 10240. ● On the S5720HI, S5720EI, S6720S-EI, and S6720EI, the value is an integer that ranges from 1536 to 12288. **NOTE** On the S1720GFR, S1720GW, S1720GWR, S1720X, S1720GW-E, S1720GWR-E, S1720X-E, S2720EI, S5720SI, S5720S-SI, S5700S-LI, S5700LI, S5720LI, S5720S-LI, S5710-X-LI, S2750, S5730SI, S5730S-EI, S6720SI, S6720S-SI, S6720LI, and S6720S-LI, *value* cannot be set to an odd number. For GE electrical interfaces on the S5730SI, S5730S-EI and S6720SI, *value* can only be set to 10232. If *value* is set to an odd number in a version earlier than V200R008, the value of *value* increases by one automatically after the system software is upgraded to V200R008 or later versions. For example, *value* is set to 8879 in V200R007. After the system software is upgraded to V200R008, the value of *value* is 8880.

Views

Ethernet interface view, GE interface view, XGE interface view, MultiGE interface view, 40GE interface view, port group view, Eth-Trunk interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When transmitting a large amount of data (such as files and videos), an Ethernet interface may receive jumbo frames. If the jumbo frame length exceeds the default data frame length that can be processed, the device directly discards the jumbo frames. You can set the jumbo frame length allowed on an interface.

After you configure the device to allow jumbo frames, packet forwarding becomes more flexible. If multiple common Ethernet frames are used to transmit a data packet, many redundant contents such as interframe gaps (IFGs) and preambles are also transmitted. If jumbo frames are used to transmit the data packet, fewer frames, as well as fewer IFGs and preambles, are transmitted, improving bandwidth efficiency.

Precautions

If you run the **jumboframe enable** command multiple times in the same interface view to set the maximum frame length allowed by the interface, only the latest configuration takes effect.

If you run the **jumboframe enable** command on an interface without specifying the *value* parameter, the interface allows the default jumbo frame length. By default, the jumbo frame length allowed by Ethernet interfaces of other models is 9216 bytes.

If the length of an outgoing packet exceeds the maximum frame length allowed on an interface, the interface can directly forward the packet.

Example

# Set the maximum frame length allowed by GE0/0/1 to 5000 bytes.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] jumboframe enable 5000
```

4.2.32 log-threshold input-rate output-rate

Function

The **log-threshold input-rate output-rate** command sets the inbound and outbound bandwidth usage thresholds for generating a log.

The **undo log-threshold input-rate output-rate** command restores the default inbound and outbound bandwidth usage thresholds for generating a log.

The default inbound and outbound bandwidth usage thresholds for generating a log is 80.

Format

log-threshold { **input-rate** | **output-rate** } *bandwidth-in-use* [**resume-rate** *resume-threshold*]

undo log-threshold { **input-rate** | **output-rate** }

Parameters

Parameter	Description	Value
input-rate	Specifies the inbound bandwidth.	-
output-rate	Specifies the outbound bandwidth.	-
bandwidth-in-use	Specifies the bandwidth usage threshold for generating a log.	The value is an integer that ranges from 1 to 100.
resume-rate *resume-threshold*	Specifies the bandwidth usage threshold for clearing a log.	The value is an integer that ranges from 1 to the value of *bandwidth-in-use*. The default value is the value of *bandwidth-in-use*.

Views

Ethernet interface view, GE interface view, XGE interface view, MultiGE interface view, 40GE interface view

Default Level

2: Configuration level

Usage Guidelines

Monitoring bandwidth usage helps you know current load on a device. If the bandwidth usage exceeds a threshold, bandwidth resources are insufficient and the device capacity needs to be expanded. For example, if the bandwidth usage exceeds 95%, an alarm is generated, indicating that bandwidth resources are almost exhausted. As a result, some services may be interrupted before device capacity expansion.

You can configure two thresholds: low threshold (log threshold) and high threshold (alarm threshold). The system generates a log when the bandwidth usage exceeds the low threshold and generates an alarm when the bandwidth usage exceeds the high threshold. This configuration ensures that you can expand the device capacity in advance to avoid service interruptions caused by bandwidth exhaustion.

NOTE

Outbound bandwidth usage threshold = (Outbound interface rate/Outbound physical interface bandwidth) x 100

Inbound bandwidth usage threshold = (Inbound interface rate/Inbound physical interface bandwidth) x 100

The **trap-threshold** command is used to set the bandwidth usage threshold for generating a trap.

The **log-threshold input-rate output-rate** command with the following parameters provides various functions:

- **log-threshold input-rate** *bandwidth-in-use* **resume-rate** *resume-threshold*: sets the inbound bandwidth usage threshold for generating a log to provide the following functions:
  - If inbound bandwidth usage value exceeds the value of *bandwidth-in-use*, an IFNET_BWRATE_IN_RISING log is generated, indicating that inbound bandwidth usage exceeds the configured threshold.
  - If inbound bandwidth usage value is lower than the value of *resume-threshold*, an IFNET_BWRATE_IN_RESUME log is generated, indicating that inbound bandwidth usage is lower than the configured threshold.
- **log-threshold output-rate** *bandwidth-in-use* **resume-rate** *resume-threshold*: sets the outbound bandwidth usage threshold for generating a log to provide the following functions:
  - If outbound bandwidth usage value exceeds the value of *bandwidth-in-use*, an IFNET_BWRATE_OUT_RISING log is generated, prompting for a bandwidth increase request.
  - If outbound bandwidth usage falls below the threshold specified by *resume-threshold*, an IFNET_BWRATE_OUT_RESUME log is generated, indicating that bandwidth usage has been restored.

If the offset between the value of *bandwidth-in-use* and the value of *resume-threshold* is too small, log information may be frequently displayed.

The log threshold must be lower than the trap threshold, providing efficient protection for services. For example, when the inbound bandwidth usage reaches 80%, a log is generated. If the inbound bandwidth usage continues to increase and reaches 95%, a trap is generated. This ensures that a log is generated for inbound bandwidth usage of 80%, and a trap is generated for inbound bandwidth usage of 95%. Either the log or the trap prompts for a bandwidth increase, preventing service interruption.

Example

# Configure GE0/0/1 to generate a log when the outbound interface rate exceeds 80% of the bandwidth.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] log-threshold output-rate 80
```

# Configure GE0/0/1 to generate a log when the outbound interface rate exceeds 80% of the bandwidth and to clear a log when the outbound interface rate is lower than 60% of the bandwidth.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] log-threshold output-rate 80 resume-rate 60
```

Related Topics

4.2.71 trap-threshold

4.2.33 log-threshold input-discard output-discard

Function

The **log-threshold input-discard output-discard** command enables the log function for inbound and outbound packet loss caused by congestion on an interface.

The **undo log-threshold input-discard output-discard** command disables the log function for inbound and outbound packet loss caused by congestion on an interface.

By default, the log function for inbound and outbound packet loss caused by congestion is enabled on an interface.

Format

log-threshold { **input-discard** | **output-discard** } [*threshold-value* **interval** *interval-value*]

undo log-threshold { **input-discard** | **output-discard** }

Parameters

Parameter	Description	Value
input-discard	Specifies the log function for inbound packet loss caused by congestion on an interface.	-
output-discard	Specifies the log function for outbound packet loss caused by congestion on an interface.	-
threshold-value	Specifies the packet loss threshold for triggering log generation.	The value is an integer that ranges from 100 to 4294967295. The default value is 300.
interval *interval-value*	Specifies the interval for collecting statistics on discarded packets.	The value is an integer that ranges from 60 to 86400, in seconds. The default value is 300.

Views

Ethernet interface view, GE interface view, XGE interface view, MultiGE interface view, 40GE interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Network congestion during service transmission may cause packet loss. If a lot of packets are discarded, services are affected. To better monitor the number of discarded packets, you can run the **log-threshold input-discard output-discard** on an interface to enable the log function for inbound and outbound packet loss caused by congestion. The device generates a log when the number of discarded incoming and outgoing packets on the interface in a specified period exceeds the threshold. Logs help you know the congestion on the interface. You can determine whether to increase the bandwidth or cancel the bandwidth limit on the interface based on the logs. In this way, the congestion problem can be solved.

Precautions

- If the number of discarded incoming and outgoing packets falls below the threshold in a specified period, the device generates a log indicating that the number of discarded packets falls below the threshold.
- If the number of discarded packets exceeds the threshold in an interval for collecting statistics on discarded packets, the device immediately generates a log indicating that the number of discarded packets exceeds the threshold, and enters the next statistics interval. In the next statistics interval, the number of discarded packets on an interface is calculated using the following formula:

  Number of discarded packets = Current number of discarded packets - Number of discarded packets in the beginning of the statistics interval
- If the number of discarded packets exceeds the threshold in several consecutive statistics intervals, the device only generates a log in the first statistics interval, indicating that the number of discarded packets exceeds the threshold. If the number of discarded packets falls below the threshold, the device generates a log indicating that the number of discarded packets falls below the threshold. If the number of discarded packets on an interface exceeds the threshold again, the device will generate a log indicating that the number of discarded packets exceeds the threshold.
- Running the **undo log-threshold input-discard output-discard** command restores the default threshold for discarded packets and default interval for collecting statistics on discarded packets, and disables the log function for inbound and outbound packet loss caused by congestion. However, the device still monitors the number of discarded packets and records the information in the diagnosis logs.

Example

# Enable the log function for inbound packet loss caused by congestion on GE0/0/1, and set the threshold for discarded packets to 100 and interval for collecting statistics on discarded packets to 60 seconds.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] log-threshold input-discard 100 interval 60
```

4.2.34 loopback

Function

The **loopback** command enables loopback detection on an interface.

The **undo loopback** command disables loopback detection on an interface.

By default, loopback detection is not configured.

Format

loopback internal

undo loopback

Parameters

Parameter	Description	Value
internal	Configures internal loopback detection on a specified interface.	-

Views

Ethernet interface view, GE interface view, XGE interface view, MultiGE interface view, 40GE interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When testing some special functions, for example, locating an Ethernet fault, you need to enable loopback detection on Ethernet interfaces to check whether the interfaces are working properly. After loopback detection is enabled on an Ethernet interface, the interface is in Up state if it works properly, and is in Down state if it fails.

Follow-up Procedure

Run the **display interface** command to check whether the current status of the interface configured with internal loopback is Up. If the **current status** of the interface is Up, the internal forwarding function works well; otherwise, a fault occurs during internal forwarding.

NOTE

After loopback detection is enabled on an interface, the **Speed** field in the **display this interface** command output indicates the configured interface rate or the rate of the installed optical module, copper module, or network cable, and the **Bandwidth** field in the **display interface ethernet brief** command output indicates the actual interface rate.

Precautions

Loopback detection interrupts the operation of Ethernet interfaces and links. After loopback detection is performed, run the **undo loopback** command to disable loopback detection immediately.

NOTE

You cannot run the **loopback** command to perform loopback detection on a fabric port.

Example

# Configure loopback detection on GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] loopback internal
```

Related Topics

4.1.10 display interface

4.2.35 loopbacktest

Function

The **loopbacktest** command configures internal loopback detection on an interface.

By default, internal loopback detection is not configured.

Format

loopbacktest internal

Parameters

Parameter	Description	Value
internal	Configures internal loopback detection. Internal loopback detection is used to check whether the internal forwarding chip controls forwarding on the interface correctly. ● If the test packet is received, the internal forwarding chip functions properly. ● If the test packet is not received, the internal forwarding chip is faulty.	-

Views

Ethernet interface view, GE interface view, XGE interface view, MultiGE interface view, 40GE interface view

Default Level

3: Management level

Usage Guidelines

You can run the **loopbacktest** command to check whether the internal forwarding chip functions properly.

NOTE

Loopback detection is not required when an interface is shut down.

Loopback detection is not supported on a service stack interface.

The internal loopback detection result can be used only when no service is configured on the switch.

You cannot run the **loopbacktest** command to perform loopback detection on a fabric port.

After the energy-saving mode is set to basic or deep, loopback detection is disabled on an interface. Therefore, before performing loopback detection, set the energy-saving mode to standard.

Example

# Configure internal loopback detection on GE0/0/1.

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

```
[HUAWEI-GigabitEthernet0/0/1] loopbacktest internal
Warning: This command may conflict with other service configurations. It can only be used on a device with
no configuration. Continu
e?[Y/N]:y
Info: This operation may take a few seconds. Please wait for a moment...................
Info: Loopback packet test succeeded.
```

Related Topics

4.1.10 display interface

4.2.36 mdi

Function

The **mdi** command configures the medium dependent interface (MDI) mode of an Ethernet electrical interface.

The **undo mdi** command restores the default MDI mode of an Ethernet electrical interface.

By default, an Ethernet electrical interface automatically identifies the network cable type.

Format

mdi { **across** | **auto** | **normal** }

undo mdi

Parameters

Parameter	Description	Value
across	Sets the MDI mode of an Ethernet electrical interface to **across**.	-
auto	Sets the MDI mode of an Ethernet electrical interface to **auto**. An Ethernet electrical interface automatically identifies the network cable type.	-
normal	Sets the MDI mode of an Ethernet electrical interface to **normal**.	-

Views

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

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Twisted pairs used to connect Ethernet devices include:

- Straight-through cable: connects devices of different types, such as a switch and a PC or a switch and a router.
- Crossover cable: connects devices of the same type, such as two switches, two routers, or two PCs.

Generally, if two interfaces are connected with a twisted-pair cable, the receive pin on the local end must be connected to the transmit pin on the remote end and the transmit pin on the local end must be connected to the receive pin on the remote end so that a link can be Up. According to pin assignment, twisted-pair cables are classified into straight-through and crossover cables. The device must support negotiation and crossover of receive and transmit pins so that Ethernet electrical interfaces can support the two types of twisted-pair cables. The device supports the following medium dependent interface (MDI) modes: auto, normal, and across.

Generally, when interfaces at both ends work in auto mode, devices can communicate regardless of whether the straight-through or crossover cable is used. Set the MDI mode to normal or across only when the device cannot identify the network cable type. When configuring an MDI mode on an interface, pay attention to the following points:

- When a straight-through cable is used, the local and remote interfaces must use different MDI modes, for example, across mode on one end and normal mode on the other end.
- When a crossover cable is used, the local and remote interfaces must use the same MDI mode. For example, both ends must use the across or normal mode, or at least one end uses the auto mode

NOTE

Electrical interfaces support the MDI type configuration.

The XGE electrical interfaces on the ES5D21X02T01 card of the S5720EI can only use the auto MDI type.

The MDI type can be configured on an XGE optical interface that has a GE copper module installed.

The MDI type can be configured on a GE optical interface that has a GE copper module installed.

Example

# Set the MDI mode of GE0/0/1 to **across**.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] mdi across
```

Related Topics

4.2.21 duplex

4.2.38 negotiation auto

4.2.37 negotiation active

Function

The **negotiation active** command configures an interface to work in slave mode.

The **undo negotiation active** command cancels the slave mode configuration on an interface.

By default, an interface does not work in slave mode.

Format

negotiation active

undo negotiation active

Parameters

None

Views

MultiGE interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When a MultiGE interface on a Huawei switch is connected to an interface on a Cisco AP, the two interfaces may both support 2.5 Gbit/s or higher rates, but cannot negotiate to work in the highest rate. You can configure the MultiGE interface on the Huawei switch to work in slave mode (the interface on the Cisco AP works in master mode). The two interfaces then can negotiate to work in the highest rate supported by both of them to improve the data transmission capability.

Precautions

- It is recommended that you run this command on an interface working in auto-negotiation mode.
- When MultiGE interfaces of two switches are connected, you cannot configure the **negotiation active** command on the MultiGE interfaces simultaneously; otherwise, the MultiGE interfaces cannot go Up.

Example

# Configure MultiGE0/0/1 to work in slave mode.

```
<HUAWEI> system-view
[HUAWEI] interface MultiGE 0/0/1
[HUAWEI-MultiGE0/0/1] negotiation active
```

4.2.38 negotiation auto

Function

The **negotiation auto** command configures an Ethernet interface to work in auto-negotiation mode.

The **undo negotiation auto** command configures an Ethernet interface to work in non-auto negotiation mode.

By default, an Ethernet interface works in auto-negotiation mode.

Format

negotiation auto

undo negotiation auto

Parameters

None

Views

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

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Earlier Ethernet worked in 10M half-duplex mode and required mechanisms such as Carrier Sense Multiple Access (CSMA)/Collision Detection (CD) to ensure system stability. As Ethernet technology develops, full-duplex Ethernet and 100 Mbit/s Ethernet emerge. This greatly improves Ethernet performance. Auto-negotiation technology allows new Ethernet to be compatible with earlier Ethernet. In auto-negotiation mode, interfaces on both ends of a link negotiate their operating parameters, including the duplex mode and rate. If the negotiation succeeds, the two interfaces work at the same operating parameters.

Precautions

- For details about Ethernet interfaces supporting the auto-negotiation function, see Licensing Requirements and Limitations for Ethernet Interfaces.

- By default, auto-negotiation is enabled on GE optical interfaces and rate auto-negotiation is disabled. You can run the **speed auto-negotiation** command to enable rate auto-negotiation.
- After configuring the auto-negotiation function on an interface, if you remove and install a single optical fiber on the interface, the interface may be Up and the remote interface may be Down. You can run the **shutdown** and **undo shutdown** commands on the remote interface to make the remote interface go Up.

Example

# Configure GE0/0/1 to work in non-auto negotiation mode.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo negotiation auto
```

Related Topics

4.2.21 duplex

4.2.36 mdi

4.2.65 speed

4.2.39 negotiation priority

Function

The **negotiation priority** command configures the protocol that a MultiGE interface in auto-negotiation mode preferentially uses.

The **undo negotiation priority** command restores the default protocol that a MultiGE interface in auto-negotiation mode preferentially uses.

By default, a MultiGE interface in auto-negotiation mode preferentially uses IEEE 802.3bz.

NOTE

Only MultiGE interfaces on the S5720-28X-PWH-LI-AC, S6720-32C-SI-AC, S6720-32C-SI-DC, S6720-32C-PWH-SI-AC, S6720-32C-PWH-SI, S6720-52X-PWH-SI, S6720-56C-PWH-SI-AC, and S6720-56C-PWH-SI support this command.

Format

negotiation priority { **802.3bz** | **mgbase-t** }

undo negotiation priority

Parameters

Parameter	Description	Value
802.3bz	Configures IEEE 802.3bz as the protocol that a MultiGE interface in auto-negotiation mode preferentially uses.	-

Parameter	Description	Value
mgbase-t	Configures Mgbase-t as the protocol that a MultiGE interface in auto-negotiation mode preferentially uses.	-

Views

MultiGE interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If the peer device supports 2.5 Gbit/s or 5 Gbit/s rate when the peer device connects to the MultiGE interface of Huawei switch and the peer device uses the proprietary protocol Mgbase-t of the Broadcom company, the MultiGE interface of the interconnected Huawei switch may fail to be enabled. You can configure Mgbase-t as the protocol that the MultiGE interface on the Huawei switch preferentially uses, so that the MultiGE interface can be properly enabled.

Example

# Configure Mgbase-t as the protocol that a MultiGE interface in auto-negotiation mode preferentially uses.

```
<HUAWEI> system-view
[HUAWEI] interface MultiGE 0/0/1
[HUAWEI-MultiGE0/0/1] negotiation priority mgbase-t
```

4.2.40 port link-flap interval

Function

The **port link-flap interval** command sets the link flapping detection interval.

The **undo port link-flap interval** command restores the default link flapping detection interval.

By default, the link flapping detection interval is 10s.

Format

port link-flap interval *interval-value*

undo port link-flap interval

Parameters

Parameter	Description	Value
interval-value	Specifies the link flapping detection interval.	The value is an integer that ranges from 5 to 60, in seconds. The default value is 10s.

Views

Ethernet interface view, GE interface view, XGE interface view, MultiGE interface view, 40GE interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Link flapping occurs when the physical status of an interface frequently alternates between Up and Down due to network flapping or network cable faults. Link flapping causes frequent network topology changes and affects user communication. For example, two links work in primary/backup mode. If the interface of the primary link experiences frequent Up/Down transitions, flows are switched between the primary and backup links. Frequent service switchovers increase load of the device and may result in service data loss.

Link flapping protection can solve the problem. You can configure this function to disable an interface that frequently alternates between Up and Down. When the interface is Down, the network topology will not change frequently. In the preceding example, you can configure link flapping protection on the interface of the primary link to prevent frequent topology changes. When the system detects frequent physical status changes on the interface of the primary link, the system directly disables the interface to trigger a primary/backup link switchover. The backup link then steadily transmits services. The link flapping protection function involves the following parameters:

- Number of link flappings: One link flapping refers to one interface Up/Down transition.
- Link flapping period: It is a period during which the system counts the number of link flappings.

If the number of link flappings on an interface reaches the threshold within a link flapping period, the system disables the interface and records its status as **ERROR DOWN(link-flap)**, indicating that the interface is Down because of link flappings. By default, after link flapping protection is enabled, an interface goes Down if its status changes five times within 10 seconds.

Prerequisites

The configured interval takes effect only after link flapping protection is enabled using the **port link-flap protection enable** command on the interface.

Precautions

If you run the **port link-flap interval** command multiple times in the same interface view, only the latest configuration takes effect.

Example

# Set the link flapping detection interval to 50s on GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] port link-flap interval 50
```

Related Topics

4.2.41 port link-flap protection enable

4.2.42 port link-flap threshold

4.2.41 port link-flap protection enable

Function

The **port link-flap protection enable** command enables link flapping protection on an interface.

The **undo port link-flap protection enable** command disables link flapping protection on an interface.

By default, link flapping protection is disabled on an interface.

Format

port link-flap protection enable

undo port link-flap protection enable

Parameters

None

Views

Ethernet interface view, GE interface view, XGE interface view, MultiGE interface view, 40GE interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Link flapping occurs when the physical status of an interface frequently alternates between Up and Down due to network flapping or network cable faults. Link flapping causes frequent network topology changes and affects user communication. For example, two links work in primary/backup mode. If the interface of the primary link experiences frequent Up/Down transitions, flows are switched between the primary and backup links. Frequent service switchovers increase load of the device and may result in service data loss.

Link flapping protection can solve the problem. You can configure this function to disable an interface that frequently alternates between Up and Down. When the interface is Down, the network topology will not change frequently. In the preceding example, you can configure link flapping protection on the interface of the primary link to prevent frequent topology changes. When the system detects frequent physical status changes on the interface of the primary link, the system directly disables the interface to trigger a primary/backup link switchover. The backup link then steadily transmits services. The link flapping protection function involves the following parameters:

- Number of link flappings: One link flapping refers to one interface Up/Down transition.
- Link flapping period: It is a period during which the system counts the number of link flappings.

If the number of link flappings on an interface reaches the threshold within a link flapping period, the system disables the interface and records its status as **ERROR DOWN(link-flap)**, indicating that the interface is Down because of link flappings. By default, after link flapping protection is enabled, an interface goes Down if its status changes five times within 10 seconds.

Follow-up Procedure

- Run the **port link-flap interval** *interval-value* command to set the link flapping interval for the interface.
- Run the **port link-flap threshold** *threshold-value* command to set the number of link flappings for the interface.
- An interface in Error-down state can be recovered using either of the following methods:
  - Manual recovery: If a few interfaces need to be recovered forcibly, run the **shutdown** and **undo shutdown** commands in the interface view. Alternatively, run the **restart** command in the interface view to restart the interfaces.
  - Automatic recovery: If a large number of interfaces need to be recovered, manual recovery is time consuming and some interfaces may be omitted. You can run the **error-down auto-recovery cause link-flap interval** *interval-value* command in the system view to enable automatic interface recovery and set the recovery delay time. An interface in Error-down state automatically recovers when the specified delay time expires.

Example

# Enable link flapping protection on GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] port link-flap protection enable
```

Related Topics

4.2.40 port link-flap interval

4.2.42 port link-flap threshold

4.2.22 error-down auto-recovery

4.2.42 port link-flap threshold

Function

The **port link-flap threshold** command sets the maximum number of link flapping events on an interface.

The **undo port link-flap threshold** command restores the default maximum number of link flapping events on an interface.

By default, the maximum number of link flapping events is 5.

Format

port link-flap threshold *threshold-value*

undo port link-flap threshold

Parameters

Parameter	Description	Value
threshold-value	Specifies the maximum number of link flapping events on an interface.	The value is an integer that ranges from 5 to 10. The default value is 5.

Views

Ethernet interface view, GE interface view, XGE interface view, MultiGE interface view, 40GE interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Link flapping occurs when the physical status of an interface frequently alternates between Up and Down due to network flapping or network cable faults. Link flapping causes frequent network topology changes and affects user communication. For example, two links work in primary/backup mode. If the interface of the primary link experiences frequent Up/Down transitions, flows are switched between the primary and backup links. Frequent service switchovers increase load of the device and may result in service data loss.

Link flapping protection can solve the problem. You can configure this function to disable an interface that frequently alternates between Up and Down. When the interface is Down, the network topology will not change frequently. In the preceding example, you can configure link flapping protection on the interface of the primary link to prevent frequent topology changes. When the system detects frequent physical status changes on the interface of the primary link, the system directly disables the interface to trigger a primary/backup link switchover. The backup link then steadily transmits services. The link flapping protection function involves the following parameters:

- Number of link flappings: One link flapping refers to one interface Up/Down transition.
- Link flapping period: It is a period during which the system counts the number of link flappings.

If the number of link flappings on an interface reaches the threshold within a link flapping period, the system disables the interface and records its status as **ERROR DOWN(link-flap)**, indicating that the interface is Down because of link flappings. By default, after link flapping protection is enabled, an interface goes Down if its status changes five times within 10 seconds.

Prerequisites

The **port link-flap threshold** command configuration takes effect only after link flapping protection is enabled using the **port link-flap protection enable** command on the interface.

Precautions

If you run the **port link-flap threshold** command multiple times in the same interface view, only the latest configuration takes effect.

Example

# Set the maximum number of link flapping events on GE0/0/1 to 10.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] port link-flap threshold 10
```

Related Topics

4.2.41 port link-flap protection enable

4.2.40 port link-flap interval

4.2.43 port-group

Function

The **port-group** command creates a permanent port group and displays the permanent port group view.

The **undo port-group** command deletes permanent port groups.

By default, no permanent port group is configured.

Format

port-group *port-group-name*

undo port-group { **all** | *port-group-name* }

Parameters

Parameter	Description	Value
port-group-name	Specifies the name of a permanent port group.	The value is a string of 1 to 32 case-insensitive characters without spaces. When double quotation marks are used around the string, spaces are allowed in the string. **NOTE** A permanent port group cannot be named **all**. Meanwhile, to avoid a usage conflict between the **port-group group-member** command and *port-group-name*, do not specify g, group-member, or first letters of group-member as the name of a permanent interface group.
all	Deletes all port groups.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If you need to perform the same operations on multiple Ethernet interfaces, configuring each interface one by one easily causes incorrect configurations and is labor-intensive.

The port group function easily solves the problem. You can add all the Ethernet interfaces to the same port group. After you run a configuration command once in the port group view, the configuration takes effect on all the Ethernet interfaces in the port group, reducing the configuration workload.

Two types of port groups are available:

- Temporary port group: To temporarily deliver a configuration to multiple interfaces, you can create a temporary port group. After you deliver the configuration and exit from the port group view, the system automatically deletes the temporary port group.

- Permanent port group: To deliver configurations to interfaces multiple times, you can create a permanent port group. After you exit from the port group view, the port group and member interfaces in the group still exist, facilitating subsequent batch configuration for the member interfaces. To delete a permanent port group, run the **undo port-group** { **all** | *port-group-name* } command.

Follow-up Procedure

Run the **group-member** command to add Ethernet interfaces to the created permanent port group.

Precautions

- The system supports a maximum of 32 permanent port groups and each port group supports a maximum of 48 member interfaces.
- Deleting a permanent port group will not clear the configurations of an interface in the port group.

Example

# Create port group **portgroup1** and enter the port group view.

```
<HUAWEI> system-view
[HUAWEI] port-group portgroup1
[HUAWEI-port-group-portgroup1]
```

Related Topics

4.2.13 display port-group

4.2.27 group-member

4.2.44 port-group group-member

Function

The **port-group group-member** command creates a temporary port group and adds specified Ethernet interfaces to the temporary port group. Commands configured for a temporary port group will be automatically run on all member interfaces.

By default, no temporary port group is created.

Format

port-group group-member { *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 Ethernet interfaces to be added to a temporary port group. **to** indicates an interface range. All interfaces numbered between *interface-number1* and *interface-number2* are added to the temporary port group.	The value of *interface-number2* must be larger than the value of *interface-number1*.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If you need to perform the same operations on multiple Ethernet interfaces, configuring each interface one by one easily causes incorrect configurations and is labor-intensive.

The port group function easily solves the problem. You can add all the Ethernet interfaces to the same port group. After you run a configuration command once in the port group view, the configuration takes effect on all the Ethernet interfaces in the port group, reducing the configuration workload.

Two types of port groups are available:

- Temporary port group: To temporarily deliver a configuration to multiple interfaces, you can create a temporary port group. After you deliver the configuration and exit from the port group view, the system automatically deletes the temporary port group.
- Permanent port group: To deliver configurations to interfaces multiple times, you can create a permanent port group. After you exit from the port group view, the port group and member interfaces in the group still exist, facilitating subsequent batch configuration for the member interfaces. To delete a permanent port group, run the **undo port-group** { **all** | *port-group-name* } command.

Configuration Impact

If the **port-group group-member** command is run more than once, all configurations take effect.

Precautions

- The **port-group group-member** command is equivalent to the **group-member** command executed in the permanent port group view. Multiple interfaces can be added to a permanent port group in batches using the **group-member** command.

- When you specify the keyword **to** in the **port-group group-member** command:
  - The interfaces specified by *interface-number1* and *interface-number2* must reside on the same member switch. To add contiguous interfaces on different member switches to the same port group, run this command several times or use the keyword **to** several times.
  - The interfaces specified by *interface-number1* and *interface-number2* must be of the same type, for example, both of the interfaces are GE interfaces.
  - The interfaces specified before and after the keyword **to** must have the same attribute. For example, both of them are main interfaces or sub-interfaces. If they are sub-interfaces, they must belong to the same main interface.
  - If **to** is not specified, the preceding limitations do not apply.
  - Only the S6720EI, S6720S-EI, S5720HI and S5720EI support sub-interfaces.

Example

# Add GE0/0/1, GE0/0/2, and GE0/0/3 to a temporary port group.

```
<HUAWEI> system-view
[HUAWEI] port-group group-member gigabitethernet 0/0/1 to gigabitethernet 0/0/3
[HUAWEI-port-group]
```

Related Topics

4.2.43 port-group

4.2.27 group-member

4.2.45 port-isolate enable

Function

The **port-isolate enable** command enables port isolation.

The **undo port-isolate enable** command disables port isolation.

By default, port isolation is disabled.

Format

port-isolate enable [**group** *group-id*]

undo port-isolate enable [**group** *group-id*]

Parameters

Parameter	Description	Value
group *group-id*	Specifies the ID of a port isolation group.	The value is an integer that ranges from 1 to 64.

Views

Ethernet interface view, GE interface view, XGE interface view, MultiGE interface view, 40GE interface view, port group view, Eth-Trunk interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To implement Layer 2 isolation between interfaces, add different interfaces to different VLANs. This, however, wastes VLAN resources. To save VLAN resources, enable port isolation to isolate interfaces in a VLAN. That is, you can add interfaces to a port isolation group to implement Layer 2 isolation between these interfaces. Port isolation provides secure and flexible networking schemes for customers.

Precautions

- After port isolation is configured, ports are isolated at Layer 2 but can communicate at Layer 3 by default. To configure both Layer 2 isolation and Layer 3 isolation, run the **port-isolate mode all** command.
- Interfaces in a port isolation group are isolated from each other, but interfaces in different port isolation groups can communicate. If *group-id* is not specified, interfaces are added to port isolation group 1 by default.

Example

# Enable port isolation on GE0/0/1.

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

Related Topics

4.2.14 display port-isolate group

4.2.46 port-isolate exclude vlan

Function

The **port-isolate exclude vlan** command excludes a VLAN where port isolation needs to be disabled.

The **undo port-isolate exclude vlan** command cancels the configuration.

By default, no VLAN is excluded when port isolation is configured.

Format

port-isolate exclude vlan { *vlan-id1* [**to** *vlan-id2*] } &<1-10>

undo port-isolate exclude vlan { *vlan-id1* [**to** *vlan-id2*] } &<1-10>

Parameters

Parameter	Description	Value
vlan-id1	Specifies the ID of a VLAN.	The value is an integer that ranges from 1 to 4094.
vlan-id1 **to** *vlan-id2*	Specifies VLAN IDs in a batch. ● *vlan-id1* specifies the first VLAN ID. ● *vlan-id2* specifies the last VLAN ID. *vlan-id2* must be greater than *vlan-id1*. *vlan-id1* and *vlan-id2* determine a VLAN range. ● If you do not specify **to** *vlan-id2*, only one VLAN is specified.	The values of *vlan-id1* and *vlan-id2* are integers that range from 1 to 4094.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To enable communication between users in a VLAN where port isolation needs to be disabled, run the **port-isolate exclude vlan** command to exclude the VLAN.

Only S1720GFR, S1720GW, S1720GWR, S1720X, S1720GW-E, S1720GWR-E, S1720X-E, S2720EI, S2750, S5700LI, S5720LI, S5720S-LI, S5720HI, S5710-X-LI, S5720SI, S5720S-SI, S5700S-LI, S5730SI, S5730S-EI, S6720SI, S6720S-SI, S6720LI, and S6720S-LI support this command.

Example

# Exclude VLAN 10 where port isolation needs to be disabled.

```
<HUAWEI> system-view
[HUAWEI] port-isolate exclude vlan 10
```

Related Topics

4.2.31 jumboframe enable

4.2.2 am isolate

4.2.14 display port-isolate group

4.2.47 protect-group member

Function

The **protect-group member** command adds the specified Ethernet interface to an interface protection group.

The **undo protect-group member** command deletes an Ethernet interface from an interface protection group.

By default, no Ethernet interface is added to an interface protection group.

Format

protect-group member *interface-type interface-number* { **master** | **standby** }

undo protect-group member *interface-type interface-number*

Parameters

Parameter	Description	Value
interface-type interface-number	Specifies the type and number of the interface to be added to an interface protection group.	-
master	Indicates the working interface.	-
standby	Indicates the protected interface.	-

Views

Interface protection group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Hosts are usually connected to an external network through a default gateway. If the outbound interface of the default gateway fails, the hosts cannot communicate with the external network, interrupting normal service transmission and degrading device reliability. The port protection function solves this problem. Without changing the networking, you can add two interfaces on the device to a port protection group to implement interface backup in active/standby mode. When the active interface fails, services are immediately switched to the standby interface, ensuring non-stop service transmission.

Prerequisites

An interface protection group has been created using the **port protect-group** command.

Precautions

An interface protection group contains only a working interface and a protected interface.

Example

# Add GigabitEthernet0/0/1 to an interface protection group.

```
<HUAWEI> system-view
[HUAWEI] port protect-group 1
[HUAWEI-protect-group1] protect-group member gigabitethernet 0/0/1 master
```

Related Topics

4.2.50 port protect-group

4.2.15 display port protect-group

4.2.48 port-isolate mode

Function

The **port-isolate mode** command sets the port isolation mode.

The **undo port-isolate mode** command restores the default port isolation mode.

By default, ports are isolated at Layer 2 but can communicate at Layer 3.

Format

port-isolate mode { **l2** | **all** }

undo port-isolate mode

Parameters

Parameter	Description	Value
l2	Indicates that ports are isolated at Layer 2 but can communicate at Layer 3.	-
all	Indicates that ports are isolated at both Layer 2 and Layer 3.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To implement Layer 2 isolation between interfaces, you can add different interfaces to different VLANs. This wastes VLAN resources. Port isolation can isolate interfaces in the same VLAN. That is, you only need to add interfaces to a port isolation group to implement Layer 2 isolation between these interfaces. Port isolation provides secure and flexible networking schemes.

You can configure the interface isolation mode to **all** to implement Layer 2 and Layer 3 isolation between interfaces in a port isolation group.

NOTE

The S1720GFR, S1720GW, S1720GWR, S1720X, S1720GW-E, S1720GWR-E, S1720X-E, S2720EI, S2750, S5700LI, S5720LI, S5720S-LI, S5710-X-LI, S5700S-LI, S6720LI and S6720S-LI support isolation at Layer 2 and interworking at Layer 3, and do not support this command.

Example

# Configure Layer 2 isolation and Layer 3 communication.

```
<HUAWEI> system-view
[HUAWEI] port-isolate mode l2
```

Related Topics

4.2.14 display port-isolate group

4.2.45 port-isolate enable

4.2.49 port media type

Function

The **port media type** command determines whether an interface configuration item belongs to the optical interface or electrical interface.

The **undo port media type** command restores the default settings.

Format

port media type { **copper** | **fiber** }

undo port media type { **copper** | **fiber** }

Parameters

Parameter	Description	Value
copper	Indicates that a configuration item belongs to the electrical interface.	-
fiber	Indicates that a configuration item belongs to the optical interface.	-

Views

GE interface view

Default Level

2: Configuration level

Usage Guidelines

This command only distinguishes optical interface configuration and electrical interface configuration, and is not configurable.

If you have specified the interface attributes (such as auto-negotiation, speed, and full-duplex mode) on a combo interface, the system automatically generates this command to determine whether an interface configuration item belongs to the optical interface or electrical interface. After this command is generated, the configuration for the other interface type (such as optical interface) will not be lost if the combo interface works as an electrical interface.

For example, after you run the **2.1.10 display this** command on a combo interface, the interface configuration is as follows:

```
#
interface GigabitEthernet0/0/1
```

```
 port media type copper
  undo negotiation auto
  speed 100
 port media type fiber
  undo negotiation auto
#
```

The command output shows that there are two configuration items **undo negotiation auto** and **speed 100** when the combo interface works as an electrical interface and one configuration item **undo negotiation auto** when the combo interface works as an optical interface.

Example

None

4.2.50 port protect-group

Function

The **port protect-group** command creates an interface protection group and enters the interface protection group view.

The **undo port protect-group** command deletes the created interface protection group.

By default, no interface protection group is created.

Format

port protect-group *protect-group-index*

undo port protect-group *protect-group-index*

Parameters

Parameter	Description	Value
protect-group-index	Specifies the ID of an interface protection group.	The value is an integer that ranges from 0 to 63.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Hosts are usually connected to an external network through a default gateway. If the outbound interface of the default gateway fails, the hosts cannot communicate with the external network, interrupting normal service transmission and degrading device reliability. The port protection function solves this problem. Without changing the networking, you can add two interfaces on the device to a port protection group to implement interface backup in active/standby mode. When the active interface fails, services are immediately switched to the standby interface, ensuring non-stop service transmission.

Follow-up Procedure

Run the **protect-group member** command to add the specified Ethernet interface to an interface protection group.

Example

# Create an interface protection group.

```
<HUAWEI> system-view
[HUAWEI] port protect-group 1
```

Related Topics

4.2.47 protect-group member

4.2.15 display port protect-group

4.2.51 port split

Function

The **port split** command splits a specified 40GE interface.

The **undo port split** command cancels the split configuration on a 40GE interface.

By default, no 40GE interface is split into four 10GE interfaces.

Format

port split split-type 40GE:4*XGE

undo port split

Parameters

Parameter	Description	Value
split-type 40GE:4*XGE	Splits a specified 40GE interface into four 10GE interfaces.	-

Views

XGE interface view, 40GE interface view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

Some 40GE optical interfaces can be used as independent interfaces or each can be split into four 10GE interfaces. With the interface split function, a device with 40GE interfaces can provide high-density 10GE interfaces, and can connect to 40GE or 10GE interfaces on the remote device. This function allows for flexible networking and lowers hardware costs.

To split an interface, run the **port split split-type 40GE:4*XGE** command in the view of the 40GE interface. To merge converted interfaces into the original 40GE interface, run the **undo port split** command in the view of only one of the four 10GE converted interfaces.

- If interface split or merge is configured on an interface, the original configuration on the interface is lost. Therefore, exercise caution when deciding to perform the interface split or merge operation.
- 10GE interfaces converted from a 40GE interface are numbered based on the number of the last 10GE interface on the switch. For interfaces on the switch panel, if the last 10GE interface is numbered XGE 0/y/m and a 40GE interface to be split is numbered 40GE 0/y/n, the four 10GE interfaces converted from the 40GE interface are numbered XGE 0/y/(m + 4 * (n - 1) + z + 1). For example, if the last 10GE interface on a switch is numbered XGE 0/0/48, the four 10GE interfaces converted from 40GE 0/0/3 are numbered XGE 0/0/57, XGE 0/0/58, XGE 0/0/59, and XGE 0/0/60. For interfaces on a card, m has a fixed value of 0. For example, the four 10GE interfaces converted from 40GE 1/1/1 on a card are numbered XGE 1/1/1, XGE 1/1/2, XGE 1/1/3, and XGE 1/1/4.
  - y: indicates the subcard number.
  - m: indicates the sequence number of the last 10GE interface on the switch.
  - n: indicates the sequence number of the 40GE interface.
  - z: indicates the interface location. The value ranges from 0 to 3.

  NOTE

  Split interfaces are numbered in the same sequence as the wires of a cable are numbered. For example, in a 1-to-4 cable, the wire numbered 1 corresponds to the interface with the lowest interface number, and the wire numbered 4 corresponds to the interface with the highest interface number.
- If an interface is split, the interface and converted interfaces cannot be added to a stack interface, regardless of whether the configuration takes effect. If an interface has been added to a stack interface, the interface cannot be split.
- After configuring interface split using the **port split split-type 40GE:4*XGE** command, restart the device to make the configuration take effect. You can run the **display port split** command in any view to check the status of a split interface.

Example

# Split a 40GE interface into four 10GE interfaces and restart the device to make the configuration take effect.

```
<HUAWEI> system-view
[HUAWEI] interface 40GE 0/0/1
[HUAWEI-40GE0/0/1] port split split-type 40GE:4*XGE
Warning: This command will take effect only after resetting the board. 40GE0/0/1 will be split up into XGE,
and the port configuration will be lost when the port type is changed. Continue? [Y/N]:y
Info: Succeeded in setting the configuration.
[HUAWEI-40GE0/0/1] return
<HUAWEI> reboot
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:/device.cfg. Continue? [Y/N]:y
Now saving the current configuration to the slot 0.
Save the configuration successfully.
Info: If want to reboot with saving diagnostic information, input 'N' and then execute 'reboot save
diagnostic-information'.
System will reboot! Continue?[Y/N]:y
```

Related Topics

4.2.16 display port split

4.2.52 portswitch

Function

The **portswitch** command changes the working mode of Ethernet interfaces from Layer 3 mode to Layer 2 mode.

The **undo portswitch** command changes the working mode of Ethernet interfaces from Layer 2 mode to Layer 3 mode.

By default, an Ethernet interface works in Layer 2 mode.

Format

portswitch

undo portswitch

Parameters

None

Views

GE interface view, XGE interface view, 40GE interface view, Eth-Trunk interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

By default, an Ethernet interface on the device works in Layer 2 mode. To enable Layer 3 functions on the interface, run the **undo portswitch** command on the interface.

Precautions

- If an interface has the non-attribute configuration, this command cannot be executed. Before running this command, delete the non-attribute configuration on the interface.
- The minimum interval between running the **portswitch** and **undo portswitch** commands must be 30s.

NOTE

Only interfaces on the S5720HI, S5720EI, S6720S-EI, and S6720EI support switching between Layer 2 and Layer 3 modes.

Ethernet interfaces working at Layer 3 support IP address configuration.

By default, Ethernet interfaces on the device work at Layer 2 mode and have been added to VLAN 1. You can run the **undo portswitch** command to change the working mode to Layer 3 mode. The Ethernet interfaces are removed from VLAN 1 only after Layer 3 protocols become Up.

Example

# Change the working mode of GE0/0/1 from Layer 2 mode to Layer 3 mode.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] ip address 10.10.10.10 255.255.255.0
```

Related Topics

4.2.53 portswitch batch

4.2.53 portswitch batch

Function

The **portswitch batch** command changes the working mode of Ethernet interfaces from Layer 3 mode to Layer 2 mode in batches.

The **undo portswitch batch** command changes the working mode of Ethernet interfaces from Layer 2 mode to Layer 3 mode in batches.

By default, the working mode of the interface is Layer 2 mode.

Format

portswitch batch *interface-type* { *interface-number1* [**to** *interface-number2*] } &<1-10>

undo portswitch batch *interface-type* { *interface-number1* [**to** *interface-number2*] } &<1-10>

Parameters

Parameter	Description	Value
interface-type interface-number1 [**to** *interface-number2*]	Specifies interfaces of which the working mode needs to be changed. ● *interface-number1* specifies the number of the first interface. ● *interface-number2* specifies the number of the last interface. The value of *interface-number2* must be larger than the value of *interface-number1*. *interface-number1* and *interface-number2* specify the range of interfaces. ● If **to** *interface-number2* is not specified, only the working mode of the interface specified by *interface-number1* is changed. **NOTE** You can specify a maximum of 10 interface number ranges at a time. The entered ranges cannot overlap.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can run the **portswitch batch** or **undo portswitch batch** command to change the working mode of interfaces in batches.

Precautions

- The mode switching function takes effect when the interface only has attribute configurations (for example, **shutdown** and **description** configurations). If the service configuration (for example, **port link-type access** configuration) exists on the interface, you must clear the service configuration before running this command.
- The minimum interval between running the **portswitch batch** and **undo portswitch batch** commands must be 30s.

NOTE

Only interfaces on the S5720HI, S5720EI, S6720S-EI, and S6720EI support switching between Layer 2 and Layer 3 modes.

Ethernet interfaces working at Layer 3 support IP address configuration.

Example

# Change the working mode of GE0/0/1, 0/0/2, and 0/0/3 to Layer 2 mode.

```
<HUAWEI> system-view
[HUAWEI] portswitch batch gigabitethernet 0/0/1 0/0/2 0/0/3
```

Related Topics

4.2.52 portswitch

4.2.54 reset statistics-peak

Function

The **reset statistics-peak** command clears Peak Information Rate (PIR) statistics on an interface.

Format

reset statistics-peak interface *interface-type interface-number*

NOTE

PIR statistics on the management interface cannot be cleared.

Parameters

Parameter	Description	Value
interface *interface-type interface-number*	Clears PIR statistics on a specified interface. ● *interface-type* specifies the interface type. ● *interface-number* specifies the interface number.	-

Views

All views

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Generally, the PIR of an interface indicates the maximum rate of the interface in a long time. To check the recent peak rate of an interface, run the **reset statistics-**

peak command to clear the previous peak rate record and obtain the new peak rate. To view the peak rate of an interface, run the **display interface** command. The following information is displayed:

```
Input peak rate 244425848 bits/sec,Record time: 2008-01-01 00:16:37
Output peak rate 753496 bits/sec,Record time: 2008-01-15 19:25:12
```

Precautions

PIR statistics on a specified interface cannot be restored after they are cleared. Exercise caution before clearing the statistics.

Example

# Clear PIR statistics on GE0/0/1.

```
<HUAWEI> reset statistics-peak interface gigabitethernet 0/0/1
```

Related Topics

4.1.10 display interface

4.2.55 reset virtual-cable-test

Function

The **reset virtual-cable-test** command deletes cable test results on an interface.

Format

reset virtual-cable-test { *interface-type interface-number* | **all** }

Parameters

Parameter	Description	Value
interface-type interface-number	Deletes cable test results on a specified interface. ● *interface-type* specifies the interface type. ● *interface-number* specifies the interface number. **NOTE** This Parameter can be an XGE optical interface when the interface has a GE copper module installed.	-
all	Deletes cable test results on all interfaces.	-

Views

All views

Default Level

3: Management level

Usage Guidelines

Usage Scenario

Before conducting a cable test on an electrical interface, you can use this command to delete the previous test results.

Precautions

The cable test results cannot be restored after they are cleared. Exercise caution before clearing the statistics.

Example

# Delete cable test results on GE0/0/1.

```
<HUAWEI> reset virtual-cable-test gigabitethernet 0/0/1
```

Related Topics

4.2.73 virtual-cable-test

4.2.20 display virtual-cable-test

4.2.56 set device port-on-card enable

Function

The **set device port-on-card enable** command configures the card interface working mode.

The **undo set device port-on-card enable** command restores the panel interface working mode.

By default, a switch works in the panel interface working mode.

NOTE

Only S6720-C-SI series switches support this command.

Format

set device port-on-card enable [**slot** *slot-id*]

undo set device port-on-card enable [**slot** *slot-id*]

Parameters

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

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

S6720-C-SI series switches support extended cards. However, the four 10GE SFP+ Ethernet optical interfaces on the front panel and interfaces on the extended cards (excluding the 4*10GE card) cannot be used simultaneously. By default, a switch uses interfaces on the panel. To use interfaces on a card, run the **set device port-on-card enable** command to configure the card interface working mode. Interfaces on the panel then cannot be used.

Precautions

- When a 4*10GE card is installed, both interfaces on the card and panel can be used.
- After running this command, you must confirm operations as prompted so that the switch automatically restarts to make the configuration take effect. Save the configuration in advance.
- When the panel interface working mode is changed to the card interface working mode, the four 10GE SFP+ Ethernet optical interfaces on the front panel cannot be used. After the **save** command is run, the configuration of the four 10GE SFP+ Ethernet optical interfaces on the front panel will be cleared. This applies to the interfaces on the card similarly when the card interface working mode is changed to the panel interface working mode.

Example

# Configure the card interface working mode.

```
<HUAWEI> system-view
[HUAWEI] set device port-on-card enable
```

Related Topics

4.2.10 display device port-on-card status

4.2.57 set ethernet speed down-grade

Function

The **set ethernet speed down-grade** command enables the rate decrease auto-negotiation function on an interface.

The **undo set ethernet speed down-grade** command disables the rate decrease auto-negotiation function on an interface.

By default, rate decrease auto-negotiation is disabled on an interface.

NOTE

Rate decrease auto-negotiation takes effect only on MultiGE interfaces, GE optical interfaces that have GE copper modules installed or GE electrical interfaces on the device.

Format

set ethernet speed down-grade

undo set ethernet speed down-grade

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Two devices are connected through two GE electrical interfaces using a network cable. The two GE interfaces are configured to work in rate auto-negotiation mode. The network cable can only work at the rate of 100 Mbit/s or 10 Mbit/s because it deteriorates, but the maximum rate supported by the two GE interfaces is 1000 Mbit/s. The interfaces negotiate the working rate to 1000 Mbit/s, but cannot go Up because the network cable does not support the rate of 1000 Mbit/s.

You can use the rate decrease auto-negotiation function to solve this problem. After rate decrease auto-negotiation is enabled using this command, the two GE interfaces can decrease the negotiated rate to 10 Mbit/s or 100 Mbit/s, and then can go Up.

Prerequisites

The two connected interfaces work in auto-negotiation mode. If an interface works in non-auto-negotiation mode, run the **negotiation auto** command in the interface view to configure it to work in auto-negotiation mode.

Precautions

If rate decrease auto-negotiation is configured on the local interface, but not on the remote interface, the local interface can still decrease the negotiated rate to 100 Mbit/s. If the rate decrease auto-negotiation function is configured on an interface of the S5720-28X-PWH-LI-AC, S6720-32C-SI-AC, S6720-32C-SI-DC, S6720-32C-PWH-SI-AC, S6720-32C-PWH-SI, S6720-52X-PWH-SI, S6720-56C-PWH-SI-AC or S6720-56C-PWH-SI, you must also configure this function on the remote interface; otherwise, the local and remote interfaces may not go Up.

If the network cable quality is low, a MultiGE interface takes longer time to go Up after the rate decrease auto-negotiation function is configured. For example, if the rate is decreased from 10 Gbit/s to 100 Mbit/s, the MultiGE interface takes about 40 seconds to go Up. If the rate is decreased from 2.5 Gbit/s to 100 Mbit/s, the MultiGE interface takes about 20 seconds to go Up. It is recommended that you replace the network cable.

After the rate decrease auto-negotiation function is configured on a MultiGE interface of the S5720-28X-PWH-LI-AC and a network cable is removed and reinstalled on the interface in Down state continuously, the interface rate automatically decreases to 1000 Mbit/s. You can remove and reinstall the network cable again after the interface goes Up or run the **shutdown** and **undo shutdown** commands on the remote interface to restore the interface rate to 2500 Mbit/s.

Example

# Configure the rate decrease auto-negotiation function on a GE interface.

```
<HUAWEI> system-view
[HUAWEI] set ethernet speed down-grade
```

Related Topics

4.2.38 negotiation auto

4.2.58 set flow-statistics include-interframe

Function

The **set flow-statistics include-interframe** command configures traffic statistics on an interface to contain the inter-frame gap and preamble.

The **undo set flow-statistics include-interframe** command configures traffic statistics on an interface not to contain the inter-frame gap and preamble.

By default, traffic statistics on an interface contain the inter-frame gap and preamble.

Format

set flow-statistics include-interframe

undo set flow-statistics include-interframe

Parameters

None

Views

Ethernet interface view, GE interface view, XGE interface view, MultiGE interface view, 40GE interface view, port group view, Eth-Trunk interface view

Default Level

2: Configuration level

Usage Guidelines

You can run the **display interface** command to view the running status and traffic statistics on an interface. The **Last 300 seconds input rate** or **Last 300 seconds output rate** field in the command output indicates the inbound or outbound traffic rate on the interface in the last 300 seconds.

- If you want to obtain the total number of bytes passing through an interface in a period, configure the device to count the bytes in the interframe gap (IFG) and preamble when collecting traffic statistics on the interface. The interface traffic rate is as follows:

  Interface traffic rate = (Original packet length + IFG + Preamble) x Number of packets passing through the interface every second
- If you want to obtain only the number of packet bytes passing through an interface in a period, configure the device not to count the bytes in the IFG and preamble when collecting traffic statistics on the interface. The interface traffic rate is as follows:

  Interface traffic rate = Original packet length x Number of packets passing through the interface every second

  By default, the IFG has a fixed value of 12 bytes and the preamble has a fixed value of 8 bytes. You can run the **ifg** command to configure the IFG.

Example

# Configure traffic statistics on GE0/0/1 to contain the inter-frame gap and preamble.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] set flow-statistics include-interframe
```

Related Topics

4.1.10 display interface

4.2.59 set flow-change-ratio

Function

The **set flow-change-ratio** { **input-threshold** | **output-threshold** } **upper-limit** command sets the trap threshold for a sudden traffic volume change on interfaces.

The **undo set flow-change-ratio** { **input-threshold** | **output-threshold** } **upper-limit** command restores the default trap threshold for a sudden traffic volume change on interfaces.

By default, the trap threshold for a sudden traffic volume change on interfaces is 50%.

The **set flow-change-ratio start-check bandwidth-usage** command sets the lower threshold of the initial bandwidth usage percentage for triggering a trap.

The **undo set flow-change-ratio start-check bandwidth-usage** command restores the default lower threshold of the initial bandwidth usage percentage for triggering a trap.

By default, the lower threshold of the initial bandwidth usage percentage for triggering a trap is 20%.

Format

set flow-change-ratio { **input-threshold** | **output-threshold** } **upper-limit** *threshold*

set flow-change-ratio start-check bandwidth-usage *bandwidth-usage-threshold*

undo set flow-change-ratio { **input-threshold** | **output-threshold** } **upper-limit**

undo set flow-change-ratio start-check bandwidth-usage

Parameters

Parameter	Description	Value
input-threshold	Specifies the trap threshold for a sudden traffic volume change in the inbound direction of interfaces.	-
output-threshold	Specifies the trap threshold for a sudden traffic volume change in the outbound direction of interfaces.	-
upper-limit *threshold*	Specifies the threshold for the traffic volume change percentage on interfaces.	The value is an integer that ranges from 0 to 100. The default value is 50.
start-check	Indicates that the switch checks the initial bandwidth usage when a trap is triggered.	-

Parameter	Description	Value
bandwidth-usage *bandwidth-usage-threshold*	Specifies the lower threshold of the initial bandwidth usage percentage for triggering a trap.	The value is an integer that ranges from 0 to 100. The default value is 20.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To allow the switch to detect real-time traffic volume changes on interfaces, you can run this command to set the trap threshold for a sudden traffic volume change on interfaces and the lower threshold of the initial bandwidth usage percentage for triggering a trap.

Traffic volume change percentage on interfaces = |Interface rate in the current traffic statistics collection interval - Interface rate in the previous traffic statistics collection interval| / Interface rate in the previous traffic statistics collection interval

Configuration Impact

If the trap function for a sudden traffic volume change is enabled (using the **snmp-agent trap enable feature ifpdt trap-name hwInputRateChangeOverThresholdNotice** or **snmp-agent trap enable feature ifpdt trap-name hwOutputRateChangeOverThresholdNotice** command) after the **set flow-change-ratio** command is enabled, a trap will be generated when the traffic volume change percentage on interfaces exceeds the specified threshold (value of *threshold*) and the bandwidth usage percentage is not lower than the lower threshold (value of *bandwidth-usage-threshold*).

Precautions

You can run the **set flow-stat interval** command to configure the traffic statistics collection interval on interfaces. The default interval is 300 seconds.

Example

# Set the trap threshold for a sudden traffic volume change in the inbound direction of interfaces to 70%.

```
<HUAWEI> system-view
[HUAWEI] set flow-change-ratio input-threshold upper-limit 70
```

Related Topics

4.1.23 set flow-stat interval

4.2.60 set flow-change-ratio input-broadcast-detect disable

Function

The **set flow-change-ratio input-broadcast-detect disable** command disables detection of a sudden broadcast traffic volume change in the inbound direction of interfaces.

The **undo set flow-change-ratio input-broadcast-detect disable** command enables detection of a sudden broadcast traffic volume change in the inbound direction of interfaces.

By default, detection of a sudden broadcast traffic volume change in the inbound direction of interfaces is enabled.

Format

set flow-change-ratio input-broadcast-detect disable

undo set flow-change-ratio input-broadcast-detect disable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

By default, the switch checks whether the volume of broadcast traffic in the inbound direction of interfaces changes suddenly, and generates a trap after detecting a sudden change, facilitating network maintenance.

If the switch has many interfaces, detection of a sudden broadcast traffic volume change in the inbound direction of interfaces consumes some CPU and memory resources. You can run the **set flow-change-ratio input-broadcast-detect disable** command to disable the function.

Precautions

If the system software is upgraded from V200R009C00 or an earlier version to V200R010C00 or a later version, detection of a sudden broadcast traffic volume change in the inbound direction of interfaces is disabled by default.

Example

# Disable detection of a sudden broadcast traffic volume change in the inbound direction of interfaces.

```
<HUAWEI> system-view
[HUAWEI] set flow-change-ratio input-broadcast-detect disable
```

4.2.61 single-fiber enable

Function

The **single-fiber enable** command enables the single-fiber communication function on an optical interface.

The **undo single-fiber enable** command disables the single-fiber communication function on an optical interface.

By default, the single-fiber communication function is disabled on an interface.

Format

single-fiber enable

undo single-fiber enable

Parameters

None

Views

XGE interface view, port group view, 40GE interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

During network management and maintenance, the administrator may need to send traffic from users to a specified server for analysis and processing. If a server can receive and send packets, there is a possibility that the server forwards user traffic to other devices, causing a security risk. The unidirectional single-fiber communication function can address this issue. A single fiber means that two optical modules are connected by only one fiber, and unidirectional communication means that packets can be sent in only one direction. With this function, a switch can only send but cannot receive packets, and an analysis server can only receive but cannot send packets. The data security on the analysis server is ensured.

Precautions

An optical interface does not support this function after it connects to a cable.

The remote interface also works in non-auto negotiation mode and the rate of the peer interface is the same as the rate of the local interface.

NOTE

The **single-fiber enable** command and the **Configuring Internal Loopback Detection** and **MAC SWAP loopback test** function cannot be configured on the same interface.

An XGE optical interface supports the **single-fiber enable** command only when it has no module installed or has an XGE optical module installed. Particularly, XGE optical interfaces on the S5720-EI, S6720-EI, and S6720S-EI also support the **single-fiber enable** command after GE optical modules are installed.

A 40GE optical interface supports the **single-fiber enable** command only when it has no optical module installed or has a 40GE optical module installed.

On an interface with the **single-fiber enable** command configured, the command is deleted by the system in the following situations:

- The XGE interface is connected to a cable or has a GE optical module installed.
- The 40GE interface is connected to a cable.

Example

# Enable XGigabitEthernet0/0/1 to send packets through a single fiber.

```
<HUAWEI> system-view
[HUAWEI] interface XGigabitEthernet 0/0/1
[HUAWEI-XGigabitEthernet0/0/1] single-fiber enable
```

Related Topics

4.2.38 negotiation auto

4.2.62 snmp-agent trap enable feature-name ifnet

Function

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

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

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

Format

snmp-agent trap enable feature-name ifnet [**trap-name** { **hwentityextcfmovercard** | **hwentityextcfmoverslot** | **hwextinterfacedelete** | **hwifflowdown** | **hwifflowup** | **hwifmonitorcrcerrorresume** | **hwifmonitorcrcerrorrising** | **hwifmonitorinputrateresume** | **hwifmonitorinputraterising** | **hwifmonitoroutputrateresume** | **hwifmonitoroutputraterising** | **hwifnamechange** | **hwifnamechangeresume** | **linkdown** | **linkup** }]

undo snmp-agent trap enable feature-name ifnet [**trap-name** { **hwentityextcfmovercard** | **hwentityextcfmoverslot** | **hwextinterfacedelete** | **hwifflowdown** | **hwifflowup** | **hwifmonitorcrcerrorresume** | **hwifmonitorcrcerrorrising** | **hwifmonitorinputrateresume** |

hwifmonitorinputraterising | **hwifmonitoroutputrateresume** | **hwifmonitoroutputraterising** | **hwifnamechange** | **hwifnamechangeresume** | **linkdown** | **linkup** }]

Parameters

Parameter	Description	Value
trap-name	Enables the traps of IFNET events of specified types.	-
hwentityextcfmover-card	Enables the trap function for configurations related to the interface sub-card.	-
hwentityextcfmoverslot	Enables the trap function for configurations related to the device.	-
hwextinterfacedelete	Enables the trap function for an interface deletion event.	-
hwifflowdown	Enables the trap function for the event that the status of traffic on an interface becomes Down.	-
hwifflowup	Enables the trap function for the event that the status of traffic on an interface becomes Up.	-
hwifmonitorcrcerrorresume	Enables the trap function for the event that the number of CRC error packets on an interface falls below the threshold.	-
hwifmonitorcrcerrorrising	Enables the trap function for the event that the number of CRC error packets on an interface exceeds the threshold.	-
hwifmonitorinputrateresume	Enables the trap function for the event that the rate of incoming traffic on an interface falls below the threshold.	-

Parameter	Description	Value
hwifmonitorinputraterising	Enables the trap function for the event that the rate of incoming traffic on an interface exceeds the threshold.	-
hwifmonitoroutputrateresume	Enables the trap function for the event that the rate of outgoing traffic on an interface falls below the threshold.	-
hwifmonitoroutputraterising	Enables the trap function for the event that the rate of outgoing traffic on an interface exceeds the threshold.	-
hwifnamechange	Enables the trap function for the event that the device joins a stack and the interface number format is changed from slot ID/subcard ID/port number to stack member ID/slot ID/subcard ID/port number.	-
hwifnamechangeresume	Enables the trap function for the event that the device leaves a stack and the interface number format is changed from stack member ID/slot ID/subcard ID/port number to slot ID/subcard ID/port number.	-
linkdown	Enables the trap function for the event that the link layer protocol status becomes Down.	-
linkup	Enables the trap function for the event that the link layer protocol status becomes Up.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

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

Example

# Enable all traps of the IFNET module.

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

Related Topics

4.2.17 display snmp-agent trap feature-name ifnet all

4.2.63 snmp-agent trap enable feature-name ifpdt

Function

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

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

The default configuration of the **snmp-agent trap enable feature-name ifpdt** command can be checked using the **display snmp-agent trap feature-name ifpdt all** command.

Format

snmp-agent trap enable feature-name ifpdt [**trap-name** { **hwcablesnrabnormal** | **hwcablesnrdetectnotsupport** | **hwcablesnrnormal** | **hwportnosupportoetrap** | **hwtrunkmemspeeddifferentalarm** | **hwtrunkmemspeeddifferentresume** | **hwporterrorrateexceed** | **hwsubifnumexceededspecalarm** | **hwsubifnumexceededspecalarmresume** | **hwinputratechangeoverthresholdnotice** | **hwoutputratechangeoverthresholdnotice** | **hwphysicalportinbroadcastrapidchange** | **hwportprotectgroupunavailable** | **hwportprotectgroupavailable** | **hwportprotectgroupdelete** }]

undo snmp-agent trap enable feature-name ifpdt [**trap-name** { **hwcablesnrabnormal** | **hwcablesnrdetectnotsupport** | **hwcablesnrnormal** | **hwportnosupportoetrap** | **hwtrunkmemspeeddifferentalarm** | **hwtrunkmemspeeddifferentresume** | **hwporterrorrateexceed** | **hwsubifnumexceededspecalarm** | **hwsubifnumexceededspecalarmresume** | **hwinputratechangeoverthresholdnotice** | **hwoutputratechangeoverthresholdnotice** | **hwphysicalportinbroadcastrapidchange** | **hwportprotectgroupunavailable** | **hwportprotectgroupavailable** | **hwportprotectgroupdelete** }]

NOTE

Only the S5720EI supports **hwporterrorrateexceed** parameter in the command.

Only the S6720EI, S6720S-EI, S5720HI, and S5720EI support **hwsubifnumexceededspecalarm** or **hwsubifnumexceededspecalarmresume** parameter in the command.

Parameters

Parameter	Description	Value
trap-name	Enables the trap function for a specified event of the IFPDT module.	-
hwcablesnrabnormal	Enables the trap function for the event that the network cable quality is abnormal.	-
hwcablesnrdetectnot-support	Enables the trap function for the event that the network cable quality cannot be checked.	-
hwcablesnrnormal	Enables the trap function for the event that the network cable quality is normal.	-
hwportnosupportoetrap	Enables the trap function for the event that a stack interface connects to a copper module or a GE optical module.	-
hwtrunkmemspeeddifferentalarm	Enables the trap function for the event that rates of active interfaces of the Eth-Trunk are different.	-
hwtrunkmemspeeddifferentresume	Enables the trap function for the event that rates of active interfaces of the Eth-Trunk are changed to be the same.	-

Parameter	Description	Value
hwporterrorrateexceed	Enables the trap function for the event that the rate of CRC, Giants, and Runts error packets received by an interface is greater than or equal to 1000 packets per second.	-
hwsubifnumexceeded-specalarm	Enables the trap function for the event that the number of sub-interfaces on the switch exceeds the maximum value.	-
hwsubifnumexceeded-specalarmresume	Enables the trap function for the event that the number of sub-interfaces on the switch is within the normal range.	-
hwinputratechangeo-verthresholdnotice	Enables the trap function for a sudden traffic volume change in the inbound direction of interfaces.	-
hwoutputratechangeo-verthresholdnotice	Enables the trap function for a sudden traffic volume change in the outbound direction of interfaces.	-
hwphysicalportinbroad-castrapidchange	Enables the trap function for the event that the rapid-change-ratio of inputbroadcast exceeded the threshold.	-
hwportprotectgroupu-navailable	Enables the trap function for the event that the port protection group function becomes unavailable.	-
hwportprotectgroupa-vailable	Enables the trap function for the event that the port protection group function becomes available.	-

Parameter	Description	Value
hwportprotectgroupdelete	Enables the trap function for the event that the port protection group is deleted.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

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

Example

# Enable all traps of the IFPDT module.

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

Related Topics

4.2.18 display snmp-agent trap feature-name ifpdt all

4.2.64 snmp-agent trap enable feature-name error-down

Function

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

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

By default, the trap function is disabled for the error-down module.

Format

snmp-agent trap enable feature-name error-down [**trap-name** { **hwerrordown** | **hwerrordownrecovery** }]

undo snmp-agent trap enable feature-name error-down [**trap-name** { **hwerrordown** | **hwerrordownrecovery** }]

Parameters

Parameter	Description	Value
trap-name	Enables or disables the trap function for a specified event of the error-down module.	-
hwerrordown	Enables the trap function for the error-down event.	-
hwerrordownrecovery	Enables the trap function for the error-down clear event.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

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

Example

# Enable the trap function for the error-down event.

```
<HUAWEI> system-view
[HUAWEI] snmp-agent trap enable feature-name error-down trap-name hwerrordown
```

Related Topics

4.2.19 display snmp-agent trap feature-name error-down all

4.2.65 speed

Function

The **speed** command sets the rate for an Ethernet interface in non-auto negotiation mode.

The **undo speed** command restores the default rate of an Ethernet interface in non-auto negotiation mode.

By default, an Ethernet interface works at its highest rate when it works in non-auto negotiation mode.

Format

speed { **10** | **100** | **1000** | **2500** | **5000** | **10000** }

undo speed

Parameters

Parameter	Description	Value
10	Indicates that the interface works at 10 Mbit/s.	-
100	Indicates that the interface works at 100 Mbit/s.	-
1000	Indicates that the interface works at 1000 Mbit/s. **NOTE** FE interfaces do not support this parameter.	-
2500	Sets the auto-negotiation rate of an Ethernet electrical interface to 2500 Mbit/s. **NOTE** Only MultiGE interfaces support this parameter.	-
5000	Sets the auto-negotiation rate of an Ethernet electrical interface to 5000 Mbit/s. **NOTE** Only MultiGE interfaces support this parameter.	-
10000	Sets the auto-negotiation rate of an Ethernet electrical interface to 10000 Mbit/s. **NOTE** Only MultiGE interfaces support this parameter.	-

Views

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

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In non-auto negotiation mode, if interfaces on two connected devices work at different rates, use the **speed** command to change the rates of the interfaces to be the same so that the two devices can communicate.

Precautions

If the remote interface does not support the auto negotiation mode, run the **undo negotiation auto** command on the local interface to configure the interface to work in non-auto negotiation mode. You can then change the rate of the local interface to be the same as the rate of the remote interface to ensure proper communication.

Example

# Configure GE0/0/1 to work at 100 Mbit/s in non-auto negotiation mode.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo negotiation auto
[HUAWEI-GigabitEthernet0/0/1] speed 100
```

Related Topics

4.2.38 negotiation auto

4.2.21 duplex

4.2.66 speed auto-negotiation

Function

The **speed auto-negotiation** command enables auto-negotiation on a GE optical interface.

The **undo speed auto-negotiation** command disables auto-negotiation on a GE optical interface.

By default, auto-negotiation is disabled on a GE optical interface.

Format

speed auto-negotiation

undo speed auto-negotiation

Parameters

None

Views

GE interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If an optical interface is configured to work in auto-negotiation mode using the **negotiation auto** command, the interface cannot negotiate the rate with another interface. You can run the **speed auto-negotiation** command to configure the auto-negotiation function on the interface.

Prerequisites

Run the **negotiation auto** command to enable auto-negotiation before using the **speed auto-negotiation** command on the interface.

Precautions

- The **speed auto-negotiation** command will make flow control auto-negotiation and internal loopback ineffective.
- After configuring the auto-negotiation function on an interface, if you remove and install a single optical fiber on the interface, the interface may be Up and the remote interface may be down. You can run the **shutdown** and **undo shutdown** commands on the remote interface to make the remote interface go Up.
- After auto-negotiation is configured on an interface, if this interface becomes Up and the remote interface becomes Down after the negotiation, run the **shutdown** and **undo shutdown** commands on the remote interface or run the **undo speed auto-negotiation** and **speed auto-negotiation** commands on this interface to enable the two ends to negotiate their rate again.
- The last four GE optical interfaces of the S5720-36PC-EI, S5720-56PC-EI, S5720-32P-EI, and S5720-52P-EI do not support this command.
- The last four GE optical interfaces of the S5720S-28P-SI, S5720S-52P-SI, S5720-28P-SI, and S5720-52P-SI do not support this command.
- For S5700LI series switches, only the first 24 GE optical interfaces of the S5700-28P-LI-24S-BAT, combo optical interfaces of the S5700-28TP-LI, S5700-28TP-PWR-LI, and S5701-28TP-PWR-LI-AC, and GE optical interfaces of the S5700-52X-LI-48CS, S5700-28X-LI-24S, and S5701-28X-LI-24S-AC support this command.
- The first two GE optical interfaces of the S2750EI and GE optical interfaces of the S5700S-LI do not support this command.

Example

# Enable auto-negotiation on GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] negotiation auto
[HUAWEI-GigabitEthernet0/0/1] speed auto-negotiation
```

Related Topics

4.2.38 negotiation auto

4.2.67 statistic enable (interface view)

Function

The **statistic enable** command enables IPv4 or IPv6 packet statistics collection on an interface.

The **undo statistic enable** command disables IPv4 or IPv6 packet statistics collection on an interface.

By default, IPv4 or IPv6 packet statistics collection is disabled on an interface.

NOTE

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

Format

{ **ipv4** | **ipv6** } * **statistic enable** { **both** | **inbound** | **outbound** }

undo { **ipv4** | **ipv6** } * **statistic enable** { **both** | **inbound** | **outbound** }

Parameters

Parameter	Description	Value
ipv4	Indicates IPv4 packet statistics collection.	-
ipv6	Indicates IPv6 packet statistics collection.	-
both	Indicates statistics collection for incoming and outgoing packets.	-
inbound	Indicates statistics collection for incoming packets.	-
outbound	Indicates statistics collection for outgoing packets.	-

Views

VLANIF interface view, Eth-Trunk interface view, GE interface view, XGE interface view, 40GE interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To check the network status or locate network faults, you can enable IPv4 or IPv6 packet statistics collection on an interface to collect IPv4 or IPv6 packet statistics on the interface.

Precautions

- This command and the **statistic enable** { **both** | **inbound** | **outbound** } command used in the VLANIF interface view are mutually exclusive.
- If this command and the **traffic-policy (interface view)** command are configured together on the S5720HI, traffic policy will fail to be applied.

Example

# Enable IPv4 packet statistics collection in the inbound direction of GigabitEthernet0/0/1.

```
<HUAWEI> system-view
[HUAWEI] interface GigabitEthernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] ipv4 statistic enable inbound
```

Related Topics

4.2.9 display counters protocol

4.2.68 traffic-pppoe

Function

The **traffic-pppoe** command configures an interface to allow only PPPoE packets to pass through.

The **undo traffic-pppoe** command cancels the configuration.

By default, an interface allows all types of packets to pass through.

NOTE

S5720HI does not support the configuration.

Format

traffic-pppoe { **any** | *source-address* } { **any** | *destination-address* }

undo traffic-pppoe { **any** | *source-address* } { **any** | *destination-address* }

Parameters

Parameter	Description	Value
{ **any** | *source-address* }	Indicates that an interface allows PPPoE packets with a specified source MAC address to pass through. ● **any** indicates that PPPoE packets with any source MAC address can pass through the interface. ● *source-address* indicates that PPPoE packets with a specified source MAC address can pass through the interface.	The value of *source-address* is in the format H-H-H. An H contains 1 to 4 hexadecimal digits.
{ **any** | *destination-address* }	Indicates that an interface allows PPPoE packets with a specified destination MAC address to pass through. ● **any** indicates that PPPoE packets with any destination MAC address can pass through the interface. ● *destination-address* indicates that PPPoE packets with a specified destination MAC address can pass through the interface.	The value of *destination-address* is in the format H-H-H. An H contains 1 to 4 hexadecimal digits.

Views

Ethernet interface view, GE interface view, XGE interface view, MultiGE interface view, 40GE interface view, port group view, Eth-Trunk interface view

Default Level

2: Configuration level

Usage Guidelines

If you run the **traffic-pppoe any any** command on an interface, the interface allows only PPPoE packets to pass through and discards other packets.

Example

# Configure GE0/0/1 to allow only PPPoE packets to pass through.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] traffic-pppoe any any
```

# Configure GE0/0/1 to allow only PPPoE packets with source MAC address 1-1-1 to pass through.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] traffic-pppoe 1-1-1 any
```

4.2.69 training (40GE interface view)

Function

The **training disable** and **undo training enable** commands disable the training function on a 40GE interface.

The **training enable** and **undo training disable** commands enable the training function on a 40GE interface.

By default, the training function is enabled on a 40GE interface.

NOTE

Only the S6720EI and S6720S-EI support this command.

Format

training { enable | disable }

undo training { enable | disable }

Parameters

None

Views

40GE interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

With the increase of transmission rate or frequency, attenuation of signal's high-frequency components becomes increasingly severe. To guarantee transmission performance of signals, it is necessary to compensate for signals, and commonly used compensation technologies are pre-emphasis and balancing. The pre-emphasis technology increases high-frequency components of signals at the transmit end of transmission lines to compensate attenuation during the transmission. However, the pre-emphasis technology increases crosstalk while amplifying high-frequency components. To solve this problem, the balancing technology is developed. The balancing technology is used at the receive end of transmission lines to function like a filter for filtering high-frequency crosstalk.

After the training function is enabled on a 40GE interface, the transmit end exchanges frames with the receive end to automatically set the pre-emphasis and balancing parameters, improving processing efficiency of the two technologies. Note that the negotiated parameters for the training function are obtained based on the site environment. If the site environment changes, for example, from high-temperature environment to low-temperature environment, the parameters may be inaccurate. Therefore, bit errors may occur when the training function is enabled. The training function is optional in IEEE802.3 standards, and its implementation on different types of products from various vendors may differ.

When connecting two devices, enable or disable the training function on both ends simultaneously. By default, the training function is enabled on a 40GE interface. If the training function is disabled on the remote device or the remote device does not support the function, run the **training disable** or **undo training enable** command to disable the function.

Precautions

- The **training disable** and **undo training enable** commands can be configured on a 40GE interface only when the interface connects to a high-speed cable and is not a physical member interface in a stack.
- After a cable is installed on a 40GE interface without the **training disable** configuration, the **training enable** configuration is automatically generated on the interface.
- If no cable is installed on an interface, only the **training enable** and **undo training disable** commands can be configured on the interface.
- If the **display this include-default** command is run on an interface to view the training configuration after a cable is installed on the interface, the default **training enable** configuration is always displayed in the command output and does not change with the training configuration change.
- The training configuration on an interface takes effect only after a cable is installed on the interface. If the cable is replaced with an optical module, the **training disable** and **training enable** configurations will be automatically deleted from the interface.
- If a 40GE interface is configured as a physical member interface in a stack system, the **training disable** and **training enable** configurations will be automatically deleted from the interface.
- If a 40GE interface has been configured as a physical member interface in a stack system, the training function is disabled on the interface by default and cannot be enabled.
- If the **training disable** or **undo training enable** command is configured on a 40GE interface of the S6720S-26Q-EI-24S-AC or S6720S-26Q-EI-24S-DC after a cable is installed on the interface, and the interface is connected to a remote interface on which the training function is disabled or a remote interface that does not support the training function, the two interfaces may not go Up or go Up after a delay. Therefore, configure the **training disable** or

undo training enable command only when the training function is disabled on the remote interface or the remote interface does not support the training function. In other scenarios, it is recommended that you do not disable the training function.

- If the training configuration does not exist on an interface of a switch running V200R008C00 or an earlier version, the **training disable** configuration is automatically generated on the interface after the system software is upgraded to a version later than V200R009C00. If the training configuration exists on the interface, the configuration remains unchanged after the system software is upgraded to a version later than V200R009C00.

Example

# Disable the training function on 40GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] interface 40ge 0/0/1
[HUAWEI-40GE0/0/1] training disable
Warning: The configuration will cause an abnormality in port running. Continue? [Y/N]:y
```

4.2.70 transceiver power low trigger error-down

Function

The **transceiver power low trigger error-down** command enables an Ethernet optical interface to enter the error-down state when the optical power is low.

The **undo transceiver power low trigger error-down** command disabled an Ethernet optical interface from entering the error-down state when the optical power is low.

By default, an Ethernet optical interface does not enter the error-down state when the optical power is low.

Format

transceiver power low trigger error-down

undo transceiver power low trigger error-down

Parameters

None

Views

Ethernet interface view, GE interface view, XGE interface view, 40GE interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Low optical power of the device may cause intermittent service interruption. To ensure that services are running properly, enable an interface to enter the error-down state when the optical power is low so that services can be switched in a timely manner.

Follow-up Procedure

An interface in Error-down state can be recovered using either of the following methods:

- Manual recovery: If a few interfaces need to be recovered forcibly, run the **shutdown** and **undo shutdown** commands in the interface view. Alternatively, run the **restart** command in the interface view to restart the interfaces.
- Automatic recovery: If a large number of interfaces need to be recovered, manual recovery is time consuming and some interfaces may be omitted. You can run the **error-down auto-recovery** **cause transceiver-power-low interval** *interval-value* command in the system view to enable automatic interface recovery and set the recovery delay time. An interface in Error-down state automatically recovers when the specified delay time expires.

Example

# Enable GE0/0/1 to enter the error-down state when the optical power is low.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] transceiver power low trigger error-down
```

Related Topics

4.2.22 error-down auto-recovery

4.2.71 trap-threshold

Function

The **trap-threshold** command sets the inbound and outbound bandwidth usage thresholds for generating a trap.

The **undo trap-threshold** command restores the default inbound and outbound bandwidth usage thresholds for generating a trap.

The default inbound or outbound bandwidth usage threshold for generating a trap is 80.

Format

trap-threshold { **input-rate** | **output-rate** } *bandwidth-in-use* [**resume-rate** *resume-threshold*]

undo trap-threshold { **input-rate** | **output-rate** }

Parameters

Parameter	Description	Value
input-rate	Indicates inbound bandwidth.	-
output-rate	Indicates outbound bandwidth.	-
bandwidth-in-use	Specifies the bandwidth usage threshold for generating a trap.	The value is an integer that ranges from 1 to 100.
resume-rate *resume-threshold*	Specifies the bandwidth usage threshold for clearing a trap.	The value is an integer that ranges from 1 to *bandwidth-in-use*. The default value is *bandwidth-in-use*.

Views

Ethernet interface view, GE interface view, XGE interface view, MultiGE interface view, 40GE interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Monitoring bandwidth usage helps you know current load on a device. If the bandwidth usage exceeds a threshold, bandwidth resources are insufficient and the device capacity needs to be expanded. For example, if the bandwidth usage exceeds 95%, an alarm is generated, indicating that bandwidth resources are almost exhausted. As a result, some services may be interrupted before device capacity expansion.

You can configure two thresholds: low threshold (log threshold) and high threshold (alarm threshold). The system generates a log when the bandwidth usage exceeds the low threshold and generates an alarm when the bandwidth usage exceeds the high threshold. This configuration ensures that you can expand the device capacity in advance to avoid service interruptions caused by bandwidth exhaustion.

NOTE

Outbound bandwidth usage = (Outbound interface rate/Outbound physical interface bandwidth) x 100

Inbound bandwidth usage = (Inbound interface rate/Inbound physical interface bandwidth) x 100

The interface rate and bandwidth are expressed in bits per second.

To set a lower threshold, run the **log-threshold** command.

The **trap-threshold** command sets the bandwidth usage threshold for generating a trap. The **trap-threshold** with the following parameters provides various functions:

- **trap-threshold input-rate** *bandwidth-in-use* **resume-rate** *resume-threshold*: sets the inbound bandwidth usage threshold for generating a trap.
  - If inbound bandwidth usage exceeds the threshold specified in *bandwidth-in-use*, an hwIfMonitorInputRateRising trap is generated, indicating that inbound bandwidth usage exceeds the configured threshold.
  - If inbound bandwidth usage falls below the threshold specified in *resume-threshold*, an hwIfMonitorInputRateResume trap is generated, indicating that inbound bandwidth usage falls between the configured threshold for clearing a trap.
- **trap-threshold output-rate** *bandwidth-in-use* **resume-rate** *resume-threshold*: sets the outbound bandwidth usage threshold for generating a trap.
  - If outbound bandwidth usage exceeds the threshold specified in *bandwidth-in-use*, an hwIfMonitorOutputRateRising trap is generated, indicating that outbound bandwidth usage exceeds the configured threshold.
  - If outbound bandwidth usage falls below the threshold specified in *resume-threshold*, an hwIfMonitorOutputRateResume trap is generated, indicating that outbound bandwidth usage falls between the configured threshold for clearing a trap.

If the offset between the value of *bandwidth-in-use* and the value of *resume-threshold* is too small, trap information may be frequently displayed.

The log threshold must be lower than the trap threshold, providing efficient protection for services. For example, when the inbound bandwidth usage reaches 80%, a log is generated. If the inbound bandwidth usage continues to increase and reaches 95%, a trap is generated. This ensures that a log is generated for inbound bandwidth usage of 80%, and a trap is generated for inbound bandwidth usage of 95%. Either the log or the trap prompts for a bandwidth increase, preventing service interruption.

Example

# Configure GE0/0/1 to generate a trap when the outbound bandwidth usage exceeds 60%.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] trap-threshold output-rate 60
```

# Configure GE0/0/1 to generate a trap when the outbound bandwidth usage exceeds 80% and clear the trap when the outbound bandwidth usage falls below 60%.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] trap-threshold output-rate 80 resume-rate 60
```

Related Topics

4.2.32 log-threshold input-rate output-rate

4.2.72 trap-threshold error-statistics

Function

The **trap-threshold error-statistics** command sets the alarm threshold for error packets and alarm interval.

The **undo trap-threshold error-statistics** command restores the default alarm threshold for error packets and default alarm interval.

By default, the alarm threshold for error packets is 3 and the alarm interval is 10 seconds.

Format

trap-threshold error-statistics *threshold-value* **interval** *interval-value*

undo trap-threshold error-statistics

Parameters

Parameter	Description	Value
threshold-value	Sets the alarm threshold for error packets.	The value is an integer that ranges from 1 to 65535. **NOTE** The value should not be greater than the alarm threshold for error packets that cause the interface status to change to Error-Down configured by the **error-down-threshold error-statistics** command.
interval *interval-value*	Sets the interval for reporting alarms for error packets.	The value is an integer that ranges from 10 to 65535, in seconds.

Views

Ethernet interface view, GE interface view, XGE interface view, MultiGE interface view, 40GE interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

The system generates an alarm when the number of error packets received by an interface within an alarm interval exceeds the alarm threshold. If the number of received error packets is 0 in the next alarm interval, the system displays an alarm clearance message.

Example

# Set the alarm threshold for error packets on GE0/0/1 to 10 and the alarm interval to 30 seconds.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] trap-threshold error-statistics 10 interval 30
```

4.2.73 virtual-cable-test

Function

The **virtual-cable-test** command tests the cable connected to an Ethernet electrical interface and displays the test result.

Format

virtual-cable-test

Parameters

None

Views

Ethernet interface view, GE interface view, XGE interface view, MultiGE interface view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

If the cable is faulty, the interface is in Down state or the interface rate is abnormal even if it is in Up state. You can run the **virtual-cable-test** command to check whether the cable works properly. According to the command output, you can locate and rectify cable faults.

- If the cable works properly, the total length of the cable is displayed.
- If the cable cannot work properly, the distance between the interface and the fault point is displayed.

Precautions

- The test result is only for reference and may be inaccurate for cables of some vendors.

- The test result is related to the cable signal attenuation. When the cable length is shorter than 3 m, the cable signal attenuation mostly results from the connector, not the cable. The test result is therefore invalid.
- Running the **virtual-cable-test** command may affect services on the interface in a short period of time, and the interface in Up state may alternate between Up and Down.
- Combo electrical interfaces support cable tests, but cable tests are not recommended on combo electrical interfaces because services will be interrupted.
- Before performing a cable test, remove the network cable from the remote interface. Otherwise, signals from the remote interface may make the test result inaccurate.
- This command can be used on an XGE optical interface or GE optical interface when the interface has a GE copper module installed.
- On the S1720GFR, S1720GW, S1720GWR, S1720GW-E, S1720GWR-E, S2720EI, S2750, S5700S-LI, S5700LI, S5720LI, S5720S-LI, S5710-X-LI, S5720SI, or S5720S-SI, when a GE electrical interface or copper transceiver works at a rate of 1000 Mbit/s or 100 Mbit/s, the test result is only for reference and may be inaccurate if the interface is in Up state.
- On the S5720EI, S5720HI, S6720S-EI, or S6720EI, when a GE electrical interface or copper transceiver works at a rate of 100 Mbit/s, the test result is only for reference and may be inaccurate.
- On the S2750, when an FE electrical interface or copper transceiver is in Up state, the test result is only for reference and may be inaccurate.
- The virtual cable test (VCT) cannot be performed on multiple interfaces of the device at the same time.

Example

# Test the cable connected to GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] virtual-cable-test
Warning: The command will stop service for a while. Continue? [Y/N]y
Info: This operation may take a few seconds. Please wait for a moment..........done.
Pair A length: 189meter(s)
Pair B length: 189meter(s)
Pair C length: 189meter(s)
Pair D length: 189meter(s)
Pair A state: Ok
Pair B state: Ok
Pair C state: Ok
Pair D state: Ok
Info: The test result is only for reference.
```

Table 4-25 Description of the virtual-cable-test command output

Item	Description
Pair A/B/C/D	Four pairs of circuits in a network cable.

Item	Description
Pair A length	Length of a network cable: ● The length is the distance between the interface and the fault point if a fault occurs. ● The length is the actual length of the cable when the cable works properly. ● The default length is 0 m if the interface is not connected to any network cable. **NOTE** If the cable length is displayed as Unknown, the cable status is OK, but the cable length test result cannot be used. If the cable status is Open (indicating open circuit), the cable length in the VCT result can be used. If the remote interface is shut down, the cable length in the VCT result can be used for combo electrical interfaces on the following switches: ● S1720-28GWR-PWR-4TP and S1720-28GWR-PWR-4TP-E ● S2720EI ● S5720SI, S5720S-SI, S5710LI ● S5700-52X-LI-48CS-AC, S5720-12TP-LI-AC, S5720-12TP-PWR-LI-AC, S5720-28TP-PWR-LI-AC, S5720S-28TP-PWR-LI-AC, S5720-28TP-PWR-LI-AC, and S5720-28TP-LI-AC If the remote interface is shut down, the cable length in the VCT result can be used for electrical interfaces on the following switches: ● S2720EI ● S5720EI ● S5720HI ● S5720-16X-PWH-LI-AC and S5720-28X-PWH-LI-AC ● S5730SI ● S5730S-EI ● S6720SI

Item	Description
Pair A state	Network cable status: - Ok: indicates that the circuit pair is terminated normally. - Open: indicates that the circuit pair is not terminated. - Short: indicates that the circuit pair is short-circuited. - Crosstalk: indicates that the circuit pairs interfere with each other. - Unknown: indicates that the circuit pair has an unknown fault.

Related Topics

4.2.20 display virtual-cable-test

4.3 Logical Interface Configuration Commands

4.3.1 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.

4.3.2 display interface loopback

Function

Using the **display interface loopback** command, you can view the status of a loopback interface.

Format

display interface loopback [*loopback-number* | **main**]

Parameters

Parameter	Description	Value
loopback-number	Specifies the number of a loopback interface. If *loopback-number* is not specified, the status of all loopback interfaces is displayed.	-
main	Displays status and traffic statistics about a Loopback interface. A Loopback interface has no sub-interfaces. Status and traffic statistics about a Loopback interface are displayed whether you specify the **main** parameter or not.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

In the scenario where you need to monitor the status of an interface or locate an interface fault, you can use the **display interface loopback** command to collect the statistics on the interface including the status. Through the displayed information, you can collect the traffic statistics and troubleshoot the interface.

Prerequisite

A loopback interface has been created using the **interface loopback** command.

Example

# Display the status of a specified loopback interface.

```
<HUAWEI> display interface loopback 6

LoopBack6 current state : UP
Line protocol current state : UP (spoofing)
Description:
Route Port,The Maximum Transmit Unit is 1500
Internet Address is 10.3.3.3/32
Current system time: 2012-02-25 09:56:04
    Input bandwidth utilization  :    0%
    Output bandwidth utilization :    0%
```

Table 4-26 Description of the **display interface loopback** command output

Item	Description
LoopBack6 current state	Physical status of a loopback interface. The physical status of a loopback interface is always Up after the loopback interface is created.
Line protocol current state	Link layer protocol status of a loopback interface. The link layer protocol status of a loopback interface is always Up after the loopback interface is created.
Description	Indicates the description of the interface, which can be set by using the **description** command.
Route Port,The Maximum Transmit Unit is 1500	Indicates the maximum transmission unit (MTU). Loopback interfaces do not support the MTU configuration. This field is fixed at 1500.
Internet Address is	Indicates the IP address of the interface.
Current system time	Indicates the current system time.
Input bandwidth utilization	Indicates the percentage of the rate for receiving packets to the total bandwidth.
Output bandwidth utilization	Indicates the percentage of the rate for sending packets to the total bandwidth.

Related Topics

4.3.5 interface loopback

4.3.3 display interface null

Function

Using the **display interface null** command, you can view the status of a null interface.

Format

display interface null [**0** | **main**]

Parameters

Parameter	Description	Value
0	Specifies the number of the null interface.	The value can be 0 only.

Parameter	Description	Value
main	Displays status and traffic statistics about a Null interface. A Null interface has no sub-interfaces. Status and traffic statistics about a Null interface are displayed whether you specify the **main** parameter or not.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

The **display interface null** command displays the status of a null interface. The interface status information includes: the physical status, link layer protocol status, description, MTU, IP address, current system time, last time statistics about the null interface are cleared, incoming and outgoing packet rates in bit/s and pps, total numbers of packets and bytes received and sent by the null interface, and percentages of the rates for receiving and sending packets to the total bandwidth.

Precautions

There is only one null interface, namely, NULL 0.

Example

# Display the status of Null 0 interface.

```
<HUAWEI> display interface null 0

NULL0 current state : UP
Line protocol current state : UP (spoofing)
Description:
Route Port,The Maximum Transmit Unit is 1500
Internet protocol processing : disabled
Physical is NULL DEV
Current system time: 2012-02-25 10:25:59
    Last 300 seconds input rate 0 bits/sec, 0 packets/sec
    Last 300 seconds output rate 0 bits/sec, 0 packets/sec
    Realtime 0 seconds input rate 0 bits/sec, 0 packets/sec
    Realtime 0 seconds output rate 0 bits/sec, 0 packets/sec
    Input: 0 packets,0 bytes
           0 unicast,0 broadcast,0 multicast
           0 errors,0 unknownprotocol
    Output:0 packets,0 bytes
           0 unicast,0 broadcast,0 multicast
           0 errors
    Input bandwidth utilization  :    0%
    Output bandwidth utilization :    0%
```

Table 4-27 Description of the display interface null command output

Item	Description
NULL0 current state	Indicates the physical status of the null interface. The physical status of the null interface is always Up.
Line protocol current state	Indicates the link layer protocol status of the interface. The protocol status of the null interface is always Up.
Description	Indicates the description of the interface, which can be set by using the **description** command.
Route Port	A Layer 3 interface.
The Maximum Transmit Unit	Indicates the MTU of the interface.
Internet protocol processing : disabled	Indicates that the Internet protocol processing is not configured.
Physical is NULL DEV	Indicates that the interface is null.
Current system time	Indicates the current system time.
Last 300 seconds input rate Last 300 seconds output rate	Indicates the rates for sending and receiving the bytes and the packets by the interface in the last five minutes.
Realtime 0 seconds input rate Realtime 0 seconds output rate	Indicates the real-time rates of sending and receiving the bytes and the packets. It refers to the interval between two **display** commands that are run on the same interface. The maximum value is the statistical interval displayed in the previous piece of information. This entry is displayed only when information about a logical interface is viewed.
Input	Indicates the total number of packets and the total number of bytes received by the interface.
Output	Indicates the total number of packets and the total number of bytes sent by the interface.
Input bandwidth utilization	Indicates the percentage of the rate for receiving packets to the total bandwidth.
Output bandwidth utilization	Indicates the percentage of the rate for sending packets to the total bandwidth.

Related Topics

4.3.6 interface null

4.3.4 display interface virtual-ethernet

Function

The **display interface virtual-ethernet** command displays status and traffic statistics about Virtual Ethernet (VE) interfaces.

NOTE

Only the S5720HI supports this command.

Format

display interface virtual-ethernet [*ve-number* | **main**]

Parameters

Parameter	Description	Value
ve-number	Displays status and statistics about a specified VE interface. If no interface number is specified, information about all VE interfaces is displayed.	The sequence number ranges from 0 to 511.
main	Displays status and traffic statistics about a VE interface. If you do not specify the **main** parameter, status and traffic statistics about both a VE interface and VE sub-interfaces are displayed.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

In the scenario where you need to monitor the status of an interface or locate an interface fault, you can use the **display interface virtual-ethernet** command to collect the statistics on the interface including the status. Through the displayed information, you can collect the traffic statistics and troubleshoot the interface.

Example

# Display the status of VE 0/0/1.

```
<HUAWEI> display interface virtual-ethernet 0/0/1
Virtual-Ethernet0/0/1 current state : UP
Line protocol current state : UP
```

```
Description:
Route Port,The Maximum Transmit Unit is 1500
Internet protocol processing : disabled
IP Sending Frames' Format is PKTFMT_ETHNT_2, Hardware address is 0000-1382-4569
Current system time: 2017-01-02 02:20:03
Last 300 seconds input rate 0 bits/sec, 0 packets/sec
Last 300 seconds output rate 0 bits/sec, 0 packets/sec
Input:  0 packets, 0 bytes
  Unicast:                     0,  Multicast:                    0
  Broadcast:                   0
Output:  0 packets, 0 bytes
  Unicast:                     0,  Multicast:                    0
  Broadcast:                   0
    Input bandwidth utilization  :    0%
    Output bandwidth utilization :    0%
```

Table 4-28 Description of the **display interface virtual-Ethernet** command output

Item	Description
Virtual-Ethernet0/0/1 current state	Physical status of the VE interface: ● UP: indicates that the interface is Up. ● DOWN: indicates that the interface is Down. ● Administratively DOWN: indicates that the administrator uses the **shutdown** command on the interface.
Line protocol current state	Indicates the link layer protocol status of the interface: ● UP: indicates that the link layer protocol on the interface is Up. ● DOWN: indicates that the link layer protocol on the interface is Down or no IP address is assigned to the interface.
Description	Description of an interface. The information allows users to know about functions of the interface and is used to identify the current interface. You can run the **description** command to configure or modify the description of an interface.
Route Port	Layer 3 interface. If this parameter specifies a Layer 2 interface, the value of this parameter will be displayed as "Switch Port". You can run the **portswitch** command to change the mode of an interface from Layer 3 to Layer 2.
The Maximum Transmit Unit is	MTU of the interface.
Internet protocol processing : disabled	No IP address is configured for the interface. If an IP address is configured for the interface, the interface's IP address and subnet mask are displayed.
IP Sending Frames' Format is	Format of frames sent by the IP protocol, including PKTFMT_ETHNT_2, Ethernet_802.3, and Ethernet_SNAP.

Item	Description
Hardware address is	MAC address of the interface.
Current system time	Current system time. If the system is configured with a time zone and is in the summer daylight saving time, the time is displayed in the format of YYYY/MM/DD HH:MM:SS UTC±HH:MM DST.
Last 300 seconds input rate	Incoming packet rate (bits per second and packets per second) within the last 300 seconds.
Last 300 seconds output rate	Outgoing packet rate (bits per second and packets per second) within the last 300 seconds.
Input	Total number of received packets.
Output	Total number of sent packets.
Unicast	Number of unicast packets that are received or sent by the interface.
Broadcast	Number of broadcast packets that are received or sent by the interface.
Input bandwidth utilization	Inbound bandwidth usage.
Output bandwidth utilization	Outbound bandwidth usage.

Related Topics

4.3.7 interface virtual-ethernet

4.3.5 interface loopback

Function

The **interface loopback** command creates a loopback interface.

The **undo interface loopback** command deletes a loopback interface.

Format

interface loopback *loopback-number*

undo interface loopback *loopback-number*

Parameters

Parameter	Description	Value
loopback-number	Specifies the number of a loopback interface.	The value is an integer. On the S1720X, S1720X-E, S6720LI, S6720S-LI, S5730SI, S5730S-EI, S6720SI and S6720S-SI series switches, the value ranges from 0 to 1023. On the S1720GFR, S1720GW, S1720GWR, S1720GW-E, S1720GWR-E, S2720EI, S2750, S5700LI, S5700S-LI , S5720LI, and S5720S-LI series switches, the value ranges from 0 to 15.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

A loopback interface is always Up.

The IP address of a loopback interface is usually specified as the source address of packets.

Example

# Create loopback interface 5.

```
<HUAWEI> system-view
[HUAWEI] interface loopback 5
[HUAWEI-LoopBack5]
```

Related Topics

4.3.2 display interface loopback

4.3.6 interface null

Function

Using the **interface null** command, you can enter the null interface view.

Format

interface null 0

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The Null0 interface never forwards or accepts any traffic. All traffic sent to this interface is directly discarded. Unnecessary traffic can be sent to the Null0 interface to avoid using ACLs.

Precautions

There is only one null interface, named null0. This interface is always Up and cannot be shut down or deleted.

Example

# Enter the view of the Null0 interface.

```
<HUAWEI> system-view
[HUAWEI] interface null 0
[HUAWEI-NULL0]
```

Related Topics

4.3.3 display interface null

4.3.7 interface virtual-ethernet

Function

The **interface virtual-ethernet** command displays the view of an existing virtual Ethernet (VE) interface, or creates a VE interface and displays the VE interface view.

The **undo interface virtual-ethernet** command deletes a VE interface.

By default, no VE interface is created.

NOTE

Only the S5720HI supports this command.

Format

interface virtual-ethernet *ve-number* [.*subnumber*]

undo interface virtual-ethernet *ve-number* [.*subnumber*]

Parameters

Parameter	Description	Value
ve-number	Specifies the number of a VE interface. The value is in the format of 0/0/sequence number.	The sequence number is an integer that ranges from 0 to 511.
subnumber	Specifies the number of a VE sub-interface.	The value is an integer that ranges from 1 to 1024.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

A VE interface is a logical interface with Ethernet features on a switch. VE interfaces are mainly used in scenarios where Ethernet over GRE is configured or an L2VPN accesses to an L3VPN. You need to create a VE sub-interface when configuring an L2VPN to access to an L3VPN.

Example

# Create VE interface 0//0/1.

```
<HUAWEI> system-view
[HUAWEI] interface virtual-ethernet 0/0/1
[HUAWEI-Virtual-Ethernet0/0/1]
```

# Create VE sub-interface VE0/0/1.1.

```
<HUAWEI> system-view
[HUAWEI] interface virtual-ethernet 0/0/1
[HUAWEI-Virtual-Ethernet0/0/1] ve-group 1 l3-access
[HUAWEI-Virtual-Ethernet0/0/1] quit
[HUAWEI] interface virtual-ethernet 0/0/1.1
[HUAWEI-Virtual-Ethernet0/0/1.1]
```

Related Topics

4.3.4 display interface virtual-ethernet

4.3.8 portswitch (VE interface view)

Function

The **portswitch** command changes the working mode of a virtual Ethernet (VE) interface from Layer 3 mode to Layer 2 mode.

The **undo portswitch** command changes the working mode of a VE interface from Layer 2 mode to Layer 3 mode.

By default, a VE interface works in Layer 3 mode.

NOTE

Only the S5720HI supports this command.

Format

portswitch

undo portswitch

Parameters

None

Views

VE interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

By default, a VE interface on the device works in Layer 3 mode. To enable Layer 2 forwarding on the VE interface, run the **portswitch** command to change the working mode to Layer 2 mode.

Precautions

- If an interface has the non-attribute configuration, this command cannot be executed. Before running this command, delete the non-attribute configuration on the interface.
- The minimum interval between running the **portswitch** and **undo portswitch** commands must be 30s.

Example

# Change VE0/0/1 to Layer 2 mode.

```
<HUAWEI> system-view
[HUAWEI] interface virtual-ethernet 0/0/1
[HUAWEI-Virtual-Ethernet0/0/1] portswitch
```

4.3.9 trigger trap

Function

Using the **trigger trap** command, you can configure an interface to send traps to the NMS.

Format

trigger trap { **linkup** | **linkdown** }

Parameters

Parameter	Description	Value
linkup	Sends the LinkUp trap to the NMS.	-
linkdown	Sends the LinkDown trap to the NMS.	-

Views

Loopback interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The traps configured by **trigger trap** are used to check whether the network between the NMS and device functions properly. If the NMS receives a trap sent from the interface, the network between the NMS and device functions properly; otherwise, a fault may occur on the network.

Prerequisites

Run the **snmp-agent trap enable feature-name** command to enable the LinkUp and LinkDown traps.

Precautions

The **trigger trap** command is used on loopback interfaces to check the network between the NMS and device. The interface status does not change according to the meaning of the trap. For example, if the **trigger trap linkdown** command is used, the loopback interface sends a LinkDown trap to the NMS but does not change its status to Down. If you have used the **trigger trap linkdown** command, you must run the **trigger trap linkup** command to clear the LinkDown trap on the NMS.

Example

# Configure a loopback interface to send the LinkUp trap to the NMS.

```
<HUAWEI> system-view
[HUAWEI] interface loopback 1
[HUAWEI-LoopBack1] trigger trap linkup
```