



Hewlett Packard
Enterprise

HPE FlexNetwork MSR Router Series

Comware 7 Layer 2 - LAN Switching

Command Reference

Part number: 5200-2989
Software version: MSR-CMW710-R0413
Document version: 6W102-20170101

© Copyright 2017 Hewlett Packard Enterprise Development LP

The information contained herein is subject to change without notice. The only warranties for Hewlett Packard Enterprise products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Hewlett Packard Enterprise shall not be liable for technical or editorial errors or omissions contained herein.

Confidential computer software. Valid license from Hewlett Packard Enterprise required for possession, use, or copying. Consistent with FAR 12.211 and 12.212, Commercial Computer Software, Computer Software Documentation, and Technical Data for Commercial Items are licensed to the U.S. Government under vendor's standard commercial license.

Links to third-party websites take you outside the Hewlett Packard Enterprise website. Hewlett Packard Enterprise has no control over and is not responsible for information outside the Hewlett Packard Enterprise website.

Acknowledgments

Intel®, Itanium®, Pentium®, Intel Inside®, and the Intel Inside logo are trademarks of Intel Corporation in the United States and other countries.

Microsoft® and Windows® are trademarks of the Microsoft group of companies.

Adobe® and Acrobat® are trademarks of Adobe Systems Incorporated.

Java and Oracle are registered trademarks of Oracle and/or its affiliates.

UNIX® is a registered trademark of The Open Group.

Contents

MAC address table commands	1
display mac-address	1
display mac-address aging-time	2
display mac-address mac-learning	3
display mac-address mac-move	4
mac-address (interface view)	5
mac-address (system view)	6
mac-address mac-learning enable	8
mac-address notification mac-move	9
mac-address notification mac-move suppression (interface view)	10
mac-address notification mac-move suppression (system view)	11
mac-address timer	11
snmp-agent trap enable mac-address	12
Ethernet link aggregation commands	14
bandwidth	14
default	15
description	15
display interface	16
display lacp system-id	20
display link-aggregation load-sharing mode	21
display link-aggregation member-port	23
display link-aggregation summary	25
display link-aggregation verbose	26
interface bridge-aggregation	28
interface route-aggregation	29
lacp edge-port	30
lacp mode	31
lacp period short	31
lacp system-priority	32
link-aggregation global load-sharing mode	32
link-aggregation ignore vlan	34
link-aggregation lacp traffic-redirect-notification enable	34
link-aggregation load-sharing mode	35
link-aggregation load-sharing mode local-first	36
link-aggregation mode	37
link-aggregation port-priority	37
link-aggregation selected-port maximum	38
link-aggregation selected-port minimum	39
mtu	40
port link-aggregation group	40
reset counters interface	41
reset lacp statistics	42
service	42
service standby	44
shutdown	45
Port isolation commands	47
display port-isolate group	47
port-isolate enable	47
VLAN commands	49
Basic VLAN commands	49
bandwidth	49
default	49
description	50
display interface vlan-interface	51

display vlan	54
display vlan brief	55
interface vlan-interface	56
mtu	57
name	58
reset counters interface vlan-interface	58
service	59
service standby	60
shutdown	62
vlan	63
Port-based VLAN commands	64
display port	64
port	65
port access vlan	65
port hybrid pvid	66
port hybrid vlan	67
port link-type	68
port trunk permit vlan	68
port trunk pvid	69
VLAN group commands	70
display vlan-group	70
vlan-group	71
vlan-list	72
Super VLAN commands	73
display supervlan	73
subvlan	75
supervlan	76
Voice VLAN commands	77
display voice-vlan mac-address	77
display voice-vlan state	78
voice-vlan aging	79
voice-vlan enable	79
voice-vlan mac-address	80
voice-vlan mode auto	81
voice-vlan security enable	82
voice-vlan track lldp	82
QinQ commands	84
display qinq	84
qinq enable	85
qinq ethernet-type	85
Loop detection commands	87
display loopback-detection	87
loopback-detection action	88
loopback-detection enable	89
loopback-detection global action	90
loopback-detection global enable	90
loopback-detection interval-time	91
Spanning tree commands	93
active region-configuration	93
check region-configuration	94
display stp	95
display stp abnormal-port	102
display stp bpdu-statistics	103
display stp down-port	105
display stp history	106
display stp region-configuration	110
display stp root	111

display stp tc	111
instance	114
region-name	115
reset stp	116
revision-level	116
snmp-agent trap enable stp	117
stp bpdu-protection	118
stp bridge-diameter	118
stp compliance	119
stp config-digest-snooping	120
stp cost	121
stp edged-port	122
stp enable	123
stp global config-digest-snooping	124
stp global enable	125
stp global mcheck	125
stp ignore-pvid-inconsistency	126
stp loop-protection	127
stp max-hops	127
stp mcheck	128
stp mode	129
stp no-agreement-check	130
stp pathcost-standard	130
stp point-to-point	131
stp port priority	132
stp port-log	133
stp priority	134
stp pvst-bpdu-protection	135
stp region-configuration	135
stp role-restriction	136
stp root primary	137
stp root secondary	138
stp root-protection	138
stp tc-protection	139
stp tc-protection threshold	140
stp tc-restriction	140
stp tc-snooping	141
stp timer forward-delay	142
stp timer hello	143
stp timer max-age	143
stp timer-factor	144
stp transmit-limit	145
stp vlan enable	146
vlan-mapping modulo	147
LLDP commands	148
display lldp local-information	148
display lldp neighbor-information	152
display lldp statistics	158
display lldp status	160
display lldp tlv-config	162
lldp admin-status	165
lldp check-change-interval	166
lldp enable	168
lldp encapsulation snap	168
lldp fast-count	169
lldp global enable	170
lldp hold-multiplier	170
lldp ignore-pvid-inconsistency	171
lldp management-address	172
lldp management-address-format string	173
lldp max-credit	174

lldp mode	174
lldp notification med-topology-change enable	175
lldp notification remote-change enable	176
lldp source-mac vlan	177
lldp timer fast-interval	177
lldp timer notification-interval	178
lldp timer reinit-delay	178
lldp timer tx-interval	179
lldp tlv-enable	179
Layer 2 forwarding commands	186
Normal Layer 2 forwarding commands	186
display mac-forwarding statistics	186
reset mac-forwarding statistics	188
Fast Layer 2 forwarding commands	188
display mac-forwarding cache ip	188
display mac-forwarding cache ip fragment	190
display mac-forwarding cache ipv6	191
Document conventions and icons	193
Conventions	193
Network topology icons	194
Support and other resources	195
Accessing Hewlett Packard Enterprise Support	195
Accessing updates	195
Websites	196
Customer self repair	196
Remote support	196
Documentation feedback	196
Index	198

MAC address table commands

This feature is supported only on the following ports:

- Layer 2 Ethernet ports on Ethernet switching modules.
- Fixed Layer 2 Ethernet ports of the following routers:
 - MSR1002-4/1003-8S.
 - MSR954 (JH296A/JH297A/JH298A/JH299A/JH373A).
 - MSR958 (JH300A/JH301A).
 - MSR2004-24/2004-48.

Commands and descriptions for centralized devices apply to the following routers:

- MSR1002-4/1003-8S.
- MSR2003.
- MSR2004-24/2004-48.
- MSR3012/3024/3044/3064.
- MSR954 (JH296A/JH297A/JH298A/JH299A/JH373A).
- MSR958 (JH300A/JH301A).

Commands and descriptions for distributed devices apply to MSR4060 and MSR4080 routers.

display mac-address

Use **display mac-address** to display MAC address entries.

Syntax

```
display mac-address [ mac-address [ vlan vlan-id ] ] [ [ dynamic | static ] [ interface interface-type interface-number ] ] [ blackhole ] [ vlan vlan-id ] [ count ] ]
```

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

mac-address: Specifies a MAC address in the format of H-H-H. When entering a MAC address, you can omit the leading zeros in each H section. For example, enter f-e2-1 for 000f-00e2-0001.

vlan *vlan-id*: Specifies a VLAN by its ID in the range of 1 to 4094.

dynamic: Displays dynamic MAC address entries.

static: Displays static MAC address entries.

interface *interface-type* *interface-number*: Specifies an interface by its type and number.

blackhole: Displays blackhole MAC address entries.

count: Displays only the number of MAC address entries that match all entry attributes you specify in the command. Detailed information about MAC address entries is not displayed. For example, you can use the **display mac-address vlan 20 dynamic count** command to display the number of dynamic entries for VLAN 20. If you do not specify an entry attribute, the command displays the

number of entries in the MAC address table. If you do not specify this keyword, the command displays detailed information about the specified MAC address entries.

Usage guidelines

A MAC address entry includes a destination MAC address, an outgoing interface, and a VLAN ID.

If you do not specify any parameters, the command displays all MAC address entries.

This command displays dynamic MAC address entries for an aggregate interface only when the aggregate interface has a minimum of one Selected member port.

Examples

Display MAC address entries for VLAN 100.

```
<Sysname> display mac-address vlan 100
```

MAC Address	VLAN ID	State	Port/NickName	Aging
0033-0033-0033	100	Blackhole	N/A	N
0000-0000-0002	100	Static	GE1/0/3	N
00e0-fc00-5829	100	Learned	GE1/0/4	Y

Display the number of MAC address entries.

```
<Sysname> display mac-address count
1 mac address(es) found.
```

Table 1 Command output

Field	Description
VLAN ID	ID of the VLAN to which the outgoing interface of the MAC address entry belongs.
State	MAC address entry state: <ul style="list-style-type: none"> • Static—Static MAC address entry. • Learned—Dynamic MAC address entry. Dynamic entries can be learned or manually configured. • Blackhole—Blackhole MAC address entry.
Port/NickName	When the field displays an interface name, the field indicates the outgoing interface for packets that are destined for the MAC address. This field displays N/A for a blackhole MAC address entry. The Nickname field is not supported in the current software version.
Aging	Whether the entry can age out: <ul style="list-style-type: none"> • Y—The entry can age out. • N—The entry never ages out.
mac address(es) found	Number of matching MAC address entries.

Related commands

mac-address

mac-address timer

display mac-address aging-time

Use **display mac-address aging-time** to display the aging timer for dynamic MAC address entries.

Syntax

display mac-address aging-time

Views

Any view

Predefined user roles

network-admin

network-operator

Examples

Display the aging timer for dynamic MAC address entries.

```
<Sysname> display mac-address aging-time
```

```
MAC address aging time: 300s.
```

Related commands

mac-address timer

display mac-address mac-learning

Use **display mac-address mac-learning** to display the global MAC address learning status and the MAC learning status of the specified interface or all interfaces.

Syntax

```
display mac-address mac-learning [ interface interface-type interface-number ]
```

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

interface *interface-type interface-number*. Specifies an interface by its type and number. If you do not specify an interface, the command displays the global MAC address learning status and the MAC address learning status of all interfaces.

Examples

Display the global MAC address learning status and the MAC learning status of all interfaces.

```
<Sysname> display mac-address mac-learning
```

```
Global MAC address learning status: Enabled.
```

Port	Learning Status
GE1/0/1	Enabled
GE1/0/2	Enabled
GE1/0/3	Enabled
GE1/0/4	Enabled

Table 2 Command output

Field	Description
Global MAC address learning status	Global MAC address learning status: <ul style="list-style-type: none">• Enabled.• Disabled.

Field	Description
Learning Status	MAC address learning status of an interface: <ul style="list-style-type: none"> • Enabled. • Disabled.

Related commands

mac-address mac-learning enable

display mac-address mac-move

Use **display mac-address mac-move** to display the MAC address move records after the device is started.

Syntax

Centralized devices in standalone mode:

display mac-address mac-move

Distributed devices in standalone mode/centralized devices in IRF mode:

display mac-address mac-move [slot slot-number]

Distributed devices in IRF mode:

display mac-address mac-move [chassis chassis-number slot slot-number]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

slot slot-number. Specifies a card by its slot number. If you do not specify a card, the command displays MAC address move records for all cards. (Distributed devices in standalone mode.)

slot slot-number. Specifies an IRF member device by its member ID. If you do not specify a member device, the command displays MAC address move records for all IRF member devices. (Centralized devices in IRF mode.)

chassis chassis-number slot slot-number. Specifies a card on an IRF member device. The *chassis-number* argument represents the member ID of the IRF member device. The *slot-number* argument represents the slot number of the card. If you do not specify a card, the command displays MAC address move records for all cards. (Distributed devices in IRF mode.)

Usage guidelines

When a MAC address frequently moves between the specified two interfaces, Layer 2 loops might occur in the network. To discover and locate loops, you can view the MAC address move records.

- In the MAC address move records, records with the same MAC address, VLAN, source port, and current port are considered to be one record.
- A device can save a maximum of 20 MAC address move records. When the number of MAC address move records exceeds 20, the most recent record will override the oldest record based on the last MAC address move time. (Centralized devices in standalone mode.)
- A card can save a maximum of 20 MAC address move records. When the number of MAC address move records exceeds 20, the most recent record will override the oldest record based on the last MAC address move time. (Distributed devices in standalone mode.)

- An IRF member device can save a maximum of 20 MAC address move records. When the number of MAC address move records exceeds 20, the most recent record will override the oldest record based on the last MAC address move time. (Centralized devices in IRF mode.)
- Each card of an IRF member device can save a maximum of 20 MAC move records. When the number of MAC address move records exceeds 20, the most recent record will override the oldest record based on the last MAC address move time. (Distributed devices in IRF mode.)

Examples

(Distributed devices in standalone mode.) Display the MAC address move records on the card in slot 1.

```
<Sysname> display mac-address mac-move slot 1
MAC address      VLAN Current port   Source port   Last time      Times
0000-0001-002c  1    GE1/0/1        GE1/0/2      2013-05-20 13:40:52  1
0000-0001-002c  1    GE1/0/2        GE1/0/1      2013-05-20 13:41:30  1
---  2 MAC address moving records found ---
```

(Distributed devices in IRF mode.) Display the MAC address move records on all cards.

```
<Sysname> display mac-address mac-move
MAC address      VLAN Current port   Source port   Last time      Times
0000-0001-002c  1    GE1/1/0/1      GE1/1/0/2    2013-05-20 13:40:52  20
0000-0001-002c  1    GE1/1/0/2      GE1/1/0/1    2013-05-20 13:41:32  20
0000-0094-0001  1    GE1/1/0/3      GE1/1/0/4    2013-05-20 13:42:22  13
0000-0094-0001  1    GE1/1/0/4      GE1/1/0/3    2013-05-20 13:42:21  12
---  4 MAC address moving records found ---
```

Table 3 Command output

Field	Description
VLAN	VLAN to which the outgoing interface of the MAC address entry belongs.
Current port	Interface to which the MAC address was moved.
Source port	Interface from which the MAC address was moved.
Last time	Last time when the MAC address was moved.
Times	Number of MAC address moves after the device is started. For a MAC address record, the number of MAC address moves is increased by 1 when a new MAC address move has the same MAC address , VLAN , Current Port , and Source Port fields as the MAC address record.

Related commands

mac-address notification mac-move

mac-address (interface view)

Use **mac-address** to add or modify a MAC address entry on an interface.

Use **undo mac-address** to delete a MAC address entry on an interface.

Syntax

mac-address { **dynamic** | **static** } *mac-address* **vlan** *vlan-id*

undo mac-address { **dynamic** | **static** } *mac-address* **vlan** *vlan-id*

Default

An interface is not configured with MAC address entries.

Views

Layer 2 Ethernet interface view

Predefined user roles

network-admin

Parameters

dynamic: Specifies dynamic MAC address entries.

static: Specifies static MAC address entries.

mac-address: Specifies a MAC address in the format of H-H-H, excluding multicast, all-zero, and all-F MAC addresses. When entering a MAC address, you can omit the leading zeros in each H section. For example, enter f-e2-1 for 000f-00e2-0001.

vlan *vlan-id*: Specifies an existing VLAN to which the specified interface belongs. The value range for the *vlan-id* argument is 1 to 4094.

Usage guidelines

Typically, the device automatically builds the MAC address table by learning the source MAC addresses of incoming frames on each interface. However, you can manually configure static MAC address entries. For a MAC address, a manually configured static entry takes precedence over a dynamically learned entry. To improve the security for the user device connected to an interface, manually configure a static entry to bind the user device to the interface. Then, the frames destined for the user device (for example, Host A) are always sent out of the interface. Other hosts using the forged MAC address of Host A cannot obtain the frames destined for Host A.

The MAC address entry configuration cannot survive a reboot unless you save it. The dynamic MAC address entries, however, are lost upon reboot whether or not you save the configuration.

Examples

```
# Add a static entry for MAC address 000f-e201-0101 on interface GigabitEthernet 1/0/1 that belongs to VLAN 2.
```

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] mac-address static 000f-e201-0101 vlan 2
```

Related commands

display mac-address

mac-address (system view)

mac-address (system view)

Use **mac-address** to add or modify a MAC address entry.

Use **undo mac-address** to delete one or all MAC address entries.

Syntax

```
mac-address { dynamic | static } mac-address interface interface-type interface-number vlan vlan-id
```

```
mac-address blackhole mac-address vlan vlan-id
```

```
undo mac-address [ [ dynamic | static ] mac-address interface interface-type interface-number vlan vlan-id ]
```

```
undo mac-address [ blackhole | dynamic | static ] [ mac-address ] vlan vlan-id
```

undo mac-address [**dynamic** | **static**] **interface** *interface-type interface-number*

Default

The system is not configured with MAC address entries.

Views

System view

Predefined user roles

network-admin

Parameters

dynamic: Specifies dynamic MAC address entries.

static: Specifies static MAC address entries.

blackhole: Specifies blackhole MAC address entries. Packets whose source or destination MAC addresses match blackhole MAC address entries are dropped.

mac-address: Specifies a MAC address in the format of H-H-H, excluding multicast, all-zero, and all-F MAC addresses. When entering a MAC address, you can omit the leading zeros in each H section. For example, enter f-e2-1 for 000f-00e2-0001.

vlan *vlan-id*: Specifies an existing VLAN to which the interface belongs. The value range for the *vlan-id* argument is 1 to 4094.

interface *interface-type interface-number*: Specifies an outgoing interface by its type and number.

interface *interface-list*: Specifies interfaces in the format of { *interface-type interface-number* [**to interface-type interface-number**] } &<1-n>. The interface can only be a Layer 2 Ethernet interface or Layer 2 aggregate interface. &<1-n> specifies that you can configure a maximum of *n* interfaces or interface ranges.

Usage guidelines

You can use this command to configure the following types of MAC address entries:

- Dynamic entries.
Dynamic entries include manually configured dynamic entries and automatically learned dynamic entries.
- Static entries.
For a MAC address, a manually configured static entry takes precedence over a dynamic entry. To improve the security for the user device connected to an interface, manually configure a static entry to bind the user device to the interface. Then, the frames destined for the user device (for example, Host A) are always sent out of the interface. Other hosts using the forged MAC address of Host A cannot obtain the frames destined for Host A.
- Blackhole entries.
To drop frames with the specified source MAC addresses or destination MAC addresses, you can configure blackhole entries.

A static or blackhole MAC address entry can overwrite a dynamic MAC address entry, but not vice versa.

If you execute the **undo mac-address** command without specifying any parameters, this command deletes all unicast MAC address entries.

You can delete all the MAC address entries of the specified VLAN. You can also delete only one type (dynamic, static, or blackhole) of MAC address entries.

The MAC address entry configuration cannot survive a reboot unless you save it. The dynamic MAC address entries, however, are lost upon reboot whether or not you save the configuration.

Examples

Add a static entry for MAC address 000f-e201-0101. Then, all frames that are destined for this MAC address are sent out of interface GigabitEthernet 1/0/1, which belongs to VLAN 2.

```
<Sysname> system-view
[Sysname] mac-address static 000f-e201-0101 interface gigabitethernet 1/0/1 vlan 2
```

Related commands

display mac-address

mac-address (interface view)

mac-address mac-learning enable

Use **mac-address mac-learning enable** to enable MAC address learning on an interface.

Use **undo mac-address mac-learning enable** to disable MAC address learning on an interface.

Syntax

mac-address mac-learning enable

undo mac-address mac-learning enable

Default

MAC address learning is enabled.

Views

Layer 2 Ethernet interface view

Predefined user roles

network-admin

Usage guidelines

To prevent the MAC address table from becoming saturated, you can disable MAC address learning.

For example, a number of packets with different source MAC addresses reaching a device can affect the MAC address table update. To avoid such attacks, you can disable MAC address learning by following these guidelines:

- You can disable MAC address learning on a per-interface basis. If you disable MAC address learning on all interfaces, the device will stop learning MAC addresses and cannot dynamically update the MAC address table.
- Because disabling MAC address learning can result in broadcast storms, enable broadcast storm suppression after you disable MAC address learning on an interface. For more information about broadcast storm suppression, see *Interface Configuration Guide*.

Examples

Disable MAC address learning on interface GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] undo mac-address mac-learning enable
```

Related commands

display mac-address mac-learning

mac-address notification mac-move

Use **mac-address notification mac-move** to enable MAC address move notifications and optionally specify a MAC move detection interval.

Use **undo mac-address notification mac-move** to disable MAC address move notifications.

Syntax

mac-address notification mac-move [*interval interval*]

undo mac-address notification mac-move

Default

MAC address move notifications are disabled.

Views

System view

Predefined user roles

network-admin

Parameters

interval *interval*: Specifies the interval for detecting MAC address moves, in the range of 1 to 60 minutes. If you do not specify this option, the default setting of 1 minute is used.

Usage guidelines

With MAC address move notifications enabled, the system records the MAC address move logs every MAC move detection interval. Each record of the MAC address move logs contains the following information:

- MAC address.
- VLAN ID of the MAC address entry.
- Current port and source port of the MAC address moves.
- Number of MAC address moves within a detection interval.

A MAC address can have only one MAC address move record. If a MAC address moves multiple times, the new record overrides the old record.

Within a detection interval, the device can record MAC address move information for a maximum of 20 MAC addresses. If the limit is reached, the device only updates existing records, and new MAC address moves are not recorded. Then in the next detection interval, a new MAC address move record will overwrite the earliest one generated in the previous detection interval. (Centralized devices in standalone mode.)

Within a detection interval, an IRF member device can record MAC address move information for a maximum of 20 MAC addresses. If the limit is reached, the device only updates existing records, and new MAC address moves are not recorded. Then in the next detection interval, a new MAC address move record will overwrite the earliest one generated in the previous detection interval. (Centralized devices in IRF mode.)

Within a detection interval, each card can record MAC address move information for a maximum of 20 MAC addresses. If the limit is reached, the card only updates existing records, and new MAC address moves are not recorded. Then in the next detection interval, a new MAC address move record will overwrite the earliest one generated in the previous detection interval. (Distributed devices in standalone mode/distributed devices in IRF mode.)

After you execute this command, the system sends only syslog messages to the information center module. If the **snmp-agent trap enable mac-address** command is also executed, the system also sends SNMP notifications to the SNMP module.

Examples

```
# Enable MAC address move notifications.
```

```
<Sysname> system-view
```

```
[Sysname] mac-address notification mac-move
```

```
[Sysname]
```

```
%May 14 17:16:45:688 2013 HPE MAC/4/MAC_FLAPPING: MAC address 0000-0012-0034 in VLAN 500 has moved from port GE1/0/1 to port GE1/0/2 for 1 times
```

The output shows that:

- The VLAN ID of MAC address 0000-0012-0034 is VLAN 500.
- The MAC address moved from port GigabitEthernet 1/0/1 to port GigabitEthernet 1/0/2.
- The MAC address has moved once within a MAC move detection interval.

Related commands

```
display mac-address mac-move
```

mac-address notification mac-move suppression (interface view)

Use **mac-address notification mac-move suppression** to enable MAC address move suppression on an interface.

Use **undo mac-address notification mac-move suppression** to disable MAC address move suppression on an interface.

Syntax

```
mac-address notification mac-move suppression
```

```
undo mac-address notification mac-move suppression
```

Default

MAC address moves are not suppressed.

Views

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

Predefined user roles

network-admin

Usage guidelines

This feature shuts an interface down when a MAC address has been moved to or from the interface more than the suppression threshold within a MAC move detection interval. The shutdown interface automatically goes up after a suppression interval. Also, you can use the **shutdown** command and then the **undo shutdown** command to bring up the interface.

When MAC address move suppression shuts an interface down, the system sends only syslog messages to the information center module. If the **snmp-agent trap enable mac-address** command is also executed, the system also sends SNMP notifications to the SNMP module.

Examples

```
# Enable MAC address move suppression on GigabitEthernet 1/0/1.
```

```
[Sysname] interface gigabitethernet 1/0/1
```

```
[Sysname-GigabitEthernet1/0/1] mac-address notification mac-move suppression
```

Related commands

mac-address notification mac-move suppression (system view)

mac-address notification mac-move suppression (system view)

Use **mac-address notification mac-move suppression** to set the suppression interval or the suppression threshold.

Use **undo mac-address notification mac-move suppression** to restore the default.

Syntax

mac-address notification mac-move suppression { **interval** *interval* | **threshold** *threshold* }

undo mac-address notification mac-move suppression { **interval** | **threshold** }

Default

The suppression interval is 30 seconds. The suppression threshold is 3.

Views

System view

Predefined user roles

network-admin

Parameters

interval *interval*: Specifies the MAC address move suppression interval during which a suppressed interface stays down. The value range for the *interval-value* argument is 30 to 86400 seconds. If you do not specify this option, the default suppression interval of 30 seconds is used.

threshold *threshold*: Specifies the suppression threshold for MAC address moves sourced from or destined for an interface within a MAC move detection interval. The value range for this argument is 0 to 1024. If you do not specify this option, the default suppression threshold of 3 is used.

Usage guidelines

For this command to take effect on an interface, you must also enable MAC address move suppression on the interface.

If you set the suppression interval or suppression threshold multiple times, the most recent configuration applies. The suppression interval setting is independent of the suppression threshold setting.

Examples

```
# Set the suppression interval to 40 seconds and the suppression threshold to 1 for MAC address moves.
```

```
<Sysname> system-view
```

```
[Sysname] mac-address notification mac-move suppression interval 40
```

```
[Sysname] mac-address notification mac-move suppression threshold 1
```

Related commands

mac-address notification mac-move suppression (interface view)

mac-address timer

Use **mac-address timer** to set the aging timer for dynamic MAC address entries.

Use **undo mac-address timer** to restore the default.

Syntax

```
mac-address timer { aging seconds | no-aging }  
undo mac-address timer
```

Default

The aging timer is 300 seconds for dynamic MAC address entries.

Views

System view

Predefined user roles

network-admin

Parameters

aging *seconds*: Specifies an aging timer (in seconds) for dynamic MAC address entries. The value range for the *seconds* argument is 10 to 630.

no-aging: Configures dynamic MAC address entries not to age.

Usage guidelines

To set the aging timer appropriately, follow these guidelines:

- A long aging interval causes the MAC address table to retain outdated entries and fail to accommodate the most recent network changes.
- A short aging interval results in removal of valid entries. Then, unnecessary broadcast packets appear and affect device performance.

Examples

```
# Set the aging time to 500 seconds for dynamic MAC address entries.  
<Sysname> system-view  
[Sysname] mac-address timer aging 500
```

Related commands

```
display mac-address aging-time
```

snmp-agent trap enable mac-address

Use **snmp-agent trap enable mac-address** to enable SNMP notifications for the MAC address table.

Use **undo snmp-agent trap enable mac-address** to disable SNMP notifications for the MAC address table.

Syntax

```
snmp-agent trap enable mac-address [ mac-move ]  
undo snmp-agent trap enable mac-address [ mac-move ]
```

Default

SNMP notifications are enabled for the MAC address table.

Views

System view

Predefined user roles

network-admin

Parameters

mac-move: Specifies notifications about the MAC address moves for the MAC address table. If you do not specify this keyword, the command enables all types of SNMP notifications for the MAC address table.

Usage guidelines

To report critical MAC address move events to an NMS, enable SNMP notifications for the MAC address table. For MAC address move event notifications to be sent correctly, you must also configure SNMP on the device.

When SNMP notifications are disabled for the MAC address table, the device sends the generated logs to the information center. To display the logs, configure the log destination and output rule configuration in the information center.

For information about SNMP and information center configuration, see the network management and monitoring configuration guide for the device.

The MAC address table supports only SNMP notifications about MAC address moves. When you enable or disable SNMP notifications about MAC address moves, you enable or disable all types of SNMP notifications for the MAC address table.

Examples

Disable SNMP notifications about MAC address moves for the MAC address table.

```
<Sysname> system-view
```

```
[Sysname] undo snmp-agent trap enable mac-address mac-move
```

Related commands

mac-address notification mac-move

Ethernet link aggregation commands

Layer 2 aggregation groups and aggregate interfaces are not supported on the following interface modules:

- DSIC-9FSW.
- DSIC-9FSW-PoE.
- SIC-4FSW.
- SIC-4FSW-PoE.

Commands and descriptions for centralized devices apply to the following routers:

- MSR1002-4/1003-8S.
- MSR2003.
- MSR2004-24/2004-48.
- MSR3012/3024/3044/3064.
- MSR954 (JH296A/JH297A/JH298A/JH299A/JH373A).
- MSR958 (JH300A/JH301A).

Commands and descriptions for distributed devices apply to MSR4060 and MSR4080 routers.

bandwidth

Use **bandwidth** to set the expected bandwidth for an interface.

Use **undo bandwidth** to restore the default.

Syntax

bandwidth *bandwidth-value*

undo bandwidth

Default

The expected bandwidth (in kbps) is the interface baud rate divided by 1000.

Views

Layer 2 aggregate interface view

Layer 3 aggregate interface view

Layer 3 aggregate subinterface view

Predefined user roles

network-admin

Parameters

bandwidth-value: Specifies the expected bandwidth in the range of 1 to 400000000 kbps.

Usage guidelines

The expected bandwidth is an informational parameter used only by higher-layer protocols for calculation. You cannot adjust the actual bandwidth of an interface by using this command.

Examples

```
# Set the expected bandwidth to 10000 kbps for Layer 2 aggregate interface Bridge-Aggregation 1.  
<Sysname> system-view
```

```
[Sysname] interface bridge-aggregation 1
[Sysname-Bridge-Aggregation1] bandwidth 10000
```

default

Use **default** to restore the default settings for an aggregate interface.

Syntax

default

Views

Layer 2 aggregate interface view
Layer 3 aggregate interface view
Layer 3 aggregate subinterface view

Predefined user roles

network-admin

Usage guidelines

CAUTION:

The **default** command might interrupt ongoing network services. Make sure you are fully aware of the impacts of this command when you execute it on a live network.

This command might fail to restore the default settings for some commands for reasons such as command dependencies and system restrictions. Use the **display this** command in interface view to identify these commands, and then use their **undo** forms or follow the command reference to restore their default settings. If your restoration attempt still fails, follow the error message instructions to resolve the problem.

Examples

```
# Restore the default settings for Layer 2 aggregate interface 1.
<Sysname> system-view
[Sysname] interface bridge-aggregation 1
[Sysname-Bridge-Aggregation1] default
```

description

Use **description** to configure the description of an interface.

Use **undo description** to restore the default.

Syntax

description *text*

undo description

Default

The description of an interface is *interface-name* **Interface**. For example, the default description of Bridge-Aggregation 1 is **Bridge-Aggregation1 Interface**.

Views

Layer 2 aggregate interface view
Layer 3 aggregate interface view

Layer 3 aggregate subinterface view

Predefined user roles

network-admin

Parameters

text: Specifies a description, a case-sensitive string of 1 to 255 characters.

Examples

```
# Configure the description as connect to the lab for Layer 2 aggregate interface Bridge-Aggregation 1.
```

```
<Sysname> system-view
```

```
[Sysname] interface bridge-aggregation 1
```

```
[Sysname-Bridge-Aggregation1] description connect to the lab
```

display interface

Use **display interface** to display aggregate interface information.

Syntax

```
display interface [ { bridge-aggregation | route-aggregation } [ interface-number ] ] [ brief [ description | down ] ]
```

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

bridge-aggregation: Specifies Layer 2 aggregate interfaces.

route-aggregation: Specifies Layer 3 aggregate interfaces.

interface-number: Specifies an existing aggregate interface number.

brief: Displays brief interface information. If you do not specify this keyword, the command displays detailed interface information.

description: Displays complete interface descriptions. If you do not specify this keyword, the command displays only the first 27 characters of each interface description.

down: Displays information about interfaces in down state and the causes for the down state. If you do not specify this keyword, the command displays information about interfaces in all states.

Usage guidelines

If you do not specify the **bridge-aggregation** and **route-aggregation** keywords, the command displays information about all interfaces.

If you specify the **bridge-aggregation** or **route-aggregation** keyword but do not specify an interface number, the command displays information about all aggregate interfaces of the specified type.

If you specify the **bridge-aggregation** *interface-number* or **route-aggregation** *interface-number* option, the command displays information about the specified aggregate interface.

Examples

```
# Display detailed information about Layer 2 aggregate interface Bridge-Aggregation 1.
```

```
<Sysname> display interface bridge-aggregation 1
```

```

Bridge-Aggregation1
Current state: UP
IP packet frame type: PKTFMT_ETHNT_2, hardware address: 000f-e207-f2e0
Description: Bridge-Aggregation1 Interface
Bandwidth: 1000kbps
2Gbps-speed mode, full-duplex mode
Link speed type is autonegotiation, link duplex type is autonegotiation
PVID: 1
Port link-type: Access
  Tagged VLANs:   None
  UnTagged VLANs: 1
Last clearing of counters:  Never
  Last 300 second input:  6900 packets/sec 885160 bytes/sec   0%
  Last 300 second output: 3150 packets/sec 404430 bytes/sec   0%
Input (total): 5364747 packets, 686688416 bytes
                2682273 unicasts, 1341137 broadcasts, 1341337 multicasts, 0 pauses
Input (normal): 5364747 packets, 686688416 bytes
                2682273 unicasts, 1341137 broadcasts, 1341337 multicasts, 0 pauses
Input: 0 input errors, 0 runts, 0 giants, 0 throttles
       0 CRC, 0 frame, 0 overruns, - aborts
       - ignored, - parity errors
Output (total): 1042508 packets, 133441832 bytes
               1042306 unicasts, 0 broadcasts, 202 multicasts, - pauses
Output (normal): 1042508 packets, 133441832 bytes
                1042306 unicasts, 0 broadcasts, 202 multicasts, 0 pauses
Output: 0 output errors, - underruns, - buffer failures
       0 aborts, 0 deferred, 0 collisions, 0 late collisions
       - lost carrier, - no carrier

```

Display detailed information about Layer 3 aggregate interface Route-Aggregation 1.

```

<Sysname> display interface route-aggregation 1
Route-Aggregation1
Current state: UP
Line protocol state: UP
Description: Route-Aggregation1 Interface
Bandwidth: 1000kbps
Maximum transmission unit: 1500
Internet protocol processing: disabled
IP packet frame type: PKTFMT_ETHNT_2, hardware address: 0000-0000-0000
IPv6 packet frame type: PKTFMT_ETHNT_2, hardware address: 0000-0000-0000
Port priority: 0
Output queue - Urgent queuing: Size/Length/Discards 0/100/0
Output queue - Protocol queuing: Size/Length/Discards 0/500/0
Output queue - FIFO queuing: Size/Length/Discards 0/75/0
Unknown-speed mode, unknown-duplex mode
Link speed type is autonegotiation, link duplex type is autonegotiation
Last clearing of counters: Never
  Last 300 seconds input rate: 0 bytes/sec, 0 bits/sec, 0 packets/sec
  Last 300 seconds output rate: 0 bytes/sec, 0 bits/sec, 0 packets/sec

```

Input: 0 packets, 0 bytes, 0 drops
Output: 0 packets, 0 bytes, 0 drops

Display brief information about Layer 2 aggregate interface Bridge-Aggregation 1.

```
<Sysname> display interface bridge-aggregation 1 brief
Brief information on interfaces in bridge mode:
Link: ADM - administratively down; Stby - standby
Speed: (a) - auto
Duplex: (a)/A - auto; H - half; F - full
Type: A - access; T - trunk; H - hybrid
Interface          Link Speed  Duplex Type PVID Description
BAGG1              UP  auto    A     A     1
```

Display brief information about Layer 3 aggregate interface Route-Aggregation 1.

```
<Sysname> display interface route-aggregation 1 brief
Brief information on interfaces in route mode:
Link: ADM - administratively down; Stby - standby
Protocol: (s) - spoofing
Interface          Link Protocol Primary IP      Description
RAGG1              UP  UP          --
```

Table 4 Command output

Field	Description
Bridge-Aggregation1	Layer 2 aggregate interface name.
Route-Aggregation1	Layer 3 aggregate interface name.
Current state	<p>Layer 3 aggregate interface status:</p> <ul style="list-style-type: none"> • DOWN (Administratively down)—The interface is administratively shut down with the shutdown command. • DOWN—The interface is administratively up but physically down (possibly because no physical link exists or the link has failed). • UP—The Ethernet interface is both administratively and physically up.
IP packet frame type	<p>IPv4 packet frame format.</p> <p>The value PKTFMT_ETHNT_2 indicates that packets are encapsulated in Ethernet II format.</p>
Description	<p>Partial or complete interface description set by using the description command.</p> <ul style="list-style-type: none"> • If you do not specify the description keyword in the display interface brief command, this field displays the first 27 characters of the description. • If you specify the description keyword in the display interface brief command, this field displays the complete description.
Bandwidth	Expected bandwidth of the interface. This field is not displayed when the bandwidth is 0 kbps.
Output queue - Urgent queuing: Size/Length/Discards	<p>Information about the urgent output queue:</p> <ul style="list-style-type: none"> • Size—Number of packets in the queue. • Length—Maximum number of packets that the queue can contain. • Discards—Number of dropped packets.

Field	Description
Output queue - Protocol queuing: Size/Length/Discards	Information about the protocol output queue: <ul style="list-style-type: none"> • Size—Number of packets in the queue. • Length—Maximum number of packets that the queue can contain. • Discards—Number of dropped packets.
Output queue - FIFO queuing: Size/Length/Discards	Information about the FIFO output queue: <ul style="list-style-type: none"> • Size—Number of packets in the queue. • Length—Maximum number of packets that the queue can contain. • Discards—Number of dropped packets.
Unknown-speed unknown-duplex mode	The interface speed and duplex mode are unknown.
Port link-type	Port link type: <ul style="list-style-type: none"> • Access. • Trunk. • Hybrid.
Tagged VLANs	VLAN whose packets are sent out of this interface with a tag.
Untagged VLANs	VLAN whose packets are sent out of this interface without a tag.
Last clearing of counters	Time when the reset counters interface command was last used to clear the interface statistics. This field displays Never if the reset counters interface command has never been used on the interface since device startup.
Last 300 seconds input/output rate	Average input or output rate over the last 300 seconds.
Input/Output (total)	Statistics of all packets received or sent on the interface.
Input/Output (normal)	Statistics of all normal packets received or sent on the interface.
Line protocol state	Data link layer protocol state of the interface: <ul style="list-style-type: none"> • UP. • DOWN.
Internet protocol processing	IP packet processing. Disabled indicates that IP packets cannot be processed. For an interface configured with an IP address, this field changes to Internet address .
Brief information on interfaces in route mode	Brief information about Layer 3 interfaces.
Brief information on interfaces in bridge mode	Brief information about Layer 2 interfaces.
Link: ADM - administratively down; Stby - standby	Link status: <ul style="list-style-type: none"> • ADM—The interface has been administratively shut down. To recover its physical layer state, use the undo shutdown command. • Stby—The interface is operating as a backup interface.
Speed: (a) - auto	If the speed of an interface is automatically negotiated, the speed attribute of the interface includes the autonegotiation flag (the letter a in parentheses). If an interface is configured to autonegotiate its speed but the autonegotiation has not started, its speed attribute is displayed as auto .

Field	Description
Duplex: (a)/A - auto; H - half; F - full	<p>If the duplex mode of an interface is automatically negotiated, the duplex mode attribute of the interface includes the letter a in parentheses. H indicates the half duplex mode. F indicates the full duplex mode.</p> <p>If an interface is configured to autonegotiate its duplex mode but the autonegotiation has not started, its duplex mode attribute is displayed as A.</p>
Type: A - access; T - trunk; H - hybrid	Port link type options for interfaces.
Protocol: (s) – spoofing	<p>The protocol attribute includes the spoofing flag (the letter s in parentheses) when the following conditions exist:</p> <ul style="list-style-type: none"> The data link layer protocol state of an interface is shown as UP. The link is an on-demand link or not present.
Interface	Abbreviated interface name.
Link	<p>Physical link state of the interface:</p> <ul style="list-style-type: none"> UP—The interface is physically up. DOWN—The interface is physically down. ADM—The interface has been administratively shut down. To bring up the interface, use the undo shutdown command. Stby—The interface is operating as a backup interface.
Speed	Interface speed, in bps.
Protocol	<p>Data link layer state of the interface:</p> <ul style="list-style-type: none"> UP—The data link layer of the interface is up. DOWN—The data link layer of the interface is down. UP(s)—The data link layer of the interface is shown as UP, but its link is an on-demand link or not present.
Cause	Cause for the physical link state of an interface to be DOWN .

display lacp system-id

Use **display lacp system-id** to display the local system ID.

Syntax

```
display lacp system-id
```

Views

Any view

Predefined user roles

network-admin

network-operator

Usage guidelines

You can use the **lacp system-priority** command to change the LACP priority of the local system. The LACP priority value is specified in decimal format in the **lacp system-priority** command. However, it is displayed in hexadecimal format in the output from the **display lacp system-id** command.

Examples

```
# Display the local system ID.
<Sysname> display lacp system-id
Actor System ID: 0x8000, 0000-fc00-6504
```

Table 5 Command output

Field	Description
Actor System ID: 0x8000, 0000-fc00-6504	Local system ID, which contains the system LACP priority (0x8000 in this sample output) and the system MAC address (0000-FC00-6504 in this sample output).

Related commands

lacp system-priority

display link-aggregation load-sharing mode

Use **display link-aggregation load-sharing mode** to display global or group-specific link-aggregation load sharing modes.

Syntax

```
display link-aggregation load-sharing mode [ interface [ { bridge-aggregation | route-aggregation } interface-number ] ]
```

Views

Any view

Predefined user roles

network-admin
network-operator

Parameters

bridge-aggregation: Specifies Layer 2 aggregate interfaces.

route-aggregation: Specifies Layer 3 aggregate interfaces.

interface-number: Specifies an existing aggregate interface number.

Usage guidelines

If you do not specify the **interface** keyword, the command displays the global link-aggregation load sharing modes.

If you specify the **interface** keyword but do not specify an interface type, the command displays all group-specific load sharing modes.

The **bridge-aggregation** or **route-aggregation** keyword is available only when the corresponding aggregate interfaces exist on the device.

Examples

```
# Display the default global link-aggregation load sharing modes.
<Sysname> display link-aggregation load-sharing mode
Link-aggregation load-sharing mode (hardware forwarding):
Layer 2 traffic: destination-mac address  source-mac address
Layer 3 traffic: destination-ip address  source-ip address
                  ip-protocol
Layer 4 traffic: destination-port        source-port
```

```

MPLS traffic    : mpls-label1
Link-aggregation load-sharing mode (software forwarding):
Layer 3 traffic: destination-ip address    source-ip address
Layer 4 traffic: destination-ip address    source-ip address

# Display the set global link-aggregation load sharing mode.
<Sysname> display link-aggregation load-sharing mode
Link-aggregation load-sharing mode:
destination-mac address source-mac address

# Display the default link-aggregation load sharing modes of Layer 2 aggregation group 1.
<Sysname> display link-aggregation load-sharing mode interface bridge-aggregation 1
Bridge-Aggregation1 load-sharing mode (hardware forwarding):
Layer 2 traffic: destination-mac address    source-mac address
Layer 3 traffic: destination-ip address    source-ip address
                  ip-protocol
Layer 4 traffic: destination-port          source-port
MPLS traffic    : mpls-label1
Bridge-Aggregation2 load-sharing mode (software forwarding):
Layer 3 traffic: destination-ip address    source-ip address
Layer 4 traffic: destination-ip address    source-ip address

# Display the set link-aggregation load sharing mode of Layer 2 aggregation group 1.
<Sysname> display link-aggregation load-sharing mode interface bridge-aggregation 1
Bridge-Aggregation1 load-sharing mode:
destination-mac address source-mac address

```

Table 6 Command output

Field	Description
Link-aggregation load-sharing mode	Global link-aggregation load sharing mode. By default, this field displays the link-aggregation load sharing modes for Layer 2, Layer 3, Layer 4, and MPLS traffic. If you have set the global link-aggregation load sharing mode, this field displays the set mode.
Bridge-Aggregation1 load-sharing mode	Link-aggregation load sharing mode of Layer 2 aggregation group 1. By default, this field displays the global link-aggregation load sharing modes. If you have set a link-aggregation load sharing mode for this aggregation group, this field displays the set mode.
Route-Aggregation1 load-sharing mode	Link-aggregation load sharing mode of Layer 3 aggregation group 1. By default, this field displays the global link-aggregation load sharing modes. If you have set a link-aggregation load sharing mode for this aggregation group, this field displays the set mode.
Layer 2 traffic: destination-mac address source-mac address	Default link-aggregation load sharing mode for Layer 2 traffic. In this sample output, Layer 2 traffic is load shared based on source and destination MAC addresses.
Layer 3 traffic: destination-ip address source-ip address	Default link-aggregation load sharing mode for Layer 3 traffic. In this sample output, Layer 3 traffic is load shared based on source and destination IP addresses.

Field	Description
Layer 4 traffic: destination-port source-port	Default link-aggregation load sharing mode for Layer 4 traffic. In this sample output, Layer 4 traffic is load shared based on source and destination ports.
MPLS traffic: mpls-label1	Default link-aggregation load sharing mode for MPLS traffic. In this sample output, MPLS traffic is load shared based on Layer 1 MPLS labels.
destination-mac address source-mac address	User-configured link-aggregation load sharing mode. In this sample output, traffic is load shared based on source and destination MAC addresses.

display link-aggregation member-port

Use **display link-aggregation member-port** to display detailed link aggregation information for the specified member ports.

Syntax

```
display link-aggregation member-port [ interface-list ]
```

Views

Any view

Predefined user roles

network-admin
network-operator

Parameters

interface-list: Specifies a list of link aggregation member ports, in the format *interface-type interface-number* [**to** *interface-type interface-number*]. The *interface-type interface-number* argument specifies an interface by its type and number.

Usage guidelines

A member port in a static aggregation group cannot obtain information about the peer group. For such member ports, the command displays the port number, port priority, and operational key of only the local end.

Examples

Display detailed link aggregation information for GigabitEthernet 1/0/1, which is a member port of a static aggregation group.

```
<Sysname> display link-aggregation member-port gigabitethernet 1/0/1
Flags: A -- LACP_Activity, B -- LACP_Timeout, C -- Aggregation,
       D -- Synchronization, E -- Collecting, F -- Distributing,
       G -- Defaulted, H -- Expired
```

```
GigabitEthernet1/0/1:
Aggregate Interface: Bridge-Aggregation1
Port Number: 1
Port Priority: 32768
Oper-Key: 1
```

Display detailed link aggregation information for GigabitEthernet 1/0/2, which is a member port of a dynamic aggregation group.

```
<Sysname> display link-aggregation member-port gigabitethernet 1/0/2
```

```
Flags: A -- LACP_Activity, B -- LACP_Timeout, C -- Aggregation,
      D -- Synchronization, E -- Collecting, F -- Distributing,
      G -- Defaulted, H -- Expired
```

```
GigabitEthernet1/0/2:
```

```
Aggregate Interface: Bridge-Aggregation1
```

```
Local:
```

```
  Port Number: 2
  Port Priority: 32768
  Oper-Key: 2
  Flag: {ACDEF}
```

```
Remote:
```

```
  System ID: 0x8000, 000f-e267-6c6a
  Port Number: 26
  Port Priority: 32768
  Oper-Key: 2
  Flag: {ACDEF}
```

```
Received LACP Packets: 5 packet(s)
```

```
Illegal: 0 packet(s)
```

```
Sent LACP Packets: 7 packet(s)
```

Table 7 Command output

Field	Description
Flags	<p>LACP state flags. This field is one byte long, represented by ABCDEFGH from the least significant bit to the most significant bit. A letter appears when its bit is 1 and does not appear when its bit is 0.</p> <ul style="list-style-type: none"> • A—Indicates whether LACP is active on the port. 1 indicates active. 0 indicates passive. • B—Indicates the LACP timeout interval. 1 indicates the short timeout interval. 0 indicates the long timeout interval. • C—Indicates whether the sending system considers that the link is aggregatable. 1 indicates yes. 0 indicates no. • D—Indicates whether the sending system considers that the link has been aggregated. 1 indicates yes. 0 indicates no. • E—Indicates whether the sending system considers that the link can collect frames. 1 indicates yes. 0 indicates no. • F—Indicates whether the sending system considers that the link can distribute frames. 1 indicates yes. 0 indicates no. • G—Indicates whether the RX state machine of the sending system is in default state. 1 indicates yes. 0 indicates no. • H—Indicates whether the RX state machine of the sending system is in expired state. 1 indicates yes. 0 indicates no.
Aggregate Interface	Aggregate interface to which the member port belongs.
Local	Information about the local end.
Oper-key	Operational key.
Flag	LACP protocol state flag.
Remote	Information about the peer end.
System ID	Peer system ID, containing the system LACP priority and the system MAC address.
Received	LACP
	Total number of LACP packets received.

Field	Description
Packets	
Illegal	Total number of illegal packets.
Sent LACP Packets	Total number of LACP packets sent.

display link-aggregation summary

Use **display link-aggregation summary** to display brief information about all aggregation groups.

Syntax

display link-aggregation summary

Views

Any view

Predefined user roles

network-admin

network-operator

Usage guidelines

Static link aggregation groups cannot obtain information about the peer groups. As a result, the **Partner ID** field displays **None** or nothing for a static link aggregation group.

Examples

Display brief information about all aggregation groups.

```
<Sysname> display link-aggregation summary
```

```
Aggregate Interface Type:
```

```
BAGG -- Bridge-Aggregation, BLAGG -- Blade-Aggregation, RAGG -- Route-Aggregation, SCH-B  
- Schannel-Bundle
```

```
Aggregation Mode: S -- Static, D -- Dynamic
```

```
Loadsharing Type: Shar -- Loadsharing, NonS -- Non-Loadsharing
```

```
Actor System ID: 0x8000, 000f-e267-6c6a
```

AGG	AGG	Partner ID	Selected	Unselected	Individual	Share
Interface	Mode		Ports	Ports	Ports	Type
RAGG1	S	None	1	0	0	NonS
BAGG2	D	0x8000,00e0-fcff-ff01	2	0	0	Shar

Table 8 Command output

Field	Description
Aggregate Interface Type	Aggregate interface type: <ul style="list-style-type: none"> BAGG—Layer 2. RAGG—Layer 3.
Aggregation Mode	Aggregation group type: <ul style="list-style-type: none"> S—Static. D—Dynamic.
Loadsharing Type	Load sharing type: <ul style="list-style-type: none"> Shar—Load-sharing.

Field	Description
	<ul style="list-style-type: none"> • NonS—Non-load-sharing.
Actor System ID	Local system ID, which contains the local system LACP priority and the local system MAC address.
AGG Interface	Type and number of the aggregate interface.
AGG Mode	Aggregation group type.
Partner ID	System ID of the peer system, which contains the peer system LACP priority and the peer system MAC address.
Selected Ports	Total number of Selected ports.
Unselected Ports	Total number of Unselected ports.
Individual Ports	Total number of Individual ports.
Share Type	Load sharing type.

display link-aggregation verbose

Use **display link-aggregation verbose** to display detailed information about the aggregation groups that correspond to the specified aggregate interfaces.

Syntax

```
display link-aggregation verbose [ { bridge-aggregation | route-aggregation }
[ interface-number ] ]
```

Views

Any view

Predefined user roles

network-admin
network-operator

Parameters

bridge-aggregation: Specifies Layer 2 aggregate interfaces.

route-aggregation: Specifies Layer 3 aggregate interfaces.

interface-number. Specifies an existing aggregate interface by its number.

Usage guidelines

If you specify the **bridge-aggregation** or **route-aggregation** keyword but do not specify an interface number, the command displays detailed information about all aggregation groups of the specified type.

If you do not specify an aggregate interface type, the command displays detailed information about all aggregation groups.

The **bridge-aggregation** or **route-aggregation** keyword is available only when the corresponding aggregate interfaces exist on the device.

Examples

Display detailed information about Layer 2 aggregation group 1, which is a dynamic aggregation group.

```
<Sysname> display link-aggregation verbose bridge-aggregation 1
Loadsharing Type: Shar -- Loadsharing, NonS -- Non-Loadsharing
```

Port Status: S -- Selected, U -- Unselected, I -- Individual
 Flags: A -- LACP_Activity, B -- LACP_Timeout, C -- Aggregation,
 D -- Synchronization, E -- Collecting, F -- Distributing,
 G -- Defaulted, H -- Expired

Aggregate Interface: Bridge-Aggregation1

Aggregation Mode: Dynamic

Loadsharing Type: Shar

System ID: 0x8000, 000f-e267-6c6a

Local:

Port	Status	Priority	Oper-Key	Flag
GE1/0/1	S	32768	2	{ACDEF}
GE1/0/2	S	32768	2	{ACDEF}
GE1/0/3	S	32768	2	{AG}

Remote:

Actor	Partner	Priority	Oper-Key	SystemID	Flag
GE1/0/1	1	32768	2	0x8000, 000f-e267-57ad	{ACDEF}
GE1/0/2	2	32768	2	0x8000, 000f-e267-57ad	{ACDEF}
GE1/0/3	0	32768	0	0x8000, 0000-0000-0000	{DEF}

Display detailed information about Layer 2 aggregation group 2, which is a static aggregation group.

<Sysname> display link-aggregation verbose bridge-aggregation 2

Loadsharing Type: Shar -- Loadsharing, NonS -- Non-Loadsharing

Port Status: S -- Selected, U -- Unselected, I -- Individual

Flags: A -- LACP_Activity, B -- LACP_Timeout, C -- Aggregation,
 D -- Synchronization, E -- Collecting, F -- Distributing,
 G -- Defaulted, H -- Expired

Aggregate Interface: Bridge-Aggregation2

Aggregation Mode: Static

Loadsharing Type: Shar

Port	Status	Priority	Oper-Key
GE1/0/1	U	32768	1
GE1/0/2	U	32768	1
GE1/0/3	U	32768	1

Table 9 Command output

Field	Description
Loadsharing Type	Load sharing type: <ul style="list-style-type: none"> • Shar—Load-sharing. • NonS—Non-load-sharing.
Port Status	Port state: Selected, Unselected, or Individual.
Flags	LACP state flags. This field is one byte long, represented by ABCDEFGH from the least significant bit to the most significant bit. A letter appears when its bit is 1 and does not appear when its bit is 0.

Field	Description
	<ul style="list-style-type: none"> A—Indicates whether LACP is active on the port. 1 indicates active. 0 indicates passive. B—Indicates the LACP timeout interval. 1 indicates the short timeout interval. 0 indicates the long timeout interval. C—Indicates whether the sending system considers that the link is aggregatable. 1 indicates yes. 0 indicates no. D—Indicates whether the sending system considers that the link has been aggregated. 1 indicates yes. 0 indicates no. E—Indicates whether the sending system considers that the link can collect frames. 1 indicates yes. 0 indicates no. F—Indicates whether the sending system considers that the link can distribute frames. 1 indicates yes. 0 indicates no. G—Indicates whether the RX state machine of the sending system is in default state. 1 indicates yes. 0 indicates no. H—Indicates whether the RX state machine of the sending system is in expired state. 1 indicates yes. 0 indicates no.
Aggregate Interface	Name of the aggregate interface.
Aggregation Mode	Aggregation group type: <ul style="list-style-type: none"> S—Static. D—Dynamic.
System ID	Local system ID, containing the local system LACP priority and the local system MAC address.
Local	Information about the local end: <ul style="list-style-type: none"> Port—Port type and number. Status—Port state, which can be Selected, Unselected, or Individual. Priority—Port priority. Oper-Key—Operational key. Flag—LACP state flag. <p>NOTE: For static aggregation groups, the Flag field is not displayed.</p>
Remote	Information about the peer end: <ul style="list-style-type: none"> Actor—Type and number of the local port. Partner—Index of the peer port. Priority—Priority of the peer port. Oper-Key—Operational key of the peer port. System ID—System ID of the peer end. Flag—LACP state flag of the peer end.

interface bridge-aggregation

Use **interface bridge-aggregation** to create a Layer 2 aggregate interface and enter its view, or enter the view of an existing Layer 2 aggregate interface.

Use **undo interface bridge-aggregation** to delete a Layer 2 aggregate interface.

Syntax

interface bridge-aggregation *interface-number*

undo interface bridge-aggregation *interface-number*

Default

No Layer 2 aggregate interfaces exist.

Views

System view

Predefined user roles

network-admin

Parameters

interface-number. Specifies a Layer 2 aggregate interface number. The value range for the *interface-number* argument is 1 to 8.

Usage guidelines

When you create a Layer 2 aggregate interface, the system automatically creates a Layer 2 aggregation group with the same number. The aggregation group operates in static aggregation mode by default.

Deleting a Layer 2 aggregate interface also deletes the Layer 2 aggregation group. At the same time, the member ports of the aggregation group, if any, leave the aggregation group.

Examples

Create Layer 2 aggregate interface Bridge-Aggregation 1, and enter its view.

```
<Sysname> system-view
[Sysname] interface bridge-aggregation 1
[Sysname-Bridge-Aggregation1]
```

interface route-aggregation

Use **interface route-aggregation** to create a Layer 3 aggregate interface or subinterface and enter its view, or enter the view of an existing Layer 3 aggregate interface or subinterface.

Use **undo interface route-aggregation** to delete a Layer 3 aggregate interface or subinterface.

Syntax

interface route-aggregation { *interface-number* | *interface-number.subnumber* }

undo interface route-aggregation { *interface-number* | *interface-number.subnumber* }

Default

No Layer 3 aggregate interfaces or subinterfaces exist.

Views

System view

Predefined user roles

network-admin

Parameters

interface-number. Specifies a Layer 3 aggregate interface number. The value range for the *interface-number* argument is 1 to 8.

interface-number.subnumber. Specifies a subinterface of a Layer 3 aggregate interface. The *interface-number* argument specifies the main interface number. The *subnumber* argument specifies the subinterface number and is separated from the main interface number by a dot (.). The value range for the *interface-number* argument is 1 to 8, and the value range for the *subnumber* argument is 1 to 4094.

Usage guidelines

When you create a Layer 3 aggregate interface, the system automatically creates a Layer 3 aggregation group with the same number. The Layer 3 aggregation group operates in static aggregation mode by default.

Deleting a Layer 3 aggregate interface also deletes the Layer 3 aggregation group. At the same time, the member ports of the aggregation group, if any, leave the aggregation group.

Deleting a Layer 3 aggregate subinterface does not affect the state of the main interface and the corresponding aggregation group.

Examples

Create Layer 3 aggregate interface Route-Aggregation 1 and enter its view.

```
<Sysname> system-view
[Sysname] interface route-aggregation 1
[Sysname-Route-Aggregation1]
```

Create Layer 3 aggregate subinterface Route-Aggregation 1.1 and enter its view.

```
<Sysname> system-view
[Sysname] interface route-aggregation 1.1
[Sysname-Route-Aggregation1.1]
```

lACP edge-port

Use **lACP edge-port** to configure an aggregate interface as an edge aggregate interface.

Use **undo lACP edge-port** to restore the default.

Syntax

lACP edge-port

undo lACP edge-port

Default

An aggregate interface does not operate as an edge aggregate interface.

Views

Layer 2 aggregate interface view

Layer 3 aggregate interface view

Predefined user roles

network-admin

Usage guidelines

Use this command on the aggregate interface that connects the device to a server if dynamic link aggregation is configured only on the device. This feature improves link reliability by enabling all member ports of the aggregation group to forward packets.

This command takes effect only on an aggregate interface corresponding to a dynamic aggregation group.

Link-aggregation traffic redirection cannot operate correctly on an edge aggregate interface.

Examples

Configure Layer 2 aggregate interface Bridge-Aggregation 1 as an edge aggregate interface.

```
<Sysname> System-view
[Sysname] interface bridge-aggregation 1
[Sysname-Bridge-Aggregation1] lACP edge-port
```

lacp mode

Use **lacp mode passive** to configure LACP to operate in passive mode on a port.

Use **undo lacp mode** to restore the default.

Syntax

lacp mode passive

undo lacp mode

Default

LACP operates in active mode on a port.

Views

Layer 2 Ethernet interface view

Layer 3 Ethernet interface view

Predefined user roles

network-admin

Usage guidelines

When LACP is operating in passive mode on a local member port and its peer port, both ports cannot send LACPDU. When LACP is operating in active mode on either end of a link, both ports can send LACPDU.

This command takes effect only on member ports of dynamic aggregation groups.

Examples

```
# Configure LACP to operate in passive mode on GigabitEthernet 1/0/1.  
<Sysname> system-view  
[Sysname] interface gigabitethernet 1/0/1  
[Sysname-GigabitEthernet1/0/1] lacp mode passive
```

lacp period short

Use **lacp period short** to set the short LACP timeout interval (3 seconds) on an interface.

Use **undo lacp period** to restore the default.

Syntax

lacp period short

undo lacp period

Default

The LACP timeout interval is the long timeout interval (90 seconds) on an interface.

Views

Layer 2 Ethernet interface view

Layer 3 Ethernet interface view

Predefined user roles

network-admin

Usage guidelines

To avoid traffic interruption during an ISSU, do not set the short LACP timeout interval before performing the ISSU. For more information about ISSU, see *Fundamentals Configuration Guide*.

Examples

```
# Set the short LACP timeout interval (3 seconds) on GigabitEthernet 1/0/1.
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] lacp period short
```

lacp system-priority

Use **lacp system-priority** to set the system LACP priority.

Use **undo lacp system-priority** to restore the default.

Syntax

```
lacp system-priority priority
undo lacp system-priority
```

Default

The system LACP priority is 32768.

Views

System view

Predefined user roles

network-admin

Parameters

priority. Specifies the system LACP priority in the range of 0 to 65535. The smaller the value, the higher the system LACP priority.

Examples

```
# Set the system LACP priority to 64.
<Sysname> system-view
[Sysname] lacp system-priority 64
```

Related commands

```
link-aggregation port-priority
```

link-aggregation global load-sharing mode

Use **link-aggregation global load-sharing mode** to set the global link-aggregation load sharing mode.

Use **undo link-aggregation global load-sharing mode** to restore the default.

Syntax

```
link-aggregation global load-sharing mode { destination-ip | destination-mac | destination-port | mpls-label1 | source-ip | source-mac | source-port }*
undo link-aggregation global load-sharing mode
```

Views

System view

Predefined user roles

network-admin

Parameters

destination-ip: Load shares traffic based on destination IP addresses.

destination-mac: Load shares traffic based on destination MAC addresses.

The following matrix shows the **destination-mac** keyword and hardware compatibility:

Hardware	Keyword compatibility
MSR954 (JH296A/JH297A/JH298A/JH299A/JH373A)	No
MSR958 (JH300A/JH301A)	No
MSR1002-4/1003-8S	No
MSR2003	No
MSR2004-24/2004-48	No
MSR3012/3024/3044/3064	Yes
MSR4060/4080	Yes

destination-port: Load shares traffic based on destination ports.

mpls-label1: Load shares MPLS traffic based on Layer 1 labels.

The following matrix shows the **mpls-label1** keyword and hardware compatibility:

Hardware	Keyword compatibility
MSR954 (JH296A/JH297A/JH298A/JH299A/JH373A)	No
MSR958 (JH300A/JH301A)	No
MSR1002-4/1003-8S	No
MSR2003	No
MSR2004-24/2004-48	No
MSR3012/3024/3044/3064	Yes
MSR4060/4080	Yes

source-ip: Load shares traffic based on source IP addresses.

source-mac: Load shares traffic based on source MAC addresses.

The following matrix shows the **source-mac** keyword and hardware compatibility:

Hardware	Keyword compatibility
MSR954 (JH296A/JH297A/JH298A/JH299A/JH373A)	No
MSR958 (JH300A/JH301A)	No
MSR1002-4/1003-8S	No
MSR2003	No
MSR2004-24/2004-48	No
MSR3012/3024/3044/3064	Yes
MSR4060/4080	Yes

source-port: Load shares traffic based on source ports.

Usage guidelines

If you execute this command multiple times, the most recent configuration takes effect.

If an unsupported load sharing mode is set, an error prompt appears.

Examples

```
# Set the global load sharing mode to load share packets based on destination MAC addresses.
<Sysname> system-view
[Sysname] link-aggregation global load-sharing mode destination-mac
```

Related commands

link-aggregation load-sharing mode

link-aggregation ignore vlan

Use **link-aggregation ignore vlan** to configure a Layer 2 aggregate interface to ignore the specified VLANs.

Use **undo link-aggregation ignore vlan** to remove the specified ignored VLANs for a Layer 2 aggregate interface.

Syntax

```
link-aggregation ignore vlan vlan-id-list
undo link-aggregation ignore vlan vlan-id-list
```

Default

A Layer 2 aggregate interface does not ignore any VLANs.

Views

Layer 2 aggregate interface view

Predefined user roles

network-admin

Parameters

vlan-id-list: Specifies a space-separated list of up to 10 VLAN items. Each item specifies a VLAN ID or a range of VLAN IDs in the form of *vlan-id1* to *vlan-id2*. The value range for VLAN IDs is 1 to 4094. The value for *vlan-id2* must be equal to or greater than the value for *vlan-id1*.

Usage guidelines

With this command configured, a Layer 2 aggregate interface ignores the permitted VLAN and VLAN tagging mode configuration of the specified VLANs when choosing Selected ports.

Examples

```
# Configure Layer 2 aggregate interface bridge-aggregation 1 to ignore VLAN 50.
<Sysname> system-view
[Sysname] interface bridge-aggregation 1
[Sysname-Bridge-Aggregation1] link-aggregation ignore vlan 50
```

link-aggregation lacp traffic-redirect-notification enable

Use **link-aggregation lacp traffic-redirect-notification enable** to enable link-aggregation traffic redirection.

Use **undo link-aggregation lacp traffic-redirect-notification enable** to disable link-aggregation traffic redirection.

Syntax

link-aggregation lacp traffic-redirect-notification enable

undo link-aggregation lacp traffic-redirect-notification enable

Default

Link-aggregation traffic redirection is disabled.

Views

Layer 3 aggregate interface view

Predefined user roles

network-admin

Usage guidelines

When you shut down a Selected port in an aggregation group, this feature redirects traffic of the port to other Selected ports. Zero packet loss is guaranteed for known unicast traffic, but not for unknown unicast traffic. (Centralized devices in standalone mode.)

When you restart a card that contains Selected ports, this feature redirects traffic of the card to other cards. Zero packet loss is guaranteed for known unicast traffic, but not for unknown unicast traffic. (Distributed devices in standalone mode.)

When you restart an IRF member device that contains Selected ports, this feature redirects traffic of the IRF member device to other IRF member devices. Zero packet loss is guaranteed for known unicast traffic, but not for unknown unicast traffic. (Centralized devices in IRF mode.)

When you restart an IRF member device that contains Selected ports, this feature redirects traffic of the IRF member device to other IRF member devices. When you restart a card that contains Selected ports, this feature redirects traffic of the card to other cards. Zero packet loss is guaranteed for known unicast traffic, but not for unknown unicast traffic. (Distributed devices in IRF mode.)

Link-aggregation traffic redirection applies only to dynamic link aggregation groups.

To prevent traffic interruption, enable link-aggregation traffic redirection on devices at both ends of the aggregate link.

Do not enable both spanning tree and link-aggregation traffic redirection on a device. Otherwise, light packet loss might occur when a card or the device reboots.

Link-aggregation traffic redirection cannot operate correctly on an edge aggregate interface.

Examples

Enable link-aggregation traffic redirection.

```
<Sysname> system-view
```

```
[Sysname] interface route-aggregation 1
```

```
[Sysname-Route-Aggregation1] link-aggregation lacp traffic-redirect-notification enable
```

link-aggregation load-sharing mode

Use **link-aggregation load-sharing mode** to set the link-aggregation load sharing mode for an aggregation group.

Use **undo link-aggregation load-sharing mode** to restore the default.

Syntax

link-aggregation load-sharing mode { { **destination-ip** | **destination-port** | **source-ip** | **source-port** } * | **per-packet** }

undo link-aggregation load-sharing mode

Views

Layer 3 aggregate interface view

Predefined user roles

network-admin

Parameters

destination-ip: Load shares traffic based on destination IP addresses.

destination-port: Load shares traffic based on destination ports.

source-ip: Load shares traffic based on source IP addresses.

source-port: Load shares traffic based on source ports.

per-packet: Load shares traffic on a per-packet basis.

Usage guidelines

If you execute this command multiple times, the most recent configuration takes effect.

If an unsupported load sharing mode is set, an error prompt appears.

Examples

```
# Configure Layer 3 aggregation group 1 to load share packets based on destination IP addresses.
<Sysname> system-view
[Sysname] interface route-aggregation 1
[Sysname-Route-Aggregation1] link-aggregation load-sharing mode destination-ip
```

Related commands

link-aggregation global load-sharing mode

link-aggregation load-sharing mode local-first

Use **link-aggregation load-sharing mode local-first** to enable local-first load sharing for link aggregation.

Use **undo link-aggregation load-sharing mode local-first** to disable local-first load sharing for link aggregation.

Syntax

link-aggregation load-sharing mode local-first

undo link-aggregation load-sharing mode local-first

Default

Local-first load sharing is enabled for link aggregation.

Views

System view

Predefined user roles

network-admin

Usage guidelines

The following matrix shows the command and hardware compatibility:

Hardware	Command compatibility
MSR954 (JH296A/JH297A/JH298A/JH299A/JH373A)	No
MSR958 (JH300A/JH301A)	No
MSR1002-4/1003-8S	No
MSR2003	Yes
MSR2004-24/2004-48	Yes
MSR3012/3024/3044/3064	Yes
MSR4060/4080	Yes

After you disable local-first load sharing, the packets will be load shared among all Selected ports of the aggregate interface on all IRF member devices.

Examples

Disable local-first load sharing for link aggregation.

```
<Sysname> system-view
[Sysname] undo link-aggregation load-sharing mode local-first
```

link-aggregation mode

Use **link-aggregation mode dynamic** to configure an aggregation group to operate in dynamic aggregation mode and enable LACP.

Use **undo link-aggregation mode** to restore the default.

Syntax

link-aggregation mode dynamic

undo link-aggregation mode

Default

An aggregation group operates in static aggregation mode.

Views

Layer 2 aggregate interface view

Layer 3 aggregate interface view

Predefined user roles

network-admin

Examples

Configure Layer 2 aggregation group 1 to operate in dynamic aggregation mode.

```
<Sysname> system-view
[Sysname] interface bridge-aggregation 1
[Sysname-Bridge-Aggregation1] link-aggregation mode dynamic
```

link-aggregation port-priority

Use **link-aggregation port-priority** to set the port priority of an interface.

Use **undo link-aggregation port-priority** to restore the default.

Syntax

link-aggregation port-priority *priority*
undo link-aggregation port-priority

Default

The port priority of an interface is 32768.

Views

Layer 2 Ethernet interface view
Layer 3 Ethernet interface view

Predefined user roles

network-admin

Parameters

priority. Specifies the port priority in the range of 0 to 65535. The smaller the value, the higher the port priority.

Examples

Set the port priority to 64 for Layer 2 Ethernet interface GigabitEthernet 1/0/1.

```
<Sysname> system-view  
[Sysname] interface gigabitethernet 1/0/1  
[Sysname-GigabitEthernet1/0/1] link-aggregation port-priority 64
```

Set the port priority to 64 for Layer 3 Ethernet interface GigabitEthernet 1/0/2.

```
<Sysname> system-view  
[Sysname] interface gigabitethernet 1/0/2  
[Sysname-GigabitEthernet1/0/2] link-aggregation port-priority 64
```

Related commands

lacp system-priority

link-aggregation selected-port maximum

Use **link-aggregation selected-port maximum** to set the maximum number of Selected ports allowed in an aggregation group.

Use **undo link-aggregation selected-port maximum** to restore the default.

Syntax

link-aggregation selected-port maximum *max-number*
undo link-aggregation selected-port maximum

Default

The maximum number of Selected ports allowed in an aggregation group depends on hardware limitation.

Views

Layer 2 aggregate interface view
Layer 3 aggregate interface view

Predefined user roles

network-admin

Parameters

max-number. Specifies the maximum number of Selected ports allowed in an aggregation group. The value range for this argument is 1 to 8.

Usage guidelines

Executing this command might cause some of the Selected ports in an aggregation group to become Unselected ports.

The maximum number of Selected ports allowed in the aggregation groups must be the same for the local and peer ends.

The maximum number of Selected ports allowed in an aggregation group is limited by one of the following values, whichever value is smaller:

- Maximum number set by using the **link-aggregation selected-port maximum** command.
- Hardware limitation.

Examples

```
# Set the maximum number of Selected ports to 5 for Layer 2 aggregation group 1.
```

```
<Sysname> system-view
```

```
[Sysname] interface bridge-aggregation 1
```

```
[Sysname-Bridge-Aggregation1] link-aggregation selected-port maximum 5
```

Related commands

link-aggregation selected-port minimum

link-aggregation selected-port minimum

Use **link-aggregation selected-port minimum** to set the minimum number of Selected ports in an aggregation group.

Use **undo link-aggregation selected-port minimum** to restore the default.

Syntax

link-aggregation selected-port minimum *min-number*

undo link-aggregation selected-port minimum

Default

The minimum number of Selected ports in an aggregation group is not specified.

Views

Layer 2 aggregate interface view

Layer 3 aggregate interface view

Predefined user roles

network-admin

Parameters

min-number. Specifies the minimum number of Selected ports in an aggregation group required to bring up the aggregate interface. The value range for this argument is 1 to 8.

Usage guidelines

Executing this command might cause all member ports in the aggregation group to become Unselected ports.

The minimum number of Selected ports allowed in the aggregation groups must be the same for the local and peer ends.

Examples

```
# Set the minimum number of Selected ports to 3 for Layer 2 aggregation group 1.
<Sysname> system-view
[Sysname] interface bridge-aggregation 1
[Sysname-Bridge-Aggregation1] link-aggregation selected-port minimum 3
```

Related commands

link-aggregation selected-port maximum

mtu

Use **mtu** to set the MTU for a Layer 3 aggregate interface or subinterface.

Use **undo mtu** to restore the default.

Syntax

mtu *size*

undo mtu

Default

The MTU for Layer 3 aggregate interfaces and subinterfaces is 1500 bytes.

Views

Layer 3 aggregate interface view

Layer 3 aggregate subinterface view

Predefined user roles

network-admin

Parameters

size: Specifies the MTU in bytes. The value range is 46 to 1560.

Examples

```
# Set the MTU to 1430 bytes for Layer 3 aggregate interface Route-Aggregation 1.
<Sysname> system-view
[Sysname] interface route-aggregation 1
[Sysname-Route-Aggregation1] mtu 1430
```

Related commands

display interface

port link-aggregation group

Use **port link-aggregation group** to assign an interface to an aggregation group.

Use **undo port link-aggregation group** to remove an interface from the aggregation group to which it belongs.

Syntax

port link-aggregation group *group-id*

undo port link-aggregation group

Default

An interface does not belong to any aggregation group.

Views

Layer 2 Ethernet interface view

Layer 3 Ethernet interface view

Predefined user roles

network-admin

Parameters

group-id: Specifies an aggregation group by its aggregate interface number. The value range for the *number* argument is 1 to 8.

Usage guidelines

A Layer 2 Ethernet interface can be assigned to a Layer 2 aggregation group only. A Layer 3 Ethernet interface can be assigned to a Layer 3 aggregation group only.

An interface can belong to only one aggregation group.

Examples

Assign Layer 2 Ethernet interface GigabitEthernet 1/0/1 to Layer 2 aggregation group 1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] port link-aggregation group 1
```

Assign Layer 3 Ethernet interface GigabitEthernet 1/0/2 to Layer 3 aggregation group 2.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/2
[Sysname-GigabitEthernet1/0/2] port link-aggregation group 2
```

reset counters interface

Use **reset counters interface** to clear statistics for the specified aggregate interfaces.

Syntax

```
reset counters interface [ { bridge-aggregation | route-aggregation } [ interface-number ] ]
```

Views

User view

Predefined user roles

network-admin

Parameters

bridge-aggregation: Specifies Layer 2 aggregate interfaces.

route-aggregation: Specifies Layer 3 aggregate interfaces.

interface-number: Specifies an aggregate interface number. The value range for the *interface-number* argument is 1 to 8.

Usage guidelines

Use this command to clear history statistics before you collect traffic statistics for a time period.

If you do not specify any parameters, the command clears statistics for all interfaces in the system.

If you specify the **bridge-aggregation** or **route-aggregation** keyword but do not specify an interface number, the command clears statistics for all aggregate interfaces of the specified type.

If you specify the **bridge-aggregation** *interface-number* or **route-aggregation** *interface-number* option, the command clears statistics for the specified aggregate interface.

The **bridge-aggregation** or **route-aggregation** keyword is available only when the corresponding aggregate interfaces exist on the device.

Examples

```
# Clear statistics for Layer 2 aggregate interface Bridge-Aggregation 1.
```

```
<Sysname> reset counters interface bridge-aggregation 1
```

reset lacp statistics

Use **reset lacp statistics** to clear LACP statistics for the specified link aggregation member ports.

Syntax

```
reset lacp statistics [ interface interface-list ]
```

Views

User view

Predefined user roles

network-admin

Parameters

interface *interface-list*: Specifies a list of link aggregation member ports, in the format *interface-type interface-number* [**to** *interface-type interface-number*]. The *interface-type interface-number* argument specifies an interface by its type and number. If you do not specify any member ports, the command clears LACP statistics for all member ports.

Examples

```
# Clear LACP statistics for all link aggregation member ports.
```

```
<Sysname> reset lacp statistics
```

Related commands

```
display link-aggregation member-port
```

service

Use **service** to specify a primary traffic processing slot for an interface.

Use **undo service** to restore the default.

Syntax

Distributed devices in standalone mode/centralized devices in IRF mode:

```
service slot slot-number
```

```
undo service slot
```

Distributed devices in IRF mode:

```
service chassis chassis-number slot slot-number
```

```
undo service chassis
```

Default

No primary traffic processing slot is specified for an interface.

Views

Layer 3 aggregate interface view

Predefined user roles

network-admin

Parameters

slot *slot-number*. Specifies a card by its slot number. (Distributed devices in standalone mode.)

slot *slot-number*. Specifies an IRF member device by its member ID. (Centralized devices in IRF mode.)

chassis *chassis-number* **slot** *slot-number*. Specifies a card on an IRF member device. The *chassis-number* argument represents the member ID of the IRF member device. The *slot-number* argument represents the slot number of the card. (Distributed devices in IRF mode.)

Usage guidelines

The following matrix shows the command and hardware compatibility:

Hardware	Command compatibility
MSR954 (JH296A/JH297A/JH298A/JH299A/JH373A)	No
MSR958 (JH300A/JH301A)	No
MSR1002-4/1003-8S	No
MSR2003	Yes
MSR2004-24/2004-48	Yes
MSR3012/3024/3044/3064	Yes
MSR4060/4080	Yes

This command is supported on distributed devices and IRF-capable centralized devices.

Specify a traffic processing slot for all traffic on a Layer 3 aggregate interface to be processed on the same slot. If the aggregate interface contains subinterfaces, traffic on the subinterfaces is also processed on the specified slot.

For high availability, you can specify one primary and one backup traffic processing slot by using the **service** command and the **service standby** command, respectively.

To avoid processing slot switchover, specify the primary slot before specifying the backup slot. If you specify the backup slot before specifying the primary slot, traffic is switched over to the primary slot immediately after you specify the primary slot.

If you specify both primary and backup slots for an interface, traffic on that interface is processed as follows:

- The backup slot takes over when the primary slot becomes unavailable. The backup slot continues to process traffic for the interface after the primary slot becomes available again. The switchover will not occur until the backup slot becomes unavailable.
- When no specified traffic processing slots are available, the traffic is processed on the slot at which it arrives. Then, the processing slot that first becomes available again takes over.

If you do not specify a primary or a backup traffic processing slot for an interface, traffic on that interface is processed on the slot at which the traffic arrives.

Examples

(Distributed devices in standalone mode.) Specify a primary traffic processing slot for Layer 3 aggregate interface Route-Aggregation 1.

```
<Sysname> system-view
```

```
[Sysname] interface route-aggregation 1
[Sysname-Route-Aggregation1] service slot 2
```

Related commands

service standby

service standby

Use **service standby** to specify a backup traffic processing slot for an interface.

Use **undo service standby** to restore the default.

Syntax

Distributed devices in standalone mode/centralized devices in IRF mode:

service standby slot *slot-number*

undo service standby slot

Distributed devices in IRF mode:

service standby chassis *chassis-number* **slot** *slot-number*

undo service standby chassis

Default

No backup traffic processing slot is specified for an interface.

Views

Layer 3 aggregate interface view

Predefined user roles

network-admin

Parameters

slot *slot-number*. Specifies a card by its slot number. (Distributed devices in standalone mode.)

slot *slot-number*. Specifies an IRF member device by its member ID. (Centralized devices in IRF mode.)

chassis *chassis-number* **slot** *slot-number*. Specifies a card on an IRF member device. The *chassis-number* argument represents the member ID of the IRF member device. The *slot-number* argument represents the slot number of the card. (Distributed devices in IRF mode.)

Usage guidelines

The following matrix shows the command and hardware compatibility:

Hardware	Command compatibility
MSR954 (JH296A/JH297A/JH298A/JH299A/JH373A)	No
MSR958 (JH300A/JH301A)	No
MSR1002-4/1003-8S	No
MSR2003	Yes
MSR2004-24/2004-48	Yes
MSR3012/3024/3044/3064	Yes
MSR4060/4080	Yes

This command is supported on distributed devices and IRF-capable centralized devices.

Specify a traffic processing slot for all traffic on a Layer 3 aggregate interface to be processed on the same slot. If the aggregate interface contains subinterfaces, traffic on the subinterfaces is also processed on the specified slot.

For high availability, you can specify one primary and one backup traffic processing slot by using the **service** command and the **service standby** command, respectively.

To avoid processing slot switchover, specify the primary slot before specifying the backup slot. If you specify the backup slot before specifying the primary slot, traffic is switched over to the primary slot immediately after you specify the primary slot.

If you specify both primary and backup slots for an interface, traffic on that interface is processed as follows:

- The backup slot takes over when the primary slot becomes unavailable. The backup slot continues to process traffic for the interface after the primary slot becomes available again. The switchover will not occur until the backup slot becomes unavailable.
- When no specified traffic processing slots are available, the traffic is processed on the slot at which it arrives. Then, the processing slot that first becomes available again takes over.

If you do not specify a primary or a backup traffic processing slot for an interface, traffic on that interface is processed on the slot at which the traffic arrives.

Examples

(Distributed devices in standalone mode.) Specify a primary and a backup traffic processing slots for Layer 3 aggregate interface Route-Aggregation 1.

```
<Sysname> system-view
[Sysname] interface route-aggregation 1
[Sysname-Route-Aggregation1] service slot 2
[Sysname-Route-Aggregation1] service standby slot 3
```

Related commands

service

shutdown

Use **shutdown** to shut down an aggregate interface or subinterface.

Use **undo shutdown** to bring up an aggregate interface or subinterface.

Syntax

shutdown

undo shutdown

Default

An aggregate interface or subinterface is up.

Views

Layer 2 aggregate interface view

Layer 3 aggregate interface view

Layer 3 aggregate subinterface view

Predefined user roles

network-admin

Usage guidelines

Shutting down or bringing up a Layer 3 aggregate interface shuts down or brings up its subinterfaces. Shutting down or bringing up a Layer 3 aggregate subinterface does not affect its main interface.

Examples

Bring up Layer 2 aggregate interface Bridge-Aggregation 1.

```
<Sysname> system-view
```

```
[Sysname] interface bridge-aggregation 1
```

```
[Sysname-Bridge-Aggregation1] undo shutdown
```

Port isolation commands

The port isolation feature is not supported on Layer 2 Ethernet ports of the following Ethernet switching modules:

- SIC-4FSW.
- SIC-4FSW-PoE.

display port-isolate group

Use **display port-isolate group** to display port isolation group information.

Syntax

```
display port-isolate group
```

Views

Any view

Predefined user roles

network-admin

network-operator

Examples

```
# Display port isolation group information.
```

```
<Sysname> display port-isolate group
```

```
Port isolation group information:
```

```
Group ID: 1
```

```
Group members:
```

```
GigabitEthernet1/0/2
```

Table 10 Command output

Field	Description
Group ID	ID of the isolation group.
Group members	Isolated ports in the isolation group. No ports indicates that the isolation group contains no isolated ports.

Related commands

```
port-isolate enable
```

port-isolate enable

Use **port-isolate enable** to assign a port to the isolation group.

Use **undo port-isolate enable** to remove a port from the isolation group.

Syntax

```
port-isolate enable
```

```
undo port-isolate enable
```

Default

The port is not assigned to the isolation group.

Views

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

Predefined user roles

network-admin

Usage guidelines

The configuration in Layer 2 Ethernet interface view applies only to the interface.

The configuration in Layer 2 aggregate interface view applies to the Layer 2 aggregate interface and its aggregation member ports. If the device fails to apply the configuration to the aggregate interface, it does not assign any aggregation member port to the isolation group. If the failure occurs on an aggregation member port, the device skips the port and continues to assign other aggregation member ports to the isolation group.

Examples

Assign GigabitEthernet 1/0/1 and GigabitEthernet 1/0/2 to the isolation group.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] port-isolate enable
[Sysname-GigabitEthernet1/0/1] quit
[Sysname] interface gigabitethernet 1/0/2
[Sysname-GigabitEthernet1/0/2] port-isolate enable
```

Assign Layer 2 aggregate interface Bridge-Aggregation 1 to the isolation group.

```
<Sysname> system-view
[Sysname] interface bridge-aggregation 1
[Sysname-Bridge-Aggregation1] quit
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] port link-aggregation group 1
[Sysname-GigabitEthernet1/0/1] quit
[Sysname] interface gigabitethernet 1/0/2
[Sysname-GigabitEthernet1/0/2] port link-aggregation group 1
[Sysname-GigabitEthernet1/0/2] quit
[Sysname] interface bridge-aggregation 1
[Sysname-Bridge-Aggregation1] port-isolate enable
```

Related commands

display port-isolate group

VLAN commands

This feature is supported only on the following ports:

- Layer 2 Ethernet ports on Ethernet switching modules.
- Fixed Layer 2 Ethernet ports of the following routers:
 - MSR954 (JH296A/JH297A/JH298A/JH299A/JH373A).
 - MSR958 (JH300A/JH301A).
 - MSR1002-4/1003-8S.
 - MSR2004-24/2004-48.

Basic VLAN commands

bandwidth

Use **bandwidth** to set the expected bandwidth of an interface.

Use **undo bandwidth** to restore the default.

Syntax

bandwidth *bandwidth-value*

undo bandwidth

Default

The expected bandwidth (in kbps) is the interface baud rate divided by 1000.

Views

VLAN interface view

Predefined user roles

network-admin

Parameters

bandwidth-value: Specifies the expected bandwidth in the range of 1 to 400000000 kbps.

Usage guidelines

The expected bandwidth is an informational parameter used only by higher-layer protocols for calculation. You cannot adjust the actual bandwidth of an interface by using this command.

Examples

```
# Set the expected bandwidth to 10000 kbps for VLAN-interface 1.
```

```
<Sysname> system-view  
[Sysname] interface vlan-interface 1  
[Sysname-Vlan-interface1] bandwidth 10000
```

default

Use **default** to restore the default settings for a VLAN interface.

Syntax

default

Views

VLAN interface view

Predefined user roles

network-admin

Usage guidelines

CAUTION:

The **default** command might interrupt ongoing network services. Make sure you are fully aware of the impact of this command when you use it on a live network.

This command might fail to restore the default settings for some commands for reasons such as command dependencies or system restrictions. Use the **display this** command in interface view to identify these commands, and then use their **undo** forms or follow the command reference to restore their default settings. If your restoration attempt still fails, follow the error message instructions to resolve the problem.

Examples

Restore the default settings for VLAN-interface 1.

```
<Sysname> system-view
[Sysname] interface vlan-interface 1
[Sysname-Vlan-interface1] default
```

description

Use **description** to set the description for a VLAN or VLAN interface.

Use **undo description** to restore the default.

Syntax

description *text*

undo description

Default

For a VLAN, the description is **VLAN** *vlan-id*. The *vlan-id* argument specifies the VLAN ID in a four-digit format. If the VLAN ID has fewer than four digits, leading zeros are added. For example, the default description of VLAN 100 is **VLAN 0100**.

For a VLAN interface, the description is the name of the interface. For example, **Vlan-interface1 Interface**.

Views

VLAN view

VLAN interface view

Predefined user roles

network-admin

Parameters

text: Specifies a description, a case-sensitive string of 1 to 255 characters.

Usage guidelines

To manage VLANs and VLAN interfaces efficiently, configure descriptions for them based on their functions or connections.

Examples

```
# Set the description of VLAN 2 to sales-private.
<Sysname> system-view
[Sysname] vlan 2
[Sysname-vlan2] description sales-private

# Set the description of VLAN-interface 2 to linktoPC56.
<Sysname> system-view
[Sysname] vlan 2
[Sysname-vlan2] quit
[Sysname] interface vlan-interface 2
[Sysname-Vlan-interface2] description linktoPC56
```

Related commands

```
display interface vlan-interface
display vlan
```

display interface vlan-interface

Use **display interface vlan-interface** to display VLAN interface information.

Syntax

```
display interface vlan-interface [ interface-number ] [ brief [ description | down ] ]
```

Views

Any view

Predefined user roles

```
network-admin
network-operator
```

Parameters

vlan-interface: Specifies VLAN interfaces.

interface-number: Specifies a VLAN interface number. If you do not specify this argument, the command displays information about all VLAN interfaces.

brief: Displays brief interface information. If you do not specify this keyword, the command displays detailed interface information.

description: Displays complete interface descriptions. If you do not specify this keyword, the command displays only the first 27 characters of each interface description.

down: Displays VLAN interfaces in down state and their down causes. If you do not specify this keyword, the command displays information about VLAN interfaces in all states.

Examples

```
# Display information about VLAN-interface 2.
<Sysname> display interface vlan-interface 2
Vlan-interface2
Current state: DOWN
Line protocol state: DOWN
Description: Vlan-interface2 Interface
Bandwidth: 100000kbps
Maximum transmission unit: 1500
```

```

Internet protocol processing : Disabled
IP packet frame type: PKTFMT_ETHNT_2, hardware address: 000f-e249-8050
IPv6 packet frame type: PKTFMT_ETHNT_2, hardware address: 000f-e249-8050
Output queue - Urgent queuing: Size/Length/Discards 0/100/0
Output queue - Protocol queuing: Size/Length/Discards 0/500/0
Output queue - FIFO queuing: Size/Length/Discards 0/75/0
Last clearing of counters: Never
Last 300 seconds input rate: 0 bytes/sec, 0 bits/sec, 0 packets/sec
Last 300 seconds output rate: 0 bytes/sec, 0 bits/sec, 0 packets/sec
Input: 0 packets, 0 bytes, 0 drops
Output: 0 packets, 0 bytes, 0 drops

```

Display brief information about VLAN-interface 2.

```

<Sysname> display interface vlan-interface 2 brief
Brief information on interfaces in route mode:
Link: ADM - administratively down; Stby - standby
Protocol: (s) - spoofing
Interface          Link Protocol Primary IP          Description
Vlan2              DOWN DOWN          --

```

Table 11 Command output

Field	Description
Vlan-interface2	VLAN interface name.
Current state	Physical state of the VLAN interface: <ul style="list-style-type: none"> • DOWN (Administratively)—The administrative state of the VLAN interface is down, because it has been shut down by using the shutdown command. • DOWN—The administrative state of the VLAN interface is up, but its physical state is down. The VLAN of this VLAN interface does not contain any physical ports in up state. The ports might not be connected correctly or the lines might have failed. • UP—Both the administrative state and the physical state of the VLAN interface are up.
Line protocol state	Link layer protocol state of the VLAN interface: <ul style="list-style-type: none"> • DOWN—The link layer protocol state of the VLAN interface is down. • UP—The link layer protocol state of the VLAN interface is up.
Description	Partial or complete VLAN interface description configured by using the description command: <ul style="list-style-type: none"> • If you do not specify the description keyword in the display interface brief command, this field displays the first 27 characters of the interface description. • If you specify the description keyword in the display interface brief command, this field displays the complete interface description.
Bandwidth	Expected bandwidth of the VLAN interface.
Maximum transmission unit	MTU of the VLAN interface.
Internet protocol processing : Disabled	The interface is not assigned an IP address and cannot process IP packets.

Field	Description
Internet address is 192.168.1.54/24 (primary)	The primary IP address of the interface is 192.168.1.54/24. This field is displayed only when the primary IP address is configured for the interface.
IP packet frame type	Framing format of sent IPv4 packets.
hardware address	MAC address of the VLAN interface.
IPv6 packet frame type	Framing format of sent IPv6 packets.
Output queue - Urgent queuing: Size/Length/Discards 0/100/0 Output queue - Protocol queuing: Size/Length/Discards 0/500/0 Output queue - FIFO queuing: Size/Length/Discards 0/75/0	Information about the urgent, protocol, and FIFO output queues: <ul style="list-style-type: none"> • Size—Number of packets in the queue. • Length—Maximum number of packets that the queue can contain. • Discards—Number of dropped packets.
Last clearing of counters	The most recent time that the reset counters interface command was executed. This field displays Never if you have never executed this command.
Last 300 seconds input rate: 0 bytes/sec, 0 bits/sec, 0 packets/sec Last 300 seconds output rate: 0 bytes/sec, 0 bits/sec, 0 packets/sec	Average rates of input packets and output packets in the last 300 seconds (in Bps, bps, and pps).
Input: 0 packets, 0 bytes, 0 drops	Total number and size (in bytes) of the received packets of the interface and the number of the dropped packets.
Output: 0 packets, 0 bytes, 0 drops	Total number and size (in bytes) of the sent packets of the interface and the number of the dropped packets.
Brief information on interfaces in route mode	Brief information about Layer 3 interfaces.
Link: ADM - administratively down; Stby - standby	Link layer state of the interface: <ul style="list-style-type: none"> • ADM—The interface has been administratively shut down. To bring up the interface, use the undo shutdown command. • Stby—The interface is operating as a backup interface. To see the primary interface, use the display interface-backup state command.
Protocol: (s) - spoofing	The protocol attribute of an interface includes the spoofing flag (the letter s in parentheses) when the following conditions exist: <ul style="list-style-type: none"> • The data link layer protocol state of an interface is shown as UP. • Its link is an on-demand link or is not present.
Interface	Abbreviated interface name.
Link	Physical link state of the interface: <ul style="list-style-type: none"> • UP—The interface is physically up. • DOWN—The interface is physically down. • ADM—The interface has been administratively shut down. To bring up the interface, use the undo shutdown command. • Stby—The interface is operating as a backup interface.
Protocol	Data link layer protocol state of the interface: <ul style="list-style-type: none"> • UP—The data link layer protocol state of the interface is up. • DOWN—The data link layer protocol state of the interface is

Field	Description
	down. <ul style="list-style-type: none"> UP(s)—The data link layer protocol state of an interface is shown as UP, but its link is an on-demand link or not present at all.
Primary IP	Primary IP address of the interface.

Related commands

reset counters interface vlan-interface

display vlan

Use **display vlan** to display VLAN information.

Syntax

display vlan [*vlan-id1* [**to** *vlan-id2*]] | **all** | **dynamic** | **reserved** | **static**]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

vlan-id1: Specifies a VLAN by its ID in the range of 1 to 4094.

vlan-id1 to vlan-id2: Specifies a VLAN ID range. Both the *vlan-id1* and the *vlan-id2* arguments are in the range of 1 to 4094. The value for the *vlan-id2* argument must be equal to or greater than the value for the *vlan-id1* argument.

all: Specifies all VLANs except the reserved VLANs.

dynamic: Specifies dynamic VLANs. If you specify this keyword, the command displays the total number of dynamic VLANs and each dynamic VLAN ID. Dynamic VLANs are assigned by a RADIUS server.

reserved: Specifies reserved VLANs. Protocol modules determine which VLANs are reserved according to function implementation. The reserved VLANs provide services for protocol modules. You cannot configure reserved VLANs.

static: Specifies static VLANs. If you specify this keyword, the command displays the total number of static VLANs and each static VLAN ID. Static VLANs are manually created.

Examples

Display information about VLAN 2.

```
<Sysname> display vlan 2
VLAN ID: 2
VLAN type: Static
Route interface: Not configured
Description: VLAN 0002
Name: VLAN 0002
Tagged ports:   None
Untagged ports:
    GigabitEthernet1/0/1  GigabitEthernet1/0/2
```

```

GigabitEthernet1/0/3
# Display information about VLAN 3.
<Sysname> display vlan 3
VLAN ID: 3
VLAN type: static
Route interface: Configured
IPv4 address: 1.1.1.1
IPv4 subnet mask: 255.255.255.0
Description: VLAN 0003
Name: VLAN 0003
Tagged ports: None
Untagged ports: None

```

Table 12 Command output

Field	Description
VLAN type	VLAN type, static or dynamic.
Route interface	Whether the VLAN interface is configured for the VLAN. <ul style="list-style-type: none"> Not configured. Configured.
Description	Description of the VLAN.
Name	VLAN name.
IP address	Primary IPv4 address of the VLAN interface. This field is displayed only when an IPv4 address is configured for the VLAN interface. When the VLAN interface is also configured with secondary IPv4 addresses, you can view them by using one of the following commands: <ul style="list-style-type: none"> display interface vlan-interface. display this (VLAN interface view).
Subnet mask	Subnet mask of the primary IP address. This field is available only when an IP address is configured for the VLAN interface.
Tagged ports	Tagged members of the VLAN.
Untagged ports	Untagged members of the VLAN.

Related commands

vlan

display vlan brief

Use **display vlan brief** to display brief VLAN information.

Syntax

display vlan brief

Views

Any view

Predefined user roles

network-admin
network-operator

Examples

Display brief VLAN information.

```
<Sysname> display vlan brief
Brief information about all VLANs:
Supported Minimum VLAN ID: 1
Supported Maximum VLAN ID: 4094
Default VLAN ID: 1
VLAN ID   Name                               Port
1         VLAN 0001                            GE1/0/1  GE1/0/2  GE1/0/3  GE1/0/4
                                                GE1/0/5  GE1/0/6  GE1/0/7  GE1/0/8
                                                GE1/0/9  GE1/0/10 GE1/0/11
                                                GE1/0/12 GE1/0/13 GE1/0/14
                                                GE1/0/15 GE1/0/16 GE1/0/17
                                                GE1/0/18 GE1/0/19 GE1/0/20
                                                GE1/0/21 GE1/0/22 GE1/0/23
                                                GE1/0/24 GE1/0/25 GE1/0/26
                                                GE1/0/27 GE1/0/28 GE1/0/29
                                                GE1/0/30 GE1/0/31 GE1/0/32
                                                GE1/0/33 GE1/0/34 GE1/0/35
                                                GE1/0/36 GE1/0/37 GE1/0/38
                                                GE1/0/39 GE1/0/40 GE1/0/41
                                                GE1/0/42 GE1/0/43 GE1/0/44
                                                GE1/0/45 GE1/0/46 GE1/0/47
                                                GE1/0/48
2         VLAN 0002
3         VLAN 0003
```

Table 13 Command output

Field	Description
Default VLAN ID	System default VLAN ID.
Name	VLAN name.
Port	Ports that allow packets from the VLAN to pass through.

interface vlan-interface

Use **interface vlan-interface** to create a VLAN interface and enter its view, or enter the view of an existing VLAN interface.

Use **undo interface vlan-interface** to delete a VLAN interface.

Syntax

interface vlan-interface *interface-number*

undo interface vlan-interface *interface-number*

Default

No VLAN interfaces exist.

Views

System view

Predefined user roles

network-admin

Parameters

interface-number: Specifies a VLAN interface number in the range of 1 to 4094.

Usage guidelines

Create the VLAN before you create the VLAN interface for a VLAN.

Examples

```
# Create VLAN-interface 2, and enter its view.
<Sysname> system-view
[Sysname] vlan 2
[Sysname-vlan2] quit
[Sysname] interface vlan-interface 2
[Sysname-Vlan-interface2]
```

Related commands

display interface vlan-interface

mtu

Use **mtu** to set the MTU for a VLAN interface.

Use **undo mtu** to restore the default.

Syntax

mtu *size*

undo mtu

Default

The MTU of a VLAN interface is 1500 bytes.

Views

VLAN interface view

Predefined user roles

network-admin

Parameters

size: Sets the MTU in bytes. The value range for this argument is 46 to 1500.

Usage guidelines

If you configure both the **mtu** and **ip mtu** commands on a VLAN interface, the MTU set by the **ip mtu** command is used for fragmentation. For more information about the **ip mtu** command, see *Layer 3—IP Services Command Reference*.

Examples

```
# Set the MTU to 1492 bytes for VLAN-interface 1.
```

```
<Sysname> system-view
[Sysname] interface vlan-interface 1
[Sysname-Vlan-interface1] mtu 1492
```

Related commands

display interface vlan-interface

name

Use **name** to assign a name to a VLAN.

Use **undo name** to restore the default.

Syntax

name *text*

undo name

Default

The name of a VLAN is **VLAN** *vlan-id*. The *vlan-id* argument specifies the VLAN ID in a four-digit format. If the VLAN ID has fewer than four digits, leading zeros are added. For example, the name of VLAN 100 is **VLAN 0100**.

Views

VLAN view

Predefined user roles

network-admin

Parameters

text: Specifies a VLAN name, a case-sensitive string of 1 to 32 characters.

Usage guidelines

For 802.1X or MAC authentication, you can specify authorization VLANs by their names or IDs. If a large number of VLANs are configured on the RADIUS sever and on the device, use VLAN names to identify them.

Examples

Assign the name **test vlan** to VLAN 2.

```
<Sysname> system-view
[Sysname] vlan 2
[Sysname-vlan2] name test vlan
```

Related commands

display vlan

reset counters interface vlan-interface

Use **reset counters interface vlan-interface** to clear statistics on a VLAN interface.

Syntax

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

Views

User view

Predefined user roles

network-admin

Parameters

interface-number. Specifies a VLAN interface by its number.

Usage guidelines

Use this command to clear the history statistics before you collect statistics within a time period.

- If you do not specify the *interface-number* argument, this command clears statistics on all VLAN interfaces.
- If you specify the *interface-number* argument, this command clears statistics on the specified VLAN interface.

Examples

Clear statistics on VLAN-interface 2.

```
<Sysname> reset counters interface vlan-interface 2
```

Related commands

display interface vlan-interface

service

Use **service** to specify the primary traffic processing slot for a VLAN interface.

Use **undo service** to restore the default.

Syntax

Distributed devices in standalone mode/centralized devices in IRF mode:

service slot *slot-number*

undo service slot

Distributed devices in IRF mode:

service chassis *chassis-number* **slot** *slot-number*

undo service chassis

Default

No primary traffic processing slot is specified for a VLAN interface.

Views

VLAN interface view

Predefined user roles

network-admin

Parameters

slot *slot-number*. Specifies a card by its slot number. (Distributed devices in standalone mode.)

slot *slot-number*. Specifies an IRF member device by its member ID. (Centralized devices in IRF mode.)

chassis *chassis-number* **slot** *slot-number*. Specifies a card on an IRF member device. The *chassis-number* argument represents the member ID of the IRF member device. The *slot-number* argument represents the slot number of the card. (Distributed devices in IRF mode.)

Usage guidelines

The following matrix shows the command and hardware compatibility:

Hardware	Command compatibility
MSR954 (JH296A/JH297A/JH298A/JH299A/JH373A)	No
MSR958 (JH300A/JH301A)	No
MSR1002-4/1003-8S	No
MSR2003	Yes
MSR2004-24/2004-48	Yes
MSR3012/3024/3044/3064	Yes
MSR4060/4080	Yes

This command is supported on distributed devices and IRF-capable centralized devices.

Specify a traffic processing slot for a VLAN interface if all traffic on the VLAN interface must be processed on the same slot.

For high availability, you can specify one primary and one backup traffic processing slot by using the **service** command and the **service standby** command, respectively. The primary and backup slots must be different slots.

To avoid processing slot switchover, specify the primary slot before specifying the backup slot. If you specify the backup slot before specifying the primary slot, traffic is switched over to the primary slot immediately after you specify the primary slot.

If you specify both primary and backup slots, the backup slot takes over when the primary slot becomes unavailable. The backup slot continues to process traffic for the interface after the primary slot becomes available again. The switchover will not occur until the backup slot becomes unavailable.

When no specified traffic processing slots are available, the device does not drop the traffic on the interface if the interface is up. Instead, the traffic is processed by the slot at which it arrives. Then, the specified processing slot that first becomes available again takes over.

If no traffic processing slots are specified, traffic on a VLAN interface is processed by the slot at which it arrives.

Examples

```
# Specify slot 2 as the primary traffic processing slot for VLAN-interface 2.
```

```
<Sysname> system-view
[Sysname] vlan 2
[Sysname-vlan2] quit
[Sysname] interface vlan-interface 2
[Sysname-Vlan-interface2] service slot 2
```

Related commands

service standby

service standby

Use **service standby** to specify the backup traffic processing slot for a VLAN interface.

Use **undo service standby** to restore the default.

Syntax

Distributed devices in standalone mode/centralized devices in IRF mode:

service standby slot *slot-number*

undo service standby slot

Distributed devices in IRF mode:

service standby chassis *chassis-number* **slot** *slot-number*

undo service standby chassis

Default

No backup traffic processing slot is specified for a VLAN interface.

Views

VLAN interface view

Predefined user roles

network-admin

Parameters

slot *slot-number*. Specifies a card by its slot number. (Distributed devices in standalone mode.)

slot *slot-number*. Specifies an IRF member device by its member ID. (Centralized devices in IRF mode.)

chassis *chassis-number* **slot** *slot-number*. Specifies a card on an IRF member device. The *chassis-number* argument represents the member ID of the IRF member device. The *slot-number* argument represents the slot number of the card. (Distributed devices in IRF mode.)

Usage guidelines

The following matrix shows the command and hardware compatibility:

Hardware	Command compatibility
MSR954 (JH296A/JH297A/JH298A/JH299A/JH373A)	No
MSR958 (JH300A/JH301A)	No
MSR1002-4/1003-8S	No
MSR2003	Yes
MSR2004-24/2004-48	Yes
MSR3012/3024/3044/3064	Yes
MSR4060/4080	Yes

This command is supported on distributed devices and IRF-capable centralized devices.

Specify a traffic processing slot for a VLAN interface if all traffic on the VLAN interface must be processed on the same slot.

For high availability, you can specify one primary and one backup traffic processing slot by using the **service** command and the **service standby** command, respectively. The primary and backup slots must be different slots.

To avoid processing slot switchover, specify the primary slot before specifying the backup slot. If you specify the backup slot before specifying the primary slot, traffic is switched over to the primary slot immediately after you specify the primary slot.

If you specify both primary and backup slots, the backup slot takes over when the primary slot becomes unavailable. The backup slot continues to process traffic for the interface after the primary

slot becomes available again. The switchover will not occur until the backup slot becomes unavailable.

When no specified traffic processing slots are available, the device does not drop the traffic on the interface if the interface is up. Instead, the traffic is processed by the slot at which it arrives. Then, the specified processing slot that first becomes available again takes over.

If no traffic processing slots are specified, traffic on a VLAN interface is processed by the slot at which it arrives.

Examples

Specify slot 2 and slot 3 as the primary traffic processing slot and the backup traffic processing slot for VLAN-interface 2, respectively.

```
<Sysname> system-view
[Sysname] vlan 2
[Sysname-vlan2] quit
[Sysname] interface vlan-interface 2
[Sysname-Vlan-interface2] service slot 2
[Sysname-Vlan-interface2] service standby slot 3
```

Related commands

service

shutdown

Use **shutdown** to shut down a VLAN interface.

Use **undo shutdown** to bring up a VLAN interface.

Syntax

shutdown

undo shutdown

Default

A VLAN interface is not manually shut down.

Views

VLAN interface view

Predefined user roles

network-admin

Usage guidelines

When a VLAN interface is not manually shut down, the following guidelines apply to the interface state:

- The VLAN interface is down if all ports in the VLAN are down.
- The VLAN interface is up if one or more ports in the VLAN are up.

When you use this command to shut down a VLAN interface, the VLAN interface remains in DOWN (Administratively) state. In this case, the VLAN interface state is not affected by the state of the ports in the VLAN.

Before you configure parameters for a VLAN interface, use this command to shut it down to prevent the configuration from affecting the network. After you complete the VLAN interface configuration, use the **undo shutdown** command to make the settings take effect.

To troubleshoot a failed VLAN interface, you can use the **shutdown** command and then the **undo shutdown** command on the interface to see whether it recovers.

In a VLAN, the state of each Ethernet port is independent of the state of the VLAN interface.

Examples

Shut down VLAN-interface 2, and then bring it up.

```
<Sysname> system-view
[Sysname] interface vlan-interface 2
[Sysname-Vlan-interface2] shutdown
[Sysname-Vlan-interface2] undo shutdown
```

vlan

Use **vlan** *vlan-id* to create a VLAN and enter its view, or enter the view of an existing VLAN.

Use **vlan** *vlan-id1* **to** *vlan-id2* to create VLANs *vlan-id1* through *vlan-id2*, except reserved VLANs.

Use **vlan all** to create VLANs 1 through 4094.

Use **undo vlan** to delete the specified VLANs.

Syntax

vlan { *vlan-id1* [**to** *vlan-id2*] | **all** }

undo vlan { *vlan-id1* [**to** *vlan-id2*] | **all** }

Default

VLAN 1 (system default VLAN) exists.

Views

System view

Predefined user roles

network-admin

Parameters

vlan-id1: Specifies a VLAN ID in the range of 1 to 4094.

vlan-id1 **to** *vlan-id2*: Specifies a VLAN range. The *vlan-id1* and *vlan-id2* arguments specify VLAN IDs. The value range for each of the two arguments is 1 to 4094. The value for the *vlan-id2* argument must be equal to or greater than the value for the *vlan-id1* argument.

all: Specifies all VLANs except reserved VLANs.

The following matrix shows the **all** keyword and hardware compatibility:

Hardware	Keyword compatibility
MSR954 (JH296A/JH297A/JH298A/JH299A/JH373A)	No
MSR958 (JH300A/JH301A)	No
MSR1002-4/1003-8S	No
MSR2003	Yes
MSR2004-24/2004-48	Yes
MSR3012/3024/3044/3064	Yes
MSR4060/4080	Yes

Usage guidelines

You cannot create or delete the system default VLAN (VLAN 1) or reserved VLANs.

Before you delete a dynamic VLAN or a VLAN locked by an application, you must first remove the configuration from the VLAN.

Examples

Create VLAN 2 and enter its view.

```
<Sysname> system-view
[Sysname] vlan 2
[Sysname-vlan2]
```

Create VLANs 4 through 100.

```
<Sysname> system-view
[Sysname] vlan 4 to 100
```

Related commands

display vlan

Port-based VLAN commands

display port

Use **display port** to display information about hybrid or trunk ports.

Syntax

```
display port { hybrid | trunk }
```

Views

Any view

Predefined user roles

network-admin
network-operator

Parameters

hybrid: Specifies hybrid ports.

trunk: Specifies trunk ports.

Examples

Display information about hybrid ports.

```
<Sysname> display port hybrid
Interface          PVID  VLAN Passing
GE1/0/4            100   Tagged: 1000, 1002, 1500, 1600-1611, 2000,
                2555-2558, 3000, 4000
                Untagged:1, 10, 15, 18, 20-30, 44, 55, 67, 100,
                150-160, 200, 255, 286, 300-302
```

Display information about trunk ports.

```
<Sysname> display port trunk
Interface          PVID  VLAN Passing
GE1/0/8            2     1-4, 6-100, 145, 177, 189-200, 244, 289, 400,
                555, 600-611, 1000, 2006-2008
```

Table 14 Command output

Field	Description
Interface	Interface name.
PVID	Port VLAN ID.
VLAN Passing	Existing VLANs allowed on the port.
Tagged	VLANs from which the port sends packets without removing VLAN tags.
Untagged	VLANs from which the port sends packets after removing VLAN tags.

port

Use **port** to assign the specified access ports to a VLAN.

Use **undo port** to remove the specified access ports from a VLAN.

Syntax

port *interface-list*

undo port *interface-list*

Default

All ports are in VLAN 1.

Views

VLAN view

Predefined user roles

network-admin

Parameters

interface-list: Specifies a space-separated list of up to 10 Ethernet interface items. Each item specifies an Ethernet interface or a range of Ethernet interfaces in the form of *interface-type interface-number1 to interface-type interface-number2*. The value for the *interface-number2* argument must be equal to or greater than the value for the *interface-number1* argument.

Usage guidelines

This command is applicable only to access ports.

By default, all ports are access ports. You can manually configure the port link type. For more information, see "[port link-type](#)."

Examples

```
# Assign GigabitEthernet 1/0/1 through GigabitEthernet 1/0/3 to VLAN 2.
<Sysname> system-view
[Sysname] vlan 2
[Sysname-vlan2] port gigabitethernet 1/0/1 to gigabitethernet 1/0/3
```

Related commands

display vlan

port access vlan

Use **port access vlan** to assign an access port to the specified VLAN.

Use **undo port access vlan** to restore the default.

Syntax

```
port access vlan vlan-id  
undo port access vlan
```

Default

All access ports belong to VLAN 1.

Views

Layer 2 aggregate interface view

Layer 2 Ethernet interface view

Predefined user roles

network-admin

Parameters

vlan-id: Specifies a VLAN by its ID in the range of 1 to 4094.

Usage guidelines

Before assigning an access port to a VLAN, make sure the VLAN has been created.

Examples

```
# Assign GigabitEthernet 1/0/1 to VLAN 3.  
<Sysname> system-view  
[Sysname] vlan 3  
[Sysname-vlan3] quit  
[Sysname] interface gigabitethernet 1/0/1  
[Sysname-GigabitEthernet1/0/1] port access vlan 3
```

port hybrid pvid

Use **port hybrid pvid** to set the PVID of a hybrid port.

Use **undo port hybrid pvid** to set the PVID of a hybrid port to 1.

Syntax

```
port hybrid pvid vlan vlan-id  
undo port hybrid pvid
```

Default

The PVID of a hybrid port is the ID of the VLAN to which the port belongs when its link type is **access**.

Views

Layer 2 aggregate interface view

Layer 2 Ethernet interface view

Predefined user roles

network-admin

Parameters

vlan-id: Specifies a VLAN by its ID in the range of 1 to 4094.

Usage guidelines

You can use a nonexistent VLAN as the PVID of a hybrid port. When you delete the PVID of a hybrid port by using the **undo vlan** command, the PVID setting of the port does not change.

For correct packet transmission, set the same PVID for a local hybrid port and its peer.

To enable a hybrid port to transmit packets from its PVID, you must assign the hybrid port to the PVID by using the **port hybrid vlan** command.

Examples

```
# Set the PVID of the hybrid port GigabitEthernet 1/0/1 to VLAN 100, and assign GigabitEthernet 1/0/1 to VLAN 100 as an untagged member.
```

```
<Sysname> system-view
[Sysname] vlan 100
[Sysname-vlan100] quit
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] port link-type hybrid
[Sysname-GigabitEthernet1/0/1] port hybrid pvid vlan 100
[Sysname-GigabitEthernet1/0/1] port hybrid vlan 100 untagged
```

Related commands

port hybrid vlan

port link-type

port hybrid vlan

Use **port hybrid vlan** to assign a hybrid port to the specified VLANs.

Use **undo port hybrid vlan** to remove a hybrid port from the specified VLANs.

Syntax

```
port hybrid vlan vlan-id-list { tagged | untagged }
```

```
undo port hybrid vlan vlan-id-list
```

Default

A hybrid port is an untagged member of the VLAN to which the port belongs when its link type is **access**.

Views

Layer 2 aggregate interface view

Layer 2 Ethernet interface view

Predefined user roles

network-admin

Parameters

vlan-id-list: Specifies a space-separated list of up to 10 VLAN items. Each item specifies a VLAN ID or a range of VLAN IDs in the form of *vlan-id1* **to** *vlan-id2*. The value range for VLAN IDs is 1 to 4094. The value for the *vlan-id2* argument must be equal to or greater than the value for the *vlan-id1* argument. The specified VLANs must already exist on the device.

tagged: Configures the port as a tagged member of the specified VLANs. A tagged member of a VLAN sends packets from the VLAN without removing VLAN tags.

untagged: Configures the port as an untagged member of the specified VLANs. An untagged member of a VLAN sends packets from the VLAN after removing VLAN tags.

Usage guidelines

A hybrid port can allow multiple VLANs. If you execute this command multiple times on a hybrid port, the hybrid port allows all the specified VLANs.

Examples

```
# Configure GigabitEthernet 1/0/1 as a hybrid port, and assign it to VLAN 2, VLAN 4, and VLAN 50 through VLAN 100 as a tagged member.
```

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] port link-type hybrid
[Sysname-GigabitEthernet1/0/1] port hybrid vlan 2 4 50 to 100 tagged
```

Related commands

port link-type

port link-type

Use **port link-type** to set the link type of a port.

Use **undo port link-type** to restore the default link type of a port.

Syntax

port link-type { access | hybrid | trunk }

undo port link-type

Default

Each port is an access port.

Views

Layer 2 aggregate interface view

Layer 2 Ethernet interface view

Predefined user roles

network-admin

Parameters

access: Sets the port link type to access.

hybrid: Sets the port link type to hybrid.

trunk: Sets the port link type to trunk.

Usage guidelines

To change the link type of a port from trunk to hybrid or vice versa, first set the link type to access.

Examples

```
# Configure GigabitEthernet 1/0/1 as a trunk port.
```

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] port link-type trunk
```

port trunk permit vlan

Use **port trunk permit vlan** to assign a trunk port to the specified VLANs.

Use **undo port trunk permit vlan** to remove a trunk port from the specified VLANs.

Syntax

port trunk permit vlan { *vlan-id-list* | **all** }

undo port trunk permit vlan { *vlan-id-list* | **all** }

Default

A trunk port allows packets only from VLAN 1 to pass through.

Views

Layer 2 aggregate interface view

Layer 2 Ethernet interface view

Predefined user roles

network-admin

Parameters

vlan-id-list: Specifies a space-separated list of up to 10 VLAN items. Each item specifies a VLAN ID or a range of VLAN IDs in the form of *vlan-id1* to *vlan-id2*. The value range for VLAN IDs is 1 to 4094. The value for the *vlan-id2* argument must be equal to or greater than the value for the *vlan-id1* argument.

all: Specifies all VLANs. To prevent unauthorized VLAN users from accessing restricted resources through the port, use the **port trunk permit vlan all** command with caution.

Usage guidelines

A trunk port can allow multiple VLANs. If you execute this command multiple times on a trunk port, the trunk port allows all the specified VLANs.

On a trunk port, packets only from the PVID can pass through untagged.

Examples

```
# Configure GigabitEthernet 1/0/1 as a trunk port, and assign it to VLAN 2, VLAN 4, and VLAN 50 through VLAN 100.
```

```
<Sysname> system-view
```

```
[Sysname] interface gigabitethernet 1/0/1
```

```
[Sysname-GigabitEthernet1/0/1] port link-type trunk
```

```
[Sysname-GigabitEthernet1/0/1] port trunk permit vlan 2 4 50 to 100
```

Related commands

port link-type

port trunk pvid

Use **port trunk pvid** to set the PVID for a trunk port.

Use **undo port trunk pvid** to restore the default.

Syntax

port trunk pvid vlan *vlan-id*

undo port trunk pvid

Default

The PVID of a trunk port is VLAN 1.

Views

Layer 2 aggregate interface view

Layer 2 Ethernet interface view

Predefined user roles

network-admin

Parameters

vlan-id: Specifies a VLAN by its ID in the range of 1 to 4094.

Usage guidelines

You can use a nonexistent VLAN as the PVID for a trunk port. When you delete the PVID of a trunk port by using the **undo vlan** command, the PVID setting of the port does not change.

For correct packet transmission, set the same PVID for a local trunk port and its peer.

To enable a trunk port to transmit packets from its PVID, you must assign the trunk port to the PVID by using the **port trunk permit vlan** command.

Examples

Set the PVID of the trunk port GigabitEthernet 1/0/1 to VLAN 100, and assign GigabitEthernet 1/0/1 to VLAN 100.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] port link-type trunk
[Sysname-GigabitEthernet1/0/1] port trunk pvid vlan 100
[Sysname-GigabitEthernet1/0/1] port trunk permit vlan 100
```

Related commands

port link-type

port trunk permit vlan

VLAN group commands

display vlan-group

Use **display vlan-group** to display VLAN group information.

Syntax

```
display vlan-group [ group-name ]
```

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

group-name: Specifies a VLAN group by its name, a case-sensitive string of 1 to 31 characters. The first character must be an alphabetical character. If you do not specify this argument, the command displays information about all VLAN groups.

Examples

Display information about the VLAN group **test001**.

```
<Sysname> display vlan-group test001
VLAN group: test001
    VLAN list: 2-4 100 200
```

Display information about all VLAN groups.

```
<Sysname> display vlan-group
VLAN group: test001
    VLAN list: 2-4 100 200
VLAN group: rnd
    VLAN list: Null
```

Table 15 Command output

Field	Description
VLAN group	Name of the VLAN group.
VLAN list	VLAN list in the VLAN group.

Related commands

vlan-group

vlan-list

vlan-group

Use **vlan-group** to create a VLAN group and enter its view, or enter the view of an existing VLAN group.

Use **undo vlan-group** to delete a VLAN group.

Syntax

vlan-group *group-name*

undo vlan-group *group-name*

Default

No VLAN groups exist.

Views

System view

Predefined user roles

network-admin

Parameters

group-name: Specifies a VLAN group by its name, a case-sensitive string of 1 to 31 characters. The first character must be an alphabetical character.

Usage guidelines

A VLAN group includes a set of VLANs. You can add multiple VLAN lists to a VLAN group.

Examples

Create a VLAN group named **test001** and enter VLAN group view.

```
<Sysname> system-view
```

```
[Sysname] vlan-group test001
[Sysname-vlan-group-test001]
```

Related commands

vlan-list

vlan-list

Use **vlan-list** to add VLANs to a VLAN group.

Use **undo vlan-list** to remove VLANs from a VLAN group.

Syntax

vlan-list *vlan-id-list*

undo vlan-list *vlan-id-list*

Default

No VLANs exist in a VLAN group.

Views

VLAN group view

Predefined user roles

network-admin

Parameters

vlan-id-list: Specifies a space-separated list of up to 10 VLAN items. Each item specifies a VLAN ID or a range of VLAN IDs in the form of *vlan-id1* **to** *vlan-id2*. The value range for VLAN IDs is 1 to 4094. The value for the *vlan-id2* argument must be equal to or greater than the value for the *vlan-id1* argument.

Examples

Add VLAN 2 through VLAN 4, VLAN 100, and VLAN 200 to the VLAN group **test001**.

```
<Sysname> system-view
```

```
[Sysname] vlan-group test001
```

```
[Sysname-vlan-group-test001] vlan-list 2 to 4 100 200
```

Related commands

vlan-group

Super VLAN commands

display supervlan

Use **display supervlan** to display information about super VLANs and their associated sub-VLANs.

Syntax

```
display supervlan [ supervlan-id ]
```

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

supervlan-id: Specifies a super VLAN ID in the range of 1 to 4094. If you do not specify a super VLAN ID, this command displays information about all super VLANs and their associated sub-VLANs.

Examples

Display information about super VLAN 2 and its associated sub-VLANs.

```
<Sysname> display supervlan 2
Super VLAN ID: 2
Sub-VLAN ID: 3-5

VLAN ID: 2
VLAN type: Static
It is a super VLAN.
Route interface: Configured
IPv4 address: 10.153.17.41
IPv4 subnet mask: 255.255.252.0
IPv6 global unicast addresses:
  2001::1, subnet is 2001::/64 [TENTATIVE]
Description: VLAN 0002
Name: VLAN 0002
Tagged ports:  None
Untagged ports: None

VLAN ID: 3
VLAN type: Static
It is a sub VLAN.
Route interface: Configured
IPv4 address: 10.153.17.41
IPv4 subnet mask: 255.255.252.0
IPv6 global unicast addresses:
  2001::1, subnet is 2001::/64 [TENTATIVE]
Description: VLAN 0003
Name: VLAN 0003
```

```

Tagged ports:   None
Untagged ports:
    GigabitEthernet1/0/3

VLAN ID: 4
VLAN type: Static
It is a sub VLAN.
Route interface: Configured
IPv4 address: 10.153.17.41
IPv4 subnet mask: 255.255.252.0
IPv6 global unicast addresses:
    2001::1, subnet is 2001::/64 [TENTATIVE]
Description: VLAN 0004
Name: VLAN 0004
Tagged ports:   None
Untagged ports:
    GigabitEthernet1/0/4

```

Table 16 Command output

Field	Description
VLAN type	VLAN type, dynamic or static.
Route interface	Whether a VLAN interface is configured for the VLAN.
IPv4 address	<p>Primary IPv4 address of the VLAN interface. This field is displayed only when an IPv4 address is configured for the VLAN interface.</p> <p>When the VLAN interface is also configured with secondary IPv4 addresses, you can view them by using one of the following commands:</p> <ul style="list-style-type: none"> • display interface vlan-interface. • display this (VLAN interface view).
IPv4 subnet mask	Subnet mask for the primary IPv4 address of the VLAN interface. This field is displayed only when an IPv4 address is configured for the VLAN interface.
IPv6 global unicast addresses	<p>Global unicast IPv6 address of the VLAN interface. This field is not displayed when no IPv6 address is configured for the VLAN interface.</p> <p>The IPv6 address states are as follows:</p> <ul style="list-style-type: none"> • TENTATIVE—Initial state. DAD is being performed or is to be performed on the address. An address in this state cannot be used as the source address or destination address of packets. • DUPLICATE—DAD has been completed for the address. The address is not unique on the link and cannot be used. • PREFERRED—The address is preferred and can be used as the source or destination address of a packet. If an address is in this state, the command does not display the address state. • DEPRECATED—The address is beyond the preferred lifetime but within the valid lifetime. It is valid, but it cannot be used as the source address for a new connection. Packets destined to the address are processed correctly.
Description	VLAN description.
Name	VLAN name.
Tagged ports	Tagged members of the VLAN.
Untagged ports	Untagged members of the VLAN.

Related commands

subvlan
supervlan

subvlan

Use **subvlan** to associate a super VLAN with the specified sub-VLANs.

Use **undo subvlan** to dissociate sub-VLANs from a super VLAN.

Syntax

subvlan *vlan-id-list*
undo subvlan [*vlan-id-list*]

Default

A super VLAN is not associated with any sub-VLANs.

Views

VLAN view

Predefined user roles

network-admin

Parameters

vlan-id-list: Specifies a space-separated list of up to 10 sub-VLAN items. Each item specifies a sub-VLAN ID or a range of sub-VLAN IDs in the form of *vlan-id1* to *vlan-id2*. The value range for sub-VLAN IDs is 1 to 4094. The value for the *vlan-id2* argument must be equal to or greater than the value for the *vlan-id1* argument.

Usage guidelines

Make sure sub-VLANs already exist before you associate them with a super VLAN.

You can add ports to and remove ports from a sub-VLAN that is already associated with a super VLAN.

When you use the **undo subvlan** command, follow these guidelines:

- If you do not specify the *vlan-id-list* argument, this command dissociates all sub-VLANs from the current super VLAN.
- If you specify the *vlan-id-list* argument, this command dissociates the specified sub-VLANs from the current super VLAN.

Examples

```
# Associate super VLAN 10 with sub-VLANs 3, 4, and 5.
<Sysname> system-view
[Sysname] vlan 3 to 5
[Sysname] vlan 10
[Sysname-vlan10] supervlan
[Sysname-vlan10] subvlan 3 to 5
```

Related commands

display supervlan
supervlan

supervlan

Use **supervlan** to configure a VLAN as a super VLAN.

Use **undo supervlan** to restore the default.

Syntax

supervlan

undo supervlan

Default

A VLAN is not a super VLAN.

Views

VLAN view

Predefined user roles

network-admin

Usage guidelines

You cannot configure a VLAN as both a super VLAN and a guest VLAN, Auth-Fail VLAN, or critical VLAN. For more information about guest VLANs, Auth-Fail VLANs, and critical VLANs, see *Security Configuration Guide*.

As a best practice, do not configure VRRP for a super VLAN interface, because the configuration affects network performance.

Layer 2 multicast configuration for super VLANs does not take effect because they do not have physical ports.

Examples

Configure VLAN 2 as a super VLAN.

```
<Sysname> system-view  
[Sysname] vlan 2  
[Sysname-vlan2] supervlan
```

Related commands

display supervlan

subvlan

Voice VLAN commands

This feature is supported only on the following ports:

- Layer 2 Ethernet ports on the following modules:
 - HMIM-8GSW.
 - HMIM-8GSWF.
 - HMIM-24GSW.
 - HMIM-24GSW-PoE.
 - SIC-4GSW.
 - SIC-4GSW-PoE.
- Fixed Layer 2 Ethernet ports on the following routers:
 - MSR954 (JH296A/JH297A/JH298A/JH299A/JH373A).
 - MSR958 (JH300A/JH301A).
 - MSR1002-4/1003-8S.
 - MSR2004-24/2004-48.

display voice-vlan mac-address

Use **display voice-vlan mac-address** to display OUI addresses and their masks and descriptions.

Syntax

```
display voice-vlan mac-address
```

Views

Any view

Predefined user roles

network-admin

network-operator

Examples

Display OUI addresses and their masks and descriptions.

```
<Sysname> display voice-vlan mac-address
OUI Address      Mask              Description
0001-e300-0000   ffff-ff00-0000   Siemens phone
0003-6b00-0000   ffff-ff00-0000   Cisco phone
0004-0d00-0000   ffff-ff00-0000   Avaya phone
000f-e200-0000   ffff-ff00-0000   H3C Aolynk phone
0060-b900-0000   ffff-ff00-0000   Philips/NEC phone
00d0-1e00-0000   ffff-ff00-0000   Pingtel phone
00e0-7500-0000   ffff-ff00-0000   Polycom phone
00e0-bb00-0000   ffff-ff00-0000   3Com phone
```

Table 17 Command output

Field	Description
OUI Address	OUI address allowed on the device.

Field	Description
Mask	Mask of the OUI address.
Description	Description of the OUI address.

Related commands

`voice-vlan mac-address`

display voice-vlan state

Use `display voice-vlan state` to display voice VLAN information.

Syntax

`display voice-vlan state`

Views

Any view

Predefined user roles

network-admin

network-operator

Examples

Display voice VLAN information.

```
<Sysname> display voice-vlan state
Current voice VLANs: 1
Voice VLAN security mode: Security
Voice VLAN aging time: 1440 minutes
Voice VLAN enabled ports and their modes:
Port                VLAN      Mode      CoS      DSCP
GE1/0/1             111      AUTO      6        46
```

NOTE:

The command output varies by device model.

Table 18 Command output

Field	Description
Current Voice VLANs	Number of existing voice VLANs.
Voice VLAN security mode	Voice VLAN mode: <ul style="list-style-type: none"> Security. Normal.
Voice VLAN enabled ports and their modes	Voice VLAN-enabled ports and their voice VLAN assignment modes.
Port	Name of the voice VLAN-enabled port.
VLAN	ID of the voice VLAN enabled on the port.
Mode	Voice VLAN assignment mode of the port: <ul style="list-style-type: none"> Manual. Automatic.

Related commands

voice-vlan aging
voice-vlan enable
voice-vlan mode auto
voice-vlan security enable

voice-vlan aging

Use **voice-vlan aging** to set the voice VLAN aging timer.

Use **undo voice-vlan aging** to restore the default.

Syntax

voice-vlan aging *minutes*
undo voice-vlan aging

Default

The voice VLAN aging timer is 1440 minutes (24 hours).

Views

System view

Predefined user roles

network-admin

Parameters

minutes: Sets the voice VLAN aging timer in the range of 5 to 43200 minutes.

Usage guidelines

In automatic voice VLAN assignment mode, the device starts an aging timer for a voice VLAN when assigning a port to the voice VLAN. If no voice packets are received on the port before the timer expires, the device removes the port from the voice VLAN.

Set the voice VLAN aging timer only when the voice VLAN assignment mode is automatic.

Examples

```
# Set the voice VLAN aging timer to 100 minutes.  
<Sysname> system-view  
[Sysname] voice-vlan aging 100
```

Related commands

display voice-vlan state

voice-vlan enable

Use **voice-vlan enable** to enable the voice VLAN feature on a port.

Use **undo voice-vlan enable** to disable the voice VLAN feature on a port.

Syntax

voice-vlan *vlan-id* **enable**
undo voice-vlan [*vlan-id*] **enable**

Default

The voice VLAN feature is disabled on ports.

Views

Layer 2 Ethernet interface view

Predefined user roles

network-admin

Parameters

vlan-id: Specifies a voice VLAN ID in the range of 2 to 4094.

Usage guidelines

Use this command only on a hybrid or trunk port operating in automatic voice VLAN assignment mode.

Before you execute this command, make sure the specified VLAN already exists.

Examples

```
# Enable the voice VLAN feature on GigabitEthernet 1/0/1.  
<Sysname> system-view  
[Sysname] interface gigabitethernet 1/0/1  
[Sysname-GigabitEthernet1/0/1] voice-vlan 2 enable
```

Related commands

display voice-vlan state

voice-vlan mode auto

voice-vlan mac-address

Use **voice-vlan mac-address** to configure the OUI address information for voice packet identification.

Use **undo voice-vlan mac-address** to delete an OUI address.

Syntax

voice-vlan mac-address *mac-address* **mask** *oui-mask* [**description** *text*]

undo voice-vlan mac-address *oui*

Default

System default OUI addresses exist.

Table 19 System default OUI addresses

Number	OUI address	Vendor
1	0001-E300-0000	Siemens phone
2	0003-6B00-0000	Cisco phone
3	0004-0D00-0000	Avaya phone
4	000F-E200-0000	H3C Aolynk phone
5	0060-B900-0000	Philips/NEC phone
6	00D0-1E00-0000	Pingtel phone
7	00E0-7500-0000	Polycom phone

Number	OUI address	Vendor
8	00E0-BB00-0000	3Com phone

Views

System view

Predefined user roles

network-admin

Parameters

mac-address: Specifies a source MAC address of voice traffic, in the format of H-H-H. For example, 1234-1234-1234.

mask oui-mask: Specifies the valid length of the OUI address by using a mask in the format of H-H-H. The mask contains consecutive 1s and 0s. For example, FFFF-0000-0000. To match the voice devices of a vendor, set the mask to FFFF-FF00-0000.

description text: Specifies the OUI address description, a case-sensitive string of 1 to 30 characters.

oui: Specifies an OUI address to delete, in the format of H-H-H. For example, 1234-1200-0000. An OUI address is the logical AND result of the *mac-address* and *oui-mask* arguments. It cannot be a broadcast address, a multicast address, or an all-zero address.

Usage guidelines

Typically, an OUI address refers to the first 24 bits of a MAC address (in binary notation) and is a globally unique identifier that IEEE assigns to a vendor. However, OUI addresses in this chapter are addresses that the system uses to identify voice packets. They are the logical AND results of the *mac-address* and *oui-mask* arguments in this command.

You can manually delete or add the system default OUI addresses.

The maximum number of configurable OUI addresses depends on the device model.

Examples

Add an OUI address 1234-1200-0000 by specifying the MAC address as 1234-1234-1234 and the mask as fff-ff00-0000. Configure the OUI address description as **PhoneA**.

```
<Sysname> system-view
```

```
[Sysname] voice-vlan mac-address 1234-1234-1234 mask ffff-ff00-0000 description PhoneA
```

Related commands

display voice-vlan mac-address

voice-vlan mode auto

Use **voice-vlan mode auto** to configure a port to operate in automatic voice VLAN assignment mode.

Use **undo voice-vlan mode auto** to configure a port to operate in manual voice VLAN assignment mode.

Syntax

voice-vlan mode auto

undo voice-vlan mode auto

Default

A port operates in automatic voice VLAN assignment mode.

Views

Layer 2 Ethernet interface view

Predefined user roles

network-admin

Usage guidelines

To make a voice VLAN take effect on a port operating in manual mode, you must manually assign the port to the voice VLAN.

Examples

```
# Configure GigabitEthernet 1/0/1 to operate in manual voice VLAN assignment mode.
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] undo voice-vlan mode auto
```

Related commands

display voice-vlan state

voice-vlan security enable

Use **voice-vlan security enable** to enable the voice VLAN security mode.

Use **undo voice-vlan security enable** to disable the voice VLAN security mode.

Syntax

voice-vlan security enable

undo voice-vlan security enable

Default

The voice VLAN security mode is enabled.

Views

System view

Predefined user roles

network-admin

Usage guidelines

In security mode, a voice VLAN transmits only voice packets whose source MAC addresses match the OUI addresses of the device.

In normal mode, a voice VLAN transmits voice packets and non-voice packets.

Examples

```
# Disable the voice VLAN security mode.
<Sysname> system-view
[Sysname] undo voice-vlan security enable
```

Related commands

display voice-vlan state

voice-vlan track lldp

Use **voice-vlan track lldp** to enable LLDP for automatic IP phone discovery.

Use **undo voice-vlan track lldp** to disable LLDP for automatic IP phone discovery.

Syntax

voice-vlan track lldp

undo voice-vlan track lldp

Views

System view

Default

LLDP for automatic IP phone discovery is disabled.

Predefined user roles

network-admin

Examples

Enable LLDP for automatic IP phone discovery.

```
<Sysname> system-view
```

```
[Sysname] voice-vlan track lldp
```

QinQ commands

This feature is supported only on the following ports:

- Layer 2 Ethernet ports on the following modules:
 - HMIM-8GSW.
 - HMIM-8GSWF.
 - HMIM-24GSW.
 - HMIM-24GSW-PoE.
- Fixed Layer 2 Ethernet ports on MSR2004-24 and MSR2004-48 routers.

This document uses the following terms:

- **CVLAN**—Customer network VLANs, also called inner VLANs, refer to VLANs that a customer uses on the private network.
- **SVLAN**—Service provider network VLANs, also called outer VLANs, refer to VLANs that a service provider uses to transmit VLAN tagged traffic for customers.

display qinq

Use **display qinq** to display QinQ-enabled interfaces.

Syntax

```
display qinq [ interface interface-type interface-number ]
```

Views

Any view

Predefined user roles

network-admin
network-operator

Parameters

interface *interface-type interface-number*. Specifies an interface by its type and number. If you do not specify an interface, this command displays all QinQ-enabled interfaces.

Usage guidelines

If QinQ is not enabled on any interfaces, this command does not provide any output.

Examples

Enable QinQ on GigabitEthernet 1/0/1. Then, verify that QinQ is enabled on the interface.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] qinq enable
[Sysname-GigabitEthernet1/0/1] display qinq interface gigabitethernet 1/0/1
Interface
  GigabitEthernet1/0/1
```

Enable QinQ on GigabitEthernet 1/0/1 and GigabitEthernet 1/0/3. Then, verify that QinQ is enabled on the interfaces.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] qinq enable
```

```

[Sysname-GigabitEthernet1/0/1] quit
[Sysname] interface gigabitethernet 1/0/3
[Sysname-GigabitEthernet1/0/3] qinq enable
[Sysname-GigabitEthernet1/0/3] display qinq
Interface
  GigabitEthernet1/0/1
  GigabitEthernet1/0/3

```

Table 20 Command output

Field	Description
Interface	Interface name.
GigabitEthernet1/0/1	QinQ-enabled interface.

Related commands

qinq enable

qinq enable

Use **qinq enable** to enable QinQ on an interface.

Use **undo qinq enable** to disable QinQ on an interface.

Syntax

qinq enable

undo qinq enable

Default

QinQ is disabled on interfaces.

Views

Layer 2 Ethernet interface view

Predefined user roles

network-admin

Examples

```

# Enable QinQ on GigabitEthernet 1/0/1.
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] qinq enable

```

Related commands

display qinq

qinq ethernet-type

Use **qinq ethernet-type** to set the TPID value in SVLAN or CVLAN tags.

Use **undo qinq ethernet-type** to restore the default TPID value in SVLAN or CVLAN tags.

Syntax

qinq ethernet-type { **customer-tag** | **service-tag** } *hex-value*

undo qinq ethernet-type { customer-tag | service-tag }

Default

The TPID value in both SVLAN and CVLAN tags is 8100 in hexadecimal notation.

Views

System view

Layer 2 Ethernet interface view

Predefined user roles

network-admin

Parameters

customer-tag: Sets the TPID value in the CVLAN tag. This keyword is available only in system view.

service-tag: Sets the TPID value in the SVLAN tag. This keyword is available only in Layer 2 Ethernet interface view.

hex-value: Sets a hexadecimal TPID value. The value range is 0x0001 to 0xFFFF, excluding the reserved EtherType values listed in [Table 21](#).

Table 21 Reserved EtherType values

Protocol type	Value
ARP	0x0806
PUP	0x0200
RARP	0x8035
IP	0x0800
IPv6	0x86DD
PPPoE	0x8863/0x8864
MPLS	0x8847/0x8848
IPX/SPX	0x8137
IS-IS	0x8000
LACP	0x8809
LLDP	0x88CC
802.1X	0x888E
802.1ag	0x8902
Cluster	0x88A7
Reserved	0xFFFD/0xFFFE/0xFFFF

Examples

Set the TPID value in CVLAN tags to 8200 (hexadecimal).

```
<Sysname> system-view  
[Sysname] qinq ethernet-type customer-tag 8200
```

Set the TPID value in SVLAN tags to 9100 (hexadecimal) on GigabitEthernet 1/0/1.

```
<Sysname> system-view  
[Sysname] interface gigabitethernet 1/0/1  
[Sysname-GigabitEthernet1/0/1] qinq ethernet-type service-tag 9100
```

Loop detection commands

This feature is supported only on the following ports:

- Layer 2 Ethernet ports on Ethernet switching modules.
- Fixed Layer 2 Ethernet ports of the following routers:
 - MSR1002-4/1003-8S.
 - MSR2004-24/2004-48.
 - MSR954(JH296A/JH297A/JH298A/JH299A/JH373A).
 - MSR958(JH300A/JH301A).

display loopback-detection

Use **display loopback-detection** to display the loop detection configuration and status.

Syntax

```
display loopback-detection
```

Views

Any view

Predefined user roles

network-admin
network-operator

Example

```
# Display the loop detection configuration and status.
```

```
<Sysname> display loopback-detection
Loopback detection is enabled.
Loopback detection interval is 30 second(s).
Loopback is detected on following interfaces:
Interface           Action mode
GigabitEthernet1/0/1  Block
GigabitEthernet1/0/2  Shutdown
GigabitEthernet1/0/3  None
GigabitEthernet1/0/4  No-learning
```

Table 22 Command output

Field	Description
Action mode	Loop protection action: <ul style="list-style-type: none">• Block—When a loop is detected on a port, the device performs the following operations:<ul style="list-style-type: none">○ Generates a log.○ Disables the port from learning MAC addresses.○ Blocks the port.• None—When a loop is detected on a port, the device generates a log but performs no action on the port.• No-learning—When a loop is detected on a port, the device generates a log and disables the port from learning MAC addresses.• Shutdown—When a loop is detected on a port, the device performs the

Field	Description
	following operations: <ul style="list-style-type: none"> ○ Generates a log. ○ Shuts down the port to disable the port from receiving or sending frames. The device automatically sets the port to the forwarding state after a time interval. Set the time interval by using the shutdown-interval command (see <i>Fundamentals Command Reference</i>).

loopback-detection action

Use **loopback-detection action** to set the loop protection action on a per-port basis.

Use **undo loopback-detection action** to restore the default.

Syntax

In Layer 2 Ethernet interface view:

loopback-detection action { block | no-learning | shutdown }

undo loopback-detection action

In Layer 2 aggregate interface view:

loopback-detection action shutdown

undo loopback-detection action

Default

When the device detects a loop on a port, it generates a log but performs no action on the port.

Views

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

Predefined user roles

network-admin

Parameters

block: Enables the block mode. If a loop is detected, the device performs the following operations:

- Generates a log.
- Disables MAC address learning.
- Blocks the port.

Layer 2 aggregate interfaces do not support this keyword.

no-learning: Enables the no-learning mode. If a loop is detected, the device generates a log and disables MAC address learning on the port. Layer 2 aggregate interfaces do not support this keyword.

shutdown: Enables the shutdown mode. If a loop is detected, the device generates a log and shuts down the port. The device automatically sets the port to the forwarding state after the time interval set by using the **shutdown-interval** command (see *Fundamentals Command Reference*).

Usage guidelines

To set the loop protection action globally, use the **loopback-detection global action** command.

The global configuration applies to all ports. The per-port configuration applies to the individual ports. The per-port configuration takes precedence over the global configuration.

Example

```
# Set the loop protection action to shutdown on port GigabitEthernet 1/0/1.
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[System-GigabitEthernet1/0/1] loopback-detection action shutdown
```

Related commands

display loopback-detection
loopback-detection global action

loopback-detection enable

Use **loopback-detection enable** to enable loop detection on a per-port basis.

Use **undo loopback-detection enable** to disable loop detection on a port.

Syntax

```
loopback-detection enable vlan { vlan-id-list | all }  
undo loopback-detection enable vlan { vlan-id-list | all }
```

Default

Loop detection is disabled on ports.

Views

Layer 2 Ethernet interface view
Layer 2 aggregate interface view

Predefined user roles

network-admin

Parameters

vlan-id-list: Specifies a space-separated list of up to 10 VLAN items. Each item specifies a VLAN ID or a range of VLAN IDs in the form of *vlan-id1* to *vlan-id2*. The value range for VLAN IDs is 1 to 4094. The ID for *vlan-id2* must be no less than the ID for *vlan-id1*.

all: Specifies all existing VLANs.

Usage guidelines

To enable loop detection globally, use the **loopback-detection global enable** command.

The global configuration applies to all ports in the specified VLAN. The per-port configuration applies to the individual port only when the port belongs to the specified VLAN. The per-port configuration takes precedence over the global configuration.

Example

```
# Enable loop detection on port GigabitEthernet 1/0/1 for VLAN 10 through VLAN 20.
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[System-GigabitEthernet1/0/1] loopback-detection enable vlan 10 to 20
```

Related commands

display loopback-detection
loopback-detection global enable

loopback-detection global action

Use **loopback-detection global action** to set the global loop protection action.

Use **undo loopback-detection global action** to restore the default.

Syntax

loopback-detection global action shutdown

undo loopback-detection global action

Default

When the device detects a loop on a port, it generates a log but performs no action on the port.

Views

System view

Predefined user roles

network-admin

Parameters

shutdown: Enables the shutdown mode. If a loop is detected, the device generates a log and shuts down the port. The device automatically sets the port to the forwarding state after you set the time interval by using the **shutdown-interval** command (see *Fundamentals Command Reference*).

Usage guidelines

To set the loop protection action on a per-port basis, use the **loopback-detection action** command in interface view.

The global configuration applies to all ports. The per-port configuration applies to the individual ports. The per-port configuration takes precedence over the global configuration.

Example

```
# Set the global loop protection action to shutdown.
<Sysname> system-view
[System] loopback-detection global action shutdown
```

Related commands

display loopback-detection

loopback-detection action

loopback-detection global enable

Use **loopback-detection global enable** to enable loop detection globally.

Use **undo loopback-detection global enable** to disable loop detection globally.

Syntax

loopback-detection global enable vlan { *vlan-id-list* | all }

undo loopback-detection global enable vlan { *vlan-id-list* | all }

Default

Loop detection is globally disabled.

Views

System view

Predefined user roles

network-admin

Parameters

vlan-id-list: Specifies a space-separated list of up to 10 VLAN items. Each item specifies a VLAN ID or a range of VLAN IDs in the form of *vlan-id1* to *vlan-id2*. The value range for VLAN IDs is 1 to 4094. The ID for *vlan-id2* must be equal to or greater than the ID for *vlan-id1*.

all: Specifies all existing VLANs.

Usage guidelines

To enable loop detection on a per-port basis, use the **loopback-detection enable** command in interface view.

The global configuration applies to all ports in the specified VLAN. The per-port configuration applies to the individual port only when the port belongs to the specified VLAN. The per-port configuration takes precedence over the global configuration.

Example

```
# Globally enable loop detection for VLAN 10 through VLAN 20.
<Sysname> system-view
[System] loopback-detection global enable vlan 10 to 20
```

Related commands

display loopback-detection

loopback-detection enable

loopback-detection interval-time

Use **loopback-detection interval-time** to set the loop detection interval.

Use **undo loopback-detection interval-time** to restore the default.

Syntax

loopback-detection interval-time *interval*

undo loopback-detection interval-time

Default

The loop detection interval is 30 seconds.

Views

System view

Predefined user roles

network-admin

Parameters

interval: Sets the loop detection interval in the range of 1 to 300 seconds.

Usage guidelines

With loop detection enabled, the device sends loop detection frames at the specified interval. A shorter interval offers more sensitive detection but consumes more resources. Consider the system performance and loop detection speed when you set the loop detection interval.

Example

```
# Set the loop detection interval to 10 seconds.
```

```
<Sysname> system-view
```

```
[Sysname] loopback-detection interval-time 10
```

Related commands

display loopback-detection

Spanning tree commands

This feature is supported only on the following ports:

- Layer 2 Ethernet ports on the following modules:
- Fixed Layer 2 Ethernet ports on Ethernet switching modules.
 - MSR1002-4/1003-8S.
 - MSR2004-24/2004-48.
 - MSR954 (JH296A/JH297A/JH298A/JH299A/JH373A).
 - MSR958 (JH300A/JH301A).

Commands and descriptions for centralized devices apply to the following routers:

- MSR1002-4/1003-8S.
- MSR2003.
- MSR2004-24/2004-48.
- MSR3012/3024/3044/3064.
- MSR954 (JH296A/JH297A/JH298A/JH299A/JH373A).
- MSR958 (JH300A/JH301A).

Commands and descriptions for distributed devices apply to MSR4060 and MSR4080 routers.

active region-configuration

Use **active region-configuration** to activate your MST region configuration.

Syntax

active region-configuration

Views

MST region view

Predefined user roles

network-admin

Usage guidelines

When you configure MST region parameters, MSTP launches a new spanning tree calculation process that might cause network topology instability. This is most likely to occur when you configure the VLAN-to-instance mapping table. The launch occurs after you execute the **active region-configuration** command or the **stp global enable** command.

As a best practice, use the **check region-configuration** command to determine whether the MST region configurations to be activated are correct. Run this command only when they are correct.

Examples

Map VLAN 2 to MSTI 1 and activate the MST region configuration.

```
<Sysname> system-view
[Sysname] stp region-configuration
[Sysname-mst-region] instance 1 vlan 2
[Sysname-mst-region] active region-configuration
```

Related commands

check region-configuration

instance
region-name
revision-level
stp global enable
vlan-mapping modulo

check region-configuration

Use **check region-configuration** to display MST region pre-configuration information, including the region name, revision level, and VLAN-to-instance mapping table settings.

Syntax

check region-configuration

Views

MST region view

Predefined user roles

network-admin

Usage guidelines

Spanning tree devices belong to the same MST region only when they are connected through a physical link and configured with the same details as follows:

- Format selector (0 by default and not configurable).
- MST region name.
- MST region revision level.
- VLAN-to-instance mapping entries in the MST region.

As a best practice, use this command to determine whether the MST region configurations to be activated are correct. Activate them only when they are correct.

Examples

Display MST region pre-configurations.

```
<Sysname> system-view
[Sysname] stp region-configuration
[Sysname-mst-region] check region-configuration
Admin Configuration
  Format selector      : 0
  Region name        : 001122334400
  Revision level     : 0
  Configuration digest : 0x3ab68794d602fdf43b21c0b37ac3bca8

Instance  VLANs Mapped
  0        1, 3 to 4094
  15       2
```

Table 23 Command output

Field	Description
Format selector	Format selector of the MST region, which is 0 (not configurable).
Region name	MST region name.

Field	Description
Revision level	Revision level of the MST region.
Instance VLANs Mapped	VLAN-to-instance mappings in the MST region.

Related commands

active region-configuration
instance
region-name
revision-level
vlan-mapping modulo

display stp

Use **display stp** to display spanning tree status and statistics. Based on the information, you can analyze and maintain the network topology or determine whether the spanning tree is working correctly.

Syntax

Centralized devices in standalone mode:

display stp [**instance** *instance-list* | **vlan** *vlan-id-list*] [**interface** *interface-list*] [**brief**]

Distributed devices in standalone mode/centralized devices in IRF mode:

display stp [**instance** *instance-list* | **vlan** *vlan-id-list*] [**interface** *interface-list* | **slot** *slot-number*] [**brief**]

Distributed devices in IRF mode:

display stp [**instance** *instance-list* | **vlan** *vlan-id-list*] [**interface** *interface-list* | **chassis** *chassis-number* **slot** *slot-number*] [**brief**]

Views

Any view

Predefined user roles

network-admin
 network-operator

Parameters

instance *instance-list*: Specifies a space-separated list of up to 10 MSTI items. Each item specifies an MSTI or a range of MSTIs in the form of *instance-id1* [**to** *instance-id2*]. The value for *instance-id2* must be equal to or greater than the value for *instance-id1*. The value range for the *instance-id* argument is 0 to 4094, and the value 0 represents the CIST.

vlan *vlan-id-list*: Specifies a space-separated list of up to 10 VLAN items. Each item specifies a VLAN or a range of VLANs in the form of *vlan-id1* [**to** *vlan-id2*]. The value for *vlan-id2* must be equal to or greater than the value for *vlan-id1*. The value range for the *vlan-id* argument is 1 to 4094.

interface *interface-list*: Specifies a space-separated list of up to 10 interface items. Each item specifies an interface or a range of interfaces in the form of *interface-type interface-number 1* [**to** *interface-type interface-number 2*]. The interface number for *interface-number 2* must be equal to or greater than the interface number for *interface-number 1*.

brief: Displays brief spanning tree status and statistics. If this keyword is not specified, the command displays detailed spanning tree status and statistics.

slot slot-number. Specifies a card by its slot number. If you do not specify a card, this command displays information for all cards. (Distributed devices in standalone mode.)

slot slot-number. Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays information for all member devices. (Centralized devices in IRF mode.)

chassis chassis-number slot slot-number. Specifies a card on an IRF member device. The *chassis-number* argument represents the member ID of the IRF member device. The *slot-number* argument represents the slot number of the card. If you do not specify a card, this command displays information for all cards. (Distributed devices in IRF mode.)

Usage guidelines

In STP or RSTP mode, the command output is sorted by port name.

- If you do not specify a port, this command applies to all ports.
- If you specify a port list, this command applies to the specified ports.

In PVST mode, the command output is sorted by VLAN ID and by port name in each VLAN.

- If you do not specify a VLAN or port, this command applies to all ports in all VLANs.
- If you only specify a VLAN list but not a port, this command applies to all ports in the specified VLANs.
- If you only specify a port list but not a VLAN, this command applies to the specified ports in all VLANs.
- If you specify both a VLAN list and a port list, this command applies to the ports in the specified VLANs.

In MSTP mode, the command output is sorted by MSTI ID and by port name in each MSTI.

- If you do not specify an MSTI or port, this command applies to all MSTIs on all ports.
- If you specify an MSTI list but not a port, this command applies to all ports in the specified MSTIs.
- If you specify a port list but not an MSTI, this command applies to all MSTIs on the specified ports.
- If you specify both an MSTI list and a port list, this command applies to the specified ports in the specified MSTIs.

Examples

In MSTP mode, display the brief spanning tree status and statistics for MSTI 0 on ports GigabitEthernet 2/0/1 through GigabitEthernet 2/0/4.

```
<Sysname> display stp instance 0 interface gigabitethernet 2/0/1 to gigabitethernet 2/0/4 brief
```

MST ID	Port	Role	STP State	Protection
0	GigabitEthernet2/0/1	ALTE	DISCARDING	LOOP
0	GigabitEthernet2/0/2	DESI	FORWARDING	NONE
0	GigabitEthernet2/0/3	DESI	FORWARDING	NONE
0	GigabitEthernet2/0/4	DESI	FORWARDING	NONE

In PVST mode, display the brief spanning tree status and statistics for VLAN 2 on ports GigabitEthernet 2/0/1 through GigabitEthernet 2/0/4.

```
<Sysname> system-view
```

```
[Sysname] stp mode pvst
```

```
[Sysname] display stp vlan 2 interface gigabitethernet 2/0/1 to gigabitethernet 2/0/4 brief
```

VLAN ID	Port	Role	STP State	Protection
2	GigabitEthernet2/0/1	ALTE	DISCARDING	LOOP
2	GigabitEthernet2/0/2	DESI	FORWARDING	NONE

```

2          GigabitEthernet2/0/3          DESI  FORWARDING  NONE
2          GigabitEthernet2/0/4          DESI  FORWARDING  NONE

```

Table 24 Command output

Field	Description
MST ID	MSTI ID in the MST region.
Port	Port name, corresponding to each MSTI or VLAN.
Role	Port role: <ul style="list-style-type: none"> • ALTE—The port is an alternate port. • BACK—The port is a backup port. • ROOT—The port is a root port. • DESI—The port is a designated port. • MAST—The port is a master port. • DISA—The port is disabled.
STP State	Spanning tree status on the port: <ul style="list-style-type: none"> • FORWARDING—The port can receive and send BPDUs and also forward user traffic. • DISCARDING—The port can receive and send BPDUs but cannot forward user traffic. • LEARNING—The port is in a transitional state. It can receive and send BPDUs but cannot forward user traffic.
Protection	Effective spanning tree protection feature on the port: <ul style="list-style-type: none"> • ROOT—Root guard. • LOOP—Loop guard. • BPDU—BPDU guard. <p>If no spanning tree protection feature is configured or spanning tree protection is not triggered, this field displays NONE.</p>

In MSTP mode, display the detailed spanning tree status and statistics for all MSTIs on all ports.

```

<Sysname> display stp
-----[CIST Global Info][Mode MSTP]-----
Bridge ID          : 32768.0001-0000-0000
Bridge times       : Hello 2s MaxAge 20s FwdDelay 15s MaxHops 20
Root ID/ERPC      : 32768.0001-0000-0000, 0
RegRoot ID/IRPC   : 32768.0001-0000-0000, 0
RootPort ID       : 0.0
BPDU-Protection   : Disabled
Bridge Config-
Digest-Snooping   : Disabled
TC or TCN received : 2
Time since last TC : 0 days 0h:0m:58s

----[Port3(GigabitEthernet2/0/2)][FORWARDING]----
Port protocol      : Enabled
Port role          : Designated Port (Boundary)
Port ID            : 128.3
Port cost(Legacy)  : Config=auto, Active=200
Desg.bridge/port   : 32768.0001-0000-0000, 128.3
Port edged         : Config=disabled, Active=disabled

```

```

Point-to-Point      : Config=auto, Active=true
Transmit limit      : 10 packets/hello-time
TC-Restriction      : Disabled
Role-Restriction    : Disabled
Protection type     : Config=none, Active=none
MST BPDU format     : Config=auto, Active=802.1s
Port Config-
Digest-Snooping     : Disabled
Rapid transition    : True
Num of VLANs mapped : 0
Port times          : Hello 2s MaxAge 20s FwdDelay 15s MsgAge 0s RemHops 20
BPDU sent           : 32
                    TCN: 0, Config: 0, RST: 0, MST: 32
BPDU received       : 2
                    TCN: 0, Config: 0, RST: 0, MST: 2

```

-----[MSTI 1 Global Info]-----

```

Bridge ID           : 32768.0001-0000-0000
RegRoot ID/IRPC    : 32768.0001-0000-0000, 0
RootPort ID        : 0.0
Master bridge       : 32768.0001-0000-0000
Cost to master      : 0
TC received         : 0

```

----[Port3(GigabitEthernet2/0/2)][FORWARDING]----

```

Port protocol       : Enabled
Port role           : Designated Port (Boundary)
Port ID             : 128.3
Port cost(Legacy)   : Config=auto, Active=200
Desg.bridge/port    : 32768.0001-0000-0000, 128.3
Protection type     : Config=none, Active=none
Rapid transition    : True
Num of VLANs mapped : 64
Port times          : RemHops 20

```

In PVST mode, display the spanning tree status and statistics for all ports in all VLANs.

```
<Sysname> system-view
```

```
[Sysname] stp mode pvst
```

```
[Sysname] display stp
```

-----[VLAN 1 Global Info]-----

```

Protocol status     : Enabled
Bridge ID           : 32768.000f-e200-2200
Bridge times        : Hello 2s MaxAge 20s FwdDelay 15s
VlanRoot ID/RPC    : 0.00e0-fc0e-6554, 200200
RootPort ID        : 128.48
BPDU-Protection     : Disabled
TC or TCN received  : 2
Time since last TC  : 0 days 0h:5m:42s

```

```
----[Port1(GigabitEthernet2/0/1)][FORWARDING]----
Port protocol      : Enabled
Port role          : Designated Port
Port ID            : 128.153
Port cost(Legacy)  : Config=auto, Active=200
Desg. bridge/port  : 32768.000f-e200-2200, 128.2
Port edged         : Config=disabled, Active=disabled
Point-to-Point    : Config=auto, Active=true
Transmit limit     : 10 packets/hello-time
Protection type    : Config=none, Active=none
Rapid transition   : False
Port times         : Hello 2s MaxAge 20s FwdDelay 15s MsgAge 2s
```

```
-----[VLAN 2 Global Info]-----
Protocol status    : Enabled
Bridge ID          : 32768.000f-e200-2200
Bridge times       : Hello 2s MaxAge 20s FwDly 15s
VlanRoot ID/RPC    : 0.00e0-fc0e-6554, 200200
RootPort ID        : 128.48
BPDU-Protection    : Disabled
TC or TCN received : 2
Time since last TC : 0 days 0h:5m:42s
```

In MSTP mode, display the spanning tree status and statistics when the spanning tree feature is disabled.

```
<Sysname> display stp
Protocol status    : Disabled
Protocol Std.      : IEEE 802.1s
Version           : 3
Bridge-Prio.       : 32768
MAC address        : 000f-e200-8048
Max age(s)         : 20
Forward delay(s)   : 15
Hello time(s)      : 2
Max hops           : 20
TC Snooping        : Disabled
```

In PVST mode, display the spanning tree status and statistics when the spanning tree feature is disabled.

```
<Sysname> display stp
Protocol status    : Disabled
Protocol Std.      : IEEE 802.1w (pvst)
Version           : 2
Bridge-Prio.       : 32768
MAC address        : 3822-d69f-0800
Max age(s)         : 20
Forward delay(s)   : 15
Hello time(s)      : 2
TC Snooping        : Disabled
```

Table 25 Command output

Field	Description
Bridge ID	Bridge ID, which contains the device's priority and its MAC address. For example, in output 32768.000f-e200-2200, the value preceding the dot is the device's priority. The value following the dot is the device's MAC address.
Bridge times	Major parameters for the bridge: <ul style="list-style-type: none"> • Hello—Hello timer. • MaxAge—Maximum age timer. • FwdDelay—Forward delay timer. • MaxHops—Maximum hops within the MST region.
Root ID/ERPC	CIST root ID and external path cost (the path cost from the device to the CIST root).
RegRoot ID/IRPC	CIST regional root ID and internal path cost (the path cost from the device to the CIST regional root).
VlanRoot ID/RPC	VLAN root ID and root path cost (the path cost from the device to the VLAN root bridge).
RootPort ID	Root port ID. The value 0.0 indicates that the device is the root and there is no root port.
BPDU-Protection	Global status of the BPDU guard feature.
Bridge Config-Digest-Snooping	Global status of Digest Snooping.
TC or TCN received	Number of TC/TCN BPDUs received in the MSTI or VLAN.
Time since last TC	Time since the latest topology change in the MSTI or VLAN.
[FORWARDING]	The port is in forwarding state.
[DISCARDING]	The port is in discarding state.
[LEARNING]	The port is in learning state.
Port protocol	Status of the spanning tree feature on the port.
Port role	Port role: <ul style="list-style-type: none"> • Alternate. • Backup. • Root. • Designated. • Master. • Disabled.
(Boundary)	The port is a regional boundary port.
Port cost(Legacy)	Path cost of the port. The field in parentheses indicates the standard (legacy, dot1d-1998, or dot1t) used for port path cost calculation. <ul style="list-style-type: none"> • Config—Configured value. • Active—Actual value.
Desg.bridge/port	Designated bridge ID and port ID of the port. The port ID displayed is insignificant for a port which does not support port priority.
Port edged	The port is an edge port or non-edge port. <ul style="list-style-type: none"> • Config—Configured value. • Active—Actual value.
Point-to-Point	The port is connected to a point-to-point link or not. <ul style="list-style-type: none"> • Config—Configured value.

Field	Description
	<ul style="list-style-type: none"> • Active—Actual value.
Transmit limit	Maximum number of BPDUs sent by a port within each hello time.
Protection type	<p>Whether spanning tree protection is configured on the port:</p> <ul style="list-style-type: none"> • Config—Configured spanning tree protection feature. • Active—Effective spanning tree protection feature. <p>Spanning tree protection features are as follows:</p> <ul style="list-style-type: none"> • ROOT—Root guard. • LOOP—Loop guard. • BPDU—BPDU guard. • PVST BPDU—PVST BPDU guard. <p>If no spanning tree protection feature is configured or spanning tree protection is not triggered, this field displays NONE.</p>
TC-Restriction	Status of TC transmission restriction on the port.
Role-Restriction	Status of port role restriction on the port.
MST BPDU format	<p>Format of the MST BPDUs that the port can send:</p> <ul style="list-style-type: none"> • Config—Configured value (legacy or 802.1s). • Active—Actual value (legacy or 802.1s).
Port Config-Digest-Snooping	Status of Digest Snooping on the port.
Rapid transition	Indicates whether the port rapidly transits to the forwarding state in the MSTI or VLAN.
Num of VLANs mapped	Number of VLANs that are mapped to the MSTI.
Port times	<p>Major parameters for the port:</p> <ul style="list-style-type: none"> • Hello—Hello timer. • MaxAge—Maximum age timer. • FwdDelay—Forward delay timer. • MsgAge—Message age timer. • RemHops—Remaining hops.
BPDU sent	Statistics on sent BPDUs.
BPDU received	Statistics on received BPDUs.
RegRoot ID/IRPC	MSTI regional root/internal path cost.
Root Type	<p>MSTI root type:</p> <ul style="list-style-type: none"> • Primary root. • Secondary root.
Master bridge	MSTI root bridge ID.
Cost to master	Path cost from the MSTI to the master bridge.
TC received	Number of received TC BPDUs.
Protocol status	Spanning tree protocol status.
Protocol Std.	Spanning tree protocol standard.
Version	Spanning tree protocol version.
Bridge-Prio.	<ul style="list-style-type: none"> • In MSTP mode: Device's priority in the CIST. • In PVST mode: Device's priority in VLAN 1.

Field	Description
Max age(s)	Aging timer for BPDUs (in seconds, which is the same as the aging timer for VLAN 1 in PVST mode).
Forward delay(s)	Port state transition delay (in seconds, which is the same as the port state transition delay for VLAN 1 in PVST mode).
Hello time(s)	Interval for the root bridge to send BPDUs (in seconds, which is the same as the interval for VLAN 1 in PVST mode).
Max hops	Maximum hops in the MSTI.
TC Snooping	Status of TC Snooping: Enabled or Disabled .

Related commands

reset stp

display stp abnormal-port

Use **display stp abnormal-port** to display information about ports that are blocked by spanning tree protection features.

Syntax

display stp abnormal-port

Views

Any view

Predefined user roles

network-admin

network-operator

Examples

In MSTP mode, display information about ports that are blocked by spanning tree protection features.

```
<Sysname> display stp abnormal-port
MST ID      Blocked Port          Reason
1           GigabitEthernet2/0/1  Root-Protected
2           GigabitEthernet2/0/2  Loop-Protected
12          GigabitEthernet2/0/3  Loopback-Protected
```

In PVST mode, display information about ports that are blocked by spanning tree protection features.

```
<Sysname> system-view
[Sysname] stp mode pvst
[Sysname] display stp abnormal-port
VLAN ID     Blocked Port          Reason
1           GigabitEthernet2/0/1  Root-Protected
2           GigabitEthernet2/0/2  Loop-Protected
2           GigabitEthernet2/0/3  Loopback-Protected
```

Table 26 Command output

Field	Description
MST ID	MSTI of a blocked port.

Field	Description
VLAN ID	VLAN of a blocked port.
Blocked Port	Name of a blocked port.
Reason	Reason that the port was blocked: <ul style="list-style-type: none"> • Root-Protected—Root guard feature. • Loop-Protected—Loop guard feature. • Loopback-Protected—Self-loop protection. A port in the MSTI receives a BPDU sent by itself. • Disputed—Dispute protection. A port receives a low-priority BPDU from a non-blocked designated port. • InconsistentPortType-Protected—Inconsistent port type protection. • InconsistentPvid-Protected—Inconsistent PVID protection.

display stp bpdu-statistics

Use **display stp bpdu-statistics** to display the BPDU statistics for ports.

Syntax

display stp bpdu-statistics [**interface** *interface-type interface-number* [**instance** *instance-list*]]

Views

Any view

Predefined user roles

network-admin
network-operator

Parameters

interface *interface-type interface-number*. Specifies an interface by its type and number.

instance *instance-list*. Specifies a space-separated list of up to 10 MSTI items. Each item specifies an MSTI or a range of MSTIs in the form of *instance-id1* [**to** *instance-id2*]. The value for *instance-id2* must be equal to or greater than the value for *instance-id1*. The value range for the *instance-id* argument is 0 to 4094, and the value 0 represents the CIST.

Usage guidelines

In MSTP mode, the command output is sorted by port name and by MSTI ID on each port.

- If you do not specify an MSTI or port, this command applies to all MSTIs on all ports.
- If you specify a port but not an MSTI, this command applies to all MSTIs on the port.
- If you specify both an MSTI ID and a port, this command applies to the specified MSTI on the port.

In STP, RSTP, or PVST mode, the command output is sorted by port name.

- If you do not specify a port, this command applies to all ports.
- If you specify a port, this command applies to the port.

Examples

In MSTP mode, display the BPDU statistics for all MSTIs on GigabitEthernet 2/0/1.

```
<Sysname> display stp bpdu-statistics interface gigabitethernet 2/0/1
Port: GigabitEthernet2/0/1
```

Instance-Independent:

Type	Count	Last Updated
Invalid BPDUs	0	
Looped-back BPDUs	0	
Max-aged BPDUs	0	
TCN sent	0	
TCN received	0	
TCA sent	0	
TCA received	2	10:33:12 01/13/2011
Config sent	0	
Config received	0	
RST sent	0	
RST received	0	
MST sent	4	10:33:11 01/13/2011
MST received	151	10:37:43 01/13/2011

Instance 0:

Type	Count	Last Updated
Timeout BPDUs	0	
Max-hoped BPDUs	0	
TC detected	1	10:32:40 01/13/2011
TC sent	3	10:33:11 01/13/2011
TC received	0	

In PVST mode, display the BPDU statistics for GigabitEthernet 2/0/1.

```
<Sysname> system-view
[Sysname] stp mode pvst
[Sysname] display stp bpdu-statistics interface gigabitethernet 2/0/1
Port: GigabitEthernet2/0/1
```

Type	Count	Last Updated
Invalid BPDUs	0	
Looped-back BPDUs	0	
Max-aged BPDUs	0	
TCN sent	0	
TCN received	0	
TCA sent	0	
TCA received	2	10:33:12 01/13/2010
Config sent	0	
Config received	0	
RST sent	0	
RST received	0	
MST sent	4	10:33:11 01/13/2010
MST received	151	10:37:43 01/13/2010
Timeout BPDUs	0	
Max-hoped BPDUs	0	

TC detected	511	10:32:40	01/13/2010
TC sent	8844	10:33:11	01/13/2010
TC received	1426	10:33:32	01/13/2010
PVID inconsistency BPDUs	0		

Table 27 Command output

Field	Description
Port	Port name.
Instance-Independent	Statistics not related to a specific MSTI.
Type	Statistical item.
Looped-back BPDUs	Number of BPDUs sent and then received by the same port.
Max-aged BPDUs	Number of BPDUs whose max age was exceeded.
TCN sent	Number of sent TCN BPDUs.
TCN received	Number of received TCN BPDUs.
TCA sent	Number of sent TCA BPDUs.
TCA received	Number of received TCA BPDUs.
Config sent	Number of sent configuration BPDUs.
Config received	Number of received configuration BPDUs.
RST sent	Number of sent RSTP BPDUs.
RST received	Number of received RSTP BPDUs.
MST sent	Number of sent MSTP BPDUs.
MST received	Number of received MSTP BPDUs.
Instance	Statistics for a specific MSTI.
Timeout BPDUs	Number of expired BPDUs.
Max-hoped BPDUs	Number of BPDUs whose maximum hops were exceeded.
TC detected	Number of detected topology changes.
TC sent	Number of sent TC BPDUs.
TC received	Number of received TC BPDUs.
PVID inconsistency BPDUs	Number of received PVST BPDUs with a PVID inconsistent with the incoming port.

display stp down-port

Use **display stp down-port** to display information about ports that were shut down by spanning tree protection features.

Syntax

display stp down-port

Views

Any view

Predefined user roles

network-admin

network-operator

Examples

Display information about ports that were shut down by spanning tree protection features.

```
<Sysname> display stp down-port
Down Port                               Reason
GigabitEthernet2/0/1                   BPDU protection
```

Table 28 Command output

Field	Description
Down Port	Name of a port that was shut down by the spanning tree protection features.
Reason	Reason that the port was shut down: <ul style="list-style-type: none">• BPDU protection—Indicates the BPDU guard feature.• PVST BPDU protection—Indicates the PVST BPDU guard feature.

display stp history

Use **display stp history** to display port role calculation history.

Syntax

Centralized devices in standalone mode:

```
display stp [ instance instance-list | vlan vlan-id-list ] history
```

Distributed devices in standalone mode/centralized devices in IRF mode:

```
display stp [ instance instance-list | vlan vlan-id-list ] history [ slot slot-number ]
```

Distributed devices in IRF mode:

```
display stp [ instance instance-list | vlan vlan-id-list ] history [ chassis chassis-number slot slot-number ]
```

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

instance *instance-list*. Specifies a space-separated list of up to 10 MSTI items. Each item specifies an MSTI or a range of MSTIs in the form of *instance-id1* [**to** *instance-id2*]. The value for *instance-id2* must be equal to or greater than the value for *instance-id1*. The value range for the *instance-id* argument is 0 to 4094, and the value 0 represents the CIST.

vlan *vlan-id-list*. Specifies a space-separated list of up to 10 VLAN items. Each item specifies a VLAN or a range of VLANs in the form of *vlan-id1* [**to** *vlan-id2*]. The value for *vlan-id2* must be equal to or greater than the value for *vlan-id1*. The value range for the *vlan-id* argument is 1 to 4094.

slot *slot-number*. Specifies a card by its slot number. If you do not specify a card, this command displays information for all cards. (Distributed devices in standalone mode.)

slot *slot-number*. Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays information for all member devices. (Centralized devices in IRF mode.)

chassis chassis-number slot slot-number. Specifies a card on an IRF member device. The *chassis-number* argument represents the member ID of the IRF member device. The *slot-number* argument represents the slot number of the card. If you do not specify a card, this command displays information for all cards. (Distributed devices in IRF mode.)

Usage guidelines

In STP or RSTP mode, the command output is sorted by port role calculation time.

In PVST mode, the command output is sorted by VLAN ID and by port role calculation time in each VLAN.

- If you do not specify a VLAN, this command applies to all VLANs.
- If you specify a VLAN list, this command applies to the specified VLANs.

In MSTP mode, the command output is sorted by MSTI ID and by port role calculation time in each MSTI.

- If you do not specify an MSTI, this command applies to all MSTIs.
- If you specify an MSTI list, this command applies to the specified MSTIs.

Examples

(Centralized devices in standalone mode.) In MSTP mode, display the port role calculation history for MSTI 2.

```
<Sysname> display stp instance 2 history
----- Instance 2 -----

Port GigabitEthernet2/0/1
  Role change       : ROOT->DESI (Aged)
  Time              : 2009/02/08 00:22:56
  Port priority     : 0.00e0-fc01-6510 0 0.00e0-fc01-6510 128.1
  Designated priority : 0.00e0-fc01-6510 0 0.00e0-fc01-6510 128.1

Port GigabitEthernet2/0/2
  Role change       : ALTER->ROOT
  Time              : 2009/02/08 00:22:56
  Port priority     : 0.00e0-fc01-6510 0 0.00e0-fc01-6510 128.2
                    128.153
  Designated priority : 0.00e0-fc01-6510 0 0.00e0-fc01-6510 128.2
                    128.153
```

(Centralized devices in standalone mode.) In PVST mode, display the port role calculation history for VLAN 2.

```
<Sysname> display stp vlan 2 history
----- VLAN 2 -----

Port GigabitEthernet2/0/1
  Role change       : ROOT->DESI (Aged)
  Time              : 2009/02/08 00:22:56
  Port priority     : 0.00e0-fc01-6510 0 0.00e0-fc01-6510 128.1
  Designated priority : 0.00e0-fc01-6510 0 0.00e0-fc01-6510 128.1

Port GigabitEthernet2/0/2
  Role change       : ALTER->ROOT
  Time              : 2009/02/08 00:22:56
  Port priority     : 0.00e0-fc01-6510 0 0.00e0-fc01-6510 128.2
```

Designated priority : 0.00e0-fc01-6510 0 0.00e0-fc01-6510 128.2

(Distributed devices in standalone mode.) In MSTP mode, display the port role calculation history for the card on slot 1 in MSTI 2.

```
<Sysname> display stp instance 2 history slot 1
----- STP slot 1 history trace -----
----- Instance 2 -----
Port GigabitEthernet2/0/1
  Role change      : ROOT->DESI (Aged)
  Time            : 2009/02/08 00:22:56
  Port priority    : 0.00e0-fc01-6510 0 0.00e0-fc01-6510 128.1
  Designated priority : 0.00e0-fc01-6510 0 0.00e0-fc01-6510 128.1
Port GigabitEthernet2/0/2
  Role change      : ALTER->ROOT
  Time            : 2009/02/08 00:22:56
  Port priority    : 0.00e0-fc01-6510 0 0.00e0-fc01-6510 128.2
                  128.153
  Designated priority : 0.00e0-fc01-6510 0 0.00e0-fc01-6510 128.2
                  128.153
```

(Distributed devices in standalone mode.) In PVST mode, display the port role calculation history for the card on slot 1 in VLAN 2.

```
<Sysname> display stp vlan 2 history slot 1
----- STP slot 1 history trace -----
----- VLAN 2 -----

Port GigabitEthernet2/0/1
  Role change      : ROOT->DESI (Aged)
  Time            : 2009/02/08 00:22:56
  Port priority    : 0.00e0-fc01-6510 0 0.00e0-fc01-6510 128.1
  Designated priority : 0.00e0-fc01-6510 0 0.00e0-fc01-6510 128.1
Port GigabitEthernet2/0/2
  Role change      : ALTER->ROOT
  Time            : 2009/02/08 00:22:56
  Port priority    : 0.00e0-fc01-6510 0 0.00e0-fc01-6510 128.2
  Designated priority : 0.00e0-fc01-6510 0 0.00e0-fc01-6510 128.2
```

(Centralized devices in IRF mode.) In MSTP mode, display the port role calculation history for IRF member device 1 in MSTI 2.

```
<Sysname> display stp instance 2 history slot 1
----- STP slot 1 history trace -----
----- Instance 2 -----
Port GigabitEthernet2/0/1
  Role change      : ROOT->DESI (Aged)
  Time            : 2009/02/08 00:22:56
  Port priority    : 0.00e0-fc01-6510 0 0.00e0-fc01-6510 128.1
  Designated priority : 0.00e0-fc01-6510 0 0.00e0-fc01-6510 128.1
Port GigabitEthernet2/0/2
  Role change      : ALTER->ROOT
  Time            : 2009/02/08 00:22:56
  Port priority    : 0.00e0-fc01-6510 0 0.00e0-fc01-6510 128.2
```

```
128.153
Designated priority : 0.00e0-fc01-6510 0 0.00e0-fc01-6510 128.2
128.153
```

(Centralized devices in IRF mode.) In PVST mode, display the port role calculation history for IRF member device 1 in VLAN 2.

```
<Sysname> display stp vlan 2 history slot 1
----- STP slot 1 history trace -----
----- VLAN 2 -----
Port GigabitEthernet2/0/1
Role change      : ROOT->DESI (Aged)
Time             : 2009/02/08 00:22:56
Port priority    : 0.00e0-fc01-6510 0 0.00e0-fc01-6510 128.1
Designated priority : 0.00e0-fc01-6510 0 0.00e0-fc01-6510 128.1
Port GigabitEthernet2/0/2
Role change      : ALTER->ROOT
Time             : 2009/02/08 00:22:56
Port priority    : 0.00e0-fc01-6510 0 0.00e0-fc01-6510 128.2
Designated priority : 0.00e0-fc01-6510 0 0.00e0-fc01-6510 128.2
```

(Distributed devices in IRF mode.) In MSTP mode, display the port role calculation history for the card on slot 1 of IRF member device 1 in MSTI 2.

```
<Sysname> display stp instance 2 history chassis 1 slot 1
----- STP chassis 1 slot 1 history trace -----
----- Instance 2 -----
Port GigabitEthernet1/2/0/1
Role change      : ROOT->DESI (Aged)
Time             : 2009/02/08 00:22:56
Port priority    : 0.00e0-fc01-6510 0 0.00e0-fc01-6510 128.1
Designated priority : 0.00e0-fc01-6510 0 0.00e0-fc01-6510 128.1
Port GigabitEthernet1/2/0/2
Role change      : ALTER->ROOT
Time             : 2009/02/08 00:22:56
Port priority    : 0.00e0-fc01-6510 0 0.00e0-fc01-6510 128.2
128.153
Designated priority : 0.00e0-fc01-6510 0 0.00e0-fc01-6510 128.2
128.153
```

(Distributed devices in IRF mode.) In PVST mode, display the port role calculation history for the card on slot 1 of IRF member device 1 in VLAN 2.

```
<Sysname> display stp vlan 2 history chassis 1 slot 1
----- STP chassis 1 slot 1 history trace -----
----- VLAN 2 -----
Port GigabitEthernet1/2/0/1
Role change      : ROOT->DESI (Aged)
Time             : 2009/02/08 00:22:56
Port priority    : 0.00e0-fc01-6510 0 0.00e0-fc01-6510 128.1
Designated priority : 0.00e0-fc01-6510 0 0.00e0-fc01-6510 128.1
Port GigabitEthernet1/2/0/2
Role change      : ALTER->ROOT
Time             : 2009/02/08 00:22:56
```

```

Port priority      : 0.00e0-fc01-6510 0 0.00e0-fc01-6510 128.2
Designated priority : 0.00e0-fc01-6510 0 0.00e0-fc01-6510 128.2

```

Table 29 Command output

Field	Description
Port	Port name.
Role change	Role change of the port (Aged means that the change was caused by expiration of the received configuration BPDU).
Time	Time of port role calculation.

display stp region-configuration

Use **display stp region-configuration** to display effective MST region configuration, including the region name, revision level, and user-configured VLAN-to-instance mappings.

Syntax

```
display stp region-configuration
```

Views

Any view

Predefined user roles

```

network-admin
network-operator

```

Examples

In MSTP mode, display effective MST region configuration.

```

<Sysname> display stp region-configuration
Oper Configuration
  Format selector      : 0
  Region name         : hello
  Revision level      : 0
  Configuration digest : 0x5f762d9a46311effb7a488a3267fca9f

Instance  VLANs Mapped
  0        21 to 4094
  1         1 to 10
  2        11 to 20

```

Table 30 Command output

Field	Description
Format selector	Format selector that is defined by the spanning tree protocol. The default value is 0, and the selector cannot be configured.
Region name	MST region name.
Revision level	Revision level of the MST region. The default value is 0, and the level can be configured by using the revision-level command.
VLANs Mapped	VLANs mapped to the MSTI.

Related commands

instance
region-name
revision-level
vlan-mapping modulo

display stp root

Use **display stp root** to display the root bridge information of spanning trees.

Syntax

display stp root

Views

Any view

Predefined user roles

network-admin
network-operator

Examples

In MSTP mode, display the root bridge information of all spanning trees.

```
<Sysname> display stp root
MST ID  Root Bridge ID      ExtPathCost  IntPathCost  Root Port
0        0.00e0-fc0e-6554        200200      0            GigabitEthernet2/0/1
```

In PVST mode, display the root bridge information of all spanning trees.

```
<Sysname> display stp root
VLAN ID  Root Bridge ID      ExtPathCost  IntPathCost  Root Port
1        0.00e0-fc0e-6554        200200      0            GigabitEthernet2/0/1
```

Table 31 Command output

Field	Description
ExtPathCost	External path cost. The default path cost of a port is either automatically calculated by the device or manually configured by using the stp cost command.
IntPathCost	Internal path cost. The default path cost of a port is either automatically calculated by the device or manually configured by using the stp cost command.
Root Port	Root port name (displayed only if a port of the device is the root port of the MSTI).

display stp tc

Use **display stp tc** to display the incoming and outgoing TC/TCN BPDU statistics for ports.

Syntax

Centralized devices in standalone mode:

display stp [instance *instance-list* | vlan *vlan-id-list*] tc

Distributed devices in standalone mode/centralized devices in IRF mode:

display stp [instance *instance-list* | vlan *vlan-id-list*] tc [slot *slot-number*]

Distributed devices in IRF mode:

```
display stp [ instance instance-list | vlan vlan-id-list ] tc [ chassis chassis-number slot slot-number ]
```

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

instance *instance-list*. Specifies a space-separated list of up to 10 MSTI items. Each item specifies an MSTI or a range of MSTIs in the form of *instance-id1* [**to** *instance-id2*]. The value for *instance-id2* must be equal to or greater than the value for *instance-id1*. The value range for the *instance-id* argument is 0 to 4094, and the value 0 represents the CIST.

vlan *vlan-id-list*. Specifies a space-separated list of up to 10 VLAN items. Each item specifies a VLAN or a range of VLANs in the form of *vlan-id1* [**to** *vlan-id2*]. The value for *vlan-id2* must be equal to or greater than the value for *vlan-id1*. The value range for the *vlan-id* argument is 1 to 4094.

slot *slot-number*. Specifies a card by its slot number. If you do not specify a card, this command displays information for all cards. (Distributed devices in standalone mode.)

slot *slot-number*. Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays information for all member devices. (Centralized devices in IRF mode.)

chassis *chassis-number* **slot** *slot-number*. Specifies a card on an IRF member device. The *chassis-number* argument represents the member ID of the IRF member device. The *slot-number* argument represents the slot number of the card. If you do not specify a card, this command displays information for all cards. (Distributed devices in IRF mode.)

Usage guidelines

In STP or RSTP mode, the command output is sorted by port name.

In PVST mode, the command output is sorted by VLAN ID and by port name in each VLAN.

- If you do not specify a VLAN, this command applies to all VLANs.
- If you specify a VLAN list, this command applies to the specified VLANs.

In MSTP mode, the command output is sorted by MSTI ID and by port name in each MSTI.

- If you do not specify an MSTI, this command applies to all MSTIs.
- If you specify an MSTI list, this command applies to the specified MSTIs.

Examples

(Centralized devices in standalone mode.) In MSTP mode, display the incoming and outgoing TC/TCN BPDU statistics for all ports in MSTI 0.

```
<Sysname> display stp instance 0 tc
```

MST ID	Port	Receive	Send
0	GigabitEthernet2/0/1	6	4
0	GigabitEthernet2/0/2	0	2

(Centralized devices in standalone mode.) In PVST mode, display the incoming and outgoing TC/TCN BPDU statistics for all ports in VLAN 2.

```
<Sysname> display stp vlan 2 tc
```

VLAN ID	Port	Receive	Send
2	GigabitEthernet2/0/1	6	4

```
2          GigabitEthernet2/0/2          0          2
```

(Distributed devices in standalone mode.) In MSTP mode, display the incoming and outgoing TC/TCN BPDU statistics for all ports on the card on slot 1 in MSTI 0.

```
<Sysname> display stp instance 0 tc slot 1
----- STP slot 1 TC or TCN count -----
MST ID      Port                               Receive      Send
0           GigabitEthernet2/0/1                6            4
0           GigabitEthernet2/0/2                0            2
```

(Distributed devices in standalone mode.) In PVST mode, display the incoming and outgoing TC/TCN BPDU statistics for all ports on slot 1 in VLAN 2.

```
<Sysname> display stp vlan 2 tc slot 1
----- STP slot 1 TC or TCN count -----
VLAN ID     Port                               Receive      Send
2           GigabitEthernet2/0/1                6            4
2           GigabitEthernet2/0/2                0            2
```

(Centralized devices in IRF mode.) In MSTP mode, display the incoming and outgoing TC/TCN BPDU statistics for all ports on IRF member device 1 in MSTI 0.

```
<Sysname> display stp instance 0 tc slot 1
----- STP slot 1 TC or TCN count -----
MST ID      Port                               Receive      Send
0           GigabitEthernet2/0/1                6            4
0           GigabitEthernet2/0/2                0            2
```

(Centralized devices in IRF mode.) In PVST mode, display the incoming and outgoing TC/TCN BPDU statistics for all ports on slot 1 of IRF member device 1 in VLAN 2.

```
<Sysname> display stp vlan 2 tc chassis 1 slot 1
----- STP chassis 1 slot 1 TC or TCN count -----
VLAN ID     Port                               Receive      Send
2           GigabitEthernet2/0/1                6            4
2           GigabitEthernet2/0/2                0            2
```

(Distributed devices in IRF mode.) In MSTP mode, display the incoming and outgoing TC/TCN BPDU statistics for all ports on slot 1 of IRF member device 1 in MSTI 0.

```
<Sysname> display stp instance 0 tc chassis 1 slot 1
----- STP chassis 1 slot 1 TC or TCN count -----
MST ID      Port                               Receive      Send
0           GigabitEthernet1/2/0/1                6            4
0           GigabitEthernet1/2/0/2                0            2
```

(Distributed devices in IRF mode.) In PVST mode, display the incoming and outgoing TC/TCN BPDU statistics for all ports on slot 1 of IRF member device 1 in VLAN 2.

```
<Sysname> display stp vlan 2 tc chassis 1 slot 1
----- STP chassis 1 slot 1 TC or TCN count -----
VLAN ID     Port                               Receive      Send
2           GigabitEthernet1/2/0/1                6            4
2           GigabitEthernet1/2/0/2                0            2
```

Table 32 Command output

Field	Description
Port	Port name.

Field	Description
Receive	Number of TC/TCN BPDUs received on a port.
Send	Number of TC/TCN BPDUs sent by a port.

instance

Use **instance** to map a list of VLANs to an MSTI.

Use **undo instance** to remap the specified VLAN or all VLANs to the CIST (MSTI 0).

Syntax

instance *instance-id* **vlan** *vlan-id-list*

undo instance *instance-id* [**vlan** *vlan-id-list*]

Default

All VLANs are mapped to the CIST.

Views

MST region view

Predefined user roles

network-admin

Parameters

instance-id: Specifies an MSTI ID in the range of 0 to 4094. A value of 0 represents the CIST. The value range for the *instance-id* argument is 1 to 4094 for the **undo instance** command.

vlan *vlan-id-list*: Specifies a space-separated list of up to 10 VLAN items. Each item specifies a VLAN or a range of VLANs in the form of *vlan-id1* [**to** *vlan-id2*]. The value for *vlan-id2* must be equal to or greater than the value for *vlan-id1*. The value range for the *vlan-id* argument is 1 to 4094.

Usage guidelines

CAUTION:

Use caution with global Digest Snooping in the following situations:

- When you modify the VLAN-to-instance mappings.
- When you restore the default MST region configuration.

If the local device has different VLAN-to-instance mappings than its neighboring devices, loops or traffic interruption will occur.

If you do not specify any VLANs in the **undo instance** command, all VLANs mapped to the specified MSTI are remapped to the CIST.

You cannot map a VLAN to different MSTIs. If you map a VLAN that has been mapped to an MSTI to a new MSTI, the old mapping is automatically deleted.

You can configure VLAN-to-instance mapping for up to 16 MSTIs.

After configuring this command, run the **active region-configuration** command to activate the VLAN-to-instance mapping.

Examples

```
# Map VLAN 2 to MSTI 1.
```

```
<Sysname> system-view
```

```
[Sysname] stp region-configuration
```

```
[Sysname-mst-region] instance 1 vlan 2
```

Related commands

active region-configuration
check region-configuration
display stp region-configuration

region-name

Use **region-name** to configure the MST region name.

Use **undo region-name** to restore the default MST region name.

Syntax

region-name *name*
undo region-name

Default

The MST region name of a device is its MAC address.

Views

MST region view

Predefined user roles

network-admin

Parameters

name: Specifies the MST region name, a string of 1 to 32 characters.

Usage guidelines

The MST region name, the VLAN-to-instance mapping table, and the MSTP revision level of a device determine the device's MST region.

After configuring this command, execute the **active region-configuration** command to activate the configured MST region name.

Examples

Set the MST region name of the device to **hello**.

```
<Sysname> system-view  
[Sysname] stp region-configuration  
[Sysname-mst-region] region-name hello
```

Related commands

active region-configuration
check region-configuration
display stp region-configuration
instance
revision-level
vlan-mapping modulo

reset stp

Use **reset stp** to clear the spanning tree statistics. The spanning tree statistics include the numbers of TCN BPDUs, configuration BPDUs, RST BPDUs, and MST BPDUs that are sent and received through the specified ports.

Syntax

```
reset stp [ interface interface-list ]
```

Views

User view

Predefined user roles

network-admin

Parameters

interface *interface-list*: Specifies a space-separated list of up to 10 interface items. Each item specifies an interface or a range of interfaces in the form of *interface-type interface-number 1* [**to** *interface-type interface-number 2*]. The interface number for *interface-number 2* must be equal to or greater than the interface number for *interface-number 1*. If you do not specify this option, this command clears the spanning tree statistics on all ports.

Examples

```
# Clear the spanning tree statistics on ports GigabitEthernet 2/0/1 through GigabitEthernet 2/0/3.  
<Sysname> reset stp interface gigabitethernet 2/0/1 to gigabitethernet 2/0/3
```

Related commands

display stp

revision-level

Use **revision-level** to configure the MSTP revision level.

Use **undo revision-level** to restore the default MSTP revision level.

Syntax

```
revision-level level  
undo revision-level
```

Default

The MSTP revision level is 0.

Views

MST region view

Predefined user roles

network-admin

Parameters

level: Specifies an MSTP revision level in the range of 0 to 65535.

Usage guidelines

The MSTP revision level, the MST region name, and the VLAN-to-instance mapping table of a device determine the device's MST region.

After configuring this command, execute the **active region-configuration** command to activate the configured MST region level.

Examples

```
# Set the MSTP revision level of the MST region to 5.
<Sysname> system-view
[Sysname] stp region-configuration
[Sysname-mst-region] revision-level 5
```

Related commands

active region-configuration
check region-configuration
display stp region-configuration
instance
region-name
vlan-mapping modulo

snmp-agent trap enable stp

Use **snmp-agent trap enable stp** to enable SNMP notifications for new-root election events or spanning tree topology changes.

Use **undo snmp-agent trap enable stp** to disable SNMP notifications for new-root election events or spanning tree topology changes.

Syntax

```
snmp-agent trap enable stp [ new-root | tc ]
undo snmp-agent trap enable stp [ new-root | tc ]
```

Default

SNMP notifications are disabled for new-root election events.

In MSTP mode, SNMP notifications are enabled in MSTI 0 and disabled in other MSTIs for spanning tree topology changes.

In PVST mode, SNMP notifications are disabled for spanning tree topology changes in all VLANs.

Views

System view

Predefined user roles

network-admin

Parameters

new-root: Enables the device to send notifications if the device is elected as a new root bridge. This keyword applies only to STP, MSTP, and RSTP modes.

tc: Enables the device to send notifications if the device receives TCN BPDUs. This keyword applies only to PVST mode.

Usage guidelines

If no keyword is specified, the **snmp-agent trap enable stp** command applies to SNMP notifications for different events as follows:

- In STP, MSTP, and RSTP modes, the command applies to SNMP notifications for new-root election events.

- In PVST mode, the command applies to SNMP notifications for spanning tree topology changes.

Examples

```
# Enable SNMP notifications for new-root election events.
<Sysname> system-view
[Sysname] snmp-agent trap enable stp new-root
```

stp bpdu-protection

Use **stp bpdu-protection** to enable BPDU guard.

Use **undo stp bpdu-protection** to disable BPDU guard.

Syntax

```
stp bpdu-protection
undo stp bpdu-protection
```

Default

BPDU guard is disabled.

Views

System view

Predefined user roles

network-admin

Examples

```
# Enable BPDU guard.
<Sysname> system-view
[Sysname] stp bpdu-protection
```

stp bridge-diameter

Use **stp bridge-diameter** to set the network diameter. The switched network diameter refers to the maximum number of devices on the path for an edge device to reach another through the root bridge.

Use **undo stp bridge-diameter** to restore the default.

Syntax

```
stp [ vlan vlan-id-list ] bridge-diameter diameter
undo stp [ vlan vlan-id-list ] bridge-diameter
```

Default

The network diameter of the switched network is 7.

Views

System view

Predefined user roles

network-admin

Parameters

vlan *vlan-id-list*: Specifies a space-separated list of up to 10 VLAN items. Each item specifies a VLAN or a range of VLANs in the form of *vlan-id1* [**to** *vlan-id2*]. The value for *vlan-id2* must be equal to or greater than the value for *vlan-id1*. The value range for the *vlan-id* argument is 1 to 4094. If you set the STP, RSTP, or MSTP switched network diameter, do not specify this option.

diameter: Specifies the switched network diameter in the range of 2 to 7.

Usage guidelines

An appropriate setting of hello time, forward delay, and max age can speed up network convergence. The values of these timers are related to the network size, and you can set the timers by setting the network diameter. With the network diameter set to 7 (the default), the three timers are also set to their defaults.

In STP, RSTP, or MSTP mode, each MST region is considered as a device. The configured network diameter of the switched network takes effect only on the CIST (or the common root bridge).

In PVST mode, the configured network diameter takes effect only on the root bridges of the specified VLANs.

Examples

In MSTP mode, set the network diameter of the switched network to 5.

```
<Sysname> system-view
[Sysname] stp bridge-diameter 5
```

In PVST mode, set the network diameter of VLAN 2 in the switched network to 5.

```
<Sysname> system-view
[Sysname] stp vlan 2 bridge-diameter 5
```

Related commands

stp timer forward-delay

stp timer hello

stp timer max-age

stp compliance

Use **stp compliance** to configure the mode a port uses to recognize and send MSTP BPDUs.

Use **undo stp compliance** to restore the default.

Syntax

stp compliance { auto | dot1s | legacy }

undo stp compliance

Default

A port automatically recognizes the formats of received MSTP packets and determines the formats of MSTP packets to be sent based on the recognized formats.

Views

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

Predefined user roles

network-admin

Parameters

auto: Configures the port to recognize the MSTP BPDU format automatically and determine the format of MSTP BPDUs to send.

dot1s: Configures the port to receive and send only standard-format (802.1s-compliant) MSTP BPDUs.

legacy: Configures the port to receive and send only compatible-format MSTP BPDUs.

Usage guidelines

If the command is configured in Layer 2 Ethernet interface view, it takes effect only on that interface.

If the command is configured in Layer 2 aggregate interface view, it takes effect only on the aggregate interface.

If the command is configured on a member port in an aggregation group, it takes effect only after the port leaves the aggregation group.

Examples

```
# Configure GigabitEthernet 2/0/1 to send only standard-format (802.1s) MSTP packets.
```

```
<Sysname> system-view
```

```
[Sysname] interface gigabitethernet 2/0/1
```

```
[Sysname-GigabitEthernet2/0/1] stp compliance dot1s
```

stp config-digest-snooping

Use **stp config-digest-snooping** to enable Digest Snooping.

Use **undo stp config-digest-snooping** to disable Digest Snooping.

Syntax

stp config-digest-snooping

undo stp config-digest-snooping

Default

Digest Snooping is disabled.

Views

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

Predefined user roles

network-admin

Usage guidelines

For Digest Snooping to take effect, you must enable Digest Snooping both globally and on associated ports. As a best practice, first enable Digest Snooping on ports connected to third-party vendor devices and then enable the feature globally. Digest Snooping takes effect on the ports simultaneously, which reduces impact on the network.

If the command is configured in Layer 2 Ethernet interface view, it takes effect only on that interface.

If the command is configured in Layer 2 aggregate interface view, it takes effect only on the aggregate interface.

If the command is configured on a member port in an aggregation group, it takes effect only after the port leaves the aggregation group.

Examples

```
# Enable Digest Snooping on GigabitEthernet 2/0/1 and then globally.
<Sysname> system-view
[Sysname] interface gigabitethernet 2/0/1
[Sysname-GigabitEthernet2/0/1] stp config-digest-snooping
[Sysname-GigabitEthernet2/0/1] quit
[Sysname] stp global config-digest-snooping
```

Related commands

display stp
stp global config-digest-snooping

stp cost

Use **stp cost** to set the path cost of a port.

Use **undo stp cost** to restore the default.

Syntax

```
stp [ instance instance-list | vlan vlan-id-list ] cost cost-value  
undo stp [ instance instance-list | vlan vlan-id-list ] cost
```

Default

The device automatically calculates the path costs of ports in each spanning tree based on the corresponding standard.

Views

Layer 2 Ethernet interface view
Layer 2 aggregate interface view

Predefined user roles

network-admin

Parameters

instance *instance-list*: Specifies a space-separated list of up to 10 MSTI items. Each item specifies an MSTI or a range of MSTIs in the form of *instance-id1* [**to** *instance-id2*]. The value for *instance-id2* must be equal to or greater than the value for *instance-id1*. The value range for the *instance-id* argument is 0 to 4094, and the value 0 represents the CIST.

vlan *vlan-id-list*: Specifies a space-separated list of up to 10 VLAN items. Each item specifies a VLAN or a range of VLANs in the form of *vlan-id1* [**to** *vlan-id2*]. The value for *vlan-id2* must be equal to or greater than the value for *vlan-id1*. The value range for the *vlan-id* argument is 1 to 4094.

cost-value: Specifies the path cost of the port, with an effective range that varies by path cost calculation standard that is used.

- When the IEEE 802.1d-1998 standard is selected for path cost calculation, the value range for the *cost* argument is 1 to 65535.
- When the IEEE 802.1t standard is selected for path cost calculation, the value range for the *cost* argument is 1 to 200000000.
- When the private standard is selected for path cost calculation, the value range for the *cost* argument is 1 to 200000.

Usage guidelines

Path cost is an important factor in spanning tree calculation. Setting different path costs for a port in MSTIs allows VLAN traffic flows to be forwarded along different physical links. This results in VLAN-based load balancing.

The path cost setting of a port can affect the role selection of the port. When the path cost of a port is changed, the system calculates the role of the port and initiates a state transition.

If the command is configured in Layer 2 Ethernet interface view, it takes effect only on that interface.

If the command is configured in Layer 2 aggregate interface view, it takes effect only on the aggregate interface.

If the command is configured on a member port in an aggregation group, it takes effect only after the port leaves the aggregation group.

If you do not specify an MSTI or VLAN, this command sets the path cost of a port in the MSTP CIST or in the STP or RSTP spanning tree.

Examples

In MSTP mode, set the path cost to 200 for GigabitEthernet 2/0/3 in MSTI 2.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 2/0/3
[Sysname-GigabitEthernet2/0/3] stp instance 2 cost 200
```

In PVST mode, set the path cost to 200 for GigabitEthernet 2/0/3 in VLAN 2.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 2/0/3
[Sysname-GigabitEthernet2/0/3] stp vlan 2 cost 200
```

Related commands

display stp

stp pathcost-standard

stp edged-port

Use **stp edged-port** to configure a port as an edge port.

Use **undo stp edged-port** to restore the default.

Syntax

stp edged-port

undo stp edged-port

Default

All ports are non-edge ports.

Views

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

Predefined user roles

network-admin

Usage guidelines

A port directly connecting to a user terminal rather than another device or a shared LAN segment can be configured as an edge port. In case the network topology changes, an edge port does not cause

a temporary loop. You can enable the port to transit to the forwarding state rapidly by configuring it as an edge port. As a best practice, configure ports that directly connect to user terminals as edge ports.

Typically, configuration BPDUs from other devices cannot reach an edge port, because the edge port does not connect to any other device. When BPDU guard is disabled, a port configured as an edge port acts as a non-edge port if it receives configuration BPDUs.

On a port, the loop guard feature and the edge port setting are mutually exclusive.

If the command is configured in Layer 2 Ethernet interface view, it takes effect only on that interface.

If the command is configured in Layer 2 aggregate interface view, it takes effect only on the aggregate interface.

If the command is configured on a member port in an aggregation group, it takes effect only after the port leaves the aggregation group.

Examples

```
# Configure GigabitEthernet 2/0/1 as an edge port.
<Sysname> system-view
[Sysname] interface gigabitethernet 2/0/1
[Sysname-GigabitEthernet2/0/1] stp edged-port
```

Related commands

stp bpd protection

stp loop-protection

stp root-protection

stp enable

Use **stp enable** to enable the spanning tree feature.

Use **undo stp enable** to disable the spanning tree feature.

Syntax

stp enable

undo stp enable

Default

The spanning tree feature is enabled on all ports.

Views

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

Predefined user roles

network-admin

Usage guidelines

When you enable the spanning tree feature, the device operates in STP, RSTP, PVST, or MSTP mode, depending on the spanning tree mode setting.

When you enable the spanning tree feature, the device dynamically maintains the spanning tree status of VLANs, based on received configuration BPDUs. When you disable the spanning tree feature, the device stops maintaining the spanning tree status.

If the command is configured in Layer 2 Ethernet interface view, it takes effect only on that interface.

If the command is configured in Layer 2 aggregate interface view, it takes effect only on the aggregate interface.

If the command is configured on a member port in an aggregation group, it takes effect only after the port leaves the aggregation group.

Examples

In MSTP mode, disable the spanning tree feature on GigabitEthernet 2/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 2/0/1
[Sysname-GigabitEthernet2/0/1] undo stp enable
```

Related commands

stp global enable

stp mode

stp vlan enable

stp global config-digest-snooping

Use **stp global config-digest-snooping** to enable Digest Snooping globally.

Use **undo stp global config-digest-snooping** to disable Digest Snooping globally.

Syntax

stp global config-digest-snooping

undo stp global config-digest-snooping

Default

Digest Snooping is disabled globally.

Views

System view

Predefined user roles

network-admin

Usage guidelines

For Digest Snooping to take effect, you must enable Digest Snooping both globally and on associated ports. As a best practice, first enable Digest Snooping on ports connected to third-party vendor devices and then enable the feature globally. Digest Snooping takes effect on the ports simultaneously, which reduces impact on the network.

Examples

Enable Digest Snooping on GigabitEthernet 2/0/1 and then globally.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 2/0/1
[Sysname-GigabitEthernet2/0/1] stp config-digest-snooping
[Sysname-GigabitEthernet2/0/1] quit
[Sysname] stp global config-digest-snooping
```

Related commands

display stp

stp config-digest-snooping

stp global enable

Use **stp global enable** to enable the spanning tree feature globally.

Use **undo stp global enable** to disable the spanning tree feature globally.

Syntax

stp global enable

undo stp global enable

Default

The spanning tree feature is globally disabled.

Views

System view

Predefined user roles

network-admin

Usage guidelines

When you enable the spanning tree feature, the device operates in STP, RSTP, PVST, or MSTP mode, depending on the spanning tree mode setting.

When the spanning tree feature is enabled, the device dynamically maintains the spanning tree status of VLANs based on received configuration BPDUs. When the spanning tree feature is disabled, the device stops maintaining the spanning tree status.

Examples

```
# Enable the spanning tree feature globally.
```

```
<Sysname> system-view
```

```
[Sysname] stp global enable
```

Related commands

stp enable

stp mode

stp global mcheck

Use **stp global mcheck** to perform mCheck globally.

Syntax

stp global mcheck

Views

System view

Predefined user roles

network-admin

Usage guidelines

When a port on an MSTP, RSTP, or PVST device connects to an STP device and receives STP BPDUs, the port automatically transits to the STP mode. However, the port cannot automatically transit back to the original mode when the following conditions exist:

- The peer STP device is shut down or removed.
- The port cannot detect the change.

In this case, you can perform an mCheck operation to forcibly transit the port to operate in the original mode.

The device operates in STP, RSTP, PVST, or MSTP mode, depending on the spanning tree mode setting.

The **stp global mcheck** command takes effect only when the device operates in MSTP, RSTP, or PVST mode.

Examples

```
# Perform mCheck globally.
<Sysname> system-view
[Sysname] stp global mcheck
```

Related commands

stp mcheck
stp mode

stp ignore-pvid-inconsistency

Use **stp ignore-pvid-inconsistency** to disable inconsistent PVID protection.

Use **undo stp ignore-pvid-inconsistency** to enable inconsistent PVID protection.

Syntax

stp ignore-pvid-inconsistency
undo stp ignore-pvid-inconsistency

Default

Inconsistent PVID protection is enabled.

Views

System view

Predefined user roles

network-admin

Usage guidelines

This command takes effect only when the device is operating in PVST mode.

Disabling inconsistent PVID protection might cause spanning tree calculation errors. To avoid such errors, make sure the following requirements are met:

- Make sure the VLANs on one device do not use the same ID as the PVID of its peer port (except the default VLAN) on another device.
- If the local port or its peer is a hybrid port, do not configure the local and peer ports as untagged members of the same VLAN.
- Disable inconsistent PVID protection on both the local device and the peer device.

Examples

```
# In PVST mode, disable the inconsistent PVID protection feature.
<Sysname> system-view
[Sysname] stp mode pvst
[Sysname] stp ignore-pvid-inconsistency
```

stp loop-protection

Use **stp loop-protection** to enable loop guard on a port.

Use **undo stp loop-protection** to disable loop guard on a port.

Syntax

stp loop-protection

undo stp loop-protection

Default

Loop guard is disabled.

Views

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

Predefined user roles

network-admin

Usage guidelines

On a port, the loop guard feature is mutually exclusive with the root guard feature or the edge port setting.

If the command is configured in Layer 2 Ethernet interface view, it takes effect only on that interface.

If the command is configured in Layer 2 aggregate interface view, it takes effect only on the aggregate interface.

If the command is configured on a member port in an aggregation group, it takes effect only after the port leaves the aggregation group.

Examples

Enable loop guard on GigabitEthernet 2/0/1.

```
<Sysname> system-view
```

```
[Sysname] interface gigabitethernet 2/0/1
```

```
[Sysname-GigabitEthernet2/0/1] stp loop-protection
```

Related commands

stp edged-port

stp root-protection

stp max-hops

Use **stp max-hops** to set the maximum number of hops for an MST region.

Use **undo stp max-hops** to restore the default.

Syntax

stp max-hops *hops*

undo stp max-hops

Default

The maximum number of hops for an MST region is 20.

Views

System view

Predefined user roles

network-admin

Parameters

hops: Specifies the maximum hops in the range of 1 to 40.

Examples

```
# Set the maximum hops of the MST region to 35.
```

```
<Sysname> system-view
```

```
[Sysname] stp max-hops 35
```

Related commands

display stp

stp mcheck

Use **stp mcheck** to perform mCheck on a port.

Syntax

stp mcheck

Views

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

Predefined user roles

network-admin

Usage guidelines

When a port on an MSTP, RSTP, or PVST device connects to an STP device and receives STP BPDUs, the port automatically transits to the STP mode. However, the port cannot automatically transit back to the original mode when the following conditions exist:

- The peer STP device is shut down or removed.
- The port cannot detect the change.

In this case, you can perform an mCheck operation to forcibly transit the port to operation in the original mode.

For example, Device A, Device B, and Device C are connected in sequence. Device A runs STP, Device B does not run any spanning tree protocol, and Device C runs RSTP, MSTP, or PVST. When Device C receives an STP BPDU transparently transmitted by Device B, the receiving port transits to the STP mode. If you configure Device B to run RSTP, MSTP, or PVST with Device C, perform mCheck operations on the ports that connect Device B and Device C.

The device operates in STP, RSTP, PVST, or MSTP mode, depending on the spanning tree mode setting.

The **stp mcheck** command takes effect only when the device operates in MSTP, RSTP, or PVST mode.

If the command is configured in Layer 2 Ethernet interface view, it takes effect only on that interface.

If the command is configured in Layer 2 aggregate interface view, it takes effect only on the aggregate interface.

If the command is configured on a member port in an aggregation group, it takes effect only after the port leaves the aggregation group.

Examples

```
# Perform mCheck on GigabitEthernet 2/0/1.
<Sysname> system-view
[Sysname] interface gigabitethernet 2/0/1
[Sysname-GigabitEthernet2/0/1] stp mcheck
```

Related commands

stp global mcheck

stp mode

stp mode

Use **stp mode** to configure the spanning tree operating mode.

Use **undo stp mode** to restore the default.

Syntax

stp mode { mstp | pvst | rstp | stp }

undo stp mode

Default

A spanning tree device operates in MSTP mode.

Views

System view

Predefined user roles

network-admin

Parameters

mstp: Configures the spanning tree device to operate in MSTP mode.

pvst: Configures the spanning tree device to operate in PVST mode.

rstp: Configures the spanning tree device to operate in RSTP mode.

stp: Configures the spanning tree device to operate in STP mode.

Usage guidelines

The MSTP mode is compatible with the RSTP mode, and the RSTP mode is compatible with the STP mode.

The PVST mode's compatibility with other modes is as follows:

- **Access port**—The PVST mode is compatible with other modes in any VLAN.
- **Trunk or hybrid port**—The PVST mode is compatible with other modes only in the default VLAN.

Examples

```
# Configure the spanning tree device to operate in STP mode.
<Sysname> system-view
[Sysname] stp mode stp
```

Related commands

stp enable

stp global enable
stp global mcheck
stp mcheck
stp vlan enable.

stp no-agreement-check

Use **stp no-agreement-check** to enable No Agreement Check on a port.

Use **undo stp no-agreement-check** to disable No Agreement Check on a port.

Syntax

stp no-agreement-check
undo stp no-agreement-check

Default

No Agreement Check is disabled.

Views

Layer 2 Ethernet interface view
Layer 2 aggregate interface view

Predefined user roles

network-admin

Usage guidelines

This command takes effect only after you enable it on the root port.

If the command is configured in Layer 2 Ethernet interface view, it takes effect only on that interface.

If the command is configured in Layer 2 aggregate interface view, it takes effect only on the aggregate interface.

If the command is configured on a member port in an aggregation group, it takes effect only after the port leaves the aggregation group.

Examples

```
# Enable No Agreement Check on GigabitEthernet 2/0/1.  
<Sysname> system-view  
[Sysname] interface gigabitethernet 2/0/1  
[Sysname-GigabitEthernet2/0/1] stp no-agreement-check
```

stp pathcost-standard

Use **stp pathcost-standard** to specify a standard for the device to use when calculating the default path costs for ports.

Use **undo stp pathcost-standard** to restore the default.

Syntax

stp pathcost-standard { dot1d-1998 | dot1t | legacy }
undo stp pathcost-standard

Default

The default standard used by the device is **legacy**.

Views

System view

Predefined user roles

network-admin

Parameters

dot1d-1998: Configures the device to calculate the default path cost for ports based on IEEE 802.1d-1998.

dot1t: Configures the device to calculate the default path cost for ports based on IEEE 802.1t.

legacy: Configures the device to calculate the default path cost for ports based on a private standard.

Usage guidelines

If you change the standard that the device uses in calculating the default path costs, you restore the path costs to the default.

Examples

```
# Configure the device to calculate the default path cost for ports based on IEEE 802.1d-1998.
```

```
<Sysname> system-view
```

```
[Sysname] stp pathcost-standard dot1d-1998
```

Related commands

display stp

stp cost

stp point-to-point

Use **stp point-to-point** to configure the link type of a port.

Use **undo stp point-to-point** to restore the default.

Syntax

```
stp point-to-point { auto | force-false | force-true }
```

```
undo stp point-to-point
```

Default

The default setting is **auto**, and the spanning tree device automatically detects whether a port connects to a point-to-point link.

Views

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

Predefined user roles

network-admin

Parameters

auto: Specifies automatic detection of the link type.

force-false: Specifies the non-point-to-point link type.

force-true: Specifies the point-to-point link type.

Usage guidelines

When connecting to a non-point-to-point link, a port is incapable of rapid state transition.

You can configure the link type as point-to-point for a Layer 2 aggregate interface or a port that operates in full duplex mode. As a best practice, use the default setting, which lets the device automatically detect the port link type.

In MSTP or PVST mode, the **stp point-to-point force-false** or **stp point-to-point force-true** command configured on a port takes effect on all MSTIs or VLANs.

Before you set the link type of a port to point-to-point, make sure the port is connected to a point-to-point link. Otherwise, a temporary loop might occur.

If the command is configured in Layer 2 Ethernet interface view, it takes effect only on that interface.

If the command is configured in Layer 2 aggregate interface view, it takes effect only on the aggregate interface.

If the command is configured on a member port in an aggregation group, it takes effect only after the port leaves the aggregation group.

Examples

Configure the link type of GigabitEthernet 2/0/3 as point-to-point.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 2/0/3
[Sysname-GigabitEthernet2/0/3] stp point-to-point force-true
```

Related commands

display stp

stp port priority

Use **stp port priority** to set the priority of a port. The port priority affects the role of a port in a spanning tree.

Use **undo stp port priority** to restore the default.

Syntax

```
stp [ instance instance-list | vlan vlan-id-list ] port priority priority
undo stp [ instance instance-list | vlan vlan-id-list ] port priority
```

Default

The port priority is 128.

Views

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

Predefined user roles

network-admin

Parameters

instance *instance-list*: Specifies a space-separated list of up to 10 MSTI items. Each item specifies an MSTI or a range of MSTIs in the form of *instance-id1* [**to** *instance-id2*]. The value for *instance-id2* must be equal to or greater than the value for *instance-id1*. The value range for the *instance-id* argument is 0 to 4094, and the value 0 represents the CIST.

vlan *vlan-id-list*. Specifies a space-separated list of up to 10 VLAN items. Each item specifies a VLAN or a range of VLANs in the form of *vlan-id1* [**to** *vlan-id2*]. The value for *vlan-id2* must be equal to or greater than the value for *vlan-id1*. The value range for the *vlan-id* argument is 1 to 4094.

priority. Specifies the port priority in the range of 0 to 240 in increments of 16 (as in 0, 16, 32).

Usage guidelines

The smaller the value, the higher the port priority. If all ports on your device use the same priority value, the port priority depends on the port index. The smaller the index, the higher the priority.

If the command is configured in Layer 2 Ethernet interface view, it takes effect only on that interface.

If the command is configured in Layer 2 aggregate interface view, it takes effect only on the aggregate interface.

If the command is configured on a member port in an aggregation group, it takes effect only after the port leaves the aggregation group.

If you do not specify an MSTI or VLAN, this command configures the priority of the ports in the MSTP CIST or in the STP or RSTP spanning tree.

Examples

In MSTP mode, set the port priority of GigabitEthernet 2/0/3 to 16 in MSTI 2.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 2/0/3
[Sysname-GigabitEthernet2/0/3] stp instance 2 port priority 16
```

In PVST mode, set the port priority of GigabitEthernet 2/0/3 to 16 in VLAN 2.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 2/0/3
[Sysname-GigabitEthernet2/0/3] stp vlan 2 port priority 16
```

Related commands

display stp

stp port-log

Use **stp port-log** to enable outputting port state transition information.

Use **undo stp port-log** to disable outputting port state transition information.

Syntax

```
stp port-log { all | instance instance-list | vlan vlan-id-list }
undo stp port-log { all | instance instance-list | vlan vlan-id-list }
```

Default

Outputting port state transition information is disabled.

Views

System view

Predefined user roles

network-admin

Parameters

all: Specifies all MSTIs or VLANs.

instance *instance-list*. Specifies a space-separated list of up to 10 MSTI items. Each item specifies an MSTI or a range of MSTIs in the form of *instance-id1* [**to** *instance-id2*]. The value for *instance-id2*

must be equal to or greater than the value for *instance-id1*. The value range for the *instance-id* argument is 0 to 4094, and the value 0 represents the CIST.

vlan *vlan-id-list*: Specifies a space-separated list of up to 10 VLAN items. Each item specifies a VLAN or a range of VLANs in the form of *vlan-id1* [**to** *vlan-id2*]. The value for *vlan-id2* must be equal to or greater than the value for *vlan-id1*. The value range for the *vlan-id* argument is 1 to 4094.

Examples

In MSTP mode, enable outputting port state transition information for MSTI 2.

```
<Sysname> system-view
[Sysname] stp port-log instance 2
%Aug 16 00:49:41:856 2011 Sysname STP/3/STP_DISCARDING: Instance 2's port
GigabitEthernet2/0/1 has been set to discarding state.
%Aug 16 00:49:41:856 2011 Sysname STP/3/STP_FORWARDING: Instance 2's port
GigabitEthernet2/0/2 has been set to forwarding state.
```

The output shows that GigabitEthernet 2/0/1 in MSTI 2 transitioned to the discarding state and GigabitEthernet 2/0/2 in MSTI 2 transitioned to the forwarding state.

In PVST mode, enable outputting port state transition information for VLAN 1 through VLAN 4094.

```
<Sysname> system-view
[Sysname] stp port-log vlan 1 to 4094
%Aug 16 00:49:41:856 2006 Sysname STP/3/STP_DISCARDING: VLAN 2's GigabitEthernet2/0/1 has
been set to discarding state.
%Aug 16 00:49:41:856 2006 Sysname STP/3/STP_FORWARDING: VLAN 2's GigabitEthernet2/0/2 has
been set to forwarding state.
```

The output shows that GigabitEthernet 2/0/1 in VLAN 2 transitioned to the discarding state and GigabitEthernet 2/0/2 in VLAN 2 transitioned to the forwarding state.

stp priority

Use **stp priority** to set the priority of the device.

Use **undo stp priority** to restore the default.

Syntax

stp [**instance** *instance-list* | **vlan** *vlan-id-list*] **priority** *priority*

undo stp [**instance** *instance-list* | **vlan** *vlan-id-list*] **priority**

Default

The device priority is 32768.

Views

System view

Predefined user roles

network-admin

Parameters

instance *instance-list*: Specifies a space-separated list of up to 10 MSTI items. Each item specifies an MSTI or a range of MSTIs in the form of *instance-id1* [**to** *instance-id2*]. The value for *instance-id2* must be equal to or greater than the value for *instance-id1*. The value range for the *instance-id* argument is 0 to 4094, and the value 0 represents the CIST.

vlan *vlan-id-list*: Specifies a space-separated list of up to 10 VLAN items. Each item specifies a VLAN or a range of VLANs in the form of *vlan-id1* [**to** *vlan-id2*]. The value for *vlan-id2* must be equal to or greater than the value for *vlan-id1*. The value range for the *vlan-id* argument is 1 to 4094.

priority. Specifies the device priority in the range of 0 to 61440 in increments of 4096 (as in 0, 4096, 8192). You can set up to 16 priority values on the device. The smaller the value, the higher the device priority.

Usage guidelines

If you do not specify an MSTI or VLAN, this command configures the priority of the device in the MSTP CIST or in the STP or RSTP spanning tree.

Examples

In MSTP mode, set the device priority to 4096 in MSTI 1.

```
<Sysname> system-view  
[Sysname] stp instance 1 priority 4096
```

In PVST mode, set the device priority to 4096 in VLAN 1.

```
<Sysname> system-view  
[Sysname] stp vlan 1 priority 4096
```

stp pvst-bpdu-protection

Use **stp pvst-bpdu-protection** to enable PVST BPDU guard.

Use **undo stp pvst-bpdu-protection** to disable PVST BPDU guard.

Syntax

```
stp pvst-bpdu-protection  
undo stp pvst-bpdu-protection
```

Default

PVST BPDU guard is disabled.

Views

System view

Predefined user roles

network-admin

Usage guidelines

PVST BPDU guard enables an MSTP-enabled device to shut down a port if the port receives PVST BPDUs. The shutdown port is brought up after a detection timer expires. To set the detection timer, use the **shutdown-interval** command.

Examples

In MSTP mode, enable PVST BPDU guard.

```
<Sysname> system-view  
[Sysname] stp pvst-bpdu-protection
```

Related commands

shutdown-interval (For more information, see *Fundamentals Command Reference*.)

stp region-configuration

Use **stp region-configuration** to enter MST region view.

Use **undo stp region-configuration** to restore the default MST region configurations.

Syntax

stp region-configuration
undo stp region-configuration

Default

The default settings for an MST region are as follows:

- The MST region name of a device is the MAC address of the device.
- All VLANs are mapped to the CIST.
- The MSTP revision level is 0.

Views

System view

Predefined user roles

network-admin

Usage guidelines

After you enter MST region view, you can configure MST region parameters, including the region name, VLAN-to-instance mappings, and revision level.

Examples

```
# Enter MST region view.  
<Sysname> system-view  
[Sysname] stp region-configuration  
[Sysname-mst-region]
```

stp role-restriction

Use **stp role-restriction** to enable port role restriction.

Use **undo stp role-restriction** to disable port role restriction.

Syntax

stp role-restriction
undo stp role-restriction

Default

Port role restriction is disabled.

Views

Layer 2 Ethernet interface view
Layer 2 aggregate interface view

Predefined user roles

network-admin

Usage guidelines

When port role restriction is enabled on a port, the port cannot become a root port.

If the command is configured in Layer 2 Ethernet interface view, it takes effect only on that interface.

If the command is configured in Layer 2 aggregate interface view, it takes effect only on the aggregate interface.

If the command is configured on a member port in an aggregation group, it takes effect only after the port leaves the aggregation group.

Examples

```
# Enable port role restriction on GigabitEthernet 2/0/1.
<Sysname> system-view
[Sysname] interface gigabitethernet 2/0/1
[Sysname-GigabitEthernet2/0/1] stp role-restriction
```

stp root primary

Use **stp root primary** to configure the device as the root bridge.

Use **undo stp root** to restore the default.

Syntax

```
stp [ instance instance-list | vlan vlan-id-list ] root primary
```

```
undo stp [ instance instance-list | vlan vlan-id-list ] root
```

Default

A device is not a root bridge.

Views

System view

Predefined user roles

network-admin

Parameters

instance *instance-list*. Specifies a space-separated list of up to 10 MSTI items. Each item specifies an MSTI or a range of MSTIs in the form of *instance-id1* [**to** *instance-id2*]. The value for *instance-id2* must be equal to or greater than the value for *instance-id1*. The value range for the *instance-id* argument is 0 to 4094, and the value 0 represents the CIST.

vlan *vlan-id-list*. Specifies a space-separated list of up to 10 VLAN items. Each item specifies a VLAN or a range of VLANs in the form of *vlan-id1* [**to** *vlan-id2*]. The value for *vlan-id2* must be equal to or greater than the value for *vlan-id1*. The value range for the *vlan-id* argument is 1 to 4094.

Usage guidelines

Once you specify the device as the root bridge, you cannot change the priority of the device.

If you do not specify an MSTI or VLAN, this command configures the device as the root bridge of the MSTP CIST or of the STP or RSTP spanning tree.

Examples

```
# In MSTP mode, specify the device as the root bridge of MSTI 1.
```

```
<Sysname> system-view
[Sysname] stp instance 1 root primary
```

```
# In PVST mode, specify the device as the root bridge of VLAN 1.
```

```
<Sysname> system-view
[Sysname] stp vlan 1 root primary
```

Related commands

stp priority

stp root secondary

stp root secondary

Use **stp root secondary** to configure the device as a secondary root bridge.

Use **undo stp root** to restore the default.

Syntax

stp [instance *instance-list* | vlan *vlan-id-list*] root secondary

undo stp [instance *instance-list* | vlan *vlan-id-list*] root

Default

A device is not a secondary root bridge.

Views

System view

Predefined user roles

network-admin

Parameters

instance *instance-list*. Specifies a space-separated list of up to 10 MSTI items. Each item specifies an MSTI or a range of MSTIs in the form of *instance-id1* [**to** *instance-id2*]. The value for *instance-id2* must be equal to or greater than the value for *instance-id1*. The value range for the *instance-id* argument is 0 to 4094, and the value 0 represents the CIST.

vlan *vlan-id-list*. Specifies a space-separated list of up to 10 VLAN items. Each item specifies a VLAN or a range of VLANs in the form of *vlan-id1* [**to** *vlan-id2*]. The value for *vlan-id2* must be equal to or greater than the value for *vlan-id1*. The value range for the *vlan-id* argument is 1 to 4094.

Usage guidelines

Once you specify the device as a secondary root bridge, you cannot change the priority of the device.

If you do not specify an MSTI or VLAN, this command configures a secondary root bridge for the MSTP CIST or the STP or RSTP spanning tree.

Examples

In MSTP mode, specify the device as a secondary root bridge in MSTI 1.

```
<Sysname> system-view
```

```
[Sysname] stp instance 1 root secondary
```

In PVST mode, specify the device as a secondary root bridge in VLAN 1.

```
<Sysname> system-view
```

```
[Sysname] stp vlan 1 root secondary
```

Related commands

stp priority

stp root primary

stp root-protection

Use **stp root-protection** to enable root guard on a port.

Use **undo stp root-protection** to disable root guard on a port.

Syntax

stp root-protection

undo stp root-protection

Default

Root guard is disabled.

Views

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

Predefined user roles

network-admin

Usage guidelines

On a port, the loop guard feature and the root guard feature are mutually exclusive.

If the command is configured in Layer 2 Ethernet interface view, it takes effect only on that interface.

If the command is configured in Layer 2 aggregate interface view, it takes effect only on the aggregate interface.

If the command is configured on a member port in an aggregation group, it takes effect only after the port leaves the aggregation group.

Examples

```
# Enable root guard on GigabitEthernet 2/0/1.
```

```
<Sysname> system-view
```

```
[Sysname] interface gigabitethernet 2/0/1
```

```
[Sysname-GigabitEthernet2/0/1] stp root-protection
```

Related commands

stp edged-port

stp loop-protection

stp tc-protection

Use **stp tc-protection** to enable TC-BPDU attack guard for the device.

Use **undo stp tc-protection** to disable TC-BPDU attack guard for the device.

Syntax

stp tc-protection

undo stp tc-protection

Default

TC-BPDU attack guard is enabled.

Views

System view

Predefined user roles

network-admin

Usage guidelines

With TC-BPDU guard, you can set the maximum number of immediate forwarding address entry flushes that a device can perform every 10 seconds. For TC-BPDUs received that exceed the limit, the device performs a forwarding address entry flush when the interval elapses. This prevents frequent flushing of forwarding address entries.

Examples

```
# Disable TC-BPDU attack guard for the device.
<Sysname> system-view
[Sysname] undo stp tc-protection
```

Related commands

stp tc-protection threshold

stp tc-protection threshold

Use **stp tc-protection threshold** to set the maximum number of forwarding address entry flushes that the device can perform every 10 seconds.

Use **undo stp tc-protection threshold** to restore the default.

Syntax

```
stp tc-protection threshold number
undo stp tc-protection threshold
```

Default

By default, the device can perform a maximum of 6 forwarding address entry flushes every 10 seconds.

Views

System view

Predefined user roles

network-admin

Parameters

number: Specifies the maximum number of immediate forwarding address entry flushes that the device can perform every 10 seconds. The value is in the range of 1 to 255.

Examples

```
# Configure the device to perform up to 10 forwarding address entry flushes every 10 seconds.
<Sysname> system-view
[Sysname] stp tc-protection threshold 10
```

Related commands

stp tc-protection

stp tc-restriction

Use **stp tc-restriction** to enable TC-BPDU transmission restriction.

Use **undo stp tc-restriction** to disable TC-BPDU transmission restriction.

Syntax

```
stp tc-restriction
undo stp tc-restriction
```

Default

TC-BPDU transmission restriction is disabled.

Views

Layer 2 Ethernet interface view
Layer 2 aggregate interface view

Predefined user roles

network-admin

Usage guidelines

When TC-BPDU transmission restriction is enabled on a port, the port does not send TC-BPDUs to other ports. It also does not delete MAC address entries.

If the command is configured in Layer 2 Ethernet interface view, it takes effect only on that interface.

If the command is configured in Layer 2 aggregate interface view, it takes effect only on the aggregate interface.

If the command is configured on a member port in an aggregation group, it takes effect only after the port leaves the aggregation group.

Examples

```
# Enable TC-BPDU transmission restriction on GigabitEthernet 2/0/1.
<Sysname> system-view
[Sysname] interface gigabitethernet 2/0/1
[Sysname-GigabitEthernet2/0/1] stp tc-restriction
```

stp tc-snooping

Use **stp tc-snooping** to enable TC Snooping.

Use **undo stp tc-snooping** to disable TC Snooping.

Syntax

```
stp tc-snooping
undo stp tc-snooping
```

Default

TC Snooping is disabled.

Views

System view

Predefined user roles

network-admin

Usage guidelines

TC Snooping and the spanning tree feature are mutually exclusive. You must globally disable the spanning tree feature before enabling TC Snooping.

Examples

```
# Globally disable the spanning tree feature and enable TC Snooping.
<Sysname> system-view
[Sysname] undo stp global enable
[Sysname] stp tc-snooping
```

Related commands

stp global enable

stp timer forward-delay

Use **stp timer forward-delay** to set the forward delay timer.

Use **undo stp timer forward-delay** to restore the default.

Syntax

stp [**vlan** *vlan-id-list*] **timer forward-delay** *time*

undo stp [**vlan** *vlan-id-list*] **timer forward-delay**

Default

The forward delay timer is 1500 centiseconds.

Views

System view

Predefined user roles

network-admin

Parameters

vlan *vlan-id-list*: Specifies a space-separated list of up to 10 VLAN items. Each item specifies a VLAN or a range of VLANs in the form of *vlan-id1* [**to** *vlan-id2*]. The value for *vlan-id2* must be equal to or greater than the value for *vlan-id1*. The value range for the *vlan-id* argument is 1 to 4094. If you set the STP, RSTP, or MSTP forward delay, do not specify this option.

time: Specifies the forward delay in centiseconds, in the range of 400 to 3000 in increments of 100 (as in 400, 500, 600).

Usage guidelines

The forward delay timer determines the time interval of state transition. To prevent temporary loops, a spanning tree port goes through the learning (intermediate) state before it transits from the discarding state to the forwarding state. To stay synchronized with the remote device, the port has a wait period that is determined by the forward delay timer between transition states.

As a best practice, do not set the forward delay with this command. Instead, you can specify the network diameter of the switched network by using the **stp bridge-diameter** command. This command makes the spanning tree protocols automatically calculate the optimal settings for the forward delay timer. If the network diameter uses the default value, the forward delay timer also uses the default value.

Examples

In MSTP mode, set the forward delay timer to 2000 centiseconds.

```
<Sysname> system-view
[Sysname] stp timer forward-delay 2000
```

In PVST mode, set the forward delay timer for VLAN 2 to 2000 centiseconds.

```
<Sysname> system-view
[Sysname] stp vlan 2 timer forward-delay 2000
```

Related commands

stp bridge-diameter

stp timer hello

stp timer max-age

stp timer hello

Use **stp timer hello** to set the hello time.

Use **undo stp timer hello** to restore the default.

Syntax

stp [**vlan** *vlan-id-list*] **timer hello** *time*

undo stp [**vlan** *vlan-id-list*] **timer hello**

Default

The hello time is 200 centiseconds.

Views

System view

Predefined user roles

network-admin

Parameters

vlan *vlan-id-list*: Specifies a space-separated list of up to 10 VLAN items. Each item specifies a VLAN or a range of VLANs in the form of *vlan-id1* [**to** *vlan-id2*]. The value for *vlan-id2* must be equal to or greater than the value for *vlan-id1*. The value range for the *vlan-id* argument is 1 to 4094. If you set the STP, RSTP, or MSTP hello time, do not specify this option.

time: Specifies the hello time in centiseconds, in the range of 100 to 1000 in increments of 100 (as in 100, 200, 300).

Usage guidelines

Hello time is the interval at which spanning tree devices send configuration BPDUs to maintain the spanning tree. If a device fails to receive configuration BPDUs within the set period of time, a new spanning tree calculation process is triggered.

As a best practice, do not set the hello time with this command. Instead, you can specify the network diameter of the switched network by using the **stp bridge-diameter** command. This command makes the spanning tree protocols automatically calculate the optimal settings for the hello timer. If the network diameter uses the default value, the hello timer also uses the default value.

Examples

In MSTP mode, set the hello time to 400 centiseconds.

```
<Sysname> system-view
[Sysname] stp timer hello 400
```

In PVST mode, set the hello time for VLAN 2 to 400 centiseconds.

```
<Sysname> system-view
[Sysname] stp vlan 2 timer hello 400
```

Related commands

stp bridge-diameter

stp timer forward-delay

stp timer max-age

stp timer max-age

Use **stp timer max-age** to set the max age timer.

Use **undo stp timer max-age** to restore the default.

Syntax

```
stp [ vlan vlan-id-list ] timer max-age time  
undo stp [ vlan vlan-id-list ] timer max-age
```

Default

The max age is 2000 centiseconds.

Views

System view

Predefined user roles

network-admin

Parameters

vlan *vlan-id-list*: Specifies a space-separated list of up to 10 VLAN items. Each item specifies a VLAN or a range of VLANs in the form of *vlan-id1* [**to** *vlan-id2*]. The value for *vlan-id2* must be equal to or greater than the value for *vlan-id1*. The value range for the *vlan-id* argument is 1 to 4094. If you set the STP, RSTP, or MSTP max age, do not specify this option.

time: Specifies the max age in centiseconds, in the range of 600 to 4000 in increments of 100 (as in 600, 700, 800).

Usage guidelines

In the CIST of an MSTP network, the device determines whether a configuration BPDU received on a port has expired based on the max age timer. If the configuration BPDU has expired, a new spanning tree calculation process starts. The max age timer takes effect only on the CIST (or MSTI 0).

As a best practice, do not set the max age timer with this command. Instead, you can specify the network diameter of the switched network by using the **stp bridge-diameter** command. This command makes the spanning tree protocols automatically calculate the optimal settings for the max age timer. If the network diameter uses the default value, the max age timer also uses the default value.

Examples

```
# In MSTP mode, set the max age timer to 1000 centiseconds.
```

```
<Sysname> system-view  
[Sysname] stp timer max-age 1000
```

```
# In PVST mode, set the max age timer for VLAN 2 to 1000 centiseconds.
```

```
<Sysname> system-view  
[Sysname] stp vlan 2 timer max-age 1000
```

Related commands

```
stp bridge-diameter  
stp timer forward-delay  
stp timer hello
```

stp timer-factor

Use **stp timer-factor** to configure the timeout period by setting the timeout factor.

Timeout period = timeout factor × 3 × hello time.

Use **undo stp timer-factor** to restore the default.

Syntax

```
stp timer-factor factor  
undo stp timer-factor
```

Default

The timeout factor of a device is set to 3.

Views

System view

Predefined user roles

network-admin

Parameters

factor: Specifies the timeout factor in the range of 1 to 20.

Usage guidelines

In a stable network, each non-root-bridge forwards configuration BPDUs to surrounding devices at the interval of hello time to determine whether any link fails. If a device does not receive a BPDU from the upstream device within nine times of the hello time, it assumes that the upstream device has failed. Then it will start a new spanning tree calculation process.

In a stable network, this type of spanning tree calculation might occur because the upstream device is busy. You can avoid such unwanted spanning tree calculations by lengthening the timeout period to save network resources. As a best practice, set the timeout factor to 5, 6, or 7 for a stable network.

Examples

```
# Set the timeout factor of the device to 7.  
<Sysname> system-view  
[Sysname] stp timer-factor 7
```

Related commands

stp timer hello

stp transmit-limit

Use **stp transmit-limit** to set the BPDU transmission rate of a port.

Use **undo stp transmit-limit** to restore the default.

Syntax

```
stp transmit-limit limit  
undo stp transmit-limit
```

Default

The BPDU transmission rate of all ports is 10.

Views

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

Predefined user roles

network-admin

Parameters

limit: Specifies the BPDU transmission rate in the range of 1 to 255.

Usage guidelines

The maximum number of BPDUs a port can send within each hello time equals the BPDU transmission rate plus the hello timer value.

A larger BPDU transmission rate value requires more system resources. An appropriate BPDU transmission rate setting can prevent spanning tree protocols from using excessive bandwidth resources during network topology changes. As a best practice, use the default value.

If the command is configured in Layer 2 Ethernet interface view, it takes effect only on that interface.

If the command is configured in Layer 2 aggregate interface view, it takes effect only on the aggregate interface.

If the command is configured on a member port in an aggregation group, it takes effect only after the port leaves the aggregation group.

Examples

```
# Set the BPDU transmission rate of GigabitEthernet 2/0/1 to 5.
```

```
<Sysname> system-view  
[Sysname] interface gigabitethernet 2/0/1  
[Sysname-GigabitEthernet2/0/1] stp transmit-limit 5
```

stp vlan enable

Use **stp vlan enable** to enable the spanning tree feature for VLANs.

Use **undo stp enable** to disable the spanning tree feature for VLANs.

Syntax

stp vlan *vlan-id-list* enable

undo stp vlan *vlan-id-list* enable

Default

The spanning tree feature is enabled in VLANs.

Views

System view

Predefined user roles

network-admin

Parameters

vlan *vlan-id-list*: Specifies a space-separated list of up to 10 VLAN items. Each item specifies a VLAN or a range of VLANs in the form of *vlan-id1* [**to** *vlan-id2*]. The value for *vlan-id2* must be equal to or greater than the value for *vlan-id1*. The value range for the *vlan-id* argument is 1 to 4094. If you do not specify this option, this command globally enables or disables the spanning tree feature (VLANs are not included).

Usage guidelines

When you enable the spanning tree feature, the device operates in STP, RSTP, PVST, or MSTP mode, depending on the spanning tree mode setting.

When you enable the spanning tree feature, the device dynamically maintains the spanning tree status of VLANs, based on received configuration BPDUs. When you disable the spanning tree feature, the device stops maintaining the spanning tree status.

Examples

```
# In PVST mode, globally enable the spanning tree feature and then enable the spanning tree feature for VLAN 2.
```

```
<Sysname> system-view
[Sysname] stp mode pvst
[Sysname] stp global enable
[Sysname] stp vlan 2 enable
```

Related commands

stp enable
stp global enable
stp mode

vlan-mapping modulo

Use **vlan-mapping modulo** to map VLANs in an MST region to MSTIs according to the specified modulo value and quickly create a VLAN-to-instance mapping table.

Syntax

```
vlan-mapping modulo modulo
```

Default

All VLANs are mapped to the CIST (MSTI 0).

Views

MST region view

Predefined user roles

network-admin

Parameters

modulo: Specifies the modulo value. The value range for the *modulo* argument is 1 to 64.

Usage guidelines

You cannot map a VLAN to different MSTIs. If you map a VLAN that has been mapped to an MSTI to a new MSTI, the old mapping is automatically deleted.

This command maps each VLAN to the MSTI with ID $(\text{VLAN ID} - 1) \% \text{modulo} + 1$. $(\text{VLAN ID} - 1) \% \text{modulo}$ is the modulo operation for $(\text{VLAN ID} - 1)$. If the modulo value is 15, then VLAN 1 is mapped to MSTI 1, VLAN 2 to MSTI 2, ..., VLAN 15 to MSTI 15, VLAN 16 to MSTI 16, and so on.

Examples

```
# Map VLANs to MSTIs as per modulo 8.
<Sysname> system-view
[Sysname] stp region-configuration
[Sysname-mst-region] vlan-mapping modulo 8
```

Related commands

active region-configuration
check region-configuration
display stp region-configuration
region-name
revision-level

LLDP commands

This feature is supported only on the following ports:

- Layer 2 Ethernet ports on Ethernet switching modules.
- Fixed Layer 2 Ethernet ports of the following routers:
 - MSR1002-4/1003-8S.
 - MSR2004-24/2004-48.
 - MSR954 (JH296A/JH297A/JH298A/JH299A/JH373A).
 - MSR958 (JH300A/JH301A).

display lldp local-information

Use **display lldp local-information** to display local LLDP information, which will be contained in the advertisable LLDP TLVs and sent to neighboring devices.

Syntax

```
display lldp local-information [ global | interface interface-type interface-number ]
```

Views

Any view

Predefined user roles

network-admin
network-operator

Parameters

global: Displays the global local LLDP information.

interface *interface-type interface-number*: Specifies a port by its type and number.

Usage guidelines

If you do not specify any keywords or arguments, the command displays all local LLDP information, which includes the following:

- The global LLDP information.
- The LLDP information about the LLDP-enabled ports in up state.

Examples

```
# Display all local LLDP information.
```

```
<Sysname> display lldp local-information
```

```
Global LLDP local-information:
```

```
Chassis ID           : 00e0-fc00-5600
System name          : Sysname
System description   : HPE Comware Platform Software
System capabilities supported : Bridge, Router, Customer Bridge, Service Bridge
System capabilities enabled   : Bridge, Router, Service Bridge
```

```
MED information:
```

```
Device class           : Connectivity device
```

```
MED inventory information of master board:
```

```
HardwareRev           : REV.A
```

```

FirmwareRev          : 109
SoftwareRev          : 5.20 Alpha 2101
SerialNum            : NONE
Manufacturer name    : HPE
Model name           : MSR2003
Asset tracking identifier : Unknown
LLDP local-information of port 52[GigabitEthernet2/0/3]:
Port ID type         : Interface name
Port ID              : GigabitEthernet2/0/3
Port description     : GigabitEthernet2/0/3 Interface
LLDP agent nearest-bridge management address:
Management address type      : IPv4
Management address          : 192.168.80.60
Management address interface type : IfIndex
Management address interface ID : Unknown
Management address OID       : 0
LLDP agent nearest-nontpmr management address:
Management address type      : IPv4
Management address          : 192.168.80.61
Management address interface type : IfIndex
Management address interface ID : Unknown
Management address OID       : 0
LLDP agent nearest-customer management address:
Management address type      : IPv4
Management address          : 192.168.80.62
Management address interface type : IfIndex
Management address interface ID : Unknown
Management address OID       : 0
Link aggregation supported : Yes
Link aggregation enabled  : Yes
Aggregation port ID       : 52
Maximum frame size        : 1500
Transmit Tw                : 100 us
Receive Tw                 : 90 us
Fallback Tw                : 90 us
Echo Transmit Tw           : 0 us
Echo Receive Tw            : 0 us
Location format           : Civic Address LCI
Location information      :
  What(1) Country(CN)
  CA type CA value
  0       Chinese
  1       Zhejiang
  2       Hangzhou
MED port information:
Media policy type         : Unknown
Unknown policy            : Yes
VLAN tagged               : No

```

```

Media policy VLANID      : 0
Media policy L2 priority : 0
Media policy DSCP        : 0
PoE PSE power source     : Primary
Port PSE priority        : Critical
Port available power value : 30.0 w

```

NOTE:

The output varies by network device configuration.

Table 33 Command output

Field	Description
Chassis ID	Bridge MAC address of the device.
System capabilities supported	Supported capabilities: <ul style="list-style-type: none"> • Repeater—Signal repeating is supported. • Bridge—Switching is supported. • WlanAccessPoint—The local device can act as a wireless AP. • Router—Routing is supported. • Telephone—The local device can act as a telephone. • DocsisCableDevice—The local device can act as a DOCSIS-compliant cable device. • StationOnly—The local device can act as a station only. • Customer Bridge—The customer bridge feature is supported. • Service Bridge—The service bridge feature is supported. • TPMR—The TPMR feature is supported. • Other—Features other than those listed above are supported.
System capabilities enabled	Enabled capabilities: <ul style="list-style-type: none"> • Repeater—Signal repeating is enabled. • Bridge—Switching is enabled. • WlanAccessPoint—The local device is acting as a wireless AP. • Router—Routing is enabled. • Telephone—The local device is acting as a telephone. • DocsisCableDevice—The local device is acting as a DOCSIS-compliant cable device. • StationOnly—The local device is acting as a station only. • Customer Bridge—The customer bridge feature is enabled. • Service Bridge—The service bridge feature is enabled. • TPMR—The TPMR feature is enabled. • Other—Features other than those listed above are enabled.
Device class	MED device class: <ul style="list-style-type: none"> • Connectivity device—Network device. • Class I—Normal terminal device. It requires the basic LLDP discovery services. • Class II—Media terminal device. It supports media streams, and can also act as a normal terminal device. • Class III—Communication terminal device. It supports the IP communication systems of end users, and can also act as a normal terminal device or media terminal device.
HardwareRev	Hardware version.
FirmwareRev	Firmware version.

Field	Description
SoftwareRev	Software version.
SerialNum	Serial number.
Manufacturer name	Device manufacturer.
Model name	Device model.
Port ID type	Port ID type: <ul style="list-style-type: none"> • MAC address. • Interface name.
Port ID	Port ID, the value of which depends on the port ID type.
Management address interface type	Numbering type of the interface identified by the management address.
Management address interface ID	Index of the interface identified by the management address.
Management address OID	Management address object ID.
Link aggregation supported	Indicates whether link aggregation is supported on the port.
Link aggregation enabled	Indicates whether link aggregation is enabled on the port.
Aggregation port ID	Member port ID, which is 0 when link aggregation is disabled.
Media policy type	Media policy type: <ul style="list-style-type: none"> • unknown. • voice. • voiceSignaling. • guestVoice. • guestVoiceSignaling. • softPhoneVoice. • videoconferencing. • streamingVideo. • videoSignaling.
Unknown policy	Indicates whether the media policy is unknown.
VLAN tagged	Indicates whether packets of the media VLAN are tagged.
Media policy VLANID	ID of the media VLAN.
Media policy L2 priority	Layer 2 priority.
Media policy DSCP	DSCP value.
Location format	Location information format: <ul style="list-style-type: none"> • Invalid—The location information is invalid. • Coordinate-based LCI—The location information is coordinate-based. • Civic Address LCI—Typical address information. • ECS ELIN—Telephone number for urgencies.
PoE PSE power source	PSE power source type: <ul style="list-style-type: none"> • Unknown—Unknown power supply. • Primary—Primary power supply. • Backup—Backup power supply.
PoE PD power source	PD power source type: <ul style="list-style-type: none"> • Unknown—Unknown power supply.

Field	Description
	<ul style="list-style-type: none"> • PSE—PSE power supply. • Local—Local power supply. • PSE and local—PSE and local power supplies.
Port PSE priority	PoE power supply priority of PSE ports: <ul style="list-style-type: none"> • Unknown. • Critical. • High. • Low.
Port PD priority	PoE power receiving priority of PD ports: <ul style="list-style-type: none"> • Unknown. • Critical. • High. • Low.
Port available power value	Available PoE power on PSE ports, or power needed on PD ports, in watts.
Transmit Tw	Sleep time of the local client, in μ s.
Receive Tw	Sleep time of the peer client expected by the local client, in μ s.
Fallback Tw	Candidate sleep time of the peer client expected by the local client, in μ s.
Echo Transmit Tw	Sleep time of the peer client, in μ s. This field displays zero when one of the following cases occurs: <ul style="list-style-type: none"> • The local client has not received the sleep time of the peer client. • The sleep time of the peer client is 0 μs.
Echo Receive Tw	Sleep time of the local client expected by the peer client, in μ s. This field displays zero when one of the following cases occurs: <ul style="list-style-type: none"> • The local client has not received the expected sleep time from the peer client. • The sleep time of the local client expected by the peer client is 0 μs.

display lldp neighbor-information

Use **display lldp neighbor-information** to display the LLDP information carried in LLDP TLVs that the local device receives from the neighboring devices.

Syntax

```
display lldp neighbor-information [ [ [ interface interface-type interface-number ] [ agent { nearest-bridge | nearest-customer | nearest-nontpmr } ] [ verbose ] ] | list [ system-name system-name ] ]
```

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

interface *interface-type interface-number*. Specifies a port by its type and number. If you do not specify this option, the command displays the LLDP information that all ports receive from the neighboring devices.

agent: Specifies an agent type. If you do not specify an agent type, the command displays the LLDP information that all LLDP agents receive from the neighboring devices.

nearest-bridge: Specifies nearest bridge agents.

nearest-customer: Specifies nearest customer bridge agents.

nearest-nontpmr: Specifies nearest non-TPMR bridge agents.

verbose: Displays the detailed LLDP information that the local device receives from the neighboring devices. If you do not specify this keyword, the command displays the brief LLDP information that the local device receives from the neighboring devices.

list: Displays the LLDP information that the local device receives from the neighboring devices in the form of a list.

system-name *system-name*: Displays the LLDP information that the local device receives from a neighboring device specified by its system name. The *system-name* argument is a string of 1 to 255 characters. If you do not specify this option, the command displays the LLDP information that the local device receives from all neighboring devices in a list.

Examples

Display the detailed LLDP information that the nearest bridge agents on all ports received from the neighboring devices.

```
<Sysname> display lldp neighbor-information agent nearest-bridge verbose
LLDP neighbor-information of port 1[GigabitEthernet2/0/1]:
LLDP agent nearest-bridge:
  LLDP Neighbor index : 1
  Update time         : 0 days, 0 hours, 1 minutes, 1 seconds
  Chassis type        : MAC address
  Chassis ID          : 000f-0055-0002
  Port ID type        : Interface name
  Port ID              : GigabitEthernet2/0/1
  Time to live        : 121
  Port description    : GigabitEthernet2/0/1 Interface
  System name         : Sysname
  System description  : HPE Comware Platform Software
  System capabilities supported : Bridge, Router, Customer Bridge, Service Bridge
  System capabilities enabled   : Bridge, Router, Customer Bridge
  Management address type       : IPv4
  Management address           : 192.168.1.55
  Management address interface type : IfIndex
  Management address interface ID : Unknown
  Management address OID       : 0
  Port VLAN ID(PVID): 1
  Port and protocol VLAN ID(PPVID) : 12
  Port and protocol VLAN supported : Yes
  Port and protocol VLAN enabled   : Yes
  VLAN name of VLAN 12: VLAN 0012
  Management VLAN ID : 5
  Auto-negotiation supported : Yes
  Auto-negotiation enabled   : Yes
  OperMau                    : Speed(1000)/Duplex(Full)
  Power port class           : PD
  PSE power supported        : Yes
```

PSE power enabled : Yes
PSE pairs control ability : Yes
Power pairs : Signal
Port power classification : Class 0
Power type : Type 2 PD
Power source : PSE and local
Power priority : High
PD requested power value : 21.1 w
PSE allocated power value : 15.3 w
Link aggregation supported : Yes
Link aggregation enabled : Yes
Aggregation port ID : 52
Maximum frame size : 1500

Display the detailed LLDP information that all LLDP agents on all ports received from the neighboring devices.

```
<Sysname> display lldp neighbor-information verbose
LLDP neighbor-information of port 1[GigabitEthernet2/0/1]:
LLDP agent nearest-bridge:
  LLDP Neighbor index : 1
  Update time : 0 days, 0 hours, 1 minutes, 1 seconds
  Chassis type : MAC address
  Chassis ID : 000f-0055-0002
  Port ID type : Interface name
  Port ID : GigabitEthernet2/0/1
  Time to live : 121
  Port description : GigabitEthernet2/0/1 Interface
  System name : Sysname
  System description : HPE Comware Platform Software
  System capabilities supported : Bridge, Router, Customer Bridge, Service Bridge
  System capabilities enabled : Bridge, Router, Customer Bridge
  Management address type : IPv4
  Management address : 192.168.1.55
  Management address interface type : IfIndex
  Management address interface ID : Unknown
  Management address OID : 0
  Port VLAN ID(PVID): 1
  Port and protocol VLAN ID(PPVID) : 12
  Port and protocol VLAN supported : Yes
  Port and protocol VLAN enabled : Yes
  VLAN name of VLAN 12: VLAN 0012
  Auto-negotiation supported : Yes
  Auto-negotiation enabled : Yes
  OperMau : Speed(1000)/Duplex(Full)
  Power port class : PD
  PSE power supported : Yes
  PSE power enabled : Yes
  PSE pairs control ability : Yes
  Power pairs : Signal
```

```

Port power classification : Class 0
Power type                : Type 2 PD
Power source              : PSE and local
Power priority            : High
PD requested power value  : 21.1 w
PSE allocated power value : 15.3 w
Link aggregation supported : Yes
Link aggregation enabled  : Yes
Aggregation port ID      : 52
Maximum frame size       : 1500

```

Display the brief LLDP information that all LLDP agents on all ports received from the neighboring devices.

```

<Sysname> display lldp neighbor-information
LLDP neighbor-information of port 52[GigabitEthernet2/0/3]:
LLDP agent nearest-bridge:
  LLDP neighbor index : 3
  ChassisID/subtype   : 0011-2233-4400/MAC address
  PortID/subtype      : 000c-29f5-c71f/MAC address
  Capabilities        : Bridge, Router, Customer Bridge

  LLDP neighbor index : 6
  ChassisID/subtype   : 0011-2233-4400/MAC address
  PortID/subtype      : 000c-29f5-c715/MAC address
  Capabilities        : None

```

```

CDP neighbor-information of port 52[GigabitEthernet2/0/3]:
LLDP agent nearest-bridge:
  CDP neighbor index : 4
  Chassis ID         : SEP00260B5C0548
  Port ID            : Port 1

  CDP neighbor index : 5
  Chassis ID         : 0011-2233-4400
  Port ID            : GigabitEthernet2/0/4

```

```

LLDP neighbor-information of port 52[GigabitEthernet2/0/3]:
LLDP agent nearest-nontpmr:
  LLDP neighbor index : 6
  ChassisID/subtype   : 0011-2233-4400/MAC address
  PortID/subtype      : 000c-29f5-c715/MAC address
  Capabilities        : None

```

Display the brief LLDP information that all LLDP agents received from all neighboring devices in a list.

```

<Sysname> display lldp neighbor-information list
Chassis ID : * -- --Nearest nontpmr bridge neighbor
             # -- --Nearest customer bridge neighbor
             Default -- -- Nearest bridge neighbor
System Name      Local Interface  Chassis ID      Port ID

```

System1	GE2/0/1	000f-e25d-ee91	GigabitEthernet2/0/5
System2	GE2/0/2	000f-e25d-ee92*	GigabitEthernet2/0/6
System3	GE2/0/3	000f-e25d-ee93#	GigabitEthernet2/0/7

NOTE:

The output varies by network device configuration.

Table 34 Command output

Field	Description
LLDP neighbor-information of port 1	LLDP information received through port 1.
Update time	Time when LLDP information about a neighboring device was last updated.
Chassis type	Chassis ID type: <ul style="list-style-type: none"> • Chassis component. • Interface alias. • Port component. • MAC address. • Network address (ipv4). • Interface name. • Locally assigned—Locally-defined chassis type other than those listed above.
Chassis ID	ID that identifies the LLDP sending device, which can be a MAC address, a network address, an interface, or some other value, depending on the chassis ID type of the neighboring device.
Port ID type	Port ID type: <ul style="list-style-type: none"> • Interface alias. • Port component. • MAC address. • Network address (ipv4). • Interface name. • Agent circuit ID. • Locally assigned—Locally-defined port ID type other than those listed above.
Port ID	Value of the type of the port ID.
System name	System name of the neighboring device.
System description	System description of the neighboring device.
System capabilities supported	Capabilities supported on the neighboring device: <ul style="list-style-type: none"> • Bridge—Switching is supported. • Router—Routing is supported. • Customer Bridge—The customer bridge feature is supported. • Service Bridge—The service bridge feature is supported. • Other—Features other than those listed above are supported.
System capabilities enabled	Capabilities enabled on the neighboring device: <ul style="list-style-type: none"> • Bridge—Switching is enabled. • Router—Routing is enabled. • Customer Bridge—The customer bridge feature is enabled. • Other—Features other than those listed above are enabled.
Management address OID	Management address object ID.

Field	Description
Port and protocol VLAN ID(PPVID)	Port protocol VLAN ID.
Port and protocol VLAN supported	Indicates whether protocol VLAN is supported on the port.
Port and protocol VLAN enabled	Indicates whether protocol VLAN is enabled on the port.
VLAN name of VLAN 12	Name of VLAN 12.
Auto-negotiation supported	Indicates whether autonegotiation is supported on the port.
Auto-negotiation enabled	Indicates whether autonegotiation is enabled on the port.
OperMau	Speed and duplex state on the port.
Power port class	PoE port class: <ul style="list-style-type: none"> • PSE—Power sourcing equipment. • PD—Powered device.
PSE power supported	Indicates whether the device can operate as a PSE.
PSE power enabled	Indicates whether the device is operating as a PSE.
PSE pairs control ability	Indicates whether the pair selection ability is available.
Power pairs	Power supply mode: <ul style="list-style-type: none"> • Signal—Uses data pairs to supply power. • Spare—Uses spare pairs to supply power.
Port power classification	Power class of the PD: <ul style="list-style-type: none"> • Class 0. • Class 1. • Class 2. • Class 3. • Class 4.
Power type	Power supply type: <ul style="list-style-type: none"> • Type 1 PD. • Type 2 PD. • Type 1 PSE. • Type 2 PSE.
Power source	Power source: <ul style="list-style-type: none"> • When the power supply type is PSE, options are: <ul style="list-style-type: none"> ○ Unknown—Unknown power supply. ○ Primary—Primary power supply. ○ Backup—Backup power supply. ○ Reserved. • When the power supply type is PD, options are: <ul style="list-style-type: none"> ○ Unknown—Unknown power supply. ○ PSE—PSE power supply. ○ Local—Local power supply. ○ PSE and local—PSE and local power supplies.
Power priority	<ul style="list-style-type: none"> • Unknown. • Critical. • High. • Low.
PD requested power value	PD requested power in watts.
PSE allocated power value	PSE allocated power in watts.

Field	Description
Link aggregation supported	Indicates whether link aggregation is supported.
Link aggregation enabled	Indicates whether link aggregation is enabled.
Capabilities	Capabilities enabled on the neighboring device: <ul style="list-style-type: none"> • Bridge—Switching is enabled. • Router—Routing is enabled. • Other—Features other than those listed above are enabled.
Local Interface	Local port that receives the LLDP information.
Chassis ID : * -- -- Nearest nontpmr bridge neighbor #-- -- Nearest customer bridge neighbor	Chassis ID flag: <ul style="list-style-type: none"> • An asterisk (*) indicates the nearest non-TPMR bridge neighbor. • A pound sign (#) indicates the nearest customer bridge neighbor.

display lldp statistics

Use **display lldp statistics** to display the global LLDP statistics or the LLDP statistics of a port.

Syntax

```
display lldp statistics [ global | [ interface interface-type interface-number ] [ agent { nearest-bridge | nearest-customer | nearest-nontpmr } ] ]
```

Views

Any view

Predefined user roles

network-admin
network-operator

Parameters

global: Displays the global LLDP statistics.

interface *interface-type interface-number*: Specifies a port by its type and number.

agent: Specifies an LLDP agent type. If you do not specify an agent type, the command displays the statistics for all LLDP agents.

nearest-bridge: Specifies nearest bridge agents.

nearest-customer: Specifies nearest customer bridge agents.

nearest-nontpmr: Specifies nearest non-TPMR bridge agents.

Usage guidelines

If you do not specify any keywords or arguments, the command displays the global LLDP statistics and the LLDP statistics of all ports.

Examples

Display the global LLDP statistics and the LLDP statistics of all ports.

```
<Sysname> display lldp statistics
LLDP statistics global information:
LLDP neighbor information last change time:0 days, 0 hours, 4 minutes, 40 seconds
The number of LLDP neighbor information inserted : 1
The number of LLDP neighbor information deleted : 1
```

The number of LLDP neighbor information dropped : 0
The number of LLDP neighbor information aged out : 1

LLDP statistics information of port 1 [GigabitEthernet2/0/1]:

LLDP agent nearest-bridge:

The number of LLDP frames transmitted : 0
The number of LLDP frames received : 0
The number of LLDP frames discarded : 0
The number of LLDP error frames : 0
The number of LLDP TLVs discarded : 0
The number of LLDP TLVs unrecognized : 0
The number of LLDP neighbor information aged out : 0
The number of CDP frames transmitted : 0
The number of CDP frames received : 0
The number of CDP frames discarded : 0
The number of CDP error frames : 0

LLDP agent nearest-nontpnr:

The number of LLDP frames transmitted : 0
The number of LLDP frames received : 0
The number of LLDP frames discarded : 0
The number of LLDP error frames : 0
The number of LLDP TLVs discarded : 0
The number of LLDP TLVs unrecognized : 0
The number of LLDP neighbor information aged out : 0
The number of CDP frames transmitted : 0
The number of CDP frames received : 0
The number of CDP frames discarded : 0
The number of CDP error frames : 0

LLDP agent nearest-customer:

The number of LLDP frames transmitted : 0
The number of LLDP frames received : 0
The number of LLDP frames discarded : 0
The number of LLDP error frames : 0
The number of LLDP TLVs discarded : 0
The number of LLDP TLVs unrecognized : 0
The number of LLDP neighbor information aged out : 0
The number of CDP frames transmitted : 0
The number of CDP frames received : 0
The number of CDP frames discarded : 0
The number of CDP error frames : 0

Display the LLDP statistics for the nearest customer bridge agents on GigabitEthernet 2/0/1.

<Sysname> display lldp statistics interface gigabitethernet 2/0/1 agent nearest-customer

LLDP statistics information of port 1 [GigabitEthernet2/0/1]:

LLDP agent nearest-customer:

The number of LLDP frames transmitted : 0
The number of LLDP frames received : 0

```

The number of LLDP frames discarded           : 0
The number of LLDP error frames               : 0
The number of LLDP TLVs discarded             : 0
The number of LLDP TLVs unrecognized         : 0
The number of LLDP neighbor information aged out : 0
The number of CDP frames transmitted          : 0
The number of CDP frames received            : 0
The number of CDP frames discarded           : 0
The number of CDP error frames                : 0

```

NOTE:

The output varies by network device configuration.

Table 35 Command output

Field	Description
LLDP statistics global information	Global LLDP statistics.
LLDP neighbor information last change time	Time when the neighbor information was last updated.
The number of LLDP neighbor information inserted	Number of times neighbor information was added.
The number of LLDP neighbor information deleted	Number of times neighbor information was removed.
The number of LLDP neighbor information dropped	Number of times neighbor information was dropped due to lack of available memory space.

display lldp status

Use **display lldp status** to display LLDP status.

Syntax

```

display lldp status [ interface interface-type interface-number ] [ agent { nearest-bridge | nearest-customer | nearest-nontpmr } ]

```

Views

Any view

Predefined user roles

network-admin
network-operator

Parameters

interface *interface-type interface-number*. Specifies a port by its type and number. If you do not specify this option, the command displays the global LLDP status and the LLDP status of all ports.

agent: Specifies an LLDP agent type. If you do not specify an agent type, the command displays the status information for all LLDP agents.

nearest-bridge: Specifies nearest bridge agents.

nearest-customer: Specifies nearest customer bridge agents.

nearest-nontpmr: Specifies nearest non-TPMR bridge agents.

Examples

Display the global LLDP status and the LLDP status of each port.

```
<Sysname> display lldp status
Global status of LLDP: Enable
Bridge mode of LLDP: customer-bridge
The current number of LLDP neighbors: 5
The current number of CDP neighbors: 0
LLDP neighbor information last changed time: 0 days, 0 hours, 4 minutes, 40 seconds
Transmit interval          : 30s
Fast transmit interval     : 1s
Transmit max credit       : 5
Hold multiplier           : 4
Reinit delay              : 2s
Trap interval             : 5s
Fast start times          : 3
```

LLDP status information of port 1 [GigabitEthernet2/0/1]:

```
LLDP agent nearest-bridge:
Port status of LLDP      : Enable
Admin status            : TX_RX
Trap flag               : No
MED trap flag          : No
Polling interval       : 0s
Number of LLDP neighbors : 5
Number of MED neighbors : 2
Number of CDP neighbors : 0
Number of sent optional TLV : 12
Number of received unknown TLV : 5
LLDP agent nearest-nontpnr:
Port status of LLDP      : Enable
Admin status            : TX_RX
Trap flag               : No
Polling interval       : 0s
Number of LLDP neighbors : 5
Number of MED neighbors : 2
Number of CDP neighbors : 0
Number of sent optional TLV : 12
Number of received unknown TLV : 5
```

```
LLDP agent nearest-customer:
Port status of LLDP      : Enable
Admin status            : TX_RX
Trap flag               : No
Polling interval       : 0s
Number of LLDP neighbors : 5
Number of MED neighbors : 2
Number of CDP neighbors : 0
Number of sent optional TLV : 12
```

Number of received unknown TLV : 5

NOTE:

The output varies by network device configuration.

Table 36 Command output

Field	Description
Bridge mode of LLDP	LLDP bridge mode: service-bridge or customer-bridge.
Global status of LLDP	Indicates whether LLDP is globally enabled.
LLDP neighbor information last changed time	Time when the neighbor information was last updated.
Transmit interval	LLDP frame transmission interval.
Hold multiplier	TTL multiplier.
Reinit delay	LLDP reinitialization delay.
Transmit max credit	Token bucket size for sending LLDP frames.
Trap interval	Trap transmission interval.
Fast start times	Number of LLDP frames sent each time fast LLDP frame transmission is triggered.
Port 1	LLDP status of port 1.
Port status of LLDP	Indicates whether LLDP is enabled on the port.
Admin status	LLDP operating mode of the port: <ul style="list-style-type: none">• TX_RX—The port can send and receive LLDP frames.• Rx_Only—The port can only receive LLDP frames.• Tx_Only—The port can only send LLDP frames.• Disable—The port cannot send or receive LLDP frames.
Trap Flag	Indicates whether trapping is enabled.
Polling interval	LLDP polling interval, which is 0 when LLDP polling is disabled.
Number of neighbors	Number of LLDP neighbors connecting to the port.
Number of MED neighbors	Number of MED neighbors connecting to the port.
Number of CDP neighbors	Number of CDP neighbors connecting to the port.
Number of sent optional TLV	Number of optional TLVs contained in an LLDP frame sent through the port.
Number of received unknown TLV	Number of unknown TLVs contained in a received LLDP frame.

display lldp tlv-config

Use **display lldp tlv-config** to display the types of advertisable optional LLDP TLVs of a port.

Syntax

```
display lldp tlv-config [ interface interface-type interface-number ] [ agent { nearest-bridge | nearest-customer | nearest-nontpmr } ]
```

Views

Any view

Predefined user roles

network-admin
network-operator

Parameters

interface *interface-type interface-number*. Specifies a port by its type and number. If you do not specify this option, the command displays the types of advertisable optional TLVs of all ports.

agent: Specifies an LLDP agent type. If you do not specify an agent type, the command displays the types of advertisable optional LLDP TLVs for all LLDP agents.

nearest-bridge: Specifies nearest bridge agents.

nearest-customer: Specifies nearest customer bridge agents.

nearest-nontpmr: Specifies nearest non-TPMR bridge agents.

Examples

Display the types of advertisable optional LLDP TLVs of interface GigabitEthernet 2/0/1.

```
<Sysname> display lldp tlv-config interface gigabitethernet 2/0/1
```

```
LLDP tlv-config of port 1[GigabitEthernet2/0/1]:
```

```
LLDP agent nearest-bridge:
```

NAME	STATUS	DEFAULT
------	--------	---------

Basic optional TLV:

Port Description TLV	YES	YES
System Name TLV	YES	YES
System Description TLV	YES	YES
System Capabilities TLV	YES	YES
Management Address TLV	YES	YES

IEEE 802.1 extend TLV:

Port VLAN ID TLV	YES	YES
Port And Protocol VLAN ID TLV	YES	YES
VLAN Name TLV	YES	YES

IEEE 802.3 extend TLV:

MAC-Physic TLV	YES	YES
Power via MDI TLV	YES	YES
Maximum Frame Size TLV	YES	YES
Energy-Efficient Ethernet TLV	NO	NO

LLDP-MED extend TLV:

Capabilities TLV	YES	YES
Network Policy TLV	YES	YES
Location Identification TLV	NO	NO
Extended Power via MDI TLV	YES	YES
Inventory TLV	YES	YES

```
LLDP agent nearest-nontpmr:
```

NAME	STATUS	DEFAULT
------	--------	---------

Basic optional TLV:

Port Description TLV	YES	NO
System Name TLV	YES	NO
System Description TLV	YES	NO
System Capabilities TLV	YES	NO
Management Address TLV	YES	NO

```

IEEE 802.1 extend TLV:
  Port VLAN ID TLV                YES      NO
  Port And Protocol VLAN ID TLV   YES      NO
  VLAN Name TLV                   YES      NO
IEEE 802.3 extend TLV:
  MAC-Physic TLV                  YES      NO
  Power via MDI TLV               YES      NO
  Maximum Frame Size TLV          YES      NO
  Energy-Efficient Ethernet TLV   NO       NO
LLDP-MED extend TLV:
  Capabilities TLV                YES      NO
  Network Policy TLV              YES      NO
  Location Identification TLV     NO       NO
  Extended Power via MDI TLV      YES      NO
  Inventory TLV                   YES      NO

LLDP agent nearest-customer:
NAME                               STATUS   DEFAULT
Basic optional TLV:
  Port Description TLV            YES      YES
  System Name TLV                 YES      YES
  System Description TLV         YES      YES
  System Capabilities TLV        YES      YES
  Management Address TLV         YES      YES
IEEE 802.3 extend TLV:
  MAC-Physic TLV                  YES      NO
  Power via MDI TLV               YES      NO
  Maximum Frame Size TLV          YES      NO
  Energy-Efficient Ethernet TLV   NO       NO
LLDP-MED extend TLV:
  Capabilities TLV                YES      YES
  Network Policy TLV              YES      YES
  Location Identification TLV     NO       NO
  Extended Power via MDI TLV      YES      NO
  Inventory TLV                   YES      YES

```

NOTE:

The output varies by network device configuration.

Table 37 Command output

Field	Description
LLDP tlv-config of port 1	Advertisable optional TLVs of port 1.
NAME	TLV type.
STATUS	Indicates whether the type of TLV is sent through a port.
DEFAULT	Indicates whether the type of TLV is sent through a port by default.
Basic optional TLV	Basic optional TLVs:

Field	Description
	<ul style="list-style-type: none"> Port Description TLV. System Name TLV. System Description TLV. System Capabilities TLV. Management Address TLV.
IEEE 802.1 extended TLV	IEEE 802.1 organizationally specific TLVs: <ul style="list-style-type: none"> Port VLAN ID TLV. Port And Protocol VLAN ID TLV. VLAN Name TLV.
IEEE 802.3 extended TLV	IEEE 802.3 organizationally specific TLVs: <ul style="list-style-type: none"> MAC-Physic TLV. Power via MDI TLV. Link Aggregation TLV. Maximum Frame Size TLV.
LLDP-MED extend TLV	LLDP-MED TLVs: <ul style="list-style-type: none"> Capabilities TLV. Network Policy TLV. Extended Power-via-MDI TLV. Location Identification TLV. Inventory TLV.
Inventory TLV	Inventory TLVs: <ul style="list-style-type: none"> Hardware Revision TLV. Firmware Revision TLV. Software Revision TLV. Serial Number TLV. Manufacturer Name TLV. Model name TLV. Asset ID TLV.

Ildp admin-status

Use **ildp admin-status** to set the LLDP operating mode.

Use **undo ildp admin-status** to restore the default.

Syntax

In Layer 2/Layer 3 Ethernet interface view or management Ethernet interface view:

ildp [agent { nearest-customer | nearest-nontpmr }] admin-status { disable | rx | tx | txrx }

undo ildp [agent { nearest-customer | nearest-nontpmr }] admin-status

In Layer 2/Layer 3 aggregate interface view:

ildp agent { nearest-customer | nearest-nontpmr } admin-status { disable | rx | tx | txrx }

undo ildp agent { nearest-customer | nearest-nontpmr } admin-status

In synchronous/asynchronous serial interface view, standard POS interface view, or POS channel interface view:

ildp admin-status { disable | rx | tx | txrx }

undo ildp admin-status

Default

The nearest bridge agent operates in **txrx** mode, and the nearest customer bridge agent and nearest non-TPMR bridge agent operate in **disable** mode.

Views

Layer 2/Layer 3 aggregate interface view

Layer 2/Layer 3 Ethernet interface view

Management Ethernet interface view

Standard POS interface view, POS channel interface view

Synchronous/asynchronous serial interface view

Predefined user roles

network-admin

Parameters

agent: Specifies an LLDP agent type. If you do not specify an agent type in Ethernet or management Ethernet interface view, the command sets the operating mode for nearest bridge agents.

nearest-customer: Specifies nearest customer bridge agents.

nearest-nontpmr: Specifies nearest non-TPMR bridge agents.

disable: Specifies the **Disable** mode. A port in this mode cannot send or receive LLDP frames.

rx: Specifies the **Rx** mode. A port in this mode can only receive LLDP frames.

tx: Specifies the **Tx** mode. A port in this mode can only send LLDP frames.

txrx: Specifies the **TxRx** mode. A port in this mode can send and receive LLDP frames.

Usage guidelines

In synchronous/asynchronous serial interface view, standard POS interface view, or POS channel interface view, only nearest bridge agents are supported.

Examples

Set the LLDP operating mode to **Rx for the nearest customer bridge agents on GigabitEthernet 2/0/1.**

```
<Sysname> system-view
[Sysname] interface gigabitethernet 2/0/1
[Sysname-GigabitEthernet2/0/1] lldp agent nearest-customer admin-status rx
```

Set the LLDP operating mode to **Rx for the nearest bridge agents on Serial 2/1/0.**

```
<Sysname> system-view
[Sysname] interface serial 2/1/0
[Sysname-Serial2/1/0] lldp admin-status rx
```

Set the LLDP operating mode to **Rx for the nearest bridge agents on POS 2/2/0.**

```
<Sysname> system-view
[Sysname] interface pos 2/2/0
[Sysname-Pos2/2/0] lldp admin-status rx
```

Ildp check-change-interval

Use **Ildp check-change-interval** to enable LLDP polling and set the polling interval.

Use **undo Ildp check-change-interval** to disable LLDP polling.

Syntax

In Layer 2/Layer 3 Ethernet interface view or management Ethernet interface view:

```
lldp [ agent { nearest-customer | nearest-nontpmr } ] check-change-interval interval
```

```
undo lldp [ agent { nearest-customer | nearest-nontpmr } ] check-change-interval
```

In Layer 2/Layer 3 aggregate interface view:

```
lldp agent { nearest-customer | nearest-nontpmr } check-change-interval interval
```

```
undo lldp agent { nearest-customer | nearest-nontpmr } check-change-interval
```

In synchronous/asynchronous serial interface view, standard POS interface view, or POS channel interface view:

```
lldp check-change-interval interval
```

```
undo lldp check-change-interval
```

Default

LLDP polling is disabled.

Views

Layer 2/Layer 3 aggregate interface view

Layer 2/Layer 3 Ethernet interface view

Management Ethernet interface view

Standard POS interface view, POS channel interface view

Synchronous/asynchronous serial interface view

Predefined user roles

network-admin

Parameters

agent: Specifies an LLDP agent type. If you do not specify an agent type in Ethernet or management Ethernet interface view, the command enables LLDP polling and sets the polling interval for nearest bridge agents.

nearest-customer: Specifies nearest customer bridge agents.

nearest-nontpmr: Specifies nearest non-TPMR bridge agents.

interval: Sets the LLDP polling interval in the range of 1 to 30 seconds.

Examples

```
# Enable LLDP polling and set the polling interval to 30 seconds for the nearest customer bridge agents on GigabitEthernet 2/0/1.
```

```
<Sysname> system-view
```

```
[Sysname] interface gigabitethernet 2/0/1
```

```
[Sysname-GigabitEthernet2/0/1] lldp agent nearest-customer check-change-interval 30
```

```
# Enable LLDP polling and set the polling interval to 30 seconds for the nearest bridge agents on Serial 2/1/0.
```

```
<Sysname> system-view
```

```
[Sysname] interface serial 2/1/0
```

```
[Sysname-Serial2/1/0] lldp check-change-interval 30
```

```
# Enable LLDP polling and set the polling interval to 30 seconds for the nearest bridge agents on POS 2/2/0.
```

```
<Sysname> system-view
```

```
[Sysname] interface pos 2/2/0
[Sysname-Pos2/2/0] lldp check-change-interval 30
```

Ildp enable

Use **lldp enable** to enable LLDP on a port.

Use **undo lldp enable** to disable LLDP on a port.

Syntax

lldp enable

undo lldp enable

Default

LLDP is enabled on a port.

Views

Layer 2/Layer 3 aggregate interface view

Layer 2/Layer 3 Ethernet interface view

Management Ethernet interface view

Standard POS interface view, POS channel interface view

Synchronous/asynchronous serial interface view

Predefined user roles

network-admin

Usage guidelines

LLDP takes effect on a port only when LLDP is enabled both globally and on the port.

Examples

```
# Disable LLDP on GigabitEthernet 2/0/1.
<Sysname> system-view
[Sysname] interface gigabitethernet 2/0/1
[Sysname-GigabitEthernet2/0/1] undo lldp enable
```

Related commands

lldp global enable

Ildp encapsulation snap

Use **lldp encapsulation snap** to set the encapsulation format for LLDP frames to SNAP.

Use **undo lldp encapsulation** to restore the default.

Syntax

In Layer 2/Layer 3 Ethernet interface view or management Ethernet interface view:

lldp [agent { nearest-customer | nearest-nontpmr }] encapsulation snap

undo lldp [agent { nearest-customer | nearest-nontpmr }] encapsulation

In Layer 2/Layer 3 aggregate interface view:

lldp agent { nearest-customer | nearest-nontpmr } encapsulation snap

undo lldp agent { nearest-customer | nearest-nontpmr } encapsulation

In synchronous/asynchronous serial interface view, standard POS interface view, or POS channel interface view:

lldp encapsulation snap

undo lldp encapsulation

Default

The encapsulation format for LLDP frames is Ethernet II.

Views

Layer 2/Layer 3 aggregate interface view

Layer 2/Layer 3 Ethernet interface view

Management Ethernet interface view

Standard POS interface view, POS channel interface view

Synchronous/asynchronous serial interface view

Predefined user roles

network-admin

Parameters

agent: Specifies an LLDP agent type. If you do not specify an agent type in Ethernet or management Ethernet interface view, the command sets the LLDP frame encapsulation format for nearest bridge agents.

nearest-customer: Specifies nearest customer bridge agents.

nearest-nontpmr: Specifies nearest non-TPMR bridge agents.

Usage guidelines

LLDP-CDP packets use only SNAP encapsulation.

Examples

Set the encapsulation format for LLDP frames to SNAP on GigabitEthernet 2/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 2/0/1
[Sysname-GigabitEthernet2/0/1] lldp encapsulation snap
```

Set the encapsulation format for LLDP frames to SNAP on Serial 2/1/0.

```
<Sysname> system-view
[Sysname] interface interface serial 2/1/0
[Sysname-Serial2/1/0] lldp encapsulation snap
```

Set the encapsulation format for LLDP frames to SNAP on POS 2/2/0.

```
<Sysname> system-view
[Sysname] interface pos 2/2/0
[Sysname-Pos2/2/0] lldp encapsulation snap
```

lldp fast-count

Use **lldp fast-count** to set the number of LLDP frames sent each time fast LLDP frame transmission is triggered.

Use **undo lldp fast-count** to restore the default.

Syntax

lldp fast-count *count*

undo lldp fast-count

Default

The number is 4.

Views

System view

Predefined user roles

network-admin

Parameters

count: Sets the number of LLDP frames sent each time fast LLDP frame transmission is triggered. The value range is 1 to 8.

Examples

Configure the device to send five LLDP frames each time fast LLDP frame transmission is triggered.

```
<Sysname> system-view  
[Sysname] lldp fast-count 5
```

lldp global enable

Use **lldp global enable** to enable LLDP globally.

Use **undo lldp global enable** to disable LLDP globally.

Syntax

lldp global enable

undo lldp global enable

Default

LLDP is disabled globally.

Views

System view

Predefined user roles

network-admin

Usage guidelines

LLDP takes effect on a port only when LLDP is enabled both globally and on the port.

Examples

Disable LLDP globally.

```
<Sysname> system-view  
[Sysname] undo lldp global enable
```

Related commands

lldp enable

lldp hold-multiplier

Use **lldp hold-multiplier** to set the TTL multiplier.

Use **undo lldp hold-multiplier** to restore the default.

Syntax

```
lldp hold-multiplier value  
undo lldp hold-multiplier
```

Default

The TTL multiplier is 4.

Views

System view

Predefined user roles

network-admin

Parameters

value: Sets the TTL multiplier in the range of 2 to 10.

Usage guidelines

The TTL TLV carried in an LLDPDU determines how long the device information carried in the LLDPDU can be saved on a recipient device.

By setting the TTL multiplier, you can set the TTL of locally sent LLDP frames. The TTL is expressed by using the following formula:

$$\text{TTL} = \text{Min} (65535, (\text{TTL multiplier} \times \text{LLDP frame transmission interval} + 1))$$

As the expression shows, the TTL can be up to 65535 seconds.

Examples

```
# Set the TTL multiplier to 6.  
<Sysname> system-view  
[Sysname] lldp hold-multiplier 6
```

Related commands

lldp timer tx-interval

lldp ignore-pvid-inconsistency

Use **lldp ignore-pvid-inconsistency** to disable LLDP PVID inconsistency check.

Use **undo lldp ignore-pvid-inconsistency** to enable LLDP PVID inconsistency check.

Syntax

```
lldp ignore-pvid-inconsistency  
undo lldp ignore-pvid-inconsistency
```

Default

LLDP PVID inconsistency check is enabled.

Views

System view

Default command level

network-admin

Usage guidelines

By default, when the system receives an LLDP packet, it compares the PVID value contained in the packet with the PVID configured on the receiving interface. If the two PVIDs do not match, a log message will be printed to notify the user.

You can disable PVID inconsistency check if different PVIDs are required on a link.

Examples

```
# Disable LLDP PVID inconsistency check.
<Sysname> system-view
[Sysname] lldp ignore-pvid-inconsistency
```

Ildp management-address

Use **lldp management-address** to enable the device to generate an ARP or ND entry after receiving an LLDP frame that carries a management address TLV.

Use **undo lldp management-address** to restore the default.

Syntax

```
lldp management-address { arp-learning | nd-learning } [ vlan vlan-id ]
undo lldp management-address { arp-learning | nd-learning }
```

Default

The device does not generate an ARP or ND entry after receiving an LLDP frame that carries a management address TLV.

Views

Layer 3 Ethernet interface view

Default command level

network-admin

Parameters

arp-learning: Generates an ARP entry if the received management address TLV contains an IPv4 address.

nd-learning: Generates an ND entry if the received management address TLV contains an IPv6 address.

vlan *vlan-id*: Specifies a VLAN ID in the range of 1 to 4094. Include this option in the command to generate the ARP or ND entry for the Layer 3 Ethernet subinterface associated with the specified VLAN ID in Dot1q termination. If the specified VLAN is not associated with any Layer 3 Ethernet subinterface, or if no VLAN is specified, the device generates the ARP or ND entry for the current Layer 3 Ethernet interface.

Usage guidelines

You can enable the device to generate both ARP entries and ND entries.

Examples

Configure the device to generate an ARP entry for the Layer 3 Ethernet subinterface after GigabitEthernet 2/0/1 receives an LLDP frame carrying management address TLV in IPv4 format. The Layer 3 Ethernet subinterface is associated with VLAN 4094 in Dot1q termination.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 2/0/1
[Sysname-GigabitEthernet2/0/1] lldp management-address arp-learning vlan 4094
```

Related command

lldp source-mac vlan

lldp management-address-format string

Use **lldp management-address-format string** to set the encoding format of the management address to string.

Use **undo lldp management-address-format** to restore the default.

Syntax

In Layer 2/Layer 3 Ethernet interface view or management Ethernet interface view:

lldp [agent { nearest-customer | nearest-nontpmr }] management-address-format string

undo lldp [agent { nearest-customer | nearest-nontpmr }] management-address-format

In Layer 2/Layer 3 aggregate interface view:

lldp agent { nearest-customer | nearest-nontpmr } management-address-format string

undo lldp agent { nearest-customer | nearest-nontpmr } management-address-format

In synchronous/asynchronous serial interface view, standard POS interface view, or POS channel interface view:

lldp management-address-format string

undo lldp management-address-format

Default

The encoding format of the management address is numeric.

Views

Layer 2/Layer 3 aggregate interface view

Layer 2/Layer 3 Ethernet interface view

Management Ethernet interface view

Standard POS interface view, POS channel interface view

Synchronous/asynchronous serial interface view

Predefined user roles

network-admin

Parameters

agent: Specifies an LLDP agent type. If you do not specify an agent type in Ethernet or management Ethernet interface view, the command sets the encoding format of the management address for nearest bridge agents.

nearest-customer: Specifies nearest customer bridge agents.

nearest-nontpmr: Specifies nearest non-TPMR bridge agents.

Usage guidelines

LLDP neighbors must use the same encoding format for the management address.

Examples

```
# Set the encoding format of the management address to string for the nearest customer bridge agents on GigabitEthernet 2/0/1.
```

```
<Sysname> system-view
```

```
[Sysname] interface gigabitethernet 2/0/1
```

```
[Sysname-GigabitEthernet2/0/1] lldp agent nearest-customer management-address-format string
```

Set the encoding format of the management address to string for the nearest bridge agents on Serial 2/1/0.

```
<Sysname> system-view
```

```
[Sysname] interface serial 2/1/0
```

```
[Sysname-Serial2/1/0] lldp management-address-format string
```

Set the encoding format of the management address to string for the nearest bridge agents on POS 2/2/0.

```
<Sysname> system-view
```

```
[Sysname] interface pos 2/2/0
```

```
[Sysname-Pos2/2/0] lldp management-address-format string
```

Ildp max-credit

Use **lldp max-credit** to set the token bucket size for sending LLDP frames.

Use **undo lldp max-credit** to restore the default.

Syntax

lldp max-credit *credit-value*

undo lldp max-credit

Default

The token bucket size for sending LLDP frames is 5.

Views

System view

Predefined user roles

network-admin

Parameters

credit-value: Specifies the token bucket size for sending LLDP frames, in the range of 1 to 100.

Examples

Set the token bucket size for sending LLDP frames to 10.

```
<Sysname> system-view
```

```
[Sysname] lldp max-credit 10
```

Ildp mode

Use **lldp mode** to configure LLDP to operate in service bridge mode.

Use **undo lldp mode** to restore the default.

Syntax

lldp mode service-bridge

undo lldp mode

Default

LLDP operates in customer bridge mode.

Views

System view

Predefined user roles

network-admin

Parameters

service-bridge: Specifies the service bridge mode.

Usage guidelines

The LLDP agent types supported by LLDP depend on the LLDP bridge mode:

- **Service bridge mode**—LLDP supports nearest bridge agents and nearest non-TPMR bridge agents. LLDP processes the LLDP frames with destination MAC addresses for these agents and transparently transmits the LLDP frames with other destination MAC addresses in the VLAN.
- **Customer bridge mode**—LLDP supports nearest bridge agents, nearest non-TPMR bridge agents, and nearest customer bridge agents. LLDP processes the LLDP frames with destination MAC addresses for these agents and transparently transmits the LLDP frames with other destination MAC addresses in the VLAN.

The bridge mode configuration takes effect only when LLDP is enabled globally. If LLDP is disabled globally, LLDP can only operate in customer bridge mode.

Examples

```
# Configure LLDP to operate in service bridge mode.
<Sysname> system-view
[Sysname] lldp mode service-bridge
```

Related commands

lldp global enable

Ildp notification med-topology-change enable

Use **lldp notification med-topology-change enable** to enable LLDP-MED trapping.

Use **undo lldp notification med-topology-change enable** to disable LLDP-MED trapping.

Syntax

```
lldp notification med-topology-change enable
undo lldp notification med-topology-change enable
```

Default

LLDP-MED trapping is disabled.

Views

Layer 2 Ethernet interface view

Layer 3 Ethernet interface view

Management Ethernet interface view

Predefined user roles

network-admin

Examples

```
# Enable LLDP-MED trapping on GigabitEthernet 2/0/1.
<Sysname> system-view
```

```
[Sysname] interface gigabitethernet 2/0/1
[Sysname-GigabitEthernet2/0/1] lldp notification med-topology-change enable
```

Ildp notification remote-change enable

Use **lldp notification remote-change enable** to enable LLDP trapping.

Use **undo lldp notification remote-change enable** to disable LLDP trapping.

Syntax

In Layer 2/Layer 3 Ethernet interface view or management Ethernet interface view:

```
lldp [ agent { nearest-customer | nearest-nontpmr } ] notification remote-change enable
```

```
undo lldp [ agent { nearest-customer | nearest-nontpmr } ] notification remote-change enable
```

In Layer 2/Layer 3 aggregate interface view:

```
lldp agent { nearest-customer | nearest-nontpmr } notification remote-change enable
```

```
undo lldp agent { nearest-customer | nearest-nontpmr } notification remote-change enable
```

In synchronous/asynchronous serial interface view, standard POS interface view, or POS channel interface view:

```
lldp notification remote-change enable
```

```
undo lldp notification remote-change enable
```

Default

LLDP trapping is disabled.

Views

Layer 2/Layer 3 aggregate interface view

Layer 2/Layer 3 Ethernet interface view

Management Ethernet interface view

Standard POS interface view, POS channel interface view

Synchronous/asynchronous serial interface view

Predefined user roles

network-admin

Parameters

agent: Specifies an LLDP agent type. If you do not specify an agent type in Ethernet or management Ethernet interface view, the command enables LLDP trapping for nearest bridge agents.

nearest-customer: Specifies nearest customer bridge agents.

nearest-nontpmr: Specifies nearest non-TPMR bridge agents.

Examples

```
# Enable LLDP trapping for the nearest customer bridge agents on GigabitEthernet 2/0/1.
```

```
<Sysname> system-view
```

```
[Sysname] interface GigabitEthernet 2/0/1
```

```
[Sysname-GigabitEthernet2/0/1] lldp agent nearest-customer notification remote-change enable
```

```
# Enable LLDP trapping for the nearest bridge agents on Serial 2/1/0.
```

```
<Sysname> system-view
```

```
[Sysname] interface serial 2/1/0
```

```
[Sysname-Serial2/1/0] lldp notification remote-change enable
# Enable LLDP trapping for the nearest bridge agents on POS 2/2/0.
<Sysname> system-view
[Sysname] interface interface pos 2/2/0
[Sysname-Pos2/2/0] lldp notification remote-change enable
```

Ildp source-mac vlan

Use **lldp source-mac vlan** to set the source MAC address of LLDP frames to the MAC address of the Layer 3 Ethernet subinterface associated with the specified VLAN.

Use **undo lldp source-mac** to restore the default.

Syntax

lldp source-mac vlan *vlan-id*

undo lldp source-mac

Default

The source MAC address of LLDP frames is the MAC address of the port.

Views

Layer 3 Ethernet interface view

Default command level

network-admin

Parameters

vlan-id: Specifies a VLAN ID in the range of 1 to 4094. After the argument is specified, the source MAC address of LLDP frames is the MAC address of the Layer 3 Ethernet subinterface associated with the VLAN in Dot1q termination. If the specified VLAN has not been associated with a Layer 3 Ethernet subinterface, the source MAC address of LLDP frames is the MAC address of the port.

Examples

Set the source MAC address of LLDP frames to the MAC address of the Layer 3 Ethernet subinterface associated with VLAN 4094 in Dot1q termination.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 2/0/1
[Sysname-GigabitEthernet2/0/1] lldp source-mac vlan 4094
```

Related command

lldp management-address arp-learning

Ildp timer fast-interval

Use **lldp timer fast-interval** to set an interval for fast LLDP frame transmission.

Use **undo lldp timer fast-interval** to restore the default.

Syntax

lldp timer fast-interval *interval*

undo lldp timer fast-interval

Default

The interval for fast LLDP frame transmission is 1 second.

Views

System view

Predefined user roles

network-admin

Parameters

interval: Sets an interval for fast LLDP frame transmission, in the range of 1 to 3600 seconds.

Examples

```
# Set the interval for fast LLDP frame transmission to 2 seconds.
```

```
<Sysname> system-view
```

```
[Sysname] lldp timer fast-interval 2
```

Ildp timer notification-interval

Use **lldp timer notification-interval** to set the LLDP trap and LLDP-MED trap transmission interval.

Use **undo lldp timer notification-interval** to restore the default.

Syntax

```
lldp timer notification-interval interval
```

```
undo lldp timer notification-interval
```

Default

The LLDP trap and LLDP-MED trap transmission interval is 30 seconds.

Views

System view

Predefined user roles

network-admin

Parameters

interval: Sets the LLDP trap and LLDP-MED trap transmission interval in the range of 5 to 3600 seconds.

Examples

```
# Set both the LLDP trap and LLDP-MED trap transmission interval to 8 seconds.
```

```
<Sysname> system-view
```

```
[Sysname] lldp timer notification-interval 8
```

Ildp timer reinit-delay

Use **lldp timer reinit-delay** to set the LLDP reinitialization delay.

Use **undo lldp timer reinit-delay** to restore the default.

Syntax

```
lldp timer reinit-delay delay
```

```
undo lldp timer reinit-delay
```

Default

The LLDP reinitialization delay is 2 seconds.

Views

System view

Predefined user roles

network-admin

Parameters

delay: Sets the LLDP reinitialization delay in the range of 1 to 10 seconds.

Examples

```
# Set the LLDP reinitialization delay to 4 seconds.
```

```
<Sysname> system-view
```

```
[Sysname] lldp timer reinit-delay 4
```

Ildp timer tx-interval

Use **lldp timer tx-interval** to set the LLDP frame transmission interval.

Use **undo lldp timer tx-interval** to restore the default.

Syntax

```
lldp timer tx-interval interval
```

```
undo lldp timer tx-interval
```

Default

The LLDP frame transmission interval is 30 seconds.

Views

System view

Predefined user roles

network-admin

Parameters

interval: Sets the LLDP frame transmission interval in the range of 5 to 32768 seconds.

Examples

```
# Set the LLDP frame transmission interval to 20 seconds.
```

```
<Sysname> system-view
```

```
[Sysname] lldp timer tx-interval 20
```

Ildp tlv-enable

Use **lldp tlv-enable** to configure the types of advertisable TLVs on a port.

Use **undo lldp tlv-enable** to disable the advertising of the specified types of TLVs on a port.

Syntax

In Layer 2 Ethernet interface view:

- For nearest bridge agents:

```
lldp tlv-enable { basic-tlv { all | port-description | system-capability | system-description | system-name | management-address-tlv [ ipv6 ] [ ip-address ] } | dot1-tlv { all | port-vlan-id | link-aggregation | protocol-vlan-id [ vlan-id ] | vlan-name [ vlan-id ] | management-vid [ mvlan-id ] } | dot3-tlv { all | mac-physic | max-frame-size | power } | med-tlv { all | capability
```

| **inventory** | **network-policy** [*vlan-id*] | **power-over-ethernet** | **location-id** { **civic-address** *device-type country-code* { *ca-type ca-value* } &<1-10> | **elin-address** *tel-number* } }

undo lldp tlv-enable { **basic-tlv** { **all** | **port-description** | **system-capability** | **system-description** | **system-name** | **management-address-tlv** [**ipv6**] [*ip-address*] } | **dot1-tlv** { **all** | **port-vlan-id** | **link-aggregation** | **protocol-vlan-id** | **vlan-name** | **management-vid** } | **dot3-tlv** { **all** | **mac-physic** | **max-frame-size** | **power** } | **med-tlv** { **all** | **capability** | **inventory** | **network-policy** [*vlan-id*] | **power-over-ethernet** | **location-id** } }

- For nearest non-TPMR bridge agents:

lldp agent nearest-nontpmr tlv-enable { **basic-tlv** { **all** | **port-description** | **system-capability** | **system-description** | **system-name** | **management-address-tlv** [**ipv6**] [*ip-address*] } | **dot1-tlv** { **all** | **port-vlan-id** | **link-aggregation** } }

undo lldp agent nearest-nontpmr tlv-enable { **basic-tlv** { **all** | **port-description** | **system-capability** | **system-description** | **system-name** | **management-address-tlv** [**ipv6**] [*ip-address*] } | **dot1-tlv** { **all** | **port-vlan-id** | **link-aggregation** } }

- For nearest customer bridge agents:

lldp agent nearest-customer tlv-enable { **basic-tlv** { **all** | **port-description** | **system-capability** | **system-description** | **system-name** | **management-address-tlv** [**ipv6**] [*ip-address*] } | **dot1-tlv** { **all** | **port-vlan-id** | **link-aggregation** } }

undo lldp agent nearest-customer tlv-enable { **basic-tlv** { **all** | **port-description** | **system-capability** | **system-description** | **system-name** | **management-address-tlv** [**ipv6**] [*ip-address*] } | **dot1-tlv** { **all** | **port-vlan-id** | **link-aggregation** } }

In Layer 3 Ethernet interface view:

- **lldp tlv-enable** { **basic-tlv** { **all** | **port-description** | **system-capability** | **system-description** | **system-name** | **management-address-tlv** [**ipv6**] [*ip-address* | **interface loopback** *interface-number*] } | **dot1-tlv** { **all** | **link-aggregation** } | **dot3-tlv** { **all** | **mac-physic** | **max-frame-size** | **power** } | **med-tlv** { **all** | **capability** | **inventory** | **power-over-ethernet** | **location-id** { **civic-address** *device-type country-code* { *ca-type ca-value* } &<1-10> | **elin-address** *tel-number* } } }

- **lldp agent** { **nearest-nontpmr** | **nearest-customer** } **tlv-enable** { **basic-tlv** { **all** | **port-description** | **system-capability** | **system-description** | **system-name** | **management-address-tlv** [**ipv6**] [*ip-address*] } | **dot1-tlv** { **all** | **link-aggregation** } }

- **undo lldp tlv-enable** { **basic-tlv** { **all** | **port-description** | **system-capability** | **system-description** | **system-name** | **management-address-tlv** [**ipv6**] [*ip-address* | **interface loopback** *interface-number*] } | **dot1-tlv** { **all** | **link-aggregation** } | **dot3-tlv** { **all** | **mac-physic** | **max-frame-size** | **power** } | **med-tlv** { **all** | **capability** | **inventory** | **power-over-ethernet** | **location-id** } }

- **undo lldp agent** { **nearest-nontpmr** | **nearest-customer** } **tlv-enable** { **basic-tlv** { **all** | **port-description** | **system-capability** | **system-description** | **system-name** | **management-address-tlv** [**ipv6**] [*ip-address*] } | **dot1-tlv** { **all** | **link-aggregation** } }

In management Ethernet interface view:

- **lldp tlv-enable** { **basic-tlv** { **all** | **port-description** | **system-capability** | **system-description** | **system-name** | **management-address-tlv** [**ipv6**] [*ip-address*] } | **dot1-tlv** { **all** | **link-aggregation** } | **dot3-tlv** { **all** | **mac-physic** | **max-frame-size** | **power** } | **med-tlv** { **all** | **capability** | **inventory** | **power-over-ethernet** | **location-id** { **civic-address** *device-type country-code* { *ca-type ca-value* } &<1-10> | **elin-address** *tel-number* } } }

- **lldp agent** { **nearest-nontpmr** | **nearest-customer** } **tlv-enable** { **basic-tlv** { **all** | **port-description** | **system-capability** | **system-description** | **system-name** | **management-address-tlv** [**ipv6**] [*ip-address*] } | **dot1-tlv** { **all** | **link-aggregation** } }

- **undo lldp tlv-enable** { **basic-tlv** { **all** | **port-description** | **system-capability** | **system-description** | **system-name** | **management-address-tlv** [**ipv6**] [*ip-address*] } | **dot1-tlv** { **all** | **link-aggregation** } | **dot3-tlv** { **all** | **mac-physic** | **max-frame-size** | **power** } | **med-tlv** { **all** | **capability** | **inventory** | **power-over-ethernet** | **location-id** } }

- **undo lldp agent { nearest-nontpmr | nearest-customer } tlv-enable { basic-tlv { all | port-description | system-capability | system-description | system-name | management-address-tlv [ipv6] [ip-address] } | dot1-tlv { all | link-aggregation } }**

In Layer 2 aggregate interface view:

- **lldp agent nearest-nontpmr tlv-enable { basic-tlv { all | management-address-tlv [ipv6] [ip-address] | port-description | system-capability | system-description | system-name } | dot1-tlv { all | port-vlan-id } }**
- **lldp agent nearest-customer tlv-enable { basic-tlv { all | management-address-tlv [ipv6] [ip-address] | port-description | system-capability | system-description | system-name } | dot1-tlv { all | port-vlan-id } }**
- **lldp tlv-enable dot1-tlv { protocol-vlan-id [vlan-id] | vlan-name [vlan-id] | management-vid [mvlan-id] }**
- **undo lldp agent nearest-nontpmr tlv-enable { basic-tlv { all | management-address-tlv [ipv6] [ip-address] | port-description | system-capability | system-description | system-name } | dot1-tlv { all | port-vlan-id } }**
- **undo lldp agent nearest-customer tlv-enable { basic-tlv { all | management-address-tlv [ipv6] [ip-address] | port-description | system-capability | system-description | system-name } | dot1-tlv { all | port-vlan-id } }**
- **undo lldp tlv-enable dot1-tlv { protocol-vlan-id | vlan-name | management-vid }**

In Layer 3 aggregate interface view:

- **lldp agent { nearest-nontpmr | nearest-customer } tlv-enable basic-tlv { all | management-address-tlv [ipv6] [ip-address] | port-description | system-capability | system-description | system-name }**
- **undo lldp agent { nearest-nontpmr | nearest-customer } tlv-enable basic-tlv { all | management-address-tlv [ipv6] [ip-address] | port-description | system-capability | system-description | system-name }**

In synchronous/asynchronous serial interface view, standard POS interface view, or POS channel interface view:

- **lldp tlv-enable { basic-tlv { all | port-description | system-capability | system-description | system-name | management-address-tlv [ipv6] [ip-address] } }**
- **undo lldp tlv-enable { basic-tlv { all | port-description | system-capability | system-description | system-name | management-address-tlv [ipv6] [ip-address] } }**

Default

On Layer 2 Ethernet interfaces:

- Nearest bridge agents can advertise all types of LLDP TLVs except the following types:
 - Location identification TLVs.
 - Port and protocol VLAN ID TLVs.
 - VLAN name TLVs.
 - Management VLAN ID TLVs.
 - Energy-Efficient Ethernet TLVs.
- Nearest customer bridge agents can advertise basic TLVs and IEEE 802.1 organizationally specific TLVs.

On Layer 3 Ethernet interfaces or management Ethernet interfaces:

- Nearest bridge agents can advertise all types of LLDP TLVs (only link aggregation TLV is supported in 802.1 organizationally specific TLVs) except network policy TLVs and Energy-Efficient Ethernet TLVs.
- Nearest non-TPMR bridge agents do not advertise TLVs.

- Nearest customer bridge agents can advertise basic TLVs and IEEE 802.1 organizationally specific TLVs (only link aggregation TLV is supported).

On Layer 2 aggregate interfaces:

Nearest customer bridge agents can advertise basic TLVs and IEEE 802.1 organizationally specific TLVs. Among the IEEE 802.1 organizationally specific TLVs, only port and protocol VLAN ID TLVs, VLAN name TLVs, and management VLAN ID TLVs are supported.

On Layer 3 aggregate interfaces:

- Nearest non-TPMR bridge agents do not advertise TLVs.
- Nearest customer bridge agents can advertise only basic TLVs.

On synchronous/asynchronous serial interfaces, standard POS interfaces, or POS channel interfaces:

- Nearest customer bridge agents and non-TPMR bridge agents are not supported.
- Nearest bridge agents can advertise only basic TLVs.

Views

Layer 2/Layer 3 aggregate interface view

Layer 2/Layer 3 Ethernet interface view

Management Ethernet interface view

Standard POS interface view, POS channel interface view

Synchronous/asynchronous serial interface view

Predefined user roles

network-admin

Parameters

agent: Specifies an LLDP agent type. If you do not specify an agent type in Ethernet or management Ethernet interface view, the command configures the types of advertisable TLVs for nearest bridge agents.

nearest-customer: Specifies nearest customer bridge agents.

nearest-nontpmr: Specifies nearest non-TPMR bridge agents.

all: Advertises all TLVs of the specified type.

- Enables the interface to advertise the following TLVs:
 - All basic LLDP TLVs if the **all** keyword is specified for **basic-tlv**.
 - All IEEE 802.1 organizationally specific LLDP TLVs if the **all** keyword is specified for **dot1-tlv**.
 - All IEEE 802.3 organizationally specific LLDP TLVs if the **all** keyword is specified for **dot3-tlv**.
- Enables the interface to advertise all LLDP-MED TLVs except location identification TLVs if the **all** keyword is specified for **med-tlv**.

basic-tlv: Advertises basic LLDP TLVs.

management-address-tlv [ipv6] [ip-address | interface loopback interface-number]: Advertises management address TLVs. The **ipv6** keyword indicates that the management address to be advertised is in IPv6 format. If you do not specify this keyword, the management address in IPv4 format will be advertised. The *ip-address* argument specifies the management address to be advertised. The **interface loopback interface-number** option specifies the management address as the IP address of a loopback interface specified by its number. By default, the following rules apply:

- When you execute the **lldp tlv-enable** command:

- For a Layer 2 Ethernet or aggregate interface, the management address is the primary IPv4/IPv6 address of the VLAN interface meeting the following requirements:
 - In up state.
 - The corresponding VLAN ID is the lowest among the VLANs permitted on the port.

If you specify the **ipv6** keyword, the management address is the primary IPv6 address. If you do not specify the **ipv6** keyword, the management address is the primary IPv4 address.

If none of the VLAN interfaces of the permitted VLANs is assigned an IP address or all VLAN interfaces are down, the MAC address of the port will be advertised.
- For a Layer 3 Ethernet interface, the IPv4/IPv6 address of the port will be advertised when the following conditions exist:
 - The *ip-address* argument is not configured.
 - The specified loopback interface does not have an IPv4/IPv6 address, or the specified loopback interface does not exist.

If you specify the **ipv6** keyword, the management address is the IPv6 address. If you do not specify the **ipv6** keyword, the management address is the IPv4 address.

If the port does not have an IP address, the MAC address of the port will be advertised.
- For a Layer 3 aggregate interface, management Ethernet interface, synchronous/asynchronous serial interface, standard POS interface, or POS channel interface, the IPv4/IPv6 address of the port will be advertised when the *ip-address* argument is not configured.

If you specify the **ipv6** keyword, the management address is the IPv6 address. If you do not specify the **ipv6** keyword, the management address is the IPv4 address.

If the port does not have an IP address, the MAC address of the port will be advertised.

- When you execute the **undo lldp tlv-enable** command:
 - For a Layer 2/Layer 3 Ethernet interface, management Ethernet interface, or Layer 2/Layer 3 aggregate interface:
 - If you do not specify **ipv6**, *ip-address*, and **interface loopback interface-number**, the port does not advertise any management address TLVs.
 - If you specify **ipv6**, *ip-address*, or **interface loopback interface-number**, the port advertises the default management address TLVs.
 - For a synchronous/asynchronous serial interface, standard POS interface, or POS channel interface:
 - If you do not specify **ipv6** and *ip-address*, the port does not advertise any management address TLVs.
 - If you specify **ipv6** or *ip-address*, the port advertises the default management address TLVs.

port-description: Advertises port description TLVs.

system-capability: Advertises system capabilities TLVs.

system-description: Advertises system description TLVs.

system-name: Advertises system name TLVs.

dot1-tlv: Advertises IEEE 802.1 organizationally specific LLDP TLVs.

port-vlan-id: Advertises port VLAN ID TLVs.

protocol-vlan-id [*vlan-id*]: Advertises port and protocol VLAN ID TLVs. The *vlan-id* argument specifies a VLAN ID in the TLVs to be advertised. The VLAN ID is in the range of 1 to 4094, and the default is the lowest VLAN ID on the port.

vlan-name [*vlan-id*]: Advertises VLAN name TLVs. The *vlan-id* argument specifies a VLAN ID in the TLVs to be advertised. The VLAN ID is in the range of 1 to 4094, and the default is the lowest VLAN

ID on the port. If you do not specify a VLAN ID and the port is not assigned to any VLAN, the PVID of the port is advertised.

management-vid [*mvlan-id*]: Advertises management VLAN ID TLVs. The *mvlan-id* argument specifies a management VLAN ID in the TLVs to be advertised. The management VLAN ID is in the range of 1 to 4094. If you do not specify this option, the value 0 is advertised, which means that the LLDP agent is not configured with a management VLAN ID.

dot3-tlv: Advertises IEEE 802.3 organizationally specific LLDP TLVs.

link-aggregation: Advertises link aggregation TLVs.

mac-physic: Advertises MAC/PHY configuration/status TLVs.

max-frame-size: Advertises maximum frame size TLVs.

power: Advertises power in MDI TLVs and power stateful control TLVs.

med-tlv: Advertises LLDP-MED TLVs.

capability: Advertises LLDP-MED capabilities TLVs.

inventory: Advertises the following TLVs: hardware revision, firmware revision, software revision, serial number, manufacturer name, model name, and asset ID.

location-id: Advertises location identification TLVs.

civic-address: Inserts the typical address information about the network device in location identification TLVs .

device-type: Sets a device type value in the range of 0 to 2:

- Value 0 specifies a DHCP server.
- Value 1 specifies a network device.
- Value 2 specifies an LLDP-MED endpoint.

country-code: Sets a country code defined in ISO 3166.

{ *ca-type ca-value* }&<1-10>: Configures address information. *ca-type* represents the address information type in the range of 0 to 255. *ca-value* represents address information, a string of 1 to 250 characters. &<1-10> indicates that you can specify up to 10 *ca-type ca-value* pairs.

elin-address: Inserts telephone numbers for emergencies in location identification TLVs.

tel-number: Sets the telephone number for emergencies, a string of 10 to 25 characters.

network-policy [*vlan-id*]: Advertises network policy TLVs. *vlan-id* specifies the voice VLAN ID to be advertised, in the range of 1 to 4094.

power-over-ethernet: Advertises extended power-via-MDI TLVs.

Usage guidelines

Nearest bridge agents are not supported on aggregate interfaces.

You can enable the device to advertise multiple types of TLVs by using this command without the **all** keyword specified.

If the MAC/PHY configuration/status TLV is not advertisable, none of the LLDP-MED TLVs will be advertised whether or not they are advertisable. If the LLDP-MED capabilities TLV is not advertisable, the other LLDP-MED TLVs will not be advertised regardless of whether or not they are advertisable.

The port and protocol VLAN ID, VLAN name, and management VLAN ID TLVs in IEEE 802.1 organizationally specific LLDP TLVs can be configured only for nearest bridge agents. The configuration can be inherited by nearest customer bridge agents and nearest non-TPMR bridge agents.

Examples

Enable the nearest customer bridge agents on GigabitEthernet 2/0/1 to advertise link aggregation TLVs of the IEEE 802.1 organizationally specific TLVs.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 2/0/1
[Sysname-GigabitEthernet2/0/1] lldp agent nearest-customer tlv-enable dot1-tlv
link-aggregation
```

Disable the nearest bridge agents on Serial 2/1/0 from advertising port description TLVs of the basic optional TLVs.

```
<Sysname> system-view
[Sysname] interface serial 2/1/0
[Sysname- Serial2/1/0] undo lldp tlv-enable basic-tlv port-description
```

Disable the nearest bridge agents on POS 2/2/0 from advertising port description TLVs of the basic optional TLVs.

```
<Sysname> system-view
[Sysname] interface pos 2/2/0
[Sysname-Pos2/2/0] undo lldp tlv-enable basic-tlv port-description
```

Layer 2 forwarding commands

This feature is supported only on the following ports:

- Layer 2 Ethernet ports on Ethernet switching modules.
- Fixed Layer 2 Ethernet ports on the following routers:
 - MSR1002-4.
 - MSR1003-8S.
 - MSR2004-24.
 - MSR2004-48.
 - MSR954 (JH296A/JH297A/JH298A/JH299A/JH373A).
 - MSR958 (JH300A/JH301A).

On Layer 2 Ethernet switching modules of MSR devices that are operating in IRF mode, Layer 2 forwarding across member devices is not supported. On SIC Layer 2 Ethernet switching modules, Layer 2 forwarding across member devices and slots is not supported.

Layer 2 forwarding across slots that reside on the same device is supported if multiple HMIM-24GSW, HMIM-24GSWP, or HMIM-8GSW Layer 2 Ethernet switching modules are installed on the following devices:

- MSR3012/3024/3044/3064.
- MSR4060/4080.

Normal Layer 2 forwarding commands

display mac-forwarding statistics

Use **display mac-forwarding statistics** to display Layer 2 forwarding statistics.

Syntax

```
display mac-forwarding statistics [ interface interface-type interface-number ]
```

Views

Any view

Predefined user roles

network-admin
network-operator

Parameters

interface *interface-type interface-number*. Specifies an interface by its type and number. If you do not specify this option, the command displays Layer 2 forwarding statistics on all interfaces.

Examples

Display Layer 2 forwarding statistics on all interfaces.

```
<Sysname> display mac-forwarding statistics
```

Input:

Sum:	888	Unknown Unicast:	0
Broadcast:	0	Multicast:	0
Filtered:	0	STP discarded:	0

```

Service dropped: 0          Source dropped: 0
Unknown dropped: 0        Learning dropped: 0
Attack dropped: 0         Suppress dropped: 0
Deliver:
  Sum: 111                L2 protocol: 11
  Local MAC address: 100
Output:
  Sum: 666                Filtered: 0
  Blackhole dropped: 0    STP discarded: 0
  Service dropped: 0      Dest MAC dropped: 0

```

Display Layer 2 forwarding statistics on GigabitEthernet 1/0/1.

```

<Sysname> display mac-forwarding statistics interface gigabitethernet 1/0/1
GigabitEthernet 1/0/1:
Input frames: 100    Output frames:100
Filtered: 0

```

Table 38 Command output

Field	Description
Input	Inbound Ethernet frame statistics.
Sum	Total number of received Ethernet frames.
Filtered	Number of Ethernet frames filtered out by 802.1Q VLAN inbound filtering rules.
STP discarded	Number of inbound Ethernet frames dropped on the ports blocked by STP.
Service dropped	Number of Ethernet frames dropped by inbound service features.
Source dropped	Number of Ethernet frames dropped because their source MAC addresses are all-zeros, multicast, or broadcast MAC addresses.
Unknown dropped	Number of Ethernet frames dropped because the device is disabled from forwarding frames with unknown source MAC addresses.
Learning dropped	Number of Ethernet frames dropped because the device is disabled from forwarding unknown frames after the number of learned MAC addresses reaches the upper limit.
Attack dropped	Number of attack Ethernet frames dropped by features based on the source MAC addresses.
Suppress dropped	Number of Ethernet frames dropped by storm suppression.
Broadcast	Number of received broadcast Ethernet frames.
Multicast	Number of received multicast Ethernet frames.
Unknown Unicast	Number of received unknown unicast Ethernet frames.
Deliver	Statistics of Ethernet frames delivered to the CPU.
Sum	Total number of Ethernet frames delivered to the CPU.
L2 protocol	Number of Layer 2 protocol Ethernet frames delivered to the CPU.
Local MAC address	Number of Ethernet frames with the destination MAC addresses being the MAC addresses of local Layer 3 VLAN interfaces.
Output	Outbound Ethernet frame statistics.
Sum	Total number of sent Ethernet frames.

Field	Description
Blackhole dropped	Number of Ethernet frames dropped because they are destined for blackhole MAC addresses.
Filtered	Number of Ethernet frames filtered out by 802.1Q VLAN outbound filtering rules.
STP discarded	Number of outbound Ethernet frames dropped on the ports blocked by STP.
Service dropped	Number of Ethernet frames dropped by outbound service features.
Dest MAC dropped	Number of Ethernet frames dropped by features based on the destination MAC addresses.
Input frames	Number of Ethernet frames received on the interface.
Output frames	Number of Ethernet frames sent out of the interface.
Filtered	Number of Ethernet frames filtered out because they are from other VLANs.

reset mac-forwarding statistics

Use **reset mac-forwarding statistics** to clear Layer 2 forwarding statistics.

Syntax

```
reset mac-forwarding statistics
```

Views

User view

Predefined user roles

network-admin
network-operator

Examples

```
# Clear Layer 2 forwarding statistics.
<Sysname> reset mac-forwarding statistics
```

Fast Layer 2 forwarding commands

Commands and descriptions for centralized devices apply to the following routers:

- MSR1002-4/1003-8S.
- MSR2003.
- MSR2004-24/2004-48.
- MSR3012/3024/3044/3064.
- MSR954 (JH296A/JH297A/JH298A/JH299A/JH373A).
- MSR958 (JH300A/JH301A).

Commands and descriptions for distributed devices apply to MSR4060 and MSR4080 routers.

display mac-forwarding cache ip

Use **display mac-forwarding cache ip** to display IPv4 fast forwarding entries.

Syntax

Centralized devices in standalone mode:

```
display mac-forwarding cache ip [ ip-address ]
```

Distributed devices in standalone mode/centralized devices in IRF mode:

```
display mac-forwarding cache ip [ ip-address ] [ slot slot-number ]
```

Distributed devices in IRF mode:

```
display mac-forwarding cache ip [ ip-address ] [ chassis chassis-number slot slot-number ]
```

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

ip-address: Specifies an IPv4 address. If you do not specify an IPv4 address, this command displays all IPv4 fast forwarding entries.

slot *slot-number*: Specifies a card by its slot number. If you do not specify a card, this command displays IPv4 fast forwarding entries for all cards. (Distributed devices in standalone mode.)

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays IPv4 fast forwarding entries for all member devices. (Centralized devices in IRF mode.)

chassis *chassis-number* **slot** *slot-number*: Specifies a card on an IRF member device. The *chassis-number* argument represents the member ID of the IRF member device. The *slot-number* argument represents the slot number of the card. If you do not specify a card, this command displays IPv4 fast forwarding entries for all cards. (Distributed devices in IRF mode)

Examples

Display all IPv4 fast forwarding entries.

```
<Sysname> display mac-forwarding cache ip
```

```
Total number of mac-forwarding entries: 2
```

SIP	SPort	DIP	DPort	Pro	Input_If	Output_If	VLAN
1.1.1.2	99	1.1.1.1	2048	1	GE0/46	GE0/47	2
1.1.1.1	98	1.1.1.2	2012	1	GE0/47	GE0/46	2

Table 39 Command output

Field	Description
Total number of mac-forwarding entries	Total number of IPv4 fast forwarding entries.
SIP	Source IPv4 address.
SPort	Source port number.
DIP	Destination IPv4 address.
DPort	Destination port number.
Pro	Protocol number.

Field	Description
Input_If	Input interface type and number. If no input interface is involved in fast forwarding, this field displays N/A . If no input interface is available, this field displays a hyphen (-).
Output_If	Output interface type and number. If no output interface is involved in fast forwarding, this field displays N/A . If no output interface is available, this field displays a hyphen (-).
VLAN	VLAN ID.

display mac-forwarding cache ip fragment

Use **display mac-forwarding cache ip fragment** to display IPv4 fast forwarding entries for fragments.

Syntax

Centralized devices in standalone mode:

display mac-forwarding cache ip fragment [*ip-address*]

Distributed devices in standalone mode/centralized devices in IRF mode:

display mac-forwarding cache ip fragment [*ip-address*] [**slot** *slot-number*]

Distributed devices in IRF mode:

display mac-forwarding cache ip fragment [*ip-address*] [**chassis** *chassis-number* **slot** *slot-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

ip-address: Specifies an IPv4 address. If you do not specify an IPv4 address, this command displays IPv4 fast forwarding entries for all fragments.

slot *slot-number*: Specifies a card by its slot number. If you do not specify a card, this command displays IPv4 fast forwarding entries for fragments on all cards. (Distributed devices in standalone mode.)

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays IPv4 fast forwarding entries for fragments on all member devices. (Centralized devices in IRF mode.)

chassis *chassis-number* **slot** *slot-number*: Specifies a card on an IRF member device. The *chassis-number* argument represents the member ID of the IRF member device. The *slot-number* argument represents the slot number of the card. If you do not specify a card, this command displays IPv4 fast forwarding entries for fragments on all cards. (Distributed devices in IRF mode)

Examples

Display IPv4 fast forwarding entries for all fragments.

```

<Sysname> display mac-forwarding cache ip fragment
Total number of fragment mac-forwarding entries: 2
SIP          SPort  DIP          DPort  Pro  Input_If    ID    VLAN
1.1.1.1      117    1.1.1.2      0       1    GE0/47      2828  1
1.1.1.2      110    1.1.1.1      67      17   GE0/48      2322  1

```

Table 40 Command output

Field	Description
Total number of fragment mac-forwarding entries	Total number of IPv4 fast forwarding entries for fragments.
SIP	Source IPv4 address.
SPort	Source port number.
DIP	Destination IPv4 address.
DPort	Destination port number.
Pro	Protocol number.
Input_If	Input interface type and number. If no input interface is involved in fast forwarding, this field displays N/A . If no input interface is available, this field displays a hyphen (-).
ID	Fragment ID.
VLAN	VLAN ID.

display mac-forwarding cache ipv6

Use **display mac-forwarding cache ipv6** to display IPv6 fast forwarding entries.

Syntax

Centralized devices in standalone mode:

```
display mac-forwarding cache ipv6 [ ipv6-address ]
```

Distributed devices in standalone mode/centralized devices in IRF mode:

```
display mac-forwarding cache ipv6 [ ipv6-address ] [ slot slot-number ]
```

Distributed devices in IRF mode:

```
display mac-forwarding cache ipv6 [ ipv6-address ] [ chassis chassis-number slot slot-number ]
```

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

ipv6-address: Specifies an IPv6 address. If you do not specify an IPv6 address, this command displays all IPv6 fast forwarding entries.

slot *slot-number*: Specifies a card by its slot number. If you do not specify a card, this command displays IPv6 fast forwarding entries for all cards. (Distributed devices in standalone mode.)

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays IPv6 fast forwarding entries for all member devices. (Centralized devices in IRF mode.)

chassis *chassis-number* **slot** *slot-number*: Specifies a card on an IRF member device. The *chassis-number* argument represents the member ID of the IRF member device. The *slot-number* argument represents the slot number of the card. If you do not specify a card, this command displays IPv6 fast forwarding entries for all cards. (Distributed devices in IRF mode)

Examples

Display all IPv6 fast forwarding entries.

```
<Sysname> display mac-forwarding cache ipv6
Total number of IPv6 mac-forwarding items: 1
Src IP: 2002::1                               Src port: 129
Dst IP: 2001::1                               Dst port: 65535
VLAN ID: 2
Protocol: 2
Input interface: GE1/0/2
Output interface: GE1/0/1
```

Table 41 Command output

Field	Description
Total number of IPv6 mac-forwarding items	Total number of IPv6 fast forwarding entries.
Src IP	Source IPv6 address.
Src port	Source port number.
Dst IP	Destination IPv6 address.
Dst Port	Destination port number.
Protocol	Protocol number.
Input interface	Input interface type and number. If no input interface is involved in fast forwarding, this field displays N/A . If no input interface is available, this field displays a hyphen (-).
Output interface	Output interface type and number. If no output interface is involved in fast forwarding, this field displays N/A . If no output interface is available, this field displays a hyphen (-).

Document conventions and icons

Conventions

This section describes the conventions used in the documentation.

Port numbering in examples

The port numbers in this document are for illustration only and might be unavailable on your device.

Command conventions

Convention	Description
Boldface	Bold text represents commands and keywords that you enter literally as shown.
<i>Italic</i>	<i>Italic</i> text represents arguments that you replace with actual values.
[]	Square brackets enclose syntax choices (keywords or arguments) that are optional.
{ x y ... }	Braces enclose a set of required syntax choices separated by vertical bars, from which you select one.
[x y ...]	Square brackets enclose a set of optional syntax choices separated by vertical bars, from which you select one or none.
{ x y ... }*	Asterisk marked braces enclose a set of required syntax choices separated by vertical bars, from which you select at least one.
[x y ...]*	Asterisk marked square brackets enclose optional syntax choices separated by vertical bars, from which you select one choice, multiple choices, or none.
&<1-n>	The argument or keyword and argument combination before the ampersand (&) sign can be entered 1 to n times.
#	A line that starts with a pound (#) sign is comments.

GUI conventions

Convention	Description
Boldface	Window names, button names, field names, and menu items are in Boldface. For example, the New User window appears; click OK .
>	Multi-level menus are separated by angle brackets. For example, File > Create > Folder .

Symbols

Convention	Description
 WARNING!	An alert that calls attention to important information that if not understood or followed can result in personal injury.
 CAUTION:	An alert that calls attention to important information that if not understood or followed can result in data loss, data corruption, or damage to hardware or software.
 IMPORTANT:	An alert that calls attention to essential information.
NOTE:	An alert that contains additional or supplementary information.
 TIP:	An alert that provides helpful information.

Network topology icons

Convention	Description
	Represents a generic network device, such as a router, switch, or firewall.
	Represents a routing-capable device, such as a router or Layer 3 switch.
	Represents a generic switch, such as a Layer 2 or Layer 3 switch, or a router that supports Layer 2 forwarding and other Layer 2 features.
	Represents an access controller, a unified wired-WLAN module, or the access controller engine on a unified wired-WLAN switch.
	Represents an access point.
	Represents a wireless terminator unit.
	Represents a wireless terminator.
	Represents a mesh access point.
	Represents omnidirectional signals.
	Represents directional signals.
	Represents a security product, such as a firewall, UTM, multiservice security gateway, or load balancing device.
	Represents a security card, such as a firewall, load balancing, NetStream, SSL VPN, IPS, or ACG card.

Support and other resources

Accessing Hewlett Packard Enterprise Support

- For live assistance, go to the Contact Hewlett Packard Enterprise Worldwide website:
www.hpe.com/assistance
- To access documentation and support services, go to the Hewlett Packard Enterprise Support Center website:
www.hpe.com/support/hpesc

Information to collect

- Technical support registration number (if applicable)
- Product name, model or version, and serial number
- Operating system name and version
- Firmware version
- Error messages
- Product-specific reports and logs
- Add-on products or components
- Third-party products or components

Accessing updates

- Some software products provide a mechanism for accessing software updates through the product interface. Review your product documentation to identify the recommended software update method.
- To download product updates, go to either of the following:
 - Hewlett Packard Enterprise Support Center **Get connected with updates** page:
www.hpe.com/support/e-updates
 - Software Depot website:
www.hpe.com/support/softwaredepot
- To view and update your entitlements, and to link your contracts, Care Packs, and warranties with your profile, go to the Hewlett Packard Enterprise Support Center **More Information on Access to Support Materials** page:
www.hpe.com/support/AccessToSupportMaterials



IMPORTANT:

Access to some updates might require product entitlement when accessed through the Hewlett Packard Enterprise Support Center. You must have an HP Passport set up with relevant entitlements.

Websites

Website	Link
Networking websites	
Hewlett Packard Enterprise Information Library for Networking	www.hpe.com/networking/resourcefinder
Hewlett Packard Enterprise Networking website	www.hpe.com/info/networking
Hewlett Packard Enterprise My Networking website	www.hpe.com/networking/support
Hewlett Packard Enterprise My Networking Portal	www.hpe.com/networking/mynetworking
Hewlett Packard Enterprise Networking Warranty	www.hpe.com/networking/warranty
General websites	
Hewlett Packard Enterprise Information Library	www.hpe.com/info/enterprise/docs
Hewlett Packard Enterprise Support Center	www.hpe.com/support/hpesc
Hewlett Packard Enterprise Support Services Central	ssc.hpe.com/portal/site/ssc/
Contact Hewlett Packard Enterprise Worldwide	www.hpe.com/assistance
Subscription Service/Support Alerts	www.hpe.com/support/e-updates
Software Depot	www.hpe.com/support/softwaredepot
Customer Self Repair (not applicable to all devices)	www.hpe.com/support/selfrepair
Insight Remote Support (not applicable to all devices)	www.hpe.com/info/insightremotesupport/docs

Customer self repair

Hewlett Packard Enterprise customer self repair (CSR) programs allow you to repair your product. If a CSR part needs to be replaced, it will be shipped directly to you so that you can install it at your convenience. Some parts do not qualify for CSR. Your Hewlett Packard Enterprise authorized service provider will determine whether a repair can be accomplished by CSR.

For more information about CSR, contact your local service provider or go to the CSR website:

www.hpe.com/support/selfrepair

Remote support

Remote support is available with supported devices as part of your warranty, Care Pack Service, or contractual support agreement. It provides intelligent event diagnosis, and automatic, secure submission of hardware event notifications to Hewlett Packard Enterprise, which will initiate a fast and accurate resolution based on your product's service level. Hewlett Packard Enterprise strongly recommends that you register your device for remote support.

For more information and device support details, go to the following website:

www.hpe.com/info/insightremotesupport/docs

Documentation feedback

Hewlett Packard Enterprise is committed to providing documentation that meets your needs. To help us improve the documentation, send any errors, suggestions, or comments to Documentation Feedback (docsfeedback@hpe.com). When submitting your feedback, include the document title,

part number, edition, and publication date located on the front cover of the document. For online help content, include the product name, product version, help edition, and publication date located on the legal notices page.

Index

[A](#) [B](#) [C](#) [D](#) [I](#) [L](#) [M](#) [N](#) [P](#) [Q](#) [R](#) [S](#) [V](#) [W](#)

A

active region-configuration, [93](#)

B

bandwidth, [49](#)

bandwidth, [14](#)

C

check region-configuration, [94](#)

Customer self repair, [196](#)

D

default, [49](#)

default, [15](#)

description, [15](#)

description, [50](#)

display interface, [16](#)

display interface vlan-interface, [51](#)

display lacp system-id, [20](#)

display link-aggregation load-sharing mode, [21](#)

display link-aggregation member-port, [23](#)

display link-aggregation summary, [25](#)

display link-aggregation verbose, [26](#)

display lldp local-information, [148](#)

display lldp neighbor-information, [152](#)

display lldp statistics, [158](#)

display lldp status, [160](#)

display lldp tlv-config, [162](#)

display loopback-detection, [87](#)

display mac-address, [1](#)

display mac-address aging-time, [2](#)

display mac-address mac-learning, [3](#)

display mac-address mac-move, [4](#)

display mac-forwarding cache ip, [188](#)

display mac-forwarding cache ip fragment, [190](#)

display mac-forwarding cache ipv6, [191](#)

display mac-forwarding statistics, [186](#)

display port, [64](#)

display port-isolate group, [47](#)

display qinq, [84](#)

display stp, [95](#)

display stp abnormal-port, [102](#)

display stp bpdu-statistics, [103](#)

display stp down-port, [105](#)

display stp history, [106](#)

display stp region-configuration, [110](#)

display stp root, [111](#)

display stp tc, [111](#)

display supervlan, [73](#)

display vlan, [54](#)

display vlan brief, [55](#)

display vlan-group, [70](#)

display voice-vlan mac-address, [77](#)

display voice-vlan state, [78](#)

Documentation feedback, [196](#)

I

instance, [114](#)

interface bridge-aggregation, [28](#)

interface route-aggregation, [29](#)

interface vlan-interface, [56](#)

L

lacp edge-port, [30](#)

lacp mode, [31](#)

lacp period short, [31](#)

lacp system-priority, [32](#)

link-aggregation global load-sharing mode, [32](#)

link-aggregation ignore vlan, [34](#)

link-aggregation lacp traffic-redirect-notification enable, [34](#)

link-aggregation load-sharing mode, [35](#)

link-aggregation load-sharing mode local-first, [36](#)

link-aggregation mode, [37](#)

link-aggregation port-priority, [37](#)

link-aggregation selected-port maximum, [38](#)

link-aggregation selected-port minimum, [39](#)

lldp admin-status, [165](#)

lldp check-change-interval, [166](#)

lldp enable, [168](#)

lldp encapsulation snap, [168](#)

lldp fast-count, [169](#)

lldp global enable, [170](#)

lldp hold-multiplier, [170](#)

lldp ignore-pvid-inconsistency, [171](#)

lldp management-address, [172](#)

lldp management-address-format string, [173](#)

lldp max-credit, [174](#)

lldp mode, [174](#)

lldp notification med-topology-change enable, [175](#)

lldp notification remote-change enable, [176](#)

- lldp source-mac vlan,177
- lldp timer fast-interval,177
- lldp timer notification-interval,178
- lldp timer reinit-delay,178
- lldp timer tx-interval,179
- lldp tlv-enable,179
- loopback-detection action,88
- loopback-detection enable,89
- loopback-detection global action,90
- loopback-detection global enable,90
- loopback-detection interval-time,91

M

- mac-address (interface view),5
- mac-address (system view),6
- mac-address mac-learning enable,8
- mac-address notification mac-move,9
- mac-address notification mac-move suppression (interface view),10
- mac-address notification mac-move suppression (system view),11
- mac-address timer,11
- mtu,57
- mtu,40

N

- name,58

P

- port,65
- port access vlan,65
- port hybrid pvid,66
- port hybrid vlan,67
- port link-aggregation group,40
- port link-type,68
- port trunk permit vlan,68
- port trunk pvid,69
- port-isolate enable,47

Q

- qinq enable,85
- qinq ethernet-type,85

R

- region-name,115
- Remote support,196
- reset counters interface,41
- reset counters interface vlan-interface,58
- reset lacp statistics,42
- reset mac-forwarding statistics,188
- reset stp,116
- revision-level,116

S

- service,59
- service,42
- service standby,44
- service standby,60
- shutdown,45
- shutdown,62
- snmp-agent trap enable mac-address,12
- snmp-agent trap enable stp,117
- stp bpdu-protection,118
- stp bridge-diameter,118
- stp compliance,119
- stp config-digest-snooping,120
- stp cost,121
- stp edged-port,122
- stp enable,123
- stp global config-digest-snooping,124
- stp global enable,125
- stp global mcheck,125
- stp ignore-pvid-inconsistency,126
- stp loop-protection,127
- stp max-hops,127
- stp mcheck,128
- stp mode,129
- stp no-agreement-check,130
- stp pathcost-standard,130
- stp point-to-point,131
- stp port priority,132
- stp port-log,133
- stp priority,134
- stp pvst-bpdu-protection,135
- stp region-configuration,135
- stp role-restriction,136
- stp root primary,137
- stp root secondary,138
- stp root-protection,138
- stp tc-protection,139
- stp tc-protection threshold,140
- stp tc-restriction,140
- stp tc-snooping,141
- stp timer forward-delay,142
- stp timer hello,143
- stp timer max-age,143
- stp timer-factor,144
- stp transmit-limit,145
- stp vlan enable,146
- subvlan,75
- supervlan,76

V

vlan,63
vlan-group,71
vlan-list,72
vlan-mapping modulo,147
voice-vlan aging,79
voice-vlan enable,79
voice-vlan mac-address,80

voice-vlan mode auto,81
voice-vlan security enable,82
voice-vlan track lldp,82

W

Websites,196