

H3C S5130S-SI[LI]&S5120V2-SI[LI]&S5110V2-SI& S5000V3-EI&S5000E-X&S3100V3-SI 系列以太网交换机

二层技术-以太网交换命令参考

新华三技术有限公司
<http://www.h3c.com>

资料版本：6W103-20190822
产品版本：Release 612x 系列

Copyright © 2019 新华三技术有限公司及其许可者 版权所有，保留一切权利。

未经本公司书面许可，任何单位和个人不得擅自摘抄、复制本书内容的部分或全部，并不得以任何形式传播。

除新华三技术有限公司的商标外，本手册中出现的其它公司的商标、产品标识及商品名称，由各自权利人拥有。

前言

本命令参考主要介绍以太网交换相关的配置命令。通过这些命令您可以实现流量控制、流量的负载分担、同一 VLAN 内用户隔离、二层环路消除、VLAN 划分、私网报文穿越公网、修改报文的 VLAN Tag 等功能。

前言部分包含如下内容：

- [读者对象](#)
- [本书约定](#)
- [资料意见反馈](#)

读者对象

本手册主要适用于如下工程师：

- 网络规划人员
- 现场技术支持与维护人员
- 负责网络配置和维护的网络管理员

本书约定

1. 命令行格式约定

格 式	意 义
粗体	命令行关键字（命令中保持不变、必须照输的部分）采用 加粗 字体表示。
<i>斜体</i>	命令行参数（命令中必须由实际值进行替代的部分）采用 <i>斜体</i> 表示。
[]	表示用“[]”括起来的部分在命令配置时是可选的。
{ x y ... }	表示从多个选项中仅选取一个。
[x y ...]	表示从多个选项选取一个或者不选。
{ x y ... } *	表示从多个选项中至少选取一个。
[x y ...] *	表示从多个选项选取一个、多个或者不选。
&<1-n>	表示符号&前面的参数可以重复输入1~n次。
#	由“#”号开始的行表示为注释行。






2. 图形界面格式约定

格 式	意 义
< >	带尖括号“< >”表示按钮名，如“单击<确定>按钮”。
[]	带方括号“[]”表示窗口名、菜单名和数据表，如“弹出[新建用户]窗口”。
/	多级菜单用“/”隔开。如[文件/新建/文件夹]多级菜单表示[文件]菜单下的[新建]子菜单下

格 式	意 义
	的[文件夹]菜单项。

3. 各类标志

本书还采用各种醒目标志来表示在操作过程中应该特别注意的地方，这些标志的意义如下：

 警告	该标志后的注释需给予格外关注，不当的操作可能会对人身造成伤害。
 注意	提醒操作中应注意的事项，不当的操作可能会导致数据丢失或者设备损坏。
 提示	为确保设备配置成功或者正常工作而需要特别关注的操作或信息。
 说明	对操作内容的描述进行必要的补充和说明。
 窍门	配置、操作、或使用设备的技巧、小窍门。

4. 图标约定

本书使用的图标及其含义如下：

	该图标及其相关描述文字代表一般网络设备，如路由器、交换机、防火墙等。
	该图标及其相关描述文字代表一般意义下的路由器，以及其他运行了路由协议的设备。
	该图标及其相关描述文字代表二、三层以太网交换机，以及运行了二层协议的设备。
	该图标及其相关描述文字代表无线控制器、无线控制器业务板和有线无线一体化交换机的无线控制引擎设备。
	该图标及其相关描述文字代表无线接入点设备。
	该图标及其相关描述文字代表无线终结单元。
	该图标及其相关描述文字代表无线终结者。
	该图标及其相关描述文字代表无线Mesh设备。
	该图标代表发散的无线射频信号。
	该图标代表点到点的无线射频信号。
	该图标及其相关描述文字代表防火墙、UTM、多业务安全网关、负载均衡等安全设备。



该图标及其相关描述文字代表防火墙插卡、负载均衡插卡、NetStream插卡、SSL VPN插卡、IPS插卡、ACG插卡等安全插卡。

5. 示例约定

由于设备型号不同、配置不同、版本升级等原因，可能造成本手册中的内容与用户使用的设备显示信息不一致。实际使用中请以设备显示的内容为准。

本手册中出现的端口编号仅作参考，并不代表设备上实际具有此编号的端口，实际使用中请以设备上存在的端口编号为准。

资料意见反馈

如果您在使用过程中发现产品资料的任何问题，可以通过以下方式反馈：

E-mail: info@h3c.com

感谢您的反馈，让我们做得更好！

目 录

1 以太网接口	1-1
1.1 以太网接口通用配置命令	1-1
1.1.1 bandwidth	1-1
1.1.2 broadcast-suppression	1-1
1.1.3 combo enable	1-3
1.1.4 dampening	1-3
1.1.5 default	1-5
1.1.6 description	1-5
1.1.7 display counters	1-6
1.1.8 display counters rate	1-7
1.1.9 display ethernet statistics	1-8
1.1.10 display interface	1-11
1.1.11 display link-flap protection	1-19
1.1.12 duplex	1-20
1.1.13 eee enable	1-21
1.1.14 flow-control	1-22
1.1.15 flow-control receive enable	1-22
1.1.16 flow-interval	1-23
1.1.17 interface	1-24
1.1.18 jumboframe enable	1-24
1.1.19 link-delay	1-25
1.1.20 link-flap protect enable	1-26
1.1.21 loopback	1-27
1.1.22 multicast-suppression	1-28
1.1.23 port auto-power-down	1-29
1.1.24 port link-flap protect enable	1-29
1.1.25 reset counters interface	1-30
1.1.26 reset ethernet statistics	1-31
1.1.27 shutdown	1-32
1.1.28 speed	1-32
1.1.29 speed auto downgrade	1-33
1.1.30 unicast-suppression	1-34
1.2 二层以太网接口的配置命令	1-35

1.2.1 display storm-constrain	1-35
1.2.2 mdix-mode	1-37
1.2.3 port bridge enable.....	1-37
1.2.4 speed auto	1-38
1.2.5 storm-constrain	1-39
1.2.6 storm-constrain control	1-40
1.2.7 storm-constrain enable log.....	1-41
1.2.8 storm-constrain enable trap	1-42
1.2.9 storm-constrain interval.....	1-42
1.2.10 virtual-cable-test	1-43

1 以太网接口

1.1 以太网接口通用配置命令

1.1.1 bandwidth

bandwidth 命令用来配置接口的期望带宽。

undo bandwidth 命令用来恢复缺省情况。

【命令】

```
bandwidth bandwidth-value  
undo bandwidth
```

【缺省情况】

接口的期望带宽 = 接口的波特率 ÷ 1000 (kbps)。

【视图】

以太网接口视图

【缺省用户角色】

network-admin

【参数】

bandwidth-value: 表示接口的期望带宽，取值范围为 1~4000000000，单位为 kbps。

【使用指导】

期望带宽供业务模块使用，不会对接口实际带宽造成影响。

【举例】

```
# 配置接口 GigabitEthernet1/0/1 的期望带宽为 1000kbps。  
<Sysname> system-view  
[Sysname] interface gigabitethernet 1/0/1  
[Sysname-GigabitEthernet1/0/1] bandwidth 1000
```

【相关命令】

- **speed**

1.1.2 broadcast-suppression

broadcast-suppression 命令用来开启端口广播风暴抑制功能，并设置广播风暴抑制阈值。

undo broadcast-suppression 命令用来关闭端口广播风暴抑制功能。

【命令】

```
broadcast-suppression { ratio | pps max-pps | kbps max-kbps }  
undo broadcast-suppression
```


【缺省情况】

所有接口不对广播流量进行抑制。

【视图】

以太网接口视图

【缺省用户角色】

network-admin

【参数】

ratio: 指定以太网接口允许通过的最大广播流量占该接口带宽的百分比，取值范围为 0~100。数值越小，允许通过的广播流量也越小。

pps max-pps: 指定以太网接口每秒允许转发的最大广播包数，单位为 pps (packets per second, 每秒转发的报文数)，取值范围为 0~1.4881×接口带宽。

kbps max-kbps: 指定以太网接口每秒允许转发的最大广播流量，单位为 kbps (kilobits per second, 每秒转发的千比特数)，取值范围为 0~接口带宽。

【使用指导】

本命令设置的是接口允许通过的最大广播报文流量。当接口上的广播流量超过用户设置的值后，系统将丢弃超出广播流量限制的报文，从而使接口广播流量所占的比例控制在限定的范围内，以便保证业务的正常运行。

执行 **broadcast-suppression** 或 **storm-constrain** 命令都能开启端口的广播风暴抑制功能，**storm-constrain** 命令通过软件对广播报文进行抑制，对设备性能有一定影响，**broadcast-suppression** 通过芯片物理上对广播报文进行抑制，相对 **storm-constrain** 来说，对设备性能影响较小。请不要同时配置 **broadcast-suppression** 和 **storm-constrain** 命令，以免配置冲突，导致抑制效果不确定。

当风暴抑制阈值配置为 **kbps** 时，若配置值小于 64，则实际生效的数值为 64；若配置值大于 64 但不是 64 的整数倍，则实际生效的数值为大于且最接近于配置值的 64 的整数倍。请注意查看设备的提示信息。

【举例】

在以太网接口 GigabitEthernet1/0/1 上，每秒最多允许 10000kbps 广播报文通过，对超出该范围的广播报文进行抑制。

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] broadcast-suppression kbps 10000
The actual value is 10048 on port GigabitEthernet1/0/1 currently.
```

以上信息表示：用户配置的值为 10000kbps，因为芯片支持的步长为 64，所以实际生效的值为 10048kbps（64 的 157 倍）。

【相关命令】

- **multicast-suppression**
- **unicast-suppression**

1.1.3 combo enable

combo enable 命令用来激活 Combo 接口中的电口或者光口。

【命令】

```
combo enable { auto | copper | fiber }
```

【缺省情况】

对于 Release 6126P20 及之前的版本，电口处于激活状态；

对于 Release 6127 及以上版本，接口根据所插入介质自动识别并激活对应的物理接口。

【视图】

以太网接口视图

【缺省用户角色】

network-admin

【参数】

auto: 表示该 Combo 接口根据所插入介质自动识别并激活对应的物理接口。

copper: 表示该 Combo 接口的电口被激活，请使用双绞线连接。

fiber: 表示该 Combo 接口的光口被激活，请使用光纤连接。

【使用指导】

Combo 接口是一个逻辑接口，一个 Combo 接口物理上对应设备面板上一个电口和一个光口。电口与其对应的光口是光电复用关系，两者不能同时工作（当激活其中的一个接口时，另一个接口就自动处于关闭状态），用户可根据组网需求选择使用电口或光口。

如果指定 **auto** 参数，并且 Combo 接口上同时连接了电缆或光模块时，请通过 **display interface** 命令查看接口信息，如果显示信息中包含“Media type is twisted pair”，则表示电口处于激活状态，否则，则表示光口处于激活状态。

请根据设备面板上的标识了解设备上有哪些 Combo 接口以及每个 Combo 接口的编号。

仅 Release 6127 及以上版本，支持配置 **auto** 参数。

【举例】

指定 GigabitEthernet1/0/1 端口的电口被激活。

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

指定 GigabitEthernet1/0/1 端口的光口被激活。

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

1.1.4 dampening

dampening 命令用来开启接口的 dampening 功能。

undo dampening 命令用来恢复缺省情况。

【命令】

```
dampening [ half-life reuse suppress max-suppress-time ]  
undo dampening
```

【缺省情况】

接口的 dampening 功能处于关闭状态。

【视图】

以太网接口视图

【缺省用户角色】

network-admin

【参数】

half-life: 半衰期，取值范围为 1~120，单位为秒，缺省值为 54。

reuse: 启用值，取值范围为 200~20000，缺省值为 750，必须要小于 *suppress* 的值。

suppress: 抑制门限，取值范围为 200~20000，缺省值为 2000。

max-suppress-time: 最大抑制时间，取值范围为 1~255，单位为秒，缺省值为半衰期的 3 倍，即 162。

【使用指导】

配置本命令时，各参数之间应满足以下关系，请根据该关系来选择参数的取值：

- 最大惩罚值 = $2^{(\text{最大抑制时间}/\text{半衰期})} \times \text{启用值}$ ，其中最大惩罚值不可配。
- 抑制值的配置值 ≤ 最大惩罚值 ≤ 抑制值可配的最大值

以太网接口上不能同时配置本命令和 **link-delay** 命令和 **port link-flap protect enable** 命令。

本命令对使用 **shutdown** 命令手动关闭的接口无效。手工 **shutdown** 接口时，dampening 的惩罚值恢复为初始值 0。

对于使能了 RRPP、MSTP 或 Smart Link 的接口不建议使用该命令。S5000E-X、S5110V2-SI 和 S5000V3-EI 系列交换机不支持 RRPP 和 Smart Link。

接口在抑制期发生 up 事件，通过 **display interface** 命令等方式查看时，该接口的状态仍然为 down。

【举例】

按照缺省值开启接口 GigabitEthernet1/0/1 的 dampening 功能。

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

开启接口 GigabitEthernet1/0/1 的 dampening 功能，配置半衰期为 2 秒，启用值为 800，抑制门限为 3000，最大抑制时间为 5 秒。

```
<Sysname> system-view  
[Sysname] interface gigabitethernet 1/0/1  
[Sysname-GigabitEthernet1/0/1] dampening 2 800 3000 5
```

【相关命令】

- `display interface`
- `link-delay`
- `port link-flap protect enable`

1.1.5 default

default 命令用来恢复当前接口的缺省配置。

【命令】

default

【视图】

以太网接口视图

【缺省用户角色】

network-admin

【使用指导】



注意

接口下的某些配置恢复到缺省情况后，会对设备上当前运行的业务产生影响。建议您在执行该命令前，完全了解其对网络产生的影响。

您可以在执行 **default** 命令后通过 **display this** 命令确认执行效果。对于未能成功恢复缺省的配置，建议您查阅相关功能的命令手册，手工执行恢复该配置缺省情况的命令。如果操作仍然不能成功，您可以通过设备的提示信息定位原因。

【举例】

将以太网接口 GigabitEthernet1/0/1 恢复为缺省配置。

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

1.1.6 description

description 命令用来设置当前接口的描述信息。

undo description 命令用来恢复缺省情况。

【命令】

description *text*

undo description

【缺省情况】

接口的描述信息为“*接口名* Interface”，例如：GigabitEthernet1/0/1 Interface。

【视图】

以太网接口视图

【缺省用户角色】

network-admin

【参数】

text: 接口的描述信息，为 1~255 个字符的字符串，区分大小写。

【举例】

设置以太网接口 GigabitEthernet1/0/1 的描述信息为“lan-interface”。

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] description lan-interface
```

1.1.7 display counters

display counters 命令用来显示接口的流量统计信息。

【命令】

```
display counters { inbound | outbound } interface [ interface-type
[ interface-number ] ]
```

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator

【参数】

inbound: 显示输入报文的流量统计信息。

outbound: 显示输出报文的流量统计信息。

interface-type: 指定接口类型。

interface-number: 指定接口编号。

【使用指导】

本命令显示的是统计周期内报文的数量，统计周期可以通过 **flow-interval** 命令进行设置。

可通过命令 **reset counters interface** 清除以太网接口的统计信息。

如果不指定接口类型，则显示所有可统计的接口的流量统计信息。

如果指定接口类型而不指定接口编号，则显示该类型下所有接口的流量统计信息。

如果同时指定接口类型和接口编号，则显示指定接口的报文流量统计信息。

【举例】

显示接口的报文输入流量统计信息。

```
<Sysname> display counters inbound interface
Interface          Total (pkts)    Broadcast (pkts)  Multicast (pkts)  Err (pkts)
```

GE1/0/1	100	100	0	0
GE1/0/2	Overflow	Overflow	Overflow	Overflow

Overflow: More than 14 digits (7 digits for column "Err").

--: Not supported.

表1-1 display counters 命令显示信息描述表

字段	描述
Interface	接口名称缩写
Total (pkts)	接口接收或发送报文的总数（单位为包）
Broadcast (pkts)	接口接收或发送广播报文的总数（单位为包）
Multicast (pkts)	接口接收或发送组播报文的总数（单位为包）
Err (pkts)	接口接收或发送错误报文的总数（单位为包）
Overflow: More than 14 digits (7 digits for column "Err").	<p>当某个统计信息的值为Overflow时，表示该项数据的长度超过了显示范围：</p> <ul style="list-style-type: none"> 对于 Err 项，Overflow 表示数据的长度超过了 7 位十进制数 对于其它项，Overflow 表示数据的长度超过了 14 位十进制数
--: Not supported.	当某个统计信息的值为“--”时，表示设备不支持该项数据的统计

【相关命令】

- **flow-interval**
- **reset counters interface**

1.1.8 display counters rate

display counters rate 命令用来显示最近一个统计周期内处于 up 状态的接口的报文速率统计信息。

【命令】

```
display counters rate { inbound | outbound } interface [ interface-type
[ interface-number ] ]
```

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator

【参数】

inbound: 显示报文接收速率统计信息。

outbound: 显示报文发送速率统计信息。

interface-type: 指定接口类型。

interface-number: 指定接口编号。

【使用指导】

如果不指定 *interface-type* 和 *interface-number*，则显示所有可统计的接口类型中最近一个统计周期内处于 **up** 状态的接口的报文速率统计信息。

如果指定 *interface-type* 而不指定 *interface-number*，则显示该类型下最近一个统计周期内处于 **up** 状态接口的报文速率统计信息。

如果同时指定 *interface-type* 和 *interface-number*，则显示指定接口在最近一个统计周期内报文速率统计信息。如果该接口在最近一个统计周期内一直处于 **down** 状态，则提示接口不支持该操作。

统计周期可以通过 **flow-interval** 命令来配置。

【举例】

显示接口的报文接收速率统计信息。

```
<Sysname> display counters rate inbound interface
Usage: Bandwidth utilization in percentage
Interface          Usage (%)    Total (pps)    Broadcast (pps)    Multicast (pps)
GE1/0/1            0           0              --                --

Overflow: More than 14 digits.
--: Not supported.
```

表1-2 display counters rate 命令显示信息描述表

字段	描述
Interface	接口名称缩写
Usage (%)	在最近一个统计周期内，接口的带宽利用率（单位为百分比）
Total (pps)	在最近一个统计周期内，接口接收或发送所有类型报文的平均速率（单位为包/秒）
Broadcast (pps)	在最近一个统计周期内，接口接收或发送广播报文的平均速率（单位为包/秒）
Multicast (pps)	在最近一个统计周期内，接口接收或发送组播报文的平均速率（单位为包/秒）
Overflow: More than 14 digits.	当某个统计信息的值为 Overflow 时，表示该项数据的长度超过了14位十进制数
--: Not supported.	当某个统计信息的值为“--”时，则表示设备不支持该项数据的统计

【相关命令】

- **flow-interval**
- **reset counters interface**

1.1.9 display ethernet statistics

display ethernet statistics 命令用来显示以太网软件模块收发报文的统计信息。

【命令】

```
display ethernet statistics slot slot-number
```

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator

【参数】

slot *slot-number*: 显示指定成员设备的统计信息，*slot-number* 表示设备在 IRF 中的成员编号。

【举例】

显示指定 slot 上的以太网软件模块收发报文的统计信息。

```
<Sysname> display ethernet statistics slot 1
ETH receive packet statistics:
    Totalnum      : 10447          ETHIINum       : 4459
    SNAPNum       : 0              RAWNum        : 0
    LLCNum        : 0              UnknownNum     : 0
    ForwardNum    : 4459          ARP            : 0
    MPLS          : 0              ISIS           : 0
    ISIS2         : 0              IP             : 0
    IPV6          : 0

ETH receive error statistics:
    NullPoint     : 0              ErrIfindex    : 0
    ErrIfcb       : 0              IfShut       : 0
    ErrAnalyse    : 5988          ErrSrcMAC     : 5988
    ErrHdrLen     : 0

ETH send packet statistics:
    L3OutNum      : 211            VLANOutNum    : 0
    FastOutNum    : 155            L2OutNum     : 0

ETH send error statistics:
    MbufRelayNum  : 0              NullMbuf      : 0
    ErrAdjFwd     : 0              ErrPrepend    : 0
    ErrHdrLen     : 0              ErrPad        : 0
    ErrQoSTrs     : 0              ErrVLANTrs    : 0
    ErrEncap      : 0              ErrTagVLAN    : 0
    IfShut        : 0              IfErr         : 0
```


表1-3 display ethernet statistics 命令显示信息描述表

字段	描述
ETH receive packet statistics	<p>以太网软件模块接收到的以太网报文的统计信息：</p> <ul style="list-style-type: none"> • Totalnum: 接收报文的总个数 • ETHIINum: 接收的 ETHII 封装格式报文个数 • SNAPNum: 接收的 SNAP 封装格式报文个数 • RAWNum: 接收的 RAW 封装格式报文个数 • ISISNum: 接收的 ISIS 封装格式报文个数（暂不支持） • LLCNum: 接收的 LLC 封装格式报文个数 • UnknowNum: 接收的未知封装格式报文个数 • ForwardNum: 二层转发或上送 CPU 的报文个数 • ARP: 接收的 ARP 报文个数 • MPLS: 接收的 MPLS 报文个数（暂不支持） • ISIS: 接收的 ISIS 报文个数（暂不支持） • ISIS2: 接收的 ISIS2 报文个数（暂不支持） • IP: 接收的 IP 报文个数 • IPv6: 接收的 IPv6 报文个数
ETH receive error statistics	<p>以太网软件模块接收错误的以太网报文的统计信息（可能是包本身包含错误或者是接收动作出错了）：</p> <ul style="list-style-type: none"> • NullPoint: 接收报文时指针为空的报文的个数 • ErrIfindex: 接收报文时接口索引错误的报文个数 • ErrIfcb: 接收报文时接口控制块错误的报文个数 • IfShut: 接收报文时接口 shutdown 的报文个数 • ErrAnalyse: 接收报文时报文解析错误的报文个数 • ErrSrcMAC: 接收的包含源 MAC 地址错误的报文个数 • ErrHdrLen: 接收的包含报文头长度错误的报文个数
ETH send packet statistics	<p>以太网软件模块发送的以太网报文的统计信息：</p> <ul style="list-style-type: none"> • L3OutNum: 通过三层以太网接口发送的报文总个数 • VLANOutNum: 通过 VLAN 接口发送的报文总个数 • FastOutNum: 快速发送的报文总个数 • L2OutNum: 通过二层以太网接口发送的报文总个数 • MbufRelayNum: 透传发送的报文总个数

字段	描述
ETH send error statistics	<p>以太网软件模块发送的错误以太网报文的统计信息：</p> <ul style="list-style-type: none"> • NullMbuf: 发送报文时空指针错误的报文个数 • ErrAdjFwd: 发送报文时邻接表错误的报文个数 • ErrPrepend: 发送报文时扩展错误的报文个数 • ErrHdrLen: 发送的包含报文头长度错误的报文个数 • ErrPad: 发送报文时填充错误的报文个数 • ErrQoSTrs: 发送报文时 QoS 发送失败的报文个数 • ErrVLANTrs: 发送报文时 VLAN 发送失败的报文个数 • ErrEncap: 发送报文时封装链路头失败的报文个数 • ErrTagVLAN: 发送报文时封装 VLAN TAG 失败的报文个数 • IfShut: 发送报文时端口 shutdown 的报文个数 • IfErr: 发送报文时出接口错误的报文个数

【相关命令】

- `reset ethernet statistics`

1.1.10 display interface

display interface 命令用来显示接口的运行状态和相关信息。

【命令】

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

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator

【参数】

interface-type: 指定接口类型。

interface-number: 指定接口编号。

brief: 显示接口的概要信息。不指定该参数时，将显示接口的详细信息。

description: 用来显示用户配置的接口的全部描述信息。如果某接口的描述信息超过 27 个字符，不指定该参数时，只显示描述信息中的前 27 个字符，超出部分不显示。

down: 显示当前物理状态为 down 的接口的信息以及 down 的原因。不指定该参数时，将不会根据接口物理状态来过滤显示信息。

【使用指导】

如果不指定接口类型和接口编号，则显示所有接口的信息。

如果仅指定接口类型，则显示所有该类型接口的信息。

【举例】

查看二层以太网接口 GigabitEthernet1/0/1 的运行状态和相关信息。

```
<Sysname> display interface gigabitethernet 1/0/1
GigabitEthernet1/0/1
Current state: DOWN
Line protocol state: DOWN
IP packet frame type: Ethernet II, hardware address: 000c-2963-b767
Description: GigabitEthernet1/0/1 Interface
Bandwidth: 100000 kbps
Loopback is not set
Media type is twisted pair, port hardware type is 1000_BASE_T_AN_SFP
Unknown-speed mode, unknown-duplex mode
Link speed type is autonegotiation, link duplex type is autonegotiation
Flow-control is not enabled
Maximum frame length: 9216
Allow jumbo frame to pass
Broadcast max-ratio: 100%
Multicast max-ratio: 100%
Unicast max-ratio: 100%
PVID: 1
MDI type: Automdix
Port link-type: Access
    Tagged VLANs:    None
    UnTagged VLANs: 1
Port priority: 2
Last link flapping: 6 hours 39 minutes 25 seconds
Last clearing of counters:  14:34:09 Tue 11/01/2011
    Peak input rate: 0 bytes/sec, at 2013-07-17 22:06:19
    Peak output rate: 0 bytes/sec, at 2013-07-17 22:06:19
    Last 300 second input:  0 packets/sec 0 bytes/sec -%
    Last 300 second output: 0 packets/sec 0 bytes/sec -%
    Input (total):  0 packets, 0 bytes
        0 unicasts, 0 broadcasts, 0 multicasts, 0 pauses
    Input (normal): 0 packets, 0 bytes
        0 unicasts, 0 broadcasts, 0 multicasts, 0 pauses
    Input:  0 input errors, 0 runts, 0 giants, 0 throttles
        0 CRC, 0 frame, 0 overruns, 0 aborts
        0 ignored, 0 parity errors
    Output (total): 0 packets, 0 bytes
        0 unicasts, 0 broadcasts, 0 multicasts, 0 pauses
    Output (normal): 0 packets, 0 bytes
        0 unicasts, 0 broadcasts, 0 multicasts, 0 pauses
    Output: 0 output errors, 0 underruns, 0 buffer failures
        0 aborts, 0 deferred, 0 collisions, 0 late collisions
        0 lost carrier, 0 no carrier
```

表1-4 display interface 命令显示信息描述表

字段	描述
GigabitEthernet1/0/1	接口GigabitEthernet1/0/1的相关信息
Current state	<p>接口的物理状态，状态可能为：</p> <ul style="list-style-type: none"> • Administratively DOWN：表示该接口已经通过 shutdown 命令被关闭，即管理状态为关闭 • DOWN：表示该接口的管理状态为开启，但物理状态为关闭（可能因为没有物理连线或者线路故障） • DOWN (Link-Aggregation interface down)：表示该接口所属的聚合接口已经通过 shutdown 命令被关闭 • mac-address moving down：由于 MAC 地址迁移抑制导致接口被关闭 • MAD ShutDown：当 IRF 分裂后，处于 Recovery 状态的 IRF 会将除了保留接口外的所有接口状态设置为 MAD ShutDown • OFDP DOWN：表示接口开启了 OpenFlow 的关闭接口功能 • Storm-Constrain：表示端口上因为未知单播、组播或广播报文中某类报文的流量大于其上限阈值而被关闭 • STP DOWN：表示接口由于触发了 STP BPDU 保护而自动关闭 • UP：该端口的管理状态和物理状态均为开启
Line protocol state	<p>接口的链路层协议状态。其值由链路层经过参数协商决定，取值为：</p> <ul style="list-style-type: none"> • UP：表示数据链路层协议状态为开启 • UP(spoofing)：表示该接口的数据链路层协议状态为开启，但实际可能没有对应的链路，或者所对应的链路不是永久存在而是按需建立。通常 NULL、LoopBack 等接口会具有该属性 • DOWN：表示数据链路层协议状态为关闭 • DOWN(<i>protocols</i>)：表示接口的数据链路层被一个或者多个协议模块关闭。<i>protocols</i> 为 DLDP、OAM、LAGG、BFD 的任意组合： <ul style="list-style-type: none"> ◦ DLDP：表示由于 DLDP 模块检测到单通而关闭接口的数据链路层 ◦ OAM：表示由于以太网 OAM 模块检测到远端链路故障而关闭接口的数据链路层 ◦ LAGG：表示聚合接口中没有选中的成员端口而关闭接口的数据链路层 ◦ BFD：表示由于 BFD 模块检测到链路故障而关闭接口的数据链路层
Description	接口的描述信息
Bandwidth	接口的期望带宽
Maximum transmission unit	接口的MTU
IP packet frame type	IPv4报文发送帧格式
hardware address	接口的MAC地址
Media type is	接口的介质类型
Port hardware type is	接口的硬件类型
Port priority	接口优先级
Loopback is set internal	以太网接口正在进行对内环回测试，该显示信息与用户的配置有关

字段	描述
Loopback is set external	对以太网接口进行对外环回测试，该显示信息与用户的配置有关
Loopback is not set	接口上未配置环回测试，该显示信息与用户的配置有关
10Mbps-speed mode	接口速率为10Mbps，该显示信息与用户的配置以及链路参数的协商结果有关
100Mbps-speed mode	接口速率为100Mbps，该显示信息与用户的配置以及链路参数的协商结果有关
1000Mbps-speed mode	接口速率为1000Mbps，该显示信息与用户的配置以及链路参数的协商结果有关
10Gbps-speed mode	接口速率为10Gbps，该显示信息与用户的配置以及链路参数的协商结果有关
Unknown-speed mode	速率未知，可能因为速率协商失败或者接口物理未连通
half-duplex mode	接口工作在半双工模式，该显示信息与用户的配置以及链路参数的协商结果有关
full-duplex mode	接口工作在全双工模式，该显示信息与用户的配置以及链路参数的协商结果有关
unknown-duplex mode	未知双工模式，可能因为双工模式协商失败或者接口物理未连通
Link speed type is autonegotiation	当用户配置了 speed auto 时显示该信息
Link speed type is force link	当用户使用 speed 命令配置了具体的速率时显示该信息，例如1000M等
link duplex type is autonegotiation	当用户配置了 duplex auto 时显示该信息
link duplex type is force link	当用户使用 duplex 命令配置了具体的双工模式时显示该信息，例如 half 或者 full
Flow-control is not enabled	未配置流量控制功能，该显示信息与用户的配置以及链路参数的协商结果有关
Maximum frame length	接口允许通过的最大以太网帧长度
Allow jumbo frame to pass	允许长帧通过
Broadcast max-	广播风暴抑制阈值，可能为ratio（百分比）、pps或者kbps，与用户的配置有关
Multicast max-	组播风暴抑制阈值，可能为ratio（百分比）、pps或者kbps，与用户的配置有关
Unicast max-	未知单播风暴抑制阈值，可能为ratio（百分比）、pps或者kbps，与用户的配置有关
PVID	接口所在的缺省VLAN ID
MDI type	网线类型，取值为automdix、mdi或mdix，与用户的配置有关
Port link-type	链路类型，取值为access、trunk或hybrid，与用户的配置有关
Tagged VLANs	通过该接口后携带Tag的VLAN
UnTagged VLANs	通过该接口后不再携带Tag的VLAN
VLAN Passing	该接口实际可以通过的VLAN（接口允许通过并且已创建的VLAN）
VLAN permitted	接口允许通过的VLAN报文
Trunk port encapsulation	Trunk接口的封装格式
Last link flapping	接口最近一次物理状态改变到现在的时长。 Never 表示接口从设备启动后一直处于down状态（没有改变过）

字段	描述
Last clearing of counters	最近一次使用 reset counters interface 命令清除接口下的统计信息的时间（如果从设备启动一直没有执行 reset counters interface 命令清除过该接口下的统计信息，则显示Never）
Last 300 second input: 0 packets/sec 0 bytes/sec 0% Last 300 second output: 0 packets/sec 0 bytes/sec 0%	端口在最近300秒接收和发送报文的平均速率，单位分别为数据包/秒和字节/秒，以及实际速率和接口带宽的百分比 如果值显示为“-”，则表示不支持该统计项
Input(total): 0 packets, 0 bytes 0 unicasts, 0 broadcasts, 0 multicasts, 0 pauses	端口接收报文的统计值，包括正常报文、异常报文和正常PAUSE帧的报文数、字节数 端口接收的单播报文、广播报文、组播报文和PAUSE帧的数量 如果值显示为“-”，则表示不支持该统计项
Input(normal): 0 packets, 0 bytes 0 unicasts, 0 broadcasts, 0 multicasts, 0 pauses	端口接收的正常报文的统计值，包括正常报文和正常PAUSE帧的报文数、字节数 端口接收的正常单播报文、广播报文、组播报文和PAUSE帧的数量 如果值显示为“-”，则表示不支持该统计项
input errors	端口接收的错误报文的统计值
runts	接收到的超小帧的数量 超小帧是指长度小于64字节、格式正确且包含有效的CRC字段的帧
giants	接收到的超大帧的数量 超大帧是指有效长度大于端口允许通过最大报文长度的帧： <ul style="list-style-type: none"> 对于禁止长帧通过的以太网端口，超大帧是指有效长度大于 1518 字节（不带 VLAN Tag）或大于 1522 字节（带 VLAN Tag 报文）的帧 对于允许长帧通过的以太网端口，超大帧是指有效长度大于指定最大长帧长度的帧
throttles	接收到的长度为非整数字节的帧的个数
CRC	接收到的CRC校验错误、长度正常的帧的数量
frame	接收到的CRC校验错误、且长度不是整数字节数的帧的数量
overruns	当端口的接收速率超过接收队列的处理能力时，导致报文被丢弃
aborts	接收到的非法报文总数，非法报文包括： <ul style="list-style-type: none"> 报文碎片：长度小于 64 字节（长度可以为整数或非整数）且 CRC 校验错误的帧 jabber 帧：有效长度大于端口允许通过的最大报文长度，且 CRC 校验错误的帧（长度可以为整数字节数或非整数字节数）。如对于禁止长帧通过的以太网端口，jabber 帧是指大于 1518（不带 VLAN Tag）或 1522（带 VLAN Tag）字节，且 CRC 校验错误的帧；对于允许长帧通过的以太网端口，jabber 帧是指有效长度大于指定最大长帧长度，且 CRC 校验错误的帧 符号错误帧：报文中至少包含 1 个错误的符号 操作码未知帧：报文是 MAC 控制帧，但不是 Pause 帧 长度错误帧：报文中 802.3 长度字段与报文实际长度（46~1500 字节）不匹配

字段	描述
ignored	由于端口接收缓冲区不足等原因而丢弃的报文数量
parity errors	接收到的奇偶校验错误的帧的数量
Output(total): 0 packets, 0 bytes 0 unicasts, 0 broadcasts, 0 multicasts, 0 pauses	端口发送报文的统计值，包括正常报文、异常报文和正常PAUSE帧的报文数、字节数 端口发送的单播报文、广播报文、组播报文和PAUSE帧的数量 如果值显示为“-”，则表示不支持该统计项
Output(normal): 0 packets, 0 bytes 0 unicasts, 0 broadcasts, 0 multicasts, 0 pauses	端口发送的正常报文的统计值，包括正常报文和正常PAUSE帧的报文数、字节数 端口发送的正常单播报文、广播报文、组播报文和PAUSE帧的数量 如果值显示为“-”，则表示不支持该统计项
output errors	各种发送错误的报文总数
underruns	当端口的发送速率超过了发送队列的处理能力，导致报文被丢弃，是一种非常罕见的硬件异常
buffer failures	由于端口发送缓冲区不足而丢弃的报文数量
aborts	发送失败的报文总数，即报文已经开始发送，但由于各种原因（如冲突）而导致发送失败
deferred	延迟报文的数量，延迟报文是指发送前检测到冲突而被延迟发送的报文
collisions	冲突帧的数量，冲突帧是指在发送过程中检测到冲突的而停止发送的报文
late collisions	延迟冲突帧的数量，延迟冲突帧是指帧的前512 bits已经被发送，由于检测到冲突，该帧被延迟发送
lost carrier	载波丢失，一般适用于串行WAN接口，发送过程中，每丢失一个载波，此计数器加一
no carrier	无载波，一般适用于串行WAN接口，当试图发送帧时，如果没有载波出现，此计数器加一
Peak input rate	接口输入流量的峰值速率大小（单位为bytes/sec）以及峰值产生的时间
Peak output rate	接口输出流量的峰值速率大小（单位为bytes/sec）以及峰值产生的时间

显示所有接口的概要信息。

```
<Sysname> display interface brief
Brief information on interfaces in route mode:
Link: ADM - administratively down; Stby - standby
Protocol: (s) - spoofing
```

Interface	Link	Protocol	Primary IP	Description
Loop0	UP	UP(s)	2.2.2.9	
NULL0	UP	UP(s)	--	
Vlan1	UP	DOWN	--	
Vlan999	UP	UP	192.168.1.42	

```
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
GE1/0/2            DOWN auto   A      A    1
GE1/0/3            UP   auto   F(a)  A    1   aaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
# 显示接口 GigabitEthernet1/0/3 的概要信息，包括用户配置的全部描述信息。
<Sysname> display interface gigabitethernet 1/0/3 brief description
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
GE1/0/3            UP   auto   F(a)  A    1   aaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
# 显示当前物理状态为 down 的接口的信息以及 down 的原因。
<Sysname> display interface brief down
Brief information on interfaces in route mode:
Link: ADM - administratively down; Stby - standby
Interface          Link Cause
Vlan2              DOWN Not connected

Brief information on interfaces in bridge mode:
Link: ADM - administratively down; Stby - standby
Interface          Link Cause
GE1/0/2            DOWN Not connected

```

表1-5 display interface brief 命令显示信息描述表

字段	描述
Brief information on interfaces in route mode:	三层模式下（route）接口的概要信息，即三层接口的概要信息
Link: ADM - administratively down; Stby - standby	<ul style="list-style-type: none"> 如果某接口的 Link 属性值为“ADM”，则表示该接口被管理员通过 shutdown 命令关闭，需要在该接口下执行 undo shutdown 命令才能恢复接口本身的物理状态 如果某接口的 Link 属性值为“Stby”，则表示该接口是一个处于 Standby 状态的备份接口
Protocol: (s) - spoofing	如果某接口的 Protocol 属性值中带有“(s)”，则表示该接口的数据链路层协议状态显示为 UP，但实际可能没有对应的链路，或者对应的链路不是永久存在而是按需建立的。通常 NULL、LoopBack 等接口会具有该属性
Interface	接口名称缩写

字段	描述
Link	<p>接口物理连接状态，取值为：</p> <ul style="list-style-type: none"> UP：表示接口物理上是连通的 DOWN：表示接口物理上不通 ADM：表示接口被管理员通过 shutdown 命令关闭，需要执行 undo shutdown 命令才能恢复接口本身的物理状态 Stby：表示该接口是一个处于 Standby 状态的备份接口
Protocol	<p>接口数据链路层协议状态，取值为：</p> <ul style="list-style-type: none"> UP：表示接口的数据链路层协议状态为开启 DOWN：表示接口的数据链路层协议状态为关闭 UP(s)：表示接口的数据链路层协议状态显示为 UP，但实际可能没有对应的链路，或者对应的链路不是永久存在而是按需建立的。通常 NULL、LoopBack 等接口会取该值
Primary IP	接口主IP地址。取值为“--”时，表示接口尚未配置IP地址
Description	接口的描述信息
Brief information of interfaces in bridge mode:	二层模式下（bridge）的接口概要信息，即二层接口的概要信息
Speed: (a) - auto	<p>如果某接口的Speed属性值为“(a)”，则表示该接口的速率是通过自动协商获取的</p> <p>如果某接口的Speed属性值为“auto”，则表示该接口的速率是通过自动协商获取的，但协商还未开始</p>
Duplex: (a)/A - auto; H - half; F - full	<p>如果某接口的Duplex属性值为“(a)”或者“A”，则表示该接口的Duplex属性是通过自动协商获取的；取值为“H”则表示为半双工；取值为“F”则表示为全双工</p> <p>当显示为“A”时表示该接口的Duplex属性是通过自动协商获取的，但协商还未开始</p>
Type: A - access; T - trunk; H - hybrid	<p>接口的链路类型：</p> <ul style="list-style-type: none"> A：表示 Access 链路类型 H：表示 Hybrid 链路类型 T：表示 Trunk 链路类型
Speed	接口的速率，单位为bps
Duplex	<p>接口的双工模式，取值为：</p> <ul style="list-style-type: none"> A：表示双工模式由自动协商结果决定 F：表示全双工 F(a)：表示自由协商的结果为全双工 H：表示半双工 H(a)：表示自由协商的结果为半双工
Type	<p>接口的链路类型：</p> <ul style="list-style-type: none"> A：表示 Access 链路类型 H：表示 Hybrid 链路类型 T：表示 Trunk 链路类型

字段	描述
PVID	接口所在的缺省VLAN ID
Cause	<p>接口物理连接状态为down的原因，取值为：</p> <ul style="list-style-type: none"> • Administratively: 表示本链路被手工关闭了（配置了 shutdown 命令），需要执行 undo shutdown 命令才能恢复真实的物理状态 • DOWN (Link-Aggregation interface down): 聚合接口被关闭后，该聚合接口的所有成员端口的状态会显示为 DOWN，down 的原因会显示为 DOWN (Link-Aggregation interface down) • DOWN (Loopback detection down): 由于环路检测模块检测到环路而自动关闭接口 • DOWN (Monitor-Link uplink down): 由于 Monitor Link 模块检测到上行链路 down 而自动关闭接口 • MAD ShutDown: 当 IRF 分裂后，处于 Recovery 状态的 IRF 会将除了保留接口外的所有接口状态设置为 DOWN，down 的原因会显示为 MAD ShutDown • Not connected: 表示没有物理连接（可能没有插网线或者网线故障） • Storm-Constrain: 表示端口上因为未知单播、组播或广播报文中某类报文的流量大于其上限阈值而被关闭 • STP DOWN: 由于触发了 STP BPDU 保护而自动关闭接口 • Port Security Disabled: 因检测到端口收到非法报文，端口安全的入侵检测机制将端口关闭 • OFP DOWN: 表示接口开启了 OpenFlow 的关闭接口功能 • Standby: 表示接口处于备份状态

【相关命令】

- **reset counters interface**

1.1.11 display link-flap protection

display link-flap protection 命令用来显示接口链路震荡保护功能的相关信息。

【命令】

```
display link-flap protection [ interface interface-type
[ interface-number ] ]
```

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator

【参数】

interface interface-type [interface-number]: 显示指定接口的链路震荡保护功能信息。其中，*interface-type* 表示接口类型，*interface-number* 表示指定接口编号。如果不指定本参数，则显示所有支持接口的链路震荡保护功能信息。

【使用指导】

如果不指定接口编号，则显示所有该类型接口的信息。

仅 Release 6127 及以上版本，支持配置本命令。

【举例】

显示接口链路震荡保护功能的相关信息。

```
<Sysname> display link-flap protection
Link-flap protection: Enabled
Interface          Link-flap  Status  Interval  Threshold
GE1/0/1            Enabled    Down    10         5
GE1/0/2            Disabled   N/A     --         --
```

表1-6 display link-flap protection 命令显示信息描述表

字段	描述
Link-flap protection	全局链路震荡保护功能，取值为： <ul style="list-style-type: none">Enabled: 表示全局的链路震荡功能处于开启状态Disabled: 表示全局的链路震荡功能处于关闭状态
Interface	接口名称缩写
Link-flap	接口链路震荡保护功能，取值为： <ul style="list-style-type: none">Enabled: 表示接口的链路震荡功能处于开启状态Disabled: 表示接口的链路震荡功能处于关闭状态
Status	接口状态，取值为： <ul style="list-style-type: none">Down: 表示接口因为受到链路震荡保护被关闭N/A: 表示接口状态未受到链路震荡保护功能影响
Interval	接口链路震荡检查时间间隔
Threshold	接口链路震荡次数

【相关命令】

- link-flap protect enable
- port link-flap protect enable

1.1.12 duplex

duplex 命令用来设置以太网接口的双工模式。

undo duplex 命令用来恢复缺省情况。

【命令】

```
duplex { auto | full | half }  
undo duplex
```

【缺省情况】

以太网接口的双工模式为 **auto**（自协商）状态。

【视图】

以太网接口视图

【缺省用户角色】

network-admin

【参数】

auto: 接口与对端接口自动协商双工状态。

full: 全双工状态，接口在发送数据包的同时可以接收数据包。

half: 半双工状态，接口同一时刻只能发送数据包或接收数据包。光口和配置了速率为 1000, 10000 的以太网电口不支持配置 **half** 参数。

【举例】

将以太网接口 GigabitEthernet1/0/1 接口设置为全双工状态。

```
<Sysname> system-view  
[Sysname] interface gigabitethernet 1/0/1  
[Sysname-GigabitEthernet1/0/1] duplex full
```

1.1.13 eee enable



说明

光口不支持本命令。

eee enable 命令用来开启 EEE（Energy Efficient Ethernet）节能功能。

undo eee enable 命令用来关闭 EEE 节能功能。

【命令】

```
eee enable  
undo eee enable
```

【缺省情况】

EEE 节能功能处于关闭状态。

【视图】

以太网接口视图

【缺省用户角色】

network-admin

【使用指导】

接口开启 **EEE** 节能功能后，如果在连续一段时间（由芯片规格决定，不能通过命令行配置）内接口状态始终为 **up** 且没有收发任何报文，则接口自动进入低功耗模式；当接口需要收发报文时，接口又自动恢复到正常工作模式，从而达到节能的效果。

【举例】

在 GigabitEthernet1/0/1 下开启 EEE 节能功能。

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

1.1.14 flow-control

flow-control 命令用来开启以太网接口的流量控制功能。

undo flow-control 命令用来关闭以太网接口流量控制功能。

【命令】

```
flow-control
undo flow-control
```

【缺省情况】

以太网接口的流量控制功能处于关闭状态。

【视图】

以太网接口视图

【缺省用户角色】

network-admin

【使用指导】

配置 **flow-control** 命令后，设备具有发送和接收流量控制报文的能力：

- 当本端发生拥塞时，设备会向对端发送流量控制报文。
- 当本端收到对端的流量控制报文后，会停止报文发送。

只有本端和对端设备都开启了流量控制功能，才能实现对本端以太网接口的流量控制。

【举例】

开启以太网接口 GigabitEthernet1/0/1 的流量控制功能。

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] flow-control
```

1.1.15 flow-control receive enable

flow-control receive enable 命令用来开启以太网接口的接收流量控制功能。

undo flow-control 命令用来关闭以太网接口的接收流量控制功能。

【命令】

```
flow-control receive enable
```

undo flow-control

【缺省情况】

以太网接口的接收流量控制功能处于关闭状态。

【视图】

以太网接口视图

【缺省用户角色】

network-admin

【使用指导】

配置 **flow-control receive enable** 命令后，设备具有接收流量控制报文的能力，但不具有发送流量控制报文的能力。

开启以太网接口的接收流量控制功能后：

- 当设备收到对端的流量控制报文，会停止向对端发送报文。
- 当本端发生拥塞时，设备不能向对端发送流量控制报文。

如果要应对单向网络拥塞的情况，可以在一端配置 **flow-control receive enable**，在对端配置 **flow-control**；如果要求本端和对端网络拥塞都能处理，则两端都必须配置 **flow-control**。

【举例】

使能以太网接口 GigabitEthernet1/0/1 的接收流量控制功能。

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

【相关配置】

- **flow-control**

1.1.16 flow-interval

flow-interval 命令用来配置接口统计报文信息的时间间隔。

undo flow-interval 命令用来恢复缺省情况。

【命令】

```
flow-interval interval
undo flow-interval
```

【缺省情况】

接口统计报文信息的时间间隔为 300 秒。

【视图】

以太网接口视图

【缺省用户角色】

network-admin

【参数】

interval: 接口统计信息的时间间隔值, 取值范围为 5~300, 单位为秒, 步长为 5 (即取值必须为 5 的整数倍)。

【举例】

设置以太网接口 GigabitEthernet1/0/1 的统计信息时间间隔为 100 秒。

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] flow-interval 100
```

1.1.17 interface

interface 命令用来进入接口视图。

【命令】

interface *interface-type interface-number*

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

interface-type: 指定接口类型。

interface-number: 指定接口编号。

【举例】

进入以太网接口 GigabitEthernet1/0/1 视图。

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

1.1.18 jumboframe enable

jumboframe enable 命令用来允许超长帧通过。

undo jumboframe enable 命令用来禁止超长帧通过。

undo jumboframe enable size 命令用来恢复缺省情况。

【命令】

```
jumboframe enable [ size ]
undo jumboframe enable [ size ]
```

【缺省情况】

设备允许最大长度为 10240 字节的超长帧通过。

【视图】

二层以太网接口视图

【缺省用户角色】

network-admin

【参数】

size: 以太网接口上允许通过的超长帧的最大长度，取值范围为 1522~10240 单位为字节。

【使用指导】

多次执行本命令，最后一次执行的命令生效。

【举例】

允许超长帧通过以太网接口 GigabitEthernet1/0/1。

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

1.1.19 link-delay

link-delay 命令用来配置以太网接口物理连接状态抑制功能。

undo link-delay 命令用来恢复缺省情况。

【命令】

```
link-delay [ msec ] delay-time [ mode { up | updown } ]
undo link-delay [ msec ] delay-time [ mode { up | updown } ]
```

【缺省情况】

接口状态改变时，系统会将接口状态改变立即上报 CPU。

【视图】

以太网接口视图

【缺省用户角色】

network-admin

【参数】

msec: 表示配置的抑制时间为毫秒级。不指定该参数时，表示配置的抑制时间为秒级。

delay-time: 接口物理连接状态抑制时间值，0 表示不抑制，即接口状态改变时立即上报 CPU。

- 未指定 **msec** 参数时，取值范围为 0~30，单位为秒。
- 指定 **msec** 参数时，取值范围为 0~10000，且为 100 的倍数，单位为毫秒。

mode up: 设置以太网接口物理连接 up 状态抑制功能。

mode updown: 设置以太网接口物理连接 up 和 down 状态抑制功能。

【使用指导】

使用该命令时，选取的参数不同，抑制效果不同：

- 不指定 **mode** 参数：表示接口状态从 up 变成 down 时，不会立即上报 CPU。而是等待 **delay-time** 时间后，再检查接口状态，如果状态仍然是 down，再上报。接口状态从 down 变成 up 时，立即上报 CPU。

- **mode up:** 表示接口状态从 down 变成 up 时，不会立即上报 CPU。而是等待 *delay-time* 时间后，再检查接口状态，如果状态仍然是 up，再上报。接口状态从 up 变成 down 时，立即上报 CPU。
- **mode updown:** 表示接口状态从 up 变成 down 或者 down 变成 up 时，都不会立即上报 CPU。等待 *delay-time* 时间后，再检查接口状态，如果状态仍然是 down 或者 up，再上报。

同一接口下，接口状态从 up 变成 down 的抑制时间和接口状态从 down 变成 up 的抑制时间可以不同。如果在同一端口下，多次执行本命令配置了不同的抑制时间，则两个抑制时间会分别以最新配置为准。

对于开启了生成树协议、RRPP 或 Smart Link 的端口不推荐使用该命令。S5000E-X、S5110V2-SI 和 S5000V3-EI 系列交换机不支持 RRPP 和 Smart Link。

以太网接口上不能同时配置本命令、**dampening** 命令和 **port link-flap protect enable** 命令。

【举例】

设置以太网接口物理连接 down 状态抑制时间为 8 秒。

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] link-delay 8
```

设置以太网接口物理连接 up 状态抑制时间为 800 毫秒。

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] link-delay msec 800 mode up
```

【相关命令】

- **dampening**
- **port link-flap protect enable**

1.1.20 link-flap protect enable

link-flap protect enable 命令用来开启全局链路震荡保护功能。

undo link-flap protect enable 命令用来关闭全局链路震荡保护功能。

【命令】

```
link-flap protect enable
undo link-flap protect enable
```

【缺省情况】

全局链路震荡功能处于关闭状态。

【视图】

系统视图

【缺省用户角色】

network-admin

【使用指导】

链路震荡即接口的物理状态频繁变化时，会导致网络拓扑结构不断变化，给系统带来额外的开销。例如，在主备链路场景中，当主链路的接口物理状态频繁 UP/DOWN 时，业务将在主备链路之间来回切换，增加了设备的负担。为了解决该问题，设备提供了链路震荡保护功能。

配置本功能后，当接口状态从 UP 变为 DOWN 时，系统会启动链路震荡检查。在链路震荡检查时间间隔内，如果该接口状态从 UP 变为 DOWN 的次数大于等于链路震荡次数阈值，则关闭该接口。

只有系统视图下和接口视图下同时开启链路震荡保护功能后，接口的链路震荡保护功能才能生效。

仅 Release 6127 及以上版本，支持配置本命令。

【举例】

全局开启链路震荡保护功能。

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

```
[Sysname] link-flap protect enable
```

【相关命令】

- **port link-flap protect enable**

1.1.21 loopback

loopback 命令用来开启以太网接口的环回功能。

【命令】

```
loopback { external | internal }
```

【缺省情况】

以太网接口的环回功能处于关闭状态。

【视图】

以太网接口视图

【缺省用户角色】

network-admin

【参数】

external：开启以太网接口的外部环回功能。

internal：开启以太网接口的内部环回功能。

【使用指导】

开启环回功能后，接口将自动切换到全双工模式，关闭环回功能后会自动恢复原有双工模式。

对以太网接口进行环回测试时，接口将不能正常转发数据包。

手工关闭以太网接口（接口状态显示为 ADM 或者 Administratively DOWN）时，则不能进行内部和外部环回测试。

在进行环回测试时系统将禁止在接口上进行 **speed**、**duplex**、**mdix-mode** 和 **shutdown** 命令的配置。

【举例】

开启以太网接口 GigabitEthernet1/0/1 的内部环回功能。

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] loopback internal
```

1.1.22 multicast-suppression

multicast-suppression 命令用来开启端口组播风暴抑制功能，并设置组播风暴抑制阈值。

undo multicast-suppression 命令用来关闭端口组播风暴抑制功能。

【命令】

```
multicast-suppression { ratio | pps max-pps | kbps max-kbps }
undo multicast-suppression
```

【缺省情况】

所有接口不对组播流量进行抑制。

【视图】

以太网接口视图

【缺省用户角色】

network-admin

【参数】

ratio: 指定以太网接口允许通过的最大组播流量占该接口带宽的百分比。取值范围为 0~100。数值越小，则允许通过的组播流量也越小。

pps max-pps: 指定以太网接口每秒最多通过的组播包包数，取值范围为 0~1.4881×接口带宽。

kbps max-kbps: 指定以太网接口每秒最多通过的组播流量，单位为 kbps，取值范围为 0~接口带宽。

【使用指导】

本命令设置的是接口允许通过的最大组播报文流量。当接口上的组播流量超过用户设置的值后，系统将丢弃超出组播流量限制的报文，从而使接口组播流量所占的比例控制在限定的范围内，以便保证业务的正常运行。

执行 **multicast-suppression** 或 **storm-constrain** 命令都能开启端口的组播风暴抑制功能，**storm-constrain** 命令通过软件对组播报文进行抑制，对设备性能有一定影响，**multicast-suppression** 通过芯片物理上对组播报文进行抑制，相对 **storm-constrain** 来说，对设备性能影响较小。请不要同时配置 **multicast-suppression** 和 **storm-constrain** 命令，以免配置冲突，导致抑制效果不确定。

当风暴抑制阈值配置为 **kbps** 时，若配置值小于 64，则实际生效的数值为 64；若配置值大于 64 但不是 64 的整数倍，则实际生效的数值为大于且最接近于配置值的 64 的整数倍。请注意查看设备的提示信息。

【举例】

在以太网接口 GigabitEthernet1/0/1 上，每秒最多允许 10000kbps 组播报文通过，对超出该范围的组播报文进行抑制。

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

```
[Sysname-GigabitEthernet1/0/1] multicast-suppression kbps 10000
The actual value is 10048 on port GigabitEthernet1/0/1 currently.
```

以上信息表示：用户配置的值为 10000kbps，因为芯片支持的步长为 64，所以实际生效的值为 10048kbps（64 的 157 倍）。

【相关命令】

- **broadcast-suppression**
- **unicast-suppression**

1.1.23 port auto-power-down



说明

光口不支持本命令。

port auto-power-down 命令用来开启 down 状态接口节能功能。

undo port auto-power-down 命令用来关闭 down 状态接口节能功能。

【命令】

```
port auto-power-down
undo port auto-power-down
```

【缺省情况】

down 状态接口节能功能处于关闭状态。

【视图】

接口视图

【缺省用户角色】

network-admin

【使用指导】

配置该命令后，如果在连续一段时间（由芯片规格决定，不能通过命令行配置）内接口状态始终为 down，则系统会自动停止对该接口供电，接口自动进入节能模式；当接口状态变为 up 时，系统会自动恢复对该接口供电，接口自动进入正常模式，从而达到节能的效果。

【举例】

开启以太网接口 GigabitEthernet1/0/1 的 down 状态节能功能。

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] port auto-power-down
```

1.1.24 port link-flap protect enable

port link-flap protect enable 命令用来开启接口链路震荡保护功能。

undo port link-flap protect enable 命令用来关闭接口链路震荡保护功能。

【命令】

```
port link-flap protect enable [ interval interval | threshold threshold ] *  
undo port link-flap protect enable [ interval | threshold ]
```

【缺省情况】

接口的链路震荡功能处于关闭状态。

【视图】

以太网接口视图

【缺省用户角色】

network-admin

【参数】

interval interval: 链路震荡检查时间间隔，取值范围 10~60，单位为秒，缺省值为 10 秒。

threshold threshold: 链路震荡次数阈值，取值范围 5~10，缺省值为 5 次。

【使用指导】

只有系统视图下和接口视图下同时配置链路震荡保护功能后，接口的链路震荡保护功能才能生效。

执行 **port link-flap protect enable** 命令时，如果未指定 **interval** 或 **threshold**，表示采用 **interval** 或 **threshold** 的缺省值。

执行 **undo port link-flap protect enable** 命令时，如果指定 **interval** 或 **threshold**，表示恢复 **interval** 或 **threshold** 的缺省值。

接口下配置本命令后，当接口状态从 UP 变为 DOWN 时，系统会启动链路震荡检查。在链路震荡检查时间间隔内，如果该接口状态从 UP 变为 DOWN 的次数大于等于链路震荡次数阈值，则关闭该接口。

接口因链路频繁震荡被关闭后，不会自动恢复，需要用户执行 **undo shutdown** 命令手工恢复。

以太网接口上不能同时配置本命令、**dampening** 命令和 **link-delay** 命令。

仅 Release 6127 及以上版本，支持配置本命令。

【举例】

开启接口的链路震荡保护功能，链路震荡检查时间间隔为 10 秒，链路震荡次数阈值为 5 次。

```
<Sysname> system-view  
[Sysname] interface gigabitethernet 1/0/1  
[Sysname-GigabitEthernet1/0/1] port link-flap protect enable interval 10 threshold 5
```

【相关命令】

- **dampening**
- **link-delay**
- **link-flap protect enable**

1.1.25 reset counters interface

reset counters interface 命令用来清除接口的统计信息。

【命令】

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

【视图】

用户视图

【缺省用户角色】

network-admin

【参数】

interface-type: 指定接口类型。

interface-number: 指定接口编号。

【使用指导】

在某些情况下，需要统计一定时间内某接口的流量，这就需要在统计开始前清除该接口原有的统计信息，重新进行统计。

如果不指定 *interface-type* 和 *interface-number*，则清除所有接口的统计信息；

如果指定 *interface-type* 而不指定 *interface-number*，则清除所有该类型接口的统计信息。

【举例】

清除以太网接口 GigabitEthernet1/0/1 的统计信息。

```
<Sysname> reset counters interface gigabitethernet 1/0/1
```

【相关命令】

- **display interface**
- **display counters interface**
- **display counters rate interface**

1.1.26 reset ethernet statistics

reset ethernet statistics 命令用来清除以太网软件模块收发报文的统计信息。

【命令】

```
reset ethernet statistics [ slot slot-number ]
```

【视图】

用户视图

【缺省用户角色】

network-admin

【参数】

slot slot-number: 清除指定成员设备的统计信息，*slot-number* 表示设备在 IRF 中的成员编号。不指定该参数时，表示所有成员设备。

【举例】

清除指定 slot 上的以太网软件模块收发报文的统计信息。

```
<Sysname> reset ethernet statistics slot 1
```

【相关命令】

- `display ethernet statistics`

1.1.27 shutdown

shutdown 命令用来关闭以太网接口。

undo shutdown 命令用来打开以太网接口。

【命令】

shutdown

undo shutdown

【缺省情况】

以太网接口处于开启状态。

【视图】

以太网接口视图

【缺省用户角色】

network-admin

【使用指导】

在某些特殊情况下（例如修改接口的工作参数），接口相关配置不能立即生效，需要关闭再打开接口后，才能生效。

在进行环回测试时，禁止在接口上配置 **shutdown** 命令

【举例】

关闭以太网接口 **GigabitEthernet1/0/1** 后打开该接口。

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] shutdown
[Sysname-GigabitEthernet1/0/1] undo shutdown
```

1.1.28 speed

speed 命令用来设置以太网接口的速率。

undo speed 命令用来恢复缺省情况。

【命令】

speed { 10 | 100 | 1000 | 10000 | auto }

undo speed

【缺省情况】

以太网接口的速率为 **auto**（自协商）状态。

【视图】

以太网接口视图

【缺省用户角色】

network-admin

【参数】

10: 表示接口速率为 10Mbps。

100: 表示接口速率为 100Mbps。

1000: 表示接口速率为 1000Mbps。

10000: 表示接口速率为 10000Mbps。

auto: 表示接口速率处于自协商状态。

【使用指导】

对于以太网电口来说，使用 **speed** 命令设置端口速率，目的是使其与对端进行速率匹配。

对于光口来说，使用 **speed** 命令设置端口速率，目的是使其与可插拔光模块进行速率匹配。

不同类型的接口支持配置的参数不同，具体情况请在相关接口视图下执行 **speed ?** 命令查看。

【举例】

将以太网接口 GigabitEthernet1/0/1 的速率设置为自协商获得。

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] speed auto
```

【相关命令】

- **speed auto**

1.1.29 speed auto downgrade

speed auto downgrade 命令用来开启以太网接口速率自动降级协商功能。

undo speed auto downgrade 命令用来关闭以太网接口速率自动降级协商功能。

【命令】

```
speed auto downgrade
undo speed auto downgrade
```

【缺省情况】

以太网接口速率自动降级协商功能处于开启状态。

【视图】

以太网接口视图

【缺省用户角色】

network-admin

【使用指导】

只要链路任何一端接口开启了速率自动降级协商功能，且两端的接口都处于速率自动协商状态，则降级协商功能就会生效。

本命令仅支持在千兆以太网接口下配置。

【举例】

在接口 GigabitEthernet1/0/1 上开启接口速率自动降级协商功能。

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] speed auto downgrade
```

【相关命令】

- **speed auto**

1.1.30 unicast-suppression

unicast-suppression 命令用来开启端口未知单播风暴抑制功能，并设置未知单播风暴抑制阈值。

undo unicast-suppression 命令用来关闭端口未知单播风暴抑制功能。

【命令】

```
unicast-suppression { ratio | pps max-pps | kbps max-kbps }
undo unicast-suppression
```

【缺省情况】

所有接口不对未知单播流量进行抑制。

【视图】

以太网接口视图

【缺省用户角色】

network-admin

【参数】

ratio: 指定以太网接口最大未知单播流量占该接口带宽的百分比。取值范围为 0~100。数值越小，则允许通过的未知单播流量也越小。

pps max-pps: 指定以太网接口每秒最多通过的未知单播包包数，取值范围为 0~1.4881×接口带宽。

kbps max-kbps: 指定以太网接口每秒通过的未知单播流量，单位为 kbps，取值范围为 0~接口带宽。

【使用指导】

本命令设置的是接口允许通过的最大未知单播报文流量。当接口上的未知单播流量超过用户设置的值后，系统将丢弃超出未知单播流量限制的报文，从而使接口未知单播流量所占的比例降低到限定的范围，保证网络业务的正常运行。

执行 **unicast-suppression** 或 **storm-constrain** 命令都能开启端口的未知单播风暴抑制功能，**storm-constrain** 命令通过软件对未知单播报文进行抑制，对设备性能有一定影响，**unicast-suppression** 通过芯片物理上对未知单播报文进行抑制，相对 **storm-constrain** 来说，对设备性能影响较小。请不要同时配置 **unicast-suppression** 和 **storm-constrain** 命令，以免配置冲突，导致抑制效果不确定。

当风暴抑制阈值配置为 **kbps** 时，若配置值小于 **64**，则实际生效的数值为 **64**；若配置值大于 **64** 但不是 **64** 的整数倍，则实际生效的数值为大于且最接近于配置值的 **64** 的整数倍。请注意查看设备的提示信息。

【举例】

在以太网接口 **GigabitEthernet1/0/1** 上，每秒最多允许 **10000kbps** 未知单播报文通过，对超出该范围的未知单播报文进行抑制。

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] unicast-suppression kbps 10000
The actual value is 10048 on port GigabitEthernet1/0/1 currently.
```

以上信息表示：用户配置的值为 **10000kbps**，因为芯片支持的步长为 **64**，所以实际生效的值为 **10048kbps**（**64** 的 **157** 倍）。

【相关命令】

- **broadcast-suppression**
- **multicast-suppression**

1.2 二层以太网接口的配置命令

1.2.1 display storm-constrain

display storm-constrain 命令用来显示接口流量控制信息。

【命令】

```
display storm-constrain [ broadcast | multicast | unicast ] [ interface  
interface-type interface-number ]
```

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator

【参数】

broadcast：只显示广播报文流量控制信息。

multicast：只显示组播报文流量控制信息。

unicast：只显示未知单播报文流量控制信息。

interface interface-type interface-number：显示指定接口的报文流量控制信息。
interface-type interface-number 指定接口类型和接口编号。不指定该参数时，显示所有接口报文的流量控制信息。

【使用指导】

不指定 **broadcast**、**known-unicast**、**multicast** 和 **unicast** 参数时，则显示所有类型报文的流量控制信息。

【举例】

显示系统当前所有接口的流量控制信息。

```
<Sysname> display storm-constrain
Abbreviation: BC - broadcast; MC - multicast; UC - unicast
              KNUC - known unicast; FW - forwarding
Flow Statistic Interval: 5 (in seconds)
Port          Type Lower      Upper      Unit CtrlMode Status   Trap Log SwitchNum
-----
GE1/0/1       MC    100        200        kbps shutdown shutdown off   on   10
```

表1-7 display storm-constrain 命令显示信息描述表

字段	描述
Flow Statistic Interval	流量统计的时间间隔，单位为秒
Port	接口名称缩写
Type	进行流量阈值控制的报文类型： <ul style="list-style-type: none">BC: broadcast，表示广播报文MC: multicast，表示组播报文UC: unicast，表示未知单播报文（暂不支持）KUNC: known unicast，表示已知单播报文
Lower	用户配置的流量控制下限阈值或百分比
Upper	用户配置的流量控制上限阈值或百分比
Unit	用户配置的流量阈值的单位，为pps、kbps或百分比
CtrlMode	用户配置的流量阈值超过上限的控制动作： <ul style="list-style-type: none">block 表示阻塞方式shutdown 表示关闭方式N/A 表示未配置控制动作
Status	接口报文转发状态，取值为： <ul style="list-style-type: none">forwarding 表示该端口处于正常转发状态shutdown 表示端口已被关闭block 表示该端口对该类报文直接丢弃
Trap	Trap信息输出开关： <ul style="list-style-type: none">on 表示打开off 表示关闭
Log	Log信息输出开关： <ul style="list-style-type: none">on 表示打开off 表示关闭
SwitchNum	接口报文转发状态切换次数 当SwitchNum达到65535次时，会自动跳转到0，重新计数

1.2.2 mdix-mode



说明

光口不支持本命令。

mdix-mode 命令用来设置以太网接口的 MDIX 模式。

undo mdix-mode 命令用来恢复缺省情况。

【命令】

```
mdix-mode { automdix | mdi | mdix }  
undo mdix-mode
```

【缺省情况】

以太网接口的 MDIX 模式为 **automdix**。

【视图】

二层以太网接口视图

【缺省用户角色】

network-admin

【参数】

automdix: 两端设备通过协商来决定引脚 1 和 2 是发送还是接收信号，引脚 3 和 6 是接收还是发送信号。

mdi: 使用引脚 1 和 2 发送信号，使用引脚 3 和 6 接收信号。

mdix: 使用引脚 1 和 2 接收信号，使用引脚 3 和 6 发送信号。

【举例】

设置以太网接口 GigabitEthernet1/0/1 的 MDIX 模式为 **automdix**。

```
<Sysname> system-view  
[Sysname] interface gigabitethernet 1/0/1  
[Sysname-GigabitEthernet1/0/1] mdix-mode automdix
```

1.2.3 port bridge enable

port bridge enable 命令用来开启接口桥功能。

undo port bridge enable 命令用来关闭接口桥功能。

【命令】

```
port bridge enable  
undo port bridge enable
```

【缺省情况】

接口桥功能处于关闭状态。

【视图】

二层以太网接口视图

【缺省用户角色】

network-admin

【使用指导】

缺省情况下，设备收到报文后会根据报文特征查找报文出接口，如果该报文出接口和入接口为同一接口，则将报文丢弃。在二层以太网接口上开启本功能后，如果该报文出接口和入接口为同一接口，则从该接口转发报文。

当设备收到未知单播或者广播报文时，会在该报文入接口所属 VLAN 内的所有接口转发该报文。

开启了本功能的二层以太网接口不建议加入聚合组，避免影响本功能使用。

【举例】

在二层以太网接口 GigabitEthernet1/0/1 上开启接口桥功能。

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

1.2.4 speed auto

speed auto 命令用来设置以太网接口的自协商速率范围。

undo speed 命令用来恢复缺省情况。

【命令】

```
speed auto { 10 | 100 | 1000 } *
undo speed
```

【缺省情况】

未配置以太网接口的自协商速率范围。

【视图】

百兆或者千兆二层以太网接口视图

【缺省用户角色】

network-admin

【参数】

10：设置接口自协商速率为 10Mbps。

100：设置接口自协商速率为 100Mbps。

1000：设置接口自协商速率为 1000Mbps。

【使用指导】

多次执行 **speed**、**speed auto** 命令，最后一次执行的命令生效。例如：

- 若在接口下先配置了 **speed auto 100 1000**，然后又配置 **speed 100**，则接口的速率强制为 100Mbps，不进行协商。

- 若在接口下先配置了 **speed 100**，然后又配置 **speed auto 100 1000**，则接口将与对端协商速率，协商的结果只能为 100Mbps 或 1000Mbps。

速率协商方法为：

- 如果两端设置的接口自协商速率的范围完全不同，例如：一端为 **speed auto 10 100**，另一端为 **speed auto 1000**，此时两端速率协商不成功；
- 如果两端设置的接口自协商速率的范围部分相同，例如：一端为 **speed auto 10 100**，另一端为 **speed auto 100 1000**，此时两端速率协商为双方都有的 100 Mbps；
- 如果两端设置的接口自协商速率的范围完全相同，例如：一端为 **speed auto 100 1000**，另一端为 **speed auto 100 1000**，此时两端取速率协商范围内最大速率 1000 Mbps。

【举例】

设置接口 GigabitEthernet1/0/1 的自协商速率为 10Mbps 或 1000Mbps。

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] speed auto 10 1000
```

【相关命令】

- **speed**

1.2.5 storm-constrain

storm-constrain 命令用来开启端口流量阈值控制功能，并设置上限阈值与下限阈值。

undo storm-constrain 命令用来关闭端口流量阈值控制功能。

【命令】

```
storm-constrain { broadcast | multicast | unicast } { pps | kbps | ratio }
upperlimit lowerlimit
undo storm-constrain { all | broadcast | multicast | unicast }
```

【缺省情况】

端口流量阈值控制功能处于关闭状态，即不对端口的报文流量进行抑制。

【视图】

二层以太网接口视图

【缺省用户角色】

network-admin

【参数】

all：取消端口所有类型（未知单播、组播和广播）报文流量阈值配置。

broadcast：设置端口广播报文流量阈值。

multicast：设置端口组播报文流量阈值。

unicast：设置端口未知单播报文流量阈值。

pps：以包每秒为单位统计流量。

kbps：以千比特每秒为单位统计流量。

ratio：以每秒钟报文所占接口物理带宽的百分比来统计流量。

upperlimit: 端口报文流量的上限阈值。当和 **pps** 一起使用时, 该参数的取值范围为 0~1.4881×接口带宽; 当和 **kpps** 一起使用时, 该参数的取值范围为 0~接口带宽; 当和 **ratio** 一起使用时, 该参数的取值范围为 0~100。

lowerlimit: 端口报文流量的下限阈值。当和 **pps** 一起使用时, 该参数的取值范围为 0~1.4881×接口带宽; 当和 **kpps** 一起使用时, 该参数的取值范围为 0~接口带宽; 当和 **ratio** 一起使用时, 该参数的取值范围为 0~100。

【使用指导】

执行本命令后, 设备就会周期性地对接口收到的指定类型的报文进行统计, 如果流量超过上限阈值, 则采取一定的措施。其中, 通过 **storm-constrain interval** 命令可以配置统计周期, 通过 **storm-constrain control** 命令可以配置流量超过上限阈值时采取的控制方式。

执行 **storm-constrain** 与 **broadcast-suppression**、**multicast-suppression**、**unicast-suppression** 命令都能开启端口的风暴抑制功能。**storm-constrain** 命令通过软件对报文流量进行抑制, 对设备性能有一定影响, **broadcast-suppression**、**multicast-suppression**、**unicast-suppression** 通过芯片物理上对报文流量进行抑制, 相对 **storm-constrain** 来说, 对设备性能影响较小。对于某种类型的报文流量, 请不要同时配置这两种方式, 以免配置冲突, 导致抑制效果不确定。

配置时, **upperlimit** 值必须大于 **lowerlimit** 值, 建议不要配成相等值。

【举例】

对 GigabitEthernet1/0/1 端口配置未知单播流量阈值, 上限阈值为 200pps、下限阈值为 150pps。

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] storm-constrain unicast pps 200 150
```

对 GigabitEthernet1/0/2 端口配置广播流量阈值, 上限阈值为 2000kbps、下限阈值为 1500kbps。

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/2
[Sysname-GigabitEthernet1/0/2] storm-constrain broadcast kbps 2000 1500
```

对 GigabitEthernet1/0/3 端口配置组播流量百分比阈值, 上限为 80%、下限为 15%。

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/3
[Sysname-GigabitEthernet1/0/3] storm-constrain multicast ratio 80 15
```

【相关命令】

- **storm-constrain control**
- **storm-constrain interval**

1.2.6 storm-constrain control

storm-constrain control 命令用来设置端口未知单播、组播或者广播流量超过上限阈值时采取的控制方式。

undo storm-constrain control 命令用来恢复缺省情况。

【命令】

```
storm-constrain control { block | shutdown }
```

undo storm-constrain control

【缺省情况】

不对端口流量进行控制。

【视图】

二层以太网接口视图

【缺省用户角色】

network-admin

【参数】

block: block 方式，即：当端口上未知单播、组播或广播报文中某类报文的流量大于其上限阈值时，端口将暂停转发该类报文（其它类型报文照常转发），端口处于阻塞状态，但仍会统计该类报文的流量。当该类报文的流量小于其下限阈值时，端口将自动恢复对此类报文的转发。

shutdown: shutdown 方式，即：当端口上未知单播、组播或广播报文中某类报文的流量大于其上限阈值时，端口将被关闭，系统停止转发所有报文。当该类报文的流量小于其下限阈值时，端口状态不会自动恢复，此时可通过执行 **undo shutdown** 命令或取消端口上流量阈值的配置来恢复。

【举例】

配置 GigabitEthernet1/0/1 端口，当流量超过上限阈值时，采用 block 方式控制。

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] storm-constrain control block
```

【相关命令】

- **storm-constrain**
- **storm-constrain control**

1.2.7 storm-constrain enable log

storm-constrain enable log 命令用来配置端口流量从小于等于上限阈值到大于上限阈值或者从超上限回落到小于下限阈值时输出 Log 信息。

undo storm-constrain enable log 命令用来禁止端口流量从小于等于上限阈值到大于上限阈值或者从超上限回落到小于下限阈值时输出 Log 信息。

【命令】

```
storm-constrain enable log
undo storm-constrain enable log
```

【缺省情况】

端口流量从小于等于上限阈值到大于上限阈值或者从超上限回落到小于下限阈值时输出 Log 信息。

【视图】

二层以太网接口视图

【缺省用户角色】

network-admin

【举例】

当 GigabitEthernet1/0/1 端口流量从小于等于上限阈值到大于上限阈值或者从超上限回落到小于下限阈值时输出 Log 信息。

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

1.2.8 storm-constrain enable trap

storm-constrain enable trap 命令用来配置端口流量从小于等于上限阈值到大于上限阈值或者从超上限回落到小于下限阈值时输出 Trap 信息。

undo storm-constrain enable trap 命令用来禁止端口流量从小于等于上限阈值到大于上限阈值或者从超上限回落到小于下限阈值时输出 Trap 信息。

【命令】

```
storm-constrain enable trap
undo storm-constrain enable trap
```

【缺省情况】

端口流量从小于等于上限阈值到大于上限阈值或者从超上限回落到小于下限阈值时输出 Trap 信息。

【视图】

二层以太网接口视图

【缺省用户角色】

network-admin

【举例】

当 GigabitEthernet1/0/1 端口流量从小于等于上限阈值到大于上限阈值或者从超上限回落到小于下限阈值时输出 Trap 信息。

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

1.2.9 storm-constrain interval

storm-constrain interval 命令用来配置端口流量阈值控制模块流量统计的时间间隔。

undo storm-constrain interval 命令用来恢复缺省情况。

【命令】

```
storm-constrain interval interval
undo storm-constrain interval
```

【缺省情况】

端口流量统计的时间间隔为 10 秒。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

interval: 端口流量统计的时间间隔, 取值范围为 1~300, 单位为秒。为了保持网络状态的稳定, 建议设置的时间间隔不低于 10 秒。

【使用指导】

本命令设置的时间间隔专门为 **storm-constrain** 命令服务的, 不同于 **flow-interval** 命令设置的时间间隔。虽然同样是统计端口流量, 但是功能是分开的。

【举例】

```
# 配置端口流量统计时间间隔为 60 秒。
<Sysname> system-view
[Sysname] storm-constrain interval 60
```

【相关命令】

- **storm-constrain**
- **storm-constrain control**

1.2.10 virtual-cable-test



说明

光口不支持本命令。

virtual-cable-test 命令用来对以太网接口连接电缆进行一次检测, 并显示检测结果。

【命令】

virtual-cable-test

【视图】

二层以太网接口视图

【缺省用户角色】

network-admin

【使用指导】

当以太网接口处于 UP 状态, 速率为 1000M 时, 使用本命令对连接电缆进行检测的结果不是太准确。不支持速率为 10M/100M 情况下的测试, 测试结果是无效值。

当通过 **shutdown** 命令手工关闭以太网接口后, 无法使用本命令对连接电缆进行检测。

检测结果仅供参考, 检测到的长度最大误差为 5 米。

如果显示值为 “-”, 则表示不支持该项参数的检测。

【举例】

开启系统对以太网电口连接电缆的检测功能。

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

```
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] virtual-cable-test
Cable status: abnormal(open), 140 metre(s)
Pair Impedance mismatch: -
Pair skew: - ns
Pair swap: -
Pair polarity: -
Insertion loss: - db
Return loss: - db
Near-end crosstalk: - db
```

表1-8 virtual-cable-test 命令显示信息描述表

字段	描述
Cable status	电缆状态，包括： <ul style="list-style-type: none">• normal: 正常• abnormal: 异常• abnormal(open): 异常开路• abnormal(short): 异常短路• failure: 检测失败
<i>n metres</i>	当电缆状态为正常时，显示的是电缆的总长度 当电缆状态非正常时，显示的是本接口到异常位置的长度
Pair Impedance mismatch	线对阻抗是否匹配，取值为： <ul style="list-style-type: none">• yes: 阻抗匹配• no: 阻抗不匹配
Pair skew	线对不对称
Pair swap	线对交换
Pair polarity	是否极性交换
Insertion loss	插入信号衰减
Return loss	返回信号衰减
Near-end crosstalk	近端串扰

目 录

1 LoopBack接口、NULL接口和InLoopBack接口	1-1
1.1 LoopBack接口、NULL接口和InLoopBack接口配置命令	1-1
1.1.1 bandwidth	1-1
1.1.2 default	1-1
1.1.3 description	1-2
1.1.4 display interface inloopback	1-3
1.1.5 display interface loopback	1-5
1.1.6 display interface null	1-8
1.1.7 interface loopback	1-9
1.1.8 interface null	1-9
1.1.9 reset counters interface loopback	1-10
1.1.10 reset counters interface null	1-10
1.1.11 shutdown	1-11

1 LoopBack接口、NULL接口和InLoopBack接口

1.1 LoopBack接口、NULL接口和InLoopBack接口配置命令

1.1.1 bandwidth

bandwidth 命令用来配置接口的期望带宽。

undo bandwidth 命令用来恢复缺省情况。

【命令】

bandwidth *bandwidth-value*

undo bandwidth

【缺省情况】

LoopBack 接口的期望带宽为 0kbps。

【视图】

LoopBack 接口视图

【缺省用户角色】

network-admin

【参数】

bandwidth-value: 表示接口的期望带宽，取值范围为 1~4000000000，单位为 kbps。

【使用指导】

期望带宽供业务模块使用，不会对接口实际带宽造成影响。

【举例】

配置 LoopBack1 的期望带宽为 1000kbps。

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

```
[Sysname] interface loopback 1
```

```
[Sysname-LoopBack1] bandwidth 1000
```

1.1.2 default

default 命令用来恢复接口的缺省配置。

【命令】

default

【视图】

LoopBack 接口视图

NULL 接口视图

【缺省用户角色】

network-admin

【使用指导】



注意

接口下的某些配置恢复到缺省情况后，会对设备上当前运行的业务产生影响。建议您在执行该命令前，完全了解其对网络产生的影响。

您可以在执行 **default** 命令后通过 **display this** 命令确认执行效果。对于未能成功恢复缺省的配置，建议您查阅相关功能的命令手册，手工执行恢复该配置缺省情况的命令。如果操作仍然不能成功，您可以通过设备的提示信息定位原因。

【举例】

将 LoopBack1 恢复为缺省配置。

```
<Sysname> system-view
[Sysname] interface loopback 1
[Sysname-LoopBack1] default
```

1.1.3 description

description 命令用来设置接口的描述信息。

undo description 命令用来恢复缺省情况。

【命令】

```
description text
undo description
```

【缺省情况】

接口的描述信息为“接口名 Interface”，比如：LoopBack1 Interface。

【视图】

LoopBack 接口视图

NULL 接口视图

【缺省用户角色】

network-admin

【参数】

text: 接口的描述信息，为 1~255 个字符的字符串，区分大小写。

【使用指导】

当设备上存在多个接口时，可以根据接口的连接信息或用途来配置接口的描述信息，以便区别和管理各接口。

配置的描述信息可通过命令行 **display interface** 查看。

【举例】

设置 LoopBack1 的描述信息为“for RouterID”。

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

```
[Sysname] interface loopback 1
[Sysname-LoopBack1] description for RouterID
```

1.1.4 display interface inloopback

display interface inloopback 命令用来显示 InLoopBack 接口的相关信息。

【命令】

```
display interface inloopback [ 0 ] [ brief [ description | down ] ]
```

【视图】

任意视图

【缺省用户角色】

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

【参数】

- 0**: InLoopBack 接口的编号。
- brief**: 显示接口的概要信息。不指定该参数时，将显示接口的详细信息。
- description**: 用来显示用户配置的接口的全部描述信息。如果某接口的描述信息超过 27 个字符，不指定该参数时，只显示描述信息中的前 27 个字符，超出部分不显示。对于 InLoopBack 接口，因为其描述信息只能为 InLoopBack0 Interface，不能配置，所以，该参数对 InLoopBack 接口无意义。
- down**: 显示当前物理状态为 down 的接口的信息以及 down 的原因。不指定该参数时，将不会根据接口物理状态来过滤显示信息。

【使用指导】

因为设备只支持一个 InLoopBack 接口 InLoopBack0，所以不管是否指定 0 参数，显示的都是 InLoopBack0 的相关信息。

【举例】

```
# 显示指定接口 InLoopBack0 的相关信息。
<Sysname> display interface inloopback
InLoopBack0
Current state: UP
Line protocol state: UP(spoofing)
Description: InLoopBack0 Interface
Maximum transmission unit: 1536
Physical: InLoopBack
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
```

表1-1 display interface inloopback 命令显示信息描述表

字段	描述
Current state	接口当前的物理层状态。始终为UP，表示接口能收发报文

字段	描述
Line protocol state	链路层协议状态。始终为UP(spoofing)，表示接口的链路层协议状态为UP，但实际可能没有对应的链路，或者对应的链路不是永久存在，而是按需建立的
Description	接口的描述信息。只能为InLoopBack0 Interface，不可配置
Maximum transmission unit	接口的MTU。只能为1536，不可配置
Physical: InLoopBack	接口的物理类型是InLoopBack
Last 300 seconds input rate: 0 bytes/sec, 0 bits/sec, 0 packets/sec	最近300秒钟的平均输入速率（只有接口支持统计功能时才显示该信息）： <ul style="list-style-type: none"> bytes/sec 表示平均每秒输入的字节数 bits/sec 表示平均每秒输入的比特数 packets/sec 表示平均每秒输入的包数
Last 300 seconds output rate: 0 bytes/sec, 0 bits/sec, 0 packets/sec	最近300秒钟的平均输出速率（只有接口支持统计功能时才显示该信息）： <ul style="list-style-type: none"> bytes/sec 表示平均每秒输出的字节数 bits/sec 表示平均每秒输出的比特数 packets/sec 表示平均每秒输出的包数
Input: 0 packets, 0 bytes, 0 drops	接口输入的报文数，输入的字节数，输入报文中丢弃的报文数（只有接口支持统计功能时才显示这些信息）
Output: 0 packets, 0 bytes, 0 drops	接口输出的报文数，输入的字节数，输入报文中丢弃的报文数（只有接口支持统计功能时才显示这些信息）

显示 InLoopBack 接口的概要信息。

```
<Sysname> display interface inloopback 0 brief
Brief information on interfaces in route mode:
Link: ADM - administratively down; Stby - standby
Protocol: (s) - spoofing
Interface          Link Protocol Primary IP      Description
InLoop0            UP    UP(s)    --
```

表1-2 display interface inloopback brief 命令显示信息描述表

字段	描述
Brief information on interfaces in route mode:	InLoopBack接口的概要信息
Link: ADM - administratively down; Stby - standby	<ul style="list-style-type: none"> 如果某接口的Link属性值为“ADM”，则表示该接口被管理员通过 shutdown 命令关闭，需要在该接口下执行 undo shutdown 命令才能恢复接口本身的物理状态 如果某接口的Link属性值为“Stby”，则表示该接口是一个处于 Standby 状态的备份接口
Protocol: (s) - spoofing	如果某接口的Protocol属性值中带有(s)，则表示该接口的数据链路层协议状态显示为UP，但实际可能没有对应的链路，或者对应的链路不是永久存在而是按需建立的。通常NULL、LoopBack、InLoopBack等接口会具有该属性
Interface	接口名称缩写

字段	描述
Link	接口物理连接状态。取值为UP，表示本链路物理上是连通的
Protocol	接口数据链路层协议状态，取值为UP(s)
Primary IP	接口IP地址 因为InLoopBack接口下不能配置命令行，所以该项对InLoopBack接口无意义
Description	接口的描述信息。因为InLoopBack接口下不能配置命令行，所以该项对InLoopBack接口无意义

1.1.5 display interface loopback

display interface loopback 命令用来显示 LoopBack 接口的相关信息。

【命令】

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

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator

【参数】

loopback interface-number: LoopBack 接口的编号，取值范围为已创建的 LoopBack 接口的编号。如果不指定接口编号，将显示所有已创建的 LoopBack 接口的相关信息。

brief: 显示接口的概要信息。不指定该参数时，将显示接口的详细信息。

description: 用来显示用户配置的接口的全部描述信息。如果某接口的描述信息超过 27 个字符，不指定该参数时，只显示描述信息中的前 27 个字符，超出部分不显示。

down: 显示当前物理状态为 down 的接口的信息以及 down 的原因。不指定该参数时，将不会根据接口物理状态来过滤显示信息。

【使用指导】

display interface loopback 命令用来显示 Loopback 接口的相关信息。只有创建 LoopBack 接口后，才支持该命令。

【举例】

显示 LoopBack0 接口的相关信息。

```
<Sysname> display interface loopback 0
LoopBack0
Current state: UP
Line protocol state: UP(spoofing)
Description: LoopBack0 Interface
Bandwidth: 1000 kbps
```

Maximum transmission unit: 1536
 Internet protocol processing: Disabled
 Physical: Loopback
 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

表1-3 display interface loopback 命令显示信息描述表

字段	描述
Current state	接口当前的物理层状态 <ul style="list-style-type: none"> UP: 表示接口能收发报文 Administratively DOWN: 表示接口被手工关闭了, 即在接口下配置了 shutdown 命令
Line protocol state	链路层协议状态: UP(spoofing), 表示接口的链路层协议状态为UP, 但实际可能没有对应的链路, 或者对应的链路不是永久存在, 而是按需建立的
Description	接口的描述信息
Bandwidth	接口的期望带宽, 只有当取值不为0时, 才显示该字段
Maximum transmission unit	接口的MTU
Internet protocol processing: Disabled	表示不能处理三层报文 (接口没有配置IP地址时, 显示该信息)
Internet address: 1.1.1.1/32 (primary)	接口的主IP地址 (接口配置了主IP地址时显示该信息)
Physical: Loopback	接口的物理类型是Loopback
Last clearing of counters	最近一次使用 reset counters interface 命令清除接口下的统计信息的时间 (如果从设备启动一直没有执行 reset counters interface 命令清除过该接口下的统计信息, 则显示Never)
Last 300 seconds input rate: 0 bytes/sec, 0 bits/sec, 0 packets/sec	最近300秒钟的平均输入速率 (只有接口支持统计功能时才显示该信息): <ul style="list-style-type: none"> bytes/sec 表示平均每秒输入的字节数 bits/sec 表示平均每秒输入的比特数 packets/sec 表示平均每秒输入的包数
Last 300 seconds output rate: 0 bytes/sec, 0 bits/sec, 0 packets/sec	最近300秒钟的平均输出速率 (只有接口支持统计功能时才显示该信息): <ul style="list-style-type: none"> bytes/sec 表示平均每秒输出的字节数 bits/sec 表示平均每秒输出的比特数 packets/sec 表示平均每秒输出的包数
Input: 0 packets, 0 bytes, 0 drops	接口输入的报文数, 输入的字节数, 输入报文中丢弃的报文数 (只有接口支持统计功能时才显示这些信息)
Output: 0 packets, 0 bytes, 0 drops	接口输出的报文数, 输入的字节数, 输入报文中丢弃的报文数 (只有接口支持统计功能时才显示这些信息)

显示 LoopBack 接口的概要信息。

```
<Sysname> display interface loopback brief
Brief information on interfaces in route mode:
Link: ADM - administratively down; Stby - standby
Protocol: (s) - spoofing
Interface          Link Protocol Primary IP      Description
Loop1              UP    UP(s)    --          forLAN1
```

显示当前物理状态为 down 的 LoopBack 接口的信息以及 down 的原因。

```
<Sysname> display interface loopback brief down
Brief information on interfaces in route mode:
Link: ADM - administratively down; Stby - standby
Interface          Link Cause
Loop1              ADM  Administratively
```

表1-4 display interface loopback brief 命令显示信息描述表

字段	描述
Brief information on interfaces in route mode:	LoopBack接口的概要信息
Link: ADM - administratively down; Stby - standby	<ul style="list-style-type: none">如果某接口的 Link 属性值为“ADM”，则表示该接口被管理员通过 shutdown 命令关闭，需要在该接口下执行 undo shutdown 命令才能恢复接口本身的物理状态如果某接口的 Link 属性值为“Stby”，则表示该接口是一个处于 Standby 状态的备份接口
Protocol: (s) - spoofing	如果某接口的Protocol属性值中带有(s),则表示该接口的数据链路层协议状态显示为UP,但实际可能没有对应的链路,或者对应的链路不是永久存在而是按需建立的。通常NULL、LoopBack等接口会具有该属性
Interface	接口名称缩写
Link	接口物理连接状态，取值可能为： <ul style="list-style-type: none">UP：表示接口物理上是连通的DOWN：表示接口物理上不通ADM：表示接口被管理员通过 shutdown 命令关闭，需要执行 undo shutdown 命令才能恢复接口本身的物理状态Stby：表示该接口是一个处于 Standby 状态的备份接口
Protocol	接口数据链路层协议状态，取值为UP(s)
Primary IP	接口主IP地址
Description	接口的描述信息
Cause	接口物理连接状态为down的原因，取值为Administratively时，表示本链路被手工关闭了（配置了 shutdown 命令），需要执行 undo shutdown 命令才能恢复真实的物理状态

【相关命令】

- **interface loopback**
- **reset counters interface loopback**

1.1.6 display interface null

display interface null 命令用来显示 NULL 接口的相关信息。

【命令】

display interface null [0] [**brief** [**description** | **down**]]

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator

【参数】

0: NULL 接口的编号。

brief: 显示接口的概要信息。不指定该参数时，将显示接口的详细信息。

description: 用来显示用户配置的接口的全部描述信息。如果某接口的描述信息超过 27 个字符，不指定该参数时，只显示描述信息中的前 27 个字符，超出部分不显示；指定该参数时，可以显示全部描述信息。

down: 显示当前物理状态为 **down** 的接口的信息以及 **down** 的原因。不指定该参数时，将不会根据接口物理状态来过滤显示信息。

【使用指导】

因为设备只支持一个 Null 接口 Null0，所以不管是否指定 **0** 参数，显示的都是 Null0 的相关信息。

【举例】

显示指定接口 NULL0 的相关信息。

```
<Sysname> display interface null 0
NULL0
Current state: UP
Line protocol state: UP(spoofing)
Description: NULL0 Interface
Bandwidth: 1000000 kbps
Maximum transmission unit: 1500
Internet protocol processing: Disabled
Physical: NULL DEV
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
```

显示 NULL 接口的概要信息。

```
<Sysname> display interface null 0 brief
Brief information on interfaces in route mode:
Link: ADM - administratively down; Stby - standby
Protocol: (s) - spoofing
Interface          Link Protocol Primary IP      Description
```

NULL0 UP UP(s) --

display interface null命令显示信息描述请参见 [表 1-3](#)和 [表 1-4](#)。

【相关命令】

- **interface null**
- **reset counters interface null**

1.1.7 interface loopback

interface loopback 命令用来创建 LoopBack 接口，并进入 LoopBack 接口视图。如果指定的 LoopBack 接口已经存在，则直接进入该 LoopBack 接口视图

undo interface loopback 命令用来删除指定的 LoopBack 接口。

【命令】

```
interface loopback interface-number  
undo interface loopback interface-number
```

【缺省情况】

不存在 LoopBack 接口。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

interface-number: LoopBack 接口的编号，取值范围为 0~127。

【使用指导】

LoopBack 接口创建后，物理层和链路层永远处于 up 状态，除非手工关闭该接口。因此，使用 LoopBack 接口建立连接，能够避免连接受接口物理状态的影响，从而提高连接的可靠性。比如，将 LoopBack 接口作为建立 FTP 连接时的源接口。

【举例】

```
# 创建接口 LoopBack1。  
<Sysname> system-view  
[Sysname] interface loopback 1  
[Sysname-LoopBack1]
```

1.1.8 interface null

interface null 命令用来进入 NULL 接口的视图。

【命令】

```
interface null 0
```

【缺省情况】

设备只支持一个 NULL 接口——NULL0，用户不能创建也不能删除。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

0: NULL 接口的编号。

【举例】

```
# 进入接口 NULL0 的视图。  
<Sysname> system-view  
[Sysname] interface null 0  
[Sysname-NULL0]
```

1.1.9 reset counters interface loopback

reset counters interface loopback 命令用来清除 LoopBack 接口的统计信息。

【命令】

```
reset counters interface loopback [ interface-number ]
```

【视图】

用户视图

【缺省用户角色】

network-admin

【参数】

interface-number: 逻辑接口编号。如果不指定该参数，则清除所有 LoopBack 接口的统计信息。

【使用指导】

如果要统计一定时间内接口的流量来判断接口和链路工作是否正常，可以使用该命令先清除接口原有的统计信息，然后让接口自动重新统计。

只有创建 LoopBack 接口后，才支持该命令。

【举例】

```
# 清除接口 LoopBack1 的统计信息。  
<Sysname> reset counters interface loopback 1
```

【相关命令】

- **display interface loopback**

1.1.10 reset counters interface null

reset counters interface null 命令用来清除 NULL 接口的统计信息。

【命令】

```
reset counters interface null [ 0 ]
```

【视图】

用户视图

【缺省用户角色】

network-admin

【参数】

0: NULL 接口的编号。

【使用指导】

如果要统计一定时间内接口的流量来判断接口工作是否正常，可以使用该命令先清除接口原有的统计信息，然后让接口自动重新统计。

【举例】

清除接口 NULL0 的统计信息。

```
<Sysname> reset counters interface null 0
```

【相关命令】

- **display interface null**

1.1.11 shutdown

shutdown 命令用来关闭 LoopBack 接口。

undo shutdown 命令用来开启 LoopBack 接口。

【命令】

```
shutdown
```

```
undo shutdown
```

【缺省情况】

LoopBack 接口处于开启状态。

【视图】

LoopBack 接口视图

【缺省用户角色】

network-admin

【使用指导】

执行 **shutdown** 命令会导致使用该接口建立的链路中断，不能通信，请谨慎使用。

【举例】

关闭接口 LoopBack1。

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

```
[Sysname] interface loopback 1
```

```
[Sysname-LoopBack1] shutdown
```

目 录

1 接口批量配置.....	1-1
1.1 接口批量配置命令.....	1-1
1.1.1 display interface range.....	1-1
1.1.2 interface range.....	1-1
1.1.3 interface range name.....	1-3

1 接口批量配置

1.1 接口批量配置命令

1.1.1 display interface range

display interface range 命令用来显示通过 **interface range name** 命令创建的批量接口的信息。

【命令】

```
display interface range [ name name ]
```

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator

【参数】

name name: 设备上已创建的批量接口的别名，为 1~32 个字符的字符串，区分大小写。不指定该参数时，显示当前设备中所有通过 **interface range name** 命令已创建的批量接口的信息。

【举例】

显示当前设备中所有通过 **interface range name** 命令创建的批量接口的信息。

```
<Sysname> display interface range  
Interface range name t2 GigabitEthernet1/0/1 GigabitEthernet1/0/2  
Interface range name test GigabitEthernet1/0/3 GigabitEthernet1/0/4
```

以上显示信息表明：批量接口 **t2** 下绑定了接口 **GigabitEthernet1/0/1** 和 **GigabitEthernet1/0/2**，批量接口 **test** 下绑定了接口 **GigabitEthernet1/0/3** 和 **GigabitEthernet1/0/4**。

【相关命令】

- **interface range name**

1.1.2 interface range

interface range 命令用来绑定一组接口，并进入接口批量配置视图。

【命令】

```
interface range interface-list
```

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

interface-list: 接口列表, 表示方式为 *interface-list* = { *interface-type interface-number1* [**to** *interface-type interface-number2*] }&<1-24>。其中 *interface-type interface-number* 表示接口类型和接口编号。&<1-24>表示前面的参数最多可以输入 24 次。*interface-type interface-number2* 的值要大于等于 *interface-type interface-number1* 的值。

【使用指导】

当多个接口需要配置某功能（比如 **shutdown**）时，需要逐个进入接口视图，在每个接口执行一遍命令，比较繁琐。**interface range** 命令提供了一种批量配置方式。使用该命令可以将不同类型的接口进行绑定，并进入接口批量配置视图。

在接口批量配置视图下，只能执行接口列表中第一个接口支持的命令，不能执行第一个接口不支持但其它成员接口支持的命令。（接口列表中的第一个接口指的是执行 **interface range** 命令时指定的接口按照字母序从小到大排序后的第一个接口）。在接口批量配置视图下，输入问号并回车，将显示该视图下支持的所有命令。

在接口批量配置视图下执行命令，会在绑定的所有接口下执行该命令：

- 当命令执行完成后，系统提示配置失败并保持在接口批量配置视图。
 - 如果配置失败的接口是接口列表的第一个接口，则表示列表中的所有接口都未配置该命令。
 - 如果配置失败的接口是其它接口，则表示除了提示失败的接口外，其它接口都已经配置成功。
- 如果命令执行完成后，退回到系统视图，则表示：
 - 接口视图和系统视图下都支持该命令。
 - 在列表中的某个接口上配置失败，在系统视图下配置成功。
 - 列表中位于这个接口后面的接口不再执行该命令。

此时，可到列表中各接口的视图下使用 **display this** 命令验证配置效果，同时如果不需要在系统视图下配置该命令的话，请使用相应的 **undo** 命令取消该配置。

在接口批量配置视图下，执行 **display this** 命令，将显示接口列表中第一个接口当前生效的配置。

批量配置接口时有如下限制：

- 设置为接口列表的第一个接口之前，需要确保可以通过 **interface interface-type interface-number** 命令进入该接口视图。
- 聚合口加入批量接口时，建议不要将该聚合口的成员接口也加入，否则在批量接口配置视图下执行某些配置命令时，可能会导致聚合分裂。
- 批量接口包含的接口数量没有上限，仅受系统资源限制。接口数量较多时，在批量接口配置视图下执行命令等待的时间将较长。

【举例】

关闭接口 GigabitEthernet1/0/1 到 GigabitEthernet1/0/5。

```
<Sysname> system-view
[Sysname] interface range gigabitethernet 1/0/1 to gigabitethernet 1/0/5
[Sysname-if-range] shutdown
```

1.1.3 interface range name

interface range name *name* **interface** *interface-list* 命令用来绑定一组接口，为这组接口指定一个别名，并使用该别名进入接口批量配置视图。

interface range name *name*（不带 **interface** 参数时）命令用来使用别名进入接口批量配置视图。

undo interface range name 命令用来取消接口绑定，删除接口别名。

【命令】

```
interface range name name [ interface interface-list ]  
undo interface range name name
```

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

name：批量接口的别名，为 1~32 个字符的字符串，区分大小写。

interface-list：接口列表，表示方式为 *interface-list* = { *interface-type* *interface-number* [**to** *interface-type* *interface-number*] }<1-24>。其中 *interface-type* *interface-number* 表示接口类型和接口编号。<1-24>表示前面的参数最多可以输入 24 次。*interface-type* *interface-number2* 的值要大于等于 *interface-type* *interface-number1* 的值。

【使用指导】

interface range name 和 **interface range** 命令都能提供接口批量配置功能，它们的差别在于：**interface range name** 命令在绑定接口的时候可以定义一个别名，可以进行多次绑定，给不同的绑定定义不同的别名，以示区别，方便记忆。并且，后续可以使用别名直接进入接口批量配置视图，不再需要输出一长串的接口列表，配置起来更简便。用户可以使用 **display interface range** 命令来查看绑定了哪些接口。

在接口批量配置视图下，只能执行接口列表中第一个接口支持的命令，不能执行第一个接口不支持但其它成员接口支持的命令。（接口列表中的第一个接口指的是执行 **interface range** 命令时指定的接口按照字母序从小到大排序后的第一个接口）。在接口批量配置视图下，输入问号并回车，将显示该视图下支持的所有命令。

在接口批量配置视图下执行命令，会在绑定的所有接口下执行该命令：

- 当命令执行完成后，系统提示配置失败并保持在接口批量配置视图。
 - 如果配置失败的接口是接口列表的第一个接口，则表示列表中的所有接口都没有配置该命令。
 - 如果配置失败的接口是其它接口，则表示除了提示失败的接口外，其它接口都已经配置成功。
- 如果命令执行完成后，退回到系统视图，则表示：
 - 在接口视图和系统视图下都支持该命令。

- 在列表中的某个接口上配置失败，在系统视图下配置成功。
- 列表中位于这个接口后面的接口不再执行该命令。

此时，可到列表中各接口的视图下使用 **display this** 命令验证配置效果，同时如果不需要在系统视图下配置该命令的话，请使用相应的 **undo** 命令取消该配置。

在接口批量配置视图下，执行 **display this** 命令，将显示接口列表中第一个接口当前生效的配置。

批量配置接口时有如下限制：

- 设置为接口列表的第一个接口之前，需要确保可以通过 **interface interface-type interface-number** 命令进入该接口视图。
- 聚合口加入批量接口时，建议不要将该聚合口的成员接口也加入，否则在批量接口配置视图下执行某些配置命令时，可能会导致聚合分裂。
- 批量接口包含的接口数量没有上限，仅受系统资源限制。接口数量较多时，在批量接口配置视图下执行命令等待的时间将较长。
- 系统中支持的批量接口别名的个数没有上限，仅受系统资源限制。推荐用户配置 1000 个以下，配置数量过多，可能引起该特性执行效率降低。

【举例】

将 5 个以太网接口 GigabitEthernet1/0/1～GigabitEthernet1/0/5 定义为 myEthPort，并进入批量接口视图。

```
<Sysname> system-view
[Sysname] interface range name myEthPort interface gigabitethernet 1/0/1 to gigabitethernet 1/0/5
[Sysname-if-range-myEthPort]
```

进入 myEthPort 别名对应的批量接口配置视图。

```
<Sysname> system-view
[Sysname] interface range name myEthPort
[Sysname-if-range-myEthPort]
```

【相关命令】

- **display interface range**

目 录

1 MAC地址表	1-1
1.1 MAC地址表配置命令	1-1
1.1.1 display mac-address	1-1
1.1.2 display mac-address aging-time.....	1-2
1.1.3 display mac-address mac-learning	1-3
1.1.4 display mac-address mac-move.....	1-4
1.1.5 display mac-address statistics	1-5
1.1.6 mac-address (interface view)	1-6
1.1.7 mac-address (system view)	1-7
1.1.8 mac-address mac-learning enable.....	1-9
1.1.9 mac-address mac-move fast-update	1-11
1.1.10 mac-address max-mac-count.....	1-11
1.1.11 mac-address max-mac-count enable-forwarding.....	1-12
1.1.12 mac-address notification mac-move	1-13
1.1.13 mac-address notification mac-move suppression (interface view)	1-14
1.1.14 mac-address notification mac-move suppression (system view)	1-14
1.1.15 mac-address timer	1-15
1.1.16 snmp-agent trap enable mac-address.....	1-16
2 MAC Information	2-1
2.1 MAC Information配置命令	2-1
2.1.1 mac-address information enable (interface view)	2-1
2.1.2 mac-address information enable (system view)	2-1
2.1.3 mac-address information interval.....	2-2
2.1.4 mac-address information mode.....	2-3
2.1.5 mac-address information queue-length.....	2-3

1 MAC地址表

1.1 MAC地址表配置命令

1.1.1 display mac-address

display mac-address 命令用来显示 MAC 地址表信息。

【命令】

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

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator

【参数】

mac-address: 显示指定 MAC 地址的 MAC 地址表项, *mac-address* 的格式为 H-H-H。在配置时, 用户可以省去 MAC 地址中每段开头的“0”, 例如输入“f-e2-1”即表示输入的 MAC 地址为“000f-00e2-0001”。

vlan *vlan-id*: 显示指定 VLAN 的 MAC 地址表项。*vlan-id* 的取值范围为 1~4094。

dynamic: 显示动态 MAC 地址表项。

static: 显示静态 MAC 地址表项。

interface *interface-type* *interface-number*: 显示指定接口的 MAC 地址表项。*interface-type* *interface-number* 为接口类型和接口编号。

blackhole: 显示黑洞 MAC 地址表项。

multiport: 显示多端口单播 MAC 地址表项。

count: 显示 MAC 地址表项的数量。如果配置本参数, 将仅显示符合条件的 (由 **count** 前面的参数决定) MAC 地址表项的数量, 而不显示 MAC 地址表项的具体内容。如果不指定本参数, 则显示符合条件的 MAC 地址表的具体内容。

【使用指导】

使用本命令可以查看静态、动态、黑洞和多端口单播 MAC 地址表项, 表项内容主要包括 MAC 地址、VLAN ID、接口等信息。

如果不指定任何参数, 将显示所有的 MAC 地址表项信息。

对于聚合接口, 需要有选中端口, 该聚合接口对应的动态 MAC 地址才能在 MAC 地址表项中显示。多端口单播 MAC 地址表项不影响对应 MAC 地址的动态学习, 对于同一 MAC 地址, 多端口单播 MAC 地址表项和动态 MAC 地址表项可以同时存在, 优先根据多端口单播 MAC 地址转发报文。

【举例】

显示 VLAN 100 的 MAC 地址表项的信息。

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

MAC Address	VLAN ID	State	Port/Nickname	Aging
0001-0101-0101	100	Multiport	GE1/0/1	N
			GE1/0/2	
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

显示 MAC 地址表项的数量。

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

表1-1 display mac-address 命令显示信息描述表

字段	描述
MAC Address	MAC地址
VLAN ID	MAC地址对应接口所属的VLAN
State	MAC地址表项的状态，包括： <ul style="list-style-type: none">• Static: 表示该表项是静态 MAC 地址表项• Learned: 动态 MAC 地址表项。可以手工配置也可以由设备学习获得• Blackhole: 表示该表项是黑洞 MAC 地址表项• Multiport: 表示该表项是多端口单播 MAC 地址表项• OpenFlow: 表示该表项是 OpenFlow 实例的 MAC 地址表项
Port/Nickname	MAC地址对应的接口名称
Aging	老化时间，该表项有两种取值： <ul style="list-style-type: none">• Y: 表示该表项会被老化• N: 表示该表项不会被老化
<i>n</i> mac address(es) found	共有 <i>n</i> 个MAC地址表项

【相关命令】

- **mac-address**
- **mac-address timer**

1.1.2 display mac-address aging-time

display mac-address aging-time 命令用来显示 MAC 地址表动态表项的老化时间。

【命令】

display mac-address aging-time

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator

【举例】

显示 MAC 地址表中动态表项的老化时间。
<Sysname> display mac-address aging-time
MAC address aging time: 300s.

【相关命令】

- `mac-address timer`

1.1.3 display mac-address mac-learning

`display mac-address mac-learning` 命令用来显示 MAC 地址学习功能的开启状态。

【命令】

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

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator

【参数】

`interface interface-type interface-number`: 显示指定接口的 MAC 地址学习状态。
`interface-type interface-number` 为接口类型和接口编号。如果不指定本参数，则显示全局和所有接口的 MAC 地址学习状态。

【举例】

显示全局和所有接口的 MAC 地址学习状态。
<Sysname> display mac-address mac-learning
Global MAC address learning status: Enabled.

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

表1-2 display mac-address mac-learning 命令显示信息描述表

字段	描述
Global MAC address learning status	全局的MAC地址学习状态：Enabled为开启， Disabled为禁止
Port	接口名称
Learning Status	接口的MAC地址学习状态：Enabled为开启， Disabled为禁止

【相关命令】

- `mac-address mac-learning enable`

1.1.4 display mac-address mac-move

`display mac-address mac-move` 命令用来显示设备启动后的 MAC 地址迁移记录。

【命令】

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

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator

【参数】

slot slot-number: 显示指定成员设备上的 MAC 地址迁移记录, *slot-number* 表示设备在 IRF 中的成员编号。如果未指定本参数, 则显示所有成员设备上的 MAC 地址迁移记录。

【使用指导】

如果 MAC 地址迁移频繁出现, 且同一 MAC 地址总是在特定的两个接口之间迁移, 那么网络中可能存在二层环路。可以通过查看 MAC 地址迁移记录, 发现和定位环路。

在迁移记录中, 如果 MAC 地址、VLAN、源端口、新端口都一样, 则视作一条表项。

每个成员设备最多能生成 200 条最近发生的 MAC 地址迁移记录。

【举例】

显示指定 slot 上的 MAC 地址迁移记录。

```
<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  ---
```

显示所有 slot 上的 MAC 地址迁移记录。

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

表1-3 display mac-address mac-move 命令显示信息描述表

字段	描述
MAC address	MAC地址
VLAN	MAC地址对应接口所属的VLAN
Current port	MAC地址迁移新接口
Source port	MAC地址迁移源接口
Last time	发生MAC地址迁移的最近一次时间
Times	设备启动后，MAC地址发生迁移的次数。对于同一MAC地址，仅当字段VLAN、Current port和Source port都相同时，次数才加1

【相关命令】

- `mac-address notification mac-move`

1.1.5 display mac-address statistics

`display mac-address statistics` 命令用来显示 MAC 地址表的统计信息。

【命令】

`display mac-address statistics`

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator

【使用指导】

本命令主要显示系统目前存在的各类 MAC 地址表项的数目、以及系统可以支持的各类表项的最大规格。

【举例】

显示 MAC 地址表中的统计信息。

```
<Sysname> display mac-address statistics
MAC Address Count:
Dynamic Unicast Address (Learned) Count:           3
Dynamic Unicast Address (Security-service-defined) Count: 4
Static Unicast Address (User-defined) Count:         0
Static Unicast Address (System-defined) Count:       3
Total Unicast MAC Addresses In Use:                  10
Total Unicast MAC Addresses Available:                16384
Multicast and Multiport MAC Address Count:           1
Static Multicast and Multiport MAC Address (User-defined) Count: 1
Total Multicast and Multiport MAC Addresses Available: 256
```

表1-4 display mac-address statistic 命令显示信息描述表

字段	描述
Dynamic Unicast Address (Learned) Count	报文触发添加的动态单播MAC地址统计
Dynamic Unicast Address (Security-service-defined) Count	安全服务触发添加的动态单播MAC地址统计
Static Unicast Address (User-defined) Count	用户添加的静态单播MAC地址统计
Static Unicast Address (System-defined) Count	系统添加的静态单播MAC地址统计
Total Unicast MAC Addresses In Use	单播MAC地址统计
Total Unicast MAC Addresses Available	单播MAC地址规格
Multicast and Multiport MAC Address Count	组播和多端口单播MAC地址统计
Static Multicast and Multiport MAC Address (User-defined) Count	用户添加的静态组播和多端口单播MAC地址统计
Total Multicast and Multiport MAC Addresses Available	组播和多端口单播MAC地址规格

1.1.6 mac-address (interface view)

mac-address 命令用来在接口下添加或者修改 MAC 地址表项。

undo mac-address 命令用来删除接口下的 MAC 地址表项。

【命令】

```
mac-address { dynamic | multiport | static } mac-address vlan vlan-id
undo mac-address { dynamic | multiport | static } mac-address vlan vlan-id
```

【缺省情况】

接口下未配置任何 MAC 地址表项。

【视图】

二层以太网接口视图

二层聚合接口视图

【缺省用户角色】

network-admin

【参数】

dynamic: 动态 MAC 地址表项。

static: 静态 MAC 地址表项。

multiport: 多端口单播 MAC 地址表项。当报文的目的 MAC 地址与多端口单播 MAC 地址表项匹配时，将该报文从多个端口复制转发出去。

mac-address: MAC 地址，格式为 H-H-H，不支持组播 MAC 地址、全 0 的 MAC 地址和全 F 的 MAC 地址。在配置时，用户可以省去 MAC 地址中每段开头的“0”，例如输入“f-e2-1”即表示输入的 MAC 地址为“000f-00e2-0001”。

vlan vlan-id: 当前接口所属的 VLAN。vlan-id 为指定 VLAN 的编号，取值范围为 1~4094。该 VLAN 必须已经创建。

【使用指导】

一般情况下，设备通过源 MAC 地址学习过程自动建立 MAC 地址表。为了提高接口安全性，网络管理员可手工在 MAC 地址表中加入特定 MAC 地址表项，将用户设备与接口绑定，从而防止非法用户骗取数据。手工配置的静态 MAC 地址表项优先级高于自动生成的表项。

如果不保存配置，设备重启后所有表项都会丢失；如果保存配置，静态 MAC 地址表项不会丢失，动态 MAC 地址表项会丢失。

【举例】

在端口 GigabitEthernet1/0/1 下增加静态 MAC 地址表项 000f-e201-0101，该端口属于 VLAN 2。

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

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

```
[Sysname-GigabitEthernet1/0/1] mac-address static 000f-e201-0101 vlan 2
```

在接口 Bridge-Aggregation1 下增加静态 MAC 地址表项 000f-e201-0102，该接口属于 VLAN 1。

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

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

```
[Sysname-Bridge-Aggregation1] mac-address static 000f-e201-0102 vlan 1
```

在端口 GigabitEthernet1/0/1 和 GigabitEthernet1/0/2 下增加多端口单播 MAC 地址表项 0001-0001-0101，两个端口均属于 VLAN 2。

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

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

```
[Sysname-GigabitEthernet1/0/1] mac-address multiport 0001-0001-0101 vlan 2
```

```
[Sysname-GigabitEthernet1/0/1] quit
```

```
[Sysname] interface gigabitethernet 1/0/2
```

```
[Sysname-GigabitEthernet1/0/2] mac-address multiport 0001-0001-0101 vlan 2
```

【相关命令】

- **display mac-address**
- **mac-address** (system view)

1.1.7 mac-address (system view)

mac-address 命令用来添加或者修改 MAC 地址表项。

undo mac-address 命令用来删除 MAC 地址表项。

【命令】

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

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

```
mac-address multiport mac-address interface interface-list 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
undo mac-address multiport mac-address interface interface-list vlan
vlan-id
undo mac-address [ multiport ] [ [ mac-address ] vlan vlan-id ]
```

【缺省情况】

未配置任何 MAC 地址表项。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

dynamic: 动态 MAC 地址表项。

static: 静态 MAC 地址表项。

blackhole: 黑洞 MAC 地址表项。当报文的源 MAC 地址或目的 MAC 地址与黑洞 MAC 地址表项匹配时，该报文被丢弃。

multiport: 多端口单播 MAC 地址表项。当报文的目的 MAC 地址与多端口单播 MAC 地址表项匹配时，将该报文从多个端口复制转发出去。

mac-address: MAC 地址，格式为 H-H-H，不支持组播 MAC 地址、全 0 的 MAC 地址和全 F 的 MAC 地址。在配置时，用户可以省去 MAC 地址中每段开头的“0”，例如输入“f-e2-1”即表示输入的 MAC 地址为“000f-00e2-0001”。

vlan vlan-id: 指定接口所属的 VLAN。**vlan-id** 为指定 VLAN 的编号，取值范围为 1~4094。该 VLAN 必须已经创建。

interface interface-type interface-number: 出接口。**interface-type interface-number** 为接口类型和接口编号。

interface interface-list: 接口列表，表示方式为 **interface-list** = { **interface-type interface-number1** [**to interface-type interface-number2**] } <1-4>。其中，**interface-type interface-number** 为接口类型和接口编号，目前只支持二层以太网接口及二层聚合接口。**interface-type interface-number2** 的值要大于等于 **interface-type interface-number1** 的值。<1-4>表示前面的参数最多可以输入 4 次。

【使用指导】

通过本命令可以添加或者修改如下类型的 MAC 地址表项：

动态 MAC 地址：设备通过源 MAC 地址学习过程自动建立 MAC 地址表或者由用户手工配置。

静态 MAC 地址：为了提高接口安全性，网络管理员可手工在 MAC 地址表中加入特定 MAC 地址表项，将用户设备与接口绑定，从而防止非法用户骗取数据。手工配置的静态 MAC 地址表项优先级高于自动生成的表项。

黑洞 MAC 地址：用于丢弃指定源 MAC 地址或目的 MAC 地址的报文。

多端口单播 MAC 地址：用于目的是某个 MAC 地址的报文从多个端口复制转发出去。第一次执行命令配置某一 MAC 地址表项时，添加该表项，再次执行命令配置除接口外其余相同的 MAC 地址表项时，则会为该表项添加一个或多个接口。

用户手工配置的静态 MAC 地址表项或黑洞 MAC 地址表项不会被动态 MAC 地址表项覆盖，而动态 MAC 地址表项可以被静态 MAC 地址表项和黑洞 MAC 地址表项覆盖。

删除 MAC 地址表项时，需要注意：

- 执行 **undo mac-address** 命令时若不指定任何参数，将删除所有单播 MAC 地址表项和静态组播 MAC 地址表项。
- 可以删除指定 VLAN 的所有 MAC 地址表项（包括单播 MAC 地址表项和静态组播 MAC 地址表项）；可以选择删除动态 MAC 地址表项、静态 MAC 地址表项、黑洞 MAC 地址表项或者多端口单播 MAC 地址表项；可以按接口删除单播 MAC 地址表项，但不能按接口删除组播 MAC 地址表项。

如果不保存配置，设备重启后所有表项都会丢失；如果保存配置，静态 MAC 地址表项、黑洞 MAC 地址表项和多端口单播 MAC 地址表项不会丢失，动态表项会丢失。

【举例】

添加静态地址表项，目的 MAC 地址为 000f-e201-0101，出接口为 GigabitEthernet1/0/1，且该接口属于 VLAN 2。

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

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

添加多端口单播 MAC 地址表项，目的 MAC 地址为 000f-e201-0101，出接口为 GigabitEthernet1/0/1、GigabitEthernet1/0/2 和 GigabitEthernet1/0/3，且出接口属于 VLAN 2。

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

```
[Sysname] mac-address multiport 000f-e201-0101 interface gigabitethernet 1/0/1 to  
gigabitethernet 1/0/3 vlan 2
```

【相关命令】

- **display mac-address**
- **mac-address** (interface view)

1.1.8 mac-address mac-learning enable

mac-address mac-learning enable 命令用来打开设备全局、接口或者 VLAN 的 MAC 地址学习功能。

undo mac-address mac-learning enable 命令用来关闭设备全局、接口或者 VLAN 的 MAC 地址学习功能。

【命令】

```
mac-address mac-learning enable
```

```
undo mac-address mac-learning enable
```

【缺省情况】

MAC 地址学习功能处于开启状态。

【视图】

系统视图

二层以太网接口视图

二层聚合接口视图

VLAN 视图

【缺省用户角色】

network-admin

【使用指导】

有时为了保证设备的安全，需要关闭 MAC 地址学习功能。常见的危及设备安全的情况是：非法用户使用大量源 MAC 地址不同的报文攻击设备，导致设备 MAC 地址表资源耗尽，造成设备无法根据网络的变化更新 MAC 地址表。关闭 MAC 地址学习功能可以有效防止这种攻击。

关闭 MAC 地址学习功能时，需要注意：

- 关闭 MAC 地址学习功能后，设备就学不到新地址，从而影响设备及时刷新 MAC 地址表。用户可以根据实际情况关闭接口的 MAC 地址学习功能。
- 关闭全局的 MAC 地址学习功能后，接口将不再学习新的 MAC 地址。
- 关闭 MAC 地址学习功能可能会导致广播，因此在关闭接口的 MAC 地址学习功能的同时，一般还要使用接口广播风暴抑制功能。有关广播风暴抑制功能的介绍，请参见“接口管理配置指导”中的“以太网接口”。
- 在开启全局的 MAC 地址学习功能的前提下，用户可以关闭设备上单个接口或指定 VLAN 的 MAC 地址学习功能。
- 关闭 MAC 地址学习功能后，设备立即删除已经存在的动态 MAC 地址表项。

【举例】

关闭全局 MAC 地址学习功能。

```
<Sysname> system-view
[Sysname] undo mac-address mac-learning enable
```

关闭 VLAN 10 的 MAC 地址学习功能。

```
<Sysname> system-view
[Sysname] vlan 10
[Sysname-vlan10] undo mac-address mac-learning enable
```

关闭端口 GigabitEthernet1/0/1 的 MAC 地址学习功能。

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

关闭接口 Bridge-Aggregation1 的 MAC 地址学习功能。

```
<Sysname> system-view
[Sysname] interface bridge-aggregation 1
[Sysname-Bridge-Aggregation1] undo mac-address mac-learning enable
```

【相关命令】

- **display mac-address mac-learning**

1.1.9 mac-address mac-move fast-update

mac-address mac-move fast-update 命令用来开启在 MAC 地址迁移后，快速更新 ARP 表项的功能。

undo mac-address mac-move fast-update 命令用来关闭在 MAC 地址迁移后，快速更新 ARP 表项的功能。

【命令】

```
mac-address mac-move fast-update
undo mac-address mac-move fast-update
```

【缺省情况】

在 MAC 地址迁移后，快速更新 ARP 表项的功能处于关闭状态。

【视图】

系统视图

【缺省用户角色】

network-admin

【举例】

开启在 MAC 地址迁移后，快速更新 ARP 表项的功能。

```
<Sysname> system-view
[Sysname] mac-address mac-move fast-update
```

1.1.10 mac-address max-mac-count

mac-address max-mac-count 命令用来配置接口的 MAC 地址数学习上限。

undo mac-address max-mac-count 命令用来恢复缺省情况。

【命令】

```
mac-address max-mac-count count
undo mac-address max-mac-count
```

【缺省情况】

接口未配置 MAC 地址数学习上限。

【视图】

二层以太网接口视图

【缺省用户角色】

network-admin

【参数】

count: 接口的 MAC 地址数学习上限，为 0 即表示不允许该接口学习 MAC 地址。取值范围为 0~4096。

【使用指导】

通过配置接口的 MAC 地址数学习上限，用户可以控制设备维护的 MAC 地址表的表项数量。如果 MAC 地址表过于庞大，可能导致设备的转发性能下降。当接口学习到的 MAC 地址数达到上限时，该接口将不再对 MAC 地址进行学习。

【举例】

```
# 配置端口 GigabitEthernet1/0/1 的 MAC 地址数学习上限为 600。
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] mac-address max-mac-count 600
```

【相关命令】

- **mac-address**
- **mac-address max-mac-count enable-forwarding**

1.1.11 mac-address max-mac-count enable-forwarding

mac-address max-mac-count enable-forwarding 命令用来配置当达到接口的 MAC 地址数学习上限时，允许转发源 MAC 地址不在 MAC 地址表里的报文。

undo mac-address max-mac-count enable-forwarding 命令用来配置当达到接口的 MAC 地址数学习上限时，禁止转发源 MAC 地址不在 MAC 地址表里的报文。

【命令】

```
mac-address max-mac-count enable-forwarding
undo mac-address max-mac-count enable-forwarding
```

【缺省情况】

当达到接口的 MAC 地址数学习上限时，允许转发源 MAC 地址不在 MAC 地址表里的报文。

【视图】

二层以太网接口视图

【缺省用户角色】

network-admin

【举例】

```
# 配置端口 GigabitEthernet1/0/1 的 MAC 地址数学习上限为 600，当端口学习的 MAC 地址数达到 600 时，禁止转发源 MAC 地址不在 MAC 地址表里的报文。
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] mac-address max-mac-count 600
[Sysname-GigabitEthernet1/0/1] undo mac-address max-mac-count enable-forwarding
```

【相关命令】

- **mac-address**
- **mac-address max-mac-count**

1.1.12 mac-address notification mac-move

mac-address notification mac-move 命令用来开启 MAC 地址迁移上报功能。

undo mac-address notification mac-move 命令用来关闭 MAC 地址迁移上报功能。

【命令】

```
mac-address notification mac-move [ interval interval ]  
undo mac-address notification mac-move
```

【缺省情况】

MAC 地址迁移上报功能处于关闭状态。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

interval interval: MAC 地址迁移检测周期，取值范围为 1~60，单位为分钟。如果未指定该参数，将采用缺省 MAC 地址迁移检测周期 1 分钟。

【使用指导】

开启 MAC 地址迁移上报功能后，当系统检测到地址迁移，会按照 MAC 地址迁移检测周期的间隔记录上一个 MAC 地址迁移检测周期内发生的 MAC 地址迁移日志，包括 MAC 地址、该 MAC 地址所在 VLAN ID、MAC 地址迁移源接口和新接口，以及该 MAC 地址在一个 MAC 地址迁移检测周期内的迁移次数。

一个 MAC 地址迁移检测周期内，每台成员设备最多能生成 20 条 MAC 地址的迁移日志，并且按迁移次数降序排列。该检测周期内，当新生成的迁移日志的迁移次数超过已存在的迁移日志的迁移次数时，迁移次数最小的迁移日志会被丢弃，新的迁移日志按迁移次数降序排列。等到下一个检测周期，上一个检测周期的所有日志信息将被丢弃，重新开始生成迁移日志。

执行本命令后，系统采用 Syslog 方式上报 MAC 地址迁移信息到信息中心模块，如果同时通过 **snmp-agent trap enable mac-address** 命令开启 MAC 地址表的告警功能，系统还会采用 Trap 信息上报 MAC 地址迁移信息到 SNMP 模块。

【举例】

开启 MAC 地址迁移上报功能。

```
<Sysname> system-view  
[Sysname] mac-address notification mac-move  
[Sysname]  
%May 14 17:16:45:688 2013 Sysname MAC/4/MAC_NOTIFICATION: MAC address 0000-0012-0034 in VLAN 500 has moved from port GE1/0/1 to port GE1/0/2 for 1 times
```

以上显示信息表明：MAC 地址 0000-0012-0034 所在 VLAN ID 为 500，MAC 地址迁移源接口为 GigabitEthernet1/0/1，MAC 地址迁移新接口为 GigabitEthernet1/0/2，该 MAC 地址在一个 MAC 地址迁移检测周期内的迁移次数为 1。

【相关命令】

- `display mac-address mac-move`

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

`mac-address notification mac-move suppression` 命令用来开启接口上的 MAC 地址迁移抑制功能。

`undo mac-address notification mac-move suppression` 命令用来关闭接口上的 MAC 地址迁移抑制功能。

【命令】

`mac-address notification mac-move suppression`

`undo mac-address notification mac-move suppression`

【缺省情况】

MAC 地址迁移抑制功能处于关闭状态。

【视图】

二层以太网接口视图

二层聚合接口视图

【缺省用户角色】

network-admin

【使用指导】

开启 MAC 地址迁移抑制功能后，当监测到一个 MAC 地址迁移检测周期内某个 MAC 地址从某端口上迁移出或者迁移到该端口的次数超过 MAC 地址迁移抑制的检测阈值，则将该端口 down，用户可以执行命令 `shutdown` 和 `undo shutdown` 将该端口恢复，也可以等 MAC 地址迁移抑制时间间隔后让该端口自行恢复 up。

MAC 地址迁移抑制功能使端口 down 后，系统将发送日志信息到信息中心模块，如果设备开启了 MAC 地址表的告警功能（`snmp-agent trap enable mac-address` 命令），系统还会发送告警信息到设备的 SNMP 模块。

【举例】

开启 MAC 地址迁移抑制功能。

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

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

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

【相关命令】

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

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

`mac-address notification mac-move suppression` 命令用来配置 MAC 地址迁移抑制功能的相关参数。

`undo mac-address notification mac-move suppression` 命令用来恢复缺省情况。

【命令】

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

【缺省情况】

MAC 地址迁移抑制功能的相关参数未配置，采用缺省抑制时间间隔 30 秒和缺省阈值 3 次。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

interval interval: MAC 地址迁移抑制时间间隔（检测攻击后，端口保持 down 状态的持续时间），取值范围为 30~86400，单位为秒。如果未指定该参数，将采用缺省抑制时间间隔 30 秒。
threshold threshold: MAC 地址迁移抑制的检测阈值（一个 MAC 地址迁移检测周期内允许 MAC 地址迁移的最大的迁移次数），取值范围为 0~1024。如果未指定该参数，将采用缺省阈值 3 次。

【使用指导】

配置本命令后，当接口上开启了 MAC 地址迁移抑制功能时，本命令配置的参数才能生效。

本命令可多次配置，配置 **interval interval** 和 **threshold threshold** 时互不影响。

【举例】

配置 MAC 地址迁移抑制功能的抑制间隔为 40s，检测阈值为 1。

```
<Sysname> system-view  
[Sysname] mac-address notification mac-move suppression interval 40  
[Sysname] mac-address notification mac-move suppression threshold 1
```

【相关命令】

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

1.1.15 mac-address timer

mac-address timer 命令用来配置动态 MAC 地址表项的老化时间。

undo mac-address timer 命令用来恢复缺省情况。

【命令】

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

【缺省情况】

动态 MAC 地址表项的老化时间为 300 秒。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

aging seconds: 动态 MAC 地址表项的老化时间，取值范围为 10~630，单位为秒。

no-aging: 不老化。

【使用指导】

用户配置的老化时间过长或者过短，都可能影响设备的运行性能：

- 如果用户配置的老化时间过长，设备可能会保存许多过时的 MAC 地址表项，从而耗尽 MAC 地址表资源，导致设备无法根据网络的变化更新 MAC 地址表。
- 如果用户配置的老化时间太短，设备可能会删除有效的 MAC 地址表项，可能导致设备广播大量的数据报文，影响设备的运行性能。

所以用户需要根据实际情况，配置合适的老化时间来有效的实现 MAC 地址老化功能。

【举例】

配置动态 MAC 地址表项的老化时间为 500 秒。

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

```
[Sysname] mac-address timer aging 500
```

【相关命令】

- **display mac-address aging-time**

1.1.16 snmp-agent trap enable mac-address

snmp-agent trap enable mac-address 命令用来开启 MAC 地址表的告警功能。

undo snmp-agent trap enable mac-address 命令用来关闭 MAC 地址表的告警功能。

【命令】

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

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

【缺省情况】

MAC 地址表的告警功能处于开启状态。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

mac-move: 打开 MAC 地址表模块的 MAC 地址迁移上报的告警功能。如果未指定该参数，则表示打开 MAC 地址模块所有的告警功能。

【使用指导】

开启 MAC 地址表的告警功能后，MAC 地址表模块会生成告警信息，用于报告该模块的重要事件。生成的告警信息将发送到设备的 SNMP 模块，请通过设置 SNMP 中告警信息的发送参数，来决定告警信息输出的相关属性。

关闭 MAC 地址表的告警功能后，设备将只发送日志信息到信息中心模块，此时请配置信息中心的输出规则和输出方向来查看 MAC 地址表模块的日志信息。

有关 SNMP 和信息中心的详细介绍，请参见“网络管理和监控配置指导”中的“SNMP”和“信息中心”。

目前 MAC 地址表模块仅有 MAC 地址迁移上报的告警功能，所以打开或关闭 MAC 地址迁移上报的告警功能，就相当于打开或关闭 MAC 地址表所有的告警功能。

【举例】

关闭 MAC 地址迁移的告警功能。

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

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

【相关命令】

- **mac-address notification mac-move**

2 MAC Information

2.1 MAC Information配置命令

2.1.1 mac-address information enable (interface view)

mac-address information enable 命令用来开启接口的 MAC Information 功能。

undo mac-address information enable 命令用来关闭接口的 MAC Information 功能。

【命令】

```
mac-address information enable { added | deleted }  
undo mac-address information enable { added | deleted }
```

【缺省情况】

接口的 MAC Information 功能处于关闭状态。

【视图】

二层以太网接口视图

【缺省用户角色】

network-admin

【参数】

added: 表示配置接口在学习到新的 MAC 地址时记录 MAC 变化信息。

deleted: 表示配置接口在删除 MAC 地址时记录 MAC 变化信息。

【使用指导】

必须同时开启全局和接口的 MAC Information 功能，MAC Information 功能才会生效。

【举例】

开启端口 GigabitEthernet1/0/1 的 MAC Information 功能，使端口在学习到新的 MAC 时记录 MAC 变化信息。

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

【相关命令】

- **mac-address information enable (system view)**

2.1.2 mac-address information enable (system view)

mac-address information enable 命令用来开启全局 MAC Information 功能。

undo mac-address information enable 命令用来关闭全局 MAC Information 功能。

【命令】

```
mac-address information enable
```

```
undo mac-address information enable
```

【缺省情况】

全局 MAC Information 功能处于关闭状态。

【视图】

系统视图

【缺省用户角色】

network-admin

【使用指导】

必须同时开启全局和接口的 MAC Information 功能，MAC Information 功能才会生效。

【举例】

开启全局 MAC Information 功能。

```
<Sysname> system-view  
[Sysname] mac-address information enable
```

【相关命令】

- `mac-address information enable` (interface view)

2.1.3 mac-address information interval

`mac-address information interval` 命令用来配置发送 MAC 变化通知的时间间隔。

`undo mac-address information interval` 命令用来恢复缺省情况。

【命令】

```
mac-address information interval interval  
undo mac-address information interval
```

【缺省情况】

发送 MAC 变化通知的时间间隔为 1 秒。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

interval: 发送 MAC 变化通知的时间间隔，取值范围为 1~20000，单位为秒。

【使用指导】

为了防止过于频繁发送的 MAC 变化通知干扰用户，可以将此时间间隔调整为较大值。

【举例】

配置设备发送 MAC 变化通知的时间间隔为 200 秒。

```
<Sysname> system-view  
[Sysname] mac-address information interval 200
```


2.1.4 mac-address information mode

mac-address information mode 命令用来配置发送 MAC 变化通知的方式。

undo mac-address information mode 命令用来恢复缺省情况。

【命令】

```
mac-address information mode { syslog | trap }  
undo mac-address information mode
```

【缺省情况】

采用 Trap 方式发送 MAC 变化通知。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

syslog: 表示采用 Syslog 方式发送 MAC 变化通知。

trap: 表示采用 Trap 方式发送 MAC 变化通知。

【举例】

```
# 配置设备采用 Trap 方式发送 MAC 变化通知。  
<Sysname> system-view  
[Sysname] mac-address information mode trap
```

2.1.5 mac-address information queue-length

mac-address information queue-length 命令用来配置 MAC Information 缓存队列长度。

undo mac-address information queue-length 命令用来恢复缺省情况。

【命令】

```
mac-address information queue-length value  
undo mac-address information queue-length
```

【缺省情况】

MAC Information 缓存队列长度为 50。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

value: MAC Information 缓存队列长度，取值范围为 0~1000，表示可存放的 MAC 地址变化信息条数。

【使用指导】

如果 MAC Information 缓存队列长度为 0，则当接口学习到或删除掉一条 MAC 地址时会立即发送日志或 SNMP 告警信息。

如果 MAC Information 缓存队列长度不为 0，则将 MAC 地址变化信息存放在缓存队列中。当未达到发送 MAC 变化通知的时间间隔，此时若缓存队列被写满，新的 MAC 地址变化信息将覆盖缓存队列中最后一条写入的信息；当达到发送 MAC 变化通知的时间间隔时，不论此时缓存队列是否已被写满，都发送日志或 SNMP 告警信息。

【举例】

配置 MAC Information 缓存队列长度为 600。

```
<Sysname> system-view  
[Sysname] mac-address information queue-length 600
```

目 录

1 以太网链路聚合.....	1-1
1.1 以太网链路聚合配置命令.....	1-1
1.1.1 bandwidth	1-1
1.1.2 default.....	1-1
1.1.3 description	1-2
1.1.4 display interface	1-2
1.1.5 display lacp system-id.....	1-6
1.1.6 display link-aggregation load-sharing mode.....	1-7
1.1.7 display link-aggregation member-port.....	1-8
1.1.8 display link-aggregation summary	1-10
1.1.9 display link-aggregation verbose	1-12
1.1.10 interface bridge-aggregation	1-14
1.1.11 jumboframe enable.....	1-15
1.1.12 lacp edge-port	1-16
1.1.13 lacp mode	1-16
1.1.14 lacp period short	1-17
1.1.15 lacp select speed	1-18
1.1.16 lacp system-priority	1-18
1.1.17 link-aggregation bfd ipv4.....	1-19
1.1.18 link-aggregation global load-sharing mode.....	1-20
1.1.19 link-aggregation lacp traffic-redirect-notification enable.....	1-21
1.1.20 link-aggregation load-sharing mode local-first.....	1-22
1.1.21 link-aggregation mode.....	1-22
1.1.22 link-aggregation port-priority	1-23
1.1.23 link-aggregation selected-port maximum	1-24
1.1.24 link-aggregation selected-port minimum	1-24
1.1.25 port bridge enable	1-25
1.1.26 port link-aggregation group	1-26
1.1.27 reset counters interface	1-27
1.1.28 reset lacp statistics	1-27
1.1.29 shutdown	1-28

1 以太网链路聚合

1.1 以太网链路聚合配置命令

1.1.1 bandwidth

bandwidth 命令用来配置接口的期望带宽。

undo bandwidth 命令用来恢复缺省情况。

【命令】

bandwidth *bandwidth-value*

undo bandwidth

【缺省情况】

接口的期望带宽 = 接口的波特率 ÷ 1000 (kbps)。

【视图】

二层聚合接口视图

【缺省用户角色】

network-admin

【参数】

bandwidth-value: 表示接口的期望带宽，取值范围为 1~400000000，单位为 kbps。

【使用指导】

期望带宽供业务模块使用，不会对接口实际带宽造成影响。

【举例】

配置二层聚合接口 1 的期望带宽为 10000kbps。

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

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

```
[Sysname-Bridge-Aggregation1] bandwidth 10000
```

1.1.2 default

default 命令用来恢复聚合接口的缺省配置。

【命令】

default

【视图】

二层聚合接口视图

【缺省用户角色】

network-admin

【使用指导】



注意

接口下的某些配置取消后，会对现有功能产生影响，建议您在执行该命令前，完全了解其对网络产生的影响。

您可以在执行 **default** 命令后通过 **display this** 命令确认执行效果。对于未能成功恢复缺省的配置，建议您查阅相关功能的命令手册，手工执行恢复该配置缺省情况的命令。如果操作仍然不能成功，您可以通过设备的提示信息定位原因。

【举例】

将二层聚合接口 1 恢复为缺省配置。

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

1.1.3 description

description 命令用来配置接口的描述信息。

undo description 命令用来恢复缺省情况。

【命令】

```
description text
undo description
```

【缺省情况】

接口的描述信息为“接口名 Interface”，比如接口 Bridge-Aggregation1 的缺省描述信息为：Bridge-Aggregation1 Interface。

【视图】

二层聚合接口视图

【缺省用户角色】

network-admin

【参数】

text：表示接口的描述信息，为 1~255 个字符的字符串，区分大小写。

【举例】

配置二层聚合接口 1 的描述信息为“connect to the lab”。

```
<Sysname> system-view
[Sysname] interface bridge-aggregation 1
[Sysname-Bridge-Aggregation1] description connect to the lab
```

1.1.4 display interface

display interface 命令用来显示聚合接口的相关信息。

【命令】

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

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator

【参数】

bridge-aggregation: 显示二层聚合接口的相关信息。

interface-number: 表示聚合接口的编号，取值范围为已创建的聚合接口的编号。

brief: 显示接口的概要信息。如果未指定该参数，将显示接口的详细信息。

description: 用来显示用户配置的接口的全部描述信息。如果某接口的描述信息超过 27 个字符，不指定该参数时，只显示描述信息中的前 27 个字符，超出部分不显示；指定该参数时，可以显示全部描述信息。

down: 显示当前物理状态为 down 的接口的信息以及 down 的原因。不指定该参数时，将不会根据接口物理状态来过滤显示信息。

【使用指导】

如果未指定聚合接口的类型，将显示设备支持的所有接口的相关信息。

如果指定了聚合接口的类型而未指定聚合接口编号，将显示所有已创建的该类型聚合接口的相关信息。

【举例】

显示二层聚合接口 1 的详细信息。

```
<Sysname> display interface bridge-aggregation 1  
Bridge-Aggregation1  
Current state: UP  
IP packet frame type: Ethernet II, hardware address: 000f-e207-f2e0  
Description: Bridge-Aggregation1 Interface  
Bandwidth: 1000 kbps  
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 seconds input: 6900 packets/sec 885160 bytes/sec 0%  
Last 300 seconds 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

```

显示二层聚合接口 1 的概要信息。

```

<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

```

表1-1 display interface 命令显示信息描述表

字段	描述
Bridge-Aggregation1	二层聚合接口名
Current state	接口的状态： <ul style="list-style-type: none"> Administratively DOWN: 表示该接口已被 shutdown 命令关闭，其管理状态为关闭 DOWN: 表示该接口的管理状态为开启，但其物理状态为关闭（可能由于没有物理连线或线路故障） UP: 表示该接口的管理状态和物理状态均为开启
IP packet frame type	IPv4报文帧格式
hardware address	接口的MAC地址
Description	接口的描述信息
Bandwidth	接口的期望带宽值，当该参数的取值为0时，不显示该参数
Port priority	接口优先级
Unknown-speed mode, unknown-duplex mode	接口的速率和双工模式均未知
Link speed type is autonegotiation, link duplex type is autonegotiation	接口的速率和双工模式都是通过自协商确定的
PVID	接口缺省VLAN的编号
Port link-type	接口的链路类型，取值可能为access、trunk或hybrid
Tagged VLANs	通过该接口后携带Tag的VLAN
Untagged VLANs	通过该接口后不再携带Tag的VLAN

字段	描述
Last clearing of counters	最后一次使用 reset counters interface 命令清除接口统计信息的时间。如果从设备启动一直没有执行 reset counters interface 命令清除过该接口下的统计信息，则显示 Never
Last 300 seconds input/output rate	接口在最近300秒接收/发送报文的平均速率
Input/Output (total)	接口接收/发送的全部报文的统计值
Input/Output (normal)	接口接收/发送的正常报文的统计值
Line protocol state	接口数据链路层协议状态： <ul style="list-style-type: none"> UP DOWN
Maximum transmission unit	接口的最大传输单元
Brief information on interfaces in bridge mode	二层接口的概要信息
Link: ADM - administratively down; Stby - standby	接口的物理连接状态： <ul style="list-style-type: none"> ADM：表示该接口已被管理员通过 shutdown 命令关闭，在该接口下执行 undo shutdown 命令才能恢复其物理状态 Stby：表示该接口是一个处于 Standby 状态的备份接口
Speed: (a) - auto	如果某接口的 Speed 属性值为“(a)”，则表示该接口的速率是通过自动协商获取的 如果某接口的 Speed 属性值为“auto”，则表示该接口的速率是通过自动协商获取的，但协商还未开始
Duplex: (a)/A - auto; H - half; F - full	接口的双工模式： <ul style="list-style-type: none"> (a)/A：表示双工模式都是通过自协商确定的 H：表示双工模式为半双工 F：表示双工模式为全双工
Type: A - access; T - trunk; H - hybrid	接口的链路类型： <ul style="list-style-type: none"> A：表示 Access 类型 H：表示 Hybrid 类型 T：表示 Trunk 类型
Protocol: (s) - spoofing	如果某接口的 Protocol 属性值中带有“(s)”字符串，则表示该接口的数据链路层协议状态显示为UP，但实际可能没有对应的链路，或者对应的链路不是永久存在而是按需建立的
Interface	接口名称的缩写
Link	接口物理连接状态，取值为： <ul style="list-style-type: none"> UP：表示接口物理上是连通的 DOWN：表示接口物理上是不通的 ADM：表示接口被管理员通过 shutdown 命令关闭，需要执行 undo shutdown 命令才能恢复接口本身的物理状态 Stby：表示该接口是一个处于 Standby 状态的备份接口

字段	描述
Speed	接口的速率（单位为bps）
Duplex	接口的双工模式
Type	接口的链路类型 <ul style="list-style-type: none"> • A: 表示 Access 链路类型 • H: 表示 Hybrid 链路类型 • T: 表示 Trunk 链路类型
Protocol	接口数据链路层协议状态，取值为： <ul style="list-style-type: none"> • UP: 表示接口的数据链路层协议状态为开启 • DOWN: 表示接口的数据链路层协议状态为关闭 • UP(s): 表示接口的数据链路层协议状态显示为 UP，但实际可能没有对应的链路，或者对应的链路不是永久存在而是按需建立的
Cause	接口物理连接状态为down的原因

1.1.5 display lacp system-id

display lacp system-id 命令用来显示本端系统的设备 ID。

【命令】

display lacp system-id

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator

【使用指导】

使用 **lacp system-priority** 命令可以改变系统的 LACP 优先级，但通过该命令输入的是十进制的优先级数值。而当使用 **display lacp system-id** 命令显示时，系统会自动将其转换为十六进制的优先级数值。

【举例】

显示本端系统的设备 ID。

```
<Sysname> display lacp system-id
Actor System ID: 0x8000, 0000-fc00-6504
```

表1-2 display lacp system-id 命令显示信息描述表

字段	描述
Actor System ID: 0x8000, 0000-fc00-6504	本端系统的设备ID（由系统的LACP优先级和系统的MAC地址共同构成）：系统的LACP优先级为0x8000，系统的MAC地址为0000-FC00-6504

【相关命令】

- `lacp system-priority`

1.1.6 display link-aggregation load-sharing mode

display link-aggregation load-sharing mode 命令用来显示全局或聚合组内采用的聚合负载分担类型。

【命令】

display link-aggregation load-sharing mode [**interface** [**bridge-aggregation** *interface-number*]]

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator

【参数】

bridge-aggregation: 显示二层聚合接口所对应聚合组内采用的聚合负载分担类型。

interface-number: 聚合接口的编号。必须是当前已经创建的聚合接口编号。

【使用指导】

如果未指定参数 **interface**，则显示全局采用的聚合负载分担类型。

如果仅指定参数 **interface** 而未指定具体的聚合接口类型，则显示所有聚合接口所对应聚合组内采用的聚合负载分担类型。

只有在设备上创建了二层聚合接口之后，才能指定 **bridge-aggregation** 参数。

【举例】

显示全局采用的聚合负载分担类型（缺省情况）。

```
<Sysname> display link-aggregation load-sharing mode
Link-aggregation load-sharing mode:
Layer 2 traffic: packet type-based sharing
Layer 3 traffic: packet type-based sharing
```

显示全局采用的聚合负载分担类型（非缺省情况）。

```
<Sysname> display link-aggregation load-sharing mode
Link-aggregation load-sharing mode:
destination-mac address, source-mac address
```

显示二层聚合接口 10 所对应聚合组内采用的聚合负载分担类型（缺省情况）。

```
<Sysname> display link-aggregation load-sharing mode interface bridge-aggregation 10
Bridge-Aggregation10 load-sharing mode:
Layer 2 traffic: packet type-based sharing
Layer 3 traffic: packet type-based sharing
```

显示二层聚合接口 10 所对应聚合组内采用的聚合负载分担类型（非缺省情况）。

```
<Sysname> display link-aggregation load-sharing mode interface bridge-aggregation 10
Bridge-Aggregation10 load-sharing mode:
destination-mac address, source-mac address
```

表1-3 display link-aggregation load-sharing mode 命令显示信息描述表

字段	描述
Link-aggregation load-sharing mode	全局采用的聚合负载分担类型： <ul style="list-style-type: none"> 缺省情况下显示：二层报文、三层报文采用的聚合负载分担类型 非缺省情况下显示：用户配置后采用的聚合负载分担类型
Bridge-Aggregation10 load-sharing mode	二层聚合接口10所对应聚合组内采用的聚合负载分担类型： <ul style="list-style-type: none"> 缺省情况下显示：全局采用的聚合负载分担类型 非缺省情况下显示：用户配置后采用的聚合负载分担类型
Layer 2 traffic: packet type-based sharing	二层报文缺省采用的聚合负载分担类型：按照源IP地址、目的IP地、源MAC地址和目的MAC地址进行负载分担
Layer 3 traffic: packet type-based sharing	三层报文缺省采用的聚合负载分担类型：按照源IP地址、目的IP地、源MAC地址和目的MAC地址进行负载分担
destination-mac address, source-mac address	用户配置后采用的聚合负载分担类型：按照源MAC地址和目的MAC地址进行负载分担

1.1.7 display link-aggregation member-port

display link-aggregation member-port 命令用来显示成员端口上链路聚合的详细信息。

【命令】

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

【视图】

任意视图

【缺省用户角色】

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

【参数】

interface-list: 成员端口列表，表示一个或多个成员端口。表示方式为 **interface-list = interface-type interface-number1 [to interface-type interface-number2]**。其中，**interface-type** 为接口类型，**interface-number1** 和 **interface-number2** 为接口编号。**interface-number2** 的值要大于等于 **interface-number1** 的值。

auto: 显示所有半自动聚合成员端口的链路聚合的详细信息。

【使用指导】

由于静态聚合组无法获知对端信息，因此静态聚合组只显示本端的端口编号、端口优先级和操作 Key 的值。

【举例】

显示静态聚合组内成员端口 **GigabitEthernet1/0/1** 上链路聚合的详细信息。

```
<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

显示动态聚合组内成员端口 **GigabitEthernet1/0/2** 上链路聚合的详细信息。

```
<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-Aggregation10

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)

显示动态聚合组内所有半自动聚合的成员端口上链路聚合的详细信息。

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

GigabitEthernet1/0/3:

Preference Aggregation Interface: Bridge-Aggregation11

Aggregate Interface: Bridge-Aggregation11

Local:

Port Number: 3

Port Priority: 32768

Oper-Key: 1

```

Flag: {ACDEF}
Remote:
  System ID: 0x8000, a057-75a2-0100
  Port Number: 3
  Port Priority: 32768
  Oper-Key: 1
  Flag: {ACDEF}
Received LACP Packets: 3 packet(s)
Illegal: 0 packet(s)
Sent LACP Packets: 6 packet(s)

```

表1-4 display link-aggregation member-port 命令显示信息描述表

字段	描述
Flags	<p>LACP协议的状态标识，长度为1字节，该字节自低位至高位分别以英文字母A~H表示，某一位为1时打印出对应的英文字母，为0时不打印对应的英文字母。各标志位的含义如下：</p> <ul style="list-style-type: none"> A: LACP 是否开启标志。1 表示开启；0 表示关闭 B: LACP 长/短超时标志。1 表示短超时；0 表示长超时 C: 发送端认为本成员端口所在链路是否可聚合。1 表示是；0 表示否 D: 发送端认为本成员端口所在链路是否处于同步状态。1 表示是；0 表示否 E: 发送端认为本成员端口所在链路是否处于收集状态。1 表示是；0 表示否 F: 发送端认为本成员端口所在链路是否处于分发状态。1 表示是；0 表示否 G: 发送端的接收状态机是否处于默认状态。1 表示是；0 表示否 H: 发送端的接收状态机是否处于超时状态。1 表示是；0 表示否
Aggregate Interface	本成员端口所属的聚合接口
Preferred Aggregate Interface	半自动聚合优先选择加入的聚合口
Local	本端信息
Port Number	端口的编号
Port Priority	端口优先级
Oper-key	操作Key的值
Flag	LACP协议的状态标志值
Remote	对端信息
System ID	设备ID（由系统的LACP优先级和系统的MAC地址共同构成）
Received LACP Packets	收到的LACP报文总数
Illegal	非法报文的总数
Sent LACP Packets	发出的LACP报文总数

1.1.8 display link-aggregation summary

display link-aggregation summary 命令用来显示所有聚合组的摘要信息。

【命令】

display link-aggregation summary

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator

【使用指导】

由于静态聚合组无法获知对端信息，因此静态聚合组的对端信息显示为 **None**，并不代表对端系统的实际信息。

【举例】

显示所有聚合组的摘要信息。

```
<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 Interface	AGG Mode	Partner ID	Selected Ports	Unselected Ports	Individual Ports	Share Type
BAGG20	D	0x8000,00e0-fcfe-ff01	2	0	0	Shar

表1-5 display link-aggregation summary 命令显示信息描述表

字段	描述
Aggregate Interface Type	聚合接口类型： <ul style="list-style-type: none">• BAGG：表示二层聚合接口• RAGG：表示三层聚合接口
Aggregation Mode	聚合组类型： <ul style="list-style-type: none">• S：表示静态聚合• D：表示动态聚合
Loadsharing Type	负载分担类型： <ul style="list-style-type: none">• Shar：表示负载分担类型• NonS：表示非负载分担类型
Actor System ID	本端的设备ID（由系统的LACP优先级和系统的MAC地址共同构成）
AGG Interface	聚合接口的类型和编号
AGG Mode	聚合组的类型
Partner ID	对端的设备ID（由系统的LACP优先级和系统的MAC地址共同构成）

字段	描述
Selected Ports	处于选中状态的成员端口数量
Unselected Ports	处于非选中状态的成员端口数量
Individual Ports	处于独立状态的成员端口数量
Share Type	负载分担类型

1.1.9 display link-aggregation verbose

display link-aggregation verbose 命令用来显示已有聚合接口所对应聚合组的详细信息。

【命令】

display link-aggregation verbose [**bridge-aggregation** [*interface-number*]]

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator

【参数】

bridge-aggregation: 显示二层聚合接口所对应聚合组的详细信息。

interface-number: 聚合接口的编号。必须是当前已经创建的聚合接口编号。

【使用指导】

如果未指定聚合接口的类型，将显示设备支持的所有接口的相关信息。

如果仅指定了聚合接口的类型，将显示所有已创建的该类型聚合接口的相关信息。

只有在设备上创建了二层聚合接口之后，才能指定 **bridge-aggregation** 参数。

实际未加入任何聚合组的自动聚合端口不会被显示。

【举例】

二层聚合接口 10 所对应的聚合组是动态聚合组，显示该聚合组的详细信息。

```
<Sysname> display link-aggregation verbose bridge-aggregation 10
Loadsharing Type: Shar -- Loadsharing, NonS -- Non-Loadsharing
Port Status: S -- Selected, U -- Unselected, I -- Individual
Port: A -- Auto port, M -- Management port, R -- Reference port
Flags: A -- LACP_Activity, B -- LACP_Timeout, C -- Aggregation,
      D -- Synchronization, E -- Collecting, F -- Distributing,
      G -- Defaulted, H -- Expired

Aggregate Interface: Bridge-Aggregation10
Aggregation Mode: Dynamic
Loadsharing Type: Shar
Management VLANs: None
System ID: 0x8000, 000f-e267-6c6a
```

```

Local:
  Port          Status  Priority Index  Oper-Key  Flag
  GE1/0/1       S       32768   61       2         {ACDEF}
  GE1/0/2       S       32768   62       2         {ACDEF}
  GE1/0/3       S       32768   63       2         {AG}

Remote:
  Actor          Priority Index  Oper-Key SystemID  Flag
  GE1/0/1(R)     32768   111    2         0x8000, 000f-e267-57ad {ACDEF}
  GE1/0/2        32768   112    2         0x8000, 000f-e267-57ad {ACDEF}
  GE1/0/3        32768   113    0         0x8000, 0000-0000-0000 {DEF}

```

二层聚合接口 20 所对应的聚合组是静态聚合组，显示该聚合组的详细信息。

```

<Sysname> display link-aggregation verbose bridge-aggregation 20
Loadsharing Type: Shar -- Loadsharing, NonS -- Non-Loadsharing
Port Status: S -- Selected, U -- Unselected, I -- Individual
Port: A -- Auto port, M -- Management port, R -- Reference port
Flags:  A -- LACP_Activity, B -- LACP_Timeout, C -- Aggregation,
        D -- Synchronization, E -- Collecting, F -- Distributing,
        G -- Defaulted, H -- Expired

```

Aggregate Interface: Bridge-Aggregation20

Aggregation Mode: Static

Loadsharing Type: Shar

Management VLANs: None


```

  Port          Status  Priority Oper-Key
  GE1/0/1(R)    S       32768   1
  GE1/0/2       S       32768   1
  GE1/0/3       S       32768   1

```

表1-6 display link-aggregation verbose 命令显示信息描述表

字段	描述
Loadsharing Type	负载分担类型： <ul style="list-style-type: none"> Shar: 表示负载分担类型 NonS: 表示非负载分担类型
Port Status	端口状态： <ul style="list-style-type: none"> Selected: 表示处于选中状态 Unselected: 表示处于非选中状态 Individual: 表示处于独立状态
Port	端口类型： <ul style="list-style-type: none"> Auto port: 表示为该端口为自动端口 Management port: （暂不支持）表示该端口为管理端口 Reference port: 表示该端口为参考端口

字段	描述
Flags	<p>LACP协议的状态标志，长度为1字节，该字节自低位至高位分别以字母A~H表示，取值为1的标志位显示为对应的字母，取值为0的标志为不显示。各标志位的含义如下：</p> <ul style="list-style-type: none"> A: LACP 是否开启标志。1 表示开启；0 表示关闭 B: LACP 长/短超时标志。1 表示短超时；0 表示长超时 C: 发送端认为本成员端口所在链路是否可聚合。1 表示是；0 表示否 D: 发送端认为本成员端口所在链路是否处于同步状态。1 表示是；0 表示否 E: 发送端认为本成员端口所在链路是否处于收集状态。1 表示是；0 表示否 F: 发送端认为本成员端口所在链路是否处于分发状态。1 表示是；0 表示否 G: 发送端的接收状态机是否处于默认状态。1 表示是；0 表示否 H: 发送端的接收状态机是否处于超时状态。1 表示是；0 表示否
Aggregate Interface	聚合接口的名称
Aggregation Mode	<p>聚合组的工作模式：</p> <ul style="list-style-type: none"> Static: 表示静态聚合 Dynamic: 表示动态聚合
Management VLANs	（暂不支持）管理VLAN，未指定时显示None
System ID	设备ID（由系统的LACP优先级和系统的MAC地址共同构成）
Local	<p>本端信息：</p> <ul style="list-style-type: none"> Port: 端口的类型和编号 Status: 端口的选中/非选中/独立状态 Priority: 端口优先级 Index: 端口索引 Oper-Key: 操作 Key 的值 Flag: LACP 协议的状态标志值 <p> 说明 静态聚合组只显示本端信息，显示信息中不包括 Flag 字段</p>
Remote	<p>对端信息：</p> <ul style="list-style-type: none"> Actor: 本端的端口类型和编号，当对端端口是参考端口时，参考端口会显示在对应的本端端口上 Priority: 对端端口的端口优先级 Index: 对端端口的端口索引 Oper-Key: 对端端口的操作 Key 的值 System ID: 对端的设备 ID Flag: 对端的 LACP 协议的状态标志值

1.1.10 interface bridge-aggregation

interface bridge-aggregation 命令用来创建二层聚合接口，并进入二层聚合接口视图。如果指定的二层聚合接口已经存在，则直接进入该二层聚合接口视图。

undo interface bridge-aggregation 命令用来删除二层聚合接口。

【命令】

```
interface bridge-aggregation interface-number  
undo interface bridge-aggregation interface-number
```

【缺省情况】

不存在二层聚合接口。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

interface-number: 指定二层聚合接口的编号，取值范围为 1～1024。

【使用指导】

创建二层聚合接口后，系统将自动生成同编号的二层聚合组，且该聚合组缺省工作在静态聚合模式下。

删除二层聚合接口的同时会删除其对应的二层聚合组，如果该聚合组内有成员端口，那么这些成员端口将自动从该聚合组中退出。

【举例】

创建二层聚合接口 1，并进入二层聚合接口 1 的视图。

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

1.1.11 jumboframe enable

jumboframe enable 命令用来允许超长帧通过。

undo jumboframe enable 命令用来禁止超长帧通过。

undo jumboframe enable size 命令用来恢复缺省情况。

【命令】

```
jumboframe enable [ size ]  
undo jumboframe enable [ size ]
```

【缺省情况】

设备允许长度为 10240 字节的超长帧通过。

【视图】

二层聚合接口视图

【缺省用户角色】

network-admin

【参数】

size: 聚合接口上允许通过的超长帧的最大长度，取值范围为 1522～10240，单位为字节。

【使用指导】

多次执行本命令，最后一次执行的命令生效。

【举例】

```
# 允许超长帧通过二层聚合接口 1。
<Sysname> System-view
[Sysname] interface bridge-aggregation 1
[Sysname-Bridge-Aggregation1] jumboframe enable
```

1.1.12 lacp edge-port

lacp edge-port 命令用来配置聚合接口为聚合边缘接口。

undo lacp edge-port 命令用来恢复缺省情况。

【命令】

```
lacp edge-port
undo lacp edge-port
```

【缺省情况】

聚合接口不是聚合边缘接口。

【视图】

二层聚合接口视图

【缺省用户角色】

network-admin

【使用指导】

该命令主要用于在网络设备与服务器等终端设备相连的场景中。当网络设备配置了动态聚合模式，而终端设备未配置动态聚合模式时，网络设备的聚合成员端口都可以作为普通物理口转发报文，从而保证终端设备与网络设备间的多条链路可以相互备份，增加可靠性。

该配置仅在聚合接口对应的聚合组为动态聚合组时生效。

当聚合接口配置为聚合边缘接口后，聚合流量重定向功能将不能正常使用。

【举例】

```
# 配置二层聚合接口 1 为聚合边缘接口。
<Sysname> System-view
[Sysname] interface bridge-aggregation 1
[Sysname-Bridge-Aggregation1] lacp edge-port
```

1.1.13 lacp mode

lacp mode passive 命令用来配置端口的 LACP 工作模式为 PASSIVE。

undo lacp mode 命令用来恢复缺省情况。

【命令】

```
lacp mode passive
undo lacp mode
```

【缺省情况】

端口的 LACP 工作模式为 ACTIVE。

【视图】

二层以太网接口视图

【缺省用户角色】

network-admin

【使用指导】

执行本命令后，只有在当前端口为动态聚合组成员端口时，配置才生效。

如果动态聚合组内成员端口的 LACP 工作模式为 PASSIVE，且对端的 LACP 工作模式也为 PASSIVE 时，两端将不能发送 LACPDU。如果两端中任何一端的 LACP 工作模式为 ACTIVE 时，两端将可以发送 LACPDU。

【举例】

配置端口 GigabitEthernet1/0/1 的 LACP 工作模式为 PASSIVE。

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] lacp mode passive
```

1.1.14 lacp period short

lacp period short 命令用来配置端口的 LACP 超时时间为短超时（3 秒）。

undo lacp period 命令用来恢复缺省情况。

【命令】

```
lacp period short
undo lacp period
```

【缺省情况】

端口的 LACP 超时时间为长超时（90 秒）。

【视图】

二层以太网接口视图

【缺省用户角色】

network-admin

【举例】

配置端口 GigabitEthernet1/0/1 的 LACP 超时时间为短超时（3 秒）。

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] lacp period short
```

1.1.15 lacp select speed

lacp select speed 命令用来配置动态聚合组内端口速率作为优先选择参考端口的条件。

undo lacp select speed 命令用来恢复缺省情况。

【命令】

```
lacp select speed
undo lacp select speed
```

【缺省情况】

动态聚合组内以成员口的端口的端口 ID 作为优先选择参考端口的条件。

【视图】

二层聚合接口视图

【缺省用户角色】

network-admin

【使用指导】

缺省情况下，聚合组可能会将速率小的端口选择为参考端口。通过配置本命令，用户可以选择速率高的端口作为参考端口。

配置该命令前，需要在聚合接口视图下先执行 **link-aggregation mode dynamic** 命令配置该聚合接口为动态聚合接口，该命令才生效。静态聚合组可以配置该命令，但不生效。

本命令会改变动态聚合口的参考端口的选择条件，可能会导致短暂的业务中断。建议在业务正常传输情况下，不要随便更改参考端口的选择条件，需要修改参考端口的选择条件时，可以先关闭聚合接口，待两端配置一致后再开启该聚合接口。

【举例】

配置端口速率作为优先选择参考端口的条件。

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

1.1.16 lacp system-priority

lacp system-priority 命令用来配置系统的 LACP 优先级。

undo lacp system-priority 命令用来恢复缺省情况。

【命令】

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

【缺省情况】

系统的 LACP 优先级为 32768。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

priority: 系统的 LACP 优先级，取值范围为 0~65535。该数值越小，优先级越高。

【举例】

```
# 配置系统的 LACP 优先级为 64。
<Sysname> system-view
[Sysname] lacp system-priority 64
```

【相关命令】

- **link-aggregation port-priority**

1.1.17 link-aggregation bfd ipv4

link-aggregation bfd ipv4 命令用来开启链路聚合的 BFD 功能。

undo link-aggregation bfd 命令用来关闭链路聚合的 BFD 功能。

【命令】

```
link-aggregation bfd ipv4 source ip-address destination ip-address
undo link-aggregation bfd
```

【缺省情况】

链路聚合的 BFD 功能处于关闭状态。

【视图】

二层聚合接口视图

【缺省用户角色】

network-admin

【参数】

source ip-address: BFD 会话的源 IP 地址，不能为 0.0.0.0。

destination ip-address: BFD 会话的目的 IP 地址，不能为 0.0.0.0。

【使用指导】

聚合口两端的 BFD 会话源 IP 地址和目的 IP 地址必须成对配置，且源地址和目的地址为不同的单播地址。例如本端聚合接口配置 **link-aggregation bfd ipv4 source 1.1.1.1 destination 2.2.2.2** 时，对端聚合接口要配置 **link-aggregation bfd ipv4 source 2.2.2.2 destination 1.1.1.1** 后，才能正确建立起 BFD 会话。

在聚合接口下配置的 BFD 会话参数，会对该聚合组内所有选中链路的 BFD 会话生效，链路聚合的 BFD 会话不支持 echo 功能和查询模式。关于 BFD 的介绍和基本功能配置，请参见“可靠性配置指导”中的“BFD”。

开启链路聚合的 BFD 功能后，不建议在该聚合接口上再开启其他应用与 BFD 联动。

开启链路聚合的 BFD 功能后，请配置聚合组中的成员端口数量不大于设备支持的 BFD 会话数量，否则可能导致聚合组内部分选中端口变为非选中状态。

当聚合链路两端最大选中端口数量不一致时，如果在链路两端都开启链路聚合的 BFD 功能，则可能会导致两端 BFD 会话数量不一致，但并不影响报文转发。

【举例】

开启二层聚合接口 1 下的链路聚合的 BFD 功能，并配置 BFD 会话的源地址为 1.1.1.1，目的地址为 2.2.2.2。

```
<Sysname> system-view
[Sysname] interface bridge-aggregation 1
[Sysname-Bridge-Aggregation1] link-aggregation bfd ipv4 source 1.1.1.1 destination 2.2.2.2
```

1.1.18 link-aggregation global load-sharing mode

link-aggregation global load-sharing mode 命令用来配置全局采用的聚合负载分担类型。

undo link-aggregation global load-sharing mode 命令用来恢复缺省情况。

【命令】

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

【缺省情况】

系统按照源 IP 地址、目的 IP 地、源 MAC 地址和目的 MAC 地址进行负载分担。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

destination-ip: 表示按报文的目的 IP 地址进行聚合负载分担。

destination-mac: 表示按报文的目的 MAC 地址进行聚合负载分担。

destination-port: 表示按报文的目的服务端口进行聚合负载分担。

ingress-port: 表示按报文的入端口进行聚合负载分担。

source-ip: 表示按报文的源 IP 地址进行聚合负载分担。

source-mac: 表示按报文的源 MAC 地址进行聚合负载分担。

source-port: 表示按报文的源服务端口进行聚合负载分担。

【使用指导】

多次执行本命令，最后一次执行的命令生效。

对于设备不支持的聚合负载分担类型，系统将提示用户不支持。

目前，在系统视图下进行全局聚合负载分担类型配置，交换机只支持：

- 根据报文类型自动匹配负载分担类型；
- 根据源 IP 地址进行聚合负载分担；

- 根据目的 IP 地址进行聚合负载分担；
- 根据源 MAC 地址进行聚合负载分担；
- 根据目的 MAC 地址进行聚合负载分担；
- 根据报文入端口进行聚合负载分担；
- 根据源 IP 地址与目的 IP 地址进行聚合负载分担；
- 根据源 IP 地址与源端口进行聚合负载分担；
- 根据目的 IP 地址与目的端口进行聚合负载分担；
- 根据源 IP 地址、源端口、目的 IP 地址与目的端口进行聚合负载分担；
- 根据报文入端口、源 MAC 地址、目的 MAC 地址之间不同的组合进行聚合负载分担。

【举例】

配置全局按照报文目的 MAC 地址进行聚合负载分担。

```
<Sysname> system-view
[Sysname] link-aggregation global load-sharing mode destination-mac
```

【相关命令】

- **link-aggregation load-sharing mode**

1.1.19 link-aggregation lacp traffic-redirect-notification enable

link-aggregation lacp traffic-redirect-notification enable 命令用来开启聚合流量重定向功能。

undo link-aggregation lacp traffic-redirect-notification enable 命令用来关闭聚合流量重定向功能。

【命令】

```
link-aggregation lacp traffic-redirect-notification enable
undo link-aggregation lacp traffic-redirect-notification enable
```

【缺省情况】

聚合流量重定向功能处于关闭状态。

【视图】

系统视图
二层聚合接口视图

【缺省用户角色】

network-admin

【使用指导】

在开启了聚合流量重定向功能后，当手工关闭聚合组内某选中端口或重启聚合组内某选中端口所在的 slot 时，系统可以将该端口上的流量重定向到其他选中端口上，从而实现聚合链路上流量的不中断。聚合流量重定向过程中，对于聚合组中新选中的端口，流量不会重定向到该端口上。其中，已知单播报文可以实现零丢包，非已知单播报文不保证不丢包。

只有动态聚合组支持聚合流量重定向功能。

必须在聚合链路两端都开启聚合流量重定向功能才能实现聚合链路上流量的不中断。

如果同时开启聚合流量重定向功能和生成树功能，在重启 slot 时会出现少量的丢包，因此不建议同时开启上述两个功能。

当聚合接口配置为聚合边缘接口后，聚合流量重定向功能将不能正常使用。

全局的配置对所有聚合组都有效，而聚合组内的配置只对当前聚合组有效。对于一个聚合组来说，优先采用该聚合组内的配置，只有该聚合组内未进行配置时，才采用全局的配置。

建议优先选择开启聚合接口的聚合流量重定向功能。开启全局的聚合流量重定向功能时，如果有连接其它厂商设备的聚合接口，可能影响该聚合组的正常通信。

【举例】

开启聚合流量重定向功能。

```
<Sysname> system-view
[Sysname] link-aggregation lacp traffic-redirect-notification enable
```

1.1.20 link-aggregation load-sharing mode local-first

link-aggregation load-sharing mode local-first 命令用来配置聚合负载分担采用本地转发优先。

undo link-aggregation load-sharing mode local-first 命令用来取消聚合负载分担采用本地转发优先。

【命令】

```
link-aggregation load-sharing mode local-first
undo link-aggregation load-sharing mode local-first
```

【缺省情况】

聚合负载分担采用本地转发优先。

【视图】

系统视图

【缺省用户角色】

network-admin

【使用指导】

取消聚合负载分担采用本地转发优先后，从聚合接口转发的报文将在 IRF 所有成员设备的所有选中端口间进行负载分担。

【举例】

取消聚合负载分担采用本地转发优先。

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

1.1.21 link-aggregation mode

link-aggregation mode dynamic 命令用来配置聚合组工作在动态聚合模式下，同时开启 LACP 协议。

undo link-aggregation mode 命令用来恢复缺省情况。

【命令】

```
link-aggregation mode dynamic
undo link-aggregation mode
```

【缺省情况】

聚合组工作在静态聚合模式下。

【视图】

二层聚合接口视图

【缺省用户角色】

network-admin

【使用指导】

当聚合组中存在成员端口时，如果修改聚合组的工作模式，则可能导致聚合组中选中端口变为非选中状态，影响流量转发，请用户根据实际情况修改聚合组的工作模式。

【举例】

```
# 配置二层聚合接口 1 对应的聚合组工作在动态聚合模式下。
<Sysname> system-view
[Sysname] interface bridge-aggregation 1
[Sysname-Bridge-Aggregation1] link-aggregation mode dynamic
```

1.1.22 link-aggregation port-priority

link-aggregation port-priority 命令用来配置端口优先级。

undo link-aggregation port-priority 命令用来恢复缺省情况。

【命令】

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

【缺省情况】

端口优先级为 32768。

【视图】

二层以太网接口视图

【缺省用户角色】

network-admin

【参数】

priority: 端口优先级，取值范围为 0~65535。该数值越小，优先级越高。

【举例】

```
# 配置二层以太网接口 GigabitEthernet1/0/1 的端口优先级为 64。
<Sysname> system-view
```

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

【相关命令】

- **lacp system-priority**

1.1.23 link-aggregation selected-port maximum

link-aggregation selected-port maximum 命令用来配置聚合组中的最大选中端口数。
undo link-aggregation selected-port maximum 命令用来恢复缺省情况。

【命令】

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

【缺省情况】

聚合组中的最大选中端口数为 8。

【视图】

二层聚合接口视图

【缺省用户角色】

network-admin

【参数】

max-number: 聚合组中的最大选中端口数，取值范围为 1~8。

【使用指导】

执行本命令可能导致聚合组内部分成员端口变为非选中状态。

本端和对端配置的聚合组中的最大选中端口数必须一致。

当配置了聚合组中的最大选中端口数之后，最大选中端口数将同时受配置值和设备硬件能力的限制，即取二者的较小值作为限制值。

用户借此可实现两端口间的冗余备份：在一个聚合组中只添加两个成员端口，并配置该聚合组中的最大选中端口数为 1，这样这两个成员端口在同一时刻就只能有一个成为选中端口，而另一个将作为备份端口。

【举例】

配置二层聚合接口 1 对应的聚合组中的最大选中端口数为 5。

```
<Sysname> system-view
[Sysname] interface bridge-aggregation 1
[Sysname-Bridge-Aggregation1] link-aggregation selected-port maximum 5
```

【相关命令】

- **link-aggregation selected-port minimum**

1.1.24 link-aggregation selected-port minimum

link-aggregation selected-port minimum 命令用来配置聚合组中的最小选中端口数。

undo link-aggregation selected-port minimum 命令用来恢复缺省情况。

【命令】

```
link-aggregation selected-port minimum min-number  
undo link-aggregation selected-port minimum
```

【缺省情况】

聚合组中的最小选中端口数不受限制。

【视图】

二层聚合接口视图

【缺省用户角色】

network-admin

【参数】

min-number: 聚合组中的最小选中端口数，取值范围为 1~8。

【使用指导】

执行本命令可能导致聚合组内所有成员端口都变为非选中状态。

本端和对端配置的聚合组中的最小选中端口数必须一致。

【举例】

```
# 配置二层聚合接口 1 对应的聚合组中的最小选中端口数为 3。  
<Sysname> system-view  
[Sysname] interface bridge-aggregation 1  
[Sysname-Bridge-Aggregation1] link-aggregation selected-port minimum 3
```

【相关命令】

- **link-aggregation selected-port maximum**

1.1.25 port bridge enable

port bridge enable 命令用来开启二层聚合接口桥功能。

undo port bridge enable 命令用来关闭二层聚合接口桥功能。

【命令】

```
port bridge enable  
undo port bridge enable
```

【缺省情况】

二层聚合接口接口桥功能处于关闭状态。

【视图】

二层聚合接口视图

【缺省用户角色】

network-admin

【使用指导】

缺省情况下，设备收到报文后会根据报文特征查找报文出接口，如果该报文出接口和入接口为同一接口，则将报文丢弃。在二层聚合接口上开启本功能后，如果该报文出接口和入接口为同一接口，则从该接口转发报文。

【举例】

配置二层聚合接口 1 上开启接口桥功能。

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

1.1.26 port link-aggregation group

port link-aggregation group 命令用来将接口加入指定的聚合组。

undo port link-aggregation group 命令用来将接口从已加入的聚合组中删除。

【命令】

```
port link-aggregation group { group-id [ force ] | auto [ group-id ] }
undo port link-aggregation group
```

【缺省情况】

以太网接口未加入任何聚合组。

【视图】

二层以太网接口视图

【缺省用户角色】

network-admin

【参数】

group-id: 指定聚合组所对应聚合接口的编号，取值范围为 1~1024。

force: 表示接口加入聚合组时同步该聚合组的属性类配置。不指定该参数时，表示接口加入聚合组时不同步该聚合组的属性类配置。

auto: 开启端口的半自动聚合功能。

【使用指导】

一个接口只能加入一个聚合组。

指定 **force** 参数后，通过 **display current-configuration** 命令显示设备生效的配置中和配置文件中不会保存 **force** 参数。

仅指定 **auto** 参数时，表示根据对端发来的 LACP 报文决定加入哪个动态聚合组；如果未找到能够加入的聚合组，则创建一个符合条件的动态聚合组，并加入该聚合组中。

指定 **auto** 和 **group-id** 时，表示优先查看该聚合组参考端口所含的对端信息和收到的 LACP 报文中的对端信息是否一致：

- 如果相同则加入该聚合组。
- 如果不同，则再选择其他动态聚合组；如果未找到能够加入的动态聚合组，则创建一个符合条件的动态聚合组，并加入该聚合组中。

group-id 必须是已经存在的动态聚合组。

【举例】

将二层以太网接口 GigabitEthernet1/0/1 加入二层聚合组 1 中。

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

1.1.27 reset counters interface

reset counters interface 命令用来清除聚合接口上的统计信息。

【命令】

reset counters interface [**bridge-aggregation** [*interface-number*]]

【视图】

用户视图

【缺省用户角色】

network-admin

【参数】

bridge-aggregation: 清除二层聚合接口上的统计信息。

interface-number: 聚合接口的编号，取值范围为已创建的聚合接口的编号。

【使用指导】

在某些情况下，需要统计一定时间内某二层聚合接口的流量，这就需要在统计开始前清除该接口上原有的统计信息，以便重新进行统计。

如果未指定聚合接口的类型，将显示设备支持的所有接口的相关信息。

如果仅指定了聚合接口的类型，将显示所有已创建的该类型聚合接口的相关信息。

只有在设备上创建了二层聚合接口之后，才能指定 **bridge-aggregation** 参数。

【举例】

清除二层聚合接口 1 上的统计信息。

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

1.1.28 reset lacp statistics

reset lacp statistics 命令用来清除成员端口上的 LACP 统计信息。

【命令】

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

【视图】

用户视图

【缺省用户角色】

network-admin

【参数】

interface interface-list: 表示清除指定成员端口上的 LACP 统计信息。*interface-list* 为成员端口列表, 表示一个或多个成员端口。表示方式为 *interface-list* = *interface-type* *interface-number1* [**to** *interface-type* *interface-number2*]。其中, *interface-type* 为接口类型, *interface-number1* 和 *interface-number2* 为接口编号。*interface-number2* 的值要大于等于 *interface-number1* 的值。若未指定本参数, 则清除所有成员端口上的 LACP 统计信息。

【举例】

清除所有成员端口上的 LACP 统计信息。

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

【相关命令】

- **display link-aggregation member-port**

1.1.29 shutdown

shutdown 命令用来关闭接口。

undo shutdown 命令用来打开接口。

【命令】

```
shutdown
```

```
undo shutdown
```

【视图】

二层聚合接口视图

【缺省用户角色】

network-admin

【举例】

开启二层聚合接口 1。

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

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

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

目 录

1 端口隔离.....	1-1
1.1 端口隔离配置命令.....	1-1
1.1.1 display port-isolate group	1-1
1.1.2 port-isolate enable	1-2
1.1.3 port-isolate group.....	1-3

1 端口隔离

1.1 端口隔离配置命令

1.1.1 display port-isolate group

`display port-isolate group` 命令用来显示隔离组的信息。

【命令】

`display port-isolate group [group-id]`

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator

【参数】

`group-id`: 隔离组编号，取值范围为 1~8。

【举例】

显示所有隔离组的信息。

```
<Sysname> display port-isolate group
Port isolation group information:
Group ID: 1
Group members:
    GigabitEthernet1/0/1

Group ID: 5
Group members:
    GigabitEthernet1/0/2          GigabitEthernet1/0/4
```

显示隔离组 1 的信息。

```
<Sysname> display port-isolate group 1
Port isolation group information:
Group ID: 1
Group members:
    GigabitEthernet1/0/1
```

表1-1 display port-isolate group 命令显示信息描述表

字段	描述
Port isolation group information	端口隔离组的信息
Group ID	隔离组编号
Group members	隔离组中包含的成员端口，若显示为No ports表示没有成员端口

【相关命令】

- `port-isolate enable`

1.1.2 port-isolate enable

`port-isolate enable` 命令用来将端口加入到隔离组中。

`undo port-isolate enable` 命令用来将端口从隔离组中删除。

【命令】

`port-isolate enable group group-id`

`undo port-isolate enable`

【缺省情况】

当前端口未加入隔离组。

【视图】

二层以太网接口视图

二层聚合接口视图

【缺省用户角色】

network-admin

【参数】

group group-id: 隔离组编号，取值范围为 1~8。

【使用指导】

在端口上执行该命令将当前端口加入到指定的隔离组中前，必须先完成该隔离组的创建。

一个端口最多只能加入一个隔离组。

二层以太网接口视图下的配置只对当前端口生效。

二层聚合接口视图下的配置对当前接口及其成员端口生效，若某成员端口配置失败，系统会跳过该端口继续配置其他成员端口，若二层聚合接口配置失败，则不会再配置成员端口。

【举例】

将端口 GigabitEthernet1/0/1、GigabitEthernet1/0/2 加入隔离组 1。

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

【相关命令】

- `display port-isolate group`

1.1.3 port-isolate group

port-isolate group 命令用来创建隔离组。

undo port-isolate group 命令用来删除指定隔离组及其配置。

【命令】

```
port-isolate group group-id  
undo port-isolate group { group-id | all }
```

【缺省情况】

不存在隔离组。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

group-id: 隔离组编号，取值范围为 1~8。

all: 删除所有隔离组。

【举例】

```
# 创建隔离组 1。  
<Sysname> system-view  
[Sysname] port-isolate group 1
```

目 录

1 生成树.....	1-1
1.1 生成树配置命令.....	1-1
1.1.1 active region-configuration.....	1-1
1.1.2 bpdu-drop any.....	1-1
1.1.3 check region-configuration.....	1-2
1.1.4 display stp.....	1-3
1.1.5 display stp abnormal-port	1-10
1.1.6 display stp bpdu-statistics.....	1-11
1.1.7 display stp down-port.....	1-14
1.1.8 display stp history	1-15
1.1.9 display stp region-configuration.....	1-17
1.1.10 display stp root	1-18
1.1.11 display stp tc.....	1-18
1.1.12 instance	1-20
1.1.13 region-name	1-21
1.1.14 reset stp.....	1-22
1.1.15 revision-level.....	1-23
1.1.16 snmp-agent trap enable stp.....	1-23
1.1.17 stp bpdu-protection.....	1-24
1.1.18 stp bridge-diameter	1-25
1.1.19 stp compliance	1-26
1.1.20 stp config-digest-snooping	1-26
1.1.21 stp cost.....	1-27
1.1.22 stp dispute-protection.....	1-29
1.1.23 stp edged-port	1-29
1.1.24 stp enable	1-30
1.1.25 stp global config-digest-snooping.....	1-31
1.1.26 stp global enable.....	1-32
1.1.27 stp global mcheck	1-32
1.1.28 stp ignore-pvid-inconsistency.....	1-33
1.1.29 stp log enable tc	1-34
1.1.30 stp loop-protection.....	1-34
1.1.31 stp max-hops	1-35

1.1.32 stp mcheck	1-36
1.1.33 stp mode	1-37
1.1.34 stp no-agreement-check	1-38
1.1.35 stp pathcost-standard	1-38
1.1.36 stp point-to-point	1-39
1.1.37 stp port bpdu-protection	1-40
1.1.38 stp port priority	1-41
1.1.39 stp port shutdown permanent	1-42
1.1.40 stp port-log	1-43
1.1.41 stp priority	1-44
1.1.42 stp pvst-bpdu-protection	1-45
1.1.43 stp region-configuration	1-45
1.1.44 stp role-restriction	1-46
1.1.45 stp root primary	1-46
1.1.46 stp root secondary	1-47
1.1.47 stp root-protection	1-48
1.1.48 stp tc-protection	1-49
1.1.49 stp tc-protection threshold	1-50
1.1.50 stp tc-restriction	1-50
1.1.51 stp tc-snooping	1-51
1.1.52 stp timer forward-delay	1-52
1.1.53 stp timer hello	1-53
1.1.54 stp timer max-age	1-54
1.1.55 stp timer-factor	1-55
1.1.56 stp transmit-limit	1-55
1.1.57 stp vlan enable	1-56
1.1.58 vlan-mapping modulo	1-57

1 生成树

1.1 生成树配置命令

1.1.1 active region-configuration

active region-configuration 命令用来激活 MST 域的配置。

【命令】

active region-configuration

【视图】

MST 域视图

【缺省用户角色】

network-admin

【使用指导】

在配置 MST 域的相关参数（特别是 VLAN 映射表）时，会引发生成树的重新计算，从而引起网络拓扑的振荡。为了减少网络振荡，新配置的 MST 域参数并不会马上生效，而是在使用本命令激活，或使用命令 **stp global enable** 全局开启生成树协议后才会生效。

在执行本命令前，建议先使用 **check region-configuration** 命令查看 MST 域的预配置是否正确，当确认这些配置无误后再执行本命令。

【举例】

将 VLAN 2 映射到 MSTI 1 上，并激活该配置。

```
<Sysname> system-view
[Sysname] stp region-configuration
[Sysname-mst-region] instance 1 vlan 2
[Sysname-mst-region] active region-configuration
```

【相关命令】

- **check region-configuration**
- **instance**
- **region-name**
- **revision-level**
- **stp global enable**
- **vlan-mapping modulo**

1.1.2 bpdu-drop any

bpdu-drop any 命令用来开启端口的 BPDU 拦截功能。

undo bpdu-drop any 命令用来关闭端口的 BPDU 拦截功能。

【命令】

```
bpdu-drop any
undo bpdu-drop any
```

【缺省情况】

端口的 BPDU 拦截功能处于关闭状态。

【视图】

二层以太网接口视图

【缺省用户角色】

network-admin

【举例】

```
# 在端口 GigabitEthernet1/0/1 上开启 BPDU 拦截功能。
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] bpdu-drop any
```

1.1.3 check region-configuration

check region-configuration 命令用来显示 MST 域的预配置信息。

【命令】

```
check region-configuration
```

【视图】

MST 域视图

【缺省用户角色】

network-admin

【使用指导】

两台或多台开启了生成树协议的设备若要属于同一个 MST 域，必须同时满足以下两个条件：

- 选择因子（取值为 0，不可配）、域名、修订级别和 VLAN 映射表的配置都相同。
- 这些设备之间的链路相通。

建议在激活 MST 域的配置前，先使用本命令查看 MST 域的预配置是否正确，当确认这些配置无误后再激活 MST 域的配置。

【举例】

```
# 显示 MST 域的预配置信息。
<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
```

表1-1 check region-configuration 命令显示信息描述表

字段	描述
Format selector	生成树协议规定的选择因子，取值为0，不可配
Region name	MST域的域名
Revision level	MST域的修订级别
Configuration digest	配置摘要
Instance VLANs Mapped	MST域的VLAN与MSTI之间的映射关系，即VLAN映射表

【相关命令】

- active region-configuration
- instance
- region-name
- revision-level
- vlan-mapping modulo

1.1.4 display stp

display stp 命令用来显示生成树的状态和统计信息。

【命令】

```
display stp [ instance instance-list | vlan vlan-id-list ] [ interface
interface-list | slot slot-number ] [ brief ]
```

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator

【参数】

instance instance-list: 显示指定 MSTI 的生成树状态和统计信息。*instance-list* 为 MSTI 列表，表示多个 MSTI，表示方式为 *instance-list* = { *instance-id1* [**to** *instance-id2*] } <1-10>。*instance-id2* 的值大于等于 *instance-id1* 的值。其中，*instance-id* 为 MSTI 的编号，取值范围为 0~4094，0 表示 CIST。<1-10>表示前面的参数最多可以输入 10 次。

vlan *vlan-id-list*: 显示指定 VLAN 的生成树状态和统计信息。*vlan-id-list* 为 VLAN 列表, 表示多个 VLAN, 表示方式为 *vlan-id-list* = { *vlan-id1* [**to** *vlan-id2*] } &<1-10>。*vlan-id2* 的值大于等于 *vlan-id1* 的值。其中, *vlan-id* 为 VLAN 的编号, 取值范围为 1~4094。&<1-10> 表示前面的参数最多可以输入 10 次。

interface *interface-list*: 显示指定端口上的生成树状态和统计信息。*interface-list* 为端口列表, 表示多个端口, 表示方式为 *interface-list* = { *interface-type interface-number1* [**to** *interface-type interface-number2*] } &<1-10>。*interface-type interface-number2* 的值大于等于 *interface-type interface-number1* 的值。其中, *interface-type* 为端口类型, *interface-number* 为端口编号。&<1-10> 表示前面的参数最多可以输入 10 次。

brief: 显示生成树状态和统计的简要信息。如果未指定本参数, 将显示生成树状态和统计的详细信息。

slot *slot-number*: 显示指定成员设备上的生成树状态和统计信息, *slot-number* 表示设备在 IRF 中的成员编号。如果不指定该参数, 将显示所有成员设备上的生成树状态和统计信息。

【使用指导】

在 STP/RSTP 模式下:

- 如果未指定端口, 则显示所有端口上的生成树状态和统计信息, 显示信息按照端口名称的顺序排列。
- 如果指定了端口, 则显示该端口上的生成树状态和统计信息, 显示信息按照端口名称的顺序排列。

在 PVST 模式下:

- 如果未指定 VLAN 和端口, 则显示所有 VLAN 在所有端口上的生成树状态和统计信息, 显示信息按照 VLAN 编号的顺序排列, 各 VLAN 内部再按照端口名称的顺序排列。
- 如果指定了 VLAN 但未指定端口, 则显示指定 VLAN 在所有端口上的生成树状态和统计信息, 显示信息按照 VLAN 编号的顺序排列, 各 VLAN 内部再按照端口名称的顺序排列。
- 如果指定了端口但未指定 VLAN, 则显示所有 VLAN 在指定端口上的生成树状态和统计信息, 显示信息按照 VLAN 编号的顺序排列, 各 VLAN 内部再按照端口名称的顺序排列。
- 如果同时指定了 VLAN 和端口, 则显示指定 VLAN 在指定端口上的生成树状态和统计信息, 显示信息按照 VLAN 编号的顺序排列, 各 VLAN 内部再按照端口名称的顺序排列。

在 MSTP 模式下:

- 如果未指定 MSTI 和端口, 则显示所有 MSTI 在所有端口上的生成树状态和统计信息, 显示信息按照 MSTI 编号的顺序排列, 各 MSTI 内部再按照端口名称的顺序排列。
- 如果指定了 MSTI 但未指定端口, 则显示指定 MSTI 在所有端口上的生成树状态和统计信息, 显示信息按照 MSTI 编号的顺序排列, 各 MSTI 内部再按照端口名称的顺序排列。
- 如果指定了端口但未指定 MSTI, 则显示所有 MSTI 在指定端口上的生成树状态和统计信息, 显示信息按照 MSTI 编号的顺序排列, 各 MSTI 内部再按照端口名称的顺序排列。
- 如果同时指定了 MSTI 和端口, 则显示指定 MSTI 在指定端口上的生成树状态和统计信息, 显示信息按照 MSTI 编号的顺序排列, 各 MSTI 内部再按照端口名称的顺序排列。

【举例】

在 MSTP 模式下, 显示 MSTI 0 在端口 GigabitEthernet1/0/1 上生成树状态和统计的简要信息。

```
<Sysname> display stp instance 0 interface gigabitethernet 1/0/1 brief
MST ID      Port                               Role  STP State  Protection
0           GigabitEthernet1/0/1             ALTE  DISCARDING LOOP
```

在 PVST 模式下，显示 VLAN 2 在端口 GigabitEthernet1/0/1 上生成树状态和统计的简要信息。

```
<Sysname> system-view
[Sysname] stp mode pvst
[Sysname] display stp vlan 2 interface gigabitethernet 1/0/1 brief
VLAN ID     Port                               Role  STP State  Protection
2           GigabitEthernet1/0/1             ALTE  DISCARDING LOOP
```

表1-2 display stp brief 命令显示信息描述表

字段	描述
MST ID	MSTI的编号
VLAN ID	VLAN的编号
Port	端口名称，和相应的MSTI对应
Role	端口角色： <ul style="list-style-type: none"> • ALTE：表示替换端口 • BACK：表示备份端口 • ROOT：表示根端口 • DESI：表示指定端口 • MAST：表示主端口 • DISA：表示失效端口
STP State	端口状态： <ul style="list-style-type: none"> • FORWARDING：表示可以接收和发送 BPDU，也转发用户流量 • DISCARDING：表示可以接收和发送 BPDU，但不转发用户流量 • LEARNING：表示可以接收和发送 BPDU，但不转发用户流量，是一种过渡状态
Protection	当触发了保护机制后，端口上生效的保护类型： <ul style="list-style-type: none"> • ROOT：表示根保护 • LOOP：表示环路保护 • BPDU：表示 BPDU 保护 • NONE：表示无保护或配置的生成树保护功能未被触发

在 MSTP 模式下，显示所有 MSTI 在所有端口上的生成树状态和统计的详细信息。

```
<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

----[Port1(GigabitEthernet1/0/1)][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

----[Port1(GigabitEthernet1/0/1)][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
# 在 PVST 模式下，显示所有 VLAN 在所有端口上的生成树状态和统计信息。
<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(GigabitEthernet1/0/1)][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

```

当生成树协议未开启时，在 **MSTP** 模式下显示生成树的状态和统计信息。

```

<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

```

当生成树协议未开启时，在 **PVST** 模式下显示生成树的状态和统计信息。

```

<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

```

表1-3 display stp 命令显示信息描述表

字段	描述
Bridge ID	网桥ID，由两部分构成：“.”之前和之后的内容分别表示为本设备的优先级和本设备的MAC地址。譬如，“32768.000f-e200-2200”表示本设备的优先级为32768，其MAC地址为000F-E200-2200
Bridge times	网桥相关的主要参数值： <ul style="list-style-type: none"> • Hello: 表示 Hello time 定时器值 • MaxAge: 表示 Max Age 定时器值 • FwdDelay: 表示 Forward delay 定时器值 • MaxHops: 表示 MST 域的最大跳数
Root ID/ERPC	总根ID/外部路径开销（即本设备到总根的路径开销）
RegRoot ID/IRPC	域根ID/内部路径开销（即本设备到域根的路径开销）
VlanRoot ID/RPC	VLAN根桥ID/根路径开销（即本设备到该VLAN根桥的路径开销）
RootPort ID	根端口的端口ID。“0.0”表示本设备为根设备，没有根端口
BPDU-Protection	BPDU保护功能的全局开启状态
Bridge Config-Digest-Snooping	摘要侦听功能的全局开启状态
TC or TCN received	MSTI或VLAN收到的TC及TCN报文数
Time since last TC	MSTI或VLAN最近一次拓扑变化后经过的时间
[FORWARDING]	端口状态为Forwarding状态
[DISCARDING]	端口状态为Discarding状态
[LEARNING]	端口状态为Learning状态
Port protocol	生成树协议在端口上的开启状态
Port role	端口角色，和MSTI相对应。具体角色分为：Alternate、Backup、Root、Designated、Master、Disabled
(Boundary)	表示该端口为域边界端口
Port ID	端口ID

字段	描述
Port cost(Legacy)	端口的路径开销（Legacy表示当前设备的路径开销的计算方法，此外还有dot1d-1998和dot1t两种计算方式）： <ul style="list-style-type: none"> Config: 表示配置值 Active: 表示实际值
Desg.bridge/port	端口的指定桥ID和端口ID（对于不支持端口优先级的端口，这里显示的端口ID没有意义）
Port edged	端口是否为边缘端口： <ul style="list-style-type: none"> Config: 表示配置值 Active: 表示实际值
Point-to-Point	端口是否与点对点链路相连： <ul style="list-style-type: none"> Config: 表示配置值 Active: 表示实际值
Transmit limit	端口每个Hello Time时间间隔发送报文的上限
Protection type	端口是否开启保护： <ul style="list-style-type: none"> Config: 表示配置值 Active: 表示实际值，即当触发了保护机制后，生效的保护类型 端口的保护类型： <ul style="list-style-type: none"> ROOT: 表示根保护 LOOP: 表示环路保护 BPDU: 表示 BPDU 保护 PVST BPDU: 表示 MSTP 的 PVST BPDU 保护 NONE: 表示无保护或配置的生成树保护功能未被触发
TC-Restriction	端口是否开启了TC-BPDU传播限制功能
Role-Restriction	端口是否开启了端口角色限制功能
MST BPDU format	端口发送MSTP报文的格式，取值为legacy和802.1s: <ul style="list-style-type: none"> Config: 表示配置值 Active: 表示实际值
Port Config-Digest-Snooping	摘要侦听功能在端口上的开启状态
Rapid transition	端口在当前MSTI或VLAN中是否快速迁移至转发状态
Num of VLANs mapped	端口在当前MSTI中的VLAN计数
Port times	端口相关的主要参数值： <ul style="list-style-type: none"> Hello: 表示 Hello time 定时器值 MaxAge: 表示 Max Age 定时器值 FwdDelay: 表示 Forward delay 定时器值 MsgAge: 表示 Message Age 定时器值 RemHops: 表示剩余跳数

字段	描述
BPDU sent	端口发送报文计数
BPDU received	端口接收报文计数
RegRoot ID/IRPC	MSTI域根/内部路径开销
Root Type	MSTI域根类型： <ul style="list-style-type: none"> Primary root: 表示根桥 Secondary root: 表示备份根桥
Master bridge	MSTI的Master桥ID
Cost to master	MSTI到Master桥的路径开销
TC received	MSTI收到的TC报文数
Protocol status	生成树协议的全局开启状态
Protocol Std.	生成树协议采用的协议标准
Version	生成树协议采用的协议版本
Bridge-Prio.	在MSTP模式下,表示本设备在CIST中的桥优先级;在PVST模式下,表示本设备在VLAN 1中的桥优先级
MAC address	本设备的MAC地址
Max age(s)	BPDU的最大生存时间（单位为秒，在PVST模式下为在VLAN 1中的配置）
Forward delay(s)	端口状态迁移的延时（单位为秒，在PVST模式下为在VLAN 1中的配置）
Hello time(s)	根设备发送BPDU的周期（单位为秒，在PVST模式下为在VLAN 1中的配置）
Max hops	MST域中的最大跳数
TC Snooping	TC Snooping开启状态： <ul style="list-style-type: none"> Enabled Disabled

【相关命令】

- `reset stp`

1.1.5 display stp abnormal-port

`display stp abnormal-port` 命令用来显示被生成树保护功能阻塞的端口历史信息。

【命令】

`display stp abnormal-port`

【视图】

任意视图

【缺省用户角色】

network-admin

【使用指导】

每个生成树实例或者 VLAN 最多显示 3 条阻塞的端口历史信息。

【举例】

在 MSTP 模式下，显示被生成树保护功能阻塞的端口历史信息。

```
<Sysname> display stp abnormal-port
---[GigabitEthernet1/0/1]---
MST ID   BlockReason           Time
0         Root-Protected       14:39:04 04/15/2016
0         Root-Protected       14:39:02 04/15/2016
0         Root-Protected       14:39:00 04/15/2016
```

在 PVST 模式下，显示被生成树保护功能阻塞的端口历史信息。

```
<Sysname> system-view
[Sysname] stp mode pvst
[Sysname] display stp abnormal-port
---[GigabitEthernet1/0/1]---
VLAN ID   BlockReason           Time
1         Root-Protected       14:49:17 04/15/2016
1         Root-Protected       14:49:15 04/15/2016
1         Root-Protected       14:49:12 04/15/2016
```

表1-4 display stp abnormal-port 命令显示信息描述表

字段	描述
MST ID	被生成树保护功能阻塞的端口所在MSTI的编号
VLAN ID	被生成树保护功能阻塞的端口所在VLAN的编号
BlockReason	导致端口阻塞的原因： <ul style="list-style-type: none">• Root-Protected: 表示发生了根保护• Loop-Protected: 表示发生了环路保护• Loopback-Protected: 表示发生了自环保护，即有端口收到了自己发出的协议报文• Disputed: 表示发生了 Dispute 保护，即端口收到了指定端口发出的低优先级消息，且发送端口处于 Forwarding 或 Learning 状态• InconsistentPortType-Protected: 表示发生了端口类型不一致保护• InconsistentPvid-Protected: 表示发生了 PVID 不一致保护
Time	触发保护的时间

1.1.6 display stp bpdu-statistics

display stp bpdu-statistics 命令用来显示端口上的 BPDU 统计信息。

【命令】

```
display stp bpdu-statistics [ interface interface-type interface-number
[ instance instance-list ] ]
```


【视图】

任意视图

【缺省用户角色】

network-admin
network-operator

【参数】

interface *interface-type interface-number*: 显示指定端口上的 BPDU 统计信息，*interface-type interface-number* 表示端口类型和端口编号。

instance *instance-list*: 显示指定 MSTI 在端口上的 BPDU 统计信息。*instance-list* 为 MSTI 列表，表示多个 MSTI，表示方式为 *instance-list* = { *instance-id1* [**to** *instance-id2*] } <1-10>。其中，*instance-id* 为 MSTI 的编号，取值范围为 0~4094，0 表示 CIST。*instance-id2* 的值大于等于 *instance-id1* 的值。<1-10> 表示前面的参数最多可以输入 10 次。

【使用指导】

在 MSTP 模式下：

- 如果未指定端口和 MSTI，则显示所有 MSTI 在所有端口上的 BPDU 统计信息，显示信息按照端口名称的顺序排列，各端口内部再按照 MSTI 编号的顺序排列。
- 如果指定了端口但未指定 MSTI，则显示所有 MSTI 在该端口上的 BPDU 统计信息，显示信息按照 MSTI 编号的顺序排列。
- 如果同时指定了 MSTI 和端口，则显示指定 MSTI 在指定端口上的 BPDU 统计信息。

在 STP/RSTP/PVST 模式下：

- 如果未指定端口，则显示所有端口上的 BPDU 统计信息，显示信息按照端口名称的顺序排列。
- 如果指定了端口，则显示该端口上的 BPDU 统计信息。

【举例】

在 MSTP 模式下，显示所有 MSTI 在端口 GigabitEthernet1/0/1 上的 BPDU 统计信息。

```
<Sysname> display stp bpdu-statistics interface gigabitethernet 1/0/1  
Port: GigabitEthernet1/0/1
```

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	

在 PVST 模式下，显示端口 GigabitEthernet1/0/1 上的 BPDU 统计信息。

```
<Sysname> system-view
[Sysname] stp mode pvst
[Sysname] display stp bpdu-statistics interface gigabitethernet 1/0/1
Port: GigabitEthernet1/0/1
```

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	

表1-5 display stp bpdu-statistics 命令显示信息描述表

字段	描述
Port	端口名称
Instance-Independent	与MSTI无关的统计信息
Type	统计类型

字段	描述
Count	统计值
Last Updated	最后更新时间
Invalid BPDUs	无效BPDU的数量
Looped-back BPDUs	自环（即收到由本端口发出）的BPDU数量
Max-aged BPDUs	超过最大生存时间的BPDU数量
TCN sent	发出的TCN报文数量
TCN received	收到的TCN报文数量
TCA sent	发出的TCA报文数量
TCA received	收到的TCA报文数量
Config sent	发出的Configuration报文数量
Config received	收到的Configuration报文数量
RST sent	发出的RSTP BPDU数量
RST received	收到的RSTP BPDU数量
MST sent	发出的MSTP BPDU数量
MST received	收到的MSTP BPDU数量
Instance	与指定MSTI相关的统计信息
Timeout BPDUs	老化的BPDU数量
Max-hopped BPDUs	超过最大跳数的BPDU数量
TC detected	监测到的拓扑变化的次数
TC sent	发出的TC报文数量
TC received	收到的TC报文数量
PVID inconsistency BPDUs	收到的PVID不一致的PVST报文数量

1.1.7 display stp down-port

display stp down-port 命令用来显示被生成树保护功能 down 掉的端口信息。

【命令】

display stp down-port

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator

【举例】

显示被生成树保护功能 down 掉的端口信息。

```
<Sysname> display stp down-port
Down Port          Reason
GigabitEthernet1/0/1    BPDU protection
```

表1-6 display stp down-port 命令显示信息描述表

字段	描述
Down Port	被生成树保护功能down掉的端口名称
Reason	导致端口down的原因： <ul style="list-style-type: none">• BPDU protection: 表示 BPDU 保护• PVST BPDU protection: 表示 MSTP 的 PVST BPDU 保护

1.1.8 display stp history

display stp history 命令用来显示生成树端口角色计算的历史信息。

【命令】

```
display stp [ instance instance-list | vlan vlan-id-list ] history [ slot
slot-number ]
```

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator

【参数】

instance instance-list: 显示指定 MSTI 中端口角色计算的历史信息。*instance-list* 为 MSTI 列表, 表示多个 MSTI, 表示方式为 *instance-list* = { *instance-id1* [**to** *instance-id2*] } &<1-10>。其中, *instance-id* 为 MSTI 的编号, 取值范围为 0~4094, 0 表示 CIST。 *instance-id2* 的值大于等于 *instance-id1* 的值。 &<1-10>表示前面的参数最多可以输入 10 次。

vlan vlan-id-list: 显示指定 VLAN 中端口角色计算的历史信息。*vlan-id-list* 为 VLAN 的列表, 表示多个 VLAN, 表示方式为 *vlan-id-list* = { *vlan-id1* [**to** *vlan-id2*] } &<1-10>。其中, *vlan-id* 为 VLAN 的编号, 取值范围为 1~4094。 *vlan-id2* 的值大于等于 *vlan-id1* 的值。 &<1-10>表示前面的参数最多可以输入 10 次。

slot slot-number: 显示指定成员设备上端口角色计算的历史信息, *slot-number* 表示设备在 IRF 中的成员编号。如果不指定该参数, 将显示所有成员设备上端口角色计算的历史信息。

【使用指导】

在 STP/RSTP 模式下, 显示信息按照端口角色计算的时间先后顺序排列。

在 PVST 模式下:

- 如果未指定 VLAN，则显示所有 VLAN 中端口角色计算的历史信息，显示信息按照 VLAN 编号的顺序排列，各 VLAN 内部再按照端口角色计算的时间先后顺序排列。
- 如果指定了 VLAN，则显示指定 VLAN 中端口角色计算的历史信息，显示信息按照 VLAN 编号的顺序排列，各 VLAN 内部再按照端口角色计算的时间先后顺序排列。

在 MSTP 模式下：

- 如果未指定 MSTI，则显示所有 MSTI 中端口角色计算的历史信息，显示信息按照 MSTI 编号的顺序排列，各 MSTI 内部再按照端口角色计算的时间先后顺序排列。
- 如果指定了 MSTI，则显示指定 MSTI 中端口角色计算的历史信息，显示信息按照 MSTI 编号的顺序排列，各 MSTI 内部再按照端口角色计算的时间先后顺序排列。

【举例】

在 MSTP 模式下，显示指定 slot 上 MSTI 2 中端口角色计算的历史信息。

```
<Sysname> display stp instance 2 history slot 1
----- STP slot 1 history trace -----
----- Instance 2 -----
Port GigabitEthernet1/0/1
  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 GigabitEthernet1/0/2
  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
```

在 PVST 模式下，显示指定 slot 上 VLAN 2 中端口角色计算的历史信息。

```
<Sysname> display stp vlan 2 history slot 1
----- STP slot 1 history trace -----
----- VLAN 2 -----

Port GigabitEthernet1/0/1
  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 GigabitEthernet1/0/2
  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
```

表1-7 display stp history 命令显示信息描述表

字段	描述
Port	端口名称

字段	描述
Role change	显示端口的角色变化（Aged表示由于报文超时引起的角色变化）
Time	端口角色计算时间
Port priority	端口优先级，由根桥ID、根路径开销、指定桥ID和指定端口ID组成，以空格分隔
Designated priority	指定优先级，由根桥ID、根路径开销、指定桥ID和指定端口ID组成，以空格分隔

1.1.9 display stp region-configuration

display stp region-configuration 命令用来显示生效的 MST 域配置信息。

【命令】

display stp region-configuration

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator

【举例】

在 MSTP 模式下，显示当前生效的 MST 域配置信息。

```
<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
```

表1-8 display stp region-configuration 命令显示信息描述表

字段	描述
Format selector	生成树协议规定的选择因子，缺省值为0，不可配置
Region name	MST域的域名
Revision level	MST域的修订级别，可使用命令 revision-level 来配置，缺省为0级
Configuration digest	配置摘要
VLANs Mapped	映射到MSTI的VLAN

【相关命令】

- instance
- region-name
- revision-level
- vlan-mapping modulo

1.1.10 display stp root

display stp root 命令用来显示所有生成树的根桥信息。

【命令】

display stp root

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator

【举例】

在 MSTP 模式下，显示所有生成树的根桥信息。

```
<Sysname> display stp root
MST ID   Root Bridge ID           ExtPathCost IntPathCost Root Port
0         0.00e0-fc0e-6554         200200      0           GigabitEthernet1/0/1
```

在 PVST 模式下，显示所有生成树的根桥信息。

```
<Sysname> display stp root
VLAN ID   Root Bridge ID           ExtPathCost IntPathCost Root Port
1         0.00e0-fc0e-6554         200200      0           GigabitEthernet1/0/1
```

表1-9 display stp root 命令显示信息描述表

字段	描述
MST ID	MSTI的编号
VLAN ID	VLAN的编号
Root Bridge ID	根桥的编号
ExtPathCost	外部路径开销。设备可自动计算端口的缺省路径开销，用户也可使用命令 stp cost 来配置端口的路径开销
IntPathCost	内部路径开销。设备可自动计算端口的缺省路径开销，用户也可使用命令 stp cost 来配置端口的路径开销
Root Port	根端口名称（若当前设备的某个端口是MSTI的根端口则显示，否则不显示）

1.1.11 display stp tc

display stp tc 命令用来显示生成树所有端口收发的 TC 或 TCN 报文数。

【命令】

```
display stp [ instance instance-list | vlan vlan-id-list ] tc [ slot slot-number ]
```

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator

【参数】

instance instance-list: 显示指定 MSTI 中所有端口收发的 TC 或 TCN 报文数。
instance-list 为 MSTI 列表，表示多个 MSTI，表示方式为 *instance-list* = { *instance-id1* [**to** *instance-id2*] } <1-10>。其中，*instance-id* 为 MSTI 的编号，取值范围为 0~4094，0 表示 CIST。*instance-id2* 的值大于等于 *instance-id1* 的值。<1-10> 表示前面的参数最多可以输入 10 次。

vlan vlan-id-list: 显示指定 VLAN 中所有端口收发的 TC 或 TCN 报文数。*vlan-id-list* 为 VLAN 列表，表示多个 VLAN，表示方式为 *vlan-id-list* = { *vlan-id1* [**to** *vlan-id2*] } <1-10>。其中，*vlan-id* 为 VLAN 的编号，取值范围为 1~4094。*vlan-id2* 的值大于等于 *vlan-id1* 的值。<1-10> 表示前面的参数最多可以输入 10 次。

slot slot-number: 显示指定成员设备上所有端口收发的 TC 或 TCN 报文数，*slot-number* 表示设备在 IRF 中的成员编号。如果不指定该参数，将显示所有成员设备上所有端口收发的 TC 或 TCN 报文数。

【使用指导】

在 STP/RSTP 模式下，显示信息按照端口名称的顺序排列。

在 PVST 模式下：

- 如果未指定 VLAN，则显示所有 VLAN 中所有端口收发的 TC 或 TCN 报文数，显示信息按照 VLAN 编号的顺序排列，各 VLAN 内部再按照端口名称的顺序排列。
- 如果指定了 VLAN，则显示指定 VLAN 中所有端口收发的 TC 或 TCN 报文数，显示信息按照 VLAN 编号的顺序排列，各 VLAN 内部再按照端口名称的顺序排列。

在 MSTP 模式下：

- 如果未指定 MSTI，则显示所有 MSTI 中所有端口收发的 TC 或 TCN 报文数，显示信息按照 MSTI 编号的顺序排列，各 MSTI 内部再按照端口名称的顺序排列。
- 如果指定了 MSTI，则显示指定 MSTI 中所有端口收发的 TC 或 TCN 报文数，显示信息按照 MSTI 编号的顺序排列，各 MSTI 内部再按照端口名称的顺序排列。

【举例】

在 MSTP 模式下，显示指定 slot 上 MSTI 0 中所有端口收发的 TC 或 TCN 报文数。

```
<Sysname> display stp instance 0 tc slot 1
----- STP slot 1 TC or TCN count -----
MST ID      Port                               Receive      Send
0           GigabitEthernet1/0/1              6             4
```



```
0          GigabitEthernet1/0/2          0          2
# 在 PVST 模式下，显示指定 slot 上 VLAN 2 中所有端口收发的 TC 或 TCN 报文数。
```

```
<Sysname> display stp vlan 2 tc slot 1
----- STP slot 1 TC or TCN count -----
VLAN ID      Port                                Receive      Send
2            GigabitEthernet1/0/1            6            4
2            GigabitEthernet1/0/2            0            2
```

表1-10 display stp tc 命令显示信息描述表

字段	描述
MST ID	MSTI的编号
VLAN ID	VLAN的编号
Port	端口名称
Receive	端口收到的TC或TCN报文数
Send	端口发出的TC或TCN报文数

1.1.12 instance

instance 命令用来将指定 VLAN 映射到指定的 MSTI 上。

undo instance 命令用来删除指定 VLAN 与指定 MSTI 之间的映射关系，这些 VLAN 将重新映射到 CIST（即 MSTI 0）上。

【命令】

```
instance instance-id vlan vlan-id-list
undo instance instance-id [ vlan vlan-id-list ]
```

【缺省情况】

所有 VLAN 都映射到 CIST（即 MSTI 0）上。

【视图】

MST 域视图

【缺省用户角色】

network-admin

【参数】

instance-id: 表示 MSTI 的编号，取值范围为 0~4094，0 表示 CIST。在执行 **undo instance** 命令时，**instance-id** 的取值范围为 1~4094。

vlan vlan-id-list: 指定 VLAN。**vlan-id-list** 为 VLAN 列表，表示多个 VLAN。表示方式为 **vlan-id-list** = { **vlan-id1** [**to** **vlan-id2**] } &<1-10>。其中，**vlan-id** 为 VLAN 的编号，取值范围为 1~4094。**vlan-id2** 的值大于等于 **vlan-id1** 的值。&<1-10>表示前面的参数最多可以输入 10 次。

【使用指导】



注意

配置全局摘要侦听功能后，进行下面的操作，均可能因与邻接设备的 VLAN 和 MSTI 映射关系不一致而导致环路或流量中断，因此请谨慎操作。

修改 VLAN 与 MSTI 间的映射关系。

执行 **undo stp region-configuration** 命令取消当前域配置。

如果 **undo instance** 命令中没有指定 VLAN，则与指定 MSTI 有映射关系的所有 VLAN 都将重新映射到 CIST 上。

不能将同一个 VLAN 映射到不同的 MSTI 上。如果将一个已映射到某 MSTI 的 VLAN 重新映射到另一个 MSTI 时，原先的映射关系将被取消。

最多只能对 65 个 MSTI 配置 VLAN 映射关系。

配置本命令后，必须执行 **active region-configuration** 命令才能激活本配置。

【举例】

将 VLAN 2 映射到 MSTI 1 上。

```
<Sysname> system-view
[Sysname] stp region-configuration
[Sysname-mst-region] instance 1 vlan 2
```

【相关命令】

- **active region-configuration**
- **check region-configuration**
- **display stp region-configuration**

1.1.13 region-name

region-name 命令用来配置 MST 域的域名。

undo region-name 命令用来恢复缺省情况。

【命令】

```
region-name name
undo region-name
```

【缺省情况】

MST 域的域名为设备的 MAC 地址。

【视图】

MST 域视图

【缺省用户角色】

network-admin

【参数】

name: 表示 MST 域的域名，为 1~32 个字符的字符串。

【使用指导】

MST 域名用来与 MST 域的 VLAN 映射表和 MSTP 的修订级别来共同确定设备所属的 MST 域。
配置本命令后，必须执行 **active region-configuration** 命令才能激活本配置。

【举例】

配置 MST 域的域名为 hello。

```
<Sysname> system-view
[Sysname] stp region-configuration
[Sysname-mst-region] region-name hello
```

【相关命令】

- **active region-configuration**
- **check region-configuration**
- **display stp region-configuration**
- **instance**
- **revision-level**
- **vlan-mapping modulo**

1.1.14 reset stp

reset stp 命令用来清除生成树的统计信息。

【命令】

```
reset stp [ interface interface-list ]
```

【视图】

用户视图

【缺省用户角色】

network-admin

【参数】

interface *interface-list*: 清除指定端口上的生成树统计信息。*interface-list* 为端口列表，表示多个端口，表示方式为 *interface-list* = { *interface-type interface-number1* [**to** *interface-type interface-number2*] }&<1-10>。其中，*interface-type* 为端口类型，*interface-number* 为端口编号。*interface-type interface-number2* 的值大于等于 *interface-type interface-number1* 的值。&<1-10> 表示前面的参数最多可以输入 10 次。如果未指定本参数，将清除所有端口上的生成树统计信息。

【举例】

清除端口 GigabitEthernet1/0/1 到 GigabitEthernet1/0/3 上的生成树统计信息。

```
<Sysname> reset stp interface gigabitethernet 1/0/1 to gigabitethernet 1/0/3
```

【相关命令】

- `display stp`

1.1.15 revision-level

`revision-level` 命令用来配置 MSTP 的修订级别。

`undo revision-level` 命令用来恢复缺省情况。

【命令】

`revision-level level`

`undo revision-level`

【缺省情况】

MSTP 的修订级别为 0。

【视图】

MST 域视图

【缺省用户角色】

network-admin

【参数】

`level`: 表示 MSTP 的修订级别，取值范围为 0~65535。

【使用指导】

MSTP 的修订级别用来与 MST 域名和 MST 域的 VLAN 映射表来共同确定设备所属的 MST 域。修订级别可以在域名和 VLAN 映射表相同的情况下，来区分不同的域。

配置本命令后，必须执行 `active region-configuration` 命令才能激活本配置。

【举例】

配置设备的 MSTP 修订级别为 5。

```
<Sysname> system-view
[Sysname] stp region-configuration
[Sysname-mst-region] revision-level 5
```

【相关命令】

- `active region-configuration`
- `check region-configuration`
- `display stp region-configuration`
- `instance`
- `region-name`
- `vlan-mapping modulo`

1.1.16 snmp-agent trap enable stp

`snmp-agent trap enable stp` 命令用来开启生成树的告警功能。

`undo snmp-agent trap enable stp` 命令用来关闭生成树的告警功能。

【命令】

```
snmp-agent trap enable stp [ new-root | tc ]
undo snmp-agent trap enable stp [ new-root | tc ]
```

【缺省情况】

生成树的 new-root 告警功能处于关闭状态。在 MSTP 模式下,生成树的 TC 告警功能在 MSTI 0 中处于开启状态,在其他 MSTI 中处于关闭状态;在 PVST 模式下,生成树的 TC 告警功能在所有 VLAN 中处于关闭状态。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

new-root: 在 STP、RSTP 或 MSTP 模式下,当设备在任意实例中由非根桥被选举为根桥后,发送 Trap 信息。

tc: 在 PVST 模式下,当端口检测或接收到 TC 报文后,发送 Trap 信息。该参数只能控制 PVST 模式下的 TC 告警功能。

【使用指导】

执行该命令时,如果未指定任何参数:

- 在 STP、RSTP 或 MSTP 模式下,表示开启或关闭生成树的 new-root 告警功能。
- 在 PVST 模式下,表示开启或关闭生成树的 TC 告警功能。

【举例】

配置当设备在任意实例中由非根桥被选举为根桥后,发送 Trap 信息。

```
<Sysname> system-view
[Sysname] snmp-agent trap enable stp new-root
```

1.1.17 stp bpdu-protection

stp bpdu-protection 命令用来开启全局的 BPDU 保护功能。

undo stp bpdu-protection 命令用来关闭全局的 BPDU 保护功能。

【命令】

```
stp bpdu-protection
undo stp bpdu-protection
```

【缺省情况】

全局的 BPDU 保护功能处于关闭状态。

【视图】

系统视图

【缺省用户角色】

network-admin

【举例】

```
# 开启全局的 BPDU 保护功能。
<Sysname> system-view
[Sysname] stp bpdu-protection
```

【相关命令】

- **stp edged-port**
- **stp port bpdu-protection**

1.1.18 stp bridge-diameter

stp bridge-diameter 命令用来配置交换网络的网络直径，即交换网络中任意两台终端设备间的最大设备数。

undo stp bridge-diameter 命令用来恢复缺省情况。

【命令】

```
stp [ vlan vlan-id-list ] bridge-diameter diameter
undo stp [ vlan vlan-id-list ] bridge-diameter
```

【缺省情况】

交换网络的网络直径为 7。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

vlan vlan-id-list: 表示配置 PVST 交换网络中指定 VLAN 的网络直径。*vlan-id-list* 为 VLAN 列表，表示多个 VLAN。表示方式为 *vlan-id-list* = { *vlan-id1* [**to** *vlan-id2*] } &<1-10>。其中，*vlan-id* 为 VLAN 的编号，取值范围为 1~4094。*vlan-id2* 的值大于等于 *vlan-id1* 的值。&<1-10> 表示前面的参数最多可以输入 10 次。如果未指定本参数，表示配置 STP/RSTP/MSTP 交换网络的网络直径。

diameter: 表示交换网络的网络直径，取值范围为 2~7。

【使用指导】

选用合适的 Hello Time、Forward Delay 和 Max Age 时间参数，可以加快生成树收敛速度。上述三个时间参数的取值与网络规模有关，因此可以通过调整网络直径使生成树协议自动调整这三个时间参数的值。当网络直径为缺省值 7 时，这三个时间参数也分别取其各自的缺省值。

在 STP/RSTP/MSTP 模式下，每个 MST 域将被视为一台设备，且网络直径配置只对 CIST 有效（即只能在总根上生效），而对 MSTI 无效。

在 PVST 模式下，网络直径的配置只能在指定 VLAN 的根桥上生效。

【举例】

```
# 在 MSTP 模式下，配置交换网络的网络直径为 5。
<Sysname> system-view
```

```
[Sysname] stp bridge-diameter 5
# 在 PVST 模式下，配置交换网络中 VLAN 2 的网络直径为 5。
<Sysname> system-view
[Sysname] stp vlan 2 bridge-diameter 5
```

【相关命令】

- **stp timer forward-delay**
- **stp timer hello**
- **stp timer max-age**

1.1.19 stp compliance

stp compliance 命令用来配置端口收发的 MSTP 报文格式。

undo stp compliance 命令用来恢复缺省情况。

【命令】

```
stp compliance { auto | dot1s | legacy }
undo stp compliance
```

【缺省情况】

端口会自动识别收到的 MSTP 报文格式并根据识别结果确定发送的报文格式。

【视图】

二层以太网接口视图
二层聚合接口视图

【缺省用户角色】

network-admin

【参数】

auto: 表示端口会自动识别收到的 MSTP 报文格式并根据识别结果确定发送的报文格式。

dot1s: 表示端口只发送标准格式（符合 802.1s 协议）的 MSTP 报文。

legacy: 表示端口只发送与非标准格式兼容的 MSTP 报文。

【使用指导】

二层以太网接口视图下的配置只对当前端口生效；二层聚合接口视图下的配置只对当前接口生效；聚合成员端口上的配置，只有当成员端口退出聚合组后才能生效。

【举例】

```
# 配置端口只发送标准格式的 MSTP 报文。
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] stp compliance dot1s
```

1.1.20 stp config-digest-snooping

stp config-digest-snooping 命令用来在端口上开启摘要侦听功能。

undo stp config-digest-snooping 命令用来在端口上关闭摘要侦听功能。

【命令】

```
stp config-digest-snooping
undo stp config-digest-snooping
```

【缺省情况】

端口上的摘要侦听功能处于关闭状态。

【视图】

二层以太网接口视图
二层聚合接口视图

【缺省用户角色】

network-admin

【使用指导】

只有当全局和端口上都开启了摘要侦听功能后，该功能才能生效。开启摘要侦听功能时，建议先在所有与第三方厂商设备相连的端口上开启该功能，再全局开启该功能，以一次性让所有端口的配置生效，从而减少对网络的冲击。

二层以太网接口视图下的配置只对当前端口生效；二层聚合接口视图下的配置只对当前接口生效；聚合成员端口上的配置，只有当成员端口退出聚合组后才能生效。

【举例】

先在端口 GigabitEthernet1/0/1 上开启摘要侦听功能，再全局开启摘要侦听功能。

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] stp config-digest-snooping
[Sysname-GigabitEthernet1/0/1] quit
[Sysname] stp global config-digest-snooping
```

【相关命令】

- **display stp**
- **stp global config-digest-snooping**

1.1.21 stp cost

stp cost 命令用来配置端口的路径开销。

undo stp cost 命令用来恢复缺省情况。

【命令】

```
stp [ instance instance-list | vlan vlan-id-list ] cost cost-value
undo stp [ instance instance-list | vlan vlan-id-list ] cost
```

【缺省情况】

自动按照相应的标准计算各生成树上的路径开销。

【视图】

二层以太网接口视图

【缺省用户角色】

network-admin

【参数】

instance *instance-list*: 表示配置端口在 MSTP 指定 MSTI 的路径开销。 *instance-list* 为 MSTI 列表, 表示多个 MSTI, 表示方式为 *instance-list* = { *instance-id1* [*to instance-id2*] } <1-10>。其中, *instance-id* 为 MSTI 的编号, 取值范围为 0~4094, 0 表示 CIST。 *instance-id2* 的值大于等于 *instance-id1* 的值。 <1-10> 表示前面的参数最多可以输入 10 次。如果未指定本参数, 表示配置端口在 MSTP CIST 或 STP/RSTP 的路径开销。

vlan *vlan-id-list*: 表示配置端口在 PVST 指定 VLAN 的路径开销。 *vlan-id-list* 为 VLAN 列表, 表示多个 VLAN。表示方式为 *vlan-id-list* = { *vlan-id1* [*to vlan-id2*] } <1-10>。其中, *vlan-id* 为 VLAN 的编号, 取值范围为 1~4094。 *vlan-id2* 的值大于等于 *vlan-id1* 的值。 <1-10> 表示前面的参数最多可以输入 10 次。

cost-value: 表示端口的路径开销值。取值范围由计算端口缺省路径开销所采用的计算方法来决定:

- 当采用 IEEE 802.1D-1998 标准来计算时, 取值范围为 1~65535。
- 当采用 IEEE 802.1t 标准来计算时, 取值范围为 1~200000000。
- 当采用私有标准来计算时, 取值范围为 1~200000。

【使用指导】

端口的路径开销是生成树计算的重要依据, 可以影响端口的角色选择。在不同生成树上为同一端口配置不同的路径开销值, 可以使不同 VLAN 的流量沿不同的物理链路转发, 从而实现按 VLAN 的负载分担的功能。

当端口的路径开销值改变时, 系统将重新计算端口的角色并进行状态迁移。

二层以太网接口视图下的配置只对当前端口生效; 二层聚合接口视图下的配置只对当前接口生效; 聚合成员端口上的配置, 只有当成员端口退出聚合组后才能生效。

如果未指定 MSTI 和 VLAN, 则表示配置端口在 MSTP CIST 或 STP/RSTP 的路径开销。

【举例】

在 MSTP 模式下, 配置端口 GigabitEthernet1/0/1 在 MSTI 2 上的路径开销值为 200。

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] stp instance 2 cost 200
```

在 PVST 模式下, 配置端口 GigabitEthernet1/0/1 在 VLAN 2 上的路径开销值为 200。

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] stp vlan 2 cost 200
```

【相关命令】

- **display stp**
- **stp pathcost-standard**

1.1.22 stp dispute-protection

stp dispute-protection 命令用来开启 Dispute 保护功能。

undo stp dispute-protection 命令用来关闭 Dispute 保护功能。

【命令】

```
stp dispute-protection
undo stp dispute-protection
```

【缺省情况】

Dispute 保护功能处于开启状态。

【视图】

系统视图

【缺省用户角色】

network-admin

【使用指导】

Dispute 保护是指当生成树检测到链路出现了单通故障时，会阻塞单通端口，以防止环路。

在某些特定的 VLAN 应用组网中,例如,用户配置下游设备的上行端口不允许 PVID 的 VLAN 通过,导致下游设备收不到上游设备发送的 PVID 对应 VLAN 的生成树协议报文,而上游设备能收到下游设备发送的生成树协议报文。此时会触发 Dispute 保护,阻塞端口,导致用户业务流量中断。为了保证业务流量正常处理,用户可以配置 **undo stp dispute-protection** 命令关闭 Dispute 保护功能,避免链路被生成树阻塞而影响用户业务。

【举例】

关闭 Dispute 保护功能。

```
<Sysname> system-view
[Sysname] undo stp dispute-protection
```

1.1.23 stp edged-port

stp edged-port 命令用来配置端口为边缘端口。

undo stp edged-port 命令用来恢复缺省情况。

【命令】

```
stp edged-port
undo stp edged-port
```

【缺省情况】

端口为非边缘端口。

【视图】

二层以太网接口视图

二层聚合接口视图

【缺省用户角色】

network-admin

【使用指导】

当端口直接与用户终端相连，而没有连接到其它设备或共享网段上，则该端口被认为是边缘端口。网络拓扑变化时，边缘端口不会产生临时环路。因此，如果将某个端口配置为边缘端口，则该端口可以快速迁移到转发状态。对于直接与用户终端相连的端口，为能使其快速迁移到转发状态，请将其设置为边缘端口。

由于边缘端口不与其它设备相连，所以不会收到其它设备发过来的 BPDU。在端口没有开启 BPDU 保护功能时，如果端口收到 BPDU，即使用户设置该端口为边缘端口，该端口的实际运行状态也是非边缘端口。

在同一个端口上，不允许同时配置边缘端口和环路保护功能。

二层以太网接口视图下的配置只对当前端口生效；二层聚合接口视图下的配置只对当前接口生效；聚合成员端口上的配置，只有当成员端口退出聚合组后才能生效。

【举例】

配置端口 GigabitEthernet1/0/1 为边缘端口。

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] stp edged-port
```

【相关命令】

- **stp bpdu-protection**
- **stp loop-protection**
- **stp port bpdu-protection**
- **stp root-protection**

1.1.24 stp enable

stp enable 命令用来在端口上开启生成树协议。

undo stp enable 命令用来在端口上关闭生成树协议。

【命令】

```
stp enable
undo stp enable
```

【缺省情况】

端口上的生成树协议处于开启状态。

【视图】

二层以太网接口视图

二层聚合接口视图

【缺省用户角色】

network-admin

【使用指导】

当生成树协议开启后,设备会根据用户配置的生成树工作模式来决定运行在 STP 模式、RSTP 模式、PVST 模式还是 MSTP 模式下。

当生成树协议开启后,系统根据收到的 BPDU 动态维护相应 VLAN 的生成树状态;当生成树协议关闭后,系统将不再维护该状态。

二层以太网接口视图下的配置只对当前端口生效;二层聚合接口视图下的配置只对当前接口生效;聚合成员端口上的配置,只有当成员端口退出聚合组后才能生效。

【举例】

在端口 GigabitEthernet1/0/1 上关闭生成树协议。

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

【相关命令】

- **stp global enable**
- **stp mode**
- **stp vlan enable**

1.1.25 stp global config-digest-snooping

stp global config-digest-snooping 命令用来全局开启摘要侦听功能。

undo stp global config-digest-snooping 命令用来全局关闭摘要侦听功能。

【命令】

```
stp global config-digest-snooping
undo stp global config-digest-snooping
```

【缺省情况】

摘要侦听功能处于全局关闭状态。

【视图】

系统视图

【缺省用户角色】

network-admin

【使用指导】

只有当全局和端口上都开启了摘要侦听功能后,该功能才能生效。开启摘要侦听功能时,建议先在所有与第三方厂商设备相连的端口上开启该功能,再全局开启该功能,以一次性让所有端口的配置生效,从而减少对网络的冲击。

【举例】

先在端口 GigabitEthernet1/0/1 上开启摘要侦听功能,再全局开启摘要侦听功能。

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] stp config-digest-snooping
```

```
[Sysname-GigabitEthernet1/0/1] quit
[Sysname] stp global config-digest-snooping
```

【相关命令】

- **display stp**
- **stp config-digest-snooping**

1.1.26 stp global enable

stp global enable 命令用来全局开启生成树协议。

undo stp global enable 命令用来全局关闭生成树协议。

【命令】

```
stp global enable
undo stp global enable
```

【缺省情况】

对于 S5000V3-EI、S5000E-X 系列交换机，缺省情况下，全局生成树协议处于关闭状态。

对于其他系列交换机：

- 空配置启动时，使用软件功能缺省值，全局生成树协议处于关闭状态。
- 出厂配置启动时，使用软件功能出厂值，全局生成树协议处于开启状态。

关于空配置启动和出厂配置启动的详细介绍，请参见“基础配置指导”中的“配置文件管理”。

【视图】

系统视图

【缺省用户角色】

network-admin

【使用指导】

当生成树协议开启后，设备会根据用户配置的生成树工作模式来决定运行在 STP 模式、RSTP 模式、PVST 模式还是 MSTP 模式下。

当生成树协议开启后，系统根据收到的 BPDU 动态维护相应 VLAN 的生成树状态；当生成树协议关闭后，系统将不再维护该状态。

【举例】

```
# 全局开启生成树协议。
<Sysname> system-view
[Sysname] stp global enable
```

【相关命令】

- **stp enable**
- **stp mode**

1.1.27 stp global mcheck

stp global mcheck 命令用来全局执行 mCheck 操作。

【命令】

```
stp global mcheck
```

【视图】

系统视图

【缺省用户角色】

network-admin

【使用指导】

在运行 MSTP、RSTP 或 PVST 的设备上，若某端口连接着运行 STP 协议的设备，该端口收到 STP 报文后会自动迁移到 STP 模式。同时满足以下情况，该端口将无法自动迁移回原有模式：

- 当对端运行 STP 协议的设备关机或撤走。
- 该端口无法感知变化。

此时需要通过执行 mCheck 操作将其手工迁移回原有模式。

设备会根据用户配置的生成树工作模式来决定运行在 STP 模式、RSTP 模式、PVST 模式还是 MSTP 模式下。

只有当生成树的工作模式为 MSTP 模式、RSTP 模式或 PVST 模式时执行本命令才有效。

【举例】

全局执行 mCheck 操作。

```
<Sysname> system-view  
[Sysname] stp global mcheck
```

【相关命令】

- **stp mcheck**
- **stp mode**

1.1.28 stp ignore-pvid-inconsistency

stp ignore-pvid-inconsistency 命令用来关闭 PVST 的 PVID 不一致保护功能。

undo stp ignore-pvid-inconsistency 命令用来开启 PVST 的 PVID 不一致保护功能。

【命令】

```
stp ignore-pvid-inconsistency  
undo stp ignore-pvid-inconsistency
```

【缺省情况】

PVST 的 PVID 不一致保护功能处于开启状态。

【视图】

系统视图

【缺省用户角色】

network-admin

【使用指导】

本命令在 PVST 工作模式下才能生效。

关闭 PVST 的 PVID 不一致保护功能后，如果链路两端端口 PVID 不一致，为了避免生成树的计算错误，需要注意：

- 除了 VLAN 1，本端所在设备不能创建对端 PVID 对应的 VLAN，同样，对端也不能创建本端 PVID 对应的 VLAN。
- 本端端口的链路类型是 Hybrid 时，建议本端所在设备不创建以 Untagged 方式允许通过的 VLAN，同样，对端也不创建本端 Untagged 方式允许通过的 VLAN。
- 建议链路对端设备也关闭 PVST 的 PVID 不一致保护功能。

【举例】

在 PVST 模式下，关闭 PVST 的 PVID 不一致保护功能。

```
<Sysname> system-view
[Sysname] stp mode pvst
[Sysname] stp ignore-pvid-inconsistency
```

1.1.29 stp log enable tc

stp log enable tc 命令用来配置在 PVST 模式下设备检测或接收到 TC 报文时打印日志信息。

undo stp log enable tc 命令用来恢复缺省情况。

【命令】

```
stp log enable tc
undo stp log enable tc
```

【缺省情况】

PVST 模式下设备检测或接收到 TC 报文后，不打印日志信息。

【视图】

系统视图

【缺省用户角色】

network-admin

【使用指导】

本命令仅在 PVST 模式下生效。

【举例】

配置在 PVST 模式下，设备检测或接收到 TC 报文，打印日志信息。

```
<Sysname> system-view
[Sysname] stp log enable tc
```

1.1.30 stp loop-protection

stp loop-protection 命令用来开启端口的环路保护功能。

undo stp loop-protection 命令用来关闭端口的环路保护功能。

【命令】

```
stp loop-protection
undo stp loop-protection
```

【缺省情况】

端口的环路保护功能处于关闭状态。

【视图】

二层以太网接口视图
二层聚合接口视图

【缺省用户角色】

network-admin

【使用指导】

在同一个端口上，不允许同时配置边缘端口和环路保护功能，或者同时配置根保护功能和环路保护功能。

二层以太网接口视图下的配置只对当前端口生效；二层聚合接口视图下的配置只对当前接口生效；聚合成员端口上的配置，只有当成员端口退出聚合组后才能生效。

【举例】

```
# 在端口 GigabitEthernet1/0/1 上开启环路保护功能。
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] stp loop-protection
```

【相关命令】

- **stp edged-port**
- **stp root-protection**

1.1.31 stp max-hops

stp max-hops 命令用来配置 MST 域的最大跳数，该跳数用来限制 MST 域的规模。

undo stp max-hops 命令用来恢复缺省情况。

【命令】

```
stp max-hops hops
undo stp max-hops
```

【缺省情况】

MST 域的最大跳数为 20 跳。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

hops: 表示最大跳数，取值范围为 1~40。

【举例】

配置 MST 域的最大跳数为 35 跳。

```
<Sysname> system-view
[Sysname] stp max-hops 35
```

【相关命令】

- **display stp**

1.1.32 stp mcheck

stp mcheck 命令用来在端口上执行 mCheck 操作。

【命令】

stp mcheck

【视图】

二层以太网接口视图

二层聚合接口视图

【缺省用户角色】

network-admin

【使用指导】

在运行 MSTP、RSTP 或 PVST 的设备上，若某端口连接着运行 STP 协议的设备，该端口收到 STP 报文后会自动迁移到 STP 模式。同时满足以下情况，该端口将无法自动迁移回原有模式：

- 当对端运行 STP 协议的设备关机或撤走。
- 该端口无法感知变化。

此时需要通过执行 mCheck 操作将其手工迁移回原有模式。

当运行 STP 的设备 A、未开启生成树协议的设备 B 和运行 RSTP/MSTP/PVST 的设备 C 三者顺次相连时，设备 B 将透传 STP 报文，设备 C 上连接设备 B 的端口将迁移到 STP 模式。在设备 B 上开启生成树协议后，若想使设备 B 与设备 C 之间运行 RSTP/MSTP/PVST 协议，除了要在设备 B 上配置生成树的工作模式为 RSTP/MSTP/PVST 外，还要在设备 B 与设备 C 相连的端口上都执行 mCheck 操作。

设备会根据用户配置的生成树工作模式来决定运行在 STP 模式、RSTP 模式、PVST 模式还是 MSTP 模式下。

只有当生成树的工作模式为 MSTP 模式、RSTP 模式或 PVST 模式时执行本命令才有效。

二层以太网接口视图下的配置只对当前端口生效；二层聚合接口视图下的配置只对当前接口生效；聚合成员端口上的配置，只有当成员端口退出聚合组后才能生效。

【举例】

在端口 GigabitEthernet1/0/1 上执行 mCheck 操作。

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

```
[Sysname-GigabitEthernet1/0/1] stp mcheck
```

【相关命令】

- **stp global mcheck**
- **stp mode**

1.1.33 stp mode

stp mode 命令用来配置生成树的工作模式。

undo stp mode 命令用来恢复缺省情况。

【命令】

```
stp mode { mstp | pvst | rstp | stp }  
undo stp mode
```

【缺省情况】

生成树工作模式为 MSTP 模式。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

mstp: 配置生成树的工作模式为 MSTP 模式。

pvst: 配置生成树的工作模式为 PVST 模式。

rstp: 配置生成树的工作模式为 RSTP 模式。

stp: 配置生成树的工作模式为 STP 模式。

【使用指导】

MSTP 模式兼容 RSTP 模式，RSTP 模式兼容 STP 模式。

PVST 模式与其他模式的兼容性如下：

- 对于 Access 端口：PVST 模式在任意 VLAN 中都能与其他模式互相兼容。
- 对于 Trunk 端口或 Hybrid 端口：PVST 模式仅在 VLAN 1 中能与其他模式互相兼容。

【举例】

配置生成树的工作模式为 STP 模式。

```
<Sysname> system-view  
[Sysname] stp mode stp
```

【相关命令】

- **stp enable**
- **stp global enable**
- **stp global mcheck**
- **stp mcheck**
- **stp vlan enable**

1.1.34 stp no-agreement-check

stp no-agreement-check 命令用来在端口上开启 No Agreement Check 功能。

undo stp no-agreement-check 命令用来在端口上关闭 No Agreement Check 功能。

【命令】

```
stp no-agreement-check
undo stp no-agreement-check
```

【缺省情况】

No Agreement Check 功能处于关闭状态。

【视图】

二层以太网接口视图

二层聚合接口视图

【缺省用户角色】

network-admin

【使用指导】

当且仅当在根端口上开启本功能才生效。

二层以太网接口视图下的配置只对当前端口生效；二层聚合接口视图下的配置只对当前接口生效；聚合成员端口上的配置，只有当成员端口退出聚合组后才能生效。

【举例】

在端口 GigabitEthernet1/0/1 上开启 No Agreement Check 功能。

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] stp no-agreement-check
```

1.1.35 stp pathcost-standard

stp pathcost-standard 命令用来配置缺省路径开销的计算标准。

undo stp pathcost-standard 命令用来恢复缺省情况。

【命令】

```
stp pathcost-standard { dot1d-1998 | dot1t | legacy }
undo stp pathcost-standard
```

【缺省情况】

缺省路径开销的计算标准为 **legacy**。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

dot1d-1998: 表示按照 IEEE 802.1D-1998 标准来计算缺省路径开销。

dot1t: 表示按照 IEEE 802.1t 标准来计算缺省路径开销。

legacy: 表示按照私有标准来计算缺省路径开销。

【使用指导】

改变缺省路径开销的计算标准，将使端口的路径开销值恢复为缺省值。

【举例】

配置按照 IEEE 802.1D-1998 标准来计算缺省路径开销。

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

```
[Sysname] stp pathcost-standard dot1d-1998
```

【相关命令】

- **display stp**
- **stp cost**

1.1.36 stp point-to-point

stp point-to-point 命令用来配置端口的链路类型。

undo stp point-to-point 命令用来恢复缺省情况。

【命令】

```
stp point-to-point { auto | force-false | force-true }
```

```
undo stp point-to-point
```

【缺省情况】

端口的链路类型为 **auto**，即由系统自动检测与本端口相连的链路是否为点对点链路。

【视图】

二层以太网接口视图

二层聚合接口视图

【缺省用户角色】

network-admin

【参数】

auto: 表示自动检测与本端口相连的链路是否为点对点链路。

force-false: 表示与本端口相连的链路不是点对点链路。

force-true: 表示与本端口相连的链路是点对点链路。

【使用指导】

当端口与非点对点链路相连时，端口的状态无法快速迁移。

如果某端口是二层聚合接口或其工作在全双工模式下，则可以将该端口配置为与点对点链路相连。

通常建议使用缺省配置，由系统进行自动检测。

在 MSTP 或 PVST 模式下，如果某端口配置了命令 **stp point-to-point force-false** 或者命令 **stp point-to-point force-true**，那么该配置对该端口所属的所有 MSTI 都有效。

如果某端口被配置为与点对点链路相连，但与该端口实际相连的物理链路不是点对点链路，则有可能引入临时回路。

二层以太网接口视图下的配置只对当前端口生效；二层聚合接口视图下的配置只对当前接口生效；聚合成员端口上的配置，只有当成员端口退出聚合组后才能生效。

【举例】

配置与端口 GigabitEthernet1/0/1 相连的链路是点对点链路。

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] stp point-to-point force-true
```

【相关命令】

- **display stp**

1.1.37 stp port bpdu-protection

stp port bpdu-protection 命令用来配置端口的 BPDU 保护功能。

undo stp port bpdu-protection 命令用来恢复缺省情况。

【命令】

```
stp port bpdu-protection { enable | disable }
undo stp port bpdu-protection
```

【缺省情况】

未配置开启或关闭端口的 BPDU 保护功能。缺省情况下，如果全局的 BPDU 保护功能处于开启状态，则边缘端口的 BPDU 保护功能处于开启状态；如果全局的 BPDU 保护功能处于关闭状态，则边缘端口的 BPDU 保护功能处于关闭状态。

【视图】

二层以太网接口视图

二层聚合接口视图

【缺省用户角色】

network-admin

【参数】

enable：表示开启端口的 BPDU 保护功能。

disable：表示关闭端口的 BPDU 保护功能。

【使用指导】

二层以太网端口视图下的配置只对当前端口生效；二层聚合接口视图下的配置只对当前接口生效；聚合成员端口上的配置，只有当成员端口退出聚合组后才能生效。

【举例】

配置端口 GigabitEthernet1/0/1 开启 BPDU 保护功能。

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] stp port bpdu-protection enable
```

【相关命令】

- **stp bpdu-protection**
- **stp edged-port**

1.1.38 stp port priority

stp port priority 命令用来配置端口的优先级。端口优先级可以影响端口在生成树上的角色选择。

undo stp port priority 命令用来恢复缺省情况。

【命令】

```
stp [ instance instance-list | vlan vlan-id-list ] port priority priority
undo stp [ instance instance-list | vlan vlan-id-list ] port priority
```

【缺省情况】

端口的优先级为 128。

【视图】

二层以太网接口视图
二层聚合接口视图

【缺省用户角色】

network-admin

【参数】

instance instance-list: 表示配置端口在 MSTP 指定 MSTI 的优先级。*instance-list* 为 MSTI 列表, 表示多个 MSTI, 表示方式为 *instance-list* = { *instance-id1* [**to** *instance-id2*] } &<1-10>。其中, *instance-id* 为 MSTI 的编号, 取值范围为 0~4094, 0 表示 CIST。 *instance-id2* 的值大于等于 *instance-id1* 的值。 &<1-10> 表示前面的参数最多可以输入 10 次。如果未指定本参数, 表示配置端口在 MSTP CIST 或 STP/RSTP 的优先级。

vlan vlan-id-list: 表示配置端口在 PVST 指定 VLAN 的优先级。*vlan-id-list* 为 VLAN 列表, 表示多个 VLAN。表示方式为 *vlan-id-list* = { *vlan-id1* [**to** *vlan-id2*] } &<1-10>。其中, *vlan-id* 为 VLAN 的编号, 取值范围为 1~4094。 *vlan-id2* 的值大于等于 *vlan-id1* 的值。 &<1-10> 表示前面的参数最多可以输入 10 次。

priority: 表示端口的优先级, 取值范围为 0~240, 以 16 为步长, 如 0、16、32 等。

【使用指导】

通常, 端口优先级的数值越小, 端口的优先级就越高。如果设备的所有端口都采用相同的优先级数值, 则端口优先级的高低就取决于该端口索引号的大小, 即索引号越小优先级越高。

二层以太网接口视图下的配置只对当前端口生效; 二层聚合接口视图下的配置只对当前接口生效; 聚合成员端口上的配置, 只有当成员端口退出聚合组后才能生效。

如果未指定 MSTI 和 VLAN, 则表示配置端口在 MSTP CIST 或 STP/RSTP 的优先级。

【举例】

在 MSTP 模式下，配置端口 GigabitEthernet1/0/1 在 MSTI 2 上的优先级为 16。

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] stp instance 2 port priority 16
```

在 PVST 模式下，配置端口 GigabitEthernet1/0/1 在 VLAN 2 上的优先级为 16。

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] stp vlan 2 port priority 16
```

【相关命令】

- **display stp**

1.1.39 stp port shutdown permanent

stp port shutdown permanent 命令用来配置被 BPDU 保护功能关闭的端口不再自动恢复。

undo stp port shutdown permanent 命令用来恢复缺省情况。

【命令】

```
stp port shutdown permanent
undo stp port shutdown permanent
```

【缺省情况】

被 BPDU 保护功能关闭的端口会自动恢复。

【视图】

系统视图

【缺省用户角色】

network-admin

【使用指导】

被关闭的端口的自动恢复时间受 **shutdown-interval time** 命令控制。有关 **shutdown-interval** 的详细介绍，请参见“基础配置指导”中的“设备管理”。

配置 **stp port shutdown permanent** 命令后，端口被 BPDU 保护功能关闭，再执行 **undo stp port shutdown permanent** 命令，端口不会 UP，端口保持关闭状态，需要执行 **undo shutdown** 命令才能恢复。

端口被 BPDU 保护功能关闭，再配置 **stp port shutdown permanent** 命令，此时端口经过自动恢复时间后会变为 UP 状态，当再次被生成树保护功能关闭时，端口才不会恢复，保持关闭状态。

【举例】

配置被 BPDU 保护功能关闭的端口不再自动恢复。

```
<Sysname> system-view
[Sysname] stp port shutdown permanent
```

1.1.40 stp port-log

stp port-log 命令用来打开端口状态变化信息显示开关。

undo stp port-log 命令用来关闭端口状态变化信息显示开关。

【命令】

```
stp port-log { all | instance instance-list | vlan vlan-id-list }
undo stp port-log { all | instance instance-list | vlan vlan-id-list }
```

【缺省情况】

端口状态变化信息显示开关处于关闭状态。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

all: 表示打开或关闭 MSTP/PVST 所有 MSTI/VLAN 中的端口状态变化信息显示开关。

instance instance-list: 表示打开或关闭 MSTP 指定 MSTI 中的端口状态变化信息显示开关；如果指定了 MSTI 0，则表示打开或关闭 STP/RSTP 的端口状态变化信息显示开关。

instance-list 为 MSTI 列表，表示多个 MSTI，表示方式为 **instance-list = { instance-id1 [to instance-id2] } <1-10>**。其中，**instance-id** 为 MSTI 的编号，取值范围为 0~4094，0 表示 CIST。**instance-id2** 的值大于等于 **instance-id1** 的值。**<1-10>** 表示前面的参数最多可以输入 10 次。

vlan vlan-id-list: 表示打开或关闭 PVST 指定 VLAN 中的端口状态变化信息显示开关。

vlan-id-list 为 VLAN 列表，表示方式为 **vlan-id-list = { vlan-id1 [to vlan-id2] } <1-10>**。其中，**vlan-id** 为 VLAN 的编号，取值范围为 1~4094。**vlan-id2** 的值大于等于 **vlan-id1** 的值。**<1-10>** 表示前面的参数最多可以输入 10 次。

【举例】

在 MSTP 模式下，打开 MSTI 2 中的端口状态变化信息显示开关。

```
<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
GigabitEthernet1/0/1 has been set to discarding state.
```

```
%Aug 16 00:49:41:856 2011 Sysname STP/3/STP_FORWARDING: Instance 2's port
GigabitEthernet1/0/2 has been set to forwarding state.
```

// 上述信息表明：在 MSTI 2 中，GigabitEthernet1/0/1 的端口状态变为 Discarding，GigabitEthernet1/0/2 的端口状态变为 Forwarding。

在 PVST 模式下，打开 VLAN 1~4094 中的端口状态变化信息显示开关。

```
<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 GigabitEthernet1/0/1 has
been set to discarding state.
```


%Aug 16 00:49:41:856 2006 Sysname STP/3/STP_FORWARDING: VLAN 2's GigabitEthernet1/0/2 has been set to forwarding state.

// 上述信息表明：在 VLAN 2 中，GigabitEthernet1/0/1 的端口状态变为 Discarding，GigabitEthernet1/0/2 的端口状态变为 Forwarding。

1.1.41 stp priority

stp priority 命令用来配置设备的优先级。

undo stp priority 命令用来恢复缺省情况。

【命令】

```
stp [ instance instance-list | vlan vlan-id-list ] priority priority
undo stp [ instance instance-list | vlan vlan-id-list ] priority
```

【缺省情况】

设备的优先级为 32768。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

instance instance-list：表示配置设备在 MSTP 指定 MSTI 的优先级。instance-list 为 MSTI 列表，表示多个 MSTI，表示方式为 instance-list = { instance-id1 [to instance-id2] } &<1-10>。其中，instance-id 为 MSTI 的编号，取值范围为 0~4094，0 表示 CIST。instance-id2 的值大于等于 instance-id1 的值。&<1-10>表示前面的参数最多可以输入 10 次。如果未指定本参数，表示配置设备在 MSTP CIST 或 STP/RSTP 的优先级。

vlan vlan-id-list：表示配置设备在 PVST 指定 VLAN 的优先级。vlan-id-list 为 VLAN 列表，表示多个 VLAN。表示方式为 vlan-id-list = { vlan-id1 [to vlan-id2] } &<1-10>。其中，vlan-id 为 VLAN 的编号，取值范围为 1~4094。vlan-id2 的值大于等于 vlan-id1 的值。&<1-10>表示前面的参数最多可以输入 10 次。

priority：表示设备的优先级，该数值越小表示优先级越高。取值范围为 0~61440，步长为 4096，即设备可以设置 16 个优先级取值，如 0、4096、8192 等。

【使用指导】

如果未指定 MSTI 和 VLAN，则表示配置设备在 MSTP CIST 或 STP/RSTP 中的优先级。

【举例】

在 MSTP 模式下，配置设备在 MSTI 1 中的优先级为 4096。

```
<Sysname> system-view
[Sysname] stp instance 1 priority 4096
```

在 PVST 模式下，配置设备在 VLAN 1 中的优先级为 4096。

```
<Sysname> system-view
[Sysname] stp vlan 1 priority 4096
```

1.1.42 stp pvst-bpdu-protection

stp pvst-bpdu-protection 命令用来开启 MSTP 的 PVST 报文保护功能。

undo stp pvst-bpdu-protection 命令用来关闭 MSTP 的 PVST 报文保护功能。

【命令】

```
stp pvst-bpdu-protection
undo stp pvst-bpdu-protection
```

【缺省情况】

MSTP 的 PVST 报文保护功能处于关闭状态。

【视图】

系统视图

【缺省用户角色】

network-admin

【使用指导】

在 MSTP 模式下，设备上开启了 PVST 报文保护功能后，如果某些端口收到了 PVST 报文，系统就将这些端口关闭。被关闭的端口在经过一定时间间隔之后将被自动重新打开，关闭的时间间隔通过 **shutdown-interval** 命令配置。

【举例】

在 MSTP 模式下，开启 MSTP 的 PVST 报文保护功能。

```
<Sysname> system-view
[Sysname] stp pvst-bpdu-protection
```

【相关命令】

- **shutdown-interval**（基础配置指导/设备管理）

1.1.43 stp region-configuration

stp region-configuration 命令用来进入 MST 域视图。

undo stp region-configuration 命令用来将 MST 域的配置恢复为缺省值。

【命令】

```
stp region-configuration
undo stp region-configuration
```

【缺省情况】

MST 域的三个参数均取缺省值，即：MST 域名为设备的桥 MAC 地址、所有 VLAN 都映射到 CIST 上、MSTP 修订级别为 0。

【视图】

系统视图

【缺省用户角色】

network-admin

【使用指导】

进入 MST 域视图后，用户可以对 MST 域的相关参数（域名、VLAN 映射表和修订级别）进行配置。

【举例】

```
# 进入 MST 域视图。
<Sysname> system-view
[Sysname] stp region-configuration
[Sysname-mst-region]
```

1.1.44 stp role-restriction

stp role-restriction 命令用来开启端口角色限制功能。

undo stp role-restriction 命令用来关闭端口角色限制功能。

【命令】

```
stp role-restriction
undo stp role-restriction
```

【缺省情况】

端口角色限制功能处于关闭状态。

【视图】

二层以太网接口视图

二层聚合接口视图

【缺省用户角色】

network-admin

【使用指导】

当开启了某端口的端口角色限制功能之后，该端口将不能被计算为根端口。

二层以太网接口视图下的配置只对当前端口生效；二层聚合接口视图下的配置只对当前接口生效；聚合成员端口上的配置，只有当成员端口退出聚合组后才能生效。

【举例】

```
# 开启端口 GigabitEthernet1/0/1 的端口角色限制功能。
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] stp role-restriction
```

1.1.45 stp root primary

stp root primary 命令用来配置设备为根桥。

undo stp root 命令用来恢复缺省情况。

【命令】

```
stp [ instance instance-list | vlan vlan-id-list ] root primary
undo stp [ instance instance-list | vlan vlan-id-list ] root
```

【缺省情况】

设备不是根桥。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

instance *instance-list*: 表示配置当前设备为 MSTP 指定 MSTI 的根桥。*instance-list* 为 MSTI 列表, 表示多个 MSTI, 表示方式为 *instance-list* = { *instance-id1* [**to** *instance-id2*] } &<1-10>。其中, *instance-id* 为 MSTI 的编号, 取值范围为 0~4094, 0 表示 CIST。*instance-id2* 的值大于等于 *instance-id1* 的值。&<1-10>表示前面的参数最多可以输入 10 次。

vlan *vlan-id-list*: 表示配置当前设备为 PVST 指定 VLAN 的根桥。*vlan-id-list* 为 VLAN 列表, 表示多个 VLAN。表示方式为 *vlan-id-list* = { *vlan-id1* [**to** *vlan-id2*] } &<1-10>。其中, *vlan-id* 为 VLAN 的编号, 取值范围为 1~4094。*vlan-id2* 的值大于等于 *vlan-id1* 的值。&<1-10>表示前面的参数最多可以输入 10 次。

【使用指导】

当设备一旦被配置为根桥之后, 便不能再修改该设备的优先级。

如果未指定 MSTI 和 VLAN, 则表示配置当前设备为 MSTP CIST 或 STP/RSTP 的根桥。

【举例】

在 MSTP 模式下, 配置设备为 MSTI 1 的根桥。

```
<Sysname> system-view
[Sysname] stp instance 1 root primary
```

在 PVST 模式下, 配置设备为 VLAN 1 的根桥。

```
<Sysname> system-view
[Sysname] stp vlan 1 root primary
```

【相关命令】

- **stp priority**
- **stp root secondary**

1.1.46 stp root secondary

stp root secondary 命令用来配置设备为备份根桥。

undo stp root 命令用来恢复缺省情况。

【命令】

```
stp [ instance instance-list | vlan vlan-id-list ] root secondary
undo stp [ instance instance-list | vlan vlan-id-list ] root
```

【缺省情况】

设备不是备份根桥。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

instance instance-list: 表示配置当前设备为 MSTP 指定 MSTI 的备份根桥。
instance-list 为 MSTI 列表，表示多个 MSTI，表示方式为 *instance-list* = { *instance-id1* [**to** *instance-id2*] }&<1-10>。其中，*instance-id* 为 MSTI 的编号，取值范围为 0~4094，0 表示 CIST。*instance-id2* 的值大于等于 *instance-id1* 的值。&<1-10> 表示前面的参数最多可以输入 10 次。

vlan vlan-id-list: 表示配置当前设备为 PVST 指定 VLAN 的备份根桥。*vlan-id-list* 为 VLAN 列表，表示多个 VLAN。表示方式为 *vlan-id-list* = { *vlan-id1* [**to** *vlan-id2*] }&<1-10>。其中，*vlan-id* 为 VLAN 的编号，取值范围为 1~4094。*vlan-id2* 的值大于等于 *vlan-id1* 的值。&<1-10> 表示前面的参数最多可以输入 10 次。

【使用指导】

当设备一旦被配置为备份根桥之后，便不能再修改该设备的优先级。

如果未指定 MSTI 和 VLAN，则表示配置当前设备为 MSTP CIST 或 STP/RSTP 的备份根桥。

【举例】

在 MSTP 模式下，配置设备为 MSTI 1 的备份根桥。

```
<Sysname> system-view
[Sysname] stp instance 1 root secondary
```

在 PVST 模式下，配置设备为 VLAN 1 的备份根桥。

```
<Sysname> system-view
[Sysname] stp vlan 1 root secondary
```

【相关命令】

- **stp priority**
- **stp root primary**

1.1.47 stp root-protection

stp root-protection 命令用来开启端口的根保护功能。

undo stp root-protection 命令用来关闭端口的根保护功能。

【命令】

```
stp root-protection
undo stp root-protection
```

【缺省情况】

端口上的根保护功能处于关闭状态。

【视图】

二层以太网接口视图

二层聚合接口视图

【缺省用户角色】

network-admin

【使用指导】

在同一个端口上，不允许同时配置根保护功能和环路保护功能。

二层以太网接口视图下的配置只对当前端口生效；二层聚合接口视图下的配置只对当前接口生效；聚合成员端口上的配置，只有当成员端口退出聚合组后才能生效。

【举例】

在端口 GigabitEthernet1/0/1 上开启根保护功能。

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] stp root-protection
```

【相关命令】

- **stp edged-port**
- **stp loop-protection**

1.1.48 stp tc-protection

stp tc-protection 命令用来开启防 TC-BPDU 攻击保护功能。

undo stp tc-protection 命令用来关闭防 TC-BPDU 攻击保护功能。

【命令】

```
stp tc-protection
undo stp tc-protection
```

【缺省情况】

防 TC-BPDU 攻击保护功能处于开启状态。

【视图】

系统视图

【缺省用户角色】

network-admin

【使用指导】

当开启了防 TC-BPDU 攻击保护功能后，如果设备在单位时间（固定为十秒）内收到 TC-BPDU 的次数大于 **stp tc-protection threshold** 命令所指定的最高次数（假设为 N 次），那么该设备在这段时间之内将只进行 N 次刷新转发地址表项的操作，而对于超出 N 次的那些 TC-BPDU，设备会在这段时间过后再统一进行一次地址表项刷新的操作，这样就可以避免频繁地刷新转发地址表项。

【举例】

关闭防 TC-BPDU 攻击保护功能。

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

```
[Sysname] undo stp tc-protection
```

【相关命令】

- **stp tc-protection threshold**

1.1.49 stp tc-protection threshold

stp tc-protection threshold 命令用来配置在单位时间(固定为十秒)内,设备收到 TC-BPDU 后一定时间内,允许收到 TC-BPDU 后立即刷新转发地址表项的最高次数。

undo stp tc-protection threshold 命令用来恢复缺省情况。

【命令】

```
stp tc-protection threshold number
```

```
undo stp tc-protection threshold
```

【缺省情况】

在单位时间(固定为十秒)内,设备收到 TC-BPDU 后立即刷新转发地址表项的最高次数为 6。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

number: 表示在单位时间(固定为十秒)内,设备收到 TC-BPDU 后立即刷新转发地址表项的最高次数,取值范围为 1~255。

【举例】

配置在单位时间(固定为十秒)内,设备收到 TC-BPDU 后一定时间内,允许收到 TC-BPDU 后立即刷新转发地址表项的最高次数为 10。

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

```
[Sysname] stp tc-protection threshold 10
```

【相关命令】

- **stp tc-protection**

1.1.50 stp tc-restriction

stp tc-restriction 命令用来开启 TC-BPDU 传播限制功能。

undo stp tc-restriction 命令用来关闭 TC-BPDU 传播限制功能。

【命令】

```
stp tc-restriction
```

```
undo stp tc-restriction
```

【缺省情况】

TC-BPDU 传播限制功能处于关闭状态。

【视图】

二层以太网接口视图
二层聚合接口视图

【缺省用户角色】

network-admin

【使用指导】

当开启了某端口的 TC-BPDU 传播限制功能之后，该端口将不再向其它端口传播 TC-BPDU，也不删除本机的转发地址表项。

二层以太网接口视图下的配置只对当前端口生效；二层聚合接口视图下的配置只对当前接口生效；聚合成员端口上的配置，只有当成员端口退出聚合组后才能生效。

【举例】

开启端口 GigabitEthernet1/0/1 的 TC-BPDU 传播限制功能。

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] stp tc-restriction
```

1.1.51 stp tc-snooping

stp tc-snooping 命令用来开启 TC Snooping 功能。

undo stp tc-snooping 命令用来关闭 TC Snooping 功能。

【命令】

```
stp tc-snooping
undo stp tc-snooping
```

【缺省情况】

TC Snooping 功能处于关闭状态。

【视图】

系统视图

【缺省用户角色】

network-admin

【使用指导】

TC Snooping 功能与生成树协议互斥，因此在开启 TC Snooping 功能之前必须全局关闭生成树协议。

【举例】

全局关闭生成树协议，并开启 TC Snooping 功能。

```
<Sysname> system-view
[Sysname] undo stp global enable
[Sysname] stp tc-snooping
```

【相关命令】

- **stp global enable**

1.1.52 stp timer forward-delay

stp timer forward-delay 命令用来配置 Forward Delay 时间参数。

undo stp timer forward-delay 命令用来恢复缺省情况。

【命令】

```
stp [ vlan vlan-id-list ] timer forward-delay time  
undo stp [ vlan vlan-id-list ] timer forward-delay
```

【缺省情况】

Forward Delay 为 1500 厘秒。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

vlan *vlan-id-list*: 表示配置 PVST 指定 VLAN 的 Forward Delay 时间参数。*vlan-id-list* 为 VLAN 列表，表示多个 VLAN。表示方式为 *vlan-id-list* = { *vlan-id1* [**to** *vlan-id2*] } &<1-10>。其中，*vlan-id* 为 VLAN 的编号，取值范围为 1~4094。*vlan-id2* 的值大于等于 *vlan-id1* 的值。&<1-10>表示前面的参数最多可以输入 10 次。如果未指定本参数，表示配置 STP/RSTP/MSTP 的 Forward Delay 时间参数。

time: 表示 Forward Delay 的时间值，取值范围为 400~3000，步长为 100，单位为厘秒。

【使用指导】

Forward Delay 用于确定状态迁移的延迟时间。为了防止产生临时环路，生成树协议在端口由 Discarding 状态向 Forwarding 状态迁移的过程中设置了 Learning 状态作为过渡，并规定状态迁移需要等待 Forward Delay 时间，以保持与远端的设备状态切换同步。

通常情况下不建议使用本命令直接调整 Forward Delay 时间参数。由于该时间参数的取值与网络规模有关，因此建议通过使用 **stp bridge-diameter** 命令调整网络直径，使生成树协议自动调整该时间参数的值。当网络直径取缺省值时，该时间参数也取缺省值。

【举例】

在 MSTP 模式下，配置 Forward Delay 为 2000 厘秒。

```
<Sysname> system-view  
[Sysname] stp timer forward-delay 2000
```

在 PVST 模式下，配置 VLAN 2 的 Forward Delay 为 2000 厘秒。

```
<Sysname> system-view  
[Sysname] stp vlan 2 timer forward-delay 2000
```

【相关命令】

- **stp bridge-diameter**
- **stp timer hello**
- **stp timer max-age**

1.1.53 stp timer hello

stp timer hello 命令用来配置 Hello Time 时间参数。

undo stp timer hello 命令用来恢复缺省情况。

【命令】

```
stp [ vlan vlan-id-list ] timer hello time  
undo stp [ vlan vlan-id-list ] timer hello
```

【缺省情况】

Hello Time 为 200 厘秒。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

vlan *vlan-id-list*: 表示配置 PVST 指定 VLAN 的 Hello Time 时间参数。*vlan-id-list* 为 VLAN 列表，表示多个 VLAN。表示方式为 *vlan-id-list* = { *vlan-id1* [to *vlan-id2*] } <1-10>。其中，*vlan-id* 为 VLAN 的编号，取值范围为 1~4094。*vlan-id2* 的值大于等于 *vlan-id1* 的值。<1-10> 表示前面的参数最多可以输入 10 次。如果未指定本参数，表示配置 STP/RSTP/MSTP 的 Hello Time 时间参数。

time: 表示 Hello Time 的时间值，取值范围为 100~1000，步长为 100，单位为厘秒。

【使用指导】

Hello Time 用于检测链路是否存在故障。生成树协议每隔 Hello Time 时间会发送 BPDU，以确认链路是否存在故障。如果设备在 Hello Time 时间内没有收到 BPDU，则会由于消息超时而重新计算生成树。

通常情况下不建议使用本命令直接调整 Hello Time 时间参数。由于该时间参数的取值与网络规模有关，因此建议通过使用 **stp bridge-diameter** 命令调整网络直径，使生成树协议自动调整该时间参数的值。当网络直径取缺省值时，该时间参数也取缺省值。

【举例】

在 MSTP 模式下，配置 Hello Time 为 400 厘秒。

```
<Sysname> system-view  
[Sysname] stp timer hello 400
```

在 PVST 模式下，配置 VLAN 2 的 Hello Time 为 400 厘秒。

```
<Sysname> system-view  
[Sysname] stp vlan 2 timer hello 400
```

【相关命令】

- **stp bridge-diameter**
- **stp timer forward-delay**
- **stp timer max-age**

1.1.54 stp timer max-age

stp timer max-age 命令用来配置 Max Age 时间参数。

undo stp timer max-age 命令用来恢复缺省情况。

【命令】

```
stp [ vlan vlan-id-list ] timer max-age time  
undo stp [ vlan vlan-id-list ] timer max-age
```

【缺省情况】

Max Age 为 2000 厘秒。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

vlan *vlan-id-list*: 表示配置 PVST 指定 VLAN 的 Max Age 时间参数。*vlan-id-list* 为 VLAN 列表，表示多个 VLAN。表示方式为 *vlan-id-list* = { *vlan-id1* [**to** *vlan-id2*] } <1-10>。其中，*vlan-id* 为 VLAN 的编号，取值范围为 1~4094。*vlan-id2* 的值大于等于 *vlan-id1* 的值。<1-10> 表示前面的参数最多可以输入 10 次。如果未指定本参数，表示配置 STP/RSTP/MSTP 的 Max Age 时间参数。

time: 表示 Max Age 的时间值，取值范围为 600~4000，步长为 100，单位为厘秒。

【使用指导】

Max Age 用于确定 BPDU 是否超时。在 MSTP 的 CIST 上，设备根据 Max Age 时间来确定端口收到的 BPDU 是否超时。如果端口收到的 BPDU 超时，则需要对该 MSTI 重新计算。Max Age 时间对 MSTP 的 MSTI 无效。

通常情况下不建议使用本命令直接调整 Max Age 时间参数。由于该时间参数的取值与网络规模有关，因此建议通过使用 **stp bridge-diameter** 命令调整网络直径，使生成树协议自动调整该时间参数的值。当网络直径取缺省值时，该时间参数也取缺省值。

【举例】

在 MSTP 模式下，配置 Max Age 为 1000 厘秒。

```
<Sysname> system-view  
[Sysname] stp timer max-age 1000
```

在 PVST 模式下，配置 VLAN 2 的 Max Age 为 1000 厘秒。

```
<Sysname> system-view  
[Sysname] stp vlan 2 timer max-age 1000
```

【相关命令】

- **stp bridge-diameter**
- **stp timer forward-delay**
- **stp timer hello**

1.1.55 stp timer-factor

stp timer-factor 命令用来配置超时时间因子，该因子用来确定设备的超时时间：超时时间 = 超时时间因子 × 3 × Hello Time。

undo stp timer-factor 命令用来恢复缺省情况。

【命令】

```
stp timer-factor factor
undo stp timer-factor
```

【缺省情况】

超时时间因子为 3。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

factor：表示超时时间因子，取值范围为 1~20。

【使用指导】

当网络拓扑结构稳定后，非根桥设备会每隔 Hello Time 时间向周围相连设备转发根桥发出的 BPDU 以确认链路是否存在故障。通常如果设备在 9 倍的 Hello Time 时间内没有收到上游设备发来的 BPDU，就会认为上游设备已经故障，从而重新进行生成树的计算。

对于以下情况，建议将设备的超时时间因子配置为 5~7：

- 有时本端设备在较长时间内收不到对端设备发来的 BPDU，可能是由于对端设备的繁忙导致的（例如，对端设备配置了大量二层接口时），在这种情况下一般不应重新进行生成树的计算，需要延长本端设备的超时时间。
- 稳定的网络中，可以通过延长超时时间来减少网络资源的浪费。

【举例】

```
# 配置超时时间因子为 7。
<Sysname> system-view
[Sysname] stp timer-factor 7
```

【相关命令】

- **stp timer hello**

1.1.56 stp transmit-limit

stp transmit-limit 命令用来配置端口发送 BPDU 的速率。

undo stp transmit-limit 命令用来恢复缺省情况。

【命令】

```
stp transmit-limit limit
undo stp transmit-limit
```

【缺省情况】

端口发送 BPDU 的速率为 10。

【视图】

二层以太网接口视图

二层聚合接口视图

【缺省用户角色】

network-admin

【参数】

limit：表示端口发送 BPDU 的速率，取值范围为 1～255。

【使用指导】

每 Hello Time 时间内端口能够发送的 BPDU 的最大数目=端口发送 BPDU 的速率+Hello Time 时间值。

端口发送 BPDU 的速率越高，每个 Hello Time 内可发送的 BPDU 数量就越多，占用的系统资源也越多。适当配置发送速率一方面可以限制端口发送 BPDU 的速度，另一方面还可以防止在网络拓扑动荡时，生成树协议占用过多的带宽资源。建议用户采用缺省配置。

二层以太网接口视图下的配置只对当前端口生效；二层聚合接口视图下的配置只对当前接口生效；聚合成员端口上的配置，只有当成员端口退出聚合组后才能生效。

【举例】

配置端口 GigabitEthernet1/0/1 发送 BPDU 的速率为 5。

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] stp transmit-limit 5
```

1.1.57 stp vlan enable

stp vlan enable 命令用来在 VLAN 中开启生成树协议。

undo stp enable 命令用来在 VLAN 中关闭生成树协议。

【命令】

```
stp vlan vlan-id-list enable
undo stp vlan vlan-id-list enable
```

【缺省情况】

生成树协议在 VLAN 中处于开启状态。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

vlan vlan-id-list: 开启或关闭指定 VLAN 上的生成树协议。*vlan-id-list* 为 VLAN 列表, 表示多个 VLAN。表示方式为 *vlan-id-list* = { *vlan-id1* [**to** *vlan-id2*] } <1-10>。其中, *vlan-id* 为 VLAN 的编号, 取值范围为 1~4094。*vlan-id2* 的值大于等于 *vlan-id1* 的值。*<1-10>* 表示前面的参数最多可以输入 10 次。

【使用指导】

当生成树协议开启后, 设备会根据用户配置的生成树工作模式来决定运行在 STP 模式、RSTP 模式、MSTP 模式还是 PVST 模式下。

当生成树协议开启后, 系统根据收到的 BPDU 动态维护相应 VLAN 的生成树状态; 当生成树协议关闭后, 系统将不再维护该状态。

【举例】

在 PVST 模式下, 先全局开启生成树协议, 再开启 VLAN 2 中的生成树协议。

```
<Sysname> system-view
[Sysname] stp mode pvst
[Sysname] stp global enable
[Sysname] stp vlan 2 enable
```

【相关命令】

- **stp enable**
- **stp global enable**
- **stp mode**

1.1.58 vlan-mapping modulo

vlan-mapping modulo 命令用来快速配置 VLAN 映射表, 使当前 MST 域内的所有 VLAN 按指定的模值映射到不同的 MSTI 上。

【命令】

```
vlan-mapping modulo modulo
```

【缺省情况】

所有 VLAN 都映射到 CIST (即 MSTI 0) 上。

【视图】

MST 域视图

【缺省用户角色】

network-admin

【参数】

modulo: 表示模值, 取值范围为 1~64。

【使用指导】

不能将同一个 VLAN 映射到不同的 MSTI 上。如果将一个已映射到某 MSTI 的 VLAN 重新映射到另一个 MSTI 时, 原先的映射关系将被取消。

本命令将 VLAN 映射到编号为 $(\text{VLAN ID} - 1) \% \text{modulo} + 1$ 的 MSTI 上。其中， $(\text{VLAN ID} - 1) \% \text{modulo}$ 表示对 $(\text{VLAN ID} - 1)$ 进行求模运算，如模值为 15，则 VLAN 1 映射到 MSTI 1、VLAN 2 映射到 MSTI 2、……、VLAN 15 映射到 MSTI 15、VLAN 16 映射到 MSTI 1，依次类推。

【举例】

将所有 VLAN 按照模 8 映射到不同的 MSTI 上。

```
<Sysname> system-view
[Sysname] stp region-configuration
[Sysname-mst-region] vlan-mapping modulo 8
```

【相关命令】

- **active region-configuration**
- **check region-configuration**
- **display stp region-configuration**
- **region-name**
- **revision-level**

目 录

1 环路检测.....	1-1
1.1 环路检测配置命令.....	1-1
1.1.1 display loopback-detection.....	1-1
1.1.2 loopback-detection action	1-2
1.1.3 loopback-detection enable	1-3
1.1.4 loopback-detection global action	1-4
1.1.5 loopback-detection global enable	1-5
1.1.6 loopback-detection interval-time.....	1-5

1 环路检测

1.1 环路检测配置命令

1.1.1 display loopback-detection

display loopback-detection 命令用来显示环路检测的配置和运行情况。

【命令】

display loopback-detection

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator

【举例】

显示环路检测的配置和运行情况。
<Sysname> display loopback-detection
Loopback detection is enabled.
Loopback detection interval is 30 second(s).
Loopback is detected on following interfaces:
Interface Action mode VLANs
GigabitEthernet1/0/3 None 10

表1-1 display loopback-detection 命令显示信息描述表

字段	描述
Loopback detection is enabled	环路检测功能已开启
Loopback detection is disabled	环路检测功能已关闭
Loopback detection interval is 30 second(s)	环路检测的时间间隔为30秒
Loopback is detected on following interfaces	下列端口被检测到存在环路
Interface	端口名称

字段	描述
Action mode	环路检测的处理模式： <ul style="list-style-type: none"> • Block: 当系统检测到端口出现环路时，除了生成日志信息外，还会禁止端口学习 MAC 地址并将端口阻塞 • None: 当系统检测到端口出现环路时，除了生成日志信息外不对该端口进行任何处理 • No-learning: 当系统检测到端口出现环路时，除了生成日志信息外，还会禁止端口学习 MAC 地址 • Shutdown: 当系统检测到端口出现环路时，除了生成日志信息外，还会自动关闭该端口，使其不能收发任何报文。端口被关闭后能够自动恢复，恢复时间由 shutdown-interval 命令（请参考“基础配置命令参考”中的“设备管理”）决定
VLANs	接口下检测到的产生环路的VLAN
No loopback is detected	未检测到环路

1.1.2 loopback-detection action

loopback-detection action 命令用来在端口上配置环路检测的处理模式。

undo loopback-detection action 命令用来恢复缺省情况。

【命令】

在二层以太网接口视图下：

```
loopback-detection action { block | no-learning | shutdown }
```

```
undo loopback-detection action
```

在二层聚合接口视图：

```
loopback-detection action shutdown
```

```
undo loopback-detection action
```

【缺省情况】

当系统检测到端口出现环路时不对该端口进行任何处理，仅生成日志信息。

【视图】

二层以太网接口视图

二层聚合接口视图

【缺省用户角色】

network-admin

【参数】

block: 表示 Block 模式，即当系统检测到端口出现环路时，除了生成日志信息外，还会禁止端口学习 MAC 地址并将端口阻塞。二层聚合接口不支持本模式。

no-learning: 表示 No-learning 模式，即当系统检测到端口出现环路时，除了生成日志信息外，还会禁止端口学习 MAC 地址。二层聚合接口不支持本模式。

shutdown: 表示 Shutdown 模式，即当系统检测到端口出现环路时，除了生成日志信息外，还会自动关闭该端口，使其不能收发任何报文。被关闭的端口将在 **shutdown-interval** 命令（请参考“基础配置命令参考”中的“设备管理”）所配置的时间之后自动恢复。

【使用指导】

用户可以使用 **loopback-detection global action** 命令在系统视图下全局配置环路检测的处理模式。

系统视图下的配置对所有端口都有效，接口视图下的配置则只对当前端口有效，且接口视图下的配置优先级较高。

【举例】

在端口 GigabitEthernet1/0/1 上配置环路检测的处理模式为 Shutdown 模式。

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[System-GigabitEthernet1/0/1] loopback-detection action shutdown
```

【相关命令】

- **display loopback-detection**
- **loopback-detection global action**

1.1.3 loopback-detection enable

loopback-detection enable 命令用来在端口上开启环路检测功能。

undo loopback-detection enable 用来在端口上关闭环路检测功能。

【命令】

```
loopback-detection enable vlan { vlan-id-list | all }
undo loopback-detection enable vlan { vlan-id-list | all }
```

【缺省情况】

端口上的环路检测功能处于关闭状态。

【视图】

二层以太网接口视图

二层聚合接口视图

【缺省用户角色】

network-admin

【参数】

vlan-id-list: VLAN 列表，表示多个 VLAN 的编号。表示方式为 **vlan-id-list = { vlan-id1 [to vlan-id2] }&<1-10>**。其中，**vlan-id** 为指定 VLAN 的编号，取值范围为 1~4094。&<1-10> 表示前面的参数最多可以输入 10 次。且 **vlan-id2** 的值大于等于 **vlan-id1** 的值。

all: 表示所有已创建的 VLAN。

【使用指导】

用户可以使用 **loopback-detection global enable** 命令在系统视图下全局开启环路检测功能。

设备全局或者端口开启环路检测功能，当设备上任一端口收到设备发送的任一 VLAN 的环路检测报文时，会触发该端口的环路保护动作。

【举例】

在端口 GigabitEthernet1/0/1 上开启 VLAN 10~20 内的环路检测功能。

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[System-GigabitEthernet1/0/1] loopback-detection enable vlan 10 to 20
```

【相关命令】

- **display loopback-detection**
- **loopback-detection global enable**

1.1.4 loopback-detection global action

loopback-detection global action 命令用来全局配置环路检测的处理模式。

undo loopback-detection global action 命令用来恢复缺省情况。

【命令】

```
loopback-detection global action shutdown
undo loopback-detection global action
```

【缺省情况】

当系统检测到端口出现环路时不对该端口进行任何处理，仅生成日志信息。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

shutdown: 表示 Shutdown 模式，即当系统检测到端口出现环路时，除了生成日志信息外，还会自动关闭该端口，使其不能收发任何报文。被关闭的端口将在 **shutdown-interval** 命令（请参考“基础配置命令参考”中的“设备管理”）所配置的时间之后自动恢复。

【使用指导】

可以使用 **loopback-detection action** 命令在接口视图下配置当前端口的环路检测处理模式。系统视图下的配置对所有端口都有效，接口视图下的配置则只对当前端口有效，且接口视图下的配置优先级较高。

【举例】

全局配置环路检测的处理模式为 Shutdown 模式。

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

```
[Sysname] loopback-detection global action shutdown
```

【相关命令】

- **display loopback-detection**
- **loopback-detection action**

1.1.5 loopback-detection global enable

loopback-detection global enable 命令用来全局开启环路检测功能。

undo loopback-detection global enable 用来全局关闭环路检测功能。

【命令】

```
loopback-detection global enable vlan { vlan-id-list | all }  
undo loopback-detection global enable vlan { vlan-id-list | all }
```

【缺省情况】

环路检测功能处于全局关闭状态。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

vlan-id-list: VLAN 列表, 表示多个 VLAN 的编号。表示方式为 **vlan-id-list = { vlan-id1 [to vlan-id2] }** &<1-10>。其中, **vlan-id** 为指定 VLAN 的编号, 取值范围为 1~4094。&<1-10> 表示前面的参数最多可以输入 10 次。且 **vlan-id2** 的值大于等于 **vlan-id1** 的值。

all: 表示所有已创建的 VLAN。

【使用指导】

可以使用 **loopback-detection enable** 命令在接口视图下开启当前端口的环路检测功能。

设备全局或者端口开启环路检测功能, 当设备上任一端口收到设备发送的任一 VLAN 的环路检测报文时, 会触发该端口的环路保护动作。

【举例】

全局开启 VLAN 10~20 内的环路检测功能。

```
<Sysname> system-view  
[Sysname] loopback-detection global enable vlan 10 to 20
```

【相关命令】

- **display loopback-detection**
- **loopback-detection enable**

1.1.6 loopback-detection interval-time

loopback-detection interval-time 命令用来配置环路检测的时间间隔。

undo loopback-detection interval-time 命令用来恢复缺省情况。

【命令】

```
loopback-detection interval-time interval  
undo loopback-detection interval-time
```

【缺省情况】

环路检测的时间间隔为 30 秒。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

interval: 环路检测的时间间隔，取值范围为 1～300，单位为秒。

【使用指导】

当开启了环路检测功能后，系统开始以一定的时间间隔发送环路检测报文，该间隔越长耗费的系统性能越少，该间隔越短环路检测的灵敏度越高。用户可以通过本命令调整发送环路检测报文的时间间隔，以在系统性能和环路检测的灵敏度之间进行平衡。

【举例】

```
# 配置环路检测的时间间隔为 10 秒。  
<Sysname> system-view  
[Sysname] loopback-detection interval-time 10
```

【相关命令】

- **display loopback-detection**

目 录

1 VLAN	1-1
1.1 VLAN配置命令	1-1
1.1.1 bandwidth	1-1
1.1.2 default	1-1
1.1.3 description	1-2
1.1.4 display interface vlan-interface	1-3
1.1.5 display vlan	1-5
1.1.6 display vlan brief	1-7
1.1.7 interface vlan-interface	1-8
1.1.8 mtu	1-9
1.1.9 name	1-10
1.1.10 reset counters interface vlan-interface	1-10
1.1.11 shutdown	1-11
1.1.12 vlan	1-12
1.2 基于端口的VLAN配置命令	1-13
1.2.1 display port	1-13
1.2.2 port	1-14
1.2.3 port access vlan	1-14
1.2.4 port hybrid pvid	1-15
1.2.5 port hybrid vlan	1-16
1.2.6 port link-type	1-17
1.2.7 port trunk permit vlan	1-18
1.2.8 port trunk pvid	1-19
1.3 基于MAC的VLAN配置命令	1-20
1.3.1 display mac-vlan	1-20
1.3.2 display mac-vlan interface	1-21
1.3.3 mac-vlan enable	1-21
1.3.4 mac-vlan mac-address	1-22
1.3.5 mac-vlan trigger enable	1-23
1.3.6 port pvid forbidden	1-24
1.3.7 vlan precedence	1-24
1.4 基于IP子网的VLAN配置命令	1-25
1.4.1 display ip-subnet-vlan interface	1-25

1.4.2 display ip-subnet-vlan vlan.....	1-26
1.4.3 ip-subnet-vlan	1-27
1.4.4 port hybrid ip-subnet-vlan	1-28
1.5 基于协议的VLAN配置命令	1-29
1.5.1 display protocol-vlan interface	1-29
1.5.2 display protocol-vlan vlan	1-30
1.5.3 port hybrid protocol-vlan.....	1-31
1.5.4 protocol-vlan.....	1-33
1.6 VLAN组配置命令	1-34
1.6.1 display vlan-group.....	1-34
1.6.2 vlan-group.....	1-35
1.6.3 vlan-list.....	1-36
2 Private VLAN.....	2-1
2.1 Private VLAN配置命令	2-1
2.1.1 display private-vlan	2-1
2.1.2 port private-vlan host.....	2-3
2.1.3 port private-vlan promiscuous.....	2-5
2.1.4 port private-vlan trunk promiscuous	2-7
2.1.5 port private-vlan trunk secondary	2-10
2.1.6 private-vlan (VLAN interface view).....	2-13
2.1.7 private-vlan (VLAN view)	2-15
2.1.8 private-vlan community	2-16
2.1.9 private-vlan isolated	2-17
2.1.10 private-vlan primary.....	2-18
3 Voice VLAN.....	3-1
3.1 Voice VLAN配置命令	3-1
3.1.1 display voice-vlan mac-address	3-1
3.1.2 display voice-vlan state	3-2
3.1.3 voice-vlan aging	3-3
3.1.4 voice-vlan enable.....	3-4
3.1.5 voice-vlan mac-address	3-4
3.1.6 voice-vlan mode auto	3-5
3.1.7 voice-vlan security enable	3-6
3.1.8 voice-vlan track lldp.....	3-7

1 VLAN

1.1 VLAN配置命令

1.1.1 bandwidth

bandwidth 命令用来配置 VLAN 接口的期望带宽。

undo bandwidth 命令用来恢复缺省情况。

【命令】

bandwidth *bandwidth-value*

undo bandwidth

【缺省情况】

接口的期望带宽 = 接口的波特率 ÷ 1000 (kbps)。

【视图】

VLAN 接口视图

【缺省用户角色】

network-admin

【参数】

bandwidth-value: 表示接口的期望带宽，取值范围为 1~400000000，单位为 kbps。

【使用指导】

期望带宽供业务模块使用，不会对接口实际带宽造成影响。

【举例】

配置 VLAN 接口 1 的期望带宽为 10000kbps。

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

```
[Sysname] interface vlan-interface 1
```

```
[Sysname-Vlan-interface1] bandwidth 10000
```

1.1.2 default

default 命令用来恢复 VLAN 接口的缺省配置。

【命令】

default

【视图】

VLAN 接口视图

【缺省用户角色】

network-admin

【使用指导】



注意

接口下的某些配置取消后，会对现有功能产生影响，建议您在执行该命令前，完全了解其对网络产生的影响。

您可以在执行 **default** 命令后通过 **display this** 命令确认执行效果。对于未能成功恢复缺省的配置，建议您查阅相关功能的命令手册，手工执行恢复该配置缺省情况的命令。如果操作仍然不能成功，您可以通过设备的提示信息定位原因。

【举例】

将 VLAN 接口 1 恢复为缺省配置。

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

1.1.3 description

description 命令用来配置 VLAN 或 VLAN 接口的描述信息。

undo description 命令用来恢复缺省情况。

【命令】

```
description text
undo description
```

【缺省情况】

VLAN 的描述信息为“VLAN *vlan-id*”，其中 *vlan-id* 为该 VLAN 的四位数编号，如果该 VLAN 的编号不足四位，则会在编号前增加 0，补齐四位。例如，VLAN 100 的描述信息为“VLAN 0100”；VLAN 接口的描述信息为该 VLAN 接口的接口名，如“Vlan-interface1 Interface”。

【视图】

VLAN 视图

VLAN 接口视图

【缺省用户角色】

network-admin

【参数】

text: VLAN 或 VLAN 接口的描述信息，为 1~255 个字符的字符串，区分大小写。

【使用指导】

用户可以根据功能或者连接情况为 VLAN 或 VLAN 接口配置特定的描述信息，以便记忆和管理 VLAN 或 VLAN 接口。

【举例】

将 VLAN 2 的描述信息配置为 sales-private。

```

<Sysname> system-view
[Sysname] vlan 2
[Sysname-vlan2] description sales-private
# 将 VLAN 接口 2 的描述信息配置为 linktoPC56。
<Sysname> system-view
[Sysname] vlan 2
[Sysname-vlan2] quit
[Sysname] interface vlan-interface 2
[Sysname-Vlan-interface2] description linktoPC56

```

【相关命令】

- **display interface vlan-interface**
- **display vlan**

1.1.4 display interface vlan-interface

display interface vlan-interface 命令用来显示 VLAN 接口的相关信息。

【命令】

```

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

```

【视图】

任意视图

【缺省用户角色】

```

network-admin
network-operator

```

【参数】

vlan-interface *interface-number*: VLAN 接口的编号，显示指定 VLAN 接口的信息。不指定 *interface-number* 时，将显示已创建的所有 VLAN 接口的信息。

brief: 显示接口的概要信息。不指定该参数时，将显示接口的详细信息。

description: 用来显示用户配置的接口的全部描述信息。如果不指定该 **description** 参数，只显示描述信息中的前 27 个字符。

down: 显示当前物理状态为 **down** 的接口的信息以及 **down** 的原因。不指定该参数时，将不会根据接口物理状态来过滤显示信息。

【举例】

显示 VLAN-interface 10 的相关信息。

```

<Sysname> display interface vlan-interface 10
Vlan-interface10
Current state: UP
Line protocol state: UP
Description: Vlan-interface10 Interface
Bandwidth: 100000 kbps
Maximum transmission unit: 1500

```

Internet Address is 192.168.1.54/24 Primary
 IP packet frame type: Ethernet II, hardware address: 0023-89b6-d613
 IPv6 packet frame type: Ethernet II, hardware address: 0023-89b6-d613
 Last clearing of counters: Never

显示 VLAN-interface 2 的概要信息。

```
<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      --
```

表1-1 display interface vlan-interface 命令显示信息描述表

字段	描述
Vlan-interface2	VLAN接口名
Current state	<p>VLAN接口的物理状态，状态可能为：</p> <ul style="list-style-type: none"> Administratively DOWN: 表示该 VLAN 接口已经通过 shutdown 命令被关闭，即管理状态为关闭 DOWN: 表示该 VLAN 接口的管理状态为开启，但物理状态为关闭，即该接口对应的 VLAN 内没有处于 UP 状态的物理端口（可能因为没有物理连线或者线路故障） UP: 该端口的管理状态和物理状态均为开启
Line protocol state	<p>VLAN接口的链路层协议状态，状态可能为：</p> <ul style="list-style-type: none"> DOWN: 该 VLAN 接口的协议状态为关闭 UP: 该 VLAN 接口的协议状态为开启
Description	VLAN接口的描述信息
Bandwidth	VLAN接口的期望带宽
Maximum transmission unit	VLAN接口允许通过的MTU
Internet protocol processing : Disabled	该接口还不具有处理IP报文的能力，当没有为该接口配置IP地址时会显示该信息
Internet Address	该接口的主IP地址
IP packet frame type	IPv4发送帧格式
hardware address	VLAN接口对应的MAC地址
IPv6 packet frame type	IPv6发送帧格式
Last clearing of counters	最近一次使用 reset counters interface vlan-interface 命令清除接口下的统计信息的时间。如果从设备启动一直没有执行 reset counters interface vlan-interface 命令清除过该接口下的统计信息，则显示Never
Brief information on interfaces in route mode	三层模式下（route）的接口的概要信息，即三层接口的概要信息

字段	描述
Link: ADM - administratively down; Stby - standby	<ul style="list-style-type: none"> 如果某接口的 Link 属性值为“ADM”，则表示该接口被管理员通过 shutdown 命令关闭，需要在该接口下执行 undo shutdown 命令才能恢复端口本身的物理状态 如果某接口的 Link 属性值为“Stby”，则表示该接口是一个处于 Standby 状态的备份接口，使用 display interface-backup state 命令可以查看该备份接口对应的主接口
Protocol: (s) - spoofing	如果某接口的 Protocol 属性值中带有“(s)”字符串，则表示该接口的数据链路层协议状态显示为 UP，但实际可能没有对应的链路，或者对应的链路不是永久存在而是按需建立的
Interface	接口名称缩写
Link	接口物理连接状态，取值为： <ul style="list-style-type: none"> UP：表示接口物理上是连通的 DOWN：表示接口物理上是不通的 ADM：表示接口被管理员通过 shutdown 命令关闭，需要执行 undo shutdown 命令才能恢复接口本身的物理状态 Stby：表示该接口是一个处于 Standby 状态的备份接口
Protocol	接口数据链路层协议状态，取值为： <ul style="list-style-type: none"> UP：表示接口的数据链路层协议状态为开启 DOWN：表示接口的数据链路层协议状态为关闭 UP(s)：表示接口的数据链路层协议状态显示为 UP，但实际可能没有对应的链路，或者对应的链路不是永久存在而是按需建立的
Primary IP	接口主 IP 地址

【相关命令】

- `reset counters interface vlan-interface`

1.1.5 display vlan

display vlan 命令用来显示 VLAN 的相关信息。

【命令】

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

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator

【参数】

vlan-id1：显示指定 VLAN 的信息。**vlan-id1** 为 VLAN 的编号，取值范围为 1~4094。

vlan-id1 to vlan-id2: 显示 ID 在指定范围内的 VLAN 的信息。vlan-id1 和 vlan-id2 为指定 VLAN 的编号，取值范围为 1~4094。vlan-id2 的值要大于或等于 vlan-id1 的值。

all: 显示除保留 VLAN 外的其他 VLAN 的信息。

dynamic: 显示系统动态创建的 VLAN 的数量和编号。动态 VLAN 是指通过 MVRP 协议生成或通过 RADIUS 服务器下发的 VLAN。

reserved: 显示系统保留 VLAN 的信息。保留 VLAN 是设备根据功能实现的需要预留的 VLAN。保留 VLAN 由协议模块来指定，为协议模块服务，用户不能对保留 VLAN 进行任何操作。

static: 显示系统静态创建的 VLAN 的数量和 VLAN 编号。静态 VLAN 是指通过命令行手工创建的 VLAN。

【举例】

显示 VLAN 2 的信息。

```
<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
```

显示 VLAN 3 的信息。

```
<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
```

表1-2 display vlan 命令显示信息描述表

字段	解释
VLAN ID	VLAN的编号
VLAN type	VLAN的类型： <ul style="list-style-type: none">Static: 静态 VLANDynamic: 动态 VLAN
Route interface	设备上是否创建了对应的VLAN接口： <ul style="list-style-type: none">Not configured: 未创建Configured: 已创建
Description	VLAN的描述信息

字段	解释
Name	VLAN的名称
IP address	VLAN接口的主用IP地址，如果VLAN接口没有配置IP地址，则不显示该字段，如果VLAN接口上还配置了从IP地址，可以使用 display interface vlan-interface 或者在VLAN接口视图下使用 display this 命令查看
Subnet mask	VLAN接口的主用IP地址的子网掩码，如果VLAN接口没有配置IP地址，则不显示该字段
Tagged ports	该VLAN报文从哪些端口发送时需要携带Tag标记
Untagged ports	该VLAN报文从哪些端口发送时不需要携带Tag标记

【相关命令】

- **vlan**

1.1.6 display vlan brief

display vlan brief 命令用来显示设备上所有已创建 VLAN 的概要信息。

【命令】

display vlan brief

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator

【举例】

显示设备上所有已创建 VLAN 的概要信息。

```
<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

```

表1-3 display vlan brief 命令显示信息描述表

字段	描述
Brief information about all VLANs:	所有VLAN的概要信息
Supported Minimum VLAN ID	系统支持的最小VLAN ID
Supported Maximum VLAN ID	系统支持的最大VLAN ID
Default VLAN ID	缺省VLAN ID
VLAN ID	VLAN的编号
Name	VLAN的名称
Port	允许该VLAN报文通过的端口

1.1.7 interface vlan-interface

interface vlan-interface 命令用来创建 VLAN 接口并进入 VLAN 接口视图。如果该 VLAN 接口已经存在，则直接进入 VLAN 接口视图。

undo interface vlan-interface 命令用来删除指定的 VLAN 接口。

【命令】

```

interface vlan-interface interface-number
undo interface vlan-interface interface-number

```

【缺省情况】

不存在 VLAN 接口。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

interface-number: VLAN 接口的编号，取值范围为 1~4094。

【使用指导】

在创建 VLAN 接口之前，对应的 VLAN 必须已经存在，否则将不能创建指定的 VLAN 接口。

Sub VLAN 不能创建对应的 VLAN 接口。

在 Primary VLAN interface 下配置了三层互通的 Secondary VLAN 不能创建对应的 VLAN 接口。

【举例】

创建 VLAN 接口 2 并进入视图。

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

【相关命令】

- **display interface vlan-interface**

1.1.8 mtu

mtu 命令用来配置 VLAN 接口的 MTU 值。

undo mtu 命令用来恢复缺省情况。

【命令】

```
mtu size
undo mtu
```

【缺省情况】

VLAN 接口的 MTU 值为 1500 字节。

【视图】

VLAN 接口视图

【缺省用户角色】

network-admin

【参数】

size: 表示接口允许通过的 MTU（Maximum Transmission Unit，最大传输单元）值的大小，取值范围为 128~1500，单位为字节。

【使用指导】

如果当前接口同时配置 **mtu** 和 **ip mtu** 命令，则设备会以 **ip mtu** 命令配置的接口 MTU 值对报文进行分片，不会再按照 **mtu** 命令配置的 MTU 值对报文进行分片。有关 **ip mtu** 命令的详细介绍，请参见“三层技术-IP 业务命令参考”中的“IP 性能优化”。

【举例】

配置 VLAN 接口 1 的 MTU 值为 1492 字节。

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

【相关命令】

- **display interface vlan-interface**

1.1.9 name

name 命令用来指定当前 VLAN 的名称。

undo name 命令用来恢复缺省情况。

【命令】

```
name text
undo name
```

【缺省情况】

VLAN 的名称为“VLAN *vlan-id*”，其中 *vlan-id* 为该 VLAN 的四位数编号，如果该 VLAN 的编号不足四位，则会在编号前增加 0，补齐四位。例如，VLAN 100 的名称为“VLAN 0100”。

【视图】

VLAN 视图

【缺省用户角色】

network-admin

【参数】

text: VLAN 名称，为 1~32 个字符的描述信息，区分大小写。

【使用指导】

当设备上配置了 802.1X 或 MAC 地址认证功能后，可以通过 RADIUS 服务器来对认证通过的端口下发 VLAN。某些 RADIUS 服务器可以向设备发送需要下发的 VLAN 编号或者 VLAN 名称，当 VLAN 数量很多的时候，使用名称可以更明确的定位 VLAN。

【举例】

指定 VLAN 2 的名称为“test vlan”。

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

【相关命令】

- **display vlan**

1.1.10 reset counters interface vlan-interface

reset counters interface vlan-interface 命令用来清除 VLAN 接口的统计信息。

【命令】

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

【视图】

用户视图

【缺省用户角色】

network-admin

【参数】

vlan-interface *interface-number*: VLAN 接口的编号，清除指定 VLAN 接口的统计信息。
不指定 *interface-number* 时，则清除所有 VLAN 接口的统计信息。

【使用指导】

在某些情况下，需要统计一定时间内某接口的流量，这就需要在统计开始前清除该接口原有的统计信息，重新进行统计。

【举例】

清除 VLAN 接口 2 的统计信息。
<Sysname> reset counters interface vlan-interface 2

【相关命令】

- **display interface vlan-interface**

1.1.11 shutdown

shutdown 命令用来手工关闭 VLAN 接口。
undo shutdown 命令用来手工开启 VLAN 接口。

【命令】

shutdown
undo shutdown

【缺省情况】

未手工关闭 VLAN 接口，此时 VLAN 接口状态受 VLAN 中端口状态的影响，即：

- 当 VLAN 中所有以太网端口状态均为 down 时，VLAN 接口为 down 状态，即关闭状态。
- 当 VLAN 中有一个或一个以上的以太网端口处于 up 状态时，则 VLAN 接口处于 up 状态。

【视图】

VLAN 接口视图

【缺省用户角色】

network-admin

【使用指导】

如果手工关闭 VLAN 接口，则 VLAN 接口的状态始终为 down (Administratively)，不受 VLAN 中端口状态的影响。

配置 VLAN 接口参数前，为了避免配置过程中对网络造成影响，建议先使用 **shutdown** 命令手工关闭接口，之后再配置参数。配置完成后，使用 **undo shutdown** 命令取消手工关闭接口，使配置参数生效。

当 VLAN 接口出现故障时，可以使用 **shutdown** 命令手工关闭接口，然后再使用 **undo shutdown** 命令取消手工关闭接口，这样有可能使接口恢复正常。

关闭和打开 VLAN 接口对于属于这个 VLAN 的任何一个以太网端口本身都不起作用，以太网端口的状态不随 VLAN 接口状态的改变而改变。

【举例】

将 VLAN 接口 2 关闭后再重新打开。

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

1.1.12 vlan

vlan *vlan-id* 命令用来创建 VLAN，并进入 VLAN 视图。如果指定的 VLAN 已存在，则直接进入该 VLAN 的视图。

vlan *vlan-id-list* 命令用来批量创建 VLAN，保留 VLAN 除外。

vlan all 命令用来批量创建 VLAN 1~4094。

undo vlan 命令用来删除 VLAN。

【命令】

```
vlan { vlan-id-list | all }
undo vlan { vlan-id-list | all }
```

【缺省情况】

系统只有一个缺省 VLAN（VLAN 1）。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

vlan-id-list：VLAN 列表。表示方式为 *vlan-id-list* = { *vlan-id1* [**to** *vlan-id2*] }&<1-32>，*vlan-id* 取值范围为 1~4094，*vlan-id2* 的值要大于或等于 *vlan-id1* 的值，&<1-32>表示前面的参数最多可以重复输入 32 次。

all：除保留 VLAN 外的其他 VLAN，当设备允许创建的最大 VLAN 数小于 4094 时，不支持该参数。

【使用指导】

用户不能创建和删除缺省 VLAN（VLAN 1）和保留 VLAN。

动态学习到的 VLAN，以及被其他应用锁定不让删除的 VLAN，都不能使用 **undo vlan** 命令直接删除。只有将相关配置删除之后，才能删除相应的 VLAN。

【举例】

创建 VLAN 2，并进入该 VLAN 视图。

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

批量创建 VLAN 2 和 VLAN 4~100。

```
<Sysname> system-view
[Sysname] vlan 2 4 to 100
```

【相关命令】

- **display vlan**

1.2 基于端口的VLAN配置命令

1.2.1 display port

display port 命令用来显示设备上存在的 Hybrid 或 Trunk 端口。

【命令】

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

【视图】

任意视图

【缺省用户角色】

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

【参数】

hybrid: 显示设备当前存在的 Hybrid 端口。

trunk: 显示设备当前存在的 Trunk 端口。

【举例】

显示当前设备存在的 Hybrid 端口。

```
<Sysname> display port hybrid
Interface          PVID  VLAN Passing
GE1/0/1            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
```

显示当前设备存在的 Trunk 端口。

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

表1-4 display port 命令显示信息描述表

字段	描述
Interface	接口名称
PVID	该端口的缺省VLAN ID
VLAN Passing	表示该端口实际通过的VLAN（该VLAN已经创建，并且接口允许其通过）
Tagged	表示哪些VLAN的报文通过该端口时必须携带VLAN Tag

字段	描述
Untagged	表示哪些VLAN的报文通过该端口时必须去掉VLAN Tag

1.2.2 port

port 命令用来向 VLAN 中添加一个或一组 Access 端口。

undo port 命令用来从 VLAN 中删除一个或一组 Access 端口。

【命令】

```
port interface-list
undo port interface-list
```

【缺省情况】

系统将所有端口都加入到 VLAN 1。

【视图】

VLAN 视图

【缺省用户角色】

network-admin

【参数】

interface-list: 以太网接口列表。表示方式为 *interface-list* = { *interface-type interface-number1* [**to** *interface-type interface-number2*] } &<1-10>, 其中 *interface-type interface-number* 为端口类型和端口编号, *interface-number2* 的值要大于或等于 *interface-number1* 的值, &<1-10>表示前面的参数最多可以输入 10 次。

【使用指导】

通过本命令只能将 Access 端口加入到 VLAN 中, 不能将 Trunk 和 Hybrid 端口加入到 VLAN 中, 并且不能通过本命令向 VLAN 1 中添加或删除 Access 端口。

设备上的所有端口的缺省链路类型都是 Access 类型, 但用户可以自行切换端口类型, 具体配置可参考命令 **port link-type**。

【举例】

向 VLAN2 中添加端口 GigabitEthernet1/0/1~GigabitEthernet1/0/3。

```
<Sysname> system-view
[Sysname] vlan 2
[Sysname-vlan2] port gigabitethernet 1/0/1 to gigabitethernet 1/0/3
```

【相关命令】

- **display vlan**

1.2.3 port access vlan

port access vlan 命令用来将 Access 端口加入到指定的 VLAN 中。

undo port access vlan 命令用来恢复缺省情况。

【命令】

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

【缺省情况】

所有 Access 端口都属于 VLAN 1。

【视图】

二层以太网接口视图
二层聚合接口视图

【缺省用户角色】

network-admin

【参数】

vlan-id: 指定的 VLAN 编号，取值范围为 1~4094。

【使用指导】

缺省情况下所有的 Access 端口都属于 VLAN 1，因此不能通过本命令将 Access 端口加入 VLAN 1。

若需将 Access 端口所属的 VLAN 从其他 VLAN 变更为 VLAN 1，请执行 **undo port access vlan** 命令。

在将 Access 端口加入到指定 VLAN 之前，该 VLAN 必须已经存在。

【举例】

将 GigabitEthernet1/0/1 端口加入到 VLAN 3 中。

```
<Sysname> system-view  
[Sysname] vlan 3  
[Sysname-vlan3] quit  
[Sysname] interface gigabitethernet 1/0/1  
[Sysname-GigabitEthernet1/0/1] port access vlan 3
```

1.2.4 port hybrid pvid

port hybrid pvid 命令用来配置 Hybrid 端口的缺省 VLAN。

undo port hybrid pvid 命令用来配置 Hybrid 端口的缺省 VLAN 为 1。

【命令】

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

【缺省情况】

Hybrid 端口的缺省 VLAN 为该端口在链路类型为 Access 时的所属 VLAN。

【视图】

二层以太网接口视图
二层聚合接口视图

【缺省用户角色】

network-admin

【参数】

vlan-id: 指定接口的缺省的 VLAN ID，取值范围为 1～4094。

【使用指导】

对 Hybrid 端口，执行 **undo vlan** 命令删除端口的缺省 VLAN 后，端口的缺省 VLAN 配置不会改变，即可以使用已经不存在的 VLAN 作为缺省 VLAN。

建议本机 Hybrid 端口的缺省 VLAN 和相连的对端交换机的 Hybrid 端口的缺省 VLAN 保持一致。

配置缺省 VLAN 后，必须使用 **port hybrid vlan** 命令配置端口允许缺省 VLAN 的报文通过，该端口才能转发缺省 VLAN 的报文。

【举例】

配置端口 GigabitEthernet1/0/1（Hybrid 类型）的缺省 VLAN 为 100，并允许 VLAN 100 通过。

```
<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
```

【相关命令】

- **port hybrid vlan**
- **port link-type**

1.2.5 port hybrid vlan

port hybrid vlan 命令用来允许指定的 VLAN 通过当前 Hybrid 端口。

undo port hybrid vlan 命令用来禁止指定的 VLAN 通过当前 Hybrid 端口。

【命令】

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

【缺省情况】

Hybrid 端口只允许该端口在链路类型为 Access 时的所属 VLAN 的报文以 Untagged 方式通过。

【视图】

二层以太网接口视图

二层聚合接口视图

【缺省用户角色】

network-admin

【参数】

vlan-id-list: VLAN 列表, Hybrid 端口允许通过的 VLAN 范围。表示方式为 `vlan-id-list = { vlan-id1 [to vlan-id2] }&<1-32>`, `vlan-id` 取值范围为 1~4094, `vlan-id2` 的值要大于或等于 `vlan-id1` 的值, `&<1-32>` 表示前面的参数最多可以重复输入 32 次。该 VLAN 必须是设备上已创建的 VLAN, 否则, 该命令执行失败。

tagged: 该端口在转发指定的 VLAN 报文时将携带 VLAN Tag。

untagged: 该端口在转发指定的 VLAN 报文时将去掉 VLAN Tag。

【使用指导】

Hybrid 端口允许多个 VLAN 通过。如果多次使用 `port hybrid vlan` 命令, 那么 Hybrid 端口上允许通过的 VLAN 是这些 `vlan-id-list` 的合集。

【举例】

配置端口 GigabitEthernet1/0/1 为 Hybrid 端口, 允许 VLAN 2、4、50~VLAN 100 通过, 并且发送这些 VLAN 的报文时携带 VLAN Tag。

```
<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
```

【相关命令】

- `port link-type`

1.2.6 port link-type

`port link-type` 命令用来配置端口的链路类型。

`undo port link-type` 命令用来恢复缺省情况。

【命令】

```
port link-type { access | hybrid | trunk }
undo port link-type
```

【缺省情况】

所有端口的链路类型均为 Access 类型。

【视图】

二层以太网接口视图

二层聚合接口视图

【缺省用户角色】

network-admin

【参数】

access: 配置端口的链路类型为 Access 类型。

hybrid: 配置端口的链路类型为 Hybrid 类型。

trunk: 配置端口的链路类型为 Trunk 类型。

【使用指导】

Trunk 端口和 Hybrid 端口之间不能直接切换，只能先设为 Access 端口，再配置为其他类型端口。

【举例】

```
# 配置端口 GigabitEthernet1/0/1 配置为 Trunk 端口。
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] port link-type trunk
```

1.2.7 port trunk permit vlan

port trunk permit vlan 命令用来允许指定的 VLAN 通过当前 Trunk 端口。

undo port trunk permit vlan 命令用来禁止指定的 VLAN 通过当前 Trunk 端口。

【命令】

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

【缺省情况】

Trunk 端口只允许 VLAN 1 的报文通过。

【视图】

二层以太网接口视图

二层聚合接口视图

【缺省用户角色】

network-admin

【参数】

vlan-id-list: VLAN 列表，Trunk 端口允许通过的 VLAN 范围。表示方式为 **vlan-id-list = { vlan-id1 [to vlan-id2] } &<1-32>**，**vlan-id** 取值范围为 1~4094，**vlan-id2** 的值要大于或等于 **vlan-id1** 的值，&<1-32>表示前面的参数最多可以重复输入 32 次。

all: 表示允许所有 VLAN 通过该 Trunk 端口。建议用户谨慎使用 **port trunk permit vlan all** 命令，以防止未授权 VLAN 的用户通过该端口访问受限资源。

【使用指导】

Trunk 端口可以允许多个 VLAN 通过。如果多次执行 **port trunk permit vlan** 命令，那么 Trunk 端口上允许通过的 VLAN 是这些 **vlan-id-list** 的集合。

Trunk 端口发送出去的报文，只有缺省 VLAN 的报文不带 VLAN Tag，其他 VLAN 的报文均会保留 VLAN Tag。

【举例】

```
# 配置端口 GigabitEthernet1/0/1 为 Trunk 端口，允许 VLAN 2、4、50~100 通过。
<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
```

【相关命令】

- `port link-type`

1.2.8 port trunk pvid

`port trunk pvid` 命令用来配置 Trunk 端口的缺省 VLAN。

`undo port trunk pvid` 命令用来恢复缺省情况。

【命令】

`port trunk pvid vlan vlan-id`

`undo port trunk pvid`

【缺省情况】

Trunk 端口的缺省 VLAN 为 VLAN 1。

【视图】

二层以太网接口视图

二层聚合接口视图

【缺省用户角色】

network-admin

【参数】

vlan-id: 指定接口的缺省 VLAN ID，取值范围为 1~4094。

【使用指导】

对 Trunk 端口，执行 `undo vlan` 命令删除端口的缺省 VLAN 后，端口的缺省 VLAN 配置不会改变，即使用已经不存在的 VLAN 作为缺省 VLAN。

本端设备 Trunk 端口的缺省 VLAN ID 和相连的对端设备的 Trunk 端口的缺省 VLAN ID 必须一致，否则报文将不能正确传输。

配置缺省 VLAN 后，必须使用 `port trunk permit vlan` 命令配置端口允许缺省 VLAN 的报文通过，该端口才能转发缺省 VLAN 的报文。

【举例】

配置端口 GigabitEthernet1/0/1（Trunk 类型）的缺省 VLAN 为 VLAN 100，并允许 VLAN 100 通过。

```
<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
```

【相关命令】

- `port link-type`
- `port trunk permit vlan`

1.3 基于MAC的VLAN配置命令

1.3.1 display mac-vlan

`display mac-vlan` 命令用来显示 MAC VLAN 表项。

【命令】

`display mac-vlan { all | dynamic | mac-address mac-address [mask mac-mask] | static | vlan vlan-id }`

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator

【参数】

- all**: 显示所有 MAC VLAN 表项。
- dynamic**: 显示动态配置的 MAC VLAN 表项。
- mac-address mac-address**: 显示指定 MAC 地址对应的 MAC VLAN 表项，*mac-address* 格式为 H-H-H。
- mask mac-mask**: 显示指定范围的 MAC VLAN 表项。*mac-mask* 为二进制时高位必须为连续 1，为十六进制时高位必须为连续 f。缺省十六进制值为全 f。
- static**: 显示静态配置的 MAC VLAN 表项。
- vlan vlan-id**: 显示指定 VLAN 对应的 MAC VLAN 表项。*vlan-id* 取值范围为 1~4094。

【举例】

显示所有 MAC VLAN 表项。

```
<Sysname> display mac-vlan all
The following MAC VLAN entries exist:
State: S - Static, D - Dynamic
```

MAC address	Mask	VLAN ID	Dot1q	State
0008-0001-0000	ffff-ff00-0000	5	3	S
0002-0001-0000	ffff-ffff-ffff	5	3	S&D

Total MAC VLAN entries count: 2

表1-5 display mac-vlan 命令显示信息描述表

字段	描述
The following MAC VLAN entries exist	目前设备上存在以下MAC VLAN表项
S - Static	以下显示信息中，S表示静态配置的MAC VLAN
D - Dynamic	以下显示信息中，D表示动态配置的MAC VLAN
MAC address	MAC地址

字段	描述
Mask	MAC地址对应的掩码
VLAN ID	MAC地址对应的VLAN ID
Dot1q	VLAN对应的802.1p优先级
State	MAC VLAN表项属性： <ul style="list-style-type: none"> • S：表示该表项是用户静态配置的 • D：表示该表项是接入认证功能动态下发的 • S&D：表示该表项既是静态配置的也是动态下发的

【相关命令】

- **mac-vlan mac-address**

1.3.2 display mac-vlan interface

display mac-vlan interface 命令用来显示所有开启了 MAC VLAN 功能的接口。

【命令】

display mac-vlan interface

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator

【举例】

显示所有开启了 MAC VLAN 功能的接口。

```
<Sysname> display mac-vlan interface
MAC VLAN is enabled on following ports:
GigabitEthernet1/0/1 GigabitEthernet1/0/2 GigabitEthernet1/0/3
```

【相关命令】

- **mac-vlan enable**

1.3.3 mac-vlan enable

mac-vlan enable 命令用来开启 MAC VLAN 功能。

undo mac-vlan enable 命令用来关闭 MAC VLAN 功能。

【命令】

mac-vlan enable
undo mac-vlan enable

【缺省情况】

MAC VLAN 功能处于关闭状态。

【视图】

二层以太网接口视图

【缺省用户角色】

network-admin

【举例】

在接口 GigabitEthernet1/0/1 上开启 MAC VLAN 功能。

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

【相关命令】

- **display mac-vlan interface**

1.3.4 mac-vlan mac-address

mac-vlan mac-address 命令用来配置 MAC VLAN 表项，即配置 MAC 地址与 VLAN 的关联。

undo mac-vlan 命令用来删除指定的 MAC VLAN 表项。

【命令】

```
mac-vlan mac-address mac-address [ mask mac-mask ] vlan vlan-id [ dot1q priority ]
undo mac-vlan { all | mac-address mac-address [ mask mac-mask ] | vlan vlan-id }
```

【缺省情况】

不存在 MAC VLAN 表项。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

mac-address *mac-address*: MAC 地址，*mac-address* 格式为 H-H-H，不支持组播 MAC 地址和全 0 的 MAC 地址。在配置时，用户可以省去 MAC 地址中每段开头的“0”，例如输入“f-e2-1”即表示输入的 MAC 地址为“000f-00e2-0001”。

mask *mac-mask*: MAC 地址的掩码，*mac-mask* 为二进制时高位必须为连续 1，为十六进制时高位必须为连续 f。缺省十六进制值为全 f。

vlan *vlan-id*: VLAN 的编号，取值范围为 1~4094。

dot1q *priority*: 802.1p 优先级，取值为 0~7，缺省值为 0。取值越大，802.1p 优先级越高。

all: 表示删除所有的静态 MAC VLAN 表项。

【使用指导】

为了 MAC VLAN 的动态触发成功，配置 MAC VLAN 表项时使用静态 VLAN。设备维护两张 MAC VLAN 表：

- 一张是通过指定 **mask** 参数配置的 MAC VLAN 表，该表里的表项描述的是一类 MAC 地址和 VLAN、802.1p 优先级之间的关系。
- 一张是不指定 **mask** 参数配置的 MAC VLAN 表，该表里的表项描述的是单个 MAC 地址和 VLAN、802.1p 优先级之间的关系。

根据用户的配置，系统将自动在这两张 MAC VLAN 表里添加/删除 MAC VLAN 表项。

【举例】

配置 MAC 地址 0000-0001-0001 与 VLAN 100 关联，并指定该表项中 VLAN 100 的 802.1p 优先级为 7。

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

```
[Sysname] mac-vlan mac-address 0-1-1 vlan 100 dot1p 7
```

配置十六进制前 6 位为 1211-22 的 MAC 地址与 VLAN 100 关联，并指定该表项中 VLAN 100 的 802.1p 优先级为 4。

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

```
[Sysname] mac-vlan mac-address 1211-2222-3333 mask ffff-ff00-0000 vlan 100 dot1p 4
```

【相关命令】

- **display mac-vlan**

1.3.5 mac-vlan trigger enable

mac-vlan trigger enable 命令用来开启 MAC VLAN 的动态触发功能。

undo mac-vlan trigger enable 命令用来关闭 MAC VLAN 的动态触发功能。

【命令】

```
mac-vlan trigger enable
```

```
undo mac-vlan trigger enable
```

【缺省情况】

MAC VLAN 的动态触发功能处于关闭状态。

【视图】

二层以太网接口视图

【缺省用户角色】

network-admin

【使用指导】

开启 MAC VLAN 的动态触发功能后，只有端口接收的报文的源 MAC 地址精确匹配了 MAC VLAN 表项，才会动态触发该端口加入相应 VLAN。

【举例】

在接口 GigabitEthernet1/0/1 上开启 MAC VLAN 的动态触发功能。

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

```
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] mac-vlan trigger enable
```

【相关命令】

- **mac-vlan mac-address**
- **port pvid forbidden**

1.3.6 port pvid forbidden

port pvid forbidden 命令用来配置当报文源 MAC 地址与 MAC VLAN 表项的 MAC 地址未精确匹配时，禁止该报文在 PVID 内转发。

undo port pvid forbidden 命令用来恢复缺省情况。

【命令】

```
port pvid forbidden
undo port pvid forbidden
```

【缺省情况】

当报文源 MAC 地址与 MAC VLAN 表项的 MAC 地址未精确匹配时，允许该报文在 PVID 内转发。

【视图】

二层以太网接口视图

【缺省用户角色】

network-admin

【使用指导】

该功能仅适用于和 MAC VLAN 的动态触发功能配合使用。

【举例】

在接口 GigabitEthernet1/0/1 上配置当报文源 MAC 地址不匹配 MAC VLAN 表项时，禁止该报文在 PVID 内转发。

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] port pvid forbidden
```

【相关命令】

- **mac-vlan trigger enable**

1.3.7 vlan precedence

vlan precedence 命令用来配置当前接口的 VLAN 优先匹配方式。

undo vlan precedence 命令用来恢复缺省情况。

【命令】

```
vlan precedence { mac-vlan | ip-subnet-vlan }
undo vlan precedence
```


【缺省情况】

对于基于 MAC 的 VLAN 和基于 IP 子网的 VLAN，优先根据 MAC 地址来匹配 VLAN。

【视图】

二层以太网接口视图

【缺省用户角色】

network-admin

【参数】

mac-vlan: 表示优先根据 MAC 地址来匹配 VLAN。

ip-subnet-vlan: 表示优先根据 IP 子网来匹配 VLAN。

【使用指导】

本命令只对基于 MAC 的 VLAN 和基于 IP 子网的 VLAN 有效。

当使用 **mac-vlan trigger enable** 命令开启 MAC VLAN 的动态触发功能后，建议用户在配置 VLAN 匹配优先级时，使用 **vlan precedence mac-vlan** 命令，使报文优先根据 MAC 地址来匹配 VLAN，此时 **vlan precedence ip-subnet-vlan** 命令不能生效。

【举例】

配置接口 GigabitEthernet1/0/1 优先根据 MAC 地址来匹配 VLAN。

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] vlan precedence mac-vlan
```

【相关命令】

- **mac-vlan trigger enable**

1.4 基于IP子网的VLAN配置命令

1.4.1 display ip-subnet-vlan interface

display ip-subnet-vlan interface 命令用于显示端口关联的子网 VLAN 的信息。

【命令】

```
display ip-subnet-vlan interface { interface-type interface-number1 [ to  
interface-type interface-number2 ] | all }
```

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator

【参数】

interface-type interface-number1 to interface-type interface-number2: 端口范围。*interface-type interface-number1* 和 *interface-type interface-number2* 为端口的类型和编号。*interface-number2* 的值要大于或等于 *interface-number1* 的值。

all: 显示所有端口关联的子网 VLAN 的信息。

【举例】

显示端口 GigabitEthernet1/0/1 关联的子网 VLAN 的信息。

```
<Sysname> display ip-subnet-vlan interface gigabitethernet 1/0/1
Interface: GigabitEthernet1/0/1
  VLAN ID   Subnet index   IP address      Subnet mask      Status
  ---
  3          0             192.168.1.0     255.255.255.0    Active
  4          N/A           N/A             N/A              Inactive
  4094       65535         172.16.1.1     255.255.0.0     Inactive
```

表1-6 display ip-subnet-vlan interface 命令显示信息描述表

字段	描述
VLAN ID	子网VLAN的编号
Subnet index	IP子网的索引，N/A表示该VLAN下未配置任何子网VLAN
IP address	IP子网的地址，N/A表示该VLAN下未配置子网地址
Subnet mask	IP子网的掩码，N/A表示该VLAN下未配置子网掩码
Status	该子网VLAN在端口的生效情况： <ul style="list-style-type: none">Active: 表示生效Inactive: 表示未生效（如子网 VLAN 配置未完成或端口未允许子网 VLAN 通过）

【相关命令】

- display ip-subnet-vlan vlan
- ip-subnet-vlan
- port hybrid ip-subnet-vlan

1.4.2 display ip-subnet-vlan vlan

display ip-subnet-vlan vlan 命令用于显示指定的或所有子网 VLAN 的信息。

【命令】

```
display ip-subnet-vlan vlan { vlan-id1 [ to vlan-id2 ] | all }
```

【视图】

任意视图

【缺省用户角色】

- network-admin
- network-operator

【参数】

vlan-id1: 显示指定的子网 VLAN 的信息, *vlan-id1* 表示 VLAN 的编号, 取值范围为 1~4094。
vlan-id1 to vlan-id2: 显示指定 VLAN 范围内的子网 VLAN 的信息。*vlan-id1* 和 *vlan-id2* 为指定 VLAN 的编号, 取值范围为 1~4094, *vlan-id2* 的值要大于或等于 *vlan-id1* 的值。
all: 显示所有子网 VLAN 的信息。

【举例】

显示所有子网 VLAN 的信息。

```
<Sysname> display ip-subnet-vlan vlan all
VLAN ID: 3
Subnet index      IP address      Subnet mask
0                  192.168.1.0     255.255.255.0
```

表1-7 display ip-subnet-vlan vlan 命令显示信息描述表

字段	描述
VLAN ID	子网VLAN的编号
Subnet index	IP子网的索引
IP address	IP子网的地址（可以是IP地址或网络地址）
Subnet mask	IP子网的掩码

【相关命令】

- **display ip-subnet-vlan interface**
- **ip-subnet-vlan**
- **port hybrid ip-subnet-vlan**

1.4.3 ip-subnet-vlan

ip-subnet-vlan 命令用来配置 VLAN 与指定的 IP 子网或 IP 地址关联。

undo ip-subnet-vlan 命令用于取消 VLAN 与 IP 子网或 IP 地址的关联。

【命令】

```
ip-subnet-vlan [ ip-subnet-index ] ip ip-address [ mask ]
undo ip-subnet-vlan { ip-subnet-index [ to ip-subnet-end ] | all }
```

【缺省情况】

VLAN 未关联 IP 子网或 IP 地址。

【视图】

VLAN 视图

【缺省用户角色】

network-admin

【参数】

ip-subnet-index: IP 子网索引值, 取值范围为 0~65535。子网索引可以由用户指定, 也可由系统根据 IP 子网或 IP 地址与 VLAN 关联的先后顺序自动编号产生。

ip ip-address [mask]: 作为子网 VLAN 划分依据的源 IP 地址或网络地址, *ip-address* 表示源 IP 地址或网络地址, 采用点分十进制格式; *mask* 表示子网掩码, 采用点分十进制格式, 缺省值为 255.255.255.0。

to ip-subnet-end: 用来确定 IP 子网索引的范围。其中 *ip-subnet-end* 表示 IP 子网索引的终止值, 取值范围为 0~65535, 其值必须大于或等于 *ip-subnet-index* 的值。

all: 取消 VLAN 与所有 IP 子网或 IP 地址的关联。

【使用指导】

VLAN 关联的 IP 网段或 IP 地址不允许是组播网段或组播地址。

【举例】

将 VLAN 3 配置为基于 IP 子网的 VLAN, 与 192.168.1.0/24 网段进行关联, 使得源地址为该网段的报文可以在 VLAN 3 中传送。

```
<Sysname> system-view
[Sysname] vlan 3
[Sysname-vlan3] ip-subnet-vlan ip 192.168.1.0 255.255.255.0
```

【相关命令】

- **display ip-subnet-vlan interface**
- **display ip-subnet-vlan vlan**
- **port hybrid ip-subnet-vlan**

1.4.4 port hybrid ip-subnet-vlan

port hybrid ip-subnet-vlan 命令用来配置端口与子网 VLAN 关联。

undo port hybrid ip-subnet-vlan 命令用于取消端口与子网 VLAN 的关联。

【命令】

```
port hybrid ip-subnet-vlan vlan vlan-id
undo port hybrid ip-subnet-vlan { vlan vlan-id | all }
```

【缺省情况】

端口未关联子网 VLAN。

【视图】

二层以太网接口视图

二层聚合接口视图

【缺省用户角色】

network-admin

【参数】

vlan *vlan-id*: VLAN 的编号, 取值范围为 1~4094。

all: 所有 VLAN。

【使用指导】

执行本命令时，需保证当前端口的链路类型为 Hybrid，并允许子网 VLAN 通过，且子网 VLAN 下存在与 IP 子网或 IP 地址关联的配置，该命令才实际生效。

【举例】

将端口 GigabitEthernet1/0/1 与子网 VLAN 3 关联。

```
<Sysname> system-view
[Sysname] vlan 3
[Sysname-vlan3] ip-subnet-vlan ip 192.168.1.0 255.255.255.0
[Sysname-vlan3] quit
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] port link-type hybrid
[Sysname-GigabitEthernet1/0/1] port hybrid vlan 3 untagged
[Sysname-GigabitEthernet1/0/1] port hybrid ip-subnet-vlan vlan 3
```

将二层聚合接口 1 与子网 VLAN 3 关联。

```
<Sysname> system-view
[Sysname] vlan 3
[Sysname-vlan3] ip-subnet-vlan ip 192.168.1.0 255.255.255.0
[Sysname-vlan3] quit
[Sysname] interface bridge-aggregation 1
[Sysname-Bridge-Aggregation1] port link-type hybrid
[Sysname-Bridge-Aggregation1] port hybrid vlan 3 untagged
[Sysname-Bridge-Aggregation1] port hybrid ip-subnet-vlan vlan 3
```

【相关命令】

- **display ip-subnet-vlan interface**
- **display ip-subnet-vlan vlan**
- **ip-subnet-vlan**

1.5 基于协议的VLAN配置命令



说明

S5000E-X、S5110V2-SI 与 S5000V3-EI 系列交换机不支持配置基于协议的 VLAN。

1.5.1 display protocol-vlan interface

display protocol-vlan interface 命令用于显示端口关联的协议 VLAN 的信息。

【命令】

```
display protocol-vlan interface { interface-type interface-number1 [ to  
interface-type interface-number2 ] | all }
```

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator

【参数】

interface-type interface-number1 to interface-type interface-number2: 端口范围。*interface-type interface-number1* 和 *interface-type interface-number2* 为端口的类型和编号。*interface-number2* 的值要大于或等于 *interface-number1* 的值。
all: 显示所有端口关联的协议 VLAN 的信息。

【举例】

显示端口 GigabitEthernet1/0/1 关联的协议 VLAN 的信息。

```
<Sysname> display protocol-vlan interface gigabitethernet 1/0/1
Interface: GigabitEthernet1/0/1
VLAN ID   Protocol index  Protocol type      Status
2         0              IPv6               Active
2         1              N/A                Inactive
4094      65535          IPv4               Inactive
```

表1-8 display protocol-vlan interface 命令显示信息描述表

字段	描述
VLAN ID	协议VLAN的编号
Protocol index	协议模板索引号
Protocol type	该协议模板指定的协议类型，N/A表示该协议模板未指定协议类型
Status	该协议VLAN在端口的生效情况： <ul style="list-style-type: none">Active: 表示生效Inactive: 表示未生效

【相关命令】

- display protocol-vlan vlan
- port hybrid protocol-vlan
- protocol-vlan

1.5.2 display protocol-vlan vlan

display protocol-vlan vlan 命令用于显示指定的或所有协议 VLAN 的信息。

【命令】

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

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator

【参数】

vlan-id1: 显示指定的协议 VLAN 的信息，*vlan-id1* 表示 VLAN 的编号，取值范围为 1~4094。
vlan-id1 to vlan-id2: 显示指定 VLAN 范围内的协议 VLAN 的信息。*vlan-id1* 和 *vlan-id2* 为指定 VLAN 的编号，取值范围为 1~4094，*vlan-id2* 的值要大于或等于 *vlan-id1* 的值。
all: 显示所有协议 VLAN 的信息。

【举例】

```
# 显示所有协议 VLAN 的信息。
<Sysname> display protocol-vlan vlan all
VLAN ID: 2
  Protocol index  Protocol type
    0              IPv4
  65535           IPv6

VLAN ID: 3
  Protocol index  Protocol type
    0              IPv4
  65535           LLC DSAP 0x11 SSAP 0x22
```

表1-9 display protocol-vlan vlan 命令显示信息描述表

字段	描述
VLAN ID	协议VLAN的编号
Protocol index	协议模板索引号
Protocol type	该协议模板所指定的协议类型或封装格式

【相关命令】

- **display protocol-vlan interface**
- **port hybrid protocol-vlan**
- **protocol-vlan**

1.5.3 port hybrid protocol-vlan

port hybrid protocol-vlan 命令用来配置端口与协议 VLAN 关联。
undo port hybrid protocol-vlan 命令用于取消端口与协议 VLAN 的关联。

【命令】

```
port hybrid protocol-vlan vlan vlan-id { protocol-index [ to protocol-end ] | all }  
  
undo hybrid protocol-vlan { vlan vlan-id { protocol-index [ to protocol-end ] | all } | all }
```

【缺省情况】

端口未关联协议 VLAN。

【视图】

二层以太网接口视图

二层聚合接口视图

【缺省用户角色】

network-admin

【参数】

vlan *vlan-id*: VLAN 的编号，取值范围为 1~4094。

protocol-index: 协议模板索引，取值范围为 0~65535

to: 协议模板索引的范围。

protocol-end: 协议模板索引终止值，取值范围为 0~65535，其值必须大于或等于 *protocol-index* 的值。

all: 所有协议模板。

【使用指导】

执行本命令时，需确保当前端口的链路类型为 Hybrid，并允许协议 VLAN 通过，且协议 VLAN 下存在与协议模板关联的配置，本命令才实际生效。

在执行 **undo port hybrid protocol-vlan** 命令时：

- 如果同时指定 *vlan-id* 和 **all**，则表示取消当前端口与指定 VLAN 下绑定的所有协议模板的关联。
- 如果仅指定 **all**，则表示取消当前端口与所有 VLAN 下绑定的所有协议模板的关联。

【举例】

配置端口 GigabitEthernet1/0/1 与协议 VLAN 2 中的协议模板 1 关联。

```
<Sysname> system-view  
[Sysname] vlan 2  
[Sysname-vlan2] protocol-vlan 1 ipv4  
[Sysname-vlan2] quit  
[Sysname] interface gigabitethernet 1/0/1  
[Sysname-GigabitEthernet1/0/1] port link-type hybrid  
[Sysname-GigabitEthernet1/0/1] port hybrid vlan 2 untagged  
[Sysname-GigabitEthernet1/0/1] port hybrid protocol-vlan vlan 2 1
```

配置二层聚合接口 1 与协议 VLAN 2 中的协议模板 1 关联。

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



```
[Sysname-vlan2] protocol-vlan 1 ipv4
[Sysname-vlan2] quit
[Sysname] interface bridge-aggregation 1
[Sysname-Bridge-Aggregation1] port link-type hybrid
[Sysname-Bridge-Aggregation1] port hybrid vlan 2 untagged
[Sysname-Bridge-Aggregation1] port hybrid protocol-vlan vlan 2 1
```

1.5.4 protocol-vlan

protocol-vlan 命令用来配置 VLAN 与指定的协议模板关联。

undo protocol-vlan 命令用于取消 VLAN 与协议模板的关联。

【命令】

```
protocol-vlan [protocol-index] { at | ipv4 | ipv6 | ipx { ethernetii | llc | raw
| snap } | mode { ethernetii etype etype-id | llc { dsap dsap-id [ ssap ssap-id ]
| ssap ssap-id } | snap etype etype-id } }
undo protocol-vlan { protocol-index [ to protocol-end ] | all }
```

【缺省情况】

VLAN 未关联协议模板。

【视图】

VLAN 视图

【缺省用户角色】

network-admin

【参数】

at: 基于 AT（AppleTalk，Apple 计算机网络协议）协议的 VLAN。

ipv4: 基于 IPv4 协议的 VLAN。

ipv6: 基于 IPv6 协议的 VLAN。

ipx: 基于 IPX 协议的 VLAN，可包括 **ethernetii**、**llc**、**raw** 和 **snap** 四种封装类型。

mode: 配置自定义协议模板，可包括 **ethernetii**、**llc** 和 **snap** 三种封装类型。

ethernetii etype etype-id: 匹配 Ethernet II 封装格式及相应的协议类型值。其中，*etype-id* 表示入报文的协议类型值，取值范围为十六进制数 600~ffff（不包括 800、86dd、809b 和 8137）。

llc: 匹配 LLC 封装格式。

dsap dsap-id: 目的服务接入点，取值范围为十六进制数 0~ff。

ssap ssap-id: 源服务接入点，取值范围为十六进制数 0~ff。

snap etype etype-id: 匹配 SNAP 封装格式及相应的协议类型值。其中，*etype-id* 表示入报文的以太网类型，取值范围为十六进制数 600~ffff（不包括 8137）。

protocol-index: 协议索引，用来标识与当前 VLAN 绑定的协议模板，取值范围为 0~65535。如果不指定该参数，则系统会自动分配一个索引值。

to protocol-end: 用来确定协议索引的范围。其中 *protocol-end* 表示协议索引终止值，取值范围为 0~65535，其值必须大于或等于 *protocol-index* 的值。

all: 与当前 VLAN 绑定的所有协议。

【使用指导】



注意

由于 IPv4 协议与 ARP 协议关系密切，建议用户将 IPv4 协议和 ARP 协议绑定到同一 VLAN，并且关联到相同的端口，避免因 ARP 报文与 IPv4 报文未划分到同一 VLAN，而造成无法正常通信的情况。

使用 **mode ethernetii etype** 关键字进行配置时，不允许将 *etype-id* 的值配置为 800、809b、8137 或 86dd，因为上述取值分别与 IPv4、AppleTalk、IPX 和 IPv6 协议模板相同。

使用 **mode llc** 关键字进行配置时，*dsap-id* 和 *ssap-id* 的值不允许同时为 e0（代表 IPX 报文的 LLC 封装格式）、ff（代表 IPX 报文的 raw 封装格式）、aa（代表 SNAP 封装格式）；如果只配置了 *dsap-id* 和 *ssap-id* 中的一个，系统会将另一参数的值自动配置为 aa。

使用 **mode snap etype** 关键字进行配置时，不允许将 *etype-id* 的值配置为 8137，因为该值与 IPX 协议模板相同。当 *etype-id* 的值取 800、809b 或 86dd 时，其对应的协议模板分别为 IPv4、AppleTalk 和 IPv6。

【举例】

将 IPv4 报文和采用 Ethernet II 封装格式的 ARP 报文(ARP 协议的协议代码为 0806)划分到 VLAN 3 中传输。

```
<Sysname> system-view
[Sysname] vlan 3
[Sysname-vlan3] protocol-vlan 1 ipv4
[Sysname-vlan3] protocol-vlan 2 mode ethernetii etype 0806
```

【相关命令】

- **display protocol-vlan interface**
- **display protocol-vlan vlan**
- **port protocol-vlan**

1.6 VLAN组配置命令

1.6.1 display vlan-group

display vlan-group 命令用来显示创建的 VLAN 组及其 VLAN 成员列表。

【命令】

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

【视图】

任意视图

【缺省用户角色】

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

【参数】

group-name: VLAN 组的名称，为 1~31 个字符的字符串，区分大小写，首字符必须为字母。若不指定该参数，则表示显示所有 VLAN 组的信息。

【举例】

显示指定 VLAN 组 test001 的信息。

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

显示所有 VLAN 组的信息。

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

表1-10 display vlan-group 命令显示信息描述表

字段	描述
VLAN group	VLAN组名称
VLAN list	对应的该VLAN组内的VLAN列表

【相关命令】

- **vlan-group**
- **vlan-list**

1.6.2 vlan-group

vlan-group 命令用来创建一个 VLAN 组，并进入 VLAN 组视图。如果指定的 VLAN 组已经存在，则直接进入该 VLAN 组视图。

undo vlan-group 命令用来删除指定的 VLAN 组。

【命令】

```
vlan-group group-name
undo vlan-group group-name
```

【缺省情况】

不存在 VLAN 组。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

group-name: VLAN 组的名称，为 1~31 个字符的字符串，区分大小写，首字符必须为字母。

【使用指导】

VLAN 组是一组 VLAN 的集合。VLAN 组内可以添加多个 VLAN 列表。

【举例】

创建一个 VLAN 组，名称为 test001，并进入 VLAN 组视图。

```
<Sysname> system-view
[Sysname] vlan-group test001
[Sysname-vlan-group-test001]
```

【相关命令】

- **vlan-list**

1.6.3 vlan-list

vlan-list 命令用来在 VLAN 组内添加 VLAN 成员。

undo vlan-list 命令用来从 VLAN 组内删除 VLAN 成员。

【命令】

```
vlan-list vlan-id-list
undo vlan-list vlan-id-list
```

【缺省情况】

当前 VLAN 组中不存在 VLAN 列表。

【视图】

VLAN 组视图

【缺省用户角色】

network-admin

【参数】

vlan-id-list: VLAN 列表。表示方式为 *vlan-id-list* = { *vlan-id1* [**to** *vlan-id2*] } &<1-10>, *vlan-id* 取值范围为 1~4094, *vlan-id2* 的值要大于或等于 *vlan-id1* 的值, &<1-10>表示前面的参数最多可以重复输入 10 次。

【举例】

向 VLAN 组 test001 内添加 VLAN 成员：VLAN 2~VLAN 4、VLAN 100、VLAN 200。

```
<Sysname> system-view
[Sysname] vlan-group test001
[Sysname-vlan-group-test001] vlan-list 2 to 4 100 200
```

【相关命令】

- **vlan-group**

2 Private VLAN



说明

S5000E-X、S5110V2-SI 与 S5000V3-EI 系列交换机不支持 Private VLAN。

2.1 Private VLAN配置命令

2.1.1 display private-vlan

display private-vlan 命令用来显示 Primary VLAN 和其包含的 Secondary VLAN 的信息。

【命令】

display private-vlan [*primary-vlan-id*]

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator

【参数】

primary-vlan-id: Primary VLAN 的编号，取值范围为 1~4094。如果未指定该参数，则显示所有 Primary VLAN 和其对应的 Secondary VLAN 的映射信息。

【举例】

显示所有 Primary VLAN 和其包含的 Secondary VLAN 的信息。

```
<Sysname> display private-vlan
Primary VLAN ID: 2
Secondary VLAN ID: 3-4

VLAN ID: 2
VLAN type: Static
Private VLAN type: Primary
Route interface: Configured
IPv4 address: 1.1.1.1
IPv4 subnet mask: 255.255.255.0
IPv6 global unicast addresses:
    2001::1, subnet is 2001::/64 [TENTATIVE]
Description: VLAN 0002
Name: VLAN 0002
Tagged ports:    None
Untagged ports:
```

```
GigabitEthernet1/0/2
GigabitEthernet1/0/3
GigabitEthernet1/0/4
```

```
VLAN ID: 3
VLAN type: Static
Private VLAN type: Secondary
Route interface: Not configured
Description: VLAN 0003
Name: VLAN 0003
Tagged ports:   None
Untagged ports:
    GigabitEthernet1/0/2
    GigabitEthernet1/0/3
```

```
VLAN ID: 4
VLAN type: Static
Private VLAN type: Secondary
Route interface: Not configured
Description: VLAN 0004
Name: VLAN 0004
Tagged ports:   None
Untagged ports:
    GigabitEthernet1/0/2
    GigabitEthernet1/0/4
```

表2-1 display private-vlan 命令显示信息描述表

字段	描述
Primary VLAN ID	Primary VLAN的编号
Secondary VLAN ID	Secondary VLAN的编号
VLAN ID	VLAN编号
VLAN type	VLAN类型: <ul style="list-style-type: none"> Dynamic: 动态 VLAN Static: 静态 VLAN
Private VLAN type	Private VLAN类型: <ul style="list-style-type: none"> Primary: 表示 Primary VLAN Secondary: 表示 Secondary VLAN Isolated secondary: 表示配置了各端口二层隔离的 Secondary VLAN
Route interface	设备上是否创建了对应的VLAN接口: <ul style="list-style-type: none"> Configured: 已创建 Not configured: 未创建
IPv4 address	VLAN接口的主用IPv4地址, 如果VLAN接口没有配置IPv4地址, 则不显示该字段, 如果VLAN接口上还配置了从IPv4地址, 可以使用 display interface vlan-interface 或者在VLAN接口视图下使用 display this 命令查看

字段	描述
IPv4 subnet mask	VLAN接口的主用IPv4地址的子网掩码，如果VLAN接口没有配置IPv4地址，则不显示该字段
IPv6 global unicast addresses	<p>VLAN接口上配置的全球单播IPv6地址（如果VLAN接口没有配置IPv6地址，则不显示该字段）</p> <p>可能的IPv6地址状态及含义如下：</p> <ul style="list-style-type: none"> • [TENTATIVE]：该状态为地址初始化状态，此时该地址可能正在进行 DAD 检测或准备进行 DAD 检测，处于该状态的地址不能作为报文的源地址或者目的地址 • [DUPLICATE]：该状态表明地址 DAD 检测已经结束，由于该地址在链路上不唯一，因此不能使用 • [PREFERRED]：该状态表明地址处于首选生命期以内。该状态的地址可以作为报文的源地址或者目的地址。为该状态时，不显示地址的状态标识 • [DEPRECATED]：该状态表明地址超过首选生命期，但是在有效生命期以内。该状态地址有效，但不应作为新建连接报文的源地址，目的地址是该地址的报文还可以被正常处理
Description	VLAN的描述信息
Name	VLAN的名称
Tagged ports	该VLAN报文从哪些端口发送需要携带VLAN Tag
Untagged ports	该VLAN报文从哪些端口发送时不需要携带VLAN Tag

【相关命令】

- `private-vlan (VLAN view)`
- `private-vlan primary`

2.1.2 port private-vlan host

`port private-vlan host` 命令用来配置端口工作在 host 模式。

`undo port private-vlan` 命令用来恢复缺省情况。

【命令】

```
port private-vlan host
undo port private-vlan
```

【缺省情况】

端口不工作在 host 模式。

【视图】

二层以太网接口视图

二层聚合接口视图

【缺省用户角色】

network-admin

【使用指导】

端口工作在 **host** 模式时，若端口已经加入了 **Secondary VLAN**，则端口也会同步加入和 **Secondary VLAN** 有映射关系的 **Primary VLAN**。

在执行 **port private-vlan host** 命令后，当端口同步加入 **Primary VLAN** 时，端口的链路类型不同，进行的操作不同：

- 若端口的链路类型为 **Access** 类型，则会：
 - 配置端口的链路类型为 **Hybrid** 类型。
 - 配置缺省 **VLAN** 为端口加入的 **Secondary VLAN**。
 - 端口会以 **Untagged** 方式加入 **Primary VLAN**。
- 若端口的链路类型为 **Trunk** 类型，则端口的链路类型及缺省 **VLAN** 不做改变。
- 若端口的链路类型为 **Hybrid** 类型，则端口的链路类型及缺省 **VLAN** 不做改变，但同步加入 **Primary VLAN** 时：
 - 若此前该端口存在以 **Tagged/Untagged** 方式加入 **Primary VLAN** 的配置，则保持原有配置。
 - 若此前该端口不存在加入 **Primary VLAN** 的配置，则该端口会以 **Untagged** 方式加入 **Primary VLAN**。

可以在执行完 **port private-vlan host** 命令后，再配置端口加入 **Secondary VLAN**，此时，该命令的功能依然生效。

undo port private-vlan 命令恢复缺省情况时，端口的 **VLAN** 属性（包括端口加入 **VLAN** 以及端口的链路类型、端口缺省 **VLAN**）不做改变。

port private-vlan host 命令与 **port private-vlan trunk promiscuous** 及 **port private-vlan trunk secondary** 命令互斥。

【举例】

VLAN 20 的类型为 **Secondary VLAN**，且 **VLAN 20** 和 **Primary VLAN 2** 关联。

配置链路类型为 **Access** 的端口 **GigabitEthernet1/0/1** 工作在 **host** 模式。

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] port private-vlan host
[Sysname-GigabitEthernet1/0/1] display this
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port private-vlan host
#
return
```

将端口 **GigabitEthernet1/0/1** 加入 **VLAN 20**。

```
[Sysname-GigabitEthernet1/0/1] port access vlan 20
```

显示端口 **GigabitEthernet1/0/1** 当前配置。

```
[Sysname-GigabitEthernet1/0/1] display this
#
interface GigabitEthernet1/0/1
 port link-mode bridge
```



```

port private-vlan host
port link-type hybrid
undo port hybrid vlan 1
port hybrid vlan 2 20 untagged
port hybrid pvid vlan 20
#
return

```

可以看出当端口 GigabitEthernet1/0/1 工作在 host 模式，且加入 Secondary VLAN 20 时，该端口会同步加入关联的 Primary VLAN 2，同时修改链路类型及缺省 VLAN

【相关命令】

- **port private-vlan promiscuous**
- **port private-vlan trunk promiscuous**
- **port private-vlan trunk secondary**
- **private-vlan** (VLAN view)
- **private-vlan primary**

2.1.3 port private-vlan promiscuous

port private-vlan promiscuous 命令用来配置端口在指定 VLAN 中工作在 promiscuous 模式并加入到该 VLAN。

undo port private-vlan 命令用来恢复缺省情况。

【命令】

```

port private-vlan vlan-id promiscuous
undo port private-vlan

```

【缺省情况】

端口在指定 VLAN 中不工作在 promiscuous 模式。

【视图】

二层以太网接口视图
 二层聚合接口视图

【缺省用户角色】

network-admin

【参数】

vlan-id: VLAN 的编号，取值范围为 1~4094。其中，VLAN 1 虽然在取值范围中，但不能配置。

【使用指导】

执行本命令时若指定 VLAN 的类型为 Primary VLAN，且存在和指定 VLAN 有映射关系的 Secondary VLAN，则端口也会同步加入这些 Secondary VLAN。

在执行 **port private-vlan promiscuous** 命令时，端口的链路类型不同，进行的操作不同：

- 若端口的链路类型为 Access 类型，则会：
 - 配置端口的链路类型为 Hybrid 类型。

- 配置缺省 VLAN 为指定 VLAN。
- 端口会以 **Untagged** 方式加入所有对应 VLAN（包括指定 VLAN 及同步加入的 **Secondary VLAN**）。
- 若端口的链路类型为 **Trunk** 类型，则端口的链路类型及缺省 VLAN 不做改变。
- 若端口的链路类型为 **Hybrid** 类型，则端口的链路类型及缺省 VLAN 不做改变。端口加入对应 VLAN（包括指定 VLAN 及同步加入的 **Secondary VLAN**）时：
 - 若端口此前存在以 **Tagged/Untagged** 方式加入某些对应 VLAN 的配置，则在保持原有配置的基础上，端口会以 **Untagged** 方式加入其他对应 VLAN
 - 若端口此前不存在加入某些对应 VLAN 的配置，则端口会以 **Untagged** 方式加入所有对应 VLAN。

如果在 **promiscuous** 端口上多次执行 **port private-vlan promiscuous** 命令，则最后一次执行的命令生效。

undo port private-vlan 命令恢复缺省情况时，端口的 VLAN 属性（包括端口加入 **Secondary VLAN** 以及端口的链路类型、缺省 VLAN 的配置）不做改变。

在执行 **undo port private-vlan** 命令时，若端口已配置在某 VLAN 中工作在 **promiscuous** 模式，则取消端口加入该 VLAN 的配置。

可以在执行完 **port private-vlan promiscuous** 命令后，再配置指定 VLAN 的类型为 **Primary VLAN**，此时，该命令的功能依然生效。

port private-vlan promiscuous 命令与 **port private-vlan trunk promiscuous** 及 **port private-vlan trunk secondary** 命令互斥。

【举例】

VLAN 2 的类型为 **Primary VLAN**，且 VLAN 2 和 **Secondary VLAN 20** 关联。

显示端口 **GigabitEthernet1/0/1** 当前配置。

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] display this
#
interface GigabitEthernet1/0/1
  port link-mode bridge
#
return
```

配置链路类型为 **Access** 的端口 **GigabitEthernet1/0/1** 在 **VLAN 2** 中工作在 **promiscuous** 模式，并显示配置结果。

```
[Sysname-GigabitEthernet1/0/1] port private-vlan 2 promiscuous
[Sysname-GigabitEthernet1/0/1] display this
#
interface GigabitEthernet1/0/1
  port link-mode bridge
  port link-type hybrid
  port private-vlan 2 promiscuous
  undo port hybrid vlan 1
  port hybrid vlan 2 20 untagged
  port hybrid pvid vlan 2
```

```
#
return
```

可以看出当该端口在 VLAN 2 中工作在 promiscuous 模式时，该端口会加入 Primary VLAN 2 及关联的 Secondary VLAN 20，同时修改端口的链路类型及缺省 VLAN。

取消端口 GigabitEthernet1/0/1 的 promiscuous 模式配置，并显示配置结果。

```
[Sysname-GigabitEthernet1/0/1] undo port private-vlan
[Sysname-GigabitEthernet1/0/1] display this
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port link-type hybrid
 undo port hybrid vlan 1
 port hybrid vlan 20 untagged
 port hybrid pvid vlan 2
#
return
```

可以看出该端口退出 Primary VLAN 2，但该端口的 VLAN 属性（包括端口加入 Secondary VLAN 以及端口的链路类型、缺省 VLAN 的配置）不做改变。

【相关命令】

- `port private-vlan host`
- `port private-vlan trunk promiscuous`
- `port private-vlan trunk secondary`
- `private-vlan (VLAN view)`
- `private-vlan primary`

2.1.4 port private-vlan trunk promiscuous

`port private-vlan trunk promiscuous` 命令用来配置端口在指定 VLAN 中工作在 trunk promiscuous 模式并加入该 VLAN。

`undo port private-vlan trunk promiscuous` 命令用来配置端口在指定 VLAN 退出 trunk promiscuous 模式。

【命令】

```
port private-vlan vlan-id-list trunk promiscuous
undo port private-vlan vlan-id-list trunk promiscuous
```

【缺省情况】

端口在指定 VLAN 中不工作在 trunk promiscuous 模式。

【视图】

二层以太网接口视图
二层聚合接口视图

【缺省用户角色】

network-admin

【参数】

vlan-id-list: VLAN 列表, Primary VLAN 的范围。表示方式为 **vlan-id-list = { vlan-id1 [to vlan-id2] } <1-10>**, **vlan-id** 取值范围为 1~4094, **vlan-id2** 的值要大于或等于 **vlan-id1** 的值, **<1-10>** 表示前面的参数最多可以重复输入 10 次。其中, 系统缺省 VLAN (VLAN 1) 虽然在取值范围中, 但不能配置。

【使用指导】

执行本命令时若指定 VLAN 的类型为 Primary VLAN, 且存在和指定 VLAN 有映射关系的 Secondary VLAN, 则端口也会同步加入这些 Secondary VLAN。

在执行 **port private-vlan trunk promiscuous** 命令时, 端口的链路类型不同, 进行的操作不同:

- 若端口的链路类型为 Access 类型, 则会:
 - 配置端口的链路类型为 Hybrid 类型, 缺省 VLAN 不做改变。
 - 端口会以 Tagged 方式加入所有对应 VLAN (包括指定 VLAN 及同步加入的 Secondary VLAN)。
- 若端口的链路类型为 Trunk 类型, 则端口的链路类型及缺省 VLAN 不做改变。
- 若端口的链路类型为 Hybrid 类型, 则端口的链路类型及缺省 VLAN 不做改变。端口加入对应 VLAN (包括指定 VLAN 及同步加入的 Secondary VLAN) 时:
 - 若端口此前存在以 Tagged/Untagged 方式加入某些对应 VLAN 的配置, 则在保持原有配置的基础上, 端口会以 Tagged 方式加入其他对应 VLAN。
 - 若端口此前不存在加入某些对应 VLAN 的配置, 则端口会以 Tagged 方式加入所有对应 VLAN。

undo port private-vlan trunk promiscuous 命令用来配置端口在指定 VLAN 中退出 trunk promiscuous 模式, 但端口的 VLAN 属性 (包括端口加入 Secondary VLAN 以及端口的链路类型、缺省 VLAN 的配置) 不做改变。

在执行 **undo port private-vlan trunk promiscuous** 命令时, 若已配置端口在 **vlan-id-list** 中工作在 trunk promiscuous 模式, 则取消端口加入 **vlan-id-list** 的配置。

可以在执行完 **port private-vlan trunk promiscuous** 命令后, 再配置指定 VLAN 的类型为 Primary VLAN, 此时, 该命令的功能依然生效。

port private-vlan trunk promiscuous 命令与 **port private-vlan promiscuous**、**port private-vlan trunk secondary** 及 **port private-vlan host** 命令互斥。

port private-vlan trunk promiscuous 命令适用于需要多个 Primary VLAN 通过上行端口的情况, 配置该命令后多个 Primary VLAN 携带 Tag 通过上行端口。**port private-vlan promiscuous** 适用于只有一个 Primary VLAN 通过上行端口的情况, 配置该命令后 Primary VLAN 不带 Tag 通过上行端口。

【举例】

VLAN 2、3 的类型为 Primary VLAN, 且 VLAN 2 和 Secondary VLAN 20 关联, VLAN 3 和 Secondary VLAN 30 关联。

显示端口 GigabitEthernet1/0/1 当前配置。

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

```
[Sysname-GigabitEthernet1/0/1] display this
```

```
#
```

```
interface GigabitEthernet1/0/1
```

```
port link-mode bridge
```

```
#
```

```
return
```

配置链路类型为 Access 的端口 GigabitEthernet1/0/1 在 VLAN 2、3 中工作在 trunk promiscuous 模式，并显示配置结果。

```
[Sysname-GigabitEthernet1/0/1] port private-vlan 2 3 trunk promiscuous
```

```
[Sysname-GigabitEthernet1/0/1] display this
```

```
#
```

```
interface GigabitEthernet1/0/1
```

```
port link-mode bridge
```

```
port link-type hybrid
```

```
port private-vlan 2 3 trunk promiscuous
```

```
port hybrid vlan 2 3 20 30 tagged
```

```
port hybrid vlan 1 untagged
```

```
#
```

```
return
```

可以看出当该端口在 VLAN 2、3 中工作在 trunk promiscuous 模式时，该端口会加入 Primary VLAN 2、3 及关联的 Secondary VLAN 20、30，同时修改端口的链路类型。

取消端口 GigabitEthernet1/0/1 在 VLAN 2、3 中的 trunk promiscuous 模式配置，并显示配置结果。

```
[Sysname-GigabitEthernet1/0/1] undo port private-vlan 2 3 trunk promiscuous
```

```
[Sysname-GigabitEthernet1/0/1] display this
```

```
#
```

```
interface GigabitEthernet1/0/1
```

```
port link-mode bridge
```

```
port link-type hybrid
```

```
port hybrid vlan 20 30 tagged
```

```
port hybrid vlan 1 untagged
```

```
#
```

```
return
```

可以看出该端口退出 Primary VLAN 2、3，但该端口的 VLAN 属性（包括端口加入 Secondary VLAN 以及端口的链路类型、缺省 VLAN 的配置）不做改变。

【相关命令】

- **port private-vlan host**
- **port private-vlan promiscuous**
- **port private-vlan trunk secondary**
- **private-vlan (VLAN view)**
- **private-vlan primary**

2.1.5 port private-vlan trunk secondary

port private-vlan trunk secondary 命令用来配置端口在指定 VLAN 中工作在 trunk secondary 模式并加入该 VLAN。

undo port private-vlan trunk secondary 命令用来配置端口在指定 VLAN 退出 trunk secondary 模式。

【命令】

```
port private-vlan vlan-id-list trunk secondary
undo port private-vlan vlan-id-list trunk secondary
```

【缺省情况】

端口在指定 VLAN 中不工作在 trunk secondary 模式。

【视图】

二层以太网接口视图

二层聚合接口视图

【缺省用户角色】

network-admin

【参数】

vlan-id-list: VLAN 列表, Secondary VLAN 的范围。表示方式为 *vlan-id-list* = { *vlan-id1* [to *vlan-id2*] } &<1-10>, *vlan-id* 取值范围为 1~4094, *vlan-id2* 的值要大于或等于 *vlan-id1* 的值, &<1-10>表示前面的参数最多可以重复输入 10 次。其中, 系统缺省 VLAN (VLAN 1) 虽然在取值范围中, 但不能配置。

【使用指导】

执行本命令时若指定 VLAN 的类型为 Secondary VLAN, 且存在和指定 VLAN 有映射关系的 Primary VLAN, 则端口也会同步加入这些 Primary VLAN。

在执行 **port private-vlan trunk secondary** 命令时, 当端口同步加入 Primary VLAN,

- 若此前端口的链路类型为 Access 类型, 则会:
 - 配置端口的链路类型为 Hybrid 类型, 缺省 VLAN 不做改变。
 - 端口会以 Tagged 方式加入所有对应 VLAN (包括指定 VLAN 及同步加入的 Primary VLAN)。
- 若此前端口的链路类型为 Trunk 类型, 则端口的链路类型及缺省 VLAN 不做改变。
- 若此前端口的链路类型为 Hybrid 类型, 则端口的链路类型及缺省 VLAN 不做改变。端口加入对应 VLAN (包括指定 VLAN 及同步加入的 Primary VLAN) 时:
 - 若端口此前存在以 Tagged/Untagged 方式加入某些对应 VLAN 的配置, 则在保持原有配置的基础上, 端口会以 Tagged 方式加入其他对应 VLAN。
 - 若端口此前不存在加入某些对应 VLAN 的配置, 则端口会以 Tagged 方式加入所有对应 VLAN。

工作在 trunk secondary 模式的端口, 对于一个 Primary VLAN 对应的 Secondary VLAN, 只能加入其中的一个, 但可以分别加入多个 Primary VLAN 对应的多个 Secondary VLAN。

undo port private-vlan trunk secondary 命令将指定 VLAN 退出 trunk secondary 模式，但端口的 VLAN 关系（包括端口加入 Primary VLAN 以及端口的链路类型、缺省 VLAN 的配置）不做改变。

在执行完 **port private-vlan trunk secondary** 命令后，再执行 **undo port private-vlan trunk secondary** 命令时：

- 若端口的链路类型为 Access 类型，则端口加入指定 VLAN 的配置不做改变。
- 若端口的链路类型为 Trunk/Hybrid 类型，则取消端口加入指定 VLAN 的配置。

可以在执行完 **port private-vlan trunk secondary** 命令后，再建立指定 VLAN 与 Primary VLAN 的映射关系，此时，该命令的功能依然生效。

在执行 **port private-vlan trunk secondary** 命令时，若其中 *vlan-id-list* 中部分 VLAN 不满足要求，则本命令只在其他满足要求的 VLAN 中生效。比如：

- 指定 VLAN 不存在。
- 指定 VLAN 的类型为除 Secondary VLAN 外的其他特殊类型 VLAN。
- 本端口已经在指定 VLAN 对应 Primary VLAN 下的其他 Secondary VLAN 中工作在 trunk secondary 模式。

port private-vlan trunk secondary 命令与 **port private-vlan host**、**port private-vlan promiscuous** 及 **port private-vlan trunk promiscuous** 命令互斥。

port private-vlan trunk secondary 命令适用于需要多个 Secondary VLAN（分别对应不同的 Primary VLAN）通过下行端口的情况，配置该命令后多个 Secondary VLAN 携带 Tag 通过下行端口。**port private-vlan host** 命令适用于只有一个 Secondary VLAN 通过下行端口的情况，配置该命令后 Secondary VLAN 不带 Tag 通过下行端口。

【举例】

- VLAN 2、3 的类型为 Primary VLAN，且 VLAN 2 和 Secondary VLAN 20 关联，VLAN 3 和 Secondary VLAN 30 关联。

显示端口 GigabitEthernet1/0/1 当前配置。

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] display this
#
interface GigabitEthernet1/0/1
 port link-mode bridge
#
return
```

配置链路类型为 Access 的端口 GigabitEthernet1/0/1 在 VLAN 20、30 中工作在 trunk secondary 模式，并显示配置结果。

```
[Sysname-GigabitEthernet1/0/1] port private-vlan 20 30 trunk secondary
[Sysname-GigabitEthernet1/0/1] display this
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port link-type hybrid
 port hybrid vlan 2 3 20 30 tagged
```

```
port hybrid vlan 1 untagged
port private-vlan 20 30 trunk secondary
#
return
```

可以看出当该端口在 VLAN 20、30 中工作在 trunk secondary 模式时，该端口会加入 Secondary VLAN 20、30 及关联的 Primary VLAN 2、3，同时修改链路类型。

取消端口 GigabitEthernet1/0/1 在 VLAN 20、30 中的 trunk secondary 模式配置，并显示配置结果。

```
[Sysname-GigabitEthernet1/0/1] undo port private-vlan 20 30 trunk secondary
[Sysname-GigabitEthernet1/0/1] display this
#
interface GigabitEthernet1/0/1
port link-mode bridge
port link-type hybrid
port hybrid vlan 2 3 tagged
port hybrid vlan 1 untagged
#
return
```

可以看出该端口退出 Secondary VLAN 20、30，但该端口的 VLAN 属性（包括端口加入 Primary VLAN 以及端口的链路类型、缺省 VLAN 的配置）不做改变。

- VLAN 10 的类型不为 Secondary VLAN。

显示端口 GigabitEthernet1/0/1 当前配置。

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] display this
#
interface GigabitEthernet1/0/1
port link-mode bridge
#
return
```

配置链路类型为 Access 的端口 GigabitEthernet1/0/1 在 VLAN 10 中工作在 trunk secondary 模式，并显示配置结果。

```
[Sysname-GigabitEthernet1/0/1] port private-vlan 10 trunk secondary
[Sysname-GigabitEthernet1/0/1] display this
#
interface GigabitEthernet1/0/1
port link-mode bridge
port link-type hybrid
port hybrid vlan 10 tagged
port hybrid vlan 1 untagged
port private-vlan 10 trunk secondary
#
return
```

可以看出该端口在 VLAN 10 中工作在 trunk secondary 模式时，该端口会加入 Secondary VLAN 10，同时修改链路类型。

取消端口 GigabitEthernet1/0/1 在 VLAN 10 中的 trunk secondary 模式配置，并显示配置结果。


```
[Sysname-GigabitEthernet1/0/1] undo port private-vlan 10 trunk secondary
[Sysname-GigabitEthernet1/0/1] display this
#
interface GigabitEthernet1/0/1
  port link-mode bridge
  port link-type hybrid
  port hybrid vlan 1 untagged
#
return
```

可以看出该端口退出 VLAN 10, 但该端口的 VLAN 属性(包括端口的链路类型、缺省 VLAN 的配置)不做改变。

【相关命令】

- `port private-vlan host`
- `port private-vlan promiscuous`
- `port private-vlan trunk promiscuous`
- `private-vlan (VLAN view)`
- `private-vlan isolated`
- `private-vlan primary`

2.1.6 private-vlan (VLAN interface view)

`private-vlan secondary` 命令用来配置 Primary VLAN 下指定的 Secondary VLAN 间三层互通。

`undo private-vlan` 用来取消 Primary VLAN 下指定的或所有的 Secondary VLAN 间三层互通。

【命令】

```
private-vlan secondary vlan-id-list
undo private-vlan [ secondary vlan-id-list ]
```

【缺省情况】

Secondary VLAN 间三层不互通。

【视图】

VLAN 接口视图

【缺省用户角色】

network-admin

【参数】

vlan-id-list: VLAN 列表, Secondary VLAN 的范围。表示方式为 *vlan-id-list* = { *vlan-id1* [**to** *vlan-id2*] } &<1-10>, *vlan-id* 取值范围为 1~4094, *vlan-id2* 的值要大于或等于 *vlan-id1* 的值, &<1-10>表示前面的参数最多可以重复输入 10 次。

【使用指导】

要使功能生效, 执行该命令时, 必须满足如下条件:

- 该命令只能在 Primary VLAN 对应的 VLAN 接口 (Primary VLAN interface) 视图下执行。

- Secondary VLAN 必须已经与该对应的 Primary VLAN 建立了映射关系。
- Secondary VLAN 不能建立对应的 VLAN 接口。
- 在该三层虚接口上配置 IP 地址。
- 本地代理 ARP/ND 功能。

没有配置三层互通的 Secondary VLAN 可以创建对应的 VLAN 接口，配置了三层互通的 Secondary VLAN 不能创建对应的 VLAN 接口。

在同一 Primary VLAN interface 下多次执行本命令时，最终生效结果是多次配置的集合。

在执行 **undo private-vlan** 命令时：

- 如果不带参数 **secondary vlan-id-list**，就解除所有 Secondary VLAN 间的三层互通。
- 如果带有该参数，就解除指定的 Secondary VLAN 间的三层互通。

【举例】

配置 Primary VLAN 2 下的 Secondary VLAN 3、4 三层互通（GigabitEthernet1/0/2 为上行端口，GigabitEthernet1/0/3、GigabitEthernet1/0/4 为下行端口）。

建立 Primary VLAN 2 和 Secondary VLAN 3、4 的映射关系。

```
<Sysname> system-view
[Sysname] vlan 3 to 4
[Sysname] vlan 2
[Sysname-vlan2] private-vlan primary
[Sysname-vlan2] private-vlan secondary 3 to 4
[Sysname-vlan2] quit
```

配置端口 GigabitEthernet1/0/2 在 VLAN 2 中工作在 promiscuous 模式。

```
[Sysname] interface gigabitethernet 1/0/2
[Sysname-GigabitEthernet1/0/2] port private-vlan 2 promiscuous
[Sysname-GigabitEthernet1/0/2] quit
```

配置链路类型为 Access 的端口 GigabitEthernet1/0/3 在 VLAN 3 中工作在 host 模式，链路类型为 Access 的端口 GigabitEthernet1/0/4 在 VLAN 4 中工作在 host 模式。

```
[Sysname] interface gigabitethernet 1/0/3
[Sysname-GigabitEthernet1/0/3] port access vlan 3
[Sysname-GigabitEthernet1/0/3] port private-vlan host
[Sysname-GigabitEthernet1/0/3] quit
[Sysname] interface gigabitethernet 1/0/4
[Sysname-GigabitEthernet1/0/4] port access vlan 4
[Sysname-GigabitEthernet1/0/4] port private-vlan host
[Sysname-GigabitEthernet1/0/4] quit
```

配置 Primary VLAN 2 下的 Secondary VLAN 3、4 三层互通，同时配置 Primary VLAN 接口的 IP 地址及开启本地代理 ARP 功能。

```
[Sysname] interface vlan-interface 2
[Sysname-Vlan-interface2] private-vlan secondary 3 to 4
[Sysname-Vlan-interface2] ip address 192.168.1.1 255.255.255.0
[Sysname-Vlan-interface2] local-proxy-arp enable
```

【相关命令】

- **private-vlan** (VLAN view)

- **private-vlan primary**

2.1.7 private-vlan (VLAN view)

private-vlan 命令用来建立 Primary VLAN 和 Secondary VLAN 的映射关系。

undo private-vlan 用来解除 Primary VLAN 和 Secondary VLAN 的映射关系。

【命令】

```
private-vlan secondary vlan-id-list
undo private-vlan [secondary vlan-id-list]
```

【缺省情况】

未建立 Primary VLAN 和 Secondary VLAN 的映射关系。

【视图】

VLAN 视图

【缺省用户角色】

network-admin

【参数】

secondary *vlan-id-list*：表示方式为 *vlan-id-list* = { *vlan-id1* [**to** *vlan-id2*] }&<1-10>, *vlan-id* 取值范围为 1~4094, *vlan-id2* 的值要大于或等于 *vlan-id1* 的值, &<1-10>表示前面的参数最多可以重复输入 10 次。其中, 系统缺省 VLAN (VLAN 1) 虽然在取值范围中, 但不能配置。

【使用指导】

Primary VLAN 可以与多个 Secondary VLAN 建立映射关系。在同一 VLAN 视图下多次执行 **private-vlan** 命令时, Primary VLAN 对应的 Secondary VLAN 是多次配置的集合。

在执行 **private-vlan** 命令时, 若满足以下条件, 则依据接口配置会触发配置同步。

- 已经配置 Primary VLAN。
- 设备上有端口工作在 promiscuous 模式、trunk promiscuous 模式或 host 模式。

在执行 **undo private-vlan** 命令时:

- 如果不带参数 **secondary** *vlan-id-list*, 就解除所有 Secondary VLAN 和对应 Primary VLAN 的映射关系。
- 如果带有该参数, 就解除参数指定的 Secondary VLAN 和对应 Primary VLAN 的映射关系。

【举例】

建立 Primary VLAN 2 和 Secondary VLAN 3、4 的映射关系。

```
<Sysname> system-view
[Sysname] vlan 3 to 4
[Sysname] vlan 2
[Sysname-vlan2] private-vlan primary
[Sysname-vlan2] private-vlan secondary 3 to 4
```

【相关命令】

- **port private-vlan host**

- `port private-vlan promiscuous`
- `port private-vlan trunk promiscuous`
- `port private-vlan trunk secondary`
- `primary-vlan primary`

2.1.8 private-vlan community

`private-vlan community` 命令用来配置同一 Secondary VLAN 内各端口二层互通。

【命令】

`private-vlan community`

【缺省情况】

同一 Secondary VLAN 内的端口二层互通。

【视图】

VLAN 视图

【缺省用户角色】

network-admin

【使用指导】

`private-vlan community` 命令实现的功能与 `undo private-vlan isolated` 命令相同。

当用户通过 `save` 命令保存配置时，`private-vlan community` 命令的配置不会被存入配置文件。

【举例】

配置 Secondary VLAN 4 内各端口二层互通（GigabitEthernet1/0/1 工作为 promiscuous 模式，GigabitEthernet1/0/2 和 GigabitEthernet1/0/3 工作在 host 模式）。完成下述配置后，Secondary VLAN 4 内端口 GigabitEthernet1/0/2 和 GigabitEthernet1/0/3 二层互通。

建立 Primary VLAN 2 和 Secondary VLAN 4 的映射关系。

```
<Sysname> system-view
[Sysname] vlan 4
[Sysname-vlan4] quit
[Sysname] vlan 2
[Sysname-vlan2] private-vlan primary
[Sysname-vlan2] private-vlan secondary 4
[Sysname-vlan2] quit
```

配置端口 GigabitEthernet1/0/1 在 VLAN 2 中工作在 promiscuous 模式。

```
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] port private-vlan 2 promiscuous
[Sysname-GigabitEthernet1/0/1] quit
```

配置链路类型为 Access 的端口 GigabitEthernet1/0/2 和 GigabitEthernet1/0/3 在 VLAN 4 中工作在 host 模式。

```
[Sysname] interface gigabitethernet 1/0/2
[Sysname-GigabitEthernet1/0/2] port access vlan 4
[Sysname-GigabitEthernet1/0/2] port private-vlan host
```

```
[Sysname-GigabitEthernet1/0/2] quit
[Sysname] interface gigabitethernet 1/0/3
[Sysname-GigabitEthernet1/0/3] port access vlan 4
[Sysname-GigabitEthernet1/0/3] port private-vlan host
[Sysname-GigabitEthernet1/0/3] quit
# 配置 Secondary VLAN 4 内各端口二层互通。
[Sysname] vlan 4
[Sysname-vlan4] private-vlan community
```

【相关命令】

- **private-vlan isolated**

2.1.9 private-vlan isolated

private-vlan isolated 命令用来配置同一 Secondary VLAN 内各端口二层隔离。

undo private-vlan isolated 命令用来恢复缺省情况。

【命令】

```
private-vlan isolated
undo private-vlan isolated
```

【缺省情况】

同一 Secondary VLAN 内的端口能够二层互通。

【视图】

VLAN 视图

【缺省用户角色】

network-admin

【使用指导】

配置 **private-vlan isolated** 命令时，需满足以下条件，命令才能生效。

- Primary VLAN 与 Secondary VLAN 建立映射关系。
- 下行端口配置为 trunk secondary 模式或 host 模式。

Secondary VLAN 隔离与 Primary VLAN 配置互斥。

【举例】

配置 Secondary VLAN 4 内各端口二层隔离（GigabitEthernet1/0/1 工作在 promiscuous 模式，GigabitEthernet1/0/2 及 GigabitEthernet1/0/3 工作在 host 模式）。完成下述配置后，Secondary VLAN 4 内端口 GigabitEthernet1/0/2 和 GigabitEthernet1/0/3 二层隔离。

建立 Primary VLAN 2 和 Secondary VLAN 4 的映射关系。

```
<Sysname> system-view
[Sysname] vlan 4
[Sysname-vlan4] quit
[Sysname] vlan 2
[Sysname-vlan2] private-vlan primary
[Sysname-vlan2] private-vlan secondary 4
[Sysname-vlan2] quit
```

配置端口 GigabitEthernet1/0/1 在 VLAN 2 中工作在 promiscuous 模式。

```
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] port private-vlan 2 promiscuous
[Sysname-GigabitEthernet1/0/1] quit
```

配置链路类型为 Access 的端口 GigabitEthernet1/0/2 和 GigabitEthernet1/0/3 在 VLAN 4 中工作在 host 模式。

```
[Sysname] interface gigabitethernet 1/0/2
[Sysname-GigabitEthernet1/0/2] port access vlan 4
[Sysname-GigabitEthernet1/0/2] port private-vlan host
[Sysname-GigabitEthernet1/0/2] quit
[Sysname] interface gigabitethernet 1/0/3
[Sysname-GigabitEthernet1/0/3] port access vlan 4
[Sysname-GigabitEthernet1/0/3] port private-vlan host
[Sysname-GigabitEthernet1/0/3] quit
```

配置 Secondary VLAN 4 内各端口二层隔离。

```
[Sysname] vlan 4
[Sysname-vlan4] private-vlan isolated
```

【相关命令】

- **private-vlan** (VLAN view)
- **private-vlan community**
- **private-vlan primary**

2.1.10 private-vlan primary

private-vlan primary 命令用来配置 VLAN 的类型为 Primary VLAN。

undo private-vlan primary 命令用来恢复缺省情况。

【命令】

```
private-vlan primary
undo private-vlan primary
```

【缺省情况】

VLAN 的类型不是 Primary VLAN。

【视图】

VLAN 视图

【缺省用户角色】

network-admin

【使用指导】

配置该命令时，若满足以下条件，则依据接口配置会触发配置同步：

- 已经配置 Primary VLAN 和 Secondary VLAN 的映射关系。
- 设备上有端口工作在 promiscuous 模式、trunk promiscuous 模式、trunk secondary 模式或 host 模式。

【举例】

配置 VLAN 5 为 Primary VLAN。

```
<Sysname> system-view
[Sysname] vlan 5
[Sysname-vlan5] private-vlan primary
```

【相关命令】

- port private-vlan host
- port private-vlan promiscuous
- port private-vlan trunk promiscuous
- port private-vlan trunk secondary
- private-vlan primary

3 Voice VLAN



说明

S5000E-X、S5110V2-SI 与 S5000V3-EI 系列交换机不支持 Voice VLAN。

3.1 Voice VLAN配置命令

3.1.1 display voice-vlan mac-address

display voice-vlan mac-address 命令用来显示 Voice VLAN 支持的 OUI 地址。

【命令】

display voice-vlan mac-address

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator

【举例】

显示 Voice VLAN 支持的 OUI 地址。

```
<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
```

表3-1 display voice-vlan mac-address 命令显示信息描述表

字段	描述
OUI Address	设备当前允许通过的OUI地址
Mask	设备当前允许通过的OUI地址的掩码
Description	设备当前允许通过的OUI地址的描述

【相关命令】

- `voice-vlan mac-address`

3.1.2 `display voice-vlan state`

`display voice-vlan state` 命令用来显示 Voice VLAN 的配置信息。

【命令】

`display voice-vlan state`

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator

【举例】

```
# 显示 Voice VLAN 的配置信息。
<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
```

表3-2 `display voice-vlan state` 命令显示信息描述表

字段	描述
Current Voice VLANs	已创建的Voice VLAN数量
Voice VLAN security mode	Voice VLAN的安全模式的开启状态： <ul style="list-style-type: none">• Security: 表示当前使用的是安全模式• Normal: 表示当前使用的是普通模式
Voice VLAN aging time	Voice VLAN的老化时间，No aging表示不老化
Voice VLAN enabled ports and their modes	当前开启了Voice VLAN的端口及其工作模式
Port	当前开启了Voice VLAN的端口的简名
VLAN	端口开启的Voice VLAN ID
Mode	端口Voice VLAN的工作模式： <ul style="list-style-type: none">• Auto: 表示自动模式• Manual: 表示手工模式
CoS	服务级别
DSCP	差分服务编码点优先级

【相关命令】

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

3.1.3 voice-vlan aging

`voice-vlan aging` 命令用来设置 Voice VLAN 的老化时间。

`undo voice-vlan aging` 命令用来恢复缺省情况。

【命令】

```
voice-vlan aging minutes  
undo voice-vlan aging
```

【缺省情况】

Voice VLAN 的老化时间为 1440 分钟（24 小时）。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

minutes: Voice VLAN 的老化时间，取值范围为 0 或 5~43200，单位为分钟。0 表示不老化。

【使用指导】

在自动模式下，当系统将入端口加入 Voice VLAN 后，老化时间由对应的老化定时器控制。当系统在老化定时器停止前没有从入端口收到任何语音报文时，系统会自动把该端口从 Voice VLAN 中删除。

Voice VLAN 的老化定时器需在对应的 MAC 地址表项老化之后才能启动，因此 Voice VLAN 的老化周期为设备上配置的 Voice VLAN 老化时间与动态 MAC 地址表项老化时间之和。有关动态 MAC 地址老化时间的详细介绍，请参见“MAC 地址表”。

老化时间只对 Voice VLAN 工作在自动模式的端口有效，对 Voice VLAN 工作在手工模式的端口无效。

【举例】

将 Voice VLAN 的老化时间配置为 100 分钟。

```
<Sysname> system-view  
[Sysname] voice-vlan aging 100
```

【相关命令】

- `display voice-vlan state`

3.1.4 voice-vlan enable

voice-vlan *vlan-id* enable 命令用来开启端口的 Voice VLAN 功能。

undo voice-vlan enable 命令用来关闭端口的 Voice VLAN 功能。

【命令】

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

【缺省情况】

端口的 Voice VLAN 功能处于关闭状态。

【视图】

二层以太网接口视图

【缺省用户角色】

network-admin

【参数】

vlan-id: Voice VLAN 编号，取值范围为 2~4094。

【使用指导】

当端口的 Voice VLAN 工作在自动模式时，只有 Trunk 或者 Hybrid 类型端口支持开启 Voice VLAN 功能。

开启端口的 Voice VLAN 功能之前，须确保对应的 VLAN 已存在。

【举例】

```
# 开启端口 GigabitEthernet1/0/1 的 Voice VLAN 功能。
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] voice-vlan 2 enable
```

【相关命令】

- **display voice-vlan state**
- **voice-vlan mode auto**

3.1.5 voice-vlan mac-address

voice-vlan mac-address 命令用来配置 Voice VLAN 中可识别的 OUI 地址。

undo voice-vlan mac-address 命令用来删除 Voice VLAN 中可识别的 OUI 地址。

【命令】

```
voice-vlan mac-address mac-address mask oui-mask [ description text ]
undo voice-vlan mac-address oui
```

【缺省情况】

设备已配置有如下表所示的 OUI 地址。

表3-3 设备缺省的 OUI 地址

序号	OUI 地址	生产厂商
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
8	00e0-bb00-0000	3Com phone

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

mac-address: 语音报文的源 MAC 地址，格式为 H-H-H，如：1234-1234-1234。

mask oui-mask: OUI 地址的有效长度，用掩码表示，格式为 H-H-H。由连续的 1 和连续的 0 组成，表示 OUI 地址的匹配长度。如：ffff-0000-0000，如果要匹配某个设备厂商的语音设备，可以设置为 ffff-ff00-0000。

description text: OUI 地址的描述字符串，长度为 1~30，区分大小写。

oui: 指定要删除的 OUI 地址，格式为 H-H-H，如 1234-1200-0000。OUI 地址不能是广播地址或者组播地址，也不能是全 0 的地址。OUI 地址是 *mac-address* 和 *oui-mask* 参数相与的结果。

【使用指导】

设备缺省的 OUI 地址可以手工删除，删除之后也可再次手工添加。

本设备最多支持配置 128 个 OUI 地址。

【举例】

配置允许来自 IP 电话 PhoneA（MAC 地址为 1234-1234-1234）的语音流通过 Voice VLAN。

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

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

【相关命令】

- **display voice-vlan mac-address**

3.1.6 voice-vlan mode auto

voice-vlan mode auto 命令用来配置端口的 Voice VLAN 工作模式为自动模式。

undo voice-vlan mode auto 命令用来配置端口的 Voice VLAN 工作模式为手工模式。

【命令】

```
voice-vlan mode auto
undo voice-vlan mode auto
```

【缺省情况】

端口的 Voice VLAN 工作模式为自动模式。

【视图】

二层以太网接口视图

【缺省用户角色】

network-admin

【使用指导】

当端口开启了 Voice VLAN 并工作在手工模式时，必须手工将端口加入 Voice VLAN，才能保证 Voice VLAN 功能生效。

【举例】

将端口 GigabitEthernet1/0/1 的 Voice VLAN 的工作模式设置为手工模式。

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] undo voice-vlan mode auto
```

【相关命令】

- **display voice-vlan state**

3.1.7 voice-vlan security enable

voice-vlan security enable 命令用来开启 Voice VLAN 的安全模式。

undo voice-vlan security enable 命令用来关闭 Voice VLAN 的安全模式。

【命令】

```
voice-vlan security enable
undo voice-vlan security enable
```

【缺省情况】

Voice VLAN 的安全模式处于开启状态。

【视图】

系统视图

【缺省用户角色】

network-admin

【使用指导】

在安全模式下，Voice VLAN 中只能有语音流量。用户开启 Voice VLAN 的安全模式以后，该 VLAN 的报文都经过过滤，设备会根据报文的源 MAC 地址是否匹配 OUI 地址来过滤所有非语音流量，增

加安全性保证语音流的优先级，保证通话质量。在普通模式下，Voice VLAN 中允许有业务流量和语音流量并存。

【举例】

关闭 Voice VLAN 的安全模式。

```
<Sysname> system-view
[Sysname] undo voice-vlan security enable
```

【相关命令】

- **display voice-vlan state**

3.1.8 voice-vlan track lldp

voice-vlan track lldp 命令用来开启通过 LLDP 自动发现 IP 电话功能。

undo voice-vlan track lldp 命令用来关闭通过 LLDP 自动发现 IP 电话功能。

【命令】

```
voice-vlan track lldp
undo voice-vlan track lldp
```

【缺省情况】

通过 LLDP 自动发现 IP 电话功能处于关闭状态。

【视图】

系统视图

【缺省用户角色】

network-admin

【举例】

开启通过 LLDP 自动发现 IP 电话功能。

```
<Sysname> system-view
[Sysname] voice-vlan track lldp
```

目 录

1 MVRP	1-1
1.1 MVRP配置命令	1-1
1.1.1 display mvrp running-status	1-1
1.1.2 display mvrp state.....	1-3
1.1.3 display mvrp statistics.....	1-4
1.1.4 mvp timer join.....	1-6
1.1.5 mvp timer leave	1-7
1.1.6 mvp timer leaveall	1-8
1.1.7 mvp timer periodic.....	1-9
1.1.8 mvrp enable	1-9
1.1.9 mvrp global enable.....	1-10
1.1.10 mvrp gvrp-compliance enable	1-11
1.1.11 mvrp registration.....	1-11
1.1.12 reset mvrp statistics.....	1-12

1 MVRP

1.1 MVRP配置命令

1.1.1 display mvrp running-status

display mvrp running-status 命令用来显示 MVRP 运行状态信息。

【命令】

display mvrp running-status [**interface** *interface-list*]

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator

【参数】

interface *interface-list*: 显示指定端口上的 MVRP 运行状态信息。*interface-list* 为以太网端口列表，表示方式为 *interface-list* = *interface-type* *interface-number1* [**to** *interface-type* *interface-number2*]。其中，*interface-type* *interface-number* 为端口类型和端口编号，且 *interface-type* *interface-number2* 的值大于等于 *interface-number1* 的值。如果指定该参数，但端口关闭 MVRP 功能，则只显示 MVRP 全局信息。如果未指定该参数，则显示 MVRP 全局信息和所有开启 MVRP 功能端口的 MVRP 运行状态信息。

【举例】

显示 MVRP 全局信息和所有开启 MVRP 功能端口的 MVRP 运行状态信息。

```
<Sysname> display mvrp running-status
-----[MVRP Global Info]-----
Global Status      : Enabled
Compliance-GVRP   : False

----[GigabitEthernet1/0/1]----
Config Status      : Enabled
Running Status     : Enabled
Join Timer         : 20 (centiseconds)
Leave Timer         : 60 (centiseconds)
Periodic Timer     : 100 (centiseconds)
LeaveAll Timer      : 1000 (centiseconds)
Registration Type   : Normal
Registered VLANs :
  1(default), 2-10
Declared VLANs :
```



```

1(default), 2-10
Propagated VLANs :
1(default), 2-10

----[GigabitEthernet1/0/2]----
Config Status           : Enabled
Running Status          : Disabled
Join Timer              : 20 (centiseconds)
Leave Timer              : 60 (centiseconds)
Periodic Timer          : 100 (centiseconds)
LeaveAll Timer           : 1000 (centiseconds)
Registration Type       : Normal
Registered VLANs :
None
Declared VLANs :
None
Propagated VLANs :
None

```

表1-1 display mvrp running-status 命令显示信息描述表

字段	描述
MVRP Global Info	MVRP全局信息
Global Status	MVRP全局状态: <ul style="list-style-type: none"> Enabled: 开启状态 Disabled: 关闭状态
Compliance-GVRP	是否兼容GVRP: <ul style="list-style-type: none"> True: 兼容 GVRP False: 不兼容 GVRP
Config Status	端口上MVRP功能的开启状态，取值为Enabled，表示开启MVRP
Running Status	端口上MVRP功能是否生效: <ul style="list-style-type: none"> Enabled: 已生效 Disabled: 未生效 端口上MVRP功能生效的决定条件: <ul style="list-style-type: none"> 全局和端口上 MVRP 功能的开启状态 端口的物理连接状态 链路类型 端口是否为聚合成员端口
Join Timer	Join定时器的值，单位是厘秒
Leave Timer	Leave定时器的值，单位是厘秒
Periodic Timer	Periodic定时器的值，单位是厘秒
LeaveAll Timer	LeaveAll定时器的值，单位是厘秒

字段	描述
Registration Type	MVRP的注册模式： <ul style="list-style-type: none"> Normal: 表示 Normal 模式 Fixed: 表示 Fixed 模式 Forbidden: 表示 Forbidden 模式
Registered VLANs	端口注册的VLAN
Declared VLANs	端口声明的VLAN，即通知对端端口学习的VLAN
Propagated VLANs	端口传播的VLAN，即端口学习并通知本设备其他端口向外声明的VLAN

1.1.2 display mvrp state

display mvrp state 命令用来显示端口在指定 VLAN 内的 MVRP 状态信息。

【命令】

display mvrp state interface *interface-type interface-number* **vlan** *vlan-id*

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator

【参数】

interface *interface-type interface-number*: 显示指定端口上的 MVRP 状态信息。其中，*interface-type interface-number* 为端口类型和端口编号。

vlan *vlan-id*: 显示指定 VLAN 内的 MVRP 状态信息。其中，*vlan-id* 为指定 VLAN 的编号，取值范围为 1~4094。

【举例】

显示端口 GigabitEthernet1/0/1 在 VLAN 2 中对应的 MVRP 状态信息。

```
<Sysname> display mvrp state interface gigabitethernet 1/0/1 vlan 2
MVRP state of VLAN 2 on port GE1/0/1:
Port                VLAN    App-state    Reg-state
-----
GE1/0/1              2      VP           IN
```

表1-2 display mvrp state 命令显示信息描述表

字段	描述
MVRP state of VLAN 2 on port GE1/0/1	端口GigabitEthernet1/0/1在VLAN 2中对应的MVRP状态信息
Port	端口简单名称，显示开启MVRP的端口的MVRP状态信息
VLAN	指定的VLAN ID

字段	描述
App-state	<p>属性声明状态，用来记录本端向对端实体声明的属性的状态。其状态包括：VO、VP、VN、AN、AA、QA、LA、AO、QO、AP、QP和LO，每个状态都由2个字母组成，各字母含义如下：</p> <p>第一个字母表示状态：</p> <ul style="list-style-type: none"> • V 代表 Very anxious（非常迫切的），表示该属性未曾声明过且没有收到过 Join 消息 • A 代表 Anxious（迫切的），表示该属性声明过一次或收到过一个 Join 消息 • Q 代表 Quiet（安静的），表示该属性声明过两次，或声明过一次且收到过一个 Join 消息，或收到过两个 Join 消息 • L 代表 Leaving（离开），表示该属性正在注销 <p>第二个字母表示成员类型：</p> <ul style="list-style-type: none"> • A 代表 Active member（主动成员），表示正在声明该属性，至少已有一次发送，可以有接收 • P 代表 Passive member（被动成员），表示正在声明该属性，但是只有接收，没有发送 • O 代表 Observer（观察者），表示未在声明该属性，只是在侦听 • N 代表 New（新属性被动端），表示正在声明该属性，但是只有接收，没有发送 <p>譬如，VP代表“Very anxious，Passive member”，表示Very anxious状态下的被动成员</p>
Reg-state	<p>属性注册状态，用来记录对端实体声明的属性在本端的注册情况。其状态包括：IN、LV和MT，各状态含义如下：</p> <ul style="list-style-type: none"> • IN：注册状态，端口已经注册了该属性 • LV：离开状态，端口正在注销该属性 • MT：注销状态，端口未注册该属性

1.1.3 display mvrp statistics

display mvrp statistics 命令用来显示 MVRP 统计信息。

【命令】

display mvrp statistics [interface interface-list]

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator

【参数】

interface interface-list：显示指定端口上的 MVRP 统计信息。*interface-list* 为以太网端口列表，表示方式为 *interface-list = interface-type interface-number1 [to interface-type interface-number2]*。其中，*interface-type interface-number* 为端口类型和端口编号，且 *interface-type interface-number2* 的值大于等于

interface-number1。如果未指定该参数，则显示所有开启 MVRP 功能的端口的 MVRP 统计信息。

【使用指导】

如果指定的端口上没有开启 MVRP 功能，则不显示任何信息。

【举例】

显示所有端口的 MVRP 统计信息。

```
<Sysname> display mvrp statistics
```

```
----[GigabitEthernet1/0/1]----
Failed Registrations      : 1
Last PDU Origin           : 000f-e200-0010
Frames Received           : 201
  New Event Received      : 0
  JoinIn Event Received   : 1167
  In Event Received       : 0
  JoinMt Event Received   : 22387
  Mt Event Received       : 31
  Leave Event Received    : 210
  LeaveAll Event Received : 63
Frames Transmitted        : 120
  New Event Transmitted   : 0
  JoinIn Event Transmitted : 311
  In Event Transmitted    : 0
  JoinMt Event Transmitted : 873
  Mt Event Transmitted    : 11065
  Leave Event Transmitted : 167
  LeaveAll Event Transmitted : 4
Frames Discarded          : 0

----[GigabitEthernet1/0/2]----
Failed Registrations      : 0
Last PDU Origin           : 0000-0000-0000
Frames Received           : 0
  New Event Received      : 0
  JoinIn Event Received   : 0
  In Event Received       : 0
  JoinMt Event Received   : 0
  Mt Event Received       : 0
  Leave Event Received    : 0
  LeaveAll Event Received : 0
Frames Transmitted        : 0
  New Event Transmitted   : 0
  JoinIn Event Transmitted : 0
  In Event Transmitted    : 0
  JoinMt Event Transmitted : 0
  Mt Event Transmitted    : 0
```

```

Leave Event Transmitted      : 0
LeaveAll Event Transmitted   : 0
Frames Discarded            : 0

```

表1-3 display mvrp statistics 命令显示信息描述表

字段	描述
Failed Registrations	本实体上通过MVRP注册VLAN失败的次数
Last PDU Origin	上一个MVRP PDU的源MAC地址
Frames Received	收到的MVRP协议帧数
New Event Received	收到的New属性事件数
JoinIn Event Received	收到的JoinIn属性事件数
In Event Received	收到的In属性事件数
JoinMt Event Received	收到的JoinMt属性事件数
Mt Event Received	收到的Mt属性事件数
Leave Event Received	收到的Leave属性事件数
LeaveAll Event Received	收到的LeaveAll属性事件数
Frames Transmitted	发送的MVRP协议帧数
New Event Transmitted	发送的New属性事件数
JoinIn Event Transmitted	发送的JoinIn属性事件数
In Event Transmitted	发送的In属性事件数
JoinMt Event Transmitted	发送的JoinMt属性事件数
Mt Event Transmitted	发送的Mt属性事件数
Leave Event Transmitted	发送的Leave属性事件数
LeaveAll Event Transmitted	发送的LeaveAll个数
Frames Discarded	丢弃的MVRP协议帧数

1.1.4 mrp timer join

mrp timer join 命令用来配置 Join 定时器的值。

undo mrp timer join 命令用来恢复缺省情况。

【命令】

```

mrp timer join timer-value
undo mrp timer join

```

【缺省情况】

Join 定时器的值为 20 厘秒。

【视图】

二层以太网接口视图
二层聚合接口视图

【缺省用户角色】

network-admin

【参数】

timer-value: Join 定时器的值，单位为厘秒（100 厘秒=1 秒）。其取值应大于等于 20 厘秒，小于 Leave 定时器值的一半，且必须是 20 厘秒的倍数。

【举例】

配置 Join 定时器的值为 40 厘秒（假设此时 Leave 定时器为 100 厘秒）。

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] mrp timer join 40
```

【相关命令】

- **display mvrp running-status**
- **mrp timer leave**

1.1.5 mrp timer leave

mrp timer leave 命令用来配置 Leave 定时器的值。

undo mrp timer leave 命令用来恢复缺省情况。

【命令】

```
mrp timer leave timer-value
undo mrp timer leave
```

【缺省情况】

Leave 定时器的值为 60 厘秒。

【视图】

二层以太网接口视图
二层聚合接口视图

【缺省用户角色】

network-admin

【参数】

timer-value: Leave 定时器的值，单位为厘秒（100 厘秒=1 秒）。其取值应大于 Join 定时器值的两倍、小于 LeaveAll 定时器的值，且必须是 20 厘秒的倍数。

【举例】

配置 Leave 定时器的值为 100 厘秒（假设此时 Join 和 LeaveAll 定时器均为缺省值）。

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

```
[Sysname-GigabitEthernet1/0/1] mrp timer leave 100
```

【相关命令】

- `display mvrp running-status`
- `mrp timer join`
- `mrp timer leaveall`

1.1.6 mrp timer leaveall

`mrp timer leaveall` 命令用来配置 LeaveAll 定时器的值。

`undo mrp timer leaveall` 命令用来恢复缺省情况。

【命令】

```
mrp timer leaveall timer-value
undo mrp timer leaveall
```

【缺省情况】

LeaveAll 定时器的值为 1000 厘秒。

【视图】

二层以太网接口视图

二层聚合接口视图

【缺省用户角色】

network-admin

【参数】

timer-value: LeaveAll 定时器的值，单位为厘秒（100 厘秒=1 秒）。其取值应大于所有端口上 Leave 定时器的值、小于等于 32760 厘秒，且必须是 20 厘秒的倍数。

【使用指导】

每一次 LeaveAll 定时器超时，都会引起全网当前端口对应 MSTI 的所有属性的注销。由于其影响范围很广，所以 LeaveAll 定时器的值不要小于其缺省值。

过小的 LeaveAll 定时器值可能会影响通过 MVRP 学习到的动态 VLAN 的稳定性，建议 LeaveAll 定时器的取值不要小于其缺省值。

为了防止每次都是同一实体的 LeaveAll 定时器先超时，每次重启时，LeaveAll 定时器的值都将在一定范围内随机变动。

【举例】

配置 LeaveAll 定时器的值为 1500 厘秒（假设此时所有端口的 Leave 定时器都为缺省值）。

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] mrp timer leaveall 1500
```

【相关命令】

- `mrp timer leave`
- `display mvrp running-status`

1.1.7 mrp timer periodic

mrp timer periodic 命令用来配置 Periodic 定时器的值。

undo mrp timer periodic 命令用来恢复缺省情况。

【命令】

```
mrp timer periodic timer-value
undo mrp timer periodic
```

【缺省情况】

Periodic 定时器的值为 100 厘秒。

【视图】

二层以太网接口视图

二层聚合接口视图

【支持的缺省用户角色】

network-admin

【参数】

timer-value: Periodic 定时器的值，取值为 0 或 100，单位为厘秒（100 厘秒=1 秒）。

【使用指导】

当 Periodic 定时器的值为 0 厘秒时，定时器关闭。

当 Periodic 定时器的值为 100 厘秒时，定时器开启，这时以 100 厘秒为周期发送 MRP 报文。

【举例】

关闭 Periodic 定时器。

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] mrp timer periodic 0
```

【相关命令】

- **display mvrp running-status**

1.1.8 mvrp enable

mvrp enable 命令用来开启端口的 MVRP 功能。

undo mvrp enable 命令用来关闭端口的 MVRP 功能。

【命令】

```
mvrp enable
undo mvrp enable
```

【缺省情况】

端口的 MVRP 功能处于关闭状态。

【视图】

二层以太网接口视图

二层聚合接口视图

【缺省用户角色】

network-admin

【使用指导】

端口上的 MVRP 功能生效，必须满足：

- 全局和端口上都开启 MVRP 功能。
- 端口的物理连接状态 UP。
- 端口链路类型为 Trunk 类型。
- 端口不为聚合成员端口。

【举例】

开启端口 GigabitEthernet1/0/1 的 MVRP 功能。

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

【相关命令】

- **display mvrp running-status**

1.1.9 mvrp global enable

mvrp global enable 命令用来全局开启 MVRP 功能。

undo mvrp global enable 命令用来关闭全局的 MVRP 功能。

【命令】

```
mvrp global enable
undo mvrp global enable
```

【缺省情况】

全局的 MVRP 功能处于关闭状态。

【视图】

系统视图

【缺省用户角色】

network-admin

【使用指导】

要使端口上的 MVRP 功能生效，必须全局开启 MVRP 功能。

【举例】

全局开启 MVRP 功能。

```
<Sysname> system-view
[Sysname] mvrp global enable
```

【相关命令】

- `display mvrp running-status`

1.1.10 mvrp gvrp-compliance enable

`mvrp gvrp-compliance enable` 命令用来配置 MVRP 兼容 GVRP。

`undo mvrp gvrp-compliance enable` 命令用来恢复缺省情况。

【命令】

```
mvrp gvrp-compliance enable
undo mvrp gvrp-compliance enable
```

【缺省情况】

MVRP 不兼容 GVRP。

【视图】

系统视图

【缺省用户角色】

network-admin

【使用指导】

执行本命令后，既可以处理 MVRP 报文，也可以处理 GVRP 报文

【举例】

```
# 配置 MVRP 兼容 GVRP。
<Sysname> system-view
[Sysname] mvrp gvrp-compliance enable
```

【相关命令】

- `display mvrp running-status`

1.1.11 mvrp registration

`mvrp registration` 命令用来配置端口的 MVRP 注册模式。

`undo mvrp registration` 命令用来恢复缺省情况。

【命令】

```
mvrp registration { fixed | forbidden | normal }
undo mvrp registration
```

【缺省情况】

端口的 MVRP 注册模式为 Normal 模式。

【视图】

二层以太网接口视图
二层聚合接口视图

【缺省用户角色】

network-admin

【参数】

fixed: 表示 Fixed 注册模式。

forbidden: 表示 Forbidden 注册模式。

normal: 表示 Normal 注册模式。

【举例】

配置端口 GigabitEthernet1/0/1 的 MVRP 注册模式为 Fixed 模式。

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

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

```
[Sysname-GigabitEthernet1/0/1] mvrp registration fixed
```

【相关命令】

- **display mvrp running-status**

1.1.12 reset mvrp statistics

reset mvrp statistics 命令用来清除端口上的 MVRP 统计信息。

【命令】

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

【视图】

用户视图

【缺省用户角色】

network-admin

【参数】

interface interface-list: 清除指定端口上的 MVRP 统计信息。*interface-list* 为以太网端口列表，表示方式为 *interface-list=interface-type interface-number1 [to interface-type interface-number2]*。其中，*interface-type interface-number* 为端口类型和端口编号，且 *interface-type interface-number2* 的值大于等于 *interface-number1*。如果未指定该参数，则清除所有端口上的 MVRP 统计信息。

【举例】

清除所有端口上的 MVRP 统计信息。

```
<Sysname> reset mvrp statistics
```

【相关命令】

- **display mvrp statistics**

目 录

1 QinQ.....	1-1
1.1 QinQ配置命令.....	1-1
1.1.1 display qinq.....	1-1
1.1.2 qinq enable	1-2
1.1.3 qinq ethernet-type (interface view).....	1-2
1.1.4 qinq ethernet-type (system view).....	1-4
1.1.5 qinq transparent-vlan.....	1-5

1 QinQ



说明

S5000E-X、S5110V2-SI 与 S5000V3-EI 系列交换机不支持 QinQ 功能。

文中用到如下两个概念：

内层 VLAN：为用户的私网 VLAN，也称为 Customer network VLAN（简称 CVLAN）；

外层 VLAN：为运营商分配给用户的公网 VLAN，也称为 Service provider network VLAN（简称 SVLAN）。

1.1 QinQ配置命令

1.1.1 display qinq

display qinq 命令用来显示使能了 QinQ 功能的端口。

【命令】

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

【视图】

任意视图

【缺省用户角色】

network-admin

network-operator

【参数】

interface interface-type interface-number：显示指定端口是否使能了 QinQ 功能。
interface-type interface-number 为端口类型和端口编号；如果未指定该参数，则显示所有使能 QinQ 功能的端口。

【使用指导】

如果端口都没有使能 QinQ 功能，则执行该命令后无显示内容。

【举例】

在端口 GigabitEthernet1/0/1 上使能 QinQ 功能，然后显示该端口是否使能了 QinQ 功能。

```
<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
```

在端口 GigabitEthernet1/0/1 和 GigabitEthernet1/0/3 上使能 QinQ 功能，然后显示所有使能了 QinQ 功能的端口。

```
<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
```

【相关命令】

- **qinq enable**

1.1.2 qinq enable

qinq enable 命令用来使能端口的 QinQ 功能。

undo qinq enable 命令用来关闭端口的 QinQ 功能。

【命令】

```
qinq enable
undo qinq enable
```

【缺省情况】

端口的 QinQ 功能处于关闭状态。

【视图】

二层以太网接口视图
二层聚合接口视图

【缺省用户角色】

network-admin

【举例】

在端口 GigabitEthernet1/0/1 上使能 QinQ 功能。

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

【相关命令】

- **display qinq**

1.1.3 qinq ethernet-type (interface view)

qinq ethernet-type 命令用来配置外层 VLAN Tag 的 TPID 值。

undo qinq ethernet-type 命令用来恢复外层 VLAN Tag 的 TPID 值为缺省值。

【命令】

```
qinq ethernet-type service-tag hex-value
undo qinq ethernet-type service-tag
```

【缺省情况】

外层 VLAN Tag 的 TPID 值为十六进制数 8100。

【视图】

二层以太网接口视图
二层聚合接口视图

【缺省用户角色】

network-admin

【参数】

service-tag: 表示配置外层 VLAN Tag 的 TPID 值。
hex-value: 表示协议类型值，取值范围为十六进制数 1~ffff，但不允许配置为 [表 1-1](#) 中列举的常用协议类型值。

表1-1 常用协议类型值

协议类型	协议类型值
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
集群	0x88a7
设备保留	0xfffd/0xfffe/0xffff

【使用指导】

没有使能 QinQ 的端口根据端口配置的外层 VLAN Tag 的 TPID 值判断入报文是否携带 VLAN Tag，并将出报文中外层 VLAN Tag 的 TPID 值修改为配置值。

【举例】

```
# 在端口 GigabitEthernet1/0/1 上配置外层 VLAN Tag 的 TPID 值为十六进制数 9100。
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] qinq ethernet-type service-tag 9100
```

【相关命令】

- **qinq ethernet-type** (system view)

1.1.4 qinq ethernet-type (system view)

qinq ethernet-type 命令用来配置内层 VLAN Tag 的 TPID 值。
undo qinq ethernet-type 命令用来恢复内层 VLAN Tag 的 TPID 值为缺省值。

【命令】

```
qinq ethernet-type customer-tag hex-value
undo qinq ethernet-type customer-tag
```

【缺省情况】

内层 VLAN Tag 的 TPID 值为十六进制数 8100。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

customer-tag: 表示配置内层 VLAN Tag 的 TPID 值。
hex-value: 表示协议类型值，取值范围为十六进制数 1~ffff，但不允许配置为 [表 1-2](#) 中列举的常用协议类型值。

表1-2 常用协议类型值

协议类型	协议类型值
ARP	0x0806
PUP	0x0200
RARP	0x8035
IP	0x0800
IPv6	0x86dd
PPPoE	0x8863/0x8864
MPLS	0x8847/0x8848
IPX/SPX	0x8137
IS-IS	0x8000
LACP	0x8809

协议类型	协议类型值
LLDP	0x88cc
802.1X	0x888e
802.1ag	0x8902
集群	0x88a7
设备保留	0xfffd/0xfffe/0xffff

【举例】

#配置内层 VLAN Tag 的 TPID 值为十六进制数 8200。

```
<Sysname> system-view
[Sysname] qinq ethernet-type customer-tag 8200
```

【相关命令】

- **qinq ethernet-type** (interface view)

1.1.5 qinq transparent-vlan

qinq transparent-vlan 命令用来配置端口的 VLAN 透传功能。

undo qinq transparent-vlan 命令用来取消端口对指定 VLAN 的报文进行透传的配置。

【命令】

```
qinq transparent-vlan vlan-id-list
undo qinq transparent-vlan { vlan-id-list | all }
```

【缺省情况】

未配置 VLAN 透传功能。

【视图】

二层以太网接口视图

二层聚合接口视图

【缺省用户角色】

network-admin

【参数】

vlan-id-list: VLAN 列表，表示一个或多个 VLAN，且这些 VLAN 必须是本地已创建好的。表示方式为 **vlan-id-list = { vlan-id1 [to vlan-id2] }<1-10>**。其中，**vlan-id1** 和 **vlan-id2** 为指定 VLAN 的编号，取值范围为 1~4094，**vlan-id2** 的值要大于或等于 **vlan-id1** 的值。<1-10>表示前面的参数最多可以输入 10 次。

all: 表示所有已创建的 VLAN。

【使用指导】

端口上使能了 QinQ 功能后，从该端口收到的报文就会被打上本端口缺省 VLAN 的 Tag。而 VLAN 透传功能则可使端口在收到带有指定 VLAN Tag 的报文后，不为其添加外层 VLAN Tag 而直接在运营商网络中传输。

多次执行本命令，指定 VLAN 的合集生效。

配置 VLAN 透传功能时，需要注意：

- 建议在配置用户侧端口的 VLAN 透传功能前，配置该端口的链路为 Trunk/Hybrid 类型，并允许透传 VLAN 通过。
- 配置了用户侧端口对指定 VLAN 的报文进行透传后，请勿在该端口上对这些 VLAN 再进行修改报文 VLAN Tag 的相关配置。
- 配置 VLAN 透传功能时，还需在报文传输路径的所有端口上都配置允许透传 VLAN 通过。
- 同一接口上同时配置 VLAN 透传和 VLAN 映射时：
 - 透传 VLAN 不能为 1:1 VLAN 映射、1:2 VLAN 映射的原始 VLAN 和转换后 VLAN。

【举例】

在端口 GigabitEthernet1/0/1 上使能 QinQ 功能，配置端口为 Trunk 类型，允许 VLAN 2、3、50～100 的报文通过，并对 VLAN 2 的报文进行透传。

```
<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 3 50 to 100
[Sysname-GigabitEthernet1/0/1] qinq enable
[Sysname-GigabitEthernet1/0/1] qinq transparent-vlan 2
```

目 录

1 VLAN映射	1-1
1.1 VLAN映射配置命令	1-1
1.1.1 display vlan mapping	1-1
1.1.2 vlan mapping	1-2

1 VLAN映射



说明

请不要在同一个二层以太网接口/二层聚合接口上同时配置 VLAN 映射功能、以太网服务实例与 VSI 的交叉连接关联，否则，可能导致这些功能不可用。

1.1 VLAN映射配置命令

1.1.1 display vlan mapping

display vlan mapping 命令用来显示 VLAN 映射信息。

【命令】

display vlan mapping [**interface** *interface-type interface-number*]

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator

【参数】

interface *interface-type interface-number*: 显示指定接口的 VLAN 映射信息，*interface-type interface-number* 为接口类型和接口编号。如果未指定该参数，将显示所有接口的 VLAN 映射信息。

【举例】

显示所有接口上的 VLAN 映射信息。

```
<Sysname> display vlan mapping
Interface GigabitEthernet1/0/1:
  Outer VLAN    Inner VLAN    Translated Outer VLAN    Translated Inner VLAN
  10            N/A          120                      N/A

Interface GigabitEthernet1/0/3:
  Outer VLAN    Inner VLAN    Translated Outer VLAN    Translated Inner VLAN
  12            N/A          110                      12
```

表1-1 display vlan mapping 命令显示信息描述表

字段	描述
Interface	接口信息

字段	描述
Outer VLAN	原始外层VLAN: <ul style="list-style-type: none"> 对于 1:1 VLAN 映射和 1:2 VLAN 映射, Outer VLAN 表示原始 VLAN
Inner VLAN	原始内层VLAN: <ul style="list-style-type: none"> 对于 1:1 VLAN 映射和 1:2 VLAN 映射, Inner VLAN 显示为 N/A
Translated Outer VLAN	转换后的外层VLAN: <ul style="list-style-type: none"> 对于 1:1 VLAN 映射, Translated Outer VLAN 表示转换后 VLAN 对于 1:2 VLAN 映射, Translated Outer VLAN 表示添加的外层 VLAN
Translated Inner VLAN	转换后的内层VLAN: <ul style="list-style-type: none"> 对于 1:1 VLAN 映射, Translated Inner VLAN 显示为 N/A

【相关命令】

- `vlan mapping`

1.1.2 vlan mapping

`vlan mapping` 命令用来在接口上配置 VLAN 映射。

`undo vlan mapping` 命令用来取消 VLAN 映射配置。

【命令】

```
vlan mapping { vlan-id translated-vlan vlan-id | nest { range vlan-range-list
| single vlan-id-list } nested-vlan vlan-id }
undo vlan mapping { vlan-id translated-vlan vlan-id | all | nest { range
vlan-range-list | single vlan-id-list } nested-vlan vlan-id }
```

【缺省情况】

接口上未配置 VLAN 映射。

【视图】

二层以太网接口视图

二层聚合接口视图

【缺省用户角色】

network-admin

【参数】

`vlan-id translated-vlan vlan-id`: 表示 1:1 VLAN 映射的原始 VLAN ID 和转换后的 VLAN ID。`vlan-id` 取值范围为 1~4094。原始 VLAN ID 和转换后的 VLAN ID 不允许相同。

`nest range vlan-range-list nested-vlan vlan-id`: 表示 1:2 VLAN 映射的原始 VLAN 段列表和添加的外层 VLAN ID。其中 `vlan-range-list = { vlan-id1 to vlan-id2 } &<1-10>`, `vlan-id2` 的值要大于 `vlan-id1` 的值, `&<1-10>` 表示前面的参数最多可以重复输入 10 次。参数涉及的 `vlan-id` 取值范围都为 1~4094。不同 VLAN 段之间不允许出现交叉重叠。

nest single vlan-id-list nested-vlan vlan-id: 表示 1:2 VLAN 映射的原始 VLAN ID 列表和添加的外层 VLAN ID。其中 **vlan-id-list = { vlan-id }&<1-10>**，&<1-10>表示前面的参数最多可以重复输入 10 次。参数涉及的 **vlan-id** 取值范围都为 1~4094。

all: 表示删除接口上所有的 VLAN 映射配置。

【使用指导】

VLAN 映射功能只对接口收到的携带 VLAN Tag 的报文生效。

配置 VLAN 映射时，对原始 VLAN 和转换后 VLAN 具有如下要求：

- 同一接口上不同类型 VLAN 映射表项的原始 VLAN 不允许相同，转换后 VLAN 也不允许相同。
- 同一接口上，多次配置 1:1 VLAN 映射，表项的转换后 VLAN 不允许和已有配置的转换后 VLAN 相同；多次配置 1:1 VLAN 映射且指定的原始 VLAN 相同时，最后一次执行的命令生效。

VLAN 映射功能和 QinQ 功能之间存在如下限制：

- 使能或关闭 QinQ 功能之前，要先清除已有的 VLAN 映射表项。

同一接口上同时配置 VLAN 透传和 VLAN 映射时：

- 透传 VLAN 不能为 1:1 VLAN 映射、1:2 VLAN 映射的原始 VLAN 和转换后 VLAN。

接口为报文添加外层 VLAN Tag 后，内层 VLAN Tag 将被当作报文的数据部分进行传输，报文长度将增加 4 个字节。因此，在携带两层 VLAN Tag 的报文的传输路径上，建议用户适当增加接口的 MTU（Maximum Transmission Unit，最大传输单元）值（至少为 1504 字节）。

【举例】

在接口 GigabitEthernet1/0/1 上配置 1:1 VLAN 映射：原始 VLAN 为 1，映射后 VLAN 为 101。

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

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

```
[Sysname-GigabitEthernet1/0/1] vlan mapping 1 translated-vlan 101
```

在接口 GigabitEthernet1/0/4 上配置 1:2 VLAN 映射：原始 VLAN 范围为 1~10、80，映射后添加的外层 VLAN 为 101。

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

```
[Sysname] interface gigabitethernet 1/0/4
```

```
[Sysname-GigabitEthernet1/0/4] vlan mapping nest range 1 to 10 nested-vlan 101
```

```
[Sysname-GigabitEthernet1/0/4] vlan mapping nest single 80 nested-vlan 101
```

【相关命令】

- **display vlan mapping**

目 录

1 LLDP	1-1
1.1 LLDP配置命令	1-1
1.1.1 cdp voice-vlan	1-1
1.1.2 display lldp local-information	1-1
1.1.3 display lldp neighbor-information	1-7
1.1.4 display lldp statistics	1-14
1.1.5 display lldp status	1-17
1.1.6 display lldp tlv-config	1-19
1.1.7 lldp admin-status	1-23
1.1.8 lldp check-change-interval	1-24
1.1.9 lldp compliance admin-status cdp	1-25
1.1.10 lldp compliance cdp	1-25
1.1.11 lldp enable	1-26
1.1.12 lldp encapsulation snap	1-27
1.1.13 lldp fast-count	1-28
1.1.14 lldp global enable	1-28
1.1.15 lldp global tlv-enable basic-tlv management-address-tlv	1-29
1.1.16 lldp hold-multiplier	1-30
1.1.17 lldp ignore-pvid-inconsistency	1-31
1.1.18 lldp management-address	1-32
1.1.19 lldp management-address-format string	1-32
1.1.20 lldp max-credit	1-33
1.1.21 lldp mode	1-34
1.1.22 lldp notification med-topology-change enable	1-35
1.1.23 lldp notification remote-change enable	1-35
1.1.24 lldp source-mac vlan	1-36
1.1.25 lldp timer fast-interval	1-37
1.1.26 lldp timer notification-interval	1-37
1.1.27 lldp timer reinit-delay	1-38
1.1.28 lldp timer tx-interval	1-39
1.1.29 lldp tlv-enable	1-39

1 LLDP

1.1 LLDP配置命令

1.1.1 cdp voice-vlan

cdp voice-vlan 命令用来配置 CDP 报文携带的 Voice VLAN ID。

undo cdp voice-vlan 命令用来恢复缺省情况。

【命令】

```
cdp voice-vlan vlan-id  
undo cdp voice-vlan
```

【缺省情况】

未配置 CDP 报文携带的 Voice VLAN ID。

【视图】

二层以太网接口视图

【缺省用户角色】

network-admin

【参数】

vlan-id: 要发布的 Voice VLAN ID，取值范围为 1～4094。

【使用指导】

配置本命令后，设备当前接口向对端 IP 电话发送的 CDP 报文携带的 Voice VLAN ID 为本命令配置的 VLAN ID。

对端 IP 电话收到本端发送的 CDP 报文后，会根据报文中携带的 Voice VLAN ID 发送语音数据。

S5000E-X、S5110V2-SI 和 S5000V3-EI 系列交换机不支持本命令。

【举例】

配置 CDP 报文携带的 Voice VLAN ID 为 100。

```
<Sysname> system-view  
[Sysname] interface gigabitethernet 1/0/1  
[Sysname-GigabitEthernet1/0/1] cdp voice-vlan 100
```

1.1.2 display lldp local-information

display lldp local-information 命令用来显示 LLDP 本地信息。

【命令】

```
display lldp local-information [ global | interface interface-type  
interface-number ]
```


【视图】

任意视图

【缺省用户角色】

network-admin
network-operator

【参数】

global: 显示全局 LLDP 本地信息。

interface interface-type interface-number: 显示指定接口上的 LLDP 本地信息，*interface-type interface-number* 表示接口类型和接口编号。

【使用指导】

如果未指定任何参数，将显示所有 LLDP 本地信息，包括全局 LLDP 信息以及所有开启了 LLDP 功能且状态为 up 的接口上的 LLDP 信息。

【举例】

显示所有 LLDP 本地信息。

```
<Sysname> display lldp local-information
Global LLDP local-information:
  Chassis ID          : 00e0-fc00-5600
  System name         : Sysname
H3C Comware Platform Software, Software Version 7.1.070, Feature 6123
  H3C S5120V2-10P-PWR-LI
  Copyright (c) 2004-2018 New H3C Technologies Co., Ltd. All rights reserved.
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               : 7.1.070 Feature 6123
SerialNum                 : NONE
Manufacturer name         : H3C
Model name                 : H3C S5120V2-10P-PWR-LI
Asset tracking identifier  : Unknown
LLDP local-information of port 52[GigabitEthernet1/0/3]:
Port ID type              : Interface name
Port ID                   : GigabitEthernet1/0/3
Port description          : GigabitEthernet1/0/3 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
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
Link aggregation supported : Yes
Link aggregation enabled   : Yes
Aggregation port ID       : 52
Auto-negotiation supported : Yes
Auto-negotiation enabled  : Yes
OperMau                   : Speed(1000)/Duplex(Full)
Power port class           : PSE
PSE power supported        : NO
PSE power enabled          : NO
PSE pairs control ability  : NO
Power pairs                : Signal
Port power classification  : Class 0
Power type                 : Type 2 PSE
Power source               : Primary
Power priority             : Unknown
PD requested power value   : 0.0 w
PSE allocated power value  : 0.0 w
Maximum frame size         : 10000
Transmit Tw                : 0 us
Receive Tw                 : 0 us
Fallback Tw                : 0 us
Echo Transmit Tw           : 0 us
Echo Receive Tw            : 0 us
PoE PSE power source       : Primary
Port PSE priority          : Critical
Port available power value : 0.0 w

```

表1-1 display lldp local-information 命令显示信息描述表

字段	描述
Global LLDP local-information	本设备的全局LLDP本地信息

字段	描述
Chassis ID	Chassis ID值，为本设备的桥MAC地址
System name	系统名称
System description	系统描述
System capabilities supported	<p>系统所支持的功能：</p> <ul style="list-style-type: none"> • Bridge: 表示支持交换功能 • Router: 表示支持路由功能 • Repeater: 表示支持信号中继功能 • Telephone: 表示支持电话功能 • DocsisCableDevice: 表示支持电缆设备功能 • StationOnly: 表示支持只作站点功能 • Customer Bridge: 表示支持客户桥功能 • Service Bridge: 表示支持服务桥功能 • TPMR: 表示支持双端口 MAC 中继功能 • Other: 表示支持不在上述列表的其它功能
System capabilities enabled	<p>系统已开启的功能：</p> <ul style="list-style-type: none"> • Bridge: 表示交换功能已开启 • Router: 表示路由功能已开启 • Repeater: 表示支持信号中继功能 • Telephone: 表示电话功能已开启 • DocsisCableDevice: 表示电缆设备功能已开启 • StationOnly: 表示只作站点功能已开启 • Customer Bridge: 表示客户桥功能已开启 • Service Bridge: 表示服务桥功能已开启 • TPMR: 表示双端口 MAC 中继功能已开启 • Other: 表示不在上述列表的其它功能已开启
MED information	MED设备相关信息
Device class	<p>MED设备类型：</p> <ul style="list-style-type: none"> • Connectivity device: 表示网络设备 • Class I: 表示一般终端设备，即所有需要 LLDP 发现服务的终端设备 • Class II: 表示媒体终端设备，即具备媒体能力的终端设备，其能力包含了一般终端设备的能力。该类设备支持媒体流 • Class III: 表示通讯终端设备，即直接支持目标用户 IP 通讯系统的终端设备，其能力包含了一般终端设备和媒体终端设备的所有能力。该类设备直接被目标用户所使用
MED inventory information of master board	MED资产信息
HardwareRev	产品的硬件版本
FirmwareRev	产品的固件版本

字段	描述
SoftwareRev	产品的软件版本
SerialNum	序列号
Manufacturer name	制造厂商
Model name	模块名称
Asset tracking identifier	资产跟踪ID
LLDP local-information of port 1	端口1上LLDP本地信息
Port ID type	端口ID类型： <ul style="list-style-type: none"> MAC address: 表示 MAC 地址 Interface name: 表示接口名称
Port ID	端口ID值，根据本设备的Port ID type取相应类型的值
Port description	端口描述
LLDP agent nearest-bridge management address	LLDP最近桥代理的管理地址
LLDP agent nearest-customer management address	LLDP最近客户桥代理的管理地址
LLDP agent nearest-nontpmr management address	LLDP最近非TPMR桥代理的管理地址
Management address type	管理地址类型
Management address	管理地址
Management address interface type	管理地址所在接口的编码方式
Management address interface ID	管理地址接口索引
Management address OID	管理地址对象标识符
Port VLAN ID(PVID)	端口VLAN ID
Port and protocol VLAN ID(PPVID)	端口协议VLAN ID
Port and protocol VLAN supported	是否支持端口协议VLAN
Port and protocol VLAN enabled	是否已开启端口协议VLAN
VLAN name of VLAN 12	VLAN 12的名称
Management VLAN ID	管理VLAN ID
Link aggregation supported	端口是否支持链路聚合
Link aggregation enabled	端口是否已开启链路聚合
Aggregation port ID	聚合组中该成员端口的编号，未开启链路聚合功能时为0
Auto-negotiation supported	端口是否支持自协商
Auto-negotiation enabled	端口是否已开启自协商
OperMau	端口自适应的速率和双工状态

字段	描述
Power port class	PoE类型： <ul style="list-style-type: none"> • PSE（Power Sourcing Equipment，供电设备） • PD（Powered Device，受电设备）
PSE power supported	是否支持PSE供电
PSE power enabled	是否已开启PSE供电
PSE pairs control ability	供电方式是否可控
Power pairs	PoE端口的远程供电模式： <ul style="list-style-type: none"> • Signal：表示信号线供电模式 • Spare：表示空闲线供电模式
Port power classification	PD的端口控制级别： <ul style="list-style-type: none"> • Class 0：表示级别 0 • Class 1：表示级别 1 • Class 2：表示级别 2 • Class 3：表示级别 3 • Class 4：表示级别 4
Power type	供电类型： <ul style="list-style-type: none"> • Type 1 PD：表示类型 1 PD • Type 2 PD：表示类型 2 PD • Type 1 PSE：表示类型 1 PSE • Type 2 PSE：表示类型 2 PSE
Power source	功率来源（功率来源根据供电类型为PD类型或PSE类型，取值不同）： <p>PSE</p> <ul style="list-style-type: none"> • Unknown：表示采用的电源类型未知 • Primary：表示采用主用电源作为电源 • Backup：表示采用备用电源作为电源 • Reserved：保留 <p>PD</p> <ul style="list-style-type: none"> • Unknown：表示采用的电源类型未知 • PSE：表示采用 PSE 作为电源 • Local：表示采用本地电源作为电源 <p>PSE and local：表示采用PSE和本地电源作为电源</p>
Power priority	功率优先级： <ul style="list-style-type: none"> • Unknown：表示优先级未知 • Critical：表示优先级为 1 级 • High：表示优先级为 2 级 • Low：表示优先级为 3 级
PD requested power value	PD请求功率值，单位为瓦特

字段	描述
PSE allocated power value	PSE分配功率值，单位为瓦特
Maximum frame size	端口支持的最大帧长度
PoE PSE power source	PSE所采用的电源类型： <ul style="list-style-type: none"> Unknown：表示采用的电源类型未知 Primary：表示采用主用电源作为电源 Backup：表示采用备用电源作为电源
PoE PD power source	PD所采用的电源类型： <ul style="list-style-type: none"> Unknown：表示采用的电源类型未知 PSE：表示采用 PSE 作为电源 Local：表示采用本地电源作为电源 PSE and local：表示采用 PSE 和本地电源作为电源
Port PSE priority	PSE上端口的供电优先级： <ul style="list-style-type: none"> Unknown：表示优先级未知 Critical：表示优先级为 1 级 High：表示优先级为 2 级 Low：表示优先级为 3 级
Port PD priority	PD上端口的受电优先级： <ul style="list-style-type: none"> Unknown：表示优先级未知 Critical：表示优先级为 1 级 High：表示优先级为 2 级 Low：表示优先级为 3 级
Port available power value	PSE上端口可提供的功率，或PD上端口所需的功率，单位为瓦特
Transmit Tw	本端发送的等待时间，单位为微秒
Receive Tw	本端向对端请求的等待时间，单位为微秒
Fallback Tw	本端向对端请求的候选等待时间，单位为微秒
Echo Transmit Tw	收到的对端发送的等待时间，单位为微秒
Echo Receive Tw	收到的对端请求的等待时间，单位为微秒

1.1.3 display lldp neighbor-information

display lldp neighbor-information 命令用来显示由邻居设备发来的 LLDP 信息。

【命令】

```
display lldp neighbor-information [ [ [ interface interface-type
interface-number ] [ agent { nearest-bridge | nearest-customer |
nearest-nontpmr } ] [ verbose ] ] | list [ system-name system-name ] ]
```

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator

【参数】

interface *interface-type interface-number*: 显示指定接口收到的由邻居设备发来的 LLDP 信息, *interface-type interface-number* 表示接口类型和接口编号。如果未指定该参数, 将显示所有接口收到的由邻居设备发来的 LLDP 信息。

agent: 显示指定类型 LLDP 代理收到的由邻居设备发来的 LLDP 信息。如果未指定该参数, 将显示所有类型 LLDP 代理收到的由邻居设备发来的 LLDP 信息。

nearest-bridge: 表示最近桥代理。

nearest-customer: 表示最近客户桥代理。

nearest-nontpmr: 表示最近非 TPMR 桥代理。

verbose: 显示由邻居设备发来的 LLDP 详细信息。如果未指定该参数, 将显示由邻居设备发来的 LLDP 概要信息。

list: 按列表显示由邻居设备发来的 LLDP 信息。

system-name *system-name*: 按列表显示由指定邻居设备发来的 LLDP 信息。*system-name* 表示邻居设备的系统名称, 为 1~255 个字符的字符串。如果未指定该参数, 将按列表显示由所有邻居设备发来的 LLDP 信息。

【举例】

显示所有接口最近桥代理收到的由邻居设备发来的 LLDP 详细信息。

```
<Sysname> display lldp neighbor-information agent nearest-bridge verbose
LLDP neighbor-information of port 1[GigabitEthernet1/0/1]:
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             : GigabitEthernet1/0/1
  Time to live        : 121
  Port description    : GigabitEthernet1/0/1 Interface
  System name         : Sysname
H3C Comware Platform Software, Software Version 7.1.070, Feature 6123
  H3C S5120V2-10P-PWR-LI
  Copyright (c) 2004-2018 New H3C Technologies Co., Ltd. All rights reserved.
  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
Link aggregation supported : Yes
Link aggregation enabled    : Yes
Aggregation port ID        : 52
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 PSE
Power source               : Primary
Power priority             : Unknown
PD requested power value   : 0.0 w
PSE allocated power value  : 0.0 w
Maximum frame size        : 9216

```

显示所有接口所有类型 LLDP 代理收到的由邻居设备发来的 LLDP 概要信息。

```

<Sysname> display lldp neighbor-information
LLDP neighbor-information of port 52[GigabitEthernet1/0/3]:
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[GigabitEthernet1/0/3]:
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            : GigabitEthernet1/0/4

LLDP neighbor-information of port 52[GigabitEthernet1/0/3]:
LLDP agent nearest-nontpmr:

```



```

LLDP neighbor index : 6
ChassisID/subtype   : 0011-2233-4400/MAC address
PortID/subtype      : 000c-29f5-c715/MAC address
Capabilities         : None

```

按列表显示类型 LLDP 代理所有邻居设备发来的 LLDP 信息。（适用于 Release 6126P09 版本）

```

<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          GE1/0/1         000f-e25d-ee91  GigabitEthernet1/0/1

```

按列表显示类型 LLDP 代理所有邻居设备发来的 LLDP 信息。（适用于 Release 6126P12 及以上版本）

```

<Sysname> display lldp neighbor-information list
Chassis ID : * -- --Nearest nontpmr bridge neighbor
              # -- --Nearest customer bridge neighbor
              Default -- -- Nearest bridge neighbor

Local Interface  Chassis ID      Port ID          System Name
GE1/0/1          000f-e25d-ee91  GigabitEthernet1/0/1  System1

```

表1-2 display lldp neighbor-information 命令显示信息描述表

字段	描述
LLDP agent nearest-bridge	LLDP缺省代理，即最近桥代理
LLDP agent nearest-customer	LLDP最近客户桥代理
LLDP agent nearest-nontpmr	LLDP最近非TPMR桥代理
LLDP neighbor-information of port 1	端口1上收到的LLDP邻居信息
LLDP Neighbor index	邻居索引
Update time	邻居信息最新更新时间
Chassis type	Chassis ID类型： <ul style="list-style-type: none"> Chassis component：表示底架组件 Interface alias：表示接口别名 Port component：表示端口组件 MAC address：表示 MAC 地址 Network address(ipv4)：表示网络地址（括号里表示地址类型） Interface name：表示接口名称 Locally assigned：表示邻居自定义
Chassis ID	Chassis ID值，根据邻居设备的Chassis type取相应类型的值

字段	描述
Port ID type	端口ID类型： <ul style="list-style-type: none"> • Interface alias: 表示接口别名 • Port component: 表示端口组件 • MAC address: 表示 MAC 地址 • Network Address(ipv4): 表示网络地址（括号里表示地址类型） • Interface name: 表示接口名称 • Agent circuit ID: 表示代理巡回标识 • Locally assigned: 表示邻居自定义
Port ID	端口ID值，根据邻居设备的Port ID type取相应类型的值
Time to live	邻居信息在本地的存活时间
Port description	端口描述
System name	系统名称
System description	系统描述
System capabilities supported	系统所支持的功能： <ul style="list-style-type: none"> • Repeater: 表示支持信号中继功能 • Bridge: 表示支持交换功能 • Router: 表示支持路由功能 • Telephone: 表示支持电话功能 • DocsisCableDevice: 表示支持电缆设备功能 • StationOnly: 表示支持只作站点功能 • Customer Bridge: 表示支持客户桥功能 • Service Bridge: 表示支持服务桥功能 • TPMR: 表示支持双端口 MAC 中继功能 • Other: 表示支持不在上述列表的其它功能
System capabilities enabled	系统已开启的功能： <ul style="list-style-type: none"> • Repeater: 表示信号中继功能已开启 • Bridge: 表示交换功能已开启 • Router: 表示路由功能已开启 • Telephone: 表示电话功能已开启 • DocsisCableDevice: 表示电缆设备功能已开启 • StationOnly: 表示只作站点功能已开启 • Customer Bridge: 表示支持客户桥功能 • Service Bridge: 表示支持服务桥功能 • TPMR: 表示支持双端口 MAC 中继功能 • Other: 表示不在上述列表的其它功能已开启
Management address type	管理地址类型
Management address	管理地址

字段	描述
Management address interface type	管理地址接口类型
Management address interface ID	管理地址接口索引
Management address OID	管理地址对象标识符
Port VLAN ID	端口VLAN ID
Link aggregation supported	端口是否支持链路聚合
Link aggregation enabled	端口是否已开启链路聚合
Aggregation port ID	聚合组中该成员端口的编号，未开启链路聚合功能时为0
Management VLAN ID	管理VLAN ID
Auto-negotiation supported	端口是否支持自协商
Auto-negotiation enabled	端口是否已开启自协商
OperMau	端口自适应的速率和双工状态
Power port class	PoE类型： <ul style="list-style-type: none"> • PSE：表示供电设备 • PD：表示受电设备
PSE power supported	是否支持PSE供电
PSE power enabled	是否已开启PSE供电
PSE pairs control ability	供电方式是否可控
Power pairs	PoE端口的远程供电模式： <ul style="list-style-type: none"> • Signal：表示信号线供电模式 • Spare：表示空闲线供电模式
Port power classification	PD的端口控制级别： <ul style="list-style-type: none"> • Class 0：表示级别 0 • Class 1：表示级别 1 • Class 2：表示级别 2 • Class 3：表示级别 3 • Class 4：表示级别 4
Power type	供电类型： <ul style="list-style-type: none"> • Type 1 PD：表示类型 1 PD • Type 2 PD：表示类型 2 PD • Type 1 PSE：表示类型 1 PSE • Type 2 PSE：表示类型 2 PSE

字段	描述
Power source	<p>功率来源（功率来源根据供电类型为PD类型或PSE类型，取值不同）：</p> <p>PSE</p> <ul style="list-style-type: none"> Unknown: 表示采用的电源类型未知 Primary: 表示采用主用电源作为电源 Backup: 表示采用备用电源作为电源 Reserved: 保留 <p>PD</p> <ul style="list-style-type: none"> Unknown: 表示采用的电源类型未知 PSE: 表示采用 PSE 作为电源 Local: 表示采用本地电源作为电源 <p>PSE and local: 表示采用PSE和本地电源作为电源</p>
Power priority	<p>功率优先级：</p> <ul style="list-style-type: none"> Unknown: 表示优先级未知 Critical: 表示优先级为 1 级 High: 表示优先级为 2 级 <p>Low: 表示优先级为3级</p>
PD requested power value	PD请求功率值，单位为瓦特
PSE allocated power value	PSE分配功率值，单位为瓦特
Maximum frame size	端口支持的最大帧长度
Unknown basic TLV	未知的基本TLV
TLV type	未知的基本TLV类型
TLV information	未知的基本TLV的具体信息
Unknown organizationally-defined TLV	未知组织定义TLV
TLV OUI	未知组织定义TLV的对象唯一标识
TLV subtype	未知的组织定义TLV类型
Index	未知组织的索引
CDP neighbor-information of port 1	端口1的CDP邻居信息
CDP neighbor index	CDP邻居索引
Chassis ID/subtype	Chassis ID值及Chassis ID类型
Port ID/subtype	Port ID值及PortID类型
Software version	邻居软件版本
Platform version	邻居平台版本
Duplex	双工状态

字段	描述
Capabilities	<p>系统已开启的功能：</p> <ul style="list-style-type: none"> • Repeater: 表示开启信号中继功能 • Bridge: 表示开启交换功能 • Router: 表示开启路由功能 • Telephone: 表示开启电话功能 • DocsisCableDevice: 表示开启电缆设备功能 • StationOnly: 表示开启只作站点功能，与其他功能不能同时出现 • Other: 表示开启不在上述列表的其他功能 • None: 表示该邻居未发布该 TLV
Local Interface	接收LLDP信息的本端端口
Chassis ID : * -- -- Nearest nontpmr bridge neighbor #-- -- Nearest customer bridge neighbor	<p>*符号: 表示该邻居是最近非TPMR桥代理类型邻居</p> <p>#符号: 表示该邻居是最近客户桥代理类型邻居</p>

1.1.4 display lldp statistics

display lldp statistics 命令用来显示 LLDP 的统计信息。

【命令】

```
display lldp statistics [ global | [ interface interface-type  
interface-number ] [ agent { nearest-bridge | nearest-customer |  
nearest-nontpmr } ] ]
```

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator

【参数】

global: 显示全局 LLDP 统计信息。

interface interface-type interface-number: 显示指定接口上的 LLDP 统计信息，
interface-type interface-number 表示接口类型和接口编号。

agent: 显示指定类型 LLDP 代理的统计信息。如果未指定该参数，将显示所有类型 LLDP 代理的统计信息。

nearest-bridge: 表示最近桥代理。

nearest-customer: 表示最近客户桥代理。

nearest-nontpmr: 表示最近非 TPMR 桥代理。

【使用指导】

如果未指定任何参数，将同时显示全局和接口上的 LLDP 统计信息。

【举例】

显示全局和接口上的 LLDP 统计信息。

```
<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 [GigabitEthernet1/0/1]:
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-nontpmr:
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

```

显示接口 GigabitEthernet1/0/1 的最近客户桥代理上的 LLDP 统计信息。

```

<Sysname> display lldp statistics interface gigabitethernet 1/0/1 agent nearest-customer
LLDP statistics information of port 1 [GigabitEthernet1/0/1]:
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

```

表1-3 display lldp statistics 命令显示信息描述表

字段	描述
LLDP agent nearest-bridge	LLDP缺省代理，即最近桥代理
LLDP agent nearest-customer	LLDP最近客户桥代理
LLDP agent nearest-nontpmr	LLDP最近非TPMR桥代理
LLDP statistics global information	全局LLDP统计信息
LLDP neighbor information last change time	邻居信息的最后更新时间
The number of LLDP neighbor information inserted	邻居信息的增加次数
The number of LLDP neighbor information deleted	邻居信息的删除次数
The number of LLDP neighbor information dropped	由于空间不足而导致丢弃邻居信息的次数
The number of LLDP neighbor information aged out	邻居信息的老化数量
LLDP statistics Information of port 1	端口1上的LLDP统计信息
The number of LLDP frames transmitted	发送的LLDP帧总数
The number of LLDP frames received	收到的LLDP帧总数
The number of LLDP frames discarded	丢弃的LLDP帧总数
The number of LLDP error frames	收到的错误LLDP帧总数
The number of LLDP TLVs discarded	丢弃的LLDP TLV总数
The number of LLDP TLVs unrecognized	不可识别的LLDP TLV总数
The number of LLDP neighbor information aged out	老化的LLDP邻居信息总数
The number of CDP frames transmitted	发送的CDP帧总数

字段	描述
The number of CDP frames received	收到的CDP帧总数
The number of CDP frames discarded	丢弃的CDP帧总数
The number of CDP error frames	收到的错误CDP帧总数

1.1.5 display lldp status

display lldp status 命令用来显示 LLDP 的状态信息。

【命令】

```
display lldp status [ interface interface-type interface-number ] [ agent
{ nearest-bridge | nearest-customer | nearest-nontpmr } ]
```

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator

【参数】

interface *interface-type interface-number*: 显示指定接口上的 LLDP 状态信息，*interface-type interface-number* 表示接口类型和接口编号。如果未指定该参数，将显示所有开启了 LLDP 功能的接口上的 LLDP 状态信息。

agent: 显示指定类型 LLDP 代理的状态信息。如果未指定该参数，将显示所有类型 LLDP 代理的状态信息。

nearest-bridge: 表示最近桥代理。

nearest-customer: 表示最近客户桥代理。

nearest-nontpmr: 表示最近非 TPMR 桥代理。

【举例】

显示全局和所有接口上的 LLDP 状态信息。

```
<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 [GigabitEthernet1/0/1]:
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
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-customer:
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

```

表1-4 display lldp status 命令显示信息描述表

字段	描述
Bridge mode of LLDP	LLDP桥模式: <ul style="list-style-type: none"> service-bridge: 表示服务桥模式 customer-bridge: 表示客户桥模式
LLDP agent nearest-bridge	LLDP缺省代理, 即最近桥代理
LLDP agent nearest-customer	LLDP最近客户桥代理

字段	描述
LLDP agent nearest-nontpmr	LLDP最近非TPMR桥代理
Global status of LLDP	LLDP功能是否已全局开启
The current number of LLDP neighbors	当前设备的LLDP邻居总数
The current number of CDP neighbors	当前设备的CDP邻居总数
LLDP neighbor information last changed time	邻居信息的最后更新时间
Transmit interval	LLDP报文的发送间隔
Hold multiplier	TTL乘数
Reinit delay	端口初始化延迟时间
Transmit max credit	LLDP报文发包限速令牌桶的最大值
Trap interval	Trap信息的发送间隔
Fast start times	快速发送LLDP报文的个数
LLDP status information of port 1	端口1上的LLDP状态信息
Port status of LLDP	LLDP功能是否已在端口上开启
Admin status	端口LLDP工作模式： <ul style="list-style-type: none"> • TX_RX: 表示既发送也接收 LLDP 报文 • Rx_Only: 表示只接收不发送 LLDP 报文 • Tx_Only: 表示只发送不接收 LLDP 报文 • Disable: 表示既不发送也不接收 LLDP 报文
Trap Flag	LLDP Trap功能是否已开启
MED trap flag	LLDP-MED Trap功能是否已开启
Polling interval	轮询间隔，0表示轮询功能处于关闭状态
Number of neighbors	端口LLDP邻居数量
Number of MED neighbors	端口MED邻居设备的数量
Number of CDP neighbors	端口CDP邻居设备的数量
Number of sent optional TLV	端口在一个LLDP报文中发送的可选TLV总数
Number of received unknown TLV	端口在所有LLDP报文中收到的不能识别的TLV总数

1.1.6 display lldp tlv-config

display lldp tlv-config 命令用来显示接口上可发送的可选 TLV 信息。

【命令】

```
display lldp tlv-config [ interface interface-type interface-number ]
[ agent { nearest-bridge | nearest-customer | nearest-nontpmr } ]
```

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator

【参数】

interface interface-type interface-number: 显示指定接口上可发送的可选 TLV 信息，*interface-type interface-number* 表示接口类型和接口编号。如果未指定该参数，将显示所有接口上可发送的可选 TLV 信息。

agent: 显示指定类型 LLDP 代理的可选 TLV 信息。如果未指定该参数，将显示所有类型 LLDP 代理的可选 TLV 信息。

nearest-bridge: 表示最近桥代理。

nearest-customer: 表示最近客户桥代理。

nearest-nontpmr: 表示最近非 TPMR 桥代理。

【举例】

显示接口 GigabitEthernet1/0/1 上可发送的可选 TLV 信息。

```
<Sysname> display lldp tlv-config interface gigabitethernet 1/0/1
LLDP tlv-config of port 1[GigabitEthernet1/0/1]:
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
DCBX TLV                           NO        NO
EVB TLV                            NO        NO
Link Aggregation TLV               YES       YES
Management VID 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
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
DCBX TLV	NO	NO
EVB TLV	YES	YES
Link Aggregation TLV	YES	NO
Management VID TLV	NO	NO
IEEE 802.3 extend TLV:		
MAC-Physic TLV	YES	NO
Power via MDI TLV	YES	NO
Maximum Frame Size TLV	YES	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 802.1 extend TLV:		
Port VLAN ID TLV	YES	YES
Port And Protocol VLAN ID TLV	YES	YES
VLAN Name TLV	YES	YES
DCBX TLV	NO	NO
EVB TLV	NO	NO
Link Aggregation TLV	YES	NO
Management VID 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

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

表1-5 display lldp tlv-config 命令显示信息描述表

字段	描述
LLDP agent nearest-bridge	LLDP 缺省代理，即最近桥代理
LLDP agent nearest-customer	LLDP最近客户桥代理
LLDP agent nearest-nontpmr	LLDP最近非TPMR桥代理
LLDP tlv-config of port 1	端口1上可发送的可选TLV类型
NAME	TLV类型
STATUS	端口是否配置发布指定类型TLV
DEFAULT	端口发布指定类型TLV的缺省情况
Basic optional TLV	端口可以发送的基本TLV类型
Port Description TLV	端口描述TLV
System Name TLV	系统名称TLV
System Description TLV	系统描述TLV
System Capabilities TLV	系统能力集TLV
Management Address TLV	管理地址TLV
IEEE 802.1 extended TLV	端口可发送的IEEE 802.1组织定义的TLV类型
Port VLAN ID TLV	端口VLAN ID TLV
Port And Protocol VLAN ID TLV	协议VLAN ID TLV
VLAN Name TLV	VLAN名称TLV
DCBX TLV	（暂不支持）DCBX（Data Center Bridging Exchange Protocol，数据中心桥能力交换协议）TLV
EVB TLV	（暂不支持）EVB（Edge Virtual Bridging，边缘虚拟桥接）模块TLV
Management VID TLV	管理VLAN TLV
IEEE 802.3 extended TLV	端口可发送的IEEE 802.3组织定义的TLV类型
MAC-Physic TLV	端口物理属性TLV
Power via MDI TLV	供电能力TLV
Link Aggregation TLV	链路聚合TLV
Maximum Frame Size TLV	最大帧长度TLV
LLDP-MED extend TLV	LLDP-MED TLV
Capabilities TLV	MED能力集TLV

字段	描述
Network Policy TLV	网络策略TLV
Location Identification TLV	位置标识TLV
Extended Power via MDI TLV	扩展供电能力TLV
Inventory TLV	资产信息TLV，包括以下几种： <ul style="list-style-type: none"> • Hardware Revision TLV：终端设备硬件版本 • Firmware Revision TLV：终端设备固件版本 • Software Revision TLV：终端设备软件版本 • Serial Number TLV：终端设备序列号 • Manufacturer Name TLV：终端设备的制造厂商名称 • Model name TLV：终端设备的模块名称 • Asset ID TLV：终端设备的资产标识符，以便目录管理和资产跟踪

1.1.7 lldp admin-status

lldp admin-status 命令用来配置 LLDP 的工作模式。

undo lldp admin-status 命令用来恢复缺省情况。

【命令】

在二层以太网接口视图下：

```
lldp [ agent { nearest-customer | nearest-nontpmr } ] admin-status { disable
| rx | tx | txrx }
```

```
undo lldp [ agent { nearest-customer | nearest-nontpmr } ] admin-status
```

在二层聚合接口视图下：

```
lldp agent { nearest-customer | nearest-nontpmr } admin-status { disable |
rx | tx | txrx }
```

```
undo lldp agent { nearest-customer | nearest-nontpmr } admin-status
```

【缺省情况】

LLDP 最近桥代理的工作模式为 TxRx，既发送也接收 LLDP 报文。其他类型的 LLDP 代理的工作模式为 Disable，即不发送也不接收 LLDP 报文。

【视图】

二层以太网接口视图

二层聚合接口视图

【缺省用户角色】

network-admin

【参数】

agent：配置指定类型 LLDP 代理的工作模式。在以太网接口视图下，未指定时表示配置最近桥代理的工作模式。

nearest-customer: 表示最近客户桥代理。

nearest-nontpmr: 表示最近非 TPMR 桥代理。

disable: 表示工作模式为 Disable，既不发送也不接收 LLDP 报文。

rx: 表示工作模式为 Rx，只接收不发送 LLDP 报文。

tx: 表示工作模式为 Tx，只发送不接收 LLDP 报文。

txrx: 表示工作模式为 TxRx，既发送也接收 LLDP 报文。

【举例】

配置接口 GigabitEthernet1/0/1 上最近客户桥代理 LLDP 的工作模式为 Rx。

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] lldp agent nearest-customer admin-status rx
```

1.1.8 lldp check-change-interval

lldp check-change-interval 命令用来开启轮询功能并配置轮询间隔。

undo lldp check-change-interval 命令用来关闭轮询功能。

【命令】

在二层以太网接口视图下：

```
lldp [ agent { nearest-customer | nearest-nontpmr } ] check-change-interval
interval
```

```
undo lldp [ agent { nearest-customer | nearest-nontpmr } ]
check-change-interval
```

在二层聚合接口视图下：

```
lldp agent { nearest-customer | nearest-nontpmr } check-change-interval
interval
```

```
undo lldp agent { nearest-customer | nearest-nontpmr }
check-change-interval
```

【缺省情况】

轮询功能处于关闭状态。

【视图】

二层以太网接口视图

二层聚合接口视图

【缺省用户角色】

network-admin

【参数】

agent: 配置指定类型 LLDP 代理的轮询功能。在以太网接口视图下，未指定时表示配置最近桥代理的轮询功能。

nearest-customer: 表示最近客户桥代理。

nearest-nontpmr: 表示最近非 TPMR 桥代理。

interval: 表示轮询间隔, 取值范围为 1~30, 单位为秒。

【举例】

在接口 GigabitEthernet1/0/1 的最近客户桥代理上开启轮询功能, 并配置轮询间隔为 30 秒。

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] lldp agent nearest-customer check-change-interval 30
```

1.1.9 lldp compliance admin-status cdp

lldp compliance admin-status cdp 命令用来配置 LLDP 兼容 CDP 功能的工作模式。

undo lldp compliance admin-status cdp 命令用来恢复缺省情况。

【命令】

```
lldp compliance admin-status cdp { disable | rx | txrx }
undo lldp compliance admin-status cdp
```

【缺省情况】

LLDP 兼容 CDP 功能的工作模式为 Disable, 既不发送也不接收 CDP 报文。

【视图】

二层以太网接口视图

【缺省用户角色】

network-admin

【参数】

disable: 表示工作模式为 Disable, 既不发送也不接收 CDP 报文。

txrx: 表示工作模式为 TxRx, 既发送也接收 CDP 报文。

rx: 表示工作模式为 Rx, 接收但不发送 CDP 报文。

【使用指导】

欲使 LLDP 兼容 CDP 的功能生效, 必须先开启 LLDP 兼容 CDP 功能, 同时将 LLDP 兼容 CDP 功能的工作模式配置为 TxRx。

【举例】

开启 LLDP 兼容 CDP 功能, 并在接口 GigabitEthernet1/0/1 上配置 LLDP 兼容 CDP 功能的工作模式为 TxRx。

```
<Sysname> system-view
[Sysname] lldp compliance cdp
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] lldp compliance admin-status cdp txrx
```

【相关命令】

- **lldp compliance cdp**

1.1.10 lldp compliance cdp

lldp compliance cdp 命令用来开启 LLDP 兼容 CDP 功能。

`undo lldp compliance cdp` 命令用来关闭 LLDP 兼容 CDP 功能。

【命令】

```
lldp compliance cdp
undo lldp compliance cdp
```

【缺省情况】

LLDP 兼容 CDP 功能处于关闭状态。

【视图】

系统视图

【缺省用户角色】

network-admin

【使用指导】

由于 CDP 报文所携 Time To Live TLV 中 TTL 的最大值为 255，而 CDP 报文的发送间隔由 LLDP 报文的发送间隔控制，因此为保证 LLDP 兼容 CDP 功能的正常运行，建议配置 LLDP 报文的发送间隔值不大于实际 TTL 的 1/3。

【举例】

```
# 开启 LLDP 兼容 CDP 功能。
<Sysname> system-view
[Sysname] lldp compliance cdp
```

【相关命令】

- `lldp hold-multiplier`
- `lldp timer tx-interval`

1.1.11 lldp enable

`lldp enable` 命令用来在接口上开启 LLDP 功能。

`undo lldp enable` 命令用来在接口上关闭 LLDP 功能。

【命令】

```
lldp enable
undo lldp enable
```

【缺省情况】

接口上的 LLDP 功能处于开启状态。

【视图】

二层以太网接口视图
二层聚合接口视图

【缺省用户角色】

network-admin

【使用指导】

只有当全局和接口上都开启了 LLDP 功能后，该功能才会生效。

在聚合接口视图下，开启或关闭 LLDP 功能只对 LLDP 最近客户桥代理和 LLDP 最近非 TPMR 代理生效。不影响聚合组中成员端口的 LLDP 最近桥代理的状态。

【举例】

在接口 GigabitEthernet1/0/1 上关闭 LLDP 功能。

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

【相关命令】

- **lldp global enable**

1.1.12 lldp encapsulation snap

lldp encapsulation snap 命令用来配置 LLDP 报文的封装格式为 SNAP 格式。

undo lldp encapsulation 命令用来恢复缺省情况。

【命令】

在二层以太网接口视图下：

```
lldp [ agent { nearest-customer | nearest-nontpmr } ] encapsulation snap
undo lldp [ agent { nearest-customer | nearest-nontpmr } ] encapsulation
```

在二层聚合接口视图下：

```
lldp agent { nearest-customer | nearest-nontpmr } encapsulation snap
undo lldp agent { nearest-customer | nearest-nontpmr } encapsulation
```

【缺省情况】

LLDP 报文的封装格式为 Ethernet II 格式。

【视图】

二层以太网接口视图

二层聚合接口视图

【缺省用户角色】

network-admin

【参数】

agent：配置指定类型 LLDP 代理的封装格式。在以太网接口视图下，未指定时表示配置最近桥代理的封装格式。

nearest-customer：表示最近客户桥代理。

nearest-nontpmr：表示最近非 TPMR 桥代理。

【使用指导】

LLDP CDP 报文的封装格式只能为 SNAP 格式，不能为 Ethernet II 格式。

【举例】

配置接口 GigabitEthernet1/0/1 上发送的 LLDP 报文的封装格式为 SNAP 格式。

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] lldp encapsulation snap
```

1.1.13 lldp fast-count

lldp fast-count 命令用来配置快速发送 LLDP 报文的个数。

undo lldp fast-count 命令用来恢复缺省情况。

【命令】

```
lldp fast-count count
undo lldp fast-count
```

【缺省情况】

快速发送 LLDP 报文的个数为 4 个。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

count：表示快速发送 LLDP 报文的个数，取值范围为 1~8。

【举例】

配置快速发送 LLDP 报文的个数为 5 个。

```
<Sysname> system-view
[Sysname] lldp fast-count 5
```

1.1.14 lldp global enable

lldp global enable 命令用来全局开启 LLDP 功能。

undo lldp global enable 命令用来全局关闭 LLDP 功能。

【命令】

```
lldp global enable
undo lldp global enable
```

【缺省情况】

对于 S5000V3-EI、S5000E-X 系列交换机，缺省情况下，全局 LLDP 功能处于关闭状态。

对于其他系列交换机：

- 空配置启动时，使用软件功能缺省值，LLDP 功能在全局处于关闭状态。
- 缺省配置启动时，使用软件功能出厂值，LLDP 功能在全局处于开启状态。

关于空配置启动和缺省配置启动的详细介绍，请参见“基础配置指导”中的“配置文件管理”。

【视图】

系统视图

【缺省用户角色】

network-admin

【使用指导】

只有当全局和接口上都开启了 LLDP 功能后，该功能才会生效。

【举例】

全局关闭 LLDP 功能。

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

```
[Sysname] undo lldp global enable
```

【相关命令】

- **lldp enable**

1.1.15 lldp global tlv-enable basic-tlv management-address-tlv

lldp global tlv-enable basic-tlv management-address-tlv 命令用来配置全局允许在 LLDP 报文中发布管理地址并配置所发布的管理地址。

undo lldp global tlv-enable basic-tlv management-address-tlv 命令用来恢复缺省情况。

【命令】

```
lldp [ agent { nearest-customer | nearest-nontpmr } ] global tlv-enable  
basic-tlv management-address-tlv [ ipv6 ] { ip-address | interface loopback  
interface-number | interface vlan-interface interface-number }
```

```
undo lldp [ agent { nearest-customer | nearest-nontpmr } ] global tlv-enable  
basic-tlv management-address-tlv
```

【缺省情况】

全局不允许在 LLDP 报文中发布管理地址 TLV。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

agent: 配置指定类型 LLDP 代理允许发布的 TLV 类型。未指定本参数时，表示配置最近桥代理允许发布的 TLV 类型。

nearest-customer: 表示最近客户桥代理。

nearest-nontpmr: 表示最近非 TPMR 桥代理。

ipv6: 表示 LLDP 报文中所要发布的管理地址为 IPv6 格式的地址，当未指定本参数时，表示 LLDP 报文中所要发布的管理地址为 IPv4 格式的地址。

ip-address: 表示在 LLDP 报文中发布的管理地址为指定的 IP 地址。

interface loopback *interface-number*: 表示在 LLDP 报文中发布的管理地址为指定的 LoopBack 接口的 IP 地址。*interface-number* 表示 LoopBack 接口的编号取值范围为 0~127。

interface vlan-interface *interface-number*: 表示在 LLDP 报文中发布的管理地址为指定的 VLAN 接口的 IP 地址。*interface-number* 表示 VLAN 接口的编号,取值范围为 1~4094。

【使用指导】

多次执行本命令, 最后一次执行的命令生效。

允许发布的管理地址 TLV 支持全局配置或在接口上配置两种方式: 全局的配置对所有接口都有效, 而接口上的配置只对当接口有效。对于一个接口来说, 优先采用该接口上的配置, 只有该接口上未进行配置时, 才采用全局的配置。当全局和接口下都未配置时, 会采用接口下的缺省配置。

在满足如下条件的情况下, 系统会将当前发送 LLDP 报文接口的 IPv4/IPv6 地址发布为管理地址:

- *ip-address* 参数未指定。
- 指定的 LoopBack 或 VLAN 接口不存在或接口未配置 IPv4/IPv6 地址。

此时, 如果当前发送 LLDP 报文的接口未配置 IPv4/IPv6 地址, 则发布的管理地址为当前接口的 MAC 地址。

如果指定了 **ipv6** 参数, 则发布的管理地址为 IPv6 地址。如果未指定 **ipv6** 参数, 则发布的管理地址为 IPv4 地址。

【举例】

配置全局最近客户桥代理允许发布的 Management Address TLV。

```
<Sysname> system-view
[Sysname] lldp agent nearest-customer global tlv-enable basic-tlv management-address-tlv
192.168.1.1
```

【相关命令】

- **lldp tlv-enable**

1.1.16 lldp hold-multiplier

lldp hold-multiplier 命令用来配置 TTL 乘数。

undo lldp hold-multiplier 命令用来恢复缺省情况。

【命令】

```
lldp hold-multiplier value
undo lldp hold-multiplier
```

【缺省情况】

TTL 乘数为 4。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

value: 表示 TTL 乘数，取值范围为 2~10。

【使用指导】

LLDP 报文所携 Time To Live TLV 中 TTL 的值用来设置邻居信息在本地设备上的老化时间，由于 $TTL = \text{Min}(65535, (TTL \text{ 乘数} \times \text{LLDP 报文的发送间隔} + 1))$ ，即取 65535 与 $(TTL \text{ 乘数} \times \text{LLDP 报文的发送间隔} + 1)$ 中的最小值，因此通过调整 TTL 乘数可以控制本设备信息在邻居设备上的老化时间。

【举例】

```
# 配置 TTL 乘数为 6。
<Sysname> system-view
[Sysname] lldp hold-multiplier 6
```

【相关命令】

- **lldp timer tx-interval**

1.1.17 lldp ignore-pvid-inconsistency

lldp ignore-pvid-inconsistency 命令用来关闭 LLDP 的 PVID 不一致检查功能。

undo lldp ignore-pvid-inconsistency 命令用来开启 LLDP 的 PVID 不一致检查功能。

【命令】

```
lldp ignore-pvid-inconsistency
undo lldp ignore-pvid-inconsistency
```

【缺省情况】

LLDP 的 PVID 不一致检查功能处于开启状态。

【视图】

系统视图

【缺省用户角色】

network-admin

【使用指导】

缺省情况下，LLDP 会对接口接收报文中的 PVID TLV 进行检查，如果发现报文中 PVID 与本端不一致，LLDP 会打印日志信息，提示用户。但在一些特殊情况下，可以允许链路两端的 PVID 配置不一致，此时可以关闭 LLDP 的 PVID 不一致性检查功能。

【举例】

```
# 关闭 LLDP 的 PVID 不一致检查功能。
<Sysname> system-view
[Sysname] lldp ignore-pvid-inconsistency
```

1.1.18 lldp management-address

lldp management-address 命令用来配置接口收到携带 Management Address TLV 的 LLDP 报文后生成 ARP 表项或 ND 表项。

undo lldp management-address 命令用来恢复缺省情况。

【命令】

在二层以太网接口视图下：

```
lldp management-address { arp-learning | nd-learning } vlan vlan-id
```

```
undo lldp management-address { arp-learning | nd-learning }
```

【缺省情况】

接口收到携带 Management Address TLV 的 LLDP 报文后不生成 ARP 表项和 ND 表项。

【视图】

二层以太网接口视图

【缺省用户角色】

network-admin

【参数】

arp-learning：表示接口收到携带 IPv4 格式 Management Address TLV 的 LLDP 报文后，会生成该报文携带的管理地址与报文源 MAC 地址组成的 ARP 表项。

nd-learning：表示接口收到携带 IPv6 格式 Management Address TLV 的 LLDP 报文后，会生成该报文携带的管理地址与报文源 MAC 地址组成的 ND 表项。

vlan *vlan-id*：对于二层以太网接口，指定该接口所属 VLAN 的 VLAN ID，且已创建该 VLAN 对应的 VLAN 虚接口，取值范围为 1～4094。

【使用指导】

ARP 表项和 ND 表项的生成互不影响，可同时配置。

【举例】

配置接口 GigabitEthernet1/0/1 收到携带 IPv4 格式 Management Address TLV 的 LLDP 报文后，生成 ARP 表项。

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] lldp management-address arp-learning
```

【相关命令】

- **lldp source-mac *vlan***

1.1.19 lldp management-address-format string

lldp management-address-format string 命令用来配置管理地址在 TLV 中的封装格式为字符串格式。

undo lldp management-address-format 命令用来恢复缺省情况。

【命令】

在二层以太网接口视图下：

```
lldp [ agent { nearest-customer | nearest-nontpmr } ]  
management-address-format string  
undo lldp [ agent { nearest-customer | nearest-nontpmr } ]  
management-address-format
```

在二层聚合接口视图下：

```
lldp agent { nearest-customer | nearest-nontpmr } management-address-format  
string  
undo lldp agent { nearest-customer | nearest-nontpmr }  
management-address-format
```

【缺省情况】

管理地址在 TLV 中的封装格式为数字格式。

【视图】

二层以太网接口视图

二层聚合接口视图

【缺省用户角色】

network-admin

【参数】

agent：配置指定 LLDP 代理类型管理地址在 TLV 中的封装格式。在以太网接口视图下，未指定时表示配置最近桥代理的管理地址在 TLV 中的封装格式。

nearest-customer：表示最近客户桥代理。

nearest-nontpmr：表示最近非 TPMR 桥代理。

【使用指导】

如果邻居将管理地址以字符串格式封装在 TLV 中，用户可在本地设备上也将封装格式改为字符串，以保证与邻居设备的正常通信。

对于 LLDP 报文中所要发布的 IPv6 格式的管理地址，仅支持数字格式的封装格式。

【举例】

在接口 GigabitEthernet1/0/1 的最近客户桥代理上配置管理地址在 TLV 中的封装格式为字符串格式。

```
<Sysname> system-view  
[Sysname] interface gigabitethernet 1/0/1  
[Sysname-GigabitEthernet1/0/1] lldp agent nearest-customer management-address-format  
string
```

1.1.20 lldp max-credit

lldp max-credit 命令用来配置限制发送报文速率的令牌桶大小。

undo lldp max-credit 命令用来恢复缺省情况。

【命令】

```
lldp max-credit credit-value
undo lldp max-credit
```

【缺省情况】

限制发送报文速率的令牌桶大小为 5。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

credit-value: 表示 LLDP 发包限速的令牌桶大小，取值范围 1~100。

【举例】

配置 LLDP 发包限速的令牌桶大小为 10。

```
<Sysname> system-view
[Sysname] lldp max-credit 10
```

1.1.21 lldp mode

lldp mode 命令用来配置 LLDP 桥模式。

undo lldp mode 命令用来恢复缺省情况。

【命令】

```
lldp mode service-bridge
undo lldp mode
```

【缺省情况】

LLDP 桥模式为客户桥模式。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

service-bridge: 表示服务桥模式。

【使用指导】

LLDP 桥模式命令用于控制设备支持不同的 LLDP 代理。

- 工作于服务桥模式时，设备可支持最近桥代理和最近非 TPMR 桥代理，即对上述类型的代理 MAC 的 LLDP 报文进行处理，其他目的 MAC 的 LLDP 报文进行 VLAN 内透传。

- 工作于客户桥模式时，设备可支持最近桥代理、最近非 TPMR 桥代理及最近客户桥代理，即对上述类型的代理 MAC 的 LLDP 报文进行处理，其他目的 MAC 的 LLDP 报文进行 VLAN 内透传。



说明

桥模式配置只在 LLDP 全局开启后才能生效，LLDP 全局关闭时，只能作为客户桥对三种类型代理 MAC 的 LLDP 报文进行拦截。

【举例】

配置 LLDP 桥模式为服务桥模式。

```
<Sysname> system-view
[Sysname] lldp mode service-bridge
```

【相关命令】

- **lldp global enable**

1.1.22 lldp notification med-topology-change enable

lldp notification med-topology-change enable 命令用来开启 LLDP-MED Trap 功能。

undo lldp notification med-topology-change enable 命令用来关闭 LLDP-MED Trap 功能。

【命令】

```
lldp notification med-topology-change enable
undo lldp notification med-topology-change enable
```

【缺省情况】

LLDP-MED Trap 功能处于关闭状态。

【视图】

二层以太网接口视图

【缺省用户角色】

network-admin

【举例】

在接口 GigabitEthernet1/0/1 上开启 LLDP-MED Trap 功能。

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] lldp notification med-topology-change enable
```

1.1.23 lldp notification remote-change enable

lldp notification remote-change enable 命令用来开启 LLDP Trap 功能。

undo lldp notification remote-change enable 命令用来关闭 LLDP Trap 功能。

【命令】

在二层以太网接口视图下：

```
lldp [ agent { nearest-customer | nearest-nontpmr } ] notification
remote-change enable
```

```
undo lldp [ agent { nearest-customer | nearest-nontpmr } ] notification
remote-change enable
```

在二层聚合接口视图下：

```
lldp agent { nearest-customer | nearest-nontpmr } notification
remote-change enable
```

```
undo lldp agent { nearest-customer | nearest-nontpmr } notification
remote-change enable
```

【缺省情况】

LLDP Trap 功能处于关闭状态。

【视图】

二层以太网接口视图

二层聚合接口视图

【缺省用户角色】

network-admin

【参数】

agent：开启指定类型 LLDP 代理的 LLDP Trap 功能。在以太网接口视图下，未指定时表示开启最近桥代理类型 LLDP 代理的 LLDP Trap 功能。

nearest-customer：表示最近客户桥代理。

nearest-nontpmr：表示最近非 TPMR 桥代理。

【举例】

在接口 GigabitEthernet1/0/1 最近客户桥代理上开启 LLDP Trap 功能。

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

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

```
[Sysname-GigabitEthernet1/0/1] lldp agent nearest-customer notification remote-change
enable
```

1.1.24 lldp source-mac vlan

lldp source-mac vlan 命令用来配置 LLDP 报文源 MAC 地址为 VLAN 虚接口的 MAC 地址。

undo lldp source-mac vlan 命令用来恢复缺省情况。

【命令】

```
lldp source-mac vlan vlan-id
```

```
undo lldp source-mac vlan
```

【缺省情况】

LLDP 报文源 MAC 地址为当前接口的 MAC 地址。

【视图】

二层以太网接口视图

【缺省用户角色】

network-admin

【参数】

vlan-id: 指定该接口所属的 VLAN 的 VLAN ID，且已创建该 VLAN 对应的 VLAN 虚接口，取值范围为 1~4094。

【举例】

配置 LLDP 报文源 MAC 地址为 VLAN 接口 4094 的 MAC 地址。

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] lldp source-mac vlan 4094
```

【相关命令】

- **lldp management-address arp-learning**

1.1.25 lldp timer fast-interval

lldp timer fast-interval 命令用来配置 LLDP 快速发送报文的时间间隔。

undo lldp timer fast-interval 命令用来恢复缺省情况。

【命令】

```
lldp timer fast-interval interval
undo lldp timer fast-interval
```

【缺省情况】

LLDP 快速发送报文的时间间隔为 1 秒。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

interval: 表示 LLDP 快速发送报文的时间间隔，取值范围为 1~3600，单位为秒。

【举例】

配置 LLDP 快速发送报文的时间间隔为 2 秒。

```
<Sysname> system-view
[Sysname] lldp timer fast-interval 2
```

1.1.26 lldp timer notification-interval

lldp timer notification-interval 命令用来配置 LLDP Trap 和 LLDP-MED Trap 信息的发送间隔。

`undo lldp timer notification-interval` 命令用来恢复缺省情况。

【命令】

```
lldp timer notification-interval interval
undo lldp timer notification-interval
```

【缺省情况】

LLDP Trap 和 LLDP-MED Trap 信息的发送间隔均为 30 秒。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

interval: 表示 LLDP Trap 和 LLDP-MED Trap 信息的发送间隔，取值范围为 5～3600，单位为秒。

【举例】

配置 LLDP Trap 和 LLDP-MED Trap 信息的发送间隔为 8 秒。

```
<Sysname> system-view
[Sysname] lldp timer notification-interval 8
```

1.1.27 lldp timer reinit-delay

`lldp timer reinit-delay` 命令用来配置接口初始化的延迟时间。

`undo lldp timer reinit-delay` 命令用来恢复缺省情况。

【命令】

```
lldp timer reinit-delay delay
undo lldp timer reinit-delay
```

【缺省情况】

接口初始化的延迟时间为 2 秒。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

delay: 接口初始化的延迟时间，取值范围为 1～10，单位为秒。

【举例】

配置接口初始化的延迟时间为 4 秒。

```
<Sysname> system-view
[Sysname] lldp timer reinit-delay 4
```

1.1.28 lldp timer tx-interval

lldp timer tx-interval 命令用来配置 LLDP 报文的发送间隔。

undo lldp timer tx-interval 命令用来恢复缺省情况。

【命令】

```
lldp timer tx-interval interval
undo lldp timer tx-interval
```

【缺省情况】

LLDP 报文的发送间隔为 30 秒。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

interval: 表示 LLDP 报文的发送间隔，取值范围为 1~32768，单位为秒。

【举例】

配置 LLDP 报文的发送间隔为 20 秒。

```
<Sysname> system-view
[Sysname] lldp timer tx-interval 20
```

1.1.29 lldp tlv-enable

lldp tlv-enable 命令用来配置接口上允许发布的 TLV 类型。

undo lldp tlv-enable 命令用来配置接口上禁止发布的 TLV 类型。

【命令】

在二层以太网接口视图下：

- 配置最近桥代理 LLDP 接口上允许发布的 TLV 类型

```
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 } }
```

- 配置最近非 TPMR 代理 LLDP 接口上允许发布的 TLV 类型

```
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 } }  
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 |  
port-description | system-capability | system-description | system-name |  
management-address-tlv [ ipv6 ] [ ip-address ] } | dot1-tlv { all |  
port-vlan-id | link-aggregation } }  
undo lldp tlv-enable dot1-tlv { protocol-vlan-id | vlan-name |  
management-vid }
```

- 配置最近客户桥代理 LLDP 接口上允许发布的 TLV 类型

```
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 } }  
lldp tlv-enable dot1-tlv { protocol-vlan-id [ vlan-id ] | vlan-name [ vlan-id ]  
| management-vid [ mvlan-id ] }  
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 } }  
undo lldp tlv-enable dot1-tlv { protocol-vlan-id | vlan-name |  
management-vid }
```

在二层聚合接口视图下：

```
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 }

```

【缺省情况】

二层以太网接口上：

- 最近桥代理允许发布除 Location-id TLV、Port And Protocol VLAN ID TLV、VLAN Name TLV、Management VLAN ID TLV 之外所有类型的 TLV；
- 最近非 TPMR 桥代理不允许发布任何 TLV；
- 最近客户桥代理允许发布基本 TLV 和 IEEE 802.1 组织定义 TLV。

二层聚合接口上：

- 最近非 TPMR 桥代理不允许发布任何 TLV；
- 最近客户桥代理允许发布基本 TLV 和 IEEE 802.1 组织定义 TLV，其中 IEEE 802.1 组织定义的 TLV 只支持 Port And Protocol VLAN ID TLV、VLAN Name TLV 及 Management VLAN ID TLV。

【视图】

二层以太网接口视图

二层聚合接口视图

【缺省用户角色】

network-admin

【参数】

agent：配置指定类型 LLDP 代理允许发布的 TLV 类型。在以太网接口视图下，未指定时表示配置最近桥代理允许发布的 TLV 类型。

nearest-customer：表示最近客户桥代理。

nearest-nontpmr：表示最近非 TPMR 桥代理。

all：发布指定类型的所有可选 TLV：

- 如果为 **basic-tlv** 参数指定 **all**，则允许发布所有基本 TLV。
- 如果为 **dot1-tlv** 参数指定 **all**，则允许发布所有 802.1 组织定义 TLV。
- 如果为 **dot3-tlv** 参数指定 **all**，则允许发布所有 802.3 组织定义 TLV。
- 如果为 **med-tlv** 参数指定 **all**，则允许发布除 **location-id** 以外所有的可选 LLDP-MED TLV。

basic-tlv：表示基本类型 TLV。

management-address-tlv [ipv6] [ip-address | interface loopback interface-number]：表示 Management Address TLV。其中，**ipv6** 表示 LLDP 报文中所要

发布的管理地址为 IPv6 格式的地址。*ip-address* 表示在 LLDP 报文中发布的管理地址为指定的 IP 地址, **interface loopback interface-number** 表示在 LLDP 报文中发布的管理地址为指定的 LoopBack 接口的 IP 地址。其缺省值如下:

- 执行 **lldp tlv-enable** 命令时:
 - 在二层以太网接口视图/二层聚合接口视图下, 如果 *ip-address* 参数未指定, 则发布的管理地址为当前接口允许通过的、对应 VLAN 接口上配置有 IPv4/IPv6 地址且处于 up 状态的最小 VLAN 的 IPv4/IPv6 地址。
如果指定了 **ipv6** 参数, 则发布的管理地址为 IPv6 地址。如果未指定 **ipv6** 参数, 则发布的管理地址为对应 VLAN 接口的 IP 地址 (包括 IPv4 地址和 IPv6 地址)。
如果当前接口允许通过的所有 VLAN 所对应的 VLAN 接口上都未配置 IPv4/IPv6 地址或均处于 down 状态, 则发布当前接口的 MAC 地址。
- 执行 **undo lldp tlv-enable** 命令时:
 - 在二层以太网接口视图/二层聚合接口视图下:
如果不带 **ipv6**、*ip-address* 和 **interface loopback interface-number** 参数表示不发布该 TLV;
如果带 **ipv6**、*ip-address* 和 **interface loopback interface-number** 参数表示按缺省值发布该 TLV。

port-description: 表示 Port Description TLV。

system-capability: 表示 System Capabilities TLV。

system-description: 表示 System Description TLV。

system-name: 表示 System Name TLV。

dot1-tlv: 表示 IEEE 802.1 组织定义的 TLV。

port-vlan-id: 表示 Port VLAN ID TLV。

protocol-vlan-id [*vlan-id*]: 表示 Port And Protocol VLAN ID TLV, *vlan-id* 为所要发布 VLAN 的 VLAN ID, 取值范围为 1~4094, 缺省值为该端口所属 VLAN 中最小的 VLAN ID。

vlan-name [*vlan-id*]: 表示 VLAN Name TLV, *vlan-id* 为所要发布 VLAN 的 VLAN ID, 取值范围为 1~4094, 缺省值为该端口所属 VLAN 中最小的 VLAN ID。如果未指定 *vlan-id*, 且端口未加入任何 VLAN, 所要发布的 VLAN 为该端口 PVID。

management-vid [*mvlan-id*]: 表示 Management VLAN ID TLV。 *mvlan-id* 指定要发布管理 VLAN 的 VLAN ID, 取值范围为 1~4094。如果未指定该参数, 则表示发布 0, 表示当前 LLDP agent 未配置管理 VLAN。

link-aggregation: 表示 Link Aggregation TLV。

dot3-tlv: 表示 IEEE 802.3 组织定义的 TLV。

mac-physic: 表示 MAC/PHY Configuration/Status TLV。

max-frame-size: 表示 Maximum Frame Size TLV。

power: 表示 Power Via MDI TLV 和 Power Stateful Control TLV。

med-tlv: 表示 LLDP-MED TLV。

capability: 表示 LLDP-MED Capabilities TLV。

inventory: 表示 Hardware Revision TLV、Firmware Revision TLV、Software Revision TLV、Serial Number TLV、Manufacturer Name TLV、Model Name TLV 和 Asset ID TLV。

location-id: 表示 Location Identification TLV。

civic-address: 表示 Location Identification TLV 封装网络设备的普通地址信息。

device-type: 表示设备类型，取值范围为 0~2。0 表示设备类型为 DHCP server，1 表示设备类型为 Network device，2 表示设备类型为 LLDP-MED Endpoint。

country-code: 表示国家编码，取值范围请参考 ISO 3166。

{ *ca-type ca-value* }&<1-10>: 地址信息。*ca-type* 表示地址信息类型，取值范围为 0~255；*ca-value* 表示地址信息，为 1~250 个字符的字符串。&<1-10>表示前面的参数最多可以输入 10 次。

elin-address: Location Identification TLV 封装紧急电话号码。

tel-number: 表示紧急电话号码，为 10~25 个字符的字符串，只能包含数字。

network-policy [*vlan-id*]: 表示 Network Policy TLV, *vlan-id* 为要发布的 Voice VLAN ID, 取值范围为 1~4094。S5000E-X、S5110V2-SI 和 S5000V3-EI 系列交换机不支持本参数。

power-over-ethernet: 表示 Extended Power-via-MDI TLV。

【使用指导】

聚合接口不支持最近桥代理。

在使用本命令时若不指定 **all** 参数，每次只能配置某类型下的一种可选 TLV，此时可通过多次使用该命令来配置各类型下的多种可选 TLV。

如果禁止发布 802.3 的组织定义的 MAC/PHY Configuration/Status TLV，则 LLDP-MED TLV 将不会被发布，不论其是否被允许发布；如果禁止发布 LLDP-MED Capabilities TLV，则其它 LLDP-MED TLV 将不会被发布，不论其是否被允许发布。

IEEE 802.1 组织定义的 TLV 的 Port And Protocol VLAN ID TLV、VLAN Name TLV 及 Management VLAN ID TLV 只能基于最近桥代理配置，但是其配置会被最近非 TPMR 桥代理和最近客户桥代理继承。

【举例】

配置接口 GigabitEthernet1/0/1 上最近客户桥代理允许发布 IEEE 802.1 组织定义的 Link Aggregation 可选 TLV。

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] lldp agent nearest-customer tlv-enable dot1-tlv
link-aggregation
```

目 录

1 L2PT.....	1-1
1.1 L2PT配置命令	1-1
1.1.1 display l2protocol statistics	1-1
1.1.2 l2protocol tunnel dot1q.....	1-2
1.1.3 l2protocol tunnel-dmac.....	1-4
1.1.4 reset l2protocol statistics	1-4

1 L2PT

1.1 L2PT配置命令

1.1.1 display l2protocol statistics

display l2protocol statistics 命令用来显示 L2PT 报文统计信息。

【命令】

display l2protocol statistics [**interface** *interface-type interface-number*]

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator

【参数】

interface interface-type interface-number: 显示指定二层以太网接口或二层聚合接口上的 L2PT 报文统计信息。*interface-type interface-number* 表示接口类型和接口编号。如未指定本参数，将显示所有二层以太网接口和二层聚合接口的 L2PT 报文统计信息。

【举例】

显示所有二层以太网接口和二层聚合接口的 L2PT 报文统计信息。

```
<Sysname> display l2protocol statistics
```

L2PT statistics information on interface Bridge-Aggregation1:

Protocol	Encapsulated	Decapsulated	Forwarded	Dropped
CDP	0	0	0	0
DLDLP	0	3	0	0
EOAM	0	2	0	0
GVRP	8	4	9	2
LACP	0	0	0	0
LLDP	0	3	0	0
MVRP	0	0	0	0
PAGP	0	1	0	0
PVST	0	0	0	0
STP	5	5	5	0
Tunnel	N/A	N/A	100	10
VTP	0	6	0	0
UDLD	0	0	0	0

L2PT statistics information on interface GigabitEthernet1/0/1:

Protocol	Encapsulated	Decapsulated	Forwarded	Dropped
CDP	0	0	0	0
DLDLP	2	3	3	0

EOAM	5	2	9	0
GVRP	8	4	9	2
LACP	0	0	0	0
LLDP	3	3	3	3
MVRP	0	0	0	0
PAGP	5	1	7	3
PVST	0	0	0	0
STP	5	5	5	0
Tunnel	N/A	N/A	100	10
VTP	0	6	0	0
UDLD	0	0	0	0

表1-1 display l2protocol statistics 命令显示信息描述表

字段	描述
Protocol	协议类型
Encapsulated	封装统计计数 用户侧收到协议报文后封装成Tunnel报文，对应的协议封装统计计数加1 对于Tunnel（表示Tunnel报文），对应值显示为N/A，为无效统计计数
Decapsulated	解封装统计计数 网络侧收到Tunnel报文后解封装成协议报文，对应的协议解封装统计计数加1 对于Tunnel，对应值显示为N/A，为无效统计计数
Forwarded	转发统计计数 <ul style="list-style-type: none"> 用户侧或网络侧收到协议报文后转发，对应的协议转发统计计数加 1 网络侧收到 Tunnel 报文后转发，对应的 Tunnel 转发统计计数加 1（如果网络侧收到 Tunnel 报文时，设备没有任何用户侧端口，则 Tunnel 转发统计计数不会增加）
Dropped	丢弃统计计数 <ul style="list-style-type: none"> 接口收到协议报文后丢弃，对应的协议丢弃统计计数加 1（如果协议报文被硬件丢弃，则协议丢弃统计计数不会增加） 接口收到 Tunnel 报文后丢弃，对应的 Tunnel 丢弃统计计数加 1

1.1.2 l2protocol tunnel dot1q

l2protocol tunnel dot1q 命令用来开启指定协议的 L2PT 功能。

undo l2protocol tunnel dot1q 命令用来关闭指定协议的 L2PT 功能。

【命令】

在二层以太网接口视图下：

```
l2protocol { cdp | dldp | eoam | gvrp | lacp | lldp | mvrp | pagp | pvst | stp | udld  
| vtp } tunnel dot1q
```

```
undo l2protocol { cdp | dldp | eoam | gvrp | lacp | lldp | mvrp | pagp | pvst | stp  
| udld | vtp } tunnel dot1q
```

在二层聚合接口视图下：

```
l2protocol { gvrp | mvrp | pvst | stp | vtp } tunnel dot1q
undo l2protocol { gvrp | mvrp | pvst | stp | vtp } tunnel dot1q
```

【缺省情况】

各协议的 L2PT 功能均处于关闭状态。

【视图】

二层以太网接口视图

二层聚合接口视图

【缺省用户角色】

network-admin

【参数】

cdp: 表示 CDP 协议。

dldp: 表示 DLDP 协议。

eoam: 表示 EOAM 协议。

gvrp: 表示 GVRP 协议。

lACP: 表示 LACP 协议。

lldp: 表示 LLDP 协议。

mvrp: 表示 MVRP 协议。

PAGP: 表示 PAGP 协议。

PVST: 表示 PVST 协议。

stp: 表示 STP 协议。

UDLD: 表示 UDLD 协议。

vtp: 表示 VTP 协议。

【使用指导】

L2PT 功能仅需在用户侧接口上开启。如果在网络侧接口上开启了 L2PT 功能，则会将该接口认为是用户侧接口。

在接口上开启某协议的 L2PT 功能时，对应的 CE 上应启用该协议，同时当前接口必须关闭该协议。

如果 CE 上与 PE 开启 L2PT 功能的接口相连的聚合接口上正在运行某协议（例如 STP），则 PE 设备上对应的接口必须关闭对应协议。

允许在二层聚合组的成员端口上开启 L2PT 功能，但配置不生效。

对于 LLDP 协议，L2PT 功能只支持 Nearest Bridge（最近桥代理）类型的 LLDP 报文。

【举例】

在接口 GigabitEthernet1/0/1 上关闭 STP 协议，并开启 STP 协议的 L2PT 功能。

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

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

```
[Sysname-GigabitEthernet1/0/1] undo stp enable
```

```
[Sysname-GigabitEthernet1/0/1] l2protocol stp tunnel dot1q
```

在二层聚合接口 Bridge-Aggregation1 上关闭 STP 协议，并开启 STP 协议的 L2PT 功能。

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

```
[Sysname] interface bridge-aggregation 1
[Sysname-Bridge-Aggregation1] undo stp enable
[Sysname-Bridge-Aggregation1] l2protocol stp tunnel dot1q
```

1.1.3 l2protocol tunnel-dmac

l2protocol tunnel-dmac 命令用来配置 Tunnel 报文的组播目的 MAC 地址。

undo l2protocol tunnel-dmac 命令用来恢复缺省情况。

【命令】

```
l2protocol tunnel-dmac mac-address
undo l2protocol tunnel-dmac
```

【缺省情况】

Tunnel 报文的组播目的 MAC 地址为 010f-e200-0003。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

mac-address: Tunnel 报文的组播目的 MAC 地址。取值为 0100-0ccd-cdd0、0100-0ccd-cdd1、0100-0ccd-cdd2 或 010f-e200-0003。

【举例】

配置 Tunnel 报文的组播目的 MAC 地址为 0100-0ccd-cdd0。

```
<Sysname> system-view
[Sysname] l2protocol tunnel-dmac 0100-0ccd-cdd0
```

1.1.4 reset l2protocol statistics

reset l2protocol statistics 命令用来清除 L2PT 报文的统计信息。

【命令】

```
reset l2protocol statistics [ interface interface-type interface-number ]
```

【视图】

用户视图

【缺省用户角色】

network-admin

【参数】

interface interface-type interface-number: 清除指定二层以太网接口或二层聚合接口上的 L2PT 报文统计信息。*interface-type interface-number* 表示接口类型和接口编号。如未指定本参数，将清除所有二层以太网接口和二层聚合接口的 L2PT 报文统计信息。

【举例】

清除所有二层以太网接口和二层聚合接口的 L2PT 报文统计信息。

```
<Sysname> reset l2protocol statistics
```