UNIS 防火墙产品

接口管理配置指导(V7)

北京紫光恒越网络科技有限公司
http://www.unis-hy.com

资料版本：5P100-20160616

前 言

UNIS 防火墙产品配置指导(V7)介绍了防火墙产品各软件特性的原理及其配置方法，包含原理简介、配置任务描述和配置举例。《接口管理配置指导》主要介绍接口批量配置、以太网接口、LoopBack 接口、Null 接口和 InLoopBack 接口相关的特性。

前言部分包含如下内容：

适用款型

防火墙产品款型较多，形态丰富，本手册所描述的内容适用于如下产品款型：

表1 手册适用的产品款型

款型	形态
UNIS F5000-M06防火墙	分布式设备，可以运行在： • 独立运行模式 • IRF 模式
UNIS F5000-G20防火墙	集中式IRF设备
UNIS F1000-G20/G50/G60/G80防火墙	集中式IRF设备

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。
斜体	命令行参数（命令中必须由实际值进行替代的部分）采用*斜体*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 | …]	表示从多个选项中选取一个或者不选。
{ x | y | … } *	表示从多个选项中至少选取一个。
[x | y | …] *	表示从多个选项中选取一个、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。
ROUTER	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。
SWITCH	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. 端口编号示例约定

本手册中出现的端口编号仅作示例，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。

技术支持

用户支持邮箱：zgsm_service@thunis.com

技术支持热线电话：400-910-9998（手机、固话均可拨打）

网址：http://www.unis-hy.com

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：zgsm_info@thunis.com

感谢您的反馈，让我们做得更好！

目 录

1 接口批量配置

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。此时，可以使用接口批量配置功能，对接口进行批量配置，节省配置工作量。

1.1 接口批量配置

将多个接口进行绑定的时候，有如下要求：

- 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* | *interface-number.subnumber* }命令进入该接口视图的接口。
- 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。

在接口批量配置视图下配置时，有如下约定：

- 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。出现以下情况时请注意：
  - 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，则表示这条命令在接口视图和系统视图下都支持，并且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。

表1-1 接口批量配置

操作	命令	说明
进入系统视图	**system-view**	-
进入接口批量配置视图	**interface range** { *interface-type interface-number* [**to** *interface-type interface-number*] } &<1-5>	二者选其一 **interface range name**和**interface range**命

操作	命令	说明
	interface range name *name* [**interface** { *interface-type interface-number* [**to** *interface-type interface-number*] } &<1-5>]	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，不再需要重新输入接口列表，配置起来更简便

1.2 接口批量配置显示和维护

在完成上述配置后，在任意视图下执行 **display** 命令可以显示配置后批量接口的信息。

表1-2 接口批量配置显示和维护

操作	命令
显示通过**interface range name**命令创建的批量接口的信息	**display interface range** [**name** *name*]

目 录

1 以太网接口配置

说明

对于本节命令中的 CPU 参数，仅 F5000-M06 产品支持。

设备上支持的以太网接口有以下几种：

- 二层以太网接口：是一种工作在数据链路层的物理接口，可以对接收到的报文进行二层交换转发。
- 三层以太网接口：是一种工作在网络层的物理接口，可以配置 IP 地址，可以对接收到的报文进行三层路由转发。
- 二、三层可切换以太网接口：是一种物理接口，可以工作在二层模式或三层模式下，作为一个二层以太网接口或三层以太网接口使用。
- 三层以太网子接口：是一种逻辑接口，工作在网络层，可以配置 IP 地址，处理三层协议。主要用来实现在三层以太网接口上支持收发 VLAN tagged 报文。用户可以在一个以太网接口上配置多个子接口，这样，来自不同 VLAN 的报文可以从不同的子接口进行转发，为用户提供了很高的灵活性。

1.1 以太网接口通用配置

该部分介绍了二层以太网接口和三层以太网接口/子接口的共有属性及其配置，各自的特有属性请参见下文中“1.2 二层以太网接口的配置”和“1.3 三层以太网接口/子接口的配置”。

1.1.1 Combo接口配置（单Combo接口）

1. Combo接口介绍

Combo 接口是一个逻辑接口，一个 Combo 接口在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共用一个转发接口和接口视图，所以，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禁用状态。用户可根据组网需求选择使用电口或光口。当用户需要激活电口或光口、配置电口或光口的属性（例如速率、双工等）时，在同一接口视图下配置。

2. 配置准备

- 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。
- 通过 **display interface** 命令了解当前处于激活状态的是电口还是光口。如果显示信息中包含“Media type is twisted pair, Port hardware type is 1000_BASE_T”，则表示电口处于激活状态，否则，则表示光口处于激活状态。也可在 Combo 端口视图下执行 **display this** 命令查看当前视图下的配置，若存在 **combo enable fiber** 命令，则表示光口处于激活状态，否则，则表示电口处于激活状态。

3. 配置步骤

表1-1 配置 Combo 接口的状态

操作	命令	说明
进入系统视图	**system-view**	-
进入以太网接口视图	**interface** *interface-type interface-number*	-
激活Combo接口中的电口或者光口	**combo enable { copper | fiber }**	缺省情况下，电口处于激活状态

1.1.2 以太网接口/子接口基本配置

1. 以太网接口基本配置

设置以太网接口的双工模式时存在以下几种情况：

- 当希望接口在发送数据包的同时可以接收数据包，可以将接口设置为全双工（**full**）属性；
- 当希望接口同一时刻只能发送数据包或接收数据包时，可以将接口设置为半双工（**half**）属性；
- 当设置接口为自协商（**auto**）状态时，接口的双工状态由本接口和对端接口自动协商而定。

表1-2 以太网接口基本配置

操作	命令	说明
进入系统视图	**system-view**	-
进入以太网接口视图	**interface** *interface-type interface-number*	-
设置当前接口的描述信息	**description** *text*	缺省情况下，接口的描述信息为“*接口名* Interface”，例如：GigabitEthernet1/0/1 Interface
设置以太网接口的双工模式	**duplex { auto | full | half }**	光类型接口不支持配置**half**参数 缺省情况下，以太网接口的双工模式为**auto**（自协商）状态，10GE/40GE接口的双工模式为全双工状态
设置以太网接口的速率	**speed { 10 | 100 | 1000 | 10000 | 40000 | 100000 | auto }**	本命令各参数的支持情况与业务板的型号有关，请参见命令参考中的介绍 本命令的缺省情况与设备的型号有关，请参见命令参考中的介绍
配置接口的期望带宽	**bandwidth** *bandwidth-value*	缺省情况下，接口的期望带宽＝接口的最大速率÷1000（kbit/s）
恢复当前接口的缺省配置	**default**	-
打开以太网接口	**undo shutdown**	缺省情况下以太网接口/子接口处于开启状态 **shutdown**和**loopback**命令互斥，后配置的失败

2. 以太网子接口基本配置

使用以太网子接口，需要注意的是：

- 以太网子接口只有在关联了 VLAN 后才能正常收发报文。相关配置请参见“二层技术-以太网交换配置指导”中的“VLAN 终结”。
- 本端设备以太网子接口号、关联的 VLAN ID 需要分别和相连的对端设备的以太网子接口号、关联的 VLAN ID 一致，否则报文将不能正确传输。
- 创建编号为 D 的三层以太网子接口，与配置预留 VLAN D 的接口资源互斥（三层以太网子接口的编号规则为 interface type A/B/C.D，D 表示子接口编号）。这是因为三层以太网子接口需要收发携带子接口编号的 VLAN Tag 的报文，因此需要使用对应 VLAN 接口的资源。

表1-3 以太网子接口基本配置

操作	命令	说明
进入系统视图	**system-view**	-
创建以太网子接口，并进入以太网子接口视图	**interface** *interface-type interface-number.subnumber*	-
设置以太网子接口的描述字符串	**description** *text*	缺省情况下，描述字符串为“该接口的接口名 Interface”，例如：GigabitEthernet1/0/1.1 Interface
恢复当前接口的缺省配置	**default**	-
配置接口的期望带宽	**bandwidth** *bandwidth-value*	缺省情况下，接口的期望带宽＝接口的最大速率÷1000（kbit/s）
打开以太网子接口	**undo shutdown**	缺省情况下，以太网接口/子接口处于开启状态 在进行环回测试时，禁止在接口上配置 **shutdown**命令

1.1.3 配置以太网接口的工作模式

注意

工作模式切换后，除了 **shutdown** 和 **combo enable** 命令，该以太网接口下的其它所有命令都将恢复到新模式下的缺省情况。

- 如果将工作模式设置为二层模式（**bridge**），则作为一个二层以太网接口使用。
- 如果将工作模式设置为三层模式（**route**），则作为一个三层以太网接口使用。

表1-4 配置以太网接口的工作模式

操作	命令	说明
进入系统视图	**system-view**	-
进入以太网接口视图	**interface** *interface-type interface-number*	-
切换以太网接口工作模式	**port link-mode { bridge | route }**	-

1.1.4 配置以太网接口允许超长帧通过

以太网接口在进行文件传输等大吞吐量数据交换的时候，可能会收到大于标准以太网帧长的帧，这种帧称为超长帧。系统对于超长帧的处理如下：

- 如果系统配置了禁止超长帧通过，会直接丢弃该帧不再进行处理。
- 如果系统允许超长帧通过，当接口收到长度在指定范围内的超长帧时，系统会继续处理；当接口收到长度超过指定最大长度的超长帧时，系统会直接丢弃该帧不再进行处理。

表1-5 配置允许超长帧通过以太网接口

操作	命令	说明
进入系统视图	**system-view**	-
进入以太网接口视图	**interface** *interface-type interface-number*	-
允许超长帧通过	**jumboframe enable** [*size*]	缺省情况下，设备允许指定长度的超长帧通过，但是允许通过的超长帧的长度与设备的型号有关，请参见命令参考中的介绍 *value*参数的支持情况与设备型号有关，请参见命令参考中的介绍。多次执行该命令配置不同的*value*值时，则最新的配置生效

1.1.5 配置以太网接口物理连接状态抑制功能

设备各款型对于本节所描述的特性支持情况有所不同，详细差异信息如下：

型号	特性	描述
F5000-M06	配置以太网接口物理连接状态抑制功能	支持
F5000-G20		不支持
F1000-G20/G50/G60/G80		不支持

提示

对于使能了生成树协议的端口不推荐使用该功能。

以太网接口有两种物理连接状态：up 和 down。当接口状态发生改变时，接口会立即上报 CPU，CPU 会立即通知上层协议模块（例如路由、转发）以便指导报文的收发，并自动生成 Trap 和 Log 信息，来提醒用户是否需要对物理链路进行相应处理。

如果短时间内接口物理状态频繁改变，上述处理方式会给系统带来额外的开销。此时，可以在接口下设置物理连接状态抑制功能，使得在抑制时间内，系统忽略接口的物理状态变化；经过抑制时间后，如果状态还没有恢复，再进行处理。

在配置本特性时，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。

表1-6 设置以太网接口物理连接状态抑制功能

操作	命令	说明
进入系统视图	**system-view**	-
进入以太网接口视图	**interface** *interface-type interface-number*	-
配置以太网接口物理连接状态抑制功能	**link-delay** [**msec**] *delay-time* [**mode** { **up** | **updown** }]	-

1.1.6 配置以太网接口dampening功能

由于线缆故障、接口连接或链路层配置错误等问题，可能会导致设备接口的状态频繁的在 down 和 up 之间切换，这种现象称为接口震荡。随着接口状态的频繁改变，设备会不停的刷新相关表项（比如路由表），消耗大量的系统资源。通过在接口上配置 dampening 功能，可以在一定条件下，屏蔽该接口的震荡对路由等上层业务的影响。此时若出现接口震荡，将不上送 CPU 处理，仅产生对应的 Trap 和 Log 信息，从而节省系统资源的消耗。

dampening 功能中各参数解释如下：

- 惩罚值（Penalty）：配置 dampening 功能后，接口对应一个惩罚值，初始值为 0。接口状态从 up 变到 down 时，惩罚值会增加 1000；接口状态从 down 变到 up 时，惩罚值不变。
- 最大惩罚值（Ceiling）：当惩罚值达到此值后，惩罚值将不再增加。
- 抑制值（Suppress-limit）：当惩罚值大于或等于这个门限时，抑制接口，即当接口状态变化时，不上送 CPU 处理，仅产生对应的 Trap 和 Log 信息。
- 启用值（Reuse-limit）：当惩罚值小于或等于这个门限时，不抑制接口，即当接口状态变化时，上送 CPU 处理，同时产生对应的 Trap 和 Log 信息。
- 半衰期（Decay）：此阶段惩罚值随着时间的推移自动的减少，满足半衰期衰减规律，即经过一个半衰周期，惩罚值减半。
- 最大抑制时间（Max-suppress-time)：如果接口一直不稳定，网络设备不能一直抑制它，必须要设定一个最大的抑制时间。最大抑制时间后，惩罚值进入完全半衰期。

其中，最大惩罚值与最大抑制时间、半衰期、启用值之间遵循公式：最大惩罚值＝$2^{(\text{最大抑制时间}/\text{半衰期})}\times$启用值，其中最大惩罚值不可配。惩罚值的变化规律如下图所示。

图1-1 dampening 惩罚值变化规律图

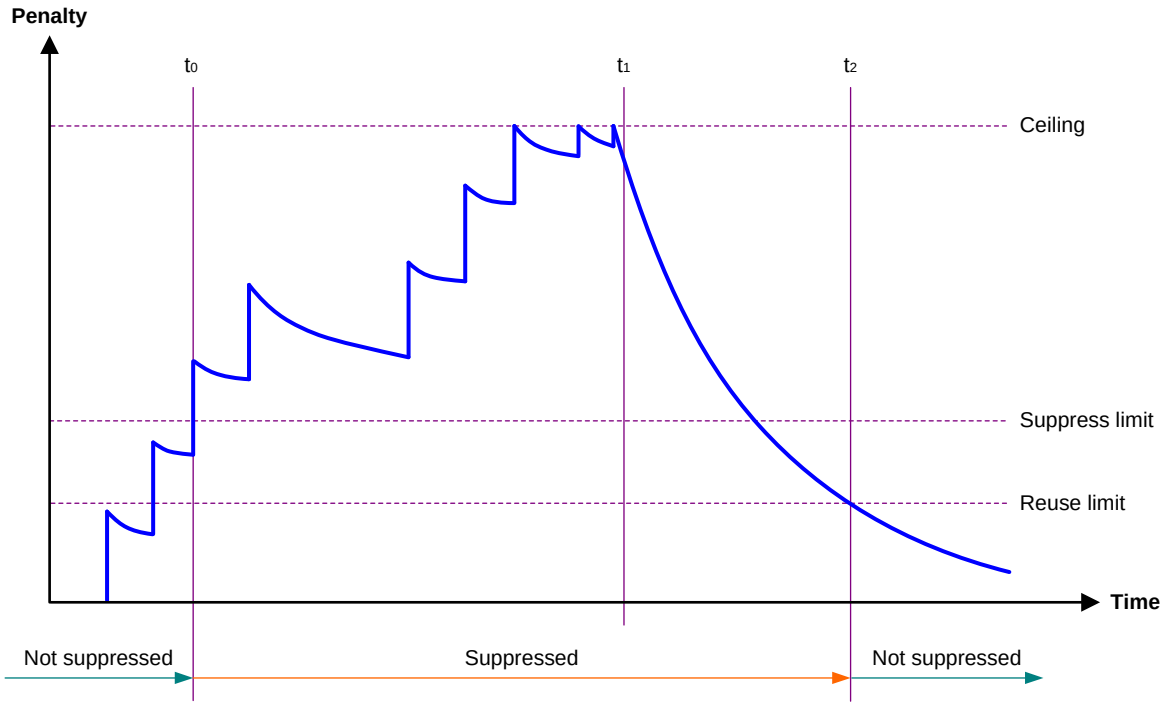

图 1-1 中，t_0 为抑制开始时间，从t_0 开始经过最大抑制时间后达到t_1，t_2 为抑制结束时间。t_0 至t_2 段对应接口抑制期，t_0 至t_1 段对应最大抑制时间，t_1 至t_2 段对应完全半衰期（此阶段惩罚值不再增加）。

配置 dampening 功能时，需要注意：

- 以太网接口上不能同时配置本功能和 **link-delay** 命令。
- 本功能对使用 **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 MSTP 的接口不建议配置该功能。

表1-7 配置以太网接口 dampening 功能

操作	命令	说明
进入系统视图	**system-view**	-
进入以太网接口视图	**interface** *interface-type interface-number*	-
开启接口的dampening功能	**dampening** [*half-life reuse suppress max-suppress-time*]	缺省情况下，接口的dampening功能处于关闭状态

1.1.7 开启以太网接口的环回功能

该功能用于检测以太网转发通路能否正常工作。环回功能包括内部环回和外部环回：

- 内部环回：配置内部环回后，接口将需要从接口转发出去的报文返回给设备内部，让报文向内部线路环回。内部环回用于定位设备是否故障。

- 外部环回：配置外部环回后，接口将来自对端设备的报文返回给对端设备，让报文向外部线路环回。外部环回用于定位设备间链路是否故障。

需要注意的是：

- 开启环回功能后，接口将不能正常转发数据包，请按需配置。
- **shutdown** 和 **loopback** 命令互斥，后配置的失败。
- 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。

表1-8 开启以太网接口的环回功能

操作	命令	说明
进入系统视图	**system-view**	-
进入以太网接口视图	**interface** *interface-type interface-number*	-
开启以太网接口的环回功能	**loopback { external | internal }**	-

1.1.8 配置以太网接口的流量控制功能

设备各款型对于本节所描述的特性支持情况有所不同，详细差异信息如下：

型号	特性	描述
F5000-M06	配置以太网接口的流量控制功能	支持
F5000-G20		不支持
F1000-G20/G50/G60/G80		不支持

以太网接口流量控制功能的基本原理是：如果本端设备发生拥塞，将通知对端设备暂时停止发送报文；对端设备收到该消息后将暂时停止向本端发送报文；反之亦然。从而避免了报文丢失现象的发生。

- 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。
- 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。当本端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。

因此，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**。

表1-9 开启以太网接口的流量控制功能

操作	命令	说明
进入系统视图	**system-view**	-
进入以太网接口视图	**interface** *interface-type interface-number*	-

操作	命令	说明
开启以太网接口的流量控制功能	**flow-control**	二者选其一 缺省情况下，以太网接口的流量控制功能处于关闭状态
配置以太网接口的接收流量控制功能	**flow-control receive enable**	

1.1.9 配置以太网接口的PFC功能

设备各款型对于本节所描述的特性支持情况有所不同，详细差异信息如下：

型号	特性	描述
F5000-M06	配置以太网接口的PFC功能	支持
F5000-G20		不支持
F1000-G20/G50/G60/G80		不支持

如果本端和对端设备的 PFC（Priority-based Flow Control，基于优先级的流量控制）功能处于使能状态，并配置了 **priority-flow-control no-drop dot1p** *dot1p-list* 命令，则当本端收到的 802.1p 优先级在 *dot1p-list* 范围内的报文发生拥塞时，会通知对端设备暂时停止向本端发送对应优先级的报文；拥塞解除后，再通知对端继续发送对应优先级的报文。从而保证本设备在转发 802.1p 优先级在 *dot1p-list* 范围内的报文时不丢包。

PFC功能的状态由本端和对端设备的配置共同决定，如 表 1-10 所示，第一行表示本端的PFC配置，第一列表示对端的PFC配置，使能和未使能表示协商结果。请在报文流经的所有端口上都进行相同的PFC功能配置。

表1-10 PFC 配置和协商结果描述表

本端配置（右） 对端配置（下）	enable	auto	缺省情况
enable	使能	使能	未使能
auto	使能	• 协商成功，则为使能 • 协商失败，则为未使能	未使能
缺省情况	未使能	未使能	未使能

需要注意的是：

- 配置本功能需要在系统视图和以太网接口视图下同时使能 PFC 功能，并且在以太网接口视图下指定的 *dot1p-list* 必须在系统视图下配置的 *dot1p-list* 范围内。如果设备处于 IRF 模式时，IRF 物理端口也需要使能 PFC 功能。IRF 相关内容的详细介绍，请参见“虚拟化技术配置指导”中的“IRF”。
- 不建议在 802.1p 优先级为 0，6 或 7 时配置 PFC 功能，以免影响设备 IRF 功能及其它协议正常运行。

- 为了避免报文在传输过程中因拥塞而发生丢包，请在报文流经的所有端口上都进行相同的 PFC 功能配置。
- 无论端口是否配置 PFC 功能，端口都可以接收 PFC pause 帧。但只有 PFC 功能处于 enabled 状态时，才对收到的 PFC pause 进行处理。所以，必须保证本端和对端的 PFC 功能都处于 enabled 状态，PFC 功能才能生效。

表1-11 配置以太网接口的 PFC 功能

操作	命令	说明
进入系统视图	**system-view**	-
配置PFC功能的开启模式	**priority-flow-control { auto | enable }**	缺省情况下，PFC功能处于关闭状态
开启指定802.1p优先级的PFC功能	**priority-flow-control no-drop dot1p** *dot1p-list*	缺省情况下，所有802.1p优先级的PFC功能都处于关闭状态
进入以太网接口视图	**interface** *interface-type interface-number*	-
配置PFC功能的开启模式	**priority-flow-control { auto | enable }**	缺省情况下，PFC功能处于关闭状态
开启指定802.1p优先级的PFC功能	**priority-flow-control no-drop dot1p** *dot1p-list*	缺省情况下，所有802.1p优先级的PFC功能都处于关闭状态

当 PFC 功能处于使能状态时又配置了 **flow-control** 或 **flow-control receive enable**，则 PFC 相应配置优先生效，**flow-control** 和 **flow-control receive enable** 的配置将被忽略；当 PFC 功能处于未使能状态时又配置了 **flow-control** 或 **flow-control receive enable**，则 **flow-control** 和 **flow-control receive enable** 的配置生效。

1.1.10 配置以太网接口统计信息的时间间隔

使用本特性可以设置统计以太网接口报文信息的时间间隔。使用 **display interface** 命令可以显示端口在该间隔时间内统计的报文信息。使用 **reset counters interface** 命令可以清除端口的统计信息。Context 中的共享接口不支持该命令。

表1-12 在以太网接口视图下配置以太网接口统计信息的时间间隔

操作	命令	说明
进入系统视图	**system-view**	-
进入以太网接口视图	**interface** *interface-type interface-number*	-
配置接口统计信息的时间间隔	**flow-interval** *interval*	缺省情况下，接口统计信息的时间间隔为300秒

1.1.11 配置以太网子接口速率统计功能

提示

开启本功能可能需要耗费大量系统资源，影响系统性能，请谨慎使用。

当以太网接口使能子接口速率统计功能后，设备会定时刷新子接口速率统计信息。用户可以通过 **display interface** 命令查看统计结果。

表1-13 配置以太网子接口速率统计功能

操作	命令	说明
进入系统视图	**system-view**	-
进入接口视图	**interface** *interface-type interface-number*	-
配置子接口速率统计功能	**sub-interface rate-statistic**	缺省情况下，接口的子接口速率统计功能处于关闭状态

1.2 二层以太网接口的配置

1.2.1 配置广播/未知单播风暴抑制功能

在接口上配置了广播/未知单播风暴抑制功能后，当接口上的广播/未知单播流量超过用户设置的抑制阈值时，系统会丢弃超出流量限制的报文，从而使接口的广播/未知单播流量降低到限定范围内，保证网络业务的正常运行。

执行**storm-constrain**与**broadcast-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**、**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。**storm-constrain**命令的详细描述请参见“1.2.2 配置以太网接口流量阈值控制功能”。

表1-14 配置以太网接口的风暴抑制比

操作	命令	说明
进入系统视图	**system-view**	-
进入以太网接口视图	**interface** *interface-type interface-number*	-
开启端口广播风暴抑制功能，并设置广播风暴抑制阈值	**broadcast-suppression** { *ratio* | **pps** *max-pps* | **kbps** *max-kbps* }	缺省情况下，所有接口不对广播流量进行抑制
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	**unicast-suppression** { *ratio* | **pps** *max-pps* | **kbps** *max-kbps* }	缺省情况下，所有接口不对未知单播流量进行抑制

说明

当风暴抑制阈值配置为 pps 或 kbps 时，设备可能会根据芯片支持的步长，将配置值转换成步长的倍数。所以，端口下配置的抑制阈值可能与实际生效抑制阈值不一致，请注意查看设备的提示信息。

1.2.2 配置以太网接口流量阈值控制功能

1. 端口流量阈值控制简介

端口流量阈值控制功能用于控制以太网上的报文风暴。启用该功能的端口会定时检测到达端口的未知单播报文流量、广播报文流量。如果某类报文流量超过预先设置的上限阈值时，用户可以通过配置来决定是阻塞该端口还是关闭该端口，以及是否输出 Log 和 Trap 信息。

- 配置成 block 方式：当端口上未知单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。
- 配置成 shutdown 方式：当端口上未知单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。

本特性实现中系统需要一个完整的周期（周期长度为 *seconds*）来收集流量数据，下一个周期分析数据、采取相应的控制措施。因此，开启端口流量阈值控制功能后，如果某类报文流量超过预先设置的上限阈值，控制动作最短将在一个周期后执行，最长不会超过两个周期。

执行**storm-constrain**与**broadcast-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**、**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。**broadcast-suppression**、**unicast-suppression**命令的详细描述请参见“1.2.1 配置广播/未知单播风暴抑制功能”。

2. 配置以太网接口流量阈值控制功能

表1-15 配置以太网接口流量阈值控制功能

操作	命令	说明
进入系统视图	**system-view**	-
（可选）配置端口流量统计时间间隔	**storm-constrain interval** *interval*	缺省情况下，端口流量统计时间间隔为10秒 为了保持网络状态的稳定，建议设置的流量统计时间间隔不低于10秒
进入以太网接口视图	**interface** *interface-type interface-number*	-
开启端口流量阈值控制功能，并设置上限阈值与下限阈值	**storm-constrain** { **broadcast** | **unicast** } { **pps** | **kbps** | **ratio** } *max-pps-values min-pps-values*	缺省情况下，端口流量阈值控制功能处于关闭状态，即端口不进行流量阈值控制

操作	命令	说明
配置端口流量大于上限阈值的控制动作	**storm-constrain control { block | shutdown }**	缺省情况下，端口不进行流量阈值控制
配置端口流量大于上限阈值或者小于下限阈值时输出Log信息	**storm-constrain enable log**	缺省情况下，端口流量大于上限阈值或者小于下限阈值时输出Log信息
配置端口流量大于上限阈值或者小于下限阈值时输出Trap信息	**storm-constrain enable trap**	缺省情况下，端口流量大于上限阈值或者小于下限阈值时输出Trap信息

1.2.3 配置以太网接口的MDIX模式

说明

光类型接口不支持本特性。

物理以太网接口由 8 个引脚组成。缺省情况下，每个引脚都有专门的作用，例如，使用引脚 1 和 2 接收信号，引脚 3 和 6 发送信号。为了配合以太网接口支持使用直通线缆和交叉线缆，设备实现了三种 MDIX（Media-dependent Interface-crossover）模式：**automdix**、**mdi** 和 **mdix**。通过配置以太网接口的 MDIX 模式，可以改变引脚在通信中的作用：

- 当配置为 **mdix** 模式时，使用引脚 1 和 2 接收信号，使用引脚 3 和 6 发送信号；
- 当配置为 **mdi** 模式时，使用引脚 1 和 2 发送信号，使用引脚 3 和 6 接收信号；
- 当配置为 **automdix** 模式时，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。

说明

物理以太网接口的引脚 4、5、7、8 不受该特性限制。

- 十兆和百兆速率接口，引脚 4、5、7、8 不收发信号。
- 千兆速率及以上接口，引脚 4、5、7、8 用来收发信号。

只有将设备的发送引脚连接到对端的接收引脚后才能正常通信，所以 MDIX 模式需要和两种线缆配合使用。

- 通常情况下，建议用户使用 **automdix** 模式。只有当设备不能获取网线类型参数时，才需要将模式手工指定为 **mdi** 或 **mdix**。
- 当使用直通线缆时，两端设备的 MDIX 模式配置不能相同。
- 当使用交叉线缆时，两端设备的 MDIX 模式配置必须相同或者至少有一端设置为 **automdix** 模式。

表1-16 配置以太网接口的 MDIX 模式

操作	命令	说明
进入系统视图	**system-view**	-
进入以太网接口视图	**interface** *interface-type interface-number*	-
设置以太网接口的MDIX模式	**mdix-mode { automdix | mdi | mdix }**	缺省情况下，以太网接口的MDIX模式为**automdix**

1.2.4 检测以太网接口的连接电缆

设备各款型对于本节所描述的特性支持情况有所不同，详细差异信息如下：

型号	特性	描述
F5000-M06	检测以太网接口的连接电缆	支持
F5000-G20		不支持
F1000-G20/G50/G60/G80		不支持

说明

光口不支持本特性。

通过以下配置任务，用户可以检测设备上以太网接口连接电缆的当前状况，系统将在 5 秒内返回检测结果。检测内容包括电缆的状态以及一些物理参数，同时可以检测出故障线缆的长度。

表1-17 检测以太网接口的连接电缆

操作	命令	说明
进入系统视图	**system-view**	-
进入以太网接口视图	**interface** *interface-type interface-number*	-
对以太网接口连接电缆进行一次检测	**virtual-cable-test**	在以太网接口上执行该操作会使得已经up的链路自动down、up一次

1.3 三层以太网接口/子接口的配置

1.3.1 配置以太网接口/子接口的MTU

修改以太网接口/子接口的 MTU（Maximum Transmission Unit，最大传输单元）值，会影响 IP 报文的分片与重组。一般情况下，不需要改变 MTU 值。

表1-18 配置以太网接口的 MTU

操作	命令	说明
进入系统视图	**system-view**	-
进入以太网接口/子接口视图	**interface** *interface-type* { *interface-number* | *interface-number.subnumber* }	-
设置MTU	**mtu** *size*	缺省情况下，以太网接口的MTU为1500Bytes

1.3.2 配置以太网接口/子接口的MAC地址

当同一网络中不同设备上的三层以太网接口/三层以太网子接口的 MAC 地址相同时，可能会导致设备无法正常通信。此时，可使用本特性，将三层以太网接口/子接口的 MAC 地址修改为其它不冲突的值。

另外，三层以太网子接口时会借用设备上对应的主接口的 MAC 地址作为自己的 MAC 地址。这样，同一个三层以太网接口的所有三层以太子网接口都共用一个 MAC 地址。如果用户需要对个别三层以太网子接口设置不同的 MAC 地址，可使用 **mac-address** 命令。

表1-19 配置三层以太网接口/子接口 MAC 地址

操作	命令	说明
进入系统视图	**system-view**	-
进入接口视图	**interface** *interface-type* { *interface-number* | *interface-number.subnumber* }	-
配置三层以太网接口/子接口MAC地址	**mac-address** *mac-address*	缺省情况下，三层以太网接口的MAC地址与设备的型号有关，请以设备的实际情况为准；三层以太网子接口的缺省MAC与主接口MAC相同 子接口MAC地址配置，不建议使用VRRP协议保留MAC地址段

1.4 以太网接口显示和维护

在完成上述配置后，在任意视图下执行 **display** 命令可以显示配置后接口的运行情况，通过查看显示信息验证配置的效果。

在用户视图下执行 **reset** 命令可以清除接口统计信息。

表1-20 以太网接口显示和维护

操作	命令
显示接口的流量统计信息	**display counters** { **inbound** | **outbound** } **interface** [*interface-type* [*interface-number* | *interface-number.subnumber*]]
显示最近一个抽样间隔内处于up状态的接口的报文速率统计信息	**display counters rate** { **inbound** | **outbound** } **interface** [*interface-type* [*interface-number* | *interface-number.subnumber*]]

操作	命令
显示指定接口当前的运行状态和相关信息	**display interface** [*interface-type* [*interface-number* | *interface-number.subnumber*]] [**brief** [**description** | **down**]]
显示接口丢弃的报文的信息	**display packet-drop** { **interface** [*interface-type* [*interface-number*]] | **summary** }
显示接口流量控制信息	**display storm-constrain** [**broadcast** | **unicast**] [**interface** *interface-type interface-number*]
显示以太网软件模块收发报文的统计信息（分布式设备－独立运行模式/集中式IRF设备）	**display ethernet statistics slot** *slot-number* [**cpu** v*cpu-numbe*]
显示以太网软件模块收发报文的统计信息（分布式设备－IRF模式）	**display ethernet statistics chassis** *chassis-number* **slot** *slot-number* [**cpu** v*cpu-numbe*]
清除指定接口的统计信息	**reset counters interface** [*interface-type* [*interface-number* | *interface-number.subnumber*]]
清除指定接口丢弃报文的统计信息	**reset packet-drop interface** [*interface-type* [*interface-number*]]
清除以太网软件模块收发报文的统计信息（分布式设备－独立运行模式/集中式IRF设备）	**reset ethernet statistics** [**slot** *slot-number* [**cpu** v*cpu-numbe*]]
清除以太网软件模块收发报文的统计信息（分布式设备－IRF模式）	**reset ethernet statistics** [**chassis** *chassis-number* **slot** *slot-number* [**cpu** v*cpu-numbe*]]

目　录

1 LoopBack接口、NULL接口和InLoopBack接口

1.1 LoopBack接口

1.1.1 LoopBack接口简介

LoopBack 接口是一种虚拟接口。LoopBack 接口创建后，除非手工关闭该接口，否则其物理层永远处于 up 状态。鉴于这个特点，LoopBack 接口的应用非常广泛，主要表现在：

- 该接口的地址常被配置为设备产生的 IP 报文的源地址。因为 LoopBack 接口地址稳定且是单播地址，所以通常将 LoopBack 接口地址视为设备的标志。在认证或安全等服务器上设置允许或禁止携带 LoopBack 接口地址的报文通过，就相当于允许或禁止某台设备产生的报文通过，这样可以简化报文过滤规则。但需要注意的是，将 LoopBack 接口地址用于 IP 报文源地址时，需借助路由配置来确保 LoopBack 接口到对端的路由可达。另外，任何送到 LoopBack 接口的 IP 报文都会被认为是送往设备本身的，设备将不再转发这些报文。
- 该接口常用于动态路由协议。比如：在一些动态路由协议中，当没有配置 Router ID 时，将选取所有 LoopBack 接口上数值最大的 IP 地址作为 Router ID；在 BGP 协议中，为了使 BGP 会话不受物理接口故障的影响，可将发送 BGP 报文的源接口配置成 LoopBack 接口。

1.1.2 配置LoopBack接口

表1-1 配置 LoopBack 接口

操作	命令	说明
进入系统视图	**system-view**	-
创建LoopBack接口并进入LoopBack接口视图	**interface loopback** *interface-number*	-
配置接口描述信息	**description** *text*	缺省情况下，接口描述信息为“*接口名* Interface”，比如：LoopBack1 Interface
配置接口的期望带宽	**bandwidth** *bandwidth-value*	缺省情况下，LoopBack接口的期望带宽为0kbit/s
恢复当前接口的缺省配置	**default**	-
开启LoopBack接口	**undo shutdown**	缺省情况下，LoopBack接口创建后永远处于开启状态

1.2 NULL接口

1.2.1 NULL接口简介

NULL 接口是一种虚拟接口。它永远处于 up 状态，但不能转发报文，也不能配置 IP 地址和链路层协议。Null 接口为设备提供了一种过滤报文的简单方法——将不需要的网络流量发送到 NULL 接口，从而免去配置 ACL 的复杂工作。比如，在路由中指定到达某一网段的下一跳为 NULL 接口，则任何送到该网段的网络数据报文都会被丢弃。

1.2.2 配置NULL接口

表1-2 配置 NULL 接口

操作	命令	说明
进入系统视图	**system-view**	-
进入NULL接口视图	**interface null 0**	缺省情况下，设备上已经存在NULL0接口，用户不能创建也不能删除 设备只支持NULL0接口，因此，NULL接口的编号只能是0
配置接口描述信息	**description** *text*	缺省情况下，接口描述信息为NULL0 Interface
恢复当前接口的缺省配置	**default**	-

1.3 InLoopBack接口

InLoopBack 接口是一种虚拟接口。InLoopBack 接口由系统自动创建，用户不能进行配置和删除，但是可以显示，其物理层和链路层协议永远处于 up 状态。InLoopBack 接口主要用于配合实现报文的路由和转发，任何送到 InLoopBack 接口的 IP 报文都会被认为是送往设备本身的，设备将不再转发这些报文。

1.4 LoopBack接口、NULL接口和InLoopBack接口显示和维护

完成上述配置后，在任意视图下执行 **display** 命令可以显示配置后接口的运行情况，通过查看显示信息验证配置的效果。

在用户视图下执行 **reset** 命令可以清除接口统计信息。

表1-3 LoopBack 接口和 NULL 接口显示和维护

操作	命令
显示LoopBack接口的相关信息	**display interface loopback** [*interface-number*] [**brief** [**description** | **down**]]

操作	命令
显示NULL接口的状态信息	**display interface null** [**0**] [**brief** [**description** | **down**]]
显示InLoopBack接口的相关信息	**display interface inloopback** [**0**] [**brief** [**description** | **down**]]
清除LoopBack接口的统计信息	**reset counters interface loopback** [*interface-number*]
清除NULL接口的统计信息	**reset counters interface null** [**0**]

目　录

1 Blade接口

1.1 Blade接口简介

设备各款型对于本节所描述的特性支持情况有所不同，详细差异信息如下：

型号	特性	描述
F5000-M06	Blade接口	支持
F5000-G20		不支持
F1000-G20/G50/G60/G80		不支持

Blade 接口是业务板的一种内部接口，也称为引擎口，用于连接防火墙与业务板，其物理层和链路层协议永远处于 up 状态。防火墙从接口板接收到流量后，根据引流规则，将需要进行安全业务处理的流量通过交换引擎发送到业务板的 Blade 接口，Blade 接口再将数据流量转发给业务板进行处理。经业务板处理后的流量再通过 Blade 接口、交换引擎转发给出接口所在的接口板，由接口板与外接设备进行通信。Blade 接口主要支持如下功能：

- 可进行链路捆绑。多个 Blade 接口捆绑在一起后形成一个引擎聚合组，其对应的聚合接口称为引擎聚合接口。引擎聚合接口的详细介绍请参见“二层技术-以太网交换配置指导”和“二层技术-以太网交换命令参考”中的“以太网链路聚合”。
- 可用于流量重定向。对于收到需要由某个引擎口处理的报文时，可以通过配置流量重定向到此引擎口。流量重定向的详细介绍请参见“ACL 和 QoS 配置指导”中的“流量重定向”。

1.2 Blade接口显示和维护

完成上述配置后，在任意视图下执行 **display** 命令可以显示配置后接口的运行情况，通过查看显示信息验证配置的效果。

在用户视图下执行 **reset** 命令可以清除接口统计信息。

表1-1 Blade 接口显示和维护

操作	命令
显示Blade接口的相关信息	**display interface** [**blade** [*interface-number*]] [**brief**]
清除Blade接口的统计信息	**reset counters interface** [**blade** [*interface-number*]]