H3C SecPath 系列安全产品

命令手册

杭州华三通信技术有限公司

http://www.h3c.com.cn

资料版本：20090812-C-1.07

声明

Copyright ©2006-2009 杭州华三通信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。

H3C、H3C、Aolynk、Aolynk、H^{3}Care、Heare、TOP G、TOPG、IRF、NetPilot、Neocean、NeoVTL、SecPro、SecPoint、SecEngine、SecPath、Comware、Secware、Storware、NQA、VVG、V^{2}G、V^{n}G、PSPT、XGbus、N-Bus、TiGem、InnoVision、HUASAN、华三均为杭州华三通信技术有限公司的商标。对于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。

由于产品版本升级或其他原因，本手册内容有可能变更。H3C 保留在没有任何通知或者提示的情况下对本手册的内容进行修改的权利。本手册仅作为使用指导，H3C 尽全力在本手册中提供准确的信息，但是 H3C 并不确保手册内容完全没有错误，本手册中的所有陈述、信息和建议也不构成任何明示或暗示的担保。

技术支持

用户支持邮箱：customer_service@h3c.com

技术支持热线电话：800-810-0504（固话拨打）

400-810-0504（手机、固话均可拨打）

网址：http://www.h3c.com.cn

相关资料及其获取方式

相关资料

手册名称	用途
《H3C SecPath 系列安全产品操作手册》	该手册介绍了H3C SecPath系列安全网关/防火墙的功能特性、工作原理和配置及操作指导。
《H3C SecPath 系列安全产品Web配置手册》	指导用户通过Web方式对H3C SecPath系列安全网关/防火墙进行配置操作。
《H3C SecPath SSL VPN管理员使用手册》	该手册介绍了H3C SecPath SSL VPN系统的管理员对系统的用户、资源以及各类策略的操作指导。
《H3C SecPath SSL VPN用户使用手册》	该手册介绍了H3C SecPath SSL VPN系统的用户对各类资源的访问方式。

资料获取方式

您可以通过H3C网站（www.h3c.com.cn）获取最新的产品资料：

H3C网站与产品资料相关的主要栏目介绍如下：

- [产品技术]：可以获取产品介绍和技术介绍的文档。
- [解决方案]：可以获取解决方案类资料。
- [服务支持/文档中心]：可以获取安装类、配置类或维护类等产品资料。
- [服务支持/软件下载]：可以获取与软件版本配套的资料。

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！

前 言

本书简介

本手册各章节内容如下：

- **第 1 部分 基础配置。**该部分包括系统基本配置命令、系统维护管理命令、自动侦测配置命令、HWPing 配置命令、SNMP 配置命令、RMON 配置命令、BIMS 配置命令、终端服务配置命令、Modem 配置命令以及接口配置命令，其中系统维护管理命令包括了日志与调试信息中心命令、文件系统与文件操作命令、FTP/TFTP 操作命令、用户界面配置命令、用户管理系统命令和 NTP 配置命令。
- **第 2 部分 用户接入。**该部分包括 PPP 配置命令、PPPoE Server 配置命令和 PPPoE Client 配置命令和 VLAN 配置命令。
- **第 3 部分 网络层协议。**该部分包括 IP 地址的介绍和配置命令、IP 应用配置命令、IP 性能配置命令、IP 单播策略路由的配置命令，还包括安全网关/防火墙作为 DHCP Server、DHCP Client 及 DHCP 中继的配置命令、BOOTP 配置命令、UDP HELPER 配置命令。
- **第 4 部分 路由协议。**该部分包括静态路由、RIP、OSPF、BGP、MBGP 协议配置和路由策略的配置命令。
- **第 5 部分 MPLS。**该部分包括 MPLS 基本能力的配置命令。
- **第 6 部分 VPN。**该部分包括 L2TP 和 GRE 的配置命令，动态 VPN 的配置命令、IPsec 和 IKE 配置命令。
- **第 7 部分 安全。**该部分包括 AAA 及 RADIUS 配置命令、访问控制列表配置命令、包过滤防火墙配置命令、状态防火墙配置命令、网络地址转换配置命令、SSL 和 PKI 配置命令、透明防火墙配置命令、混合模式配置命令、面向对象管理配置命令、Web 和邮件过滤配置命令、攻击防范配置命令、IDS 联动配置命令与报文统计配置命令以及日志维护统计配置命令等。
- **第 8 部分 可靠性。**该部分包括 VRRP 配置命令和双机热备配置命令。
- **第 9 部分 QoS。**该部分包括流分类、流量监管和流量整形的配置命令、拥塞管理配置命令和拥塞避免配置命令。其中拥塞管理配置命令包括 FIFO、PQ、CQ、WFQ、CBQ 和 RTPQ 几种队列机制的配置命令。
- **第 10 部分 附录。**该部分包含本套用户手册中的所有命令，按字母顺序排列，对每条命令指明了该命令所在的功能模块和具体页码，以便于查找。

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 | … }	表示从两个或多个选项中选取一个。
[x | y | …]	表示从两个或多个选项中选取一个或者不选。
{ x | y | … }*	表示从两个或多个选项中选取多个，最少选取一个，最多选取所有选项。
[x | y | …]*	表示从两个或多个选项中选取多个或者不选。
&<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：

⚠ **小心、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。

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。

🕮 **说明、提示、窍门、思考：**对操作内容的描述进行必要的补充和说明。

目 录

第 1 章 基本配置命令 1-1
1.1 基本配置命令 1-1
1.1.1 clock datetime 1-1
1.1.2 clock summer-time 1-1
1.1.3 clock timezone 1-2
1.1.4 command-privilege 1-3
1.1.5 cpu-usage cycle 1-4
1.1.6 display clipboard 1-4
1.1.7 display clock 1-5
1.1.8 display cpu-usage 1-5
1.1.9 display cpu-usage history 1-7
1.1.10 display history-command 1-8
1.1.11 display memory 1-9
1.1.12 display version 1-9
1.1.13 header 1-10
1.1.14 hotkey 1-12
1.1.15 language-mode 1-13
1.1.16 lock 1-14
1.1.17 quit 1-15
1.1.18 return 1-15
1.1.19 super 1-16
1.1.20 super password 1-17
1.1.21 sysname 1-18
1.1.22 system-view 1-18
1.1.23 vrbd 1-19
1.2 命令行别名配置命令 1-19
1.2.1 command-alias enable 1-19
1.2.2 command-alias mapping 1-20
1.2.3 display command-alias 1-21
第 2 章 系统维护管理命令 2-1
2.1 网络测试工具命令 2-1
2.1.1 debugging 2-1
2.1.2 display debugging 2-2
2.1.3 display device 2-2
2.1.4 display diagnostic-information 2-3
2.1.5 display schedule reboot 2-5
2.1.6 ping 2-5
2.1.7 reboot 2-7
2.1.8 remove slot 2-8
2.1.9 schedule reboot at 2-9

2.1.10 schedule reboot delay 2-10
2.1.11 tracert 2-11
2.2 信息处理命令 2-12
2.2.1 display channel 2-12
2.2.2 display info-center 2-14
2.2.3 display logbuffer 2-15
2.2.4 display logbuffer summary 2-17
2.2.5 display trapbuffer 2-18
2.2.6 info-center channel 2-19
2.2.7 info-center console channel 2-20
2.2.8 info-center enable 2-20
2.2.9 info-center logbuffer 2-21
2.2.10 info-center loghost 2-22
2.2.11 info-center loghost source 2-23
2.2.12 info-center monitor channel 2-24
2.2.13 info-center snmp channel 2-24
2.2.14 info-center source 2-25
2.2.15 info-center timestamp 2-27
2.2.16 info-center timestamp loghost 2-28
2.2.17 info-center trapbuffer 2-28
2.2.18 reset logbuffer 2-29
2.2.19 reset trapbuffer 2-29
2.2.20 terminal debugging 2-30
2.2.21 terminal logging 2-30
2.2.22 terminal monitor 2-31
2.2.23 terminal trapping 2-32
2.3 HTTP服务器配置命令 2-32
2.3.1 ip http acl 2-32
2.3.2 ip http shutdown 2-33
第 3 章 自动侦测配置命令 3-1
3.1 自动侦测基本配置命令 3-1
3.1.1 debugging detect-group 3-1
3.1.2 detect-group 3-1
3.1.3 detect-list 3-2
3.1.4 display detect-group 3-3
3.1.5 option 3-4
3.1.6 retry 3-5
3.1.7 timer loop 3-5
3.1.8 timer wait 3-6
3.2 自动侦测应用命令 3-7
3.2.1 ip route-static detect-group 3-7
3.2.2 vrrp vrid track detect-group 3-8
第 4 章 HWPing配置命令 4-1
4.1 HWPing客户端命令 4-1

4.1.1 count 4-1
4.1.2 datafill 4-1
4.1.3 datasize 4-2
4.1.4 debugging hwping 4-3
4.1.5 description 4-3
4.1.6 destination-ip 4-4
4.1.7 destination-port 4-4
4.1.8 display hwping 4-5
4.1.9 filename 4-7
4.1.10 frequency 4-8
4.1.11 ftp-operation 4-8
4.1.12 history-records 4-9
4.1.13 http-operation 4-9
4.1.14 hwping 4-10
4.1.15 hwping-agent enable 4-11
4.1.16 hwping-agent max-requests 4-11
4.1.17 jitter-interval 4-12
4.1.18 jitter-packetnum 4-12
4.1.19 password 4-13
4.1.20 probe-failtimes 4-14
4.1.21 send-trap 4-14
4.1.22 sendpacket passroute 4-15
4.1.23 source-interface 4-16
4.1.24 source-ip 4-16
4.1.25 source-port 4-17
4.1.26 test-type 4-17
4.1.27 test-enable 4-18
4.1.28 test-failtimes 4-19
4.1.29 timeout 4-19
4.1.30 tos 4-20
4.1.31 ttl 4-20
4.1.32 username 4-21
4.1.33 vpninstance 4-22
4.2 HWPing服务器端命令 4-22
4.2.1 hwping-server enable 4-22
4.2.2 hwping-server tcpconnect 4-23
4.2.3 hwping-server udpecho 4-23
第 5 章 文件管理命令 5-1
5.1 文件系统命令 5-1
5.1.1 boot bootrom 5-1
5.1.2 cd 5-1
5.1.3 copy 5-2
5.1.4 delete 5-3
5.1.5 detach 5-4
5.1.6 dir 5-5

5.1.7 execute 5-6
5.1.8 file prompt 5-6
5.1.9 format 5-7
5.1.10 mkdir 5-8
5.1.11 more 5-8
5.1.12 move 5-9
5.1.13 pwd 5-10
5.1.14 rename 5-10
5.1.15 reset recycle-bin 5-11
5.1.16 rmdir 5-12
5.1.17 undelete 5-13
5.1.18 upgrade 5-14
5.2 FTP服务器配置命令 5-15
5.2.1 display ftp-server 5-15
5.2.2 display ftp-user 5-15
5.2.3 display ftp-server source-ip 5-16
5.2.4 ftp server enable 5-16
5.2.5 ftp-server source-interface 5-17
5.2.6 ftp-server source-ip 5-18
5.2.7 ftp timeout 5-18
5.2.8 ftp update 5-19
5.3 FTP客户端命令 5-20
5.3.1 ascii 5-20
5.3.2 binary 5-21
5.3.3 bye 5-21
5.3.4 cd 5-22
5.3.5 cdup 5-22
5.3.6 close 5-23
5.3.7 debugging 5-23
5.3.8 delete 5-24
5.3.9 dir 5-24
5.3.10 disconnect 5-25
5.3.11 display ftp source-ip 5-25
5.3.12 ftp 5-26
5.3.13 ftp source-interface 5-26
5.3.14 ftp source-ip 5-27
5.3.15 get 5-28
5.3.16 lcd 5-28
5.3.17 ls 5-29
5.3.18 mkdir 5-29
5.3.19 open 5-30
5.3.20 passive 5-30
5.3.21 put 5-31
5.3.22 pwd 5-31
5.3.23 quit 5-32

5.3.24 remotehelp 5-32
5.3.25 rename 5-33
5.3.26 rmdir 5-33
5.3.27 user 5-34
5.3.28 verbose 5-34
5.4 TFTP配置命令 5-35
5.4.1 display tftp source-ip 5-35
5.4.2 tftp 5-35
5.4.3 tftp-server acl 5-36
5.4.4 tftp source-interface 5-37
5.4.5 tftp source-ip 5-38
5.5 配置文件管理命令 5-38
5.5.1 display current-configuration 5-38
5.5.2 display saved-configuration 5-41
5.5.3 display startup 5-44
5.5.4 display this 5-44
5.5.5 reset saved-configuration 5-45
5.5.6 save 5-46
5.5.7 startup saved-configuration 5-46
第 6 章 用户界面配置命令 6-1
6.1 用户界面配置命令 6-1
6.1.1 accounting commands scheme 6-1
6.1.2 acl 6-1
6.1.3 authentication-mode 6-2
6.1.4 auto-execute command 6-3
6.1.5 databits 6-4
6.1.6 debugging vty 6-4
6.1.7 display user-interface 6-5
6.1.8 display users 6-6
6.1.9 flow-control 6-7
6.1.10 free user-interface 6-8
6.1.11 history-command max-size 6-8
6.1.12 idle-timeout 6-9
6.1.13 modem 6-10
6.1.14 modem auto-answer 6-10
6.1.15 modem timer answer 6-11
6.1.16 parity 6-11
6.1.17 protocol inbound 6-12
6.1.18 screen-length 6-13
6.1.19 send 6-13
6.1.20 set authentication password 6-14
6.1.21 shell 6-15
6.1.22 speed 6-16
6.1.23 stopbits 6-17
6.1.24 user privilege 6-17

6.1.25 user-interface 6-18
第 7 章 NTP配置命令 7-1
7.1 NTP配置命令 7-1
7.1.1 debugging ntp-service 7-1
7.1.2 display ntp-service sessions 7-2
7.1.3 display ntp-service status 7-3
7.1.4 display ntp-service trace 7-4
7.1.5 ntp-service access 7-5
7.1.6 ntp-service authentication enable 7-6
7.1.7 ntp-service authentication-keyid 7-6
7.1.8 ntp-service broadcast-client 7-7
7.1.9 ntp-service broadcast-server 7-7
7.1.10 ntp-service in-interface disable 7-8
7.1.11 ntp-service max-dynamic-sessions 7-9
7.1.12 ntp-service multicast-client 7-9
7.1.13 ntp-service multicast-server 7-10
7.1.14 ntp-service refclock-master 7-11
7.1.15 ntp-service reliable authentication-keyid 7-11
7.1.16 ntp-service source-interface 7-12
7.1.17 ntp-service unicast-peer 7-13
7.1.18 ntp-service unicast-server 7-14
第 8 章 SNMP配置命令 8-1
8.1 SNMP配置命令 8-1
8.1.1 debugging snmp-agent 8-1
8.1.2 display snmp-agent 8-1
8.1.3 display snmp-agent community 8-2
8.1.4 display snmp-agent group 8-3
8.1.5 display snmp-agent mib-view 8-4
8.1.6 display snmp-agent statistics 8-5
8.1.7 display snmp-agent sys-info 8-7
8.1.8 display snmp-agent usm-user 8-8
8.1.9 enable snmp trap updown 8-9
8.1.10 snmp-agent 8-10
8.1.11 snmp-agent community 8-10
8.1.12 snmp-agent group 8-11
8.1.13 snmp-agent local-engineid 8-13
8.1.14 snmp-agent mib-view 8-13
8.1.15 snmp-agent packet max-size 8-14
8.1.16 snmp-agent sys-info 8-14
8.1.17 snmp-agent target-host 8-15
8.1.18 snmp-agent trap enable 8-17
8.1.19 snmp-agent trap life 8-18
8.1.20 snmp-agent trap queue-size 8-18
8.1.21 snmp-agent trap source 8-19
8.1.22 snmp-agent usm-user 8-20

第 9 章 BIMS配置命令 9-1
9.1 BIMS配置命令 9-1
9.1.1 debugging bims all 9-1
9.1.2 bims boot request 9-3
9.1.3 bims device-id 9-3
9.1.4 bims enable 9-4
9.1.5 bims interval 9-4
9.1.6 bims ip address 9-5
9.1.7 bims request 9-6
9.1.8 bims sharekey 9-6
9.1.9 bims source ip-address 9-7
9.1.10 bims specify-time 9-7
第 10 章 RMON配置命令 10-1
10.1 RMON配置命令 10-1
10.1.1 display rmon alarm 10-1
10.1.2 display rmon event 10-2
10.1.3 display rmon eventlog 10-3
10.1.4 display rmon history 10-3
10.1.5 display rmon prialarm 10-5
10.1.6 display rmon statistics 10-6
10.1.7 rmon alarm 10-7
10.1.8 rmon event 10-8
10.1.9 rmon history 10-9
10.1.10 rmon prialarm 10-9
10.1.11 rmon statistics 10-11
第 11 章 终端服务命令 11-1
11.1 Telnet终端服务配置命令 11-1
11.1.1 debugging telnet 11-1
11.1.2 display tcp status 11-1
11.1.3 display telnet source-ip 11-2
11.1.4 display telnet-server source-ip 11-3
11.1.5 telnet 11-3
11.1.6 telnet source-interface 11-4
11.1.7 telnet source-ip 11-5
11.1.8 telnet-server source-interface 11-5
11.1.9 telnet-server source-ip 11-6
11.2 SSH配置命令 11-7
11.2.1 debugging ssh client 11-7
11.2.2 debugging ssh server 11-7
11.2.3 display rsa local-key-pair public 11-8
11.2.4 display rsa peer-public-key 11-10
11.2.5 display ssh server 11-10
11.2.6 display ssh-server source-ip 11-11
11.2.7 display ssh user-information 11-12

11.2.8 peer-public-key end 11-12
11.2.9 protocol inbound 11-13
11.2.10 public-key-code begin 11-14
11.2.11 public-key-code end 11-14
11.2.12 rsa local-key-pair create 11-15
11.2.13 rsa local-key-pair destroy 11-16
11.2.14 rsa peer-public-key 11-17
11.2.15 ssh authentication-type default 11-18
11.2.16 ssh server authentication-retries 11-18
11.2.17 ssh server compatible-ssh1x enable 11-19
11.2.18 ssh server rekey-interval 11-20
11.2.19 ssh server timeout 11-20
11.2.20 ssh-server source-interface 11-21
11.2.21 ssh-server source-ip 11-21
11.2.22 ssh user 11-22
11.2.23 ssh user assign 11-23
11.2.24 ssh user authentication-type 11-24
11.2.25 ssh user service-type 11-24
11.3 SSH Client配置命令 11-25
11.3.1 display ssh server-info 11-25
11.3.2 display ssh2 source-ip 11-26
11.3.3 quit 11-26
11.3.4 ssh client assign rsa-key 11-27
11.3.5 ssh client first-time enable 11-27
11.3.6 ssh2 11-28
11.3.7 ssh2 source-interface 11-29
11.3.8 ssh2 source-ip 11-30
11.4 SFTP Server配置命令 11-31
11.4.1 sftp server enable 11-31
11.5 SFTP Client配置命令 11-31
11.5.1 bye 11-31
11.5.2 cd 11-32
11.5.3 cdup 11-32
11.5.4 delete 11-33
11.5.5 dir 11-33
11.5.6 display sftp source-ip 11-34
11.5.7 exit 11-34
11.5.8 get 11-35
11.5.9 help 11-35
11.5.10 ls 11-36
11.5.11 mkdir 11-37
11.5.12 put 11-37
11.5.13 pwd 11-38
11.5.14 quit 11-38
11.5.15 remove 11-39

11.5.16 rename 11-39
11.5.17 rmdir 11-40
11.5.18 sftp 11-40
11.5.19 sftp source-interface 11-41
11.5.20 sftp source-ip 11-42
第 12 章 Modem管理配置命令 12-1
12.1 Modem管理配置命令 12-1
12.1.1 debugging modem 12-1
12.1.2 modem 12-1
12.1.3 modem auto-answer 12-2
12.1.4 script-string 12-3
12.1.5 start-script 12-5
第 13 章 接口配置命令 13-1
13.1 接口管理命令 13-1
13.1.1 debugging physical 13-1
13.1.2 description 13-2
13.1.3 display brief interface 13-2
13.1.4 display interface 13-3
13.1.5 flow-interval 13-5
13.1.6 insulate 13-6
13.1.7 interface 13-8
13.1.8 mtu 13-9
13.1.9 reset counters interface 13-10
13.1.10 shutdown 13-10
13.2 Ethernet接口配置命令 13-11
13.2.1 display interface ethernet 13-11
13.2.2 duplex 13-12
13.2.3 flow-control 13-13
13.2.4 loopback (Ethernet/Gigabitethernet Interface) 13-14
13.2.5 promiscuous 13-14
13.2.6 speed 13-15
13.3 AUX口配置命令 13-16
13.3.1 async mode 13-16
13.3.2 detect 13-17
13.3.3 loopback 13-17
13.4 以太网子接口配置命令 13-18
13.4.1 display vlan interface 13-18
13.4.2 display vlan max-packet-process 13-18
13.4.3 display vlan statistics vid 13-19
13.4.4 interface { ethernet | gigabitethernet } 13-19
13.4.5 max-packet-process 13-20
13.4.6 reset vlan statistics vid 13-21
13.4.7 vlan-type dot1q 13-21
13.5 Dialer口配置命令 13-22

13.5.1 interface dialer 13-22
13.5.2 virtualbaudrate 13-22
13.6 虚拟模板接口和虚拟访问接口配置命令 13-25
13.6.1 broadcast-limit link 13-25
13.6.2 display interface virtual-template 13-26
13.6.3 display virtual-access 13-27
13.6.4 interface virtual-template 13-27
13.7 Loopback接口和Null接口配置命令 13-28
13.7.1 display interface looback 13-28
13.7.2 display interface null 13-29
13.7.3 interface loopback 13-29
13.7.4 interface null 13-30

第1章 基本配置命令

1.1 基本配置命令

1.1.1 clock datetime

【命令】

clock datetime *time date*

【视图】

用户视图

【参数】

time：当前时钟，格式为 *HH:MM:SS*，即时/分/秒，*HH* 范围为 0～23，*MM* 和 *SS* 范围为 0～59。

date：当前日期，格式为 *MM/DD/YYYY*（月/日/年）或 *YYYY/MM/DD*（年/月/日），*MM* 范围为 1～12，*DD* 范围为 1～31，*YYYY* 范围为 2000～2099。

【描述】

clock datetime 命令用来设置防火墙当前日期和时钟。

在需要严格获取绝对时间的应用环境中，必须设定防火墙当前日期和时钟。

您在输入设定的时间参数时，可以不输入分和秒。

相关配置可参考命令 **display clock**。

【举例】

设置防火墙当前日期为 2001 年 1 月 1 日 0 时 0 分 0 秒。

```
<H3C> clock datetime 0:0:0 01/01/2001
```

1.1.2 clock summer-time

【命令】

clock summer-time *zone_name* { **one-off** | **repeating** } *start-time start-date end-time end-date add-time*

undo clock summer-time

【视图】

用户视图

【参数】

zone_name：夏令时名称，字符长度范围<1～32>。

one-off：表示仅对某一年的夏令时时间进行设置。

repeating：表示对从某一年开始的以后每年的夏令时时间的设置。

start-time：起始时间，格式为 *HH:MM:SS*（时/分/秒）。

start-date：起始日期，格式为 *MM/DD/YYYY*（月/日/年）或 *YYYY/MM/DD*（年/月/日），*YYYY* 的取值范围为 2000～2099。

end-time：终止时间，格式为 *HH:MM:SS*（时/分/秒）。

end-date：终止日期，格式为 *MM/DD/YYYY*（月/日/年）或 *YYYY/MM/DD*（年/月/日），*YYYY* 的取值范围为 2000～2099。

add-time：夏令时时差，格式为 *HH:MM:SS*（时/分/秒）。

【描述】

clock summer-time 命令用来设置夏令时的名称和起始、终止时间，**undo clock summer-time** 命令用来取消当前设置。

设置生效后，可以用 **display clock** 命令进行查看。另外，日志、debug 等信息时间采用经过时区和夏令时调整过的本地时间。

相关配置可参考命令 **clock timezone**。

【举例】

对 z2 夏令时，从 2002/06/08 的 06:00:00 开始到 2002/09/01 的 06:00:00 结束，时间增加 1 小时。

```
<H3C> clock summer-time z2 one-off 06:00:00 06/08/2002 06:00:00 09/01/2002
01:00:00
```

对 z2 夏令时，从 2002 年开始，每年的 06/08 的 06:00:00 开始到 09/01 的 06:00:00 结束，时间增加 1 小时。

```
<H3C> clock summer-time z2 repeating 06:00:00 06/08/2002 06:00:00 09/01/2002
01:00:00
```

1.1.3 clock timezone

【命令】

clock timezone *zone_name* { **add** | **minus** } *time*

undo clock timezone

【视图】

用户视图

【参数】

zone_name：时区名称，字符长度范围<1～32>。

add：与 UTC 时间比较增加。

minus：与 UTC 时间比较减少。

time：时间（小时/分钟/秒）。

【描述】

clock timezone 命令用来对本地时区信息进行设置，**undo clock timezone** 命令用来将本地时区恢复为缺省的 UTC 时区。

设置生效后，可以用 **display clock** 命令进行查看。另外，日志、debug 等信息时间采用经过时区和夏令时调整过的本地时间。

相关配置可参考命令 **clock summer-time**。

【举例】

设置本地时区名称为 Z5，与 UTC 时间比较增加 5 小时。

```
<H3C> clock timezone z5 add 05:00:00
```

1.1.4 command-privilege

【命令】

command-privilege level *level* **view** *view command-key*

undo command-privilege view *view command-key*

【视图】

系统视图

【参数】

level *level*：命令的优先级，0～3。

view *view*：指定的视图。

command-key：指定视图下需要设置的命令。

【描述】

command-privilege 命令用来设置指定视图内的命令的级别，**undo command-privilege view** 命令用来恢复命令的缺省优先级。

命令权限共分为参观、监控、系统、管理 4 个级别，标识为 0～3。管理员可以根据用户需要分配权限，使其在相应的视图下工作。用户登录时，可以根据用户名对应的权限设置对命令进行操作；也可以根据用户界面（user-interface）自身的权限设置进行操作。如果两者权限发生冲突时，取最小权限。

缺省情况下，**ping、tracert、telnet** 等为参观级（0 级）；**display、debugging** 为监控级（1 级）；配置命令为系统级（2 级）；用户密钥设置、用户界面的验证方式和访问级别、FTP、XMODEM、TFTP 以及文件系统操作的命令为管理级（3 级）。

【举例】

设置“interface”命令的优先级为 0。

```
[H3C] command-privilege level 0 view system interface
```

1.1.5 cpu-usage cycle

【命令】

cpu-usage cycle { **5sec** | **1min** | **5min** | **72min** }

【视图】

系统视图

【参数】

5sec：统计周期为 5 秒。

1min：统计周期为 1 分钟。

5min：统计周期为 5 分钟。

72min：统计周期为 72 分钟。

【描述】

cpu-usage cycle 命令用来设置 CPU 占用率统计的周期。设置的周期不同，使用 **display cpu-usage history** 查询到的统计周期不同。

缺省情况下，统计周期为 60 秒。

【举例】

设置统计周期为 5 秒。

```
[H3C] cpu-usage cycle 5sec
```

1.1.6 display clipboard

【命令】

display clipboard

【视图】

所有视图

【参数】

无

【描述】

display clipboard 命令用来显示剪贴板的内容。

【举例】

查看系统剪贴板的内容。

```
<H3C> display clipboard
-----------------clipboard -----------------
        ip route 10.1.0.0 255.0.0.0 eth 0
```

1.1.7 display clock

【命令】

display clock

【视图】

所有视图

【参数】

无

【描述】

display clock 命令用来显示系统当前日期和时钟。

用户可以通过该命令查看系统日期和时钟，如果发现系统时间有误，可及时调整。

相关配置可参考命令 **clock datetime**。

【举例】

查看系统当前日期和时间。

```
<H3C> display clock
15:50:45 UTC Mon 02/12/2003
```

1.1.8 display cpu-usage

【命令】

display cpu-usage [**configuration** | *number* [*offset*] [**verbose**] [**from-device**]]

【视图】

所有视图

【参数】

configuration：查看 CPU 占用率统计的配置信息，包括 CPU 占用率统计是否打开、统计周期以及 CPU 占用率告警阈值。

number：查询 CPU 占用率统计信息的个数。

offset：起始显示条目序号到最新条目序号之间的偏移量。

verbose：查询详细信息。

from-device：查看外部存储设备中保存的信息（flash，硬盘等）（暂不支持）。

【描述】

display cpu-usage 命令用来显示 CPU 占用率的统计信息。

只配 **display cpu-usage** 等价于 **display cpu-usage 1 0 verbose**，显示最近一次 CPU 占用率统计的详细信息。

【举例】

显示 CPU 占用率统计信息的详细信息。

```
[H3C] display cpu-usage
===== Current CPU usage info =====
CPU Usage Stat. Cycle: 1 (Second)
CPU Usage            : 1%
CPU Usage Stat. Time : 2004-09-15  15:51:48
CPU Usage Stat. Tick : 0x27(CPU Tick High) 0x88cf18e4(CPU Tick Low)
Actual Stat. Cycle   : 0x0(CPU Tick High) 0x2264cc2(CPU Tick Low)

TaskName        CPU        Runtime(CPU Tick High/CPU Tick Low)
VIDL            99%               0/ 222de39
TICK             0%               0/    88d8
 co0             0%               0/     6e5
 SRM             0%               0/     1da
ROUT             0%               0/    1d6c
SOCK             0%               0/    3c65
VTYD             0%               0/    1074
IPSP             0%               0/     28b
 TAC             0%               0/    15ac
  SC             0%               0/    10de
 RDS             0%               0/     e71
 ACM             0%               0/    180a
LSSO             0%               0/     3a2
TRAP             0%               0/     2d0
NTPT             0%               0/   1082a
PIMT             0%               0/     2f8
```

```
LSPM              0%              0/     90c
 L2V              0%              0/    1066
 IPS              0%              0/    7575
 SIP              0%              0/    6b87
DHCP              0%              0/     33d
 HOT              0%              0/     fca
DHCC              0%              0/     414
```

1.1.9 display cpu-usage history

【命令】

display cpu-usage history [**task** *task-id*]

【视图】

所有视图

【参数】

task *task-id*：指定任务 ID。

【描述】

display cpu-usage history 命令用来以图形方式显示 CPU 占用率统计历史信息。不指定参数时显示整个系统的 CPU 占用率统计信息。

【举例】

显示整个系统的 CPU 占用率统计信息。

```
[H3C] display cpu-usage history
 100%|
 95%|
 90%|
 85%|
 80%|
 75%|
 70%|
 65%|
 60%|
 55%|
 50%|
 45%|
 40%|
 35%|
 30%|
 25%|
```

```
 20%|
 15%|
 10%|
  5%|
     ------------------------------------------------------------
               10        20        30        40        50        60  (minutes)
                       cpu-usage last 60 minutes(SYSTEM)
```

显示 task 6 的 CPU 占用率统计信息。

```
[H3C] display cpu-usage history task 6
 100%|
 95%|
 90%|
 85%|
 80%|
 75%|
 70%|
 65%|
 60%|
 55%|
 50%|
 45%|
 40%|
 35%|
 30%|
 25%|
 20%|
 15%|
 10%|
  5%|
     ------------------------------------------------------------
               10        20        30        40        50        60  (minutes)
                       cpu-usage last 60 minutes(T03M)
```

1.1.10 display history-command

【命令】

display history-command

【视图】

所有视图

【参数】

无

【描述】

display history-command 命令用来显示历史命令。

终端将用户键入的历史命令自动保存，即记录用户在键盘上的任何输入，以回车为一个单位，您可以通过 **display history-command** 查看保存的历史命令。

【举例】

显示历史命令。

```
<H3C> display history-command
display interface
displayinterface e 1/0/0
interface e 1/0/0
```

1.1.11 display memory

【命令】

display memory [**limit**]

【视图】

所有视图

【参数】

limit：显示内存使用限制信息。

【描述】

display memory 命令用来显示系统内存使用情况。

【举例】

显示当前系统内存使用情况。

```
<H3C> display memory
System Available Memory(bytes): 449691264
System Used Memory(bytes): 188857760
Used Rate: 41%
```

1.1.12 display version

【命令】

display version

【视图】

所有视图

【参数】

无

【描述】

display version 命令用来显示系统版本信息。

通过查看版本信息，可以获知系统当前使用的软件版本、BootRom 版本、CPU 类型、SDRAM 和 Flash 等相关信息。

【举例】

显示系统版本信息。

```
<H3C> display version
 H3C Comware Platform Software
 Comware software, Version , V1.00
 Copyright (c) 2004-2007 Hangzhou H3C Technologies Co., Ltd.
 All rights reserved.
 Without the owner's prior written consent, no decompiling
 nor reverse-engineering shall be allowed.
 H3C SecPath F1000-S uptime is 0 week, 0 day, 1 hour, 45 minutes

  CPU type: Mips BCM1125H 600MHz
  512M bytes DDR SDRAM Memory
  16M bytes Flash Memory
  Pcb      Version:2.0
  Logic    Version:1.0
  BootROM  Version:1.17
  [SLOT 0] 2GBE     (Hardware)2.0, (Driver)2.0, (Cpld)1.0
  [SLOT 1] 2GBE     (Hardware)2.0, (Driver)2.0, (Cpld)1.0
  [SLOT 2] NDEC     (Hardware)2.0, (Driver)3.3, (Cpld)1.0
```

1.1.13 header

【命令】

header [**incoming** | **login** | **shell**] *text*

undo header { **incoming** | **login** | **shell** }

【视图】

系统视图

【参数】

incoming：登录终端用户界面时的提示信息。

login：登录验证时的提示信息。

shell：进入用户视图时的提示信息。

text：提示信息内容。当 **login**、**shell**、**incoming** 没有配置时，缺省为登录信息 login 的内容。系统支持两种输入方式：一种方式为所有内容在同一行输入，此时包括命令关键字在内总共可以输入 255 个字符；另一种方式为所有内容可以通过按<回车>键分多行输入，此时不包括命令关键字在内总共可以输入 1004 个字符（包括不可见字符）。标题内容以第一个英文字符作为起始和结束符，输入结束符后，按<回车>键退出交互过程。

【描述】

header 命令用来设置提示信息，**undo header** 命令用来关闭提示信息。

文本是以第一个英文字符作为起始和结束符。输入结束符后，系统自动退出交互过程。若 *text* 前不指定参数，则缺省为设置登录验证时的提示信息（**login**）

【举例】

配置进入用户视图的提示信息。

```
[H3C] header shell %SHELL : Hello! Welcome use SecPath.%
[H3C]
```

说明：“%”为 TEXT 的起始字符，也将是结束字符，故再次输入“%”时表示文本结束，退出 header 命令。

测试以上设置。

```
[H3C] quit
<H3C> quit
******************************************************************************
* Copyright(c) 2004-2007 Hangzhou H3C Technologies Co., Ltd.                 *
* Without the owner's prior written consent,                                 *
* no decompiling or reverse-engineering shall be allowed.                    *
******************************************************************************

User interface con0 is available.



Please press ENTER.

SHELL : Hello! Welcome use SecPath.
<H3C>
```

1.1.14 hotkey

【命令】

hotkey { **CTRL_G** | **CTRL_L** | **CTRL_O** | **CTRL_T** | **CTRL_U** } *command_text*

undo hotkey { **CTRL_G** | **CTRL_L** | **CTRL_O** | **CTRL_T** | **CTRL_U** }

【视图】

系统视图

【参数】

CTRL_G：表示为快捷键“CTRL+G”指定一条命令。

CTRL_L：表示为快捷键“CTRL+L”指定一条命令。

CTRL_O：表示为快捷键“CTRL+O”指定一条命令。

CTRL_T：表示为快捷键“CTRL+T”指定一条命令。

CTRL_U：表示为快捷键“CTRL+U”指定一条命令。

command_text：为快捷键关联的命令行。

【描述】

hotkey 命令用来为某一快捷键指定相应的命令行。**undo hotkey** 命令用来恢复系统的默认值。

缺省情况下，系统给 CTRL_G、CTRL_L、CTRL_O 三个快捷键指定了默认值，其它快捷键默认值为空。CTRL_G、CTRL_L、CTRL_O 三个快捷键的含义分别为：

CTRL_G 对应命令 **display current-configuration**（显示当前配置）；

CTRL_L 对应命令 **display ip routing-table**（显示路由表信息）；

CTRL_O 对应命令 **undo debugging all**（停止所有调试信息的输出）。

但是用户完全可以根据自己的需要改变它们的定义。

【举例】

将命令 **display tcp status** 与快捷键 CTRL_T 关联。

```
[H3C] hotkey CTRL_T display tcp status
[H3C] display hotkey
----------------- HOTKEY -----------------

            =Defined hotkeys=
Hotkeys Command
CTRL_G  display current-configuration
CTRL_L  display ip routing-table
CTRL_O  undo debug all
```

```
CTRL_T  display tcp status
           =Undefined hotkeys=
Hotkeys Command
CTRL_U  NULL

            =System hotkeys=
Hotkeys Function
CTRL_A  Move the cursor to the beginning of the current line.
CTRL_B  Move the cursor one character left.
CTRL_C  Stop current command function.
CTRL_D  Erase current character.
CTRL_E  Move the cursor to the end of the current line.
CTRL_F  Move the cursor one character right.
CTRL_H  Erase the character left of the cursor.
CTRL_K  Kill outgoing connection.
CTRL_N  Display the next command from the history buffer.
CTRL_P  Display the previous command from the history buffer.
CTRL_R  Redisplay the current line.
CTRL_V  Paste text from the clipboard.
CTRL_W  Delete the word left of the cursor.
CTRL_X  Delete all characters up to the cursor.
CTRL_Y  Delete all characters after the cursor.
CTRL_Z  Return to the user view.
CTRL_]  Kill incoming connection or redirect connection.
ESC_B   Move the cursor one word back.
ESC_D   Delete remainder of word.
ESC_F   Move the cursor forward one word.
ESC_N   Move the cursor down a line.
ESC_P   Move the cursor up a line.
ESC_<   Specify the beginning of clipboard.
ESC_>   Specify the end of clipboard.
```

1.1.15 language-mode

【命令】

language-mode { **chinese** | **english** }

【视图】

用户视图

【参数】

chinese：中文模式。

english：英文模式。

【描述】

language-mode 命令用来切换命令行接口的语言模式。

缺省情况下，为英文模式。

为了方便国内广大用户，系统命令行接口除支持英文模式外还支持中文模式。

【举例】

将英文模式切换为中文模式。

```
<H3C> language-mode chinese
Change language mode, confirm? [Y/N]y
% 改变到中文模式。
```

1.1.16 lock

【命令】

lock

【视图】

用户视图

【参数】

无

【描述】

lock 命令用来锁住当前用户界面，防止未授权的用户操作该终端界面。

用户界面包括 Console 口、AUX 口以及 VTY 虚拟终端等用户界面。

用户输入 **lock** 命令后，系统提示输入屏保密码，并提示再次输入屏保密码，如果两次输入的密码相同，那么锁定成功。之后，如果您想进入系统，必须先按回车，此时，提示输入密码，输入刚才配置的密码后，才可以结束锁定进入系统。

【举例】

用户从 Console 口登录，锁住当前用户界面。

```
<H3C> lock
Password：
Again：
```

1.1.17 quit

【命令】

quit

【视图】

所有视图

【参数】

无

【描述】

quit 命令用来使用户从当前视图退回到较低级别视图，如果是用户视图，则退出系统。

视图分为三个级别，由低到高分别为：

- 用户视图（用户级别为 0）
- 系统视图（用户级别为 3）
- 配置视图（路由协议视图、接口视图、L2TP 组视图等等）

相关配置可参考命令 **return**。

【举例】

从接口 Ethernet1/0/0 视图返回到系统视图，再返回到用户视图。

```
[H3C-Ethernet1/0/0] quit
[H3C] quit
<H3C>
```

1.1.18 return

【命令】

return

【视图】

除用户视图外的所有视图

【参数】

无

【描述】

return 命令用来退回到用户视图，与 **return** 命令功能相同的是快捷键<Ctrl+Z>。

相关配置可参考命令 **quit**。

【举例】

从系统视图返回到用户视图。

```
[H3C] return
<H3C>
```

1.1.19 super

【命令】

super [*level*]

【视图】

用户视图

【参数】

level：用户的级别，为 0～3。

【描述】

super 命令用来使用户从当前级别切换到指定的级别。

用户级别指登录用户的分类，共划分为 4 个级别，与命令级别对应，不同级别的用户登录后，只能使用等于或低于自己级别的命令。

命令的级别分为参观级、监控级、系统级、管理级，简介如下：

- 参观级：网络诊断工具命令（**ping**、**tracert**）、从本设备出发访问外部设备的命令（包括：Telnet 客户端、SSH 客户端、RLOGIN）等，该级别命令不允许进行配置文件保存的操作。
- 监控级：用于系统维护、业务故障诊断等，包括 **display**、**debugging** 命令，该级别命令不允许进行配置文件保存的操作。
- 系统级：业务配置命令，包括路由、各个网络层次的命令，这些用于向用户提供直接网络服务。
- 管理级：关系到系统基本运行、系统支撑模块的命令，这些命令对业务提供支撑作用，包括文件系统、FTP、TFTP、XModem 下载、用户管理命令、级别设置命令、系统内部参数设置命令（非协议规定、非 RFC 规定）等。

为了防止未授权用户的非法侵入，在从低级别用户切换到高级别用户时，要进行用户身份验证，即需要输入高级别用户口令（如果用户设置了 **super password** [**level** *user-level*] { **simple** | **cipher** } *line*）。为了保密，用户键入的口令在屏幕上不作显示，如果三次以内输入正确的口令，则切换到高级别用户，否则保持原用户级别不变。

缺省情况下，若不指定级别，则切换到 3 级。

相关配置可参考命令 **super password**。

【举例】

```
<H3C> super 3
 Password:
User privilege level is 3, and only those commands can be used
whose level is equal or less than this.
Privilege note: 0-VISIT, 1-MONITOR, 2-SYSTEM, 3-MANAGE
```

1.1.20 super password

【命令】

super password [**level** *user-level*] { **simple** | **cipher** } *password*

undo super password [**level** *user-level*]

【视图】

系统视图

【参数】

user-level：用户的级别，为 1～3。

simple *password*：配置明文密码。明文密码是长度小于等于 16 的连续字符串，如 1234567。

cipher *password*：配置密文密码。密文密码有两种配置方式，一种为明文配置方式，为用户自定义的长度小于等于 16 的字符串，由系统自动生成对应的密文密码（如用户输入 123，系统自动生成密文密码 7-CZB#/YX]KQ=^Q`MAF4<1!!）；另一种为密文配置方式，直接输入长度为 24 的密文密码，如 7-CZB#/YX]KQ=^Q`MAF4<1!!。因无论采用哪种方式配置密文密码，验证时均需要输入明文密码，故建议用户采用前一种方式进行配置。

【描述】

super password 命令用来设置切换低级别用户到高级别（*user-level*）用户的密码，**undo super password** 命令用来取消当前设置。

缺省情况下，若不指定级别，则设置的为切换到 3 级的密码。

【举例】

配置升级用户权限至 level 3 时的口令为 zbr。

```
[H3C] super password level 3 simple zbr
```

1.1.21 sysname

【命令】

sysname sys*name*

【视图】

系统视图

【参数】

sysname：防火墙名称，字符串，范围为 1～30 个字符。

【描述】

sysname 命令用来设置防火墙的名称。

缺省情况下，防火墙名称为 H3C。

修改防火墙的名称将影响命令行接口的提示符，如防火墙的名称为 SecPath，用户视图的提示符为<SecPath>。

【举例】

设置防火墙的名称为 gateway。

```
[H3C] sysname gateway
[gateway]
```

1.1.22 system-view

【命令】

system-view

【视图】

用户视图

【参数】

无

【描述】

system-view 命令用来使用户从用户视图进入系统视图。

相关配置可参考命令 **quit**，**return**。

【举例】

```
<H3C> system-view
 System View: return to User View with Ctrl+Z.
```

```
[H3C]
```

1.1.23 vrbd

【命令】

vrbd

【视图】

所有视图

【参数】

无

【描述】

vrbd 命令用来显示详细的软件版本信息，主要包括产品软件版本及相应的平台软件版本信息。

【举例】

显示内部版本信息。

```
[H3C] vrbd
Routing Platform Software
Version SecPath 1000F 8042V100R002B02D006SP02 (COMWAREV300R002B14D006),
RELEASE SOFTWARE
Compiled Jul 18 2005 18:29:20 by xiedong
```

1.2 命令行别名配置命令

1.2.1 command-alias enable

【命令】

command-alias enable

undo command-alias enable

【视图】

系统视图

【参数】

无

【描述】

command-alias enable 命令用来使能命令行别名的功能。**undo command-alias enable** 命令用来关闭命令行别名的功能。

缺省情况下，关闭命令行别名的功能。

【举例】

使能命令行别名的功能。

```
[H3C] command-alias enable
```

关闭命令行别名的功能。

```
[H3C] undo command-alias enable
```

1.2.2 command-alias mapping

【命令】

command-alias mapping *cmdkey alias*

undo command-alias mapping *alias*

【视图】

系统视图

【参数】

cmdkey：用以被别名替代的现有的某个命令的第一关键字。要求一定输入完整的关键字名。

alias：用户设置的别名。要求该别名不能与已有第一关键字冲突（即完全匹配）。

【描述】

command-alias mapping 命令用来配置用户指定的命令行别名，**undo command-alias mapping** 命令用来取消用户设置的别名。

缺省情况下，没有配置命令行别名。

【举例】

配置关键字 display 的别名为 show。

```
[H3C] command-alias mapping display show
```

取消别名 show。

```
[H3C] undo command-alias mapping show
```

1.2.3 display command-alias

【命令】

display command-alias

【视图】

所有视图

【参数】

无

【描述】

display command-alias 命令用来显示当前用户设置别名的情况。

【举例】

显示当前用户设置别名的情况。

```
[H3C] display command-alias
Command alias is enabled
index alias                command key
1     show                 display
```

第2章 系统维护管理命令

2.1 网络测试工具命令

2.1.1 debugging

【命令】

debugging { **all** [**timeout** *minutes*] | *module-name* [*debug-option1*] [*debug-option2*] …}

undo debugging { **all** | *module-name* [*debug-option1*] [*debug-option2*] … }

【视图】

用户视图

【参数】

all：表示打开或关闭全部调试开关。

timeout *minutes*：**debugging all** 命令的有效时长，取值范围为 1～1440 分钟。

module-name：模块名。

debug-option：调试选项。

【描述】

debugging 命令用来打开系统调试开关，**undo debugging** 命令用来关闭系统调试开关。

缺省情况下，系统关闭全部调试开关。

防火墙提供种类丰富的调试功能，一般用于技术支持人员和资深维护人员进行网络故障诊断。

由于打开调试开关，会产生大量的调试信息，导致系统效率的降低，尤其在执行 **debugging all** 命令打开全部调试开关后，可能会引起网络系统瘫痪，建议不要使用 **debugging all** 命令，而 **undo debugging all** 命令却给用户带来极大方便，可以一次关闭全部调试开关，不必去一一关闭。

相关配置可参考命令 **display debugging**。

【举例】

打开 IP Packet 调试开关。

```
<H3C> debugging ip packet
```

2.1.2 display debugging

【命令】

display debugging [**interface** *interface-type interface-number*] [*module-name*]

【视图】

所有视图

【参数】

module-name：模块名。

interface-type：接口类型。

interface-number：接口编号。

【描述】

display debugging 命令用来显示已经打开的调试开关。

缺省情况下，不带任何参数显示所有打开的调试开关。

相关配置可参考命令 **debugging**。

【举例】

显示所有打开的调试开关。

```
<H3C> display debugging
IP packet debugging is on.
```

2.1.3 display device

【命令】

display device [*slot-id*]

【视图】

任意视图

【参数】

slot-id：指定的槽位号。

【描述】

display device 命令用来显示设备和插卡的状态信息。若指定 *slot-id*，将显示指定槽位的信息，否则显示所有设备信息。

【举例】

显示设备和插卡的状态信息。

```
<H3C> display device
Slot #    Type        Online    Status
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
0         2GBE        Present   Normal
1         2FE         Present   Normal
```

2.1.4 display diagnostic-information

【命令】

display diagnostic-information

【视图】

所有视图

【参数】

无

【描述】

display diagnostic-information 命令用来显示系统当前各模块的运行信息。

在系统出现故障时，为了便于问题定位，需要收集很多的信息，但相应的 **display** 命令很多，很难一次把信息收集全，这时，可以使用 **display diagnostic-information** 命令，进行系统当前各个模块的运行信息收集。

【举例】

显示技术支持信息

```
<H3C> display diagnostic-information
==================================================
  ===============display clock===============
==================================================
14:04:23 UTC Thu 09/16/2004

==================================================
  ===============display version====
==================================================
… …

==========================
  ===============vrbd===============
========================================
… …

==================================================
```

```
  ===============display device===============
================================================
… …
================================================================
===============display current-configuration===============
================================================================
… …

================================================================
  ===============display saved-configuration=====
================================================================
… …

=========================================================
  ===============display interface===============
=========================================================
… …

=========================================================
  ===============display ip interface===============
=========================================================
… …

=========================================================
  ===============display ip statistics===============
=========================================================
… …

=========================================================
  ===============display exception 20===============
=========================================================
… …

================================================================
  ===============display exception 3 verbose===============
================================================================

=========================================================
  ===============display logbuffer===============
=========================================================
… …
```

其中详细的显示内容略。

2.1.5 display schedule reboot

【命令】

display schedule reboot

【视图】

任意视图

【参数】

无

【描述】

display schedule reboot 命令用来查看系统定时重启功能的配置信息。

相关配置可参考命令 **reboot**、**schedule reboot at**、**schedule reboot delay**

【举例】

显示当前的 **schedule reboot** 终端服务参数设置

```
<H3C> display schedule reboot
```

2.1.6 ping

【命令】

ping [**-a** *X.X.X.X* | **-c** *count* | **-d** | **-f** | **-h** *ttl_value* | **-i** { *interface-type interface-number* } | **ip** | **-n** | **-p** *pattern* | **-q** | **-r** | **-s** *packetsize* | **-t** *timeout* | **-tos** | **-v** | **-vpn-instance** *vpn-instance-name*] * *host*

【视图】

所有视图

【参数】

-a *X.X.X.X*：设置发送 ICMP ECHO-REQUEST 报文的源 IP 地址。

-c *count*：发送 ICMP ECHO-REQUEST 报文次数，范围 1～4294967295。

-d：设置 socket 为 DEBUG 模式。

-f：当数据包长度大于接口 MTU 时不被分片，直接丢弃。

-h *ttl_value*：设置 TTL_value 的值，范围 1～255。

-i：设置发送 ICMP ECHO-REQUEST 报文的接口。将报文的 ttl 设为 1，用来测试直连设备。**-i** 选项和**-vpn-instance** 选项不能同时使用。

interface-type：接口类型。

interface-number：接口号。

-**n**：将 host 参数直接作为 IP 地址，而不需作域名解析。

-**p** *pattern*：为 ICMP ECHO-REQUEST 报文填充字节，格式为 16 进制，范围为<0-FFFFFFFF>，如-**p** ff 将报文全部填充为 ff。

-**q**：除统计数字外，不显示其它详细信息。

-**r**：记录路由。

-**s** *packetsize*：ECHO-REQUEST 报文数据字段的长度（不包括 IP 和 ICMP 报文头），以字节为单位，范围为<20～32000>。当数据包长度大于接口 MTU 时被自动分片发送。

-**t** *timeout*：为发送完 ECHO-REQUEST 后，等待 ECHO-RESPONSE 的超时时间，以 ms 为单位，范围为<0～65535>。

-**tos**：ECHO-REQUEST 报文的 TOS 值。

-**v**：显示接收到的非 ECHO-RESPONSE 的其它 ICMP 报文。

-**vpn-instance** *vpn-instance-name*：设置 MPLS VPN 的 *vpn-instance* name，指明本次 Ping 命令配置的 VPN 属性，即关联的 *vpn-instance* 的名称，而且必须是本地创建的 *vpn-instance*。-**i** 选项和-**vpn-instance** 选项不能同时使用。

host：目的主机名或 IP 地址。

ip：使用 IP 协议。

【描述】

ping 命令用来检查 IP 网络连接及主机是否可达。

上述各项参数没有指定时，缺省情况为：

发送 ECHO-REQUEST 的报文次数缺省为 5 次。

socket 为非 DEBUG 模式。

host 首先被当作 IP 地址，如果不是 IP 地址则进行域名解析。

缺省填充方式为从 0x00 开始，逐渐递增至 0xff 后，重复从 0x00 开始填充。

缺省为显示包括统计信息在内的全部信息。

缺省不记录路由。

ECHO-REQUEST 的缺省报文长度为 56 字节。

等待 ECHO-RESPONSE 报文的缺省超时时间为 2000ms。

缺省不显示其它非 ECHO-RESPONSE 的 ICMP 报文。

ping 执行过程为，向目的地发送 ICMP ECHO-REQUEST 报文，如果到目的地网络连接工作正常，则目的地主机接收到 ICMP ECHO-REQUEST 报文后，向源主机响应 ICMP ECHO-REPLY 报文。

可以用 **ping** 命令测试网络连接是否出现故障或网络线路质量等，其输出信息包括：

目的地对每个 ECHO-REQUEST 报文的响应情况。如果在超时时间内没有收到响应报文，则输出“Request time out.”；否则，显示响应报文的字节数、报文序号、TTL 和响应时间等。

最后的统计信息，包括发送报文个数、接收到响应报文个数、未响应报文数百分比和响应时间的最小、最大和平均值。

如果网络传输速度较慢，可以适当加大等待响应报文的超时时间。

相关配置可参考命令 **tracert**。

【举例】

检查 IP 地址为 202.38.160.244 的主机是否可达。

```
<H3C> ping 202.38.160.244
ping 202.38.160.244 : 56 data bytes , press CTRL_C to break
Reply from 202.38.160.244 : bytes=56 sequence=1 ttl=255 time = 1ms
Reply from 202.38.160.244 : bytes=56 sequence=2 ttl=255 time = 2ms
Reply from 202.38.160.244 : bytes=56 sequence=3 ttl=255 time = 1ms
Reply from 202.38.160.244 : bytes=56 sequence=4 ttl=255 time = 3ms
Reply from 202.38.160.244 : bytes=56 sequence=5 ttl=255 time = 2ms
--202.38.160.244 ping statistics--
5 packet(s) transmitted
5 packet(s) received
0.00% packet loss
round-trip min/avg/max = 1/2/3 ms
```

2.1.7 reboot

【命令】

reboot

【视图】

用户视图

【参数】

无

【描述】

reboot 命令用来重启防火墙。

该命令功能与防火墙关闭电源再上电效果相同，但在对防火墙远程维护时，不需用户到防火墙所在地重启防火墙，而直接在远程即可重启防火墙。

在一般情况下，禁止使用该命令，因为它将导致网络工作在短时间内被中断；另外，在重启防火墙时，要确认防火墙配置文件是否需要保存。

【举例】

重新启动防火墙。

```
<H3C> reboot
This command will reboot the system. The current configuration has not been
saved and will be lost if you continue. Continue? [Y/N]
```

2.1.8 remove slot

【命令】

remove slot *slot-id*

undo remove slot *slot-id*

【视图】

用户视图

【参数】

slot-id：插卡所在的槽位号。

【描述】

remove slot 命令用来对槽位中的插卡进行拔出预处理操作，**undo remove slot** 命令用来取消对插卡的拔出预处理操作，恢复该插卡的原状态。

缺省情况下，未对插卡进行拔出预处理操作。

⚠ 注意：

- 若在拔出插卡前，未使用 **remove slot** 命令对插卡进行拔出预处理操作，则设备可能会出现异常。
- 系统启动过程中，请勿进行插卡的插拔操作。
- 当前静态路由不支持插卡热插拔事件，即拔掉插卡后，相应的静态路由仍然存在，需要手工删除。
- 当前 **ftp source-interface** 命令、**ftp-server source-interface** 命令、**tftp source-interface** 命令、**telnet source-interface** 命令、**telnet-server source-interface** 命令、**ssh-server source-interface** 命令、**ssh2 source-interface** 命令、**sftp source-interface** 命令、Tunnel 接口下的 **source** 命令、HWPing 测试组视图下的 **source-interface** 命令、BGP 的 **peer connect-interface** 命令、路由策略视图下的 **if-match interface** 命令和 **apply output-interface** 命令不支持插卡热插拔事件，即拔掉插卡后，相应的配置仍然存在，需要手工删除。
- 目前，热插拔支持的插卡包括 1FE、2FE、4FE、1GBE、2GBE、1GEF、2GEF 插卡，不支持加密卡等其他类型的 PCI 插卡。

【举例】

对 1 号槽位中的插卡进行拔出预处理操作。

```
<H3C> remove slot 1
```

2.1.9 schedule reboot at

【命令】

schedule reboot at *time* [*date*]

undo schedule reboot

【视图】

用户视图

【参数】

time：重新启动时间，格式为 *hh:mm*，即几点几分。其中 *hh* 取值范围为 0～23，*mm* 取值范围为 0～59。

date：重新启动日期，格式为 *mm/dd/yyyy* 或 *yyyy/mm/dd*，即月/日/年或年/月/日。其中 *mm* 的取值范围为 1～12；*dd* 的取值与具体月份相关；*yyyy* 的取值范围为 2000～2099。

【描述】

schedule reboot at 命令用来使能定时重启功能，并设置具体的重启日期和时间。**undo schedule reboot** 命令用来取消定时重启功能。

缺省情况下，未配置定时重启功能。

如果 **schedule reboot at** 命令设置了具体的日期（年月日）参数，而且参数表示的是将来的日期，则系统将在设定的时间点重新启动，误差在 1 分钟左右。

如果没有指定具体的日期参数，分为两种情况：1）设置的时间点在当前时间之后，系统在当天的该时间点重新启动；2）设置的时间点在当前时间之前，系统在第二天的该时间点重新启动。

设置的日期与当前日期相比，不能大于 30 天。配置该命令后，如果以前有相应的设置，则直接覆盖原有信息。

使用 **schedule reboot at** 命令设置系统的重启日期和时间后，若通过 **clock** 或 NTP 等方式修改了系统的时间，则 **schedule reboot at** 的设置将失效。

配置了 **schedule reboot at** 命令之后，将启动一个定时器，这个定时器是以分钟为单位的循环定时器。因此如果在 12：05：26 设置了 12：06 重启，将在 12：06：26 秒重启，而不是 12：06：00 重启。

相关配置可参考命令 **reboot**、**schedule reboot delay**、**display schedule reboot**。

【举例】

当前时间为 15：50，设置系统在当天晚上 22：00 重新启动。

```
<H3C> schedule reboot at 22:00
```

2.1.10 schedule reboot delay

【命令】

schedule reboot delay { *time* | *minutes* }

undo schedule reboot

【视图】

用户视图

【参数】

time：重新启动的等待时延，格式为“小时：分钟”，小时的取值范围为 0～720；分钟的取值范围为 0～59。

minutes：重新启动的等待时延，格式为“绝对分钟数”，取值范围为 0～43200。

【描述】

schedule reboot delay 命令用来使能定时重启功能，并设定等待时延。**undo schedule reboot** 命令用来取消定时重启功能。

缺省情况下，未配置定时重启功能。

可以用两种格式来设置定时重启的等待时延，即“小时：分钟”和“绝对分钟数”。但总的分钟数要小于等于 30×24×60 分钟，即不能大于 30 天。

使用 **schedule reboot at** 命令设置系统的重启日期和时间后，若通过 **clock** 或 NTP 等方式修改了系统的时间，则 **schedule reboot at** 的设置将失效。

配置了 **schedule reboot at** 命令之后，将启动一个定时器，这个定时器是以分钟为单位的循环定时器。因此如果在 12：05：26 设置了 12：06 重启，将在 12：06：26 秒重启，而不是 12：06：00 重启。

相关配置可参考命令 **reboot**、**schedule reboot at**、**display schedule reboot**。

【举例】

当前时间是 21：32，配置系统在 88 分钟后重新启动。

```
<H3C> schedule reboot delay 88
```

2.1.11 tracert

【命令】

tracert [**-a** *X.X.X.X* | **-f** *first_TTL* | **-m** *max_TTL* | **-p** *port* | **-q** *nqueries* | **-w** *timeout* | **vpn-instance** *vpn-instance-name*] * *host*

【视图】

所有视图

【参数】

-a *X.X.X.X*：指明本次 tracert 命令配置的报文源地址，*X.X.X.X* 指明要配置的 tracert 报文的 IP 地址，形式为 *X.X.X.X*，其必须为一个本地接口的地址。

-f *first_TTL*：*first_TTL* 指定探测报文的初始 TTL，范围为 1～255。

-m *max_TTL*：*max_TTL* 指定探测报文的最大 TTL，范围为 1～255。

-p *port*：指定探测报文的目的端口号，范围为 0～65535，用户一般无须更改此选项。

-q *nqueries*：指定每次发送的探测数据包的个数，范围为 0～65535。

-w *timeout*：指定收到响应报文的超时时间，单位为秒，范围为 0～65535。

vpn-instance *vpn-instance-name*：设置 MPLS VPN 的 *vpn-instance* name，指明本次 Tracert 命令配置的 VPN 属性，即关联的 *vpn-instance* 的名称，而且必须是本地创建的 *vpn-instance*。

host：目的主机的 IP 地址。

【描述】

tracert 命令用来测试数据包从发送主机到目的地所经过的网关，主要用于检查网络连接是否可达，以及分析网络什么地方发生了故障。

各项参数在没有指定时，缺省情况如下：

不带**-a**、**-vpn-instance** 参数；

first_TTL 缺省为 1；

max_TTL 缺省为 30；

port 缺省为 33434；

nqueries 缺省为 3；

timeout 缺省为 5s。

tracert 命令的执行过程：首先发送一个 TTL 为 1 的数据包，因此第一跳发送回一个 ICMP 错误消息以指明此数据包不能被发送（因为 TTL 超时），之后此数据包被重新发送，TTL 为 2，同样第二跳返回 TTL 超时，这个过程不断进行，直到到达目的地。执行这些过程的目的是记录每一个 ICMP TTL 超时消息的源地址，以提供一个

IP 数据包到达目的地所经历的路径。由于一般情况下，不会有任何应用程序去监听 tracert 发送的 UDP 报文所使用的端口。因此，当探测报文到达目的地时，目标设备会发送一个“端口不可达”的 ICMP 差错报文给源地址，当 tracert 程序接收到这个报文时，整个探测过程结束。

当用 **ping** 命令测试发现网络出现故障后，可以用 **tracert** 测试网络何处有故障。

tracert 命令的输出信息包括到达目的地所经过的所有网关的 IP 地址，如果某网关超时，则输出“***”。

在测试过程中，可以使用组合键 CTRL_C 来终止测试。

【举例】

```
<H3C> tracert 18.26.0.115
tracert to allspice.lcs.mit.edu(18.26.0.115) 30 hops max,40 bytes packet
press CTRL_C to break
1 helios.ee.lbl.gov (128.3.112.1) 0 ms 0 ms 0 ms
2 lilac-dmc.Berkeley.EDU (128.32.216.1) 19 ms 19 ms 19 ms
3 lilac-dmc.Berkeley.EDU (128.32.216.1) 39 ms 19 ms 19 ms
4 ccngw-ner-cc.Berkeley.EDU (128.32.136.23) 19 ms 39 ms 39 ms
5 ccn-nerif22.Berkeley.EDU (128.32.168.22) 20 ms 39 ms 39 ms
6 128.32.197.4 (128.32.197.4) 59 ms 119 ms 39 ms
7 131.119.2.5 (131.119.2.5) 59 ms 59 ms 39 ms
8 129.140.70.13 (129.140.70.13) 80 ms 79 ms 99 ms
9 129.140.71.6 (129.140.71.6) 139 ms 139 ms 159 ms
10 129.140.81.7 (129.140.81.7) 199 ms 180 ms 300 ms
11 129.140.72.17 (129.140.72.17) 300 ms 239 ms 239 ms
12 * * *
13 128.121.54.72 (128.121.54.72) 259 ms 499 ms 279 ms
14 * * *
15 * * *
16 * * *
17 * * *
18 ALLSPICE.LCS.MIT.EDU (18.26.0.115) 339 ms 279 ms 279 ms
```

2.2 信息处理命令

2.2.1 display channel

【命令】

display channel [*channel-number* | *channel-name*]

【视图】

所有视图

【参数】

channel-number：通道号可以取的值为 0～9，即系统可以有 10 个通道。

channel-name：通道名。

表2-1 通道名通道号对照关系表

通道名	信息通道号
channel6	6 号通道的名字为 channel6
channel7	7 号通道的名字为 channel7
channel8	8 号通道的名字为 channel8
channel9	9 号通道的名字为 channel9
console	0 号通道的名字为 console
logbuffer	4 号通道的名字为 logbuffer
loghost	2 号通道的名字为 loghost
monitor	1 号通道的名字为 monitor
snmpagent	5 号通道的名字为 snmpagent
trapbuffer	3 号通道的名字为 trapbuffer

【描述】

display channel 命令用来显示信息通道的内容。

display channel 不带参数，表示显示所有通道的设置情况。

【举例】

显示 0 号信息通道的内容。

```
<H3C> display channel 0
channel number:0, channel name:console
 MODU_ID  NAME ENABLE  LOG_LEVEL    ENABLE   TRAP_LEVEL   ENABLE
  DEBUG_LEVEL
ffff0000  all Y       warning  Y       debugging    Y       debugging
```

表2-2 display channel 命令显示信息说明

内容	内容说明
channel number:0,	通道号
channel name:console	通道名称

内容	内容说明
MODU_ID	模块号
NAME	模块名
ENABLE LOG_LEVEL	LOG 日志状态/LOG 日志级别
ENABLE TRAP_LEVEL	TRAP 日志状态/TRAP 日志级别
ENABLE DEBUG_LEVEL	DEBUG 日志状态/DEBUG 日志级别

2.2.2 display info-center

【命令】

display info-center

【视图】

所有视图

【参数】

无

【描述】

display info-center 命令用来显示信息中心记录的各项信息。

相关配置可参考命令 **info-center enable**，**info-center loghost**，**info-center logbuffer**，**info-center trapbuffer**，**info-center console channel**，**info-center monitor channel**。

【举例】

显示信息中心记录的各项信息。

```
<H3C> display info-center
Information Center: enabled
Log host:
Console:
        channel number : 0, channel name : console
Monitor:
        channel number : 1, channel name : monitor
SNMP Agent:
        channel number : 5, channel name : snmpagent
Log buffer:
        enabled,max buffer size 1024, current buffer size 512,
current messages 89, channel number : 4, channel name : logbuffer
dropped messages 0, overwrote messages 0
```

```
Trap buffer:
        enabled,max buffer size 1024, current buffer size 256,
current messages 0, channel number:3, channel name:trapbuffer
dropped messages 0, overwrote messages 0
logfile:
        channel number:9, channel name:channel9, language:English
Information timestamp setting:
        log - date, trap - date, debug – boot
```

表2-3 display info-center 命令显示信息说明

显示信息	说明
Information Center: enabled	信息中心的状态为使能状态
Log host:	日志主机的状态，包括日志主机的 IP 地址，所使用的通道号、通道名，语言及日志主机的级别
Console: channel number : 0, channel name : console	控制口的使用状态，包括控制口所使用的通道名，通道号
Monitor: channel number : 1, channel name : monitor	监视口的使用状态，包括监视口所使用的通道名，通道号
SNMP Agent: channel number : 5, channel name : snmpagent	网管代理的使用状态，包括网管代理所使用的通道名和通道号
Trap buffer: enabled,max buffer size 1024, current buffer size : 256, current messages 0, channel number:3, channel name:trapbuffer dropped messages 0, overwrote messages 0	告警缓冲区的使用状态，包括使能态，最大容量，当前容量，当前信息数，通道名，通道号，已丢弃的信息数，被覆盖的信息数
logfile: channel number:9, channel name:channel9, language:English	日志文件的包含的信息。通道号为 9，通道名为 channel9，使用的语言为英语
Information timestamp setting: log - date, trap - date, debug - boot	信息中心时间格式： log 日志的时间戳格式为 date trap 日志的时间戳格式为 date debug 日志的时间戳格式为 boot

2.2.3 display logbuffer

【命令】

display logbuffer [**size** *size-value* | **summary**] [**level** *level-number*] [| { **begin** | **include** | **exclude** } *string*]

【视图】

所有视图

【参数】

size：指定显示日志缓冲区内信息的条数。

size-value：显示的信息条数，范围为 1～1024。

summary：日志缓冲区摘要。

level：只显示指定级别的信息条目。

level-number：指定的级别，取值为 0～7。

|：使用正则表达式过滤显示信息。

begin：显示以指定文字（*string*）开头的信息。

include：显示包含指定文字（*string*）的信息。

exclude：显示不含指定文字（*string*）的信息。

string：正则表达式文字。

【描述】

display logbuffer 命令用来显示日志缓冲区记录的信息。

缺省情况下，不带任何参数表示显示日志缓冲区记录的所有信息。

如果当前日志缓冲区内的信息数少于用户指定的 *size-value*，则显示实际条数的日志信息。

相关配置可参考命令 **info-center enable**，**info-center logbuffer**，**display info-center**。

【举例】

显示日志缓冲区的信息。

```
<H3C> display logbuffer
Logging buffer configuration and contents:enabled
Allowed max buffer size : 1024
Actual buffer size : 512
Channel number : 4 , Channel name : logbuffer
Dropped messages : 0
Overwritten messages : 0
Current messages : 4

%Sep 30 01:47:59:909 2005 H3C SHELL/5/CMD:task:co0 ip:** user:** command:reset
logbuffer
%Sep 30 01:48:01:530 2005 H3C SHELL/5/CMD:task:co0 ip:** user:** command:sys
```

```
%Sep 30 01:48:01:531 2005 H3C HWCM/5/TRAPLOG:
        1.3.6.1.4.1.2011.10.2.4.2.1 configure changed:
        EventIndex=7,CommandSource=1,ConfigSource=3,ConfigDestination=2
%Sep 30 01:48:07:880 2005 H3C SHELL/5/CMD:task:co0 ip:** user:**
command:display logbuffer
```

表2-4 display logbuffer 命令显示信息说明

显示信息	说明
Logging buffer configuration and contents:enabled	日志缓冲区的状态为 enable 状态
Allowed max buffer size : 1024	允许的日志缓冲区信息最大存储条数为 1024 条
Actual buffer size : 256	实际缓冲区的信息条数大小为 256 条
Channel number : 4 , Channel name : logbuffer	通道号：4，通道名称：日志缓冲区
Dropped messages : 0	丢弃的信息：0
Overwritten messages : 0	被覆盖的信息：0
Current messages : 96	当前的信息：96

2.2.4 display logbuffer summary

【命令】

display logbuffer summary [**level** *severity*]

【视图】

所有视图

【参数】

level：*severity*：信息级别，取值范围 0～7。

表2-5 信息中心定义的优先级（severity）

严重等级	取值	描述
emergencies	0	极其紧急的错误
alerts	1	需立即纠正的错误
critical	2	关键错误
errors	3	需关注但不关键的错误
warnings	4	警告，可能存在某种差错
notifications	5	需注意的信息
informational	6	一般提示信息

严重等级	取值	描述
debugging	7	调试信息

【描述】

display logbuffer summary 命令用来显示防火墙日志缓冲区的概要信息。

【举例】

显示防火墙日志缓冲区的概要信息。

```
<H3C> display logbuffer summary
EMERG ALERT CRIT ERROR WARN NOTIF INFO DEBUG
0     0     0    0     94   0     1    0
```

上例中显示了日志缓冲去中各类日志信息的条数。

2.2.5 display trapbuffer

【命令】

display trapbuffer [**size** *sizeval*]

【视图】

所有视图

【参数】

size：指定显示告警缓冲区内信息的条数。

sizeval：显示的信息条数，范围为 1～1024。

【描述】

display trapbuffer 命令用来显示告警缓冲区记录的信息。

缺省情况下，不带参数表示显示告警缓冲区记录的所有信息。

如果当前告警缓冲区内的信息数少于用户指定的 *sizeval*，则显示实际条数的告警信息。

相关配置可参考命令 **info-center enable**，**info-center trapbuffer**，**display info-center**。

【举例】

显示告警缓冲区的信息。

```
<H3C> display trapbuffer
Trapping Buffer Configuration and contents:
enabled
```

```
allowed max buffer size : 1024
actual buffer size : 256
channel number : 3 , channel name : trapbuffer
dropped messages : 0
overwrote messages : 0
current messages : 0
```

显示告警缓冲区的 23 条记录信息

```
<H3C> display trapbuffer size 23
Trapping Buffer Configuration and contents:
enabled
allowed max buffer size : 1024
actual buffer size : 256
channel number : 3 , channel name : trapbuffer
dropped messages : 0
overwrote messages : 0
current messages : 0
```

表2-6 display trapbuffer 命令显示信息说明

显示信息	说明
Trapping Buffer Confiuration and contents: enabled	告警缓冲区的状态为：Enable
Allowed max buffer size : 1024	允许的告警缓冲区最大信息条数为 1024 条
Actual buffer size : 256	告警缓冲区实际信息的条数为 256 条
channel number : 3 , channel name : trapbuffer	通道号：3，通道名称：告警缓冲区
Dropped messages : 0	丢弃的信息：0
Overwritten messages : 0	被覆盖的信息：0
Current messages : 0	当前的信息：0

2.2.6 info-center channel

【命令】

info-center channel *channel-number* **name** *channel-name*

【视图】

系统视图

【参数】

channel-number：通道号，取值为 0～9，即系统有 10 个通道。

channel-name：通道名，最长为 30 个字符，不支持“-”、“/”和“\”等字符。

【描述】

info-center channel 命令用来将编号为 *channel-number* 的信息通道命名为 *channel-name*。

用户在命名时注意，通道不可重名。

【举例】

将 0 号通道命名为 execconsole。

```
[H3C] info-center channel 0 name execconsole
```

2.2.7 info-center console channel

【命令】

info-center console channel { *channel-number* | *channel-name* }

undo info-center console channel

【视图】

系统视图

【参数】

channel-number：通道号，取值为 0～9，即系统有 10 个通道。

channel-name：通道名。

【描述】

info-center console channel 命令用来设置向控制台输出信息以及所使用的信息通道，**undo info-center console channel** 命令用来取消当前设置。

缺省情况下，不向控制台输出日志信息。

只有启动了系统日志功能，该命令才会生效。

相关配置可参考命令 **info-center enable**，**display info-center**。

【举例】

设置向控制台输出信息及使用的通道。

```
[H3C] info-center console channel console
```

2.2.8 info-center enable

【命令】

info-center enable

undo info-center enable

【视图】

系统视图

【参数】

无

【描述】

info-center enable 命令用来启动信息中心，**undo info-center enable** 命令用来关闭信息中心。

缺省情况下，启动信息中心。

只有启动了信息中心，系统才会向日志主机、控制台等方向输出系统信息。

相关配置可参考命令 **info-center loghost，info-center logbuffer，info-center trapbuffer，info-center console channel，info-center monitor channel，display info-center。**

【举例】

启动信息中心。

```
[H3C] info-center enable
% Information center is enabled
```

2.2.9 info-center logbuffer

【命令】

info-center logbuffer [**channel** { *channel-number* | *channel-name* } | **size** *buffersize*] *

undo info-center logbuffer [**channel** | **size**]

【视图】

系统视图

【参数】

channel：设置向日志缓冲区输出信息的通道。

channel-number：通道号，取值为 0～9，即系统有 10 个通道。

channel-name：通道名。

size：设置日志缓冲区的大小。

buffersize：日志缓冲区的大小（可容纳消息的条数），范围为 0～1024。

【描述】

info-center logbuffer 命令用来打开日志缓冲区，设置输出日志信息的通道号和日志缓冲区大小；**undo info-center logbuffer** 命令用来取消当前设置。

缺省情况下，允许向日志缓冲区输出信息，日志缓冲区的大小为 512。

只有启动了信息中心，该命令才会生效。

通过设置日志缓冲区的通道号，可使信息在该方向输出。

相关配置可参考命令 **info-center enable**，**display info-center**。

【举例】

使防火墙向日志缓冲区发送信息，设定日志缓冲区的大小为 50。

```
[H3C] info-center logbuffer size 50
```

2.2.10 info-center loghost

【命令】

info-center loghost *X.X.X.X* [**channel** { *channel-number* | *channel-name* } | **facility** *local-number* | **language** { **chinese** | **english** }] *

undo info-center loghost *X.X.X.X*

【视图】

系统视图

【参数】

X.X.X.X：日志主机的 IP 地址。

channel：设置日志主机的信息通道。

channel-number：通道号，取值为 0～9，即系统有 10 个通道。

channel-name：通道名。

facility：设置日志主机记录工具。

local-number：日志主机的记录工具，范围在 local0～local7。

language：日志记录语言设置。

chinese、**english**：日志记录语言，中英文的切换。

【描述】

info-center loghost 命令用来设置向日志主机输出信息，**undo info-center loghost** 命令用来取消当前设置。

缺省情况下，不向日志主机输出信息。

如果不指明，日志主机的信息通道缺省使用 2 号信息通道，通道名为 loghost，日志主机记录工具 *local-number* 缺省使用 local7，语言缺省为 **english**。

只有启动了信息中心，该命令才会生效。

通过设置日志主机的 IP 地址，可使信息在该方向输出。最多可以设置 4 个日志主机。

相关配置可参考命令 **info-center enable**，**display info-center**。

【举例】

使防火墙向 IP 地址为 202.38.160.1 的 UNIX 工作站发送信息。

```
[H3C] info-center loghost 202.38.160.1
```

2.2.11 info-center loghost source

【命令】

info-center loghost source *interface-type interface-number*

undo info-center loghost source

【视图】

系统视图

【参数】

interface-type：接口类型。

interface-number：接口编号。

【描述】

info-center loghost source 命令用来指定发向日志主机的包的源地址，**undo info-center loghost source** 命令用来取消当前配置。

从防火墙发出的日志消息，默认的源地址是发送该日志消息的接口的 IP 地址。如果用户想改变这个源地址，可以使用这条配置命令。对不同的设备设置不同的源地址，就可以通过源地址判断日志消息是从哪台设备发出的，从而便于对收到的日志消息检索。

【举例】

将接口 Loopback0 的 IP 地址作为日志消息报文的源地址。

```
[H3C] interface loopback 0
[H3C-LoopBack0] ip address 1.1.1.1 255.255.255.0
[H3C-LoopBack0] quit
[H3C] info-center loghost source loopback 0
```

2.2.12 info-center monitor channel

【命令】

info-center monitor channel { *channel-number* | *channel-name* }

undo info-center monitor channel

【视图】

系统视图

【参数】

channel-number：通道号，取值为 0～9，即系统有 10 个通道。

channel-name：通道名。

【描述】

info-center monitor channel 命令用来设置向用户终端输出信息以及所使用的信息通道，**undo info-center monitor channel** 命令用来取消当前设置。

缺省情况下，不向用户终端输出信息。

只有启动了信息中心，该命令才会生效。

相关配置可参考命令 **info-center enable**，**display info-center**。

【举例】

设置向用户终端输出信息及使用的信息通道。

```
[H3C] info-center monitor channel monitor
```

2.2.13 info-center snmp channel

【命令】

info-center snmp channel { *channel-number* | *channel-name* }

undo info-center snmp channel

【视图】

系统视图

【参数】

channel-number：通道号，取值为 0～9，即系统有 10 个通道。

channel-name：通道名。

【描述】

info-center snmp channel 命令用来设置 **snmp** 的信息通道，**undo info-center snmp channel** 命令用来取消当前配置。

缺省情况下，使用 5 号通道。

相关配置可参考命令 **display snmp-agent statistics**。

【举例】

设置 SNMP 信息通道为 6 号通道。

```
[H3C] info-center snmp channel 6
```

2.2.14 info-center source

【命令】

info-center source { *module-name* | **default** } { **channel** { *channel-number* | *channel-name* } } [**log** { **state** { **on** | **off** } | **level** *severity* }* | **trap** { **state** { **on** | **off** } | **level** *severity* } * | **debug** { **state** { **on** | **off** } | **level** *severity* }*]*

undo info-center source { *module-name* | **default** } { **channel** { *channel-number* | *channel-name* }

【视图】

系统视图

【参数】

module-name：模块名。

default：设置情况下包含所有的模块。

channel-number：要设置的信息通道号。

channel-name：要设置的信息通道名。

log：日志信息。

trap：告警信息。

debug：调试信息。

on：开启信息。

off：关闭信息。

level：设置信息级别，禁止信息级别大于所设置的 *severity* 的信息输出。

severity：信息级别，信息中心按信息的严重等级或紧急程度划分为八个级别，如下表所示，越紧急其信息级别越小，**emergencies** 表示的等级为 0，**debugging** 为 7。

表2-7 信息级别的定义

严重等级	描述
emergencies	极其紧急的错误
alerts	需立即纠正的错误
critical	关键错误
errors	需关注但不关键的错误
warnings	警告，可能存在某种差错
notifications	需注意的信息
informational	一般提示信息
debugging	调试信息

*：表示选项中选取多个，最少选取一个，最多选取所有选项。

【描述】

info-center source 命令用来向信息通道中添加记录，**undo info-center source** 命令用来删除信息通道中的记录。

缺省情况下，对于指定的具体模块：

日志类信息，状态为 **on**，允许的信息级别为 **informational**。

告警类信息，状态为 **on**，允许的信息级别为 **informational**。

调试类信息，状态为 **off**。

目前，系统对每个输出方向缺省分配一个信息通道，它们是：

输出方向	信息通道号	缺省的信息通道名
控制台	0	console
监视终端	1	monitor
日志主机	2	loghost
告警缓冲区	3	trapbuffer
日志缓冲区	4	logbuffer
snmp	5	snmpagent

此外，对每个信息通道设有一条缺省记录，它的模块名为 default，模块号为 0xffff0000，但对于不同信息通道，此记录对日志、告警、调试类信息的缺省设置值可能不同。当某一个模块在此通道中没有明确的配置记录时，使用这条缺省的配置记录。

⚠ 注意：

对于新添加或重复添加的记录，用户需要同时指定其日志信息、告警信息和调试信息的级别，否则系统会将信息级别恢复为缺省级别。

【举例】

设置将 snmp 通道中的 ip 模块的日志类信息打开，且允许输出信息的最高级别为 emergencies。

```
[H3C] info-center source ip channel snmpagent log level emergencies
```

将 snmp 通道中 cmd 模块的设置删除。

```
[H3C] undo info-center source cmd channel snmpagent
```

2.2.15 info-center timestamp

【命令】

info-center timestamp { **trap** | **debugging** | **log** } { **boot** | **date** | **none** }

undo info-center timestamp { **trap** | **debugging** | **log** }

【视图】

系统视图

【参数】

trap：告警信息。

debugging：调试信息。

log：日志信息。

boot：绝对时间类型的信息时间戳。

date：日期时间类型的信息时间戳。

none：无信息时间戳。

【描述】

info-center timestamp 命令用来设置输出到终端和 buffer 中的调试/告警/日志信息中的时间戳格式，**undo info-center timestamp** 命令用来取消当前设置。

缺省情况下，debugging 信息使用 boot 时间戳，其他类型都使用 date 时间戳。

【举例】

设置告警（**trap**）信息时间戳格式为 **boot**。

```
[H3C] info-center timestamp trap boot
```

2.2.16 info-center timestamp loghost

【命令】

info-center timestamp loghost { **date** | **no-year-date** | **none** }

undo info-center timestamp loghost

【视图】

系统视图

【参数】

date：日期时间类型的信息时间戳。

no-year-date：没有年份的日期时间类型的信息时间戳。

none：无信息时间戳。

【描述】

info-center timestamp loghost 命令用来设置输出到日志主机的日志信息的时间戳格式，**undo** 命令用来取消当前设置。

缺省情况下，使用 date 日期时间类型的信息时间戳。

【举例】

设置输出到日志主机的日志信息的时间戳为 no-year-date。

```
[H3C] info-center timestamp loghost no-year-date
```

2.2.17 info-center trapbuffer

【命令】

info-center trapbuffer [**channel** { *channel-number* | *channel-name* } | **size** *buffersize*] *

undo info-center trapbuffer [**channel** | **size**]

【视图】

系统视图

【参数】

channel：设置向告警缓冲区输出信息的通道。

channel-number：通道号，取值为 0～9，即系统有 10 个通道。

channel-name：通道名。

size：设置告警缓冲区的大小。

buffersize：告警缓冲区的大小（可容纳消息的条数），范围为 0～1024。

【描述】

info-center trapbuffer 命令用来打开告警缓冲区，并设置输出告警信息的通道号和告警缓冲区大小，**undo info-center trapbuffer** 命令用来取消当前设置。

缺省情况下，允许向告警缓冲区输出信息，告警缓冲区的大小为 256。

只有启动了信息中心，该命令才会生效。

通过设置告警缓冲区的大小，可使信息在该方向输出。

相关配置可参考命令 **info-center enable**，**display info-center**。

【举例】

使防火墙向告警缓冲区发送信息，设定告警缓冲区的大小为 30。

```
[H3C] info-center trapbuffer size 30
```

2.2.18 reset logbuffer

【命令】

reset logbuffer

【视图】

用户视图

【参数】

无

【描述】

reset logbuffer 命令用来清除日志缓冲区中的信息。

【举例】

```
<H3C> reset logbuffer
```

2.2.19 reset trapbuffer

【命令】

reset trapbuffer

【视图】

用户视图

【参数】

无

【描述】

reset trapbuffer 命令用来清除告警缓冲区中的信息。

【举例】

```
<H3C> reset trapbuffer
```

2.2.20 terminal debugging

【命令】

terminal debugging

undo terminal debugging

【视图】

用户视图

【参数】

无

【描述】

terminal debugging 命令用来打开终端显示调试信息功能，**undo terminal debugging** 命令用来关闭终端显示调试信息功能。

缺省情况下，关闭终端显示功能

相关配置可参考命令 **debugging**。

【举例】

打开终端显示调试信息功能。

```
<H3C> terminal debugging
```

2.2.21 terminal logging

【命令】

terminal logging

undo terminal logging

【视图】

用户视图

【参数】

无

【描述】

terminal logging 命令用来打开终端显示的日志信息功能，**undo terminal logging** 命令用来关闭终端显示的日志信息功能。

缺省情况下，系统配置为打开日志信息显示功能。

【举例】

关闭终端日志显示功能。

```
<H3C> undo terminal logging
```

2.2.22 terminal monitor

【命令】

terminal monitor

undo terminal monitor

【视图】

用户视图

【参数】

无

【描述】

terminal monitor 命令用来打开终端显示信息中心发送的调试/日志/告警信息功能，**undo terminal monitor** 命令用来关闭终端显示上述信息功能。

缺省情况下，控制台用户显示功能为打开，终端用户缺省配置为关闭。

此命令只影响输入命令的当前终端。**undo terminal monitor**，相当于执行 **undo terminal debugging**，**undo terminal logging**，**undo terminal trapping** 命令，所有的调试/日志/告警信息在本终端都不显示；在 **terminal monitor** 为打开的情况下，可以分别使用 **terminal debugging/undo terminal debugging**，**terminal logging/undo terminal logging**，**terminal trapping/undo terminal trapping** 打开或关闭调试/日志/告警信息。

缺省情况下，控制台用户（Console 用户）的终端显示功能为打开，所有提示信息都能够直接输出到配置终端；其它终端用户（AUX、VTY 用户）的终端显示功能缺省为关闭，因此配置 **terminal monitor** 命令后其提示信息才能输出到配置终端。

【举例】

关闭终端显示功能。

```
<H3C> undo terminal monitor
```

2.2.23 terminal trapping

【命令】

terminal trapping

undo terminal trapping

【视图】

用户视图

【参数】

无

【描述】

terminal trapping 命令用来打开终端告警信息显示功能，**undo terminal trapping** 命令用来关闭终端显示告警信息功能。

缺省情况下，系统的配置为打开显示功能。

【举例】

关闭告警信息显示功能。

```
<H3C> undo terminal trapping
```

2.3 HTTP 服务器配置命令

2.3.1 ip http acl

【命令】

ip http acl *acl-number*

undo ip http acl

【视图】

系统视图

【参数】

acl-number：基本访问控制列表的编号，范围为 2000～2999。

【描述】

ip http acl 命令用来配置 HTTP 服务器的访问限制，**undo ip http acl** 命令用来取消所做的配置。

仅 ACL 中允许的 IP 地址才可以访问 HTTP 服务器。

缺省情况下，未配置 HTTP 服务器的访问限制。

【举例】

配置仅允许位于管理区域 192.168.1.0/24 中的用户访问 HTTP 服务器。

```
[H3C] acl number 2000
[H3C-acl-basic-2000] rule 0 permit source 192.168.1.0 0.0.0.255
[H3C-acl-basic-2000] rule 1 deny source any
[H3C-acl-basic-2000] quit
[H3C] ip http acl 2000
```

2.3.2 ip http shutdown

【命令】

ip http shutdown

undo ip http shutdown

【视图】

系统视图

【参数】

无

【描述】

ip http shutdown 命令用来关闭 HTTP 服务器，**undo ip http shutdown** 命令用来使能 HTTP 服务器。

仅当登录用户具有 Telnet 的服务类型时（**service-type telnet**），才允许登录 HTTP 服务器，且不同等级的用户在 Web 界面中的可配置项也会不同。

缺省情况下，使能 HTTP 服务器。

【举例】

关闭 HTTP 服务器。

```
[H3C] ip http shutdown
```

第3章 自动侦测配置命令

3.1 自动侦测基本配置命令

3.1.1 debugging detect-group

【命令】

debugging detect-group { **all** | **packet** | **state** | **timer** }

undo debugging detect-group { **all** | **packet** | **state** | **timer** }

【视图】

用户视图

【参数】

all：所有调试开关。

packet：报文调试开关。

state：状态变化调试开关。

timer：定时器调试开关。

【描述】

debugging detect-group 命令用来打开自动侦测的调试信息开关，**undo debugging detect-group** 命令用来关闭自动侦测的调试信息开关。

缺省情况下，未打开自动侦测的调试信息开关。

【举例】

打开自动侦侧的报文调试开关。

```
<H3C> debugging detect-group packet
```

3.1.2 detect-group

【命令】

detect-group *group-number*

undo detect-group *group-number*

【视图】

系统视图

【参数】

group-number：自动侦测组的编号，取值范围为 1～50。

【描述】

detect-group 命令用来创建一个自动侦测组，并进入侦测组视图；**undo detect-group** 命令用来删除一个指定的自动侦测组。

【举例】

创建一个自动侦测组 10。

```
<H3C> system-view
System View: return to User View with Ctrl+Z.
[H3C] detect-group 10
[H3C-detect-group-10]
```

3.1.3 detect-list

【命令】

detect-list *list-number* **ip address** *ip-address* [**nexthop** *ip-address*]

undo detect-list *list-number*

【视图】

侦测组视图

【参数】

list-number：侦测组中各个侦测地址的序号，取值范围为 1～20。

ip-address：自动侦测的 IP 地址。

nexthop *ip-address*：指定自动侦测从下一跳的某个 IP 地址开始（即自动侦测的起始地址）。

【描述】

detect-list 命令用来配置在某一个侦测组中，需要侦测的 IP 地址及侦测的先后顺序。**undo detect-list** 命令用来取消配置的侦测对象。

配置好要侦测的 IP 地址后，防火墙就按照 *list-number* 指定的序号，从小到大，依次对 IP 地址进行侦测。一个侦测组中最多可以配置 20 个侦测地址。多个侦测地址之间的关系由 **option** 命令确定。

相关配置可参考 **option** 命令。

【举例】

在侦测组 10 中，增加侦测对象 202.13.1.55，侦测序号为 1。自动侦测从下一跳地址 1.1.1.1 开始。

```
<H3C> system-view
System View: return to User View with Ctrl+Z.
[H3C] detect-group 10
[H3C-detect-group-10] detect-list 1 ip address 202.13.1.55 nexthop 1.1.1.1
```

3.1.4 display detect-group

【命令】

display detect-group [*group-number*]

【视图】

任意视图

【参数】

group-number：自动侦测组的编号，取值范围为 1～50。

【描述】

display detect-group 命令用来显示某个指定侦测组或所有侦测组的配置信息。

【举例】

显示侦测组 1 的配置信息。

```
[H3C] display detect-group 1
detect-group 1 :
 detect loop time(s) : 15
   ping wait time(s) : 2
  detect retry times : 2
    detect ip option : and
         group state : not detecting
 register module num : 0
     detect ip count : 0
detect-list  ip address       next hop
1            1.1.1.1          1.1.1.5
```

表3-1 display detect-group 命令显示信息描述表

域名	描述
detect-group 1	自动侦测组 1
detect loop time(s): 15	自动侦测的循环周期为 15 秒

域名	描述
ping wait time(s): 2	一次侦测中的超时时间为 2 秒
detect retry times: 2	一次侦测中重试的次数为 2 次
detect ip option: and	侦测组中各个侦测对象间的逻辑关系为“与”
group state: not detecting	自动侦测组目前的状态：没有进行侦测
register module num: 0	引用侦测组的次数
detect ip number: 1	自动侦测的 IP 地址数目
detect-list	侦测对象的序号
ip address	需要侦测的 IP 地址
next hop	下一跳的 IP 地址

3.1.5 option

【命令】

option { **and** | **or** }

undo option

【视图】

侦测组视图

【参数】

and：侦测对象之间的关系为“逻辑与”。

or：侦测对象之间的关系为“逻辑或”。

【描述】

option 命令用来设置一个侦测组中各个侦测对象间的逻辑关系。**undo option** 命令用来恢复一个侦测组中各个侦测对象间设置的逻辑关系的缺省值。

进行每轮侦测时，防火墙按照侦测对象对应的序号（*list-number*），从小到大依次侦测各个 IP 地址的可达性：

- 当侦测对象之间的关系为 **and** 时：有一个 IP 地址无法 **ping** 通即认为该侦测组不可达，并不再侦测其余的地址；
- 当侦测对象之间的关系为 **or** 时：有一个 IP 地址 **ping** 通即认为该侦测组可达，并不再侦测其余的地址。

缺省情况下，各个侦测对象之间的逻辑关系为 **and**。

【举例】

设置侦测组 10 中的侦测对象之间的关系为逻辑或。

```
<H3C> system-view
System View: return to User View with Ctrl+Z.
[H3C] detect-group 10
[H3C-detect-group-10] option or
```

3.1.6 retry

【命令】

retry *retry-times*

undo retry

【视图】

侦测组视图

【参数】

retry-times：一次侦测中重试的次数，取值范围为 0～10，缺省值是 2。

【描述】

retry 命令用来设置侦测组在一次侦测中的最大重试次数，**undo retry** 命令用来恢复最大重试次数的缺省值。

【举例】

配置侦测组 10 中，一轮侦测中最大的重试次数为 3。

```
<H3C> system-view
System View: return to User View with Ctrl+Z.
[H3C] detect-group 10
[H3C-detect-group-10] retry 3
```

3.1.7 timer loop

【命令】

timer loop *seconds*

undo timer loop

【视图】

侦测组视图

【参数】

seconds：自动侦测的循环周期，取值范围为 1～86400，单位秒，缺省值是 15。

【描述】

timer loop 命令用来设置自动侦测的循环周期，即每隔一定的时间对所有侦测对象进行一次侦测。**undo timer loop** 命令用来恢复自动侦测循环周期的缺省值。

【举例】

配置侦测组 10 的侦测循环周期为 60 秒。

```
<H3C> system-view
System View: return to User View with Ctrl+Z.
[H3C] detect-group 10
[H3C-detect-group-10] timer loop 60
```

3.1.8 timer wait

【命令】

timer wait *seconds*

undo timer wait

【视图】

侦测组视图

【参数】

seconds：一次侦测中的超时时间。取值范围为 1～30，单位秒，缺省值是 2。

【描述】

timer wait 命令用来设置一次侦测中的超时时间，**undo timer wait** 命令用来恢复超时时间的缺省值。

【举例】

在侦测组 10 中，配置一次侦测中的超时时间为 3 秒。

```
<H3C> system-view
System View: return to User View with Ctrl+Z.
[H3C] detect-group 10
[H3C-detect-group-10] timer wait 3
```

3.2 自动侦测应用命令

> 说明：
> - 对于静态路由的详细介绍，请参见本手册中有关“路由协议”的章节。
> - 对于 VRRP 的详细介绍，请参见本手册中有关“可靠性”的章节。

3.2.1 ip route-static detect-group

【命令】

ip route-static *ip-address* { *mask* | *mask-length* } { *interface-type interface-number* | *nexthop* } [**preference** *preference-value*] **detect-group** *group-number*

【视图】

系统视图

【参数】

ip-address：目的 IP 地址（点分十进制格式）。

mask：子网掩码。

mask-length：子网掩码长度，即子网掩码中连续“1”的位数。

interface-type：出接口的类型。

interface-number：出接口的编号。

nexthop：下一跳 IP 地址（点分十进制格式）。

preference-value：为该路由的优先级别，范围 1～255。

group-number：自动侦测组的编号，取值范围为 1～50。

【描述】

ip route-static detect-group 命令用来配置一条静态路由，并将侦测组返回的结果（可达或不可达）作为静态路由是否生效的一个必要条件：

- 当侦测组可达时，此静态路由生效；
- 当侦测组不可达时，此静态路由无效。

当希望在静态路由中取消自动侦测功能时，只能先使用 **undo ip route-static** 命令用来取消所配置的静态路由，然后再重新配置该路由。

【举例】

配置一条到 192.168.0.5/24 的静态路由，下一跳为 192.168.0.2。如果侦测组 10 可达，则使该静态路由生效。

```
<H3C> system-view
System View: return to User View with Ctrl+Z.
[H3C] ip route-static 192.168.0.5 24 192.168.0.2 detect-group 10
```

3.2.2 vrrp vrid track detect-group

【命令】

vrrp vrid *virtual-router-ID* **track detect-group** *group-number* [**reduced** *value-reduced*]

undo vrrp vrid *virtual-router-ID* **track detect-group** [*group-number*]

【视图】

以太网接口视图

【参数】

virtual-router-ID：虚拟路由器 ID，取值范围为 1～255。

group-number：自动侦测组的编号，取值范围为 1～50。

value-reduced：优先级降低的数值，取值范围为 1～255，缺省值为 10。

【描述】

vrrp vrid 命令用来启动在 VRRP 中的 **track** 侦测功能。**undo vrrp vrid** 命令用来取消侦测功能。

用户可以利用自动侦测的返回结果来控制 VRRP 备份组的优先级，实现主备路由器的自动切换：

- 当侦测组不可达时，降低备份组的优先级；
- 当侦测组可达时，恢复备份组的优先级。

【举例】

创建侦测组 10，配置侦测对象 202.13.1.55。

```
<H3C> system-view
System View: return to User View with Ctrl+Z.
[H3C] detect-group 10
[H3C-detect-group-10] detect-list 1 ip address 202.13.1.55
```

当侦测组 10 不可达时，备份组 1 的优先级降低 20。

```
[H3C] interface ethernet 0/0/0
[H3C-Ethernet0/0/0] vrrp vrid 1 track detect-group 10 reduced 20
```

第4章 HWPing 配置命令

4.1 HWPing 客户端命令

4.1.1 count

【命令】

count *times*

undo count

【视图】

HWPing 测试组视图

【参数】

times：一次测试中进行探测的次数。取值范围为 1～15。缺省情况下，探测的次数为 1。

【描述】

count 命令用来配置一次测试中进行探测的次数。**undo count** 命令用来将探测次数恢复到缺省值。

如果设置该参数大于 1，那么系统在进行第一次探测之后，如果收到响应报文就进行第二次探测。如果一直没有收到响应报文，则等到测试定时器超时后，再进行第二次探测。如此直到完成最后一次探测。

相关配置可参考命令 **frequency**。

【举例】

设置一次测试中进行探测的次数为 10。

```
[H3C-hwping-administrator-icmp] count 10
```

4.1.2 datafill

【命令】

datafill *string*

undo datafill

【视图】

HWPing 测试组视图

【参数】

string：测试数据包的填充数据。可以是长度不超过 230 的任意字符串，缺省情况下，采用 0～255 循环填充。

【描述】

datafill 命令用来配置测试操作所用的数据包的填充数据，命令 **undo datafill** 可以将数据包的填充数据恢复为缺省方式。

HWPing 测试数据包的填充数据可以为任意字符串。如果测试数据包大小比配置的填充数据小，那么系统在组包时只使用此字符串的前一部分；如果测试数据包大小比配置的填充数据大，那么，系统在组包时将使用此字符串循环进行填充。例如，配置填充数据为“abcd”，当测试数据包大小为 3 时，则只使用“abc”作为填充数据；当测试数据包大小为 6 时，则只使用“abcdab”作为填充数据。

只有 ICMP、UDP 和 jitter 测试支持配置填充字符，此配置对于其它测试类型无效。

【举例】

设置测试数据包的填充模式为“abcd”。

```
[H3C-hwping-administrator-icmp] datafill abcd
```

4.1.3 datasize

【命令】

datasize *size*

undo datasize

【视图】

HWPing 测试组视图

【参数】

size：测试数据包的数据段长度，单位为字节，取值范围为 4～8100。测试类型为 ICMP 时，数据段长度的缺省值为 56 个字节；测试类型为 UDP 时，数据段长度的缺省值为 100 个字节；测试类型为 jitter 时，数据段长度在 68～100 字节之间（此时取其它值无效）。

【描述】

datasize 命令用来配置测试操作所用的数据包的数据段长度，命令 **undo datasize** 可以将数据包的数据段长度恢复到缺省值。

只有 ICMP、UDP 和 jitter 测试支持配置报文的数据段长度，此配置对于其它测试类型无效。

📖 **说明：**

当对此命令配置了缺省值后，其缺省值的配置结果也会显示在配置文件中。

【举例】

设置测试数据包的数据段长度为 50。

```
[H3C-hwping-administrator-icmp] datasize 50
```

4.1.4 debugging hwping

【命令】

debugging hwping { **all | error | event** }

undo debugging hwping { **all | error | event** }

【视图】

用户视图

【参数】

all：所有调试信息开关。

error：错误调试信息开关。

event：事件调试信息开关。

【描述】

debugging hwping 命令用来打开 HWPing 的调试信息开关，**undo debugging hwping** 命令用来关闭调试信息开关。

缺省情况下，关闭调试信息开关。

【举例】

打开 HWPing 的事件调试信息开关。

```
<H3C> debugging hwping event
```

4.1.5 description

【命令】

description *string*

undo description

【视图】

HWPing 测试组视图

【参数】

string：对本次操作进行的简要描述，长度为 1～230 个字符。缺省情况下无描述信息。

【描述】

description 命令用来配置对本次操作进行的简要描述，**undo description** 命令用来恢复接口缺省的描述信息。

可以使用 **display interface** 命令查看接口缺省的描述信息。

【举例】

对本操作描述为“icmp-test”。

```
[H3C-hwping-administrator-icmp] description icmp-test
```

4.1.6 destination-ip

【命令】

destination-ip *ip-address*

undo destination-ip

【视图】

HWPing 测试组视图

【参数】

ip-address：测试操作的目的 IP 地址

【描述】

destination-ip 命令用来配置测试操作的目的 IP 地址，**undo destination-ip** 用来删除配置的目的 IP 地址。

缺省情况下，未配置测试操作的目的 IP 地址。

【举例】

设置测试的目的 IP 地址为 169.254.10.3。

```
[H3C-hwping-administrator-icmp] destination-ip 169.254.10.3
```

4.1.7 destination-port

【命令】

destination-port *port-number*

undo destination-port

【视图】

HWPing 测试组视图

【参数】

port-number：测试操作的目的端口。取值范围为 1～65535。

【描述】

destination-port 命令用来配置测试操作的目的端口，**undo destination-port** 用来删除已配置的目的端口。

缺省情况下，未配置测试操作的目的端口。

📖 说明：

只有在测试类型为 Jitter、TCP-private、UDP-private 时，才能配置此命令。

相关配置可参考命令 **destination-ip**。

【举例】

设置测试的目的端口为 9000。

```
[H3C-hwping-administrator-tcp] destination-port 9000
```

4.1.8 display hwping

【命令】

display hwping { **results** | **history | jitter** } [*administrator-name test-tag*]

【视图】

所有视图

【参数】

results：显示测试结果。

history：显示历史表信息。

jitter：显示抖动信息。

administrator-name：指定创建操作的管理员名字。

test-tag：指定测试操作的标签。

【描述】

display hwping 命令用来显示测试操作的结果。

如果不指定测试组参数（*administrator-name* 和 *test-tag*），将显示所有测试组的结果，否则只显示指定测试组操作的结果。

相关配置可参考命令 **test-enable**。

【举例】

查看测试结果。

```
[H3C-hwping-administrator-icmp] display hwping results administrator icmp
  HWPing entry(admin administrator, tag icmp) test result:
     Destinationip address:169.254.10.2
     Send operation times: 10             Receive response times: 10
     Min/Max/Average Round Trip Time: 1/2/1
     Square-Sum of Round Trip Time: 13
     Last complete test time: 2004-11-25 16:28:55.0
   Extend result:
     Disconnect operation number:0        Operation timeout number:0
     System busy operation number:0       Connection fail number:0
     Operation sequence errors:0          Drop operation number:0
     Operation statistics errors:0
```

表4-1 display hwping results 命令输出信息描述

主要字段	描述
Destion ip address	目的 IP 地址
Send operation times	发送测试次数
Receive respondse times	成功测试次数
Min/Max/Average Round Trip Time	最小/最大/平均往返时间
Square-Sum of Round Trip Time	往返时间平方和
Last complete test time	最后成功测试时间
Disconnect operation number	对方强制断开连接的次数
System busy operation number	因系统忙测试失败的次数
Operation sequence errors	收到的失序包数
Operation statics errors	其它错误数

```
[H3C-hwping-administrator-icmp] display hwping history administrator icmp
  HWPing entry(admin administrator, tag icmp) history record:
    Index     Response    Status      LasrRC      Time
       1            1         1           0    2004-11-25 16:28:55.0
       2            1         1           0    2004-11-25 16:28:55.0
       3            1         1           0    2004-11-25 16:28:55.0
       4            1         1           0    2004-11-25 16:28:55.0
```

```
5           1           1           0     2004-11-25 16:28:55.0
6           2           1           0     2004-11-25 16:28:55.0
7           1           1           0     2004-11-25 16:28:55.0
8           1           1           0     2004-11-25 16:28:55.0
9           1           1           0     2004-11-25 16:28:55.9
10          1           1           0     2004-11-25 16:28:55.9
```

表4-2 display hwping history 命令输出信息描述

主要字段	描述
Response	往返测试毫秒级时间，或超时时间，当不能完成测试时为 0
Status	测试结果值
LasrRC	接收到最后一个基于实现方法的应答编码。在启用 ICMP Echo 功能的情况下，如果收到包含 ICMP_ECHOREPLY(0)的 ICMP 应答就说明探测成功。ICMP 应答通常在包含 ip_icmp 的文件中定义。
Time	测试时间

4.1.9 filename

【命令】

filename *file-name*

undo filename

【视图】

HWPing 测试组视图

【参数】

file-name：和 FTP 服务器之间待传送文件的文件名，长度为 1～230 个字符。

【描述】

filename 命令用来配置和 FTP 服务器之间待传送文件的文件名，**undo filename** 命令取消已配置的文件名。

缺省情况下，未配置和 FTP 服务器之间待传送文件的文件名。

📖 **说明：**

此命令仅对 FTP 类型的测试操作适用。

相关配置可参考命令 **username**、**password**、**ftp-operation**。

【举例】

配置和 FTP 服务器之间要传送文件的文件名为“config.txt”。

```
[H3C-hwping-administrator-ftp] filename config.txt
```

4.1.10 frequency

【命令】

frequency *interval*

undo frequency

【视图】

HWPing 测试组视图

【参数】

interval：自动测试的时间间隔，以秒为单位，取值范围为 0～65535，缺省值为 0，即不自动测试。

【描述】

frequency 命令用来配置自动测试的时间间隔，命令 **undo frequency** 用来取消自动测试。

配置自动测试的间隔时间大于 0 时，系统会自动的每隔这个时间就进行一次测试。

相关配置可参考命令 **count**。

【举例】

设置自动测试的时间间隔为 10 秒。

```
[H3C-hwping-administrator-icmp] frequency 10
```

4.1.11 ftp-operation

【命令】

ftp-operation { **get** | **put** }

【视图】

HWPing 测试组视图

【参数】

get：从 FTP 服务器获取文件。

put：向 FTP 服务器传送文件。

【描述】

ftp-operation 命令用来配置 FTP 的操作方式。

FTP 的操作方式分为 get 和 put。get 是从 FTP 服务器获取文件。put 是向 FTP 服务器传送文件。

缺省情况下的操作方式为 get。

📖 **说明：**

此命令仅对 FTP 类型的测试操作适用。

相关配置可参考命令 **username**、**password**。

【举例】

配置 FTP 的操作方式为 put。

```
[H3C-hwping-administrator-ftp] ftp-operation put
```

4.1.12 history-records

【命令】

history-records *number*

undo history-records

【视图】

HWPing 测试组视图

【参数】

number：在历史记录中能够保存的测试结果数目，取值范围为 0～50，缺省值为 50。

【描述】

history-records 命令用来配置在历史记录中能够保存的测试结果数目，**undo history-records** 命令将历史记录中能够保存的测试结果数目恢复到缺省值。

【举例】

设置在历史表中保存的与本操作相关的条目数为 10。

```
[H3C-hwping-administrator-icmp] history-records 10
```

4.1.13 http-operation

【命令】

http-operation { **get** | **post** }

【视图】

HWPing 测试组视图

【参数】

get：从 HTTP 服务器获取数据。

post：向 HTTP 服务器传送数据。

【描述】

http-operation 命令用来配置 HTTP 的操作方式。

HTTP 的操作方式分为 get 和 post。get 是从 HTTP 服务器获取数据，post 是向 HTTP 服务器传送数据。

缺省情况下的操作方式为 get。

📖 **说明：**

此命令仅对 HTTP 类型的测试操作适用。

【举例】

配置 HTTP 的操作方式为 post。

```
[H3C-hwping-administrator-http] http-operation post
```

4.1.14 hwping

【命令】

hwping *administrator-name test-tag*

undo hwping *administrator-name test-tag*

【视图】

系统视图

【参数】

administrator-name：指定创建操作的管理员名字。

test-tag：指定测试操作的标签。

【描述】

hwping 命令用来创建一个 HWPing 测试组。

执行此命令后，进入 HWPing 测试组视图。

【举例】

创建一个管理员名为 administrator，测试标签为 icmp 的 HWPing 测试组。

```
[H3C] hwping administrator icmp
[H3C-hwping-administrator-icmp]
```

4.1.15 hwping-agent enable

【命令】

hwping-agent enable

undo hwping-agent enable

【视图】

系统视图

【参数】

无

【描述】

hwping-agent enable 命令用来使能 HWPing 客户端功能，**undo hwping-agent enable** 命令用来取消 HWPing 客户端功能。

只有使能了 HWPing 客户端功能，才能进行各类测试操作。

【举例】

使能 HWPing 客户端。

```
[H3C] hwping-agent enable
```

4.1.16 hwping-agent max-requests

【命令】

hwping-agent max-requests *max-number*

undo hwping-agent max-requests

【视图】

系统视图

【参数】

max-number：能同时启动的测试操作的最大的个数，取值范围为 1～5，缺省情况下可同时启动的测试操作个数为 5。

【描述】

hwping-agent max-requests 命令用来设置能同时启动的测试操作的个数。**undo hwping-agent max-requests** 用来恢复能同时启动的测试操作个数为缺省值。

【举例】

配置能同时启动的测试操作的最大个数为 4。

```
[H3C] hwping-agent max-requests 4
```

4.1.17 jitter-interval

【命令】

jitter-interval *interval*

undo jitter-interval

【视图】

HWPing 测试组视图

【参数】

interval：测试抖动时间时发送测试包的时间间隔。取值范围是 10～1000 毫秒，缺省值为 20 毫秒。

【描述】

jitter-interval 命令用来配置 Jitter 测试时发送测试包的时间间隔，**undo jitter-interval** 用来恢复发送测试包的时间间隔为缺省值。

📖 说明：

此命令仅对 Jitter 类型的测试操作适用。

相关配置可参考命令 **jitter-packetnum**。

【举例】

配置 Jitter 测试发送测试包的时间间隔为 30 毫秒。

```
[H3C-hwping-administrator-icmp] jitter-interval 30
```

4.1.18 jitter-packetnum

【命令】

jitter-packetnum *number*

undo jitter-packetnum

【视图】

HWPing 测试组视图

【参数】

number：Jitter 测试时发送测试包的个数。取值范围是 10～100，缺省值为 10。

【描述】

jitter-packetnum 命令用来配置 Jitter 测试时发送测试包的个数，**undo jitter-packetnum** 命令用来恢复发送测试包的个数为缺省值。

📖 说明：

此命令仅对 Jitter 类型的测试操作适用。

相关配置可参考命令 **jitter-interval**。

【举例】

配置发送测试包的个数为 30。

```
[H3C-hwping-administrator-icmp] jitter-packetnum 30
```

4.1.19 password

【命令】

password *password*

undo password

【视图】

HWPing 测试组视图

【参数】

password：登录 FTP 服务器时所需的口令，长度为 1～32 个字符。

【描述】

password 命令用来配置登录 FTP 服务器时所需的口令，**undo password** 命令用来取消已配置的口令。

缺省情况下，未配置登录 FTP 服务器时所需的用户密码。

📖 说明：

此命令仅对 FTP 类型的测试操作适用。

相关配置可参考命令 **username**、**ftp-operation**。

【举例】

配置登录 FTP 服务器的口令为“hwping”。

```
[H3C-hwping-administrator-ftp] password hwping
```

4.1.20 probe-failtimes

【命令】

probe-failtimes *times*

undo probe-failtimes

【视图】

HWPing 测试组视图

【参数】

times：连续测试失败的次数，取值范围 1～15。缺省值为 1 次。

【描述】

probe-failtimes 命令用来设置 HWPing 测试连续多少次探测失败之后向网管发送 Trap。**undo probe-failtimes** 命令用来恢复连续探测失败几次后发送 Trap 的缺省值。

📖 说明：

一次测试中可以包含多次探测。

【举例】

设置 HWPing 测试连续探测失败 3 次之后发送 Trap。

```
[H3C-hwping-administrator-icmp] probe-failtimes 3
```

4.1.21 send-trap

【命令】

send-trap { **all** | { **probefailure** | **testcomplete** | **testfailure** } * }

undo send-trap { **all** | { **probefailure** | **testcomplete** | **testfailure** } * }

【视图】

HWPing 测试组视图

【参数】

probefailure：当发送测试包失败时发送 trap。

testcomplete：当测试完成时发送 trap。

testfailure：当测试失败时发送 trap。

all：上面任何一种情况发生时都发送 trap。

【描述】

send-trap 命令用来配置 trap 的发送条件，**undo send-trap** 命令取消已配置的发送条件。

缺省情况下，不发送 Trap。

【举例】

配置 trap 的发送条件为 testcomplete。

```
[H3C-hwping-administrator-icmp] send-trap testcomplete
```

4.1.22 sendpacket passroute

【命令】

sendpacket passroute

undo sendpacket passroute

【视图】

HWPing 测试组视图

【参数】

无

【描述】

sendpacket passroute 命令用来设置路由表旁路，**undo sendpacket passroute** 命令用来关闭路由表旁路。

缺省情况下，关闭路由表旁路。

路由表旁路功能是指远端主机将不进行通常的路由表查找，而直接发送报文到相连网络上的主机。如果主机所在网络不是直连的，就返回错误。例如，在接口上 ping 一个无路由的本地主机时可以使用本功能。

【举例】

设置在发送 ICMP 报文的时候不要查找路由表。

```
[H3C-hwping-administrator-icmp] sendpacket passroute
```

4.1.23 source-interface

【命令】

source-interface *interface-type interface-number*

undo source-interface

【视图】

HWPing 测试组视图

【参数】

interface-type：接口类型。

interface-number：接口编号。

【描述】

source-interface 命令用来配置发送测试包的源接口，**undo source-interface** 命令用来取消已配置的源接口。

缺省情况下，未配置发送测试包的源接口。

【举例】

配置发送测试包的源接口为 Ethernet1。

```
[H3C-hwping-administrator-dhcp] source-interface ethernet 1
```

4.1.24 source-ip

【命令】

source-ip *ip-address*

undo source-ip

【视图】

HWPing 测试组视图

【参数】

ip-address：测试的源 IP 地址。

【描述】

source-ip 命令用来配置本次测试的源 IP 地址，**undo source-ip** 命令取消已配置的源地址。

缺省情况下，使用发送测试报文的接口的 IP 地址作为源 IP 地址。

【举例】

配置本次测试的源 IP 地址为 192.168.1.1。

```
[H3C-hwping-administrator-icmp] source-ip 192.168.1.1
```

4.1.25 source-port

【命令】

source-port *port-number*

undo source-port

【视图】

HWPing 测试组视图

【参数】

port-number：测试的源端口号，范围为 1～65535。

【描述】

source-port 命令用来配置本次测试的源端口号，**undo source-port** 命令用来取消已配置的端口号。

对于 TCP 类型的测试，当使用此命令指定源端口时，只有第一次测试能够成功（一次测试中进行探测的次数通过 **count** 命令进行配置），后续测试将会失败。若不指定源端口，系统会自动选择没有使用的端口发送报文，所有测试均可成功。

【举例】

配置本次测试的源端口号为 8000。

```
[H3C-hwping-administrator-icmp] source-port 8000
```

4.1.26 test-type

【命令】

test-type *type*

【视图】

HWPing 测试组视图

【参数】

test-type：测试的类型，可以为以下关键字：

- **dhcp**：DHCP 测试。
- **ftp**：FTP 连接测试。

- **http**：HTTP 连接测试。
- **icmp**：ICMP 类型。
- **jitter**：对 UDP 报文传输的延时的变化进行分析。
- **snmpquery**：SNMP 测试。
- **tcpprivate**：指定端口（非知名端口）的 TCP 连接测试。
- **tcppublic**：对 7 号端口的 TCP 连接测试。
- **udpprivate**：指定端口（非知名端口）的 UDP 连接测试。
- **udppublic**：对 7 号端口的 UDP 连接测试。

缺省的类型为 **icmp**。

【描述】

test-type 命令用来配置测试的类型。

HWPing 可以测试的类型有 DHCP、FTP、HTTP、ICMP、Jitter、SNMP、TCP 以及 UDP。

【举例】

设置测试的类型为 FTP。

```
[H3C-hwping-administrator-ftp] test-type ftp
```

4.1.27 test-enable

【命令】

test-enable

undo test-enable

【视图】

HWPing 测试组视图

【参数】

无

【描述】

test-enable 命令用来执行 HWPing 测试，**undo test-enable** 命令用来取消测试。

📖 **说明：**

执行 HWPing 测试后不能自动显示测试结果，需要使用 **display hwping** 命令来显示测试结果。

相关配置可参考命令 **display hwping**。

【举例】

在“wgw-testicmp”测试组中执行 HWPing 测试。

```
[H3C-hwping-wgw-testicmp] test-enable
```

4.1.28 test-failtimes

【命令】

test-failtimes *times*

undo test-failtimes

【视图】

HWPing 测试组视图

【参数】

times：连续测试失败的次数，取值范围 1～15。缺省值为 1 次。

【描述】

test-failtimes 命令用来设置 HWPing 测试连续多少次测试失败之后向网管发送 Trap。**undo test-failtimes** 命令用来恢复连续测试失败的次数的缺省值。

📖 说明：

一次测试中可以包含多次探测。

【举例】

设置 HWPing 测试连续测试失败的次数为 3。

```
[H3C-hwping-administrator-icmp] test-failtimes 3
```

4.1.29 timeout

【命令】

timeout *time*

undo timeout

【视图】

HWPing 测试组视图

【参数】

time：超时时间，取值范围为 1～60，超时时间的缺省值为 3 秒

【描述】

timeout 命令用来配置测试操作的超时时间，命令 **undo timeout** 用来将超时时间恢复到缺省值。

【举例】

设置超时时间为 10 秒。

```
[H3C-hwping-administrator-icmp] timeout 10
```

4.1.30 tos

【命令】

tos *value*

undo tos

【视图】

HWPing 测试组视图

【参数】

value：HWPing 测试报文头中的 ToS 域值，取值范围 0～255，缺省未设置 ToS。

【描述】

tos 命令用来配置 HWPing 测试报文头中的 ToS 域值，**undo tos** 命令用来取消 HWPing 测试报文头中的 ToS 域值。

该参数相当于防火墙的 ping 命令中的“**-o**”参数。

【举例】

配置 HWPing 测试报文头中的 ToS 域值为 1。

```
[H3C-hwping-administrator-ftp] tos 1
```

4.1.31 ttl

【命令】

ttl *number*

undo ttl

【视图】

HWPing 测试组视图

【参数】

number：HWPing ICMP 测试报文生存时间，取值范围 1～255。缺省值为 20。

【描述】

ttl 命令用来配置 HWPing ICMP 测试报文生存时间，**undo ttl** 命令用来恢复 HWPing ICMP 测试报文生存时间的缺省值。

所谓报文生存时间，实际上是指测试报文在网络中可以经过的跳数。该参数相当于防火墙的 ping 命令中的“-**h**”参数。

📖 **说明：**

此命令适用于除 DHCP 类型外的其它测试类型。当配置了 **sendpacket passroute** 命令时，**ttl** 命令不起作用。

【举例】

配置 HWPing ICMP 测试报文生存时间为 16。

```
[H3C-hwping-administrator-icmp] ttl 16
```

4.1.32 username

【命令】

username *name*

undo username

【视图】

HWPing 测试组视图

【参数】

name：登录 FTP 服务器时所需的用户名，长度为 1～32 个字符。

【描述】

username 命令用来配置登录 FTP 服务器时所需的用户名，**undo username** 命令用来取消已配置的用户名。

缺省情况下，未配置登录 FTP 服务器时所需的用户名。

📖 **说明：**

此命令仅对 FTP 类型的测试操作适用。

相关配置可参考命令 **password**、**ftp-operation**。

【举例】

配置登录 FTP 服务器的用户名为“administrator”。

```
[H3C-hwping-administrator-ftp] username administrator
```

4.1.33 vpninstance

【命令】

vpninstance *name*

undo vpninstance

【视图】

HWPing 测试组视图

【参数】

name：指定的 VPN instance 的名字。

【描述】

vpninstance 命令用来设置 ICMP 的 VPN instance 信息。**undo vpninstance** 命令用来取消 ICMP 的 VPN instance 信息。

缺省情况下，未设置 ICMP 的 VPN instance 信息。

【举例】

设置 ICMP 的 VPN instance 信息为 vpn1。

```
[H3C-hwping-administrator-icmp] vpninstance vpn1
```

4.2 HWPing 服务器端命令

4.2.1 hwping-server enable

【命令】

hwping-server enable

undo hwping-server enable

【视图】

系统视图

【参数】

无

【描述】

hwping-server enable 命令用来使能 HWPing 服务器功能，**undo hwping-server enable** 用来取消 HWPing 服务器功能。

缺省情况下，关闭 HWPing 服务器功能。

进行 Jitter、指定端口的 UDP 测试和指定端口的 TCP 测试时，如果将本公司设备作为 HWPing 测试的服务器，则需要在服务器上启动 HWPing 服务才能进行测试。

只有使能了 HWPing 服务器功能，HWPing 服务器才能发挥作用。

相关配置可参考命令 **hwping-agent enable**、**hwping-server tcpconnect**、**hwping-server udpconnet**。

【举例】

使能 HWPing 服务器。

```
[H3C] hwping-server enable
```

4.2.2 hwping-server tcpconnect

【命令】

hwping-server tcpconnect *ip-address port-number*

undo hwping-server tcpconnect *ip-address port-number*

【视图】

系统视图

【参数】

ip-address：HWPing 服务器 TCP 监听服务的 IP 地址。

port-number：HWPing 服务器 TCP 监听服务的端口号，范围为 1～50000。

【描述】

hwping-server tcpconnect 命令用来创建 TCP 监听服务，**undo hwping-server tcpconnect** 命令用来删除已建立的 TCP 监听服务。

当 HWPing 客户端进行指定端口的 TCP 连接测试时，如果将本公司设备作为 HWPing 测试的服务器，则必须在服务器上创建 TCP 监听服务，测试才能完成。

相关配置可参考命令 **hwping-server enable**。

【举例】

创建 IP 地址为 10.1.1.1，端口号为 9000 的 TCP 监听服务。

```
[H3C] hwping-server tcpconnect 10.1.1.1 9000
```

4.2.3 hwping-server udpecho

【命令】

hwping-server udpecho *ip-address port-number*

undo hwping-server udpecho *ip-address port-number*

【视图】

系统视图

【参数】

ip-address：HWPing 服务器 UDP 监听服务的 IP 地址。

port-number：HWPing 服务器 UDP 监听服务的端口号，范围为 1～49999。

【描述】

hwping-server udpecho 命令用来创建 HWPing 服务器 UDP 监听服务，**undo hwping-server udpecho** 命令用来删除已建立的 HWPing 服务器 UDP 监听服务。

当 HWPing 客户端进行 Jitter 测试或指定端口的 UDP 测试时，如果将本公司设备为 HWPing 测试的服务器，则必须在服务器上创建 UDP 监听服务，测试才能完成。

配置 UDP 监听服务时，如果配置了系统已监听的端口号，当在进行 UDP 类型的测试时测试将不成功，但配置仍存在。

相关配置可参考命令 **hwping-server enable**。

【举例】

创建 IP 地址为 10.1.1.1，端口号为 9000 的 UDP 监听服务。

```
[H3C] hwping-server udpecho 10.1.1.1 9000
```

第5章 文件管理命令

5.1 文件系统命令

5.1.1 boot bootrom

【命令】

boot bootrom *file-url*

【视图】

用户视图

【参数】

file-url：Flash Memory 中 BootRom 的文件路径和名称。BootRom 中的文件名必须带扩展名。

【描述】

boot bootrom 命令用来升级 BootRom。

【举例】

升级防火墙的 BootRom。

```
<H3C> boot bootrom secpath.btm
```

5.1.2 cd

【命令】

cd *directory*

【视图】

用户视图

【参数】

directory：目标目录名。

【描述】

cd 命令用来改变防火墙当前配置用户的当前路径，改变防火墙当前工作路径为指定存在的目录。

缺省情况下，为“flash:”。

【举例】

修改防火墙当前工作路径为 test。

```
<H3C> pwd
flash:
<H3C> cd test
<H3C> pwd
flash:/test
```

5.1.3 copy

【命令】

copy *filename_source filename_dest*

【视图】

用户视图

【参数】

filename_source：源文件名。

filename_dest：目标文件名或目录名。

【描述】

copy 命令用来复制文件。

若目标文件名与已经存在的目录名重名，则将文件复制到该目录下；若目标文件名与已经存在的文件名重名，将提示是否覆盖。

若要复制的文件为隐藏文件时，系统会提示“% Access failure”访问权限不足。

【举例】

```
<H3C> pwd
flash:
<H3C> dir
Directory of flash:/

   1   -rw-   7654528  Oct 10 2002 10:10:10   system
   2   -rw-         4  Aug 23 2052 15:44:54   snmpboots
   3   -rw-       300  Aug 23 2052 15:45:58   config.cfg

15621 KB total (8140 KB free)
```

将文件 config.cfg 从 Flash 中拷贝到 backup 中（backup 目录应预先建好）。

```
<H3C> copy config.cfg backup
Copy flash:/config.cfg to flash:/backup/config.cfg ?[Y/N]:y
```

```
%Copy file flash:/config.cfg to flash:/backup/config.cfg...Done.

<H3C> cd backup
<H3C> dir
Directory of flash:/backup/

   1   -rw-       300  Aug 23 2052 15:57:46   config.cfg

15621 KB total (8137 KB free)
```

5.1.4 delete

【命令】

delete [**/unreserved**] { *filename* | **flash:** }

【视图】

用户视图

【参数】

/unreserved：表示彻底删除指定文件，删除的文件将不可恢复。

filename：要删除的文件名（含路径信息）。

flash:：删除 flash 根目录下的所有文件。

【描述】

delete 命令用来删除防火墙存储设备中的指定文件。

delete 命令支持“*”通配符。

使用不带参数的 **delete** 命令删除文件，是将文件放在回收站目录中，删除的文件可以使用 **undelete** 命令恢复。若要从回收站中删除该文件，使用 **reset recycle-bin** *filename* 命令。

使用带参数（**/unreserved**）的 **delete** 命令可彻底删除指定文件，删除的文件不可恢复。

若要删除的文件为隐藏文件时，系统会提示“% Access failure”访问权限不足。

使用 **dir** 命令不显示已经删除的文件信息；可使用 **dir /all** 命令显示所有文件信息，其中包括删除到回收站中的文件的信息。

⚠ 注意：

当系统中只有一个应用程序文件时（即 system 文件），禁止删除该文件。

【举例】

删除文件 flash:/test/test.txt。

```
<H3C> delete flash:/test/test.txt
Delete flash:/test/test.txt?[Y/N]:y
%Delete file flash:/test/test.txt...Done.
```

5.1.5 detach

【命令】

detach *web-bind-filename* [*http-filename*]

【视图】

用户视图

【参数】

web-bind-filename：要解包的捆绑文件名。

http-filename：解包后的 Web 文件名。

【描述】

detach 命令用来解包捆绑 Web 文件的文件。

如果要解包的文件没有捆绑 Web 文件，则提示文件中没有捆绑 Web 文件；如果没有指定解包出的 Web 文件名，则 Web 文件名缺省为 http.zip。

【举例】

解包捆绑 web 文件的文件。

```
<H3C> dir
Directory of flash:/

   1   -rw-   8691281  Jun 16 2009 06:46:36   system
   2   -rw-      1830  Jun 17 2009 07:47:16   config.cfg

15621 KB total (7126 KB free)

<H3C> detach config.cfg
  No http file!
<H3C> dir
Directory of flash:/

   1   -rw-   8691281  Jun 16 2009 06:46:36   system
```

```
   2   -rw-      1830  Jun 17 2009 07:47:16   config.cfg

15621 KB total (7126 KB free)

<H3C> detach system
    System file length 7856557 bytes, http file length 834724 bytes.
<H3C> dir
Directory of flash:/

   1   -rw-   8691281  Jun 16 2009 06:46:36   system
   2   -rw-      1830  Jun 17 2009 07:47:16   config.cfg
   3   -rw-    834724  Jun 18 2009 02:22:39   http.zip
```

5.1.6 dir

【命令】

dir [**/all**] [*file-url* | **flash:**]

【视图】

用户视图

【参数】

/all：显示所有的文件（包括回收站中的文件）。

file-url：显示的文件或目录名（含路径信息）。

flash:：显示 flash 中的所有文件。

【描述】

dir 命令用来显示防火墙存储设备中的指定文件或目录的信息。

缺省情况下，显示当前路径下的文件信息。

支持使用通配符“*”匹配。

使用 **dir /all** 命令显示所有文件信息，包括回收站中的文件信息，回收站中的文件的名字用“[ ]”括起来表示，例如[temp.cfg]。这种已删除文件可以使用 **undelete** 命令恢复，若要从回收站中彻底删除该文件，使用 **reset recycle-bin** 命令。

【举例】

显示 flash 中的文件。

```
<H3C> dir flash:
Directory of flash:/

   1   -rw-   5878540  Jul 05 2004 10:39:36   AR46XX-V3.30-0006.BIN
```

```
   2   -rw-       670  Sep 15 2004 11:46:51   config.cfg
   3   -rw-   8271372  Aug 17 2004 14:04:15   ar46.bin
   4   -rw-   8701964  Sep 22 2004 14:25:49   main.bin
   5   -rw-       670  Sep 30 2004 10:49:15   ar46.cfg

31750 KB total (9427 KB free)
```

5.1.7 execute

【命令】

execute { *filename* | **flash:** }

【视图】

系统视图

【参数】

filename：批处理文件名（含路径），以“.bat”为后缀。

flash:：指定存储设备为 flash。若要执行 flash 根目录下的名为 abc.bat 的批处理文件，命令格式应输入 flash:/abc.bat。

【描述】

execute 命令用来执行指定的批处理文件。

批处理命令逐条执行批处理文件中的命令行；批处理文件中不能包含不可见字符。如果发现有不可见字符，批处理命令则退出当前执行过程，并且不进行回退操作。

批处理命令的执行过程相当于手工逐条执行的自动化过程。批处理命令不保证每一条命令的执行，批处理命令本身不进行热备份处理；批处理文件中不限制命令的形式和内容。

【举例】

执行 flash:/目录下的 test.bat 批处理文件。

```
[H3C] execute flash:/test.bat
```

5.1.8 file prompt

【命令】

file prompt { **alert** | **quiet** }

【视图】

系统视图

【参数】

alert：由于用户操作（比如删除文件操作）而可能导致数据破坏或丢失时，进行交互式确认。

quiet：由于用户操作（比如删除文件操作）而可能会导致数据的破坏或丢失时，不作提示。

【描述】

file prompt 命令用来修改防火墙文件操作的提醒方式。

缺省情况下，为 **alert** 提醒方式。

如果将文件操作的提醒方式设置为 **quiet**，则不会对用户的危险操作（比如删除文件操作）给出提示，虽然这类操作有可能导致数据的丢失。

【举例】

设置防火墙文件操作的提醒方式为 **quiet**。

```
[H3C] file prompt quiet
```

设置防火墙文件操作的提醒方式为 **alert**。

```
[H3C] file prompt alert
```

5.1.9 format

【命令】

format *device-name*

【视图】

用户视图

【参数】

device-name：设备名。

【描述】

format 命令用来格式化存储设备。

格式化操作将导致指定的存储设备上所有的文件丢失，并且不可恢复。

【举例】

格式化 flash。

```
<H3C> format flash:
All data on flash: will be lost, proceed with format? [Y/N]:
Format flash: completed
```

5.1.10 mkdir

【命令】

mkdir *directory*

【视图】

用户视图

【参数】

directory：目录名。

【描述】

mkdir 命令用来在指定存储设备的指定目录下创建目录。

创建的目录名不能与指定目录下其它目录或文件名重名。

【举例】

创建目录 dd。

```
<H3C> mkdir dd
%Created dir flash:/dd.
```

5.1.11 more

【命令】

more *filename*

【视图】

用户视图

【参数】

filename：文件名。

【描述】

more 命令用来显示指定文件。

若要显示的文件为隐藏文件时，系统会提示“% Access failure”访问权限不足。

缺省情况下，文件系统以文本形式显示文件，即显示一个文件的内容。

【举例】

显示文件 test.txt 的内容。

```
<H3C> more test.txt
AppWizard has created this test application for you.
```

```
This file contains a summary of what you will find in each of the files that
make up your test application.
Test.dsp
This file (the project file) contains information at the project level and is
used to build a single project or subproject. Other users can share the project
(.dsp) file, but they should export the makefiles locally.
```

5.1.12 move

【命令】

move *filename_source filename_dest*

【视图】

用户视图

【参数】

filename_source：源文件名。

filename_dest：目标文件名。

【描述】

move 命令用来移动文件。

若目标文件名是一个已经存在的目录，则将文件移入该目录，并保持原文件名不变；若目标文件名与已经存在的文件名重名，将提示是否覆盖。

若要移动的文件为隐藏文件时，系统会提示“% Access failure”访问权限不足。

【举例】

```
<H3C> dir
 Directory of flash:/
   1   -rw-   2145123  Jul 12 2001 12:28:08   AR46.bin
   2   -rw-       595   Jul 12 2001 10:47:50  config.cfg
   3   drw-         0  Jul 12 2001 19:41:20  test
6477 KB total (2144 KB free)
<H3C> dir flash:/test/
Directory of flash:/test/
   1   drw-         -  Jul 12 2001 20:23:37   subdir
   2   -rw-       595  Jul 12 2001 20:13:19   config.cfg
   3   -rw-        50  Jul 12 2001 20:08:32   sample.txt
6477 KB total (2144 KB free)
```

移动文件从 flash:/test/sample.txt 到 flash:/sample.txt。

```
<H3C> move flash:/test/sample.txt flash:/sample.txt
Move flash:/test/sample.txt to flash:/sample.txt?[Y/N]:y
```

```
%Moved file flash:/test/sample.txt to flash:/sample.txt
<H3C> dir
 Directory of flash:/
   1   -rw-   2145123  Jul 12 2001 12:28:08    ne80.bin
   2   -rw-       595   Jul 12 2001 10:47:50   config.cfg
   3   drw-         0   Jul 12 2001 19:41:20   test
   4   -rw-        50   Jul 12 2001 20:26:48   sample.txt
6477 KB total (2144 KB free)
<H3C> dir flash:/test/
Directory of flash:/test/
   1   drw-             Jul 12 2001 20:23:37   subdir
   2   -rw-       595   Jul 12 2001 20:13:19   config.cfg
6477 KB total (2144 KB free)
```

5.1.13 pwd

【命令】

pwd

【视图】

用户视图

【参数】

无

【描述】

pwd 命令用来显示当前路径。

若没有设置当前路径，操作将出错。

【举例】

显示当前路径。

```
<H3C> pwd
flash:/test
```

5.1.14 rename

【命令】

rename *source-name new-name*

【视图】

用户视图

【参数】

source-name：源文件名或目录名。

new-name：重命名后的文件名或目录名。

【描述】

rename 命令用来重命名文件或目录。

若重命名后的文件名或目录名与已经存在的文件名或目录名重名，则执行失败。

若要重命名的文件为隐藏文件时，系统会提示“% Access failure”访问权限不足。

⚠ 注意：

当系统中只有一个应用程序文件时（即 system 文件），禁止修改其文件名，否则在升级防火墙应用程序时，容易造成无法启动。

【举例】

```
<H3C> dir
 Directory of flash:/
   1   -rw-   2145123  Jul 12 2001 12:28:08   system
   2   -rw-       595  Jul 12 2001 10:47:50   config.cfg
   3   drw-         -  Jul 12 2001 19:41:20   test
   4   -rw-        50  Jul 12 2001 20:26:48   sample.txt
6477 KB total (2144 KB free)
```

重命名文件 sample.txt 为 sample.bak。

```
<H3C> rename sample.txt sample.bak
Rename flash:/sample.txt to flash:/sample.bak ?[Y/N]:y
%Renamed file flash:/sample.txt to flash:/sample.bak
<H3C> dir
 Directory of flash:/
   1   -rw-   2145123  Jul 12 2001 12:28:08   system
   2   -rw-       595  Jul 12 2001 10:47:50   config.cfg
   3   drw-         -  Jul 12 2001 19:41:20   test
   4   -rw-        50  Jul 12 2001 20:29:55   sample.bak
6477 KB total (2144 KB free)
```

5.1.15 reset recycle-bin

【命令】

reset recycle-bin [*filename* | **flash:**] [**/force**]

【视图】

用户视图

【参数】

filename：要删除的文件名(需指定路径)。

flash:：删除 flash 根目录下的所有文件。

/force：清空指定目录中回收站的文件，如果未指定则清空当前目录中回收站的文件。

【描述】

reset recycle-bin 命令用来彻底删除回收站中的文件。

此命令支持“*”通配符。用 **delete** 命令删除文件是将文件放在回收站目录中；但如果想要彻底删除此文件，可以使用 **reset recycle-bin** 命令。

【举例】

删除回收站中的指定文件。

```
<H3C> reset recycle-bin flash:/p1h_logic.out
Clear flash:/plh_logic.out?[Y/N]
```

清空回收站。

```
<H3C> reset recycle-bin /force
Clear files in recycle-bin directly?[Y/N]:y
%Cleared file flash:/test/~/a.cfg.
%Cleared file flash:/test/~/b.cfg.
%Cleared file flash:/test/~/c.cfg.
Finished.
```

5.1.16 rmdir

【命令】

rmdir *directory*

【视图】

用户视图

【参数】

directory：目录名。

【描述】

rmdir 命令用来删除目录。

要删除的目录必须为空目录。删除该目录后，此目录下的回收站中的文件将无法恢复。

【举例】

```
<H3C> dir
 Directory of flash:/
   1   drw-          -  Jul 12 2001 20:23:37   subdir
   2   -rw-        595  Jul 12 2001 20:13:19   config.cfg
6477 KB total (5944 KB free)
```

删除目录 subdir。

```
<H3C> rmdir subdir
Rmdir flash:/subdir?[Y/N]:y
The file in the recycle-bin of this directory can not be restored after removing
 the directory! Continue?[Y/N]:y
...
%Removed directory flash:/subdir.
<H3C> dir
 Directory of flash:/
   1   -rw-        595  Jul 12 2001 20:13:19   config.cfg
6477 KB total (5944 KB free)
```

5.1.17 undelete

【命令】

undelete { *filename* | **flash:** }

【视图】

用户视图

【参数】

filename：要恢复的文件名。

flash:：恢复 flash 根目录中的所有文件。

【描述】

undelete 命令用来恢复删除的文件。

恢复的文件名如果与现有的目录名重名，则执行失败；若与当前存在的文件名重名，将会提示是否覆盖。

【举例】

```
<H3C> dir /all
Directory of flash:/
```

```
   1   -rw-       595  Jul 12 2001 20:13:19   config.cfg
   2   -rw-        50  Jul 12 2001 20:09:23   [sample.bak]
6477 KB total (2144 KB free)
```

恢复删除的文件 sample.bak。

```
<H3C> undelete sample.bak
Undelete flash:/test/sample.bak?[Y/N]:y
%Undeleted file flash:/test/sample.bak
<H3C> dir /all
 Directory of flash:/
   1   -rw-        50  Jul 12 2001 20:34:19   sample.bak
   2   -rw-       595  Jul 12 2001 20:13:19   config.cfg
6477 KB total (2144 KB free)
```

5.1.18 upgrade

【命令】

upgrade bootrom [**full**]

【视图】

用户视图

【参数】

bootrom：升级 Bootrom 程序。

full：升级全部 Bootrom。

【描述】

upgrade 命令用来升级 Bootrom 程序。

SecPath 防火墙的 Bootrom 程序可以在线升级。使用 upgrade 命令在线升级 Bootrom 程序时，将 Bootrom 程序从升级软件包中解出，写到 Bootrom 中。

当使用 **upgrade bootrom** 命令进行升级时，必须确保名为“bootrom”的升级软件包存在于 Flash 的根目录下；当使用 **upgrade bootrom full** 命令进行升级时，必须确保名为“bootromfull”的升级软件包存在于 Flash 的根目录下。

【举例】

升级防火墙的 BootRom，假定升级软件包已存放在 Flash 的根目录下，文件名为 bootromfull。

```
<H3C> upgrade bootrom full
```

5.2 FTP 服务器配置命令

5.2.1 display ftp-server

【命令】

display ftp-server

【视图】

所有视图

【参数】

无

【描述】

display ftp-server 命令用来显示当前 FTP 服务器的各项参数。

进行 FTP 参数设置后，可通过此命令查看设置结果。

【举例】

显示 FTP 服务器参数设置结果。

```
<H3C> display ftp-server
   FTP server is running
   Max user number       1
   User count            0
   Timeout value(in minute)       30
   Put Method                     fast
```

以上显示信息表示：FTP 服务器已经启动，支持同时登录的最大用户数为 1 个，现在登录的用户数为 0 个，FTP 用户的超时时间为 30 分钟，文件传输方式为快速方式。

5.2.2 display ftp-user

【命令】

display ftp-user

【视图】

所有视图

【参数】

无

【描述】

display ftp-user 命令用来显示当前 FTP 用户的各项参数。

【举例】

显示 FTP 用户参数设置。

```
<H3C> display ftp-user
Username      HostIP       port     Idle     HomeDir
ftpuser       10.110.3.5   1024     2        flash:/ftpuser
```

以上显示信息表示：有一个 FTP 用户和 FTP 服务器建立了连接，该用户的用户名为 ftpuser，远程主机 IP 地址为 10.110.3.5，远程端口号为 1024，授权目录为 flash:/ftpuser，现在，已经有 2 分钟没有向 FTP 服务器发送服务请求。

5.2.3 display ftp-server source-ip

【命令】

display ftp-server source-ip

【视图】

所有视图

【参数】

无

【描述】

display ftp-server source-ip 命令用来显示当前为 FTP Server 设置的源 IP 地址。

如果为 FTP Server 指定了源接口，则此命令显示的是该接口的 IP 地址；如果没有为 FTP Server 指定源接口和源 IP 地址，则显示 0.0.0.0。

【举例】

显示当前为 FTP Server 设置的源 IP 地址。

```
<H3C> display ftp-server source-ip
The source IP specified is 0.0.0.0
```

5.2.4 ftp server enable

【命令】

ftp server enable

undo ftp server

【视图】

系统视图

【参数】

无

【描述】

ftp server enable 命令用来启动 FTP 服务器，允许 FTP 用户登录，**undo ftp server** 命令用来关闭 FTP 服务器，禁止 FTP 用户登录。

缺省情况下，系统关闭 FTP 服务器功能。

【举例】

关闭 FTP 服务器。

```
[H3C] undo ftp server
```

5.2.5 ftp-server source-interface

【命令】

ftp-server source-interface *interface-type interface-number*

undo ftp-server source-interface

【视图】

系统视图

【参数】

interface-type interface-number：源接口类型及接口号。

【描述】

ftp-server source-interface 命令用来为 FTP Server 指定源接口，**undo ftp-server source-interface** 命令用来删除为 FTP Server 指定的源接口。

源接口必须是本地存在的接口，否则命令提示不成功。配置源接口后，FTP Server 发送报文中的源 IP 地址为源接口的 IP 地址；删除源接口后，FTP Server 发送报文中的源 IP 地址为出接口的 IP 地址。

缺省情况下，发送报文中的源 IP 地址为出接口的 IP 地址。

📖 **说明：**

指定源 IP 地址和指定源接口命令是互斥的，后配置的命令将覆盖先前配置的命令。

【举例】

为 FTP Server 指定源接口为 ethernet0/0/0。

```
[H3C] ftp-server source-interface Ethernet 0/0/0
```

5.2.6 ftp-server source-ip

【命令】

ftp-server source-ip *ip-address*

undo ftp-server source-ip

【视图】

系统视图

【参数】

ip-address：源 IP 地址。

【描述】

ftp-server source-ip 命令用来为 FTP Server 指定发送报文中的源 IP 地址，**undo ftp-server source-ip** 命令用来删除为 FTP Server 指定的源 IP 地址。

指定的源 IP 地址必须是本地地址，否则命令提示不成功。删除源 IP 地址后，FTP Server 发送报文中的源 IP 地址为出接口的 IP 地址。

缺省情况下，发送报文中的源 IP 地址为出接口的 IP 地址。

📖 说明：

指定源 IP 地址和指定源接口命令是互斥的，后配置的命令将覆盖先前的配置。

【举例】

为 FTP Server 指定发送报文中的源 IP 地址为 192.168.0.1。

```
[H3C] ftp-server source-ip 192.168.0.1
```

5.2.7 ftp timeout

【命令】

ftp timeout *minutes*

undo ftp timeout

【视图】

系统视图

【参数】

minutes：连接空闲超时时间，单位为分钟，范围为 1～35791。缺省情况下，连接空闲超时时间为 30 分钟。

【描述】

ftp timeout 命令用来设置连接空闲超时时间，**undo ftp timeout** 命令用来恢复缺省的连接空闲超时时间。

用户登录到 FTP 服务器，与之建立了连接，若连接异常中断或用户非正常中断连接，FTP 服务器是无法知道的。因而，连接仍保持着。为处理这类情况，应设置连接空闲超时时间。如果连接在一定时间内没有进行命令交互，FTP 服务器即可认为连接已经失效，而断开连接。

【举例】

设置连接空闲超时时间为 36 分钟。

```
[H3C] ftp timeout 36
```

5.2.8 ftp update

【命令】

ftp update { **fast** | **normal** }

undo ftp update

【视图】

系统视图

【参数】

fast：快速升级方式。

normal：普通升级方式。

【描述】

ftp update 命令用来设置 FTP 升级方式，**undo ftp update** 用来恢复缺省的 FTP 升级方式。

缺省情况下，FTP 升级方式为快速升级方式。

用户登录到 FTP Server，使用 **put** 命令上载文件的过程中，FTP Server 中文件的更新有两种方式，快速升级方式与普通升级方式。

- 快速升级方式，即 FTP Server 在全部接收完用户上载的文件后，才开始将该文件写入 Flash 中。采用这种方式，即使文件传送过程发生断电等异常情况，也不会损坏防火墙的现有文件。

- 普通升级方式，即 FTP Server 一边接收用户的文件，一边将其写入 Flash 中。采用这种方式，可能会因为断电等异常情况致使防火墙现有文件被损坏。与快速升级方式相比，普通升级方式只需要防火墙有较少的空闲内存。

📖 **说明：**

当 FTP Server 将文件写入 Flash 中时，禁止用户使用 **reboot** 命令重启设备。

【举例】

设置 FTP 升级方式为普通升级方式。

```
[H3C] ftp update normal
```

5.3 FTP 客户端命令

📖 **说明：**

当使用防火墙的 FTP 客户端命令登录到 FTP 服务器时，由于 FTP 服务器的版本不同，FTP 客户端命令的执行结果和提示信息可能会有所差异。

5.3.1 ascii

【命令】

ascii

【视图】

FTP client 视图

【参数】

无

【描述】

ascii 命令用来设置传输的数据类型为 ASCII 格式。

缺省情况下，数据类型为 ASCII 模式。

【举例】

设置传输的数据类型为 ASCII 格式

```
[ftp] ascii
200 Type set to A.
```

5.3.2 binary

【命令】

binary

【视图】

FTP client 视图

【参数】

无

【描述】

binary 命令用来设置文件传输的数据类型为二进制格式。

【举例】

设置文件传输类型支持二进制模式。

```
[ftp] binary
200 Type set to I.
```

5.3.3 bye

【命令】

bye

【视图】

FTP client 视图

【参数】

无

【描述】

bye 命令用来终止与远程 FTP server 的连接，并退回到用户视图。

【举例】

终止与远程 FTP server 的连接，并退回到用户视图。

```
[ftp] bye
<H3C>
```

5.3.4 cd

【命令】

cd *pathname*

【视图】

FTP client 视图

【参数】

pathname：路径名。

【描述】

cd 命令用来改变远程 FTP 服务器上的工作路径。

用户访问 FTP 服务器上的另一目录时，可使用本命令。

【举例】

改变工作路径到 d:/temp。

```
[ftp] cd d:/temp
```

5.3.5 cdup

【命令】

cdup

【视图】

FTP client 视图

【参数】

无

【描述】

cdup 命令用来改变工作路径到上一级目录。

当用户退出当前目录，返回上层目录时，使用本命令。

【举例】

改变工作路径到上一级目录。

```
[ftp] cdup
```

5.3.6 close

【命令】

close

【视图】

FTP client 视图

【参数】

无

【描述】

close 命令用来终止与远程 FTP server 的连接，仍保持在 FTP client 视图。

该命令同时终止与远程 FTP Server 的控制连接和数据连接。

【举例】

终止与远程 FTP server 的连接，保持在 FTP client 视图。

```
[ftp] close
[ftp]
```

5.3.7 debugging

【命令】

debugging

undo debugging

【视图】

FTP client 视图

【参数】

无

【描述】

debugging 命令用来打开 debugging 开关，**undo debugging** 命令用来关闭 debugging 开关。

缺省情况下，关闭 FTP client 命令 debugging 开关。

【举例】

打开 debugging 调试开关。

```
[ftp] debugging
```

5.3.8 delete

【命令】

delete *remotefile*

【视图】

FTP client 视图

【参数】

remotefile：文件名。

【描述】

delete 命令用来删除指定的文件。

【举例】

删除文件 temp.c。

```
[ftp] delete temp.c
```

5.3.9 dir

【命令】

dir [*remotefile* [*localfile*]]

【视图】

FTP client 视图

【参数】

remotefile：查询的目录或文件名。

localfile：存储列表的本地文件名。

【描述】

dir 命令用来查询目录下的所有文件或指定的文件。*localfile* 指定要存储列表的本地文件，若没有指定 *localfile*，列表输出将显示在终端屏幕上。

【举例】

查询文件 temp.c。

```
[ftp] dir temp.c
```

5.3.10 disconnect

【命令】

disconnect

【视图】

FTP client 视图

【参数】

无

【描述】

disconnect 命令用来终止与远程 FTP server 的连接，仍保持在 FTP client 视图。该命令同时终止与远程 FTP Server 的控制连接和数据连接。

【举例】

终止与远程 FTP server 的连接，保持在 FTP client 视图。

```
[ftp] disconnect
```

5.3.11 display ftp source-ip

【命令】

display ftp source-ip

【视图】

所有视图

【参数】

无

【描述】

display ftp source-ip 命令用来显示当前为 FTP Client 设置的源 IP 地址。

如果为 FTP Client 指定了源接口，则此命令显示的是该接口的 IP 地址；如果没有为 FTP Client 指定源接口和源 IP 地址，则显示为 0.0.0.0。

【举例】

显示当前为 FTP Client 设置的源 IP 地址。

```
<H3C> display ftp source-ip
The source IP you specified is 0.0.0.0
```

5.3.12 ftp

【命令】

ftp [*host* [*port*]] [**source-interface** *interface-type interface-number* | **source-ip** *ip-address*]

【视图】

用户视图

【参数】

host：远程 FTP server 的 IP 地址或主机名称。

port：远程 FTP server 的端口号。

interface-type interface-number：指定 FTP 客户端的源接口类型和编号。

ip-address：指定 FTP 客户端的源地址。

【描述】

ftp 命令用来与远程 FTP 服务器建立控制连接，并进入 FTP client 视图。

【举例】

连接到地址为 1.1.1.1 的远程 FTP 服务器。

```
<H3C> ftp 1.1.1.1
```

5.3.13 ftp source-interface

【命令】

ftp source-interface *interface-type interface-number*

undo ftp source-interface

【视图】

系统视图

【参数】

interface-type interface-number：源接口类型及接口号。

【描述】

ftp source-interface 命令用来为 FTP Client 指定源接口，**undo ftp source-interface** 命令用来删除为 FTP Client 指定的源接口。

源接口必须是本地存在的接口，否则命令提示不成功。配置源接口后，FTP Client 发送报文中的源 IP 地址为源接口的 IP 地址；删除源接口后，FTP Client 发送报文中的源 IP 地址为出接口的 IP 地址。

缺省情况下，发送报文中的源 IP 地址为出接口的 IP 地址。

📖 说明：

指定源 IP 地址和指定源接口命令是互斥的，后配置的命令将覆盖先前的配置。

【举例】

为 FTP Client 指定发送报文中的源接口为 ethernet0/0/0。

```
[H3C] ftp source-interface ethernet0/0/0
```

5.3.14 ftp source-ip

【命令】

ftp source-ip *ip-address*

undo ftp source-ip

【视图】

系统视图

【参数】

ip-address：源 IP 地址。

【描述】

ftp source-ip 命令用来为 FTP Client 指定发送报文中的源 IP 地址，**undo ftp source-ip** 命令用来删除为 FTP Client 指定的源 IP 地址。

指定的源 IP 地址必须是本地地址，否则命令提示不成功。删除源 IP 地址后，FTP Client 发送报文中的源 IP 地址为出接口的 IP 地址。

缺省情况下，发送报文中的源 IP 地址为出接口的 IP 地址。

📖 说明：

指定源 IP 地址和指定源接口命令是互斥的，后配置的命令将覆盖先前的配置。

【举例】

为 FTP Client 指定发送报文中的源 IP 地址为 192.168.0.1。

```
[H3C] ftp source-ip 192.168.0.1
```

5.3.15 get

【命令】

get *remotefile* [*localfile*]

【视图】

FTP client 视图

【参数】

localfile：本地文件名。

remotefile：远程 FTP server 上文件名。

【描述】

get 命令用来下载远程文件并存储在本地。

缺省情况下，如果没有指定本地文件名，则认为与远程 FTP server 上文件同名。

【举例】

下载 temp1.c 文件，并以 temp.c 文件名保存。

```
[ftp] get temp1.c temp.c
```

5.3.16 lcd

【命令】

lcd

【视图】

FTP client 视图

【参数】

无

【描述】

lcd 命令用来获得 FTP client 本地的工作路径。

【举例】

显示本地的工作路径。

```
[ftp] lcd
% Local directory now flash:.
```

5.3.17 ls

【命令】

ls [*remotefile*] [*localfile*]

【视图】

FTP client 视图

【参数】

remotefile：查询的远程文件。

localfile：保存的本地文件名。

【描述】

ls 命令用来查询指定的文件。

缺省情况下，不带任何参数时将显示所有的文件和目录。

【举例】

查询文件 temp.c。

```
[ftp] ls temp.c
```

5.3.18 mkdir

【命令】

mkdir *pathname*

【视图】

FTP client 视图

【参数】

pathname：目录名。

【描述】

mkdir 命令用来在远程 FTP server 上建立目录。

【举例】

在远程 FTP 服务器上建立目录 test。

```
[ftp] mkdir test
```

5.3.19 open

【命令】

open *ipaddr* [*port*]

【视图】

FTP client 视图

【参数】

ipaddr：远程 FTP server 的 IP 地址。

port：远程 FTP server 的端口号。

【描述】

open 命令用来与远程 FTP server 建立控制连接。

【举例】

与主机 10.110.3.1 FTP 服务器建立 FTP 连接。

```
[ftp] open 10.110.3.1
```

5.3.20 passive

【命令】

passive

undo passive

【视图】

FTP client 视图

【参数】

无

【描述】

passive 命令用来设置数据传输的方式为被动方式，**undo passive** 命令用来设置数据传输的方式为主动方式。

缺省情况下，数据传输方式为被动方式。

【举例】

设置数据传输的方式为被动方式。

```
[ftp] passive
```

5.3.21 put

【命令】

put *localfile* [*remotefile*]

【视图】

FTP client 视图

【参数】

localfile：本地的文件名。

remotefile：远程 FTP server 上的文件名。

【描述】

put 命令用来将本地的文件上传到远程 FTP server。

缺省情况下，如果没有指定远程服务器上的文件名，则认为与本地文件同名。

【举例】

将本地 temp.c 文件上传到远程 FTP server，并以 temp1.c 文件名保存。

```
[ftp] put temp.c temp1.c
```

5.3.22 pwd

【命令】

pwd

【视图】

FTP client 视图

【参数】

无

【描述】

pwd 命令用来显示远程 FTP server 上的工作目录。

【举例】

显示远程 FTP server 上的工作目录。

```
[ftp] pwd
"d:/temp" is current directory.
```

5.3.23 quit

【命令】

quit

【视图】

FTP client 视图

【参数】

无

【描述】

quit 命令用来终止与远程 FTP server 的连接，并退回到用户视图。

【举例】

终止与远程 FTP server 的连接，并退回到用户视图。

```
[ftp] quit
221 Server closing.
<H3C>
```

5.3.24 remotehelp

【命令】

remotehelp [*protocol-command*]

【视图】

FTP client 视图

【参数】

protocol-command：FTP 协议命令。

【描述】

remotehelp 命令用来显示 FTP 协议命令的帮助。

【举例】

查看协议命令 **user** 的语法。

```
[ftp] remotehelp user
214 Syntax: USER <sp> <username>
```

5.3.25 rename

【命令】

rename *filename1 filename2*

【视图】

FTP client 视图

【参数】

filename1：FTP Server 上的原文件名。

filename2：修改后的文件名。

【描述】

rename 命令用来在 FTP Client 端对 FTP Server 上的文件名进行重命名。

该命令可以与不同厂家的产品或软件兼容，即 FTP Server 为其他厂家的路由器或应用程序均可。

📖 **说明：**

现在 FTP Server 软件在安装时有一些功能是可选的，比如 rename 、delete 等（默认情况是关闭）。若用户希望在 FTP Client 端能够实现 **rename** 功能，请先在 FTP Server 端选中 rename 选项。

【举例】

将 FTP Server 上的文件 config.cfg 重命名为 secpath.cfg。

```
[ftp] rename config.cfg secpath.cfg
```

5.3.26 rmdir

【命令】

rmdir *pathname*

【视图】

FTP client 视图

【参数】

pathname：远程 FTP server 上的目录名。

【描述】

rmdir 命令用来删除 FTP 服务器上指定的目录。

【举例】

删除 FTP 服务器上的 d:/temp1 目录。

```
[ftp] rmdir d:/temp1
```

5.3.27 user

【命令】

user *username* [*password*]

【视图】

FTP client 视图。

【参数】

username：登录用户名。

password：登录密码。

【描述】

user 命令用来进行 FTP 用户登录。

【举例】

以 FTP 服务器上用户名为 tom，口令为 bjhw 的用户身份登录。

```
[ftp] user tom bjhw
```

5.3.28 verbose

【命令】

verbose

undo verbose

【视图】

FTP client 视图

【参数】

无

【描述】

verbose 命令用来打开 verbose 开关，用以显示 FTP 服务器返回信息，**undo verbose** 命令用来关闭 verbose 开关，用以关闭显示 FTP 服务器返回信息。

缺省情况下，verbose 开关设置为打开状态。

【举例】

关闭 verbose 开关。

```
[ftp] undo verbose
```

5.4 TFTP 配置命令

5.4.1 display tftp source-ip

【命令】

display tftp source-ip

【视图】

所有视图

【参数】

无

【描述】

display tftp source-ip 命令用来显示当前为 TFTP Client 设置的源 IP 地址。

如果为 TFTP Client 指定了源接口，则此命令显示的是该接口的 IP 地址；如果没有为 TFTP Client 指定源接口和源 IP 地址，则显示为 0.0.0.0。

【举例】

显示当前为 TFTP Client 设置的源 IP 地址。

```
<H3C> display tftp source-ip
The source IP you specify is 0.0.0.0
```

5.4.2 tftp

【命令】

tftp *host* [**source-interface** *interface-type interface-number* | **source-ip** *ip-address*] { **get** | **sget** | **put** } *source-filename* [*destination-filename*]

【视图】

用户视图

【参数】

host：TFTP 服务器的 IP 地址或主机名。

interface-type interface-number：指定 TFTP 客户端的源接口类型和编号。

source-ip *ip-addres*：指定 FTP 客户端的源 IP 地址。

source-filename：源文件名。

destination-filename：目标文件名。

get：表示普通的下载文件操作，在这种方式下防火墙一边接收用户文件，一边将其写入 Flash，故当 *destination-filename* 指定为 **system** 时，新的系统文件会实时覆盖原有的系统文件。如果系统文件下载失败（如网络断开等原因），由于原有的系统文件已经被覆盖，会造成防火墙无法启动。这种升级方法安全系数较低。

sget：表示带有保护措施的下载操作。在这种方式下，安全网关将接收到的用户文件保存到内存中，等用户文件全部接收完毕，才将其写到 Flash 中。这样如果文件下载失败（如网络断开等原因），因为原有的文件没有被覆盖，所以仍保留在 Flash 中。这种方法安全系数较高，但需要较大的内存空间和 Flash 空间。不能使用此方式下载系统应用程序。

put：表示进行上传文件操作。

【描述】

tftp 命令用来上传文件到 TFTP 服务器或下载文件至本地。

相关配置可参考命令 **tftp-server acl**。

【举例】

将 TFTP 服务器根目录下的 config.cfg 文件下载到本地。TFTP 服务器的 IP 地址为 1.1.254.2，下载到本地之后以文件名 config.bak 保存。

```
<H3C> tftp 1.1.254.2 get config.cfg flash:/config.bak
```

将存储设备 Flash 根目录下的文本文件 config.cfg 上传到 TFTP 服务器缺省路径下。TFTP 服务器的 IP 地址为 1.1.254.2，config.cfg 文件在 TFTP 服务器上以文件名 config.bak 保存。

```
<H3C> tftp 1.1.254.2 put flash:/config.cfg config.bak
```

5.4.3 tftp-server acl

【命令】

tftp-server acl *acl-number*

【视图】

系统视图

【参数】

acl-number：IP 地址访问列表标号，基本标号范围 2000～2999。

【描述】

tftp-server acl 命令用来设置可以访问 TFTP 服务器的访问控制列表号。

相关配置可参考命令 **tftp**。

【举例】

设置可以访问 TFTP 服务器的访问控制列表号为 2001。

```
[H3C] tftp-server acl 2001
```

5.4.4 tftp source-interface

【命令】

tftp source-interface *interface-type interface-number*

undo tftp source-interface

【视图】

系统视图

【参数】

interface-type interface-number：源接口类型及接口号。

【描述】

tftp source-interface 命令用来为 TFTP Client 指定源接口，**undo tftp source-interface** 命令用来删除为 TFTP Client 指定的源接口。

源接口必须是本地存在的接口，否则命令提示不成功。配置源接口后，TFTP Client 发送报文中的源 IP 地址为源接口的 IP 地址；删除源接口后，TFTP Client 发送报文中的源 IP 地址为出接口的 IP 地址。

缺省情况下，发送报文中的源 IP 地址为出接口的 IP 地址。

📖 **说明：**

指定源 IP 地址和指定源接口命令是互斥的，后配置的命令将覆盖先前的配置。

【举例】

为 TFTP Client 指定发送报文中的源接口为 ethernet0/0/0。

```
[H3C] tftp source-interface ethernet0/0/0
```

5.4.5 tftp source-ip

【命令】

tftp source-ip *ip-address*

undo tftp source-ip

【视图】

系统视图

【参数】

ip-address：源 IP 地址。

【描述】

tftp source-ip 命令用来为 TFTP Client 指定发送报文中的源 IP 地址，**undo tftp source-ip** 命令用来删除为 TFTP Client 指定的源 IP 地址。

指定的源 IP 地址必须是本地地址，否则命令提示不成功。删除源 IP 地址后，TFTP Client 发送报文中的源 IP 地址为出接口的 IP 地址。

缺省情况下，发送报文中的源 IP 地址为出接口的 IP 地址。

🕮 **说明：**

指定源 IP 地址和指定源接口命令是互斥的，后配置的命令将覆盖先前的配置。

【举例】

为 TFTP Client 指定发送报文中的源 IP 地址为 192.168.0.1。

```
[H3C] tftp source-ip 192.168.0.1
```

5.5 配置文件管理命令

5.5.1 display current-configuration

【命令】

display current-configuration [**interface** *interface-type* [*interface-number*] | **configuration** [**isp** | **zone** | **interzone** | **system** | **user-interface** | **radius-template**]] [**by-linenum**] [| { **begin** | **include** | **exclude** } *string*]

【视图】

所有视图

【参数】

interface：显示接口的配置。

interface-type：接口类型。

interface-number：接口编号。

configuration：显示指定的配置。

isp：服务提供商类型。

luser：本地用户类型。

zone：区域类型。

interzone：区域间类型。

system：显示系统配置。

user-interface：显示用户接口的配置。

radius-template：显示 RADIUS 模板信息。

by-linenum：显示信息带有行编号。

|：使用正则表达式过滤显示防火墙的配置。

begin：显示以指定文字（*string*）开头的配置。

include：显示包含指定文字（*string*）的配置。

exclude：显示不含指定文字（*string*）的配置。

string：正则表达式文字。

【描述】

display current-configuration 命令用来显示防火墙当前的配置。

对于某些当前配置的参数，如果与缺省参数相同，则不显示。

当用户完成一组配置之后，需要验证是否配置正确，则可以执行 **display current-configuration** 命令来查看当前生效的参数。对于某些参数，虽然用户已经配置，但如果这些参数所在的功能如果没有生效，则不予显示。

相关配置可参考命令 **save**，**reset saved-configuration**，**display saved-configuration**。

【举例】

显示防火墙当前生效的配置参数。

```
<H3C> display current-configuration
#
radius scheme system
#
domain system
```

```
#
local-user admin
 password simple admmin
 service-type telnet
#
interface Aux0
 async mode flow
#
interface Ethernet1/0
#
interface Ethernet1/1
#
interface GigabitEthernet0/0
 ip address 172.16.2.2 255.255.255.0
#
interface GigabitEthernet0/1
 ip address 192.168.2.1 255.255.255.0
#
interface NULL0
#
interface LoopBack0
 ip address 3.3.3.3 255.255.255.255
#
firewall zone local
 set priority 100
#
firewall zone trust
 add interface GigabitEthernet0/0
 add interface GigabitEthernet0/1
 set priority 85
#
firewall zone untrust
 set priority 5
#
firewall zone DMZ
 set priority 50
#
firewall interzone local trust
#
firewall interzone local untrust
#
firewall interzone local DMZ
#
```

```
firewall interzone trust untrust
#
firewall interzone trust DMZ
#
firewall interzone DMZ untrust
#
bgp 1
 undo synchronization
 group ibgp internal
 peer ibgp next-hop-local
 peer ibgp connect-interface LoopBack0
 peer 2.2.2.2 group ibgp
 peer 1.1.1.1 group ibgp
 group ebgp external
 peer 192.168.2.2 group ebgp as-number 3
#
rip
 undo summary
 network 172.16.0.0
 network 3.0.0.0
#
user-interface con 0
user-interface aux 0
user-interface vty 0 4
 authentication-mode scheme
#
 sysname H3C
#
 dvpn service enable
#
 firewall packet-filter enable
 firewall packet-filter default permit
#
 firewall statistic system enable
#
return
```

5.5.2 display saved-configuration

【命令】

display saved-configuration [**by-linenum**]

【视图】

所有视图

【参数】

by-linenum：显示信息带有行编号。

【描述】

display saved-configuration 命令用来显示防火墙下次启动时加载的配置文件。

相关配置可参考命令 **save**，**reset saved-configuration**，**display current-configuration**。

【举例】

显示防火墙下次启动时加载的配置文件，

```
<H3C> display saved-configuration
#
 sysname H3C
#
 dvpn service enable
#
 firewall packet-filter enable
#
 firewall url-filter parameter add ^select^
 firewall url-filter parameter add ^insert^
 firewall url-filter parameter add ^update^
 firewall url-filter parameter add ^delete^
 firewall url-filter parameter add ^drop^
 firewall url-filter parameter add --
 firewall url-filter parameter add '
 firewall url-filter parameter add ^exec^
 firewall url-filter parameter add %27
#
 firewall statistic system enable
#
radius scheme system
#
domain system
#
interface Aux0
 async mode flow
#
interface GigabitEthernet0/0
```

```
 ip address 192.168.1.1 255.255.255.0
#
interface GigabitEthernet0/1
 ip address 192.168.4.1 255.255.255.0
#
interface NULL0
#
interface LoopBack1
 ip address 200.200.200.200 255.255.255.0
#
firewall zone local
 set priority 100
#
firewall zone trust
 add interface NULL0
 add interface GigabitEthernet0/0
 add interface GigabitEthernet0/1
 set priority 85
#
firewall zone untrust
 set priority 5
#
firewall zone DMZ
 set priority 50
#
firewall interzone local trust
#
firewall interzone local untrust
#
firewall interzone local DMZ
#
firewall interzone trust untrust
#
firewall interzone trust DMZ
#
firewall interzone DMZ untrust
#
bgp 1
 undo synchronization
 group ex2 external
 peer 192.168.1.2 group ex2 as-number 2
 group ex4 external
 peer 192.168.4.2 group ex4 as-number 4
```

```
#
user-interface con 0
user-interface aux 0
user-interface vty 0 4
#
return
```

5.5.3 display startup

【命令】

display startup

【视图】

所有视图

【参数】

无

【描述】

display startup 命令用来查看系统保存的用于本次启动和下次启动的配置文件。

【举例】

显示系统保存的用于本次启动和下次启动的配置文件。

```
<H3C> display startup
  Startup saved-configuration file:          flash:/config.cfg
  Next startup saved-configuration file:     flash:/ipsec.cfg
```

5.5.4 display this

【命令】

display this

【视图】

所有视图

【参数】

无

【描述】

display this 命令用来显示所在视图的当前配置。

【举例】

显示所在视图的当前配置。

```
[H3C] display this
#
 sysname H3C
#
 dvpn service enable
#
 firewall packet-filter enable
 firewall packet-filter default permit
#
 firewall statistic system enable
#
 FTP server enable
#
```

5.5.5 reset saved-configuration

【命令】

reset saved-configuration

【视图】

用户视图

【参数】

无

【描述】

reset saved-configuration 命令用来删除 Flash 中保存的下次启动时的配置文件。

慎重执行该命令，最好在技术支持人员指导下使用。

当将一台已经使用过的防火墙用于新的应用环境，原有的配置文件不能适应新环境需求，需要对防火墙重新配置，这时，可以在删除原配置文件后，重新配置。

相关配置可参考命令 **save**，**display current-configuration**，**display saved-configuration**。

【举例】

删除 Flash 中保存的配置文件。

```
<H3C> reset saved-configuration
The saved configuration will be erased.
Are you sure?[Y/N]y
```

```
Configuration in the device is being cleared.
Please wait ...
....
Configuration in the device is cleared.
```

5.5.6 save

【命令】

save [*file-name* | **safely**]

【视图】

所有视图

【参数】

file-name：文件名，扩展名必须为 cfg。当没有指定 *file-name* 时，配置文件缺省保存到下次启动加载的配置文件中。

safely：不带 safely 参数表示快速保存配置文件，保存过程中不能对进行设备重启动、断电等。否则，会丢失配置文件。带有 **safely** 参数，保存配置文件的速度会慢一点。但是，如果保存过程中出现设备重启动，断电等问题，配置文件会在 Flash 中一直保存，不会丢失。

【描述】

save 命令用来保存当前配置信息到存储设备中。

当完成一组配置，并且已经达到预定功能时，则应将当前配置文件保存到存储设备中。缺省方式下，采用快速保存模式。对于电源稳定程度较好的环境，推荐使用默认的快速模式。对于电源环境恶劣，或者远程维护等情况，推荐使用带有 **safely** 参数的保存配置命令。

相关配置可参考命令**reset saved-configuration**，**display current-configuration**，**display saved-configuration**。

【举例】

保存当前配置文件到默认存储设备中。

```
<H3C> save
```

5.5.7 startup saved-configuration

【命令】

startup saved-configuration *filename*

【视图】

用户视图

【参数】

filename：配置文件名。

【描述】

startup saved-configuration 命令用来设置系统下次启动时使用的配置文件。设置完成后，系统下次启动时会以此文件作为启动文件。

📖 说明：

配置文件的命名：

config.cfg：是用户保存配置的缺省文件名，名字由厂商规定，内容可由用户修改。

系统启动时配置文件的选择顺序分为如下三种情况：

(1) 如果用户没有设置跳过配置文件启动，就按下面 2)、3)的顺序进行选择；否则，以空配置启动。

(2) 如果用户指定了启动的配置文件，则按下面的顺序进行选择：

- 若配置文件存在，则以该文件为启动配置文件。
- 若配置文件不存在，则以空配置启动。

(3) 如果用户不指定启动配置文件，则按下面的顺序进行选择：

- 若 config.cfg 存在，则以 config.cfg 为启动文件。
- 若 config.cfg 不存在，则以空配置启动。

【举例】

设置系统下次启动时使用的配置文件名为 master.cfg。

```
<H3C> startup saved-configuration master.cfg
```

显示系统保存的用于启动的配置文件。

```
<H3C> display startup
  Startup saved-configuration file:          flash:/config.cfg
  Next startup saved-configuration file:     flash:/master.cfg
```

config.cfg 为系统缺省配置文件，master.cfg 为指定的下次启动使用的配置文件。

第6章 用户界面配置命令

6.1 用户界面配置命令

6.1.1 accounting commands scheme

【命令】

accounting commands scheme

undo accounting commands scheme

【视图】

用户界面视图

【参数】

scheme：通过 scheme 方案（这里指 TACACS 方案）实现按命令计费。

【描述】

accounting commands 命令用来配置 Terminal 用户登录用户界面后以命令行方式进行计费，**undo accounting commands** 用于取消 Terminal 用户的命令行计费。

缺省情况下，未设定命令行计费。

HWTACACS 协议支持按命令行数量进行统计计费。Terminal 用户每执行一条命令，向 TACACS 服务器发送一次命令统计报文，用以实现命令统计和计费。

如果配置了 TACACS 命令行计费功能后，TACACS 计费服务器由于某种原因不可达时，用户仍可以正常地执行命令，但命令计费功能终止。对于此情况，系统不会给出任何提示信息，也不进行任何的记录。

【举例】

配置 TACACS 服务器对 VTY0 用户按命令行进行计费。

```
[H3C] user-interface vty 0
[H3C-ui-vty0] accounting commands scheme
```

6.1.2 acl

【命令】

acl *acl-number* { **inbound** | **outbound** }

undo acl { **inbound** | **outbound** }

【视图】

用户界面视图

【参数】

acl-number：地址访问控制列表号，取值范围为 2000～3999。

inbound：表示对用户界面的呼入进行限制。

outbound：表示对用户界面的呼出进行限制。

【描述】

acl 命令用来通过引用 ACL 控制列表，对 VTY（Telnet、SSH 等）用户的呼入/呼出权限进行限制，**undo acl** 命令用来取消当前设置。

缺省情况下，不对 VTY 用户呼入/呼出进行限制。

【举例】

取消对 Telnet 呼出的限制。

```
[H3C-ui-vty0] undo acl outbound
```

6.1.3 authentication-mode

【命令】

authentication-mode { **password** | **scheme** [**command-authorization**] }

authentication-mode none

【视图】

用户界面视图

【参数】

password：设置进行本地密码验证方式。

scheme：设置进行 AAA 授权验证方式。

command-authorization：设置命令行授权，HWTACACS 协议支持对每条命令进行授权。授权通过，执行用户操作，否则拒绝执行。

none：设置验证方式为不验证。

【描述】

authentication-mode 命令用来设置登录用户界面的验证方式，**authentication-mode none** 命令用来设置验证方式为不验证，即登录用户界面不需要验证。

缺省情况下，VTY、AUX 类型用户界面验证方式为 **password**，其它类型用户界面验证方式为不需要验证。

相关命令请参考 **set authentication password**。

【举例】

使能本地口令验证。

```
[H3C-ui-vty0-4] authentication-mode password
```

6.1.4 auto-execute command

【命令】

auto-execute command *command*

undo auto-execute command

【视图】

用户界面视图

【参数】

command：需要自动执行的某条命令。

【描述】

auto-execute command 命令用来设置自动执行命令，**undo auto-execute command** 命令用来取消自动执行命令。

缺省情况下，未设定自动执行命令。

auto-execute command 命令使用时有如下的限制：

- 如果防火墙上只有一个 Console 口或只有一个 AUX 口（Console 口和 AUX 口共一个口），那么这个口将不支持 **auto-execute command**。
- 如果防火墙上有一个 Console 口和一个 AUX 口（共两个口）则 Console 口不支持 **auto-execute command**，AUX 口支持 **auto-execute command**。
- 对其他类型的接口，该命令不作限制。

用户在登录时自动执行某条在该终端上用 **auto-execute command** 配置好的命令，命令执行结束后，自动断开用户连接。

通常的用法是用 **auto-execute command** 为终端配置 Telnet 命令，使用户自动连接到指定的主机。

该命令的使用，将导致不能使用该用户界面对本系统进行常规的配置，需谨慎使用。

⚠ 注意：

在配置 **auto-execute command** 命令并保存配置（执行 **save** 操作）之前，要确保可以通过其他方法登录系统以去掉此配置。

【举例】

配置用户从 AUX 接口登录后，自动执行 **telnet** 10.110.100.1 命令。

```
[H3C-ui-aux0] auto-execute command telnet 10.110.100.1
```

6.1.5 databits

【命令】

databits { **5** | **6** | **7** | **8** }

undo databits

【视图】

用户界面视图

【参数】

5：数据位为 5 位。

6：数据位为 6 位。

7：数据位为 7 位。

8：数据位为 8 位。

【描述】

databits 命令用来设置用户界面的数据位，**undo databits** 命令用来恢复缺省的数据位。

缺省情况下，为 8 位数据位。

只有串口工作在异步流方式下时，配置才有效。

【举例】

设置数据位为 5 位。

```
[H3C-ui-aux0] databits 5
```

6.1.6 debugging vty

【命令】

debugging vty { **fsm** | **negotiate** }

undo debugging vty { **fsm** | **negotiate** }

【视图】

用户视图

【参数】

fsm：Telnet 状态机调试开关。

negotiate：VTY 选项协商调试开关。

【描述】

debugging vty 命令用来打开 VTY 的调试信息开关。**undo debugging vty** 用来关闭 VTY 协议的调试信息开关。

【举例】

打开 VTY 选项协商调试开关。

```
<H3C> debugging vty negotiate
```

6.1.7 display user-interface

【命令】

display user-interface [[*type-name*] *number*] [**summary**]

【视图】

所有视图

【参数】

type-name：用户界面的类型名。

number：用户界面编号。不键入 *type-name* 时，*number* 为绝对编号，取值为 0～38；键入 *type-name* 时，*number* 为相对编号，取值范围与用户界面类型有关。

summary：显示用户界面摘要信息。

【描述】

display user-interface 命令用来显示用户界面的相关信息。

【举例】

显示用户界面 0 的相关信息。

```
<H3C> display user-interface 0
   Idx  Type     Tx/Rx      Modem Privi Auth  Int
+ 0    CON 0    9600       -     3     N     -
```

```
  +    : Current user-interface is active.
  F    : Current user-interface is active and work in async mode.
  Idx  : Absolute index of user-interface.
  Type : Type and relative index of user-interface.
  Privi: The privilege of user-interface.
  Auth : The authentication mode of user-interface.
  Int  : The physical location of UIs.
  A    : Authentication use AAA.
  L    : Authentication use local database.
  N    : Current UI need not authentication.
  P    : Authentication use current UI's password.
```

显示用户界面 0 的摘要信息。

```
<H3C> display user-interface 0 summary
          0: U

   1 character mode users.     (U)
   1 total UIs in use.
   UI's name: con0
```

6.1.8 display users

【命令】

display users [**all**]

【视图】

所有视图

【参数】

all：显示所有用户界面用户的信息。

【描述】

display users 命令用来显示每个用户界面用户的登录信息。

【举例】

显示每个用户界面用户的状态信息。

```
<H3C> display users
        UI    Delay     Type   Ipaddress     Username        Userlevel
+ 0   CON 0   00:00:00                                          3
  34  VTY 0   00:00:56  TEL  192.168.1.2     teluser             0

 +   : Current operation user.
 F   : Current operation user work in async mode.
```

显示所有处于活动状态的终端线。其中各部分含义如下：

+：当前用户正在使用的用户界面。

UI：第一列数字是用户界面的绝对编号，第二列数字是用户界面的相对编号。

Delay：表明用户自最近一次输入到现在的时间间隔，格式为 hh:mm:ss。

Type：显示用户类型，如 Telnet、SSH。

Ipaddress：显示起始连接位置，即入连接的主机 IP 地址。

Username：显示使用该用户界面的用户名，即该用户的登入 username。当前正在使用的终端线是匿名登录，没有 AAA 验证，此项为空。

Userlevel：显示用户的权限，即用户级别（0-VISIT 参观，1-MONITOR 监控，2-CONFIG 配置，3-MANAGE 管理）。

在 Console 控制台上执行 **display users all**，有如下结果：

```
<H3C> display users all
        UI    Delay     Type   Ipaddress     Username        Userlevel
+ 0   CON 0   00:00:00                                          3
  33  AUX 0
+ 34  VTY 0   00:02:08  TEL  192.168.1.2     teluser             0
  35  VTY 1
  36  VTY 2
  37  VTY 3
  38  VTY 4

 +   :  User-interface is active.
 F   :  User-interface is active and work in async mode.
```

显示所有的终端线。“+”表示处于活动状态的终端线。

6.1.9 flow-control

【命令】

flow-control { **hardware** | **software** | **none** }

undo flow-control

【视图】

用户界面视图

【参数】

none：不进行流控。

software：进行软件流控。

hardware：进行硬件流控，只对 AUX 口有效。

【描述】

flow-control 命令用来对流控方式进行配置，**undo flow-control** 命令用来恢复流控方式的缺省值。

AUX 口缺省情况下，流控方式为硬件流控。

只有相应的串口工作在异步流模式下，配置有效。

在输出过程中，按<Ctrl+s>停止屏幕输出；按<Ctrl+q>继续输出。

【举例】

在用户界面视图下，配置软件流控。

```
[H3C-ui-console0] flow-control software
```

6.1.10 free user-interface

【命令】

free user-interface [*type-name*] *number*

【视图】

用户视图

【参数】

type-name：用户界面类型。

number：用户界面的绝对/相对编号。不键入 *type-name* 时，*number* 为绝对编号，取值为 0～38；键入 *type-name* 时，*number* 为相对编号，取值范围与用户界面类型有关。

【描述】

free user-interface *number* 命令用来断开第 *number* 个用户界面对应的用户。**free user-interface** *type-name number* 命令用来断开 *type-name* 类型中第 *number* 个用户界面对应的用户。

该命令不能断开使用 Web 界面登录的用户。

【举例】

断开 user-interface 0 对应的用户。

```
<H3C> free user-interface 0
```

6.1.11 history-command max-size

【命令】

history-command max-size *size-value*

undo history-command max-size

【视图】

用户界面视图

【参数】

size-value：历史缓冲区的大小，取值范围为 0～256。缺省情况下，*size-value* 值为 10，存放 10 条历史命令。

【描述】

history-command max-size 命令用来设置历史命令缓冲区的大小，**undo history-command max-size** 命令用来恢复历史命令缓冲区的大小。

【举例】

设置历史命令缓冲区的大小为 20 条。

```
[H3C-ui-console0] history-command max-size 20
```

6.1.12 idle-timeout

【命令】

idle-timeout *minutes* [*seconds*]

undo idle-timeout

【视图】

用户界面视图

【参数】

minutes：分钟数，范围为<0～35791>。

seconds：秒数，范围为<0～59>。

【描述】

idle-timeout 命令用来设置用户定时断连功能，**undo idle-timeout** 命令用来恢复用户定时断连的缺省值。

缺省情况下，超时时间为 10 分钟。

设置超时时间为 0 时，关闭定时断连功能，既永不超时断开连接。

【举例】

设置超时为 1 分钟 30 秒。

```
[H3C-ui-console0] idle-timeout 1 30
```

6.1.13 modem

【命令】

modem [**call-in** | **call-out** | **both**]

undo modem [**call-in** | **call-out** | **both**]

【视图】

用户界面视图

【参数】

call-in：仅允许呼入。

call-out：仅允许呼出。

both：允许呼入/呼出。

【描述】

modem 命令用来设置 Modem 呼入/呼出属性，**undo modem** 命令用来禁止呼入/呼出。

缺省情况下，为允许呼入/呼出。

modem 命令不带参数表示允许呼入/呼出。

undo modem 命令不带参数表示禁止呼入/呼出。

该命令只对 AUX 口有效，对 Console 口无效。

【举例】

设置 AUX 口的 Modem 呼入/呼出属性。

```
[H3C] user-interface aux 0
[H3C-ui-aux0] modem
```

6.1.14 modem auto-answer

【命令】

modem auto-answer

undo modem auto-answer

【视图】

用户界面视图

【参数】

无

【描述】

modem auto-answer 命令用来设置应答方式为自动应答方式，**undo modem auto-answer** 命令用来设置应答方式为手动方式。

缺省情况下，为手动应答。

该命令只对 AUX 口有效，对 Console 口无效。

在使用 Modem 拨号连接时，需要首先在相应的用户界面上设置 Modem 参数。

【举例】

设置应答方式为自动应答。

```
[H3C-ui-aux0] modem auto-answer
```

6.1.15 modem timer answer

【命令】

modem timer answer *seconds*

undo modem timer answer

【视图】

用户界面视图

【参数】

seconds：超时时间，以秒为单位，范围为<1～60>。

【描述】

modem timer answer 命令用来设置呼入连接建立时，从摘机到检测到载波的等待超时时间，**undo modem timer answer** 命令用来恢复缺省的等待超时时间。

缺省情况下，等待超时时间为 30 秒。

该命令只对 AUX 口有效，对 Console 口无效。

6.1.16 parity

【命令】

parity { **none** | **even** | **odd** | **mark** | **space** }

undo parity

【视图】

用户界面视图

【参数】

none：无校验。

even：进行偶校验。

odd：进行奇校验。

mark：进行 mark 校验。

space：进行 space 校验。

【描述】

parity 命令用来设置用户界面的校验位，**undo parity** 命令用来恢复用户界面的校验方式为无校验。

缺省情况下，无校验。

只有串口工作在异步流方式下时，配置才有效。

【举例】

将 AUX 口传输校验位设为奇校验。

```
[H3C-ui-aux0] parity odd
```

6.1.17 protocol inbound

【命令】

protocol inbound { **all** | **ssh** | **telnet** }

【视图】

VTY 类型的用户界面视图

【参数】

all：支持所有的协议，包括 Telnet 和 SSH。

ssh：支持 SSH 协议。

telnet：支持 Telnet 协议。

【描述】

protocol inbound 命令用来指定所在的用户界面所支持的协议。

缺省情况下，系统支持所有的协议，即支持 Telnet 和 SSH。

使用该命令指定所在用户界面支持的协议时，且在 SSH 使能的情况下，如果本机 rsa 密钥没有配置，则 SSH 仍然不可用。配置结果待下次登录请求时生效。

如果在该用户界面上配置支持的协议是 SSH，为确保登录成功，请您务必配置相应的验证方式为 **authentication-mode scheme**；若配置验证方式为

authentication-mode password 和 **authentication-mode none**，则 **protocol inbound ssh** 配置结果将失败。

相关配置可参考命令 **user-interface vty**。

【举例】

禁止 vty0 到 vty4 的 Telnet 功能，只支持 SSH 功能。

```
[H3C] user-interface vty 0 4
[H3C-ui-vty0-4] protocol inbound ssh
```

禁止 vty0 的 Telnet 功能，只支持 SSH。

```
[H3C] user-interface vty 0
[H3C-ui-vty0] protocol inbound ssh
```

6.1.18 screen-length

【命令】

screen-length *screen-length*

undo screen-length

【视图】

用户界面视图

【参数】

screen-length：屏幕分屏显示的行数，取值范围为 0～512。

【描述】

screen-length 命令用来设置终端屏幕的一屏行数，**undo screen-length** 命令用来恢复终端屏幕的一屏行数为 24 行。

缺省情况下，为 24 行。

screen-length 0 表示关闭分屏功能。

【举例】

设置屏幕的一屏行数为 30。

```
[H3C-ui-console0] screen-length 30
```

6.1.19 send

【命令】

send [*number* | **all** | *type-name number*]

【视图】

用户视图

【参数】

all：向所有用户界面发送消息。

type-name：用户界面的类型名。

number：用户界面的绝对/相对编号。

【描述】

send 命令用来在用户界面之间传递消息。

send all 向所有用户界面发送消息。

send *number* 向第 *number* 个用户界面发送消息（*number* 为绝对编号）。

send *type-name number* 向 *type-name* 类型中的第 *number* 个用户界面发送消息（*number* 为相对编号）。

【举例】

向 Console 口类型用户界面发送消息。

```
<H3C> send con 0
Enter message, end with CTRL+Z or Enter; abort with CTRL+C:
Hello,good morning!
Send message? [Y/N]
```

6.1.20 set authentication password

【命令】

set authentication password { **simple** | **cipher** } *password*

undo set authentication password

【视图】

用户界面视图

【参数】

simple：配置密码以明文显示。

cipher：配置密码以密文显示。

password：如果密码形式是 **simple**，则 *password* 必须是明文密码。如果密码形式是 **cipher**，则 *password* 可以是密文密码也可以是明文密码，结果视输入而定。明文密码可以是长度小于等于 16 的连续字符串，如：1234567。密文密码的长度必须是 24，并且必须是密文形式如：_(TT8F]Y\5SQ=^Q`MAF4<1!!。

【描述】

set authentication password 命令用来设置本地验证的口令，**undo set authentication password** 命令用来取消本地验证的口令。

不论配置的是明文密码还是密文密码，验证时必须输入明文形式的密码。

配置时必须指定是 **simple** 还是 **cipher**，如果指定 **simple** 形式，则配置文件中保存的是明文密码；如果指定 **cipher** 形式，则不管你输入的是 1 到 16 字节的明文密码，还是 24 位的密文密码，都一律显示为密文。

Telnet 配置用户缺省需要登录口令的验证（authentication-mode password）。如果没有配置口令（password），则将显示：

```
Login password has not been set !
```

相关命令请参考 **authentication-mode**。

【举例】

设置用户界面 vty 0～4 的本地验证口令为 pwd。

```
[H3C-ui-vty0-4] authentication-mode password
[H3C-ui-vty0-4] set authentication password simple pwd
```

6.1.21 shell

【命令】

shell

undo shell

【视图】

用户界面视图

【参数】

无

【描述】

shell 命令用来设置允许在用户界面上启动终端服务，**undo shell** 命令用来取消当前设置，若要启动 telnet 重定向，必须配置该命令。

缺省情况下，在所有的用户界面上启动终端服务。

需要对 **undo shell** 命令做几点限制如下：Console 口不支持该命令；如果防火墙上只有一个 AUX 口，而没有 Console 口（Console 口与 AUX 口共用），则此 AUX 口不支持该命令；对其他类型的用户界面不做限制。

【举例】

设置在虚拟终端（VTY）0 到 4 上终止终端服务。

```
[H3C] user-interface vty 0 4
[H3C-ui-vty0-4] undo shell
```

对于 Telnet 终端，登录后将显示：

```
The connection was closed by the remote host!
```

6.1.22 speed

【命令】

speed *speed-value*

undo speed

【视图】

用户界面视图

【参数】

speed-value：传输速率，单位为 bps。

【描述】

speed 命令用来设置用户界面的传输速率，**undo speed** 命令用来恢复用户界面的缺省传输速率。

缺省情况下，传输速率为 9600bps。

只有串口工作在异步流方式下时，该配置才有效。

异步串口支持的传输速率有：

- 1200bps
- 2400bps
- 4800bps
- 9600bps
- 19200bps
- 38400bps
- 57600bps
- 115200bps

【举例】

将用户界面的传输速率为 19200bps。

```
[H3C-ui-aux0] speed 19200
```

6.1.23 stopbits

【命令】

stopbits { **1.5** | **1** | **2** }

undo stopbits

【视图】

用户界面视图

【参数】

1.5：停止位为 1.5 位。

1：停止位为 1 位。

2：停止位为 2 位。

【描述】

stopbits 命令用来设置用户界面的停止位，**undo stopbits** 命令用来恢复缺省的用户界面停止位。

缺省情况下，停止位为 1 位。

只有串口工作在异步流方式下时，配置有效。

【举例】

设置用户界面的停止位为 1.5 位。

```
[H3C-ui-aux0] stopbits 1.5
```

6.1.24 user privilege

【命令】

user privilege level *level*

undo user privilege level

【视图】

用户界面视图

【参数】

level *level*：命令级别，范围为<0～3>。

【描述】

user privilege 命令用来配置从当前用户界面登录系统的用户所能访问的命令级别，**undo user privilege** 命令用来取消当前设置。

缺省情况下，CON 口用户界面对应的默认命令访问级别是 3，而其它 ui 对应的默认级别是 0。

如果用户界面下配置的命令级别访问权限与用户名本身对应的操作权限冲突，则以用户名本身对应的级别为准。例如：如果用户 007 本身对应权限为能访问 3 级命令，而用户界面 VTY 0 配置的命令级别访问权限为 2，则用户 007 从 VTY0 登录系统时，能访问 3 级及以下的命令。

【举例】

配置通过该用户界面登录系统的用户能访问的命令级别为 2。

```
[H3C-ui-vty0] user privilege level 2
```

6.1.25 user-interface

【命令】

user-interface [*type-keyword*] *number* [*ending-number*]

【视图】

系统视图

【参数】

type-keyword：用户界面（User-interface）的类型名称。

number：欲配置的第一个用户界面。

ending-number：欲配置的最后一条用户界面。

【描述】

user-interface 命令用来进入单一或多个用户界面视图。

本命令可以按用户界面视图的相对编号进行配置，也可以按绝对编号进行配置。按相对编号进行配置时，需要配置用户界面类型；按绝对编号进行配置时，直接配置编号即可。关于相对编号和绝对编号的编号原则请参考操作手册中“系统管理”的相应部分。

【举例】

进入 user-interface console 0 视图，可以对 console 0 进行配置。

```
[H3C] user-interface console 0
[H3C-ui-console0]
```

进入 user-interface vty 0 视图，可以对 vty 0 进行配置。

```
[H3C] user-interface vty 0
[H3C-ui-vty0]
```

进入 user-interface vty 视图，对 vty 0 到 3 进行配置。

```
[H3C] user-interface vty 0 3
[H3C-ui-vty0-3]
```

进入用户界面视图，对 user-interface 0 到 3 进行配置，其中包括 Console 口类型、Aux 口类型和 VTY 类型的用户界面，共 4 条，具体包括哪些类型的用户界面，根据防火墙配置的接口而定。

例如：如果防火墙不包括 Aux 口，下面的例子则针对一个 Console 口类型的用户界面和 3 个 VTY 类型的用户界面。

```
[H3C] user-interface 0 3
[H3C-ui0-3]
```

第7章 NTP 配置命令

7.1 NTP 配置命令

7.1.1 debugging ntp-service

【命令】

debugging ntp-service { **adjustment** | **authentication** | **event** | **filter** | **packet** | **parameter** | **refclock** | **selection** | **synchronization** | **validity** | **all** }

undo debugging ntp-service { **access** | **adjustment** | **authentication** | **event** | **filter** | **packet** | **parameter** | **refclock** | **selection** | **synchronization** | **validity** | **all** }

【视图】

用户视图

【参数】

adjustment：NTP 时钟调节调试开关。

all：NTP 的所有调试信息开关。

authentication：NTP 身份验证调试开关。

event：NTP 事件调试开关。

filter：NTP 过滤信息调试开关。

packet：NTP 包调试开关。

parameter：NTP 时钟参数调试开关。

refclock：NTP 参考时钟调试开关。

selection：NTP 时钟选择信息调试开关。

synchronization：NTP 时钟同步信息调试开关。

validity：NTP 远程主机的合法性调试开关。

【描述】

debugging ntp-service 命令用来打开 NTP 服务各项信息的调试开关，**undo debugging ntp-service** 命令用来关闭相应的调试开关。

缺省情况下，关闭所有调试信息开关。

【举例】

打开 NTP 事件调试开关。

```
<H3C> debugging ntp-service event
```

7.1.2 display ntp-service sessions

【命令】

display ntp-service sessions [**verbose**]

【视图】

所有视图

【参数】

verbose：指定显示 sessions 的详细信息。

【描述】

display ntp-service sessions 命令用来显示本地设备 NTP 服务维护的所有 sessions 状态。

不带参数 **verbose** 时，显示本地设备维护的所有 sessions 的简要信息；

带参数 **verbose** 时，显示本地设备维护的所有 sessions 的详细信息。

所显示的 NTP session 中，不包括组播类型和广播类型的 session，但是会统计到 session 总数中。

【举例】

显示本地设备 NTP 服务维护的信息。

```
<H3C> display ntp-service sessions
source        reference    stra reach  pollnow offset   delay    disper
**************************************************************************
[12345]1.0.1.11  LOCL(0)    3    377      64    1    199.53 26.1      9.7
Total associations : 1
note: 1 source(master),2 source(peer),3 selected,4 candidate,5 configured
```

表7-1 display ntp-service sessions 命令显示信息说明

显示信息	说明
source	源端 IP 地址
reference	参考时钟 id
stra	层数
reach	是否可达

显示信息	说明
poll	收发消息间隔
now	发消息之后的时间
offset	时钟偏差
delay	网络延时
disper	时钟离差
Total associations	总会话数
note: 1 source(master),2 source(peer),3 selected,4 candidate,5 configured	souceip 方括号中数字意义的注释

7.1.3 display ntp-service status

【命令】

display ntp-service status

【视图】

所有视图

【参数】

无

【描述】

display ntp-service status 命令用来显示 NTP 服务的状态信息。

【举例】

```
<H3C> display ntp-service status
Clock status: unsynchronized
 Clock stratum: 16
 Reference clock ID: none
 Nominal frequency: 100.0000 Hz
 Actual frequency: 100.0000 Hz
 Clock precision: 2^17
 Clock offset: 0.0000 ms
 Root delay: 0.00 ms
 Root dispersion: 0.00 ms
 Peer dispersion: 0.00 ms
 Reference time: 00:00:00.000 UTC Jan 1 1900(00000000.00000000)
```

显示信息的解释如下表：

表7-2 NTP 服务的状态信息

显示信息	意义
synchronized	表示本地系统被同步到一个远程 NTP 服务器或某个时钟源
unsynchronized	表示本地系统未被同步到任何一个远程 NTP 服务器
stratum	本地系统所处的 NTP stratum
reference	当本地系统已被同步到一个远程 NTP 服务器或某个时钟源时，指示远程服务器的地址或时钟源的标识。
nominal freq	本地系统硬件时钟的标称频率
actual freq	本地系统硬件时钟的实际频率
precision	本地系统时钟的精度
reference time	参考时间戳
offset	本地时钟相对 NTP 服务器的 offset
root delay	本地到主参考时钟总的 delay
root dispersion	本地相对主参考时钟的 dispersion
peer dispersion	远程 NTP 服务器的 dispersion

7.1.4 display ntp-service trace

【命令】

display ntp-service trace

【视图】

所有视图

【参数】

无

【描述】

display ntp-service trace 命令用来显示从本地设备回溯到参考时钟源的各个 NTP 时间服务器的简要信息。

从本地设备，沿着时间同步 NTP 服务器链，一直回溯到参考时钟源，并显示各个 NTP 服务器的简要信息。

【举例】

```
<H3C> display ntp-service trace
server4: stratum 4, offset 0.0019529, synch distance 0.144135
server3: stratum 3, offset 0.0124263, synch distance 0.115784
```

```
server2: stratum 2, offset 0.0019298, synch distance 0.011993
server1: stratum 1, offset 0.0019298, synch distance 0.011993 refid  'GPS
Reciever'
```

以上信息显示服务器 server4 的同步链，表示 server4 同步到 server3，server3 同步到 server2，server2 同步到 server1，server1 从参考时钟源 GPS Reciever 得到同步。

7.1.5 ntp-service access

【命令】

ntp-service access { **query** | **synchronization** | **server** | **peer** } *acl-number*

undo ntp-service access { **query** | **synchronization** | **server** | **peer** }

【视图】

系统视图

【参数】

query：允许控制查询权限。

synchronization：只允许服务器访问。

server：允许服务器访问与查询。

peer：完全访问权限。

acl-number：IP 地址访问列表标号，基本标号范围 2000～2999。

【描述】

ntp-service access 命令用来设置对本地设备服务的访问控制权限，**undo ntp-service access** 命令用来取消设置的访问控制权限。

缺省情况下，没有访问限制。

设置对本地设备 NTP 服务的访问控制权限。这里提供了一种最小限度的安全措施，更安全的方法是进行身份验证。当有一个访问请求时，按照最小访问限制到最大访问限制依次匹配，以第一个匹配的为准，匹配顺序为 **peer**，**server**，**synchronization**，**query**。

【举例】

设置允许第 2001 号访问列表中的设备可以对本地设备进行时间请求、查询控制、时间同步。

```
[H3C] ntp-service access peer 2001
```

只允许第 2111 号访问列表中的设备对本地设备进行时间请求、查询控制。

```
[H3C] ntp-service access server 2111
```

7.1.6 ntp-service authentication enable

【命令】

ntp-service authentication enable

undo ntp-service authentication enable

【视图】

系统视图

【参数】

无

【描述】

ntp-service authentication enable 命令用来设置 NTP-service 身份验证功能，**undo ntp-service authentication enable** 命令用来取消身份验证功能。

缺省情况下，无身份验证功能。

【举例】

启动 NTP 身份验证功能。

```
[H3C] ntp-service authentication enable
```

7.1.7 ntp-service authentication-keyid

【命令】

ntp-service authentication-keyid *number* **authentication-mode md5** *value*

undo ntp-service authentication-keyid *number*

【视图】

系统视图

【参数】

number：密钥编号，范围从 1～4294967295。

value：密钥字符串，1～32 个 ASCII 码字符。

【描述】

ntp-service authentication-keyid 命令用来设置NTP验证密钥，**undo ntp-service authentication-keyid** 命令用来取消 NTP 验证密钥。

缺省情况下，无验证密钥。

设置 NTP 验证密钥，只支持 MD5 验证。

【举例】

设置 MD5 身份验证密钥，密钥 ID 号为 10，密钥为 BetterKey。

```
[H3C] ntp-service authentication-keyid 10 authentication-mode md5 BetterKey
```

7.1.8 ntp-service broadcast-client

【命令】

ntp-service broadcast-client

undo ntp-service broadcast-client

【视图】

接口视图

【参数】

无

【描述】

ntp-service broadcast-client 命令用来配置 NTP 广播客户模式，**undo ntp-service broadcast-client** 命令用来取消 NTP 广播客户模式。

缺省情况下，不配置 NTP 广播客户服务。

指定本地设备上的本接口来接收 NTP 广播消息包，本地设备运行在客户端（broadcast-client）模式。本地设备首先侦听来自服务器的广播消息包，当接收到第一个广播消息包时，本地设备为了估计网络延迟，先启用一个短暂的 client/server 模式与远程服务器交换消息，然后，本地设备就进入 client 模式，继续侦听广播消息包的到来，根据到来的广播消息包，对本地时钟进行同步。

【举例】

配置在 Ethernet 1/0/1 接口上接收 NTP 广播消息。

```
[H3C] interface ethernet 1/0/1
[H3C-Ethernet1/0/1] ntp-service broadcast-client
```

7.1.9 ntp-service broadcast-server

【命令】

ntp-service broadcast-server [**authentication-keyid** *keyid* | **version** *number*] *

undo ntp-service broadcast-server

【视图】

接口视图

【参数】

authentication-keyid：定义身份验证密钥。

keyid：向广播客户端发送消息时使用的密钥 ID 号，范围 1～4294967295。

version：定义 NTP 版本号。

number：NTP 版本号，范围为 1～3。

【描述】

ntp-service broadcast-server 命令用来配置 NTP 广播服务器模式，**undo ntp-service broadcast-server** 命令用来取消 NTP 广播服务器模式。

缺省情况下，不配置广播服务、版本号缺省为 3。

指定本地设备上的一个接口来发送 NTP 广播消息包，本地运行在服务器（broadcast-server）模式，作为广播服务器，周期性地发送广播消息到广播客户端。

【举例】

配置在 Ethernet 1/0/0 接口上发送 NTP 广播消息包，用 4 号密钥进行加密，设置 NTP 版本号为 3。

```
[H3C] interface ethernet 1/0/0
[H3C-Ethernet1/0/0] ntp-service broadcast-server authentication-key 4 version 3
```

7.1.10 ntp-service in-interface disable

【命令】

ntp-service in-interface disable

undo ntp-service in-interface disable

【视图】

接口视图

【参数】

无

【描述】

ntp-service in-interface disable 命令用来设置禁止接口接收 NTP 消息，**undo ntp-service in-interface disable** 命令用来设置允许接口接收 NTP 消息。

缺省情况下，允许接口接收 NTP 消息。

【举例】

禁止接口接收 NTP 消息。

```
[H3C-Ethernet1/0/0] ntp-service in-interface disable
```

7.1.11 ntp-service max-dynamic-sessions

【命令】

ntp-service max-dynamic-sessions *number*

undo ntp-service max-dynamic-sessions

【视图】

系统视图

【参数】

number：本地允许建立 sessions 的数目，范围 0～100。

【描述】

ntp-service max-dynamic-sessions 命令用来设置本地允许建立的 sessions 的数目，**undo ntp-service max-dynamic-sessions** 命令用来恢复 sessions 数目的缺省值。

缺省情况下，允许建立 100 个 sessions。

【举例】

设置本地允许建立的 sessions 的数目为 50。

```
[H3C] ntp-service max-dynamic-sessions 50
```

7.1.12 ntp-service multicast-client

【命令】

ntp-service multicast-client [*X.X.X.X*]

undo ntp-service multicast-client [*X.X.X.X*]

【视图】

接口视图

【参数】

X.X.X.X：组播 IP 地址，D 类地址。

【描述】

ntp-service multicast-client 命令用来配置 NTP 组播客户模式，**undo ntp-service multicast-client** 命令用来取消 NTP 组播客户模式。

缺省情况下，不配置组播客户服务、*X.X.X.X* 缺省为 224.0.1.1。

指定本地设备上的一个接口来接收 NTP 组播消息包，本地设备运行在 client（multicast-client）模式。本地设备首先侦听来自服务器的组播消息包，当接收到第一个组播消息包时，本地服务器为了估计网络延迟，先启用一个短暂的 client/server 模式与远程服务器交换消息，然后，本地设备就进入 client 模式，继续倾听组播消息包的到来，根据到来的组播消息包，对本地时钟进行同步。

【举例】

配置在 Ethernet 1/0/0 接口上接收 NTP 组播消息包，组播消息包对应的组播组地址为默认的 224.0.1.1。

```
[H3C] interface ethernet 1/0/0
[H3C-Ethernet1/0/0] ntp-service multicast-client
```

7.1.13 ntp-service multicast-server

【命令】

ntp-service multicast-server [*X.X.X.X*] [**authentication-keyid** *keyid* | **ttl** *ttl-number* | **version** *number*] *

undo ntp-service multicast-server [*X.X.X.X*]

【视图】

接口视图

【参数】

X.X.X.X：组播 IP 地址，D 类地址，缺省为 224.0.1.1。

authentication-keyid：定义身份验证密钥。

keyid：向组播客户端发送消息时使用的密钥 ID 号，范围 1～4294967295。

ttl：定义组播包的生存期。

ttl-number：组播包生存期的大小，范围为 1～255。

version：定义 NTP 版本号。

number：NTP 版本号，范围为 1～3。

【描述】

ntp-service multicast-server 命令用来配置 NTP 组播服务器模式，**undo ntp-service multicast-server** 命令用来取消 NTP 组播服务器模式。

缺省情况下，不配置组播服务、IP 地址缺省为 224.0.1.1、版本号缺省为 3。

指定本地设备上的一个接口来发送 NTP 组播消息包，本地设备运行在服务器（multicast-server）模式，作为组播服务器周期性地发送组播消息到组播客户端。

【举例】

配置在 Ethernet 1/0/0 接口上发送 NTP 组播消息包，组播组地址为默认的 224.0.1.1，用 4 号密钥进行加密，设置 NTP 版本号为 3。

```
[H3C] interface ethernet 1/0/0
[H3C-Ethernet1/0/0] ntp-service multicast-server authentication-keyid 4 version 3
```

7.1.14 ntp-service refclock-master

【命令】

ntp-service refclock-master [*X.X.X.X*] [*layers-number*]

undo ntp-service refclock-master [*X.X.X.X*]

【视图】

系统视图

【参数】

X.X.X.X：参考时钟 IP 地址 127.127.1.u，u 的取值范围为 0～3。

layers-number：指定本地时钟所处的层数，范围为 1～15。

【描述】

ntp-service refclock-master 命令用来设置本地时钟作为 NTP 主时钟，**undo ntp-service refclock-master** 命令用来取消 NTP 主时钟设置。

X.X.X.X 缺省不指定、*layers-number* 缺省值为 8。

设置本地时钟作为 NTP 主时钟，为其它设备提供同步时间。*X.X.X.X* 为参考时钟 IP 地址 127.127.1.u，当不指定 IP 地址时，默认设置本地时钟为 NTP 主时钟；可以指定 NTP 主时钟所处的层次数。

【举例】

设置本地设备时钟作为 NTP 主时钟，为其他 peer 提供同步时间，*layers-number* 为 3。

```
[H3C] ntp-service refclock-master 3
```

7.1.15 ntp-service reliable authentication-keyid

【命令】

ntp-service reliable authentication-keyid *number*

undo ntp-service reliable authentication-keyid *number*

【视图】

系统视图

【参数】

number：密钥编号，范围从 1～4294967295。

【描述】

ntp-service reliable authentication-keyid 命令用来指定密钥是可信的，**undo ntp-service reliable authentication-keyid** 命令用来取消当前配置。

缺省情况下，不设置可信验证密钥。

当启用身份验证时，该命令用于指定一个或多个密钥是可信的，也就是说 client 只会同步到提供可信密钥的服务器，如果服务器提供的密钥不是可信的密钥，那么 client 不会与其同步。

【举例】

设置启用 NTP 身份验证，采用 MD5 加密方法，密钥 ID 号为 37，密钥为 BetterKey，指定该密钥为可信密钥。

```
[H3C] ntp-service authentication enable
[H3C] ntp-service authentication-keyid 37 authentication-mode md5 BetterKey
[H3C] ntp-service reliable authentication-keyid 37
```

7.1.16 ntp-service source-interface

【命令】

ntp-service source-interface *interface-type interface-number*

undo ntp-service source-interface

【视图】

系统视图

【参数】

interface-type：接口类型，与接口编号 *interface-number* 共同确定一个接口。

interface-number：接口编号，与接口类型 *interface-type* 共同确定一个接口。

【描述】

ntp-service source-interface 命令用来指定本地发送 NTP 消息的接口，**undo ntp-service source-interface** 命令用来取消当前配置。

指定本地发送接口后，NTP 消息的源地址将被设置为指定接口的主 IP 地址。

当不想本地设备上其它接口的 IP 地址成为应答消息的目的地址时，可以使用该命令指定一个特定接口来发送所有的 NTP 消息包。此时消息包中的源 IP 地址都用该接口的主 IP 地址。

【举例】

指定 NTP 所有输出消息包的源 IP 地址都用接口 Loopback0 的 IP 地址。

```
[H3C] ntp-service source-interface loopback 0
```

7.1.17 ntp-service unicast-peer

【命令】

ntp-service unicast-peer [**vpn-instance** *vpn-instance-name*] { *X.X.X.X* | *server-name* } [**version** *number* | **authentication-key** *keyid* | **source-interface** *interface-type interface-number* | **priority**] *

undo ntp-service unicast-peer [**vpn-instance** *vpn-instance-name*] { *X.X.X.X* | *server-name* }

【视图】

系统视图

【参数】

vpn-instance *vpn-instance-name*：指定 VPN 实例名，此时本地安全网关可以通过指定相应的 VPN 实例同步到远程服务器，远程服务器也能同步到本地服务器。

X.X.X.X：远程服务器 IP 地址。

server-name：远程服务器名字。

version：定义 NTP 版本号。

number：NTP 版本号，范围为 1～3。

authentication-keyid：定义身份验证密钥。

keyid：向该远程服务器发送消息使用的密钥 ID 号，范围为 1～4294967295。

source-interface：指定接口名称。

interface-type：接口类型，与接口编号 *interface-number* 共同确定一个接口。

interface-number：接口编号，与接口类型 *interface-type* 共同确定一个接口。本地设备给这个 peer 发送 NTP 消息时，消息包中的源 IP 地址从该接口获取。

priority：指定该服务器为优先选择的服务器。

【描述】

ntp-service unicast-peer 命令用来配置 NTP 对等体模式，**undo ntp-service unicast-peer** 命令用来取消 NTP 对等体模式。

缺省情况下，版本号缺省为 3、不支持身份验证、不是优先选择的服务器。

设置以 *X.X.X.X* 或 *server-name* 所指定的远程服务器作为本地的对等体，本地运行在 symmetric active 模式。*X.X.X.X* 是一个主机地址，不能为广播、组播地址或参考时钟的 IP 地址。在这种配置下，本地设备能同步到远程服务器，远程服务器也能同步到本地服务器。

【举例】

本地被配置成由 peer 128.108.22.44 提供同步时间，本地对等体也能为 peer 提供同步时间，版本号为 3。NTP 消息包的 IP 地址从 Loopback0 获得。

```
[H3C] ntp-service unicast-peer 128.108.22.44 version 3 source-interface loopback 0
```

7.1.18 ntp-service unicast-server

【命令】

ntp-service unicast-server [**vpn-instance** *vpn-instance-name*] { *X.X.X.X* | *server-name* } [**version** *number* | **authentication-keyid** *keyid* | **source-interface** *interface-type interface-number* | **priority**] *

undo ntp-service unicast-server [**vpn-instance** *vpn-instance-name*] { *X.X.X.X* | *server-name* }

【视图】

系统视图

【参数】

vpn-instance *vpn-instance-name*：指定 VPN 实例名，此时本地客户机可以通过指定的 VPN 实例同步到远程服务器，而远程服务器不会同步到本地客户机。

X.X.X.X：远程服务器 IP 地址。

server-name：远程服务器名字。

version：定义 NTP 版本号。

number：NTP 版本号，范围为 1～3。

authentication-keyid：定义身份验证密钥。

keyid：向该远程服务器发送消息使用的密钥 ID 号，范围 1～4294967295。

source-interface：指定接口名称。

interface-type：接口类型，与接口编号 *interface-number* 共同确定一个接口。

interface-number：接口编号，与接口类型 *interface-type* 共同确定一个接口。本地设备给这个服务器发送 NTP 消息时，消息包中的源 IP 地址从该接口获取。

priority：指定该服务器为优先选择的服务器。

【描述】

ntp-service unicast-server 命令用来配置 NTP 服务器模式，**undo ntp-service unicast-server** 命令用来取消 NTP 服务器模式。

缺省情况下，版本号缺省为 3、启用身份验证、不是优先选择的服务器。

声明以 *X.X.X.X* 所指定的远程服务器作为本地时间服务器。*X.X.X.X* 是一个主机地址，不能为广播、组播地址或参考时钟的 IP 地址。本地设备工作在 client 模式，在这种工作模式下，只能是本地客户机同步到远程服务器，而远程服务器从来不会同步到本地客户机。

【举例】

本地设备被配置成由服务器 128.108.22.44 提供同步时间，版本号为 3。

```
[H3C] ntp-service unicast-server 128.108.22.44 version 3
```

第8章 SNMP 配置命令

8.1 SNMP 配置命令

8.1.1 debugging snmp-agent

【命令】

debugging snmp-agent { **header** | **packet** | **process** | **trap** }

undo debugging snmp-agent { **header** | **packet** | **process** | **trap** }

【视图】

用户视图

【参数】

header：打开数据包消息头调试功能。

packet：打开报文调试功能。

process：打开 SNMP 包的过程调试功能。

trap：打开 Trap 数据包调试功能。

【描述】

debugging snmp-agent 命令用来打开 SNMP Agent 调试开关，指定 SNMP 模块调试信息，**undo debugging snmp-agent** 命令用来取消当前设置。

缺省情况下，关闭 SNMP Agent 调试功能。

【举例】

打开 SNMP Agent 模块数据包消息头调试功能。

```
<H3C> debugging snmp-agent header
```

8.1.2 display snmp-agent

【命令】

display snmp-agent { **local-engineid** | **remote-engineid** }

【视图】

所有视图

【参数】

local-engineid：本地 SNMP 实体引擎 ID；

remote-engineid：远端 SNMP 实体引擎 ID。

【描述】

display snmp-agent 命令用来显示本地或远程 SNMP 实体引擎 ID。

SNMP 引擎是 SNMP 实体的唯一标识，它在一个管理域内唯一的标识一个 SNMP 实体。SNMP 引擎是 SNMP 实体的重要组成部分，完成 SNMP 消息的消息调度、消息处理、安全验证、访问控制等功能。

📖 说明：

使用 **display snmp-agent remote-engineid** 命令，目前软件版本尚无内容显示。

【举例】

显示本地设备的引擎 ID

```
<H3C> display snmp-agent local-engineid
SNMP local EngineID: 000007DB7F0000013859
```

8.1.3 display snmp-agent community

【命令】

display snmp-agent community [**read** | **write**]

【视图】

所有视图

【参数】

read：显示只读访问权限的团体名信息。

write：显示读写访问权限的团体名信息。

【描述】

display snmp-agent community 命令用来显示 SNMPv1 或 SNMPv2c 当前配置的团体名信息。

【举例】

显示当前配置的团体名。

```
<H3C> display snmp-agent community
Community name:8040zlz
```

```
        Group name:8040zlz
        Storage-type: nonVolatile

   Community name:8040core
        Group name:8040core
        Storage-type: nonVolatile
```

表8-1 display snmp-agent community 命令显示内容说明

内容	内容说明
community name	团体名
Group name	组名
storage-type	存储方式

8.1.4 display snmp-agent group

【命令】

display snmp-agent group [*group-name*]

【视图】

所有视图

【参数】

group-name：指定要显示 SNMP 信息的组名，1～32 字节。

【描述】

display snmp-agent group 命令用来显示基于 USM 的组信息。不带参数的情况下，显示所有组名对应的组信息，包括组名、安全模式、存储方式等。

【举例】

显示SNMP组名以及安全模式。以下显示内容相应的域的说明见 表 8-2。

```
<H3C> display snmp-agent group
   Group name: v3r2
        Security model: v3 noAuthnoPriv
        Readview: ViewDefault
        Writeview: <no specified>
        Notifyview :<no specified>
        Storage-type: nonVolatile
```

表8-2 display snmp-agent group 显示域说明表

内容	内容说明
Groupname	用户对应的 SNMP 组名
Security model	SNMP 的安全模型
Readview	该组对应的只读的 MIB 视图名
Writeview	该组对应的可写的 MIB 视图名
Notifyview	该组对应的通知的 MIB 视图名
storage-type	存储方式

8.1.5 display snmp-agent mib-view

【命令】

display snmp-agent mib-view [**exclude** | **include** | **viewname** *view-name*]

【视图】

所有视图

【参数】

exclude：指定要排除显示且已设定的 SNMP MIB 视图属性。

include：指定要包含显示且已设定的 SNMP MIB 视图属性。

viewname：指定要显示的视图名称。

【描述】

display snmp-agent mib-view 命令用来显示当前配置的 MIB 视图。

【举例】

显示当前配置的 MIB 视图。

```
<H3C> display snmp-agent mib-view
   View name:ViewDefault
       MIB Subtree:internet
       Subtree mask:
       Storage-type: nonVolatile
       View Type:included
       View status:active

   View name:ViewDefault
       MIB Subtree:snmpUsmMIB
       Subtree mask:
```

```
        Storage-type: nonVolatile
        View Type:excluded
        View status:active
    View name:ViewDefault
        MIB Subtree:snmpVacmMIB
        Subtree mask:
        Storage-type: nonVolatile
        View Type:excluded
        View status:active

    View name:ViewDefault
        MIB Subtree:snmpModules.18
        Subtree mask:
        Storage-type: nonVolatile
        View Type:excluded
        View status:active
```

对上述显示域中，参数的说明如下表：

表8-3 display snmp-agent mib-view 命令显示内容说明

内容	内容说明
View name	视图名
MIB Subtree	MIB 子树
Subtree mask	MIB 子树掩码
Storage-type	存储方式
ViewType: Included/excluded	标志对一个 MIB 对象的访问是允许或者是禁止
Active	用来指示表中行的状态

8.1.6 display snmp-agent statistics

【命令】

display snmp-agent statistics

【视图】

所有视图

【参数】

无

【描述】

display snmp-agent statistics 命令用来显示 SNMP 状态和统计信息。

【举例】

检查 SNMP 通讯的统计信息

```
<H3C> display snmp-agent statistics
  0 Messages delivered to the SNMP entity
  0 Messages which were for an unsupported version
  0 Messages which used a SNMP community name not known
  0 Messages which represented an illegal operation for the community supplied
  0 ASN.1 or BER errors in the process of decoding
  0 Messages passed from the SNMP entity
  0 SNMP PDUs which had badValue error-status
  0 SNMP PDUs which had genErr error-status
  0 SNMP PDUs which had noSuchName error-status
  0 SNMP PDUs which had tooBig error-status (Maximum packet size 500)
  0 MIB objects retrieved successfully
  0 MIB objects altered successfully
  0 GetRequest-PDU accepted and processed
  0 GetNextRequest-PDU accepted and processed
  0 GetBulkRequest-PDU accepted and processed
  0 GetResponse-PDU accepted and processed
  0 SetRequest-PDU accepted and processed
  0 Trap PDUs accepted and processed
```

对上述显示域中参数的说明如下表：

表8-4 display snmp-agent statistics 命令显示内容说明

内容	内容说明
0 Messages delivered to the SNMP entity	表示没有消息传输到 SNMP 实体
0 Messages which were for an unsupported version	表示没有使用不支持版本的消息
0 Messages which used a SNMP community name not known	表示没有使用无法识别的 SNMP 团体名的消息
0 Messages which represented an illegal operation for the community supplied	表示团体非法操作的返回信息为 0
0 ASN.1 or BER errors in the process of decoding	表示解码过程中的 asn.1 与 ber 错误数为 0
0 Messages passed from the SNMP entity	表示 snmp 实体传输的信息为 0
0 SNMP PDUs which had badValue error-status	表示错误状态为 badValue 的 snmp 协议数据单元数为 0

内容	内容说明
0 SNMP PDUs which had genErr error-status	表示数据状态为 genErr 的 snmp 协议数据单元数为 0
0 SNMP PDUs which had noSuchName error-status	表示错误状态为 noSuchName 的 snmp 协议数据单元数为 0
0 SNMP PDUs which had tooBig error-status (Maximum packet size 500)	表示错误状态为 tooBig 的 snmp 协议数据单元数为 0 (最大 size 为 500)
0 MIB objects retrieved successfully	表示被匹配的 mib 对象数为 0
0 MIB objects altered successfully	表示被改变的 mib 对象数为 0
0 GetRequest-PDU accepted and processed	表示收到并处理的 GetRequest 协议数据单元为 0
0 GetNextRequest-PDU accepted and processed	表示收到并处理的 GetNextRequest 协议数据单元为 0
0 GetBulkRequest-PDU accepted and processed	表示收到并处理的 GetBulkRequest 协议数据单元为 0
0 GetResponse-PDU accepted and processed	表示收到并处理的 GetResponse 协议数据单元为 0
0 SetRequest-PDU accepted and processed	表示收到并处理的 setRequest 协议数据单元为 0
0 Trap PDUs accepted and processed	表示收到并处理的 trap 协议数据单元为 0

8.1.7 display snmp-agent sys-info

【命令】

display snmp-agent sys-info [**contact** | **location** | **version**]*

【视图】

所有视图

【参数】

contact：显示当前设备节点的联系信息。

location：显示当前设备节点的物理位置信息。

version：显示当前代理中运行的 SNMP 版本号。

【描述】

display snmp-agent sys-info 命令用来显示当前 SNMP 设备的系统信息。

【举例】

显示设备系统信息。

```
<H3C> display snmp-agent sys-info
   The contact person for this managed node:
           R&D Hangzhou, Hangzhou H3C Technologies Co.,Ltd.

   The physical location of this node:
           Hangzhou China

   SNMP version running in the system:
           SNMPv3
```

对上述显示域中参数的说明如下表：

表8-5 display snmp-agent sys-info 命令显示内容说明

内容	内容说明
The contact person for this managed node	当前设备节点的联系信息
The physical location of this node:	当前设备节点的物理位置
SNMP version running in the system:	当前系统运行的 SNMP 版本号

8.1.8 display snmp-agent usm-user

【命令】

display snmp-agent usm-user [**engineid** *engineid* | **username** *user-name* | **group** *group-name*] *

【视图】

所有视图

【参数】

engineid：显示指定引擎 ID 的 SNMPv3 的用户信息。

engineid：引擎 ID 字符串。

username：显示指定 SNMPv3 用户的信息。

user-name：用户名，1～32 字节。

group：显示属于相关 SNMP 组的用户信息。

group-name：组名，1～32 字节。

【描述】

display snmp-agent usm-user 命令用来显示 SNMP 用户信息。

SNMP 用户是执行 SNMP 管理操作的远端用户。

【举例】

显示当前所有的用户信息

```
<H3C> display snmp-agent usm-user
User name: authuser
Group name: 1
Engine ID: 8000007DB20000000C025808 active
Storage-type: nonVolatile
UserStatus: active
```

以上显示内容相应的域的说明见下表：

表8-6 display snmp-agent usm-user 显示域说明表

内容	内容说明
User name	标识 SNMP 用户的字符串
Group name	标识 SNMP 用户所属的组
Engine ID	标识 SNMP 设备的字符串
Active	用来指示 SNMP user 的状态
Storage-type	SNMP 信息的存储类型
UserStatus	SNMP 用户的状态

8.1.9 enable snmp trap updown

【命令】

enable snmp trap updown

undo enable snmp trap updown

【视图】

接口视图

【参数】

无

【描述】

enable snmp trap updown 命令用来设置当接口状态发生变化时（如从 UP 变为 DOWN），接口发送状态 Trap 报文到 Trap 目标主机，**undo enable snmp trap updown** 命令用来禁止接口发送状态 Trap 报文。

缺省情况下，接口发送状态 Trap 报文。

相关配置命令请参考 **snmp-agent target-host**。

【举例】

禁止接口发送状态 Trap 报文。

```
[H3C-GigabitEthernet0/0] undo enable snmp trap updown
```

8.1.10 snmp-agent

【命令】

snmp-agent

undo snmp-agent

【视图】

系统视图

【参数】

无

【描述】

snmp-agent 命令用来启动 SNMP Agent，**undo snmp-agent** 命令用来禁止 SNMP Agent。

缺省情况下，关闭 SNMP Agent 功能。

可以使用 **snmp-agent** 命令来启动 SNMP Agent。同时，执行 **snmp-agent** 的任何一条配置命令，也将启动 SNMP Agent。但是，相应配置命令的 **undo** 形式不能启动 SNMP Agent。

在 SNMP Agent 没有使能的时候，配置 **undo** 命令将无效。在 SNMP Agent 使能的情况下，可以用 **undo snmp-agent** 命令禁止 SNMP Agent。

【举例】

禁止正在运行的 SNMP Agent。

```
[H3C] undo snmp-agent
```

8.1.11 snmp-agent community

【命令】

snmp-agent community { **read** | **write** } *community-name* [**mib-view** *view-name* | **acl** *acl-number*] *

undo snmp-agent community *community-name*

【视图】

系统视图

【参数】

read：表明该团体名在指定视图内有只读权限。

write：表明该团体名在指定视图内有读写权限。

community-name：团体名字符串。

mib-view：设置团体名可以访问的 MIB 视图名。

view-name：MIB 视图名。

acl：设置团体名所对应的访问控制列表。

acl-number：访问控制列表号，范围 2000～2999。

【描述】

snmp-agent community 命令用来配置某个团体的读写属性，以及它所对应的 MIB 视图和访问控制列表，**undo snmp-agent community** 命令用来取消团体访问名设置。对同一个团体名进行重复配置时，后配置的属性会覆盖先前配置的属性。

相关配置可参考命令 **snmp-agent group**，**snmp-agent usm-user**。

【举例】

设置团体名为 comaccess，并且允许使用该团体名进行只读访问。

```
[H3C] snmp-agent community read comaccess
```

设置团体名为 mgr，并且可以进行读写访问。

```
[H3C] snmp-agent community write mgr
```

删除团体名 comaccess。

```
[H3C] undo snmp-agent community comaccess
```

8.1.12 snmp-agent group

【命令】

snmp-agent group { **v1** | **v2c** } *group-name* [**read-view** *read-view*] [**write-view** *write-view*] [**notify-view** *notify-view*] [**acl** *acl-number*]

undo snmp-agent group { **v1** | **v2c** } *group-name*

snmp-agent group v3 *group-name* [**authentication** | **privacy**] [**read-view** *read-view*] [**write-view** *write-view*] [**notify-view** *notify-view*] [**acl** *acl-number*]

undo snmp-agent group v3 *group-name* [**authentication** | **privacy**]

【视图】

系统视图

【参数】

v1：团体使用 V1 的安全模式。

v2c：团体使用 V2C 的安全模式。

v3：用户使用 V3 的安全模式。

group-name：组名，1～32 字节。

authentication：指明对报文进行认证，但不加密。

privacy：指明对报文进行认证和加密。

read-view：该选项允许设置只读视图。

read-view：只读视图名，1～32 字节。

write-view：该选项允许设置读写视图。

write-view：读写视图名，1～32 字节。

notify-view：该选项允许设置通知视图。

notify-view：通知视图名，1～32 字节。

acl：该选项用来设置 SNMP 组的访问控制列表。

acl-number：基本访问列表，<2000～2999>。

【描述】

snmp-agent group 命令用来配置一个新的 SNMP 组，即将 SNMP 用户或团体映射到 SNMP 视图，**undo snmp-agent group** 命令用来删除一个指定的 SNMP 组。

缺省情况下，**snmp-agent group v3** *group-name* 命令配置采用不认证、不加密方式。

snmp-agent group v3 命令在不配置视图的情况下默认 ViewDefault 视图为只读视图；其他的视图的权限需要配置。

snmp-agent group { **v1** | **v2c** } 实际上是配置 SNMP 的团体属性。缺省情况下，与 **snmp-agent group v3** 相同。

相关配置可参考命令 **snmp-agent mib-view**，**snmp-agent usm-user**。

【举例】

创建一个 SNMPv3 组 Johngroup。

```
[H3C] snmp-agent group v3 Johngroup
```

8.1.13 snmp-agent local-engineid

【命令】

snmp-agent local-engineid *engineid*

undo snmp-agent local-engineid

【视图】

系统视图

【参数】

engineid：引擎 ID 字符串，必须为十六进制数字，取值为 10～64 个十六进制数。

【描述】

snmp-agent local-engineid 命令用来设置本地 SNMP 实体的引擎 ID，**undo snmp-agent local-engineid** 命令用来取消当前设置。

缺省情况下，设备引擎 ID 为公司的“企业号＋设备信息”。设备信息由各个产品自己决定，可以是 IP 地址，MAC 地址或者自己定义的十六进制数字字符串。

相关配置可参考命令 **snmp-agent usm-user**。

【举例】

配置本地设备的名称为 123456789A。

```
[H3C] snmp-agent local-engineid 123456789A
```

8.1.14 snmp-agent mib-view

【命令】

snmp-agent mib-view { **included** | **excluded** } *view-name oid-tree*

undo snmp-agent mib-view *view-name*

【视图】

系统视图

【参数】

view-name：视图名。

oid-tree：MIB 对象子树的 OID MIB 子树，可以是变量 OID 的字符串，也可以是变量名的字符串。例如：可以是象 1.4.5.3.1 或者 system 这样的字符串，还可以有“*”来做通配符，例如：1.4.5.*.*.1。

included：表示包括该 MIB 子树。

excluded：表示排除该 MIB 子树。

【描述】

snmp-agent mib-view 命令用来创建或者更新视图的信息，**undo snmp-agent mib-view** 命令用来取消当前设置。

缺省情况下，视图名为 ViewDefault，OID 为 1.3.6.1。

目前，该命令不仅支持以变量 OID 的字符串作为参数输入，同时，还支持以节点名作为参数输入。

相关配置可参考命令 **snmp-agent group**。

【举例】

创建一个视图包含 MIB-II 的所有对象。

```
[H3C] snmp-agent mib-view included mib2 1.3.6.1
```

8.1.15 snmp-agent packet max-size

【命令】

snmp-agent packet max-size *byte-count*

undo snmp-agent packet max-size

【视图】

系统视图

【参数】

byte-count：Agent 能接收/发送的 SNMP 消息包长度的最大值，单位字节，取值范围 484～17940。缺省值为 1500 字节。

【描述】

snmp-agent packet max-size 命令用来设置 Agent 能接收/发送的 SNMP 消息包长度的最大值，**undo snmp-agent packet max-size** 命令用来取消当前设置。

【举例】

设置 Agent 能接收/发送的 SNMP 消息包最长为 1042 字节。

```
[H3C] snmp-agent packet max-size 1042
```

8.1.16 snmp-agent sys-info

【命令】

snmp-agent sys-info { **contact** *sysContact* | **location** sys*Location* | **version** { { **v1** | **v2c** | **v3** } * | **all** } }

undo snmp-agent sys-info { { **contact** | **location** }* | **version** { { **v1** | **v2c** | **v3** } * | **all** } }

【视图】

系统视图

【参数】

contact：设置系统维护联系信息。

sysContact：描述系统维护联系信息的字符串。

location：设置设备节点的物理位置。

sysLocation：设备节点的物理位置信息。

version：设置系统启用的 SNMP 版本号。

v1：SNMP V1 版本。

v2c：SNMP V2C 版本。

v3：SNMP V3 版本。

*：表示从 **v1**、**v2c**、**v3** 这三个选项中选取多个，最少选取一个，最多选取所有三个选项。

all：SNMP V1、SNMP V2C、SNMP V3 版本。

【描述】

snmp-agent sys-info 命令用来设置系统信息，包括系统维护信息、设备节点的物理位置信息、启用的 SNMP 版本号等，**undo snmp-agent sys-info** 命令用来取消当前设置。

相关配置可参考命令 **diplay snmp-agent sys-info**。

【举例】

设置系统维护信息为 call Operator at 010-82882488。

```
[H3C] snmp-agent sys-info contact call Operator at 010-82882488
```

8.1.17 snmp-agent target-host

【命令】

snmp-agent target-host trap address udp-domain *X.X.X.X* [**udp-port** *port-number*] **params securityname** *security-string* [**v1** | **v2c** | **v3** [**authentication** | **privacy**]]

undo snmp-agent target-host *X.X.X.X* **securityname** *security-string*

【视图】

系统视图

【参数】

trap：指定该主机为 trap 主机。

address：指定 SNMP 消息传输的目标主机地址。

udp-domain：指定目标主机的传输域基于 UDP。

X.X.X.X：主机的 IP 地址。

udp-port：指定端口。

port-number：指定接收 trap 报文的端口号。

params：指定产生 SNMP 消息的日志主机信息。

securityname：指定 SNMPV1、V2C 的团体名或 SNMPV3 的用户名。

security-string：SNMPV1、SNMPV2C 的团体名或 SNMPV3 的用户名，1～32 字节。

v1：代表 SNMPV1 版本。

v2c：代表 SNMPV2C 版本。

v3：代表 SNMPV3 版本。

authentication：指明对报文进行认证但不加密。

privacy：指明对报文进行认证和加密。

【描述】

snmp-agent target-host 命令用来设置接收 SNMP 通知的目的地，**undo snmp-agent target-host** 命令用来取消当前设置。

snmp-agent target-host 命令与 **snmp-agent trap enable** 命令协同使用。使用 **snmp-agent trap enable** 来设置允许设备发送 Trap 报文。若要一台主机可以发送通知消息，需要在该主机上配置一条 **snmp-agent target-host** 命令。

相关配置可参考命令 **snmp-agent trap enable**，**snmp-agent trap source**，**snmp-agent trap life**。

【举例】

允许向 10.1.1.1 发送 SNMP Trap 报文，使用团体名 comaccess。

```
[H3C] snmp-agent trap enable standard
[H3C] snmp-agent target-host trap address udp-domain 10.1.1.1 params securityname comaccess
```

允许向 10.1.1.1 发送 SNMP Trap 报文，并且使用团体名 public。

```
[H3C] snmp-agent trap enable standard
[H3C] snmp-agent target-host trap address udp-domain 10.1.1.1 params securityname public
```

8.1.18 snmp-agent trap enable

【命令】

snmp-agent trap enable [*trap-type* [*trap-list*]]

undo snmp-agent trap enable [*trap-type* [*trap-list*]]

【视图】

系统视图

【参数】

trap-type：使能 *trap-type* 类型的陷阱报文。

trap-list：与 *trap-type* 类型陷阱报文对应的参数列表。

【描述】

snmp-agent trap enable 命令用来允许设备发送 Trap 报文，并设置陷阱或通知的参数，**undo snmp-agent trap enable** 命令用来取消当前设置。

缺省情况下，所有模块都允许发送 Trap 报文。

snmp-agent trap enable 命令不带参数，表示允许发送所有模块的所有类型的 SNMP Trap 报文。

snmp-agent trap enable 命令与 **snmp-agent target-host** 命令协同使用，使用 **snmp-agent target-host** 命令来指定向哪些主机发送 Trap 信息。为了发送 Trap 信息，用户必须配置至少一条 **snmp-agent target-host** 命令。

发送 Trap 报文的模块 *trap-type* 可以为：**bgp**，**configuration**，**flash**，**ldp**，**lsp**，**ospf**，**standard**，**system**，**vrrp** 等。

standard trap 包括的类型有：**authentication**，**coldstart**，**linkdown**，**linkup**，**warmstart**。

具有 2 级权限的用户，仅能访问 SNMP 的 **snmp-agent trap enable** 命令。

相关配置可参考命令 **snmp-agent target-host**，**snmp-agent trap-source**，**snmp-agent trap-timout**。

【举例】

允许向 10.1.1.1 发送 SNMP 认证失败 Trap 报文，Trap 报文格式为 V2C，使用团体名为 public。

```
[H3C] snmp-agent trap enable standard authentication
```

```
[H3C] snmp-agent target-host trap address udp-domain 10.1.1.1 params
securityname public v2c
```

允许向 10.1.1.1 发送所有类型的 BGP Trap 报文，Trap 报文格式为 V3，对报文进行认证但不加密，用户名为 super。

```
[H3C] snmp-agent trap enable bgp
[H3C] snmp-agent target-host trap address udp-domain 10.1.1.1 params
securityname super v3 authentication
```

8.1.19 snmp-agent trap life

【命令】

snmp-agent trap life *seconds*

undo snmp-agent trap life

【视图】

系统视图

【参数】

seconds：超时时间，单位为秒，取值范围为<1～2592000>，缺省值为 120。

【描述】

snmp-agent trap life 命令用来设置 Trap 报文的保存时间，超过该时间的 Trap 报文都将被丢弃，**undo snmp-agent trap life** 命令用来取消当前设置。

如果系统设置 Trap 报文的保存时间为 *seconds* 秒，若 Trap 报文的保存时间超过了 *senconds* 秒，则该 Trap 报文将被丢弃，不再发送，也不再保存。

相关配置可参考命令 **snmp-agent trap enable**，**snmp-agent target-host**。

【举例】

设置 Trap 报文的超时时间为 60 秒。

```
[H3C] snmp-agent trap life 60
```

8.1.20 snmp-agent trap queue-size

【命令】

snmp-agent trap queue-size *size*

undo snmp-agent trap queue-size

【视图】

系统视图

【参数】

size：消息队列的长度，取值范围 1～1000。

【描述】

snmp-agent trap queue-size 命令用来设置发往目的主机（host）的 Trap 报文的消息队列的长度，**undo snmp-agent trap queue-size** 命令用来取消当前设置。

缺省情况下，*size* 值为 100。

相关配置可参考命令 **snmp-agent trap enable**，**snmp-agent target-host**，**snmp-agent trap life**。

【举例】

设置发送 Trap 报文的消息队列的长度为 200。

```
[H3C] snmp-agent trap queue-size 200
```

8.1.21 snmp-agent trap source

【命令】

snmp-agent trap source *interface-type interface-number*

undo snmp-agent trap source

【视图】

系统视图

【参数】

interface-type：接口类型。

interface-number：接口编号。

【描述】

snmp-agent trap source 命令用来指定发送 Trap 的源地址，**undo snmp-agent trap source** 命令用来取消当前配置。

从一台服务器发出的 SNMP Trap 消息，无论从那个接口发出，都有一个 Trap 地址。如果用户想使用 Trap 地址来跟踪特定事件时，可以使用这条配置命令。

相关配置可参考命令 **snmp-agent trap enable**，**snmp-agent target-host**。

【举例】

将以太网接口 1/0/0 的 IP 地址作为 Trap 报文的源地址。

```
[H3C] snmp-agent trap source ethernet 1/0/0
```

8.1.22 snmp-agent usm-user

【命令】

snmp-agent usm-user { **v1** | **v2c** } *user-name group-name* [**acl** *acl-number*]

undo snmp-agent usm-user { **v1** | **v2c** } *user-name group-name*

snmp-agent usm-user v3 *user-name group-name* [**authentication-mode** { **md5** | **sha** } *auth-password* [**privacy des56** *priv-password*]] [**acl** *acl-number*]

undo snmp-agent usm-user v3 *user-name group-name* { **local** | **engineid** *engineid-string* }

【视图】

系统视图

【参数】

v1：用户使用 V1 的安全模式。

v2c：用户使用 V2C 的安全模式。

v3：用户使用 V3 的安全模式。

user-name：用户名，1～32 字节。

group-name：该用户对应的组名，1～32 字节。

authentication-mode：指明安全级别为需要认证。

md5：指定认证协议为 HMAC-MD5-96。

sha：指定认证协议为 HMAC-SHA-96。

auth-password：认证密码，字符串，1～64 字节。

privacy：指明安全级别为加密。

des56：指定加密协议为 DES。

priv-password：加密密码，字符串，1～64 字节。

acl：该选项用来设置访问视图的 acl 列表。

acl-number：基本访问列表，<2000～2999>。

local：表示本地实体用户。

engineid：指定与该用户相关联的引擎 ID。

engineid-string：引擎 ID 字符串。

【描述】

snmp-agent usm-user 命令用来为一个 SNMP 组添加一个新用户，**undo snmp-agent usm-user** 命令用来删除 SNMP 组的一个用户。

用户在为某个代理配置了远端用户后，在进行验证时，需要用到 engineID。如果配置用户后引擎 ID（engineID）改变，则原引擎 ID 相应的用户无效。

执行该命令，对于 SNMPV1、SNMPV2C 来说，是添加一个新的团体名；对 SNMPV3 来说，是为一个 SNMP 的组添加一个新用户。

相关配置可参考命令 **snmp-agent group**，**snmp-agent community**，**snmp-agent local-engineid**。

【举例】

为 SNMP 组 Johngroup 加入一个用户 John，安全级别为需要认证、指定认证协议为 HMAC-MD5-96、认证密码为 hello。

```
[H3C] snmp-agent usm-user v3 John Johngroup authentication-mode md5 hello
```

第9章 BIMS 配置命令

9.1 BIMS 配置命令

9.1.1 debugging bims all

【命令】

debugging bims all

undo debugging bims

【视图】

用户视图

【描述】

debugging bims all 命令用于配置设备打开 BIMS 的调试信息开关，**undo debugging bims all** 命令用来关闭 BIMS 的调试信息开关。

缺省情况下，未打开 BIMS 调试信息开关。

相关配置可参考命令 **bims enable**。

【举例】

配置打开 bims 调试信息开关 。

```
<H3C> debugging bims all
<H3C> system-view
[H3C] bims request
Now start visit the bims server .
*0.1252374 H3C BIMS/8/debug2:
The host name is:10.153.21.96, the Path is:/bims/service, Port:80
HTC_SendMessage req msg action!
[H3C]
[H3C]
*0.1253285 H3C BIMS/8/debug2:
HTC_SendMessage req msg action,ulRet = 0
*0.1253286 H3C BIMS/8/debug2:
Msgid = 2
*0.1253287 H3C BIMS/8/debug2:
The return code string is: 0
*0.1253287 H3C BIMS/8/debug2:
FileID is = 12
```

```
*0.1253288 H3C BIMS/8/debug2:
FileType is cfg
*0.1253289 H3C BIMS/8/debug2:
FileSize = 775
*0.1253289 H3C BIMS/8/debug2:
Digest = 90 1b b6 c9 2f e7 4e ec 8d 8f 5a d6 13 0d 55 3e
*0.1253290 H3C BIMS/8/debug2:
The length of the cfg file is 775
*0.1253291 H3C BIMS/8/debug2:
Come into BIMS_ExcuteDownCfg!
[H3C]
[H3C]
% FTP server has been started
[H3C]
[H3C]
% Unrecognized command found at '^' position.
[H3C]
  bims is enable
Ready to save current build run info! ........
Current configuration has been saved to the device successfully.
*0.1271100 H3C BIMS/8/debug2:
Ok,success to deal with the download config file!
*0.1271101 H3C BIMS/8/debug2:
The host name is:10.153.21.96, the Path is:/bims/service, Port:80
<H3C>
*0.1271553 H3C BIMS/8/debug2:
Have send file confirm request message,ulRet = 0
*0.1271553 H3C BIMS/8/debug2:
Msgid = 6
*0.1271554 H3C BIMS/8/debug2:
The return code string is: 0
*0.1271555 H3C BIMS/8/debug2:
Parse the Xml file Ret = 0
```

表9-1 debugging bims all 命令输出信息列表

字段	含义
The host name is:10.153.21.111, the Path is:/bims/service, Port:80	此次访问 BIMS 中心的 URL
HTC_SendMessage req msg action,ulRet =	设备向 BIMS 中心发送完请求消息包及返回值
Msgid = 2	得到 BIMS 中心的消息类型
The return code string is: 0	BIMS 中心下传的返回码
FileID is = 1	BIMS 中心下传的文件 id

字段	含义
FileType is cfg	BIMS 中心下传的文件类型
FileSize = 561	BIMS 中心下传的文件大小
Digest = 68 65 1a e2 51 3b 3d 7e b2 b5 49 4b 7a 83 c5 2e	BIMS 中心下传的文件摘要
The length of the cfg file is 561	设备解析得到的文件内容大小
Come into BIMS_ExcuteDownCfg!	开始执行下传的配置文件命令
Ok,success to deal with the download config file!	执行配置文件成功
Have send file confirm request message,ulRet = 0	已经向 BIMS 中心成功发送确认信息
Url=http://10.153.21.111/download/device_001_1_M8XXRAM.ARJ	得到应用软件的 URL
Parse the Xml file Ret = 0	解析 BIMS 中心下传的 xml 文件成功

9.1.2 bims boot request

【命令】

bims boot request

undo bims boot request

【视图】

系统视图

【描述】

bims boot request 命令用于配置设备上电时要访问 BIMS 中心，**undo bims boot request** 命令用来配置设备上电时不需要立即访问 BIMS 中心。

缺省情况下，设备上电时立即访问 BIMS 中心。

相关配置可参考命令 **bims request**。

【举例】

配置设备上电时要立即访问 BIMS 中心。

```
[H3C] bims boot request
```

9.1.3 bims device-id

【命令】

bims device-id *string*

undo bims device-id

【视图】

系统视图

【参数】

string：设备的唯一标识符，长度最长为 30 个字符，合法字符为“0～9”、“a～z”、“A～Z”、“-”、“_”、“@”、“.”。

【描述】

bims device-id 命令用于配置设备的唯一标识符，**undo bims device-id** 命令用来删除设备的唯一标识符。

缺省情况下，没有配置设备的唯一标识符。

相关配置可参考命令 **bims interval**。

【举例】

配置设备的唯一标识符为 R2102311042W033000076。

```
[H3C] bims device-id R2102311042W033000076
```

9.1.4 bims enable

【命令】

bims enable

undo bims enable

【视图】

系统视图

【描述】

bims enable 命令用于配置启动设备的 BIMS 功能，**undo bims enable** 命令用来关闭设备的 BIMS 功能。

缺省情况下，未启动设备的 BIMS 功能。

【举例】

配置设备启动 BIMS 功能。

```
[H3C] bims enable
bims is enable
```

9.1.5 bims interval

【命令】

bims interval *number*

undo bims interval

【视图】

系统视图

【参数】

number：设备访问 BIMS 中心的时间间隔，单位为分钟，范围为 10～10080。

【描述】

bims interval 命令用于配置设备访问 BIMS 中心的时间间隔。**undo bims interval** 命令用于删除设备访问 BIMS 中心的时间间隔。

缺省情况下，未配置此时间间隔。

【举例】

配置设备访问 BIMS 的时间间隔为 20 分钟 。

```
[H3C] bims interval 20
```

9.1.6 bims ip address

【命令】

bims ip address *ip-address* [**port** *portnumber*]

undo bims ip address

【视图】

系统视图

【参数】

ip-address：BIMS 中心的 IP 地址。

portnumber：BIMS 中心使用的端口号。

【描述】

bims ip address 命令用于配置 BIMS 中心的地址和使用的端口号，**undo bims ip address** 命令用来删除此配置。

缺省情况下，未配置此 IP 地址。在配置 BIMS 中心的 IP 地址时，如果没有配置端口号，则默认使用端口 80。

相关配置可参考命令 **bims interval**。

【举例】

配置 BIMS 中心的 IP 地址为 129.33.72.66，使用的端口号为 81 。

```
[H3C] bims ip address 129.33.72.66 port 81
```

9.1.7 bims request

【命令】

bims request

【视图】

系统视图

【描述】

bims request 命令用于配置设备立即访问一次 BIMS 中心。

相关配置可参考命令 **bims boot request**。

【举例】

配置设备立即访问 BIMS 中心。

```
[H3C] bims request
```

9.1.8 bims sharekey

【命令】

bims sharekey { **simple** | **cipher** } *sharekey*

undo bims sharekey

【视图】

系统视图

【参数】

sharekey：BIMS 设备和 BIMS 中心的共享密钥。

simple：配置密码以明文显示。明文密码是长度小于等于 16 的连续字符串，如 1234567。

cipher：配置密码以密文显示。密文密码有两种配置方式，一种为明文配置方式，为用户自定义的长度小于等于 16 的字符串，由系统自动生成对应的密文密码（如用户输入 123，系统自动生成密文密码 7-CZB#/YX]KQ=^Q`MAF4<1!!）；另一种为密文配置方式，直接输入长度为 24 的密文密码，如 7-CZB#/YX]KQ=^Q`MAF4<1!!。因无论采用哪种方式配置密文密码，验证时均需要输入明文密码，故建议用户采用前一种方式进行配置。

【描述】

bims sharekey 命令用于配置 BIMS 设备侧和 BIMS 中心侧之间的共享密钥，**undo bims sharekey** 命令是用来删除 BIMS 设备侧和 BIMS 中心侧之间的共享密钥。

相关配置可参考命令 **bims ip address**。

【举例】

配置 BIMS 设备侧和 BIMS 中心侧之间的共享密钥为 1234567812345678，并且以明文显示。

```
[H3C] bims sharekey simple 1234567812345678
```

9.1.9 bims source ip-address

【命令】

bims source ip-address *ip-address*

undo bims source ip-address

【视图】

系统视图

【参数】

ip-address：BIMS 设备发送报文时携带的源 IP 地址。

【描述】

bims source ip-address 命令用于配置 BIMS 设备发送报文时携带的源 IP 地址，**undo bims source ip-address** 命令用来删除此配置。

可以使用某个接口的 IP 地址作为 BIMS 设备发送报文时携带的源 IP 地址。

在分支和总部类型的网络中，在使用 VPN 的情况下，BIMS 中心位于私网上而分支机构的设备是动态获得公网地址的时候，设备使用公网地址不能访问 BIMS 中心，这时可以在设备侧配置设备发起 BIMS 请求的源地址，该设备就可以使用私网地址通过 VPN 来访问 BIMS 中心了。

缺省情况下，未配置此 IP 地址。

【举例】

配置 BIMS 设备的源 IP 地址为 10.153.72.66。

```
[H3C] bims source ip-address 10.153.72.66
```

9.1.10 bims specify-time

【命令】

bims specify-time *hh:mm yyyy/mm/dd* [[*hh:mm yyyy/mm/dd*] **period-days** *numberdays*]

undo bims specify-time

【视图】

系统视图

【参数】

hh:mm yyyy/mm/dd：设备访问 BIMS 中心的特定的时间点或截止时间点。

numberdays：设备访问 BIMS 中心的周期，以天为单位。

【描述】

bims specify-time 命令是用于配置设备在特定的时间点以及在此基础上设定的访问周期和终止时间访问 BIMS 中心。**undo bims specify-time** 命令则用来删除此配置。

【举例】

配置设备在 2004 年 12 月 12 日的 01 点 01 分访问 BIMS 中心，以后每 7 天时间再访问一次 BIMS 中心，直到 2005 年 12 月 12 日 01 点 01 分为止 。

```
[H3C] bims specify-time 01:01 2004/12/12 01:01 2005/12/12 period 7
```

第10章 RMON 配置命令

10.1 RMON 配置命令

10.1.1 display rmon alarm

【命令】

display rmon alarm [*alarm-entry*]

【视图】

所有视图

【参数】

alarm-entry：告警表项索引号。

【描述】

display rmon alarm 命令用来显示 RMON 告警信息表。

相关配置可参考命令 **rmon alarm**。

【举例】

显示 RMON 告警信息。

```
<H3C> display rmon alarm
Alarm table 1 owned by H3C is VALID.
  Samples absolute value : 1.3.6.1.2.1.16.1.1.1.4.1 <etherStatsOctets.1>
  Sampling interval         : 10(sec)
  Rising threshold          : 1000(linked with event 1)
  Falling threshold         : 100(linked with event 1)
  When startup enables      : risingOrFallingAlarm
Latest value              : 0
```

表10-1 display rmon alarm 显示信息描述表

域名	描述
Alarm table 1	告警表中的索引 1
H3C	所有者
Samples absolute value	节点 1.3.6.1.2.1.16.1.1.1.4.1 的采样绝对值
VALID	与该索引对应的告警表项有效
Sampling interval	采样的时间间隔

域名	描述
Rising threshold is 1000	上限阈值为 1000
Falling threshold is 100	下限阈值为 100
When startup enables : risingOrFallingAlarm	第一次告警的类型，可以是只引发上限告警或者下限告警，也可以进行上下限告警

10.1.2 display rmon event

【命令】

display rmon event [*event-entry*]

【视图】

所有视图

【参数】

event-entry：事件表项索引号。

【描述】

display rmon event 命令用来显示 RMON 的事件表。

显示信息包括：事件表中的事件索引、事件的所有者、对事件的描述、事件引发的动作（日志或告警消息）、最近一次事件发生的时刻（此时间是以系统初始化/启动以来的厘秒数计算的）等。

相关配置可参考命令 **rmon event**。

【举例】

显示 RMON 事件。

```
<H3C> display rmon event
Event table 1 owned by null is VALID.
  Description: null.
  Will cause log-trap when triggered, last triggered at 0days 00h:02m:27s.
```

表10-2 display rmon event 显示信息描述表

域名	描述
Event table 1	事件表中的索引 1
VALID	索引对应的表项的状态为有效
cause log-trap when triggered	事件引发日志和 Trap 通知
last triggered at 0days 00h:02m:27s	最近一次事件发生的时刻

10.1.3 display rmon eventlog

【命令】

display rmon eventlog [*event-entry*]

【视图】

所有视图

【参数】

event-entry：事件表项索引号。

【描述】

display rmon eventlog 命令用来显示 RMON 的事件日志。

显示的 RMON 事件日志信息包括：事件表中的事件索引及事件当前的状态。事件产生日志的时刻（此时间是以系统初始化/启动以来的厘秒数计算的），以及事件的描述等。

【举例】

显示 RMON 事件日志。

```
<H3C> display rmon eventlog 1
Event table 1 owned by null is VALID.
Generates eventLog 1.1 at 0days 00h:01m:39s.
Description: The 1.3.6.1.2.1.16.1.1.1.4.1 defined in alarm table 1,
less than(or =) 100 with alarm value 0. Alarm sample type is absolute.
Generates eventLog 1.2 at 0days 00h:02m:27s.
Description: The alarm formula defined in private alarm table 1,
less than(or =) 100 with alarm value 0. Alarm sample type is absolute.
```

表10-3 display rmon eventlog 显示信息描述表

域名	描述
Event table 1	事件表中的索引 1
VALID	索引对应的表项状态为有效
Generates eventLog 1.2 at 0days 00h:02m:27s	最近一次事件发生时刻
Description	事件描述

10.1.4 display rmon history

【命令】

display rmon history [*interface-type interface-number*]

【视图】

所有视图

【参数】

interface-type interface-number：接口名称及接口号。

【描述】

display rmon history 命令用来显示 RMON 历史控制表及其最近一次历史采样信息，这些信息包括利用率、错误数和总包数等。

相关配置可参考命令 **rmon history**。

【举例】

显示 ethernet2/0/1 接口的历史信息。

```
<H3C> display rmon history ethernet 2/0/1
History control entry 1 owned by null is VALID
  Samples interface     : Ethernet2/0/1<ifEntry.642>
  Sampling interval     : 10(sec) with 10 buckets max
  Latest sampled values :
  Dropevents        :0         , octets               :0
  packets           :0         , broadcast packets    :0
  multicast packets :0         , CRC alignment errors :0
  undersize packets :0         , oversize packets     :0
  fragments         :0         , jabbers              :0
  collisions        :0         , utilization          :0
```

表10-4 display rmon history 显示信息描述表

域名	描述
History control entry 1	历史控制表中的索引号
VALID	有效
Samples interface	采样接口
Sampling interval : 10(sec)	采样间隔，每 10 秒一次
buckets	历史控制表中的记录数
Latest sampled values	最新的采样信息
dropevents	丢包事件
octets	采样时间内接收或发送的字节数
packet	采样时间内接收或发送的包数
broadcastpacket	广播包数
multicastpacket	组播包数

域名	描述
CRC alignment errors	校验错误的包数
undersize packets	过小的包数
oversize packets	超大的包数
fragments	过小且校验错误的包数
jabbers	超大且校验错误的包数
collisions	冲突的包数
utilization	利用率

10.1.5 display rmon prialarm

【命令】

display rmon prialarm [*prialarm-entry*]

【视图】

所有视图

【参数】

prialarm-entry：告警扩展表项索引号。

【描述】

display rmon prialarm 命令用来显示 RMON 告警扩展表信息。

相关配置可参考命令 **rmon prialarm**。

【举例】

显示 RMON 告警扩展表信息。

```
<H3C> display rmon prialarm
Prialarm table 1 owned by null is VALID.
  Samples    absolute value : .1.3.6.1.2.1.16.1.1.1.4.1
  Sampling interval         : 10(sec)
  Rising threshold          : 1000(linked with event 1)
  Falling threshold         : 100(linked with event 1)
  When startup enables      : risingOrFallingAlarm
  This entry will exist     : forever.
  Latest value              : 0
```

表10-5 display rmon prialarm 显示信息描述表

域名	描述
Prialarm table 1	扩展告警表项的索引号
owned by null	该扩展告警表项的创建者
VALID	有效
Samples absolute value : .1.3.6.1.2.1.16.1.1.1.4.1	节点 1.3.6.1.2.1.16.1.1.1.4.1 的采样绝对值
Sampling interval : 10(sec)	采样间隔
Rising threshold : 1000	采样上限阈值，当采样值从正常值达到该值时引发上限告警
Falling threshold : 100	采样下限阈值，当采样值从正常值达到该值时引发下限告警
linked with event 1	上下限告警对应的事件索引
When startup enables : risingOrFallingAlarm	第一次告警的类型，可以是只引发上限告警或者下限告警，也可以进行上下限告警
This entry will exist : forever	该表项存在的期限， 可以是永远存在， 也可以是在规定的事件内存在
Latest value 0	最近一次采样值

10.1.6 display rmon statistics

【命令】

display rmon statistics [*interface-type interface-number*]

【视图】

所有视图

【参数】

interface-type interface-number：接口名称及接口号。

【描述】

display rmon statistics 命令用来显示 RMON 统计表信息。

显示的 RMON 统计信息包括：冲突，循环冗余校验和队列，太小或超大的包，超时传送，碎片，广播、组播、单播消息，以及带宽使用等。

相关配置可参考命令 **rmon statistics**。

【举例】

显示 RMON 统计信息。

```
<H3C> display rmon statistics ethernet2/0/1
Statistics entry 1 owned by monitor is VALID.
  Interface : Ethernet0/0/0<ifIndex.642>
  etherStatsOctets         : 9760      , etherStatsPkts          : 79
  etherStatsBroadcastPkts  : 0         , etherStatsMulticastPkts : 0
  etherStatsUndersizePkts  : 0         , etherStatsOversizePkts  : 0
  etherStatsFragments      : 0         , etherStatsJabbers       : 0
  etherStatsCRCAlignErrors : 0         , etherStatsCollisions    : 0
  etherStatsDropEvents (insufficient resources): 0
  Packets received according to length:
  64     : 0         ,  65-127  : 0         ,  128-255  : 0
  256-511: 0         ,  512-1023: 0         ,  1024-1518: 0
```

10.1.7 rmon alarm

【命令】

rmon alarm *entry-number alarm-variable sampling-time* { **delta** | **absolute** } **rising_threshold** *threshold-value1 event-entry1* **falling_threshold** *threshold-value2 event-entry2* [**owner** *text*]

undo rmon alarm *entry-number*

【视图】

系统视图

【参数】

entry-number：告警表项索引号，取值范围为 1～65535。

alarm-variable：告警变量，字符串类型，长度为 1～256 字符，格式为节点 OID 的点分格式，如 1.3.6.1.2.1.2.2.1.10（或 ifInOctets）。

sampling-time：采样间隔时间，取值范围为 5～65535，单位为秒。

delta：采样类型为变化值。

absolute：采样类型为绝对值。

rising_threshold *threshold-value1*：上限阈值，取值范围为 0～2147483647。

event-entry1：上限阈值相应的事件号，取值范围为 0～65535。

falling_threshold *threshold-value2*：下限阈值，取值范围为 0～2147483647。

event-entry2：下限阈值相应的事件号，取值范围为 0～65535。

owner *text*：该表项的创建者，字符串长度为 1～127。

【描述】

rmon alarm 命令用来在告警表中添加一个表项，**undo rmon alarm** 命令用来在告警表中删除一个表项。

本命令用来设置告警项。设置告警项以便在出现异常时触发告警事件，再由告警事件来决定记录日志和向网管站发送 Trap。

当添加了无效的表项时，其配置将不显示在配置文件中，但是可以通过 **display rmon alarm** 命令查看到。

【举例】

在告警表中删除第 15 个表项。

```
[H3C] undo rmon alarm 15
```

10.1.8 rmon event

【命令】

rmon event *event-entry* [**description** *string*] { **log** | **trap** *trap-community* | **log-trap** *log-trapcommunity* | **none** } [**owner** *text*]

undo rmon event *event-entry*

【视图】

系统视图

【参数】

event-entry：事件表项索引号，取值范围为 1～65535。

description *string*：事件的描述，字符串长度为 1～127 个字符。

log：日志事件。

trap：Trap 事件。

log-trap：日志和 Trap 事件。

trap-community：Trap 消息发往的团体。

log-trap：日志和 Trap 事件。

log-trapcommunity：Trap 消息发往的团体。

none：非日志和 Trap 事件。

owner *text*：该表项的创建者，字符串长度为 1～127 个字符。

【描述】

rmon event 命令用来在事件表中添加一个表项，**undo rmon event** 命令用来在事件表中删除一个表项。

RMON 的事件管理定义事件号及事件的处理方式包括：记日志、向网管站发 Trap 消息、记日志同时向网管站发 Trap 消息。这样系统就可以对告警事件作出相应的处理。

【举例】

在事件表中添加第 10 个表项，标记为日志事件。

```
[H3C] rmon event 10 log
```

10.1.9 rmon history

【命令】

rmon history *history-control-entry* **buckets** *number* **interval** *sampling-interval* [**owner** *text-string*]

undo rmon history *entry-number*

【视图】

以太网接口视图

【参数】

history-control-entry：历史控制表项索引号，取值范围为 1～65535。

buckets *number*：该表项对应的历史控制表的容量。

interval *sampling-interval*：采样时间，取值范围为 5～3600，单位为秒。

owner *text*：该表项的创建者，字符串长度为 1～127 个字符。

【描述】

rmon history 命令用来在历史控制表中添加一个表项，**undo rmon history** 命令用来在历史控制表中删除一个表项。

本命令可以设定对某个接口进行抽样，设置抽样参数（抽样时间间隔）和保存数量。设置之后 RMON 就定期对指定的接口进行数据采集并保存起来以备查看。抽样信息包括利用率、错误数和总包数等。

【举例】

在历史控制表中添加一个表项。

```
[H3C-Ethernet0/0/0] rmon history 1 buckets 10 interval 10
```

10.1.10 rmon prialarm

【命令】

rmon prialarm *entry-number prialarm-formula prialarm-des sampling-timer* { **delta** | **absolute** | **changeratio** } **rising_threshold** *threshold-value1 event-entry1*

falling_threshold *threshold-value2 event-entry2* **entrytype** { **forever** | **cycle** *cycle-period* } [**owner** *text*]

undo rmon prialarm *entry-number*

【视图】

系统视图

【参数】

entry-number：告警扩展表项索引号，取值范围为 1～65535；

prialarm-fromula：对告警变量进行计算的告警公式，取值为 1～256 个字符的字符串。公式中的告警变量必须以 OID 来表示，OID 表达式必须以小数点开始，例如(.1.3.6.1.2.1.2.1.10.1)*8。用户可以使用加减乘除四种运算方法对告警变量进行运算，该运算公式的结果取值为长整型数。用户在编写公式的时候需要注意，公式中每一步的运算结果都不能超过长整型数的取值范围，否则可能会得出错误的结果。

prialarm-des：对该告警的描述，长度为 1～127 个字符；

sampling-timer：采样间隔时间，取值范围为 10～65535 秒；

delta | absolute | changeratio：采样类型，变化值（**delta | changeratio**）或绝对值（**absolute**）；

threshold-value1：上限阈值，取值范围为 0～4294967295；

event-entry1：上限阈值相应的事件号，取值范围为 0～65535；

threshold-value2：下限阈值，取值范围为 0～4294967295；

event-entry2：下限阈值相应的事件号，取值范围为 0～65535 ；

forever | cycle *cycle-period*：本告警表项的类型，分为永久存在和在指定时间内存在；

cycle-period：告警表项在的周期；

owner *text*：该表项的创建者，字符串长度为 1～127。

【描述】

rmon prialarm 命令用来在 RMON 告警扩展表中增加一个表项。**undo rmon prialarm** 命令用来在扩展 RMON 告警表中删除一个表项。

表中可以创建的最大表项的个数依赖于产品的硬件资源。

【举例】

在 RMON 告警扩展表中删除第 10 个表项。

```
[H3C] undo rmon prialarm 10
```

10.1.11 rmon statistics

【命令】

rmon statistics *entry-number* [**owner** *text*]

undo rmon statistics *entry-number*

【视图】

以太网接口视图

【参数】

entry-number：统计表表项的索引号，取值范围为 1～65535。

owner *text*：该表项的创建者，字符串长度为 1～127 个字符。

【描述】

rmon statistics 命令用来在统计表中添加一个表项，**undo rmon statistics** 命令用来在统计表中删除一个表项。

RMON 统计管理功能可以用于统计监视接口的使用及错误。统计信息包括：冲突、循环冗余校验和队列、过小或超大数据包、超时传送、碎片、广播、组播、单播消息以及带宽使用等。

可以指定要监视的以太网接口。

【举例】

在 Ethernet2/0/1 接口的统计表中添加第 20 个表项。

```
[H3C-Ethernet2/0/1] rmon statistic 20 owner null
```

第11章 终端服务命令

11.1 Telnet 终端服务配置命令

11.1.1 debugging telnet

【命令】

debugging telnet

undo debugging telnet

【视图】

用户视图

【参数】

无

【描述】

debugging telnet 命令用来打开 Telnet 连接的调试开关，**undo debugging telnet** 命令用来关闭 Telnet 连接的调试开关。

缺省情况下，关闭调试开关。

相关配置可参考命令 **telnet**。

【举例】

打开 Telnet 连接的调试开关。

```
<H3C> debugging telnet
```

11.1.2 display tcp status

【命令】

display tcp status

【视图】

所有视图

【参数】

无

【描述】

display tcp status 命令用来显示防火墙当前所有的 TCP 连接情况。

相对于 **display users**，**display tcp status** 能够显示更多有关 telnet 客户端和服务器的情况。

该命令的显示信息中包括 TCP 连接的本地地址，本地端口号，外部地址，外部端口号以及连接的状态。

相关配置可参考命令 **telnet**。

【举例】

```
<H3C> display tcp status
 TCPCB      Local Add:port          Foreign Add:port        State
235a6284    129.102.100.142:23      129.102.1.92            Established
235a66c4    0.0.0.0:23              0.0.0.0.0               Listening
```

以上显示信息表示：一个 TCP 连接已经建立，该 TCP 连接的本地 IP 地址为 129.102.100.142，本地端口号为 23，远程 IP 地址为 129.102.001.92，另外，本地有一个对 23 号端口监听的服务器进程。

11.1.3 display telnet source-ip

【命令】

display telnet source-ip

【视图】

所有视图

【参数】

无

【描述】

display telnet source-ip 命令用来显示当前为 Telnet Client 设置的源 IP 地址。

如果为 Telnet Client 指定了源接口，则此命令显示的是该接口的 IP 地址；如果没有为 Telnet Client 指定源接口和源 IP 地址，则显示 0.0.0.0。

【举例】

显示当前为 Telnet Client 设置的源 IP 地址。

```
<H3C> display telnet source-ip
The source IP you specified is 0.0.0.0
```

11.1.4 display telnet-server source-ip

【命令】

display telnet-server source-ip

【视图】

所有视图

【参数】

无

【描述】

display telnet-server source-ip 命令用来显示当前为 Telnet Server 设置的源 IP 地址。

如果为 Telnet Server 指定了源接口，则此命令显示的是该接口的 IP 地址；如果没有为 Telnet Server 指定源接口和源 IP 地址，则显示 0.0.0.0。

【举例】

显示当前为 Telnet Server 设置的源 IP 地址。

```
<H3C> display telnet-server source-ip
The source IP you specified is 0.0.0.0
```

11.1.5 telnet

【命令】

telnet *host-ip-address* [*service-port*] [**source-interface** *interface-type interface-number* | **source-ip** *ip-address*]

【视图】

用户视图

【参数】

host-ip-address：远端设备的主机名或 IP 地址，点分十进制格式。

service-port：远端设备提供 Telnet 服务的 TCP 端口号，范围 0～65535。

interface-type interface-number：指定 Telnet 客户端的源接口类型和编号。

ip-address：指定 Telnet 客户端的源地址。

【描述】

telnet 命令用来从当前防火墙再登录到其它设备。

缺省情况下，在不指定 *service-port* 时，Telnet 端口号为 23。

通过执行 **telnet** 命令，用户可以很方便地从一个防火墙登录到另一个防火墙，对它进行远程管理。

相关配置可参考命令 **display tcp status**。

【举例】

从当前防火墙 SecPath 1 登录到另外一台防火墙 SecPath 2（IP 地址为 129.102.0.1）。

```
<H3C> telnet 129.102.0.1
Trying 129.102.0.1 ...
Press CTRL+K to abort
Connected to 129.102.0.1 ...
<H3C>
```

11.1.6 telnet source-interface

【命令】

telnet source-interface *interface-type interface-number*

undo telnet source-interface

【视图】

系统视图

【参数】

interface-type interface-number：指定建立 Telnet 连接使用的源接口。

【描述】

telnet source-interface 命令用来指定 Telnet 客户端建立连接时使用的源接口，**undo telnet source-interface** 命令用来删除指定的源接口。

源接口必须是本地存在的接口，否则命令提示不成功。配置源接口后，Telnet 客户端发送报文中的源 IP 地址为源接口的 IP 地址；删除源接口后，Telnet 客户端发送报文中的源 IP 地址为出接口的 IP 地址。

缺省情况下，发送报文中的源 IP 地址为出接口的 IP 地址。

📖 **说明：**

指定源 IP 地址和指定源接口的命令是互斥的，后配置的命令将覆盖先前的配置。

【举例】

指定 Telnet 客户端建立连接时的源接口为 Ethernet 1/0/1。

```
[H3C] telnet source-interface ethernet 1/0/1
```

11.1.7 telnet source-ip

【命令】

telnet source-ip *source-address*

undo telnet source-ip

【视图】

系统视图

【参数】

source-address：指定建立 Telnet 连接使用的源 IP 地址。

【描述】

telnet source-ip 命令用来指定 Telnet 客户端建立连接时使用的源 IP 地址，**undo telnet source-ip** 命令用来删除指定的源 IP 地址。

指定的源 IP 地址必须是本地地址，否则命令提示不成功。删除源 IP 地址后，Telnet 客户端发送报文中的源 IP 地址为出接口的 IP 地址。

缺省情况下，发送报文中的源 IP 地址为出接口的 IP 地址。

📖 **说明：**

指定源 IP 地址和指定源接口的命令是互斥的，后配置的命令将覆盖先前的配置。

【举例】

指定 Telnet 客户端建立连接时的源 IP 地址为 1.1.1.1。

```
[H3C] telnet source-ip 1.1.1.1
```

11.1.8 telnet-server source-interface

【命令】

telnet-server source-interface *interface-type interface-number*

undo telnet-server source-interface

【视图】

系统视图

【参数】

interface-type interface-number：源接口类型及接口号。

【描述】

telnet-server source-interface 命令用来为 Telnet Server 指定源接口。**undo telnet-server source-interface** 命令用来删除为 Telnet Server 指定的源接口。

源接口必须是本地存在的接口，否则命令提示不成功。配置源接口后，Telnet Server 发送报文中的源 IP 地址为源接口的 IP 地址；删除源接口后，Telnet Server 发送报文中的源 IP 地址为出接口的 IP 地址。

缺省情况下，发送报文中的源 IP 地址为出接口的 IP 地址。

📖 **说明：**

指定源 IP 地址和指定源接口命令是互斥的，后配置的命令将覆盖先前的配置。

【举例】

为 Telnet Server 指定源接口为 ethernet0/0/0。

```
[H3C] telnet-server source-interface Ethernet 0/0/0
```

11.1.9 telnet-server source-ip

【命令】

telnet-server source-ip *ip-address*

undo telnet-server source-ip

【视图】

系统视图

【参数】

ip-address：源 IP 地址。

【描述】

telnet-server source-ip 命令用来为 Telnet Server 指定发送报文中的源 IP 地址。**undo telnet-server source-ip** 命令用来删除为 Telnet Server 指定的源 IP 地址。

指定的源 IP 地址必须是本地地址，否则命令提示不成功。删除源 IP 地址后，Telnet Server 发送报文中的源 IP 地址为出接口的 IP 地址。

缺省情况下，发送报文中的源 IP 地址为出接口的 IP 地址。

📖 **说明：**

指定源 IP 地址和指定源接口命令是互斥的，后配置的命令将覆盖先前的配置。

【举例】

为 Telnet Server 指定发送报文中的源 IP 地址为 192.168.0.1。

```
[H3C] telnet-server source-ip 192.168.0.1
```

11.2 SSH 配置命令

11.2.1 debugging ssh client

【命令】

debugging ssh client

undo debugging ssh client

【视图】

用户视图

【参数】

无

【描述】

debugging ssh client 命令用来打开 SSH 客户端的调试信息开关，**undo** 命令用来关闭调试开关。

缺省情况下，关闭调试开关。

【举例】

打开 SSH 客户端的调试信息开关。

```
<H3C> debugging ssh client
```

11.2.2 debugging ssh server

【命令】

debugging ssh server { **vty** *index* | **all** }

undo debugging ssh server { **vty** *index* | **all** }

【视图】

用户视图

【参数】

index：调试的 SSH 通道，取值受限于 VTY 的编号，缺省为 0～4。

all：所有的 SSH 通道。

【描述】

debugging ssh server 命令用来打开 SSH 服务器的调试信息开关，**undo debugging ssh server** 命令用来关闭调试开关。

缺省情况下，关闭调试开关。

相关配置可参考命令 **ssh server authentication-retries**，**ssh server rekey-interval**，**ssh server timeout**。

【举例】

打开终端 VTY0 的 SSH 调试信息开关。

```
<H3C> debugging ssh server vty 0
00:23:20: SSH0: starting SSH control process
00:23:20: SSH0: sent protocol version id SSH-1.5-H3C-1.25
00:23:20: SSH0: protocol version id is - SSH-1.5-1.2.26
00:23:20: SSH0: SSH_SMSG_PUBLIC_KEY msg
00:23:21: SSH0: SSH_CMSG_SESSION_KEY msg - length 112, type 0x03
00:23:21: SSH: RSA decrypt started
00:23:21: SSH: RSA decrypt finished
00:23:21: SSH: RSA decrypt started
00:23:21: SSH: RSA decrypt finished
```

11.2.3 display rsa local-key-pair public

【命令】

display rsa local-key-pair public

【视图】

所有视图

【参数】

无

【描述】

display rsa local-key-pair public 命令用来显示服务器端主机密钥对和服务器密钥对的公钥部分，如果没有生成密钥，则提示没有找到密钥，例如：RSA keys not found。

相关配置可参考命令 **rsa local-key-pair create**。

【举例】

```
<H3C> display rsa local-key-pair public
=====================================================
```

```
Time of Key pair created: 15:58:04  2009/08/29
Key name: H3C_Host
Key type: RSA encryption Key
=====================================================
Key code:
3047
  0240
    D7FCA515 53ACB9A2 15E1EC8A B9F63832 F04D473E
    145DB768 2BF3B416 28B192D2 F19809BF 729B369F
    227EE674 7405C0C8 2B829613 96B69E85 89AF7E08
    081217B9
  0203
    010001

 Host public key for PEM format code:
---- BEGIN SSH2 PUBLIC KEY ----
AAAAB3NzaC1yc2EAAAADAQABAAAAQQDX/KUVU6y5ohXh7Iq59jgy8E1HPhRdt2gr
87QWKLGS0vGYCb9ymzafIn7mdHQFwMgrgpYTlraehYmvfggIEhe5
---- END SSH2 PUBLIC KEY ----

Public key code for pasting into OpenSSH authorized_keys file :
ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAAAQQDX/KUVU6y5ohXh7Iq59jgy8E1HPhRdt2gr87QWKLGS
0vGYCb9ymzafIn7mdHQFwMgrgpYTlraehYmvfggIEhe5 rsa-key


=====================================================
Time of Key pair created: 15:58:17  2009/08/29
Key name: H3C_Server
Key type: RSA encryption Key
=====================================================
Key code:
3067
  0260
    B819407E D9132A75 D0512E44 BAAC906F AE8BFDF1
    9CDFCF2C 1B801FDC 8DFD46AD 3409A9F1 AAA9B530
    CBE37F55 1C6604E5 78CE1FB2 FB501D8D 7D9EC70F
    A1648C5B F1776B4E 92C2EEED CCB930B5 04C15DF3
    98FCECB4 2A820E5F 3090473E A4BF1C57
  0203
    010001
```

11.2.4 display rsa peer-public-key

【命令】

display rsa peer-public-key [**brief** | **name** *keyname*]

【视图】

所有视图

【参数】

brief：显示所有远端公钥的概要信息。

keyname：指定要显示的密钥名称，长度为 1～64 的连续字符串。

【描述】

display rsa peer-public-key 命令用来显示指定的 RSA 公共密钥，如果没有指定，则显示所有的公共密钥。

相关配置可参考命令 **rsa local-key-pair create**。

【举例】

```
<H3C> display rsa peer-public-key
=====================================
    Key name: aa
    Key address:
=====================================
Key Code:
308186
  028180
    6B494EC4 EBD23DEE 1375C2B5 AB892F69 F2529D09 5B559E26 26011A1F C58AA5E3
    60258B01 26494D0E 7221BB98 1C844CCD 8F0F8AEA 4AA1CD5B 9C3C5EF5 3093319F
    6F3AEA80 351E5E8D 29F1511C D4AC08B4 3FDF5B7B E30A4E47 6FF75B9A 63BE5E94
    E9C344B7 F0EC9D53 AE54E0A3 0567184A 2E80BEC3 89A2DAFA 83C18591 5B29EAA1
  0201
    25
```

11.2.5 display ssh server

【命令】

display ssh server { **status** | **session** }

【视图】

所有视图

【参数】

status：显示 SSH 状态信息。

session：显示 SSH 会话信息。

【描述】

display ssh server 命令用来显示 SSH 的状态或会话信息。

相关配置可参考命令 **ssh server authentication-retries**，**ssh server rekey-interval**，**ssh server timeout**。

【举例】

显示 SSH 状态和配置参数。

```
[H3C] display ssh server status
 SSH version : 1.99
 SSH connection timeout : 60 seconds
 SSH server key generating interval : 0 hours
 SSH Authentication retries : 3 times
  SFTP Server: Disable
```

显示 SSH 会话。

```
[H3C] display ssh server session
 Conn    Ver   Encry    State     Retry    Username
 VTY 0   1.5   3DES     started   0        ssher
 VTY 0   2.0   AES      started   0        secuser
```

11.2.6 display ssh-server source-ip

【命令】

display ssh-server source-ip

【视图】

所有视图

【参数】

无

【描述】

display ssh-server source-ip 命令用来显示当前为 SSH Server 设置的源 IP 地址。

如果为 SSH Server 指定了源接口，则此命令显示的是该接口的 IP 地址；如果没有为 SSH Server 指定源接口和源 IP 地址，则显示为 0.0.0.0。

【举例】

显示当前为 SSH Server 设置的源 IP 地址。

```
[H3C] display ssh-server source-ip
The source IP you specified is 0.0.0.0
```

11.2.7 display ssh user-information

【命令】

display ssh user-information [*username*]

【视图】

所有视图

【参数】

username：SSH 用户名。

【描述】

display ssh user-information 命令用来显示当前 SSH 用户的信息，包括用户名、用户对应的密钥名称、用户的验证方式。如果命令中指定参数 *username*，那么将显示指定用户名的用户信息。

相关配置可参考命令 **ssh user username assign rsa-key**，**ssh user authentication-type**。

【举例】

显示用户信息

```
[H3C] display ssh user-information
 Username           Authentication-type  User-public-key-name  Service-type
 abc                password             null                  sftp
 teluser            password             null                  stelnet
 ssher              rsa                  ssherkey              stelnet|sftp
```

11.2.8 peer-public-key end

【命令】

peer-public-key end

【视图】

公共密钥视图

【参数】

无

【描述】

peer-public-key end 命令用来从公共密钥视图退回到系统视图。

相关配置可参考命令 **rsa peer-public-key**，**public-key-code begin**。

【举例】

退出公共密钥视图并保留配置。

```
[H3C] rsa peer-public-key secpath003
[H3C-rsa-public-key] peer-public-key end
```

11.2.9 protocol inbound

【命令】

protocol inbound { **all** | **ssh** | **telnet** }

【视图】

VTY 类型的用户界面视图

【参数】

all：支持所有的协议，包括 Telnet 和 SSH。

ssh：只支持 SSH 协议。

telnet：只支持 Telnet 协议。

【描述】

protocol inbound 命令用来指定所在的用户界面所支持的协议。

缺省情况下，系统支持所有的协议，即支持 Telnet 和 SSH。

使用该命令指定所在用户界面支持的协议时，且在 SSH 使能的情况下，如果本机 RSA 密钥没有配置，则 SSH 仍然不可用。配置结果待下次登录请求时生效。

如果在该用户界面上配置支持的协议是 SSH，为确保登录成功，请您务必配置相应的验证方式为 **authentication-mode scheme**；若配置验证方式为 **authentication-mode password** 和 **authentication-mode none**，则 **protocol inbound ssh** 配置结果将失败。

相关配置可参考命令 **user-interface vty**。

【举例】

禁止 vty0 到 vty4 的 Telnet 功能，只支持 SSH 功能。

```
[H3C] user-interface vty 0 4
[H3C-ui-vty0-4] protocol inbound ssh
```

禁止 vty0 的 Telnet 功能，只支持 SSH。

```
[H3C] user-interface vty 0
[H3C-ui-vty0] protocol inbound ssh
```

11.2.10 public-key-code begin

【命令】

public-key-code begin

【视图】

公共密钥视图

【参数】

无

【描述】

public-key-code begin 命令用来进入公共密钥编辑视图。

使用该命令前，必须使用命令 **rsa peer-public-key** 指定一个密钥名称。输入 **public-key-code begin** 命令后，进入公共密钥编辑视图，您可以开始输入密钥数据。在输入密钥数据时，字符之间可以有空格，也可以按回车键继续输入数据。所配置的公钥必须是按公钥格式编码的十六进制字符串，是由支持 SSH 的客户端软件随机生成的。

相关配置可参考命令 **rsa peer-public-key**，**public-key-code end**。

【举例】

进入公共密钥编辑视图，输入密钥。

```
[H3C] rsa peer-public-key secpath003
[H3C-rsa-public-key] public-key-code begin
[H3C-key-code] 308186028180739A291ABDA704F5D93DC8FDF84C427463
[H3C-key-code] 1991C164B0DF178C55FA833591C7D47D5381D09CE82913
[H3C-key-code] D7EDF9C08511D83CA4ED2B30B809808EB0D1F52D045DE4
[H3C-key-code] 0861B74A0E135523CCD74CAC61F8E58C452B2F3F2DA0DC
[H3C-key-code] C48E3306367FE187BDD944018B3B69F3CBB0A573202C16
[H3C-key-code] BB2FC1ACF3EC8F828D55A36F1CDDC4BB45504F020125
[H3C-key-code] public-key-code end
```

11.2.11 public-key-code end

【命令】

public-key-code end

【视图】

公共密钥编辑视图

【参数】

无

【描述】

public-key-code end 命令可以用来从公共密钥编辑视图退回到公共密钥视图，并且保存用户配置的公共密钥。当执行此命令后，结束公钥的编辑过程，在存储之前，要进行密钥合法性的检测，如果用户配置的公钥字符串中存在非法字符，那么将会显示相关提示信息，说明输入了非法字符，用户配置的密钥将被丢弃，本次配置失败。如果配置的密钥合法，将会保存到客户公钥链表中。

相关配置可参考命令 **rsa peer-public-key**，**public-key-code begin**。

【举例】

退出公共密钥编辑视图并保留配置。

```
[H3C-rsa-key-code] public-key-code end
[H3C-rsa-public-key]
```

11.2.12 rsa local-key-pair create

【命令】

rsa local-key-pair create

【视图】

系统视图

【参数】

无

【描述】

rsa local-key-pair create 命令用来生成本地 RSA 主机密钥对和服务器密钥对。

用命令 **rsa local-key-pair create** 创建本地密钥对时，生成两个文件 hostkey 和 serverkey，在两个文件中都分别包含一对本地的公钥和私钥。hostkey 中的密钥对是保持不变的，serverkey 中的密钥对会根据配置以一定的时间间隔自动更新。

使用该命令进行配置时，如果 RSA 密钥已经存在，则进行告警，并提示原有密钥被更换。产生的密钥对命名方式为防火墙名称+server 和防火墙名称+host，如：H3C_host、H3C_server。本命令不被保存到配置文件中。

输入该命令后，会提示您输入主机密钥的位数，服务器密钥对的位数与主机密钥对的位数至少相差 128 位。服务器密钥对和主机密钥对的最小长度为 512 位，最大长度为 2048 位。如果已有密钥对存在，则需用户确认是否进行修改。

如果服务器端和客户端都为 SecPath 防火墙时，则要求服务器端使用此命令生成的密钥对至少要为 768 位。当防火墙作为 SSH2.0 服务器端，且需要对客户端进行 RSA 认证，那么要求客户端生成的密钥对至少为 768 位。

成功完成 SSH 登录的首要操作是：配置并产生本地 RSA 密钥对。请您在进行其它 SSH 配置之前，一定记得完成 **rsa local-key-pair create** 配置，生成本地密钥对。此命令只需执行一遍，防火墙重新启动后不必再次执行。

相关配置可参考命令 **rsa local-key-pair destroy**。

【举例】

配置生成本地主机密钥对和服务器密钥对。

```
[H3C] rsa local-key-pair create
The key name will be: H3C_Host
The range of public key size is (512 ~ 2048).
NOTES: If the key modulus is greater than 512,
       It will take a few minutes.
Input the bits in the modulus[default = 512]:
Generating keys...
........++++++++++++
..............................++++++++++++
.......++++++++
...++++++++
......
[H3C]
```

11.2.13 rsa local-key-pair destroy

【命令】

rsa local-key-pair destroy

【视图】

系统视图

【参数】

无

【描述】

rsa local-key-pair destroy 命令用来销毁服务器端所有的 RSA 密钥，包括主机密钥对 Host key 和服务器密钥对 Server key。

输入该命令后，需要您确认是否销毁服务器端所有的 RSA 密钥，本命令不被保存在配置文件中。

相关配置可参考命令 **rsa local-key-pair create**。

【举例】

销毁服务器端所有的密钥。

```
[H3C] rsa local-key-pair destroy
% The name for the keys which will be destroyed is H3C_Host .
% Confirm to destroy these keys? [Y/N]:y
.............
[H3C]
```

11.2.14 rsa peer-public-key

【命令】

rsa peer-public-key *key-name*

【视图】

系统视图

【参数】

key-name：公共密钥名。

【描述】

rsa peer-public-key 命令用来进入公共密钥视图。

输入该命令后，将进入公共密钥视图，和 **public-key-code begin** 一同使用，可以对客户端的公钥进行配置。客户端的公钥是由客户端软件随机生成的，请使用支持 SSH1.5 的客户端软件。

相关配置可参考命令 **public-key-code begin**，**public-key-code end**。

【举例】

进入公共密钥视图。

```
[H3C] rsa peer-public-key secpath002
[H3C-rsa-public-key]
```

11.2.15 ssh authentication-type default

【命令】

ssh authentication-type default { **password** | **rsa** | **all** | **password-publickey** }

undo ssh authentication-type default

【视图】

系统视图

【参数】

password：指定 SSH 用户缺省采用 AAA 认证；

rsa：指定 SSH 用户缺省采用 RSA 认证；

all：指定 SSH 用户缺省采用 AAA 认证或者是 RSA 认证；

password-publickey：指定 SSH 用户缺省采用 AAA 认证+RSA 认证。

【描述】

ssh authentication-type default 命令用来为 SSH 用户指定一种缺省的认证方式。配置该命令后，每当增加一个 SSH 用户（通过 **ssh user** 命令配置）时，若没有通过 **ssh user authentication-type** 命令单独为这个用户指定认证方式，则该用户采用缺省认证方式。

undo ssh authentication-type default 命令用来清除所指定的缺省认证方式，也就是不再指定缺省认证方式。此时每当增加一个 SSH 用户时，必须同时为其指定认证方式。

当使用 SSH 1.5 版本的客户端时，如果服务器端配置 password-publickey 认证方式，则只要一种认证方式认证成功，则通过认证。

缺省情况下，没有指定缺省的认证方式。

相关配置可参考命令 **ssh user authentication-type**。

【举例】

配置 SSH 用户缺省的认证方式为 AAA 认证。

```
[H3C] ssh authentication-type default password
```

11.2.16 ssh server authentication-retries

【命令】

ssh server authentication-retries *times*

undo ssh server authentication-retries

【视图】

系统视图

【参数】

times：指定验证重试次数，大于等于 1 而小于等于 5。

【描述】

ssh server authentication-retries 命令用来设置 SSH 连接验证重试次数，在下次登录时生效，**undo ssh server authentication-retries** 命令用来恢复 SSH 连接验证重试次数的默认值。

缺省情况下，*times* 值为 3。

相关配置可参考命令 **display ssh server**。

【举例】

指定登录认证的重试次数为 4 次

```
[H3C] ssh server authentication-retries 4
```

11.2.17 ssh server compatible-ssh1x enable

【命令】

ssh server compatible-ssh1x enable

undo ssh server compatible-ssh1x

【视图】

系统视图

【参数】

无

【描述】

ssh server compatible-ssh1x enable 命令用来设定服务器端兼容 SSH1.x 版本的客户端，**undo ssh server compatible-ssh1x** 命令用来设定服务器端不兼容 SSH1.x 版本的客户端。

缺省情况下，服务器端兼容 SSH1.x 版本的客户端。

【举例】

设定服务器端兼容 SSH1.x 版本的客户端。

```
[H3C] ssh server compatible-ssh1x enable
```

11.2.18 ssh server rekey-interval

【命令】

ssh server rekey-interval *hours*

undo ssh server rekey-interval

【视图】

系统视图

【参数】

hours：更新周期，以小时为单位，最大为 24 小时，最小值为 1 小时。注意，该参数处不能输入 0。

【描述】

ssh server rekey-interval 命令用来设置服务器密钥的更新时间，**undo ssh server rekey-interval** 命令用来取消当前设置。

缺省情况下，为不更新。

相关配置可参考命令 **display ssh server**。

【举例】

设置每 3 小时更新一次服务器密钥

```
[H3C] ssh server rekey-interval 3
```

11.2.19 ssh server timeout

【命令】

ssh server timeout *seconds*

undo ssh server timeout

【视图】

系统视图

【参数】

seconds：指定登录超时时间，单位为秒，取值范围为 1～120。

【描述】

ssh server timeout 命令用来设置 SSH 连接认证超时时间，在下次登录时生效，**undo ssh server timeout** 命令用来恢复 SSH 连接认证超时时间的默认值。

缺省情况下，*seconds* 值为 60 秒。

相关配置可参考命令 **display ssh server**。

【举例】

设定登录超时时间为 80 秒

```
[H3C] ssh server timeout 80
```

11.2.20 ssh-server source-interface

【命令】

ssh-server source-interface *interface-type interface-number*

undo ssh-server source-interface

【视图】

系统视图

【参数】

interface-type interface-number：源接口类型及接口号。

【描述】

ssh-server source-interface 命令用来为 SSH Server 指定源接口，**undo ssh-server source-interface** 命令用来删除为 SSH Server 指定的源接口。

源接口必须是本地存在的接口，否则命令提示不成功。配置源接口后，SSH Server 发送报文中的源 IP 地址为源接口的 IP 地址；删除源接口后，SSH Server 发送报文中的源 IP 地址为出接口的 IP 地址。

缺省情况下，发送报文中的源 IP 地址为出接口的 IP 地址。

📖 **说明：**

指定源 IP 地址和指定源接口命令是互斥的，后配置的命令将覆盖先前的配置。

【举例】

为 SSH Server 指定源接口为 ethernet0/0/0。

```
[H3C] ssh-server source-interface Ethernet 0/0/0
```

11.2.21 ssh-server source-ip

【命令】

ssh-server source-ip *ip-address*

undo ssh-server source-ip

【视图】

系统视图

【参数】

ip-address：源 IP 地址。

【描述】

ssh-server source-ip 命令用来为 SSH Server 指定发送报文中的源 IP 地址，**undo ssh-server source-ip** 命令用来删除为 SSH Server 指定的源 IP 地址。

指定的源 IP 地址必须是本地地址，否则命令提示不成功。删除源 IP 地址后，SSH Server 发送报文中的源 IP 地址为出接口的 IP 地址。

缺省情况下，发送报文中的源 IP 地址为出接口的 IP 地址。

📖 **说明：**

指定源 IP 地址和指定源接口命令是互斥的，后配置的命令将覆盖先前的配置。

【举例】

为 SSH Server 指定发送报文中的源 IP 地址为 192.168.0.1。

```
[H3C] ssh-server source-ip 192.168.0.1
```

11.2.22 ssh user

【命令】

ssh user *username*

undo ssh user *username*

【视图】

系统视图

【参数】

username：SSH 用户名。password 认证时，*username* 应与 AAA 中定义的有效用户名一致；RSA 认证时， *username* 就是 SSH 本地用户名，不需要在 AAA 中定义用户。

【描述】

ssh user 命令用来配置 SSH 用户名，**undo ssh user** 命令用来删除 SSH 用户名。

当用 **ssh authentication-type default** 命令指定了缺省认证类型时，可以用命令 **ssh user** 来增加用户，该用户的认证方式为缺省的认证方式。

如果用户配置的缺省验证方式是 password，并且采用 AAA 本地认证，则还需要用 **local-user** 命令在本地数据库中添加用户名和密码。在这种情况下，可以直接使用 **local-user** 命令配置用户名和密码（ 配置 service-type 为 ssh）登录 SSH 服务器，省略掉 **ssh user** 命令的配置。

相关配置可参考命令 **ssh authentication-type default**。

【举例】

配置 SSH 用户名为 zhangsan。

```
[H3C] ssh user zhangsan
```

11.2.23 ssh user assign

【命令】

ssh user *username* **assign rsa-key** *keyname*

undo ssh user *username* **assign rsa-key**

【视图】

系统视图

【参数】

username：当使用 password 认证时，*username* 应与 AAA 中定义的有效用户名一致；使用 RSA 认证时，*username* 就是 SSH 用户名，不需要在 AAA 中定义用户。

keyname：配置的客户端公共密钥名，长度为 1～64 个字符串。

【描述】

ssh user assign 命令用来为用户 *username* 分配一个已经存在的公钥 *keyname*，**undo ssh user assign** 命令用来删除此用户和它的公钥之间的对应关系。

使用该命令为用户分配公钥时，如果此用户已经被分配了公钥，那么，以最后一次分配的公钥为准。

AAA 模块负责系统本地用户名的创建和删除，当 AAA 模块创建一个 SSH 类型的用户时通知 SSH，SSH 将此用户名加入自身维护的用户集合中。同样当 AAA 模块删除任一个用户时，也需要通知 SSH，SSH 从自己的用户名集中匹配，如果匹配到该用户，则将该用户从用户集中删除。

新配置的用户公钥下次登录时生效。

相关配置可参考命令 **display ssh user-information**。

【举例】

为用户 zhangsan 分配密钥 *key1*

```
[H3C] ssh user zhangsan assign rsa-key key1
```

11.2.24 ssh user authentication-type

【命令】

ssh user *username* **authentication-type** { **password** | **rsa** | **password-publickey** | **all** }

undo ssh user *username* **authentication-type**

【视图】

系统视图

【参数】

username：SSH 用户名。

password：强制指定该用户的验证方式为 password。

rsa：强制指定该用户的验证方式为 RSA。

password-publickey：指定 SSH 用户的认证方式为 AAA 认证和 RSA 认证。

all：指定该用户的验证方式可以是 password 也可以是 RSA。

【描述】

ssh user authentication-type 命令用来为某一特定的用户指定验证方法，**undo ssh user authentication-type** 命令用来恢复系统默认的无法登录方式。

当使用 SSH 1.5 版本的客户端时，如果服务器端配置 password-publickey 认证方式，则只要一种认证方式认证成功，则通过认证。

缺省情况下，系统为无法登录方式。对于新的用户必须指定其验证方式。否则将无法登录。新配置的验证方式，待下次登录时生效。

相关配置可参考命令 **display ssh user-information**。

【举例】

为用户 zhangsan 指定验证方式为 password。

```
[H3C] ssh user zhangsan authentication-type password
```

11.2.25 ssh user service-type

【命令】

ssh user *username* **service-type** { **all** | **sftp** | **stelnet** }

undo ssh user *username* **service-type**

【视图】

系统视图

【参数】

username：当使用 password 认证时，*username* 应与 AAA 中定义的有效用户名一致；使用 RSA 认证时，*username* 就是 SSH 本地用户名，不需要在 AAA 中定义用户。

stelnet：服务类型为 STelnet。

sftp：服务类型为 SFTP。

all：包括 STelnet 和 SFTP 两种服务类型。

【描述】

ssh user service-type 命令用来为某一特定的用户指定服务类型；**undo ssh user service-type** 命令用来恢复系统缺省的服务类型。

缺省情况下，服务类型为 **stelnet**。

相关配置可参考命令 **display ssh user-information**。

【举例】

为用户 zhangsan 指定服务类型为 SFTP。

```
[H3C] ssh user zhangsan service-type sftp
```

11.3 SSH Client 配置命令

📖 **说明：**

public-key-code begin 和 **public-key-code end** 命令 SSH Client 端也支持，参见 SSH Server 部分的说明。

11.3.1 display ssh server-info

【命令】

display ssh server-info

【视图】

所有视图

【参数】

无

【描述】

display ssh server-info 命令用来查看客户端的服务器公钥和服务器的对应关系。

【举例】

显示客户端的服务器和公钥的对应关系。

```
[H3C] display ssh server-info
Server Name(IP)       Server public key name
192.168.0.1           secpath_key01
192.168.0.2           secpath_key02
```

11.3.2 display ssh2 source-ip

【命令】

display ssh2 source-ip

【视图】

所有视图

【参数】

无

【描述】

display ssh2 source-ip 命令用来显示当前为 SSH Client 设置的源 IP 地址。

如果为 SSH Client 指定了源接口，则此命令显示的是该接口的 IP 地址；如果没有为 SSH Client 指定源接口和源 IP 地址，则显示为 0.0.0.0。

【举例】

显示当前为 SSH Client 设置的源 IP 地址。

```
<H3C> display ssh2 source-ip
The source IP you specified is 0.0.0.0
```

11.3.3 quit

【命令】

quit

【视图】

用户视图

【参数】

无

【描述】

quit 命令用来终止与远程 SSH Server 的连接。

【举例】

终止与远程 SSH Server 的连接。

```
<H3C> quit
```

11.3.4 ssh client assign rsa-key

【命令】

ssh client *server* **assign rsa-key** *keyname*

undo ssh client *server* **assign rsa-key**

【视图】

系统视图

【参数】

server：服务器的 IP 地址或名称。

keyname：公钥名称。

【描述】

ssh client assign rsa-key 命令用来在客户端上指定要连接的服务器的公钥名称，以便客户端认证连接的服务器是否为可信赖的服务器；**undo ssh client assign rsa-key** 命令用来取消该服务器公钥的指定关系。

【举例】

在客户端为 IP 地址为 192.168.0.1 的服务器指定公钥名称。

```
[H3C] ssh client 192.168.0.1 assign rsa-key serverkey
```

11.3.5 ssh client first-time enable

【命令】

ssh client first-time enable

undo client ssh first-time

【视图】

系统视图

【参数】

无

【描述】

ssh client first-time enable 命令用来设置 SSH 客户端对访问的 SSH 服务器进行首次认证；**undo ssh client first-time** 命令用来取消 SSH 客户端对访问的 SSH 服务器进行首次认证。

所谓首次认证，是指如果当 SSH 客户端首次访问的服务器公钥在本地不存在时，用户可以选择继续访问该服务器，并在本地保存该服务器的公钥；当用户下次访问该服务器时，就以保存的公钥来认证该服务器。

如果不支持首次认证，那么当连接的服务器公钥在本地不存在时，客户端将拒绝访问该服务器。用户可以事先通过其它途径将要访问的服务器的公钥保存在本地中。

缺省情况下，客户端对服务器进行首次认证。

【举例】

设置 SSH 客户端对访问的 SSH 服务器进行首次认证。

```
[H3C] ssh client first-time enable
```

11.3.6 ssh2

【命令】

ssh2 { *host-ip* | *host-name* } [*port*] [**prefer_kex** { **dh_group1** | **dh_exchange_group** }] [**prefer_ctos_cipher** { **des** | **3des** | **aes128** }] [**prefer_stoc_cipher** { **des** | **3des** | **aes128** }] [**prefer_ctos_hmac** { **sha1** | **sha1_96** | **md5** | **md5_96** }] [**prefer_stoc_hmac** { **sha1** | **sha1_96** | **md5** | **md5_96** }]

【视图】

系统视图

【参数】

host-ip：服务器 IP 地址。

host-name：服务器名称，取值是一个长度为 1～20 的字符串。

port-num：服务器端口号，取值范围为 0～65535，缺省值为 22。

prefer_kex：Key 交换首选算法，选择两种算法之间的一种。

dh_group1：Key 交换算法 diffie-hellman-group1-sha1，为缺省 Key 交换方法。

dh_exchange_group：Key 交换算法 diffie-hellman-group-exchange-sha1

prefer_ctos_cipher：客户端到服务器端的首选加密算法，缺省算法为 aes128。

prefer_stoc_cipher：服务器端到客户端的首选加密算法，缺省算法为 aes128。

des：des_cbc 加密方法。

3des：3des_cbc 加密方法。

aes128：aes_128 加密方法。

prefer_ctos_hmac：客户端到服务器端的首选 HMAC 算法，缺省为 sha1_96。

prefer_stoc_hmac：服务器端到客户端的首选 HMAC 算法，缺省为 sha1_96。

sha1：HMAC 算法 hmac-sha1。

sha1_96：HMAC 算法 hmac-sha1-96。

md5：HMAC 算法 hmac-md5。

md5_96：HMAC 算法 hmac-md5-96。

【描述】

ssh2 命令用来启动 SSH 客户端向服务器发起连接，并指定客户端和服务器的首选密钥交换算法、首选加密算法和首选 HMAC 算法。

【举例】

登入地址为 10.214.50.51 的远程 SSH2 服务器，具体配置如下：

- 首选 KEY 交换算法为 dh_exchange_group
- 客户端到服务器的首选加密算法为 3DES-CBC
- 客户端到服务器的首选 HMAC 算法为 HMAC-MD5
- 服务器到客户端的首选加密算法为 AES-128
- 服务器到客户端的 HMAC 算法为 HMAC-SHA1-96

```
[H3C] ssh2 10.214.50.51 prefer_kex dh_exchange_group prefer_ctos_cipher 3des
prefer_ctos_hmac md5
```

11.3.7 ssh2 source-interface

【命令】

ssh2 source-interface *interface-type interface-number*

undo ssh2 source-interface

【视图】

系统视图

【参数】

interface-type interface-number：源接口类型及接口号。

【描述】

ssh2 source-interface 命令用来为 SSH Client 指定源接口，**undo ssh2 source-interface** 命令用来删除为 SSH Client 指定的源接口。

源接口必须是本地存在的接口，否则命令提示不成功。配置源接口后，SSH Client 发送报文中的源 IP 地址为源接口的 IP 地址；删除源接口后，SSH Client 发送报文中的源 IP 地址为出接口的 IP 地址。

缺省情况下，发送报文中的源 IP 地址为出接口的 IP 地址。

📖 **说明：**

指定源 IP 地址和指定源接口命令是互斥的，后配置的命令将覆盖先前的配置。

【举例】

为 SSH Client 指定发送报文中的源接口为 ethernet0/0/0。

```
[H3C] ssh2 source-interface ethernet0/0/0
```

11.3.8 ssh2 source-ip

【命令】

ssh2 source-ip *ip-address*

undo ssh2 source-ip

【视图】

系统视图

【参数】

ip-address：源 IP 地址。

【描述】

ssh2 source-ip 命令用来为 SSH Client 指定发送报文中的源 IP 地址，**undo ssh2 source-ip** 命令用来删除为 SSH Client 指定的源 IP 地址。

指定的源 IP 地址必须是本地地址，否则命令提示不成功。删除源 IP 地址后，SSH Client 发送报文中的源 IP 地址为出接口的 IP 地址。

缺省情况下，发送报文中的源 IP 地址为出接口的 IP 地址。

📖 **说明：**

指定源 IP 地址和指定源接口命令是互斥的，后配置的命令将覆盖先前的配置。

【举例】

为 SSH Client 指定发送报文中的源 IP 地址为 192.168.0.1。

```
[H3C] ssh2 source-ip 192.168.0.1
```

11.4 SFTP Server 配置命令

11.4.1 sftp server enable

【命令】

sftp server enable

undo sftp server

【视图】

系统视图

【参数】

无

【描述】

sftp server enable 命令用来启动 SFTP 服务器，**undo sftp server** 命令用来关闭 SFTP 服务器。

缺省情况下，SFTP 服务器处于关闭状态。

【举例】

启动 SFTP 服务器。

```
[H3C] sftp server enable
```

关闭 SFTP 服务器。

```
[H3C] undo sftp server
```

11.5 SFTP Client 配置命令

11.5.1 bye

【命令】

bye

【视图】

SFTP client 视图

【参数】

无

【描述】

bye 命令用来终止与远程 SFTP server 的连接，并退回到系统视图。

该命令功能与 **exit**，**quit** 相同。

【举例】

终止与远程 SFTP server 的连接。

```
sftp-client> bye
[H3C]
```

11.5.2 cd

【命令】

cd [*remote-path*]

【视图】

SFTP client 视图

【参数】

remote-path：服务器上的路径名。

【描述】

cd 命令用来改变远程 SFTP 服务器上的工作路径。如果没有指定 *remote-path*，则显示当前工作路径。

【举例】

改变工作路径到 d:/temp。

```
sftp-client> cd d:/temp
```

11.5.3 cdup

【命令】

cdup

【视图】

SFTP client 视图

【参数】

无

【描述】

cdup 命令用来返回到上一级目录。

【举例】

改变工作路径到上一级目录。

```
sftp-client> cdup
```

11.5.4 delete

【命令】

delete *remote-file*

【视图】

SFTP client 视图

【参数】

remote-file：服务器上的文件名。

【描述】

delete 命令用来删除服务器上指定的文件。

该命令和 **remove** 功能相同。

【举例】

删除服务器上的文件 temp.c。

```
sftp-client> delete temp.c
```

11.5.5 dir

【命令】

dir [*remote-path*]

【视图】

SFTP client 视图

【参数】

remote-path：查询的目录名。

【描述】

dir 命令用来查询指定目录下的文件。

如果没有指定 *remote-path*，则查询当前工作目录下的文件。

该命令功能与 **ls** 相同。

【举例】

查询目录 flash:/

```
sftp-client> dir flash:/
-rwxrwxrwx   1 noone    nogroup      1759 Aug 23 06:52 config.cfg
-rwxrwxrwx   1 noone    nogroup       225 Aug 24 08:01 pubkey2
-rwxrwxrwx   1 noone    nogroup       283 Aug 24 07:39 pubkey1
-rwxrwxrwx   1 noone    nogroup       225 Sep 28 08:28 pub1
drwxrwxrwx   1 noone    nogroup         0 Sep 28 08:24 new1
drwxrwxrwx   1 noone    nogroup         0 Sep 28 08:18 new2
-rwxrwxrwx   1 noone    nogroup       225 Sep 28 08:30 pub2
```

11.5.6 display sftp source-ip

【命令】

display sftp source-ip

【视图】

所有视图

【参数】

无

【描述】

display sftp source-ip 命令用来显示当前为 SFTP Client 设置的源 IP 地址。

如果为 SFTP Client 指定了源接口，则此命令显示的是该接口的 IP 地址；如果没有为 SFTP Client 指定源接口和源 IP 地址，则显示为 0.0.0.0。

【举例】

显示当前为 SFTP Client 设置的源 IP 地址。

```
<H3C> display sftp source-ip
The source IP you specified is 0.0.0.0
```

11.5.7 exit

【命令】

exit

【视图】

SFTP client 视图

【参数】

无

【描述】

exit 命令用来终止与远程 SFTP server 的连接，并退回到系统视图。

该命令功能与 **bye**，**quit** 相同。

【举例】

终止与远程 SFTP server 的连接。

```
sftp-client> exit
[H3C]
```

11.5.8 get

【命令】

get *remote-file* [*local-file*]

【视图】

SFTP client 视图

【参数】

remote-file：远程 SFTP Server 上的文件名。

local-file：本地文件名。

【描述】

get 命令用来从远程服务器上下载文件并存储在本地。

缺省情况下，如果没有指定本地文件名，则认为本地文件与远程 SFTP Server 上的文件同名。

【举例】

下载 temp1.c 文件，并以 temp.c 文件名保存。

```
sftp-client> get temp1.c temp.c
```

11.5.9 help

【命令】

help [*command*]

【视图】

SFTP client 视图

【参数】

command：命令名。

【描述】

help 命令用来显示 SFTP 客户端命令的帮助信息。

如果没有指定 *command*，系统将显示所有命令的名字。

【举例】

查看命令 **get** 的帮助信息。

```
sftp-client> help get
get remote-path [local-path]  Download file
Default local-path is the same with remote-path
```

11.5.10 ls

【命令】

ls [*remote-path*]

【视图】

SFTP client 视图

【参数】

remote-path：查询的目录名。

【描述】

ls 命令用来查询指定目录下的文件。

如果没有指定 *remote-path*，则查询当前工作目录下的文件。

该命令功能与 **dir** 相同。

【举例】

查询目录 flash:/

```
sftp-client> ls flash:/
-rwxrwxrwx   1 noone    nogroup      1759 Aug 23 06:52 config.cfg
-rwxrwxrwx   1 noone    nogroup       225 Aug 24 08:01 pubkey2
-rwxrwxrwx   1 noone    nogroup       283 Aug 24 07:39 pubkey1
-rwxrwxrwx   1 noone    nogroup       225 Sep 28 08:28 pub1
drwxrwxrwx   1 noone    nogroup         0 Sep 28 08:24 new1
drwxrwxrwx   1 noone    nogroup         0 Sep 28 08:18 new2
-rwxrwxrwx   1 noone    nogroup       225 Sep 28 08:30 pub2
```

11.5.11 mkdir

【命令】

mkdir *remote-path*

【视图】

SFTP client 视图

【参数】

remote-path：远程 SFTP server 上的目录名。

【描述】

mkdir 命令用来在远程 SFTP server 上建立目录。

【举例】

在远程 SFTP 服务器上建立目录 test。

```
sftp-client> mkdir test
```

11.5.12 put

【命令】

put *local-file* [*remote-file*]

【视图】

SFTP client 视图

【参数】

local-file：本地的文件名。

remote-file：远程 SFTP Server 上的文件名。

【描述】

put 命令用来将本地的文件上传到远程 SFTP Server。

缺省情况下，如果没有指定远程服务器上的文件名，则认为服务器上的文件与本地文件同名。

【举例】

将本地 temp.c 文件上传到远程 SFTP Server，并以 temp1.c 文件名保存。

```
sftp-client> put temp.c temp1.c
```

11.5.13 pwd

【命令】

pwd

【视图】

SFTP client 视图

【参数】

无

【描述】

pwd 命令用来显示远程 SFTP Server 上的工作目录。

【举例】

显示远程 SFTP Server 上的工作目录。

```
sftp-client> pwd
flash:
```

11.5.14 quit

【命令】

quit

【视图】

SFTP client 视图

【参数】

无

【描述】

quit 命令用来终止与远程 SFTP server 的连接，并退回到用户视图。

该命令功能与 **bye**，**exit** 相同。

【举例】

终止与远程 SFTP server 的连接。

```
sftp-client> quit
<H3C>
```

11.5.15 remove

【命令】

remove *remote-file*

【视图】

SFTP client 视图

【参数】

remote-file：服务器上的文件名。

【描述】

remove 命令用来删除服务器上指定的文件。

该命令和 **delete** 功能相同。

【举例】

删除服务器上的文件 temp.c。

```
sftp-client> remove temp.c
```

11.5.16 rename

【命令】

rename *oldname newname*

【视图】

SFTP client 视图

【参数】

oldname：原文件名。

newname：新文件名。

【描述】

rename 命令用来改变 SFTP 服务器上指定的文件名。

【举例】

将 SFTP 服务器上的文件 temp1 改名为 temp2。

```
sftp-client> rename temp1 temp2
```

11.5.17 rmdir

【命令】

rmdir *remote-path*

【视图】

SFTP client 视图

【参数】

remote-path：远程 SFTP server 上的目录名。

【描述】

rmdir 命令用来删除 SFTP 服务器上指定的目录。

【举例】

删除 SFTP 服务器上的 D:/temp1 目录。

```
sftp-client> rmdir D:/temp1
```

11.5.18 sftp

【命令】

sftp { *host-ip* | *host-name* } [*port-num*] [**prefer_kex** { **dh_group1** | **dh_exchange_group** }] [**prefer_ctos_cipher** { **des** | **3des** | **aes128** }] [**prefer_stoc_cipher** { **des** | **3des** | **aes128** }] [**prefer_ctos_hmac** { **sha1** | **sha1_96** | **md5** | **md5_96** }] [**prefer_stoc_hmac** { **sha1** | **sha1_96** | **md5** | **md5_96** }]

【视图】

系统视图

【参数】

host-ip：服务器 IP 地址。

host-name：服务器名称，取值是一个长度为 1～20 的字符串。

port-num：服务器端口号，取值范围为 0～65535，缺省值为 22。

prefer_kex：Key 交换首选算法，选择两种算法之间的一种。

dh_group1：Key 交换算法 diffie-hellman-group1-sha1，为缺省 Key 交换方法。

dh_exchange_group：Key 交换算法 diffie-hellman-group-exchange-sha1。

prefer_ctos_cipher：客户端到服务器端的首选加密算法，缺省算法为 aes128。

prefer_stoc_cipher：服务器端到客户端的首选加密算法，缺省算法为 aes128。

des：des_cbc 加密方法。

3des：3des_cbc 加密方法。

aes128：aes_128 加密方法。

prefer_ctos_hmac：客户端到服务器端的首选 HMAC 算法，缺省为 sha1_96。

prefer_stoc_hmac：服务器端到客户端的首选 HMAC 算法，缺省为 sha1_96。

sha1：HMAC 算法 hmac-sha1。

sha1_96：HMAC 算法 hmac-sha1-96。

md5：HMAC 算法 hmac-md5。

md5_96：HMAC 算法 hmac-md5-96。

【描述】

sftp 命令用来与远程 SFTP 服务器建立连接，并进入 SFTP client 视图。

【举例】

连接 IP 地址为 10.214.49.126 的 SFTP 服务器，加密算法等均取缺省值。

```
[H3C] sftp 10.214.49.126
```

11.5.19 sftp source-interface

【命令】

sftp source-interface *interface-type interface-number*

undo sftp source-interface

【视图】

系统视图

【参数】

interface-type interface-number：源接口类型及接口号。

【描述】

sftp source-interface 命令用来为 SFTP Client 指定源接口，**undo sftp source-interface** 命令用来删除为 SFTP Client 指定的源接口。

源接口必须是本地存在的接口，否则命令提示不成功。配置源接口后，SFTP Client 发送报文中的源 IP 地址为源接口的 IP 地址；删除源接口后，SFTP Client 发送报文中的源 IP 地址为出接口的 IP 地址。

缺省情况下，发送报文中的源 IP 地址为出接口的 IP 地址。

📖 **说明：**

指定源 IP 地址和指定源接口命令是互斥的，后配置的命令将覆盖先前的配置。

【举例】

为 SFTP Client 指定发送报文中的源接口为 ethernet0/0/0。

```
[H3C] sftp source-interface ethernet0/0/0
```

11.5.20 sftp source-ip

【命令】

sftp source-ip *ip-address*

undo sftp source-ip

【视图】

系统视图

【参数】

ip-address：源 IP 地址。

【描述】

sftp source-ip 命令用来为 SFTP Client 指定发送报文中的源 IP 地址，**undo sftp source-ip** 命令用来删除为 SFTP Client 指定的源 IP 地址。

指定的源 IP 地址必须是本地地址，否则命令提示不成功。删除源 IP 地址后，SFTP Client 发送报文中的源 IP 地址为出接口的 IP 地址。

缺省情况下，发送报文中的源 IP 地址为出接口的 IP 地址。

📖 **说明：**

指定源 IP 地址和指定源接口命令是互斥的，后配置的命令将覆盖先前的配置。

【举例】

为 SFTP Client 指定发送报文中的源 IP 地址为 192.168.0.1。

```
[H3C] sftp source-ip 192.168.0.1
```

第12章 Modem 管理配置命令

12.1 Modem 管理配置命令

12.1.1 debugging modem

【命令】

debugging modem

undo debugging modem

【视图】

用户视图

【参数】

无

【描述】

debugging modem 命令用来打开 Modem 调试信息开关，**undo debugging modem** 用来关闭 Modem 调试信息开关。

根据该命令输出信息，可以确认对特定事件是否指定了正确的 Modem 脚本。

【举例】

打开 Modem 调试信息开关。

```
<H3C> debugging modem
```

12.1.2 modem

【命令】

modem [**both** | **call-in** | **call-out**]

undo modem [**both** | **call-in** | **call-out**]

【视图】

用户界面视图

【参数】

both：表示同时允许 Modem 呼入和呼出。

call-in：仅允许 Modem 呼入。

call-out：仅允许 Modem 呼出。

【描述】

modem 命令用来允许 Modem 呼入和呼出，**undo modem** 和 **undo modem both** 命令用来禁止 Modem 呼入和呼出，**undo modem** [**call-in** | **call-out**]命令用来禁止 Modem 呼入或呼出。

接口上缺省为禁止 Modem 呼入和呼出。

使用该命令可以设置接口上 Modem 呼入和呼出的权限。

【举例】

仅允许 AUX 口接收 Modem 呼入。

```
[H3C-ui-aux0] modem call-in
```

12.1.3 modem auto-answer

【命令】

modem auto-answer

undo modem auto-answer

【视图】

用户界面视图

【参数】

无

【描述】

modem auto-answer 命令用来设置异步口外接 Modem 为自动应答（即摘机）方式，**undo modem auto-answer** 命令用来设置异步口外接 Modem 为非自动应答方式，即通过软件发送 AT 指令给 Modem 来应答。

系统缺省为外接 Modem 是非自动应答方式。

建议根据防火墙外接 Modem 的当前应答状态配置该命令，当 Modem 状态为自动应答（Modem 的 AA 灯亮）时，配置 **modem auto-answer**（以避免 Modem 自动应答后，防火墙又发出应答指令）；如果外接 Modem 为非自动应答方式，则可配置 **undo modem auto-answer**。

📖 **说明：**

当该命令的配置与 Modem 当前的应答状态不一致时，对于某些 Modem 可能会造成应答不正常。

相关配置可参考命令 **modem**。

【举例】

设置 AUX 口外接 Modem 为自动应答方式。

```
[H3C-ui-aux0] modem auto-answer
```

12.1.4 script-string

【命令】

script-string *script-name script-content*

undo script-string *script-name*

【视图】

系统视图

【参数】

script-name：脚本名称。

script-content：脚本内容。

【描述】

script-string 命令用来定义 Modem 脚本，**undo script-string** 命令用来删除 Modem 脚本。

系统缺省没有 Modem 脚本。

SecPath 系列防火墙提供了 Modem 脚本，其主要用途包括：

- 使用 Modem 脚本可以灵活地控制不同型号的 Modem，如使用不同的初始化字符串，使不同厂家和型号的设备可以和防火墙更好地协调工作。
- 使用 Modem 脚本可以进行远端系统的交互登录，可以通过脚本的交互协商转入不同的连接状态。如双方设备的异步串口（例如 AUX 口）通过 Modem 建立连接之后，在该物理链路上封装何种协议，以及该协议的各种工作参数等都可以互相协商确定。

Modem 脚本常见格式如下：

send-string1 receive-string1 send-string2 receive-string2 .....

其中：

- *send-string* 表示发送字符串。
- *receive-string* 表示接收字符串。

- *send-string* 和 *receive-string* 一般成对出现，而且脚本必须以发送字符串为开始，如 *send-string1 receive-string1* ..... 表示的执行流程为：向 Modem 发送字符串 *send-string1*，希望接收到字符串 *receive-string1*，如果在超时之前，接收到字符串与 *receive-string1* 匹配成功，则继续执行以下脚本，否则终止脚本的执行。
- 如果最后一个字符串为发送字符串，则表明发送该字符串后，即可结束脚本的执行，不需再等待接收字符串。
- 如果脚本的开始不需发送字符串，而直接等待接收字符串，这时可以将第一个发送字符串置为""，关于双引号的意义后面有详细介绍。
- 对于发送字符串，除以\c 结束之外，发送时均会在字符串结尾自动附加一个回车符。
- 对于接收字符串的匹配，采用与位置无关的匹配方法，即只要接收的内容中含有希望接收的串，就认为匹配成功。
- 接收字符串的匹配，希望接收的字符串可以有多个，它们之间用-连接，只要与其中之一匹配，即认为匹配成功。
- 等待接收字符串的缺省超时时间为 5 秒，在脚本中可随时插入 **TIMEOUT** *seconds* 来调整等待接收字符串的超时时间，并在同一个脚本的下一次 **TIMEOUT** 设置前一直有效。其含义参见下表。

表12-1 脚本关键字列表

关键字	说明
ABORT receive-string	ABORT 后跟一个字符串，用于和 Modem 或对端的 DTE 设备传送来的字符串进行匹配，匹配的方式是完全匹配，一个脚本中可以有多个 ABORT 指定，每一个都在脚本的整个执行期有效。
TIMEOUT seconds	TIMEOUT 后跟一数字，用于设置接收字符串的超时等待时间，在等待的时间内如果没有收到希望的字符串，则脚本执行失败。此设置在设置以后有效，一直作用到下一次进行 TIMEOUT 设置。

- 脚本中所有字符串和关键字都是大小写敏感的。
- 各字符串或关键字之间用空格进行分割，如果一个字符串内部包含空格，则需要用双引号（" "）括起来，如果双引号内没有任何内容（即为""），则该字符串可能有两种意义，如果""位于脚本的开始，表明不需发送任何字符串，而直接等待接收字符串，而在其它位置则认为字符串内容为""。
- 在脚本中可随时插入 **ABORT** *receive-string* 来改变脚本的执行流程，表示如果接收字符串与 *receive-string* 完全匹配，则终止脚本的执行。在脚本中 **ABORT** *receive-string* 可以出现多次，它们将会共同起作用，只要与其中之一

匹配，即终止脚本的执行，而且无论 **ABORT** *receive-string* 在何处出现，它在整个脚本执行过程中均起作用。

- 在脚本中可以插入转义字符，用于更好的对于脚本进行控制并增加脚本的灵活性，另外所有的转义字符同时也是字符串的分隔符。具体请参见下表。

表12-2 脚本转义字符列表

转义字符	说明
\c	表示只发送所指定的字符串，不自动附加回车符。\c 位置只能在发送字符串的末尾，其他的位置无效。
\d	表示暂停 2 秒
\n	表示换行字符
\r	表示回车字符
\s	表示空格字符
\t	表示制表字符
\\	表示反斜杠字符
\T	表示电话号码

【举例】

```
[H3C] script-string example "" AT OK ATS0=1 OK
```

12.1.5 start-script

【命令】

start-script *script-name number*

【视图】

用户视图

【参数】

script-name：脚本集中的一个脚本。

number：运行脚本的接口编号。

【描述】

start-script 命令用来执行指定的 Modem 脚本。

这条命令提供了 Modem 脚本立即执行的方法，如果相应的接口上正在执行一个脚本，则本次命令不会执行，并且会报告一条错误消息。

相关配置可参考命令 **script-string**。

【举例】

在对应的接口编号为 1 上执行指定 Modem 脚本“example”。

```
<H3C> start-script example 1
```

第13章 接口配置命令

13.1 接口管理命令

13.1.1 debugging physical

【命令】

debugging physical { **all** | **error** | **event** | **packet** { **all** | **input** | **output** } } [**interface** *interface-type interface-number*]

undo debugging physical { **all** | **error** | **event** | **packet** { **all** | **input** | **output** } } [**interface** *interface-type interface-numbe*r]

【视图】

用户视图

【参数】

all：打开指定接口所有 debug 信息调试开关。

error：打开错误信息调试开关。

event：打开事件信息调试开关。

packet：打开数据包信息调试开关。

input：打开数据包的输入调试开关。

output：打开数据包的输出调试开关。

all：打开数据包的输入和输出调试开关。

interface *interface-type interface-number*：指定的接口类型及编号。

【描述】

debugging physical 命令用来打开接口物理模块的 debug 信息调试开关，**undo debugging physical** 命令用来关闭接口的 debug 信息调试开关。

缺省情况下，未打开调试信息开关。

【举例】

打开所有接口的事件信息调试开关。

```
<H3C> debugging physical event
```

13.1.2 description

【命令】

description *interface-description*

undo description

【视图】

接口视图

【参数】

interface-description：防火墙接口的描述字符串，不超过 80 个字符。缺省的描述为“xxxxxx Interface”。

【描述】

description 命令用来设置接口描述，**undo description** 命令用来恢复缺省的接口描述。

本命令仅仅用于标识某接口，并无特别的意义和用途。

相关配置可参考命令 **display interface**。

【举例】

修改以太网接口 Ethernet 0/0/0 的描述为“SecPath gateway ethernet interface”。

```
[H3C] interface ethernet 0/0/0
[H3C-Ethernet0/0/0] description SecPath gateway ethernet interface
```

13.1.3 display brief interface

【命令】

display brief interface [*type* [*number*]] [| { **begin** | **include** | **exclude**} *text*]

【视图】

所有视图

【参数】

type：接口类型。

number：接口号。

begin：显示以指定正则表达式（*text*）开头的信息。

include：显示包含指定正则表达式（*text*）的信息。

exclude：显示不含指定正则表达式（*text*）的信息。

text：正则表达式文字。

【描述】

display brief interface 命令用来显示接口概要信息。

【举例】

显示包含正则表达式“down”的接口概要信息。

```
<H3C> display brief interface | include down
Interface          Link      Protocol-link  Protocol type  Main IP
Aux0               DOWN      DOWN               PPP                --
Dialer0            UP        UP (spoofing)      PPP                --
Ethernet0/0/0      DOWN      DOWN               ETHERNET         --
NULL0              UP        UP (spoofing)      NULL               --
```

13.1.4 display interface

【命令】

display interface [*type* [*number*]] [*.sub-number*]

【视图】

所有视图

【参数】

type：接口类型，与 *number* 一起指定了一个接口。

number：接口号，与 *type* 一起指定了一个接口。

sub-number：子接口编号。

【描述】

display interface 命令用来显示接口当前的运行状态和相关信息。

使用本命令能显示的信息包括：

- 接口的物理状态和协议状态
- 接口的物理特性（同异步、DTE/DCE、时钟选择、外接电缆等）
- 接口的 IP 地址
- 接口的链路层协议以及链路层协议运行状态和统计信息等
- 接口的输入输出报文统计信息

相关配置可参考命令 **reset counters interface**。

【举例】

查看接口 ethernet 2/0/0 的运行状态和相关信息。

```
<H3C> display interface ethernet 2/0/0
```

```
Ethernet2/0/0 current state : UP
Line protocol current state : UP
Description : Ethernet2/0/0 Interface
The Maximum Transmit Unit is 1500, Hold timer is 10(sec)
Internet Address is 172.31.29.103/16
IP Sending Frames' Format is PKTFMT_ETHNT_2, Hardware address is
00e0.fc06.3085
Media type is twisted pair, loopback not set, promiscuous mode not set
100Mb/s-speed mode,Full-duplex mode,link type is autonegotiation
Output flow-control is unsupported, input flow-control is unsupported
Output queue : (Urgent queue : Size/Length/Discards)  0/500/0
Output queue : (FIFO queuing : Size/Length/Discards)  0/75/0
    Last 5 minutes input rate 227.13 bytes/sec, 2.67 packets/sec
    Last 5 minutes output rate 0.00 bytes/sec, 0.00 packets/sec
    Input: 542665 packets, 47721004 bytes
           271460 broadcasts, 271205 multicasts
           0 errors, 0 runts, 0 giants,
           0 CRC, 0 align errors, 0 overruns,
           0 dribbles, 0 aborts, 0 no buffers
    Output:0 packets, 0 bytes
           0 errors, 0 underruns, 0 collisions
           0 deferred
```

表13-1 display interface 命令显示信息说明

域名	描述
Ethernet2/0/0 current state : UP	以太网接口当前的状态
Line protocol current state	以太网接口链路协议当前的状态
Description	以太网接口的描述信息
The Maximum Transmit Unit is 1500	以太网接口设置的最大传输单元（MTU）
Hold timer is 10(sec)	轮询时间间隔
Internet Address is 172.31.29.103/16	以太网接口的 IP 地址及子网掩码
IP Sending Frames' Format is PKTFMT_ETHNT_2, Hardware address is 00e0.fc06.3085	IP 传输帧使用的格式和硬件地址（MAC）
Media type is twisted pair	介质类型
loopback not set	接口是否设置了环回
promiscuous mode not set	是否设置了混杂模式
100Mb/s-speed mode,Full-duplex mode,link type is autonegotiation	以太网接口的速率、双工模式和链路的类型
Output flow-control is unsupported, input flow-control is unsupported	表示接口输出和输入的数据报文的流控方式

域名	描述
Output queue : (Urgent queue : Size/Length/Discards) 0/500/0	输出紧急队列的大小、长度和丢包数
Output queue : (FIFO queuing : Size/Length/Discards) 0/75/0	先进现出队列的大小、长度和丢包数
Last 5 minutes input rate 227.13 bytes/sec, 2.67 packets/sec Last 5 minutes output rate 0.00 bytes/sec, 0.00 packets/sec	接口最后五分钟输入和输出率的统计，包括每秒输入/输出的字节数和每秒输入/输出的报文数
Input: 542665 packets, 47721004 bytes 271460 broadcasts, 271205 multicasts 0 errors, 0 runts, 0 giants, 0 CRC, 0 align errors, 0 overruns, 0 dribbles, 0 aborts, 0 no buffers	接口输入数据报文的统计，包括接口总共输入的报文数、字节数、广播报文数、多播报文数、错误报文数等

📖 **说明：**

由于 SecPath 系列中不同型号的产品使用的芯片不同，所以对于报文的统计方式可能会略有不同，请用户以实际产品为准。

13.1.5 flow-interval

【命令】

flow-interval *seconds*

undo flow-interval

【视图】

系统视图

【参数】

seconds：统计周期，缺省为 300 秒钟，取值范围为 5～1500 秒钟。

【描述】

flow-interval 命令用来配置接口平均速率的统计周期，此配置将应用到所有的接口。

undo flow-interval 命令用来恢复接口平均速率统计周期的缺省值。

相关配置可参考命令 **display interface**。

【举例】

配置接口的平均速率统计周期为 10 秒钟。

```
[H3C] flow-interval 10
```

显示 Ethernet0/0/0 的相关信息。

```
[H3C] display interface Ethernet 0/0/0
Ethernet0/0/0 current state :UP
Line protocol current state :UP
Description :  Ethernet0/0/0 Interface
The Maximum Transmit Unit is 1500, Hold timer is 10(sec)
Internet Address is 202.82.28.28/28
Internet Address is 10.0.103.254/24 Sub
Internet Address is 10.0.102.254/24 Sub
IP Sending Frames' Format is PKTFMT_ETHNT_2, Hardware address is
00e0-fc12-384f
Media type is twisted pair, loopback not set, promiscuous mode not set
100Mb/s, Full-duplex, link type is force link
Output flow-control is disabled, input flow-control is disabled
Output queue : (Urgent queue : Size/Length/Discards)  0/50/0
Output queue : (Protocol queue : Size/Length/Discards) 0/500/0
Output queue : (FIFO queuing : Size/Length/Discards)  0/75/0
    Last 10 seconds input rate 138.36 bytes/sec, 1.63 packets/sec
    Last 10 seconds output rate 5.59 bytes/sec, 0.13 packets/sec
    Input: 492731 packets, 84128872 bytes, 492731 buffers
           156266 broadcasts, 145584 multicasts, 0 pauses
           79 errors, 78 runts, 0 giants
           1 crc, 0 align errors, 0 overruns
           0 dribbles, 0 drops, 0 no buffers
    Output:230681 packets, 165591360 bytes, 230683 buffers
           10916 broadcasts, 0 multicasts, 0 pauses
           0 errors, 0 underruns, 0 collisions
           0 deferred, 0 lost carriers
```

13.1.6 insulate

【命令】

insulate

undo insulate

【视图】

系统视图

【参数】

无

【描述】

insulate 命令用来配置 LAN 以太网接口之间进行隔离，**undo insulate** 命令用来配置 LAN 以太网接口之间不进行隔离。

当 LAN 以太网接口处于隔离模式时，各个 LAN 以太网接口工作在第三层，作为可路由接口使用，即可以为其配置各种第三层属性，如 IP 地址等。当 LAN 以太网接口处于非隔离模式时，各个 LAN 以太网接口工作在 Hub 方式，即工作在物理层，不能为其配置如 IP 地址等第三层属性。当 LAN 以太网接口工作在非隔离模式下时，可以通过配置一个管理 IP 地址以对其进行管理或使其提供网络服务（例如 Telnet、SNMP、NAT 等）。

由于接口性质的因素，只能在第一个 LAN 口（即编号最小的）上配置子接口。在隔离模式下扩展出来的另外三个 LAN 口都不能配置子接口，且第一个 LAN 口上配置的子接口只能在非隔离模式下工作。

仅 SecPath F100-A 防火墙、SecPath V100-S 安全网关支持此命令。

缺省情况下，LAN 以太网接口之间相互隔离。

【举例】

将各个 LAN 以太网接口进行隔离。

```
[H3C] insulate
```

当接口之间被隔离后，所有 LAN 以太网接口（Ethernet0/0、Ethernet0/1、Ethernet0/2、Ethernet0/3）都可见，并可以为其进行单独配置如 IP 地址等第三层属性。

```
<H3C> display ip interface brief
*down: administratively down
(s): spoofing
 Interface                IP Address      Physical Protocol    Description
 Aux0                     unassigned      down     up(s)       Aux0 Inte...
 Encrypt2/0               unassigned      down     down        Encrypt2/...
 Ethernet0/0              unassigned      up       down        Ethernet0...
 Ethernet0/1              unassigned      up       down        Ethernet0...
 Ethernet0/2              unassigned      down     down        Ethernet0...
 Ethernet0/3              unassigned      down     down        Ethernet0...
 Ethernet1/0              unassigned      down     down        Ethernet1...
 Ethernet1/1              unassigned      down     down        Ethernet1...
 Ethernet1/2              unassigned      down     down        Ethernet1...
```

配置不将 LAN 以太网接口之间进行隔离。

```
[H3C] undo insulate
```

当接口之间未被隔离时，可以看到只有一个管理接口 Ethernet0/0 可见，其它所有 LAN 以太网接口都将不可见。可以在管理接口上配置 IP 地址作为管理 IP 地址。

```
<H3C> display ip interface brief
*down: administratively down
(s): spoofing
 Interface                IP Address      Physical Protocol    Description
 Aux0                     unassigned      down     up(s)       Aux0 Inte...
 Encrypt2/0               unassigned      down     down        Encrypt2/...
 Ethernet0/0              unassigned      up       down        Ethernet0...
 Ethernet1/0              unassigned      down     down        Ethernet1...
 Ethernet1/1              unassigned      down     down        Ethernet1...
 Ethernet1/2              unassigned      down     down        Ethernet1...
```

13.1.7 interface

【命令】

interface *type number* [*.sub-number*]

undo interface *type number* [*.sub-number*]

【视图】

系统视图

【参数】

type：接口类型。防火墙目前支持的接口类型请见下表。

number：接口编号。Comware 将防火墙的各种类型接口分别编号，每类接口的编号从 0 或 1 开始。

sub-number：子接口编号，与主接口编号之间用符号“.”隔开。

【描述】

interface 命令用来进入相应接口视图，或创建逻辑接口和子接口，**undo interface** 命令用来删除指定的逻辑接口或子接口。

表13-2 防火墙支持的接口类型

接口类型	说明	接口属性
AUX	备份接口	物理接口
Dialer	拨号接口	逻辑接口
Ethernet	以太网接口	物理接口
gigabitethernet	千兆以太网接口	物理接口
Loopback	环回接口	逻辑接口
NULL	空接口	逻辑接口
Virtual-Template	虚拟模板接口	逻辑接口

接口类型	说明	接口属性
Tunnel	隧道接口	逻辑接口

在了解接口编号规则之后，即可知道接口的命名，物理接口名为接口类型+接口编号。如 Ethernet 0/0/0 表示编号为 0/0/0 的以太网口，Ethernet 0/0/0.1 表示接口 Ethernet0/0/0 的第 1 个子接口。

为了方便用户输入，接口名中接口类型可以简写（只取前几个字母，与其它接口类型不冲突即可），如 Ethernet 0/0/0 可以简写为 e0/0/0，Ethernet 0/0/0.1 可以简写为 e0/0/0.1。

逻辑接口名一般为接口类型+接口号，如 tunnel0。

执行 **interface** 命令不仅可进入实际物理接口视图，也可根据用户需要创建逻辑接口或子接口。

对于以太网接口，可以为其创建子接口。编号为 0 的子接口即为其所对应的主接口。

需要注意的是：**undo interface** 命令可以删除用户定义的逻辑接口（如 Dialer、Tunnel、Virtual-template）和子接口。

【举例】

从系统视图进入到以太网口视图。

```
[H3C] interface ethernet 0/0/0
[H3C-Ethernet0/0/0]
```

从接口 Ethernet0/0/0 视图切换到 AUX 口视图。

```
[H3C-Ethernet0/0/0] interface aux 0
[H3C-Aux0]
```

13.1.8 mtu

【命令】

mtu *size*

undo mtu

【视图】

接口视图

【参数】

size：接口 MTU 的大小，单位为字节。以太网接口的 MTU 取值范围为 46～1500；Dialer 接口的 MTU 取值范围为 128～1500；Virtual-Template 的 MTU 取值范围为 128～1500；Tunnel 接口的 MTU 取值范围为 100～64000。

【描述】

mtu 命令用来设置接口的 MTU（最大传输单元），**undo mtu** 命令用来恢复 MTU 的缺省值。

接口的最大传输单元将影响 IP 报文在接口的分片与重组。

使用 **display interface** 命令可以查看接口缺省的 MTU 值。

【举例】

设置以太网接口的最大传输单元为 1492。

```
[H3C-Ethernet0/0/0] mtu 1492
```

13.1.9 reset counters interface

【命令】

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

【视图】

用户视图

【参数】

type：接口类型，与 *number* 一起指定了一个接口。

number：接口号，与 *type* 一起指定了一个接口。

【描述】

reset counters interface 命令用来清除接口对收发报文的统计信息及 IP、ARP、ICMP 的统计信息。

如果不指定一个具体的接口，则缺省清除全部接口的报文收发统计信息及 IP、ARP、ICMP 的统计信息。

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。

相关配置可参考命令 **display interface**。

【举例】

清除接口 Ethernet 0/0/0 的统计信息。

```
<H3C> reset counters interface Ethernet 0/0/0
```

13.1.10 shutdown

【命令】

shutdown

undo shutdown

【视图】

接口视图

【参数】

无

【描述】

shutdown 命令用来关闭一个接口，**undo shutdown** 命令用于启用一个接口。

本命令除在物理接口上有效之外，对于 LoopBack 接口、Tunnel 接口和 MFR 接口也有效。

在某些特殊情况下，如修改接口的工作参数时，改动不能立即生效，需要关闭和重启接口后才能生效。

相关配置可参考命令 **display interface**。

【举例】

关闭接口 Ethernet 0/0/0。

```
[H3C-Ethernet0/0/0] shutdown
%Dec 15 13:48:39:630 2004 28-31 PHY/2/PHY:   Ethernet0/0/0: change status to
down
%Dec 15 13:48:39:730 2004 28-31 IFNET/5/UPDOWN:Line protocol on the interface
Et
```

13.2 Ethernet 接口配置命令

13.2.1 display interface ethernet

【命令】

display interface { **ethernet** | **gigabitethernet** } [*interface-number*]

【视图】

所有视图

【参数】

ethernet：查看快速以太网接口的状态信息。

gigabitethernet：查看千兆以太网接口的状态信息。

interface-number：接口编号。如果不指定接口编号，将显示所有接口的配置及状态信息。

【描述】

display interface { **ethernet** | **gigabitethernet** } 命令用来显示以太网接口各种配置参数以及当前运行状态等信息。

【举例】

查看以太网接口 2/0/0 的状态信息。

```
<H3C> display interface ethernet 2/0/0
Ethernet2/0/0 current state : UP
Line protocol current state : UP
Description : Ethernet2/0/0 Interface
The Maximum Transmit Unit is 1500, Hold timer is 10(sec)
Internet Address is 172.31.29.103/16
IP Sending Frames' Format is PKTFMT_ETHNT_2, Hardware address is
00e0.fc06.3085
Media type is twisted pair, loopback not set, promiscuous mode not set
100Mb/s-speed mode,Full-duplex mode,link type is autonegotiation
Output flow-control is unsupported, input flow-control is unsupported
Output queue : (Urgent queue : Size/Length/Discards)  0/500/0
Output queue : (FIFO queuing : Size/Length/Discards)  0/75/0
    Last 5 minutes input rate 227.13 bytes/sec, 2.67 packets/sec
    Last 5 minutes output rate 0.00 bytes/sec, 0.00 packets/sec
    Input: 542665 packets, 47721004 bytes
           271460 broadcasts, 271205 multicasts
           0 errors, 0 runts, 0 giants,
           0 CRC, 0 align errors, 0 overruns,
           0 dribbles, 0 aborts, 0 no buffers
    Output:0 packets, 0 bytes
           0 errors, 0 underruns, 0 collisions
           0 deferred
```

13.2.2 duplex

【命令】

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

undo duplex

【视图】

以太网接口视图

【参数】

full：设置以太网接口为全双工模式。

half：设置以太网接口为半双工模式。

negotiation：设置以太网接口为自动协商模式。

【描述】

duplex 命令用来设置以太网接口的工作模式，**undo duplex** 命令用来恢复以太网接口的缺省工作模式。

缺省情况下，以太网接口工作在自动协商模式。

当防火墙的以太网接口与 HUB 相连时，应工作于半双工模式；当防火墙的以太网接口与交换式 LAN Switch 等支持全双工模式的网络设备相连，而且对端设备设置为全双工模式时，应工作于全双工模式。FE 电接口和 GE 电接口对这两种模式都支持，而 FE 光接口和 GE 光接口只能工作在全双工模式。

将以太网接口设置为自动协商模式时，应确保连接对端也工作于自动协商模式，如不能确定，则建议双方使用强制设置，以保持工作模式的一致性。

SecPath F100-C 防火墙的 WAN 接口不支持自动协商。

相关配置可参考命令 **speed**，**display interface**。

【举例】

设置快速以太网接口工作在全双工模式。

```
[H3C-Ethernet0/0/0] duplex full
```

13.2.3 flow-control

【命令】

flow-control

undo flow-control

【视图】

以太网接口视图

【参数】

无

【描述】

flow-control 命令用来设置以太网接口启用流控，这种方式只有在对端支持流控时才有效。**undo flow-control** 命令用来恢复缺省设置。

缺省情况下，不启用流控。

使用此命令时，应与对端配置保持一致。

【举例】

设置以太网接口 Ethernet 0/0/0 启用流控方式。

```
<H3C> system-view
[H3C] interface Ethernet 0/0/0
[H3C-Ethernet0/0/0] flow-control
```

13.2.4 loopback (Ethernet/Gigabitethernet Interface)

【命令】

loopback

undo loopback

【视图】

以太网接口视图

【参数】

无

【描述】

loopback 命令用来允许以太网接口对内自环，**undo loopback** 命令用来禁止以太网接口对内自环。

缺省情况下，禁止以太网接口对内自环。

只有在进行某些特殊功能测试时，才需要将以太网接口设为对内自环。

【举例】

允许快速以太网接口对内自环。

```
[H3C-Ethernet0/0/0] loopback
```

13.2.5 promiscuous

【命令】

promiscuous

undo promiscuous

【视图】

以太网接口视图

【参数】

无

【描述】

promiscuous 命令用来将以太网接口设为混杂模式，**undo promiscuous** 命令用来取消以太网接口混杂模式。

缺省情况下，以太网接口为非混杂模式。

当以太网接口被配置为混杂模式后将不再进行 MAC 地址过滤，接收所有正确的以太网报文。该模式主要用于网络监听功能。

当启动桥功能并将以太网接口加入 bridge-set 后，该以太网接口将自动进入混杂模式；当将以太网接口退出 bridge-set 后，该以太网接口将自动进入非混杂模式。

【举例】

将 ethernet0/0/0 设置为混杂模式。

```
[H3C-Ethernet0/0/0] promiscuous
```

13.2.6 speed

【命令】

speed { **10** | **100** | **1000**| **negotiation** }

undo speed

【视图】

以太网接口视图

【参数】

10：强制以太网接口工作速率为 10Mbps 模式。

100：强制以太网接口工作速率为 100Mbps 模式。

1000：强制以太网接口工作速率为 1000Mbps 模式（仅对千兆接口可用）。

negotiation：设置以太网接口工作速率为自动协商模式。

【描述】

speed 命令用来设置以太网接口的工作速率，**undo speed** 命令用来恢复以太网接口的缺省工作速率。

缺省情况下，以太网接口工作速率为自动协商模式。

将以太网接口的工作速率设置为自动协商模式时，应确保连接对端也为自动协商模式，如不能确定，则建议双方使用强制设置，以保持工作速率的一致性。

对于快速以太网的电接口，可以设置速率为 10Mbit/s、100Mbit/s 或自适应方式；对于千兆以太网的电接口，可以设置速率为 10Mbit/s、100Mbit/s、1000Mbit/s 或自适

应方式。而快速以太网的光接口速率固定为 100Mbit/s，千兆以太网的光接口速率固定为 1000Mbit/s，都不能通过配置命令改变。

📖 说明：

对于 GE 电接口，工作速率 1000Mbit/s 与半双工模式是互斥的，不能同时配置。

相关配置可参考命令 **duplex**，**display interface**。

【举例】

设置快速以太网接口工作速率为 10Base-T 模式。

```
[H3C-Ethernet0/0/0] speed 10
```

13.3 AUX 口配置命令

13.3.1 async mode

【命令】

async mode { **protocol** | **flow** }

【视图】

AUX 接口视图

【参数】

protocol：协议模式。指物理连接建立之后，接口直接采用已有的链路层协议配置参数建立链路。

flow：流模式，也称交互模式。指物理连接建立之后，链路的两端进行交互，主叫端向接收端发送配置命令（与用户从远端手工键入配置命令效果相同），设置接收端的链路层协议工作参数，然后建立链路。一般用于拨号等人机交互的情况。

【描述】

async mode 命令用来设置 AUX 接口的工作方式。目前版本只支持流方式建立链路。

缺省情况下，AUX 接口缺省工作在流方式（**flow**）。

相关配置可参考命令 **modem**。

【举例】

设置 AUX 接口工作在流方式。

```
[H3C-Aux0] async mode flow
```

13.3.2 detect

【命令】

detect dsr-dtr

undo detect dsr-dtr

【视图】

AUX 口视图

【参数】

dsr-dtr：检测 DSU/CSU 的 DSR 和 DTR 信号。

【描述】

detect 命令用来启用数据载波检测和电平检测功能，**undo detect** 命令用来禁止该功能。

缺省情况下，允许数据载波检测和电平检测功能。

如果禁用了此功能，防火墙在判断接口状态为 UP 或 DOWN 时，将不会检测 DCD 信号和 DSR/DTR 信号。

【举例】

禁止数据载波检测功能。

```
[H3C-Aux0] undo detect dsr-dtr
```

13.3.3 loopback

【命令】

loopback

undo loopback

【视图】

AUX 接口视图

【参数】

无

【描述】

loopback 命令用来允许 AUX 接口对内自环对外回波，**undo loopback** 命令用来禁止 AUX 接口对内自环对外回波。

缺省情况下，禁止 AUX 接口对内自环对外回波。

只有在进行某些特殊功能测试时，才将 AUX 接口设为对内自环对外回波。

【举例】

允许 AUX 接口对内自环对外回波。

```
[H3C-Aux0] loopback
```

13.4 以太网子接口配置命令

13.4.1 display vlan interface

【命令】

display vlan interface *interface-type interface-num*

【视图】

所有视图

【参数】

interface-type interface-num：参数用于指定接口。目前支持接口类型有以太网接口和千兆以太网接口，只支持子接口。

【描述】

display vlan interface 命令用来显示某个接口的 VLAN 配置信息，只支持子接口。

【举例】

显示以太网子接口 Ethernet 1/0/0.1 的 VLAN 配置信息。

```
<H3C> display vlan interface Ethernet 1/0/0.1
encapsulation dot1q vid 2
```

13.4.2 display vlan max-packet-process

【命令】

display vlan max-packet-process *vid*

【视图】

所有视图

【参数】

vid：VLAN ID，用来标识一个 VLAN。

【描述】

display vlan max-packet-process 命令用来显示某个 VLAN 上配置的每秒的最大处理报文数目。

相关配置可参考命令 **max-packet-process**。

【举例】

显示 VLAN 10 上配置的最大处理报文数目。

```
<H3C> display vlan max-packet-process 10
Max Packet Process Count for Vid 10 is 300000
```

13.4.3 display vlan statistics vid

【命令】

display vlan statistics vid *vid*

【视图】

所有视图

【参数】

vid：VLAN ID，用来标识一个 VLAN。

【描述】

display vlan statistics vid 命令用来显示某个 VLAN 上的报文统计信息，如接收的报文数目，发送的报文数目。

相关配置可参考命令 **reset vlan statistics interface**。

【举例】

显示 VLAN 10 上的报文统计信息。

```
<H3C> display vlan statistics vid 10
Packets received: 53
Packets transmitted: 14
```

13.4.4 interface { ethernet | gigabitethernet }

【命令】

interface ethernet *interface-number.subinterface-number*

undo interface ethernet *interface-number.subinterface-number*

interface gigabitethernet *number.sub-number*

undo interface gigabitethernet *number.sub-number*

【视图】

系统视图

【参数】

interface-number：接口编号。

subinterface-number：子接口编号，取值范围为 1～4096。

【描述】

interface { **ethernet** | **gigabitethernet** }命令用来创建以太网子接口，**undo interface** { **ethernet** | **gigabitethernet** }命令用来删除指定的以太网子接口。

系统最多支持创建 1024 个以太网子接口。

【举例】

在以太网接口 1/0/0 上创建一个子接口。

```
[H3C] interface ethernet 1/0/0.1
[H3C-Ethernet1/0/0.1]
```

13.4.5 max-packet-process

【命令】

max-packet-process *count vid*

undo max-packet-process *vid*

【视图】

系统视图

【参数】

count：最大处理报文数目。

vid：VLAN ID，用来标识一个 VLAN。

【描述】

max-packet-process 命令用来设置某个 VLAN 的每秒的最大处理报文数目，**undo max-packet-process** 命令用来将某个 VLAN 的每秒的最大处理报文数目恢复为缺省配置。

缺省情况下，系统没有最大处理报文数目的限制。

设置了某个 VLAN 的每秒的最大处理报文数目后，当接收到的属于这个 VLAN 的报文达到这个限制后，就会丢弃以后接收到的属于这个 VLAN 的报文。通过这个命令可以进行流量控制。

相关配置可参考命令 **display vlan max-packet-process**。

【举例】

设置 VLAN 10 的每秒的最大处理报文数目为 200000。

```
[H3C] max-packet-process 200000 10
```

13.4.6 reset vlan statistics vid

【命令】

reset vlan statistics vid *vid*

【视图】

用户视图

【参数】

vid：VLAN ID，用来标识一个 VLAN。

【描述】

reset vlan statistics vid 命令用来清除 VLAN 统计信息。

相关配置可参考命令 **display vlan statistics vid**。

【举例】

清除 VLAN ID 为 10 的统计信息。

```
<H3C> reset vlan statistics vid 10
```

13.4.7 vlan-type dot1q

【命令】

vlan-type dot1q vid *vid*

undo vlan-type dot1q vid

【视图】

接口视图

【参数】

vid：VLAN ID，用来标识一个 VLAN，取值范围为 1～4094。

【描述】

vlan-type dot1q 命令用来设置子接口上的封装类型和 VLAN ID，**undo vlan-type dot1q** 用来取消为接口设置的封装类型和 VLAN ID.

缺省情况下，系统子接口上无封装，也没有与子接口关联的 VLAN ID。

相关配置可参考命令 **display vlan interface**。

【举例】

设置以太网子接口 2/0/0.1 与 VLAN ID 60 相关联，以太网子接口 2/0/0.1 的封装格式为 dot1q。

```
[H3C-Ethernet2/0/0.1] vlan-type dot1q vid 60
```

13.5 Dialer 口配置命令

13.5.1 interface dialer

【命令】

interface dialer *number*

undo interface dialer *number*

【视图】

系统视图

【参数】

number：接口序号，取值范围为 0～1023。

【描述】

interface dialer 命令用来创建一个 Dialer 接口。**undo interface dialer** 命令用来删除一个 Dialer 接口。

缺省情况下，无 Dialer 接口。

【举例】

定义一个 Dialer 接口，并进入 Dialer 接口视图。

```
[H3C] interface dialer1
[H3C-Dialer1]
```

13.5.2 virtualbaudrate

【命令】

virtualbaudrate { *baudrate1* | **mbps** *baudrate2* }

undo virtualbaudrate

【视图】

Dialer 接口视图

【参数】

baudrate1：设置接口虚拟波特率，单位为 bps，取值范围为 1～2048000。

mbps *baudrate2*：设置接口虚拟波特率，单位为 mbps，取值范围为 1～1023。

【描述】

virtualbaudrate 命令用来配置接口的虚拟波特率，**undo virtualbaudrate** 命令用来取消虚拟波特率的配置。

接口的虚拟波特率可以向上层协议（如 OSPF 路由协议）准确的告知接口的波特率，并使上层协议准确地运行。

配置了 **virtualbaudrate** 命令后，需要使用命令 **shutdown** 关闭接口，然后再使用 **undo shutdown** 命令启用接口，这样该配置对于上层协议才能生效。

缺省情况下，未配置接口的虚拟波特率。

【举例】

不为 Dialer1 接口设置虚拟波特率，可看到 Dialer1 接口的波特率为 1000000000bps，并且 OSPF 计算得到的接口 cost 为 1。

```
<H3C> display interface Dialer 1
Dialer1 current state :UP
Line protocol current state :UP
Description : Dialer1 Interface
The Maximum Transmit Unit is 1492, Hold timer is 10(sec)
Internet Address is negotiated, 1.1.1.2/32
Link layer protocol is PPP
LCP initial
Physical is Dialer, baudrate: 1000000000 bps
Output queue : (Urgent queuing : Size/Length/Discards)  0/50/0
Output queue : (Protocol queuing : Size/Length/Discards) 0/500/0
Output queue : (FIFO queuing : Size/Length/Discards)  0/75/0
    Last 300 seconds input:  0 bytes/sec 0 packets/sec
    Last 300 seconds output:  6 bytes/sec 0 packets/sec
    10 packets input, 840 bytes, 0 drops
    283 packets output, 18312 bytes, 7 drops
Bound to Dialer1:0:
Dialer1:0 current state :UP ,
Line protocol current state :UP
Link layer protocol is PPP
LCP opened, IPCP opened
Packets statistics:
  Input packets:0,  0 bytes
  Output packets:10, 640 bytes
```

```
  FCS error packets:0
  Address error packets:0
  Control field control error packets:0

<H3C> display ospf interface

                OSPF Process 1 with Router ID 1.1.1.2
                            Interfaces

  Area: 0.0.0.0
      IP Address      Type  State    Cost Pri DR              BDR
      1.1.1.2         PtoP  PtoP     1    1   None            None
```

设置 Dialer1 接口的虚拟波特率为 64000bps，可看到 Dialer1 接口的虚拟波特率为 64000bps。

```
<H3C> display interface Dialer 1
Dialer1 current state :UP
Line protocol current state :UP
Description : Dialer1 Interface
Virtualbaudrate is 64000 bps
The Maximum Transmit Unit is 1492, Hold timer is 10(sec)
Internet Address is negotiated, 1.1.1.2/32
Link layer protocol is PPP
LCP initial
Physical is Dialer, baudrate: 1000000000 bps
Output queue : (Urgent queuing : Size/Length/Discards)  0/50/0
Output queue : (Protocol queuing : Size/Length/Discards) 0/500/0
Output queue : (FIFO queuing : Size/Length/Discards)  0/75/0
    Last 300 seconds input:  0 bytes/sec 0 packets/sec
    Last 300 seconds output:  6 bytes/sec 0 packets/sec
    10 packets input, 840 bytes, 0 drops
    342 packets output, 22088 bytes, 7 drops
Bound to Dialer1:0:
Dialer1:0 current state :UP ,
Line protocol current state :UP
Link layer protocol is PPP
LCP opened, IPCP opened
Packets statistics:
  Input packets:0,  0 bytes
  Output packets:69, 4416 bytes
  FCS error packets:0
  Address error packets:0
```

```
  Control field control error packets:0
```

对 Dialer1 接口执行 **shutdown** 和 **undo shutdown** 操作后，可以看到 OSPF 计算得到的接口 cost 为 1562。

```
[H3C] interface Dialer 1
[H3C-Dialer1] shutdown
[H3C-Dialer1] undo shutdown
[H3C-Dialer1] quit
[H3C] display ospf interface

                OSPF Process 1 with Router ID 1.1.1.2
                            Interfaces

  Area: 0.0.0.0
      IP Address      Type  State    Cost Pri DR              BDR
      1.1.1.2         PtoP  PtoP     1562 1   None            None
```

13.6 虚拟模板接口和虚拟访问接口配置命令

13.6.1 broadcast-limit link

【命令】

broadcast-limit link *number*

undo broadcast-limit link

【视图】

虚拟模板接口视图

【参数】

number：虚拟模板接口支持发送组播或广播报文的最大链路数，取值范围为 0～128。缺省值为 30。

【描述】

broadcast-limit link 命令用来设置虚拟模板接口支持发送组播或广播报文的最大链路数，**undo broadcast-limit link** 命令用来恢复缺省设置。

当虚拟模板接口下的链路数目比较多时，组播或广播报文从每条链路上发出会影响系统性能，可以使用 **broadcast-limit link** 命令进行限制，当链路数超过限定值时，就将组播或广播报文丢弃。

【举例】

设置虚拟模板接口 1 支持发送组播或广播报文的最大链路数为 100。

```
[H3C] interface virtual-template 1
[H3C-Virtual-Template1] broadcast-limit link 100
```

13.6.2 display interface virtual-template

【命令】

display interface virtual-template [*number*]

【视图】

所有视图

【参数】

number：虚拟模板接口的编号，取值范围为 0～1023。不指定编号将显示所有虚拟模板接口状态。

【描述】

display interface virtual-template 命令用来查看虚拟模板接口的状态。

【举例】

查看指定虚拟模板接口的状态。

```
<H3C> display interface virtual-template 1
Virtual-Template1 current state :DOWN
Line protocol current state :DOWN
Description : Virtual-Template1 Interface
The Maximum Transmit Unit is 1500
Internet protocol processing : disabled
Link layer protocol is PPP
LCP initial
Physical is None
Output queue : (Urgent queuing : Size/Length/Discards)  0/50/0
Output queue : (Protocol queuing : Size/Length/Discards) 0/500/0
Output queue : (FIFO queuing : Size/Length/Discards)  0/75/0
    Last 300 seconds input:  0 bytes/sec 0 packets/sec
    Last 300 seconds output:  0 bytes/sec 0 packets/sec
    0 packets input, 0 bytes, 0 drops
    0 packets output, 0 bytes, 0 drops
```

13.6.3 display virtual-access

【命令】

display virtual-access { **dialer** *number* | **vt** *vt-number* | **user** *user-name* | **peer** *peer-address* | *va-number* }*

【视图】

所有视图

【参数】

dialer *number*：Dialer 接口号。

vt-number：虚拟访问接口所属的虚拟模板接口号。

user-name：虚拟访问接口的登录用户名。

peer-address：虚拟访问接口的对端地址。

va-number：虚拟访问接口的顺序号。

【描述】

display virtual-access 命令用来查看虚拟访问接口的状态。

对于由 PPPoE Client 的 Dialer 接口所生成的虚拟访问接口，不能通过此命令来查看。

【举例】

查看所有虚拟访问接口的状态信息。

```
<H3C> display virtual-access
```

13.6.4 interface virtual-template

【命令】

interface virtual-template *number*

undo interface virtual-template *number*

【视图】

系统视图

【参数】

number：虚拟模板接口的编号，取值范围为 0～1023。

【描述】

interface virtual-template 命令用来创建虚拟模板接口，或进入已经存在的虚拟模板接口视图，**undo interface virtual-template** 命令用来删除指定的虚拟模板接口。

虚拟模板接口要保证在虚拟访问接口建立之前已经建立，在虚拟访问接口关闭且不再使用之后再关闭。

在删除时，要确保相关的虚拟访问接口都已经删除，而且该虚拟模板接口不再被使用。

【举例】

创建虚拟模板接口 10，并进入虚拟模板接口视图。

```
[H3C] interface virtual-template 10
[H3C-Virtual-Template10]
```

13.7 Loopback 接口和 Null 接口配置命令

13.7.1 display interface looback

【命令】

display interface loopback [*number*]

【视图】

所有视图

【参数】

number：Loopback 接口的编号，取值范围为现有的 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 接口的状态。

【描述】

display interface looback 命令用来查看 Loopback 接口的状态信息。

相关配置可参考命令 **interface loopback**。

【举例】

查看指定 Loopback 接口的状态。

```
<H3C> display interface loopback 0
LoopBack0 current state :UP
Line protocol current state :UP (spoofing)
Description :  LoopBack0 Interface
The Maximum Transmit Unit is 1536
Internet Address is 1.1.1.1/32
Physical is Loopback
    Last 300 seconds input:  0 bytes/sec 0 packets/sec
    Last 300 seconds output:  0 bytes/sec 0 packets/sec
    0 packets input, 0 bytes, 0 drops
```

```
    0 packets output, 0 bytes, 0 drops
```

13.7.2 display interface null

【命令】

display interface null [**0**]

【视图】

所有视图

【参数】

0：Null 接口的编号，取值固定为 0。

【描述】

display interface null 命令用来查看 Null 接口的状态信息。有无参数，效果是一样的。

相关配置可参考命令 **interface null**。

【举例】

查看指定 Null0 接口的状态。

```
<H3C> display interface null 0
NULL0 current state :UP
Line protocol current state :UP (spoofing)
Description :  NULL0 Interface
The Maximum Transmit Unit is 1500
Internet protocol processing : disabled
Physical is NULL DEV
    Last 300 seconds input:  0 bytes/sec 0 packets/sec
    Last 300 seconds output:  0 bytes/sec 0 packets/sec
    0 packets input, 0 bytes, 0 drops
    0 packets output, 0 bytes, 0 drops
```

13.7.3 interface loopback

【命令】

interface loopback *number*

undo interface loopback *number*

【视图】

系统视图

【参数】

number：Loopback 接口的编号，取值范围为 0～1023。

【描述】

interface loopback 命令用来创建 Loopback 接口，或进入 Loopback 接口视图。**undo interface loopback** 命令用来删除指定 Loopback 接口。

Loopback 接口创建后一直保持 Up 状态，并具有环回的特性，因此，常被用于提高配置的可靠性。

Loopback 接口也可以被 shutdown。由于该接口是 spoofing 接口，当接口被 shutdown 之后，链路层协议显示为 Line protocol current state :UP (spoofing)。

相关配置可参考命令 **display interface loopback**。

【举例】

创建 Loopback 接口 5，并进入 Loopback 接口视图。

```
[H3C] interface loopback 5
[H3C-LoopBack5]
```

13.7.4 interface null

【命令】

interface null 0

【视图】

系统视图

【参数】

无

【描述】

interface null 命令用来进入 Null 接口的视图。

Null 接口只有一个，固定为 null0，该接口始终处于 Up 状态，不能被 down 或删除。

相关配置可参考命令 **display interface null**。

【举例】

进入 Null0 接口的视图。

```
[H3C] interface null 0
[H3C -NULL0]
```

目 录

第 1 章 PPP配置命令 1-1
1.1 PPP配置命令 1-1
1.1.1 debugging ppp { all | cbcp | ccp | scp } 1-1
1.1.2 debugging ppp { chap | compression | pap | vjcomp packet } 1-2
1.1.3 debugging ppp { core | ip | ipcp | lcp | lqc | mp } 1-3
1.1.4 link-protocol ppp 1-4
1.1.5 ppp authentication-mode 1-4
1.1.6 ppp chap password 1-5
1.1.7 ppp chap user 1-6
1.1.8 ppp ipcp dns 1-6
1.1.9 ppp ipcp dns admit-any 1-7
1.1.10 ppp ipcp remote-address forced 1-8
1.1.11 ppp ipcp dns request 1-9
1.1.12 ppp lqc 1-10
1.1.13 ppp pap local-user 1-11
1.1.14 ppp timer negotiate 1-11
1.1.15 timer hold 1-12
1.2 PPP链路效率机制配置命令 1-13
1.2.1 debugging ppp compression iphc rtp 1-13
1.2.2 debugging ppp compression iphc tcp 1-13
1.2.3 display ppp compression iphc rtp 1-14
1.2.4 display ppp compression iphc tcp 1-14
1.2.5 display ppp compression stac-lzs 1-15
1.2.6 ip tcp vjcompress 1-16
1.2.7 ppp compression iphc 1-16
1.2.8 ppp compression iphc rtp-connections 1-17
1.2.9 ppp compression iphc tcp-connections 1-18
1.2.10 ppp compression stac-lzs 1-18
1.2.11 reset ppp compression iphc 1-19
1.2.12 reset ppp compression stac-lzs 1-19
第 2 章 PPPoE Server配置命令 2-1
2.1 PPPoE Server配置命令 2-1
2.1.1 display pppoe-server session 2-1
2.1.2 pppoe-server bind virtual-template 2-2
2.1.3 pppoe-server log-information off 2-3
2.1.4 pppoe-server max-sessions local-mac 2-3
2.1.5 pppoe-server max-sessions remote-mac 2-4
2.1.6 pppoe-server max-sessions total 2-4
2.1.7 reset pppoe-server 2-5

第 3 章 PPPoE Client配置命令 3-1
3.1 PPPoE Client配置命令 3-1
3.1.1 debugging pppoe-client 3-1
3.1.2 dialer enable-circular 3-1
3.1.3 dialer bundle 3-2
3.1.4 dialer-group 3-2
3.1.5 dialer-rule 3-3
3.1.6 dialer user 3-4
3.1.7 display pppoe-client session 3-5
3.1.8 interface dialer 3-7
3.1.9 pppoe-client 3-7
3.1.10 reset pppoe-client 3-9
第 4 章 VLAN配置命令 4-1
4.1 VLAN配置命令 4-1
4.1.1 display vlan interface 4-1
4.1.2 display vlan max-packet-process 4-1
4.1.3 display vlan statistics vid 4-2
4.1.4 max-packet-process 4-2
4.1.5 reset vlan statistics vid 4-3
4.1.6 vlan-type dot1q 4-3

第1章 PPP 配置命令

1.1 PPP 配置命令

1.1.1 debugging ppp { all | cbcp | ccp | scp }

【命令】

debugging ppp { **all** | **cbcp packet** | **ccp** { **all** | **event** | **error** | **packet** | **state** } | **scp packet** } [**interface** *interface-type interface-number*]

undo debugging ppp { **all** | **cbcp packet** | **ccp** { **all** | **event** | **error** | **packet** | **state** } | **scp packet** } [**interface** *interface-type interface-number*]

【视图】

用户视图

【参数】

cbcp packet：打开 cbcp 报文的调试开关。

scp packet：打开 scp 报文的调试开关。

ccp：打开关于 ccp 的调试开关。

all：打开所有的调试开关。

event：打开事件信息的调试开关。

error：打开错误信息的调试开关。

packet：打开报文信息的调试开关。

state：打开状态信息的调试开关。

interface *interface-type interface-number*：接口类型及接口编号。

【描述】

debugging ppp { **all** | **cbcp** | **ccp** | **scp** }命令用来打开 ppp 相关的 cbcp、ccp、scp 或所有的调试开关。**undo debugging ppp** { **all** | **cbcp** | **ccp** | **scp** }命令用来恢复 ppp 相关的 cbcp、ccp、scp 或所有的调试开关的缺省设置。

缺省情况下，ppp 的所有调试开关都是关闭的。

【举例】

无

1.1.2 debugging ppp { chap | compression | pap | vjcomp packet }

【命令】

debugging ppp { **chap** { **all** | **event** | **error** | **packet** | **state** } | **compression iphc** { **rtp** | **tcp** } | **pap** { **all** | **event** | **error** | **packet** | **state** } | **vjcomp packet** } [**interface** *interface-type interface-number*]

undo debugging ppp { **chap** { **all** | **event** | **error** | **packet** | **state** }| **compression iphc** { **rtp** | **tcp** } | **pap** { **all** | **event** | **error** | **packet** | **state** } | **vjcomp packet** } [**interface** *interface-type interface-number*]

【视图】

用户视图

【参数】

chap：打开 PPP 的 CHAP 认证调试开关。

compression iphc rtp：打开 IP 报文头压缩中 IP/UDP/RTP 头压缩的调试开关。

compression iphc tcp：打开 IP 报文头压缩中 IP/TCP 头压缩的调试开关。

pap：打开 PPP 的 PAP 认证调试开关。

vjcomp packet：打开 PPP 的 vjcomp 报文调试开关。

all：打开所有的调试开关。

event：打开事件信息的调试开关。

error：打开错误信息的调试开关。

packet：打开报文信息的调试开关。

state：打开状态信息的调试开关。

interface *interface-type interface-number*：接口类型及接口编号。

【描述】

debugging ppp { **chap**| **compression** | **pap** | **vjcomp packet** }命令用来打开 PPP 相关的 CHAP、compression、PAP 或 vjcomp 的调试开关。**undo debugging ppp** { **chap**| **compression** | **pap** | **vjcomp packet** }命令用来恢复 PPP 相关的 CHAP、compression、PAP 或 vjcomp 的调试开关的缺省设置。

缺省情况下，PPP 的所有调试开关都是关闭的。

【举例】

无

1.1.3 debugging ppp { core | ip | ipcp | lcp | lqc | mp }

【命令】

debugging ppp { **core event** | **ip packet** | **ipcp** { **all** | **event** | **error** | **packet** | **state** } | **lcp** { **all** | **event** | **error** | **packet** | **state** } | **lqc packet** | **mp** { **all** | **event** | **error** | **packet** } } [**interface** *interface-type interface-number*]

undo debugging ppp { **core event** | **ip packet**| **ipcp** { **all** | **event** | **error** | **packet** | **state** } | **lcp** { **all** | **event** | **error** | **packet** | **state** } | **lqc packet** | **mp** { **all** | **event** | **error** | **packet** } } [**interface** *interface-type interface-number*]

【视图】

用户视图

【参数】

core event：打开 PPP 核心状态事件信息的调试开关。

ip packet：打开 PPP 的 ip 报文的调试开关。

ipcp：打开 PPP 的 IP 控制协议的调试开关。

lcp：打开 PPP 的网络控制协议的调试开关。

lqc packet：打开 PPP 链路质量控制协议的调试开关。

mp：打开 PPP 多链路协议的调试开关。

all：打开所有的调试开关。

event：打开事件信息的调试开关。

error：打开错误信息的调试开关。

packet：打开报文信息的调试开关。

state：打开状态信息的调试开关。

interface *interface-type interface-number*：接口类型及接口编号。

【描述】

debugging ppp { **core** | **ip** | **ipcp** | **lcp** | **lqc** | **mp** }命令用来打开 PPP 相关的 core、ip、ipcp、lcp、lqc 或 mp 的调试开关。**undo debugging ppp** { **core** | **ip** | **ipcp** | **lcp** | **lqc** | **mp** }命令用来恢复 PPP 相关的 core、ip、ipcp、lcp、lqc 或 mp 的调试开关的缺省设置。

缺省情况下，PPP 的所有调试开关都是关闭的。

【举例】

无

1.1.4 link-protocol ppp

【命令】

link-protocol ppp

【视图】

接口视图

【参数】

无

【描述】

link-protocol ppp 命令用来配置接口封装的链路层协议为 PPP。

缺省情况下，除以太网接口外，其它接口链路层协议均封装为 PPP。

PPP 协议是在点到点链路上承载网络层数据包的一种链路层协议。PPP 定义了一整套的协议，包括链路控制协议（LCP）、网络层控制协议（NCP）和验证协议（PAP 和 CHAP）等等。PPP 由于能够提供用户验证、易于扩充和支持同/异步而获得了较广泛的应用。

相关配置可参考命令 **display interface**。

【举例】

设置接口 Dialer1 封装的链路层协议为 PPP。

```
[H3C-Dialer1] link-protocol ppp
```

1.1.5 ppp authentication-mode

【命令】

ppp authentication-mode { **chap** | **pap** } [[**call-in**] **domain** *isp-name*]

undo ppp authentication-mode

【视图】

接口视图

【参数】

chap 和 **pap** 二者必选其一，也只能选一种。

call-in：表示只在远端用户呼入时才验证对方。

domain：表示用户认证采用的域名。

【描述】

ppp authentication-mode 命令用来设置本端 PPP 协议对对端的验证方式，**undo ppp authentication-mode** 命令用来取消配置的验证方式，即不进行验证。

当配置 **ppp authentication-mode** { **pap** | **chap** } 后不加 **domain** 时，默认使用的 domain 是系统缺省的域 system，认证方式是本地验证，地址分配使用的是 system 域中的地址池（通过 **display domain** 命令可以查看该域的配置）。如果在该命令加了 **domain**，则必须在对应的 **domain** 中配置地址池。

如果用户名中带有 domain，则以用户名中的 domain 为准（若该 domain 名不存在，则认证被拒绝），否则应使用为 PPP 认证配置的 domain 名。

缺省情况下，不验证。

PPP 有两种验证方式：

- PAP 为两次握手验证，口令为明文。
- CHAP 为三次握手验证，口令为密文。

另外可以采用已经定义的 AAA 验证方法表进行验证。

无论是 CHAP 或 PAP，只是一种验证过程，最终能否通过验证，还需要 AAA 来作决定，AAA 可以利用本地验证数据库验证或由 AAA 服务器进行验证。

相关配置可参考命令 **local-user**，**ppp chap user**，**ppp pap local-user**，**ppp pap password**，**ppp chap password**。

【举例】

在接口 Virtual-Template1 上，采用 PAP 方法验证对端。

```
[H3C-Virtual-Template1] ppp authentication-mode pap
```

1.1.6 ppp chap password

【命令】

ppp chap password { **simple** | **cipher** } *password*

undo ppp chap password

【视图】

接口视图

【参数】

password：为发送的口令。

simple 和 **cipher**：表示不加密显示和加密显示口令。

【描述】

ppp chap password 命令用来配置进行 CHAP 验证时采用的缺省 CHAP 口令，**undo ppp chap password** 命令用来取消配置的口令。

配置 CHAP 验证时，要将本端的 *password* 配置为对端相应 *user* 的 *password*。

相关配置可参考命令 **ppp authentication-mode chap**，**local-user**。

【举例】

设置本地防火墙以 CHAP 方式被验证时，用户口令为 mypwd 且为明文显示。

```
[H3C-Virtual-Template1] ppp chap password simple mypwd
```

1.1.7 ppp chap user

【命令】

ppp chap user *username*

undo ppp chap user

【视图】

接口视图

【参数】

username：CHAP 验证用户名，为长度为 1～80 的字符串，该名称是发送到对端设备进行 CHAP 验证的用户名。

【描述】

ppp chap user 命令用来配置采用 CHAP 认证时的用户名称，**undo ppp chap user** 命令用来删除已有的配置。

配置 CHAP 验证时，要将各自的 *username* 配置为对端的 *local-user*，而且对应的 *password* 要一致。

相关配置可参考命令 **ppp authentication-mode**，**local-user**。

【举例】

配置接口 Dialer1 进行 CHAP 验证时，本地用户名为 Root。

```
[H3C-Dialer1] ppp chap user Root
```

1.1.8 ppp ipcp dns

【命令】

ppp ipcp dns *primary-dns-address* [*secondary-dns-address*]

undo ppp ipcp dns *primary-dns-address* [*secondary-dns-address*]

【视图】

接口视图

【参数】

primary-dns-address：主 DNS 服务器地址。

secondary-dns-address：从 DNS 服务器地址。

【描述】

ppp ipcp dns 命令用来使能防火墙为对端分配 DNS 服务器地址，**undo ppp ipcp dns** 命令用来禁止防火墙为对端分配 DNS 服务器地址。

缺省情况下，防火墙不为对端分配 DNS 服务器地址。

当其他设备与防火墙通过 PPP 协议相连时，通过协商，防火墙可以为对端设备分配 DNS 服务器地址（但需要等待对端请求，不会主动给对端分配 DNS 服务器地址）。这样，对端设备就可以通过域名直接访问网络。

如果用户通过PC机连接防火墙，用户可以在PC机上使用命令**winipcfg**或**ipconfig /all** 来查看防火墙为其提供的 DNS 服务器地址。

防火墙可以为对端设备提供主 DNS 服务器和从 DNS 服务器两个服务器地址。

相关配置可参考命令 **ppp authentication-mode pap**，**ppp ipcp dns admit-any**。

【举例】

设置防火墙为对端分配的主 DNS 服务器地址为 100.1.1.1，从 DNS 服务器地址为 100.1.1.2。

```
[H3C-Dialer1] ppp ipcp dns 100.1.1.1 100.1.1.2
```

1.1.9 ppp ipcp dns admit-any

【命令】

ppp ipcp dns admit-any

undo ppp ipcp dns admit-any

【视图】

接口视图

【参数】

无

【描述】

ppp ipcp dns admit-any 命令用来配置防火墙可以被动地接收对端分配的 DNS 地址，即防火墙不发送 DNS 请求，也能接收对端分配的 DNS 地址。**undo ppp ipcp dns admit-any** 命令用来禁止防火墙被动地接收对端分配的 DNS 地址。

缺省情况下，防火墙不会被动地接收对端分配的 DNS 地址。

当防火墙通过 PPP 协议与其他设备相连时（通常为防火墙拨号连接运营商的接入服务器），通过协商，防火墙可以被动地接收对端分配的 DNS 地址，这样防火墙就可以使用对端设备分配的 DNS 服务器来解析域名。

相关配置可参考命令 **ppp authentication-mode pap**，**ppp ipcp dns**。

【举例】

设置防火墙可以被动地接收对端分配的 DNS 地址。

```
[H3C-Dialer1] ppp ipcp dns admit-any
```

1.1.10 ppp ipcp remote-address forced

【命令】

ppp ipcp remote-address forced

undo ppp ipcp remote-address forced

【视图】

接口视图

【参数】

无

【描述】

ppp ipcp remote-address forced 命令用来使防火墙为对端分配 IP 地址时具有强制性，不允许对端使用自行配置的固定 IP 地址；**undo ppp ipcp remote-address forced** 命令用来取消这种强制性，允许对端使用自行配置的固定 IP 地址。

缺省情况下，PPP IPCP 的 IP 地址协商情况为本端不具有地址分配的强制，即防火墙允许对端自行配置地址。当对端明确请求本端分配地址时，本端给对端分配地址；若对端已自行配置 IP 地址时，本端不再强行给对端分配地址。在不允许对端自行指定 IP 地址的情况下，防火墙接口下一定要配置 **ppp ipcp remote-address forced** 命令。

相关配置可参考命令 **remote address**。

【举例】

封装 PPP 的拨号接口 Dialer1 为对端分配的 IP 地址为 10.0.0.1，此时，对端可以接收这个分配的地址，也可以自行配置 IP 地址或无地址。

```
[H3C-Dialer1] remote address 10.0.0.1
```

封装 PPP 的拨号接口 Dialer1 为对端分配的 IP 地址为 10.0.0.1，此时，对端必须接收这个地址，不允许对端自行配置 IP 地址或无地址。

```
[H3C-Dialer1] remote address 10.0.0.1
[H3C-Dialer1] ppp ipcp remote-address forced
```

1.1.11 ppp ipcp dns request

【命令】

ppp ipcp dns request

undo ppp ipcp dns request

【视图】

接口视图

【参数】

无

【描述】

ppp ipcp dns request 命令用来配置防火墙主动向对端请求 DNS 地址。**undo ppp ipcp dns request** 命令用来禁止防火墙主动向对端请求 DNS 地址。

缺省情况下，禁止防火墙主动向对端请求对端的 DNS 地址。

当防火墙通过 PPP 协议与其他设备相连时（通常为防火墙拨号连接运营商的接入服务器），通过协商，防火墙可以主动向对端请求 DNS 地址，这样防火墙就可以使用对端设备分配的 DNS 服务器来解析域名。

📖 **说明：**

如果协商到有效的 DNS 地址，将在接口显示信息中打印出来。

相关配置可参考命令 **ppp authentication-mode pap**，**ppp ipcp dns**。

【举例】

配置 Dialer0 接口主动请求 DNS 地址。

```
[H3C-Dialer0] ppp ipcp dns request
```

1.1.12 ppp lqc

【命令】

ppp lqc *forbidden-percentage* [*resumptive-percentage*]

undo ppp lqc

【视图】

接口视图

【参数】

forbidden-percentage：禁用链路质量百分比，取值范围为 0～100。

resumptive-percentage：恢复链路质量百分比，取值范围为 0～100。

【描述】

ppp lqc 命令用来使能 PPP 链路质量监测功能，**undo ppp lqc** 命令用来禁用 PPP 链路质量监测功能。

缺省情况下，不启用 PPP 链路质量监测功能。

参数 *resumptive-percentage* 的缺省值等于 *forbidden-percentage* 之值。

PPP 链路质量监测可以实时对 PPP 链路（包括绑定在 MP 中的 PPP 链路）的质量进行监测。当链路的质量低于禁用链路质量百分比时，链路会被禁用；当链路质量恢复到恢复链路质量百分比时，链路会被自动重新启用。为了保证链路不会在禁用和恢复之间反复振荡，PPP 链路质量监测在重新启用链路时会有一定的时间延迟。

配置时参数 *resumptive-percentage* 的值必须大于等于参数 *forbidden-percentage* 的值。

当在 PPP 链路两端同时启用链路质量监测时，两端设备的参数必须相等。一般来说，不建议在链路两端同时使用链路质量监测功能。

不建议在拨号线路上使用 PPP 链路质量监测。当在拨号线路上启用链路质量监测功能后，由于拨号线路的特点，一旦链路被禁用 DCC 模块就会把拨号线路挂断，因此链路质量监测就不能正常的运行。只有当有数据需要传输时，DCC 模块把拨号线路重新呼起，链路质量监测才能恢复正常。

相关配置可参考命令 **timer hold**。

【举例】

在接口 Dialer1 上启用 PPP 链路质量监测功能，禁用链路质量百分比为 90%，恢复链路质量百分比为 95%。

```
[H3C-Dialer1] ppp lqc 90 95
```

1.1.13 ppp pap local-user

【命令】

ppp pap local-user *username* **password** { **simple** | **cipher** } *password*

undo ppp pap local-user

【视图】

接口视图

【参数】

username：为发送的用户名，为长度为 1～80 的字符串；

password：为发送的口令；

simple：表示不加密显示口令；

cipher：表示加密显示口令。

【描述】

ppp pap local-user 命令用来配置本地防火墙被对端采用 PAP 方式验证时发送的用户名和口令，**undo ppp pap local-user** 命令用来取消配置的发送的用户名和口令。

缺省情况下，被对端以 PAP 方式验证时，本地防火墙发送的用户名和口令均为空。

当本地防火墙被对端以 PAP 方式验证时，本地防火墙发送的用户名 *username* 和口令 *password* 应与对端设备的 *user* 和 *password* 一致。

相关配置可参考命令 **ppp authentication-mode pap**，**local-user**。

【举例】

设置本地防火墙被对端以 PAP 方式验证时发送的用户名为 myuser，口令为 mypwd。

```
[H3C-Dialer1] ppp pap local-user myuser password simple mypwd
```

1.1.14 ppp timer negotiate

【命令】

ppp timer negotiate *seconds*

undo ppp timer negotiate

【视图】

接口视图

【参数】

seconds：为协商超时时间，单位为秒。在 PPP 协商过程中，如果在这个时间间隔内没有收到对端的应答报文，则 PPP 将会重发前一次发送的报文。该时间取值范围为 1 秒到 10 秒。

【描述】

ppp timer negotiate 命令用来设置 PPP 协商超时时间，**undo ppp timer negotiate** 命令用来恢复 PPP 协商超时时间的缺省值。

缺省情况下，PPP 协商超时时间为 3 秒。

相关配置可参考命令 **link-protocol ppp**。

【举例】

设置 PPP 协商超时时间为 5 秒。

```
[H3C-Dialer1] ppp timer negotiate 5
```

1.1.15 timer hold

【命令】

timer hold *seconds*

undo timer hold

【视图】

接口视图

【参数】

seconds：接口发送 keepalive 报文的时间周期，单位为秒，取值范围为 0～32767，缺省值为 10 秒。

【描述】

timer hold 命令用来设置接口发送 keepalive 报文的周期，**undo timer hold** 命令用来恢复发送 keepalive 报文的时间周期的缺省值。

相关配置可参考命令 **display interface**。

【举例】

设置接口 Ethernet0/0/0 的 keepalive 报文发送周期为 20 秒。

```
[H3C-Ethernet0/0/0] timer hold 20
```

1.2 PPP 链路效率机制配置命令

1.2.1 debugging ppp compression iphc rtp

【命令】

debugging ppp compression iphc rtp { **all** | **context_state** | **error** | **full_header** | **general_info** }

undo debugging ppp compression iphc rtp { **all** | **context_state** | **error** | **full_header** | **general_info** }

【视图】

用户视图

【参数】

all：表示打开 IPHC RTP 的所有调试开关。

context_state：表示打开 IPHC RTP context_state 报文调试开关。

error：表示打开 IPHC RTP 错误信息调试开关。

full_header：表示打开 IPHC RTP full_header 报文调试开关。

general_info：表示打开 IPHC RTP 总体信息调试开关。

【描述】

debugging ppp compression iphc rtp 命令用来显示 IP 报文头压缩中 IP/UDP/RTP 头压缩的调试信息。**undo debugging ppp compression iphc rtp** 命令用来关闭 IP 报文头压缩中 IP/UDP/RTP 头压缩的调试开关。

【举例】

打开 IP 报文头压缩中 IP/UDP/RTP 头压缩的错误调试开关。

```
<H3C> debugging ppp compression iphc rtp error
```

1.2.2 debugging ppp compression iphc tcp

【命令】

debugging ppp compression iphc tcp { **all** | **context_state** | **error** | **full_header** | **general_info** }

undo debugging ppp compression iphc tcp { **all** | **context_state** | **error** | **full_header** | **general_info** }

【视图】

用户视图

【参数】

all：表示打开 IPHC TCP 的所有调试开关。

context_state：表示打开 IPHC TCP context_state 报文调试开关。

error：表示打开 IPHC TCP 错误信息调试开关。

full_header：表示打开 IPHC TCP full_header 报文调试开关。

general_info：表示打开 IPHC TCP 总体信息调试开关。

【描述】

debugging ppp compression iphc tcp 命令用于显示 IP 报文头压缩中 IP/TCP 头压缩的调试信息。**undo debugging ppp compression iphc tcp** 用来关闭 IP 报文头压缩中 IP/TCP 头压缩的调试开关。

【举例】

打开 IP 报文头压缩中 IP/TCP 头压缩的错误信息调试开关。

```
<H3C> debugging ppp compression iphc tcp error
```

1.2.3 display ppp compression iphc rtp

【命令】

display ppp compression iphc rtp [*interface-type interface-number*]

【视图】

所有视图

【参数】

interface-type：接口类型。

interface-number：接口编号。

【描述】

display ppp compression iphc rtp 命令用来显示 RTP 头压缩的统计信息。

【举例】

显示 RTP 头压缩的统计信息。

```
[H3C] display ppp compression iphc rtp
```

1.2.4 display ppp compression iphc tcp

【命令】

display ppp compression iphc tcp [*interface-type interface-number*]

【视图】

所有视图

【参数】

interface-type：接口类型。

interface-number：接口编号。

【描述】

display ppp compression iphc tcp 命令用来显示 TCP 头压缩的统计信息。

【举例】

显示 TCP 头压缩的统计信息。

```
[H3C] display ppp compression iphc tcp
```

1.2.5 display ppp compression stac-lzs

【命令】

display ppp compression stac-lzs [*interface-type interface-number*]

【视图】

所有视图

【参数】

interface-type：接口类型。

interface-number：接口编号。

【描述】

display ppp compression stac-lzs 命令用来显示 **stac-lzs** 压缩的统计信息。

【举例】

显示 **stac-lzs** 压缩的统计信息。

```
[H3C] display ppp compression stac-lzs
Staz-lzs compression
  Interface: Dialer1
    Received:
      Compress/Error/Discard/Total: 302/0/0/302 (Packets)
    Sent:
      Compress/Error/Total: 302/0/302 (Packets)
```

1.2.6 ip tcp vjcompress

【命令】

ip tcp vjcompress

undo ip tcp vjcompress

【视图】

接口视图

【参数】

无

【描述】

ip tcp vjcompress 命令用来允许 PPP 接口进行 VJ TCP 头压缩，**undo ip tcp vjcompress** 命令用来禁止 PPP 接口进行 VJ TCP 头压缩。

如果允许 PPP 接口进行 VJ TCP 头压缩，线路对端的接口也应同时允许 VJ TCP 头压缩。该命令只用在集中式环境下。

缺省情况下，PPP 接口禁止使用 VJ TCP 头压缩。

【举例】

在 PPP 接口上允许 VJ TCP 头压缩。

```
[H3C-Dialer0] ip tcp vjcompress
```

1.2.7 ppp compression iphc

【命令】

ppp compression iphc [**nonstandard**]

undo ppp compression iphc

【视图】

接口视图

【参数】

nonstandard：非标准兼容的封装格式。

【描述】

ppp compression iphc 命令用来启动某接口上的 IP 头压缩，这里主要指 TCP 头压缩与 RTP 头压缩，**undo ppp compression iphc** 命令用来关闭 TCP 头压缩与 RTP 头压缩功能。

缺省情况下，不启动接口上的 TCP 头压缩与 RTP 头压缩功能。

用户必须在链路的两端同时配置压缩命令才能生效。

在配置完成后，只有对接口进行 **shutdown** 与 **undo shutdown** 操作后，配置才能生效。如果是应用在 MP 上，要对所有 MP 捆绑的接口执行 **shutdown** 与 **undo shutdown** 操作。

相关配置可参考命令 **ppp compression iphc rtp-connection**，**ppp compression iphc tcp-connections**。

【举例】

启动拨号接口 Dialer1 上的 IP 头压缩。

```
[H3C-Dialer1] ppp compression iphc
```

1.2.8 ppp compression iphc rtp-connections

【命令】

ppp compression iphc rtp-connections *number*

undo ppp compression iphc rtp-connections

【视图】

接口视图

【参数】

number：指该接口上 IPHC 功能的 RTP 头压缩的最大连接数，取值范围 3～1000，缺省值为 16。

【描述】

ppp compression iphc rtp-connections 命令用来指定某一个接口上允许存在 RTP 头压缩连接的总数，**undo ppp compression iphc rtp-connections** 命令可以取消配置，恢复缺省值。

RTP 是面向连接的协议，一条链路上所能承载的 RTP 连接的数目是比较多的，但压缩算法压缩时需对每个连接维护一定的信息，从而占用一定的内存，因此可以用 **ppp compression iphc rtp-connections** 命令来配置 RTP 压缩的最大连接数。例如连接数限定为 3 时，第 4 条 RTP 连接上的报文就不会被压缩了。

配置将在对接口进行 **shutdown** 与 **undo shutdown** 操作后生效。如果是对 MP 进行配置，则 **shutdown** 与 **undo shutdown** 操作必须在所有 MP 上实施。

【举例】

配置接口 Dialer1 上 RTP 头压缩连接的总数为 10。

```
[H3C-Dialer1] ppp compression iphc rtp-connections 10
```

1.2.9 ppp compression iphc tcp-connections

【命令】

ppp compression iphc tcp-connections *number*

undo ppp compression iphc tcp-connections

【视图】

接口视图

【参数】

number：该接口上 IPHC 功能的 TCP 头压缩的最大连接数，取值范围 3～256，缺省值为 16。

【描述】

ppp compression iphc tcp-connections 命令用来配置 TCP 头压缩的最大连接数，**undo ppp compression iphc tcp-connections** 命令用来恢复 TCP 头压缩的最大连接数的缺省值。

TCP 是面向连接的协议，一条链路上所能承载的 TCP 连接的数目是比较多的，但压缩算法压缩时需对每个连接维护一定的信息，从而占用一定的内存，因此可以用 **ppp compression iphc tcp-connections** 命令来配置 TCP 压缩的最大连接数。例如连接数限定为 3 时，第 4 条 TCP 连接上的报文就不会被压缩了。

【举例】

配置接口 Dialer1 上 TCP 头压缩连接的总数为 10。

```
[H3C-Dialer1] ppp compression iphc-connections 10
```

1.2.10 ppp compression stac-lzs

【命令】

ppp compression stac-lzs

undo ppp compression stac-lzs

【视图】

接口视图

【参数】

无

【描述】

ppp compression stac-lzs 命令用来设置 PPP 协议启用 Stac 压缩算法，**undo ppp compression stac-lzs** 命令用来禁止在相应接口使用 Stac 压缩算法。

缺省情况下，禁止使用 Stac 压缩算法。

在接口配置 **stac-lzs** 压缩，能通过无损的数据压缩减小数据帧的尺寸，但是使用这项配置将增加防火墙的负担，所以推荐您在防火墙负担过重的时候，禁止该功能。同时只有当链路两端都配置了 **stac-lzs** 选项的时候，该 PPP 链路才支持 **stac-lzs** 压缩。

相关配置可参考命令 **link-protocol ppp**。

【举例】

设置防火墙支持 **stac-lzs** 压缩。

```
[H3C-Dialer1] ppp compression stac-lzs
```

1.2.11 reset ppp compression iphc

【命令】

reset ppp compression iphc [*interface-type interface-number*]

【视图】

用户视图

【参数】

interface-type：接口类型。

interface-number：接口编号。

【描述】

reset ppp compression iphc 命令用来删除那些已经无效的 IP/UDP/RTP IP 头压缩或解压上下文存储表，并清除 IP/UDP/RTP 头压缩的统计信息。

如果不指定参数，将清空所有接口的 RTP 头压缩存储表项。

【举例】

清除 IP/UDP/RTP 头压缩的统计信息。

```
<H3C> reset ppp compression iphc
```

1.2.12 reset ppp compression stac-lzs

【命令】

reset ppp compression stac-lzs [*interface-type interface-number*]

【视图】

用户视图

【参数】

interface-type：接口类型。

interface-number：接口编号。

【描述】

reset ppp compression stac-lzs 命令用来清除 Stac-lzs 压缩的统计信息。

如果不指定参数，将清空所有接口的 Stac-lzs 压缩统计信息。

【举例】

清除 Stac-lzs 压缩的统计信息。

```
<H3C> reset ppp compression stac-lzs
```

第2章 PPPoE Server 配置命令

2.1 PPPoE Server 配置命令

2.1.1 display pppoe-server session

【命令】

display pppoe-server session { **all** | **packet** }

【视图】

所有视图

【参数】

all：显示各 PPPoE session 的所有信息。

packet：显示各 PPPoE session 的报文统计信息。

【描述】

display pppoe-server session 命令用来显示 PPPoE session 的状态和统计数据。

相关配置可参考命令 **link-protocol ppp**，**pppoe-server bind**。

【举例】

查看所有 PPPoE 的会话信息。

```
<H3C> display pppoe-server session all
There is 1 session in total:
SID   Intf           State  OIntf          RemMAC          LocMAC
2  Virtual-Template1:0  UP  Ethernet0/0/0   0050.ba22.7369  00e0.fc08.f4de
```

表2-1 display pppoe-server session all 命令输出信息描述

项目	描述
SID	Session Identifier
Intf	对应的虚拟模板接口
State	会话的状态
OIntf	对应的以太网口
RemMAC	Remote MAC，对端 MAC 地址
LocMAC	Local MAC，本端 MAC 地址

查看 PPPoE 会话统计信息。

```
<H3C> display pppoe-server session packet
SID    RemMAC      LocMAC          InP       InO    InD      OutP      OutO   OutD
1   0050ba1a02ce 0001af02a40f   42       2980   0        16        343     0
```

表2-2 display pppoe-server session packet 命令输出信息描述

项目	描述
InP	In Packets，接收报文数
InO	In Octets，接收字节数
InD	In Discards，入方向丢弃的报文数
OutP	Out Packets，发送报文数
OutO	Out Octets，发送字节数
OutD	Out Discard，出方向丢弃的报文数

2.1.2 pppoe-server bind virtual-template

【命令】

pppoe-server bind virtual-template *number*

undo pppoe-server bind

【视图】

接口视图

【参数】

number：接入 PPPoE 的 virtual-template 数值，取值范围 0～1023。

【描述】

pppoe-server bind virtual-template 命令用来在以太网接口指定的虚拟模板上使能 PPPoE，**undo pppoe-server bind virtual-template** 命令用来在相应接口禁止 PPPoE 协议。

缺省情况下，禁止 PPPoE 协议。

相关配置可参考命令 **link-protocol ppp**。

【举例】

在以太网口 E0/0/0 的虚拟模板 1 上使能 PPPoE。

```
[H3C-Ethernet0/0/0] pppoe-server bind virtual-template 1
```

2.1.3 pppoe-server log-information off

【命令】

pppoe-server log-information off

undo pppoe-server log-information off

【视图】

系统视图

【参数】

无

【描述】

pppoe-server log-information off 命令用来关闭 PPPoE Server 产生的 PPP 日志信息的显示开关。**undo pppoe-server log-information off** 命令用来打开 PPPoE Server 产生的 PPP 日志信息的显示开关。

缺省情况下，系统显示 PPPoE Server 产生的 PPP 日志信息。

【举例】

关闭 PPPoE Server 产生的 PPP 日志信息的显示开关。

```
[H3C] pppoe-server log-information off
```

2.1.4 pppoe-server max-sessions local-mac

【命令】

pppoe-server max-sessions local-mac *number*

undo pppoe-server max-sessions local-mac

【视图】

系统视图

【参数】

number：一个本端 MAC 地址上能创建的最大 session 数目。

【描述】

pppoe-server max-sessions local-mac 命令用来配置一个本端 MAC 地址上能创建的最大 PPPoE session 数目，**undo pppoe-server max-sessions local-mac** 命令用来恢复本参数为缺省值。

相关配置可参考命令 **pppoe-server max-sessions remote-mac**，**pppoe-server max-sessions total**。

【举例】

设置一个本端 MAC 地址上能创建的最大 PPPoE session 数目为 50。

```
[H3C] pppoe-server max-sessions local-mac 50
```

2.1.5 pppoe-server max-sessions remote-mac

【命令】

pppoe-server max-sessions remote-mac *number*

undo pppoe-server max-sessions remote-mac

【视图】

系统视图

【参数】

number：一个对端 MAC 地址上能创建的最大 PPPoE session 数目。

【描述】

pppoe-server max-sessions remote-mac 命令用来配置一个对端 MAC 地址上能创建的最大 PPPoE session 数目，**undo pppoe-server max-sessions remote-mac** 命令用来恢复本参数为缺省值。

相关配置可参考命令 **pppoe-server max-sessions local-mac**，**pppoe-server max-sessions total**。

【举例】

设置一个对端 MAC 地址上能创建的最大 PPPoE session 数目为 50。

```
[H3C] pppoe-server max-sessions remote-mac 50
```

2.1.6 pppoe-server max-sessions total

【命令】

pppoe-server max-sessions total *number*

undo pppoe-server max-sessions total

【视图】

系统视图

【参数】

number：设置本系统能创建的最大 PPPoE session 数目。

【描述】

pppoe-server max-sessions total 命令用来配置本系统能创建的最大 PPPoE session 数目，**undo pppoe-server max-sessions total** 命令用来将本系统创建的最大 PPPoE session 数目恢复为缺省值。

相关配置可参考命令 **pppoe-server max-sessions remote-mac**，**pppoe-server max-sessions local-mac**。

【举例】

设置系统能创建的最大 PPPoE session 数目为 300。

```
[H3C] pppoe-server max-sessions total 300
```

2.1.7 reset pppoe-server

【命令】

reset pppoe-server { **all** | **virtual-template** *number* | **interface** *interface-type interface-num* }

【视图】

用户视图

【参数】

all：清除 PPPoE 全部会话。

virtual-template *number*：虚拟模板接口编号。

interface *interface-type interface-num*：接口类型和接口编号。

【描述】

reset pppoe-server 命令用来在 Server 端清除 PPPoE 会话。

【举例】

清除虚拟模板接口 1 上的会话。

```
<H3C> reset pppoe-server virtual-template1
```

第3章 PPPoE Client 配置命令

3.1 PPPoE Client 配置命令

3.1.1 debugging pppoe-client

【命令】

debugging pppoe-client { **all** | **data** | **error** | **event** | **packet** | **verbose** } [**interface** *type number*]

【视图】

用户视图

【参数】

all：打开所有 PPPoE Client 调试开关。

data：打开 PPPoE Session 阶段数据报文调试开关。

error：打开 PPPoE Client 的错误信息调试开关。

event：打开 PPPoE Client 事件调试开关。

packet：打开 PPPoE Discovery 阶段协商报文调试开关。

verbose：显示 PPPoE 数据的详细内容。

interface *type number*：接口类型及编号，用于打开指定接口的调试信息开关。如果不指定接口，则打开所有接口的调试信息开关。

【描述】

debugging pppoe-client 命令用来打开 PPPoE Client 的调试信息开关。

【举例】

无

3.1.2 dialer enable-circular

【命令】

dialer enable-circular

undo dialer enable-circular

【视图】

Dialer 接口视图

【参数】

无

【描述】

dialer enable-circular 命令用来使能轮询 DCC（Circular DCC）配置，**undo dialer enable-circular** 命令用来禁用轮询 DCC。

在 ISDN 接口上缺省为使能轮询 DCC，在其它接口上缺省为禁止轮询 DCC。

用户在使用轮询 DCC 方法前，必须首先使用此命令使能轮询 DCC 功能。

【举例】

在 Dialer1 上使能轮询 DCC。

```
[H3C-Dialer1] dialer enable-circular
```

3.1.3 dialer bundle

【命令】

dialer bundle *number*

undo dialer bundle

【视图】

Dialer 接口视图

【参数】

number：Dialer pool 序号，取值范围为 1～255。

【描述】

dialer bundle 命令用来设置一个 Dialer 接口使用的拨号池，**undo dialer bundle** 命令用来将 dialer bundle 与 Dialer 接口脱离。

缺省没有使能共享 DCC，也没有指定 **dialer bundle**。

此命令仅用于 Dialer 接口，并且一个 Dialer 接口只能对应一个 **dialer bundle**。

【举例】

在 Dialer1 上配置接口使用 Dialer bundle 3。

```
[H3C-Dialer1] dialer bundle 3
```

3.1.4 dialer-group

【命令】

dialer-group *group-number*

undo dialer-group

【视图】

Dialer 接口视图

【参数】

group-number：接口属于的拨号访问组的序号，这个拨号访问组由 **dialer-rule** 命令设定，取值范围为 1～255。

【描述】

dialer-group 命令用来对通过 DCC 接口发送的报文进行访问控制，将接口置于一个拨号访问组（dialer access group）中，**undo dialer-group** 命令用来将接口从此 dialer access group 中删除。

缺省情况下，未将接口加入到拨号访问组中。

此命令将接口置于一个拨号访问组中，通过 **dialer-rule** 命令将 dialer access group 与 **acl** 命令对应起来。一个 DCC 接口只能属于一个 **dialer group**，若配置第二次，则覆盖第一次的配置。

🕮 **说明：**

接口的缺省配置中，**dialer-group** 是未配置的。用户必须配置此命令，否则 DCC 将无法发送报文。

相关配置可参考命令 **dialer-rule**。

【举例】

将接口 dialer1 置入 dialer-group 1。

```
[H3C] dialer-rule 1 acl 3101
[H3C] interface dialer1
[H3C-dialer1] dialer-group 1
```

3.1.5 dialer-rule

【命令】

dialer-rule *dialer-number* { *protocol-name* { **permit** | **deny** } | **acl** *acl-number* }

undo dialer-rule *dialer-number*

【视图】

系统视图

【参数】

dialer-number：拨号访问组（dialer access group）的序号，范围为 1～255，与 DCC 接口配置中的 **dialer-group** *group-number* 相对应。

protocol-name：网络协议名，为 IP 等。

permit：表示允许相应协议的数据报文。

deny：表示禁止相应协议的数据报文。

acl *acl-number*：拨号访问组对应的 **acl** 序号。

【描述】

dialer-rule 命令用来设定控制 DCC 呼叫发生的数据报文的条件，**undo dialer-rule** 命令用来取消该设置。

缺省不设定控制 DCC 呼叫发生的数据报文的条件。

通过此命令设定一个拨号访问组对应的呼叫触发条件，通过 **dialer-group** 命令将 Dialer 接口置于一个拨号访问组中，从而完成对一个 DCC 接口的报文发送控制。

若一个 **dialer-group** 找不到对应的 **dialer-rule**，DCC 将报文作为 Uninteresting 报文。

相关配置可参考命令 **dialer-group**。

【举例】

设置 dialer-rule。

```
[H3C] acl number 3101
[H3C-acl-adv-3101] rule permit ip source 0.0.0.0 255.255.255.255 destination
0.0.0.0 255.255.255.255
[H3C-acl-adv-3101] quit
[H3C] dialer-rule 1 acl 3101
[H3C] interface dialer1
[H3C-dialer1] dialer-group 1
```

3.1.6 dialer user

【命令】

dialer user *username*

undo dialer user

【视图】

Dialer 接口视图

【参数】

username：对端用户名，为长度为 1～80 的字符串，用于 PPP 验证。

【描述】

dialer user 命令用来设置对端用户名，以便接收呼叫时能验证请求，**undo dialer user** 命令用来删除对端用户名。

缺省无对端用户名。

该命令仅在 Dialer 接口上有效。在一个 Dialer 口下最多可以配置 255 个 Dialer user。当一个 Dialer 口下配置多个 Dialer user 时，可以实现用一个 Dialer 接口同时接入多个物理接口。

当 Dialer 接口封装 PPP 时，利用 PPP 验证得到的对端用户名决定接收呼叫时的 Dialer 接口，此时可以选择配置 **dialer number** 命令。

相关配置可参考命令 **ppp pap local-user**，**ppp chap user**。

【举例】

设置对端用户名为“GWB”。

```
[H3C-Dialer3] dialer user GWB
```

3.1.7 display pppoe-client session

【命令】

display pppoe-client session { **summary** | **packet** } [**dial-bundle-number** *number*]

【视图】

所有视图

【参数】

summary：显示 PPPoE 会话的概要信息。

packet：显示 PPPoE 会话的数据收发统计信息。

dial-bundle-number *number*：显示指定 PPPoE 会话的统计信息。如果不指定 PPPoE 会话，则显示所有 PPPoE 会话的统计信息。

【描述】

display pppoe-client session 命令用来显示 PPPoE 会话的状态和统计信息。

【举例】

显示 PPPoE 会话的概要信息。

```
[H3C] display pppoe-client session summary
There is 2 session in total:
ID   Bundle  Dialer  Intf            Client-MAC    Server-MAC    State
1     1        1     Eth0          00e0fc0254f3  00049a23b050  PPPUP
2     2        2     Eth0          00e0fc0254f3  00049a23b050  PPPUP
```

显示信息的详细说明请见下表。

表3-1 display pppoe-client session summary 显示信息的含义

域	意义
ID	Session ID，PPPoE 会话的编号
Server-MAC	服务器 MAC 地址
Client-MAC	客户端 MAC 地址
Dialer	PPPoE 会话所对应的 Dialer 接口
Bundle	PPPoE 会话所属的 Dialer Bundle
Intf	PPPoE 会话所属的以太网接口
State	PPPoE 会话所处的状态

显示 PPPoE 会话的数据收发统计信息

```
[H3C] display pppoe-client session packet
PPPoE Client Session:
ID     InP        InO        InD       OutP       OutO      OutD
============================================================
1      164        6126       0          83        1069       0
2      304        9886       0          156       2142       0
```

显示信息的详细说明请见下表。

表3-2 display pppoe-client session packet 显示信息的含义

域	意义
ID	Session ID，PPPoE 会话的编号
InP	In Packets，接收报文数
InO	In Octets，接收字节数
InD	In Discards，接收非法报文并抛弃的报文数
OutP	Out Packets，发送报文数
OutO	Out Octets，发送字节数
OutD	Out Discards，发送非法报文并抛弃的报文数

3.1.8 interface dialer

【命令】

interface dialer *number*

undo interface dialer *number*

【视图】

系统视图

【参数】

number：接口序号，取值范围为 0～1023。

【描述】

interface dialer 命令用来在轮询 DCC 配置中，创建一个 Dialer Circular Group；在共享 DCC 配置中，定义一个 Dialer 接口。**undo interface dialer** 命令用来取消已有的设置。

缺省情况下，未定义 Dialer 接口。

轮询 DCC 中，Dialer Circular Group 允许将一个 Dialer 接口的配置用于一组物理接口，这些物理接口继承 Dialer 接口的属性。这种方式在需要同时呼叫多个目的地址时是非常有效的，即在 Dialer 接口上配置多条 **dialer route** 命令，而每个物理接口中只需执行 **dialer circular-group** 命令。

共享 DCC 中，虽然任意一个 Dialer 接口也可以有多个物理接口为它提供服务，但任意一个物理接口可同时服务于多个 Dialer 接口，而这些物理接口上必须配置验证，通过拨入方的用户名寻找它本次呼叫所对应的 Dialer 接口；该方式下，物理接口与 Dialer 接口是动态绑定的，而且一个 Dialer 接口只能呼叫一个目的地址，由命令 **dialer number** 来指定。

轮询 DCC 和共享 DCC 的物理接口不具有单独的网络地址。它们都使用 Dialer 接口中对应的地址。

【举例】

定义一个 Dialer 接口 dialer1。

```
[H3C] interface dialer1
```

3.1.9 pppoe-client

【命令】

pppoe-client dial-bundle-number *number* [**no-hostuniq**] [**idle-timeout** *seconds* [**queue-length** *packets*]]

undo pppoe-client dial-bundle-number *number*

【视图】

以太网接口或者虚拟以太网接口视图

【参数】

dial-bundle-number *number*：与 PPPoE 会话相对应的 Dialer Bundle 编号，取值范围为 1～255。参数 *number* 可以用来唯一标识一个 PPPoE 会话，也可以把它作为 PPPoE 会话的编号。

no-hostuniq：在 PPPoE Client 发起的呼叫中不携带 Host-Uniq 字段。

idle-timeout *seconds*：允许 PPPoE 会话空闲的时间，单位为秒，取值范围为 1～65535。如果不配置此参数，则 PPPoE 会话工作在永久在线方式；如果配置此参数，则 PPPoE 会话工作在报文触发方式。

queue-length *packets*：在 PPPoE 会话没有建立之前，系统可以缓存的报文个数，取值范围为 1～100。此参数只有在配置了 **idle-timeout** 后才有效。*packets* 的缺省值为 10。

【描述】

pppoe-client 命令用来建立一个 PPPoE 会话，并且指定该会话所对应的 Dialer Bundle；**undo pppoe-client** 命令用来删除一个 PPPoE 会话。

缺省情况下，没有配置 PPPoE 会话。

在一个以太网接口上可以配置多个 PPPoE 会话，即一个以太网接口可以同时属于多个 Dialer Bundle，但是一个 Dialer Bundle 中只能拥有一个以太网接口。PPPoE 会话是和 Dialer Bundle 一一对应的。如果某一 Dialer 接口的 Dialer Bundle 已经有一个以太网接口被用于 PPPoE，那么此 Dialer Bundle 中不能加入其他任何接口。同样，如果在 Dialer Bundle 中已经有除 PPPoE 以太网接口以外的接口，那么此 Dialer Bundle 也同样不能加入被用于 PPPoE Client 的以太网接口。

当 PPPoE 会话工作在永久在线方式时，物理线路 UP 后，防火墙会立即发起 PPPoE 呼叫，建立 PPPoE 会话。除非用户使用命令 **undo pppoe-client** 命令删除 PPPoE 会话，否则此 PPPoE 连接会一直存在。当 PPPoE 会话工作在报文触发方式时，防火墙只有在有数据需要传送时才会发起 PPPoE 呼叫，建立 PPPoE 会话。如果在 *seconds* 时间内 PPPoE 链路上没有数据传输，则防火墙会自动中止 PPPoE 会话，直到有新的数据需要被传送，PPPoE 会话才会被重新建立。

相关配置可参考命令 **reset pppoe-client**。

【举例】

在接口 Ethernet 1/0/0 上创建一个 PPPoE 会话。

```
[H3C-Ethernet1/0/0] pppoe-client dial-bundle-number 1
```

3.1.10 reset pppoe-client

【命令】

reset pppoe-client { **all** | **dial-bundle-number** *number* }

【视图】

用户视图

【参数】

all：清除所有的 PPPoE 会话。

dial-bundle-number *number*：Dialer Bundle 编号，取值范围为 1～255。用于清除与指定 Dialer Bundle 相对应的 PPPoE 会话。

【描述】

reset pppoe-client 命令用来复位 PPPoE 会话，并在稍后重新发起连接。

当 PPPoE 会话工作在永久在线方式时，如果使用 **reset pppoe-client** 命令中止 PPPoE 会话，防火墙会在 16 秒后自动重新建立 PPPoE 会话。当 PPPoE 会话工作在报文触发方式时，如果使用 **reset pppoe-client** 命令中止 PPPoE 会话，防火墙会在有数据需要传送时，才重新建立 PPPoE 会话。

相关配置可参考命令 **pppoe-client**。

【举例】

清除所有的 PPPoE 会话，并在稍后重新发起 PPPoE 会话。

```
<H3C> reset pppoe-client all
```

第4章 VLAN 配置命令

4.1 VLAN 配置命令

4.1.1 display vlan interface

【命令】

display vlan interface *interface-type interface-num*

【视图】

所有视图

【参数】

interface-type interface-num：参数用于指定接口。目前支持接口类型有以太网接口和千兆以太网接口，只支持子接口。

【描述】

display vlan interface 命令用来显示某个接口的 VLAN 配置信息，只支持子接口。

【举例】

显示以太网子接口 2/0/0.1 的 VLAN 配置信息。

```
<H3C> display vlan interface ethernet 2/0/0.1
encapsulation dot1q vid 60
```

4.1.2 display vlan max-packet-process

【命令】

display vlan max-packet-process *vid*

【视图】

所有视图

【参数】

vid：VLAN ID，用来标识一个 VLAN。

【描述】

display vlan max-packet-process 命令用来显示某个 VLAN 上配置的每秒的最大处理报文数目。

相关配置可参考命令 **max-packet-process**。

【举例】

显示 VLAN 10 上配置的最大处理报文数目。

```
<H3C> display vlan max-packet-process 10
Max Packet Process Count for Vid 10 is 300000
```

4.1.3 display vlan statistics vid

【命令】

display vlan statistics vid *vid*

【视图】

所有视图

【参数】

vid：VLAN ID，用来标识一个 VLAN。

【描述】

display vlan statistics vid 命令用来显示某个 VLAN 上的报文统计信息，如接收的报文数目，发送的报文数目。

相关配置可参考命令 **reset vlan statistics interface**。

【举例】

显示 VLAN 10 上的报文统计信息。

```
<H3C> display vlan statistics vid 10
Packets received: 53
Packets transmitted: 14
```

4.1.4 max-packet-process

【命令】

max-packet-process *count vid*

undo max-packet-process *vid*

【视图】

系统视图

【参数】

count：最大处理报文数目。

vid：VLAN ID，用来标识一个 VLAN。

【描述】

max-packet-process 命令用来设置某个 VLAN 的每秒的最大处理报文数目，**undo max-packet-process** 命令用来将某个 VLAN 的每秒的最大处理报文数目恢复为缺省配置。

缺省情况下，系统没有最大处理报文数目的限制。

设置了某个 VLAN 的每秒的最大处理报文数目后，当接收到的属于这个 VLAN 的报文达到这个限制后，就会丢弃以后接收到的属于这个 VLAN 的报文。通过这个命令可以进行流量控制。

相关配置可参考命令 **display vlan max-packet-process**。

【举例】

设置 VLAN 10 的每秒的最大处理报文数目为 200000。

```
[H3C] max-packet-process 200000 10
```

4.1.5 reset vlan statistics vid

【命令】

reset vlan statistics vid *vid*

【视图】

用户视图

【参数】

vid：VLAN ID，用来标识一个 VLAN。

【描述】

reset vlan statistics vid 命令用来清除 VLAN 统计信息。

相关配置可参考命令 **display vlan statistics vid**。

【举例】

清除 VLAN ID 为 10 的统计信息。

```
<H3C> reset vlan statistics vid 10
```

4.1.6 vlan-type dot1q

【命令】

vlan-type dot1q vid *vid*

【视图】

接口视图

【参数】

vid：VLAN ID，用来标识一个 VLAN，取值范围为 1～4094。

【描述】

vlan-type dot1q 命令用来设置子接口上的封装类型。

缺省情况下，系统子接口上无封装，也没有与子接口关联的 VLAN ID。

相关配置可参考命令 **display vlan interface**。

【举例】

设置以太网子接口 2/0/0.1 与 VLAN ID 60 相关联，以太网子接口 2/0/0.1 的封装格式为 dot1q。

```
[H3C-Ethernet2/0/0.1] vlan-type dot1q vid 60
```

目 录

第 1 章 IP地址配置命令 1-1
1.1 IP地址配置命令 1-1
1.1.1 display ip interface 1-1
1.1.2 ip address 1-1
1.1.3 ip address ppp-negotiate 1-3
1.1.4 ip address unnumbered 1-3
1.1.5 remote address 1-4
第 2 章 IP应用配置命令 2-1
2.1 ARP配置命令 2-1
2.1.1 arp check enable 2-1
2.1.2 arp send-gratuitous-arp 2-1
2.1.3 arp static 2-2
2.1.4 arp-proxy enable 2-3
2.1.5 debugging arp packet 2-3
2.1.6 display arp 2-4
2.1.7 gratuitous-arp-learning enable 2-5
2.1.8 gratuitous-arp-sending enable 2-6
2.1.9 naturemask-arp 2-7
2.1.10 reset arp 2-7
2.2 静态域名解析（DNS）命令 2-8
2.2.1 display ip host 2-8
2.2.2 ip host 2-8
2.3 DNS client配置命令 2-9
2.3.1 debugging dns 2-9
2.3.2 dns resolve 2-10
2.3.3 dns server 2-10
2.3.4 dns domain 2-11
2.3.5 display dns domain 2-12
2.3.6 display dns server 2-12
2.3.7 display dns dynamic-host 2-13
2.3.8 nslookup type 2-14
2.3.9 reset dns dynamic-host 2-15
2.4 DNS Proxy配置命令 2-15
2.4.1 dns-proxy enable 2-15
2.5 URPF配置命令 2-16
2.5.1 ip urpf 2-16
2.5.2 debugging ip urpf 2-17
第 3 章 UDP HELPER配置命令 3-1
3.1 UDP HELPER配置命令 3-1

3.1.1 debugging udp-helper 3-1
3.1.2 display udp-helper server 3-1
3.1.3 udp-helper enable 3-2
3.1.4 udp-helper port 3-2
3.1.5 udp-helper server 3-3
第 4 章 BOOTP客户端配置命令 4-1
4.1 BOOTP客户端配置命令 4-1
4.1.1 display bootp client 4-1
4.1.2 ip address bootp-alloc 4-2
第 5 章 DHCP配置命令 5-1
5.1 DHCP公共配置命令 5-1
5.1.1 dhcp enable 5-1
5.1.2 dhcp select （接口视图） 5-1
5.1.3 dhcp select interface（系统视图） 5-2
5.1.4 dhcp server detect 5-3
5.2 DHCP服务器配置命令 5-4
5.2.1 accounting domain 5-4
5.2.2 bims-server 5-4
5.2.3 debugging dhcp server 5-5
5.2.4 dhcp server accounting domain（系统视图） 5-7
5.2.5 dhcp server accounting domain（接口视图） 5-8
5.2.6 dhcp server bims-server （接口视图） 5-8
5.2.7 dhcp server bims-server （系统视图） 5-9
5.2.8 dhcp server dns-list （接口视图） 5-10
5.2.9 dhcp server dns-list（系统视图） 5-11
5.2.10 dhcp server domain-name（接口视图） 5-11
5.2.11 dhcp server domain-name（系统视图） 5-12
5.2.12 dhcp server expired （接口视图） 5-13
5.2.13 dhcp server expired（系统视图） 5-14
5.2.14 dhcp server forbidden-ip 5-14
5.2.15 dhcp server ip-pool 5-15
5.2.16 dhcp server nbns-list （系统视图） 5-16
5.2.17 dhcp server nbns-list（接口视图） 5-17
5.2.18 dhcp server netbios-type（接口视图） 5-18
5.2.19 dhcp server netbios-type（系统视图） 5-18
5.2.20 dhcp server option（系统视图） 5-19
5.2.21 dhcp server option（接口视图） 5-20
5.2.22 dhcp server ping 5-21
5.2.23 dhcp server static-bind 5-22
5.2.24 dhcp server voice-config（接口视图） 5-22
5.2.25 dhcp server voice-config（系统视图） 5-24
5.2.26 display dhcp server conflict 5-25

5.2.27 display dhcp server expired 5-26
5.2.28 display dhcp server free-ip 5-27
5.2.29 display dhcp server ip-in-use 5-27
5.2.30 display dhcp server statistics 5-29
5.2.31 display dhcp server tree 5-30
5.2.32 dns-list 5-33
5.2.33 domain-name 5-33
5.2.34 expired 5-34
5.2.35 gateway-list 5-35
5.2.36 nbns-list 5-35
5.2.37 netbios-type 5-36
5.2.38 network 5-37
5.2.39 option 5-38
5.2.40 reset dhcp server conflict 5-38
5.2.41 reset dhcp server ip-in-use 5-39
5.2.42 reset dhcp server statistics 5-39
5.2.43 static-bind ip-address 5-40
5.2.44 static-bind { mac-address | client-identifier } 5-41
5.2.45 voice-config 5-41
5.3 DHCP 客户端配置命令 5-43
5.3.1 debugging dhcp client 5-43
5.3.2 display dhcp client 5-43
5.3.3 ip address dhcp-alloc 5-45
5.4 DHCP中继配置命令 5-46
5.4.1 debugging dhcp relay 5-46
5.4.2 dhcp relay release 5-47
5.4.3 display dhcp relay address 5-47
5.4.4 display dhcp relay statistics 5-48
5.4.5 ip relay address 5-49
5.4.6 ip relay address cycle 5-50
5.4.7 ip relay address interface 5-50
5.4.8 reset dhcp relay statistics 5-51
第 6 章 IP性能配置命令 6-1
6.1 IP性能配置命令 6-1
6.1.1 debugging ip 6-1
6.1.2 debugging tcp event 6-2
6.1.3 debugging tcp md5 6-3
6.1.4 debugging tcp packet 6-4
6.1.5 debugging udp packet 6-5
6.1.6 display fib 6-5
6.1.7 display fib acl 6-6
6.1.8 display fib begin 6-7
6.1.9 display fib ip-prefix 6-8
6.1.10 display fib longer 6-9
6.1.11 display fib statistics 6-10

6.1.12 display icmp statistics 6-11
6.1.13 display ip fast-forwarding cache 6-12
6.1.14 display ip interface 6-13
6.1.15 display ip interface brief 6-14
6.1.16 display ip socket 6-15
6.1.17 display ip statistics 6-16
6.1.18 display tcp statistics 6-17
6.1.19 display tcp status 6-19
6.1.20 display udp statistics 6-20
6.1.21 icmp redirect send 6-21
6.1.22 ip fast-forwarding 6-22
6.1.23 reset ip fast-forwarding cache 6-23
6.1.24 reset ip statistics 6-23
6.1.25 reset tcp statistics 6-24
6.1.26 reset udp statistics 6-24
6.1.27 tcp mss 6-24
6.1.28 tcp timer fin-timeout 6-25
6.1.29 tcp timer syn-timeout 6-26
6.1.30 tcp window 6-26
第 7 章 IP单播策略路由配置命令 7-1
7.1 IP单播策略路由配置命令 7-1
7.1.1 apply default output-interface 7-1
7.1.2 apply ip-address default next-hop 7-1
7.1.3 apply ip-address next-hop 7-2
7.1.4 apply ip-precedence 7-3
7.1.5 apply output-interface 7-4
7.1.6 display ip policy 7-4
7.1.7 display ip policy setup 7-5
7.1.8 display ip policy statistic 7-6
7.1.9 if-match acl 7-6
7.1.10 if-match packet-length 7-7
7.1.11 ip local policy route-policy 7-8
7.1.12 ip policy route-policy 7-8
7.1.13 route-policy 7-9

第1章 IP 地址配置命令

1.1 IP 地址配置命令

1.1.1 display ip interface

【命令】

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

【视图】

所有视图

【参数】

brief：显示概要信息。

interface-type：接口类型。

interface-number：接口序号。

【描述】

display ip interface 命令用来显示当前接口的 IP 信息。

【举例】

显示接口 Ethernet0/0/0 的 IP 信息。

```
<H3C> display ip interface Ethernet0/0/0
Ethernet0/0/0 current state : UP
Line protocol current state : UP
Internet Address : 5.5.5.5/8
Broadcast address : 5.255.255.255
The Maximum Transmit Unit : 1500 bytes
input packets : 1231, bytes : 57557, multicasts : 1177
output packets : 0, bytes : 0, multicasts : 0
```

上面显示信息表示接口 Ethernet0/0/0 的物理链路状态为 UP，链路层协议状态为 UP，IP 地址为 5.5.5.5，广播地址为 5.255.255.255，最大传输单元是 1500 字节，以及该接口报文的收发情况。

1.1.2 ip address

【命令】

ip address *ip-address net-mask* [**sub**]

undo ip address [*ip-address net-mask* [**sub**]]

【视图】

接口视图

【参数】

ip-address：接口 IP 地址，为点分十进制格式。

net-mask：相应的子网掩码，为点分十进制格式或指定掩码长度。

sub：为了使不同的子网之间进行通讯，需要配置从 IP 地址。

【描述】

ip address 命令用来配置接口 IP 地址，**undo ip address** 命令用来取消接口的 IP 地址。

缺省情况下，接口无 IP 地址。

用户可以根据实际情况选择合适的 IP 子网，另外主机地址部分全为 0 表示网络地址，全为 1 表示广播地址，不能作为一般的 IP 地址使用。

通过子网掩码来标识 IP 地址包含的网络号，例如：防火墙以太网口的 IP 地址是 129.9.30.42，掩码是 255.255.0.0，将 IP 地址与掩码相与，可知防火墙以太网接口所在的网络号为 129.9.0.0。

在一般情况下，一个接口配置一个 IP 地址即可，为了使防火墙的一个接口可以与多个子网相连，在一个接口可以配置多个 IP 地址，其中一个为主 IP 地址，其余为从 IP 地址。主从地址的配置关系为：

- 当配置主 IP 地址时，如果接口上已经有主 IP 地址，则原主 IP 地址被删除，新配置的地址成为主 IP 地址。
- **undo ip address** 命令不带任何参数表示删除该接口的所有 IP 地址。**undo ip address** *ip-address net-mask* 表示删除主 IP 地址，**undo ip address** *ip-address net-mask* **sub** 表示删除从 IP 地址。在删除主 IP 地址前必须先删除完所有的从 IP 地址。

另外，对防火墙的各个接口上配置的 IP 地址都不能位于相同的子网。

相关配置可参考命令 **ip route-static**，**display ip interface**，**display interface**。

【举例】

为接口 Ethernet 0/0/0 配置主 IP 地址为 129.102.0.1，从 IP 地址为 202.38.160.1，子网掩码都为 255.255.255.0。

```
[H3C-Ethernet0/0/0] ip address 129.102.0.1 255.255.255.0
[H3C-Ethernet0/0/0] ip address 202.38.160.1 255.255.255.0 sub
```

1.1.3 ip address ppp-negotiate

【命令】

ip address ppp-negotiate

undo ip address ppp-negotiate

【视图】

接口视图

【参数】

无

【描述】

ip address ppp-negotiate 命令用来允许接口的 IP 地址由对端协商分配，**undo ip address ppp-negotiate** 命令用来禁止接口 IP 地址的协商。

缺省情况下，系统不允许接口 IP 地址的协商。

因为 PPP 支持 IP 地址的协商，只有当接口封装链路层协议 PPP 时，才能设置接口 IP 地址的协商。

在一般情况下，不需要配置 IP 地址的协商，只有在一些特殊情况下，如接入 ISP 访问 Internet，此时与 ISP 相连接口的 IP 地址由 ISP 协商分配。

配置接口 IP 地址的协商后，不需给该接口配置 IP 地址。

【举例】

设置接口 Dialer0 的 IP 地址由对端协商分配。

```
[H3C-Dialer0] ip address ppp-negotiate
```

1.1.4 ip address unnumbered

【命令】

ip address unnumbered interface *interface-type interface-number*

undo ip address unnumbered

【视图】

接口视图

【参数】

interface-type：被借用接口的接口类型。

interface-number：被借用接口的接口序号。

【描述】

ip address unnumbered 命令用来配置接口可借用其它接口的 IP 地址，**undo ip address unnumbered** 命令用来取消借用其它接口的 IP 地址。

缺省情况下，不借用其它接口的 IP 地址。

封装了 PPP 的 Dialer 接口、虚模板接口和 Tunnel 接口可以使用该命令借用以太网口或其它接口的 IP 地址。以太网口不能借用其它接口的 IP 地址。

在 Tunnel 接口配置地址借用后，必须手工配置到 Tunnel 对端接口的静态路由，且建议掩码为 32 位，以免与其它路由冲突，导致报文被错误路由。

【举例】

封装 PPP 的拨号接口 Dialer0 借用以太网口 Ethernet 0/0/0 的 IP 地址。

```
[H3C-Dialer0] ip address unnumbered interface Ethernet 0/0/0
```

1.1.5 remote address

【命令】

remote address { *ip-address* | **pool** [*pool-number*] }

undo remote address

【视图】

接口视图

【参数】

ip-address：IP 地址。

pool-number：为地址池号，即将分配 *pool-number* 中的一个地址给对端接口。地址池号的范围是 0～99，缺省值是 0。

【描述】

remote address 命令用来配置为对端接口分配 IP 地址，**undo remote address** 命令用来取消为对端接口分配 IP 地址。

缺省情况下，接口不分配地址给对端。

当接口封装了 PPP，并且该接口还未配置 IP 地址而对端已经有 IP 地址时，可为该接口配置 IP 地址可协商属性（在本端上配置 **ip address ppp-negotiate** 命令，在对端上配置 **remote address** 命令），使本接口接受由 PPP 协商产生的对端分配的 IP 地址。该配置主要用于通过 ISP 访问 Internet 时，得到由 ISP 分配的 IP 地址。

⚠ 注意：

该命令不具有地址分配的强制性，即在配置该命令后，也允许对端自行配置 IP 地址；如不希望（或不允许）对端自行配置 IP 地址，必须再配置 **ppp ipcp remote-address forced**。

相关配置可参考命令 **ip address ppp-negotiate**、**ppp ipcp address forced**。

【举例】

封装 PPP 的拨号接口 Dialer0 为对端分配的 IP 地址为 10.0.0.1。

```
[H3C-Dialer0] remote address 10.0.0.1
```

第2章 IP 应用配置命令

2.1 ARP 配置命令

2.1.1 arp check enable

【命令】

arp check enable

undo arp check enable

【视图】

系统视图

【参数】

无

【描述】

arp check enable 命令用来使能 ARP 表项的检查功能，即不学习 MAC 地址为组播 MAC 的 ARP 表项。**undo arp check enable** 命令用来关闭 ARP 表项的检查功能，即学习 MAC 地址为组播 MAC 的 ARP 表项。

缺省情况下，使能 ARP 表项的检查功能，即不学习 MAC 地址为组播 MAC 的 ARP 表项。

【举例】

使能 ARP 表项的检查功能。

```
[H3C] arp check enable
```

2.1.2 arp send-gratuitous-arp

【命令】

arp send-gratuitous-arp *seconds*

undo arp send-gratuitous-arp

【视图】

接口视图

【参数】

seconds：发送免费 ARP 报文的周期，取值范围为 1～180，单位为秒。

【描述】

arp send-gratuitous-arp 命令用来在本接口上使能周期性发送免费 ARP 的功能并设置发送免费 ARP 报文的周期。**undo arp send-gratuitous-arp** 命令用来关闭周期性发送免费 ARP 的功能。

缺省情况下，接口不会周期性的发送免费 ARP 报文。

注意事项：

- 发送的免费 ARP 报文是本接口主地址的免费 ARP，这个主地址可以是使用命令行配置的，也可以是通过协商等其他方式获得的；
- 不发送从地址的免费 ARP；
- 接口链路层没有 UP 的情况下不发送免费 ARP 报文。

【举例】

在以太网接口 Ethernet0/0/0 上使能周期性发送免费 ARP 报文功能，并设置发送周期为 120 秒。

```
[H3C-Ethernet0/0/0] arp send-gratuitous-arp 120
```

2.1.3 arp static

【命令】

arp static *ip-address mac-address* [*vpn-instance-name*]

undo arp *ip-address* [*vpn-instance-name*]

【视图】

系统视图

【参数】

ip-address：为 ARP 映射项的 IP 地址，为点分十进制格式。

mac-address：ARP 映射项的以太网 MAC 地址，格式为 H-H-H。

vpn-instance-name：VPN 实例的名称。

【描述】

arp static 命令用来配置 ARP 映射表，**undo arp** 命令用来取消 ARP 映射表中对应地址的映射项。

缺省情况下，系统 ARP 映射表为空，由动态 ARP 协议获取地址映射。

一般情况下，ARP 映射表由动态 ARP 协议维护，在特殊情况下，才需要手工配置。另外 ARP 映射表只用于局域网内，对于广域网的地址解析，有其它的配置或获取方法（如帧中继的逆向地址解析）。

相关配置可参考命令 **reset arp**，**display arp**。

【举例】

配置 IP 地址 129.102.0.1 对应的以太网 MAC 地址为 00e0-fc01-0ec5。

```
[H3C] arp static 129.102.0.1 00e0-fc01-0ec5
```

2.1.4 arp-proxy enable

【命令】

arp-proxy enable

undo arp-proxy enable

【视图】

以太网接口视图

【参数】

无

【描述】

arp-proxy enable 命令用来使能以太网接口的代理 ARP 功能，**undo arp-proxy enable** 命令用来禁用代理 ARP 功能。

缺省情况下，禁用代理 ARP 功能。

该命令应用在以太网口上，对于处在同一网段，却在不同物理网络上的主机而言，代理 ARP 功能屏蔽了分离的物理网络这一事实，使用户使用起来，好象在同一个物理网络上。

【举例】

在以太网口使能代理 ARP。

```
[H3C-Ethernet0/0/0] arp-proxy enable
```

2.1.5 debugging arp packet

【命令】

debugging arp packet

undo debugging arp packet

【视图】

用户视图

【参数】

无。

【描述】

debugging arp packet 命令用来打开 ARP 报文调试功能，**undo debugging arp packet** 命令用来关闭 ARP 报文调试功能。

【举例】

打开 ARP 报文调试功能。

```
<H3C> debugging arp packet
```

2.1.6 display arp

【命令】

display arp [**static** | **dynamic** | **all**] [| { **begin** *text* | **exclude** *text* | **include** *text* }]

【视图】

所有视图

【参数】

static：表示显示静态 ARP 项。

dynamic：表示显示动态 ARP 项。

all：表示显示所有的 ARP 项。

|：匹配输出。

begin：匹配正则表达式起始的串。

exclude：匹配排除正则表达式的串。

include：匹配包含正则表达式的串。

text：正则表达式。

【描述】

display arp 命令用来显示 ARP 映射表。

相关配置可参考命令 **arp static**，**reset arp**。

【举例】

显示所有 ARP 表项。

```
<H3C> display arp
Type: S-Static   D-Dynamic
IP Address    MAC Address      Type    Vpn-instance Name    Interface
1.1.1.1       0012-0012-0012       S
10.153.72.2   00e0-fc00-0007       D                        Eth0/0/1
```

显示静态 ARP 表项。

```
<H3C> display arp static
Type: S-Static   D-Dynamic
IP Address    MAC Address      Type    Vpn-instance Name    Interface
1.1.1.1       0012-0012-0012       S
```

显示动态 ARP 表项。

```
<H3C> display arp dynamic
Type: S-Static   D-Dynamic
IP Address    MAC Address      Type Vpn-instance Name       Interface
10.153.72.2   00e0-fc00-0007   D                        Eth0/0/1
```

表2-1 display arp 显示解释表

域名	解释
Ip Address	IP 地址
Mac Address	MAC 地址
Type	ARP 表项类型
Vpn-instance Name	Vpn-instance 名称
interface	接口名称

2.1.7 gratuitous-arp-learning enable

【命令】

gratuitous-arp-learning enable

undo gratuitous-arp-learning enable

【视图】

系统视图

【参数】

无

【描述】

gratuitous-arp-learning enable 命令用来使能免费 ARP 报文的学习功能。**undo gratuitous-arp-learning enable** 命令用来关闭免费 ARP 报文的学习功能。

缺省情况下，关闭免费 ARP 报文的学习功能。

免费 ARP 是指设备通过对外发送免费 ARP 报文，来实现以下功能：

- 网络中设备可以通过发送免费 ARP 报文来确定其它设备的 IP 地址是否与自己冲突。
- 如果发送免费 ARP 报文的设备正好改变了硬件地址（很可能是设备关机了，并换了一块接口卡，然后重新启动），那么这个报文就可以使其它设备高速缓存中旧的硬件地址进行相应的更新。

相关配置可参考命令 **gratuitous-arp-sending enable**。

【举例】

使能学习免费 ARP 报文信息。

```
[H3C] gratuitous-arp-learning enable
```

2.1.8 gratuitous-arp-sending enable

【命令】

gratuitous-arp-sending enable
undo gratuitous-arp-sending enable

【视图】

系统视图

【参数】

无

【描述】

gratuitous-arp-sending enable 命令用来配置当收到不同网段的 APR 请求报文时，回送免费 ARP 报文（但此时自己并不学习收到的 ARP 表项）。**undo gratuitous-arp-sending enable** 命令用来取消应答不同网段的 ARP 请求报文的功能。

缺省情况下，关闭应答不同网段的 ARP 请求报文的功能。

相关配置可参考命令 **gratuitous-arp-learning enable**。

【举例】

使能发送免费 ARP 报文信息。

```
[H3C] gratuitous-arp-sending enable
```

2.1.9 naturemask-arp

【命令】

naturemask-arp enable

undo naturemask-arp enable

【视图】

系统视图

【参数】

无

【描述】

naturemask-arp enable 命令用来取消对 ARP 报文必须是同一子网网段的限制，支持自然网段的 ARP 请求。**undo naturemask-arp enable** 命令用来关闭支持自然网段的 ARP 请求的功能。

缺省情况下，不支持自然网段的 ARP 请求。

【举例】

取消对 ARP 报文必须是同一子网网段的限制。

```
[H3C] naturemask-arp enable
```

2.1.10 reset arp

【命令】

reset arp [**all** | **dynamic** | **static** | **interface** *interface-type interface-number*]

【视图】

用户视图

【参数】

static：表示清除静态 ARP 项。

dynamic：表示清除动态 ARP 项。

all：表示清除所有的 ARP 项。

interface：表示选择接口。

interface-type：接口类型。

interface-number：接口序号。

【描述】

reset arp 命令用来清除 ARP 映射表中的 ARP 项。

对指定 **interface** 的接口进行操作时，接口类型只能是以太网口，而且只能删除该接口的动态（**dynamic**）表项。

相关配置可参考命令 **arp static**，**display arp**。

【举例】

删除接口 Ethernet 0/0/0 的 ARP 映射表中的 **dynamic** 项。

```
<H3C> reset arp interface Ethernet 0/0/0
```

2.2 静态域名解析（DNS）命令

2.2.1 display ip host

【命令】

display ip host

【视图】

所有视图

【参数】

无

【描述】

display ip host 命令用来显示所有的主机名和对应的 IP 地址。

【举例】

显示所有的主机名和对应的 IP 地址。

```
<H3C> display ip host
  Host                 Age        Flags  Address
  eth                  0          static 6.1.1.1
  secpath              0          static 1.1.1.1
```

2.2.2 ip host

【命令】

ip host *hostname ip-address*

undo ip host *hostname* [*ip-address*]

【视图】

系统视图

【参数】

hostname：主机名，字符串类型，取值范围为 1～20。

ip-address：与主机名对应的 IP 地址。

【描述】

ip host 命令用来配置静态域名解析表项，即主机名和对应的 IP 地址，**undo ip host** 命令用来取消主机名和对应的 IP 地址。

每个主机名只能对应一个 IP 地址。当对同一主机名配置对应多个 IP 地址时，后配置的对应关系生效。

主机名中可以包括大小写英文字母（a-z、A-Z）、数字（0-9）、下划线（_）和点（.），但主机名中必须至少含有一个英文字母（a-z 或 A-Z）。

缺省情况下，静态域名解析表为空，即无主机名与 IP 地址对应。

【举例】

设置主机名 router1 对应的 IP 地址为 10.110.0.1。

```
[H3C] ip host router1 10.110.0.1
```

设置主机名 router2 对应的 IP 地址为 10.110.0.2。

```
[H3C] ip host router2 10.110.0.2
```

设置主机名 router3 对应的 IP 地址为 10.110.0.3。

```
[H3C] ip host router3 10.110.0.3
```

取消主机名 router2 与 IP 地址 10.110.0.2 的对应关系。

```
[H3C] undo ip host router2 10.110.0.2
```

2.3 DNS client 配置命令

2.3.1 debugging dns

【命令】

debugging dns

undo debugging dns

【视图】

用户视图

【参数】

无

【描述】

debugging dns 命令用来打开 DNS Client 的调试开关，**undo debugging dns** 用来关闭 DNS Client 的调试开关。

缺省情况下，关闭 DNS Client 的调试开关。

【举例】

打开 DNS Client 的调试开关。

```
<H3C> debugging dns
```

关闭 DNS Client 的调试开关。

```
<H3C> undo debugging dns
```

2.3.2 dns resolve

【命令】

dns resolve

undo dns resolve

【视图】

系统视图

【参数】

无

【描述】

dns resolve 命令用来启动 DNS 域名解析功能。**undo dns resolve** 命令用来关闭 DNS 域名解析功能。

缺省情况下，DNS 域名解析功能没有开启。

【举例】

打开域名解析功能。

```
[H3C] dns resolve
```

2.3.3 dns server

【命令】

dns server *ip-address*

undo dns server [*ip-address*]

【视图】

系统视图

【参数】

ip-address：DNS 服务器的 IP 地址。

【描述】

dns server 命令用来配置 DNS 服务器的 IP 地址，**undo dns server** 命令用来删除 DNS 服务器的 IP 地址。

【举例】

配置 DNS 服务器的 IP 地址。

```
[H3C] dns server 10.110.66.1
```

删除指定 IP 地址的 DNS 服务器。

```
[H3C] undo dns server 10.110.66.1
```

删除所有 DNS 服务器。

```
[H3C] undo dns server
```

2.3.4 dns domain

【命令】

dns domain *domain-name*

undo dns domain [*domain-name*]

【视图】

系统视图

【参数】

domain-name：DNS 域后缀。

【描述】

dns domain 命令用来配置 DNS 域后缀，**undo dns domain** 命令用来删除 DNS 域后缀的配置。

【举例】

配置 DNS 域后缀。

```
[H3C] dns domain h3c.com
```

删除指定名称的 DNS 域后缀。

```
[H3C] undo dns domain h3c.com
```

删除所有 DNS 域后缀。

```
[H3C] undo dns domain
```

2.3.5 display dns domain

【命令】

display dns domain [**dynamic**]

【视图】

所有视图

【参数】

dynamic：显示通过 DHCP 等协议动态获得的域后缀。

【描述】

display dns domain 命令用来显示用户手工配置的 DNS 域后缀，**display dns domain dynamic** 命令用来显示通过 DHCP 等协议动态获得的 DNS 域后缀。

【举例】

显示手工获得的 DNS 域后缀。

```
[H3C] display dns domain
No          Domain-name
0           h3c.com
```

显示动态配置的 DNS 域后缀。

```
[H3C] display dns domain dynamic
No          Domain-name
0           h3c.com
```

2.3.6 display dns server

【命令】

display dns server [**dynamic**]

【视图】

所有视图

【参数】

dynamic：显示通过 DHCP 等协议动态获得的域名服务器地址。

【描述】

display dns server 命令用来显示用户手工配置的 DNS 服务器地址，**display dns server dynamic** 命令用来显示通过 DHCP 等协议动态获得的 DNS 服务器地址。

【举例】

显示动态获得的 DNS 服务器地址。

```
[H3C] display dns server dynamic
Domain-server        IpAddress
     0               10.72.66.36
```

显示手工配置的 DNS 服务器地址。

```
[H3C] display dns server
Domain-server        IpAddress
     0               10.72.74.5
```

2.3.7 display dns dynamic-host

【命令】

display dns dynamic-host

【视图】

所有视图

【参数】

无

【描述】

display dns dynamic-host 命令用来显示当前 DNS Client 解析的域名缓存中的内容。

在一次成功的域名解析之后，DNS Client 会把解析的结果放到缓存中，如果再有相同的域名解析请求，那么 DNS Client 会首先在缓存中查找，如果没有，再向 DNS 服务器发送域名解析请求，使用该命令可以显示当前缓存中的内容。

【举例】

显示 DNS Client 的缓存中的内容。

```
[H3C] display dns dynamic-host
No    Host          -->             Ipaddress                  TTL   Alias
1     www.sohu.com                91.1.1.1                   3521
2     www.sina.com.cn              87.1.1.1                  3000

No    Host          <--             Ipaddress                  TTL   Alias
```

```
1     www.163.com                191.1.1.1                3561
2     www.263.com                187.1.1.1                3300
```

表2-2 display dns dynamic-host 命令显示信息说明

项目	含义
Host	字段表示主机名
Ipaddress	字段表示对应主机的 IP 地址
TTL	表示该映射项存在的时间，单位是秒
Alias	显示的是主机名对应的别名。

📖 说明：

上半部显示的是从 Host 查询到的列表，为 A 类查询结果;

下半部显示的是从 IP address 查询到 Host”，为 PTR 类查询结果;

2.3.8 nslookup type

【命令】

nslookup type { **ptr** *ip-address* | **a** *domain-name* }

【视图】

所有视图

【参数】

ptr *ip-address*：解析 IP 地址对应的 DNS 域名。

a *domain-name*：解析 DNS 域名对应的 IP 地址。域名长度为小于 30 的字符串，支持自动域名追加。

【描述】

nslookup type 命令用来解析指定 IP 地址对应的域名或解析指定域名对应的 IP 地址。

【举例】

解析 192.168.3.2 对应的域名。

```
<H3C> nslookup type ptr 192.168.3.2
Trying DNS server （10.72.66.36）
Name:    www.h3c.com
Address:  192.168.3.2
```

解析 www.h3c.com 对应的 IP 地址。

```
<H3C> nslookup type a www.h3c.com
Trying DNS server  （10.72.66.36）
Name:    www.h3c.com
Address:  192.168.3.2
```

2.3.9 reset dns dynamic-host

【命令】

reset dns dynamic-host

【视图】

用户视图

【参数】

无

【描述】

reset dns dynamic-host 命令用来清空当前 DNS Client 解析的域名缓存中的内容。

【举例】

清空 DNS Client 的缓存中的内容。

```
<H3C> reset dns dynamic-host
```

2.4 DNS Proxy 配置命令

2.4.1 dns-proxy enable

【命令】

dns-proxy enable

undo dns-proxy enable

【视图】

系统视图

【参数】

无

【描述】

dns-proxy enable 命令用来启动 DNS 代理功能。**undo dns-proxy enable** 命令用来禁止 DNS 代理功能。

缺省情况下，禁止 DNS 代理功能。

【举例】

启用 DNS 代理功能。

```
[H3C] dns-proxy enable
```

2.5 URPF 配置命令

2.5.1 ip urpf

【命令】

ip urpf { **strict** | **loose** } [**allow-default-route**] [**acl** *acl-number*]

undo ip urpf

【视图】

接口视图

【参数】

strict：严格型检查。报文的源地址必须在防火墙的 FIB 表存在，并对收到的报文反向查找出接口，要求其中至少有一个出接口和报文的入接口相匹配，否则报文将被 URPF 丢弃。

loose：松散型检查。只要求报文的源地址在防火墙的 FIB 表中存在（不管反向查找的出接口和报文的入接口是否一致），否则报文将被 URPF 丢弃。

allow-default-route：允许对缺省路由进行特殊处理。当同时配置了缺省路由及 **allow-default-route** 参数，**strict** 和 **loose** 型检查的处理原则有所变化。

acl-number：ACL 规则号，范围是 2000～3999。

【描述】

ip urpf 命令将在接口上使能 URPF 检查，**undo ip urpf** 命令在接口上禁止 URPF 检查。

缺省情况下不使能 URPF 检查。

【举例】

在以太口 Ethernet1/0/0 上使能严格 URPF 检查，同时允许对缺省路由进行特殊处理，并配置 ACL 列表号为 2999。

```
[H3C-Ethernet1/0/0] ip urpf strict allow-default-route acl 2999
```

2.5.2 debugging ip urpf

【命令】

debugging ip urpf discards [**interface** *interface-type interface-num*]

undo debugging ip urpf discards [**interface** *interface-type interface-num*]

【视图】

用户视图

【参数】

interface *interface-type interface-num*：接口类型及接口号。

【描述】

debugging ip urpf 命令用于打开 URPF 的调试信息开关，**undo debugging ip urpf** 命令用来关闭 URPF 的调试信息开关。

【举例】

如果以太网接口 Ethernet1/0/0 使能了 URPF，则通过如下的配置可以看到它的丢包信息。

```
<H3C> debugging ip urpf discards interface Ethernet1/0/0
```

第3章 UDP HELPER 配置命令

3.1 UDP HELPER 配置命令

3.1.1 debugging udp-helper

【命令】

debugging udp-helper { **event** | **packet** [**receive** | **send**] }

undo debugging udp-helper { **event** | **packet** [**receive** | **send**] }

【视图】

用户视图

【参数】

event：UDP HELPER 的事件调试开关。

packet：UDP HELPER 的收/发报文调试开关。

receive：UDP HELPER 的接收报文调试开关。

send：UDP HELPER 的发送报文调试开关。

【描述】

debugging udp-helper 命令用来打开 UDP HELPER 的调试开关，**undo debugging udp-helper** 命令用来关闭 UDP HELPER 的调试开关。

缺省情况下，UDP HELPER 的调试开关处于关闭状态。

【举例】

打开 UDP HELPER 的收/发报文调试开关。

```
<H3C> debugging udp-helper packet
```

3.1.2 display udp-helper server

【命令】

display udp-helper server [**interface** *type number*]

【视图】

所有视图

【参数】

type number：以太网接口类型和接口号。

【描述】

display udp-helper server 命令用来显示以太网接口对应的目的服务器信息。

【举例】

显示以太网接口对应的目的服务器信息。

```
<H3C> display udp-helper server interface ethernet 0/0/0
Interface name        Server address       Packets send
Ethernet0/0/0     192.1.1.2           0
```

以上显示信息表示以太网接口 Ethernet0/0/0 对应的目的服务器的 IP 地址为 192.1.1.2，发送报文数为 0。

3.1.3 udp-helper enable

【命令】

udp-helper enable

undo udp-helper enable

【视图】

系统视图

【参数】

无

【描述】

udp-helper enable 命令用来启动 UDP 中继转发功能，**undo udp-helper enable** 命令用来关闭 UDP 中继转发功能。

缺省情况下，UDP 中继转发处于关闭状态。

【举例】

启动 UDP 中继转发功能。

```
[H3C] udp-helper enable
```

3.1.4 udp-helper port

【命令】

udp-helper port { *port* | **dns** | **netbios-ds** | **netbios-ns** | **tacacs** | **tftp** | **time** }

undo udp-helper port { *port* | **dns** | **netbios-ds** | **netbios-ns** | **tacacs** | **tftp** | **time** }

【视图】

系统视图

【参数】

port：需要中继转发的 UDP 端口号，取值范围为 1～65535。

dns：Domain Name Service，对应的 UDP 端口为 53。

netbios-ds：NetBIOS datagram service，对应的 UDP 端口为 138。

netbios-ns：NetBIOS name service，对应的 UDP 端口为 137。

tacacs：TACACS，对应的 UDP 端口为 49。

tftp：Trivial File Transfer Protocol，对应的 UDP 端口为 69。

time：Time service，对应的 UDP 端口为 37。

【描述】

udp-helper port 命令用来配置需要中继转发的 UDP 端口，**undo udp-helper port** 命令用来删除需要中继转发的 UDP 端口。

【举例】

配置需要中继转发的 UDP 端口为 DNS 协议对应的端口。

```
[H3C] udp-helper port dns
```

3.1.5 udp-helper server

【命令】

udp-helper server *ip-address*

undo udp-helper server [*ip-address*]

【视图】

以太网接口视图

【参数】

ip-address：目的服务器的 IP 地址，为点分十进制格式。

【描述】

udp-helper server 命令用来配置广播报文中继转发的目的服务器，**undo udp-helper server** 命令用来删除广播报文中继转发的目的服务器。

缺省情况下，没有配置目的服务器。

相关配置可参考命令 **display udp-helper server**。

【举例】

配置广播报文中继转发的目的服务器为 192.1.1.2。

```
[H3C-Ethernet0/0/0] udp-helper server 192.1.1.2
```

第4章 BOOTP 客户端配置命令

4.1 BOOTP 客户端配置命令

4.1.1 display bootp client

【命令】

display bootp client [**interface** *interface-type interface-number*]

【视图】

所有视图

【参数】

interface *interface-type interface-number*：接口类型及接口号。

【描述】

display bootp client 命令用来显示 BOOTP 客户端的相关信息，包括 BOOTP 客户端的 MAC 地址和申请到的 IP 地址等信息。

【举例】

显示 BOOTP 客户端的相关信息。

```
[H3C] display bootp client interface ethernet0/0/0
Interface ethernet0/0/0:
Allocated IP: 169.254.0.2 255.255.0.0
Transaction ID = 0x3d8a7431
Mac Address  00e0-fc0a-c3ef
```

表4-1 display bootp client 显示解释表

域名	解释
Interface ethernet0/0/0	Interface ethernet0/0/0 接口配置为通过 BOOTP 方式获取 IP 地址
Allocated IP	所分配到的 IP 地址
Transaction ID	BOOTP 报文中 XID 字段值
Mac Address	BOOTP 客户端的 MAC 地址

4.1.2 ip address bootp-alloc

【命令】

ip address bootp-alloc

undo ip address bootp-alloc

【视图】

以太网接口视图

【参数】

无

【描述】

ip address bootp-alloc 命令用来配置以太网接口通过 BOOTP 协议获取 IP 地址，**undo ip address bootp-alloc** 命令用来取消以太网接口通过 BOOTP 协议获取 IP 地址。

缺省情况下，以太网接口不通过 BOOTP 协议获取 IP 地址。

【举例】

配置以太网接口 Ethernet 0/0/0 通过 BOOTP 协议获取 IP 地址。

```
[H3C-Ethernet0/0/0] ip address bootp-alloc
```

第5章 DHCP 配置命令

5.1 DHCP 公共配置命令

5.1.1 dhcp enable

【命令】

dhcp enable

undo dhcp enable

【视图】

系统视图

【参数】

无

【描述】

dhcp enable 命令用来使能 DHCP 服务，**undo dhcp enable** 命令用来禁止 DHCP 服务。

缺省情况下，使能 DHCP 服务。

在进行DHCP配置之前，必须先使能DHCP服务。该配置对于DHCP服务器和DHCP中继都是必须的。

🕮 **说明：**

在正确配置系统时钟后，DHCP 才会正常运行。

【举例】

使能 DHCP 服务。

```
[H3C] dhcp enable
```

5.1.2 dhcp select （接口视图）

【命令】

dhcp select { **global** [**subaddress**] | **interface** | **relay** }

undo dhcp select

【视图】

接口视图

【参数】

global：将 DHCP 报文发送到本地的 DHCP 服务器，由本地 DHCP 服务器从全局地址池分配地址。

subaddress：使能 DHCP Server 从地址分配功能，即服务器分配给客户端的 IP 地址为服务器上以太网口从地址网段的 IP 地址，该地址从全局地址池中分配。此时服务器端以太网接口下也要配置从 IP 地址，且要求全局地址池的网段与接口下从 IP 地址在同一网段。

interface：将 DHCP 报文发送到本地的 DHCP 服务器，由本地 DHCP 服务器从接口地址池分配地址。

relay：将 DHCP 报文通过中继发送外部的 DHCP 服务器，由外部 DHCP 服务器分配地址。

【描述】

dhcp select 命令用来设置对目的地址是本机的 DHCP 报文的处理模式，**undo dhcp select** 命令用来恢复缺省设置。

缺省情况下，目的地址是本机的 DHCP 报文将被送到内部服务器，从全局地址池中分配地址（global 方式）。

相关配置可参考命令 **dhcp select interface**。

【举例】

对于目的地址是本机的 DHCP 报文，从内部 DHCP 服务器的接口地址池中分配地址。

```
[H3C-Ethernet1/0/0] dhcp select interface
```

5.1.3 dhcp select interface（系统视图）

【命令】

dhcp select { **global** [**subaddress**] | **interface** | **relay** } { **interface** *ethernet-subinterface-range* | **all** }

undo dhcp select { **interface** *ethernet-subinterface-range* | **all** }

【视图】

系统视图

【参数】

global：将 DHCP 报文发送到本地的 DHCP 服务器，由本地 DHCP 服务器从全局地址池分配地址。

subaddress：使能 DHCP Server 从地址分配功能，即服务器分配给客户端的 IP 地址为服务器上以太网口从地址网段的 IP 地址，该地址从全局地址池中分配。此时服务器端以太网接口下也要配置从 IP 地址，且要求全局地址池的网段与接口下从 IP 地址在同一网段。

interface：将 DHCP 报文发送到本地的 DHCP 服务器，由本地 DHCP 服务器从接口地址池分配地址。

relay：将 DHCP 报文通过中继发送到外部的 DHCP 服务器，由外部 DHCP 服务器分配地址。

ethernet-subinterface-range：用关键字“**to**”连接两个子接口，表示子接口号在两个接口之间的所有子接口（包含这两个子接口）。该接口必须为以太网接口。

all：表示所有接口。

【描述】

dhcp select interface 命令用来设置指定接口收到目的地址是本机的 DHCP 报文的处理模式，**undo dhcp select interface** 命令用来恢复缺省设置。

缺省情况下，目的地址是本机的 DHCP 报文将被送到内部服务器，从全局地址池中分配地址（global 方式）。

相关配置可参考命令 **dhcp select**。

【举例】

配置 Ethernet2/0/0.1 到 Ethernet2/0/0.5 之间的子接口，对于目的地址是本机的 DHCP 报文，从内部服务器的接口地址池中分配地址。

```
[H3C] dhcp select interface interface ethernet 2/0/0.1 to ethernet 2/0/0.5
```

5.1.4 dhcp server detect

【命令】

dhcp server detect

undo dhcp server detect

【视图】

系统视图

【参数】

无

【描述】

dhcp server detect 命令用来使能伪 DHCP 服务器检测功能，**undo dhcp server detect** 命令用来禁止此功能。

缺省情况下，禁止伪 DHCP 服务器检测功能。

【举例】

启动伪 DHCP 服务器检测功能。

```
[H3C] dhcp server detect
```

5.2 DHCP 服务器配置命令

5.2.1 accounting domain

【命令】

accounting domain *domain-name*

undo accounting domain

【视图】

DHCP 地址池视图

【参数】

domain-name：DHCP 服务器计费所使用的域。注意该域必须配置为 RADIUS 方案。

【描述】

accounting domain 命令用来配置 DHCP 服务器计费所使用的域；**undo accounting domain** 命令用于取消 DHCP 服务器计费功能。

DHCP 服务器计费功能用于 DHCP 服务器在分配和释放租约时，向指定域的 RADIUS 计费服务器发送计费报文。此时 RADIUS 服务器只是记录了用户使用 IP 地址的情况，并不真正进行计费。

缺省情况下，未启动 DHCP 服务器计费功能。

【举例】

配置 DHCP 服务器计费功能。

```
[H3C-dhcp-pool-pool1] accounting domain h3c
```

5.2.2 bims-server

【命令】

bims-server ip *ip-address* [**port** *port-number*] **sharekey** *key*

undo bims-server

【视图】

DHCP 地址池视图

【参数】

ip *ip-address*：BIMS 服务器的 IP 地址。

port *port-number*：BIMS 服务器的协议端口号，范围为 1～65534。

sharekey *key*：BIMS 服务器的共享密钥，范围为 1～16 个字符。

【描述】

bims-server 命令用来在 DHCP 服务器上全局地址池中启动并配置 BIMS option。**undo bims-server** 命令用来在 DHCP 服务器上全局地址池中删除 BIMS option 配置。

在 DHCP 服务器上配置了 BIMS option 后，DHCP 服务器将会在返回给 DHCP 客户端的 DHCP_OFFER 以及 DHCP_ACK 回应报文中均携带 BIMS option。

在全局地址池中配置了 BIMS option 后，DHCP 服务器从全局地址池给客户端分配地址时将携带 BIMS option。

缺省情况下，DHCP 服务器没有配置 BIMS option。

【举例】

在全局地址池视图中配置 BIMS option，BIMS 服务器的 IP 地址是 192.168.1.1，协议端口为 80，共享密钥为 abcdefg。

```
[H3C] dhcp server ip-pool 123
[H3C-dhcp-pool-123] bims-server ip 192.168.1.1 port 80 sharekey abcdefg
```

5.2.3 debugging dhcp server

【命令】

debugging dhcp server { **all** | **error** | **event** | **packet** }

undo debugging dhcp server { **all** | **error** | **event** | **packet** }

【视图】

用户视图

【参数】

all：DHCP 服务器的所有调试功能。

error：DHCP 服务器的错误调试功能，包括 DHCP 服务器处理 DHCP 报文、分配地址时出现的错误等。

event：DHCP 服务器事件调试功能，包括地址分配、ping 检测超时等。

packet：DHCP 报文调试功能，包括 DHCP 服务器收发的报文以及用于检测的 ping 报文的发送和响应情况。

【描述】

debugging dhcp server 命令用来使能 DHCP 服务器的调试功能。**undo debugging dhcp server** 命令用来禁止调试功能。

缺省情况下，DHCP 服务器的调试功能是禁止的。

【举例】

使能 DHCP 服务器的事件调试功能。

```
<H3C> debugging dhcp server event
*0.62496500-DHCP SER-8-DHCPS_DEBUG_COMMON:
DhcpServer: ICMP Timeout
*0.62496583-DHCP SER-8-DHCPS_DEBUG_COMMON:
DhcpServer: Still Need to ICMP detect for 1 times
*0.62497000-DHCP SER-8-DHCPS_DEBUG_COMMON:
DhcpServer: ICMP Timeout
*0.62497083-DHCP SER-8-DHCPS_DEBUG_COMMON:
DhcpServer: All Try finished
*0.62497166-DHCP SER-8-DHCPS_DEBUG_COMMON:
DhcpServer: Ack User's Lease
```

使能 DHCP 服务器的报文调试功能。

```
<H3C> debugging dhcp server packet
*0.62080906-DHCP SER-8-DHCPS_DEBUG_COMMON:
DhcpServer: receive DHCPRELEASE from 00.05.5D.85.D5.45.
*0.62081016-DHCP SER-8-DHCPS_DEBUG_COMMON:
DhcpServer: Release Lease for MAC 00.05.5D.85.D5.45. IP is 5.5.5.2
*0.62082240-DHCP SER-8-DHCPS_DEBUG_COMMON:
DhcpServer: receive DHCPDISCOVER from 00.05.5D.85.D5.45.
*0.62082350-DHCP SER-8-DHCPS_DEBUG_COMMON:
DhcpServer: Sending ICMP ECHO to Target IP: 5.5.5.2
*0.62082733-DHCP SER-8-DHCPS_DEBUG_COMMON:
DhcpServer: Sending ICMP ECHO to Target IP: 5.5.5.2
*0.62083233-DHCP SER-8-DHCPS_DEBUG_COMMON:
DhcpServer: Send DHCPOFFER to MAC=> 00.05.5D.85.D5.45. Offer IP=> 5.5.5.2
*0.62083366-DHCP SER-8-DHCPS_DEBUG_COMMON:
DhcpServer: receive DHCPREQUEST from 00.05.5D.85.D5.45.
*0.62083483-DHCP SER-8-DHCPS_DEBUG_COMMON:
DhcpServer: Send DHCPACK to MAC=> 00.05.5D.85.D5.45. Offer IP=> 5.5.5.2
```

使能 DHCP 服务器的错误调试功能。

```
<H3C> debugging dhcp server error
*0.63269475-DHCP SER-8-DHCPS_DEBUG_COMMON:
DhcpServer: Icmp Packet is not EHHOREPLY!
```

5.2.4 dhcp server accounting domain（系统视图）

【命令】

dhcp server accounting domain *domain-name* { **interface** *ethernet-subinterface-range* | **all** }

undo dhcp server accounting domain { **interface** *ethernet-subinterface-range* | **all** }

【视图】

系统视图

【参数】

domain-name：DHCP 服务器计费所使用的域。注意该域必须配置为 RADIUS 方案。

ethernet-subinterface-range：用关键字“to”连接两个子接口，表示子接口号在两个接口之间的所有子接口（包含这两个子接口）。

all：表示所有接口。

【描述】

dhcp server accounting domain interface 命令用来针对指定接口地址池中的地址启动 DHCP 计费功能，并配置 DHCP 计费所使用的域。**undo dhcp server accounting domain interface** 命令用来关闭针对指定接口地址池中的地址的 DHCP 计费功能。

缺省情况下，未配置 DHCP 计费功能。

本命令配置后不能通过 **display current-configuration** 查看，它是通过循环执行 **dhcp server accounting domain** 命令实现批量配置。

相关配置可参考命令 **accounting domain**。

【举例】

针对 Ethernet2/0/0.1 到 Ethernet2/0/0.5 之间的接口地址池中的地址启动 DHCP 计费功能，并将 radius_domain 指定为 DHCP 计费的域。

```
[H3C] dhcp server accounting domain radius_domain interface ethernet 2/0/0.1
to ethernet 2/0/0.5
```

5.2.5 dhcp server accounting domain（接口视图）

【命令】

dhcp server accounting domain *domain-name*

undo dhcp server accounting domain

【视图】

接口视图

【参数】

domain-name：DHCP 服务器计费所使用的域。注意该域必须配置为 RADIUS 方案。

【描述】

dhcp server accounting domain 命令用来针对接口地址池中的地址启动 DHCP 计费功能，并配置 DHCP 计费所使用的域。**undo dhcp server accounting domain** 命令用来关闭针对该接口地址池中地址的 DHCP 计费功能。

缺省情况下，未配置 DHCP 计费功能。

相关配置可参考命令 **accounting domain**。

【举例】

针对本接口地址池中的地址启动 DHCP 计费功能，并将 radius_domain 指定为 DHCP 计费的域。

```
[H3C-Ethernet0/0/0] dhcp server accounting domain radius_domain
```

5.2.6 dhcp server bims-server （接口视图）

【命令】

dhcp server bims-server ip *ip-address* [**port** *port-number*] **sharekey** *key*

undo dhcp server bims-server

【视图】

接口视图

【参数】

ip *ip-address*：BIMS 服务器的 IP 地址。

port *port-number*：BIMS 服务器的协议端口号，范围为 1～65534。

sharekey *key*：BIMS 服务器的共享密钥，范围为 1～16 个字符。

【描述】

dhcp server bims-server 命令用来在当前接口 DHCP 地址池中启动并配置 BIMS option，**undo dhcp server bims-server** 命令用来在当前接口 DHCP 地址池中删除 BIMS option 配置。

缺省情况下，DHCP 服务器没有配置 BIMS option。

【举例】

配置 Ethernet1/0/0 的接口地址池的 BIMS option，BIMS 服务器 IP 地址为 192.168.1.1，协议端口号为 80，共享密钥为 abcdefg。

```
[H3C] interface ethernet 1/0/0
[H3C-Ethernet1/0/0] dhcp server bims-server ip 192.168.1.1 port 80 sharekey
abcdefg
```

5.2.7 dhcp server bims-server （系统视图）

【命令】

dhcp server bims-server ip *ip-address* [**port** *port-number*] **sharekey** *key* { **interface** *interface-type interface-number* [**to** *interface-type interface-number*] | **all** }

undo dhcp server bims-server { **interface** *interface-type interface-number* [**to** *interface-type interface-number*] | **all** }

【视图】

系统视图

【参数】

ip *ip-address*：BIMS 服务器的 IP 地址。

port *port-number*：BIMS 服务器的协议端口号，范围为 1～65534。

sharekey *key*：BIMS 服务器的共享密钥，范围为 1～16 个字符。

interface-type interface-number [**to** *interface-type interface-number*]：用关键字“to”连接两个子接口，表示在两个子接口之间的所有子接口（包含这两个子接口）。该接口必须为以太网接口。

all：表示所有配置了接口地址池的接口。

【描述】

dhcp server bims-server 命令用来在 DHCP 服务器上配置了接口地址池的接口上启动并配置 BIMS option。**undo dhcp server bims-server** 命令用来在 DHCP 服务器上配置了接口地址池的接口上删除 BIMS option 配置。

在 DHCP 服务器上配置了支持 BIMS option 后，DHCP 服务器将会在返回给 DHCP 客户端的 DHCP_OFFER 以及 DHCP_ACK 回应报文中均携带 BIMS option。

在指定的配置了接口地址池的接口上启动 BIMS option 后，DHCP 服务器在给客户分配该接口地址池中的地址时将携带 BIMS option，若在 **dhcp server bims-server** 命令中配置了 **all** 关键字，则在所有配置的接口地址池中启动 BIMS option。

缺省情况下，DHCP 服务器没有配置 BIMS option。

【举例】

在配置了接口地址池的以太网接口 Ethernet0/0/0 上配置 BIMS option，BIMS 服务器 IP 地址为 192.168.1.1，协议端口号为 80，共享密钥为 abcdefg。

```
[H3C] dhcp server bims-server ip 192.168.1.1 port 80 sharekey abcdefg interface ethernet0/0/0
```

5.2.8 dhcp server dns-list （接口视图）

【命令】

dhcp server dns-list *ip-address* [*ip-address*]

undo dhcp server dns-list { *ip-address* | **all** }

【视图】

接口视图

【参数】

ip-address：DNS 的 IP 地址，一条命令中最多可以配置 8 个 IP 地址，用空格分隔。

【描述】

dhcp server dns-list 命令是用于在配置了单个接口的 DHCP 地址池的情况下，为 DHCP 客户端指定 DNS 服务器的 IP 地址，**undo dhcp server dns-list** 命令用来删除配置。

缺省情况下，未配置 DNS 地址。

在目前的实现中，每个 DHCP 地址池最多可以设置 8 个 DNS 服务器地址。

相关配置可参考命令 **dhcp server dns-list interface**，**dhcp server ip-pool** 和 **dns-list**。

【举例】

为 Ethernet1/0/0 的接口 DHCP 地址池指定 DNS 服务器的地址为 1.1.1.254。

```
[H3C] interface ethernet 1/0/0
[H3C-Ethernet 1/0/0] dhcp server dns-list 1.1.1.254
```

5.2.9 dhcp server dns-list（系统视图）

【命令】

dhcp server dns-list *ip-address* [*ip-address*] { **interface** *ethernet-subinterface-range* | **all** }

undo dhcp server dns-list { *ip-address* | **all** } { **interface** *ethernet-subinterface-range* | **all** }

【视图】

系统视图

【参数】

ip-address：DNS 服务器的 IP 地址，一条命令中最多可以配置 8 个 IP 地址，用空格分隔。

ethernet-subinterface-range：用关键字“**to**”连接两个子接口，表示子接口号在两个接口之间的所有子接口（包含这两个子接口）。

all：**undo** 命令中的前一个“all”表示所有网关地址，后一个表示所有接口。

【描述】

dhcp server dns-list interface 命令是用于配置指定范围的接口 DHCP 地址池的 DNS 服务器的 IP 地址，**undo dhcp server dns-list interface** 命令用来删除分配的 IP 地址。

缺省情况下，未配置 DNS 地址。

在目前的实现中，每个 DHCP 地址池最多可以设置 8 个 DNS 服务器地址。

相关配置可参考命令 **dhcp server dns-list**，**dhcp server ip-pool** 和 **dns-list**。

【举例】

为 Ethernet2/0/0.0 到 Ethernet2/0/0.5 的接口 DHCP 地址池指定 DNS 服务器的地址为 1.1.1.254。

```
[H3C] dhcp server dns-list 1.1.1.254 interface ethernet 2/0/0.0 to ethernet 2/0/0.5
```

5.2.10 dhcp server domain-name（接口视图）

【命令】

dhcp server domain-name *domain-name*

undo dhcp server domain-name

【视图】

接口视图

【参数】

domain-name：DHCP 服务器分配给客户机的域名，字符串形式，长度为 3～50。

【描述】

dhcp server domain-name 命令用来配置 DHCP 服务器当前接口的 DHCP 地址池分配给客户端的域名，**undo dhcp server domain-name** 命令用来删除分配的域名。

缺省情况下，未配置分给 DHCP 客户端的域名，域名为空。

相关配置可参考命令 **dhcp server ip-pool**，**dhcp server domain-name interface** 和 **domain-name**。

【举例】

将 h3c.com.cn 设为接口 DHCP 地址池的域名。

```
[H3C] interface ethernet 1/0/0
[H3C-Ethernet1/0/0] dhcp server domain-name h3c.com.cn
```

5.2.11 dhcp server domain-name（系统视图）

【命令】

dhcp server domain-name *domain-name* { **interface** *ethernet-subinterface-range* | **all** }

undo dhcp server domain-name { **interface** *ethernet-subinterface-range* | **all** }

【视图】

系统视图

【参数】

domain-name：DHCP 服务器分配给客户机的域名，字符串形式，长度为 3～50。

ethernet-subinterface-range：用关键字“**to**”连接两个子接口，表示子接口号在两个接口之间的所有子接口（包含这两个子接口）。

all：表示所有接口。

【描述】

dhcp server domain-name 命令用来配置指定范围的接口的地址池分配给 DHCP 客户端的域名，**undo dhcp server domain-name** 命令用来删除分配给 DHCP 客户端的域名。

缺省情况下，未配置 DHCP 客户端的域名。

本命令配置后不能通过 **display current-configuration** 查看，它是通过在指定接口上分别执行 **dhcp server domain-name** 命令实现批量配置。

相关配置可参考命令 **dhcp server ip-pool**。

【举例】

将 eth2_1_5.com.cn 设为 Ethernet2/0/0.1 到 Ethernet2/0/0.5 之间的接口 DHCP 地址池的域名。

```
[H3C] dhcp server domain-name eth1_1_5.com.cn interface ethernet 2/0/0.1 to
ethernet 2/0/0.5
```

5.2.12 dhcp server expired （接口视图）

【命令】

dhcp server expired { **day** *day* [**hour** *hour* [**minute** *minute*]] | **unlimited** }

undo dhcp server expired

【视图】

接口视图

【参数】

day *day*：天数，取值范围为 0～365。

hour *hour*：小时数，取值范围为 0～23。

minute *minute*：分钟数，取值范围为 0～59。

unlimited：有效期限无限长。

【描述】

dhcp server expired 命令用来配置当前接口 DHCP 地址池中 IP 地址的租用有效期限，**undo dhcp server expired** 命令用来恢复缺省设置。

缺省情况下，有效期限为 1 天。

相关配置可参考命令 **dhcp server ip-pool**，**dhcp server expired interface** 和 **expired**。

【举例】

配置 Ethernet1/0/0 的接口地址池的 IP 地址租用有效期无限长。

```
[H3C] interface ethernet 1/0/0
[H3C-Ethernet 1/0/0] dhcp server expired unlimited
```

5.2.13 dhcp server expired（系统视图）

【命令】

dhcp server expired { **day** *day* [**hour** *hour* [**minute** *minute*]] | **unlimited** } { **interface** *ethernet-subinterface-range* | **all** }

undo dhcp server expired { **interface** *ethernet-subinterface-range* | **all** }

【视图】

系统视图

【参数】

day *day*：天数，取值范围为 0～365。

hour *hour*：小时数，取值范围为 0～23。

minute *minute*：分钟数，取值范围为 0～59。

unlimited：有效期限无限长。

ethernet-subinterface-range：用关键字“**to**”连接两个子接口，表示子接口号在两个子接口之间的所有子接口（包含这两个子接口）。

all：所有接口。

【描述】

dhcp server expired interface 命令用来配置指定范围的接口 DHCP 地址池中 IP 地址的租用有效期限，**undo dhcp server expired interface** 命令用来恢复缺省设置。

缺省情况下，有效期限为 1 天。

本命令配置后，不能使用 **display current-configuration** 命令查看，实际执行时，通过循环调用 **dhcp server expired** 命令实现批量配置。

相关配置可参考命令 **dhcp server ip-pool**，**dhcp server expired** 和 **expired**。

【举例】

配置 Ethernet2/0/0.1 到 Ethernet2/0/0.5 之间的接口地址池的 IP 地址租用有效期无限长。

```
[H3C] dhcp server expired unlimited interface ethernet 2/0/0.1 to ethernet 2/0/0.5
```

5.2.14 dhcp server forbidden-ip

【命令】

dhcp server forbidden-ip *low-ip-address* [*high-ip-address*]

undo dhcp server forbidden-ip *low-ip-address* [*high-ip-address*]

【视图】

系统视图

【参数】

low-ip-address：不参与自动分配的最小 IP 地址。

high-ip-address：不参与自动分配的最大 IP 地址，应与 *low-ip-address* 在同一网段，并且不能小于 *low-ip-address*。如果不指定该参数，表示只有一个 IP 地址，即 *low-ip-address*。

【描述】

dhcp server forbidden-ip 命令用来配置 DHCP 地址池中不参与自动分配的 IP 地址范围，**undo dhcp server forbidden-ip** 命令用来删除指定的不参与自动分配的 IP 地址范围。

缺省情况下，地址池中所有 IP 地址都参与自动分配。

多次执行本命令，可以配置多个不参与自动分配的 IP 地址段。

相关配置可参考命令 **dhcp server ip-pool**，**network** 和 **static-bind ip-address**。

【举例】

将 10.110.1.1 到 10.110.1.63 之间的 IP 地址保留，不参与地址自动分配。

```
[H3C] dhcp server forbidden-ip 10.110.1.1 10.110.1.63
```

5.2.15 dhcp server ip-pool

【命令】

dhcp server ip-pool *pool-name*

undo dhcp server ip-pool *pool-name*

【视图】

系统视图

【参数】

pool-name：地址池名称，是地址池的唯一标识，字符串形式，长度为 1～35。

【描述】

dhcp server ip-pool 命令用来创建 DHCP 地址池并进入 DHCP 地址池视图，**undo dhcp server ip-pool** 命令用来删除指定的地址池。

缺省情况下，未创建 DHCP 地址池。

执行 **dhcp server ip-pool** 命令时，如果指定的地址池已经存在，则直接进入 DHCP 地址池视图；否则先创建这样的地址池，再进入 DHCP 地址池视图。每个 DHCP 服务器可以配置多个地址池，目前支持 128 个全局地址池。

DHCP Server 地址池中的子网网段地址和子网广播地址不参与地址的分配。

相关配置可参考命令 **dhcp enable**，**expired** 和 **network**。

【举例】

创建标识为 0 的 DHCP 地址池。

```
[H3C] dhcp server ip-pool 0
[H3C-dhcp-pool-0]
```

5.2.16 dhcp server nbns-list （系统视图）

【命令】

dhcp server nbns-list *ip-address* [*ip-address*] { **interface** *ethernet-subinterface-range* | **all** }

undo dhcp server nbns-list { *ip-address* | **all** } { **interface** *ethernet-subinterface-range* | **all** }

【视图】

系统视图

【参数】

ip-address：NetBIOS 服务器的 IP 地址，一条命令中最多可以配置 8 个 IP 地址，用空格分隔。

all：**undo** 命令中的前一个 **all** 表示所有 NetBIOS 服务器的 IP 地址；后一个 **all** 表示所有接口。

ethernet-subinterface-range：用关键字“**to**”连接两个子接口，表示子接口号在两个子接口之间的所有子接口（包含这两个子接口）。

【描述】

dhcp server nbns-list interface 命令用来配置指定一定范围的接口地址池的 NetBIOS 服务器地址，**undo dhcp server nbns-list interface** 命令用来删除配置。

缺省情况下，未配置 NetBIOS 服务器的地址。

在目前的实现中，每个 DHCP 地址池最多可以配置 8 个 NetBIOS 服务器 IP 地址。

本命令配置后，不能通过 **display current-configuration** 查看配置，该命令的执行是通过循环调用 **dhcp server nbns-list** 实现的。

相关配置可参考命令 **dhcp server ip-pool**，**nbns-list**，**dhcp server nbns-list** 和 **netbios-type**。

【举例】

配置 Ethernet2/0/0.1 到 Ethernet2/0/0.5 之间的接口地址池为其客户端分配的 NetBIOS 服务器地址为 10.12.1.99。

```
[H3C] dhcp server nbns-list 10.12.1.99 interface ethernet 2/0/0.1 to ethernet 2/0/0.5
```

5.2.17 dhcp server nbns-list（接口视图）

【命令】

dhcp server nbns-list *ip-address* [*ip-address*]

undo dhcp server nbns-list { *ip-address* | **all** }

【视图】

接口视图

【参数】

ip-address：NetBIOS 服务器的 IP 地址，一条命令中最多可以配置 8 个 IP 地址，用空格分隔。

all：所有 NetBIOS 服务器的 IP 地址。

【描述】

dhcp server nbns-list 命令用来配置当前接口的 DHCP 地址池为其客户端分配的 NetBIOS 服务器地址，**undo dhcp server nbns-list** 命令用来删除配置。

缺省情况下，未配置 NetBIOS 服务器的地址。

在目前的实现中，每个 DHCP 地址池最多可以配置 8 个 NetBIOS 服务器。

相关配置可参考命令 **dhcp server ip-pool**，**dhcp server nbns-list interface**，**nbns-list** 和 **netbios-type**。

【举例】

配置 Ethernet1/0/0 的 DHCP 地址池为其客户端分配的 NetBIOS 服务器地址为 10.12.1.99。

```
[H3C] interface ethernet 1/0/0
[H3C-Ethernet 1/0/0] dhcp server nbns-list 10.12.1.99
```

5.2.18 dhcp server netbios-type（接口视图）

【命令】

dhcp server netbios-type { **b-node** | **h-node** | **m-node** | **p-node** }

undo dhcp server netbios-type

【视图】

接口视图

【参数】

b-node：广播模式（broadcast），即采用广播的方式获取主机名和 IP 地址之间的映射。

p-node：端对端模式（peer-to-peer），即采用与 NetBIOS 服务器通信的方式来获取映射关系。

m-node：混合 m 模式（mixed），即具备“端对端”通信机制的 b 类节点。

h-node：混合 h 模式（hybrid），即具有部分广播特性的 p 类节点。

【描述】

dhcp server netbios-type 命令用来配置当前接口地址池的 DHCP 客户端 NetBIOS 节点类型，**undo dhcp server netbios-type** 命令用来恢复缺省设置。

缺省情况下，客户端采用 h 类节点（**h-node**）。

DHCP 客户端在广域网上使用 NetBIOS 协议时，需要在主机名和 IP 地址之间建立映射关系。

相关配置可参考命令 **dhcp server ip-pool**，**netbios-type**，**dhcp server netbios-type interface** 和 **nbns-list**。

【举例】

配置 Ethernet1/0/0 的 DHCP 地址池为其客户端分配的 NetBIOS 节点类型为 p-node。

```
[H3C] interface ethernet 1/0/0
[H3C-Ethernet1/0/0] dhcp server netbios-type p-node
```

5.2.19 dhcp server netbios-type（系统视图）

【命令】

dhcp server netbios-type { **b-node** | **h-node** | **m-node** | **p-node** } { **interface** *ethernet-subinterface-range* | **all** }

undo dhcp server netbios-type { **interface** *ethernet-subinterface-range* | **all** }

【视图】

系统视图

【参数】

b-node：广播模式（broadcast），即采用广播的方式获取主机名和 IP 地址之间的映射。

p-node：端对端模式（peer-to-peer），即采用与 NetBIOS 服务器通信的方式来获取映射关系。

m-node：混合 m 模式（mixed），即具备“端对端”通信机制的 b 类节点。

h-node：混合 h 模式（hybrid），即具有部分广播特性的 p 类节点。

ethernet-subinterface-range：用关键字“**to**”连接两个子接口，表示子接口号在两个子接口之间的所有子接口（包含这两个子接口）。

all：表示所有接口。

【描述】

dhcp server netbios-type 命令用来配置指定接口范围的接口地址池的 DHCP 客户端 NetBIOS 节点类型，**undo dhcp server netbios-type** 命令用来恢复缺省设置。

缺省情况下，客户端采用 h 类节点（**h-node**）。

DHCP 客户端在广域网上使用 NetBIOS 协议时，需要在主机名和 IP 地址之间建立映射关系。

该命令配置后，不能通过 **display current-configuration** 命令查看配置情况，它的执行是通过循环调用 **dhcp server netbios-type** 命令实现的。

相关配置可参考命令 **dhcp server ip-pool**，**netbios-type**，**dhcp server netbios-type** 和 **nbns-list**。

【举例】

配置 Ethernet2/0/0.1 到 Ethernet2/0/0.5 之间的接口地址池为其客户端分配的 NetBIOS 节点类型为 p-node。

```
[H3C] dhcp server netbios-type p-node interface ethernet 2/0/0.1 to ethernet 2/0/0.5
```

5.2.20 dhcp server option（系统视图）

【命令】

dhcp server option *code* { **ascii** *ascii-string* | **hex** *hex-string* | **ip-address** *ip-address* } { **interface** *ethernet-subinterface-range* | **all** }

undo dhcp server option *code* { **interface** *ethernet-subinterface-range* | **all** }

【视图】

系统视图

【参数】

code：用户定义的选项 option 的数值，范围为 2～254 之间，其中 3、6、15、44、46、50～55、57～61、184 和 217 被系统保留使用。

ascii *ascii-string*：ASCII 字符串，长度为 1～63 个字符。

hex *hex-string*：16 进制数字串，最大长度为 128 个字符，可以 aa、aabb、aabb12 或 aabb1234 的形式进行输入。

ip-address *ip-address*：IP 地址，最多可以配置 8 个。

ethernet-subinterface-range：用关键字“**to**”连接两个子接口，表示子接口号在两个子接口之间的所有子接口（包含这两个子接口）。

all：所有接口。

【描述】

dhcp server option interface 命令用来配置指定范围内的接口地址池的 DHCP 自定义选项，**undo dhcp server option interface** 命令用来删除配置。

该命令配置后，不能通过 **display current-configuration** 命令查看配置情况，它的执行是通过循环调用 **dhcp server option** 命令实现的。

相关配置可参考命令 **dhcp server option** 和 **option**。

【举例】

为 Ethernet2/0/0.1 到 Ethernet2/0/0.5 之间的接口 DHCP 地址池定义 code 为 100 的 16 进制数字为 0x11 和 0x22。

```
[H3C] dhcp server option 100 hex 11 22 interface ethernet 2/0/0.1 to ethernet 2/0/0.5
```

5.2.21 dhcp server option（接口视图）

【命令】

dhcp server option *code* { **ascii** *ascii-string* | **hex** *hex-string* | **ip-address** *ip-address* }

undo dhcp server option *code*

【视图】

接口视图

【参数】

code：用户定义的选项 option 的数值，范围为 2～254 之间，其中 3、6、15、44、46、50～55、57～61、184 和 217 被系统保留使用。

ascii *ascii-string*：ASCII 字符串，长度为 1～63 个字符。

hex *hex-string*：16 进制数字串，最大长度为 128 个字符，可以 aa、aabb、aabb12 或 aabb1234 的形式进行输入。

ip-address *ip-address*：IP 地址，最多可以配置 8 个。

【描述】

dhcp server option 命令用来配置当前接口的 DHCP 地址池的自定义选项，**undo dhcp server option** 命令用来删除配置。

相关配置可参考命令 **option** 和 **dhcp server option interface**。

【举例】

为 Ethernet1/0/0 的 DHCP 地址池定义 code 为 100 的 16 进制数字为 0x11 和 0x22。

```
[H3C] interface ethernet 1/0/0
[H3C-Ethernet1/0/0] dhcp server option 100 hex 11 22
```

5.2.22 dhcp server ping

【命令】

dhcp server ping { **packets** *number* | **timeout** *milliseconds* }

undo dhcp server ping { **packets** | **timeout** }

【视图】

系统视图

【参数】

packets *number*：发送 ping 报文的最大数目，取值范围是 0～10，0 表示不进行 ping 操作，缺省值为 2。

timeout *milliseconds*：每个 ping 报文的最长等待回应时间，单位是毫秒，取值范围是 0～10000，缺省值为 500 毫秒。

【描述】

dhcp server ping 命令用来配置 DHCP 服务器发送 ping 报文的最大数量和最长等待回应时间，**undo dhcp server ping** 命令用来恢复缺省值。

DHCP 服务器通过发送 ping 报文探测地址的使用情况，以防止 IP 地址的重复分配导致地址冲突。

【举例】

设置 DHCP 服务器最多发送 10 个 ping 数据包，等待时间采用缺省值 500ms。

```
[H3C] dhcp server ping packets 10
```

5.2.23 dhcp server static-bind

【命令】

dhcp server static-bind ip-address *ip-address* { **mac-address** *mac-address* | **client-identifier** *client-identifier* }

undo dhcp server static-bind { **ip-address** *ip-address* | **mac-address** *mac-address* | **client-identifier** *client-identifier* }

【视图】

接口视图

【参数】

ip-address：静态绑定的 IP 地址。必须是当前接口地址池中的合法 IP 地址。

mac-address：静态绑定的 MAC 地址。

client-identifier：待绑定的主机 ID。

【描述】

dhcp server static-bind 命令用来配置当前接口的 DHCP 地址池中地址的静态绑定，**undo dhcp server static-bind** 命令用来删除配置。

缺省情况下，接口地址池中没有配置静态地址捆绑。

在一个接口的所有静态绑定中，IP 地址和 MAC 地址/identifier 必须是唯一的。

每个 MAC 地址或 identifier 只能与一个 IP 地址进行绑定。

【举例】

将 MAC 地址为 0000-e03f-0305 与 IP 地址 10.1.1.1 进行静态绑定。

```
[H3C-Ethernet1/0/0] dhcp server static-bind ip-address 10.1.1.1 mac-address
0000-e03f-0305
```

5.2.24 dhcp server voice-config（接口视图）

【命令】

dhcp server voice-config { **ncp-ip** *ip-address* | **as-ip** *ip-address* | **voice-vlan** *vlan-id* { **enable** | **disable** } | **fail-over** *ip-address dialer-string* }

undo dhcp server voice-config [**ncp-ip** | **as-ip** | **voice-vlan** | **fail-over**]

【视图】

接口视图

【参数】

ncp-ip：Network Call Processor IP Address，网络呼叫处理器的 IP 地址。

as-ip：Alternate Server IP Address，备选 NCP 服务器的 IP 地址

voice-vlan：语音 VLAN。

fail-over：Fail-Over 呼叫路由。

ip-address：NCP、Alternate 服务器或 Fail-Over 的 IP 地址。

vlan-id：语音 VLAN 的 ID，取值范围为 1～4094。

enable：VLAN 处于使能状态。

disable：VLAN 处于非使能状态。

dialer-string：Fail-Over 拨号串，取值为 0～9 及通配符“*”。

【描述】

dhcp server voice-config 命令用来配置 DHCP 服务器从当前接口地址池中分配地址时携带 option 184 及其子选项。**undo dhcp server voice-config** 命令用来禁止 DHCP 服务器从当前接口地址池中分配地址时携带 option 184 及其子选项。

只有当 DHCP 客户端请求了 option 184 后，DHCP 服务器才回应 option 184 及相应的子选项。

在配置其它子选项前必需先配置 **ncp-ip** 子选项，否则其它选项将不生效。

缺省情况下 DHCP 服务器不支持 option 184 及其子选项。

相关配置可参考命令 **voice-config**。

【举例】

在接口 Ethernet0/0/1 上配置 DHCP 服务器支持 option 184 的所有子选项：NCP-IP 地址为 1.1.1.1，Alternate Server IP 地址为 2.2.2.2，Voice VLAN 为使能状态，ID 为 1，Fail-Over IP 地址为 3.3.3.3，拨号串为 99*。

```
[H3C] interface Ethernet 0/0/1
[H3C-Ethernet0/0/1] dhcp select interface
[H3C-Ethernet0/0/1] dhcp server voice-config ncp-ip 1.1.1.1
[H3C-Ethernet0/0/1] dhcp server voice-config as-ip 2.2.2.2
[H3C-Ethernet0/0/1] dhcp server voice-config voice-vlan 1 enable
[H3C-Ethernet0/0/1] dhcp server voice-config fail-over 3.3.3.3 99*
```

5.2.25 dhcp server voice-config（系统视图）

【命令】

dhcp server voice-config { **ncp-ip** *ip-address* | **as-ip** *ip-address* | **voice-vlan** *vlan-id* { **enable** | **disable** } | **fail-over** *ip-address dialer-string* } { **all** | **interface** *interface-type interface-number* [**to** *interface-type interface-number*] }

undo dhcp server voice-config [**ncp-ip** | **as-ip** | **voice-vlan** | **fail-over**] { **all** | **interface** *interface-type interface-number* [**to** *interface-type interface-number*] }

【视图】

系统视图

【参数】

ncp-ip：Network Call Processor IP Address，网络呼叫处理器的 IP 地址。

as-ip：Alternate Server IP Address，备选 NCP 服务器的 IP 地址

voice-vlan：语音 VLAN。

fail-over：Fail-Over 呼叫路由。

ip-address：NCP、Alternate 服务器或 Fail-Over 的 IP 地址。

vlan-id：语音 VLAN 的 ID，取值范围为 1～4094。

enable：VLAN 处于使能状态。

disable：VLAN 出于非使能状态。

dialer-string：Fail-Over 拨号串，取值为 0～9 及通配符“*”。

all：表示所有的接口。

interface-type interface-number [**to** *interface-type interface-number*]：用关键字“**to**”连接两个子接口，表示接口号在两个接口之间的所有接口（包含这两个接口）。该接口必须为以太网接口（或子接口）。

【描述】

dhcp server voice-config interface 命令用来配置 DHCP 服务器从指定接口地址池中分配地址时携带 option 184 及其子选项。**undo dhcp server voice-config interface** 命令用来禁止 DHCP 服务器从指定接口地址池中分配地址时携带 option 184 及其子选项。

只有当 DHCP 客户端请求了 option 184 后，DHCP 服务器才回应 option 184 及相应的子选项。

在配置其它子选项前必需先配置 **ncp-ip** 子选项，否则其它选项将不生效。

缺省情况下，DHCP 服务器不支持 option 184 及其子选项。

相关配置可参考命令 **voice-config**。

【举例】

在接口 ethernet0/0/1 上配置 DHCP 服务器支持 option 184 的所有子选项：NCP-IP 地址为 1.1.1.1，Alternate Server IP 地址为 2.2.2.2，Voice VLAN 为使能状态，ID 为 1，Fail-Over IP 地址为 3.3.3.3，拨号串为 99*。

```
[H3C] dhcp select interface ethernet 0/0/1
[H3C] dhcp server voice-config ncp-ip 1.1.1.1 interface ethernet 0/0/1
[H3C] dhcp server voice-config as-ip 2.2.2.2 interface ethernet 0/0/1
[H3C] dhcp server voice-config voice-vlan 1 enable interface ethernet 0/0/1
[H3C] dhcp server voice-config fail-over 3.3.3.3 99* interface ethernet 0/0/1
```

5.2.26 display dhcp server conflict

【命令】

display dhcp server conflict { **ip** *ip-address* | **all** }

【视图】

所有视图

【参数】

ip-address：指定 IP 地址。

all：表示所有 IP 地址。

【描述】

display dhcp server conflict 命令用来查看 DHCP 的地址冲突的统计信息，包括冲突 IP 地址、冲突检测类型、地址冲突发生的时间等。

相关配置可参考命令 **reset dhcp server conflict**。

【举例】

查看 DHCP 的地址冲突的统计信息。

```
<H3C> display dhcp server conflict all
    Address             Discover Time
    10.110.1.2          Jan 11 2003 11:57: 7 PM
```

表5-1 display dhcp server conflict 命令显示信息说明

主要字段	解释
Address	发生冲突的 IP 地址
Discover Time	检测到冲突的时间

5.2.27 display dhcp server expired

【命令】

display dhcp server expired { **ip** *ip-address* | **pool** [*pool-name*] | **interface** [*interface-type interface-number*] | **all** }

【视图】

所有视图

【参数】

ip-address：指定 IP 地址。

pool-name：全局地址池的名称，不指定地址池名则表示所有全局地址池。

interface-type interface-number：指定接口的地址池，不指定接口名则表示所有的接口地址池。

all：表示所有地址。

【描述】

display dhcp server expired 命令用来查看 DHCP 地址池中已经超期的租约，在一定条件下这类租约的地址将被分配给其它 DHCP 客户端。

【举例】

查看 DHCP 地址池的超期租约信息。

```
<H3C> display dhcp server expired all
Global pool:
 IP address     Client-identifier/        Lease expiration        Type
                Hardware address

Interface pool:
 IP address     Client-identifier/        Lease expiration        Type
                Hardware address

 --- total 0 entry ---
```

表5-2 display dhcp server expired 命令显示信息说明

主要字段	解释
Global pool:	全局地址池的超期租约信息
Interface pool:	接口地址池的超期租约信息
IP address	绑定的 IP 地址
Client-identifier/Hardware address	绑定的 MAC 地址或 identifier

主要字段	解释
Lease expiration	租约到期的时间
Type	地址绑定的类型

5.2.28 display dhcp server free-ip

【命令】

display dhcp server free-ip

【视图】

所有视图

【参数】

无

【描述】

display dhcp server free-ip 命令用来查看 DHCP 地址池的空闲的地址范围，即尚未分配的 IP 地址信息。

【举例】

查看 DHCP 地址池的空闲的地址范围。

```
<H3C> display dhcp server free-ip
IP Range from 1.0.0.0             to  2.2.2.1
IP Range from 2.2.2.3             to  2.255.255.255
IP Range from 4.0.0.0             to  4.255.255.255
IP Range from 5.5.5.0             to  5.5.5.0
IP Range from 5.5.5.2             to  5.5.5.255
```

5.2.29 display dhcp server ip-in-use

【命令】

display dhcp server ip-in-use { **all** | **ip** *ip-address* | **pool** [*pool-name*] | **interface** [*interface-type interface-number*] }

【视图】

所有视图

【参数】

all：显示所有信息。

ip-address：显示特定 IP 地址的绑定信息。

pool-name：作用范围为指定的全局地址池，不指定地址池名时显示所有全局地址池的地址绑定信息。

interface-type interface-number：作用范围为指定的接口地址池，不指定接口名时显示所有接口地址池的地址绑定信息。

【描述】

display dhcp server ip-in-use 命令用来查看 DHCP 客户端的地址绑定信息，如硬件地址、IP 地址、地址租用期限等信息。

相关配置可参考命令 **reset dhcp server ip-in-use**。

【举例】

查看 DHCP 的地址绑定信息。

```
<H3C> display dhcp server ip-in-use all
Global pool:
 IP address     Client-identifier/        Lease expiration        Type
                Hardware address
 2.2.2.2        000f-1f7e-fec5            NOT Used                Manual

Interface pool:
 IP address   Client-identifier/    Lease expiration         Type
              Hardware address
 5.5.5.1      0050-ba28-930a        Jun  5 2003 10:56:7 AM   Auto:COMMITED

 --- total 2 entry ---
```

表5-3 display dhcp server ip-in-use 命令输出信息描述

主要字段	解释
Global pool	全局地址池的地址绑定信息
Interface pool	接口地址池的地址绑定信息
IP address	绑定的 IP 地址
Client-identifier/Hardware address	绑定的 MAC 地址或 identifier
Lease expiration	租约到期时间
Type	地址绑定的类型

5.2.30 display dhcp server statistics

【命令】

display dhcp server statistics

【视图】

所有视图

【参数】

无

【描述】

display dhcp server statistics 命令用来查看 DHCP 服务器的统计信息，包括 DHCP 地址池数目，自动、手工和过期绑定的地址数目，不可识别的报文数量、DHCP 请求和应答的报文数目统计等。

相关配置可参考命令 **reset dhcp server statistics**。

【举例】

查看 DHCP 服务器的统计信息。

```
<H3C> display dhcp server statistics
    Global Pool:
     Pool Number:            5
     Binding
      Auto:                  0
      Manual:                1
      Expire:                0
    Interface Pool:
     Pool Number:            1
     Binding
      Auto:                  1
      Manual:                0
      Expire:                0
    Boot Request:            6
     Dhcp Discover:          1
     Dhcp Request:           4
     Dhcp Decline:           0
     Dhcp Release:           1
     Dhcp Inform:            0
    Boot Reply:              4
     Dhcp Offer:             1
     Dhcp Ack:               3
```

```
 Dhcp Nak:                0
Bad Messages:             0
```

表5-4 display dhcp server statistics 命令输出信息描述

主要字段	解释
Global Pool:	全局地址池的统计信息
Interface Pool:	接口地址池的统计信息
Pool Number	地址池的数目
Auto	自动绑定的 IP 地址数
Manual	手工绑定的 IP 地址数
Expire	租约超期的 IP 地址数
Boot Request	DHCP 客户端发给 DHCP 服务器的消息数量
Dhcp Discover, Dhcp Request, Dhcp Decline, Dhcp Release, Dhcp Inform	收到的 DHCP 报文统计
Boot Reply	DHCP 服务器发给 DHCP 客户端的消息数量
Dhcp Offer, Dhcp Ack, Dhcp Nak	发送的 DHCP 报文统计
Bad Messages	错误的报文统计

5.2.31 display dhcp server tree

【命令】

display dhcp server tree { **pool** [*pool-name*] | **interface** [*interface-type interface-number*] | **all** }

【视图】

所有视图

【参数】

pool-name：全局地址池的名称，不指定地址池名则表示所有全局地址池。

interface-type interface-number：指定接口的地址池，不指定接口名则表示所有的接口地址池。

all：表示所有 DHCP 地址池。

【描述】

display dhcp server tree 命令用来查看 DHCP 地址池的树状结构信息，包括各节点的地址池、option 参数、地址租用期限、DNS 服务器的信息。

【举例】

查看 DHCP 地址池的树状结构信息。

```
<H3C> display dhcp server tree all
Global pool:
Pool name: 5
network 10.10.1.0  255.255.255.0
Child node:6
Sibling node:7
  option 1 ip-address 255.0.0.0
  expired Day 1 Hour 0 Minute 0
  option 58 hex 00 00 A8 C0
  option 59 hex 00 00 00 3C

Pool name: 6
static-bind ip-address 10.10.1.2  255.0.0.0
static-bind mac-address 1111.2222.3333
Parent node:5
  option 1 ip-address 255.255.0.0
  expired Day 1 Hour 0 Minute 0
  option 58 hex 00 00 A8 C0
  option 59 hex 00 00 00 3C

Pool name: 7
network 10.10.1.64  255.255.255.192
PrevSibling node:5
Sibling node:8
  option 1 ip-address 255.0.0.0

Pool name: 8
network 20.10.1.1  255.255.255.0
Child node:9
PrevSibling node:7
  option 1 ip-address 255.0.0.0
  gateway-list 2.2.2.2
  nbns-list 3.3.3.3
  netbios-type  m-node
  expired Day 2 Hour 0 Minute 0
  option 58 hex 00 01 51 80
  option 59 hex 00 00 00 3C

Pool name: 9
network 30.10.1.64  255.255.255.0
```

```
Parent node:8
  option 1 ip-address 255.0.0.0
  gateway-list 2.2.2.2
  dns-list 1.1.1.1
  domain-name 444444
  nbns-list 3.3.3.3
  netbios-type  m-node
  expired Day 2 Hour 0 Minute 0
  option 58 hex 00 01 51 80
  option 59 hex 00 00 00 3C

Interface pool:
Pool name: Ethernet1/0/0
  network 5.5.5.0 mask 255.255.255.0
  option 1 ip-address 255.255.255.0
  gateway-list 5.5.5.5
  expired Day 1 Hour 0 Minute 0
  option 58 hex 00 00 A8 C0
  option 59 hex 00 00 00 3C
```

表5-5 display dhcp server tree 命令输出信息描述

主要字段	解释
Global pool:	全局地址池信息
Interface pool:	接口地址池信息
Pool Name:	地址池名称
network	可分配的地址段范围
static-bind ip-address 10.10.1.2 255.0.0.0 static-bind mac-address 1111.2222.3333	静态绑定的 IP 地址和 MAC 地址
child node:6	此节点的子节点为地址池 6 在这一位置可能出现的节点类型包括： child node：此地址池的子节点（子网）地址池 parent node：此节点的父节点（自然网段）地址池 Sibling node：此节点的下一个兄弟节点（同一自然网段的其它子网）地址池。兄弟节点之间的顺序由配置的先后决定。 PrevSibling node：此节点的前一个兄弟节点
option	自定义的 DHCP 选项
expired	地址租约期限，包括天数、小时数、分钟数
gateway-list	为 DHCP 客户端分配的出口网关

主要字段	解释
dns-list	为 DHCP 客户端分配的 DNS 服务器
domain-name	为 DHCP 客户端指定的域名
nbns-list	为 DHCP 客户端分配的 NetBIOS 服务器
netbios-type	为 DHCP 客户端指定的 NetBIOS 节点类型

5.2.32 dns-list

【命令】

dns-list *ip-address* [*ip-address*]

undo dns-list { *ip-address* | **all** }

【视图】

DHCP 地址池视图

【参数】

ip-address：DNS 的 IP 地址，一条命令中最多可以配置 8 个 IP 地址，用空格分隔。

【描述】

dns-list 命令用来配置全局 DHCP 地址池分配给客户端的 DNS 服务器的 IP 地址，**undo dns-list** 命令用来删除配置。

缺省情况下，未配置 DNS 服务器地址。

在目前的实现中，每个 DHCP 地址池最多可以设置 8 个 DNS 服务器地址。

相关配置可参考命令 **dhcp server dns-list interface**，**dhcp server dns-list** 和 **dhcp server ip-pool**。

【举例】

为 DHCP 地址池 mypool 指定 DNS 服务器的地址为 1.1.1.254。

```
[H3C] dhcp server ip-pool mypool
[H3C-dhcp-pool-mypool] dns-list 1.1.1.254
```

5.2.33 domain-name

【命令】

domain-name *domain-name*

undo domain-name

【视图】

DHCP 地址池视图

【参数】

domain-name：DHCP 服务器分配给客户机的域名，字符串形式，长度为 3～50。

【描述】

domain-name 命令用来配置 DHCP 服务器的全局地址池分配给客户端的域名，**undo domain-name** 命令用来删除分配的域名。

缺省情况下，未配置分配给 DHCP 客户端的域名，域名为空。

相关配置可参考命令 **dhcp server ip-pool**，**dhcp server domain-name** 和 **dhcp server domain-name interface**。

【举例】

将 mydomain.com.cn 设定为 DHCP 地址池 mypool 的域名。

```
[H3C] dhcp server ip-pool mypool
[H3C-dhcp-pool-mypool] domain-name mydomain.com.cn
```

5.2.34 expired

【命令】

expired { **day** *day* [**hour** *hour* [**minute** *minute*]] | **unlimited** }

undo expired

【视图】

DHCP 地址池视图

【参数】

day *day*：天数，取值范围为 0～365。

hour *hour*：小时数，取值范围为 0～23。

minute *minute*：分钟数，取值范围为 0～59。

unlimited：有效期限无限长。

【描述】

expired 命令用来配置 DHCP 全局地址池中 IP 地址的租用有效期限，**undo expired** 命令用来恢复缺省设置。

缺省情况下，有效期限为 1 天。

相关配置可参考命令 **dhcp server ip-pool**，**dhcp server expired** 和 **dhcp server expired interface**。

【举例】

配置全局地址池 mypool 的 IP 地址租用有效期为 1 天 2 小时 3 分。

```
[H3C] dhcp server ip-pool mypool
[H3C-dhcp-pool-mypool] expired day 1 hour 2 minute 3
```

5.2.35 gateway-list

【命令】

gateway-list *ip-address* [*ip-address*]

undo gateway-list { *ip-address* | **all** }

【视图】

DHCP 地址池视图

【参数】

ip-address：出口网关的 IP 地址，一条命令中最多可以配置 8 个 IP 地址，用空格分隔。

all：所有出口网关 IP 地址。

【描述】

gateway-list 命令用来配置 DHCP 客户端使用的出口网关的 IP 地址，**undo gateway-list** 命令用来删除配置。

缺省情况下，未配置出口网关。

相关配置可参考命令 **dhcp server ip-pool** 和 **network**。

【举例】

将 DHCP 地址池 mypool 对应的出口网关设为 10.110.1.99。

```
[H3C] dhcp server ip-pool mypool
[H3C-dhcp-pool-mypool] gateway-list 10.110.1.99
```

5.2.36 nbns-list

【命令】

nbns-list *ip-address* [*ip-address*]

undo nbns-list { *ip-address* | **all** }

【视图】

DHCP 地址池视图

【参数】

ip-address：NetBIOS 服务器的 IP 地址，一条命令中最多可以配置 8 个 IP 地址，用空格分隔。

all：所有 NetBIOS 服务器的 IP 地址。

【描述】

nbns-list 命令用来配置全局 DHCP 地址池的客户端的 NetBIOS 服务器地址，**undo nbns-list** 命令用来删除分配的 NetBIOS 服务器地址。

缺省情况下，未配置 NetBIOS 地址。

在目前的实现中，每个 DHCP 地址池最多可以配置 8 个 NetBIOS 服务器。

相关配置可参考命令 **dhcp server ip-pool**，**dhcp server nbns-list**，**dhcp server nbns-list interface** 和 **netbios-type**。

【举例】

配置地址池 mypool 为它的客户端分配的 NetBIOS 服务器地址为 10.12.1.99。

```
[H3C] dhcp server ip-pool mypool
[H3C-dhcp-pool-mypool] nbns-list 10.12.1.99
```

5.2.37 netbios-type

【命令】

netbios-type { **b-node** | **h-node** | **m-node** | **p-node** }

undo netbios-type

【视图】

DHCP 地址池视图

【参数】

b-node：广播模式节点（broadcast），采用广播方式获取主机名和 IP 地址之间的映射。

p-node：端对端模式节点（peer-to-peer），采用与 NetBIOS 服务器通信的方式来获取映射关系。

m-node：混合 m 模式节点（mixed），是具备“端对端”通信机制的 b 类节点。

h-node：混合 h 模式节点（hybrid），是具有部分广播特性的 p 类节点。

【描述】

netbios-type 命令用来配置全局 DHCP 地址池的客户端的 NetBIOS 节点类型，**undo netbios-type** 命令用来恢复缺省设置。

缺省情况下，客户端采用 h 类节点（**h-node**）。

相关配置可参考命令 **dhcp server ip-pool**，**dhcp server netbios-type**，**dhcp server netbios-type interface** 和 **nbns-list**。

【举例】

将 DHCP 地址池 mypool 的客户端 NetBIOS 节点类型指定为 b-node。

```
[H3C] dhcp server ip-pool mypool
[H3C-dhcp-pool-mypool] netbios-type b-node
```

5.2.38 network

【命令】

network *ip-address* [**mask** *netmask*]

undo network

【视图】

DHCP 地址池视图

【参数】

ip-address：用于动态分配的 IP 地址池子网地址。

mask *netmask*：IP 地址池网络掩码，不指定该参数时表示采用自然掩码。

【描述】

network 命令用来配置动态分配的 IP 地址范围，**undo network** 命令用来删除配置。

缺省情况下，未配置动态分配的 IP 地址范围。

每个 DHCP 地址池只能配置一个网段，新的配置将覆盖原先的配置。如果系统需要多段地址，则应该使用多个地址池。

相关配置可参考命令 **dhcp server ip-pool** 和 **dhcp server forbidden-ip**。

【举例】

将 192.168.8.0/24 作为 DHCP 地址池 mypool 的地址空间。

```
[H3C-dhcp-pool-mypool] network 192.168.8.0 mask 255.255.255.0
```

5.2.39 option

【命令】

option *code* { **ascii** *ascii-string* | **hex** *hex-string* | **ip-address** *ip-address* }

undo option *code*

【视图】

DHCP 地址池视图

【参数】

code：用户定义的选项 option 的数值，范围为 2～254 之间，其中 3、6、15、44、46、50～55、57～61、184 和 217 被系统保留使用。

ascii *ascii-string*：ASCII 字符串，长度为 1～63 个字符。

hex *hex-string*：16 进制数字串，最大长度为 128 个字符，可以 aa、aabb、aabb12 或 aabb1234 的形式进行输入。

ip-address *ip-address*：IP 地址，最多可以配置 8 个。

【描述】

option 命令用来配置 DHCP 全局地址池的自定义选项，**undo option** 命令用来删除 DHCP 自定义选项。

随着 DHCP 的不断发展，新的可选参数（option）会陆续出现，为了支持这些新的选项，可以通过手工定义的方式将它们添加到 DHCP 服务器的属性列表中。

相关配置可参考命令 **dhcp server option** 和 **dhcp server option interface**。

【举例】

定义 code 为 100 的 16 进制数字为 0x11 和 0x22。

```
[H3C-dhcp-pool-mypool] option 100 hex 11 22
```

5.2.40 reset dhcp server conflict

【命令】

reset dhcp server conflict { **ip** *ip-address* | **all** }

【视图】

用户视图

【参数】

ip-address：指定 IP 地址。

all：所有地址池。

【描述】

reset dhcp server conflict 命令用来清除 DHCP 地址冲突的统计信息。

相关配置可参考命令 **display dhcp server conflict**。

【举例】

清除全部地址冲突统计信息。

```
<H3C> reset dhcp server conflict all
```

5.2.41 reset dhcp server ip-in-use

【命令】

reset dhcp server ip-in-use { **ip** *ip-address* | **pool** [*pool-name*] | **interface** [*interface-type interface-number*] | **all** }

【视图】

用户视图

【参数】

ip-address：指定 IP 地址的绑定信息。

pool-name：指定全局地址池，如果不指定地址池名，表示所有全局地址池。

interface-type interface-number：指定接口的地址池，如果不指定接口名，表示所有接口地址池。

all：所有地址池。

【描述】

reset dhcp server ip-in-use 命令用来清除 DHCP 动态地址绑定信息。

相关配置可参考命令 **display dhcp server ip-in-use**。

【举例】

清除地址 10.110.1.1 的绑定信息。

```
<H3C> reset dhcp server ip-in-use ip 10.110.1.1
```

5.2.42 reset dhcp server statistics

【命令】

reset dhcp server statistics

【视图】

用户视图

【参数】

无

【描述】

reset dhcp server statistics 命令用来清除 DHCP 服务器的统计信息，包括 DHCP 地址池数目，自动、手工和过期绑定的地址数目，不可识别的报文数量，DHCP 请求和应答的报文数目统计等。

相关配置可参考命令 **display dhcp server statistics**。

【举例】

清除 DHCP 服务器统计信息。

```
<H3C> reset dhcp server statistics
```

5.2.43 static-bind ip-address

【命令】

static-bind ip-address *ip-address* [**mask** *netmask*]

undo static-bind ip-address

【视图】

DHCP 地址池视图

【参数】

ip-address：待绑定的 IP 地址。

netmask：待绑定 IP 地址的掩码，不指定该参数表示使用自然掩码。

【描述】

static-bind ip-address 命令用来配置静态绑定的 IP 地址，**undo static-bind ip-address** 命令用来删除静态绑定的 IP 地址。

缺省情况下，未配置静态绑定的 IP 地址。

static-bind ip-address 命令必须与 **static-bind** { **mac-address** | **client-identifier** } 命令配合使用，分别配置静态绑定的 IP 地址和 MAC 地址或 identifier。

相关配置可参考命令 **dhcp server ip-pool** 和 **static-bind** { **mac-address** | **client-identifier** }。

【举例】

将 MAC 地址为 0000-e03f-0305 的 PC 机与 IP 地址 10.1.1.1 绑定，掩码为 255.255.255.0。

```
[H3C-dhcp-pool-mypool] static-bind ip-address 10.1.1.1 mask 255.255.255.0
[H3C-dhcp-pool-mypool] static-bind mac-address 0000-e03f-0305
```

5.2.44 static-bind { mac-address | client-identifier }

【命令】

static-bind { **mac-address** *mac-address* | **client-identifier** *client-identifier* }

undo static-bind { **mac-address** | **client-identifier** }

【视图】

DHCP 地址池视图

【参数】

mac-address：待绑定的主机 MAC 地址，格式为 H-H-H。

client-identifier：待绑定的主机 ID。

【描述】

static-bind { **mac-address** | **client-identifier** }命令用来配置静态绑定的 MAC 地址或 identifier，**undo static-bind** { **mac-address** | **client-identifier** }命令用来删除静态绑定的 MAC 地址或 identifier。

缺省情况下，未配置静态绑定的 MAC 地址或 identifier。

static-bind { **mac-address** | **client-identifier** }命令必须与 **static-bind ip-address** 命令配合使用，分别配置静态绑定的 MAC 地址/identifier 和 IP 地址。

每个 MAC 地址或 identifier 只能与一个 IP 地址进行绑定。

相关配置可参考命令 **dhcp server ip-pool** 和 **static-bind ip-address**。

【举例】

将 MAC 地址为 0000-e03f-0305 的 PC 机与 IP 地址 10.1.1.1 绑定，掩码为 255.255.255.0。

```
[H3C-dhcp-pool-mypool] static-bind ip-address 10.1.1.1 mask 255.255.255.0
[H3C-dhcp-pool-mypool] static-bind mac-address 0000-e03f-0305
```

5.2.45 voice-config

【命令】

voice-config { **ncp-ip** *ip-address* | **as-ip** *ip-address* | **voice-vlan** *vlan-id* { **disable** | **enable** } | **fail-over** *ip-address dialer-string* }

undo voice-config [**ncp-ip** | **as-ip** | **voice-vlan** | **fail-over**]

【视图】

DHCP 地址池视图

【参数】

ncp-ip：Network Call Processor IP Address，网络呼叫处理器的 IP 地址。

as-ip：Alternate Server IP Address，备选 NCP 服务器的 IP 地址

voice-vlan：语音 VLAN。

fail-over：Fail-Over 呼叫路由。

ip-address：NCP、Alternate 服务器或 Fail-Over 的 IP 地址。

vlan-id：语音 VLAN 的 ID，取值范围为 1～4094。

enable：VLAN 处于使能状态。

disable：VLAN 出于非使能状态。

dialer-string：Fail-Over 拨号串，取值为 0～9 及通配符“*”。

【描述】

voice-config 命令用来配置 DHCP 服务器从全局地址池中分配地址时携带 option 184 及其子选项。**undo voice-config** 命令用来禁止 DHCP 服务器从全局地址池中分配地址时携带 option 184 及其子选项。

只有 DHCP 客户端请求了 option 184 后，DHCP 服务器才回应 option 184 及相应的子选项。

在配置其它子选项前必需先配置 **ncp-ip** 子选项，否则其它子选项将不生效。

缺省情况下，DHCP 服务器不支持 option 184 及其子选项。

相关配置可参考命令 **dhcp server voice-config**。

【举例】

在 DHCP 全局地址池 123 下配置 DHCP 服务器支持 option 184：NCP-IP 地址为 1.1.1.1，Alternate Server IP 地址为 2.2.2.2，Voice VLAN 为使能状态，ID 为 1，Fail-Over IP 地址为 3.3.3.3，拨号串为 99*。

```
[H3C] dhcp select global all
[H3C] dhcp server ip-pool 123
[H3C-dhcp-pool-123] voice-config ncp-ip 1.1.1.1
[H3C-dhcp-pool-123] voice-config as-ip 2.2.2.2
[H3C-dhcp-pool-123] voice-config voice-vlan 1 enable
[H3C-dhcp-pool-123] voice-config fail-over 3.3.3.3 99*
```

5.3 DHCP 客户端配置命令

5.3.1 debugging dhcp client

【命令】

debugging dhcp client { **event** | **packet** | **error** | **all** }

undo debugging dhcp client { **event** | **packet** | **error** | **all** }

【视图】

用户视图

【参数】

event：DHCP 客户端的协议事件，包括地址分配、数据更新。

packet：DHCP 客户端收发的 DHCP 协议报文。

error：表示报文不可识别信息或错误信息。

all：打开所有调试信息开关 。

【描述】

debugging dhcp client 命令用来打开 DHCP 客户端的调试开关，**undo debugging dhcp client** 命令用来关闭 DHCP 客户端的调试开关。

缺省情况，关闭所有的 DHCP 客户端调试开关。

【举例】

打开 DHCP 客户端的事件调试开关。

```
<H3C> debugging dhcp client event
```

5.3.2 display dhcp client

【命令】

display dhcp client [**verbose**]

【视图】

所有视图

【参数】

verbose：DHCP 客户端详细的统计信息。

【描述】

display dhcp client 命令用来显示 DHCP 客户端的统计信息。使用命令 **display dhcp client** 可以显示 DHCP 客户端地址分配的一些信息。命令 **display dhcp client verbose** 可以显示 DHCP 客户端地址分配的详细信息。

【举例】

显示 DHCP 客户端的统计信息。

```
[H3C] display dhcp client verbose
DHCP client statistic infomation:
Ethernet0/0:
Current machine state: BOUND
Alloced IP: 169.254.0.2 255.255.0.0
Alloced lease: 86400 seconds, T1: 43200 seconds, T2: 75600 seconds
Lease from 2002.09.20 01:05:03   to   2002.09.21 01:05:03
Server IP: 169.254.0.1
Transaction ID = 0x3d8a7431
Default router: 2.2.2.2
DNS server: 1.1.1.1
Domain name: h3c.com
Client ID: H3C-00e0.fc0a.c3ef-Ethernet0/0
Next timeout will happen after 0 days 11 hours 56 minutes 1 seconds.

Ethernet2/0:
Current machine state: HALT
```

统计信息显示共有两个接口配置成 DHCP 客户端。

Ethernet0/0 接口已经分配到地址，当前状态为 BOUND，分配的地址为 169.254.0.2/16，租约为 86400 秒，Renewal 定时器时长为 43200 秒，rebinding 定时器时长为 75600 秒，租约自 2002.09.20 01:05:03 至 2002.09.21 01:05:03；选择的 DHCP 服务器地址为 169.254.0.1；网关地址为 2.2.2.2，DNS 服务器地址为 1.1.1.1，域名为 h3c.com；下一次定时器超时将出现在 11 小时 56 分 1 秒后；

Ethernet2/0 接口尚未启动分配过程，当前状态为 HALT，一般是由于接口状态还不是 UP 状态。

显示 DHCP client 更详细的信息。

```
[H3C] display dhcp client verbose
DHCP client statistic infomation:
Ethernet0/0:
Current machine state: BOUND
Alloced IP: 169.254.0.2 255.255.0.0
Alloced lease: 300 seconds, T1: 150 seconds, T2: 262 seconds
```

```
Lease from 2002.09.15 07:11:55   to   2002.09.15 07:16:55
Server IP: 169.254.0.1
Transaction ID = 0x3d8432b1
Client ID: H3C-00e0.fc0a.c3ef-Ethernet0/0
Next timeout will happen after 0 days 0 hours 1 minutes 36 seconds.
```

以上统计信息显示 DHCP client 端动态分配 IP 地址的接口、当前状态机的状态、分配到的 IP 地址、租约时长、T1 时长、T2 时长、服务器 IP 地址、事务 ID 以及 Client ID 等信息。

表5-6 DHCP client 统计信息域说明

项目	描述
Ethernet0/0	client 端进行动态获取 IP 地址的接口
Current machine state	client 状态机状态
Alloced IP	client 分配到 IP 地址
lease	租约时长
T1	Renewal 定时器时长
T2	Rebinding 定时器时长
Lease from….to….	租约起止时间
Server IP	选择的 DHCP server 地址
Transaction ID	事务标识
Client ID	用户 ID
Default router	网关地址
DNS server	DNS 服务器地址
Domain name	域名
Requested IP	请求分配的 IP 地址
Offered IP	提供使用的 IP 地址

5.3.3 ip address dhcp-alloc

【命令】

ip address dhcp-alloc

undo ip address dhcp-alloc

【视图】

接口视图

【参数】

无

【描述】

ip address dhcp-alloc 命令用来在以太网接口配置使用 DHCP（Dynamic Host Configuration Protocol）动态主机配置协议分配本地 IP 地址，**undo ip address dhcp-alloc** 命令用来取消使用 DHCP 协商分配本地 IP 地址。本命令必须在以太网接口（包括子接口）视图下配置使用。

缺省不使用 DHCP 协商分配本地 IP 地址。

【举例】

指定在以太网接口 Ethernet0/0/0 上使用 DHCP 协商分配本地 IP 地址。

```
[H3C-Ethernet0/0/0] ip address dhcp-alloc
```

5.4 DHCP 中继配置命令

5.4.1 debugging dhcp relay

【命令】

debugging dhcp relay { **all** | **error** | **event** | **packet** [**client mac** *mac-address*] }

undo debugging dhcp relay { **all** | **error** | **event** | **packet** [**client mac** *mac-address*] }

【视图】

用户视图

【参数】

all：DHCP-relay 模块所有的调试开关。

error：DHCP-relay 模块错误调试开关。

event：DHCP-relay 模块事件调试开关。

packet：DHCP-relay 模块报文调试开关。

client mac：DHCP 客户端 MAC 地址，只显示指定的 DHCP 客户端信息。

【描述】

debugging dhcp relay 命令用来打开 DHCP-relay 模块调试功能，**undo debugging dhcp relay** 命令用来关闭 DHCP-relay 模块调试功能。

【举例】

打开 DHCP-relay 模块调试功能。

```
<H3C> debugging dhcp relay error
```

5.4.2 dhcp relay release

【命令】

dhcp relay release *client-ip mac-address* [*server-ip*]

【视图】

接口视图、系统视图

【参数】

client-ip：DHCP 客户端的 IP 地址。

mac-address：DHCP 客户端的 MAC 地址，形式为 H-H-H。

server-ip：DHCP 服务器的 IP 地址。

【描述】

dhcp relay release 命令用来通过 DHCP 中继向 DHCP 服务器发出释放客户端申请到的 IP 地址的请求。

当不指定 DHCP 服务器的 IP 地址时，如果在系统视图下，则向所有 DHCP 服务器发送 Release 报文。如果在接口视图下，向该接口下的所有中继地址发送 Release 报文。

在 DHCP Relay 中配置手工释放 IP 地址后，会通知 DHCP Server 释放 DHCP ip-in-use 地址池中的地址，该 IP 地址在释放后会放入过期队列，一般情况下不会马上被分配出去；此时仅仅释放的是 DHCP ip-in-use 地址池中的地址，Client 端主机是无法真正释放该地址的，所以 Client 端主机会使用该地址直到租约超时。

在执行该命令时，不打印调试信息。

【举例】

向 IP 地址为 10.110.91.174 的 DHCP 服务器发送 Release 报文，请求释放 MAC 地址为 0050-ba34-2000 的客户端申请到的 IP 地址 192.2.2.25。

```
[H3C] dhcp relay release 192.2.2.25 0050-ba34-2000 10.110.91.174
```

5.4.3 display dhcp relay address

【命令】

display dhcp relay address { **interface** *interface-type interface-num* | **all** }

【视图】

所有视图

【参数】

interface-type interface-num：指定接口的类型和编号。

all：所有接口。

【描述】

display dhcp relay address 命令用来查看接口的 DHCP 中继地址配置情况。

相关配置可参考命令 **ip relay address** 和 **ip relay address interface**。

【举例】

查看所有接口的 DHCP 中继地址配置情况。

```
<H3C> display dhcp relay address all
    **  Ethernet1/0/0 DHCP Relay Address  **
    Relay Address [0] :    3.3.3.3
```

5.4.4 display dhcp relay statistics

【命令】

display dhcp relay statistics

【视图】

所有视图

【参数】

无

【描述】

display dhcp relay statistics 命令用来查看 DHCP 中继的相关统计信息，包括错误的报文数、从客户端接收的 DHCP 报文数、从服务器接收的 DHCP 报文数、发给服务器的 DHCP 报文数、发给客户端的 DHCP 报文数（包括单播报文和广播报文）。

【举例】

查看 DHCP 中继的统计信息。

```
<H3C> display dhcp relay statistics
    Bad Packets recieved:                   0
    DHCP packets received from clients:     0
        DHCP DISCOVER packets received:     0
        DHCP REQUEST packets received:      0
```

```
    DHCP INFORM packets received:        0
    DHCP DECLINE packets received:       0
    DHCP BOOTPREQUEST packets received:  0
DHCP packets received from servers:      0
    DHCP OFFER packets received:         0
    DHCP ACK packets received:           0
    DHCP NAK packets received:           0
    DHCP BOOTPREPLY packets received:    0
DHCP packets sent to servers:            0
DHCP packets sent to clients:            0
    Unicast packets sent to clients:     0
    Broadcast packets sent to clients:   0
```

5.4.5 ip relay address

【命令】

ip relay address *ip-address*

undo ip relay address { *ip-address* | **all** }

【视图】

接口视图

【参数】

ip-address：IP 中继地址，为点分十进制格式。

all：所有 IP 中继地址。

【描述】

ip relay address 命令用来增加一条 IP 中继地址以指明 DHCP 服务器的具体位置，**undo ip relay address** 命令用来删除该接口使用的一条（或全部）IP 中继地址。

缺省情况下，不配置任何 IP 中继地址。

📖 说明：

由于 DHCP 客户机在 DHCP 配置的某些阶段发送的报文为广播报文，因此配置 IP 中继地址的接口应当支持广播方式，即本命令只能在像以太网接口这样的支持广播的网络接口上使用。

相关配置可参考命令 **display ip interface**。

【举例】

为以太网接口 Ethernet 0/0/0 增加两个 IP 中继地址。

```
[H3C-Ethernet0/0/0] ip relay address 202.38.1.2
[H3C-Ethernet0/0/0] ip relay address 202.38.1.3
```

5.4.6 ip relay address cycle

【命令】

ip relay address cycle

undo ip relay address cycle

【视图】

系统视图

【参数】

无

【描述】

当在 DHCP 中继上配置了多个 DHCP 服务器时，可以使用 **ip relay address cycle** 命令用来设置 DHCP 中继采用负载分担方式来分配服务器。这时 DHCP 中继通过 HASH 算法尽可能保证不同的客户使用不同的 DHCP 服务器，同一个客户始终使用同一个DHCP服务器。**undo ip relay address cycle** 命令用来设置中继为广播方式，把客户请求报文（广播报文）以广播方式中继给所有 DHCP 服务器。

不同用户根据 MAC 的不同，可能会被 DHCP 中继分配给不同的服务器，但是只要用户的 MAC 不变，用户对应的服务器就始终不会变。也就是说用户与服务器的对应关系是：一个用户对应唯一一台 DHCP 服务器，一台 DHCP 服务器可以对应多个用户。这种机制可能导致当某台服务器故障时，它所负责的用户将无法申请到地址，也就是说这些客户不会被重新分配给其它服务器。解决方法是将服务器恢复，或者在 DHCP 中继上将这台服务器删除，这时 DHCP 中继才会把这些用户分配给其它服务器。

缺省情况下，为广播方式。

相关配置可参考命令 **ip relay address**。

【举例】

设置中继方式为负载分担方式。

```
[H3C] ip relay address cycle
```

5.4.7 ip relay address interface

【命令】

ip relay address *ip-address* { **interface** *ethernet-subinterface-range* | **all** }

undo ip relay address { *ip-address* | **all** } { **interface** *ethernet-subinterface-range* | **all** }

【视图】

系统视图

【参数】

ip-address：DHCP 服务器的 IP 地址。

ethernet-subinterface-range：用关键字“**to**”连接两个子接口，表示子接口号在两个子接口之间的所有子接口（包含这两个子接口）。

all：**undo** 命令中的前一个 **all** 指所有中继地址，后一个 **all** 指所有接口。

【描述】

ip relay address interface 命令用来配置指定范围内的以太网接口进行透明传输转发的中继地址，**undo ip relay address interface** 命令用来删除配置的中继地址。

缺省情况下，没有配置 IP 中继地址。

相关配置可参考命令 **ip relay address**。

【举例】

为 Ethernet2/0/0.1 到 Ethernet2/0/0.5 之间的接口增加一个 IP 中继地址。

```
[H3C] ip relay address 202.38.1.2 interface ethernet 2/0/0.1 to ethernet
2/0/0.5
```

5.4.8 reset dhcp relay statistics

【命令】

reset dhcp relay statistics

【视图】

用户视图

【参数】

无

【描述】

reset dhcp relay statistics 命令用来清除 DHCP 中继的统计信息。

相关配置可参考命令 **display dhcp relay statistics**。

【举例】

清除 DHCP 中继的统计信息。

```
<H3C> reset dhcp relay statistics
```

第6章 IP 性能配置命令

6.1 IP 性能配置命令

6.1.1 debugging ip

【命令】

debugging ip { **icmp** | **packet** [**acl** { *acl-number1* | *acl-number2* }] }

undo debugging ip { **icmp** | **packet** }

【视图】

用户视图

【参数】

acl-number1：范围为 1000～1999，基于接口的访问控制列表；

acl-number2：范围为 2000～3999，表示访问控制列表。2000～2999 范围的数字型访问控制列表是基本的访问控制列表；3000～3999 范围的数字型访问控制列表是高级的访问控制列表。

【描述】

debugging ip icmp 命令用来打开 ICMP 报文的调试开关，**undo debugging ip icmp** 命令用来关闭 ICMP 报文的调试开关。

debugging ip packet 命令用来打开 IP 报文的调试开关，用户可以通过 **acl** 来对 IP 报文进行过滤，从而对调试信息进行过滤。**undo debugging ip packet** 命令用来关闭 IP 报文的调试开关。

【举例】

打开 IP 报文的调试开关。

```
<H3C> debugging ip packet
*0.129680-IP-8-debug_case:
Delivering, interface = Ethernet0/0/0, version = 4, headlen = 20, tos = 6,pktlen
= 70, pktid = 49, offset = 0, ttl = 1, protocol = 17,checksum = 50, s = 1.1.1.2,
d = 224.0.0.2
prompt: IP packet is delivering up!

*0.129680-IP-8-debug_case:
Sending, interface = Ethernet0/0/0, version = 4, headlen = 20, tos = 6,pktlen
```

```
= 70, pktid = 49, offset = 0, ttl = 1, protocol = 17,checksum = 55147, s = 1.1.1.2,
d = 224.0.0.2
prompt: Sending the packet from local at Ethernet0/0/0
<H3C> debugging ip icmp
*0.157090-IP-8-debug_icmp:
ICMP Receive: echo(Type=8, Code=0), Src = 127.0.0.1, Dst = 1.1.1.2

*0.157090-IP-8-debug_icmp:
ICMP Send: echo-reply(Type=0, Code=0), Src = 1.1.1.2, Dst = 127.0.0.1

*0.157090-IP-8-debug_icmp:
ICMP Receive: echo-reply(Type=0, Code=0), Src = 1.1.1.2, Dst = 127.0.0.1
```

6.1.2 debugging tcp event

【命令】

debugging tcp event [*task_id socket_id*]

undo debugging tcp event [*task_id socket_id*]

【视图】

用户视图

【参数】

task_id：任务 ID；

socket_id：套接口号。

【描述】

debugging tcp event 命令用来打开 TCP 事件的调试开关，**undo debugging tcp event** 命令用来关闭 TCP 事件的调试开关。

该命令用来打开 TCP 事件的调试开关，用户打开的调试开关数目是有限的，即只能同时打开固定数目的调试开关（任务 ID 和套接口号的组合）。另外注意，TCP 在被动打开即接收连接请求时，是创建新的套接口来建立连接，而且有的应用程序还会再创建一个任务来处理连接，如：Telnet 服务器，所以要想看到连接建立的信息，就不要使用参数 *task_id 和 socket_id* 来进行过滤。

【举例】

打开 TCP 事件的调试开关。

```
<H3C> debugging tcp event
*0.630270-SOCKET-8-TCP EVENT:
1043494683: task = Co0(2), socketid = 0,
TCPCB 0x02c6fd74 created
```

```
*0.630270-SOCKET-8-TCP EVENT:
1043494683: task = Co0(2), socketid = 1,
state  CLOSED changed to SYN_SENT

*0.630270-SOCKET-8-TCP EVENT:
1043494683: task = Co0(2), socketid = 1,
sending SYN, seq = 74249530,
LA = 127.0.0.1:1025, FA = 1.1.1.1:23

*0.630270-SOCKET-8-TCP EVENT:
1043494683: task = Co0(2), socketid = 1,
advertising MSS = 512,
LA = 127.0.0.1:1025, FA = 1.1.1.1:23

*0.630270-SOCKET-8-TCP EVENT:
1043494683: task = VTYD(9), socketid = 0,
received MSS = 512,
LA = 1.1.1.1:23, FA = 127.0.0.1:1025

*0.50959090-SOCKET-8-TCP EVENT:
733759463: sending RST to 2.2.2.1:11022

*0.1293330-SOCKET-8-TCP EVENT:
1043495346: task = Co0(2), socketid = 1,
connection refused because remote sent RST!
LA = 1.1.1.1:1026, FA = 1.1.1.2:21
<H3C> display debugging
TCP:
  TCP event debugging is on for task any socket any
debugging tcp md5
```

6.1.3 debugging tcp md5

【命令】

debugging tcp md5

undo debugging tcp md5

【视图】

用户视图

【参数】

无

【描述】

debugging tcp md5 命令用来打开 TCP 连接的 MD5 认证调试开关，**undo debugging tcp md5** 命令用来关闭 TCP 连接的 MD5 认证调试开关。

【举例】

打开 TCP 连接的 MD5 认证调试开关。

```
<H3C> debugging tcp md5
```

6.1.4 debugging tcp packet

【命令】

debugging tcp packet [*task_id socket_id*]

undo debugging tcp packet [*task_id socket_id*]

【视图】

用户视图

【参数】

task_id：任务 ID；

socket_id：套接口号。

【描述】

debugging tcp packet 命令用来打开 TCP 报文的报文调试开关，用户打开的调试开关数目是有限的，即只能同时打开固定数目的调试开关（任务 ID 和套接口号的组合）。**undo debugging tcp packet** 命令用来关闭 TCP 报文的调试开关。

【举例】

打开 TCP 报文的调试开关。

```
<H3C> debugging tcp packet
<H3C> display debugging
*0.100070-SOCKET-8-TCP PACKET:
1043204051:  Input: Co0(5) socketId = 2, state = SYN_SENT,
src = 127.0.0.1:1025, dst = 2.2.2.2:23,
seq = 11084380, ack = 0, optlen = 4, flag = SYN ,
window = 8192
1043204051:  Output: Co0(5) SocketId = 2, State = SYN_SENT,
src = 127.0.0.1:1025, Dst = 2.2.2.2:23,
Seq = 11084380, Ack = 0,  Datalen = 4, Flag = ACK PSH ,
Window = 8192
1043204051:  Retrans: Co0(5) SocketId = 2, State = SYN_SENT,
```

```
Src = 127.0.0.1:1025, Dst = 2.2.2.2:23,
Seq = 11084380, Ack = 0,  Optlen = 4, Flag = SYN ,
Window = 8192
```

6.1.5 debugging udp packet

【命令】

debugging udp packet [*task_id socket_id*]

undo debugging udp packet [*task_id socket_id*]

【视图】

用户视图

【参数】

task_id：任务 ID；

socket_id：套接口号。

【描述】

debugging udp packet 命令用来打开 UDP 报文的调试信息，用户打开的调试开关数目是有限的，即只能同时打开固定数目的调试开关（任务 ID 和套接口号的组合）。

undo debugging udp packet 命令用来关闭 UDP 报文的调试信息。

【举例】

打开 UDP 报文的调试信息。

```
<H3C> debugging udp packet
*0.377770-SOCKET-8-UDP:
1043494431: Output: task = ROUT(6), socketid = 3,
src = 1.1.1.1:520, dst = 255.255.255.255:520, datalen = 24,
```

6.1.6 display fib

【命令】

display fib

【视图】

所有视图

【参数】

无

【描述】

display fib 命令用来显示转发信息表摘要信息。

该命令以列表的方式输出转发信息表，每一行代表一条路由，内容包括：

- 目的地址/掩码长度
- 下一跳
- 当前标志，G、H、U 的组合。G 表示 Gateway（网关），H 表示 Host（主机路由），U 表示 UP（可用）。
- 时间戳
- 输出接口

【举例】

显示转发信息表摘要信息。

```
<H3C> display fib
Destination/Mask      Nexthop      Flag     TimeStamp    Interface
80.10.0.2/32          80.10.0.2    GHU      t[0]         Ethernet0/0/0
80.10.255.255/32      127.0.0.1    HU       t[0]         InLoopBack0
80.10.0.0/16          80.10.0.1    U        t[0]         Ethernet1/0/0
80.50.0.2/32          80.50.0.2    GHU      t[0]         Ethernet2/0/0
80.50.255.255/32      127.0.0.1    HU       t[0]         InLoopBack0
```

6.1.7 display fib acl

【命令】

display fib acl *number*

【视图】

所有视图

【参数】

number：基本 ACL 的编号，范围为 2000～2999。

【描述】

display fib acl 命令用来过滤显示 FIB 信息，根据所输入的访问控制列表数字，把通过了该过滤规则的 FIB 表项按照一定格式显示出来。

如果输入的 ACL 号为 2000～2999 之间的数字，查找相应的访问列表，如果找不到，则将所有的 FIB 表项信息显示出来；如果找到，则按照相应格式输出相应 FIB 表项的信息。

如果匹配的 FIB 表项条数为 0，则输出如下内容：

```
Route entry matched by access-list 2000:
Summary count: 0
```

如果输出的 FIB 表项条数不为 0，则按照如下格式输出 FIB 表项信息：

```
Route entry matched by access-list 2000:
Summary count: 1
Destination/Mask      Nexthop      Flag    TimeStamp    Interface
127.0.0.0/8           127.0.0.1    U       t[0]         InLoopBack0
```

📖 **说明：**

当前版本尚不支持共同使用多种过滤方式查看 FIB 的信息。

【举例】

显示通过了过滤列表的 FIB 表项。

```
<H3C> display fib acl 2000
Route entry matched by access-list 2000:
Summary counts: 1
Destination/Mask      Nexthop      Flag    TimeStamp    Interface
127.0.0.0/8           127.0.0.1    U       t[0]         InLoopBack0
```

6.1.8 display fib begin

【命令】

display fib | { **begin** | **include** | **exclude** } *text*

【视图】

所有视图

【参数】

text：字符

【描述】

display fib 命令用来根据正则表达式输出缓冲区中与包含字符串 *text* 相关的行。

该命令的功能是根据正则表达式输出缓冲区中与包含字符串 *text* 相关的行。

对于 **display fib** | **begin** *text*：显示从包含字符串 *text* 的那一行开始到缓冲区结束的所有行。

对于 **display fib** | **include** *text*：只显示包含字符串 *text* 的那几行。

对于 **display fib** | **exclude** *text*：显示不包含字符串 *text* 的行。

📖 **说明：**

当前版本尚不支持共同使用多种过滤方式查看 FIB 的信息。

【举例】

显示从包含字符串“169.254.0.0”那一行开始的所有行：

```
<H3C> display fib | begin 169.254.0.0
Destination/Mask      Nexthop      Flag    TimeStamp    Interface
169.254.0.0/16        2.1.1.1      U       t[0]         Ethernet0/0/0
2.0.0.0/16            2.1.1.1      U       t[0]         Ethernet0/0/0
127.0.0.0/8           127.0.0.1    U       t[0]         InLoopBack0
```

显示包含字符串“Ethernet0”的所有行：

```
<H3C> display fib | include ethernet0/0/0
Destination/Mask      Nexthop  Flag    TimeStamp        Interface
169.254.0.0/16        2.1.1.1  U       t[0]             Ethernet0/0/0
2.0.0.0/16            2.1.1.1  U       t[0]             Ethernet0/0/0
```

显示不包含字符串“169.254.0.0”的所有行：

```
<H3C> display fib | exclude 169.254.0.0
Destination/Mask      Nexthop      Flag    TimeStamp    Interface
2.0.0.0/16            2.1.1.1      U       t[0]         Ethernet0/0/0
127.0.0.0/8           127.0.0.1    U       t[0]         InLoopBack0
```

6.1.9 display fib ip-prefix

【命令】

display fib ip-prefix *listname*

【视图】

所有视图

【参数】

listname：前缀列表名。

【描述】

display fib ip-prefix 命令用来过滤显示 FIB 信息，根据所输入的前缀列表名称，把通过了该过滤规则的 FIB 表项按照一定格式显示出来。

如果匹配的 FIB 表项条数为 0，则提示与之匹配的 FIB 表项为 0。如果输出的 FIB 表项条数不为 0，则按照一定格式输出 FIB 表项信息。

如果匹配的 FIB 表项条数为 0，则输出如下内容：

```
Route entry matched by prefix-list abc1:
Summary count: 0
```

如果输出的 FIB 表项条数不为 0，则按照如下格式输出 FIB 表项信息：

```
Route entry matched by prefix-list abc2:
Summary count: 1
Destination/Mask    Nexthop      Flag   TimeStamp       Interface
127.0.0.0/8         127.0.0.1    U      t[0]            InLoopBack0
```

📖 **说明：**

当前版本尚不支持共同使用多种过滤方式查看 FIB 的信息。

【举例】

显示通过 abc0 前缀链表过滤的 FIB 表项。

```
<H3C> display fib ip-prefix abc0
Route Entry matched by prefix-list abc0:
Summary count: 4
Destination/Mask      Nexthop      Flag    TimeStamp    Interface
127.0.0.0/8           127.0.0.1    U       t[0]         InLoopBack0
127.0.0.1/32          127.0.0.1    U       t[0]         InLoopBack0
169.0.0.0/8           2.1.1.1      SU      t[0]         Ethernet 0/0/0
169.0.0.0/15          2.1.1.1      SU      t[0]         Ethernet 0/0/0
```

6.1.10 display fib longer

【命令】

display fib *dest-addr1* [*dest-mask1*] [**longer**]

display fib *dest-addr1 dest-mask1 dest-addr2 dest-mask2*

【视图】

所有视图

【参数】

dest-addr1：为目的 IP 地址 1，点分十进制表示。

dest-mask1：相应的子网掩码 1，为点分十进制格式的掩码或整数形式的掩码长度。

dest-addr2：为目的 IP 地址 2，点分十进制表示。

dest-mask2：相应的子网掩码 2，为点分十进制格式的掩码或整数形式的掩码长度。

【描述】

对于该命令，按照后面选择参数的不同匹配的方式也不同。

对于 **display fib** *dest-addr* 命令，如果目的地址在自然掩码范围内能找到相应的 FIB 表项，则将其子网全部显示出来，否则显示与目的地址最长匹配的 FIB 表项。

对于 **display fib** *dest-addr dest-mask* 命令，该命令用来显示与目的地址和掩码精确匹配的 FIB 表项。

对于 **display fib** *dest-addr* **longer** 命令，该命令用来显示与目的地址在自然掩码范围内的 IP 地址匹配的所有的目的地址 FIB 表项。

对于 **display fib** *dest-addr dest-mask* **longer** 命令，该命令用来显示与目的地址在输入的掩码范围内的 IP 地址匹配的所有的目的地址 FIB 表项。

对于 **display fib** *dest-addr1 dest-mask1 dest-addr2 dest-mask2* 命令，该命令用来显示目的地址在输入的 *dest-addr1 dest-mask1* 到 *dest-addr2 dest-mask2* 范围内的 FIB 表项。

📖 **说明：**

当前版本尚不支持共同使用多种过滤方式查看 FIB 的信息。

【举例】

显示目的地址与 169.253.0.0 在自然掩码范围内匹配的 FIB 项或最长匹配的 FIB 项。

```
<H3C> display fib 169.253.0.0 longer
Destination/Mask      Nexthop      Flag    TimeStamp    Interface
169.0.0.0/16          2.1.1.1      U       t[0]         Ethernet0/0/0
```

显示目的地址在 169.254.0.0/16 和 169.254.0.6/16 范围内的 FIB 项。

```
<H3C> display fib 169.254.0.0 255.255.0.0 169.254.0.6 255.255.0.0
Destination/Mask      Nexthop      Flag    TimeStamp    Interface
169.254.0.1/16        2.1.1.1      U       t[0]         Ethernet0/0/0
```

6.1.11 display fib statistics

【命令】

display fib statistics

【视图】

所有视图

【参数】

无

【描述】

display fib statistics 命令用来显示 FIB 表项的总数目。

【举例】

该命令显示 FIB 表项总数。

```
<H3C> display fib statistics
Route Entry Count : 30
```

6.1.12 display icmp statistics

【命令】

display icmp statistics

【视图】

所有视图

【参数】

无

【描述】

display icmp statistics 命令用来显示 ICMP 报文统计信息。

相关命令请参考 **display interface**

【举例】

显示 ICMP 报文统计信息。

```
[H3C] display icmp statistics
  Input: bad formats   0          bad checksum            0
         echo          5          destination unreachable 0
         source quench 0          redirects               0
         echo reply    15         parameter problem       0
         timestamp     0          information request     0
         mask requests 0          mask replies            0
         time exceeded 1
  Output:echo          15         destination unreachable 0
         source quench 0          redirects               0
         echo reply    5          parameter problem       0
         timestamp     0          information reply       0
         mask requests 0          mask replies            0
         time exceeded 1
```

表6-1 display icmp statistics 命令显示信息说明

项目	说明
Input: bad formats	输入的格式错误报文数
bad checksum	输入的校验和错误报文数
echo	输入（输出）的 echo 请求类型报文数
destination unreachable	输入（输出）的目的不可达报文数
source quench	输入（输出）的源站抑制报文数
redirects	输入（输出）的重定向报文数
echo reply	输入（输出）的 echo 应答报文数
parameter problem	输入（输出）的参数错误报文数
timestamp	输入（输出）的时间戳报文数
information request	输入的信息请求报文数
mask requests	输入（输出）的掩码请求报文数
mask replies	输入（输出）的掩码应答报文数
information reply	输出的信息应答报文数
time exceeded	超时的报文数

6.1.13 display ip fast-forwarding cache

【命令】

display ip fast-forwarding cache [*ip-address*]

【视图】

所有视图

【参数】

ip-address：使用 IP 地址对显示信息进行过滤。

【描述】

display ip fast-forwarding cache 命令用来显示快速转发表信息。

【举例】

```
[H3C] display ip fast-forwarding cache
Fast-Forwarding cache:
Index   SrIP    SrPort   DsIP       DsPort Pro Input_If   Output_If  FLAG
600:0 1.1.3.149  1463 10.10.26.30  23     6  Ethernet0/0 Ethernet1/0 81
```

以上信息表明：最近刚使用过的 cache 是从 1.1.3.149 的 1463 端口到达 10.10.26.30 的 23 端口的数据流，协议号是 6，表明是 TCP 数据，输入接口是 Ethernet0/0，输出接口为 Ethernet1/0。

6.1.14 display ip interface

【命令】

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

【视图】

所有视图

【参数】

interface-type：接口类型。

interface-number：接口编号。

【描述】

display ip interface 用来显示接口的 IP 信息。

缺省情况下，如果不指定接口，则显示全部接口的 IP 信息。

该命令输出接口上全部与 IP 有关的信息，有助于故障诊断。

相关配置可参考命令 **display interface**，**display ip interface brief**。

【举例】

查看接口 Ethernet0/0/0 的 IP 相关信息。

```
<H3C> display ip interface Ethernet 0/0/0
Ethernet0/0/0 current state :UP
Line protocol current state :UP
Internet Address is 192.168.2.1/24
Broadcast address : 192.168.2.255
The Maximum Transmit Unit : 1500 bytes
ip fast-forwarding incoming packets state is Enabled
ip fast-forwarding outgoing packets state is Enabled
IP packets input number: 190, bytes: 9900, multicasts: 0
IP packets output number: 0, bytes: 0, multicasts: 0
ARP packets input number:          1
  Request packet:                  1
  Reply packet:                    0
  Unknown packet:                  0
TTL invalid packet number:         0
ICMP packet input number:          0
```

```
  Echo reply:                    0
  Unreachable:                   0
  Source quench:                 0
  Routing redirect:              0
  Echo request:                  0
  Router advert:                 0
  Router solicit:                0
  Time exceed:                   0
  IP header bad:                 0
  Timestamp request:             0
  Timestamp reply:               0
  Information request:           0
  Information reply:             0
  Netmask request:               0
  Netmask reply:                 0
  Unknown type:                  0
DHCP packet deal mode:  interface
```

6.1.15 display ip interface brief

【命令】

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

【视图】

所有视图

【参数】

interface-type：接口类型。

interface-number：接口编号。

【描述】

display ip interface brief 用来显示 IP 接口摘要信息。

缺省情况下，如果不指定接口，则显示全部 IP 接口摘要信息。

相关配置可参考命令 **display ip interface**，**display interface**。

【举例】

显示接口摘要信息。

```
[H3C-Virtual-Template0] display ip interface brief
*down: administratively down
(s): spoofing
 Interface        IP Address   Physical    Protocol Description
```

```
Aux0              unassigned   down         down     Aux0 Interface
Ethernet0/0/0     192.168.0.1  down         down     Ethernet0/0/0 Interface
Ethernet0/0/1     unassigned   down         down     Ethernet0/0/1 Interface
Virtual-Template0unassigned    up           up(s)    changchen
```

6.1.16 display ip socket

【命令】

display ip socket [**socktype** *sock_type*] [*task_id socket_id*]

【视图】

所有视图

【参数】

sock_type：套接口类型：（tcp：1，udp 2，raw ip 3）

task_id：任务 ID；

socket_id：套接口号。

【描述】

display ip socket 命令用来显示系统当前所有的套接口信息。

【举例】

显示套接口类型为 TCP 的信息。

```
<H3C> display ip socket socktype 1
SOCK_STREAM:
Task = VTYD(9), socketid = 1, Proto = 6,
LA = 0.0.0.0:23, FA = 0.0.0.0:0,
sndbuf = 4096, rcvbuf = 4096, sb_cc = 0, rb_cc = 0,
socket option = SO_ACCEPTCONN
socket state = SS_PRIV  SS_ASYNC
SOCK_DGRAM:
Task = ROUT(6), socketid = 1, Proto = 17,
LA = 0.0.0.0:0, FA = 0.0.0.0:0,
sndbuf = 9216, rcvbuf = 41600, sb_cc = 0, rb_cc = 0,
socket option = SO_UDPCHECKSUM
socket state = SS_PRIV  SS_ASYNC
SOCK_RAW:
Task = ROUT(6), socketid = 2, Proto = 2,
LA = 0.0.0.0, FA = 0.0.0.0,
sndbuf = 32767, rcvbuf = 32767, sb_cc = 0, rb_cc = 0,
socket option = 0,
```

```
socket state = SS_PRIV  SS_NBIO  SS_ASYNC
```

主要的显示信息解释如下：

SOCK_STREAM：套接口类型；

Proto：该套接口使用的协议号；

sndbuf：套接口的发送缓冲区大小；

rcvbuf：套接口的接收缓冲区大小；

sb_cc：发送缓存中现有的数据大小，只有 TCP 会缓存数据，这个值才有用；

rb_cc：接收缓存中现有的数据大小；

socket option：套接口选项；

socket state：套接口状态；

显示任务 ID 为 8，套接口号为 4 的信息。

```
<H3C> display ip socket 8 4
Task = VTYD(8), socketid = 4, Proto = 6,
LA = 0.0.0.0:23, FA = 0.0.0.0:0,
sndbuf = 4096, rcvbuf = 4096, sb_cc = 0, rb_cc = 0,
socket option = SO_ACCEPTCONN
socket state = SS_PRIV  SS_ASYNC
```

6.1.17 display ip statistics

【命令】

display ip statistics

【视图】

所有视图

【参数】

无

【描述】

display ip statistics 命令用来显示 IP 流量统计信息，显示 IP 收发和拆包、组包的统计信息，有助于故障诊断。

相关配置可参考命令 **display interface**，**display ip interface**，**reset ip statistics**。

【举例】

显示 IP 流量统计信息。

```
<SecPath> display ip statistics
  Input:   sum            7120            local            112
```

```
          bad protocol   0                bad format        0
          bad checksum   0                bad options       0
Output:   forwarding     0                local             27
          dropped        0                no route          2
          compress fails 0
Fragment:input           0                output            0
          dropped        0
          fragmented     0                couldn't fragment 0
Reassembling:sum         0                timeouts          0
```

表6-2 display ip statistics 命令显示信息说明

项目	说明
Input: sum	输入报文总数
local	输入的目的地址是本地的报文
bad protocol	协议号错的报文数
bad format	格式错误的报文数
bad checksum	校验和错误的报文数
bad options	选项错误的报文数
Output: forwarding	转发的报文数
local	本地发送报文数
dropped	发送时丢弃的报文数
no route	查不到路由的报文数
compress fails	压缩失败的报文数
Fragment: input	输入的分片数
output	输出的分片数
dropped	丢弃的分片数
fragmented	成功分片的报文数
couldn't fragment	不能分片的报文数
Reassembling: sum	重组报文总数
timeouts	超时的分片报文数

6.1.18 display tcp statistics

【命令】

display tcp statistics

【视图】

所有视图

【参数】

无

【描述】

display tcp statistics 命令用来显示 TCP 流量统计信息。

显示系统当前所有 TCP 连接的流量统计信息。统计信息主要分为发送和接收两大部分，每部分再细分为不同类型报文，如：接收的有重复的报文、校验和错误报文等等。最后还有一些与连接密切相关的统计信息，如：接受的连接数、重传报文数、保活探测报文数等。以上信息大都是以包为单位，个别的将给出字节数。

相关配置可参考命令 **display tcp status**。

【举例】

显示 TCP 流量统计信息。

```
<H3C> display tcp statistics
Received packets:
Total: 0
packets in sequence: 0 (0 bytes)
window probe packets: 0, window update packets: 0
checksum error : 0, bad offset : 0, too short : 0
duplicate packets : 0 (0 bytes),  partially duplicate packets : 0(0 bytes)
out-of-order packets : 0 (0 bytes)
packets with data after window : 0 (0 bytes)
packets after close : 0
ack packets:0 (0 bytes), duplicate ack packets:0, ack packets with unsend
data:0
Sent packets:
Total: 0
urgent packets: 0
control packets: 0 ( 0 RST)
window probe packets: 0, window update packets: 0
data packets : 0 (0 bytes), data packets retransmitted: 0 (0 bytes)
ack only packets : 0(0 delayed)
Total  retransmit timeout: 0, connections dropped in retransmit timeout: 0
Keepalive timeout: 0, keepalive probe: 0, dropped connections in keepalive:
0
Initiated connections: 0,  accepted connections: 0,established connections:
0
Closed connections: 0,( dropped: 0, initiated dropped: 0)
```

```
Packets dropped with MD5 authentication : 0
Packets permitted with MD5 authentication : 0
```

以上显示信息表示：

接收数据统计：

总计收到报文数：0

报文（共计字节数：0）按顺序到达数：0

窗口探测报文数：0，窗口更新报文数：0

报文校验出错数：0，报文长度出错数：0，报文太短数：0

完全重复报文数：0（共计字节数：0），部分重复报文数：0（共计字节数：0）

乱序报文数：0（共计 字节数：0）

报文落在接收窗口外数：0（共计字节数：0）

报文在连接关闭后到达数：0

确认报文数：0（确认数据字节数：0），重复的确认报文数：0，经过确认但未发送数据的 ACK 报文数：0

发送数据统计：

总计发送报文数：0

紧急数据报文数：0

控制报文数：0（RST 报文数：0）

窗口探测报文数：0，窗口更新报文数：0

数据报文数：0（共计字节数：0），报文重发数：0（共计字节数：0）

ACK 报文数：0（延迟 ACK 报文数：0）

重传定时器超时次数：0，重传次数超过限制而丢弃的连接数：0

保活定时器超时次数：0，发送保活探测报文数：0，保活探测失败丢弃连接数：0

发起连接次数：0，接受连接：0，已建立连接：0

已关闭连接数目：0（意外丢弃连接（收到 SYN 之后）：0，主动连接失败到对端 SYN 之前的次数：0）

MD5 验证丢弃报文数：0

MD5 验证通过报文数：0

6.1.19 display tcp status

【命令】

display tcp status

【视图】

所有视图

【参数】

无

【描述】

display tcp status 命令用来显示 TCP 连接状态，使用户随时监控 TCP 连接。

相关配置可参考命令 **display local-user**。

【举例】

显示 TCP 连接状态。

```
<H3C> display tcp status
*: TCP MD5 Connection
TCPCB         Local Address        Foreign Add:port         State
0442c394      10.110.93.146:23     10.110.93.175:1538       Established
045d8074      0.0.0.0:21           0.0.0.0:0                Listening
```

以上显示信息表示：一个 TCP 连接已经建立，TCP 任务控制块编号为 0442c394，该 TCP 连接的本地 IP 地址为 10.110.93.146，本地端口号为 23，远程 IP 地址为 10.110.93.175，远程端口号为 1538，另外本地有一个对 21 号端口监听的服务器。

6.1.20 display udp statistics

【命令】

display udp statistics

【视图】

所有视图

【参数】

无

【描述】

display udp statistics 命令用来显示 UDP 流量统计信息。

显示系统当前所有 UDP 报文的流量统计信息。统计信息主要分为发送和接收两大部分，每部分再细分为不同类型报文，如校验和错误报文等等。最后还有一些与连接密切相关的统计信息，如：广播包的报文的个数等。以上信息都是以包为单位。

相关配置可参考命令 **reset udp statistics**。

【举例】

显示 UDP 流量统计信息。

```
<H3C> display udp statistics
Received packets:
     Total: 210
     checksum error: 0
     shorter than header: 0, data length larger than packet: 0
     no socket on port: 0
     total broadcast or multicast packets : 210
     no socket broadcast or multicast packets: 210
     not delivered, input socket full: 0
     input packets missing pcb cache: 0
Sent packets:
     Total: 0
```

主要的信息解释如下：

总计收到 210 个 UDP 报文。0 个报文校验和出错，0 个报文长度比报文头短，0 个报文数据长度超过了报文长，0 个报文没有哪个 SOCKET 使用这个端口号，210 个报文是广播包或多播包，210 个报文是非 SOCKET 的广播包或多播包，0 个报文因为 SOCKET 缓冲已经满而没有上送，0 个报文没有找到 pcb，总计发送 0 个 UDP 报文。

6.1.21 icmp redirect send

【命令】

icmp redirect send

undo icmp redirect send

【视图】

系统视图

【参数】

无

【描述】

icmp redirect send 命令用来打开 ICMP 发送重定向报文功能，**undo icmp redirect send** 命令用来关闭 ICMP 发送重定向报文功能。

缺省情况下，打开 ICMP 发送重定向报文功能。

【举例】

打开 ICMP 发送重定向报文功能。

```
[H3C] icmp redirect send
```

6.1.22 ip fast-forwarding

【命令】

ip fast-forwarding [**inbound** | **outbound**]

undo ip fast-forwarding [**inbound | outbound**]

【视图】

接口视图

【参数】

inbound：只允许在入接口方向上进行快速转发。

outbound：只允许在出接口方向上进行快速转发。

【描述】

ip fast-forwarding 命令用来允许接口进行快速转发报文，**undo ip fast-forwarding** 命令用来禁止接口进行快速转发。

缺省情况下，允许接口在出入两个方向都进行快速转发。

使能或禁止对接口的接收报文进行快速转发。快速转发适用于高速链路接口（如以太网、帧中继等），因为低速链路本身传输率低，使用快速转发也没有实际意义。

SecPath 系列防火墙支持在高速链路接口（如以太网接口）上提供快速转发，支持在配置了防火墙、NAT、GRE 特性下的快速转发功能。需要注意的是：当在接口上配置了快速转发，该接口将不再发送 ICMP 重定向报文。

当在接口上配置了快速转发且应用了包过滤防火墙后，ACL 只对数据流（即相同五元组的报文）的首包进行检查。若允许报文通过则建立快速转发表项，之后匹配此快转表项的报文将不再经过 ACL 的检查，只对 ACL 的计数器进行添加。当同一数据流(即相同五元组的报文)中的报文拥有不同的五元组以外的字段值时(例如 ToS、DSCP 等），这些报文也将被视为同一数据流，并根据快转表项进行转发。故当在 ACL 规则中配置了对同一条数据流的不同的五元组以外字段值的不同操作时，需要关闭快速转发功能。

【举例】

禁止接口进行快速转发。

```
[H3C-Ethernet0/0/0] undo ip fast-forwarding
```

允许在入口方向上进行快速转发。

```
[H3C-Ethernet0/0/0] ip fast-forwarding inbound
```

6.1.23 reset ip fast-forwarding cache

【命令】

reset ip fast-forwarding cache

【视图】

用户视图

【参数】

无

【描述】

reset ip fast-forwarding cache 命令用来清除快速转发缓冲区中的内容，清除后的快速转发表不再有任何快速转发项。

【举例】

清除快速转发缓冲区中的内容。

```
<H3C> reset ip fast-forwarding cache
```

6.1.24 reset ip statistics

【命令】

reset ip statistics

【视图】

用户视图

【参数】

无。

【描述】

reset ip statistics 命令用来清除 IP 统计信息。在某些特殊情况下，需要清除 IP 统计信息，重新进行统计。

相关配置可参考命令 **display ip interface**，**display ip statistics**。

【举例】

清除 IP 统计信息。

```
<H3C> reset ip statistics
```

6.1.25 reset tcp statistics

【命令】

reset tcp statistics

【视图】

用户视图

【参数】

无

【描述】

reset tcp statistics 命令用来清除 TCP 流量统计信息。

相关配置可参考命令 **display tcp statistics**。

【举例】

清除 TCP 流量统计信息。

```
<H3C> reset tcp statistics
```

6.1.26 reset udp statistics

【命令】

reset udp statistics

【视图】

用户视图

【参数】

无

【描述】

reset udp statistics 命令用来清除 UDP 流量统计信息

【举例】

清除 UDP 流量统计信息。

```
<H3C> reset udp statistics
```

6.1.27 tcp mss

【命令】

tcp mss *value*

undo tcp mss

【视图】

接口视图

【参数】

value：指定 TCP 报文分片的最大值，范围 128～2048。

【描述】

tcp mss 命令用来配置 TCP 最大报文分片的长度，**undo tcp mss** 命令用来取消 TCP 报文分片。

由于我们接口缺省的 MTU 是 1500 字节，故一般要求加密报文头+链路层开销+IP 头+TCP 报文小于 1500 字节，即 TCP 分片配置 1200 左右比较适合。

缺省情况下，TCP 报文不分片。

【举例】

配置 TCP 报文分片的最大值为 300。

```
[H3C-Ethernet0/0/0] tcp mss 300
```

6.1.28 tcp timer fin-timeout

【命令】

tcp timer fin-timeout *time-value*

undo tcp timer fin-timeout

【视图】

系统视图

【参数】

time-value：TCP finwait 定时器值，单位为秒，范围为 76～3600。

【描述】

tcp timer fin-timeout 命令用来配置 TCP finwait 定时器，**undo tcp timer fin-timeout** 命令用来恢复 TCP finwait 定时器的缺省值。

缺省情况下，TCP finwait 定时器值为 675 秒。

当 TCP 的连接状态由 FIN_WATI_1 变为 FIN_WAIT_2 时启动 finwait 定时器。若 finwait 定时器超时前仍未收到 FIN 报文，则 TCP 连接被终止。

对该参数的配置最好在技术支持人员的指导下进行。

相关配置可参考命令 **tcp timer syn-timeout**，**tcp window**。

【举例】

配置 TCP finwait 定时器的值为 700 秒。

```
[H3C] tcp timer fin-timeout 700
```

6.1.29 tcp timer syn-timeout

【命令】

tcp timer syn-timeout *time-value*

undo tcp timer syn-timeout

【视图】

系统视图

【参数】

time-value：TCP synwait 定时器值，单位为秒，范围为 2～600。

【描述】

tcp timer syn-timeout 命令用来配置 TCP synwait 定时器，**undo tcp timer syn-timeout** 命令用来恢复 TCP synwait 定时器的缺省值。

缺省情况下，TCP synwait 定时器值为 75 秒。

当发送 syn 报文时，TCP 启动 synwait 定时器，若 synwait 超时前未收到回应报文，则 TCP 连接将被终止。

对该参数的配置最好在技术支持人员的指导下进行。

相关配置可参考命令 **tcp timer fin-timeout**，**tcp window**。

【举例】

配置 TCP synwait 定时器为 80 秒。

```
[H3C] tcp timer syn-timeout 80
```

6.1.30 tcp window

【命令】

tcp window *window-size*

undo tcp window

【视图】

系统视图

【参数】

window-size：面向连接 Socket 的收发缓冲区大小，单位 K 字节，范围 1～32。

【描述】

tcp window 命令用来配置面向连接 Socket 的收发缓冲区大小，**undo tcp window** 命令用来恢复面向连接 Socket 的收发缓冲区大小的缺省值。

缺省情况下，面向连接 Socket 的收发缓冲区大小为 8K 字节。

对该参数的配置最好在技术支持人员的指导下进行。

相关配置可参考命令 **tcp timer fin-timeout**，**tcp timer syn-timeout**。

【举例】

配置面向连接 Socket 的收发缓冲区大小为 4K 字节。

```
[H3C] tcp window 4
```

第7章 IP 单播策略路由配置命令

7.1 IP 单播策略路由配置命令

7.1.1 apply default output-interface

【命令】

apply default output-interface *interface-type interface-number* [*interface-type interface-number*]

undo apply default output-interface [*interface-type interface-number* [*interface-type interface-number*]]

【视图】

route-policy 视图

【参数】

interface-type：为接口类型。

interface-number：为接口的编号。

【描述】

apply default output-interface 命令用来设置报文的缺省发送接口，**undo apply default output-interface** 命令用来取消报文缺省发送接口的设置。

本命令对已经匹配的 IP 报文设置缺省发送的接口，最多可以指定两个缺省发送的接口。该子句对未查得路由的报文起作用。

相关配置可参考命令 **apply ip-precedence**，**apply ip-address next-hop**，**apply output-interface**，**apply ip-address default next-hop**。

【举例】

设置报文的缺省发送接口为 Tunnel0。

```
[H3C-route-policy] apply default output-interface Tunnel 0
```

7.1.2 apply ip-address default next-hop

【命令】

apply ip-address default next-hop *ip-address* [*ip address*]

undo apply ip-address default next-hop [*ip-address* [*ip address*]]

【视图】

route-policy 视图

【参数】

ip-address：缺省下一跳的 IP 地址。

【描述】

apply ip-address default next-hop 命令用来设置报文的缺省下一跳，**undo apply ip-address default next-hop** 命令用来取消已设置的报文缺省下一跳。

本命令对已经匹配的 IP 报文设置缺省下一跳，最多可以指定两个下一跳地址。本子句只对未查得路由的报文起作用。

相关配置可参考命令 **apply ip-precedence**，**apply output-interface**，**apply default output-interface**，**apply ip-address next-hop**。

【举例】

设置报文的缺省下一跳为 1.1.1.1。

```
[H3C-route-policy] apply ip-address default next-hop 1.1.1.1
```

7.1.3 apply ip-address next-hop

【命令】

apply ip-address next-hop *ip-address* [*ip-address*]

undo apply ip-address next-hop [*ip-address* [*ip-address*]]

【视图】

route-policy 视图

【参数】

ip-address：下一跳 IP 地址。

【描述】

apply ip-address next-hop 命令用来设置报文投递的下一跳，**undo apply ip-address next-hop** 命令用来取消下一跳的设置。

本命令对匹配的 IP 报文设置转发的下一跳，最多可以指定两个下一跳。下一跳应与本机邻接。

acl 参数在单播策略路由中不起作用。

相关配置可参考命令 **apply ip-precedence**，**apply output-interface**，**apply default output-interface**，**apply ip-address default next-hop**。

【举例】

设置报文投递的下一跳为 1.1.1.1。

```
[H3C-route-policy] apply ip-address next-hop 1.1.1.1
```

7.1.4 apply ip-precedence

【命令】

apply ip-precedence *value*

undo apply ip-precedence

【视图】

route-policy 视图

【参数】

value：优先级值。IP 报文共有 8（0～7）个优先级，每个优先级对应一个关键字，如下表：

表7-1 IP 优先级值与关键字对应表

优先级值	关键字
0	routine
1	priority
2	immediate
3	flash
4	flash-override
5	critical
6	internet
7	network

【描述】

apply ip-precedence 命令用来置 IP 报文优先级，**undo apply ip-precedence** 命令用来取消报文优先级设置。

相关配置可参考命令 **apply output-interface**，**apply ip-address next-hop**，**apply default output-interface**，**apply ip-address default next-hop**。

【举例】

设置 IP 报文优先级为 5（critical）。

```
[H3C-route-policy] apply ip-precedence critical
```

7.1.5 apply output-interface

【命令】

apply output-interface *interface-type interface-number* [*interface-type interface-number*]

undo apply output-interface [*interface-type interface-number* [*interface-type interface-number*]]

【视图】

route-policy 视图

【参数】

interface-type：为接口的类型。

interface-number：为接口的编号。

【描述】

apply output-interface 命令用来设置报文发送的接口，**undo apply output-interface** 命令用来取消发送接口的设置。

本命令对已经匹配的 IP 报文设置报文发送接口，最多可以指定两个发送接口。

ACL 参数在单播策略路由中不起作用。

当前策略路由不支持插卡热插拔事件，即拔掉插卡后，相应的配置仍然存在，需要手工删除。

相关配置可参考命令 **apply ip-precedence**，**apply ip-address next-hop**，**apply default output-interface**，**apply ip-address default next-hop**。

【举例】

对已经匹配的 IP 报文指定发送接口为 Tunnel0。

```
[H3C-route-policy] apply output-interface Tunnel 0
```

7.1.6 display ip policy

【命令】

display ip policy

【视图】

所有视图

【参数】

无

【描述】

display ip policy 命令用来显示本地和接口设置的策略路由的策略。

【举例】

显示本地和接口设置的策略路由的策略。

```
<H3C> display ip policy
Route-policy              Interface
pr02                      Local
pr02                      Virtual-Template0
pr01                      Ethernet0/0/0
```

其中，第一行是提示信息。第一列显示的是第二列指明的策略路由所作用的场所。以第一行为例，其中 local 代表该策略路由使能在本机，即所有从本机发送的（而不是通过本机转发的）报文应用策略路由 pr02。第二行和第三行代表 virtual-template0 和 Ethernet 0/0/0 接口分别应用了 pr02 和 pr01。

7.1.7 display ip policy setup

【命令】

display ip policy setup { **local** | **interface** *interface-type interface-number* }

【视图】

所有视图

【参数】

local：显示本地策略路由的设置情况。

interface：显示接口策略路由的设置情况。

interface-type：接口类型。

interface-number：接口编号。

【描述】

display ip policy setup 命令用来显示策略路由的设置情况。

【举例】

显示指定接口上的策略路由包含的具体配置情况，不论指定的策略路由是否已经被使能。

```
<H3C> display ip policy setup interface ethernet 0/0/0
 route-policy pr01 permit 0
 if-match acl 3101
 apply ip-address next-hop 10.0.0.1
```

这条命令显示接口 ethernet 0/0/0 上名称为 pr01 的这条策略路由的具体配置情况。如上所示，该策略路由只有一个 0 节点并且包含一条 **if-match** 语句和一条 **apply** 语句。**if-match** 语句和 **apply** 语句的准确含义可以参考该命令的配置说明。

display ip policy setup local 命令的显示形式与以上命令完全相同，不同之处在于显示的是在本机使能的策略路由。

7.1.8 display ip policy statistic

【命令】

display ip policy statistic { **local** | **interface** *interface-type interface-number* }

【视图】

所有视图

【参数】

local：显示本地策略路由报文的统计信息。

interface：显示接口策略路由报文的统计信息。

interface-type：接口类型。

interface-number：接口编号。

【描述】

display ip policy statistic 命令用来显示策略路由的统计信息。

【举例】

显示指定接口的策略路由匹配情况的统计信息。

```
<H3C> display ip policy statistic interface ethernet0/0/0
Interface Ethernet0/0/0 policy routing information:
 Route-policy: aaa
   permit node 5
     apply ip-address next-hop 10.0.0.1
       Denied: 0,
       Forwarded: 0
 Total denied: 0, forwarded: 0
```

该显示信息表示配置在接口 ethernet0/0/0 上的策略路由的所有发送策略（即 **apply** 语句）发送成功和失败的次数。

7.1.9 if-match acl

【命令】

if-match acl *acl-number*

undo if-match acl

【视图】

route-policy 视图

【参数】

acl-number：访问控制列表号。

【描述】

if-match acl 命令用来设置 IP 地址匹配条件，**undo if-match acl** 命令用来删除 IP 地址匹配条件。

acl-number 可以是基本的 ACL，也可以是高级的 ACL。

相关配置可参考命令 **if-match packet-length。**

【举例】

设置满足访问列表 2010 的报文被匹配。

```
[H3C] route-policy map1 permit node 1
[H3C-route-policy] if-match acl 2010
```

7.1.10 if-match packet-length

【命令】

if-match packet-length *min-len max-len*

undo if-match packet-length

【视图】

route-policy 视图

【参数】

min-len：最短网络层报文长度，取值范围为 0～2147483647。

max-len：最长网络层报文长度，取值范围为 0～2147483647。

【描述】

if-match packet-length 命令用来设置 IP 报文长度匹配条件，**undo if-match packet-length** 命令用来删除 IP 报文长度匹配条件的设置。

相关配置可参考命令 **if-match acl**。

【举例】

设置报文长度在 100～200 字节之间报文被匹配。

```
[H3C] route-policy map1 permit node 10
```

```
[H3C-route-policy] if-match packet-length 100 200
```

7.1.11 ip local policy route-policy

【命令】

ip local policy route-policy *policy-name*

undo ip local policy route-policy *policy-name*

【视图】

系统视图

【参数】

policy-name：策略名。

【描述】

ip local policy route-policy 命令用来使能本地策略路由，**undo ip local policy route-policy** 命令用来删除本地策略路由的设置。

缺省情况下，禁止本地策略路由。

对从本机向外发出的报文使用或禁止使用本地策略路由。若无特殊需求，建议用户不要配置本地策略路由。

相关配置可参考命令 **ip policy route-policy**。

【举例】

使能本地策略路由，该策略路由由路由策略“AAA”指定。

```
[H3C] ip local policy route-policy AAA
```

7.1.12 ip policy route-policy

【命令】

ip policy route-policy *policy-name*

undo ip policy route-policy *policy-name*

【视图】

接口视图

【参数】

policy-name：策略名。

【描述】

ip policy route-policy 命令用来在接口上使能策略路由，**undo ip policy route-policy** 命令用来删除接口上已有的策略路由。

缺省情况下，禁止接口策略路由。

相关配置可参考命令 **ip local policy route-policy**。

【举例】

在接口 Ethernet 0/0/0 上使能策略路由，该策略路由由路由策略“AAA”指定。

```
[H3C-Ethernet0/0/0] ip policy route-policy AAA
```

7.1.13 route-policy

【命令】

route-policy *route-policy-name* { **permit** | **deny** } **node** *sequence-number*

undo route-policy *route-policy-name* [**permit** | **deny** | **node** *sequence-number*]

【视图】

系统视图

【参数】

route-policy-name：指定路由策略名。

permit：指定所定义的 route-policy 节点的匹配模式为允许模式。当报文满足该节点的所有 if-match 子句时，被允许通过该节点的过滤并执行该节点的 apply 子句；如报文不满足该节点的 if-match 子句，该 route-policy 的下一个节点将被测试。

deny：指定所定义的 route-policy 节点的匹配模式为拒绝模式。当报文满足该节点的所有 if-match 子句时被拒绝通过该节点的过滤，并且不会进行下一个节点的测试。

node：策略节点。

sequence-number：标识 route-policy 中的一个节点索引，当该 route-policy 用于路由信息过滤时，*sequence-number* 小的节点先被测试。

【描述】

route-policy 命令用来创建策略或一个策略节点，并进入 route-policy 视图，**undo route-policy** 命令用来删除已创建的 route-policy。

缺省情况下，没有 route-policy 被定义。

Route-policy 用于策略路由。一个 Route-policy 由若干节点组成，每一节点由一些 **if-match** 子句和 **apply** 子句组成。**if-match** 子句定义该节点的匹配规则，**apply** 子句定义通过该节点过滤后进行的动作。节点的 **if-match** 子句之间的过滤关系是“与”的关系，即必须满足该节点的所有 **if-match** 子句。Route-policy 节点之间的过滤关

系是“或”的关系，即通过一个节点的过滤就意味着通过该 Route-policy 的过滤。若没有通过任一节点的过滤，则通不过该 Route-policy 的过滤。

相关配置可参考命令 **if-match packet-length**、**if-match acl**、**apply ip-precedence**、**apply output-interface**、**apply ip-address next-hop**、**apply default output-interface**、**apply ip-address default next-hop**。

【举例】

配置一个路由策略 policy1，其节点序列号为 10，匹配模式为 permit，并进入 Route-policy 视图。

```
[H3C] route-policy policy1 permit node 10
[H3C-route-policy]
```

目 录

第 1 章 静态路由配置命令 1-1
1.1 路由表的显示命令 1-1
1.1.1 display ip routing-table 1-1
1.1.2 display ip routing-table acl 1-2
1.1.3 display ip routing-table *ip-address* 1-3
1.1.4 display ip routing-table *ip-address1 ip-address2* 1-5
1.1.5 display ip routing-table ip-prefix 1-6
1.1.6 display ip routing-table protocol 1-7
1.1.7 display ip routing-table radix 1-9
1.1.8 display ip routing-table statistics 1-9
1.1.9 display ip routing-table verbose 1-10
1.1.10 display ip routing-table vpn-instance 1-12
1.1.11 reset ip routing-table statistics protocol 1-13
1.2 静态路由配置命令 1-13
1.2.1 delete static-routes all 1-13
1.2.2 ip route-static 1-14
第 2 章 RIP配置命令 2-1
2.1 RIP配置命令 2-1
2.1.1 checkzero 2-1
2.1.2 debugging rip 2-2
2.1.3 default cost 2-2
2.1.4 display rip 2-3
2.1.5 display rip interface 2-4
2.1.6 display rip routing 2-5
2.1.7 filter-policy export 2-6
2.1.8 filter-policy import 2-7
2.1.9 host-route 2-8
2.1.10 import-route 2-9
2.1.11 ipv4-family vpn-instance 2-10
2.1.12 network 2-10
2.1.13 peer 2-11
2.1.14 preference 2-12
2.1.15 reset 2-12
2.1.16 rip 2-13
2.1.17 rip authentication-mode 2-13
2.1.18 rip input 2-14
2.1.19 rip metricin 2-15
2.1.20 rip metricout 2-16
2.1.21 rip output 2-16
2.1.22 rip split-horizon 2-17

2.1.23 rip version 2-17
2.1.24 rip work 2-18
2.1.25 summary 2-19
2.1.26 timers 2-20
2.1.27 traffic-share-across-interface 2-21
2.1.28 validate-source-address 2-21
第 3 章 OSPF配置命令 3-1
3.1 OSPF配置命令 3-1
3.1.1 abr-summary 3-1
3.1.2 area 3-2
3.1.3 asbr-summary 3-2
3.1.4 authentication-mode 3-3
3.1.5 debugging ospf 3-4
3.1.6 default cost 3-5
3.1.7 default interval 3-6
3.1.8 default limit 3-6
3.1.9 default tag 3-7
3.1.10 default type 3-7
3.1.11 default-cost 3-8
3.1.12 default-route-advertise 3-9
3.1.13 display debugging ospf 3-10
3.1.14 display ospf abr-asbr 3-10
3.1.15 display ospf asbr-summary 3-11
3.1.16 display ospf brief 3-13
3.1.17 display ospf cumulative 3-14
3.1.18 display ospf error 3-16
3.1.19 display ospf interface 3-19
3.1.20 display ospf lsdb 3-20
3.1.21 display ospf nexthop 3-22
3.1.22 display ospf peer 3-23
3.1.23 display ospf request-queue 3-25
3.1.24 display ospf retrans-queue 3-26
3.1.25 display ospf routing 3-27
3.1.26 display ospf vlink 3-28
3.1.27 filter-policy export 3-29
3.1.28 filter-policy import 3-30
3.1.29 import-route 3-31
3.1.30 log-peer-change 3-32
3.1.31 multi-path-number 3-33
3.1.32 network 3-34
3.1.33 nssa 3-34
3.1.34 ospf 3-35
3.1.35 ospf authentication-mode 3-36
3.1.36 ospf cost 3-37
3.1.37 ospf dr-priority 3-38

3.1.38 ospf mib-binding 3-38
3.1.39 ospf mtu-enable 3-39
3.1.40 ospf network-type 3-40
3.1.41 ospf timer dead 3-41
3.1.42 ospf timer hello 3-41
3.1.43 ospf timer poll 3-42
3.1.44 ospf timer retransmit 3-43
3.1.45 ospf trans-delay 3-43
3.1.46 peer 3-44
3.1.47 preference 3-45
3.1.48 reset ospf 3-45
3.1.49 router id 3-46
3.1.50 silent-interface 3-47
3.1.51 snmp-agent trap enable ospf 3-48
3.1.52 spf-schedule-interval 3-49
3.1.53 stub 3-50
3.1.54 vlink-peer 3-50
第 4 章 BGP配置命令 4-1
4.1 BGP配置命令 4-1
4.1.1 aggregate 4-1
4.1.2 bgp 4-2
4.1.3 compare-different-as-med 4-3
4.1.4 confederation id 4-3
4.1.5 confederation nonstandard 4-4
4.1.6 confederation peer-as 4-5
4.1.7 dampening 4-5
4.1.8 debugging bgp 4-6
4.1.9 default-route imported 4-7
4.1.10 default local-preference 4-8
4.1.11 default med 4-9
4.1.12 display bgp group 4-9
4.1.13 display bgp network 4-10
4.1.14 display bgp paths 4-11
4.1.15 display bgp peer 4-12
4.1.16 display bgp routing 4-15
4.1.17 display bgp routing as-path-acl 4-16
4.1.18 display bgp routing cidr 4-18
4.1.19 display bgp routing community 4-19
4.1.20 display bgp routing community-list 4-20
4.1.21 display bgp routing dampened 4-21
4.1.22 display bgp routing different-origin-as 4-22
4.1.23 display bgp routing flap-info 4-23
4.1.24 display bgp routing peer 4-25
4.1.25 display bgp routing peer dampened 4-26
4.1.26 display bgp routing peer regular-expression 4-27

4.1.27 display bgp routing regular-expression 4-28
4.1.28 display bgp routing statistic 4-29
4.1.29 display ip community-list 4-30
4.1.30 display ip as-path-acl 4-30
4.1.31 filter-policy export 4-31
4.1.32 filter-policy import 4-31
4.1.33 group 4-32
4.1.34 import-route 4-33
4.1.35 ip as-path-acl 4-34
4.1.36 ip community-list 4-35
4.1.37 log-peer-change 4-36
4.1.38 network 4-37
4.1.39 peer advertise-community 4-37
4.1.40 peer allow-as-loop 4-38
4.1.41 peer as-number 4-38
4.1.42 peer as-path-acl 4-39
4.1.43 peer connect-interface 4-40
4.1.44 peer default-route-advertise 4-40
4.1.45 peer description 4-41
4.1.46 peer ebgp-max-hop 4-42
4.1.47 peer enable 4-42
4.1.48 peer filter-policy 4-43
4.1.49 peer group 4-44
4.1.50 peer ip-prefix 4-45
4.1.51 peer next-hop-local 4-46
4.1.52 peer password 4-46
4.1.53 peer public-as-only 4-47
4.1.54 peer reflect-client 4-48
4.1.55 peer route-policy 4-48
4.1.56 peer route-update-interval 4-49
4.1.57 peer shutdown 4-50
4.1.58 peer timer 4-50
4.1.59 preference 4-51
4.1.60 reflect between-clients 4-52
4.1.61 reflector cluster-id 4-52
4.1.62 refresh bgp 4-53
4.1.63 reset bgp 4-54
4.1.64 reset bgp flap-info 4-55
4.1.65 reset bgp group 4-55
4.1.66 reset bgp dampening 4-56
4.1.67 summary 4-56
4.1.68 timer keep-alive hold 4-57
4.1.69 undo synchronization 4-57
4.2 MBGP配置命令 4-58
4.2.1 ipv4-family 4-58
4.2.2 ipv4-family vpnv4 4-59

4.2.3 peer enable 4-60
第 5 章 IP路由策略配置命令 5-1
5.1 IP路由策略配置命令 5-1
5.1.1 apply as-path 5-1
5.1.2 apply community 5-1
5.1.3 apply cost 5-2
5.1.4 apply cost-type 5-3
5.1.5 apply local-preference 5-3
5.1.6 apply origin 5-4
5.1.7 apply tag 5-5
5.1.8 display ip ip-prefix 5-6
5.1.9 display route-policy 5-6
5.1.10 filter-policy export 5-7
5.1.11 filter-policy import 5-7
5.1.12 if-match acl 5-8
5.1.13 if-match as-path 5-9
5.1.14 if-match community 5-10
5.1.15 if-match cost 5-10
5.1.16 if-match interface 5-11
5.1.17 if-match ip next-hop 5-12
5.1.18 if-match ip-prefix 5-13
5.1.19 if-match tag 5-13
5.1.20 ip ip-prefix 5-14
5.1.21 route-policy 5-15
第 6 章 路由容量配置命令 6-1
6.1 路由容量配置命令 6-1
6.1.1 display memory 6-1
6.1.2 memory auto-establish disable 6-2
6.1.3 memory auto-establish enable 6-3
6.1.4 memory 6-3

第1章 静态路由配置命令

📖 **说明：**

本章中有关 VPN 实例的参数解释及举例，请参见本手册的“VPN”模块。

1.1 路由表的显示命令

1.1.1 display ip routing-table

【命令】

display ip routing-table

【视图】

所有视图

【参数】

无

【描述】

display ip routing-table 命令用来查看路由表的摘要信息。

该命令以摘要形式显示路由表信息，每一行代表一条路由，内容包括：目的地址/掩码长度、协议、优先级、度量值、下一跳、输出接口。

使用 **display ip routing-table** 命令仅能查看到当前被使用的路由，即最佳路由。

【举例】

查看当前路由表的摘要信息。

```
<H3C> display ip routing-table
Routing Table: public net
Destination/Mask   Protocol   Pre Cost    Nexthop     Interface
1.1.1.0/24         DIRECT     0   0      1.1.1.1      Ethernet1/0/0
1.1.1.1/32         DIRECT     0   0      127.0.0.1    InLoopBack0
2.2.2.0/24         DIRECT     0   0      2.2.2.1      Ethernet2/0/0
2.2.2.1/32         DIRECT     0   0      127.0.0.1    InLoopBack0
127.0.0.0/8        DIRECT     0   0      127.0.0.1    InLoopBack0
127.0.0.1/32       DIRECT     0   0      127.0.0.1    InLoopBack0
```

1.1.2 display ip routing-table acl

【命令】

display ip routing-table acl *acl-number* [**verbose**]

【视图】

所有视图

【参数】

acl-number：通过数字引用的基本访问控制列表的编号，取值范围为 2000～2999。

verbose：当使用该参数时，显示通过过滤规则的、处于 active 状态和 inactive 状态的路由的详细信息。如果不使用该参数，将只显示通过过滤规则，且处于 active 状态的路由的摘要信息。

【描述】

display ip routing-table acl 命令用来查看通过指定基本访问控制列表过滤的路由。

此命令主要用于路由策略的跟踪显示，根据所输入的基本访问控制列表编号，显示通过该过滤规则的路由。

该命令只适用于查看通过基本访问控制列表过滤规则的路由。

【举例】

查看通过基本访问控制列表 ACL 2001 过滤的、处于 active 状态的路由的摘要信息。

```
<H3C> display ip routing-table acl 2001
Routes matched by access-list 2001:
Summary count: 4
Destination/Mask   Protocol   Pre      Cost     Nexthop      Interface
127.0.0.0/8        Direct     0        0        127.0.0.1    InLoopBack0
127.0.0.1/32       Direct     0        0        127.0.0.1    InLoopBack0
169.0.0.0/8        Static     60       0        2.1.1.1      LoopBack1
169.0.0.0/15       Static     60       0        2.1.1.1      LoopBack1
```

查看通过基本访问控制列表 ACL2001 过滤的 active 和 inactive 的路由的详细信息。

```
<H3C> display ip routing-table acl 2001 verbose
Routes matched by access-list 2001:
Generate Default: no
+ = Active Route, - = Last Active, # = Both* = Next hop in use
Summary count:5
**Destination: 127.0.0.0       Mask: 255.0.0.0
  Protocol: #Direct         Preference: 0
```

```
  *NextHop: 127.0.0.1      Interface: 127.0.0.1(InLoopBack0)
  Vlinkindex: 0
  State:  <NoAdvise Int ActiveU Retain Multicast Unicast>
  Age: 3:47    Metric: 0/0
**Destination: 127.0.0.1       Mask: 255. 255. 255. 255
  Protocol: #Direct        Preference: 0
  *NextHop: 127.0.0.1      Interface: 127.0.0.1(InLoopBack0)
Vlinkindex: 0
State: <NotInstall NoAdvise Int ActiveU Retain Gateway Multicast Unicast>
  Age: 3:47    Metric: 0/0
**Destination: 179.0.0.0       Mask: 255.0.0.0
  Protocol: #Static        Preference: 60
  *NextHop: 4.1.1.1
  Vlinkindex: 0
  State: <Int Hidden Static Unicast>
  Age: 3:47    Metric: 0/0
**Destination: 169.0.0.0       Mask: 255.0.0.0
  Protocol: #Static        Preference: 60
  *NextHop: 2.1.1.1        Interface: 2.1.1.1(LoopBack1)
  Vlinkindex: 0
  State: <Int ActiveU Static Unicast>
  Age: 3:47    Metric: 0/0
**Destination: 169.0.0.0       Mask: 255.254.0.0
  Protocol: #Static        Preference: 60
  *NextHop: 2.1.1.1        Interface: 2.1.1.1(LoopBack1)
  Vlinkindex: 0
  State: <Int ActiveU Static Unicast>
  Age: 3:47    Metric: 0/0
```

1.1.3 display ip routing-table *ip-address*

【命令】

display ip routing-table *ip-address* [*mask*] [**longer-match**] [**verbose**]

【视图】

所有视图

【参数】

ip-address：目的 IP 地址，点分十进制格式。

mask：IP 地址掩码，点分十进制格式或以整数形式表示的长度，当用整数时，取值范围为 0～32。

longer-match：自然掩码范围内匹配的所有目的地址路由。

verbose：当使用该参数时，显示处于 active 状态和 inactive 状态的路由的详细信息。如果不使用该参数，将只显示处于 active 状态的路由的摘要信息。

【描述】

display ip routing-table *ip-address* 命令用来查看指定目的地址的路由信息。

使用不同的可选参数，命令的输出也不相同，以下是对该命令不同形式的输出说明：

- **display ip routing-table** *ip-address*

如果目的地址 *ip-address* 在自然掩码范围内有相应的路由，则将显示其全部子网路由，否则只显示与目的地址 *ip-address* 最长匹配的路由。只显示处于 active 状态的匹配路由。

- **display ip routing-table** *ip-address mask*

只显示与指定目的地址及掩码精确匹配的路由。

- **display ip routing-table** *ip-address* **longer-match**

显示目的地址在自然掩码范围内匹配的所有目的地址路由。

【举例】

在自然掩码范围内有相应路由，查看摘要信息。

```
<H3C> display ip routing-table 169.0.0.0
Routing Tables:
Summary count:1
Destination/Mask      Protocol    Pre Cost    Nexthop      Interface
169.0.0.0/16          Static      60  0       2.1.1.1      LoopBack1
```

在自然掩码范围内没有相应的路由（只显示最长匹配的路由），查看摘要信息。

```
<H3C> display ip routing-table 169.253.0.0
Routing Tables:
Summary count:1
Destination/Mask      Protocol    Pre     Cost    Nexthop      Interface
169.0.0.0/8           Static      60      0       2.1.1.1      LoopBack1
```

在自然掩码范围内有相应路由，查看详细信息。

```
<H3C> display ip routing-table 169.0.0.0 verbose
Routing Tables:
Generate Default: no
+ = Active Route, - = Last Active, # = Both* = Next hop in use
Summary count:2
**Destination: 169.0.0.0      Mask: 255.0.0.0
  Protocol: #Static        Preference: 60
  *NextHop: 2.1.1.1        Interface: 2.1.1.1(LoopBack1)
  Vlinkindex: 0
```

```
  State: <Int ActiveU Static Unicast>
  Age: 3:47    Metric: 0/0
**Destination: 169.0.0.0       Mask: 255.254.0.0
  Protocol: #Static         Preference: 60
  *NextHop: 2.1.1.1         Interface: 2.1.1.1(LoopBack1)
  Vlinkindex: 0
  State: <Int ActiveU Static Unicast>
  Age: 3:47    Metric: 0/0
```

在自然掩码范围内没有相应的路由（只显示最长匹配的路由），查看详细信息。

```
<H3C> display ip routing-table 169.253.0.0 verbose
Routing Tables:
Generate Default: no
+ = Active Route, - = Last Active, # = Both* = Next hop in use
Summary count:1
**Destination: 169.0.0.0       Mask: 255.0.0.0
  Protocol: #Static         Preference: -60
  *NextHop: 2.1.1.1
  Vlinkindex: 0
  State: <Int ActiveU Static Unicast>
  Age: 3:47    Metric: 0/0
```

1.1.4 display ip routing-table *ip-address1 ip-address2*

【命令】

display ip routing-table *ip-address1 mask1 ip-address2 mask2* [**verbose**]

【视图】

所有视图

【参数】

ip-address1、*ip-address2*：目的 IP 地址，点分十进制格式。*ip-address1* 和 *ip-address2* 共同确定一个地址范围，显示该地址范围内的路由。

mask1、*mask2*：IP 地址掩码，点分十进制格式或以整数形式表示的长度。

verbose：当使用该参数时，显示处于 active 状态和 inactive 状态的路由的详细信息。如果不使用该参数，将只显示处于 active 状态的路由的摘要信息。

【描述】

display ip routing-table *ip-address1 ip-address2* 命令用来查看指定目的地址范围内的路由信息。

【举例】

查看目的地址从 1.1.1.0 到 2.2.2.0 范围内的路由信息。

```
<H3C> display ip routing-table 1.1.1.0 24 2.2.2.0 24
Routing tables:
  Summary count: 3
Destination/Mask   Protocol   Pre Cost   Nexthop       Interface
1.1.1.0/24         DIRECT      0   0     1.1.1.1       Ethernet1/0/0
1.1.1.1/32         DIRECT      0   0     127.0.0.1     InLoopBack0
2.2.2.0/24         DIRECT      0   0     2.2.2.1       Ethernet2/0/0
```

1.1.5 display ip routing-table ip-prefix

【命令】

display ip routing-table ip-prefix *ip-prefix-name* [**verbose**]

【视图】

所有视图

【参数】

ip-prefix-name：前缀列表名称。

verbose：当使用该参数时，显示通过过滤规则的、处于 active 状态和 inactive 状态的路由的详细信息。如果不使用该参数，将只显示通过过滤规则且处于 active 状态的路由的摘要信息。

【描述】

display ip routing-table ip-prefix 命令用来查看通过指定前缀列表过滤的路由。

如果指定的前缀列表不存在，当使用了 **verbose** 参数时将显示所有 active 及 inactive 路由的详细信息，不使用 **verbose** 参数则只显示所有 active 路由的摘要信息。

【举例】

查看通过前缀列表 abc2 过滤的 active 路由的摘要信息。

```
<H3C> display ip routing-table ip-prefix abc2
Routes matched by ip-prefix abc2:
 Summary count: 4
Destination/Mask  Protocol    Pre Cost    Nexthop      Interface
127.0.0.0/8       Direct      0   0       127.0.0.1    InLoopBack0
127.0.0.1/32      Direct      0   0       127.0.0.1    InLoopBack0
169.0.0.0/8       Static      60  0       2.1.1.1      LoopBack1
169.0.0.0/15      Static      60  0       2.1.1.1      LoopBack1
```

查看通过前缀列表 abc2 过滤的 active 和 inactive 路由的详细信息。

```
<H3C> display ip routing-table ip-prefix abc2 verbose
Routes matched by ip-prefix abc2:
 Generate Default: no
 + = Active Route, - = Last Active, # = Both   * = Next hop in use
Summary count:4
**Destination: 127.0.0.0  Mask: 255.0.0.0
 Protocol: #Direct        Preference: 0
 *NextHop: 127.0.0.1      Interface: 127.0.0.1(InLoopBack0)
 Vlinkindex: 0
 State:  <NoAdvise Int ActiveU Retain Multicast Unicast>
 Age: 3:47    Metric: 0/0
**Destination: 127.0.0.1  Mask: 255. 255. 255. 255
 Protocol: #Direct        Preference: 0
 *NextHop: 127.0.0.1      Interface: 127.0.0.1(InLoopBack0)
 Vlinkindex: 0
State: <NotInstall NoAdvise Int ActiveU Retain Gateway Multicast Unicast>
 Age: 3:47    Metric: 0/0
**Destination: 179.0.0.0      Mask: 255.0.0.0
 Protocol: #Static        Preference:-60
 *NextHop: 4.1.1.1
 Vlinkindex: 0
 State: <Int Hidden Static Unicast>
 Age: 3:47    Metric: 0/0
**Destination: 169.0.0.0      Mask: 255.0.0.0
Protocol: #Static     Preference: 60
*NextHop: 2.1.1.1     Interface: 2.1.1.1(LoopBack1)
Vlinkindex: 0
State: <Int ActiveU Static Unicast>
Age: 3:47             Metric: 0/0
**Destination: 169.0.0.0      Mask: 255.254.0.0
Protocol: #Static     Preference: 60
*NextHop: 2.1.1.1     Interface: 2.1.1.1(LoopBack1)
Vlinkindex: 0
State: <Int ActiveU Static Unicast>
Age: 3:47             Metric: 0/0
```

1.1.6 display ip routing-table protocol

【命令】

display ip routing-table protocol *protocol* [**inactive** | **verbose**] [**vpn-instance** *vpn-instance-name*]

【视图】

所有视图

【参数】

protocol：该参数有以下多种可选值：

- **direct**：显示直连路由信息。
- **static**：显示静态路由信息。
- **bgp**：显示 BGP 路由信息。
- **ospf**：显示 OSPF 路由信息。
- **ospf-ase**：显示 OSPF ASE 路由信息。
- **ospf-nssa**：显示 OSPF NSSA 路由信息。
- **rip**：显示 RIP 路由信息。

inactive：显示处于 inactive 状态的路由信息。如果不使用该参数，则显示处于 active 和 inactive 状态的路由信息。

verbose：当使用该参数时，显示路由的详细信息。如果不使用该参数，将只显示处于 active 状态的路由信息。

vpn-instance *vpn-instance-name*： 指定 VPN 实例名。

【描述】

display ip routing-table protocol 命令用来查看指定路由协议的路由信息。

没有指定 **vpn-instance** 时，显示的是公网路由信息；当指定了 **vpn-instance** 时，显示的是私网路由信息。

【举例】

查看所有直连路由的摘要信息。

```
<H3C> display ip routing-table protocol direct
DIRECT Routing tables:
Summary count: 4
DIRECT Routing tables status:<active>:
Summary count: 3
Destination/Mask      Protocol     Pre Cost     Nexthop      Interface
20.1.1.1/32           DIRECT       0   0        127.0.0.1    InLoopBack0
127.0.0.0/8           DIRECT       0   0        127.0.0.1    InLoopBack0
127.0.0.1/32          DIRECT       0   0        127.0.0.1    InLoopBack0
DIRECT Routing tables status:<inactive>:
Summary count: 1
Destination/Mask      Protocol    Pre  Cost     Nexthop      Interface
210.0.0.1/32          DIRECT       0   0        127.0.0.1    InLoopBack0
```

查看静态路由表。

```
<H3C> display ip routing-table protocol static
STATIC Routing tables:
  Summary count: 1
STATIC Routing tables status:<active>:
  Summary count: 0
STATIC Routing tables status:<inactive>:
  Summary count: 1
Destination/Mask   Protocol   Pre Cost      Nexthop      Interface
1.2.3.0/24         STATIC      60  0         1.2.4.5      Ethernet2/0/0
```

1.1.7 display ip routing-table radix

【命令】

display ip routing-table radix

【视图】

所有视图

【参数】

无

【描述】

display ip routing-table radix 命令用来查看以树的形式表示的路由表信息。

【举例】

查看以树的形式表示的路由表信息。

```
<H3C> display ip routing-table radix
Radix tree for INET (2) inodes 7 routes 5:
              +-32+--{210.0.0.1
          +--0+
           | | +--8+--{127.0.0.0
           | | | +-32+--{127.0.0.1
           | +--1+
           |  +--8+--{20.0.0.0
           |  +-32+--{20.1.1.1
```

1.1.8 display ip routing-table statistics

【命令】

display ip routing-table statistics [**vpn-instance** *vpn-instance-name*]

【视图】

所有视图

【参数】

vpn-instance *vpn-instance-name*：指定 vpn-instance 的名称。

【描述】

display ip routing-table statistics 命令用来查看路由的统计信息。

当 **display ip routing-table statistics** 命令中没有指定 **vpn-instance** 时，显示的是公网路由信息；当指定了 **vpn-instance** 时，显示的是私网路由信息。

路由的统计信息包括路由总数目，协议添加、删除路由数目、打上 deleted 标志没有删除的路由、active 路由、inactive 路由数目。

【举例】

查看路由的统计信息。

```
<H3C> display ip routing-table statistics
Routing tables:
Proto      route       active      added       deleted
DIRECT     6           6           10          4
STATIC     1           0           1           0
BGP        0           0           0           0
RIP        0           0           0           0
OSPF       2           0           2           0
O_ASE      0           0           0           0
O_NSSA     0           0           0           0
AGGRE      0           0           0           0
Total      9           6           13          4
```

1.1.9 display ip routing-table verbose

【命令】

display ip routing-table verbose

【视图】

所有视图

【参数】

无

【描述】

display ip routing-table verbose 命令查看路由表的全部详细信息。

当带关键字 **verbose** 时显示全部路由表的详细信息。先显示用于路由状态描述的符号，然后输出整个路由表的统计数字，最后依次输出每条路由的详细描述。

使用 **display ip routing-table verbose** 命令能查看到当前所有的路由，包括未激活的和无效的路由。

【举例】

查看路由表的全部详细信息。

```
<H3C> display ip routing-table verbose
 Routing Tables:
  + = Active Route, - = Last Active, # = Both    * = Next hop in use

  Destinations: 10012    Routes: 10012
  Holddown: 0    Delete: 102611  Hidden: 0

**Destination: 1.1.1.0           Mask: 255.255.255.0
         Protocol: #DIRECT       Preference: 0
         *NextHop: 1.1.1.2          Interface: 1.1.1.2(Ethernet0/0)
         State: <Int ActiveU Retain Unicast>
         Age: 22:35:10           Cost: 0/0
```

首先显示整个路由表的统计数据，然后依次输出每条路由的详细描述。路由状态的含义如下表所示：

表1-1 display ip routing-table verbose 命令输出信息描述

主要字段	描述
Holddown	当前被 Holddown 的路由数目——Holddown 是某些 D-V（distance vector）路由协议（如 RIP）为了避免错误路由的扩散、提高路由不可达信息的快速准确传播而采用的一种路由发布策略。它往往在一段时间间隔内固定地发布某条路由，而不管当前实际找到的到同一目的地的路由发生了什么变化。其细节参见具体的路由协议。
Delete	当前被删除的路由数目。
Hidden	当前被隐藏的路由数目——有些路由由于某种原因（如接口 Down）暂时不可用，但是又不希望被删除，我们把这种路由隐藏起来，以便以后能重新恢复。

1.1.10 display ip routing-table vpn-instance

【命令】

display ip routing-table vpn-instance *vpn-instance-name* [*ip-address*] [**verbose**]

【视图】

所有视图

【参数】

vpn-instance-name：VPN 实例名。

ip-address：目的 IP 地址，点分十进制形式。

verbose：当使用该参数时，显示路由的详细信息。如果不使用该参数，将只显示路由的摘要信息。

【描述】

display ip routing-table vpn-instance 命令用来查看指定 VPN-instance 中的路由信息。

如果在指定目的 IP 地址的同时使用 **verbose** 参数，可以查看到 VPN-instance 中到指定目的地址的所有路由，包括本地路由和从远端学到的路由。

【举例】

查看名为 vpn1 的 VPN-instance 中，目的地址为 10.1.1.1 的所有路由的详细信息。

```
<H3C> display ip routing-table vpn-instance vpn1 10.1.1.1 verbose
Routing tables:
  Generate Default: no
  + = Active Route, - = Last Active, # = Both    * = Next hop in use
  Summary count: 2
**Destination: 10.1.1.1          Mask: 255.255.255.255
         Protocol: #DIRECT       Preference: 0
         *NextHop: 127.0.0.1        Interface: 127.0.0.1(InLoopBack0)
         Vlinkindex: 0
         State: <NoAdvise Int ActiveU Retain Gateway Unicast>
         Age: 54  Cost: 0/0
**Destination: 10.1.1.0          Mask: 255.255.255.0
         Protocol: #DIRECT       Preference: 0
         *NextHop: 10.1.1.1         Interface: 10.1.1.1(LoopBack0)
         Vlinkindex: 0
         State: <Int ActiveU Retain Unicast>
         Age: 54  Cost: 0/0
```

查看名为 vpn1 的 VPN-instance 中，目的地址为 10.1.1.1 路由概要信息。

```
<H3C> display ip routing-table vpn-instance vpn1 10.1.1.1
Routing tables: vpn1                    Route-Distinguisher: 100:1
Destination/Mask   Protocol  Pre  Cost     Nexthop         Interface
10.1.1.1/32        DIRECT    0    0        127.0.0.1       InLoopBack0
10.1.1.0/24        DIRECT    0    0        10.1.1.1        LoopBack0
```

1.1.11 reset ip routing-table statistics protocol

【命令】

reset ip routing-table [**vpn-instance** *vpn-instance-name*] **statistics protocol** *protocol-type*

【视图】

用户视图

【参数】

vpn-instance *vpn-instance name*：指定 VPN 实例的名称。

protocol-type：指定协议类型，包括所有协议、BGP、直连路由、OSPF、OSPF_ASE、OSPF_NSSA、RIP、静态路由可选项。

【描述】

reset ip routing-table statistics protocol 命令用来清除路由表信息。

【举例】

清除 OSPF 路由信息。

```
<H3C> reset ip routing-table statistics protocol ospf
This will erase the specific routing counters information.
Are you sure?[Y/N]y
<H3C>
%Sep  12  15:33:42:652  2005  H3C  RTPRO/5/ResetStatistics:reset  ip  route
statistics protocol OSPF
```

1.2 静态路由配置命令

1.2.1 delete static-routes all

【命令】

delete static-routes all

【视图】

系统视图

【参数】

无

【描述】

delete static-routes all 命令用来删除全部静态路由。

使用本命令删除静态路由时，系统会提示确认，确认后才会删除所配置的全部静态路由。

相关配置可参考命令 **ip route-static** 和 **display ip routing-table**。

【举例】

删除防火墙的全部静态路由。

```
[H3C] delete static-routes all
Are you sure to delete all the unicast static routes?[Y/N]
```

1.2.2 ip route-static

【命令】

ip route-static *ip-address* { *mask* | *mask-length* } { *interface-type interface-number* | *nexthop-address* } [**preference** *preference-value*] [**reject** | **blackhole**] [**detect-group** *group-number*] [**description** *text*]

undo ip route-static *ip-address* { *mask* | *mask-length* } [*interface-type interface-number* | *nexthop-address*] [**preference** *preference-value*]

ip route-static vpn-instance *vpn-instance-name1 vpn-instance-name2 …* *ip-address* { *mask* | *mask-length* } [*interface-type interface-number* [*nexthop-address*] | **vpn-instance** *vpn-nexthop-name nexthop-address* | *nexthop-address* [**public**]] [**preference** *preference-value*] [**reject** | **blackhole**] [**detect-group** *group-number*] [**description** *text*]

undo ip route-static vpn-instance *vpn-instance-name1 vpn-instance-name2 …* *ip-address* { *mask* | *mask-length* } [*interface-type interface-number* | **vpn-instance** *vpn-nexthop-name nexthop-address* | *nexthop-address* [**public**]] [**preference** *preference-value*]

【视图】

系统视图

【参数】

ip-address：目的 IP 地址，用点分十进制格式表示。

mask：掩码。

mask-length：掩码长度。由于要求 32 位掩码中的“1”必须是连续的，因此点分十进制格式的掩码也可以用掩码长度 *mask-length* 来代替（掩码长度是掩码中连续“1”的位数）。

interface-type interface-number：指定该静态路由的出接口类型及接口号。可以指定公网或者其他 vpn-instance 下面的接口作为该静态路由的出接口。

vpn-instance-name：指定 VPN 实例的名字，最多可以指定 6 个。

vpn-nexthop-name：用于指定该静态路由下一跳所在的 vpn-instance。

nexthop-address：指定该静态路由的下一跳 IP 地址（点分十进制格式）。

preference-value：为该静态路由的优先级别，范围 1～255。

reject：指明为不可达路由。

blackhole：指明为黑洞路由。

group-number：自动侦测组的编号，取值范围为 1～50。

text：静态路由的描述，描述内容最长为 60 个字符。

【描述】

ip route-static 命令用来配置静态路由，**undo ip route-static** 命令用来删除静态路由配置。

到同一目的地址、下一跳相同、**preference** 不同的两条静态路由是两条完全不同的路由，系统会优先选择 **preference** 值小（即优先级较高）的作为当前路由。

undo ip route-static 命令可以删除到同一目的地址、下一跳相同的所有静态路由，而 **undo ip route-static preference** 命令可以删除指定 **preference** 的静态路由。

ip route-static vpn-instance 命令用来配置静态路由，在多角色主机应用背景下，用于配置一个私网下面的静态路由指向另外一个私网或者公网的接口作为该静态路由的出接口。**undo ip route-static vpn-instance** 命令用来取消静态路由的配置。

缺省情况下，系统可以获取到去往与防火墙直连的子网路由。在配置静态路由时如果不指定优先级，则缺省为 60。如果没有指明 **reject** 或 **blackhole**，则缺省为可达路由。

配置静态路由的注意事项：

- 当目的 IP 地址和掩码均为 0.0.0.0 时，就是缺省路由。当查找路由表失败后，根据缺省路由进行包的转发。
- 对优先级的不同配置，可以灵活应用路由管理策略。比如配置到达相同目的地的多条路由，如果指定相同优先级，则可实现负载分担，如果指定不同优先级，则可实现路由备份。

- 在配置静态路由时，可指定发送接口，也可指定下一跳地址，具体采用哪种方法，可需要根据实际情况而定。对于支持网络地址到链路层地址解析的接口或点到点接口，可以指定发送接口，也可以指定下一跳地址；对于 NBMA 接口，如封装 X.25 或帧中继的接口、拨号口等，支持点到多点，这时除了配置 IP 路由外，还需在链路层建立二次路由，即 IP 地址到链路层地址的映射，这种情况下配置静态路由不能指定发送接口，应配置下一跳 IP 地址。
- 在某些情况下（如链路层封装 PPP），配置防火墙的时候可能根本就不知道对端地址，这时可以指定发送接口；在指定发送接口后，当对端地址更改时此防火墙的配置就不需要修改了。
- 当前静态路由不支持插卡热插拔事件，即拔掉插卡后，相应的静态路由仍然存在，需要手工删除。

相关配置可参考命令 **display ip routing-table**。

【举例】

配置缺省路由的下一跳为 129.102.0.2。

```
[H3C] ip route-static 0.0.0.0 0.0.0.0 129.102.0.2
```

配置静态路由，该静态路由的目的地址为 100.1.0.0，下一跳地址为 1.1.1.2。

```
[H3C] ip route-static 100.1.0.0 16 1.1.1.2
```

第2章 RIP 配置命令

📖 **说明：**

本章中有关 VPN 实例的参数解释及举例，请参见本手册的“VPN”模块。

2.1 RIP 配置命令

2.1.1 checkzero

【命令】

checkzero

undo checkzero

【视图】

RIP 视图

【参数】

无

【描述】

checkzero 命令用来对 RIP-1 报文的零域进行检查，**undo checkzero** 命令用来取消对零域的检查操作。

RIP-1 缺省进行零域检查操作。

根据协议（RFC1058）规定，RIP-1 的报文中有些区域必须为零，称之为零域（zero field）。可以使用 **checkzero** 命令来启动和禁止对 RIP-1 报文的查零操作。进行查零操作时如果收到零域不为零的 RIP-1 报文，则拒绝处理。

由于 RIP-2 的报文没有零域，所以此命令对 RIP-2 没有作用。

【举例】

不对 RIP-1 报文进行零域检查操作。

```
[H3C-rip] undo checkzero
```

2.1.2 debugging rip

【命令】

debugging rip { **packet** | **receive** | **send** } [**interface** *type number*]

undo debugging rip { **packet** | **receive** | **send** }

【视图】

用户视图

【参数】

packet：打开 RIP 报文调试信息开关。

receive：打开 RIP 接收报文情况调试开关。

send：打开 RIP 发送报文情况调试开关。

interface *type number*：在指定接口上打开 RIP 调试信息开关。

【描述】

debugging rip 命令用来打开 RIP 调试信息开关，**undo debugging rip** 命令用来关闭 RIP 调试信息开关。

该命令可使用户了解当前各接口收发 RIP 报文的情况。

【举例】

打开 RIP 报文调试信息开关。

```
<H3C> debugging rip packet
```

2.1.3 default cost

【命令】

default cost *value*

undo default cost

【视图】

RIP 视图

【参数】

value：所要设定的缺省路由权值，取值范围为 1～16，缺省的路由权值为 1。

【描述】

default cost 命令用来设置引入路由的缺省路由权，**undo default cost** 命令用来将其恢复为缺省值。

当使用 **import-route** 命令引入其它协议路由时，如果不指定具体的路由权值，则以 **default cost** 所指定的缺省路由权值引入。

相关配置可参考命令 **import-route**。

【举例】

设定引入其它路由协议路由的缺省路由权为 3。

```
[H3C-rip] default cost 3
```

2.1.4 display rip

【命令】

display rip [**vpn-instance** *vpn-instance-name*]

【视图】

所有视图

【参数】

vpn-instance *vpn-instance-name*：VPN 实例名。

【描述】

display rip 命令用来显示 RIP 协议的当前运行状态及配置信息。

【举例】

查看 RIP 协议的当前运行状态及配置信息。

```
<H3C> display rip
  RIP is running
  public net
    Checkzero is on         Default cost : 1
    Summary is on           Preference : 100
    Validate-source-address is on
    Traffic-share-across-interface is off
    Period update timer : 30
    Timeout timer : 180
    Garbage-collection timer : 120
    No peer router

<H3C> display rip vpn-instance aaa
  RIP is running
  private net VPN-Instance: aaa
    Checkzero is on         Default cost : 1
    Summary is on           Preference : 100
```

```
Validate-source-address is on
Traffic-share-across-interface is off
Period update timer : 30
Timeout timer : 180
Garbage-collection timer : 120
No peer router
Network :
1.0.0.0
```

表2-1 display rip 命令显示说明

项目	描述
RIP is turned on	RIP 被使能
public net	公网路由信息
private net VPN-Instance	私网路由信息
Checkzero is on	使能 RIP 的零域检查
Default cost : 1	引入路由的缺省路由权值为 1
Summary is on	使能 RIP 的路由聚合功能
Preference : 100	RIP 协议的优先级为 100
Validate-source-address is on	使能检查 RIP 报文的源地址
Traffic-share-across-interface is off	关闭 RIP 在接口间实现负载分担功能
Period update timer : 30 Timeout timer : 180 Garbage-collection timer : 120	RIP 三个定时器的设置
No peer router	没有 RIP 邻居

2.1.5 display rip interface

【命令】

display rip interface [**vpn-instance** *vpn-instance-name*]

【视图】

所有视图

【参数】

vpn-instance *vpn-instance-name*：VPN 实例名。

【描述】

display rip interface 命令用来显示 RIP 的接口信息。

【举例】

显示 RIP 的接口信息。

```
<H3C> display rip interface
                        RIP Interface: public net

Address         Interface         Ver MetrIn/Out Input Output  Split-horizon
1.0.0.1         Vlan-interface100 2   0/1        on     on      on
```

表2-2 display rip interface 命令显示信息说明

项目	描述
Address	运行 RIP 协议的接口的 IP 地址（需要在 RIP 协议视图下，通过 **network** 命令使能该地址所在网段）
Interface	运行 RIP 协议的接口的名称，该接口的 IP 地址与 Address 字段的 IP 地址对应
Ver	接口上运行的 RIP 协议的版本
MetrIn/Out	接收/发送路由时添加的附加路由权值
Input	是否允许接口接收 RIP 报文（on 表示允许，off 表示不允许）
Output	是否允许接口发送 RIP 报文（on 表示允许，off 表示不允许）
Split-horizon	是否启用了水平分割（on 表示启用，off 表示关闭）

2.1.6 display rip routing

【命令】

display rip routing [**vpn-instance** *vpn-instance-name*]

【视图】

所有视图

【参数】

vpn-instance *vpn-instance-name*：指定 VPN 实例的名称。

【描述】

display rip routing 命令用来显示 RIP 路由表，包括正常路由和 garbage-collection 状态的路由。

如果没有指定 vpn-instance 参数，则显示公网的 RIP 路由；如果有 vpn-instance 参数，则显示指定 vpn-instance 的 RIP 路由。

【举例】

显示 RIP 路由。

```
[H3C] display rip routing
                    RIP routing table: public net

A = Active     I = Inactive     G = Garbage collection
C = Change     T = Trigger RIP

Destination/Mask    Cost  NextHop          Age    SourceGateway     Att
90.0.0.0/8          1     30.0.0.1         6s     30.0.0.1          A
95.0.0.0/8          1     30.0.0.1         6s     30.0.0.1          A
```

表2-3 display rip routing 命令显示信息说明

项目	含义
Destination/Mask	目的地址/掩码长度
Cost	路由权值
NextHop	路由的下一跳地址
Age	路由在路由表中存在的时间（老化时间）
SourceGateway	源网关地址，路由是从该地址对应的网关学习到的
Att	表示该条路由的状态，包含下面几种取值： A = Active I = Inactive G = Garbage collection C = Change T = Trigger RIP

2.1.7 filter-policy export

【命令】

filter-policy { *acl-number* | **ip-prefix** *ip-prefix-name* | **route-policy** *route-policy-name* } **export** [*routing-protocol*]

undo filter-policy { *acl-number* | **ip-prefix** *ip-prefix-name* | **route-policy** *route-policy-name* } **export** [*routing-protocol*]

【视图】

RIP 视图

【参数】

acl-number：用于过滤路由信息目的地址的访问列表号。

ip-prefix-name：用于过滤路由信息目的地址的地址前缀列表名。

route-policy-name：用于过滤路由信息的路由策略名。使得 RIP 协议能够根据 acl/cost/interface/ip/ip-prefix/tag 等字段来决定发送或者接受哪些路由。

routing-protocol：将被过滤路由信息的路由协议，目前可选择 **direct**、**bgp**、**ospf**、**ospf-ase**、**ospf-nssa** 和 **static**。

【描述】

filter-policy export 命令用来设置 RIP 对发布的路由信息进行过滤，**undo filter-policy export** 命令用来取消对发布路由信息的过滤。

缺省情况下，RIP 不对发布的路由信息进行过滤。

相关配置可参考命令 **acl**，**filter-policy import** 和 **ip ip-prefix**。

【举例】

设置按照访问列表 acl 2003 来过滤发布的路由信息。

```
[H3C-rip] filter-policy 2003 export
```

2.1.8 filter-policy import

【命令】

filter-policy gateway *ip-prefix-name* **import**

undo filter-policy gateway *ip-prefix-name* **import**

filter-policy { *acl-number* | **ip-prefix** *ip-prefix-name* [**gateway** *ip-prefix-name*] | **route-policy** *route-policy-name* } **import**

undo filter-policy { *acl-number* | **ip-prefix** *ip-prefix-name* [**gateway** *ip-prefix-name*] | **route-policy** *route-policy-name* } **import**

【视图】

RIP 视图

【参数】

ip-prefix-name：用于过滤路由信息目的地址的地址前缀列表名。

acl-number：用于过滤路由信息目的地址的访问列表号。

gateway *ip-prefix-name*：用于过滤发布该路由信息的邻居路由器地址的地址前缀列表名。

route-policy-name：用于过滤路由信息的路由策略名。使得 RIP 协议能够根据 acl/cost/interface/ip/ip-prefix/tag 等字段来决定来发送或者接受哪些路由。

【描述】

filter-policy gateway 命令用来配置对接收的指定地址发布的路由信息进行过滤，**undo filter-policy gateway** 命令用来取消对接收的指定地址发布的路由信息进行过滤。

filter-policy import 命令配置对接收的全局路由信息进行过滤，**undo filter-policy import** 命令用来取消对接收的全局路由信息进行过滤。

缺省情况下，RIP 不对接收的路由信息进行过滤。

通过指定访问列表和地址前缀列表可以控制 RIP 接收路由的范围。

相关配置可参考命令 **acl**，**filter-policy export** 和 **ip ip-prefix**。

【举例】

设置按照访问列表 acl 2003 来过滤全局路由信息。

```
[H3C-rip] filter-policy 2003 import
```

2.1.9 host-route

【命令】

host-route

undo host-route

【视图】

RIP 视图

【参数】

无

【描述】

host-route 命令用来控制 RIP 接收主机路由，**undo host-route** 命令用来拒绝接收主机路由。

缺省情况下，防火墙接收主机路由。

在某些特殊情况下，RIP 会收到大量的同一网段的主机路由，这些路由对于选路没有多少作用，却占用了大量的资源。这时可以使用 **undo host-route** 来拒绝接受主机路由。

【举例】

指定 RIP 拒绝接收主机路由。

```
[H3C-rip] undo host-route
```

2.1.10 import-route

【命令】

import-route *protocol* [**allow-ibgp**] [**cost** *value*] [**route-policy** *route-policy-name*]

undo import-route *protocol*

【视图】

RIP 视图

【参数】

protocol：可引入的源路由协议，目前 RIP 可引入的路由包括：**direct**、**ospf**、**ospf-ase**、**ospf-nssa**、**static** 和 **bgp**。

allow-ibgp：当 *protocol* 为 BGP 时，**allow-ibgp** 为可选关键字。**import-route bgp** 表示只引入 EBGP 路由，**import-route bgp allow-ibgp** 表示将 IBGP 路由也引入，该配置危险，请慎用！

value：所要引入的路由权值。取值范围为 1～16，缺省为 1。

route-policy *route-policy-name*：只有满足指定 Route-policy 的匹配条件的路由才被引入。

【描述】

import-route 命令用来在 RIP 协议中引入其它协议的路由，**undo import-route** 命令用来取消已经引入的相应协议的路由。

缺省情况下，RIP 不引入其它路由。

import-route 命令用于以一定的 *value* 值引入其它协议的路由。RIP 将引入的路由视同自己的路由并以指定的 *value* 一同发送。此命令能大大地提高 RIP 获取路由的能力，从而提高 RIP 的性能。

如果不指定 **cost** *value*，则按缺省路由权（**default cost**）引入，取值范围为 1～16，如果大于或等于 16，表示为不可达路由，在 120 秒之后不再发送。

相关配置可参考命令 **default cost**。

【举例】

引入静态路由，权值为 4。

```
[H3C-rip] import-route static cost 4
```

设定缺省路由权，并以缺省路由权引入 OSPF 路由。

```
[H3C-rip] default cost 3
[H3C-rip] import-route ospf
```

2.1.11 ipv4-family vpn-instance

【命令】

ipv4-family [**unicast**] **vpn-instance** *vpn-instance-name*

undo ipv4-family [**unicast**] **vpn-instance** *vpn-instance-name*

【视图】

RIP 视图

【参数】

unicast：使用单播地址。

vpn-instance-name：将指定的 VPN 实例与 IPv4 地址族进行关联，使用该参数将进入 RIP 的 MBGP 地址族视图。

【描述】

ipv4-family 命令用于进入 RIP 的地址族视图，**undo ipv4-family** 命令用于删除地址族视图下的所有配置。

使用 **ipv4-family** 命令进入地址族视图，在这个视图下，可以为 RIP 配置地址族相关的参数。

ipv4-family vpn-instance 命令用于 BGP/MPLS VPN，相关内容请参见本手册的“VPN”部分。

相关配置可参考命令 **dispaly rip vpn-instance**。

【举例】

进入 RIP 的地址族视图。

```
[H3C] rip
[H3C-rip] ipv4-family vpn-instance abc
[H3C-rip-af-vpn-instance]
```

2.1.12 network

【命令】

network *network-address*

undo network *network-address*

【视图】

RIP 视图

【参数】

network-address：使能或不使能的网络的地址，其取值可以为各个接口 IP 网络地址。*network-address* 可以配置为 0.0.0.0，表示使能所有网段。

【描述】

network 命令用来使能 RIP 接口，**undo network** 命令用来禁用 RIP 接口。

缺省情况下，禁用所有 RIP 接口。

启动 RIP 路由进程后，RIP 路由进程缺省在所有的接口禁用。为了在某一接口上使能 RIP 路由则必须使用 **newtork** 命令。

undo network 命令与接口的 **undo rip work** 命令功能相近，但它们并不完全相同。相同点在于，使用任一命令都可使相应接口都不再收发 RIP 路由。区别在于：执行了 **undo rip work** 命令的情况下，其它接口对使用该命令的接口的路由仍然转发；而执行 **undo network** 命令，则相应的接口路由不能被 RIP 传播出去，导致到该接口的报文不能被转发。

当对某一地址使用命令 **network** 时，效果是使能该地址的网段的接口。例如：**network** 129.102.1.1，用 **display current-configuration** 和 **display rip** 命令看到的均是 **network** 129.102.0.0。

相关配置可参考命令 **rip work**。

【举例】

在网络地址为 129.102.0.0 的接口上使能 RIP。

```
[H3C-rip] network 129.102.0.0
```

2.1.13 peer

【命令】

peer *ip-address*

undo peer *ip-address*

【视图】

RIP 视图

【参数】

ip-address：要与之交换信息的需定点发送的对端路由器的 IP 地址，用点分十进制格式表示。

【描述】

peer 命令用来指定需要定点发送的目的地址，**undo peer** 命令用来取消指定的地址。

RIP 缺省不向任何定点地址发送。

peer 命令指定需要定点传送的地址，这主要是为了适应某些非广播网的特殊需求。在通常情况下，我们并不建议用户使用该命令。

【举例】

配置定点发送地址 202.38.165.1。

```
[H3C-rip] peer 202.38.165.1
```

2.1.14 preference

【命令】

preference *value*

undo preference

【视图】

RIP 视图

【参数】

value：优先级，取值范围为 1～255，缺省值为 100。

【描述】

preference 命令用来指定 RIP 协议的路由优先级，**undo preference** 命令用来恢复路由优先级的缺省值。

每一种路由协议都有自己的优先级，它的缺省取值由具体的路由策略决定。优先级的高低将最后决定 IP 路由表中的路由采取哪种路由算法获取的最佳路由。可以利用此命令手动调整 RIP 的优先级。

【举例】

指定 RIP 的优先级为 20。

```
[H3C-rip] preference 20
```

2.1.15 reset

【命令】

reset

【视图】

RIP 视图

【参数】

无

【描述】

reset 命令用来复位 RIP 协议的系统配置参数。

当需要重新配置 RIP 协议参数时，可以使用该命令恢复 RIP 协议的缺省配置。

【举例】

将 RIP 系统配置复位。

```
[H3C-rip] reset
```

2.1.16 rip

【命令】

rip

undo rip

【视图】

系统视图

【参数】

无

【描述】

rip 命令用来启动 RIP 协议的运行并进入其视图，**undo rip** 命令用来停止 RIP 协议的运行。

缺省情况下，系统不运行 RIP 协议。

【举例】

启动 RIP 协议并进入其视图。

```
[H3C] rip
[H3C-rip]
```

2.1.17 rip authentication-mode

【命令】

rip authentication-mode { **simple** *password* | **md5** { **rfc2082** *key-string key-id* | **rfc2453** *key-string* } }

undo rip authentication-mode

【视图】

接口视图

【参数】

simple：采用明文验证方式。

password：明文验证关键字，字符串形式，如果以明文形式输入，长度为 1～16；如果以密文形式输入，长度必须为 24。

md5：采用 MD5 密文验证方式。

rfc2082：指定使用非标准（RFC 2082）MD5 认证报文格式。

rfc2453：指定使用一般（RFC 2453）MD5 认证格式。

key-string：MD5 密文验证字，字符串形式，如果以明文形式输入，长度为 1～16，如：1234567；如果以密文形式输入，长度必须为 24，并且必须是密文形式，如：_(TT8F]Y\5SQ=^Q`MAF4<1!!。

key-id：MD5 密文验证标识符，取值范围为 1～255。

【描述】

rip authentication-mode 命令用来配置 RIP-2 的认证方式及认证参数。**undo rip authentication-mode** 命令用来取消 RIP-2 认证。

RIP-1 不支持验证报文。RIP 的验证报文主要有两种类型，明文验证和 MD5 密文验证。其中，采用 MD5 密文验证方式时有两种报文格式，一种是在 RFC 2453 中所描述的；另一种在 RFC 2082 中专门阐述。防火墙对这两种报文格式均提供支持，用户可以根据不同的需要自行选择。

相关配置可参考命令 **rip version**。

【举例】

配置接口 Ethernet1/0/0 使用明文验证，关键字为 aaa。

```
[H3C] interface Ethernet1/0/0
[H3C-Ethernet1/0/0] rip version 2
[H3C-Ethernet1/0/0] rip authentication-mode simple aaa
```

2.1.18 rip input

【命令】

rip input

undo rip input

【视图】

接口视图

【参数】

无

【描述】

rip input 命令用来允许接口接收 RIP 报文，**undo rip input** 命令用来禁止接口接收 RIP 报文。

缺省情况下，除 loopback 接口之外的所有接口都接收 RIP 报文。

此命令是与其它两条命令 **rip output** 和 **rip work** 协作使用的，**rip work** 从功能上等价于 **rip input** 和 **rip output**，后两条命令分别控制接口上对 RIP 报文的接收和发送，前一项命令等于后两条命令作用之和。

相关配置可参考命令 **rip output**，**rip work**。

【举例】

指定接口 Ethernet1/0/0 不接收 RIP 报文。

```
[H3C-Ethernet1/0/0] undo rip input
```

2.1.19 rip metricin

【命令】

rip metricin *value*

undo rip metricin

【视图】

接口视图

【参数】

value：在接收报文时增加的附加路由权值，取值范围为 0～16，缺省值为 0。

【描述】

rip metricin 命令用来设置接口接收 RIP 报文时给路由增加的附加路由权值，**undo rip metricin** 命令用来恢复该附加路由权值的缺省值。

该命令的有效范围为：本地 network 发布的路由、其它路由器引入的路由；它对于本地引入的路由无效。

相关配置可参考命令 **rip metricout**。

【举例】

指定接口 Ethernet1/0/0 在接收 RIP 报文时添加的附加路由权值为 2。

```
[H3C] interface Ethernet 1/0/0
[H3C-Ethernet1/0/0] rip metricin 2
```

2.1.20 rip metricout

【命令】

rip metricout *value*

undo rip metricout

【视图】

接口视图

【参数】

value：在发送报文时增加的附加路由权值，取值范围为 1～16，缺省值为 1。

【描述】

rip metricout 命令用来设置接口发送 RIP 报文时给路由增加的附加路由权值，**undo rip metricout** 命令用来恢复该附加路由权值的缺省值。

该命令的有效范围为：本地 network 发布的路由、其它路由器引入的路由；该命令对于本地引入的路由无效。

相关配置可参考命令 **rip metricin**。

【举例】

设定接口 Ethernet1/0/0 发送 RIP 报文时添加的附加路由权值为 2。

```
[H3C] interface Ethernet1/0/0
[H3C-Ethernet1/0/0] rip metricout 2
```

2.1.21 rip output

【命令】

rip output

undo rip output

【视图】

接口视图

【参数】

无

【描述】

rip output 命令用来允许接口向外发送 RIP 报文，**undo rip output** 命令用来禁止接口向外发送 RIP 报文。

缺省情况下，除 loopback 接口之外的所有接口向外发送 RIP 报文。

此命令是与其它两条命令 **rip input** 和 **rip work** 协作使用的，**rip work** 从功能上等价于 **rip input** 和 **rip output**，后两条命令分别控制接口上对 RIP 报文的接收和发送，前一项命令等于后两条命令作用之和。

相关配置可参考命令 **rip input** 和 **rip work**。

【举例】

禁止接口 Ethernet1/0/0 发送 RIP 报文。

```
[H3C] interface Ethernet1/0/0
[H3C-Ethernet1/0/0] undo rip output
```

2.1.22 rip split-horizon

【命令】

rip split-horizon

undo rip split-horizon

【视图】

接口视图

【参数】

无

【描述】

rip split-horizon 命令用来指定接口使能水平分割，**undo rip split-horizon** 命令用来指定接口禁止使用水平分割。

缺省情况下，接口使能水平分割。

通常情况下，为了防止路由环的出现，水平分割都是必要的。只是在某些特殊情况下，为保证协议的正确执行，需要关闭水平分割。例如在 NBMA 网络中，对于采用帧中继封装的主接口和点对多点子接口，为了使接口可以发送从该接口学到的路由，则需要禁止水平分割。在关闭水平分割时一定要确认是否必要。

【举例】

指定接口 Ethernet1/0/0 处理 RIP 报文时不使用水平分割。

```
[H3C] interface Ethernet1/0/0
[H3C-Ethernet1/0/0] undo rip split-horizon
```

2.1.23 rip version

【命令】

rip version { **1** | **2** [**broadcast** | **multicast**] }

undo rip version

【视图】

接口视图

【参数】

1：接口版本为 RIP-1。

2：接口版本为 RIP-2。缺省情况下，采用多播方式。

broadcast：RIP-2 报文的发送方式为广播方式。

multicast：RIP-2 报文的发送方式为多播方式。

【描述】

rip version 命令用来指定接口上运行 RIP 的版本，**undo rip version** 命令用来恢复接口上运行 RIP 版本的缺省值。

缺省情况下，接口 RIP 版本是 RIP-1。

RIP-2 有两种传送方式，广播方式和组播方式，缺省采用组播方式发送报文。RIP-2 中组播地址为 224.0.0.9。组播发送报文的好处是在同一网络中那些没有运行 RIP 的主机可以避免处理 RIP 的广播报文；另外，还可以使运行 RIP-1 的主机避免错误地接收和处理 RIP-2 中带有子网掩码的路由。

当指定接口版本为 RIP-1 时，只接收 RIP-1 与 RIP-2 广播报文，不接收 RIP-2 多播报文。当指定接口运行在 RIP-2 广播方式时，只接收 RIP-1 与 RIP-2 广播报文，不接收 RIP-2 多播报文；当指定接口运行在 RIP-2 多播方式时，只接收 RIP-2 多播报文，不接收 RIP-1 与 RIP-2 广播报文。

【举例】

将接口 Ethernet1/0/0 配置成 RIP-2 的广播模式。

```
[H3C] interface Ethernet 1/0/0
[H3C-Ethernet1/0/0] rip version 2 broadcast
```

2.1.24 rip work

【命令】

rip work

undo rip work

【视图】

接口视图

【参数】

无

【描述】

rip work 命令用来启动接口运行 RIP 协议，**undo rip work** 命令用来禁止接口运行 RIP 协议。

缺省情况下，接口上运行 RIP 协议。

该命令与 **rip input**、**rip output** 和 **network** 命令共同作用，相关配置可参考命令 **network**、**rip input** 和 **rip output**。

【举例】

禁止接口 Ethernet1/0/0 运行 RIP 协议。

```
[H3C] interface Ethernet1/0/0
[H3C-Ethernet1/0/0] undo rip work
```

2.1.25 summary

【命令】

summary

undo summary

【视图】

RIP 视图

【参数】

无

【描述】

summary 命令用来激活 RIP-2 自动路由聚合功能，**undo summary** 命令用来关闭 RIP-2 的路由聚合功能。

缺省情况下，激活 RIP-2 的路由聚合功能。

为了减少网络上的路由流量，减小路由表的大小，可以对路由进行聚合操作。如果使用 RIP-2，当你需要将子网路由广播出去时，可以通过 **undo summary** 命令关闭路由聚合功能。

RIP-1 不支持子网掩码，如果转发子网路由有可能会引起歧义。所以，RIP-1 始终启用路由聚合功能。**undo summary** 命令对 RIP-1 不起作用。

相关配置可参考命令 **rip version**。

【举例】

将接口 Ethernet1/0/0 上的 RIP 版本设为 RIP-2 并关闭路由聚合功能。

```
[H3C] interface Ethernet1/0/0
[H3C-Ethernet1/0/0] rip version 2
[H3C-Ethernet1/0/0] quit
[H3C] rip
[H3C-rip] undo summary
```

2.1.26 timers

【命令】

timers { **update** *update-timer-length* | **timeout** *timeout-timer-length* } *

undo timers { **update** | **timeout** } *

【视图】

RIP 视图

【参数】

update-timer-length：定时器 Period Update 的值，单位为秒，取值范围为 1～3600。缺省值为 30 秒。

timeout-timer-length：定时器 Timeout 的值，单位为秒，取值范围为 1～3600。缺省值为 180 秒。

【描述】

timers 命令用来修改 RIP 的三个定时器 Period update、Timeout 和 Garbage-collection 的值，**undo timers** 命令用来恢复缺省设置。

缺省情况下，定时器 Period update、Timeout 和 Garbage-collection 的值分别是 30s、180s 和 120s。

通常情况下，可以认为 Garbage-collection 定时器的值固定为 Period update 定时器的 4 倍，但实际上，不可达路由在被从路由表中彻底删除前，需要等待 4 个来自同一邻居的更新报文。因此，Garbage-collection 定时器的实际时长是 Period update 定时器的 3～4 倍。调整 Period update 将同时影响 Garbage-collection 定时器。

RIP 定时器的值更改后将立即生效。

相关配置可参考命令 **display rip**。

【举例】

配置 RIP 的 Period udpate 定时器为 10 秒，Timeout 定时器为 30 秒。

```
[H3C] rip
[H3C-rip] timers update 10 timeout 30
```

2.1.27 traffic-share-across-interface

【命令】

traffic-share-across-interface

undo traffic-share-across-interface

【视图】

RIP 协议视图

【参数】

无

【描述】

traffic-share-across-interface 命令用来使能 RIP 在接口间实现负载分担功能，即可以使流量通过等价路由均衡地在防火墙的各个接口之间分配，**undo traffic-share-across-interface** 命令用来取消该配置。

缺省情况下，关闭 RIP 接口间流量负载分担功能。

【举例】

使能 RIP 在接口间实现流量负载分担功能。

```
[H3C-rip] traffic-share-across-interface
```

2.1.28 validate-source-address

【命令】

validate-source-address

undo validate-source-address

【视图】

RIP 协议视图

【参数】

无

【描述】

validate-source-address 命令用来配置收到 RIP 报文后，检查 RIP 报文的源地址。**undo validate-source-address** 命令用来取消 RIP 报文的源地址检查。不检查收到的 RIP 报文的源地址，可以实现非直连 RIP 路由的交互。

缺省情况下，检查 RIP 报文的源地址。

【举例】

配置取消对收到的 RIP 报文的源地址检查。

```
[H3C-rip] undo validate-source-address
```

第3章 OSPF 配置命令

3.1 OSPF 配置命令

3.1.1 abr-summary

【命令】

abr-summary *ip-address mask* [**advertise** | **not-advertise**]

undo abr-summary *ip-address mask*

【视图】

OSPF 区域视图

【参数】

ip-address：网段地址。

mask：网络掩码。

advertise：将到这一聚合网段路由的摘要信息广播出去。

not-advertise：不将到这一聚合网段路由的摘要信息广播出去。

【描述】

abr-summary 命令用来在区域边界路由器（ABR）上配置路由聚合，**undo abr-summary** 命令用来取消在区域边界路由器上进行路由聚合的功能。

缺省情况下，区域边界路由器不对路由聚合。

本命令只适用于边界路由器（ABR），用来对某一个区域进行路由聚合。ABR 向其它区域只发送一条聚合后的路由。路由聚合是指：路由信息在 ABR 处进行处理，对于每一个配置了聚合的网段，只有一条路由被发送到其它区域。一个区域可配置多条聚合网段，这样 OSPF 可对多个网段进行聚合。

【举例】

将 OSPF 区域 1 中两个网段 36.42.10.0，36.42.110.0 的路由聚合成一条聚合路由 36.42.0.0 向其它区域发送。

```
[H3C-ospf-1] area 1
[H3C-ospf-1-area-0.0.0.1] network 36.42.10.0 0.0.0.255
[H3C-ospf-1-area-0.0.0.1] network 36.42.110.0 0.0.0.255
[H3C-ospf-1-area-0.0.0.1] abr-summary 36.42.0.0 255.255.0.0
```

3.1.2 area

【命令】

area *area-id*

undo area *area-id*

【视图】

OSPF 视图、OSPF 区域视图

【参数】

area-id：区域的标识，可以是十进制整数（取值范围为 0～4294967295）或 IP 地址格式。

【描述】

area 命令用来进入 OSPF 区域视图。**undo area** 命令用来删除指定区域。

【举例】

进入区域 0 视图。

```
[H3C-ospf-1] area 0
[H3C-ospf-1-area-0.0.0.0]
```

3.1.3 asbr-summary

【命令】

asbr-summary *ip-address mask* [**not-advertise** | **tag** *tag-value*]

undo asbr-summary *ip-address mask*

【视图】

OSPF 视图

【参数】

ip-address：匹配的 IP 地址，点分十进制格式。

mask：IP 地址掩码，点分十进制格式。

not-advertise：不通告匹配指定 IP 地址/掩码的路由。如果不指定该参数将通告聚合路由。

tag-value：用于通过 Route-policy 控制路由发布，*tag-value* 的取值范围为 0～4294967295。如果不指定该参数，缺省值为 1。

【描述】

asbr-summary 命令用来设置 OSPF 对引入的路由进行聚合，**undo asbr-summary** 命令用来取消聚合。

缺省情况下，不对引入路由进行聚合。

配置引入路由聚合后，如果本地防火墙是自治系统边界路由器 ASBR，将对引入的聚合地址范围内的 Type-5 LSA 进行聚合，当配置了 NSSA 区域时，还要对引入的聚合地址范围内的 Type-7 LSA 进行聚合。

如果本地防火墙是区域边界路由器 ABR，且是 NSSA 区域的转换路由器，则对由 Type-7 LSA 转化成的 Type-5 LSA 进行聚合处理，对于不是 NSSA 区域转换路由器的则不进行聚合处理。

相关配置可参考命令 **display ospf asbr-summary**。

【举例】

设置防火墙的引入路由聚合。

```
[H3C-ospf-1] asbr-summary 10.2.0.0 255.255.0.0
```

3.1.4 authentication-mode

【命令】

authentication-mode { **simple** | **md5** }

undo authentication-mode

【视图】

OSPF 区域视图

【参数】

simple：使用明文验证方式。

md5：使用 MD5 密文验证方式。

【描述】

authentication-mode 命令用来指定 OSPF 中的一个区域使能验证，**undo authentication-mode** 命令用来取消该区域的验证功能。

缺省情况下，区域不使能验证。

在 OSPF 中，一个区域中所有路由器的验证类型必须一致（不支持验证、支持明文验证、支持 MD5 密文验证），但每条链路上的密码可以是不同的。命令 **ospf authentication-mode simple** 用来配置明文验证字口令。若该区域配置支持 MD5 密文验证类型，则用命令 **ospf authentication-mode md5** 来配置 MD5 密文验证字口令。

相关配置可参考命令 **ospf authentication-mode**。

【举例】

进入区域 0 视图。

```
[H3C-ospf-1] area 0
```

指定 OSPF 区域 0 支持 MD5 密文验证。

```
[H3C-ospf-1-area-0.0.0.0] authentication-mode md5
```

3.1.5 debugging ospf

【命令】

debugging ospf [*process-id*] { **event** | **packet** [**ack** | **dd** | **hello** | **request** | **update**] [**interface** *type num*] | **lsa-generate** | **spf** }

undo debugging ospf [*process-id*] { **event** | **packet** [**ack** | **dd** | **hello** | **request** | **update**] [**interface** *type num*] | **lsa-generate** | **spf** }

【视图】

用户视图

【参数】

process-id：OSPF 进程号。如果不指定进程号，则打开或关闭所有进程的调试信息开关。

event：表示打开 OSPF 事件信息调试开关。

packet：表示打开 OSPF 报文信息调试开关。

ack：LSAck 报文；

dd：Database Descrition 报文；

hello：Hello 报文；

request：Link State Request 报文；

update：Link State Update 报文。

interface *type num*：接口类型及接口号。

lsa-generate：表示打开 OSPF LSA 报文信息调试开关。

spf：表示打开 OSPF 最小树计算信息调试开关。

【描述】

debugging ospf 命令用于打开 OSPF 进程的调试信息开关，此命令的 **undo debugging ospf** 命令用于关闭调试信息开关。

在 OSPF 多进程中，**debugging** 命令可以同时打开全部进程的某种调试开关，也可以只打开其中一个进程的调试开关。

如果 **debugging** 命令中没有指定进程号，那么该调试命令将对所有的进程生效。并且在整个防火墙活动期间，不管是否有 OSPF 进程存在，该调试开关状态一直保留。因此，执行该命令将给每个已经使能的 OSPF 进程打开或关闭该调试开关。同时，当启动新的 OSPF 进程时，也会自动打开该命令指定的调试开关。

如果 **debugging** 命令中指定了进程号，那么就只对指定进程的调试开关进行调整。如果该 OSPF 进程还没有使能，那么命令配置将不成功，进程退出后，该进程的调试开关状态也不能保留。

如果 **debugging** 命令中不加 **interface** 参数时，可以显示所有接口的调试信息，加 **interface** 时，只显示指定接口的调试信息。

相关配置可参考命令 **display debugging ospf**。

【举例】

打开 OSPF 报文调试信息开关。

```
<H3C> debugging ospf packet
```

3.1.6 default cost

【命令】

default cost *value*

undo default cost

【视图】

OSPF 视图

【参数】

value：OSPF 引入外部路由的缺省路由权值，取值范围为 0～16777214，缺省路由权值为 1。

【描述】

default cost 命令用来设置 OSPF 引入外部路由的缺省路由权，**undo default cost** 命令用来恢复配置 OSPF 引入外部路由的缺省路由权的缺省值。

由于 OSPF 可引入外部路由信息并将它们传播到整个自治系统中去，因此，有必要规定协议引入外部路由的缺省路由权。

如果启动了多个 OSPF 进程，该命令只对本进程起作用。

【举例】

指定 OSPF 引入外部路由的缺省路由权为 10。

```
[H3C-ospf-1] default cost 10
```

3.1.7 default interval

【命令】

default interval *seconds*

undo default interval

【视图】

OSPF 视图

【参数】

seconds：引入外部路由的缺省时间间隔，单位为秒，取值范围为 1～2147483647，缺省值为 1 秒。

【描述】

default interval 命令用来设置 OSPF 引入外部路由的缺省时间间隔，**undo default interval** 命令用来恢复引入外部路由缺省时间间隔的缺省值。

由于 OSPF 可引入外部路由信息并将它们传播到整个自治系统中去，因此，有必要规定协议引入外部路由的缺省时间间隔。

【举例】

指定 OSPF 引入外部路由的缺省时间间隔为 10 秒。

```
[H3C-ospf-1] default interval 10
```

3.1.8 default limit

【命令】

default limit *routes*

undo default limit

【视图】

OSPF 视图

【参数】

routes：每单位时间内引入外部路由数量的缺省限制，取值范围为 200～2147483647，缺省值为 1000 条。

【描述】

default limit 命令用来设置 OSPF 在每单位时间内引入外部路由数量的缺省限制，**undo default limit** 命令用来恢复引入外部路由数量的缺省限制的缺省值。

由于 OSPF 能引入外部的路由信息并将它们传播到整个自治系统中去。因此，有必要规定在一次传播中引入外部路由信息数量的缺省条数。

相关配置可参考命令 **default interval**。

【举例】

指定 OSPF 引入外部路由数量的缺省限制为 200 条。

```
[H3C-ospf-1] default limit 200
```

3.1.9 default tag

【命令】

default tag *tag*

undo default tag

【视图】

OSPF 视图

【参数】

tag：缺省标记，取值范围为 0～4294967295。缺省值为 1。

【描述】

default tag 命令用来设置 OSPF 在引入外部路由时的缺省标记，**undo default tag** 命令用来恢复引入外部路由时的缺省标记的缺省值。

在 OSPF 将防火墙上其它路由协议发现的路由引入作为自己的自治系统外部路由信息时，还需要一些额外的参数，包括：路由的缺省花费和缺省标记等。

相关配置可参考命令 **default type**。

【举例】

设置 OSPF 引入自治系统外部路由的缺省标记为 10。

```
[H3C-ospf-1] default tag 10
```

3.1.10 default type

【命令】

default type { **1** | **2** }

undo default type

【视图】

OSPF 视图

【参数】

1：第一类外部路由。

2：第二类外部路由。

【描述】

default type 命令用来设置 OSPF 在引入外部路由时的缺省类型，**undo default type** 命令用来恢复 OSPF 在引入外部路由时缺省类型的缺省值。

缺省情况下，引入的路由为第二类外部路由。

OSPF 在协议中规定了两类外部路由信息，可以用该命令规定引入外部路由信息时的缺省类型。

相关配置可参考命令 **default tag**。

【举例】

指定 OSPF 引入外部路由时的缺省类型为第一类路由。

```
[H3C-ospf-1] default type 1
```

3.1.11 default-cost

【命令】

default-cost *value*

undo default-cost

【视图】

OSPF 区域视图

【参数】

value：OSPF 发送到 STUB 区域或者 NSSA 区域的缺省路由的开销，取值范围为 0～16777214，缺省值为 1。

【描述】

default-cost 命令用来指定 OSPF 发送到 STUB 区域或者 NSSA 区域的缺省路由的开销，**undo default-cost** 命令用来将 OSPF 发送到 STUB 区域或者 NSSA 区域缺省路由的开销恢复为缺省值。

本命令只适用于连接到 STUB 区域或者 NSSA 区域的边界路由器。

配置 STUB 区域需要两条配置命令：**stub** 和 **default-cost**，所有连接到 STUB 区域的路由器，必须使用 **stub** 命令将该区域设置成 STUB 属性。**default-cost** 指定区域边界路由器发送到 STUB 区域或者 NSSA 区域的缺省路由的开销。

如果启动了多个 OSPF 进程，该命令只对本进程起作用。

相关配置可参考命令 **stub** 和 **nssa**。

【举例】

将区域 1 设置成 STUB 区域，使发送到该 STUB 区域的缺省路由的开销为 60。

```
[H3C-ospf-1] area 1
[H3C-ospf-1-area-0.0.0.1] network 20.0.0.0 0.255.255.255
[H3C-ospf-1-area-0.0.0.1] stub
[H3C-ospf-1-area-0.0.0.1] default-cost 60
```

3.1.12 default-route-advertise

【命令】

default-route-advertise [**always** | **cost** *cost-value* | **type** *type-value* | **route-policy** *route-policy-name*] *

undo default-route-advertise [**always** | **cost** | **type** | **route-policy**] *

【视图】

OSPF 视图

【参数】

always：该参数只对 ASBR 有效，使用此参数后，不论本地是否存在缺省路由，都将产生一条 LSA 发布缺省路由。对于普通区域的 ASBR，产生一条 Type-5 LSA 向 OSPF 路由域内发布缺省路由；对于 NSSA 区域的 ASBR，产生一条 Type-7 LSA 向本区域内发布缺省路由。

cost-value：产生的 LSA 的路由权值。取值范围为 0～16777214，缺省值为 1。

type-value：产生的 LSA 的路由权类型。取值范围为 1～2，缺省值为 2，即 Type-2 External Route。

route-policy-name：如果缺省路由匹配 *route-policy-name* 指定的路由策略，那么 route-policy 将影响 LSA 中的值，参数 *route-policy-name* 为长度 1～19 的字符串。

【描述】

default-route-advertise 命令用来在 OSPF 中生成并发布缺省路由，**undo default-route-advertise** 命令用来取消生成的缺省路由。

缺省情况下，OSPF 不生成缺省路由。

需要说明的是：当在 OSPF 路由器上配置 **default-route-advertise** 命令后，这台路由器就成为 ASBR，这一点与在 OSPF 路由器上配置 **import-route** 命令的效果类似。但 **import-route** 命令不能向 OSPF 路由域中引入缺省路由。

另外，**default-route-advertise** 命令对 Stub 区域无效。而在配置 NSSA 区域时，执行 **nssa default-route-advertise** 命令与 **default-route-advertise** 命令效果相同。

如果启动了多个 OSPF 进程，该命令只对当前所在进程起作用。

相关配置可参考命令 **import-route** 和 **nssa**。

【举例】

配置 ASBR 只在本地有缺省路由时，才生成发布缺省路由的 LSA。

```
[H3C-ospf-1] default-route-advertise
```

配置 ASBR 不论本地是否存在缺省路由，都产生发布缺省路由的 LSA。

```
[H3C-ospf-1] default-route-advertise always
```

3.1.13 display debugging ospf

【命令】

display debugging ospf

【视图】

所有视图

【描述】

display debugging ospf 命令用于查看全局 OSPF 调试开关状态和各进程的调试开关状态。

相关配置可参考命令 **debugging ospf**。

【举例】

查看 OSPF 各进程的调试开关状态。

```
<H3C> display debugging ospf
OSPF process 1 debugging state:
OSPF SPF debugging switch is on
OSPF EVENT debugging switch is on
OSPF LSA debugging switch is on
OSPF Hello PACKET debugging switch is on
OSPF Database Description PACKET debugging switch is on
OSPF Link State Request PACKET debugging switch is on
OSPF Link State Update PACKET debugging switch is on
OSPF Link State Acknowledgment PACKET debugging switch is on
```

3.1.14 display ospf abr-asbr

【命令】

display ospf [*process-id*] **abr-asbr**

【视图】

所有视图

【参数】

process-id：OSPF 进程号。如果不指定进程号，则对当前所有 OSPF 进程有效。

【描述】

display ospf abr-asbr 命令用来显示到OSPF的区域边界路由器和自治系统边界路由器的路由信息。

【举例】

显示 OSPF 的区域边界路由器和自治系统边界路由器信息。

```
<H3C> display ospf abr-asbr
OSPF Process 1 with Router ID 1.1.1.1
Routing Table to ABR and ASBR
 I = Intra i = Inter A = ASBR B = ABR S = SumASBR
Destination        Area         Cost   Nexthop         Interface
IA 2.2.2.2         0.0.0.0      10     10.153.17.89    ethernet0/0/0
```

表3-1 display ospf abr-asbr 命令显示信息解释

符号	意义
Destination	ABR 或者 ASBR 的 Router ID
Area	本路由器与该 ABR 或 ASBR 相连的区域
Cost	该路由的开销值为 10
Nexthop	下一跳地址
Interface	本地路由器的输出接口

3.1.15 display ospf asbr-summary

【命令】

display ospf [*process-id*] **asbr-summary** [*ip-address mask*]

【视图】

所有视图

【参数】

process-id：OSPF 进程号。如果不指定进程号，则对当前所有 OSPF 进程有效。

ip-address：匹配的 IP 地址，点分十进制格式。

mask：IP 地址掩码，点分十进制格式。

【描述】

display ospf asbr-summary 命令用来查看 OSPF 的引入路由聚合信息。

如果不指定 IP 地址和掩码，将显示所有引入路由聚合信息。

相关配置可参考命令 **asbr-summary**。

【举例】

查看 OSPF 的所有引入路由聚合信息。

```
<H3C> display ospf asbr-summary
OSPF Process 1 with Router ID 1.1.1.1
Summary Addresses
Total summary address count:   2

                Summary Address
net      : 168.10.0.0
mask     : 255.254.0.0
tag      : 1
status   : Advertise
The Count of Route is 0

                Summary Address
net      : 1.1.0.0
mask     : 255.255.0.0
tag      : 100
status   : DoNotAdvertise
The Count of Route is 0
```

表3-2 display ospf asbr-summary 命令显示信息解释

符号	意义	
net	目的网段	
mask	掩码	
tag	标记	
status	状态信息，有两种取值：	
	DoNotAdvertise	到这一网段的聚合路由信息将不被发布出去
	Advertise	到这一网段的聚合路由信息将会被发布出去

3.1.16 display ospf brief

【命令】

display ospf [*process-id*] **brief**

【视图】

所有视图

【参数】

process-id：OSPF 进程号。如果不指定进程号，将按进程号配置顺序显示所有 OSPF 进程的主要信息。

【描述】

display ospf brief 命令用来显示 OSPF 的概要信息。

【举例】

显示 OSPF 的概要信息。

```
<H3C> display ospf brief

                OSPF Process 1 with Router ID 1.1.1.1
                       OSPF Protocol Information

 RouterID: 172.16.2.2
 Spf-schedule-interval: 5
 Routing preference: Inter/Intra: 10 External: 150
 Default ASE parameters: Metric: 1 Tag: 1 Type: 2
 SPF computation count: 4
 Area Count: 1    Nssa Area Count: 0

 Area 0.0.0.0:
   Authtype: none   Flags: <>
   SPF scheduled: <>
   Interface: 172.16.2.2 (Ethernet0/0/0)
     Cost: 1 State: BackupDR    Type: Broadcast
     Priority: 1
     Designated Router: 172.16.2.1
     Backup Designated Router: 172.16.2.2
     Timers: Hello 10, Dead 40, Poll 40, Retransmit 5, Transmit Delay 1

   Interface: 10.0.0.1 (Ethernet0/0/1)
     Cost: 1 State: DR    Type: Broadcast
     Priority: 1
```

```
Designated Router: 10.0.0.1
Timers: Hello 10, Dead 40, Poll 40, Retransmit 5, Transmit Delay 1OSPF
```

表3-3 display ospf brief 命令显示信息解释

符号	意义	
RouterID	本路由器的 Router ID	
spf-schedule-interval	SPF 计算间隔	
Routing preference	OSPF 路由优先级，OSPF 内部路由包括 intra/inter area 路由，优先级缺省是 10，OSPF 外部路由的缺省值是 150	
Default ASE parameters	OSPF 引入外部路由时的缺省参数，包括 metric、type、tag	
SPF computation count	自从 OSPF 启动以来进行的 SPF 计算的次数	
Area Count	本路由器所连接的各个区域	
Nssa Area Count	NSSA 区域数目	
Authtype	OSPF 验证类型	
SPF scheduled	SPF 计算时序（标志）	
Interface	属于该区域的接口名称	
Cost	路由开销	
State	状态信息	
Type	OSPF 接口的网络类型	
Priority	优先级	
Designated Router	指定路由器 DR（IP 地址）	
Backup Designated Router	备份指定路由器 BDR（IP 地址）	
Timers	OSPF 计时器，分别定义：	
	Hello	hello 报文间隔
	Dead	邻居失效时间间隔
	Poll	轮询时间间隔
	Retransmit	接口重传 LSA 时间间隔
Transmit Delay	接口对 LSA 的传输延迟时间	

3.1.17 display ospf cumulative

【命令】

display ospf [*process-id*] **cumulative**

【视图】

所有视图

【参数】

process-id：OSPF 进程号。如果不指定进程号，则对当前所有 OSPF 进程有效。

【描述】

display ospf cumulative 命令用来显示 OSPF 的统计信息。

【举例】

显示 OSPF 的统计信息。

```
<H3C> display ospf cumulative

                OSPF Process 1 with Router ID 1.1.1.1
                          Cumulations

  IO Statistics
             Type        Input     Output
            Hello          151        306
   DB Description            5          3
   Link-State Req            1          2
Link-State Update           10          2
   Link-State Ack            2          9
  ASE: 0 Checksum Sum: 0
  Opq-11: 0  Checksum Sum:0
  LSAs originated by this router
  Router: 4  Opq-9: 0  Opq-10: 0  Opq-11: 0
  LSAs Originated: 4  LSAs Received: 13

  Area 0.0.0.0:
    Neighbors: 1  Interfaces: 2
    Spf: 4  Checksum Sum 3F587
    rtr: 3 net: 1 sumasb: 1 sumnet: 1 opq-9: 0 opq-10: 0

  Routing Table:
    Intra Area: 2  Inter Area: 1  ASE: 0
```

表3-4 display ospf cumulative 命令显示信息解释

符号		意义
IO Statistics	Type	输入、输出的 OSPF 报文的种类
	Input	收到的每种报文的个数
	Output	发送的每种报文的个数
ASE		所有的 ASE LSA 的个数
Opq-11		Type-11 Opaque LSA 的个数
checksum sum		ASE LSA 的校验和
LSAs	originated	自己生成的 LSA 的个数
	received	收到的别的路由器产生的 LSA 的个数
Router		所有的 Router LSA 的个数
SumNet		所有的 Sumnet LSA 的个数
SumASB		所有的 SumASB LSA 的个数
Area	Neighbors	本 area 中的邻居个数
	Interfaces	本 area 中的接口个数
	Spf	本 area 已经进行的 SPF 计算的次数
	rtr；net；sumasb；sumnet；opq-9；opq-10	本 area 中的各种 LSA 的个数
Routing Table	Intra Area	域内路由的条数
	Inter Area	域间路由的条数
	ASE	外部路由的条数

3.1.18 display ospf error

【命令】

display ospf [*process-id*] **error**

【视图】

所有视图

【参数】

process-id：OSPF 进程号。如果不指定进程号，则对当前所有 OSPF 进程有效。

【描述】

display ospf error 命令用来显示 OSPF 接收到的错误报文的统计信息。

【举例】

显示 OSPF 接收到的错误报文的统计信息。

```
<H3C> display ospf error

                OSPF Process 1 with Router ID 201.201.201.201

 OSPF packet error statistics:
   0: IP: received my own packet          0: OSPF: wrong packet type
   0: OSPF: wrong version                 0: OSPF: wrong checksum
   0: OSPF: wrong area id                 0: OSPF: area mismatch
   0: OSPF: wrong virtual link            0: OSPF: wrong authentication type
   0: OSPF: wrong authentication key      0: OSPF: too small packet
   0: OSPF: packet size > ip length       0: OSPF: transmit error
   0: OSPF: interface down                0: OSPF: unknown neighbor
   0: HELLO: netmask mismatch             0: HELLO: hello timer mismatch
   0: HELLO: dead timer mismatch          0: HELLO: extern option mismatch
   0: HELLO: router id confusion          0: HELLO: virtual neighbor unknown
   0: HELLO: NBMA neighbor unknown        0: DD: neighbor state low
   0: DD: router id confusion             0: DD: extern option mismatch
   0: DD: unknown LSA type                0: LS ACK: neighbor state low
   0: LS ACK: wrong ack                   0: LS ACK: duplicate ack
   0: LS ACK: unknown LSA type            0: LS REQ: neighbor state low
   0: LS REQ: empty request               0: LS REQ: wrong request
   0: LS UPD: neighbor state low          0: LS UPD: newer self-generate LSA
   0: LS UPD: LSA checksum wrong          0: LS UPD: received less recent LSA
   0: LS UPD: unknown LSA type            0: OSPF routing: next hop not exist
   0: DD: MTU option mismatch             0: ROUTETYPE: wrong type value
   0: OPQ-9  : out of flooding scope      0: OPQ-10 : out of flooding scope
   0: OPQ-11 : out of flooding scope
```

表3-5 display ospf error 命令显示信息解释

域名	意义
IP: received my own packet	收到自己发出的数据包
OSPF: wrong packet type	OSPF 数据包类型错误
OSPF: wrong version	OSPF 版本错误
OSPF: wrong checksum	OSPF 校验和错误
OSPF: wrong area id	OSPF 区域标识（ID）错误
OSPF: area mismatch	OSPF 区域不匹配
OSPF: wrong virtual link	OSPF 虚连接错误

域名	意义
OSPF: wrong authentication type	OSPF 验证类型错误
OSPF: packet too small	OSPF 数据包太小
OSPF: packet size > ip length	OSPF 数据包大小超过 IP 数据包长度
OSPF: transmit error	OSPF 传输错误
OSPF: interface down	OSPF 接口 down，不可用
OSPF: unknown neighbor	OSPF 邻居未知
HELLO: netmask mismatch	网络掩码不匹配
HELLO: hello timer mismatch	发送 HELLO 报文的时间间隔不匹配
HELLO: dead timer mismatch	发送邻居失效报文的时间间隔不匹配
HELLO: extern option mismatch	Hello 报文 extern 选项不匹配
HELLO: router id confusion	Hello 报文：Router ID 冲突
HELLO: virtual neighbor unknown	Hello 报文：未知的虚拟邻居
HELLO: NBMA neighbor unknown	Hello 报文：未知的 NBMA 邻居
DD: neighbor state low	DD（数据库描述）报文：邻居状态不同步
DD: unknown LSA type	DD 报文：未知的 LSA 类型
LS ACK: neighbor state low	Link state acknowledgment 报文（链路状态响应报文）：邻居状态不同步
LS ACK: wrong ack	Link state acknowledgment 报文：错误的 ack
LS ACK: duplicate ack	Link state acknowledgment 报文：重复的 ack
LS ACK: unknown LSA type	Link state acknowledgment 报文：未知的 LSA 类型
LS REQ: neighbor state low	Link state request（链路状态请求）报文：
LS REQ: empty request	Link state request（链路状态请求）报文：空请求
LS REQ: wrong request	Link state request（链路状态请求）报文：错误的请求
LS UPD: neighbor state low	Link state update 报文：邻居状态不同步
LS UPD: newer self-generate LSA	Link state update 报文：自己有较新的 LSA
LS UPD: LSA checksum wrong	Link state update 报文：LSA 校验和错误
LS UPD:received less recent LSA	Link state update 报文：收到非最新的 LSA
LS UPD: unknown LSA type	Link state update 报文：未知的 LSA 类型
OSPF routing: next hop not exist	OSPF 路由下一跳不存在
DD: MTU option mismatch	数据库描述报文的 MTU 选项不匹配
ROUTETYPE: wrong type value	路由类型错误
OPQ-9 ：out of flooding scope	9 类 LSA 泛洪超出范围

域名	意义
OPQ-10 : out of flooding scope	10 类 LSA 泛洪超出范围
OPQ-11 : out of flooding scope	11 类 LSA 泛洪超出范围

3.1.19 display ospf interface

【命令】

display ospf [*process-id*] **interface** [*interface-type interface-number*]

【视图】

所有视图

【参数】

process-id：OSPF 进程号。如果不指定进程号，则对当前所有 OSPF 进程有效。

interface-type interface-number：接口类型和接口号。

【描述】

display ospf interface 命令用来显示 OSPF 的接口信息。

【举例】

显示 OSPF 的 ethernet2/0/0 接口信息。

```
<H3C> display ospf interface ethernet2/0/0

                OSPF Process 1 with Router ID 1.1.1.1
                        Interfaces

Interface: 10.110.10.2 (Ethernet0/0/0)
 Cost: 1 State: BackupDR    Type: Broadcast
 Priority: 1
 Designated Router: 10.110.10.1
 Backup Designated Router: 10.110.10.2
 Timers: Hello 10, Dead 40, Poll 40, Retransmit 5, Transmit Delay 1
```

表3-6 display ospf interface 命令显示信息说明

符号	意义
Cost	此接口的花费
State	接口状态机的状态
Type	接口的 OSPF 网络类型

符号	意义	
Priority	此接口参与选举所在网络的 DR 的优先级	
Designated Router	此接口所在网络的 DR	
Backup Designated Router	此接口所在网络的 BDR	
Timers	OSPF 计时器，分别定义：	
	Hello	hello 报文间隔
	Dead	邻居失效时间间隔
	Poll	轮询时间间隔
	Retransmit	接口重传 LSA 时间间隔
Transmit Delay	接口对 LSA 的传输延迟时间	

3.1.20 display ospf lsdb

【命令】

display ospf [*process-id*] [*area-id*] **lsdb** [**brief** | **asbr** | **ase** | **network** | **nssa** | **router** | **summary**] [*ip-address*] [**originate-router** *ip-address* | **self-originate**]

【视图】

所有视图

【参数】

process-id：OSPF 进程号。如果不指定进程号，则对当前所有 OSPF 进程有效。

area-id：区域的标识，可以是十进制整数（取值范围为 0～4294967295）或 IP 地址格式。

brief：显示数据库的概要信息。

asbr：显示数据库中 ASBR 路由器发布的 Type-4 LSA（summary-Asbr-LSA）的信息。

ase：显示数据库中 Type-5 LSA（AS-external-LSA）的信息。

network：显示数据库中 Type-2 LSA（Network-LSA）的信息。

nssa：显示数据库中 Type-7 LSA（NSSA-external-LSA）的信息。

router：显示数据库中 Type-1 LSA（Router-LSA）的信息。

summary：显示数据库中 Type-3 LSA（Summary-Net-LSA）的信息。

ip-address：以 IP 地址形式表示的链路状态 ID。

originate-router *ip-address*：发布 LSA 报文的路由器的 IP 地址。

self-originate：查看本地防火墙自己产生的 LSA（self-originate LSA）的数据库信息。

【描述】

display ospf lsdb 命令用来显示 OSPF 的连接状态数据库信息。

【举例】

显示 OSPF 的链路状态数据库信息。

```
<H3C> display ospf lsdb
                OSPF Process 1 with Router ID 123.1.1.1
                        Link State Database


                         Area: 0.0.0.0
Type LinkState ID    AdvRouter        Age Len  Sequence   Metric Where
Rtr  1.1.1.1         1.1.1.1          563 36   80000008        0 SpfTree
Net  1.1.1.2         123.1.1.1        595 32   80000001        0 SpfTree

                     AS External Database:
Type LinkState ID    AdvRouter        Age Len  Sequence   Metric Where
ASE  1.1.0.0        1.1.1.1         561 36   80000001        1 Uninitialized
ASE  123.1.1.1      1.1.1.1         561 36   80000001        1 Uninitialized
```

表3-7 display ospf lsdb 命令显示信息说明

符号	意义
Type	此 LSA 的类型
LinkStateID	此 LSA 的链路状态 ID
AdvRouter	发布此 LSA 的路由器的 router ID
Age	此 LSA 的年龄
Len	此 LSA 的长度
Sequence	此 LSA 的序列号
Metric	发布此 lsa 的路由器到此 lsa 描述的目的地的花费
Where	此 LSA 的位置

```
<H3C> display ospf lsdb ase

                OSPF Process 1 with Router ID 172.16.2.2
                        Link State Database

 Type: ASE
```

```
Ls id :  2.2.0.0
Adv rtr: 1.1.1.1
Ls age:  349
Len:36
Seq#:   80000001
Chksum:  0xfcaf
Options: (DC)
Net mask:255.255.0.0
    Tos 0 metric: 1
    E type :2
    Forwarding Address: 0.0.0.0
    Tag: 1
```

表3-8 display ospf lsdb ase 命令显示信息说明

符号	意义
Type	此 LSA 的类型
Ls id	此 LSA 的链路状态 ID
Adv rtr	发布此 LSA 的路由器的 Router ID
Ls age	此 LSA 已经存在的时间
Len	此 LSA 的长度
Seq#	此 LSA 的序列号
Chksum	此 LSA 的校验和
Options	此 LSA 的选项
Net mask	网络掩码
E type	外部路由类型
Forwarding Address	转发地址
Tag	标记

3.1.21 display ospf nexthop

【命令】

display ospf [*process-id*] **nexthop**

【视图】

所有视图

【参数】

process-id：OSPF 进程号。如果不指定进程号，则对当前所有 OSPF 进程有效。

【描述】

display ospf nexthop 命令用来显示 OSPF 的下一跳信息。

【举例】

显示 OSPF 的下一跳信息。

```
<H3C> display ospf nexthop
                OSPF Process 1 with Router ID 2.2.2.2

Next hops:
Address          Type      Refcount  Intf Addr       Intf Name
------------------------------------------------------------------------
10.0.0.2         Direct           3  10.0.0.2        Ethernet0/0/1
10.1.1.1         Neighbor         6  10.0.0.2        Ethernet0/0/1
60.0.0.1         Direct           3  60.0.0.1        Dialer0
80.0.0.1         Direct           3  80.0.0.1        Dialer1
90.0.0.1         Direct           3  90.0.0.1        Dialer3
```

表3-9 display ospf nexthop 命令显示信息说明

符号	意义
Address	下一跳地址
Type	下一跳类型
Refcount	此下一跳的引用计数，即多少条路由使用此下一跳
Intf Addr	到此下一跳的出接口 IP 地址
Intf Name	到此下一跳的出接口

3.1.22 display ospf peer

【命令】

display ospf [*process-id*] **peer** [**brief** | **statistics**]

【视图】

所有视图

【参数】

process-id：OSPF 进程号。如果不指定进程号，则对当前所有 OSPF 进程有效。

brief：当使用该参数时，显示各区域邻居的简要信息。

statistics：显示邻居的统计信息

【描述】

display ospf peer 命令用来显示 OSPF 中各区域邻居的信息。

OSPF 邻居的存活时间显示格式根据时间长短，有不同的显示格式。说明如下：

XXYXXMXXD：超过一年，即年：月：日

XXXdXXhXXm：超过一天但是不到一年，即日：时：分

XX:XX:XX：小于一天，即时：分：秒

【举例】

显示 OSPF 的邻接点信息。

```
<H3C> display ospf peer

                OSPF Process 1 with Router ID 1.1.1.1
                          Neighbors

Area 0.0.0.0 interface 10.153.17.88(Rthernet0/0/0)'s neighbor(s)
  RouterID: 2.2.2.2         Address: 10.153.17.89
        State: Full  Mode: Nbr is Master  Priority: 1
        DR: 10.153.17.89  BDR: 10.153.17.88
        Dead timer expires in 31s
        Neighbor has been up for 01:14:14
```

表3-10 display ospf peer 命令显示信息说明

符号	意义
Router ID	邻居路由器的 Router ID
Address	邻居路由器与本路由器通信的接口的地址
State	邻接关系的状态
Mode	交换 DD 报文时协商形成的主从模式，或是 master 或是 slave
Priority	邻居参与选举 DR/BDR 的优先级
DR	选出的 DR 在此网路中的接口的 ip 地址
BDR	选出的 BDR 在此网路中的接口的 ip 地址
Dead timer expires in 31s	离邻居失效还剩多长时间
Neighbor has been up for 01:14:14	邻居存在的时间

显示 OSPF 的邻接点的简要信息。

```
<H3C> display ospf peer brief
```

```
                OSPF Process 1 with Router ID 1.1.1.1
                       Neighbor Brief Information

 Area 0.0.0.0:
 Router ID       Address         Pri  DeadTime(s) Interface          State
 2.2.2.2         172.16.2.1       1    35          Ethernet0/0/0  Full/DR
```

表3-11 display ospf peer brief 命令显示信息说明

符号	意义
RouterID	邻居路由器的 Router ID
Address	邻居路由器与本路由器通信的接口的地址
Pri	邻居参与选举 DR/BDR 的优先级
DeadTime(s)	离邻居失效还剩多长时间
Interface	与邻居连接的接口
State	邻接关系的状态

3.1.23 display ospf request-queue

【命令】

display ospf [*process-id*] **request-queue**

【视图】

所有视图

【参数】

process-id：OSPF 进程号。如果不指定进程号，则对当前所有 OSPF 进程有效。

【描述】

display ospf request-queue 命令用来显示 OSPF 的请求列表信息。

【举例】

查看 OSPF 请求列表信息。

```
<H3C> display ospf request-queue
   The Router's Neighbors is
  RouterID:  1.1.1.1         Address: 1.1.1.1
  Interface: 1.1.1.3         Area: 0.0.0.0
  LSID:1.1.1.3          AdvRouter:1.1.1.3  Sequence:80000017  Age:35
```

表3-12 display ospf request-queue 命令显示信息说明

符号	意义
RouterID	邻居路由器的 Router ID
Address	邻居路由器与本路由器通信的接口的地址
Interface	该网段接口地址
Area	OSPF 区域号
LSID:1.1.1.3	此 LSA 的 Link State ID（链路状态标识）
AdvRouter	发布此 LSA 的路由器的 Router ID
Sequence	此 LSA 的序列号，以发现旧的和重复的 LSA
Age	此 LSA 的存活时间

3.1.24 display ospf retrans-queue

【命令】

display ospf [*process-id*] **retrans-queue**

【视图】

所有视图

【参数】

process-id：OSPF 进程号。如果不指定进程号，则对当前所有 OSPF 进程有效。

【描述】

display ospf retrans-queue 命令用来显示 OSPF 的重传列表信息。

【举例】

显示 OSPF 重传列表信息。

```
<H3C> display ospf retrans-queue
OSPF Process 200 with Router ID 103.160.1.1
Retransmit List
      The Router's Neighbors is
  RouterID: 162.162.162.162 Address: 103.169.2.2
  Interface: 103.169.2.5     Area: 0.0.0.1
          Retrans list:
          Type: ASE  LSID:129.11.77.0  AdvRouter:103.160.1.1
          Type: ASE  LSID:129.11.108.0  AdvRouter:103.160.1.1
```

表3-13 display ospf retrans-queue 命令显示信息说明

符号	意义
RouterID	邻居路由器的 Router ID
Address	邻居路由器与本路由器通信的接口的地址
Interface	该网段接口地址
Area	OSPF 区域号
Type	此 LSA 的类型
LSID	此 LSA 的 Link State ID（链路状态标识）
AdvRouter	发布此 LSA 的路由器的 Router ID

3.1.25 display ospf routing

【命令】

display ospf [*process-id*] **routing**

【视图】

所有视图

【参数】

process-id：OSPF 进程号。如果不指定进程号，则对当前所有 OSPF 进程有效。

【描述】

display ospf routing 命令用来显示 OSPF 路由表的信息。

【举例】

显示 OSPF 路由表的信息。

```
<H3C> display ospf routing

                OSPF Process 1 with Router ID 1.1.1.1
                        Routing Tables

Routing for Network
Destination          Cost Type NextHop         AdvRouter        Area
172.16.2.0/24           1 Net  172.16.2.1      2.2.2.2          0.0.0.0
2.2.2.2/32              2 Stub 172.16.2.1      2.2.2.2          0.0.0.0
172.16.1.0/24           2 SNet 172.16.2.1      2.2.2.2          0.0.0.0
3.3.3.3/32              3 SNet 172.16.2.1      2.2.2.2          0.0.0.0
```

```
1.1.1.1/32              1 Stub 1.1.1.1        1.1.1.1          0.0.0.0

Total Nets: 5
  Intra Area: 3  Inter Area: 2  ASE: 0  NSSA: 0
```

表3-14 display ospf routing 命令显示信息说明

符号	意义
Destination	目的网段
Cost	路由花费
Type	路由类型
NextHop	路由下一跳
AdvRouter	发布此路由的路由器的 Router ID
Area	区域 ID
Intra Area	区域内部路由条数
Inter Area	域间路由条数
ASE	外部路由条数
NSSA	NSSA 路由条数

3.1.26 display ospf vlink

【命令】

display ospf [*process-id*] **vlink**

【视图】

所有视图

【参数】

process-id：OSPF 进程号。如果不指定进程号，则对当前所有 OSPF 进程有效。

【描述】

display ospf vlink 命令用来显示 OSPF 的虚连接信息。

【举例】

显示 OSPF 的虚连接信息。

```
<H3C> display ospf vlink

        OSPF Process 1 with Router ID 2.2.2.2
```

```
                Virtual Links

 Virtual-link Neighbor-id  -> 3.3.3.3, State: Full
 Interface: 172.16.1.1 (Ethernet0/0/1)
   Cost: 1 State: PtoP    Type: Virtual
   Transit Area: 0.0.0.1
   Timers: Hello 10, Dead 40, Poll 0, Retransmit 5, Transmit Delay 1
```

表3-15 display ospf vlink 命令显示信息说明

符号	意义	
Virtual-link Neighbor-id	虚连接邻居路由器的 Router ID	
State	状态	
Interface	属于此虚连接的本端接口 IP 地址	
Cost	接口的路由开销	
State	点到点	
Type	类型：虚连接	
Transit Area	此虚连接所穿越的转换区 ID，此区域不可以是骨干区、STUB 区和 NSSA 区	
Timers	OSPF 计时器，分别定义：	
	Hello	hello 报文间隔
	Dead	邻居失效时间间隔
	Poll	轮询时间间隔
	Retransmit	接口重传 LSA 时间间隔
Transmit Delay	接口对 LSA 的传输延迟时间	

3.1.27 filter-policy export

【命令】

filter-policy { *acl-number* | **ip-prefix** *ip-prefix-name* } **export** [*routing-protocol*]

undo filter-policy { *acl-number* | **ip-prefix** *ip-prefix-name*} **export** [*routing-protocol*]

【视图】

OSPF 视图

【参数】

acl-number：访问列表的序号。

ip-prefix-name：地址前缀列表的序号。

routing-protocol：发布路由信息的协议，目前可包括：**direct**、**bgp**、**rip** 和 **static**。

【描述】

filter-policy export 命令用来设置 OSPF 对向外发布的引入路由的 LSA 进行过滤，**undo filter-policy export** 命令用来取消已设置的过滤规则。

缺省情况下，不对发布的任何路由的 LSA 信息进行过滤。

某些情况下，可能要求只发布某些满足条件的路由的 LSA 信息，此时，可以定义 filter-policy 设置过滤条件，只有通过了过滤的路由的 LSA 信息才能被发布。

相关配置可参考命令 **acl** 和 **ip ip-prefix**。

【举例】

配置 OSPF 仅发布通过 acl 2001 的路由信息。

```
[H3C] acl number 2001
[H3C-acl-basic-1] rule permit source 11.0.0.0 0.255.255.255
[H3C-acl-basic-1] rule deny source any
[H3C-ospf-1] filter-policy 2001 export
```

3.1.28 filter-policy import

【命令】

filter-policy { *acl-number* | **ip-prefix** *ip-prefix-name* | **gateway** *prefix-list- name* } **import**

undo filter-policy { *acl-number* | **ip-prefix** *ip-prefix-name* | **gateway** *ip-prefix-name* } **import**

【视图】

OSPF 视图

【参数】

acl-number：用于过滤路由信息目的地址的访问列表号。

ip-prefix-name：用于过滤路由信息目的地址的地址前缀列表名。

gateway *ip-prefix-name*：用于过滤发布该路由信息的邻居路由器地址的地址前缀列表名。

【描述】

filter-policy import 命令用来设置 OSPF 对接收的路由信息进行过滤的规则，**undo filter-policy import** 命令用来取消对接收路由信息的过滤。

缺省情况下，不对接收的任何路由信息进行过滤。

某些情况下，可能要求只接收某些满足条件的路由信息，此时，可以定义 **filter-policy** 设置所发布路由信息的过滤条件，只有通过了过滤的路由信息才能被接收。

filter-policy import 命令对 OSPF 计算出来的路由进行过滤，只有通过过滤器的路由才被添加到路由表中，通不过的路由不被加入到路由表中。可以根据路由的下一跳和目的地进行过滤。

由于 OSPF 是基于链路状态的动态路由协议，路由信息隐藏在链路状态中，不能对发布和接收的链路状态信息进行过滤。该命令在 OSPF 中的使用比在距离向量的路由协议中的使用要有限得多。

如果启动了多个 OSPF 进程，该命令只对本进程起作用。

【举例】

按照访问控制列表 2002 定义的规则对接收的路由信息进行过滤。

```
[H3C] acl number 2002
[H3C-acl-basic-2002] rule permit source 20.0.0.0 0.255.255.255
[H3C-acl-basic-2002] rule deny source any
[H3C-ospf-1] filter-policy 2002 import
```

3.1.29 import-route

【命令】

import-route *protocol* [**allow-ibgp**] [**cost** *value*] [**type** *value*] [**tag** *value*] [**route-policy** *route-policy-name*]

undo import-route *protocol*

【视图】

OSPF 视图

【参数】

protocol：可引入的源路由协议，目前可为 **direct**、**bgp**、**static**、**rip**、**ospf**、**ospf-ase**、**ospf-nssa**。

ospf *process-id*：只引入 OSPF 进程 *process-id* 发现的内部路由作为外部路由信息。若未指定进程号，则采用 OSPF 的缺省进程号 1。

ospf-ase *process-id*：只引入 OSPF 进程 *process-id* 发现的 ASE 外部路由作为外部路由信息。若未指定进程号，则采用 OSPF 的缺省进程号 1。

ospf-nssa *process-id*：只引入 OSPF 进程 *process-id* 发现的 NSSA 外部路由作为外部路由信息。若未指定进程号，则采用 OSPF 的缺省进程号 1。

allow-ibgp：当 *protocol* 为 BGP 时，**allow-ibgp** 为可选关键字。**import-route bgp** 表示只引入 EBGP 路由，**import-route bgp allow-ibgp** 表示将 IBGP 路由也引入，该配置危险，请慎用！

cost *value*：引入路由的 cost 值。缺省情况下，cost 为 1。

type *value*：指定 OSPF 在引入其它协议路由时的路由类型，*value* 的取值为 1 或 2，**type 1** 为一类外部路由，**type 2** 为二类外部路由，缺省为 **type 2**。

tag *value*：对引入的外部路由设定标记。缺省情况下，tag 为 1。

route-policy *route-policy-name*：只有满足指定 Route-policy 的匹配条件的路由才被引入。

【描述】

import-route 命令用来引入外部路由信息，**undo import-route** 命令用来取消对外部路由信息的引入。

如果引入类型为 1 的外部路由，则在路由表中，metric 值为本防火墙到达广播此条外部路由的路由器的 metric 值加上引入时使用的 cost 值。如果引入类型 2 的外部路由，则路由表中的 metric 值就是引入时设定的 cost 值。

此命令不是累加形式，cost、type、tag 等参数应在同一条命令中一次设定，否则后配置的命令会覆盖先配置的命令。

缺省情况下，不引入其它协议的路由信息。

【举例】

指定引入 RIP 路由为第二类外部路由，路由标记为 33 而且路由花费值为 50。

```
[H3C-ospf-1] import-route rip type 2 tag 33 cost 50
```

OSPF 进程 100 引入 OSPF 进程 160 发现的路由。

```
[H3C-ospf-100] import-route ospf 160
```

3.1.30 log-peer-change

【命令】

log-peer-change

undo log-peer-change

【视图】

OSPF 视图

【参数】

无

【描述】

log-peer-change 命令用来打开该 OSPF 进程下的邻接状态变化的输出开关，**undo log-peer-change** 命令用来关闭输出开关。

缺省情况下，输出开关关闭。

当打开邻接状态输出开关后，该 OSPF 进程下邻接状态的变化会输出到配置终端上，直至邻接状态输出开关被关闭。

【举例】

在当前防火墙上打开 OSPF 进程 1 的邻接状态变化的输出开关。

```
[H3C-ospf-1] log-peer-change
%Nov 15 09:08:23:233 2005 H3C RM/5/RTLOG:
OSPF-ADJCHANGE:Process 1,Adjacency To 172.16.2.1 (Ethernet0/0/0) from Fullto
Down

%Nov 15 09:07:18:368 2005 H3C RM/5/RTLOG:
OSPF-ADJCHANGE:Process 1,Adjacency To 172.16.2.1 (GigabitEthernet0/0/0) from
Loading to Full
```

3.1.31 multi-path-number

【命令】

multi-path-number *number*

undo multi-path-number

【视图】

OSPF 视图

【参数】

number：等价路由的个数，取值范围为 1～3，缺省为 3。

【描述】

multi-path-number 命令用来配置 OSPF 等价路由的最大个数，**undo multi-path-number** 命令用来恢复 OSPF 等价路由最大个数的缺省值。

【举例】

配置 OSPF 等价路由的个数为 2

```
[H3C-ospf-1] multi-path-number 2
```

3.1.32 network

【命令】

network *ip-address wildcard*

undo network *ip-address wildcard*

【视图】

OSPF 区域视图

【参数】

ip-address：接口所在网段地址。

wildcard：IP 地址通配符。

【描述】

network 命令用来指定运行 OSPF 的接口，**undo network** 命令用来取消运行 OSPF 的接口。

缺省情况下，接口不属于任何区域。

为了在一个接口上运行 OSPF 协议，必须使该接口的主 IP 地址落入该命令指定的网段范围。如果只有接口的从 IP 地址落入该命令指定的网段范围，则该接口不会运行 OSPF 协议。

相关配置可参考命令 **ospf**。

【举例】

指定主 IP 地址在 10.110.36.0 网段范围内的接口运行 OSPF 协议，并指定这些接口所在的 OSPF 区域号为 6。

```
[H3C-ospf] area 6
[H3C-ospf-1-area-0.0.0.6] network 10.110.36.0 0.0.0.255
```

3.1.33 nssa

【命令】

nssa [**default-route-advertise** | **no-import-route** | **no-summary**] *

undo nssa

【视图】

OSPF 区域视图

【参数】

default-route-advertise：该参数只用于 NSSA 区域的 ABR 或 ASBR，配置后，对于 ABR，不论本地是否存在缺省路由，都将生成一条 Type-7 LSA 向区域内发布缺省路由；对于 ASBR，只有当本地存在缺省路由时，才产生 Type-7 LSA 向区域内发布缺省路由。

no-import-route：该参数用于禁止将 AS 外部路由以 Type-7 LSA 的形式引入到 NSSA 区域中，这个参数通常只用在既是 NSSA 区域的 ABR，也是 OSPF 自治系统的 ASBR 的路由器上，以保证所有外部路由信息能正确地进入 OSPF 路由域。

no-summary：该参数只用于 NSSA 区域的 ABR，配置后，NSSA ABR 只通过 Type-3 的 Summary-LSA 向区域内发布一条缺省路由，不再向区域内发布任何其它 Summary-LSAs（这种区域又称为 NSSA totally stub 区域）。

【描述】

nssa 命令用来将一个 OSPF 区域配置为 NSSA 区域，**undo nssa** 命令用来取消区域的 NSSA 属性。

缺省情况下，不配置 NSSA 区域。

如果要将一个区域配置成 NSSA 区域，则该区域中的所有路由器都必须配置此属性。

【举例】

将区域 1 配置成 NSSA 区域。

```
[H3C-ospf-1] area 1
[H3C-ospf-1-area-0.0.0.1] network 10.110.0.0 0.0.255.255
[H3C-ospf-1-area-0.0.0.1] nssa
```

3.1.34 ospf

【命令】

ospf [*process-id* [[**router-id** *router-id*] **vpn-instance** *vpn-instance-name*]]

undo ospf [*process-id*]

【视图】

系统视图

【参数】

process-id：OSPF 进程号，取值范围为 1～65535。如果不指定进程号，将使用缺省进程号 1。

router-id：OSPF 进程使用的 Router ID，点分十进制形式。

vpn-instance-name：OSPF 进程绑定的 VPN 实例的名称。

【描述】

ospf 命令用来启动 OSPF 进程，**undo ospf** 命令用来关闭 OSPF 进程。

缺省情况下，系统不运行 OSPF 协议。

通过指定不同的进程号，可以在一台防火墙上运行多个 OSPF 进程。这种情况下，建议用户使用命令中的 **router-id** 为不同进程指定不同的 Router ID。

如果将 OSPF 用于 MPLS VPN 解决方案的 VPN 内部路由协议，需要将 OSPF 进程与 VPN 实例进行绑定，详细介绍请参考本手册的“VPN”部分。

相关配置可参考命令 **network**。

【举例】

启动 OSPF 协议的运行。

```
[H3C] router id 10.110.1.8
[H3C] ospf
[H3C-ospf-1]
```

启动进程号为 120 的 OSPF 进程，运行 OSPF 协议。

```
[H3C] router id 10.110.1.10
[H3C] ospf 120
[H3C-ospf-120]
```

3.1.35 ospf authentication-mode

【命令】

ospf authentication-mode { **simple** *password* | **md5** *key-id key* }

undo ospf authentication-mode { **simple** | **md5** }

【视图】

接口视图

【参数】

simple *password*：采用明文验证，*password* 的最大长度为 8 个字符的字符串。

key-id：MD5 密文验证方式时的验证字标识符，取值范围为 1～255。

key：MD5 验证字，如果用户采用明文形式输入验证字，则可输入长度为 1～16 个字符的字符串；当用户使用 **display current-configuration** 命令显示系统信息时，系统以 24 个字符的 cipher 密文形式显示配置的 MD5 验证字。系统也支持直接输入长度为 24 个字符的 cipher 密文形式验证字。

【描述】

ospf authentication-mode 命令用来设置相邻路由器之间的验证方式及验证字，**undo ospf authentication-mode** 命令用来删除已设置的验证字。

缺省情况下，接口不对 OSPF 报文进行验证。

同一网段的路由器的验证字口令必须相同；并且，需使用 **authentication-mode** 命令来设置区域验证字的验证类型，以达到使配置生效的目的。

相关配置可参考命令 **authentication-mode**。

【举例】

配置接口 Ethernet1/0/0 的网段 131.119.0.0 所在的区域 1 支持 MD5 密文验证，验证字标识符为 15，验证字为 ospfpwd。

```
[H3C-ospf-1] area 1
[H3C-ospf-1-area-0.0.0.1] network 131.119.0.0 0.0.255.255
[H3C-ospf-1-area-0.0.0.1] authentication-mode md5
[H3C-ospf-1-area-0.0.0.1] interface Ethernet 1/0/0
[H3C-Ethernet1/0/0] ospf authentication-mode md5 15 ospfpwd
```

3.1.36 ospf cost

【命令】

ospf cost *value*

undo ospf cost

【视图】

接口视图

【参数】

value：运行 OSPF 协议所需的开销，取值范围为 1～65535。

【描述】

ospf cost 命令用来配置不同的发送报文的开销值，以便在不同的接口上发送报文，**undo ospf cost** 命令用来恢复运行 OSPF 所需开销的缺省值。

缺省情况下，接口按照当前的波特率自动计算接口运行 OSPF 协议所需的开销。

【举例】

指定接口运行 OSPF 协议的开销为 33。

```
[H3C] interface Ethernet1/0/0
[H3C-Ethernet1/0/0] ospf cost 33
```

3.1.37 ospf dr-priority

【命令】

ospf dr-priority *value*

undo ospf dr-priority

【视图】

接口视图

【参数】

value：接口在选举“指定路由器”时的优先级，取值范围为 0～255，缺省值为 1。

【描述】

ospf dr-priority 命令用来设置接口在选举“指定路由器”时的优先级，**undo ospf dr-priority** 命令用来恢复其缺省值。

接口的优先级决定了该接口在选举“指定路由器”时所具有的资格，优先级高的在选举权发生冲突时被首先考虑。

【举例】

设置接口 Ethernet1/0/0 在选举 DR 时的优先级为 8。

```
[H3C] interface ethernet1/0/0
[H3C-Ethernet1/0/0] ospf dr-priority 8
```

3.1.38 ospf mib-binding

【命令】

ospf mib-binding *process-id*

undo ospf mib-binding

【视图】

系统视图

【参数】

process-id：OSPF 进程号。

【描述】

ospf mib-binding 命令用于将 MIB 操作绑定在指定的 OSPF 进程上，**undo ospf mib-binding** 命令用于恢复缺省设置。

OSPF 协议启动第一个进程时，总是将 MIB 的操作绑定在该进程上。使用该命令可以将 MIB 的操作绑定到其它的 OSPF 进程。若想取消绑定设置，可以使用 **undo ospf mib-binding** 命令，OSPF 将自动把 MIB 的操作重新绑定在第一个启动的进程上。

缺省情况下，MIB 操作绑定在第一个启动的 OSPF 进程上。

【举例】

将 MIB 的操作绑定在进程号为 100 的 OSPF 进程上。

```
[H3C] ospf mib-binding 100
```

取消 MIB 的操作绑定。

```
[H3C] undo ospf mib-binding
```

3.1.39 ospf mtu-enable

【命令】

ospf mtu-enable

undo ospf mtu-enable

【视图】

接口视图

【参数】

无

【描述】

ospf mtu-enable 命令用来使能接口在发送 DD 报文时填 MTU 值，**undo ospf mtu-enable** 命令用来恢复缺省设置。

缺省情况下，接口发送 DD 报文时 MTU 值为 0，即不填接口的实际 MTU 值。

运行 OSPF 协议的路由器在进行数据库同步时，使用 DD 报文（Database Description Packet）描述自己的 LSDB。

DD 报文中的 MTU 值缺省为 0，使用本命令可以手工设定指定接口在发送时填写 DD 报文中的 MTU 值域，即使用接口的实际 MTU 值填写。

【举例】

指定 Ethernet1/0/0 接口在发送 DD 报文时，填写 MTU 值域：

```
[H3C] interface Ethernet1/0/0
[H3C-Ethernet1/0/0] ospf mtu-enable
```

3.1.40 ospf network-type

【命令】

ospf network-type { **broadcast** | **nbma** | **p2mp** | **p2p** }

undo ospf network-type

【视图】

接口视图

【参数】

broadcast：将接口的网络类型改为广播。

nbma：将接口的网络类型改为 NBMA。

p2mp：将接口的网络类型改为点到多点。

p2p：将接口的网络类型改为点到点。

【描述】

ospf network-type 命令用来设置 OSPF 接口的网络类型，**undo ospf network-type** 命令用来恢复 OSPF 接口缺省的网络类型。

OSPF 根据链路层协议类型将网络分为下列四种类型：

- 当链路层协议是 Ethernet 时，OSPF 缺省认为网络类型是 Broadcast。
- 当链路层协议是 ATM、帧中继、HDLC 或 X.25 时，OSPF 缺省认为网络类型是 NBMA。
- 没有一种链路层协议会被 OSPF 缺省认为是 Point-to-Multipoint 类型，通常由 NBMA 的类型手工修改而来，如果 NBMA 类型的网络不是全连通的。
- 当链路层协议是 PPP、LAPB 时，OSPF 缺省认为网络类型是 Point-to-Point。

如果在广播网络上有不支持组播地址的路由器，可以将接口的网络类型改为 NBMA。也可以将接口的网络类型由 NBMA 改为广播。

一个非广播多点可达的网络符合 NBMA 类型或可以改为广播类型的条件是：任意两台路由器之间都有一条虚电路直接可达，或者说，这个网络是全连通的。如果网络不满足这个条件，必须将接口的网络类型改为点到多点。这样，两台不能直接可达的路由器之间可以通过一台与两者都直接可达的路由器来交换路由信息。

如果同一网段内只有两台路由器运行 OSPF 协议，也可以将接口的网络类型改为点到点。

注意：接口的网络类型为 NBMA 或使用本命令将接口的网络类型手工改为 NBMA 时，必须使用命令 **peer** 来配置邻接点。

相关配置可参考命令 **ospf dr-priority**。

【举例】

将接口 Ethernet1/0/0 设置为非广播 NBMA 类型。

```
[H3C] interface Ethernet1/0/0
[H3C-Ethernet1/0/0] ospf network-type nbma
```

3.1.41 ospf timer dead

【命令】

ospf timer dead *seconds*

undo ospf timer dead

【视图】

接口视图

【参数】

seconds：OSPF 邻居失效的时间，单位为秒，取值范围为 1～65535。

【描述】

ospf timer dead 命令用来设置 OSPF 的邻居失效时间，**undo ospf timer dead** 命令用来恢复邻居失效时间的缺省值。

point-to-point、**broadcast** 类型接口的 OSPF 邻居失效时间为 40 秒，**point-to-multipoint**、**non-broadcast** 类型接口的 OSPF 邻居失效时间为 120 秒。

OSPF 邻居的失效时间是指：在该时间间隔内，若未收到邻居的 Hello 报文，就认为该邻居已失效。**dead** *seconds* 值至少应为 **hello** *seconds* 值的 4 倍，同一网段上的路由器的 **dead** *seconds* 也必须相同。

相关配置可参考命令 **ospf timer hello**。

【举例】

配置接口 Ethernet1/0/0 上的邻居失效时间为 80 秒。

```
[H3C] interface Ethernet1/0/0
[H3C-Ethernet1/0/0] ospf timer dead 80
```

3.1.42 ospf timer hello

【命令】

ospf timer hello *seconds*

undo ospf timer hello

【视图】

接口视图

【参数】

seconds：接口发送 Hello 报文的时间间隔，单位为秒，取值范围为 1～255。

【描述】

ospf timer hello 命令用来设置接口发送 Hello 报文的时间间隔，**undo ospf timer hello** 命令用来恢复该时间间隔的缺省值。

point-to-point、**broadcast** 类型接口发送 Hello 报文的时间间隔的值为 10 秒；**point-to-multipoint**、**non-broadcast** 类型接口发送 Hello 报文的时间间隔的值为 30 秒。

相关配置可参考命令 **ospf timer dead**。

【举例】

配置接口 Ethernet1/0/0 发送 Hello 报文的间隔时间为 20 秒。

```
[H3C] interface Ethernet1/0/0
[H3C-Ethernet1/0/0] ospf timer hello 20
```

3.1.43 ospf timer poll

【命令】

ospf timer poll *seconds*

undo ospf timer poll

【视图】

接口视图

【参数】

seconds：为发送轮询 Hello 报文的时间间隔，取值范围为 1～65535 秒，缺省值为 40 秒。

【描述】

ospf timer poll 命令用来配置 NBMA 和点到多点网络上发送轮询 Hello 报文的时间间隔，**undo ospf timer poll** 命令用来恢复发送轮询 Hello 报文间隔的缺省值。

在 NBMA 和点到多点的网络上，当邻居失效后，将按轮询时间间隔 **poll** *seconds* 定期地发送 Hello 报文。用户可配置轮询时间间隔 **poll** *seconds* 以指定该接口在与相邻路由器构成邻居关系之前发送 Hello 报文的时间间隔。轮询时间间隔 **poll** *seconds* 值至少应为 Hello *seconds* 值的 3 倍。

【举例】

配置接口 Ethernet2/0/0 上发送轮询 Hello 报文的时间间隔为 130 秒。

```
[H3C-Ethernet2/0/0] ospf timer poll 130
```

3.1.44 ospf timer retransmit

【命令】

ospf timer retransmit *interval*

undo ospf timer retransmit

【视图】

接口视图

【参数】

interval：接口重传 LSA 的时间间隔，单位为秒，取值范围为 1～65535，缺省值为 5 秒。

【描述】

ospf timer retransmit 命令用来设置接口重传 LSA 的时间间隔，**undo ospf timer retransmit** 命令用来将接口重传 LSA 的时间间隔恢复为缺省值。

当防火墙向它的邻居发送一条“链路状态广播”（LSA）后，需要等到对方的确认报文。若在该重传 LSA 的时间间隔内未收到对方的确认报文，就会重传这条 LSA。

相邻路由器重传LSA时间间隔的值不要设置得太小，否则将会引起不必要的重传（参见 RFC2328）。

【举例】

指定接口 Ethernet1/0/0 与邻接路由器之间传送链路状态广播时的重传间隔为 12 秒。

```
[H3C] interface Ethernet1/0/0
[H3C-Ethernet1/0/0] ospf timer retransmit 12
```

3.1.45 ospf trans-delay

【命令】

ospf trans-delay *seconds*

undo ospf trans-delay

【视图】

接口视图

【参数】

seconds：接口对 LSA 的传输延迟时间，单位为秒，取值范围为 1～3600，缺省值为 1 秒。

【描述】

ospf trans-delay 命令用来设置接口对 LSA 的传输延迟时间，**undo ospf trans-delay** 命令用来将接口对 LSA 的传输延迟时间恢复为缺省值。

LSA 在本防火墙的链路状态数据库 LSDB 中会随时间老化 Aging（每秒钟加 1），但在网络的传输过程中却不会，所以有必要在发送之前将 LSA 的年龄增加本命令所设置的一段时间。

【举例】

指定接口 Ethernet1/0/0 上传送链路状态广播的时延值为 3 秒。

```
[H3C] interface Ethernet1/0/0
[H3C-Ethernet1/0/0] ospf trans-delay 3
```

3.1.46 peer

【命令】

peer *ip-address* [**dr-priority** *dr-priority-number*]

undo peer *ip-address*

【视图】

OSPF 视图

【参数】

ip-address：邻接点的 IP 地址。

dr-priority-number：用于表示网络邻居的优先级的相应数值，为 0～255 之间的整数，缺省值为 1。

【描述】

peer 命令用来设定相邻路由器 IP 地址以及在一个 NBMA 网络上指定 DR 优先级。**undo peer** 命令用来取消该操作。

在帧中继网络上，可以通过配置映射使整个网络达到全连通（即网络中任意两台路由器之间都存在一条虚电路而直接可达）。这样 OSPF 就可以像广播网络一样处理（如选举 DR、BDR）。但由于无法通过组播 HELLO 报文的形式动态发现相邻路由器，必须手工为接口指定相邻路由器的 IP 地址，该相邻路由器是否有选举权等。

【举例】

设置对端路由器的 IP 地址为 10.1.1.1。

```
[H3C-ospf-1] peer 10.1.1.1
```

3.1.47 preference

【命令】

preference [**ase**] *value*

undo preference [**ase**]

【视图】

OSPF 视图

【参数】

value：OSPF 协议的优先级，取值范围为 1～255。

ase：指明引入自治系统外部路由的优先级。

【描述】

preference 命令用来设置 OSPF 协议路由的优先级，**undo preference** 命令用来恢复 OSPF 协议优先级的缺省值。

缺省情况下，OSPF 内部路由的优先级为 10；外部路由的优先级为 150。

由于防火墙上可能同时运行多个动态路由协议，就存在各个路由协议之间路由信息共享和选择的问题，所以为每一种路由协议指定了一个缺省的优先级。在不同的路由协议发现去往同一目的地的多条路由时，优先级高的协议发现的路由将被选中以转发 IP 报文。

【举例】

指定 OSPF 引入自治系统外部路由的优先级为 160。

```
[H3C-ospf-1] preference ase 160
```

3.1.48 reset ospf

【命令】

reset ospf [**statistics**] { **all** | *process-id* }

【视图】

用户视图

【参数】

statistics：重新初始化 OSPF 进程的统计信息。

process-id：OSPF 进程号。重新启动指定进程号的 OSPF。

all：重新启动所有进程的 OSPF 参数。

【描述】

reset ospf all 命令用来重启 OSPF 的所有 OSPF 进程。使用 **statistics** 参数清除统计数据。

reset ospf *process-id* 命令用来重启 OSPF 相应的进程，使用 **statistics** 参数清除统计数据。

使用 **reset ospf** 命令重启 OSPF，可以获得如下效果：

- 可以立即清除无效的 LSA，而不必等到 LSA 超时；
- 如果改变了 Router ID，该命令的执行会导致新的 Router ID 生效；
- 方便地重新选举 DR、BDR；
- 重启前的 OSPF 配置不会丢失；
- 删除原先生成的 OSPF 路由；
- 重启 OSPF 进程后，将生成相应的路由及全新的 LSA，并发布新的 LSA。

执行该命令后，系统将要求用户确认是否重启 OSPF 协议。

【举例】

重启 OSPF 所有进程。

```
<H3C> reset ospf all
```

重启 OSPF 进程 200。

```
<H3C> reset ospf 200
```

3.1.49 router id

【命令】

router id *router-id*

undo router id

【视图】

系统视图

【参数】

router-id：路由器 ID 号，点分十进制形式。

【描述】

router id 命令用来设置运行 OSPF 协议的路由器 ID 号，**undo router id** 命令用来删除已设置的路由器 ID 号。

缺省情况下，没有配置路由器 ID 号时。

在 OSPF 协议中，路由器 ID 号是一个 32 比特无符号整数，是一台路由器在 OSPF 自治系统中的唯一标识。如果用户没有指定路由器 ID 号，系统会选择所有 loopback 接口中最大的 IP 地址作为路由器的 Router ID。如果没有 loopback 接口，系统会选择所有物理接口的最大 IP 地址作为路由器的 Router ID。若路由器的所有接口都未配置 IP 地址，则必须在系统视图下配置路由器 ID 号，否则 OSPF 无法运行。

在手工设置路由器 ID 号时，必须保证自治系统中任意两台路由器 ID 号都不相同。为此，建议选择 loopback 接口的 IP 地址作为本机 ID 号，因为该接口永远 UP（除非手工 shutdown）。

🕮 **说明：**

- 修改后的路由器 ID 号要在 OSPF 重启后才生效。
- 使用 **router** id 命令配置的路由器 ID 只对公网的 OSPF 有效。

相关配置可参考命令 **ospf**。

【举例】

设置路由器 ID 号为 1.1.1.1。

```
[H3C] router id 1.1.1.1
```

3.1.50 silent-interface

【命令】

silent-interface *interface-type interface-number*

undo silent-interface *interface-type interface-number*

【视图】

OSPF 视图

【参数】

interface-type：接口类型。

interface-number：接口编号。

【描述】

silent-interface 命令用来禁止接口发送 OSPF 报文，**undo silent-interface** 命令用来恢复缺省设置。

缺省情况下，允许接口发送 OSPF 报文。

如果要使 OSPF 路由信息不被某一网络中的路由器获得，可使用本命令禁止在此接口上发送 OSPF 报文。

不同的进程可以对同一接口禁止发送 OSPF 报文，但 **silent-interface** 命令只对本进程已经使能的 OSPF 接口起作用，对其它进程的接口不起作用。

【举例】

禁止接口 Ethernet2/0/0 发送 OSPF 报文。

```
[H3C-ospf-1] silent-interface Ethernet2/0/0
```

3.1.51 snmp-agent trap enable ospf

【命令】

snmp-agent trap enable ospf [*process-id*] [*trap-type*]

undo snmp-agent trap enable ospf [*process-id*] [*trap-type*]

【视图】

系统视图

【参数】

process-id：OSPF 进程号。如果不指定进程号，则对当前所有 OSPF 进程有效。

trap-type：OSPF 发送的 SNMP Trap 报文类型，可以为下表中的关键字。

表3-16 SNMP Trap 报文类型关键字

关键字	用处
ifauthfail	发送接口认证失败 Trap
ifcfgerror	发送接口配置错误 Trap
ifrxbadpkt	发送接口接收到错误报文 Trap
ifstatechange	发送接口状态改变 Trap
iftxretransmit	发送接口重发报文 Trap
lsdbapproachoverflow	发送 LSDB 接近满载 Trap
lsdboverflow	发送 LSDB 超载 Trap
maxagelsa	发送 MaxAge Lsa Trap
nbrstatechange	发送邻居路由器状态改变 Trap

关键字	用处
originatelsa	发送 Originate Lsa Trap
virifauthfail	发送虚接口认证失败 Trap
virifcfgerror	发送虚接口配置错误 Trap
virifrxbadpkt	发送虚接口接收到错误报文 Trap
virifstatechange	发送虚接口状态改变 Trap
viriftxretransmit	发送虚接口重发报文 Trap
virnbrstatechange	发送虚连接邻居路由器状态改变 Trap

【描述】

snmp-agent trap enable ospf 命令用于使能 OSPF 的 Trap 功能，**undo snmp-agent trap enable ospf** 命令用于禁止 OSPF 的 Trap 功能。

该命令对命令执行之后启动的 OSPF 进程无效。

缺省情况下，禁止任何 OSPF 进程发送 Trap 报文。

关于 SNMP Trap 的详细配置，请参考本手册的“基础配置”部分。

【举例】

使能 OSPF 进程 100 的 Trap 功能。

```
[H3C] snmp-agent trap enable ospf 100
```

3.1.52 spf-schedule-interval

【命令】

spf-schedule-interval *interval*

undo spf-schedule-interval

【视图】

OSPF 视图

【参数】

interval：OSPF 的 SPF 计算间隔时间，单位为秒，取值范围为 1～10，缺省值为 5 秒。

【描述】

spf-schedule-interval 命令用来设置 OSPF 路由计算时间间隔，**undo spf-schedule-interval** 命令用来恢复缺省设置。

根据本地维护的链路状态数据库 LSDB，运行 OSPF 协议的防火墙通过 SPF 算法计算出以自己为根的最短路径树，并根据这一最短路径树决定到目的网络的下一跳。通过调节 SPF 的计算间隔，可以抑制网络频繁变化可能导致的占用过多带宽资源和系统资源。

【举例】

设置防火墙的 OSPF 路由计算间隔时间为 6 秒。

```
[H3C-ospf-1] spf-schedule-interval 6
```

3.1.53 stub

【命令】

stub [**no-summary**]

undo stub

【视图】

OSPF 区域视图

【参数】

no-summary：该参数只用于 Stub 区域的 ABR，配置后，ABR 只向区域内发布一条缺省路由的 Summary-LSA，不生成任何其它 Summary-LSAs（这种区域又称为 totally stub 区域）。

【描述】

stub 命令用来将一个区域设置为 Stub 区域，**undo stub** 命令用来取消这种设置。

缺省情况下，没有区域被设置为 Stub 区域。

如果要将一个区域配置成 Stub 区域，则该区域中的所有路由器都必须配置此属性。

相关配置可参考命令 **default-cost**。

【举例】

将 OSPF 区域 1 设置为 Stub 区域。

```
[H3C-ospf-1] area 1
[H3C-ospf-1-area-0.0.0.1] stub
```

3.1.54 vlink-peer

【命令】

vlink-peer *router-id* [**hello** *seconds* | **retransmit** *seconds* | **trans-delay** *seconds* | **dead** *seconds* | **simple** *password* | **md5** *keyid key*] *

undo vlink-peer *router-id*

【视图】

OSPF 区域视图

【参数】

router-id：虚连接邻居的路由器的 ID。

hello *seconds*：接口发送 Hello 报文的时间间隔，单位为秒，取值范围为 1～8192，缺省为 10 秒。该值必须与其建立虚连接路由器上的 **hello** *seconds* 值相等。

retransmit *seconds*：接口重传 LSA 报文的时间间隔，单位为秒，取值范围为 1～3600，缺省为 5 秒。

trans-delay *seconds*：接口延迟发送 LSA 报文的时间间隔，单位为秒，取值范围为 1～3600，缺省为 1 秒。

dead *seconds*：死亡定时器的时间间隔，单位为秒，取值范围为 1～8192，缺省为 40 秒。该值必须与其建立虚连接路由器的 **dead** *seconds* 值相等并至少为 **hello** *seconds* 值的 4 倍。

simple *password*：接口的明文验证字，最多 8 个字符。该值必须与虚连接邻居的验证字相一致。

keyid：接口的 MD5 验证字标识符。取值范围为 1～255。它必须与虚连接邻居的验证字标识符相等。

key：接口的验证字，最多由 16 个字符组成的字符串。它必须与虚连接邻居的验证字相等。当用户使用 **display current-configuration** 命令显示系统信息时，系统以 24 个字符的密文形式显示配置的 MD5 验证字。系统也支持直接输入长度为 24 个字符的密文形式验证字。

【描述】

vlink-peer 命令用来创建并配置一条虚连接，**undo vlink-peer** 命令用来删除一条已有的虚连接。

根据 RFC2328 的规定，OSPF 的区域必须是和骨干区域保持连通的，可以使用 **vlink-peer** 命令建立逻辑上的连通性。在某种程度上，可以将虚连接看做一个普通的使能了 OSPF 的接口，因为在其上配置的 hello、retransmit 和 trans-delay 等参数的原理是类似的。

需要注意的是，当配置虚连接验证时，由骨干区域的 **authentication-mode** 命令来确定使用的验证类型是 MD5 密文验证或是明文验证。

相关配置可参考命令 **authentication-mode** 和 **display ospf**。

【举例】

创建一条到 10.110.0.3 的虚连接，采用 MD5 验证方式。

```
[H3C-ospf-1] area 1
[H3C-ospf-1-area-0.0.0.1] vlink-peer 10.110.0.3 md5 3 345
```

第4章 BGP 配置命令

4.1 BGP 配置命令

说明：

- BGP 中有关用来定义路由策略的命令，请参见下一章“IP 路由策略配置”。
- BGP 中有关 VPN 实例及 VPNv4 的具体参数解释及举例,请参见本手册的“VPN”部分。

4.1.1 aggregate

【命令】

aggregate *address mask* [**as-set**] [**detail-suppressed**] [**suppress-policy** *route-policy-name*] [**origin-policy** *route-policy-name*] [**attribute-policy** *route-policy-name*]

undo aggregate *address mask* [**as-set**] [**detail-suppressed**] [**suppress-policy** *route-policy-name*] [**origin-policy** *route-policy-name*] [**attribute-policy** *route-policy-name*]

【视图】

BGP 视图

【参数】

address：聚合路由的地址，点分十进制格式。

mask：聚合路由的网络掩码，点分十进制格式。

as-set：生成具有 AS 集合段的路由。

detail-suppressed：仅通告聚合路由。

suppress-policy *route-policy-name*：抑制选定的具体路由，不通告部分具体路由。

origin-policy *route-policy-name*：选择用于聚合的源路由。

attribute-policy *route-policy-name*：设置聚合路由的属性。

【描述】

aggregate 命令用来在 BGP 路由表中创建一条聚合记录，**undo aggregate** 命令用来使该功能无效。

缺省情况下，不进行路由聚合。

上述命令的关键字的用处如下表所示：

表4-1 关键字的用处

关键字	用处
as-set	通过设置该关键字，可创建一条聚合路由，该路由的 AS 路径包含了具体路由的 AS 路径信息。若需聚合较多 AS 路径时，请慎用此关键字，因为当具体路由的变化较频繁时，会导致路由振荡。
detail-suppressed	该关键字不抑制聚合路由，但抑制所有具体路由的通告。如果只想对一部分具体路由进行抑制，可以使用 **peer filter-policy** 命令。
suppress-policy	该关键字能产生聚合路由，但抑制指定路由的通告。可以用 **route-policy** 的 **if-match** 子句有选择地抑制一些具体路由，其它具体路由仍被通告。
origin-policy	该关键字仅选择符合 Route-policy 的具体路由来生成聚合路由。
attribute-policy	该关键字可设置聚合路由的属性。通过 **peer route-policy** 等方式也可以完成同样的工作。

【举例】

在 BGP 路由表中创建一条聚合记录。

```
[H3C-bgp] aggregate 192.213.0.0 255.255.0.0
```

4.1.2 bgp

【命令】

bgp *as-number*

undo bgp [*as-number*]

【视图】

系统视图

【参数】

as-number：为指定的本地 AS 号，参数范围为 1～65535。

【描述】

bgp 命令用来启动 BGP，进入 BGP 视图，**undo bgp** 命令用来关闭 BGP。

缺省情况下，系统不运行 BGP。

使用此命令启动和关闭 BGP，并指定 BGP 的本地 AS 号。

【举例】

启动 BGP，本地 AS 号为 100。

```
[H3C] bgp 100
```

```
[H3C-bgp]
```

4.1.3 compare-different-as-med

【命令】

compare-different-as-med

undo compare-different-as-med

【视图】

BGP 视图

【参数】

无

【描述】

compare-different-as-med 命令用来配置允许比较来自不同自治系统中的邻居的路由的 MED 值，**undo compare-different-as-med** 命令用来禁止进行比较。

缺省情况下，不允许比较来自不同 AS 邻居的路由路径的 MED 属性值。

如果到达同一目的地址有多条可选有效路径，可以选择 MED 参数较小的路由作为最终实际使用的路由项。

除非能够确认不同的自治系统采用了同样的 IGP 和路由选择方式，否则不要使用此命令。

【举例】

允许比较来自不同 AS 邻居的路由路径的 MED 属性值。

```
[H3C-bgp] compare-different-as-med
```

4.1.4 confederation id

【命令】

confederation id *as-number*

undo confederation id

【视图】

BGP 视图

【参数】

as-number：为内部包括多个子自治系统的自治系统号，取值范围为 1～65535。

【描述】

confederation id 命令用来配置联盟的 ID，**undo confederation id** 命令用来取消配置的联盟 ID。

缺省情况下，未配置联盟的 ID。

为解决在一个大的 AS 域中可能存在的 IBGP 全连接数过大的问题，可以考虑采用联盟的方法：先将这个 AS 域划分为几个较小的子自治系统（每个子自治系统中均保持全连接的状态），这些子自治系统组成一个联盟体；路由的一些关键的 IGP 属性（下一跳、MED、本地优先级）在通过每个子自治系统时没有丢弃，因此每个子自治系统之间虽然存在 EBGP 关系，但是从联盟外部来看还是一个整体。这样做既保证了原来 AS 域的完整性，同时还可以缓解域中过多的连接数的问题。

相关配置可参考命令 **confederation nonstandard** 和 **confederation peer-as**。

【举例】

ID 号是 9 的联盟体由 38、39、40、41 四个子自治系统组成，其中对端 10.1.1.1 是 AS 联盟体中的成员，而对端 200.1.1.1 则是 AS 联盟体的外部成员，对于外部成员来讲，9 号联盟体就是一个统一的 AS 域。

```
[H3C] bgp 41
[H3C-bgp] confederation id 9
[H3C-bgp] confederation peer-as 38 39 40
[H3C-bgp] peer 10.1.1.1 as-number 38
[H3C-bgp] peer 200.1.1.1 as-number 98
```

4.1.5 confederation nonstandard

【命令】

confederation nonstandard

undo confederation nonstandard

【视图】

BGP 视图

【参数】

无

【描述】

confederation nonstandard 命令用来配置与未采用 RFC1965 配置的 AS 联盟兼容，**undo confederation nonstandard** 命令用来取消同未采用 RFC1965 的兼容。

缺省情况下，配置的联盟与 RFC1965 一致。

为了同采用非标准的设备互通，必须对联盟中所有设备配置该命令。

相关配置可参考命令 **confederation id** 和 **confederation peer-as**。

【举例】

AS100 内有未采用 RFC1965 的路由器，它由 64000、65000 两个子 AS 组成。

```
[H3C] bgp 64000
[H3C-bgp] confederation id 100
[H3C-bgp] confederation peer-as 65000
[H3C-bgp] confederation nonstandard
```

4.1.6 confederation peer-as

【命令】

confederation peer-as *as-number-1* [*.....as-number-n*]

undo confederation peer-as [*as-number-1*] [*.....as-number-n*]

【视图】

BGP 视图

【参数】

as-number-1...as-number-n：为子自治系统号，取值范围从 1 到 65535。最多可配置属于联盟的 32 个子自治系统。

【描述】

confederation peer-as 命令用来指定一个联盟体中包含了哪些子自治系统，**undo confederation peer-as** 命令用来可以删除联盟体中指定的子自治系统。

缺省情况下，未配置属于联盟的子自治系统。

命令中定义的子自治系统属于一个联盟内部，每个子自治系统使用全闭合网。**confederation id** 命令指定各子自治系统所属的联盟，若未配置，本命令无效。

相关配置可参考命令 **confederation nonstandard** 和 **confederation id**。

【举例】

配置属于联盟的子自治系统号为 2000 和 2001。

```
[H3C-bgp] confederation peer-as 2000 2001
```

4.1.7 dampening

【命令】

dampening [*half-life-reachable half-life-unreachable reuse suppress ceiling*] [**route-policy** *policy-name*]

undo dampening

【视图】

BGP 视图

【参数】

half-life-reachable：路由可达时的半衰期，取值范围为 1～45 分钟。缺省值为 15 分钟。

half-life-unreachable：路由不可达时的半衰期，取值范围为 1～45 分钟。缺省值为 15 分钟。

reuse：当惩罚降低到该值以下，路由就被再使用，取值范围为 1～20000。缺省值为 750。

suppress：当惩罚超过该极限时，路由受到抑制，取值范围为 1～20000。缺省值为 2000。

ceiling：惩罚的最高限度，取值范围为 1001～20000。缺省值为 16000。

policy-name：路由策略名。

【描述】

dampening 命令用来使 BGP 路由衰减有效或修改各种 BGP 路由衰减参数，**undo dampening** 命令用来取消路由衰减。

缺省情况下，没有配置路由衰减。

若未配置参数，将取各个参数的缺省值。*half-life-reachable*、*half-life-unreachable*、*reuse*、*suppress* 和 *ceiling* 都是相互依存的，因此如果调整了以上参数中的任何一个，那么所有参数都应该做相应调整。

dampening 命令只对从 EBGP 邻居学到的路由进行衰减，对 IBGP 路由不进行衰减。

相关配置可参考命令 **reset dampening**、**reset bgp flap-info**、**display bgp routing dampened** 和 **display bgp routing flap-info**。

【举例】

修改 BGP 路由衰减参数。

```
[H3C-bgp] dampening 15 15 1000 2000 10000
```

4.1.8 debugging bgp

【命令】

debugging bgp { **all** | **event** | **normal** }

debugging bgp { **keepalive** | **mp-update** | **open** | **packet** | **route-refresh** | **update** } [**receive** | **send**] [**verbose**]

undo debugging bgp { **all** | **event** | **normal** | **keepalive** | **mp-update** | **open** | **packet** | **route-refresh** | **update** }

【视图】

用户视图

【参数】

all：BGP 的所有调试信息开关。

event：BGP 事件调试信息开关。

normal：BGP 一般运行信息的调试信息开关。

keepalive：BGP Keepalive 报文的调试信息开关。

mp-update：MBGP Update 报文调试信息开关。

open：BGP Open 报文的调试信息开关。

packet：BGP 报文调试信息开关。

route-refresh：BGP Route-Refresh 报文调试信息开关。

update：BGP Update 报文调试信息开关。

receive：接收方向的调试信息开关。

send：发送方向的调试信息开关。

verbose：使用此参数查看详细的调试信息。

【描述】

debugging bgp 命令用来打开 BGP 指定类型的调试信息开关；**undo debugging bgp** 命令用来关闭 BGP 指定类型的调试信息开关。

缺省情况下，BGP 所有的调试信息开关都是关闭的。

打开调试信息开关会影响系统的性能，因此，请不要轻易打开调试信息开关，调试完毕后，请及时关闭调试信息开关。

【举例】

打开 BGP 报文调试信息开关。

```
<H3C> debugging bgp packet
```

4.1.9 default-route imported

【命令】

default-route imported

undo default-route imported

【视图】

BGP 视图

【参数】

无

【描述】

default-route imported 命令用来将本地的默认路由引入 BGP 中，**undo default-route imported** 命令用来禁止将本地的默认路由引入 BGP 中。

缺省情况下，本地默认路由没有引入到 BGP 中。

【举例】

用来将本地的默认路由引入 BGP 中。

```
[H3C-bgp] default-route imported
```

4.1.10 default local-preference

【命令】

default local-preference *value*

undo default local-preference

【视图】

BGP 视图

【参数】

value：配置的缺省本地优先级，取值范围为 0～4294967295，该值越大则优先级越高。缺省的本地优先级为 100。

【描述】

default local-preference 命令用来配置本地优先级，**undo default local-preference** 命令用来恢复本地优先级的缺省值。

可以用配置不同本地优先级的方法来影响 BGP 的路由选择。

在配置完缺省的本地优先级后，只有在此之后接收和发送路由时才会触发 BGP 对路径的重新优选。若要立即或对已有的路由进行重新优选，需要使用 **refresh bgp all import** 或 **reset bgp all** 命令。

【举例】

将防火墙的 BGP 缺省本地优先级 100 更改为 180。

```
[H3C-bgp] default local-preference 180
```

4.1.11 default med

【命令】

default med *med-value*

undo default med

【视图】

BGP 视图

【参数】

med-value：为指定的 MED 值，取值范围为 0～4294967295。缺省的 *med-value* 为 0。

【描述】

default med 命令用来配置系统的 MED 值，**undo default med** 命令用来恢复 MED 的缺省值。

多出口区分（MED）属性是一个路由的外部度量（metric），与本地优先级属性不同，MED 在自治系统间交换，但进入 AS 的 MED 不离开该 AS。MED 属性用于选择最佳路由，MED 较小的路由被选择。当一个运行 BGP 的路由器通过不同的外部伙伴（External Peer）得到目的地址相同、下一跳不同的路由时，将根据不同路由的 MED 值进行优先选择。在其它条件相同的情况下，MED 较小的路由作为自治系统的外部路由。

【举例】

配置防火墙的 BGP 的 MED 为 25。

```
[H3C-bgp] default med 25
```

4.1.12 display bgp group

【命令】

display bgp [**multicast** | **vpnv4** { **all** | **route-distinguisher** *route-distinguisher* | **vpn-instance** *vpn-instance-name* }] **group** [*group-name*]

【视图】

所有视图

【参数】

multicast：多播地址族。

vpnv4：VPNv4 地址族。

vpn-instance *vpn-instance-name*：VPN 实例名称。

route-distinguisher *route-distinguisher*：路由标识的名称。

group-name：为指定的对等体组。

【描述】

display bgp group 命令用来显示对等体组信息。

【举例】

显示对等体组 aaa 的信息。

```
<H3C> display bgp group aaa
Group : aaa  type : external
  as-number : 200
  members in this group :
                10.1.1.1         11.1.1.1
  configuration within the group :
    no export policy route-policy
    no export policy filter-policy
    no export policy as-path-acl
    no export policy ip-prefix
    route-policy specified in import policy : aaa
    no import policy filter-policy
    no import policy as-path-acl
    no import policy ip-prefix
```

表4-2 display bgp group 命令显示信息说明

符号	意义
Group	对等体组名称
type	对等体组类型：IBGP 或者 EBGP
as-number	对等体组 AS 号
members in this group	属于此对等体组的成员
route-policy	配置的路由策略名称
filter-policy	配置的对 BGP 发布（export）和接收（import）路由过滤
as-path-acl	配置的 AS 路径访问控制列表
ip-prefix	配置的地址前缀列表

4.1.13 display bgp network

【命令】

display bgp [**multicast** | **vpnv4** { **all** | **route-distinguisher** *route-distinguisher* | **vpn-instance** *vpn-instance-name* }] **network**

【视图】

所有视图

【参数】

multicast：多播地址族。

vpnv4：VPNv4 地址族。

vpn-instance *vpn-instance-name*：VPN 实例名称。

route-distinguisher *route-distinguisher*：路由标识的名称。

【描述】

display bgp network 命令用来显示已经配置的路由信息。

【举例】

显示已经配置的路由信息。

```
<H3C> display bgp network
          Network             Mask          Route-policy
  ------------------------------------------------------------
        133.1.1.0         255.255.255.0         None
        112.1.0.0         255.255.0.0           None
```

表4-3 display bgp network 命令显示信息说明

符号	意义
Network	网络地址
Mask	掩码
Route-policy	配置的路由策略

4.1.14 display bgp paths

【命令】

display bgp paths *as-regular-expression*

【视图】

所有视图

【参数】

as-regular-expression：为匹配的 AS 的正则表达式。

【描述】

display bgp paths 命令用来显示 AS 路径信息。

【举例】

显示 AS 路径信息。

```
<H3C> display bgp paths 500
Id  Hash-index References Aggregator Origin As-Path
-------------------------------------------------
3   214        1          <null>      INC   500
```

表4-4 display bgp paths 命令显示信息说明

符号	意义	
Id	次序值	
Hash-Index	哈希值	
References	使用该路径的路由条数	
Aggregator	聚合路由的掩码长度	
Origin	路由的起源（ORIGIN）属性，表示路由条目是以什么方式被通告到 BGP 路由表中。它有如下 3 种取值：	
	IGP	此路由是 AS 内部的；BGP 把聚合路由和用 **network** 命令定义的路由看成是 AS 内部的，起点类型设置为 IGP
	EGP	此路由是从外部网关协议 EGP（Exterior Gateway Protocol）学习到的
	INC	即 INCOMPLETE：表示此路由信息的来源为未知源，即通过其它方式学习到的；BGP 把通过其它 IGP 协议引入的路由的起点设置为 INCOMPLETE
As-path	路由的 AS 路径（AS_PATH）属性，记录了此路由所穿过的所有 AS 区域，可以避免路由环路的出现	

4.1.15 display bgp peer

【命令】

display bgp [**multicast** | **vpnv4** { **all** | **route-distinguisher** *route-distinguisher* | **vpn-instance** *vpn-instance-name* }] **peer** [[*peer-address*] **verbose**]

【视图】

所有视图

【参数】

multicast：多播地址族。

vpnv4：VPNv4 地址族。

vpn-instance *vpn-instance-name*：VPN 实例名称。

route-distinguisher *route-distinguisher*：路由标识的名称。

peer-address：指定要显示的对等体的地址，点分十进制形式。

verbose：显示对等体的详细信息。

【描述】

display bgp peer 命令用来显示对等体信息。

display bgp multicast peer 命令用来显示 MBGP 对等体信息。

display bgp vpnv4 peer 命令用来显示 VPN 对等体信息。

【举例】

查看所有 BGP 对等体的信息。

```
<H3C> display bgp peer
   Peer    AS-num  Ver Queued-Tx  Msg-Rx Msg-Tx Up/Down  State
------------------------------------------------------------------------
1.1.1.10    300     4      0          3     5   00:00:10  Established
2.2.2.11   100      4     0        0        0   Never    Idle
```

表4-5 display bgp peer 命令显示信息描述

项目	描述
Peer	对等体的 IP 地址
AS-num	对等体的 AS 号
Ver	对等体的 BGP 版本
Queued-Tx	发送队列中的报文数
Msg-Rx	从此对等体接收到的消息数目
Msg-Tx	向此对等体发送的消息数目
Up/Down	对等体 Up/Down 的时间
State	对等体当前的状态

查看对等体 1.1.1.10 的详细信息。

```
<H3C> display bgp peer 1.1.1.10 verbose
         Peer: 1.1.1.10+1024     Local: 1.1.1.20+179
         Type: Internal
         State: Established      Flags: <>
         Expiring Time: 00:02:49
         Last State: OpenConfirm Last Event: RecvKeepAlive
```

```
        Last Error: None
        Options: <>
        Peer Version: 4 Peer ID: 1.1.1.10       Local ID: 8.8.8.8
        Active Holdtime: 180s, Keepalive: 60s
        Group Bit: 0    Send state: in sync
        Last traffic (seconds): Received 11     Sent 17 Checked 17
        Input messages: Total 3         Updates 2       Octets 439
        Output messages: Total 5        Updates 3       Octets 264

        Peer capabilities:
          Route refresh: advertised and received
          Ipv4-family Unicast: advertised and received
          Ipv4-family Multicast: advertised and received
          Ipv4-family VPNv4: advertised and received

 Configuration within the peer :
   no export policy route-policy
   no export policy ip-prefix
   no export policy filter-policy
   no export policy as-path-acl
   no import policy route-policy
   no import policy ip-prefix
   no import policy filter-policy
   no import policy as-path-acl
```

表4-6 display bgp peer verbose 命令显示信息描述

项目	描述
Peer: 1.1.1.10+1024	对等体的 IP 地址及建立 TCP 连接使用的端口号
Local: 1.1.1.20+179	本地的 IP 地址及建立 TCP 连接使用的端口号
Type: Internal	对等体的类型，Internal 表示是 IBGP 对等体，External 是 EBGP 对等体
State: Established	对等体目前的状态
Expiring Time: 00:02:49	显示该对等体将在多长时间后超时（此项只对于 Established 状态的对等体有效，其它状态的对等体没有此项显示）
Last State: OpenConfirm	进入此状态之前所处的状态
Last Event: RecvKeepAlive	最近一个导致状态发生变化的事件
Peer capabilities:	对等体能力协商的结果
Route refresh:	路由刷新能力，advertised 表示能够发布；received 表示能够接收
Ipv4-family Unicast:	IPv4 单播地址族能力

项目	描述
Ipv4-family Multicast:	IPv4 多播地址族能力
Ipv4-family VPNv4:	IPv4 VPN 地址族能力

4.1.16 display bgp routing

【命令】

display bgp [**multicast** | **vpnv4** { **all** | **route-distinguisher** *route-distinguisher* | **vpn-instance** *vpn-instance-name* }] **routing** [*ip-address* [*mask*] | **statistic**]

【视图】

所有视图

【参数】

multicast：显示 BGP 路由表中的 MBGP 路由信息。

vpnv4：VPNv4 地址族。

all：显示全部 VPNv4 路由信息。

vpn-instance *vpn-instance-name*：显示与指定名称的 VPN 实例关联的路由信息。

route-distinguisher *route-distinguisher*：显示匹配路由标识（RD）的路由信息。

ip-address：目的网络地址，点分十进制形式。

mask：网络掩码，点分十进制形式。

statistic：使用此参数查看路由的统计信息。

【描述】

display bgp routing 命令用来查看 BGP 路由表中 BGP 路由信息。

display bgp multicast routing 命令用来查看 BGP 路由表中 MBGP 路由信息。

display bgp vpnv4 routing 命令用来查看 BGP 路由表中 VPN 路由信息。

【举例】

查看 BGP 的路由信息。

```
<H3C> display bgp routing
Flags:   # - valid       ^ - active      I - internal
         D - damped      H - history     S - aggregate suppressed

    Dest/Mask          Next-hop        Med        Local-pref Origin As-path
------------------------------------------------------------------------------
#^  129.1.1.0/24       5.5.5.5         0          100         IGP   600
```

```
#^  129.1.2.0/24      5.5.5.5         0          100          IGP   600
#^  129.1.3.0/24      5.5.5.5         0          100          IGP   600
#^  129.1.4.0/24      5.5.5.5         0          100          IGP   600
#^  129.1.5.0/24      5.5.5.5         0          100          IGP   600
#^  129.1.6.0/24      5.5.5.5         0          100          IGP   600
#^  129.1.7.0/24      5.5.5.5         0          100          IGP   600
#^  129.1.8.0/24      5.5.5.5         0          100          IGP   600
#^  129.1.9.0/24      5.5.5.5         0          100          IGP   600
#^  129.1.10.0/24     5.5.5.5         0          100          IGP   600
```

表4-7 display bgp routing 命令显示信息说明

符号	意义	
Flags	状态码： # – valid（合法） ^ – active（选中） D – damped（衰减） H – history（历史） I – internal（内部网关协议） S – aggregate suppressed（抑制）	
Dest/Mask	目的地址/掩码	
Next Hop	下一跳 IP 地址	
Med	MULTI_EXIT_DISC 属性值<0-4294967295>	
Local-Pref	本地优先级<0-4294967295>	
Origin	路由的起源（ORIGIN）属性，表示路由条目是以什么方式被通告到 BGP 路由表中，它有如下 3 种取值：	
	IGP	此路由是 AS 内部的；BGP 把聚合路由和用 **network** 命令定义的路由看成是 AS 内部的，起点类型设置为 IGP
	EGP	此路由是从外部网关协议 EGP（Exterior Gateway Protocol）学习到的
	INC	即 INCOMPLETE：表示此路由信息的来源为未知源，即通过其它方式学习到的；BGP 把通过其它 IGP 协议引入的路由的起点设置为 INCOMPLETE
As-path	路由的 AS 路径（AS_PATH）属性，记录了此路由所穿过的所有 AS 区域，可以避免路由环路的出现	

4.1.17 display bgp routing as-path-acl

【命令】

display bgp [**multicast** | **vpnv4** { **all** | **route-distinguisher** *route-distinguisher* | **vpn-instance** *vpn-instance-name* }] **routing as-path-acl** *aspath-acl-number*

【视图】

所有视图

【参数】

multicast：显示 BGP 路由表中的 MBGP 路由信息。

vpnv4：VPNv4 地址族。

all：显示全部 VPNv4 路由信息。

vpn-instance *vpn-instance-name*：显示与指定名称的 VPN 实例关联的路由信息。

route-distinguisher *route-distinguisher*：显示匹配路由标识（RD）的路由信息。

acl-number：指定匹配的 AS 路径列表号，取值范围为 1～199。

【描述】

display bgp routing as-path-acl 命令用来显示匹配过滤列表的路由。

【举例】

显示匹配过滤列表的路由。

```
<H3C> display bgp routing as-path-acl 1
Flags:   # - valid       ^ - active      I - internal
         D - damped      H - history     S - aggregate suppressed

  Dest/Mask         Next-Hop      Med     Local-pref   Origin    As-path
------------------------------------------------------------------------
#^ 1.1.1.0/24       10.10.10.1    0       100           IGP      200
#^ 1.1.2.0/24       10.10.10.1    0       100           IGP      200
#^ 1.1.3.0/24       10.10.10.1    0       100           IGP      200
#^ 2.2.3.0/24       10.10.10.1    0       100           INC      200
#^ 4.4.4.0/24       10.10.10.1    0       100           INC      200
#^ 9.9.9.0/24       10.10.10.1    0       100           INC      200
#^ 10.10.10.0/24    10.10.10.1    0       100           IGP      200
#^ 22.1.0.0/16      200.1.7.2     100     100           INC      200
```

表4-8 display bgp routing as-path-acl 命令显示信息说明

符号	意义
Dest/Mask	目的地址/掩码
Pref	优先级
Nexthop	下一跳 IP 地址
Med	MULTI_EXIT_DISC 属性值
Local-pref	本地优先级

符号	意义	
Origin	路由的起源（ORIGIN）属性，表示路由条目是以什么方式被通告到 BGP 路由表中，它有如下 3 种取值：	
	IGP	此路由是 AS 内部的；BGP 把聚合路由和用 **network** 命令定义的路由看成是 AS 内部的，起点类型设置为 IGP
	EGP	此路由是从外部网关协议 EGP（Exterior Gateway Protocol）学习到的
	INC	即 INCOMPLETE：表示此路由信息的来源为未知源，即通过其它方式学习到的；BGP 把通过其它 IGP 协议引入的路由的起点设置为 INCOMPLETE
As-path	路由的 AS 路径（AS_PATH）属性，记录了此路由所穿过的所有 AS 区域，可以避免路由环路的出现	

4.1.18 display bgp routing cidr

【命令】

display bgp [**multicast** | **vpnv4** { **all** | **route-distinguisher** *route-distinguisher* | **vpn-instance** *vpn-instance-name* }] **routing cidr**

【视图】

所有视图

【参数】

multicast：显示 BGP 路由表中的 MBGP 路由信息。

vpnv4：VPNv4 地址族。

all：显示全部 VPNv4 路由信息。

vpn-instance *vpn-instance-name*：显示与指定名称的 VPN 实例关联的路由信息。

route-distinguisher *route-distinguisher*：显示匹配路由标识（RD）的路由信息。

【描述】

display bgp routing cidr 命令用来显示非自然网络掩码（即无类别域间路由，classless interdomain routing，CIDR）的路由信息。

【举例】

```
<H3C> display bgp routing cidr
Flags:   # - valid       ^ - active      I - internal
         D - damped      H - history     S - aggregate suppressed

  Dest/Mask         Next-Hop      Med     Local-pref   Origin    As-path
------------------------------------------------------------------------
```

```
#^ 1.1.1.0/24       10.10.10.1    0       100          IGP       200
#^ 1.1.2.0/24       10.10.10.1    0       100          IGP       200
#^ 1.1.3.0/24       10.10.10.1    0       100          IGP       200
#^ 2.2.3.0/24       10.10.10.1    0       100          INC       200
#^ 4.4.4.0/24       10.10.10.1    0       100          INC       200
#^ 9.9.9.0/24       10.10.10.1    0       100          INC       200
#^ 10.10.10.0/24    10.10.10.1    0       100          IGP       200
#^ 22.1.0.0/16      200.1.7.2     100     100          INC       200
```

以上显示信息各域的解释请参见 表 4-7。

4.1.19 display bgp routing community

【命令】

display bgp [**multicast** | **vpnv4** { **all** | **route-distinguisher** *route-distinguisher* | **vpn-instance** *vpn-instance-name* }] **routing community** [*aa:nn*] [**no-export-subconfed**] [**no-advertise**] [**no-export**] [**whole-match**]

【视图】

所有视图

【参数】

multicast：显示 BGP 路由表中的 MBGP 路由信息。

vpnv4：VPNv4 地址族。

all：显示全部 VPNv4 路由信息。

vpn-instance *vpn-instance-name*：显示与指定名称的 VPN 实例关联的路由信息。

route-distinguisher *route-distinguisher*：显示匹配路由标识（RD）的路由信息。

aa:nn：为指定团体号。

no-export-subconfed：为不在本地自治系统外发送匹配路由。

no-advertise：为不向任何对等体发送匹配路由。

no-export：为不向自治系统外部通告路由，但发布给其它子自治系统。

whole-match：为确切匹配。

【描述】

display bgp routing community 命令用来查看路由表中指定 BGP 团体序号相关的路由信息。

【举例】

显示属于指定 BGP 团体序号的路由信息。

```
<H3C> display bgp routing community 11:22
```

```
Flags:   # - valid       ^ - active      I - internal
         D - damped      H - history     S - aggregate suppressed

    Dest/Mask      Next-Hop     Med     Local-pref   Origin    As-path
------------------------------------------------------------------------
#^  1.0.0.0/8      172.10.0.2   0       100           IGP      2
#^  2.0.0.0/8      172.10.0.2   0       100           IGP      2
```

以上显示信息各域的解释请参见 表 4-7。

4.1.20 display bgp routing community-list

【命令】

display bgp [**multicast** | **vpnv4** { **all** | **route-distinguisher** *route-distinguisher* | **vpn-instance** *vpn-instance-name* }] **routing community-list** *community-list-number* [**whole-match**]

【视图】

所有视图

【参数】

multicast：显示 BGP 路由表中的 MBGP 路由信息。

vpnv4：VPNv4 地址族。

all：显示全部 VPNv4 路由信息。

vpn-instance *vpn-instance-name*：显示与指定名称的 VPN 实例关联的路由信息。

route-distinguisher *route-distinguisher*：显示匹配路由标识（RD）的路由信息。

community-list-number：指定团体列表号。

whole-match：只显示精确匹配的路由。

【描述】

display bgp routing community-list 命令用来显示匹配指定的 BGP 团体列表的路由信息。

【举例】

显示匹配 BGP 团体列表 1 的路由信息。

```
[H3C] display bgp routing community-list 1
Flags:   # - valid       ^ - active      I - internal
         D - damped      H - history     S - aggregate suppressed

    Dest/Mask          Next-hop        Med        Local-pref Origin As-path
------------------------------------------------------------------------------
```

```
#^ 1.1.1.0/24          10.10.10.1      0          100          IGP       200
#^ 1.1.2.0/24          10.10.10.1      0          100          IGP       200
#^ 1.1.3.0/24          10.10.10.1      0          100          IGP       200
#^ 2.2.3.0/24          10.10.10.1      0          100          INC       200
#^ 4.4.4.0/24          10.10.10.1      0          100          INC       200
#^ 9.9.9.0/24          10.10.10.1      0          100          INC       200
#^ 10.10.10.0/24 0     10.10.10.2      0          100          IGP       200
#^ 10.10.10.0/24       10.10.10.1      0          100          IGP       200
```

以上显示信息各域的解释请参见 表 4-7。

4.1.21 display bgp routing dampened

【命令】

display bgp routing dampened

【视图】

所有视图

【参数】

无

【描述】

display bgp routing dampened 命令用来显示 BGP 衰减的路由。

【举例】

显示 BGP 衰减的路由。

```
<H3C> display bgp routing dampened
Flags:   # - valid       ^ - active      I - internal
         D - damped      H - history     S - aggregate suppressed
Dest/Mask             Source    Damping-limit   Origin   As-path
------------------------------------------------------------------
#D  11.1.0.0        133.1.1.2      1:20:00       IGP      200
```

表4-9 display bgp routing dampened 命令显示信息说明

符号	意义	
Flags	状态码： # – valid（合法） ^ – active（选中） D – damped（丢弃） H – history（历史） I – internal（内部网关协议） S – aggregate suppressed（抑制）	
#D	有效的和衰减的路由	
Dest/Mask	到该网段的路由被衰减	
Source	路由的下一跳	
Damping-limit	衰减无效的时间，即此路由可重新使用的时间	
Origin	路由的起源（ORIGIN）属性，表示路由条目是以什么方式被通告到 BGP 路由表中，它有如下 3 种取值：	
	IGP	此路由是 AS 内部的；BGP 把聚合路由和用 **network** 命令定义的路由看成是 AS 内部的，起点类型设置为 IGP
	EGP	此路由是从外部网关协议 EGP（Exterior Gateway Protocol）学习到的
	INC	即 INCOMPLETE：表示此路由信息的来源为未知源，即通过其它方式学习到的；BGP 把通过其它 IGP 协议引入的路由的起点设置为 INCOMPLETE
As-path	路由的 AS 路径（AS_PATH）属性，记录了此路由所穿过的所有 AS 区域，可以避免路由环路的出现	

4.1.22 display bgp routing different-origin-as

【命令】

display bgp [**multicast** | **vpnv4** { **all** | **route-distinguisher** *route-distinguisher* | **vpn-instanc}e** *vpn-instance-name* } **routing different-origin-as**

【视图】

所有视图

【参数】

multicast：显示 BGP 路由表中的 MBGP 路由信息。

vpnv4：VPNv4 地址族。

all：显示全部 VPNv4 路由信息。

vpn-instance *vpn-instance-name*：显示与指定名称的 VPN 实例关联的路由信息。

route-distinguisher *route-distinguisher*：显示匹配路由标识（RD）的路由信息。

【描述】

display bgp routing different-origin-as 命令用来显示具有不一致的起源 AS 的路由。

【举例】

显示具有不一致的起源 AS 的路由。

```
<H3C> display bgp routing different-origin-as
Flags:   # - valid       ^ - active      I - internal
         D - damped      H - history     S - aggregate suppressed

Dest/Mask         Next-hop       Med       Local-Pref  Origin   As-Path
------------------------------------------------------------------------------
#^ 10.10.10.0/24     10.10.10.2     0         100          IGP
#^ 10.10.10.0/24     10.10.10.1     0         100          IGP     200
```

以上显示信息的说明请参见 表 4-7。

4.1.23 display bgp routing flap-info

【命令】

display bgp routing flap-info [**regular-expression** *as-regular-expression* | **as-path-acl** *aspath-acl-number* | *network-address* [*mask* [**longer-match**]]]

【视图】

所有视图

【参数】

as-regular-expression：显示匹配 AS 路径正则表达式的路由振荡信息。

acl-number：指定匹配的 AS 路径列表号，取值范围为 1～199。

network-address：显示此 IP 地址的摆动统计信息。

mask：网络掩码。

longer-match：显示比<*network-address*, *mask*>更具体的路由的摆动统计信息。

【描述】

display bgp routing flap-info 命令用来显示 BGP 的摆动统计信息。当<*network-address mask*>为<0.0.0.0 0.0.0.0>时，该命令将显示所有 BGP 路由的摆动统计信息。

【举例】

显示 BGP 的摆动统计信息。

```
<H3C> display bgp routing flap-info
Flags:   # - valid       ^ - active      I - internal
         D - damped      H - history     S - aggregate suppressed
Dest/Mask   Source  Keepup-time  Damping-limit  Flap-times  Origin  As-path
------------------------------------------------------------------------
#D  11.1.0.0/16 133.1.1.2  48      1:20:30      4           IGP     200
```

表4-10 display bgp routing flap-info 命令显示信息说明

符号	意义	
Flags	状态码： # – valid（合法） ^ – active（选中） D – damped（丢弃） H – history（历史） I – internal（内部网关协议） S – aggregate suppressed（抑制）	
#D	有效的和衰减的路由	
Dest/Mask	到该网段的路由被衰减	
Source	路由的下一跳	
Keepup-time	衰减已经持续的时间	
Damping-limit	衰减无效的时间，即此路由可重新使用的时间	
Flap-times	路由振荡的次数	
Origin	路由的起源（ORIGIN）属性，表示路由条目是以什么方式被通告到 BGP 路由表中，它有如下 3 种取值：	
	IGP	此路由是 AS 内部的；BGP 把聚合路由和用 **network** 命令定义的路由看成是 AS 内部的，起点类型设置为 IGP
	EGP	此路由是从外部网关协议 EGP（Exterior Gateway Protocol）学习到的
	INC	即 INCOMPLETE：表示此路由信息的来源为未知源，即通过其它方式学习到的；BGP 把通过其它 IGP 协议引入的路由的起点设置为 INCOMPLETE
As-path	路由的 AS 路径（AS_PATH）属性，记录了此路由所穿过的所有 AS 区域，可以避免路由环路的出现	

4.1.24 display bgp routing peer

【命令】

display bgp [**multicast** | **vpnv4** { **all** | **route-distinguisher** *route-distinguisher* | **vpn-instance** *vpn-instance-name* } **routing peer** *peer-address* { **advertised** | **received** } [*network-address* [*mask*] | **statistic**]

【视图】

所有视图

【参数】

multicast：显示 BGP 路由表中的 MBGP 路由信息。

vpnv4：VPNv4 地址族。

all：显示全部 VPNv4 路由信息。

vpn-instance *vpn-instance-name*：显示与指定名称的 VPN 实例关联的路由信息。

route-distinguisher *route-distinguisher*：显示匹配路由标识（RD）的路由信息。

peer-address：指定要显示的对等体。

advertised：向该对等体通告的路由信息。

received：从该对等体收到的路由信息。

network-address：目的网段的 IP 地址。

mask：网段掩码。

statistic：显示路由的统计信息。

【描述】

display bgp routing peer 命令用来显示向 BGP 对等体通告或者从 BGP 对等体收到的路由信息。

相关配置命令请参考 **display bgp peer**。

【举例】

显示向 BGP 对等体 10.10.10.1 通告的路由信息。

```
<H3C> display bgp routing peer 10.10.10.1 advertised
Flags:   # - valid       ^ - active      I - internal
         D - damped      H - history     S - aggregate suppressed

    Dest/Mask          Next-hop        Med        Local-pref Origin As-path
------------------------------------------------------------------------------
#^I 10.10.10.0/24      1.1.1.1         0          100        INC
```

以上显示信息各域的说明请参见 表 4-7。

4.1.25 display bgp routing peer dampened

【命令】

display bgp [**multicast**] **routing peer** *peer-address* **dampened** [**statistic** | *ip-address*]

【视图】

所有视图

【参数】

multicast：显示 BGP 路由表中的 MBGP 路由信息。

peer-address：BGP 对等体的 IP 地址。

statistic：显示衰减路由的统计数目。

ip-address：显示指定衰减路由的详细信息。

【描述】

display bgp routing peer dampened 命令用来显示从 peer 收到的衰减路由信息。

【举例】

显示从 peer 收到的衰减路由的信息。

```
<H3C> display bgp routing peer 133.1.1.1 dampened

Flags:   # - valid       ^ - active      I - internal
         D - damped      H - history     S - aggregate suppressed

    Dest/Mask           Source         Damping-limit Origin Path
------------------------------------------------------------------------------
#D  10.0.0.0/8         133.1.1.1       28:30          INC   200
```

显示从对等体收到的衰减路由信息的统计结果。

```
<H3C> display bgp routing peer 133.1.1.1 dampened statistic
  Received damping routes total: 1
```

显示从对等体收到的到 10.0.0.0 网段的衰减路由的详细信息。

```
<H3C> display bgp routing peer 133.1.1.1 dampened 10.0.0.0

Flags:   # - valid       ^ - active      I - internal
         D - damped      H - history     S - aggregate suppressed

    Dest/Mask           Source         Damping-limit Origin Path
```

```
------------------------------------------------------------------------
#D  10.0.0.0/8         133.1.1.1       28:00          INC    200
```

表4-11 display bgp routing peer dampened 命令显示信息说明

符号	意义	
Flags	状态码： # – valid（合法） ^ – active（选中） D – damped（丢弃） H – history（历史） I – internal（内部网关协议） S – aggregate suppressed（抑制）	
Dest/Mask	目的地址/掩码	
Source	源 IP 地址	
Damping-limit	指该衰减路由还有多长时间可以从抑制状态中恢复过来	
Origin	路由的起源（ORIGIN）属性，表示路由条目是以什么方式被通告到 BGP 路由表中，它有如下 3 种取值：	
	IGP	此路由是 AS 内部的；BGP 把聚合路由和用 **network** 命令定义的路由看成是 AS 内部的，起点类型设置为 IGP
	EGP	此路由是从外部网关协议 EGP（Exterior Gateway Protocol）学习到的
	INC	即 INCOMPLETE：表示此路由信息的来源为未知源，即通过其它方式学习到的；BGP 把通过其它 IGP 协议引入的路由的起点设置为 INCOMPLETE
As-path	路由的 AS 路径（AS_PATH）属性，记录了此路由所穿过的所有 AS 区域，可以避免路由环路的出现	

4.1.26 display bgp routing peer regular-expression

【命令】

display bgp [**multicast** | **vpnv4** { **all** | **route-distinguisher** *route-distinguisher* | **vpn-instance** *vpn-instance-name* } **routing peer** *peer-address* **regular-expression** *text*

【视图】

所有视图

【参数】

multicast：显示 BGP 路由表中的 MBGP 路由信息。

vpnv4：VPNv4 地址族。

all：显示全部 VPNv4 路由信息。

vpn-instance *vpn-instance-name*：显示与指定名称的 VPN 实例关联的路由信息。

route-distinguisher *route-distinguisher*：显示匹配路由标识（RD）的路由信息。

peer-address：BGP peer 地址。

text：需要匹配的 AS 正则表达式。

【描述】

display bgp routing peer regular-expression 命令用来显示从peer收到的匹配正则表达式的路由信息。

【举例】

显示从 peer 收到的匹配 AS 正则表达式“200”的路由信息。

```
<H3C> display bgp routing peer 133.1.1.1 regular-expression 200
Flags:   # - valid       ^ - active      I - internal
         D - damped      H - history     S - aggregate suppressed

    Dest/Mask          Next-Hop        Med        Local-pref Origin Path
------------------------------------------------------------------------

   Received Routes:
#^I 100.100.100.0/24   1.1.1.1        0          100         IGP   200
#^I 101.101.101.0/24   1.1.1.1        0          100         IGP   200
```

以上显示信息各域的说明请参见 表 4-7。

4.1.27 display bgp routing regular-expression

【命令】

display bgp [**multicast** | **vpnv4** { **all** | **route-distinguisher** *route-distinguisher* | **vpn-instance** *vpn-instance-name* } **routing regular-expression** *as-regular-expression*

【视图】

所有视图

【参数】

multicast：显示 BGP 路由表中的 MBGP 路由信息。

vpnv4：VPNv4 地址族。

all：显示全部 VPNv4 路由信息。

vpn-instance *vpn-instance-name*：显示与指定名称的 VPN 实例关联的路由信息。

route-distinguisher *route-distinguisher*：显示匹配路由标识（RD）的路由信息。

as-regular-expression：为匹配的 AS 正则表达式。

【描述】

display bgp routing regular-expression 命令用来显示指定的 AS 正则表达式相匹配的路由信息。

【举例】

显示与 AS 正则表达式^200$相匹配的路由信息。

```
<H3C> display bgp routing regular-expression ^200$
Flags:   # - valid       ^ - active      I - internal
         D - damped      H - history     S - aggregate suppressed

    Dest/Mask          Next-Hop        Med        Local-pref Origin Path
--------------------------------------------------------------------------------
#^I 100.100.100.0/24   1.1.1.1        0          100         IGP   200
#^I 101.101.101.0/24   1.1.1.1        0          100         IGP   200
```

以上显示信息各域的说明请参见 表 4-7。

4.1.28 display bgp routing statistic

【命令】

display bgp [**multicast** | **vpnv4** { **all** | **route-distinguisher** *route-distinguisher* | **vpn-instance** *vpn-instance-name* }] **routing statistic**

【视图】

所有视图

【参数】

multicast：显示 BGP 路由表中的 MBGP 路由信息。

vpnv4：VPNv4 地址族。

all：显示全部 VPNv4 路由信息。

vpn-instance *vpn-instance-name*：显示与指定名称的 VPN 实例关联的路由信息。

route-distinguisher *route-distinguisher*：显示匹配路由标识（RD）的路由信息。

【描述】

display bgp routing statistic 命令用来显示 BGP 的路由统计信息。

【举例】

显示 BGP 路由统计信息。

```
<H3C> display bgp routing statistic
Routes total: 4
```

4.1.29 display ip community-list

【命令】

display ip community-list [*stand-comm-list-number* | *ext-comm-list-number*]

【视图】

所有视图

【参数】

stand-comm-list-number：标准团体表号，范围 1～99。

ext-comm-list-number：扩展团体表号，范围 100～199。

【描述】

display ip community-list 命令用来显示配置的团体列表。

【举例】

显示所有团体列表。

```
<H3C> display ip community-list
```

4.1.30 display ip as-path-acl

【命令】

display ip as-path-acl [*number*]

【视图】

所有视图

【参数】

*numbe*r：AS 路径列表的序号，显示指定的 AS 路径列表，范围为 1～99。

【描述】

display ip as-path-acl 命令用来显示配置的 AS 路径列表。

【举例】

显示编号为 100 的 AS 路径列表。

```
<H3C> display ip as-path-acl 100
        No.      Mode    Expression
        100     permit  _65001$
```

```
permit  ^254$
```

4.1.31 filter-policy export

【命令】

filter-policy { *acl-number* | **ip-prefix** *ip-prefix-name* } **export** [*protocol*]

undo filter-policy { *acl-number* | **ip-prefix** *ip-prefix-name* } **export** [*protocol*]

【视图】

BGP 视图

【参数】

acl-number：指定用于匹配路由信息目的地址域的访问列表号。

ip-prefix-name：指定用于匹配路由信息目的地址域的地址前缀列表，取值长度为 1～19。

protocol：指定何种路由协议的路由信息将被过滤。目前可包括：**direct**、**ospf**、**ospf-ase**、**ospf-nssa**、**rip** 和 **static**。

【描述】

filter-policy export 命令用来配置对发布的路由进行过滤，只有通过过滤器的路由才被 BGP 发布，**undo filter-policy export** 命令用来取消对发布的路由进行过滤。

缺省情况下，不对发布的路由信息进行过滤。

这个命令对 BGP 发布路由有影响，如果指定 *protocol* 参数，将只对引入的这种协议产生的路由进行过滤，对引入的其它协议产生的路由不受影响。如果没有指定 *protocol* 参数，对引入的任何一个协议产生的路由都要进行过滤。

【举例】

使用 acl 2003 对 BGP 发布路由进行过滤。

```
[H3C-bgp] filter-policy 2003 export
```

4.1.32 filter-policy import

【命令】

filter-policy gateway *ip-prefix-name* **import**

undo filter-policy gateway *ip-prefix-name* **import**

filter-policy { *acl-number* | **ip-prefix** *ip-prefix-name* } **import**

undo filter-policy { *acl-number* | **ip-prefix** *ip-prefix-name* } **import**

【视图】

BGP 视图

【参数】

acl-number：指定用于匹配路由信息的目的地址域的访问列表号。

ip-prefix *ip-prefix-name*：地址前缀列表名，其匹配对象为路由信息的目的地址域，取值长度为 1～19。

gateway *ip-prefix-name*：邻居路由器地址的地址前缀列表名，其匹配对象为指定的邻居路由器发布的路由信息，取值长度为 1～19。

【描述】

filter-policy gateway import 命令用来配置对接收的指定邻居路由器地址发布的路由信息进行过滤，**undo filter-policy gateway import** 命令用来取消对指定邻居路由器地址发布路由信息进行过滤。

filter-policy import 命令用来配置对接收的全局路由信息进行过滤，**undo filter-policy import** 命令用来取消对接收的全局路由信息进行过滤。

缺省情况下，不对接收的路由信息进行过滤。

该命令可以对 BGP 接收路由进行过滤，决定是否将路由添加到 BGP 路由表中。

【举例】

使用 acl 2003 对 BGP 接收的路由信息进行过滤。

```
[H3C-bgp] filter-policy 2003 import
```

4.1.33 group

【命令】

group *group-name* [**internal** | **external**]

undo group *group-name*

【视图】

BGP 视图

【参数】

group-name：对等体组的名称。可使用字母和数字，长度范围为 1～47。

internal：创建的对等体组为内部对等体组。

external：创建的对等体组为外部对等体组，包括联盟内其它子 AS 的组。

【描述】

group 命令用来创建一个对等体组，**undo group** 命令用来删除创建的对等体组。

BGP 对等体组的使用是为了方便用户配置。当用户启动若干配置相同的对等体时，可先创建一个对等体组，并将其配置好。然后将各对等体加入到此对等体组中，以使其获得与此对等体组相同的配置。

如果不指定对等体组的类型，缺省为 internal。

【举例】

创建一个对等体组 test。

```
[H3C-bgp] group test
```

4.1.34 import-route

【命令】

import-route *protocol* [**med** *med-value*] [**route-policy** *route-policy-name*]

undo import-route *protocol*

【视图】

BGP 视图

【参数】

protocol：指定可引入的源路由协议，目前包括 **direct**、**static**、**rip**、**ospf**、**ospf-ase**、**ospf-nssa** 等。

med *med-value*：指定引入路由的 MED 值，取值范围为 0～4294967295。缺省值为 0。

route-policy *route-policy-name*：指定用于过滤引入协议路由的 Route-policy。可使用字母和数字，长度范围为 1～19。

【描述】

import-route 命令用来引入其它路由协议的路由信息，**undo import-route** 命令用来取消引入其它路由协议的路由信息。

缺省情况下，BGP 将不引入其它路由协议的路由。

【举例】

引入 RIP 的路由。

```
[H3C-bgp] import-route rip med 400
```

4.1.35 ip as-path-acl

【命令】

ip as-path-acl *aspath-acl-number* { **permit** | **deny** } *as-regular-expression*

undo ip as-path-acl *aspath-acl-number*

【视图】

系统视图

【参数】

aspath-acl-number：AS 路径列表的标号，范围为 1～199；

as-regular-expression：AS 路径的正则表达式。

BGP 协议的路由信息更新中，包含一个自治系统路径域，在 BGP 协议交换路由信息的过程中，该路由所经过的所有自治系统都会记录在这个域中。试图识别 AS 路径列表就是要把其与一个称为正则表达式进行比较。一个正则表达式就是用一个公式代表的字符组合。例如^200.*100$，表示匹配所有 AS200 开始、以 AS100 结束的自治系统路径域。

自治系统正则表达式所用到的特殊字符及其含义参见下表：

表4-12 正则表达式的特殊字符表

符号	特殊意义
.	匹配任何单字符，包括空白
*	匹配模式中 0 或更多的序列
+	匹配模式中 1 或更多的序列
^	匹配输入字符串的开始
$	匹配输入字符串的结束
_	匹配逗号、左大括号、右大括号、左括号、右括号、输入字符串的开始、输入字符串的结束、或一个空格
[范围]	表示一个单字符模式的范围
-	把一个范围的结束点分开

用户可在定义 **aspath-acl** 的同时指定一个用于匹配 AS 路径信息的正则表达式。通过匹配 **aspath-acl**，过滤掉不符合条件的路由信息。对于同一列表号，用户可定义多条 **aspath-acl** 命令，也即一个访问列表号可代表一组自治系统访问列表。每个 AS 路径列表是用数字来标识的。

【描述】

ip as-path-acl 命令用来配置一个 AS 的正则表达式，**undo ip as-path-acl** 命令用来取消定义的正则表达式。

配置的 AS 路径列表可用于 BGP 策略。

相关配置可参考命令 **peer as-path-acl** 和 **display bgp routing as-path-acl**。

【举例】

配置一个 AS 路径列表。

```
[H3C] ip as-path-acl 10 permit ^200.*100$
```

4.1.36 ip community-list

【命令】

ip community-list *stand-comm-list-number* { **permit** | **deny** } [*aa:nn*] [**internet**] [**no-export-subconfed**] [**no-advertise**] [**no-export**]

ip community-list *ext-comm-list-number* { **permit** | **deny** } *as-regular-expression*

undo ip community-list { *stand-comm-list-number* | *ext-comm-list-number* }

【视图】

系统视图

【参数】

stand-comm-list-number：标准团体表号，范围 1～99。

ext-comm-list-number：扩展团体表号，范围 100～199。

permit：允许对匹配条件访问。

deny：禁止对匹配条件访问。

aa:nn：为团体号。*aa* 为 AS 号，*nn* 为 community 的序号。

internet：通告所有路由。

no-export-subconfed：不向本地自治系统外发送匹配路由。

no-advertise：为不向任何同伴发送匹配路由。

no-export：不向自治系统外部通告路由，但发布给其它子自治系统。

as-regular-expression：正则表达式格式的团体属性。

【描述】

ip community-list 命令用来配置一个 BGP 团体列表，**undo ip community-list** 命令用来取消配置的团体列表。

配置的团体列表可用于 BGP 策略。

相关配置可参考命令 **apply community** 和 **display bgp routing community-list**。

【举例】

定义一个团体属性列表，不向本地自治系统外通告具有该团体属性的路由。

```
[H3C] ip community-list 6 permit no-export-subconfed
```

4.1.37 log-peer-change

【命令】

log-peer-change

undo log-peer-change

【视图】

BGP 视图

【参数】

无

【描述】

log-peer-change 命令用来打开 BGP 邻接状态变化的输出开关，**undo log-peer-change** 命令用来关闭输出开关。

缺省情况下，输出开关关闭。

当打开邻接状态输出开关后，BGP 邻接状态的变化会输出到配置终端上，直至邻接状态输出开关被关闭。

【举例】

在当前路由器上打开 BGP 邻接状态变化的输出开关。

```
[H3C-bgp] log-peer-change
%Aug 24 15:50:40:361 2009 H3C PHY/2/PHY:   GigabitEthernet0/0: change status
to down
%Aug 24 15:50:40:361 2009 H3C IFNET/5/UPDOWN:Line protocol on the interface
GigabitEthernet0/0 is DOWN

%Aug 24 15:50:40:361 2009 H3C RM/5/RTLOG:
BGP-ADJCHANGE: Adjacency To 192.168.1.2 (External AS 2) DOWN
```

上面加粗内容即表示邻接状态的变化。

4.1.38 network

【命令】

network *ip-address* [*address-mask*] [**route-policy** *route-policy-name*]

undo network *ip-address* [*address-mask*] [**route-policy** *route-policy-name*]

【视图】

BGP 视图

【参数】

ip-address：BGP 通告的网络地址。

address-mask：网络地址的掩码。

route-policy-name：对通告的路由使用的 Route-policy。

【描述】

network 命令用来配置本地 BGP 通告的网络路由，**undo network** 命令用来取消已有的配置。

缺省情况下，本地 BGP 不通告任何路由。

【举例】

通告到达 10.0.0.0/16 网段的路由。

```
[H3C-bgp] network 10.0.0.0 255.255.0.0
```

4.1.39 peer advertise-community

【命令】

peer *group-name* **advertise-community**

undo peer *group-name* **advertise-community**

【视图】

BGP 视图

【参数】

group-name：对等体组的名称。

【描述】

peer advertise-community 命令用来配置将团体属性传给对等体组，**undo peer advertise-community** 命令用来取消已有的配置。

缺省情况下，不将团体属性传给任何对等体组。

相关配置可参考命令 **if-match community-list** 和 **apply community**。

【举例】

将团体属性传给对等体组 test。

```
[H3C-bgp] peer test advertise-community
```

4.1.40 peer allow-as-loop

【命令】

peer { *group-name* | *peer-address* } **allow-as-loop** [*number*]

undo peer { *group-name* | *peer-address* } **allow-as-loop**

【视图】

BGP 视图

【参数】

group-name：对等体组的名称。

peer-address：对等体的 IP 地址。

number：表示本地 AS 号的重复次数。取值范围为 1～10。缺省情况下，取值为 3。

【描述】

peer allow-as-loop 命令用来配置本地 AS 号的重复次数，**undo peer allow-as-loop** 命令用来取消本地 AS 号的重复次数。

相关配置可参考命令 **display current-configuration** 和 **display bgp routing peer**。

【举例】

配置本地 AS 号的重复次数为 2。

```
[H3C-bgp] peer 1.1.1.1 allow-as-loop 2
```

4.1.41 peer as-number

【命令】

peer *group-name* **as-number** *as-number*

undo peer *group-name* **as-number**

【视图】

BGP 视图

【参数】

group-name：对等体组的名称。

as-number：对等体组的对端 AS 号，取值范围为 1～65535。

【描述】

peer as-number 命令用来配置指定对等体组的对端 AS 号，**undo peer as-number** 命令用来删除对等体组的 AS 号。

缺省情况下，对等体组对端无 AS 号。

【举例】

配置指定对等体组 test 的对端 AS 号为 100。

```
[H3C-bgp] peer test as-number 100
```

4.1.42 peer as-path-acl

【命令】

peer { *group-name* | *peer-address* } **as-path-acl** *number* **import**

undo peer { *group-name* | *peer-address* } **as-path-acl** *number* **import**

peer *group-name* **as-path-acl** *number* **export**

undo peer *group-name* **as-path-acl** *number* **export**

【视图】

BGP 视图

【参数】

group-name：对等体组的名称。

peer-address：对等体的 IP 地址。

aspath-acl-number：AS 正则表达式过滤列表号，取值范围为 1～199。

import：接收分发列表。

export：出口分发列表。

【描述】

命令 **peer as-path-acl import** 用来配置 BGP 基于 AS 路径列表过滤从对等体/对等体组收到的路由，命令 **undo peer as-path-acl import** 用于取消对接收路由的过滤。命令 **peer as-path-acl export** 用来配置 BGP 基于 AS 路径列表过滤向对等体组发布的路由，命令 **undo peer as-path-acl export** 用于取消对发布路由的过滤。

缺省情况下，不对接收及发布的路由进行过滤。

【举例】

设置对等体组 test 的 AS 路径访问列表。

```
[H3C] ip as-path-acl 10 permit 200 300
[H3C] bgp 100
[H3C-bgp] peer test as-number 100
[H3C-bgp] peer test as-path-acl 10 export
```

4.1.43 peer connect-interface

【命令】

peer { *group-name* | *peer-address* } **connect-interface** *interface-type interface-number*

undo peer { *group-name* | *peer-address* } **connect-interface**

【视图】

BGP 视图

【参数】

group-name：指定的对等体组。

peer-address：对等体的 IP 地址。

interface-type interface-number：接口类型及接口号。

【描述】

peer connect-interface 命令用来指定路由更新报文的源接口，**undo peer connect-interface** 命令用来恢复使用最佳的路由更新报文的源接口。

缺省情况下，BGP 使用最佳路由更新报文的源接口。

一般情况下，BGP 是使用最佳的路由更新报文的源接口；但为使接口在出现问题时，仍能发送路由更新报文，可将接口配置成 Loopback 接口等。

【举例】

指定路由更新报文的源接口为 loopback0 接口。

```
[H3C-bgp] peer test connect-interface loopback 0
```

4.1.44 peer default-route-advertise

【命令】

peer *group-name* **default-route-advertise**

undo peer *group-name* **default-route-advertise**

【视图】

BGP 视图

【参数】

group-name：对等体组的名称。

【描述】

peer default-route-advertise 命令用来设置向对等体组通告缺省路由，**undo peer default-route-advertise** 命令用来取消已有的设置。

缺省情况下，不向对等体组通告引入缺省路由。

该命令不需要在路由表中存在缺省路由，而是无条件地向对等体组发送一个下一跳为自身的缺省路由。

【举例】

向对等体组 test 通告缺省路由。

```
[H3C-bgp] peer test as-number 100
[H3C-bgp] peer test default-route-advertise
```

4.1.45 peer description

【命令】

peer { *group-name* | *peer-address* } **description** *description-line*

undo peer { *group-name* | *peer-address* } **description**

【视图】

BGP 视图

【参数】

group-name：对等体组的名称。

peer-address：对等体的 IP 地址。

description-line：配置的描述信息，可使用字母和数字，长度最多可达 79。

【描述】

peer description 命令用来配置对等体/对等体组的描述信息，**undo peer description** 命令用来删除对等体/对等体组的描述信息。

缺省情况下，不对对等体/对等体组配置描述信息。

相关配置可参考命令 **display current-configuration** 和 **display bgp peer**。

【举例】

配置名称为 group1 的对等体组描述信息为 beijing1。

```
[H3C-bgp] peer group1 description beijing1
```

4.1.46 peer ebgp-max-hop

【命令】

peer *group-name* **ebgp-max-hop** [*ttl*]
undo peer *group-name* **ebgp-max-hop**

【视图】

BGP 视图

【参数】

group-name：对等体组的名称。
ttl：最大步跳计数，范围为 1～255，缺省值为 64。

【描述】

peer ebgp-max-hop 命令用来配置允许同非直连相连网络上的邻居建立 EBGP 连接，**undo peer ebgp-max-hop** 命令用来取消已有的配置。

缺省情况下，该功能取消。

【举例】

允许同不直接相连网络上的 EBGP 对等体组 test 建立连接。

```
[H3C-bgp] peer test ebgp-max-hop
```

4.1.47 peer enable

【命令】

peer { *group-name* | *peer-address* } **enable**
undo peer { *group-name* | *peer-address* } **enable**

【视图】

BGP 视图

【参数】

group-name：对等体组名称，指定整个对等体组。

peer-address：对等体 IP 地址，指定某个特定的对等体。

【描述】

peer enable 命令用来激活指定对等体（组），**undo peer enable** 命令用来去掉已激活的指定对等体（组）。

peer *peer-address* **enable** 只能在单播地址族配置，如果要取消对等体的单播能力，使用此命令。

如果要取消对等体的组播或 VPNV4 能力，在相应的地址下将此对等体从组中删除即可。

缺省情况下，BGP 对等体（组）在单播地址族是激活的，在 VPN 和 MBGP 地址族是没有激活的。

如果去掉已激活的指定对等体（组），则本防火墙与指定对等体（组）之间不再交换路由信息。

【举例】

去掉已激活指定的对等体。

```
[H3C] bgp 180
[H3C-bgp] peer 18.10.0.9 as-number 180
[H3C-bgp] undo peer 18.10.0.9 enable
```

配置并激活 VPNv4 单播地址族的指定对等体。

```
[H3C] bgp 100
[H3C-bgp] peer 10.15.0.15 as-number 100
[H3C-bgp] ipv4-family vpnv4 unicast
[H3C-bgp-af-vpn] peer 10.15.0.15 enable
```

配置并激活 IPv4 组播地址族的指定对等体。

```
[H3C] bgp 200
[H3C-bgp] peer 20.10.0.1 as-number 200
[H3C-bgp] ipv4-family multicast
[H3C-bgp-af-mul] peer 20.10.0.1 enable
```

4.1.48 peer filter-policy

【命令】

peer { *group-name* | *peer-address* } **filter-policy** *acl-number* **import**

undo peer { *group-name* | *peer-address* } **filter-policy** *acl-number* **import**

peer *group-name* **filter-policy** *acl-number* **export**

undo peer *group-name* **filter-policy** *acl-number* **export**

【视图】

BGP 视图

【参数】

group-name：对等体组的名称。

peer-address：对等体的 IP 地址。

acl-number：IP 访问列表号。

import：应用于接收的路由。

export：应用于发布的路由。

【描述】

命令 **peer filter-policy import** 用来配置 BGP 基于访问控制列表过滤从对等体/对等体组收到的路由，命令 **undo peer filter-policy import** 用来取消对接收路由的过滤。命令 **peer filter-policy export** 用来配置 BGP 基于访问控制列表过滤向对等体组发布的路由，命令 **undo peer filter-policy export** 用来取消对发布路由的过滤。

缺省情况下，不对接收及发布的路由进行过滤。

相关配置可参考命令 **ip as-path-acl** 和 **peer as-path-acl**。

【举例】

设置对等体组 test 的过滤策略。

```
[H3C] acl number 2003
[H3C-acl-basic-2003] rule 0 deny source 98.12.0.0 0.0.0.255
[H3C-acl-basic-2003] quit
[H3C] bgp 100
[H3C-bgp] peer test as-number 100
[H3C-bgp] peer test filter-policy 2003 import
```

4.1.49 peer group

【命令】

对于组播/VPNv4 地址族：

peer *peer-address* **group** *group-name*

undo peer *peer-address*

单播/VPN-INSTANCE 地址族：

peer *peer-address* **group** *group-name* [**as-number** *as-number*]

undo peer *peer-address*

【视图】

BGP 视图

【参数】

group-name：对等体组的名称。可使用字母和数字，长度范围为 1～47。

peer-address：对等体的 IP 地址。

as-number：为对等体指定 AS 号。

【描述】

peer group 命令用来将对等体加入对等体组，**undo peer** 命令删除对等体组中指定的对等体。

在单播/VPN-INSTANCE 地址族，当将对等体加入没有指定 AS 号的外部对等体组时，需要同时指定对等体的 AS 号，将对等体加入内部对等体组或指定了 AS 号的外部对等体组时可以不指定对等体的 AS 号。

在组播或 VPNV4 地址族下，要将一个对等体加入一个对等体组，要求在单播地址族下已经存在此对等体，即在单播地址族下此对等体已经加入了某一个组中（此对等体在单播地址族下可以是未使能的）。

在不同的地址族下，同一对等体可以加入不同的对等体组，同一个组在不同的地址族下也可以有不同的成员。

【举例】

将 IP 地址为 10.1.1.1 的对等体加入到对等体组 TEST。

```
[H3C-bgp] group TEST
[H3C-bgp] peer 10.1.1.1 group TEST
```

4.1.50 peer ip-prefix

【命令】

peer { *group-name* | *peer-address* } **ip-prefix** *prefixname* **import**

undo peer { *group-name* | *peer-address* } **ip-prefix** *prefixname* **import**

peer *group-name* **ip-prefix** *prefixname* **export**

undo peer *group-name* **ip-prefix** *prefixname* **export**

【视图】

BGP 视图

【参数】

group-name：对等体组的名称。

prefixname：指定的前缀列表名称。

import：对由指定对等体/对等体组接收的路由应用过滤策略。

export：对向指定对等体组发送的路由应用过滤策略。

【描述】

命令 **peer ip-prefix import** 用来配置 BGP 基于地址前缀列表过滤从对等体/对等体组收到的路由，命令 **undo peer ip-prefix import** 用于取消对接收路由的过滤。命令 **peer ip-prefix export** 用来配置 BGP 基于地址前缀列表过滤向对等体组发布的路由，命令 **undo peer ip-prefix export** 用于取消对发布路由的过滤。

缺省情况下，不对接收及发布的路由进行过滤。

相关配置可参考命令 **ip ip-prefix**。

【举例】

配置基于地址前缀列表的路由过滤策略。

```
[H3C-bgp] peer group1 ip-prefix list1 import
```

4.1.51 peer next-hop-local

【命令】

peer *group-name* **next-hop-local**

undo peer *group-name* **next-hop-local**

【视图】

BGP 视图

【参数】

group-name：对等体组的名称。

【描述】

peer next-hop-local 命令用来把向对等体组发布的路由的下一跳设置为自身的地址，**undo peer next-hop-local** 命令用来取消已有的设置。

【举例】

BGP 向对等体组 test 发布路由时，将自身地址作为下一跳。

```
[H3C-bgp] peer test next-hop-local
```

4.1.52 peer password

【命令】

peer { *group-name* | *peer-address* } **password** { **cipher** | **simple** } *password*

undo peer { *group-name* | *peer-address* } **password**

【视图】

BGP 视图

【参数】

group-name：对等体组的名称。

peer-address：对等体的 IP 地址，点分十进制形式。

cipher：以密文形式显示设置的密码。

simple：以明文形式显示设置的密码。

password：密码，字符串形式，当选择 **cipher** 参数但以明文形式输入密码、或选择 **simple** 参数时，长度为 1～16；当选择 **cipher** 参数并以密文形式输入密码时，长度必须为 24。

【描述】

peer password 命令用来配置 BGP 建立 TCP 连接时进行 MD5 认证，**undo peer password** 命令用来取消此功能。

缺省情况下，BGP 在建立 TCP 连接时，不进行 MD5 认证。

如果启用 MD5 认证，参与认证的双方必须配置完全一致的认证方式和密码，否则将因为无法通过认证而不能建立 TCP 连接。

只有当对等体所在的对等体组没有配置 MD5 认证时，才能对指定对等体进行专门的 MD5 认证配置，否则，将以对等体组的配置为准。

【举例】

配置对本地防火墙 10.1.100.1 与对等体 10.1.100.2 之间的 TCP 连接使用 MD5 认证。

```
[H3C-bgp] peer 10.1.100.2 password cipher bgppwd
```

在对端也需要进行类似的配置。

```
[H3C-bgp] peer 10.1.100.1 password cipher bgppwd
```

4.1.53 peer public-as-only

【命令】

peer *group-name* **public-as-only**

undo peer *group-name* **public-as-only**

【视图】

BGP 视图

【参数】

group-name：为对等体组的名称。

【描述】

peer public-as-only 命令用来配置发送 BGP 更新报文时不携带私有自治系统号，**undo peer public-as-only** 命令用来配置发送 BGP 更新报文时携带私有自治系统号。

缺省情况下，发送 BGP 更新报文时，携带私有自治系统号。

为使某些出口路由器在发送更新报文时忽略掉私有 AS 号，可配置发送 BGP 更新报文时不携带私有自治系统号。

【举例】

配置向同伴 test 发送 BGP 更新报文时不携带私有自治系统号。

```
[H3C-bgp] peer test public-as-only
```

4.1.54 peer reflect-client

【命令】

peer *group-name* **reflect-client**

undo peer *group-name* **reflect-client**

【视图】

BGP 视图

【参数】

group-name：对等体组的名称。

【描述】

peer reflect-client 命令用来配置将对等体组作为路由反射器的客户，**undo peer reflect-client** 命令用来取消已有的配置。

缺省情况下，自治系统中无路由反射器。

相关配置可参考命令 **reflect between-clients** 和 **reflect cluster-id**。

【举例】

将对等体组 test 作为路由反射器的客户。

```
[H3C-bgp] peer test reflect-client
```

4.1.55 peer route-policy

【命令】

peer { *group-name* | *peer-address* } **route-policy** *policy-name* **import**

undo peer { *group-name* | *peer-address* } **route-policy** *policy-name* **import**

peer *group-name* **route-policy** *policy-name* **export**

undo peer *group-name* **route-policy** *policy-name* **export**

【视图】

BGP 视图

【参数】

group-name：对等体组的名称。

peer-address：对等体的 IP 地址。

route-policy-name：指定的 Route-policy。

import：对从对等体（组）来的路由应用 Route-policy。

export：对向对等体组发布的路由应用 Route-policy。

【描述】

命令 **peer route-policy import** 用来配置 BGP 对从对等体/对等体组接收到的路由应用路由策略，命令 **undo peer route-policy import** 用于取消该路由策略。命令 **peer route-policy export** 用来配置 BGP 对向对等体组发送的路由应用路由策略，命令 **undo peer route-policy export** 用于取消该路由策略。

缺省情况下，不对接收及发送的路由应用路由策略。

【举例】

对来自对等体组 test 的路由应用名为 test-policy 的 Route-policy。

```
[H3C-bgp] peer test route-policy test-policy import
```

4.1.56 peer route-update-interval

【命令】

peer *group-name* **route-update-interval** *seconds*

undo peer *group-name* **route-update-interval**

【视图】

BGP 视图

【参数】

group-name：对等体组的名称。

seconds：发送 Update 消息的最小时间间隔，范围为 0～600 秒。缺省情况下，内部对等体组为 5 秒，外部对等体组为 30 秒。

【描述】

peer route-update-interval 命令用来配置向对等体组发送路由的时间间隔，**undo peer route-update-interval** 命令用来恢复向对等体组发送的路由时间间隔的缺省值。

【举例】

设置 BGP 对等体组 test 发送路由更新报文的间隔时间为 10 秒。

```
[H3C-bgp] peer test as-number 100
[H3C-bgp] peer test route-update-interval 10
```

4.1.57 peer shutdown

【命令】

peer { *group-name* | *peer-address* } **shutdown**

undo peer {*group-name* | *peer-address* } **shutdown**

【视图】

BGP 视图

【参数】

group-name：对等体组的名称。

peer-address：对等体的 IP 地址。

【描述】

peer shutdown 命令用来配置禁止 BGP 对等体/对等体组发起或接收 BGP 连接；若 BGP 连接已经存在，则断开连接。**undo peer shutdown** 命令用来恢复缺省设置。

缺省情况下，允许对等体/对等体组发起或接收 BGP 连接。

【举例】

配置禁止 BGP 对等体 1.1.1.1 发起或接收 BGP 连接。

```
[H3C-bgp] peer 1.1.1.1 shutdown
```

4.1.58 peer timer

【命令】

peer { *group-name* | *peer-address* } **timer keep-alive** *keepalive-interval* **hold** *holdtime*

undo peer { *group-name* | *peer-address* } **timer**

【视图】

BGP 视图

【参数】

group-name：对等体组的名称。

peer-address：对等体的 IP 地址。

keepalive-interval：指定的 Keepalive 时间间隔。取值范围为 0～65535 秒。缺省值为 60 秒。

holdtime：指定的 Holdtime 保持时间。取值范围为 0，3～65535 秒。缺省值为 180 秒。

【描述】

peer timer 命令用来配置指定对等体/对等体组的 Keepalive 时间间隔与保持时间，**undo peer timer** 命令用来恢复缺省值。

使用该命令配置的定时器比使用 **timer** 命令配置的定时器优先级高。

当 **peer timer** 命令中配置的值与全局 **timer** 命令的配置相同时，**peer timer** 命令的配置结果将不显示在当前配置中。

【举例】

配置向指定对等体组 test 发送 Keepalive 的时间间隔与保持时间。

```
[H3C-bgp] peer test timer keep-alive 50 hold 150
```

4.1.59 preference

【命令】

preference *value1 value2 value3*

undo preference

【视图】

BGP 协议视图

【参数】

value：优先级，*value1* 为从 EBGP 邻居收到的路由的优先级，*value2* 为从 IBGP 邻居收到的路由的优先级，*value3* 为本地产生的路由的优先级，取值范围均为 1～256。缺省情况下，*value1*、*value2*、*value3* 的值分别为 256、256、130。

【描述】

preference 命令用来配置 BGP 协议的优先级，**undo preference** 命令用来恢复 BGP 协议的缺省优先级。

每一种路由协议都有自己的优先级（preference），协议的优先级将最后决定路由策略采用哪种路由协议获取的路由作为最佳路由。优先级的数值越大，其实际的优先级越低。BGP 有三种路由：从外部对等体学到的路由，从内部对等体学到的路由及本地产生地路由。这三种路由的优先级可以是不同的，可以分别针对这三种路由手工设定 BGP 的优先级。

【举例】

配置 BGP 协议的优先级分别为 150、120、100。

```
[H3C-bgp] preference 150 120 100
```

4.1.60 reflect between-clients

【命令】

reflect between-clients

undo reflect between-clients

【视图】

BGP 视图

【参数】

无

【描述】

reflect between-clients 命令用来允许客户到客户的路由反射，**undo reflect between-clients** 命令用来禁止客户到客户的路由反射。

缺省情况下，允许客户到客户的路由反射。

配置路由反射器后，路由反射器把一个客户的路由反射给其它客户。

相关配置可参考命令 **reflector cluster-id** 和 **peer reflect-client**。

【举例】

关闭路由反射功能。

```
[H3C-bgp] undo reflect between-clients
```

4.1.61 reflector cluster-id

【命令】

reflector cluster-id { *cluster-id* | *address* }

undo reflector cluster-id

【视图】

BGP 视图

【参数】

cluster-id：为路由反射器群 ID 的整数格式，范围为 1～4294967295。

address：路由反射器群 ID 的 IP 地址表达形式。

【描述】

reflector cluster-id 命令用来配置路由反射器的群 ID，**undo reflector cluster-id** 命令用来删除路由反射器的群 ID。

缺省情况下，每个路由反射器是使用自己的路由 ID 作为集群 ID。

通常，一个群里只有一个路由反射器。此时是由反射器的路由器 ID 来识别该群的。设置多个路由反射器可提高网络的稳定性。如果一个群中配有多个路由反射器，请使用该命令为所有的路由反射器配置同样的群 ID。

相关配置可参考命令 **reflect between-clients** 和 **peer reflect-client**。

【举例】

本地防火墙是群中的路由反射器之一，它用群 ID 来标识该群。

```
[H3C-bgp] reflector cluster-id 80
[H3C-bgp] peer group1 reflect-client
```

4.1.62 refresh bgp

【命令】

refresh bgp { **all** | *peer-address* | **group** *group-name* } [**multicast** | **vpnv4** | **vpn-instance** *vpn-instance-name*] { **import** | **export** }

【视图】

用户视图

【参数】

all：刷新所有对等体。

peer-address：刷新指定地址的对等体。

group-name：刷新制定对等体组中的所有成员。

vpnv4：向对等体刷新 VPNV4 地址族的路由。

multicast：向对等体刷新组播地址族的路由。

vpn-instance *vpn-instance-name*：向指定 VPN-INSTANCE 中的对等体刷新 VPN 路由。

import：向对方发送 ROUTE-REFRESH 报文，请求对方重新将所有路由发送一遍。

export：向对方重新将所有路由发送一遍。

【描述】

refresh bgp 命令用来请求对方重新发送路由，或向对方重新发送路由。

BGP 连接建立以后，只发送增量路由，但在有些情况下，例如路由策略改变时，需要对方重新发送路由，或向对方重新发送路由，以按照新的策略重新过滤路由。

【举例】

请求所有对等体重新发送路由。

```
<H3C> refresh bgp all import
```

向 VPN-INSTANCE vpn1 中的 CE 对等体 10.1.1.1 重新发送所有路由。

```
<H3C> refresh bgp 10.1.1.1 vpn-instance vpn1 export
```

4.1.63 reset bgp

【命令】

reset bgp { **all** | *peer-address* } [**vpn-instance** *vpn-instance-name*]

【视图】

用户视图

【参数】

all：复位当前所有的 BGP 连接。

peer-address：只复位与指定 BGP 对等体的连接。

vpn-instance *vpn-instance-name*：指定 VPN 实例的名称。

【描述】

reset bgp *peer-address* 命令用来复位 BGP 与特定对等体间的连接。

reset bgp all 命令用来复位当前所有的 BGP 连接。

在 BGP 的策略或协议配置改变后，复位 BGP 连接可使新配置的策略立即生效。

【举例】

用 **timer** 命令配置了新的 Keepalive 间隔和 Holdtime 后，可通过复位所有的 BGP 连接使新配置立即生效。

```
<H3C> reset bgp all
```

4.1.64 reset bgp flap-info

【命令】

reset bgp flap-info [**regular-expression** *as-regular-expression* | **as-path-acl** *aspath-acl-number* | *network-address* [*mask*]]

reset bgp *peer-address* [**flap-info**]

【视图】

用户视图

【参数】

regular-expression *as-regular-expression*：清除匹配 AS 路径正则表达式的路由的摆动统计信息。

as-path-acl *aspath-acl-number*：清除匹配指定过滤列表的路由的摆动统计信息，取值范围为 1～199。

network-address：清除该网络地址的摆动统计信息。

mask：网络掩码。

peer-address：清除来自该对等体的所有路由的摆动统计信息。

【描述】

reset bgp flap-info 命令用来清除 BGP 的路由摆动统计信息。

相关配置可参考命令 **dampening**。

【举例】

清除匹配过滤列表 10 的所有 BGP 路由的摆动统计信息。

```
<H3C> reset bgp flap-info as-path-acl 10
```

4.1.65 reset bgp group

【命令】

reset bgp group *group-name* [**vpn-instance** *vpn-instance-name*]

【视图】

用户视图

【参数】

group-name：对等体组的名称，取值范围为 1～47 个字符。

vpn-instance *vpn-instance-name*：指定 VPN 实例的名称。

【描述】

reset bgp group 命令用来复位指定对等体组中的所有成员的 BGP 连接。

相关配置可参考命令 **peer group**。

【举例】

复位对等体组 group1 中所有成员的 BGP 连接。

```
<H3C> reset bgp group group1
```

4.1.66 reset bgp dampening

【命令】

reset bgp dampening [*network-address* [*mask*]]

【视图】

用户视图

【参数】

network-address：清除指定网络的路由摆动衰减信息。

mask：网络掩码。

【描述】

reset bgp dampening 命令用来清除路由摆动衰减信息以及解除对已抑制路由的抑制。

相关配置可参考命令 **dampening** 和 **display bgp routing dampened**。

【举例】

清除到网络 20.1.0.0 的路由的衰减信息，且对受抑制的路由解除抑制。

```
<H3C> reset bgp dampening 20.1.0.0 255.255.0.0
```

4.1.67 summary

【命令】

summary

undo summary

【视图】

BGP 视图

【参数】

无

【描述】

summary 命令用来配置对子网路由进行自动聚合，**undo summary** 命令用来取消对子网路由进行自动聚合。

缺省情况下，不对子网路由进行自动聚合。

配置 **summary** 后，BGP 不能接收从 IGP 引入的子网路由，可通过该命令来减少路由选择信息的数量。

【举例】

对子网路由进行自动聚合。

```
[H3C-bgp] summary
```

4.1.68 timer keep-alive hold

【命令】

timer keep-alive *keepalive-interval* **hold** *holdtime-interval*

undo timer

【视图】

BGP 视图

【参数】

keepalive-interval：发送 Keepalive 消息的间隔时间，取值范围为 0～65535。缺省值为 60 秒。

holdtime-interval：BGP 的保持时间，取值范围为 0，3～65535。缺省值为 180 秒。

【描述】

timer keep-alive hold 命令用来配置 BGP 的 Keepalive 和 Holdtime 定时器，**undo timer** 命令用来恢复 Keepalive 和 Holdtime 定时器的缺省值。

【举例】

配置 BGP 的 Keepalive 和 Holdtime 定时器各为 30 秒和 90 秒。

```
[H3C-bgp] timer keep-alive 30 hold 90
```

4.1.69 undo synchronization

【命令】

undo synchronization

【视图】

BGP 视图

【参数】

无

【描述】

undo synchronization 命令用来取消 IGP 和 IBGP 路由的一致性。

【举例】

配置取消 IGP 和 IBGP 路由同步。

```
[H3C-bgp] undo synchronization
```

4.2 MBGP 配置命令

4.2.1 ipv4-family

【命令】

ipv4-family { **multicast** | **vpn-instance** *vpn-instance-name* }

undo ipv4-family { **multicast** | **vpn-instance** *vpn-instance-name* }

【视图】

BGP 视图

【参数】

multicast：使用该参数将进入 BGP 的组播扩展地址族视图。

vpn-instance *vpn-instance-name*：将指定的 VPN 实例与 IPv4 地址族进行关联，使用该参数将进入 MBGP 地址族视图。

【描述】

ipv4-family 命令用来进入 BGP 的 IPv4 扩展地址族视图，**undo ipv4-family** 命令用来删除扩展地址族视图下的所有配置，并退回到 BGP 的 IPv4 单播地址族视图。

使用此命令进入 IPv4 的扩展地址族视图，在这个视图下，可以为 BGP 配置地址族相关的参数。

执行 **undo ipv4-family multicast** 命令将退出组播扩展地址族视图，删除该地址族下的所有配置，退回到 BGP 单播视图。

执行 **undo ipv4-family vpn-instance** *vpn-instance-name* 命令将取消指定 VPN 实例与 IPv4 地址族的关联，删除该地址族下的所有配置，退回到 BGP 单播视图。

ipv4-family multicast 命令用于组播。

ipv4-family vpn-instance 命令用于 BGP/MPLS VPN，相关内容请参见本手册的“VPN”部分。

相关配置可参考命令 **ipv4-family vpnv4** 和 **peer enable**。

【举例】

进入 VPN 实例地址族视图。

```
[H3C] bgp 1
[H3C-bgp] ipv4-family vpn-instance abc
[H3C-bgp-af-vpn-instance]
```

4.2.2 ipv4-family vpnv4

【命令】

ipv4-family vpnv4 [**unicast**]

undo ipv4-family vpnv4 [**unicast**]

【视图】

BGP 视图

【参数】

unicast：使用该参数将进入 VPN-IPv4 单播地址族视图。

【描述】

ipv4-family vpnv4 命令用来进入 BGP 的 VPNv4 地址族视图，**undo ipv4-family vpnv4** 命令用来删除 VPNv4 地址族视图下的所有配置，并退回到 BGP 的 IPv4 单播地址族视图。

ipv4-family vpnv4 命令用于 BGP/MPLS VPN，相关内容请参见本手册的“MPLS”之“MPLS VPN”。

目前的 Comware 平台只支持 VPN 的 IPv4 单播地址，执行 **ipv4-family vpnv4** 命令时，即使不指定 unicast 参数，进入的也是 VPN-IPv4 单播地址族视图。

相关配置可参考命令 **ipv4-family** 和 **peer activate**。

【举例】

进入 VPNv4 地址族视图。

```
[H3C] bgp 1
[H3C-bgp]ipv4-family vpnv4
[H3C-bgp-af-vpn]
```

4.2.3 peer enable

【命令】

peer *group-name* **enable**

undo peer *group-name* **enable**

【视图】

VPNv4 视图、组播视图

【参数】

group-name：对等体组名称，指定整个对等体组。

【描述】

peer enable 命令用来激活指定对等体/对等体组，**undo peer enable** 命令用来去激活指定对等体/对等体组。

缺省情况下，IPv4 地址族的单播对等体/对等体组是激活的，其它对等体/对等体组都是去激活的。

使用该命令允许或禁止与对等体/对等体组的路由交换。

IPv4 单播在缺省时对等体/对等体组是激活的，可通过 **undo** 命令去激活，当单播和组播公用一条连接时，如果需要去掉单播连接但保持组播连接，可以配置去激活单播对等体。

其它的地址族对等体/对等体组缺省都是去激活的，必须激活后才能正常交换路由信息。

【举例】

配置并激活 VPNv4 单播地址族的指定对等体。

```
[H3C] bgp 100
[H3C-bgp] peer 10.15.0.15 as-number 100
[H3C-bgp] ipv4-family vpnv4 unicast
[H3C-bgp-af-vpn] peer 10.15.0.15 enable
```

配置并激活 IPv4 组播地址族的指定对等体。

```
[H3C] bgp 200
[H3C-bgp] peer 20.10.0.1 as-number 200
[H3C-bgp] ipv4-family multicast
[H3C-bgp-af-mul] peer 20.10.0.1 enable
```

第5章 IP 路由策略配置命令

5.1 IP 路由策略配置命令

5.1.1 apply as-path

【命令】

apply as-path *as-number-1* [*as-number-2* [*as-number-3* ...]]

undo apply as-path

【视图】

路由策略视图

【参数】

as-number-1... *as-number-n*：加入的 AS 号。

【描述】

apply as-path 命令用来指定 Route-policy 中在原 AS 路径前加入 AS 号，**undo apply as-path** 命令用来取消在原 AS 路径前加入的 AS 序号。

缺省情况下，不设置 AS 号。

若匹配了 Route-policy 的匹配条件，则改变发送路由的 AS 属性。最多可加入 10 个 AS 号。

as-path 号主要用来防止路由环路，通过设置 as-path 可以改变 BGP 的路径选择。

【举例】

在原 AS 路径前加入 AS 号 200。

```
[H3C-route-policy] apply as-path 200
```

5.1.2 apply community

【命令】

apply community { { [*aa:nn*] [**no-export-sunconfed**] [**no-export**] [**no-advertise**] [**additive**] } | **additive** | **none** }

undo apply community

【视图】

路由策略视图

【参数】

aa:nn：为团体号。

no-export-subconfed：为不向本地自治系统外部发布匹配的路由。

no-advertise：为不向任何对等体发布匹配的路由。

no-export：为不向自治系统外部通告路由，但发布给其它子自治系统。

additive：为附加路由的团体属性。

none：为删除路由的团体属性。

【描述】

apply community 命令用来指定 Route-policy 中设置 BGP 团体属性，**undo apply community** 命令用来取消设置 BGP 团体的属性。

缺省情况下，不设置 BGP 团体属性。

如果匹配了 Route-policy 的匹配条件，则设置 BGP 团体属性。

相关配置可参考命令 **ip community-list**、**if-match community-list**、**route-policy** 和 **display bgp routing community**。

【举例】

配置一个名为 setcommunity 的 Route-policy，其节点序列号为 16，匹配模式为 permit，并进入路由策略视图，设置匹配条件及执行的属性修改动作。

```
[H3C] route-policy setcommunity permit node 16
[H3C-route-policy] if-match as-path 8
[H3C-route-policy] apply community no-export
```

5.1.3 apply cost

【命令】

apply cost *value*

undo apply cost

【视图】

路由策略视图

【参数】

value：指定路由信息的路由权值。

【描述】

apply cost 命令用来设置路由信息的路由权值，**undo apply cost** 命令用来取消该设置子句。

相关配置可参考命令 **if-match interface**、**if-match acl**、 **if-match ip-prefix**、**if-match ip next-hop**、**if-match cost**、**if-match tag**、**route-policy**、**apply local-preference**、**apply origin** 和 **apply tag**。

【举例】

本例定义一条 apply 子句，当用于路由信息属性设置时，设置路由信息的路由权值为 120。

```
[H3C-route-policy] apply cost 120
```

5.1.4 apply cost-type

【命令】

apply cost-type [**internal** | **external**]

undo apply cost-type

【视图】

路由策略视图

【参数】

internal：向 EBGP 对等体通告路由时使用 IGP 的 cost 作为 BGP 的 MED 值。

external：IS-IS 外部权值。

【描述】

apply cost-type 命令用来设置路由信息的路由权类型，**undo apply cost-type** 命令用来取消该设置子句。

缺省情况下，不设置路由权属性。

【举例】

设置 IGP 的 cost 作为 BGP 的 MED 值。

```
[H3C-route-policy] apply cost-type internal
```

5.1.5 apply local-preference

【命令】

apply local-preference *local-preference*

undo apply local-preference

【视图】

路由策略视图

【参数】

local-preference：本地优先级。

【描述】

apply local-preference 命令用来设置路由信息的本地优先级，**undo apply local-preference** 命令用来取消该设置子句。

相关配置可参考命令 **if-match interface**、**if-match acl**、 **if-match ip-prefix**、**if-match ip next-hop**、**if-match cost**、**if-match tag**、**route-policy**、**apply local-preference**、**apply origin** 和 **apply tag**。

【举例】

本例定义一条 apply 子句，当用于路由信息属性设置时，设置路由信息的本地优先级为 130。

```
[H3C-route-policy] apply local-preference 130
```

5.1.6 apply origin

【命令】

apply origin { **igp** | **egp** *as-number* | **incomplete** }

undo apply origin

【视图】

路由策略视图

【参数】

igp：设定 BGP 路由信息的来源为内部路由。

egp：设定 BGP 路由信息的来源为外部路由。

as-number：指定外部路由的自治系统号。

incomplete：设定 BGP 路由信息的来源为未知来源。

【描述】

apply origin 命令用来设置 BGP 路由信息的路由源，**undo apply origin** 命令用来取消该设置子句。

相关配置可参考命令 **if-match interface**、**if-match acl**、 **if-match ip-prefix**、**if-match ip next-hop**、**if-match cost**、**if-match tag**、**route-policy**、**apply local-preference**、**apply cost** 和 **apply tag**。

【举例】

本例定义一条 apply 子句，当用于路由信息属性设置时，设置 BGP 路由信息的路由源为 igp。

```
[H3C-route-policy] apply origin igp
```

5.1.7 apply tag

【命令】

apply tag *value*

undo apply tag

【视图】

路由策略视图

【参数】

value：指定路由信息的标记值。

【描述】

apply tag 命令用来设置 OSPF 路由信息的标记域，**undo apply tag** 命令用来取消该设置子句。

当一个路由被从协议 A 引入到协议 B，并且在其它一些点又被引回到协议 A 时，协议 A 允许路由协议更新报文中的 tag 域被传递到它另一侧的 peer 中，即 tag 域中的信息可以从协议 A 穿过协议 B 传递到协议 A 中，不会被丢失。

OSPF，RIP2，ISIS 和 BGP 都支持 tag 域，RIP1 不支持。

例如 BGP 路由被引入到 OSPF 而在另一点又被引回到 BGP 时，BGP 路由的 as-path 属性将会丢失，此时可以利用 **aplly tag** 来设置 OSPF 的 tag 域为 as-path，保证 as-path 属性的完整。

相关配置可参考命令 **if-match interface**、**if-match acl**、 **if-match ip-prefix**、**if-match ip next-hop**、**if-match cost**、**if-match tag**、**route-policy**、**apply local-preference**、**apply cost** 和 **apply origin**。

【举例】

本例定义一条 apply 子句，当用于路由信息属性设置时，设置路由信息的标记域为 100。

```
[H3C-route-policy] apply tag 100
```

5.1.8 display ip ip-prefix

【命令】

display ip ip-prefix [*ip-prefix-name*]

【视图】

所有视图

【参数】

ip-prefix-name：指定显示的地址前缀列表名。

【描述】

display ip ip-prefix 命令用来显示地址前缀列表。

不指定 *ip-prefix-name* 时，将显示所有已配置的地址前缀列表。

相关配置可参考命令 **ip ip-prefix**。

【举例】

本例显示名为 p1 的地址前缀列表的信息。

```
<H3C> display ip ip-prefix p1
name      index   conditions   ip-prefix/mask   GE   LE
p1        10      deny         1.1.1.0/24       --   --
```

5.1.9 display route-policy

【命令】

display route-policy [*route-policy-name*]

【视图】

所有视图

【参数】

route-policy-name：指定显示的 Route-policy 名。

【描述】

display route-policy 命令用来显示配置的 Route-policy。

不指定 *route-policy-name* 时，显示所有已配置的 Route-policy。

相关配置可参考命令 **route-policy**。

【举例】

显示名为 policy 1 的 Route-policy 信息。

```
<H3C> display route-policy policy1
Route-policy : policy1
  Permit 10 : if-match (prefixlist) p1
              apply cost 100
```

5.1.10 filter-policy export

【命令】

filter-policy { *acl-number* | **ip-prefix** *ip-prefix-name* } **export** [*protocol*]

undo filter-policy { *acl-number* | **ip-prefix** *ip-prefix-name* } **export** [*protocol*]

【视图】

路由协议视图

【参数】

acl-number：指定用于匹配路由信息目的地址域的访问列表号。

ip-prefix-name：指定用于匹配路由信息目的地址域的地址前缀列表。

protocol：指定何种路由协议的路由信息将被过滤。

【描述】

filter-policy export 命令用来设置对某类路由协议所发布路由信息的过滤条件，**undo filter-policy export** 命令用来取消所设置的过滤条件。

缺省情况下，不对发布的路由进行过滤。

某些情况下，可能要求只发布某些满足条件的路由信息，此时，可以定义 filter-policy 设置所发布路由信息的过滤条件，只有通过了过滤的路由信息才能被发布。

相关配置可参考命令 **filter-policy import**。

【举例】

定义 RIP 的路由信息发布过滤规则，只有通过地址前缀列表 p1 过滤的路由信息才会被 RIP 发布。

```
[H3C-rip] filter-policy ip-prefix p1 export
```

5.1.11 filter-policy import

【命令】

filter-policy gateway *ip-prefix-name* **import**

undo filter-policy gateway *ip-prefix-name* **import**

filter-policy { *acl-number* | **ip-prefix** *ip-prefix-name* } **import**

undo filter-policy { *acl-number* | **ip-prefix** *ip-prefix-name* } **import**

【视图】

路由协议视图

【参数】

acl-number：指定用于匹配路由信息的目的地址域的访问列表号。

ip-prefix *ip-prefix-name*：地址前缀列表名，其匹配对象为路由信息的目的地址域。

gateway *ip-prefix-name*：邻居路由器地址的地址前缀列表名，其匹配对象为指定的邻居路由器发布的路由信息。

【描述】

filter-policy gateway import 命令用来对指定路由器发布的路由信息进行过滤，**undo filter-policy gateway import** 命令用来取消过滤条件的设置。

filter-policy import 命令用来设置路由信息的过滤条件，**undo filter-policy import** 命令用来取消对过滤条件的设置。

缺省情况下，不对接收的路由信息进行过滤。

某些情况下，路由协议可能要求忽略所接收到的某些路由信息，可以定义 **filter-policy**，指定路由信息的过滤条件。*acl-number* 指定用于过滤路由信息目的地址的访问列表号。*ip-prefix* 选项用于过滤指定目的地址的路由信息；**gateway** 选项用于过滤指定的邻居路由器发布的路由信息。

相关配置可参考命令 **filter-policy export**。

【举例】

定义 RIP 的路由信息接收过滤规则，凡通过地址前缀列表 p1 过滤的路由信息才会被 RIP 接收。

```
[H3C-rip] filter-policy ip-prefix p1 import
```

5.1.12 if-match acl

【命令】

if-match acl *acl-number*

undo if-match [**acl** *acl-number*]

【视图】

路由策略视图

【参数】

acl-number：指定用于过滤的访问列表号。

【描述】

if-match acl 命令用来指定 Route-policy 的匹配规则之一，指定 Route-policy 中匹配的 IP 地址范围，**undo if-match acl** 命令用来取消匹配规则的设置。

该命令通过对一个 ACL 的引用实现过滤的功能。

相关配置可参考命令 **if-match ip-prefix**、**if-match interface**、**if-match ip next-hop**、**if-match cost**，**if-match tag**、**route-policy**、**apply cost**、**apply local-preference**、**apply origin** 和 **apply tag**。

【举例】

定义一条 if-match 子句，当用于过滤路由信息时，允许目的地址通过 ACL 2010 过滤的路由信息通过该 if-match 子句。

```
[H3C-route-policy] if-match acl 2010
```

5.1.13 if-match as-path

【命令】

if-match as-path *aspath-acl-number*

undo if-match as-path

【视图】

路由策略视图

【参数】

aspath-acl-number：为 AS 路径列表号，取值范围为 1～199。*aspath-acl-number* 是由 **ip as-path-acl** 命令定义的。

【描述】

if-match as-path 命令用来过滤 BGP 路由信息，**undo if-match as-path** 命令用来取消匹配的正则表达式。

缺省情况下，Route-policy 中不匹配 AS 路径列表。

Route-policy 的 if-match 子句之一，用于过滤 BGP 路由信息，根据路由信息的自治系统路径属性指定匹配条件。

相关配置可参考命令 **ip as-path-acl**。

【举例】

首先定义一个编号为 2 的 as-path。然后定义名为 test 的 route-policy，该 route-policy 编号为 10 的节点定义了一条 if-match 子句，它引用的是 as-path 的定义。

```
[H3C] ip as-path-acl 2 permit 200 300
[H3C] route-policy test permit node 10
[H3C-route-policy] if-match as-path 2
```

5.1.14 if-match community

【命令】

if-match community { *standard-community-list-number* [**whole-match**] | *extended-community-list-number* }

undo if-match community

【视图】

路由策略视图

【参数】

standard-community-list-number：为标准团体表号，范围为 1～99。

extended-community-list-number：为扩展团体表号，范围为 100～199。

whole-match：为确切匹配，即所有团体而且仅有这些团体必须出现。

【描述】

if-match community 命令用来指定 Route-policy 中匹配的团体列表号，**undo if-match community** 命令用来取消匹配的团体列表号。

缺省情况下，不匹配团体列表。

Route-policy 的 if-match 子句之一，用于过滤 BGP 路由信息，根据路由信息的团体属性指定匹配条件。

相关配置可参考命令 **route-policy** 和 **ip community-list**。

【举例】

首先定义一个编号为 1 的 community-list，然后定义名为 test 的 route-policy，该 route-policy 编号为 10 的节点定义了一条 if-match 子句，它引用的是 community-list 的定义。

```
[H3C] ip community-list 1 permit 100:200
[H3C] route-policy test permit node 10
[H3C-route-policy] if-match community 1
```

5.1.15 if-match cost

【命令】

if-match cost *value*

undo if-match cost

【视图】

路由策略视图

【参数】

value：指定要求的路由权值，范围是 0～4294967295。

【描述】

if-match cost 命令用来指定 Route-policy 的匹配规则之一，用来匹配路由信息的路由权值，**undo if-match cost** 命令用来取消匹配规则的设置。

缺省情况下，没有 if-match 子句被定义。

Route-policy 的 if-match 子句之一，指定满足条件的路由信息的路由权值。

相关配置可参考命令 **if-match interface**，**if-match acl**， **if-match ip-prefix**，**if-match ip next-hop**， **if-match tag**， **route-policy**， **apply cost**， **apply local-preference**，**apply origin**，**apply tag**。

【举例】

定义一条 if-match 子句，允许路由权值为 8 的路由信息通过该 if-match 子句。

```
[H3C-route-policy] if-match cost 8
```

5.1.16 if-match interface

【命令】

if-match interface *interface-type interface-number*

undo if-match interface

【视图】

路由策略视图

【参数】

interface-type：指定接口类型。

interface-number：指定接口编号。

【描述】

if-match interface 命令用来匹配下一跳为指定接口的路由，**undo if-match interface** 命令用来取消匹配条件的设置。

缺省情况下，没有 if-match 子句被定义。

Route-policy 的 if-match 子句之一，当用于过滤路由时，匹配路由下一跳对应的接口。

当前策略路由不支持插卡热插拔事件，即拔掉插卡后，相应的配置仍然存在，需要手工删除。

相关配置可参考命令 **if-match acl**、**if-match ip-prefix**、**if-match ip next-hop**、**if-match cost**、**if-match tag**、**route-policy**、**apply cost**、**apply local-preference**、**apply origin** 和 **apply tag**。

【举例】

本例定义一条 if-match 子句，匹配下一跳接口为 Ethernet1/0/2 的路由。

```
[H3C-route-policy] if-match interface Ethernet1/0/2
```

5.1.17 if-match ip next-hop

【命令】

if-match ip next-hop { **acl** *acl-number* | **ip-prefix** *ip-prefix-name* }

undo if-match ip next-hop [**ip-prefix**]

【视图】

路由策略视图

【参数】

acl-number：指定用于过滤的访问列表号。取值范围为 2000～2999。

ip-prefix-name：指定用于过滤的地址前缀列表名。取值长度为 1～19。

【描述】

if-match ip next-hop 命令用来指定 Route-policy 的匹配规则之一，用于匹配路由信息的下一跳地址，**undo if-match ip next-hop** 命令用来取消匹配规则的设置。

缺省情况下，没有 if-match 子句被定义。

Route-policy 的 if-match 子句之一，当用于过滤路由信息时指定匹配路由信息的下一跳地址域，通过对一个 ACL 或地址前缀列表的引用实现过滤的功能。

相关配置可参考命令 **if-match interface**、**if-match acl**、**if-match ip-prefix**、**if-match cost**、**if-match tag**、**route-policy**、**apply cost**、**apply local-preference**、**apply origin** 和 **apply tag**。

【举例】

定义一条 if-match 子句，允许路由下一跳地址通过地址前缀列表 p1 过滤的路由信息通过该 if-match 子句。

```
[H3C-route-policy] if-match ip next-hop ip-prefix p1
```

5.1.18 if-match ip-prefix

【命令】

if-match ip-prefix *ip-prefix-name*

undo if-match ip-prefix

【视图】

路由策略视图

【参数】

ip-prefix-name：指定用于过滤的地址前缀列表名。

【描述】

if-match ip-prefix 命令用来指定 Route-policy 的匹配规则之一，指定 Route-policy 中匹配的 IP 地址范围，**undo if-match ip-prefix** 命令用来取消匹配规则的设置。

该命令通过对一个地址前缀列表的引用实现过滤的功能。

相关配置可参考命令 **if-match acl**、**if-match interface**、**if-match ip next-hop**、**if-match cost**，**if-match tag**、**route-policy**、**apply cost**、**apply local-preference**、**apply origin** 和 **apply tag**。

【举例】

定义一条 if-match 子句，当用于过滤路由信息时，允许目的地址通过地址前缀列表 p1 过滤的路由信息通过该 if-match 子句。

```
[H3C-route-policy] if-match ip-prefix p1
```

5.1.19 if-match tag

【命令】

if-match tag *value*

undo if-match tag

【视图】

路由策略视图

【参数】

value：指定的标记值。

【描述】

if-match tag 命令用来匹配路由信息的标记域，**undo if-match tag** 命令用来取消已有的匹配规则。

当一个路由被从协议 A 引入到协议 B，并且在其它一些点又被引回到协议 A 时，协议 A 允许路由协议更新报文中的 tag 域被传递到它另一侧的 peer 中，即 tag 域中的信息可以从协议 A 穿过协议 B 在在协议 A 中，不会被丢失。

OSPF，RIP2，ISIS。BGP 都支持 tag 域，RIP 不支持。

例如 BGP 路由被引入 OSPF，在另一点又被引入回到 BGP 时，BGP 路由的 as-path 属性将会丢失，此时可以利用 aplly 来设置 OSPF 的 tag 域为 as-path，保证 as-path 属性的完整。

相关配置可参考命令 **if-match interface**、**if-match acl**、**if-match ip-prefix**、**if-match ip next-hop**、**if-match cost**、**route-policy**、**apply cost**、**apply local-preference**、**apply origin** 和 **apply tag**。

【举例】

定义一条 if-match 子句，允许标记域为 8 的路由信息通过该 if-match 子句的过滤。

```
[H3C-route-policy] if-match tag 8
```

5.1.20 ip ip-prefix

【命令】

ip ip-prefix *ip-prefix-name* [**index** *index-number*] { **permit** | **deny** } *network len* [**greater-equal** *greater-equal* | **less-equal** *less-equal*] *

undo ip ip-prefix *ip-prefix-name* [**index** *index-number* | **permit** | **deny**]

【视图】

系统视图

【参数】

ip-prefix-name：指定地址前缀列表名，唯一标识一个地址前缀列表。

index-number：标识地址前缀列表中的一条表项，*index-number* 小的表项先被测试。

permit：指定所定义的地址前缀列表表项的匹配模式为允许模式。当指定为允许模式并且待过滤的 IP 地址在该表项指定的前缀范围内时，通过该表项的过滤不进入下一个结点的测试）；如待过滤的 IP 地址不在该表项指定的前缀范围内，则进行下一表项测试。

deny：指定所定义的地址前缀列表表项的匹配模式为拒绝模式。当指定为拒绝模式并且待过滤的 IP 地址在该表项指定的前缀范围内时，不能通过该表项的过滤，并且不会进行下一个表项的测试。

network len：指定 IP 地址及掩码长度，当指定为 0.0.0.0 0 时匹配所有 IP 地址。

greater-equal、*less-equal*：指定匹配 network len 地址前缀后还需匹配的地址前缀范围[*greater-equal*，*less-equal*]。**greater-equal** 的含义为“大于等于”，**less-equal**

的含义为“小于等于”，其取值范围为 *len* <= *greater-equal* <= *less-equal* <= 32，当只指定**greater-equal**时，表示前缀范围[*greater-equal*，32]，当只指定**less-equal**时，表示前缀范围[*len*，*less-equal*]。

【描述】

ip ip-prefix 命令用来配置一条地址前缀列表或其某个表项，**undo ip ip-prefix** 命令用来删除一个地址前缀列表或其某个表项。

地址前缀列表用于 IP 地址的过滤。一个地址前缀列表可以有若干条表项，每一表项指定一个地址前缀范围。表项之间的过滤关系是“或”的关系，即通过一条表项的过滤就意味着通过该地址前缀列表的过滤。若没有通过任一表项的过滤，则不能通过该地址前缀列表的过滤。

地址前缀范围可以有两部分，分别由 *len* 与[*greater-equal*，*less-equal*]确定。如果这两部分前缀范围都被指定，则待过滤的 IP 必须匹配这两部分的前缀范围。

如果将 *network len* 指定为 0.0.0.0 0，则只匹配缺省路由。

如果需要匹配所有路由，则应配置为 0.0.0.0 0 *less-equal* 32。

【举例】

定义一条名称为 p1 的地址前缀列表，只允许 10.0.0.0/8 网段的，掩码长度为 17 或 18 的路由通过。

```
[H3C] ip ip-prefix p1 permit 10.0.0.0 8 greater-equal 17 less-equal 18
```

5.1.21 route-policy

【命令】

route-policy *route-policy-name* { **permit** | **deny** } **node** *node-number*

undo route-policy *route-policy-name* [**permit** | **deny** | **node** *node-number*]

【视图】

系统视图

【参数】

route-policy-name：指定 Route-policy 名，唯一标识一个 Route-policy。

permit：指定所定义的 Route-policy 节点的匹配模式为允许模式。当路由项满足该节点的所有 if-match 子句时被允许通过该节点的过滤并执行该节点的 apply 子句，如路由项不满足该节点的 if-match 子句，该 Route-policy 的下一个节点将被测试。

deny：指定所定义的 Route-policy 节点的匹配模式为拒绝模式，当路由项满足该节点的所有 if-match 子句时被拒绝通过该节点的过滤，并且不会进行下一个节点的测试。

node：路由策略的节点。

node-number：标识 Route-policy 中的一个节点索引，当该 Route-policy 用于路由信息过滤时，*node-number* 小的节点先被测试。

【描述】

route-policy 命令用来创建路由策略并进入路由策略视图，**undo route-policy** 命令用来删除已创建的 Route-policy。

缺省情况下，没有 Route-policy 被定义。

Route-policy 用于路由信息过滤或策略路由。一个 Route-policy 由若干节点组成，每一节点由一些 if-match 子句和 apply 子句组成。if-match 子句定义该节点的匹配规则，apply 子句定义通过该节点过滤后进行的动作。节点的 if-match 子句之间的过滤关系是“与”的关系，即必须满足该节点的所有 if-match 子句。Route-policy 节点之间的过滤关系是“或”的关系，即通过一个节点的过滤就意味着通过该 Route-policy 的过滤。若没有通过任一节点的过滤，则不能通过该 Route-policy 的过滤。

相关配置可参考命令 **if-match interface**、**if-match acl**、**if-match ip-prefix**、**if-match ip next-hop**、**if-match cost**、**if-match tag**、**apply local-preference**、**apply cost**、**apply origin** 和 **apply tag**。

【举例】

配置一个 Route-policy policy1，其节点序列号为 10，匹配模式为 permit，并进入路由策略视图。

```
[H3C] route-policy policy1 permit node 10
[H3C-route-policy]
```

第6章 路由容量配置命令

6.1 路由容量配置命令

6.1.1 display memory

【命令】

dispaly memory [**limit**]

【视图】

所有视图

【参数】

limit：显示防火墙空闲内存的下限值及安全值的配置。

【描述】

dispaly memory 命令用来查看与路由容量相关的内存设置和状态信息。

该命令可用来察看当前的配置信息、可用内存多少，以及关于连接的状态信息：包括连接断开次数、重新建立连接次数、当前是否进入紧急状态。

【举例】

查看当前的内存设置和状态信息。

```
<H3C> display memory limit
Current memory limit configuration information:
system memory safety: 30 (MBytes)
system memory limit: 20 (MBytes)
  memory auto-establish enabled

Free Memory: 73855332 (Bytes)

The state information about connection:
  The times of disconnect: 0
  The times of reconnect: 0
  The current state: Normal
```

该命令显示的内容包括当前对于路由容量的内存限制、空闲内存的大小、连接断开的次数、连接重建的次数，以及目前的状态。

显示信息的详细说明参见下表：

表6-1 dispaly memory limit 命令显示说明

项目	描述
memory safety: 30	防火墙内存安全值为 30Mbytes
memory limit: 20	防火墙内存下限为 20Mbytes
memory auto-establish enabled	允许自动恢复连接（如果禁止了自动恢复功能，将显示 auto-establish disabled）
Free Memory: 73855332 (Bytes)	当前的空闲内存大小为 73855332 字节，即 73.855M
The times of disconnect: 0	路由协议的连接断开次数为 0
The times of reconnect: 0	路由协议的连接重新建立次数为 0
The current state: Normal	当前状态正常（如果进入紧急状态，将显示 Exigence）

6.1.2 memory auto-establish disable

【命令】

memory auto-establish disable

【视图】

系统视图

【参数】

无

【描述】

memory auto-establish disable 命令用来禁止恢复路由协议的连接（即使空闲内存恢复到安全值）。

缺省情况下，当防火墙的空闲内存恢复到一个安全的值时，总是自动恢复各个路由协议的连接（该连接在防火墙空闲内存减少到一个下限值时被强制断开）。

如果使用了该命令，当防火墙的空闲内存恢复到安全值时，并不会自动的恢复各个路由协议的连接；如果此时需要恢复连接，需要重启路由协议。

建议慎重使用该命令。

相关配置可参考命令 **memory auto-establish enable**、**memory** 和 **display memory limit**。

【举例】

禁止当前防火墙内存恢复时自动恢复各协议的连接。

```
[H3C] memory auto-establish disable
[H3C]
```

```
%Dec 15 15:53:38:298 2004 H3C RM/5/RTLOG:You have changed the model of
connection
```

6.1.3 memory auto-establish enable

【命令】

memory auto-establish enable

【视图】

系统视图

【参数】

无

【描述】

memory auto-establish enable 命令用来确定当空闲内存恢复到指定的值时，自动恢复各个路由协议的连接。

缺省情况下，当防火墙的空闲内存恢复到一个安全的值时，总是自动恢复各个路由协议的连接（该连接在防火墙空闲内存减少到一个下限值时被强制断开）。

使用 **memory auto-establish disable** 命令，可以禁止上述功能；使用 **memory auto-establish enable** 命令则可以重新启用上述功能。缺省情况下，该功能总是被启用。

相关配置可参考命令 **memory auto-establish disable**、**memory** 和 **display memory limit**。

【举例】

使能当前防火墙的内存恢复时自动恢复各协议的连接。

```
[H3C] memory auto-establish enable
[H3C]
%Dec 15 15:53:38:298 2004 H3C RM/5/RTLOG:You have changed the model of
connection
```

6.1.4 memory

【命令】

memory { **safety** *safety-value* | **limit** *limit-value* }*

undo memory { **safety** | **limit** }

【视图】

系统视图

【参数】

safety-value：防火墙空闲内存的安全值，单位为 Mbytes，取值范围由当前的防火墙空闲内存决定。

limit-value：防火墙空闲内存的下限值，单位为 Mbytes，取值范围由当前的防火墙空闲内存决定。

【描述】

memory 命令用来设置防火墙空闲内存的安全值及下限值。当防火墙的空闲内存少于 *limit-value* 值时，将强制断开所有路由协议的连接；如果使用了 **memory auto-establish enable** 命令（缺省配置），当防火墙的空闲内存达到 *safety-value* 值时，将自动恢复被强制断开的路由协议的连接。**undo memory** 命令用来将防火墙空闲内存的安全值与下限值恢复为缺省配置。

命令中的 *limit-value* 必须小于 *safety-value*，否则配置不会成功。

相关配置可参考命令 **memory auto-establish disable**、**memory auto-establish enable** 和 **display memory limit**。

【举例】

设置防火墙内存的下限值为 25Mbytes。

```
[H3C] memory limit 25
[H3C]
%Dec 15 16:51:29:987 2004 H3C RM/5/RTLOG:You have changed the memory limit/safety value
```

设置防火墙空闲内存的下限值为 25Mbytes、安全值为 30Mbytes。

```
[H3C] memory safety 30 limit 25
[H3C]
%Dec 15 15:51:29:987 2004 H3C RM/5/RTLOG:Changed the system memory limit(20->25)/ safety(30->35) successfully
```

目 录

第 1 章 MPLS基本配置命令 1-1
1.1 MPLS基本配置命令 1-1
1.1.1 debugging mpls lspm 1-1
1.1.2 display mpls fast-forwarding cache 1-2
1.1.3 display mpls interface 1-2
1.1.4 display mpls lsp 1-3
1.1.5 display mpls static-lsp 1-3
1.1.6 display mpls statistics 1-4
1.1.7 lsp-trigger 1-6
1.1.8 mpls 1-6
1.1.9 mpls lsr-id 1-7
1.1.10 reset mpls fast-forwarding cache 1-8
1.1.11 reset mpls statistics 1-8
1.1.12 snmp-agent trap enable ldp 1-9
1.1.13 snmp-agent trap enable lsp 1-10
1.1.14 static-lsp egress 1-10
1.1.15 static-lsp ingress 1-11
1.1.16 static-lsp transit 1-12
1.1.17 ttl expiration 1-13
1.1.18 ttl propagate 1-13
第 2 章 LDP配置命令 2-1
2.1 LDP配置命令 2-1
2.1.1 debugging mpls ldp 2-1
2.1.2 display mpls ldp 2-2
2.1.3 display mpls ldp buffer-info 2-2
2.1.4 display mpls ldp interface 2-3
2.1.5 display mpls ldp lsp 2-4
2.1.6 display mpls ldp peer 2-4
2.1.7 display mpls ldp remote 2-5
2.1.8 display mpls ldp session 2-5
2.1.9 mpls ldp 2-6
2.1.10 mpls ldp enable 2-6
2.1.11 mpls ldp hops-count 2-7
2.1.12 mpls ldp loop-detect 2-8
2.1.13 mpls ldp password 2-8
2.1.14 mpls ldp path-vectors 2-9
2.1.15 mpls ldp remote-peer 2-10
2.1.16 mpls ldp reset-session 2-10
2.1.17 mpls ldp timer 2-11
2.1.18 mpls ldp timer targeted-hello 2-12

2.1.19 mpls ldp timer targeted-session-hold 2-12
2.1.20 mpls ldp transport-ip..... 2-13
2.1.21 remote-ip 2-14

第1章 MPLS 基本配置命令

1.1 MPLS 基本配置命令

1.1.1 debugging mpls lspm

【命令】

debugging mpls lspm { **agent** | **all** | **event | ftn** | **interface** | **packet | policy** | **process** | **vpn** }

undo debugging mpls lspm { **agent** | **all** | **event | ftn** | **interface** | **packet | policy** | **process** | **vpn** }

【视图】

用户视图

【参数】

agent：打开 MPLS Agent 的所有调试信息开关。

all：打开所有和 MPLS 相关的调试信息开关。

event：打开 MPLS 各种事件的调试信息开关。

ftn：打开 MPLS ftn 调试开关。

interface：打开 MPLS 发送和接收消息的接口的调试信息开关。

packet：打开 MPLS 报文调试信息开关。

policy：打开 MPLS 的调试信息开关。

process：打开 MPLS 内部处理的调试信息开关。

vpn：打开 MPLS VPN 的所有调试信息开关。

【描述】

debugging mpls lspm 命令用来打开 LSP 的各种调试信息的开关，**undo debugging mpls lspm** 命令用来关闭相应的调试开关。

缺省情况下，所有调试开关均不打开。

此命令用于对 MPLS LSPM 运行过程中出现的问题进行调试。打开调试开关对安全网关性能有一定影响，建议慎用此命令。

【举例】

打开 MPLS LSP 的 VPN 所有相关调试信息的开关。

```
<H3C> debugging mpls lspm vpn
```

1.1.2 display mpls fast-forwarding cache

【命令】

display mpls fast-forwarding cache

【视图】

任意视图

【参数】

无

【描述】

display mpls fast-forwarding cache 命令用来显示 MPLS 的快速转发信息。

【举例】

显示 MPLS 的快速转发信息。

```
<H3C> display mpls fast-forwarding cache
```

1.1.3 display mpls interface

【命令】

display mpls interface

【视图】

所有视图

【参数】

无

【描述】

display mpls interface 命令用来显示所有使能了 MPLS 能力的接口的信息。

相关配置可参考命令 **display mpls lsp**，**display mpls statistics**，**display static-lsp**。

【举例】

显示所有使能了 MPLS 能力的接口的信息。

```
[H3C] display mpls interface
```

1.1.4 display mpls lsp

【命令】

display mpls lsp [**verbose**] [**include** *text*]

【视图】

所有视图

【参数】

verbose：显示详细信息。

include *text*：匹配包含指定信息的字符串。

【描述】

display mpls lsp 命令用来显示 LSP 的信息。

缺省情况下，**display mpls lsp** 表示显示所有 LSP。

相关配置可参考命令 **display mpls interface**，**display mpls statistics**，**display static-lsp**。

【举例】

显示所有入接口是 Ethernet 0/0/0 的 LSP。

```
[H3C] display mpls lsp include incoming-interface Ethernet 0/0/0
```

1.1.5 display mpls static-lsp

【命令】

display mpls static-lsp [**verbose**] [**include** *text*]

【视图】

所有视图

【参数】

verbose：显示详细信息。

include *text*：匹配包含指定信息的字符串。

【描述】

display mpls static-lsp 命令用来显示全部或单个静态 LSP 的信息。

相关配置可参考命令 **display mpls interface**，**display mpls lsp**，**display mpls statistics**。

【举例】

显示名为 beijing-shanghai 的静态 LSP 下的信息：

```
[H3C] display mpls static-lsp include beijing-shanghai
```

1.1.6 display mpls statistics

【命令】

display mpls statistics { **interface** { **all** | *interface-type interface-number* } } | { **lsp** [*lsp-Index* | **all** | **name** *lsp-name*] } }

【视图】

所有视图

【参数】

interface-type：接口类型。

interface-number：接口号。

lsp-Index：标签转发路径索引号。

all：所有的标签转发路径。

name *lsp-name*：标签转发路径名称。

【描述】

display mpls statistics 命令用来显示全部或单个 LSP 的统计信息，可以显示全部或单个接口上的 LSP 统计信息。

具体的信息包括每一条 LSP 的入口处理的字节数、报文数、错误数，丢弃报文数，LSP 出口的处理字节数、报文数、错误数，丢弃报文数；每个具有 MPLS 能力的接口进入的字节数、报文数、错误数，丢弃报文数，接口发送的字节数、报文数、错误数，丢弃报文数。

此命令显示的为公网 LSP 的统计信息，对于仅携带私网标签的报文并不在统计范围。

相关配置可参考命令 **display mpls interface**，**display mpls lsp**，**display mpls static-lsp**。

【举例】

显示 MPLS 统计信息。

```
[H3C] display mpls statistics lsp all
Building the information...
  LSP Index/LSP Name :  1/lsp1
    InSegment Octets of LSP is: 0            LSP 的入口处理的字节数
    InSegment Packets of LSP is: 0          LSP 的入口处理的报文数:
```

```
    InSegment Errors of LSP is: 0          LSP 的入口处理的错误数
    InSegment Discard Packets of LSP is: 0    LSP 的入口处理的丢弃报文数
  LSP Index/LSP Name :  1/lsp1
    OutSegment Octets of LSP is: 0              LSP 的出口处理的字节数
    OutSegment Packets of LSP is: 0             LSP 的出口处理的报文数
    OutSegment Errors of LSP is: 0              LSP 的出口处理的错误数
    OutSegment Discard Packets of LSP is: 0     LSP 的出口处理的丢弃报文数
  LSP Index/LSP Name :  17416/dynamic-lsp
    InSegment Octets of LSP is: 0
    InSegment Packets of LSP is: 0
    InSegment Errors of LSP is: 0
    InSegment Discard Packets of LSP is: 0
  LSP Index/LSP Name :  17416/dynamic-lsp
    OutSegment Octets of LSP is: 0
    OutSegment Packets of LSP is: 0
    OutSegment Errors of LSP is: 0
    OutSegment Discard Packets of LSP is: 0
```

显示所有接口 MPLS 统计信息。

```
[H3C] display mpls statistics interface all
  Showing statistics about all MPLS interface:
  The statistics of interface : Ethernet0/0/0
  The statistics of interface in :
      In Octets of Mpls interface is: 0    从该接口进入的字节数
      In Packets of Mpls interface is: 0   从该接口进入的报文数
      In Errors of Mpls interface is: 0    从该接口进入的报文处理错误数
      In Discard Packets of Mpls interface is: 0 从该接口进入的丢弃报文数
The statistics of interface out :
      Out Octets of Mpls interface is: 0      从该接口发送的字节数
      Out Packets of Mpls interface is: 0    从该接口发送的报文数
      Out Errors of Mpls interface is: 0     从该接口发送的报文处理错误数
      Out Discard Packets of Mpls interface is: 0 从该接口发送的丢弃报文数
  The statistics of interface : Ethernet 1/0/0
  The statistics of interface in :
      In Octets of Mpls interface is: 0
      In Packets of Mpls interface is: 0
      In Errors of Mpls interface is: 0
      In Discard Packets of Mpls interface is: 0
The statistics of interface out :
      Out Octets of Mpls interface is: 0
      Out Packets of Mpls interface is: 0
      Out Errors of Mpls interface is: 0
      Out Discard Packets of Mpls interface is: 0
```

1.1.7 lsp-trigger

【命令】

lsp-trigger { **all** | **ip-prefix** *ip-prefix* }

undo lsp-trigger { **all** | **ip-prefix** [*ip-prefix*] }

【视图】

MPLS 视图

【参数】

all: 允许任意路由建立 LSP。

ip-prefix：对匹配地址前缀列表的路由建立 LSP。

ip-prefix：地址前缀列表名，长度为 1～19 个字符的字符串。

【描述】

lsp-trigger 命令用来配置拓扑驱动建立 LSP 的建立策略，**undo lsp-trigger** 命令用来取消参数所指定的过滤条件，任何路由都不允许触发建立 LSP。

缺省情况下，过滤掉所有的路由协议类型。

🕮 **说明：**

在未配置路由触发策略的情况下，系统默认 32 位掩码的所有主机路由允许创建 LSP。

如果用户引用了一条没有配置内容的 ip-prefix 规则，按照 Comware 中 ip-prefix 的使用约定，此时默认为所有路由都允许触发建立 LSP。

相关配置可参考命令 **ip ip-prefix**。

【举例】

配置使所有路由均可驱动建立 LSP。

```
[H3C-mpls] lsp-trigger all
```

1.1.8 mpls

【命令】

mpls

undo mpls

【视图】

系统视图、接口视图、虚拟接口视图

【参数】

无

【描述】

在系统视图下，**mpls** 命令用来在全局下启动 MPLS 功能并进入 MPLS 视图。**undo mpls** 用来在全局下关闭 MPLS 功能。

在接口视图下，**mpls** 命令用来使能接口的 MPLS 能力，**undo mpls** 用来关闭接口 MPLS 功能。

缺省情况下，不进入该视图。

执行该命令之后，用户会进入 MPLS 视图。只有在进入 MPLS 视图以后才可以配置 MPLS 的其它命令。

需首先配置 **mpls lsr-id**，才可以进入 MPLS 视图。

相关配置可参考命令 **mpls enable | disable**。

【举例】

系统视图下进入 MPLS 视图。

```
[H3C] mpls
[H3C-mpls]
```

接口视图下执行 MPLS。

```
[H3C-Ethernet0/0/0] mpls
% Info: MPLS in the interface is starting, please wait...OK
```

1.1.9 mpls lsr-id

【命令】

mpls lsr-id *ip-address*

undo mpls lsr-id

【视图】

系统视图

【参数】

ip-address：LSR 的 ID，形如 IP 地址，用来标识一个 LSR。

【描述】

mpls lsr-id 命令用来配置 LSR 的 ID，**undo mpls lsr-id** 命令用来删除 LSR 的 ID。

缺省情况下，LSR 没有 ID 号。

要求 LSR-ID 的地址是本机的接口地址，且这个地址全网内路由可达，一般情况下建议使用 loopback 接口的地址。

使用这个命令配置 LSR 的 ID 号，是配置其它 MPLS 命令的前提。

相关配置可参考命令 **display mpls interface**。

【举例】

配置该 LSR 的 ID 为 202.17.41.246。

```
[H3C] mpls lsr-id 202.17.41.246
% Mpls lsr-id changed.
```

1.1.10 reset mpls fast-forwarding cache

【命令】

reset mpls fast-forwarding cache

【视图】

用户视图

【参数】

无

【描述】

reset mpls fast-forwarding cache 命令用来清除 MPLS 的快速转发信息。

【举例】

清除 MPLS 的快速转发信息。

```
<H3C> reset mpls fast-forwarding cache
```

1.1.11 reset mpls statistics

【命令】

reset mpls statistics { **interface** { **all** | *interface-type interface-num* } | **lsp** {*lsp-index* | **all** | **name** *lsp-name* } }

【视图】

用户视图

【参数】

all: 所有接口或所有 LSP。

interface-type：网络接口类型。

Interface-num：网络接口编号。

lsp-Index：标签转发路径索引号。

name *lsp-name*：标签转发路径名称。

【描述】

reset mpls statistics 命令用来清除 MPLS 统计数据。

使用这个命令可以清除全部或单个接口上的统计信息，或者清除全部或单个 LSP 下的统计信息。

相关配置可参考命令 **display mpls statistics**。

【举例】

清除名为 beijing-shanghai 的 LSP 下的所有统计信息。

```
<H3C> reset mpls statistics lsp name beijing-shanghai
```

1.1.12 snmp-agent trap enable ldp

【命令】

snmp-agent trap enable ldp

undo snmp-agent trap enable ldp

【视图】

系统视图

【参数】

无

【描述】

snmp-agent trap enable ldp 命令用来使能 MPLS 的 LDP 建立过程的 Trap 功能。**undo snmp-agent trap enable ldp** 命令用来取消 MPLS 的 LDP 建立过程的 Trap 功能。

缺省情况下，不使能 MPLS 的 LDP 建立过程的 TRAP 功能。

【举例】

使能 MPLS 的 LDP 建立过程的 TRAP 功能。

```
[H3C] snmp-agent trap enable ldp
```

1.1.13 snmp-agent trap enable lsp

【命令】

snmp-agent trap enable lsp

undo snmp-agent trap enable lsp

【视图】

系统视图

【参数】

无

【描述】

snmp-agent trap enable lsp 命令用来使能 MPLS 的 LSP 建立过程的 Trap 功能。**undo snmp-agent trap enable lsp** 命令用来取消 MPLS 的 LSP 建立过程的 Trap 功能。

缺省情况下，不使能 MPLS 的 LSP 建立过程的 TRAP 功能。

【举例】

使能 MPLS 的 LSP 建立过程的 TRAP 功能。

```
[H3C] snmp-agent trap enable lsp
```

1.1.14 static-lsp egress

【命令】

static-lsp egress *lsp-name* **incoming-interface** *interfac-type interfac-num* **in-label** *in-label-value*

undo static-lsp egress *lsp-name*

【视图】

MPLS 视图

【参数】

lsp-name：标签转发路径名称。

interface-type：网络接口类型。

Interface-num：网络接口编号。

in-label-value：入标签值，取值范围 16～1023。

【描述】

static-lsp egress 命令用来为出口 LSR 配置静态 LSP，**undo static-lsp egress** 命令用来为出口 LSR 删除一条 LSP。

相关配置可参考命令 **static-lsp ingress**，**debugging mpls**。

【举例】

在出口 LSR 上配置一条名为 bj-sh 的静态 LSP。

```
[H3C-mpls] static-lsp egress bj-sh incoming-interface Ethernet 1/0/0 in-label
233
```

1.1.15 static-lsp ingress

【命令】

static-lsp ingress *lsp-name* **destination** *dest-addr* { *addr-mask* | *mask-length* } { **nexthop** *next-hop-addr* | **outgoing-interface** *interfac-type interfac-num* } **out-label** *out-label-value*

undo static-lsp ingress *lsp-name*

【视图】

MPLS 视图

【参数】

lsp-name：标签转发路径名称。

dest-addr：目的 IP 地址。

addr-mask：目的 IP 地址掩码。

mask-length：目的 IP 地址掩码长度。

next-hop-addr：下一跳地址。

interface-type：网络接口类型。

Interface-num：网络接口编号。

out-label-value：出标签值，取值范围 16～1023。

【描述】

static-lsp ingress 命令用来为入口 LSR 配置静态 LSP，**undo static-lsp ingress** 命令用来为入口 LSR 删除一条 LSP。

使用这个命令可以为入口 LSR 配置静态 LSP，同时可以为这条 LSP 设定优先级及度量值。

相关配置可参考命令 **static-lsp egress**，**static-lsp transit**，**debugging mpls**。

【举例】

为入口 LSR 配置一条到目的地址 202.25.38.1 的静态 LSP。

```
[H3C-mpls] static-lsp ingress bj-sh destination 202.25.38.1 24 nexthop
202.55.25.33 out-label 237
```

1.1.16 static-lsp transit

【命令】

static-lsp transit *lsp-name* **incoming-interface** *interface-type interface-num* **in-label** *in-label-value* { **nexthop** *next-hop-addr* | **outgoing-interface** *interface-type interface-num* } **out-label** *out-label-value*

undo static-lsp transit *lsp-name*

【视图】

MPLS 视图

【参数】

lsp-name：标签转发路径名称。

interface-type：入或出接口的接口类型。

Interface-num：入或出接口的接口编号。

next-hop-addr：下一跳地址。

in-label-value：入标签值，取值范围 16～1023。

out-label-value：出标签值，取值范围 16～1023。

【描述】

static-lsp transit 命令用来为中间传送 LSR 配置静态 LSP，**undo static-lsp transit** 命令用来为中间传送 LSR 删除一条 LSP。

使用这个命令可以为中间传送 LSR 配置静态 LSP。

相关配置可参考命令 **static-lsp egress**，**static-lsp ingress**。

【举例】

为中间传送 LSR 的接口 Ethernet 配置了一条静态 LSP，其中入标签为 123，出标签为 253。

```
[H3C-mpls] static-lsp transit bj-sh incoming-interface Ethernet0/0/0 in-label
123 nexthop 202.34.114.7 out-label 253
```

1.1.17 ttl expiration

【命令】

ttl expiration pop

undo ttl expiration pop

【视图】

MPLS 视图

【参数】

无

【描述】

ttl expiration 命令用来配置 MPLS TTL 超时后 ICMP 响应报文沿本地 IP 路由转发。**undo ttl expiration** 命令用来取消此功能。

缺省情况下，对于一层标签的 MPLS TTL 超时报文，将根据本地 IP 路由返回 ICMP 报文。

建议对 ASBR 路由器以及 HoVPN 组网应用中的 SPE 配置 **undo ttl expiration** 命令，以便在对 VPN 私网进行 tracert 操作时能够查看到正确的公网路由器转发路径。

undo mpls 命令将清除所有 **ttl expiration** 的相关配置。

相关配置可参考命令 **ttl propagate**。

【举例】

配置 MPLS TTL 超时时，沿 LSP 返回 ICMP 报文。

```
[H3C-mpls] undo ttl expiration pop
```

1.1.18 ttl propagate

【命令】

ttl propagate { **public** | **vpn** }

undo ttl propagate { **public** | **vpn** }

【视图】

MPLS 视图

【参数】

public：对公网报文进行设置。

vpn：对 VPN 报文进行设置。

【描述】

ttl propagate 命令用来使能 MPLS 的 IP TTL 复制功能。**undo ttl propagate** 命令用来去使能 MPLS 的 IP TTL 复制功能。

缺省情况下，对公网报文使能 TTL 复制功能，对 VPN 报文不使能 TTL 复制功能。

⚠ 注意：

所有 PE 上的 TTL 复制功能配置保持一致，如果只在部分 PE 上使能 TTL 复制功能，将可能导致 traceroute 结果无法真实反映网络状况。

相关配置可参考命令 **tracert** 和 **ttl expiration**。

【举例】

使能 VPN 报文的 MPLS IP TTL 复制功能。

```
[H3C-mpls] ttl propagate vpn
```

第2章 LDP 配置命令

2.1 LDP 配置命令

2.1.1 debugging mpls ldp

【命令】

debugging mpls ldp {{ **all** | **main** | **advertisement** | **session** | **pdu** | **notification** } [**interface** *interface-type interface-number*] | **remote** }

undo debugging mpls ldp { **all** | **main** | **advertisement** | **session** | **pdu** | **notification** } [**interface** *interface-type interface-number*] | **remote** }

【视图】

用户视图

【参数】

all：显示所有和 LDP 相关的调试信息。

main：显示 LDP 主任务的调试信息。

advertisement：显示处理 LDP 通告消息过程中的调试信息。

session：显示处理 LDP 会话过程中的调试信息

pdu：显示处理 PDU 数据包过程中的调试信息。

notification：显示处理通知消息过程中的调试信息。

remote：显示所有 remote peer 的调试信息。

interface *interface-type interface-number*：显示指定接口的所有的调试信息。

【描述】

debugging mpls ldp 命令用来打开 LDP 各种消息的调试开关，**undo debugging mpls ldp** 命令用来关闭 LDP 各种消息的调试开关。

查看 LDP 的各种调试信息，建议用户谨慎使用。

【举例】

打开 LDP 的调试开关。

```
<H3C> debugging mpls ldp all
```

2.1.2 display mpls ldp

【命令】

display mpls ldp

【视图】

所有视图

【参数】

无

【描述】

display mpls ldp 命令用来显示 LDP 及 LSR 的信息。

缺省情况下，显示 LDP 及 LSR 的信息

相关配置可参考命令 **mpls ldp**，**mpls ldp hops-count**，**mpls ldp loop-detection**，**mpls ldp path-vectors**。

【举例】

显示 LDP 及 LSR 的信息。

```
[H3C] display mpls ldp
```

2.1.3 display mpls ldp buffer-info

【命令】

display mpls ldp buffer-info

【视图】

所有视图

【参数】

无

【描述】

display mpls ldp buffer-info 命令用来显示 LDP 的 **buffer** 信息。

【举例】

显示 LDP 的 **buffer** 信息。

```
[H3C] display mpls ldp buffer-info
-------------------------------------------------------------
Buffer-Name     Buffer-ID    Buffer-Size  Total-Count  Free-Count
```

```
-------------------------------------------------------------
ENTITY          0           292         199         195
LOCAL-IF        1           36          200         196
PEER-IF         2           40          201         195
PDU             3           204         249         249
ADJACENCY       4           56          201         198
PEER-INF        5           116         201         198
SESSION         6           176         201         198
US-BLK          7           264         1052        1028
DS-BLK          8           240         1052        1042
FEC             9           40          1042        1032
US-LIST         10          16          1052        1028
TRIG-BLK        11          56          2076        2071
LABEL-RANGE     12          20          198         198
CR-TUNNEL       13          124         128         128
ER-HOP          14          40          4096        4096
IF-MSG          15          24          9999        9999
-------------------------------------------------------------
Buffer no error.
```

2.1.4 display mpls ldp interface

【命令】

display mpls ldp interface

【视图】

所有视图

【参数】

无

【描述】

display mpls ldp interface 命令用来显示使能了 LDP 的接口信息。

相关配置可参考命令 **mpls ldp enable**，**display mpls ldp session**。

【举例】

显示使能了 LDP 的接口信息

```
[H3C-Ethernet3/0/0] display mpls ldp interface
```

2.1.5 display mpls ldp lsp

【命令】

display mpls ldp lsp

【视图】

所有视图

【参数】

无

【描述】

display mpls ldp lsp 命令用来显示 LDP 协议建立好的 LSP 的相关信息。

相关配置可参考命令 **display mpls lsp**。

【举例】

显示 LSP。

```
[H3C-Ethernet3/0/0] display mpls ldp lsp
```

2.1.6 display mpls ldp peer

【命令】

display mpls ldp peer

【视图】

所有视图

【参数】

无

【描述】

display mpls ldp peer 命令用来显示邻接体信息。

缺省情况下，显示所有邻接体信息。

【举例】

显示邻接体信息。

```
[H3C] display mpls ldp peer
```

2.1.7 display mpls ldp remote

【命令】

display mpls ldp remote

【视图】

所有视图

【参数】

无

【描述】

display mpls ldp remote 命令用来显示配置的 remote peer 信息。

缺省情况下，显示所有配置的 remote-peer 信息。

相关配置可参考命令 **mpls ldp remote，remote-peer**。

【举例】

显示配置的 remote-peer 信息。

```
[H3C] display mpls ldp remote
```

2.1.8 display mpls ldp session

【命令】

display mpls ldp session

【视图】

所有视图

【参数】

无

【描述】

display mpls ldp session 命令用来显示与对等实体会话。

缺省情况下，显示与对等实体会话。

相关配置可参考命令 **mpls ldp enable**。

【举例】

显示与对等实体的会话。

```
[H3C] display mpls ldp session
Local LDP ID: 1.1.1.9:5;   Peer LDP ID: 4.4.4.9:0
```

```
TCP Connection: 1.1.1.9 <- 4.4.4.9
Session State: Operational
Session Role: Passive
Session existed time:
Basic Hello Packets Sent/Received: 85/67
KeepAlive Packets Sent/Received: 1/1
Negotiated Keepalive hold time: 60   Peer PV Limit: 0
LDP Basic Discovery Source((A) means active):
Ethernet1/0/1.3(A)            Ethernet1/0/1.2
Ethernet1/0/1.1
```

显示信息“Ethernet1/0/1.3(A)”中的（A）表示此接口为主用接口。

2.1.9 mpls ldp

【命令】

mpls ldp

undo mpls ldp

【视图】

系统视图

【参数】

无

【描述】

mpls ldp 命令用来使能 LDP 协议，**undo mpls ldp** 命令用来禁止 LDP 协议。

缺省情况下，LDP 协议未启动。

使能 LDP 前需要首先使能 MPLS，并且配置 LSR ID。

相关配置可参考命令 **mpls lsr-id**。

【举例】

使能 LDP 协议。

```
[H3C] mpls ldp
```

2.1.10 mpls ldp enable

【命令】

mpls ldp enable

mpls ldp disable

【视图】

接口视图

【参数】

无

【描述】

mpls ldp enable 命令用来在接口上使能 LDP 协议，**mpls ldp disable** 命令用来在接口上禁止 LDP 协议。

缺省情况下，接口未使能 LDP 协议。

首先要使能 LDP 协议，然后才可以配置接口使能。接口使能 LDP 协议后，就开始对等体发现和会话建立过程。

【举例】

接口使能 LDP 协议。

```
[H3C-Ethernet3/0/0] mpls ldp enable
```

2.1.11 mpls ldp hops-count

【命令】

mpls ldp hops-count *hop-mumber*

undo mpls ldp hops-count

【视图】

系统视图

【参数】

hop-mumber：环路检测最大跳数的值，取值范围为 1～32。

【描述】

mpls ldp hops-count 命令用来设置环路检测最大跳数，**undo mpls ldp hops-count** 命令用来恢复缺省值。

缺省情况下，环路检测最大跳数的缺省值为 32。

此配置命令应该在所有接口 LDP 使能之前配置，其值的大小决定 LSP 建立过程中检测到环路的快慢程度，此值应该根据实际的组网情况决定。

相关配置可参考命令 **mpls ldp loop-detection**，**mpls ldp path-vector**。

【举例】

设置环路检测最大跳数为 22。

```
[H3C] mpls ldp hops-count 22
```

设置环路检测最大跳数为缺省值 32

```
[H3C] undo mpls ldp hops-count
```

2.1.12 mpls ldp loop-detect

【命令】

mpls ldp loop-detect

undo mpls ldp loop-detect

【视图】

系统视图

【参数】

无

【描述】

mpls ldp loop-detect 命令用来打开环路检测功能，**undo mpls ldp loop-detect** 命令用来关闭环路检测。

缺省情况下，系统不进行环路检测。

此配置需要在所有接口没有 ldp 使能之前进行配置。

相关配置可参考命令 **mpls ldp hops-count**，**mpls ldp path-vectors**。

【举例】

打开环路检测

```
[H3C] mpls ldp loop-detect
```

关闭环路检测

```
[H3C] undo mpls ldp loop-detect
```

2.1.13 mpls ldp password

【命令】

mpls ldp password { **cipher** | **simple** } *password*

undo mpls ldp password

【视图】

接口视图，remote-peer 视图

【参数】

cipher：以密文方式（MD5）发送口令。

simple：以明文方式发送。

password：用户口令。

【描述】

mpls ldp password 命令用来配置 LDP 验证方式，**undo mpls ldp password** 命令用来取消该配置。

当采用 **simple** 明文密码时，*password* 为明文验证字，长度为 1～16 个字符。

当采用 **cipher** 密文密码时，*password* 为密文验证字。如果以明文形式输入，长度为 1～16 个字符，如：1234567；如果以密文形式输入，长度必须为 24，并且必须是密文形式，如：_(TT8F]Y\5SQ=^Q`MAF4<1!!。

【举例】

配置 LDP 验证方式为明文，口令 123。

```
[H3C-Ethernet0/0/0.1] mpls ldp password simple 123
```

2.1.14 mpls ldp path-vectors

【命令】

mpls ldp path-vectors *pv-number*

undo mpls ldp path-vectors

【视图】

系统视图

【参数】

pv-number：配置的路径向量最大值，取值范围为 1～32。

【描述】

mpls ldp path-vectors 命令用来设置路径向量最大值，**undo mpls ldp path-vectors** 命令用来恢复路径向量最大值。

缺省情况下，*pv-number* 缺省值为 32。

此配置命令应该在所有接口 LDP 使能之前配置，其值的大小决定 LSP 建立过程中检测到环路的快慢程度，此值应该根据实际的组网情况决定。

相关配置可参考命令 **mpls ldp loop-detection**，**mps ldp hops-count**。

【举例】

设置路径向量最大值为 23

```
[H3C] mpls ldp path-vectors 23
```

恢复路径向量最大值

```
[H3C] undo mpls ldp path-vectors
```

2.1.15 mpls ldp remote-peer

【命令】

mpls ldp remote-peer *Index*

undo mpls ldp remote-peer *Index*

【视图】

系统视图或 Remote-peer 视图

【参数】

Index：为 remote peer 实体的索引，主要用来标识一个 entity。取值范围为 0～99。

【描述】

mpls ldp remote-peer 命令用来创建 Remote-peer 实体并进入 Remote-peer 视图，**undo mpls ldp remote-peer** 命令用来删除 Remote-peer 实体。

通过配置此命令，可以用创建 remote peer，从而建立 remote session。

相关配置可参考命令 remote-peer。

【举例】

创建一个 remote-peer。

```
[H3C] mpls ldp remote-peer 22
[H3C-mpls-remote22]
```

删除一个 remote-peer。

```
[H3C-mpls-remote22] undo mpls ldp remote-peer 22
[H3C]
```

2.1.16 mpls ldp reset-session

【命令】

mpls ldp reset-session *peer-address*

【视图】

接口视图

【参数】

peer-address：对应的对端 LDP Peer 地址（IP 地址形式）。

【描述】

mpls ldp reset-session 命令用来对接口上某一个指定的会话进行复位操作。

当在接口上配置了 LDP，并建立起 LDP 会话之后，可以在接口下通过这条命令对该接口上某一个指定的会话进行复位操作，只需指明要复位的会话对应的 Peer 的地址即可。

相关配置可参考命令 **mpls ldp**，**mpls ldp enable**。

【举例】

对接口 Ethernet0/0/0 上的会话进行复位操作。

```
[H3C-Ethernet0/0/0] mpls ldp reset-session 10.1.1.1
```

2.1.17 mpls ldp timer

【命令】

mpls ldp timer { **session-hold** *session-holdtime* | **hello** *hello-holdtime* }

undo mpls ldp timer { **session-hold** | **hello** }

【视图】

接口视图

【参数】

hello *hello-holdtime*：hello 保持定时器的保持时间，即超时时间。单位为秒，取值范围为 6～65535。缺省情况下，*hello-holdtime* 的缺省值为 15 秒。

session-hold *session-holdtime*：session 保持定时器发送 session 报文的间隔时间，单位为秒，取值范围为 1～65535。缺省情况下，*session-holdtime* 的缺省值为 60 秒。

【描述】

mpls ldp timer 命令用来设置 hello 保持定时器和 session 保持定时器的保持时间，**undo mpls ldp timer** 命令用来恢复缺省值。

hello 保持定时器超时表示与邻居（peer)的邻接关系（adjacent）Down 掉了，session 保持定时器超时表示于邻居（peer）的会话关系（session） Down 掉了。

一般情况下 hello/keepalive 报文发送间隔是 hello 保持定时器/session 保持定时器超时时间的三分之一。

相关配置可参考命令 **mpls ldp**，**mpls ldp enable**。

【举例】

修改 hello 定时器的保持时间。

```
[H3C-Ethernet3/0/0] mpls ldp timer hello 30
```

2.1.18 mpls ldp timer targeted-hello

【命令】

mpls ldp timer targeted-hello { **interval** *time* **| holdtime** *time* }

undo mpls ldp timer targeted-hello { **interval | holdtime** }

【视图】

remote-peer 视图

【参数】

interval *time*：指定 hello 报文间隔。

holdtime *time*：指定 hello 报文的保持时间。

【描述】

mpls ldp timer targeted-hello 命令用来配置远程 LDP 对等体的 hello 计时器参数，**undo mpls ldp timer targeted-hello** 命令用来恢复计时器的缺省值。

缺省情况下，hello 报文间隔为 13 秒，保持时间为 45 秒。

【举例】

配置 hello 报文间隔为 10 秒。

```
[H3C] mpls ldp remote-peer 1
[H3C-mpls-remote1] mpls ldp timer targeted-hello interval 10
```

2.1.19 mpls ldp timer targeted-session-hold

【命令】

mpls ldp timer targeted-session-hold { **interval** *time* **| holdtime** *time* }

undo mpls ldp timer targeted-session-hold { **interval | holdtime** }

【视图】

remote-peer 视图

【参数】

interval *time*：指定会话 keepalive 报文间隔。

holdtime *time*：指定会话 keepalive 报文的保持时间。

【描述】

mpls ldp timer targeted-session-hold 命令用来配置远程 LDP 对等体的会话 keepalive 计时器参数，**undo mpls ldp timer targeted-session-hold** 命令用来恢复计时器的缺省值。

缺省情况下，keepalive 报文间隔为 24 秒，保持时间为 60 秒。

【举例】

配置会话 keepalive 报文间隔为 20 秒。

```
[H3C] mpls ldp remote-peer 1
[H3C-mpls-remote1] mpls ldp timer targeted-session-hold interval 20
```

2.1.20 mpls ldp transport-ip

【命令】

mpls ldp transport-ip { **interface** | *ip-address* }

undo mpls ldp transport-ip

【视图】

接口视图

【参数】

interface：用本接口的 IP 地址作为传输地址。

Ip-address：用此地址作为传输地址。

【描述】

mpls ldp transport-ip 命令用来配置 LDP 会话的传输地址，**undo mpls ldp transport-ip** 命令用来恢复缺省的 LDP 传输地址。

缺省情况下，传输地址为 LSR 的 LSR ID。一般情况下 LSR ID 为某一个 loopback 接口的地址，对端应该有到此 loopback 接口地址的路由，这样才能成功建立会话。

对于 remote peer 的情况，不支持传输地址可配置，其传输地址一定为 LSR 的 ID。

对于 local peer 情况下可以使用本接口的地址或者 LSR 的 Router ID 作为传输地址。

当两个 LSR 邻居之间有多条链路直接相连并且都使能 mpls ldp 时，要求使能 mpls ldp 的多个链路必须配置相同的传输地址，建议采用缺省的 lsr-id 作为传输地址，否则将可能导致 ldp 会话无法稳定建立。

【举例】

使用本接口的地址作为传输地址。

```
[H3C-Ethernet0/0/0] mpls ldp transport-ip interface
```

使用另外接口的地址作为传输地址。

```
[H3C-Ethernet0/0/0] mpls ldp transport-ip 10.1.11.2
```

2.1.21 remote-ip

【命令】

remote-ip *ip-address*

【视图】

remote-peer 视图

【参数】

ip-address：remote peer 的 ip 地址。

【描述】

remote-ip 命令用来配置 remote-ip 地址。此地址应该是对端 lsr 的 lsr id，对于 remote，由于传输地址都是用的 lsr id，故最后两个 remote peer 之间通过其 lsr id 作为建立 tcp 连接的传输地址。

remote-peer 命令主要用于扩展发现模式，以便与链路不直接相连的对等体建立会话。

相关配置可参考命令 **mpls ldp remote-peer**。

【举例】

配置 remote-peer 地址。

```
[H3C] mpls ldp remote-peer 12
[H3C-mpls-remote12] remote-ip 192.168.1.1
```

目 录

第 1 章 L2TP配置命令 1-1
1.1 L2TP配置命令 1-1
1.1.1 allow l2tp 1-1
1.1.2 debugging l2tp 1-2
1.1.3 display l2tp session 1-3
1.1.4 display l2tp tunnel 1-4
1.1.5 display l2tp user 1-5
1.1.6 display ppp access-control 1-6
1.1.7 interface virtual-template 1-7
1.1.8 l2tp enable 1-8
1.1.9 l2tp-auto-client enable 1-8
1.1.10 l2tp-group 1-9
1.1.11 l2tpmoreexam enable 1-9
1.1.12 mandatory-chap 1-10
1.1.13 mandatory-lcp 1-11
1.1.14 ppp access-control enable 1-11
1.1.15 ppp access-control match-fragments 1-12
1.1.16 reset l2tp session 1-13
1.1.17 reset l2tp tunnel 1-13
1.1.18 reset l2tp user 1-14
1.1.19 session idle-time 1-14
1.1.20 start l2tp 1-15
1.1.21 start l2tp tunnel 1-16
1.1.22 tunnel authentication 1-17
1.1.23 tunnel avp-hidden 1-17
1.1.24 tunnel flow-control 1-18
1.1.25 tunnel keepstanding 1-18
1.1.26 tunnel name 1-19
1.1.27 tunnel password 1-20
1.1.28 tunnel timer hello 1-20
第 2 章 GRE配置命令 2-1
2.1 GRE配置命令 2-1
2.1.1 debugging tunnel 2-1
2.1.2 destination 2-1
2.1.3 display interface tunnel 2-2
2.1.4 gre checksum 2-4
2.1.5 gre key 2-4
2.1.6 interface tunnel 2-5
2.1.7 keepalive 2-6
2.1.8 source 2-6

2.1.9 tunnel-protocol gre 2-7
第 3 章 IPsec配置命令 3-1
3.1 IPsec配置命令 3-1
3.1.1 ah authentication-algorithm 3-1
3.1.2 debugging ike dpd 3-2
3.1.3 debugging ipsec 3-2
3.1.4 display ike dpd 3-3
3.1.5 display ipsec fragment buffer-chain 3-4
3.1.6 display ipsec fragment statistics 3-5
3.1.7 display ipsec policy 3-6
3.1.8 display ipsec policy-template 3-9
3.1.9 display ipsec proposal 3-10
3.1.10 display ipsec sa 3-11
3.1.11 display ipsec statistics 3-14
3.1.12 display ipsec tunnel 3-15
3.1.13 dpd 3-16
3.1.14 encapsulation-mode 3-16
3.1.15 esp authentication-algorithm 3-17
3.1.16 esp encryption-algorithm 3-18
3.1.17 ike dpd 3-19
3.1.18 interval-time 3-20
3.1.19 ipsec fragment-chain 3-20
3.1.20 ipsec fragment-chain timeout 3-21
3.1.21 ipsec policy（接口视图） 3-21
3.1.22 ipsec policy（系统视图） 3-22
3.1.23 ipsec policy-template 3-24
3.1.24 ipsec proposal 3-25
3.1.25 ipsec sa global-duration 3-26
3.1.26 pfs 3-27
3.1.27 proposal 3-28
3.1.28 reset ipsec fragment buffer-chain 3-29
3.1.29 reset ipsec fragment statistics 3-29
3.1.30 reset ipsec sa 3-29
3.1.31 reset ipsec statistics 3-31
3.1.32 sa authentication-hex 3-31
3.1.33 sa duration 3-33
3.1.34 sa encryption-hex 3-34
3.1.35 sa spi 3-35
3.1.36 sa string-key 3-36
3.1.37 security acl 3-38
3.1.38 time-out 3-39
3.1.39 transform 3-39
3.1.40 tunnel local 3-41
3.1.41 tunnel remote 3-41
3.2 加密卡配置命令 3-42

3.2.1 debugging encrypt-card host 3-42
3.2.2 display encrypt-card fast-switch 3-43
3.2.3 display interface encrypt 3-44
3.2.4 encrypt-card backuped 3-45
3.2.5 encrypt-card fast-switch 3-45
3.2.6 interface encrypt 3-46
3.2.7 ipsec card-proposal 3-47
3.2.8 reset counters interface encrypt 3-48
3.2.9 reset encrypt-card fast-switch 3-48
3.2.10 reset encrypt-card sa 3-49
3.2.11 reset encrypt-card statistics 3-49
3.2.12 reset encrypt-card syslog 3-50
3.2.13 snmp-agent trap enable encrypt-card 3-51
3.2.14 use encrypt-card 3-51

第 4 章 IKE配置命令 4-1

4.1 IKE配置命令 4-1
4.1.1 authentication-algorithm 4-1
4.1.2 authentication-method 4-1
4.1.3 debugging ike 4-2
4.1.4 dh 4-3
4.1.5 display ike peer 4-4
4.1.6 display ike proposal 4-4
4.1.7 display ike sa 4-5
4.1.8 encryption-algorithm 4-6
4.1.9 exchange-mode 4-7
4.1.10 id-type 4-8
4.1.11 ike encrypt-card dh-computation disabled 4-9
4.1.12 ike local-name 4-9
4.1.13 ike next-payload check disabled 4-10
4.1.14 ike peer 4-10
4.1.15 ike-peer 4-11
4.1.16 ike proposal 4-11
4.1.17 ike sa keepalive-timer interval 4-13
4.1.18 ike sa keepalive-timer timeout 4-13
4.1.19 ike sa nat-keepalive-timer interval 4-14
4.1.20 local 4-15
4.1.21 local-address 4-15
4.1.22 nat traversal 4-16
4.1.23 pre-shared-key 4-17
4.1.24 peer 4-17
4.1.25 remote-address 4-18
4.1.26 remote-name 4-18
4.1.27 reset ike sa 4-19
4.1.28 sa duration 4-20

第 5 章 动态VPN配置命令 5-1
5.1 动态VPN配置命令 5-1
5.1.1 algorithm-suite 5-1
5.1.2 authentication-client method 5-2
5.1.3 authentication-server method 5-2
5.1.4 data algorithm-suite 5-3
5.1.5 data ipsec-sa duration 5-4
5.1.6 debugging dvpn 5-4
5.1.7 display dvpn ipsec-sa 5-5
5.1.8 display dvpn map 5-6
5.1.9 display dvpn session 5-7
5.1.10 display dvpn info 5-7
5.1.11 display dvpn online-user 5-9
5.1.12 dvpn class 5-9
5.1.13 dvpn client register-dumb 5-10
5.1.14 dvpn client register-interval 5-10
5.1.15 dvpn client register-retry 5-11
5.1.16 dvpn dvpn-id 5-11
5.1.17 dvpn interface-type 5-12
5.1.18 dvpn policy（系统视图） 5-13
5.1.19 dvpn policy（Tunnel接口视图） 5-13
5.1.20 dvpn register-type 5-14
5.1.21 dvpn security 5-15
5.1.22 dvpn server 5-15
5.1.23 dvpn server authentication-client method 5-16
5.1.24 dvpn server map age-time 5-17
5.1.25 dvpn server pre-shared-key 5-17
5.1.26 dvpn service enable 5-18
5.1.27 local-user 5-19
5.1.28 public-ip 5-19
5.1.29 pre-shared-key 5-20
5.1.30 private-ip 5-20
5.1.31 reset dvpn all 5-21
5.1.32 reset dvpn map 5-21
5.1.33 reset dvpn session 5-22
5.1.34 reset dvpn statistics 5-22
5.1.35 session algorithm-suite 5-23
5.1.36 session idle-time 5-24
5.1.37 session keepalive-interval 5-24
5.1.38 session setup-interval 5-25
5.1.39 tunnel-protocol dvpn 5-25
第 6 章 BGP/MPLS VPN配置命令 6-1
6.1 BGP/MPLS VPN配置命令 6-1
6.1.1 apply access-vpn vpn-instance 6-1
6.1.2 apply mpls-label 6-1

6.1.3 description 6-2
6.1.4 display bgp routing label 6-2
6.1.5 display bgp vpnv4 6-3
6.1.6 display ip routing-table vpn-instance 6-5
6.1.7 display ip vpn-instance 6-6
6.1.8 display mpls l3vpn-lsp 6-6
6.1.9 display ospf sham-link 6-7
6.1.10 domain-id 6-8
6.1.11 if-match mpls-label 6-9
6.1.12 import-route ospf 6-9
6.1.13 ip binding vpn-instance 6-10
6.1.14 ip route-static vpn-instance 6-11
6.1.15 ip vpn-instance 6-12
6.1.16 ipv4-family 6-12
6.1.17 ospf vpn-instance 6-13
6.1.18 peer default-route-advertise 6-15
6.1.19 peer label-route-capability 6-16
6.1.20 peer next-hop-invariable 6-16
6.1.21 policy vpn-target 6-17
6.1.22 route-distinguisher 6-18
6.1.23 route-tag 6-19
6.1.24 routing-table limit 6-20
6.1.25 sham-link 6-21
6.1.26 vpn-instance-capability simple 6-22
6.1.27 vpn-target 6-23

第1章 L2TP 配置命令

1.1 L2TP 配置命令

1.1.1 allow l2tp

【命令】

allow l2tp virtual-template *virtual-template-number* **remote** *remote-name* [**domain** *domain-name*]

undo allow

【视图】

L2TP 组视图

【参数】

virtual-template-number：指定用于创建新的虚拟访问接口（virtual access interface）时所用的虚接口模板，取值范围是整数 0～1023。

remote-name：指定发起连接请求的隧道对端的名称，对大小写有区别，取值为字符串，长度为 1～30。

domain-name：指定企业的名称，取值为字符串，长度为 1～30。

【描述】

allow l2tp 命令用来指定接受呼叫时隧道对端的名称及所使用的 Virtual-Template，**undo allow** 命令用来取消隧道对端的名称及所使用的 Virtual-Template。

缺省情况下，为禁止接受呼入。

此命令在 LNS 端使用。

在 L2TP 多域应用中，必须配置参数 *domain-name*。

使用 L2TP 组号 1 时（缺省的 L2TP 组号），可以不指定通道对端名 *remote-name*，在组 1 下进行配置时，本命令的格式为：

allow l2tp virtual-template *virtual-template-number* [**remote** *remote-name*] [**domain** *domain-name*]

如果在 L2TP 组 1 的配置模式下，仍指定对端名称，则 L2TP 组 1 不作为缺省的 L2TP 组。如在 Windows 2000 beta 2 版本中，VPN 连接的本端名称为 NONE，则防火墙收到的对端名称为 NONE。为了接收这种不知名的对端发起的通道请求连接，或者用于测试目的，可以设置一个缺省的 L2TP 组。

命令 **allow l2tp** 使用在 LNS 侧，如果配置了通道对端名称，必须确保通道对端的名称和 LAC 侧配置的本端名称一致。

相关配置可参考命令 **l2tp-group**。

【举例】

接受名称为 AS8010 的对端（LAC）发起的 L2TP 隧道连接请求，并在 virtual-template 1 上创建 virtual-access 接口。

```
[H3C-l2tp2] allow l2tp virtual-template 1 remote AS8010
```

将 L2TP 组 1 作为缺省的 L2TP 组，接受任何对端发起的 L2TP 通道连接请求，并根据 virtual-template 1 创建 virtual-access 接口。

```
[H3C] l2tp-group 1
[H3C-l2tp1] allow l2tp virtual-template 1
```

1.1.2 debugging l2tp

【命令】

debugging l2tp { **all** | **control** | **dump** | **error** | **event** | **hidden** | **payload** | **time-stamp** }

undo debugging l2tp { **all** | **control** | **dump** | **error** | **event** | **hidden** | **payload** | **time-stamp** }

【视图】

用户视图

【参数】

all：表示打开所有 L2TP 调试信息开关。

control：表示打开控制报文调试开关。

dump：表示打开 PPP 报文调试开关。

error：表示打开差错信息的调试开关。

event：表示打开事件调试信息开关。

hidden：表示打开隐藏 AVP 的调试开始信息开关。

payload：表示打开 L2TP 数据报文调试开关。

time-stamp：表示打开显示时间戳的调试开关。

【描述】

debugging l2tp 命令用来打开 L2TP 调试信息开关，**undo debugging l2tp** 命令用来关闭 L2TP 调试信息开关。

【举例】

打开所有 L2TP 调试信息开关。

```
<H3C> debugging l2tp all
```

1.1.3 display l2tp session

【命令】

display l2tp session

【视图】

所有视图

【参数】

无

【描述】

display l2tp session 命令用来显示当前的 L2TP 会话的信息。

该命令的输出信息，可以帮助用户确定当前建立的 L2TP 会话信息。

相关配置可参考命令 **display l2tp tunnel**。

【举例】

显示当前 L2TP 会话信息。

```
<H3C> display l2tp session
LocalSID      RemoteSID    LocalTID IdleTimeLeft
       1              1           2          600
Total session = 1
```

表1-1 display L2tp session 显示信息的域描述

域	描述
Total session	Session 的数目
LocalSID	本端唯一标识一个会话的数值
RemoteSID	对端唯一标识一个会话的数值
LocalTID	隧道的本端标识号
Idle-Time-Left	会话距离超时挂断剩余时间

1.1.4 display l2tp tunnel

【命令】

display l2tp tunnel

【视图】

所有视图

【参数】

无

【描述】

display l2tp tunnel 命令用来显示当前的 L2TP 隧道的信息。

该命令的输出信息，可以帮助用户确定当前所建立的 L2TP 隧道信息。

相关配置可参考命令 **display l2tp session**。

【举例】

显示当前 L2TP 隧道信息。

```
<H3C> display l2tp tunnel
LocalTID RemoteTID RemoteAddress   Port  Sessions  RemoteName KeepStanding
       2     22849      11.1.1.1   1701         1         lns          YES
 Total tunnel = 1
```

表1-2 display L2tp tunnel 显示信息的域描述

域	描述
Total tunnel	Tunnel 的数目
LocalTID	本端唯一标识一个隧道的数值
RemoteTID	对端唯一标识一个隧道的数值
RemoteAddress	对端的 IP 地址
Port	对端的端口号
Sesssions	此隧道上的会话数目
RemoteName	对端的名称
KeepStanding	是否设置了连接保持功能

📖 **说明：**

防火墙作为 LNS 时，当存在域用户和非域用户时，对于非域用户触发的隧道，在设备上可能会显示错误的 L2TP 信息。

1.1.5 display l2tp user

【命令】

display l2tp user

【视图】

所有视图

【参数】

无

【描述】

display l2tp user 命令用来显示当前 L2TP 用户的信息。

相关配置可参考命令 **display l2tp tunnel**，**display l2tp session**。

【举例】

显示当前 L2TP 会话信息。

```
<H3C> display l2tp user
User Name        LocalSID  RemoteSID  LocalTID
     w@h3c               1          1         2

 Total user = 1
```

表1-3 display l2tp user 显示信息的域描述

域	描述
User Name	用户名
LocalSID	会话连接的本端标识号
RemoteSID	会话连接的对端标识号
LocalTID	隧道的本端标识号
Total user	用户的数目

1.1.6 display ppp access-control

【命令】

display ppp access-control { **interface** *type number* }

【视图】

任意视图

【参数】

interface *type number*：指定接口类型和接口号，目前只支持 Virtual-Template 接口。

【描述】

display ppp access-control 命令用来显示 VT 接口下 virtual-access 接口的访问控制统计信息。

【举例】

显示 virtual-access 接口的访问控制统计信息。

```
<H3C> display ppp access-control interface Virtual-Template 1
Interface: Virtual-Template1:0
  User Name: mike
  In-bound Policy: acl 3000
  From 2000-04-29 18:47:05  to 2000-04-29 18:47:16
     0 packets, 0 bytes, 0% permitted,
     0 packets, 0 bytes, 0% denied,
     0 packets, 0 bytes, 0% permitted default,
     0 packets, 0 bytes, 0% denied default,
  Totally 0 packets, 0 bytes, 0% permitted,
  Totally 0 packets, 0 bytes, 0% denied.

  Interface: Virtual-Template1:1
  User Name: tim
  In-bound Policy: acl 3001
  From 2000-04-30 18:41:05  to 2000-04-30 18:47:16
     0 packets, 0 bytes, 0% permitted,
     0 packets, 0 bytes, 0% denied,
     0 packets, 0 bytes, 0% permitted default,
     0 packets, 0 bytes, 0% denied default,
  Totally 0 packets, 0 bytes, 0% permitted,
  Totally 0 packets, 0 bytes, 0% denied.
```

表1-4 display ppp access-control 信息显示描述表

域名	描述
Interface	PPP 用户接入的 virtual-access 接口
User Name	PPP 用户名
In-bound Policy	为 PPP 用户创建的包过滤防火墙的 ACL 规则
From xx to xx	防火墙生效的时间段
x packets, x bytes, x% permitted	匹配防火墙 ACL 规则通过的报文数、报文字节数、通过率
x packets, x bytes, x% denied	匹配防火墙 ACL 规则拒绝的报文数、报文字节数、拒绝率
x packets, x bytes, x% permitted default	未匹配防火墙 ACL 规则缺省通过的报文数、报文字节数、通过率
x packets, x bytes, x% denied default	未匹配防火墙 ACL 规则缺省拒绝的报文数、报文字节数、拒绝率
Totally x packets, x bytes, x% permitted	总共通过的报文数、报文字节数、通过率
Totally x packets, x bytes, x% denied	总共拒绝的报文数、报文字节数、拒绝率

1.1.7 interface virtual-template

【命令】

interface virtual-template *virtual-template-number*

undo interface virtual-template *virtual-template-number*

【视图】

系统视图

【参数】

virtual-template-number：标识虚接口模板序号，取值为整数，范围是 0～1023。

【描述】

interface virtual-template 命令用来创建虚拟模板接口，**undo interface virtual-template** 命令用来删除虚拟模板接口。

缺省情况下，系统没有创建虚拟模板接口。

虚拟模板接口主要用于配置防火墙在运行过程中动态创建的虚接口的工作参数，如 L2TP 逻辑接口。

相关配置可参考命令 **allow l2tp**。

【举例】

创建虚拟模板接口 1 并进入该视图。

```
[H3C] interface virtual-template 1
```

1.1.8 l2tp enable

【命令】

l2tp enable

undo l2tp enable

【视图】

系统视图

【参数】

无

【描述】

l2tp enable 命令用来启用 L2TP 功能，**undo l2tp enable** 命令用来禁止 L2TP 功能。

缺省情况下，L2TP 功能被禁止。

相关配置可参考命令 **l2tp-group**。

【举例】

在防火墙上启用 L2TP 功能。

```
[H3C] l2tp enable
```

1.1.9 l2tp-auto-client enable

【命令】

l2tp-auto-client enable

undo l2tp-auto-client enable

【视图】

虚拟模板接口视图

【参数】

无

【描述】

l2tp-auto-client enable 命令用来使能 LAC 客户端建立 L2TP 隧道。**undo l2tp-auto-client enable** 命令用来取消 LAC 客户端建立 L2TP 隧道。

【举例】

进入虚拟模板接口视图。

```
[H3C] interface virtual-template 1
```

使能 LAC 客户端建立 L2TP 隧道。

```
[H3C-Virtual-Template1] l2tp-auto-client enable
```

1.1.10 l2tp-group

【命令】

l2tp-group *group-number*

undo l2tp-group *group-number*

【视图】

系统视图

【参数】

group-number：标识 L2TP 组号，取值为整数，范围为 1～1000。

【描述】

l2tp-group 命令用来创建 L2TP 组，**undo l2tp-group** 命令用来删除 L2TP 组。

缺省情况下，系统没有创建 L2TP 组。

使用 **l2tp-group** 命令创建一个 L2TP 组（L2TP 组 1 可以作为缺省的 L2TP 组）。使用 **undo l2tp-group** 命令删除 L2TP 组后，该组的所有配置信息也将被删除。

相关配置可参考命令 **allow l2tp**，**start l2tp**。

【举例】

创建 L2TP 组 2，并进入 L2TP 组 2 视图。

```
[H3C] l2tp-group 2
[H3C-l2tp2]
```

1.1.11 l2tpmoreexam enable

【命令】

l2tpmoreexam enable

undo l2tpmoreexam enable

【视图】

系统视图

【参数】

无

【描述】

本命令在 LNS 端配置。

l2tpmoreexam enable 命令用来启用 L2TP 多域功能，**undo l2tpmoreexam enable** 命令用来禁止 L2TP 多域功能。

缺省情况下，L2TP 多域功能被禁止。

使用 **l2tpmoreexam enable** 命令启用 L2TP 多域功能，只有启用该功能后才能开展 L2TP 多域业务。

相关配置可参考命令 **l2tp enable**。

【举例】

在防火墙（LNS 端）上启用 L2TP 多域功能。

```
[H3C] l2tp-group 2
```

1.1.12 mandatory-chap

【命令】

mandatory-chap

undo mandatory-chap

【视图】

L2TP 组视图

【参数】

无

【描述】

mandatory-chap 命令用来强制 LNS 与用户端（Client）之间重新进行 CHAP 验证，**undo mandatory-chap** 命令用来禁止 CHAP 的重新验证。

缺省情况下，系统不进行 CHAP 的重新验证。

在 LAC 对用户端进行代理验证后，LNS 对用户端再次进行验证，可以增加安全性。如果使用 **mandatory-chap** 命令，则对于由接入服务器初始化隧道连接的 VPN 的用户端来说，会经过两次验证：一次是用户端在接入服务器端的验证，另一次是用户端在 LNS 端的验证。一些 PPP 用户端可能不支持进行第二次验证，这时，本端的 CHAP 验证会失败。

相关配置可参考命令 **mandatory-lcp**。

【举例】

强制进行 CHAP 验证。

```
[H3C-l2tp1] mandatory-chap
```

1.1.13 mandatory-lcp

【命令】

mandatory-lcp

undo mandatory-lcp

【视图】

L2TP 组视图

【参数】

无

【描述】

mandatory-lcp 命令用来在 LNS 与用户端（Client）之间重新进行链路控制协议（Link Control Protocol）的协商，**undo mandatory-lcp** 命令用来禁止 LCP 的重新协商。

缺省情况下，系统不重新进行 LCP 协商。

对于 NAS-Initialized VPN 的用户端，在一个 PPP 会话开始时，将先和网络接入服务器（NAS）进行 PPP 协商。如果协商通过，则由接入服务器初始化隧道连接，并把与用户端协商收集到的信息传给 LNS；LNS 根据收到的代理验证信息判断用户是否合法。使用 **mandatory-lcp** 命令可以强制 LNS 与用户端重新进行 LCP 协商，这就忽略 NAS 的代理验证信息。如果一些 PPP 用户端可能不支持 LCP 的重新协商，则 LCP 重新协商过程会失败。

相关配置可参考命令 **mandatory-chap**。

【举例】

允许进行 LCP 重新协商。

```
[H3C-l2tp1] mandatory-lcp
```

1.1.14 ppp access-control enable

【命令】

ppp access-control enable

undo ppp access-control enable

【视图】

虚拟模板接口视图

【参数】

无

【描述】

ppp access-control enable 命令用来使能 PPP 基于用户的 EAD 功能，**undo ppp access-control enable** 命令用来关闭 PPP 基于用户的 EAD 功能。

缺省情况下，关闭 PPP 基于用户的 EAD 功能。

【举例】

使能 PPP 基于用户的 EAD 功能。

```
[H3C] interface virtual-template 1
[H3C-Virtual-Template1] ppp access-control enable
```

1.1.15 ppp access-control match-fragments

【命令】

ppp access-control match-fragments { **normally** | **exactly** }

undo ppp access-control match-fragments

【视图】

虚拟模板接口视图

【参数】

normally：设置 VT 接口下所有 virtual-access 接口的包过滤防火墙的分片匹配模式为标准模式。

exactly：设置 VT 接口下所有 virtual-access 接口的包过滤防火墙的分片匹配模式为精确模式。

【描述】

ppp access-control match-fragments 命令用来设置 VT 接口下所有 virtual-access 接口的包过滤防火墙的分片匹配模式，**undo ppp access-control match-fragments** 命令用来恢复分片匹配模式为缺省模式。

关于标准匹配模式和精确匹配模式的介绍请参见命令 **firewall packet-filter** *acl-number*。

缺省情况下，分片匹配模式为标准模式。

相关配置可参考命令 **firewall packet-filter enable**，**firewall packet-filter** *acl-number*，**firewall packet-filter fragments-inspect**。

【举例】

设置 VT1 接口下所有 virtual-access 接口的包过滤防火墙的分片匹配模式为精确匹配。

```
[H3C] interface virtual-template 1
[H3C-Virtual-Template1] ppp access-control match-fragments exactly
```

1.1.16 reset l2tp session

【命令】

reset l2tp session *session-id*

【视图】

用户视图

【参数】

session-id：会话连接的本端标识号。

【描述】

reset l2tp session 命令用于强制断开一个会话连接。当用户再次呼入时，会话可以重新建立。

相关配置可参考命令 **reset l2tp tunnel**。

【举例】

强制断开 L2TP 会话连接。

```
<H3C> reset l2tp session 1
```

1.1.17 reset l2tp tunnel

【命令】

reset l2tp tunnel { **name** *remote-name* | **id** *tunnel-id* }

【视图】

用户视图

【参数】

remote-name：隧道对端的名称。

tunnel-id：隧道本端的标识号。

【描述】

reset l2tp tunnel 命令用来断开指定的隧道（Tunnel）连接，同时断开隧道内的所有会话（session）连接。

reset l2tp tunnel 命令用于强制断开一个隧道连接。当对端用户再次呼入时，隧道可以重新建立。通过指定隧道的对端名称来确定需要断开的隧道连接。如果没有符合条件的隧道连接存在，则对当前的隧道连接没有影响。如果有多个符合条件的隧道连接存在（同一个名称，不同 IP 地址），则断开所有符合条件的隧道连接。指定 *tunnel-id* 时，只断开对应的隧道连接。

相关配置可参考命令 **display l2tp tunnel**。

【举例】

断开对端名称为 AS8010 的 Tunnel 连接。

```
<H3C> reset l2tp tunnel name AS8010
```

1.1.18 reset l2tp user

【命令】

reset l2tp user *user-name*

【视图】

用户视图

【参数】

user-name：L2TP 的用户名。

【描述】

reset l2tp user 命令用于强制断开该用户的连接。当用户再次呼入时，可以重新接入。

相关配置可参考命令 **reset l2tp tunnel**，**reset l2tp session**。

【举例】

强制断开当前 L2TP 用户的连接。

```
<H3C> reset l2tp user l2tpuser@h3c
```

1.1.19 session idle-time

【命令】

session idle-time *time*

undo session idle-time

【视图】

L2TP 组视图

【参数】

time：超时时间长度，以秒为单位，取值范围为 0～10000。缺省为 0，表示不超时。

【描述】

session idle-time 命令用来设置 L2TP 会话超时挂断的超时时间，并触发超时挂断功能。**undo session idle-time** 命令用来禁止 L2TP 会话超时断开。

缺省情况下，L2TP 会话不会超时。

【举例】

进入 L2TP 组视图。

```
[H3C] l2tp-group 1
```

设定 L2TP 会话超时挂断时间为 600 秒。

```
[H3C-l2tp1] session idle-time 600
```

1.1.20 start l2tp

【命令】

start l2tp { **ip** *ip-addr* [**ip** *ip-addr*] [**ip** *ip-addr*] **...** } { **domain** *domain-name* | **fullusername** *user-name* }

undo start

【视图】

L2TP 组视图

【参数】

ip *ip-addr*：隧道对端（LNS）的 IP 地址，最多可以设置五个，彼此形成备份 LNS。

domain-name：指定触发连接请求的用户域名，取值为字符串，长度为 1～30。

user-name：指定触发连接请求的用户全名，取值为字符串，长度为 1～80。

【描述】

start l2tp 命令用来指定本端作为 L2TP LAC 端时发起呼叫的触发条件，**undo start l2tp** 命令用来删除指定的触发条件。

此命令在 LAC 端使用。使用此命令指定 LNS 的 IP 地址，并支持多种触发连接请求。

- 可以根据用户域名来发起建立隧道的连接请求。比如用户所在公司的域名为 h3c.com，则可以指定包含 h3c.com 域名的用户为 VPN 用户。

- 可以直接通过用户全名来指定该用户为 VPN 用户。

如果发现是 VPN 用户，则本端（LAC）按照配置的 LNS 的先后顺序向某个 LNS 发送建立 L2TP 隧道的连接请求，当得到 LNS 的接收应答后，该 LNS 就作为隧道的对端；否则 LAC 向下一个 LNS 发起隧道连接请求。

这几种 VPN 用户判定方式之间可能存在冲突的情况，如对全用户名指定的 LNS 地址是 1.1.1.1，而根据域名指定的 LNS 地址为 1.1.1.2，有必要规定一下查找用户的先后顺序。查找的顺序为：先根据完整的用户名查看是否存在根据此用户名指定的 L2TP 组；如果没有找到，再根据域名进行查找。

当配置多个 LNS 时，因客户端 PPP 的超时时间不同，可能会导致不能与后续几个 IP 地址（备份 LNS）建立连接，故建议最多配置两个 LNS。

【举例】

根据域名 h3c.com 来判断 VPN 用户，对应的总部 L2TP 接入服务器的 IP 地址为 202.38.168.1。

```
[H3C-l2tp1] start l2tp ip 202.38.168.1 domain h3c.com
```

1.1.21 start l2tp tunnel

【命令】

start l2tp tunnel

【视图】

L2TP 组视图

【参数】

无

【描述】

start l2tp tunnel 命令用来启动 L2TP LAC 端发起呼叫。

此命令只在 LAC 端使用。

相关命令请参考 **tunnel keepstanding**。

【举例】

启动 LAC 按照配置的 LNS 的先后顺序发送建立 L2TP 隧道的连接请求，即先向地址为 1.1.1.1 的 LNS 发起，没有应答则顺序向下一个地址为 2.2.2.2 的 LNS 发起。

```
[H3C-l2tp1] start l2tp ip 1.1.1.1 ip 2.2.2.2 fullusername vpdnuser
[H3C-l2tp1] start l2tp tunnel
```

⚠ 注意：

该命令需要与 **tunnel keepstanding** 命令配合使用，否则隧道不会被建立。

1.1.22 tunnel authentication

【命令】

tunnel authentication

undo tunnel authentication

【视图】

L2TP 组视图

【参数】

无

【描述】

tunnel authentication 命令用来启用 L2TP 的隧道验证功能，**undo tunnel authentication** 命令用来取消 L2TP 隧道验证功能。

缺省情况下，系统对 L2TP 隧道进行验证。

L2TP 隧道验证是缺省允许的。一般情况下，为了安全起见，隧道两端都需要对对方进行验证。如果为了进行网络的连通性测试或者是接收不知名对端发起的连接，可以不进行隧道验证。

【举例】

设置不验证隧道对端。

```
[H3C-l2tp1] undo tunnel authentication
```

1.1.23 tunnel avp-hidden

【命令】

tunnel avp-hidden

undo tunnel avp-hidden

【视图】

L2TP 组视图

【参数】

无

【描述】

tunnel avp-hidden 命令用来配置对 AVP（Attribute Value Pair，属性值对）数据采用隐藏的方式进行传输，**undo tunnel avp-hidden** 命令用来恢复 AVP 数据的缺省传输方式。

缺省情况下，隧道采用明文方式传输 AVP 数据。

L2TP 协议的一些参数是通过 AVP 数据来传输的，如果用户对这些数据的安全性要求高，可以使用本命令将 AVP 数据的传输方式配置成为隐藏传输。

【举例】

设置 AVP 数据隐含传输。

```
[H3C-l2tp1] tunnel avp-hidden
```

1.1.24 tunnel flow-control

【命令】

tunnel flow-control

undo tunnel flow-control

【视图】

L2TP 组视图

【参数】

无

【描述】

tunnel flow-control 命令用来开启 L2TP 通道流控功能，**undo tunnel flow-control** 命令用来关闭通道流控功能。

缺省情况下，关闭 L2TP 通道流控功能。

使用此命令来开启 L2TP 通道流控功能，以达到流控目的。

【举例】

开启通道流控。

```
[H3C-l2tp1] tunnel flow-control
```

1.1.25 tunnel keepstanding

【命令】

tunnel keepstanding

undo tunnel keepstanding

【视图】

L2TP 组视图

【参数】

无

【描述】

tunnel keepstanding 命令用来配置 L2TP Tunnel 连接保持功能。**undo tunnel keepstanding** 命令用来取消 L2TP Tunnel 连接保持功能。

配置 L2TP Tunnel 连接保持功能后，即使隧道上没有 Session 也不会因超时而挂断。

⚠ 注意：

此命令需要在隧道两端同时配置才会生效。

缺省情况下，未配置隧道连接保持功能。

【举例】

进入 L2TP 组视图。

```
[H3C] l2tp-group 1
```

使能 L2TP Tunnel 连接保持功能。

```
[H3C-l2tp1] tunnel keepstanding
```

1.1.26 tunnel name

【命令】

tunnel name *name*

undo tunnel name

【视图】

L2TP 组视图

【参数】

name：标识隧道本端的名称，取值为字符串，长度为 1～30。

【描述】

tunnel name 命令用来指定隧道本端的名称，**undo tunnel name** 命令用来恢复本端名称为缺省值。

缺省情况下，系统的本端名称为防火墙的系统名称。

当创建一个 L2TP 组时，本端名称将被初始化成防火墙的名称。

LNS 根据 LAC 的 tunnel 名来选择其本端的 L2TP 组，如果 tunnel 名相同，LNS 将以第一个符合配置的组建立隧道。所以若要建立多条隧道，需要配置不同的 tunnel 名。

相关配置可参考命令 **sysname**。

【举例】

设置隧道本端名称为 itsme。

```
[H3C-l2tp1] tunnel name itsme
```

1.1.27 tunnel password

【命令】

tunnel password { **simple** | **cipher** } *password*

undo tunnel password

【视图】

L2TP 组视图

【参数】

simple：密码以明文方式显示。

cipher：密码以密文方式显示。

password：标识隧道验证时使用的密码，取值为字符串，长度为 1～16。

【描述】

tunnel password 命令用来指定隧道验证时的密码，**undo tunnel password** 命令用来取消隧道验证的密码。

缺省情况下，系统的隧道验证密码为空。

【举例】

设置隧道验证的密码为 yougotit，并且以密文方式显示。

```
[H3C-l2tp1] tunnel password cipher yougotit
```

1.1.28 tunnel timer hello

【命令】

tunnel timer hello *hello-interval*

undo tunnel timer hello

【视图】

L2TP 组视图

【参数】

hello-interval：LAC 或 LNS 在没有报文接收时发送 Hello 报文的时间间隔，单位为秒，范围为 60～1000。

【描述】

tunnel timer hello 命令用来设置隧道中 Hello 报文发送时间间隔，**undo tunnel timer hello** 命令用来恢复隧道中 Hello 报文发送时间间隔为缺省值。

缺省情况下，Hello 报文每隔 60 秒发送一次。

在 LNS 和 LAC 侧，可以分别配置不同的 Hello 报文时间间隔。

【举例】

设置发送 Hello 报文的时间间隔为 99 秒

```
[H3C-l2tp1] tunnel timer hello 99
```

第2章 GRE 配置命令

2.1 GRE 配置命令

2.1.1 debugging tunnel

【命令】

debugging tunnel

undo debugging tunnel

【视图】

用户视图

【参数】

无

【描述】

debugging tunnel 命令用来打开 tunnel 调试信息开关，**undo debugging tunnel** 命令用来关闭 tunnel 调试信息开关。

【举例】

打开 tunnel 调试信息开关。

```
<H3C> debugging tunnel
```

2.1.2 destination

【命令】

destination *ip-addr*

undo destination

【视图】

Tunnel 接口视图

【参数】

ip-addr：标识 Tunnel 对端使用的实际物理接口的 IP 地址。

【描述】

destination 命令用来指定 Tunnel 接口进行封装时对添加的 IP 报头填入的目的端 IP 地址，**undo destination** 命令用来删除设置的目的地址。

缺省情况下，系统不指定隧道的目的地址。

指定的隧道目的地址是接收 GRE 报文的实际物理接口的 IP 地址，该地址必须与对端 Tunnel 接口指定的源地址相同，并且要保证到对端物理接口的路由可达。

不能对两个或两个以上使用同种封装协议的 Tunnel 接口配置完全相同的源地址和目的地址。

相关配置可参考命令 **interface tunnel**，**source**。

【举例】

在防火墙 SecPath1 的 Ethernet 0/0/0 接口（IP 地址是 193.101.1.1）和 SecPath2 的 Ethernet 1/0/0 接口（IP 地址是 192.100.1.1）间建立 tunnel 连接。

```
[H3C-Tunnel0] source 193.101.1.1
[H3C-Tunnel0] destination 192.100.1.1
[H3C-Tunnel1] source 192.100.1.1
[H3C-Tunnel1] destination 193.101.1.1
```

2.1.3 display interface tunnel

【命令】

display interface tunnel [*number*]

【视图】

所有视图

【参数】

number：Tunnel 接口的编号，范围 0～1023。

【描述】

display interface tunnel 命令用来显示 Tunnel 接口的工作状态。

执行 **display interface tunnel** 命令显示指定 Tunnel 接口的源地址、目的地址（收发 GRE 报文的实际物理接口地址）、封装模式、识别关键字及端到端校验等信息。

相关配置可参考命令 **source**，**destination**，**gre key**，**gre checksum**，**tunnel-protocol**。

【举例】

显示当前 Tunnel 通道接口信息。

```
<H3C> display interface tunnel 2
Tunnel2 current state :UP
Line protocol current state :DOWN
Description : Tunnel0 Interface
The Maximum Transmit Unit is 64000
Internet Address is 192.168.2.1/24
Encapsulation is TUNNEL, loopback not set
Tunnel source 192.168.0.1 (Ethernet0/0/0), destination 202.38.16.188
Tunnel keepalive disable
Tunnel protocol/transport GRE/IP, key disabled
Checksumming of packets disabled
    Last 300 seconds input:  0 bytes/sec, 0 packets/sec
    Last 300 seconds output:  0 bytes/sec, 0 packets/sec
    0 packets input,  0 bytes
    0 input error
    0 packets output,  0 bytes
    0 output error
```

表2-1 display interface tunnel 2 显示信息的域描述

域	描述
Tunnel2 current state	Tunnel 接口的当前状态
Line protocol current state	Tunnel 接口协议的当前状态
Description	Tunnel 接口描述信息
The Maximum Transmit Unit	Tunnel 接口的 MTU 值
Internet Address	Tunnel 接口的 IP 地址
Encapsulation	封装 GRE 协议形成隧道
Loopback	是否启动回环测试
Tunnel source	Tunnel 源地址
destination	Tunnel 目的地址
Tunnel keepalive	是否启用 Tunnel Keepalive 功能
Tunnel protocol/transport	Tunnel 封装协议和传输协议
key	Tunnel 接口的识别关键字
Checksumming of packets	Tunnel 端到端校验
Last 300 seconds input	离现在最近的 5 分钟内，每秒输入的字节数和报文数
Last 300 seconds output	离现在最近的 5 分钟内，每秒输出的字节数和报文数
packets input, bytes	总计输入的报文数和字节数
packets output, bytes	总计输出的报文数和字节数

域	描述
input error	在所有输入的报文中，出现错误的报文数
output error	在所有输出的报文中，出现错误的报文数

2.1.4 gre checksum

【命令】

gre checksum

undo gre checksum

【视图】

Tunnel 接口视图

【参数】

无

【描述】

gre checksum 命令用来设置隧道两端进行端到端校验，从而验证报文的正确性，并丢掉验证不通过的报文，**undo gre checksum** 命令用来取消校验。

缺省情况下，禁止 Tunnel 两端进行端到端校验。

隧道两端可以根据实际应用需要，配置校验和或禁止校验和。如果本端配置了校验和而对端没有配置，则本端将不会对接收到的报文进行校验和检查，但对发送的报文计算校验和；相反，如果本端没有配置校验和而对端已配置，则本端将对从对端发来的报文进行校验和检查，但对发送的报文不计算校验和。

相关配置可参考命令 **interface tunnel**。

【举例】

防火墙 SecPath1 和 SecPath2 之间建立隧道，在隧道两端设置校验。

```
[H3C-Tunnel3] gre checksum
[H3C-Tunnel2] gre checksum
```

2.1.5 gre key

【命令】

gre key *key-number*

undo gre key

【视图】

Tunnel 接口视图

【参数】

key-number：标识隧道两端的识别关键字，取值为整数，范围为 0～4294967295。

【描述】

gre key 命令用来设置 Tunnel 接口的识别关键字，通过这种弱安全机制防止错误识别、接收其它地方来的报文，**undo gre key** 命令用来取消当前配置。

缺省情况下，系统不设置隧道的识别关键字。

如果在隧道两端设置了 *key-number*，则要求在一条隧道的两端必须指定相同的 *key-number*；或隧道两端都不设置 *key-number*。

相关配置可参考命令 **interface tunnel**。

【举例】

防火墙 SecPath1 和 SecPath2 之间建立隧道，设置隧道的识别关键字。

```
[H3C-Tunnel3] gre key 123
[H3C-Tunnel2] gre key 123
```

2.1.6 interface tunnel

【命令】

interface tunnel *numbe*

undo interface tunnel *number*

【视图】

系统视图

【参数】

number：Tunnel 接口号，范围 0～1023。

【描述】

interface tunnel 命令用来创建一个 Tunnel 接口，并进入该 Tunnel 接口视图，**undo interface tunnel** 命令用来删除指定的 Tunnel 接口。

缺省情况下，系统无 Tunnel 接口。

执行 **interface tunnel** 命令进入指定隧道的接口视图。如果 Tunnel 接口尚未创建，则先创建再进入接口视图。

Tunnel 接口号只具有本地意义，隧道两端可以使用相同或不同的接口号。

相关配置可参考命令 **source**，**destination**，**gre key**，**gre checksum**，**tunnel-protocol**。

【举例】

创建接口 Tunnel3。

```
[H3C] interface tunnel 3
```

2.1.7 keepalive

【命令】

keepalive [*seconds* [*times*]]

undo keepalive

【视图】

Tunnel 接口视图

【参数】

seconds：keepalive 报文发送周期，缺省为 10 秒，取值范围为 1～32767。

times：keepalive 报文的最大传送次数，缺省为 3 次，取值范围为 1～255。

【描述】

keepalive 命令用来使能 GRE 的 keepalive 功能，并配置 keepalive 报文发送周期及最大发送次数，**undo keepalive** 命令用来关闭 keepalive 功能。

缺省情况下，不启用 GRE 的 keepalive。当配置了该命令后，防火墙会从 Tunnel 口定期发送 GRE 的 keepalive 报文。如果超时时间内对端没有回应，则本端防火墙重新发送 keepalive 报文。如果超过最大传送次数后仍然没有接受到对端的回应，则本端 Tunnel 口的协议状态将变为 down。

相关配置可参考命令 **interface tunnel**。

【举例】

配置 GRE keepalive 的报文发送周期 20s，最大传送次数为 5 次。

```
[H3C-Tunnel5] keepalive 20 5
```

2.1.8 source

【命令】

source { *ip-addr* | *interface-type interface-num* }

undo source

【视图】

Tunnel 接口视图

【参数】

ip-addr：使用 A.B.C.D 的地址形式来指定发出 GRE 报文的实际接口的 IP 地址。

interface-type interface-num：接口类型及接口号。

【描述】

source 命令用来指定 Tunnel 接口进行封装时对添加的 IP 报头填入的源端 IP 地址，**undo source** 命令用来删除设置的源地址。

缺省情况下，系统不指定隧道的源地址。

指定的隧道源地址是发出 GRE 报文的实际接口地址，该地址应和隧道对端指定的目的地址一致。

不能对两个或两个以上使用同种封装协议的 Tunnel 接口配置完全相同的源地址和目的地址。

当前该配置不支持插卡热插拔事件，即拔掉插卡后，相应的配置仍然存在，需要手工删除。

相关配置可参考命令 **interface tunnel**，**destination**。

【举例】

在防火墙 SecPath1 上配置 Tunnel5 接口，此接口封装的报文实际出口为 Ethernet 0/0/0 接口（接口 IP 地址为 192.100.1.1）。

```
[H3C-Tunnel5] source 192.100.1.1
```

或使用接口形式：

```
[H3C-Tunnel5] source Ethernet 0/0/0
```

2.1.9 tunnel-protocol gre

【命令】

tunnel-protocol gre

【视图】

Tunnel 接口视图

【参数】

无

【描述】

tunnel-protocol gre 命令用来设置 Tunnel 接口为 GRE 封装模式。

缺省情况下，是 GRE 模式。在 GRE 模式下，用户只能看见和执行 GRE 有关的配置命令；在其他模式下，用户才能看见和执行相应的配置命令。

相关配置可参考命令 **interface tunnel**。

【举例】

防火墙 SecPath1 和 SecPath2 之间建立隧道，配置封装协议为 GRE。

```
[H3C-Tunnel3] tunnel-protocol gre
[H3C-Tunnel2] tunnel-protocol gre
```

第3章 IPsec 配置命令

3.1 IPsec 配置命令

3.1.1 ah authentication-algorithm

【命令】

ah authentication-algorithm { **md5** | **sha1** }

undo ah authentication-algorithm

【视图】

IPsec 提议（ipsec proposal）视图

【参数】

md5：设置采用 MD5 认证算法。

sha1：设置采用 SHA-1 认证算法。

【描述】

命令 **ah authentication-algorithm** 用来设置 IPsec 安全提议中 AH（Authentication Header）协议采用的认证算法，命令 **undo ah authentication-algorithm** 用来恢复缺省的认证算法。

缺省情况下，在 IPsec 安全提议中 AH 协议采用 MD5 认证算法。

AH 协议没有加密的功能，只对报文进行认证。

MD5 算法使用 128 位的消息摘要（message-digest），SHA-1 算法使用 160 位的消息摘要（message-digest）。MD5 算法的计算速度比 SHA-1 算法快，而 SHA-1 算法的安全强度比 MD5 算法高。

在安全隧道的两端设置安全策略时，所引用的提议中，AH 协议必须设置成采用同样的认证算法。

只有先使用 **transform** 命令选择了 **ah** 或 **ah-esp** 安全协议后，才能够配置 AH 认证算法。

相关配置可参考命令 **ipsec proposal**，**proposal**，**sa spi**，**transform**。

【举例】

在配置安全提议 prop1 时，设定 AH 协议采用 SHA-1 算法。

```
[H3C] ipsec proposal prop1
```

```
[H3C-ipsec-proposal-prop1] transform ah
[H3C-ipsec-proposal-prop1] ah authentication-algorithm sha1
```

3.1.2 debugging ike dpd

【命令】

debugging ike dpd

undo debugging ike dpd

【视图】

用户视图

【参数】

无

【描述】

debugging ike dpd 命令打开 IKE DPD 调试开关，**undo debugging ike dpd** 命令用来关闭 IKE DPD 调试开关。

【举例】

打开 IKE DPD 调试开关。

```
<H3C> debugging ike dpd
```

3.1.3 debugging ipsec

【命令】

debugging ipsec { **all** | **sa** | **fragment** | **misc** | **packet** [**policy** *policy-name* [*seq-number*] | **parameters** *ip-address protocol spi-number*] }

undo debugging ipsec { **all** | **sa** | **fragment** | **misc** | **packet** [**policy** *policy-name* [*seq-number*] | **parameters** *ip-address protocol spi-number*] }

【视图】

用户视图

【参数】

all：打开 IPsec 所有的调试开关。

sa：显示安全联盟的调试信息。

fragment：显示分片报文处理调试信息。

packet：显示 IPsec 数据报文的调试信息。

policy *policy-name*：显示安全策略名为 *policy-name* 的 IPsec 调试信息。

seq-number：显示安全策略顺序号为 *seq-number* 的 IPsec 调试信息。

parameters：显示由目的地址 *ip-address*、*protocol*（**ah** 或 **esp**）、SPI（*spi-number*）所唯一确定的一个安全联盟的调试信息。

misc：显示 IPsec 其他调试信息。

【描述】

debugging ipsec 命令用来打开 IPsec 调试开关， **undo debugging ipsec** 命令用来关闭 IPsec 调试开关。

缺省情况下，关闭 IPsec 调试开关。

【举例】

打开 IPsec 的安全联盟的调试开关。

```
<H3C> debugging ipsec sa
```

3.1.4 display ike dpd

【命令】

display ike dpd [*dpd-name*]

【视图】

所有视图

【参数】

dpd-name：DPD 结构名。

【描述】

display ike dpd 命令用来显示配置的 DPD 结构信息。

【举例】

显示配置的 DPD 结构信息。

```
[H3C] display ike dpd
---------------------------
 IKE dpd: aaa
   references: 0
   interval-time: 10
   time_out: 5
---------------------------
---------------------------
 IKE dpd: xhy
   references: 1
```

```
interval-time: 10
time_out: 5
```

表3-1 display ike dpd 命令显示信息描述表

字段	描述
IKE dpd	IKE DPD 结构名
references	引用计数
interval-time	触发 DPD 查询的时间间隔
time_out	单次 DPD 查询的超时间隔

3.1.5 display ipsec fragment buffer-chain

【命令】

display ipsec fragment buffer-chain

【视图】

任意视图

【参数】

无

【描述】

display ipsec fragment buffer-chain 命令用来显示 IPsec 分片报文的缓存信息。

【举例】

显示 IPsec 分片报文的缓存信息。

```
<H3C> display ipsec fragment buffer-chain
  -------------------------
  ipsec fragment buffer-chain
  -------------------------
  input  fragment buffer-chain packet  :  0
  output fragment buffer-chain packet  :  0
  buffer-chain upper limit             :  4096
  buffer-chain timeout                 :  3
```

表3-2 IPsec 分片报文缓存信息显示描述表

域名	描述
input fragment buffer-chain packet	IPsec 缓存的接收分片报文数
output fragment buffer-chain packet	IPsec 缓存的发送分片报文数

域名	描述
buffer-chain upper limit	IPsec 最大缓存分片报文数
buffer-chain timeout	IPsec 缓存分片报文超时时间

3.1.6 display ipsec fragment statistics

【命令】

display ipsec fragment statistics

【视图】

任意视图

【参数】

无

【描述】

display ipsec fragment statistics 命令用来显示 IPsec 分片报文的统计信息。

【举例】

显示 IPsec 分片报文的统计信息。

```
<H3C> display ipsec fragment statistics
  --------------------------
  ipsec fragment statistics
  --------------------------
  input  fragment packet         :   200
  input  fragment dropped packet :   200
  output fragment packet         :   200
  output fragment dropped packet :   50
```

表3-3 IPsec 分片报文统计信息显示描述表

域名	描述
input fragment packet	IPsec 处理的接收分片报文数
input fragment dropped packet	IPsec 丢弃的接收分片报文数
output fragment packet	IPsec 处理的发送分片报文数
output fragment dropped packet	IPsec 丢弃的发送分片报文数

3.1.7 display ipsec policy

【命令】

display ipsec policy [**brief** | **name** *policy-name* [*seq-number*]]

【视图】

所有视图

【参数】

brief：表示显示所有安全策略的简要信息。

name：表示显示名字为 *policy-name*，顺序号为 *seq-number* 的安全策略的信息。

policy-name：指定安全策略的名称。

seq-number：指定安全策略的顺序号。

如果不指定任何参数，则表示要显示所有安全策略的详细信息。如果指定了 *name policy-name*，而没有指定 *seq-number*，则表示要显示指定的安全策略组的信息。

【描述】

display ipsec policy 命令用来显示安全策略的信息。

brief 参数表示将显示所有安全策略的简要信息，显示格式为简要格式（参见下面的举例）。利用 **brief** 参数可以快速查看所有的安全策略。简要信息包括：安全策略名及顺序号、协商方式、访问控制列表号、提议、本端地址、对端地址。

相关配置可参考命令 **ipsec policy**（系统视图）。

【举例】

显示所有安全策略的简要信息。

```
[H3C] display ipsec policy brief
IPsec-Policy-Name     Mode    acl          Local-Address  Remote-Address
------------------------------------------------------------------------
policy1-1             isakmp  3000                        172.16.2.1
policy2-1             manual  3001        172.16.2.1      172.16.2.2
```

表3-4 IPsec 安全策略简要信息描述表

域名	描述
IPsec-Policy-Name	安全策略组的名字和安全策略顺序号(其中策略组名和策略顺序号之间用“-”隔开)
Mode	安全策略采用的协商方式
acl	安全策略引用的访问控制列表
Local Address	本端的 IP 地址

域名	描述
Remote Address	对端的 IP 地址
ike-peer name	在 ISAKMP 协商模式下，安全策略所引用的 IKE 对等体的名称（manual 模式下无此信息显示）

显示所有安全策略的信息。

```
[H3C] display ipsec policy

==========================================
IPsec Policy Group: "policy1"
Using interface: {Ethernet0/0/0}
==========================================

  ----------------------------
  IPsec policy name: "policy1"
  sequence number: 1
  mode: isakmp
  ----------------------------
    security data flow : 3000
    selector mode: standard
    ike-peer name:  ikepeer
    perfect forward secrecy: DH group 1
    proposal name:  proposal1
    IPsec sa local duration(time based): 3600 seconds
    IPsec sa local duration(traffic based): 1843200 kilobytes

==========================================
IPsec Policy Group: "policy2"
Using interface: {Ethernet0/0/1}
==========================================

  ----------------------------
  IPsec policy name: "policy2"
  sequence number: 1
  mode: manual
  ----------------------------
    security data flow : 3001
    tunnel local  address: 172.16.2.1
    tunnel remote address: 172.16.2.2
    proposal name: proposal2
    inbound AH setting:
```

```
    AH spi:
    AH string-key:
    AH authentication hex key:
  inbound ESP setting:
    ESP spi:
    ESP string-key:
    ESP encryption hex key:
    ESP authentication hex key:
  outbound AH setting:
    AH spi:
    AH string-key:
    AH authentication hex key:
  outbound ESP setting:
    ESP spi:
    ESP string-key:
    ESP encryption hex key:
    ESP authentication hex key: :
```

表3-5 IPsec 安全策略详细信息显示描述表

域名	描述
IPsec policy name	安全策略的名称
sequence number	安全策略的序号
mode	安全策略的协商方式：isakmp 或 manual
security data flow	安全策略引用的访问控制列表
selector mode	表明数据流的保护方式
ike-peer name	引用的 IKE 对等体的名称
perfect forward secrecy	完善的前向安全性（PFS）的配置信息
proposal name	安全策略引用的提议的名字
IPsec sa local duration(time based)	IPsec 安全联盟的生存周期（基于时间的）
IPsec sa local duration(traffic based)	IPsec 安全联盟的生存周期（基于流量的）
tunnel local address	隧道的本端 IP 地址
tunnel remote address	隧道的对端 IP 地址
inbound AH setting	入方向的 AH 协议的设置
inbound ESP setting:	入方向的 ESP 协议的设置
outbound AH setting	出方向的 AH 协议的设置
outbound ESP setting	出方向的 ESP 协议的设置

3.1.8 display ipsec policy-template

【命令】

display ipsec policy-template [**brief** | **name** *template-name* [*seq-number*]]

【视图】

所有视图

【参数】

brief：表示显示所有安全策略模板的简要信息。

name：表示显示名字为 *template-name*，顺序号为 *seq-number* 的安全策略模板的信息。

template-name：指定安全策略模板的名字。

seq-number：指定安全策略模板的顺序号。

如果不指定任何参数，则表示要显示所有安全策略模板的详细信息。如果指定了 **name** *template-name*，而没有指定 *seq-number*，则表示要显示指定的安全策略模板组的信息。

【描述】

命令 **display ipsec policy-template** 用来显示安全策略模板的信息。

brief 参数表示将显示所有安全策略模板的简要信息，显示格式为简要格式（参见下面的举例）。利用 **brief** 参数，可以快速查看所有的安全策略模板。简要信息包括：安全策略模板名及顺序号、访问控制列表号、对端地址。

相关配置可参考命令 **ipsec policy-template**（系统视图）。

【举例】

显示所有安全策略模板的简要信息。

```
[H3C] display ipsec policy-template brief
Policy-Template-Name     acl            Remote-Address
-------------------------------------------------------
test-tplt300             3300
```

表3-6 IPsec 安全策略模板简要信息描述表

域名	描述
Policy-Template-Name	安全策略模板的名字和顺序号
acl	安全策略模板引用的访问控制列表
Remote-Address	对端的 IP 地址

3.1.9 display ipsec proposal

【命令】

display ipsec proposal [*proposal-name*]

【视图】

所有视图

【参数】

proposal-name：指定安全提议的名称。

【描述】

display ipsec proposal 命令用来显示安全提议的配置信息，如果没有指定安全提议的名称，则显示所有的提议的信息。

相关配置可参考命令 **ipsec proposal**，**display ipsec sa**，**display ipsec policy**。

【举例】

显示所有的提议。

```
[H3C] display ipsec proposal
IPsec proposal name: prop2
     encapsulation mode: tunnel
     transform: ah-new
     AH protocol: authentication sha1-hmac-96
IPsec proposal name: prop1
     encapsulation mode: transport
     transform: esp-new
     ESP protocol: authentication md5-hmac-96, encryption des
```

表3-7 IPsec 安全提议信息显示描述表

域名	描述
IPsec proposal name	提议的名字
encapsulation mode	提议采用的模式，包括两种：传输（transport）和隧道（tunnel）模式
transform	提议采用的安全协议，包括两种：AH 协议和 ESP 协议
AH protocol	AH 协议采用的认证算法
ESP protocol	ESP 协议采用的认证算法和加密算法

3.1.10 display ipsec sa

【命令】

display ipsec sa [**brief** | **remote** *ip-address* | **policy** *policy-name* [*seq-number*] | **duration**]

【视图】

所有视图

【参数】

brief：表示显示所有的安全联盟的简要信息。

remote *ip-address*：表示显示对端地址为 *ip-address* 的安全联盟的信息。

policy：表示显示由指定安全策略创建的安全联盟的信息。

policy-name：指定安全策略的名称。

seq-number：指定安全策略的顺序号。

duration：表示显示全局的安全联盟生存周期。

【描述】

display ipsec sa 命令用来显示安全联盟的相关信息。

使用 **brief** 参数显示所有的安全联盟的简要信息，显示格式为简要格式（参见下面的举例），简要信息包括：源地址、目的地址、安全参数索引、协议、算法。其中，算法的显示以“E:”开头的表示加密算法，以“A:”开头的表示认证算法。利用 **brief** 参数可以快速查看所有已经建立的安全联盟。

使用 **remote** 和 **policy** 参数均显示安全联盟的详细信息，显示格式是先显示安全策略的部分信息，再显示此安全策略中的安全联盟的详细信息。

使用 **duration** 参数显示全局的安全联盟的生存时间，包括“基于时间”和“基于流量”两种类型。参见下面的举例。

当未指定任何参数时，显示所有的安全联盟的信息。

相关配置可参考命令 **reset ipsec sa**，**ipsec sa global-duration**，**display ipsec policy**。

【举例】

下面是 **display ipsec sa brief** 命令的输出：

```
[H3C] display ipsec sa brief
Total IPsec SAs: 2
Src Address  Dst Address  SPI    Protocol     Algorithm
-------------------------------------------------------
10.1.1.1     10.1.1.2     300    ESP        E:DES; A:HMAC-MD5-96
```

```
10.1.1.2      10.1.1.1      400     ESP         E:DES; A:HMAC-MD5-96
```

表3-8 IPsec 安全联盟简要信息显示描述表

域名	描述
Src Address	本端的 IP 地址
Dst Address	对端的 IP 地址
SPI	安全参数索引
Protocol	IPsec 采用的安全协议
Algorithm	安全协议采用的认证算法和加密算法，其中，以“E:”开头表示加密算法；以“A:”开头表示认证算法

显示安全联盟的全局生存时间。

```
[H3C] display ipsec sa duration
     IPsec sa global duration（traffic based）: 1843200 kilobytes
     IPsec sa global duration（time based）: 3600 seconds
```

下面是 **display ipsec sa** 命令的输出：

```
<H3C> display ipsec sa
==============================
Interface: Ethernet0/0/0
    path MTU: 1500
==============================

  ----------------------------
  IPsec policy name: "1"
  sequence number: 1
  mode: isakmp
  ----------------------------
    Created by: "Encrypt-card"
    connection id: 5
    encapsulation mode: tunnel
    perfect forward secrecy: None
    tunnel:
        local  address: 2.1.1.1
        remote address: 2.1.1.3
    flow:    (8 times matched)
        sour addr: 192.168.1.0/255.255.255.0  port: 0  protocol: IP
        dest addr: 10.1.1.0/255.255.255.0  port: 0  protocol: IP

    [inbound AH SAs]
      spi: 1369228154 (0x519cc37a)
```

```
  proposal: AH-SHA1HMAC96
  sa remaining key duration (bytes/sec): 1887436256/3594
  max received sequence-number: 4
  udp encapsulation used for nat traversal: N

[inbound ESP SAs]
  spi: 2673492781 (0x9f5a432d)
  proposal: ESP-ENCRYPT-3DES ESP-AUTH-MD5
  sa remaining key duration (bytes/sec): 1887436448/3594
  max received sequence-number: 4
  udp encapsulation used for nat traversal: N

[outbound ESP SAs]
  spi: 1109683945 (0x42246ee9)
  proposal: ESP-ENCRYPT-3DES ESP-AUTH-MD5
  sa remaining key duration (bytes/sec): 1887436256/3594
  max sent sequence-number: 5
  udp encapsulation used for nat traversal: N

[outbound AH SAs]
  spi: 3969283528 (0xec9675c8)
  proposal: AH-SHA1HMAC96
  sa remaining key duration (bytes/sec): 1887436160/3594
  max sent sequence-number: 5
  udp encapsulation used for nat traversal: N
```

表3-9 IPsec 安全联盟详细信息显示描述表

域名	描述
Interface	应用了安全策略的接口
path MTU	从该接口发送出去的最大 IP 数据报文长度
IPsec policy	采用的安全策略，包括策略名、顺序号和协商方式
Created by	"Encrypt-card"表示使用加密卡进行加密；"Host"表示使用软件加密
connection id	安全通道标识符
encapsulation mode	IPsec 采用的模式，有两种：传输（transport）和隧道（tunnel）模式
perfect forward secrecy	是否使用完善的前向安全（Perfect Forward Secrecy）特性
tunnel local	本端的 IP 地址
tunnel remote	对端的 IP 地址
sour addr	安全策略所引用的 ACL 的源地址
dest addr	安全策略所引用的 ACL 的目的地址

域名	描述
inbound	输入端 SA 的信息
transform	安全策略所引用的提议
sa remaining key duration	安全联盟剩余的存活时间
max received sequence-number	接收的报文最大序列号（安全协议提供的防重放功能）
udp encapsulation used for nat traversal	是否使用 IKE NAT 穿越
outbound	输出端 SA 的信息
max sent sequence-number	发送的报文最大序列号（安全协议提供的防重放功能）

3.1.11 display ipsec statistics

【命令】

display ipsec statistics

【视图】

所有视图

【参数】

无

【描述】

显示 IPsec 处理报文的统计信息。包括输入输出的安全报文数、字节数、被丢弃的报文数以及被丢弃的报文的详细说明。

相关配置可参考命令 **reset ipsec statistics**。

【举例】

显示 IPsec 的报文统计信息。

```
[H3C] display ipsec statistics
the security packet statistics:
    input/output security packets: 5124/8231
    input/output security bytes: 52348/64356
    input/output dropped security packets: 0/0
    dropped security packet detail:
      no enough memory: 0
      can't find SA: 0
      queue is full: 0
```

```
authentication is failed: 0
wrong length: 0
replay packet: 0
too long packet: 0
wrong SA: 0
other error packet: 0
```

表3-10 IPsec 处理报文的统计信息显示描述表

域名	描述
input/output security packets	受安全保护的输入/输出数据包
input/output security bytes	受安全保护的输入/输出字节数
input/output dropped security packets	被防火墙丢弃了的受安全保护的输入/输出数据包

3.1.12 display ipsec tunnel

【命令】

display ipsec tunnel

【视图】

所有视图

【参数】

无

【描述】

display ipsec tunnel 命令用来显示 IPsec 的隧道信息。

【举例】

显示 IPsec 的隧道信息。

```
<H3C> display ipsec tunnel
    -----------------------------------------------
    Connection ID : 5
    Perfect forward secrecy: None
    SA's SPI :
        Inbound :  1369228154 (0x519cc37a) [AH]
                   2673492781 (0x9f5a432d) [ESP]
        Outbound : 1109683945 (0x42246ee9) [ESP]
                   3969283528 (0xec9675c8) [AH]
    Tunnel :
        Local Address:  2.1.1.1  Remote Address : 2.1.1.3
```

```
Flow :     (8 times matched)
    Sour Addr : 0.0.0.0/0.0.0.0  Port: 0  Protocol : IP
    Dest Addr : 0.0.0.0/0.0.0.0  Port: 0  Protocol : IP
```

3.1.13 dpd

【命令】

dpd *dpd-name*

undo dpd

【视图】

ike-peer 视图

【参数】

dpd-name：DPD 结构名。

【描述】

dpd 命令用来为 IKE Peer 指定 DPD 结构，**undo dpd** 用来取消 IKE Peer 的 DPD 结构。

指定的 DPD 结构应预先建立好，否则将返回错误信息。执行 **dpd** 命令时，该 DPD 结构的引用计数器加 1；执行 **undo dpd** 命令时，该 DPD 结构的引用计数器减 1。

相关配置可参考命令 **ike dpd**。

【举例】

指定 IKE Peer1 的 DPD 结构为 aaa

```
[H3C-ike-peer-peer1] dpd aaa
```

取消 IKE Peer1 的 DPD 结构。

```
[H3C-ike-peer-peer1] undo dpd
```

3.1.14 encapsulation-mode

【命令】

encapsulation-mode { **transport** | **tunnel** }

undo encapsulation-mode

【视图】

安全提议视图

【参数】

transport：设置 IP 报文的封装形式采用传输模式。

tunnel：设置 IP 报文的封装形式采用隧道模式。

【描述】

encapsulation-mode 命令用来设置安全协议对 IP 报文的封装形式，有传输模式（**transport**）和隧道模式（**tunnel**）两种， **undo encapsulation-mode** 命令用来恢复到缺省的报文封装形式。

缺省情况使用 **tunnel**，即隧道模式。

使用 IPsec 对 IP 报文进行加密或认证有两种封装形式，分别是传输模式和隧道模式。对于传输模式，不增加新 IP 头，原始报文的源地址和目的地址就是安全隧道的端点；对于隧道模式，IPsec 对整个 IP 报文进行保护，并在原 IP 报文的前面增加一个新的 IP 头，新 IP 头的源地址和目的地址分别是安全隧道的两个端点的 IP 地址。

通常，在两个防火墙（路由器）之间，总是使用隧道模式。在一端被加密的报文，只有另一端能够解密。因此，必须对 IP 报文进行隧道封装，即增加一个新的 IP 头，进行隧道封装后的 IP 报文被发送到另一端，才能够被解密。

传输模式适合两台主机之间的通讯，或者是一台主机和一个防火墙之间的通讯。在传输模式下，对报文进行加密和解密的两台设备本身必须是报文的原始发送者和最终接收者。在两个防火墙之间的数据流量，绝大部分都不是防火墙本身的通讯量，因此，在防火墙之间不使用传输模式。

在安全隧道的两端设置的安全策略所引用的提议必须设置成采用同样的报文封装形式。

相关配置可参考命令 **ah authentication-algorithm**，**ipsec proposal**，**esp encryption-algorithm**，**esp authentication-algorithm**，**proposal**，**transform**。

【举例】

设置名为 prop2 的提议采用传输模式对 IP 报文进行封装。

```
[H3C] ipsec proposal prop2
[H3C-ipsec-proposal-prop2] encapsulation-mode transport
```

3.1.15 esp authentication-algorithm

【命令】

esp authentication-algorithm { **md5** | **sha1** }

undo esp authentication-algorithm

【视图】

安全提议视图

【参数】

md5：采用 MD5 认证算法，密钥长度 128 位。

sha1：采用 SHA-1 认证算法，密钥长度 160 位。

【描述】

esp authentication-algorithm 命令用来设置 ESP 协议采用的认证算法，**undo esp authentication-algorithm** 命令用来设置 ESP 协议不对报文进行认证。

缺省情况下，使用 **md5**，即 MD5 认证算法。

MD5 算法的计算速度比 SHA-1 算法快，而 SHA-1 算法的安全强度比 MD5 算法高。

ESP 协议允许对报文同时进行加密和认证，或只加密，或只认证。

ESP 协议采用的加密算法和认证算法不能同时设置为空。

注意：**undo esp authentication-algorithm** 命令不是恢复认证算法为缺省算法，而是设置认证算法为空，即不认证。当加密算法不为空时，**undo esp authentication-algorithm** 命令才起作用。

在安全隧道的两端设置的安全策略所引用的提议必须设置成采用同样的认证算法。

相关配置可参考命令 **ipsec proposal**，**esp encryption-algorithm**，**proposal**，**transform**。

【举例】

设定提议 prop1 采用 ESP 协议并使用 SHA-1 认证算法。

```
[H3C] ipsec proposal prop1
[H3C-ipsec-proposal-prop1] transform esp
[H3C-ipsec-proposal-prop1] esp authentication-algorithm sha1
```

3.1.16 esp encryption-algorithm

【命令】

esp encryption-algorithm { **3des** | **des** | **aes** }

undo esp encryption-algorithm

【视图】

安全提议视图

【参数】

des：即数据加密标准 DES（Data Encryption Standard），是国际通用的加密算法，密钥长度 56 位。

3des：即 3DES（Triple DES），也是一种国际通用的加密算法，密钥长度 168 位。

aes：即 AES（Advanced Encryption Standard），是 IETF 标准要求的一种加密算法，Comware 实现的密钥长度是 128 位、192 位和 256 位。

【描述】

esp encryption-algorithm 命令用来设置 ESP 协议采用的加密算法，**undo esp encryption-algorithm** 命令用来设置 ESP 协议不对报文进行加密。

缺省情况使用 **des**，即 DES 加密算法。

对于保密及安全性要求非常高的地方，采用 3DES 算法可以满足需要，但 3DES 加密速度比较慢；对于普通的安全要求，DES 算法则可以满足需要。

ESP 协议允许对报文同时进行加密和认证，或只加密，或只认证。

ESP 协议采用的加密算法和认证算法不能同时设置为空。当认证算法不为空时，**undo esp encryption-algorithm** 命令才起作用。

相关配置可参考命令 **ipsec proposal**，**esp authentication-algorithm**，**proposal**，**transform**。

【举例】

设定提议 prop1 采用 ESP 协议并使用 3DES 加密算法。

```
[H3C] ipsec proposal prop1
[H3C-ipsec-proposal-prop1] transform esp
[H3C-ipsec-proposal-prop1] esp encryption-algorithm 3des
```

3.1.17 ike dpd

【命令】

ike dpd *dpd-name*

undo ike dpd *dpd-name*

【视图】

系统视图

【参数】

dpd-name：DPD（Dead Peer Detection）结构名。

【描述】

ike dpd 命令用来创建 DPD 结构并进入 DPD 结构视图，**undo ike dpd** 命令用来删除一个 DPD 结构。

如 DPD 结构已经被 IKE Peer 引用，则不能删除。

相关配置可参考命令 **dpd**。

【举例】

创建一个名称为 aaa 的 DPD 结构。

```
[H3C] ike dpd aaa
```

删除一个名称为 aaa 的 DPD 结构。

```
[H3C] undo ike dpd aaa
```

3.1.18 interval-time

【命令】

interval-time *seconds*

undo interval-time

【视图】

DPD 结构视图

【参数】

seconds：触发 DPD 查询的时间间隔，取值范围 1～300 秒。缺省情况下，*seconds* 为 10 秒。

【描述】

interval-time 命令用来配置触发 DPD 查询的时间间隔，**undo interval-time** 命令用来恢复触发 DPD 查询的时间间隔为缺省值。

【举例】

设置 interval-time 为 20 秒。

```
[H3C-ike-dpd-aaa] interval-time 20
```

重置 interval-time 为 10 秒。

```
[H3C-ike-dpd-aaa] undo interval-time
```

3.1.19 ipsec fragment-chain

【命令】

ipsec fragment-chain { **inbound** | **outbound** } { **disable** | **enable** }

【视图】

系统视图

【参数】

inbound：设置 IPsec 入方向的分片报文缓存策略。

outbound：设置 IPsec 出方向的分片报文缓存策略。

disable：关闭 IPsec 分片报文缓存机制。

enable：使能 IPsec 分片报文缓存机制。

【描述】

ipsec fragment-chain 命令用来设置 IPsec 对于分片报文缓存的处理方式。

缺省情况下，关闭 IPsec 分片报文缓存机制，即非首片报文先于首片报文到达时，非首片报文将被丢弃。

【举例】

使能入方向的 IPsec 分片报文缓存机制。

```
[H3C] ipsec fragment-chain inbound enable
```

3.1.20 ipsec fragment-chain timeout

【命令】

ipsec fragment-chain timeout *seconds*

【视图】

系统视图

【参数】

timeout *seconds*：分片报文缓存时间，单位为秒，取值范围为 3～60。

【描述】

ipsec fragment-chain timeout 命令用来设置报文的缓存时间。

缺省情况下，IPsec 分片报文缓存超时时间为 3 秒。

【举例】

设置分片报文的缓存时间为 10 秒。

```
[H3C] ipsec fragment-chain timeout 10
```

3.1.21 ipsec policy（接口视图）

【命令】

ipsec policy *policy-name*

undo ipsec policy [*policy-name*]

【视图】

接口视图

【参数】

policy-name：指定应用在接口上的安全策略组的名称。在系统视图下，必须已经配置了名称为 *policy-name* 的安全策略组。

【描述】

ipsec policy *policy-name* 命令用来在接口上应用名称为 *policy-name* 的安全策略组，**undo ipsec policy** 命令用来从接口上取消应用的所有的或特定的安全策略组，使此接口不再具有 IPsec 的安全保护功能。

在一个接口上，只能应用一个安全策略组。如果要在接口上应用另一个安全策略组，必须先从接口上取消应用的安全策略组，再在接口上应用另外一个安全策略组。一个安全策略组可应用到多个接口上。

当从一个接口发送报文时，将按照顺序号从小到大的顺序查找安全策略组中每一条安全策略。如果报文匹配了一条安全策略引用的访问控制列表，则使用这条安全策略对报文进行处理；如果报文没有匹配安全策略引用的访问控制列表，则继续查找下一条安全策略；如果报文对所有安全策略引用的访问控制列表都不匹配，则报文直接被发送（IPsec 不对报文加以保护）。

想要实现在接口上不发送任何不加密的报文，需要结合防火墙和 IPsec 一起使用，用防火墙将不需要加密的报文全部丢弃。

当在所有接口上都删除了安全策略后，才会删除所有的 IKE SA，否则需要手工删除或等到 SA 超时。

相关配置可参考命令 **ipsec policy**（系统视图）。

【举例】

在 Ethernet 1/0/0 接口上应用名为 pg1 的安全策略组。

```
[H3C] interface Ethernet 1/0/0
[H3C-Ethernet1/0/0] ipsec policy pg1
```

3.1.22 ipsec policy（系统视图）

【命令】

ipsec policy *policy-name seq-number* [**manual** | **isakmp** [**template** *template-name*]]

undo ipsec policy *policy-name* [*seq-number*]

【视图】

系统视图

【参数】

policy-name：安全策略的名称。命名规则为：长度为 1～15 个字符，不区分大小写，字符可以是英文字母或者数字，不能带减号“-”。

seq-number：安全策略的顺序号，取值范围 1～10000，值越小优先级越高。

manual：指定用手工方式建立安全联盟。

isakmp：指定通过 IKE 协商建立安全联盟。

template：指定采用策略模板动态创建安全联盟。

template-name：指定被引用的 template 的名称。此 *policy-name* 将引用 *template-name*。*template-name* 是一个策略模板。在此之前，名为 *template-name* 的安全策略模板必须已经创建。

【描述】

在系统视图下，**ipsec policy** 命令用来创建或修改一条安全策略，并进入安全策略（ipsec policy）视图，**undo ipsec policy** 命令用来删除安全策略。使用 **undo ipsec policy** *policy-name* 命令，用来删除名称为 *policy-name* 的安全策略组；使用 **undo ipsec policy** *policy-name seq-number* 命令，用来删除名称为 *policy-name*，顺序号为 *seq-number* 的一条安全策略。当安全策略被应用到接口时，则不允许将其删除。

缺省情况下，没有安全策略存在。

使用此命令创建安全策略时，必须指定协商方式；在安全策略创建后，不能修改协商方式，如果要修改安全策略的协商方式，只能先删除这条安全策略，在重新创建安全策略时，指定新的协商方式。

具有相同名字的安全策略一起组成一个安全策略组。由名字和顺序号一起确定一条唯一的安全策略。在一个安全策略组中最大可以设置 500 条安全策略。在一个安全策略组中，顺序号 *seq-number* 越小的安全策略，优先级越高。在一个接口上应用一个安全策略组，实际上是同时应用了安全策略组中所有的安全策略，从而能够对不同的数据流采用不同的安全联盟进行保护。

ipsec policy *policy-name seq-number* **isakmp template** *template-name* 命令创建一个安全策略，该策略由 IKE 协商建立安全联盟，而策略的参数根据 *template-name* 指定的策略模板来确定。在配置此命令前，必须已经使用命令 **ipsec policy-template** 创建策略模板。在协商过程中进行策略匹配时，策略模板中定义的参数必须相符，而策略模板中没有定义的参数由发起方来决定，响应方接受发起方的建议。策略模板中必须定义的参数是提议（proposal），其它参数为可选配置。

注意：IKE 不会用带有 **template** 参数的策略去发起协商。但可以用带有 **template** 参数的策略响应对方发起的协商。

相关配置可参考命令 **ipsec policy**（接口视图），**security acl**，**tunnel local**，**tunnel remote**，**sa duration**，**proposal**，**display ipsec policy**，**ipsec policy-template**，**ike-peer**。

【举例】

设置名称为 policy1，顺序号为 100，采用 ISAKMP 方式协商的安全策略。

```
[H3C] ipsec policy policy1 100 isakmp
[H3C-ipsec-policy-isakmp-policy1-100]
```

3.1.23 ipsec policy-template

【命令】

ipsec policy-template *template-name seq-number*

undo ipsec policy-template *template-name* [*seq-number*]

【视图】

系统视图

【参数】

template-name：安全策略模板的名称。命名规则为：长度为 1～15 个字符，不区分大小写，字符可以是英文字母或者数字，不能带减号“-”。

seq-number：为此安全策略模板的顺序号，取值范围 1～10000。在一个安全策略模板中，顺序号越小的安全策略，优先级越高。

【描述】

ipsec policy-template 命令用来创建或修改一个安全策略模板，并进入安全策略模板（ipsec policy template）视图，**undo ipsec policy-template** 命令用来删除一个安全策略模板组或者安全策略模板组中的一个安全策略模板。使用 **undo ipsec policy-template** *template-name* 命令删除名称为 *template-name* 的安全策略模板组；使用 **undo ipsec policy-template** *template-name seq-number* 命令删除名称为 *template-name*、序号为 *seq-number* 的一个安全策略模板。

缺省情况下，没有安全策略模板存在。

创建一个策略模板以后，在使用 **ipsec policy** *policy-name seq-number* **isakmp template** *template-name* 命令创建一个安全策略时，通过 *template-name* 参数引用此模板。

IPsec 安全策略模板的参数与 IPsec ISAKMP 协商方式的安全策略的参数是一样的，包括所引用的 IPsec proposal、保护的数据流、PFS 特性、生存周期、隧道对端地址。但需要注意的是，proposal 参数是必须配置的，而其它参数是可选的。在 IKE

协商时，如果使用 IPsec 策略模板进行策略匹配，则配置的参数必须匹配，而没有配置的参数采用发起方的。

相关配置可参考命令 **ipsec policy**，**security acl**，**tunnel local**，**tunnel remote**，**proposal**，**display ipsec policy**，**ike-peer**。

【举例】

创建一个模板名称为 template1，顺序号为 100 的安全策略模板。

```
[H3C] ipsec policy-template template1 100
[H3C-ipsec-policy-template-template1-100]
```

3.1.24 ipsec proposal

【命令】

ipsec proposal *proposal-name*

undo ipsec proposal *proposal-name*

【视图】

系统视图

【参数】

proposal-name：指定 IPsec 提议的名字。命名规则为：长度为 1～15 个字符，不区分大小写。

【描述】

ipsec proposal *proposal-name* 命令用来创建或修改一个名称为 *proposal-name* 的 IPsec 提议，并进入 IPsec 提议视图，**undo ipsec proposal** *proposal-name* 命令用来删除一个名称为 *proposal-name* 的 IPsec 提议。

缺省情况下，系统没有任何提议。

IPsec 提议（Proposal）是用于实施 IPsec 安全时所采取的一系列的措施，提议包含了所采用的安全协议、加密和认证算法、报文封装形式。

在配置安全策略时，需要通过引用提议来确定在安全隧道的两端所采用的安全协议、加密和认证算法和报文封装形式。

在使用 **ipsec proposal** 命令创建一个新的 IPsec 安全提议后，其缺省参数为采用 ESP 协议、DES 加密算法、MD5 认证算法。

相关配置可参考命令 **ah authentication-algorithm**，**esp encryption-algorithm**，**esp authentication-algorithm**，**encapsulation-mode**，**proposal**，**display ipsec proposal**，**transform**。

【举例】

创建名为 newprop1 的提议。

```
[H3C] ipsec proposal newprop1
```

3.1.25 ipsec sa global-duration

【命令】

ipsec sa global-duration { **time-based** *seconds* | **traffic-based** *kilobytes* }

undo ipsec sa global-duration { **time-based** | **traffic-based** }

【视图】

系统视图

【参数】

time-based *seconds*：指定以时间为基准的全局生存周期，*seconds* 的取值范围是 120～604800，单位是秒，缺省值是 3600 秒。

traffic-based *kilobytes*：指定以流量为基准的全局生存周期，*kilobytes* 的取值范围是 256～4194303，单位是千字节，缺省值是 1843200 千字节，如果流量达到此值，则生存周期到期。

【描述】

ipsec sa global-duration 命令用来设置全局的安全联盟生存周期，**undo ipsec sa global-duration** 命令用来恢复全局的安全联盟生存周期的缺省值。

当 IKE 协商安全联盟时，如果采用的安全策略没有配置自己的生存周期，将采用此命令所定义的全局生存周期与对端协商。如果安全策略配置了自己的生存周期，则系统使用安全策略自己的生存周期与对端协商。IKE 为 IPsec 协商建立安全联盟时，对于 IKE 第 1 阶段，安全联盟的生存周期由发起方决定；对于 IKE 第 2 阶段，采用本地设置的和对端提议的生存周期中较小的一个。

衡量生存周期有两种方式：“基于时间”的生存周期和“基于流量”的生存周期。基于时间的生存周期是从安全联盟建立开始到此安全联盟协商存活的时间；基于流量的生存周期是此安全联盟允许处理的最大流量。如果生存周期到达指定的时间或指定的流量，则安全联盟就会失效。安全联盟失效前，IKE 将为 IPsec 协商建立新的安全联盟，这样，在旧的安全联盟失效前新的安全联盟就已经准备好。在新的安全联盟开始协商而没有协商好之前，继续使用旧的安全联盟保护通信。在新的安全联盟协商好之后，则立即采用新的安全联盟保护通信。

使用该命令可以改变安全联盟的全局生存周期，改变全局生存周期以后，没有单独配置生存周期的安全联盟，在下次 IKE 协商中，会使用新的全局生存周期。

安全联盟的生存周期只对通过 IKE 协商的安全联盟起作用，对通过手工方式建立的安全联盟不起作用。

相关配置可参考命令 **sa duration**，**display ipsec sa duration**。

【举例】

设置全局的安全联盟生存时间为 2 小时。

```
[H3C] ipsec sa global-duration time-based 7200
```

设置全局的安全联盟生存时间为：传输 10M 字节的流量后，安全联盟即过期。

```
[H3C] ipsec sa global-duration traffic-based 10000
```

3.1.26 pfs

【命令】

pfs { **dh-group1** | **dh-group2** | **dh-group5** | **dh-group14** }

undo pfs

【视图】

安全策略视图、安全策略模板视图

【参数】

dh-group1：指定使用 768-bit Diffie-Hellman 组。

dh-group2：指定使用 1024-bit Diffie-Hellman 组。

dh-group5：指定使用 1536-bit Diffie-Hellman 组。

dh-group14：指定使用 2048bit Diffie-Hellman 组。

【描述】

pfs 命令用来设置使用此安全策略发起协商时使用完善的前向安全（Perfect Forward Secrecy）特性，**undo pfs** 命令用来设置在协商时不使用 PFS 特性。

缺省情况下，没有使用 PFS 特性。

此命令使 IPsec 在使用此安全策略发起一个协商时，在阶段 2 的协商中进行一次附加的密钥交换以提高通讯的安全性。本端和对端指定的 Diffie-Hellman 组必须一致，否则协商会失败。

此命令仅在通过 IKE 方式建立安全联盟时才可以进行配置。

相关配置可参考命令 **ipsec policy-template**，**ipsec policy**（系统视图），**ipsec policy**（接口视图），**tunnel local**，**tunnel remote**，**sa duration**，**proposal**。

【举例】

设置使用安全策略 shanghai 200 进行协商时使用 PFS 特性。

```
[H3C] ipsec policy shanghai 200 isakmp
[H3C-ipsec-policy-isakmp-shanghai-200] pfs dh-group1
```

3.1.27 proposal

【命令】

proposal *proposal-name1* [*proposal-name2*...*proposal-name6*]

undo proposal [*proposal-name*]

【视图】

安全策略视图、安全策略模板视图

【参数】

proposal-name1，…，*proposal-name6*：所采用的提议名。

【描述】

proposal 命令用来设置安全策略所引用的提议，命令 **undo proposal** 用来取消安全策略引用的提议。

缺省情况下，不引用任何提议。

在使用此命令之前，必须已经配置了相应的安全提议。

如果安全策略是手工（**manual**）方式的，则安全策略在引用提议时只能指定一个安全提议。如果需要改变已配置好的安全提议，必须先使用命令 **undo proposal** 取消原先的安全提议，再设置新的安全提议。

如果安全策略是 IKE（**isakmp**）协商方式的，则一条安全策略最多可以引用六个安全提议，IKE 协商时将在安全策略中搜索能够完全匹配的安全提议。

如果是安全策略模板，则每个模板最多可以引用六个安全提议，IKE 协商时将搜索能够完全匹配的安全提议。

相关配置可参考命令 **ipsec proposal**，**ipsec policy**（系统视图），**ipsec policy**（接口视图），**security acl**，**tunnel local**，**tunnel remote**。

【举例】

设置名称为 prop1 的安全提议，采用 ESP 协议和缺省算法。并设置安全策略引用此安全提议。

```
[H3C] ipsec proposal prop1
[H3C-ipsec-proposal-prop1] transform esp
[H3C-ipsec-proposal-prop1] quit
[H3C] ipsec policy policy1 100 manual
[H3C-ipsec-policy-manual-policy1-100] proposal prop1
```

3.1.28 reset ipsec fragment buffer-chain

【命令】

reset ipsec fragment buffer-chain

【视图】

用户视图

【参数】

无

【描述】

reset ipsec fragment buffer-chain 命令用来清除 IPsec 缓存队列中的分片报文。

【举例】

清除 IPsec 缓存队列中的分片报文。

```
<H3C> reset ipsec fragment buffer-chain
```

3.1.29 reset ipsec fragment statistics

【命令】

reset ipsec fragment statistics

【视图】

用户视图

【参数】

无

【描述】

reset ipsec fragment statistics 命令用来清除 IPsec 分片报文统计信息。

【举例】

清除 IPsec 分片报文统计信息。

```
<H3C> reset ipsec fragment statistics
```

3.1.30 reset ipsec sa

【命令】

reset ipsec sa [**remote** *ip-address* | **policy** *policy-name* [*seq-number*] | **parameters** *ip-address protocol spi-number*]

【视图】

用户视图

【参数】

remote *ip-address*：指定对端地址为 *ip-address*，地址为点分十进制格式。

policy：指定安全策略。

policy-name：指定安全策略的名称。命名规则为：长度为 1～15 个字符，不区分大小写，字符可以是英文字母或者数字。

seq-number：为可选参数，指定安全策略的顺序号。如果不指定 *seq-number*，则是指名称为 *policy-name* 的安全策略组中所有安全策略。

parameters：指定一个安全联盟 SA（Security Association）所对应的目的 IP 地址、安全协议、SPI（Security Parameter Index）。

ip-address：指定目的地址，格式为点分十进制的 IP 地址格式。

protocol：指定安全协议，可选关键字为 **ah** 或 **esp**，不区分大小写。**ah** 是指报文头认证（Authentication Header）协议，**esp** 是指封装安全协议（Encapsulation Security Protocol）。

spi-number：指定安全参数索引，取值范围是 256～4294967295。

【描述】

reset ipsec sa 命令删除已经建立的安全联盟（无论是手工建立的还是通过 IKE 协商建立的）。如果未指定 **remote**、**policy**、**parameters**，则删除所有的安全联盟。

一个安全联盟由三元组目的 IP 地址、安全协议、SPI 唯一地标识，安全联盟可以通过手工建立，也可以通过 IKE（Internet Key Exchange）协商建立。

通过手工建立的安全联盟被删除后，系统会自动根据对应的手工安全策略建立新的安全联盟。

而通过 IKE 协商建立的安全联盟被删除后，如果有报文重新触发 IKE 协商，IKE 将重新协商并建立新的安全联盟。

如果指定了 **parameters** 关键字，由于安全联盟是成对出现的，删除了一个方向的安全联盟，另一个方向的安全联盟也会被删除。

相关配置可参考命令 **display ipsec sa**。

【举例】

删除所有安全联盟。

```
<H3C> reset ipsec sa
```

删除对端地址为 10.1.1.2 的安全联盟。

```
<H3C> reset ipsec sa remote 10.1.1.2
```

删除安全策略模板 policy1 中的所有安全联盟。

```
<H3C> reset ipsec sa policy policy1
```

删除安全策略名称为 policy1、顺序号为 10 的安全联盟。

```
<H3C> reset ipsec sa policy policy1 10
```

删除对端地址为 10.1.1.2、安全协议为 AH、安全参数索引为 10000 的安全联盟。

```
<H3C> reset ipsec sa parameters 10.1.1.2 ah 10000
```

3.1.31 reset ipsec statistics

【命令】

reset ipsec statistics

【视图】

用户视图

【参数】

无

【描述】

reset ipsec statistics 命令用来清除 IPsec 的报文统计信息，所有的统计信息都被设置成 0。

相关配置可参考命令 **display ipsec statistics**。

【举例】

清除 IPsec 的报文统计信息。

```
<H3C> reset ipsec statistics
```

3.1.32 sa authentication-hex

【命令】

sa authentication-hex { **inbound** | **outbound** } { **ah** | **esp** } *hex-key*

undo sa authentication-hex { **inbound** | **outbound** } { **ah** | **esp** }

【视图】

手工方式安全策略视图

【参数】

inbound：设置入方向安全联盟的参数，IPsec 使用入方向安全联盟处理接收的报文。

outbound：设置出方向安全联盟的参数，IPsec 使用出方向安全联盟处理发送的报文。

ah：设置采用 AH 协议的安全联盟的参数。如果安全策略引用的提议规定了采用 AH 协议，使用 **ah** 关键字来设置安全联盟的参数。

esp：设置采用 ESP 协议的安全联盟的参数。如果安全策略引用的提议规定了采用 ESP 协议，使用 **esp** 关键字来设置安全联盟的参数。

hex-key：指定安全联盟的认证密钥，以 16 进制格式输入。如果使用 MD5 算法，密钥长度为 16 个字节；如果使用 SHA1 算法，密钥长度为 20 个字节。

【描述】

sa authentication-hex 命令用来对 **manual** 方式安全策略手工设置安全联盟的认证密钥，**undo sa authentication-hex** 命令用来删除设置的安全联盟的认证密钥。

此命令仅用于 **manual** 方式的安全策略。

对于 **isakmp** 方式的安全策略，IKE 将自动协商安全联盟的参数并创建安全联盟，不需要手工设置安全联盟的参数，该命令无效。

在配置 **manual** 方式的安全策略时，必须分别设置 **inbound** 和 **outbound** 两个方向安全联盟的参数。

在安全隧道的两端设置的安全联盟参数必须是完全匹配的。本端的入方向安全联盟的密钥必须和对端的出方向安全联盟的密钥一样；本端的出方向安全联盟密钥必须和对端的入方向安全联盟的密钥一样。

输入密钥有两种方式：16 进制方式和字符串方式。如果以字符串方式输入密钥，需要使用命令 **sa string-key**。如果分别以两种方式输入了密钥，则最后设定的密钥有效。在安全隧道的两端，应当以相同的方式输入密钥。如果一端以字符串方式输入密钥，另一端以 16 进制方式输入密钥，则不能通讯。

相关配置可参考命令 **ipsec policy**（系统视图），**ipsec policy**（接口视图），**security acl**，**tunnel local**，**tunnel remote**，**sa duration**，**proposal**。

【举例】

在采用 AH 协议及 MD5 算法的安全策略中，设置输入安全联盟的 SPI 为 10000，密钥为 0x112233445566778899aabbccddeeff00；输出安全联盟的 SPI 为 20000，密钥为 0xaabbccddeeff001100aabbccddeeff00。

```
[H3C] ipsec proposal prop_ah
[H3C-ipsec-proposal-prop_ah] transform ah
[H3C-ipsec-proposal-prop_ah] ah authentication-algorithm md5
[H3C-ipsec-proposal-prop_ah] quit
[H3C] ipsec policy tianjin 100 manual
[H3C-ipsec-policy-manual-tianjin-100] proposal prop_ah
[H3C-ipsec-policy-manual-tianjin-100] sa spi inbound ah 10000
```

```
[H3C-ipsec-policy-manual-tianjin-100] sa authentication-hex inbound ah
11223344556677889aabbccddeeff00
[H3C-ipsec-policy-manual-tianjin-100] sa spi outbound ah 20000
[H3C-ipsec-policy-manual-tianjin-100] sa authentication-hex outbound ah
aabbccddeeff001100aabbccddeeff00
```

3.1.33 sa duration

【命令】

sa duration { **traffic-based** *kilobytes* | **time-based** *seconds* }

undo sa duration { **traffic-based** | **time-based** }

【视图】

安全策略视图、安全策略模板视图

【参数】

time-based *seconds*：指定以时间为基准的生存周期，*seconds* 的取值范围是 120～604800，单位是秒，缺省值是 3600 秒。

traffic-based *kilobytes*：指定以流量为基准的生存周期，*kilobytes* 的取值范围是 256～4194303，单位是千字节，缺省值是 1843200 千字节。

【描述】

sa duration 命令用来为安全策略设置安全联盟的生存周期，**undo sa duration** 命令用来取消设置的生存周期，即恢复使用设定的全局生存周期。

当 IKE 协商安全联盟时，如果采用的安全策略没有配置自己的生存周期，将采用全局生存周期与对端协商。如果安全策略配置了自己的生存周期，则系统使用安全策略自己的生存周期与对端协商。IKE 为 IPsec 协商建立安全联盟时，对于 IKE 第 1 阶段，安全联盟的生存周期由发起方决定；对于 IKE 第 2 阶段，采用本地设置的生和对端提议的生存周期中较小的一个。

衡量生存周期有两种方式：“基于时间”的生存周期和“基于流量”的生存周期。基于时间的生存周期是从安全联盟建立开始，此安全联盟存活的时间；基于流量的生存周期是此安全联盟允许处理的最大流量。如果生存周期到达指定的时间或指定的流量，则安全联盟就会失效。安全联盟失效前，IKE 将为 IPsec 协商建立新的安全联盟，这样，在旧的安全联盟失效前，新的安全联盟就已经准备好。在新的安全联盟开始协商而没有协商好之前，继续使用旧的安全联盟保护通信。在新的安全联盟协商好之后，则立即采用新的安全联盟保护通信。

安全联盟的生存周期只对通过 IKE 协商的安全联盟起作用，而对通过手工方式建立的安全联盟不起作用。

相关配置可参考命令 **ipsec sa global-duration**，**ipsec policy**（系统视图），**ipsec policy**（接口视图），**security acl**，**tunnel local**，**tunnel remote**，**proposal**。

【举例】

设置安全策略的安全联盟生存周期为两个小时，即 7200 秒。

```
[H3C] ipsec policy shenzhen 100 isakmp
[H3C-ipsec-policy-isakmp-shenzhen-100] sa duration time-based 7200
```

设置安全策略的安全联盟生存周期为 20M 字节，即 20,000 千字节。

```
[H3C] ipsec policy shenzhen 100 isakmp
[H3C-ipsec-policy-isakmp-shenzhen-100] sa duration traffic-based 20000
```

3.1.34 sa encryption-hex

【命令】

sa encryption-hex { **inbound** | **outbound** } **esp** *hex-key*

undo sa encryption-hex { **inbound** | **outbound** } **esp**

【视图】

手工方式安全策略视图

【参数】

inbound：设置入方向安全联盟的参数，IPsec 使用入方向安全联盟处理接收的报文。

outbound：设置出方向安全联盟的参数，IPsec 使用出方向安全联盟处理发送的报文。

esp：设置采用 ESP 协议的安全联盟的参数。如果安全策略引用的提议规定了采用 ESP 协议，使用 **esp** 关键字来设置安全联盟的参数。

hex-key：使用 ESP 协议时，指定安全联盟的加密密钥。以 16 进制格式输入，输入的密钥长度必须符合所采用的加密算法的要求。如果使用 DES 算法，密钥长度为 8 个字节；如果使用 3DES 算法，密钥长度为 24 个字节。

【描述】

sa encryption-hex 命令用来对 **manual** 方式的安全策略手工设置安全联盟的加密密钥参数，**undo sa encryption-hex** 命令用来删除设置的安全联盟的加密密钥参数。

此命令仅用于 **manual** 方式的安全策略，来手工设置安全联盟的参数，实现手工创建安全联盟。

对于 **isakmp** 方式的安全策略，IKE 将自动协商安全联盟的参数并创建安全联盟，不需要手工设置安全联盟的参数，该命令无效。

在为系统配置安全联盟时，必须分别设置 **inbound** 和 **outbound** 两个方向安全联盟的参数。

在安全隧道的两端设置的安全联盟参数必须是完全匹配的。本端的入方向安全联盟的加密密钥必须和对端的出方向安全联盟的加密密钥一样；本端的出方向安全联盟的加密密钥必须和对端的入方向安全联盟的加密密钥一样。

相关配置可参考命令 **ipsec policy**（系统视图），**ipsec policy**（接口视图），**security acl**，**tunnel local**，**tunnel remote**，**sa duration**，**proposal**。

【举例】

在采用 ESP 协议及 DES 加密算法的安全策略中，设置入方向安全联盟的 SPI 为 1001，加密算法的密钥为 0x1234567890abcdef；输出安全联盟的 SPI 为 2001，加密算法的密钥为 0x abcdefabcdef1234。

```
[H3C] ipsec proposal prop_esp
[H3C-ipsec-proposal-prop_esp] transform esp
[H3C-ipsec-proposal-prop_esp] esp encryption-algorithm des
[H3C-ipsec-proposal-prop_esp] quit
[H3C] ipsec policy tianjin 100 manual
[H3C-ipsec-policy-manual-tianjin-100] proposal prop_esp
[H3C-ipsec-policy-manual-tianjin-100] sa spi inbound esp 1001
[H3C-ipsec-policy-manual-tianjin-100]  sa  encryption-hex  inbound  esp
1234567890abcdef
[H3C-ipsec-policy-manual-tianjin-100] sa spi outbound esp 2001
[H3C-ipsec-policy-manual-tianjin-100]  sa  encryption-hex  outbound  esp
abcdefabcdef1234
```

3.1.35 sa spi

【命令】

sa spi { **inbound** | **outbound** } { **ah** | **esp** } *spi-number*

undo sa spi { **inbound** | **outbound** } { **ah** | **esp** }

【视图】

手工方式安全策略视图

【参数】

inbound：设置入方向安全联盟的参数，IPsec 使用入方向安全联盟处理接收的报文。

outbound：设置出方向安全联盟的参数，IPsec 使用出方向安全联盟处理发送的报文。

ah：设置采用 AH 协议的安全联盟的参数。如果安全策略引用的提议规定了采用 AH 协议，使用 **ah** 关键字来设置安全联盟的参数。

esp：设置采用 ESP 协议的安全联盟的参数。如果安全策略引用的提议规定了采用 ESP 协议，使用 **esp** 关键字来设置安全联盟的参数。

spi-number：安全联盟三元组标识中的安全参数索引 SPI（Security Parameter Index），取值范围为 256～4294967295。在系统中，安全联盟的三元组标识<SPI、目的地址、安全协议>必须是唯一的。

【描述】

sa spi 命令用来对 **manual** 方式的安全策略手工设置安全联盟的 SPI（安全参数索引）参数，**undo sa spi** 命令用来删除设置的安全联盟的 SPI（安全参数索引）参数。

此命令仅用于 **manual** 方式的安全策略，用该命令手工设置安全联盟的参数，实现手工创建安全联盟。

对于 **isakmp** 方式的安全策略，IKE 将自动协商安全联盟的参数并创建安全联盟，不需要手工设置安全联盟的参数，该命令无效。

在为系统配置安全联盟时，必须分别设置 **inbound** 和 **outbound** 两个方向安全联盟的参数。

在安全隧道的两端设置的安全联盟参数必须是完全匹配的。本端的入方向安全联盟的 SPI 必须和对端的出方向安全联盟的 SPI 一样；本端的出方向安全联盟的 SPI 必须和对端的入方向安全联盟的 SPI 一样。

相关配置可参考命令 **ipsec policy**（系统视图），**ipsec policy**（接口视图），**security acl**，**tunnel local**，**tunnel remote**，**sa duration**，**proposal**。

【举例】

在采用 AH 协议及 MD5 算法的安全策略中设置输入安全联盟的 SPI 为 10000，输出安全联盟的 SPI 为 20000。

```
[H3C] ipsec proposal prop_ah
[H3C-ipsec-proposal-prop_ah] transform ah
[H3C-ipsec-proposal-prop_ah] ah authentication-algorithm md5
[H3C-ipsec-proposal-prop_ah] quit
[H3C] ipsec policy tianjin 100 manual
[H3C-ipsec-policy-manual-tianjin-100] proposal prop_ah
[H3C-ipsec-policy-manual-tianjin-100] sa spi inbound ah 10000
[H3C-ipsec-policy-manual-tianjin-100] sa spi outbound ah 20000
```

3.1.36 sa string-key

【命令】

sa string-key { **inbound** | **outbound** } { **ah** | **esp** } *string-key*

undo sa string-key { **inbound** | **outbound** } { **ah** | **esp** }

【视图】

手工方式安全策略视图

【参数】

inbound：设置入方向安全联盟的参数，IPsec 使用入方向安全联盟处理接收的报文。

outbound：设置出方向安全联盟的参数，IPsec 使用出方向安全联盟处理发送的报文。

ah：设置采用 AH 协议的安全联盟的参数。如果安全策略引用的提议规定了采用 AH 协议，使用 **ah** 关键字来设置安全联盟的参数。

esp：设置采用 ESP 协议的安全联盟的参数。如果安全策略引用的提议规定了采用 ESP 协议，使用 **esp** 关键字来设置安全联盟的参数。

string-key：指定安全联盟的密钥，以字符串格式输入，长度 1～255 个字符。对不同的算法，均可输入不超过长度范围的字符串，系统会根据输入的字符串自动生成符合算法要求的密钥。对于 ESP 协议，系统会自动地同时生成认证算法的密钥和加密算法的密钥。

【描述】

sa string-key 命令用来对 **manual** 方式的安全策略手工设置安全联盟的参数，**undo sa string-key** 命令用来删除设置的安全联盟的参数。

此命令仅用于 **manual** 方式的安全策略，用该命令手工设置安全联盟的参数，实现手工创建安全联盟。

对于 **isakmp** 方式的安全策略，IKE 将自动协商安全联盟的参数并创建安全联盟，不需要手工设置安全联盟的参数，该命令无效。

在为系统配置安全联盟时，必须分别设置 **inbound** 和 **outbound** 两个方向安全联盟的参数。

在安全隧道的两端设置的安全联盟参数必须是完全匹配的。本端入方向安全联盟的密钥必须和对端出方向安全联盟的密钥一样；本端出方向安全联盟的密钥必须和对端入方向安全联盟的密钥一样。

输入密钥有两种方式：16 进制方式和字符串方式。如果以 16 进制方式输入密钥需要使用命令 **sa authentication-hex** 和 **sa encryption-hex**。如果分别以两种方式输入了密钥，则最后设定的密钥有效。在安全隧道的两端，应当以相同的方式输入密钥。如果一端以字符串方式输入密钥，另一端以 16 进制方式输入密钥，则不能正确地建立安全隧道。

相关配置可参考命令 **ipsec policy**（系统视图），**ipsec policy**（接口视图），**security acl**，**tunnel local**，**tunnel remote**，**sa duration**，**proposal**。

【举例】

在采用 AH 协议及 MD5 算法的安全策略中，设置输入安全联盟的 SPI 为 10000，密钥为字符串 abcdef；输出安全联盟的 SPI 为 20000，密钥为字符串 efcdab。

```
[H3C] ipsec proposal prop_ah
[H3C-ipsec-proposal-prop_ah] transform ah
[H3C-ipsec-proposal-prop_ah] ah authentication-algorithm md5
[H3C-ipsec-proposal-prop_ah] quit
[H3C] ipsec policy tianjin 100 manual
[H3C-ipsec-policy-manual-tianjin-100] proposal prop_ah
[H3C-ipsec-policy-manual-tianjin-100] sa spi inbound ah 10000
[H3C-ipsec-policy-manual-tianjin-100] sa string-key inbound ah abcdef
[H3C-ipsec-policy-manual-tianjin-100] sa spi outbound ah 20000
[H3C-ipsec-policy-manual-tianjin-100] sa string-key outbound ah efcdab
```

3.1.37 security acl

【命令】

security acl *acl-number*

undo security acl

【视图】

安全策略视图、安全策略模板视图

【参数】

acl-number：指定安全策略所引用的访问控制列表号，取值范围是 3000～3999。

【描述】

security acl 命令用来设置安全策略引用的访问控制列表，**undo security acl** 命令用来取消安全策略引用的访问控制列表。

缺省情况下，安全策略没有指定访问控制列表。

安全策略所保护的数据流由此命令指定的 ACL 来定义。在实施 IPsec 安全策略时，系统首先检查通过接口的报文是否与 ACL 中的规则匹配，如果匹配且是被访问控制列表允许（**permit**）的报文，则系统对报文进行 IPsec 保护后再发送。如果不匹配，或者访问控制列表拒绝（**deny**）的报文，则直接发送报文。

对于手工方式创建的安全策略，只支持保护访问控制列表下的一条规则，即只有最先匹配此访问控制列表的报文被保护，后续匹配此访问控制列表中其它规则的报文不会被保护。

相关配置可参考命令 **ipsec policy**（系统视图），**ipsec policy**（接口视图），**tunnel local**，**tunnel remote**，**sa duration**，**proposal**。

【举例】

设置安全策略引用 3001 号访问控制列表。

```
[H3C] acl number 3001
[H3C-acl-adv-3001] rule permit tcp source 10.1.1.0 0.0.0.255 destination
10.1.2.0 0.0.0.255
[H3C] ipsec policy beijing 100 manual
[H3C-ipsec-policy-manual-beijing-100] security acl 3001
```

3.1.38 time-out

【命令】

time-out *seconds*

undo time-out

【视图】

DPD 结构视图

【参数】

seconds：等待 DPD 应答报文的超时时间，取值范围 1～60 秒。

【描述】

time-out 命令用来配置等待 DPD 应答报文的超时时间，**undo time-out** 命令用来恢复等待 DPD 应答报文超时时间为缺省值。

缺省情况下，超时时间为 5 秒。

【举例】

设置 time-out 为 2 秒。

```
[H3C-ike-dpd-aaa] time-out 2
```

重置 time-out 为 5 秒。

```
[H3C-ike-dpd-aaa] undo time-out
```

3.1.39 transform

【命令】

transform { **ah** | **ah-esp** | **esp** }

undo transform

【视图】

安全提议视图

【参数】

ah：设置采用 RFC 2402 规定的 AH 协议。

ah-esp：设置先用 ESP 协议对报文进行保护，再用 AH 协议进行保护。

esp：设置采用 RFC 2406 规定的 ESP 协议。

【描述】

transform 命令用来设置提议采用的安全协议，**undo transform** 命令用来恢复缺省的安全协议。

缺省情况使用 **esp**，即 RFC 2406 规定的 ESP 协议。

如果采用 ESP 协议，则缺省的加密算法为 DES，认证算法为 MD5。

如果采用 AH 协议，则缺省的认证算法为 MD5。

如果指定参数 **ah-esp**，则 AH 缺省的认证算法为 MD5，ESP 协议缺省使用的加密算法为 DES，不使用认证算法。

AH 协议提供数据源认证、数据完整性校验和防报文重放功能。

ESP 协议提供数据源认证、数据完整性校验、防报文重放和数据加密功能。

在安全隧道的两端，IPsec 提议所使用的安全协议需要匹配。

不同安全协议在 transport 和 tunnel 模式下的数据封装形式如下图：

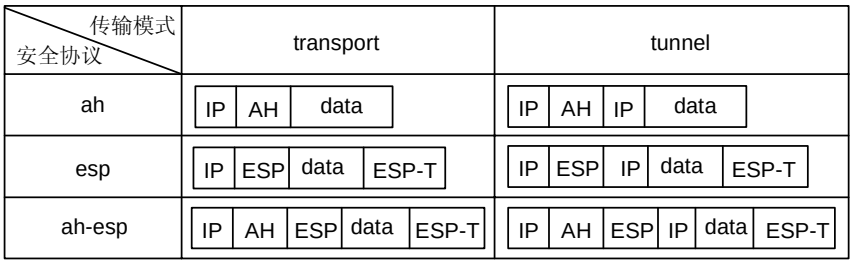

图3-1 安全协议数据封装格式

上图中的 data 为原 IP 报文。

相关配置可参考命令 **ah authentication-algorithm**，**ipsec proposal**，**esp encryption-algorithm**，**esp authentication-algorithm**，**encapsulation-mode**，**proposal**。

【举例】

设置一个采用 AH 协议的提议。

```
[H3C] ipsec proposal prop1
[H3C-ipsec-proposal-prop1] transform ah
```

3.1.40 tunnel local

【命令】

tunnel local *ip-address*

undo tunnel local

【视图】

手工方式安全策略视图

【参数】

ip-address：本端地址，格式为点分十进制格式。

【描述】

tunnel local 命令用来设置安全策略的本端地址，**undo tunnel local** 命令用来删除在安全策略中设定的本端地址。

缺省情况下，没有配置安全隧道的本端地址。

对于 **isakmp** 方式的安全策略，不需要设置本端地址，该命令无效。IKE 能够自动从应用该安全策略的接口上获取本端地址。

对于 **manual** 方式的安全策略，必须设置本端地址才能够创建安全联盟。安全隧道是建立在本端和对端之间的，故必须正确设置本端地址和对端地址才能成功地建立一条安全隧道。

相关配置可参考命令 **ipsec policy**（系统视图），**ipsec policy**（接口视图），**security acl**，**tunnel remote**，**sa duration**，**proposal**。

【举例】

设置安全策略的本地地址，该安全策略应用在 IP 地址为 10.0.0.1 的 Ethernet 1/0/0 接口上。

```
[H3C] ipsec policy guangzhou 100 manual
[H3C-ipsec-policy-manual-guangzhou-100] tunnel local 10.0.0.1
[H3C-ipsec-policy-manual-guangzhou-100] quit
[H3C] interface Ethernet 1/0/0
[H3C-Ethernet1/0/0] ipsec policy guangzhou
```

3.1.41 tunnel remote

【命令】

tunnel remote *ip-address*

undo tunnel remote [*ip-address*]

【视图】

手工方式安全策略视图

【参数】

ip-address：安全策略的隧道对端地址，格式为点分十进制格式。

【描述】

tunnel remote 命令用来设置安全策略的隧道对端地址，**undo tunnel remote** 命令用来删除安全策略中设置的隧道对端地址。

缺省情况下，没有配置安全隧道的对端地址。

对于 **manual** 方式的安全策略，如果已经设置了对端地址，必须先删除原先的地址才能设置新的对端地址。

安全隧道是建立在本端和对端之间，在安全隧道的两端，均需要正确设置对端地址。

相关配置可参考命令 **ipsec policy**（系统视图），**ipsec policy**（接口视图），**security acl**，**tunnel local**，**sa duration**，**proposal**。

【举例】

设置安全策略的对端地址为 10.1.1.2。

```
[H3C] ipsec policy shanghai 10 manual
[H3C-ipsec-policy-manual-shanghai-10] tunnel remote 10.1.1.2
```

3.2 加密卡配置命令

3.2.1 debugging encrypt-card host

【命令】

debugging encrypt-card host { **all** | **command** | **error** | **misc** | **packet** | **sa** }

undo debugging encrypt-card host { **all** | **command** | **error** | **misc** | **packet** | **sa** }

【视图】

用户视图

【参数】

all：打开加密卡上所有信息的调试开关。

command：打开加密卡上命令信息的调试开关。

error：打开加密卡上错误信息的调试开关。

misc：打开加密卡上其他信息的调试开关。

packet：打开加密卡上报文处理开关。

sa：打开加密卡上安全联盟信息调试开关。

【描述】

debugging encrypt-card host 命令用来打开加密卡侧 Comware 主体测试软件的调试信息开关，**undo debugging encrypt-card host** 命令用来关闭调试信息开关。

【举例】

打开加密卡侧 Comware 主体测试软件的命令调试开关。

```
<H3C> debugging encrypt-card host command
```

3.2.2 display encrypt-card fast-switch

【命令】

display encrypt-card fast-switch

【视图】

所有视图

【参数】

无

【描述】

display encrypt-card fast-switch 命令用来显示加密卡的快转表项。

【举例】

显示加密卡的快转表项。

```
[H3C] display encrypt-card fast-switch
  encrypt-card Fast-Forwarding cache:
Index SourIP   SourPort     DestIP   DestPort     Prot     TdbID    Type
18    1.1.1.2      8        1.1.1.1      0        1 0x00000024     encrypt
130   1.1.1.1      0        1.1.1.2      0        50 0x00000023    decrypt
```

表3-11 display encrypt-card fast-switch 命令显示信息描述表

域名	描述
Index	快转表项的索引
SourIP	源 IP
SourPort	源端口
DestIP	目的 IP
DestPort	目的端口

域名	描述
Prot	指协议号
TdbID	为加密这条流所使用的 TDB 的 ID
Type	有两种，encrypt 和 decrypt，指出方向（加密）和入方向（解密）

3.2.3 display interface encrypt

【命令】

display interface encrypt [*slot-id*]

【视图】

所有视图

【参数】

slot-id：防火墙槽位号。

【描述】

display interface encrypt 命令用来显示加密卡接口信息。

该命令可以查询加密卡的状态、加密卡收发的报文总数、每秒丢弃的最大报文数以及过去 5 秒的相关的信息。

相关配置可参考 **interface encrypt**。

【举例】

显示防火墙 1/0 槽位加密卡接口的信息。

```
[H3C] display interface Encrypt 1/0
Description :  Encrypt1/0 Interface
  Protocol Status:    READY
  Driver Status  :    READY
  Total Statistics
    Packets sent to card              :    10
    Packets received from card        :    9
    Bytes sent to card                :    1216
    Bytes received from card          :    584
    Dropped packets                 :    0
  Statistics during last 5 seconds
    Packets sent to card              :    0
    Packets received from card        :    0
    Bytes sent to card                :    0
    Bytes received from card          :    0
```

```
    Dropped packets                 :    0
```

以上信息显示了防火墙 1/0 槽位加密卡的协议状态、驱动器状态、收发包总数、收发字节总数、每秒的最大丢包数以及在过去 5 秒中的相应的信息的统计。

3.2.4 encrypt-card backuped

【命令】

encrypt-card backuped

undo encrypt-card backuped

【视图】

系统视图

【参数】

无

【描述】

encrypt-card backuped 命令用来使能加密卡的主机备份功能。**undo encrypt-card backuped** 命令用来禁止加密卡的主机备份功能。

缺省情况下，主机备份加密卡功能是被禁止的。

对于使用加密卡进行 IPsec 处理的安全联盟，若该加密卡状态正常，IPsec 就由该加密卡进行处理。当该加密卡状态异常时，如果已经开启了加密卡主机备份开关，并且 Comware 主体软件 IPsec 模块支持该安全联盟所使用的加密/认证算法，则由 Comware 主体软件 IPsec 模块替代加密卡对报文进行 IPsec 处理；若 Comware 主体软件 IPsec 模块不支持该安全联盟使用的算法，则报文被丢弃。

【举例】

使能加密卡主机备份功能

```
[H3C] encrypt-card backuped
```

3.2.5 encrypt-card fast-switch

【命令】

encrypt-card fast-switch

undo encrypt-card fast-switch

【视图】

系统视图

【参数】

无

【描述】

encrypt-card fast-switch 命令用来使能加密卡快转功能，**undo encrypt-card fast-switch** 命令用来关闭加密卡快转功能。

缺省情况下，关闭加密卡快转功能。

加密卡快转指的是对于[SourIP, SourPort, DestIP, DestPort, Prot] 五元组相同的一系列报文，防火墙在接收或发送第一个报文时就会创建一个快转表项，之后符合此表项的所有报文都会直接被发往加密卡进行加密或解密，然后再由加密卡发往目的出口，这样省去了对每个报文逐一进行从 IP 到 IPsec 的处理，加速了处理过程。

⚠ 注意：

开启加密卡快转功能后，经过加密卡快转的报文将不进行 ACL 的统计计数。

【举例】

使能加密卡快转功能。

```
[H3C] encrypt-card fast-switch
```

3.2.6 interface encrypt

【命令】

interface encrypt *slot-id*

【视图】

系统视图

【参数】

slot-id：防火墙槽位号。

【描述】

interface encrypt 命令用来进入加密卡接口视图。

进入加密卡的接口模式后，只能进行 **shutdown** 和 **undo shutdown** 命令的操作，分别对加密卡进行禁用和使能操作。

【举例】

进入槽位 1/0 的加密卡接口

```
[H3C] interface encrypt 1/0
```

```
[H3C-Encrypt1/0]
```

3.2.7 ipsec card-proposal

【命令】

ipsec card-proposal *proposal-name*

undo ipsec card-proposal *proposal-name*

【视图】

系统视图

【参数】

proposal-name：加密卡安全提议的名称，小于 16 个字符组成的字符串，不区分大小写。

【描述】

ipsec card-proposal 命令用来创建并进入加密卡安全提议视图。**undo ipsec card-proposal** 命令用来删除加密卡安全提议。

本命令适用于加密卡提议视图（相应的加密/解密/认证在加密卡上完成）；而主机软件同时还兼容应用于主机本身的安全提议视图（命令为 **ipsec proposal**），相应的加密/解密/认证处理由主机完成。在本视图下的操作中除了增加了 **use encrypt-card** 命令用来指定加密卡安全提议使用的加密卡的槽位外，其他的配置与 **ipsec proposal** 命令完全相同。

在完成安全提议下的配置后，需要使用命令 **quit** 退回到系统视图进行其他信息的设置。

【举例】

创建名称为 card 的加密卡安全提议、使用 1/0 槽位的加密卡，并且进行安全和加密算法的配置。

```
[H3C] ipsec card-proposal card
[H3C-ipsec-card-proposal-card] use encrypt-card 1/0
[H3C-ipsec-card-proposal-card] transform ah-esp
[H3C-ipsec-card-proposal-card] ah authentication-algorithm sha1
[H3C-ipsec-card-proposal-card] esp authentication-algorithm sha1
[H3C-ipsec-card-proposal-card] esp encryption-algorithm 3des
[H3C-ipsec-card-proposal-card] quit
[H3C]
```

以上配置创建了名为 card 的加密卡安全提议，使用防火墙槽位 1/0 上的加密卡，设置采用的安全协议为 ah-esp，AH 的认证算法为 SHA1，ESP 的认证和加密算法分别为 SHA1 和 3DES。最后退回到系统视图。

3.2.8 reset counters interface encrypt

【命令】

reset counters interface encrypt [*slot-id*]

【视图】

用户视图

【参数】

slot-id：防火墙槽位号。

【描述】

reset counters interface encrypt 命令用来清除加密卡的统计信息。

加密卡的统计信息记录了从加密卡正常工作到清除前的所有的统计信息，在调试的过程中，往往需要通过一段时间的统计信息来分析问题，这样，就需要现将加密卡的统计信息清除，使加密卡的计数器重新开始计数来获得特定时间段的统计信息。

相关配置可参考命令 **ipsec card-proposal**。

【举例】

删除 1/0 槽位上加密卡的统计信息。

```
<H3C> reset counters interface encrypt-card 1/0
```

3.2.9 reset encrypt-card fast-switch

【命令】

reset encrypt-card fast-switch

【视图】

用户视图

【参数】

无

【描述】

reset encrypt-card fast-switch 命令用来清除加密卡的快速转发信息。

【举例】

清除加密卡的快速转发信息。

```
<H3C> reset encrypt-card fast-switch
```

3.2.10 reset encrypt-card sa

【命令】

reset encrypt-card sa [*slot-id*]

【视图】

用户视图

【参数】

slot-id：防火墙槽位号。

【描述】

reset encrypt-card sa 命令用来删除指定加密卡上的安全联盟。

在调试的过程中为了仅输出需要的信息，可以通过 **reset encrypt-card sa** 命令删除加密卡上备份的主机安全联盟数据库的信息。

相关配置可参考命令 **ipsec card-proposal**。

📖 **说明：**

目前的加密卡尚不支持此命令。

【举例】

删除 1/0 槽位上加密卡上的安全联盟。

```
<H3C> reset encrypt-card sa 1/0
```

3.2.11 reset encrypt-card statistics

【命令】

reset encrypt-card statistics [*slot-id*]

【视图】

用户视图

【参数】

slot-id：防火墙槽位号。

【描述】

reset encrypt-card statistics 命令用来清除加密卡处理过程中的统计信息。

加密卡记录了自上次复位至当前为止的协议处理情况，包括 ESP/AH 包的输入/输出个数、丢包统计、认证失败统计、错误 SA 统计、非法加密卡安全提议统计、非法协议统计等信息。

📖 **说明：**

目前的加密卡尚不支持此命令。

【举例】

清除 1/0 槽位上加密卡处理过程中的统计信息。

```
<H3C> reset encrypt-card statistic 1/0
```

3.2.12 reset encrypt-card syslog

【命令】

reset encrypt-card syslog [*slot-id*]

【视图】

用户视图

【参数】

slot-id：防火墙槽位号。

【描述】

reset encrypt-card syslog 命令用来清除加密卡上所有的日志信息。

加密卡侧保留了日志历史信息，并以增量形式逐渐增多，每次查询加密卡日志时都会上报所有信息（包含很久以前的过时信息），不利于对日志的监控和定位问题，因此可以通过 **reset encrypt-card syslog** 命令及时清除加密卡日志缓冲区中的信息。

📖 **说明：**

目前的加密卡尚不支持此命令。

【举例】

删除 1/0 槽位加密卡上的所有日志信息。

```
<H3C> reset encrypt-card syslog 1/0
```

3.2.13 snmp-agent trap enable encrypt-card

【命令】

snmp-agent trap enable encrypt-card

undo snmp-agent trap enable encrypt-card

【视图】

系统视图

【参数】

无

【描述】

snmp-agent trap enable encrypt-card 命令用来使能加密卡 SNMP 代理的 trap 监控信息开关。**undo snmp-agent trap enable encrypt-card** 命令用来关闭加密卡 trap 信息开关。

使能 trap 信息后结合简单网络管理的配置，用户将能够在网管及防火墙的控制台上查看加密卡复位信息、状态变迁信息和加密卡处理异常丢包等信息。

缺省情况下，加密卡 trap 信息开关是打开的。

【举例】

使能加密卡 trap 信息开关。

```
[H3C] snmp-agent trap enable encrypt-card
```

3.2.14 use encrypt-card

【命令】

use encrypt-card *slot-id*

undo use encrypt-card

【视图】

加密卡提议视图

【参数】

slot-id：防火墙槽位号。

【描述】

use encrypt-card 命令用来指定某个加密卡提议所使用的加密卡。**undo use encrypt-card** 命令用来取消某加密卡提议所使用的加密卡。

对于同一个加密卡提议，仅可以指定一块加密卡来进行处理，也就是说不支持多块加密卡轮循处理同一个加密卡安全提议；对于不同的加密卡安全提议可以指定相同的加密卡进行处理，即同一块加密卡可以处理多个加密卡安全提议。

相关配置可参考命令 **ipsec card-proposal**。

【举例】

加密卡提议 card 所使用的加密卡所在的槽位为 1/0。

```
[H3C] ipsec card-proposal card
[H3C-ipsec-card-proposal-card] use encrypt-card 1/0
```

第4章 IKE 配置命令

4.1 IKE 配置命令

4.1.1 authentication-algorithm

【命令】

authentication-algorithm { **md5** | **sha** }

undo authentication-algorithm

【视图】

IKE 提议视图

【参数】

md5：指定认证算法为 HMAC-MD5。

sha：指定认证算法为 HMAC-SHA1。

【描述】

authentication-algorithm 命令用来指定一个供 IKE 提议使用的认证算法，**undo authentication-algorithm** 命令用来设置认证算法为缺省值。

缺省使用 SHA1 认证算法。

相关配置可参考命令 **ike proposal**，**display ike proposal**。

【举例】

指定 IKE 提议 10 的认证算法为 MD5。

```
[H3C] ike proposal 10
[H3C-ike-proposal-10] authentication-algorithm md5
```

4.1.2 authentication-method

【命令】

authentication-method { **pre-share** | **rsa-signature** }

undo authentication-method

【视图】

IKE 提议视图

【参数】

pre-share：指定认证方法为预共享密钥（pre-shared-key）方法。

rsa-signature：指定认证方法为 PKI 数字签名方法。

【描述】

authentication-method 命令用来指定一个供 IKE 提议使用的认证方法，**undo authentication-method** 命令用来设置认证方法为缺省值。

缺省情况下，使用 pre-shared key 的认证方法。

使用此命令指定一个 IKE 策略使用的认证方法。

使用 pre-shared-key 的认证方法时必须配置认证字，请参考命令 **pre-shared-key**。

在 IKE 协商中，如果发起方使用 RSA 数字签名验证方式，那么在 IKE 对等体（IKE Peer）中配置的 **id-type**，**remote-name** 将不生效，响应方只会根据 IKE 对等体中的 **remote-address** 来选择 IKE Peer，故当使用 RSA 数字签名验证方式时，发起方和响应方都要具体指定 **remote-address**，若未配置 **remote-address**，则默认为匹配所有地址。

相关配置可参考命令 **pre-shared-key**，**ike proposal**，**display ike proposal**，**pki domain**，**pki entity**。

📖 说明：

关于 PKI 的配置，请参考本手册中的“PKI 配置”部分。

【举例】

指定 IKE 提议 10 的认证方法为 pre-shared key。

```
[H3C] ike proposal 10
[H3C-ike-proposal-10] authentication-method pre-share
```

4.1.3 debugging ike

【命令】

debugging ike { **all** | **error** | **exchange** | **message** | **misc** | **transport** }

undo debugging ike { **all** | **error** | **exchange** | **message** | **misc** | **transport** }

【视图】

用户视图

【参数】

all：所有 IKE 调试功能。

error：IKE 错误调试信息。

exchange：IKE 交换状态机调试信息。

message：IKE 消息包调试信息。

misc：IKE 所有其他调试信息。

transport：IKE 传输功能调试信息。

【描述】

debugging ike 命令用来打开 IKE 调试开关，**undo debugging ike** 命令用来关闭 IKE 调试开关。

缺省情况下，IKE 调试开关关闭。

【举例】

打开 IKE 错误信息调试开关。

```
<H3C> debugging ike error
```

4.1.4 dh

【命令】

dh { **group1** | **group2** | **group5** | **group14** }

undo dh

【视图】

IKE 提议视图

【参数】

group1：指定阶段 1 密钥协商时采用 768-bit 的 Diffie-Hellman 组。

group2：指定阶段 1 密钥协商时采用 1024-bit 的 Diffie-Hellman 组。

group5：指定阶段 1 密钥协商时采用 1536-bit 的 Diffie-Hellman 组。

group14：指定阶段 1 密钥协商时采用 2048-bit 的 Diffie-Hellman 组。

【描述】

dh 命令用来配置 IKE 阶段 1 密钥协商时所使用的 DH 密钥交换参数，**undo dh** 命令用来设置 Diffie-Hellman 组标识为缺省值。

缺省为 group1，即 768-bit 的 Diffie-Hellman 组。

相关配置可参考命令 **ike proposal**，**display ike proposal**。

【举例】

指定 IKE 提议 10 使用 1024-bit 的 Diffie-Hellman 组。

```
[H3C] ike proposal 10
[H3C-ike-proposal-10] dh group2
```

4.1.5 display ike peer

【命令】

display ike peer [*peer-name*]

【视图】

所有视图

【参数】

peer-name：IKE 对等体名，取值范围为长度 1～15 的字符串。

【描述】

display ike peer 命令用来显示 IKE 对等体的相关配置信息。

【举例】

显示 IKE 对等体的相关配置信息。

```
[H3C] display ike peer

---------------------------
 IKE Peer: remotepeer
   exchange mode: main on phase 1
   pre-shared-key: 1234567
   peer id type: ip
   peer ip address: 20.20.20.1
   local ip address: 20.20.20.100
   peer name:
   nat traversal: disable
   max-connection: 1
   dpd: ikedpd
---------------------------
```

4.1.6 display ike proposal

【命令】

display ike proposal

【视图】

所有视图

【参数】

无

【描述】

display ike proposal 命令用来显示每个 IKE 提议配置的参数。

IKE 提议按照优先级的先后顺序显示。

相关配置可参考命令 **authentication-method**，**ike proposal**，**encryption-algorithm**，**authentication-algorithm**，**dh**，**sa duration**。

【举例】

下面是一个配置了两个 IKE 提议后显示的例子。

```
[H3C] display ike proposal
priority authentication authentication encryption Diffie-Hellman duration
              method       algorithm    algorithm     group       (seconds)
------------------------------------------------------------------------------
-
 10       PRE_SHARED     SHA            DES_CBC    MODP_1024      5000
 11       PRE_SHARED     MD5            DES_CBC    MODP_768       50000
 default  PRE_SHARED     SHA            DES_CBC    MODP_768       86400
```

4.1.7 display ike sa

【命令】

display ike sa [**verbose** [**connection-id** *id* | **remote-address** *ip-address*]]

【视图】

所有视图

【参数】

verbose：显示 IKE 安全联盟的详细信息。

connection-id *id*：IKE 安全联盟的连接号。

remote-address *ip-address*：IKE 安全联盟的对端 IP 地址。

【描述】

display ike sa 命令用来显示当前由 IKE 建立的安全隧道。

相关配置可参考命令 **ike proposal**。

【举例】

显示当前由 IKE 建立的安全通道。

```
[H3C] display ike sa
    Total IKE phase-1 SAs:  1
    connection-id  peer            flag        phase   doi
  -----------------------------------------------------------
        1          172.16.2.1      RD            1     IPSEC
        2          172.16.2.1      RD            2     IPSEC

  flag meaning
  RD--READY ST--STAYALIVE RL--REPLACED FD--FADING TO--TIMEOUT
```

下表为显示信息各域的描述。

表4-1 IKE SA 显示信息描述

域名	描述
connection-id	安全通道的标识符
peer	此安全联盟的对端的 IP 地址
flag	显示此安全联盟的状态： RD（READY）：表示此 SA 已建立成功； ST（STAYALIVE）：表示此端是通道协商发起方； RL（REPLACED）：表示此通道已经被新的通道代替，一段时间后将被删除； FD（FADING）：表示此通道已发生过一次软超时，目前还在使用，在硬超时发生时，会删除此通道。 TO（TIMEOUT）：表示此 SA 在上次 keepalive 超时发生后还没有收到 keepalive 报文，如果在下次 keepalive 超时发生时仍没有收到 keepalive 报文，此 SA 将被删除。
phase	此 SA 所属阶段： Phase 1：建立安全通道进行通信的阶段，此阶段建立 ISAKMP SA； Phase 2：协商安全服务的阶段，此阶段建立 IPsec SA。
doi	SA 所属解释域

4.1.8 encryption-algorithm

【命令】

encryption-algorithm { **des-cbc** | **3des-cbc** | **aes-cbc** }

undo encryption-algorithm

【视图】

IKE 提议视图

【参数】

des-cbc：指定 IKE 安全提议采用的加密算法为 CBC 模式的 DES 算法，DES 算法采用 56 bits 的密钥进行加密。

3des-cbc：指定 IKE 安全提议采用的加密算法为 CBC 模式的 3DES 算法。3DES 算法采用 168 bits 的密钥进行加密。

aes-cbc：指定 IKE 安全提议采用的加密算法为 CBC 模式的 AES 算法。

【描述】

encryption-algorithm 命令用来指定一个 IKE 提议使用的加密算法，**undo encryption-algorithm** 命令用来设置加密算法为缺省值。

缺省情况下，使用 CBC 模式的 56-bit DES 加密算法。

相关配置可参考命令 **ike proposal**，**display ike proposal**。

【举例】

指定 IKE 提议 10 的加密算法为 CBC 模式的 56-bit DES。

```
[H3C] ike proposal 10
[H3C-ike-proposal-10] encryption-algorithm des-cbc
```

4.1.9 exchange-mode

【命令】

exchange-mode { **aggressive** | **main** }

undo exchange-mode

【视图】

ike-peer 视图

【参数】

aggressive：野蛮模式。

main：主模式。

【描述】

exchange-mode 命令用于选择 IKE 阶段 1 的协商模式，**undo exchange-mode** 命令用来恢复缺省的协商模式。

缺省情况下使用主模式。

在主模式下，只能使用 IP 地址进行 IKE 协商建立 SA，这种模式用于隧道两端都有固定 IP 地址的情况。

在 IKE 野蛮模式下，不但可以使用 IP 地址进行协商，也可以使用名称进行 IKE 协商建立 SA。当安全隧道一端的 IP 地址为自动获取时（如一端用户为拨号方式），则协商模式必须配置为 **aggressive**。

当响应方使用策略模板接受发起方的协商请求时，会根据发起方的协商模式而进行选择。

相关配置可参考命令 **id-type**。

【举例】

配置 IKE 使用主模式。

```
[H3C] ike peer new_peer
[H3C-ike-peer-new_peer] exchange-mode main
```

4.1.10 id-type

【命令】

id-type { **ip** | **name** }

undo id-type

【视图】

ike-peer 视图

【参数】

ip：选择 IP 地址作为 IKE 协商过程中使用的 ID。

name：选择名字作为 IKE 协商过程中使用的 ID。

【描述】

id-type 命令用于选择 IKE 协商过程中使用的 ID 的类型，**undo id-type** 命令恢复缺省值。

在主模式下，只能使用 IP 地址进行 IKE 协商，建立 SA。

在 IKE 野蛮模式下，不但可以使用 IP 地址进行协商，也可以使用名称进行 IKE 协商，建立 SA。

缺省情况下，使用 IP 地址作为 IKE 协商过程中使用的 ID。

相关配置可参考命令 **ike local-name**。

【举例】

配置使用名称作为 IKE 协商的依据。

```
[H3C] ike peer new_peer
[H3C-ike-peer-new_peer] id-type name
```

4.1.11 ike encrypt-card dh-computation disabled

【命令】

ike encrypt-card dh-computation disabled

undo ike encrypt-card dh-computation disabled

【视图】

系统视图

【参数】

无

【描述】

ike encrypt-card dh-computation disabled 命令用来禁止 DH 交换的硬件加速，改用软件处理。**undo ike encrypt-card dh-computation disabled** 命令用来使能 DH 交换的硬件加速。

缺省情况下，使能 DH 交换的硬件加速。

【举例】

禁止 DH 交换的硬件加速。

```
[H3C] ike encrypt-card dh-computation disabled
```

4.1.12 ike local-name

【命令】

ike local-name *name*

undo ike local-name

【视图】

系统视图

【参数】

name：指定 IKE 协商时的本端网关的名称，取值为 1～32 个字符。

【描述】

ike local-name 命令用于配置本端网关的名称，**undo ike local-name** 用来恢复本端网关的缺省名称。缺省情况下，直接使用防火墙的名称作为本端网关的名称。

当 IKE 协商的发起端使用网关名称进行协商时（即配置了 **id-type name**），本端需要配置命令 **ike local**-name。

相关配置可参考命令 **remote-name**。

【举例】

设置本端网关名为“beijing_VPN”。

```
[H3C] ike local-name beijing_VPN
```

4.1.13 ike next-payload check disabled

【命令】

ike next-payload check disabled

undo ike next-payload check disabled

【视图】

系统视图

【参数】

无

【描述】

ike next-payload check disabled 命令用来配置在 IPsec 协商过程中取消对最后一个 payload 的 next payload 域的检查，以便与某些公司的产品互通。**undo ike next-payload check disabled** 命令用来恢复缺省设置。

缺省情况下，检查 next payload 域。

Next payload 是指在 IKE 协商报文（由几个 payload 组装而成）的最后一个 payload 的通用头中 Next Payload 域。按协议规定该域必须为 0，但某些公司的设备会将该域赋其它值，为增强设备的互通性，可以通过 **ike next-payload check disabled** 命令取消 IPsec 协商过程对该域的检查。

【举例】

配置在 IPsec 协商过程中取消对最后一个 payload 的 next payload 域的检查。

```
[H3C] ike next-payload check disabled
```

4.1.14 ike peer

【命令】

ike peer *peer-name*

undo ike peer *peer-name*

【视图】

系统视图

【参数】

peer-name：IKE 对等体名，最多 15 个字符。

【描述】

ike peer 命令用于配置一个 IKE 对等体，并进入 ike peer 视图，**undo ike peer** 命令用于删除一个 IKE 对等体。

【举例】

配置 IKE 对等体为 new_peer，并进入 ike peer 视图。

```
[H3C] ike peer new_peer
[H3C-ike-peer-new_peer]
```

4.1.15 ike-peer

【命令】

ike-peer *peer-name*

undo ike-peer [*peer-name*]

【视图】

安全策略视图、安全策略模板视图

【参数】

peer-name：IKE 对等体名称，最多 15 个字符。

【描述】

ike-peer 命令用于在安全策略或安全策略模板中引用 IKE 对等体，**undo ike peer** 命令用于取消在安全策略或安全策略模板中引用 IKE 对等体。

相关配置可参考命令 **ipsec policy**。

【举例】

配置在安全策略中引入 IKE 对等体。

```
[H3C-ipsec-policy-isakmp-policy-10] ike-peer new_peer
```

4.1.16 ike proposal

【命令】

ike proposal *proposal-number*

undo ike proposal *proposal-number*

【视图】

系统视图

【参数】

proposal-number：IKE 提议序号，取值为 1～100。该序号同时表示优先级，数值越小，优先级越高。在进行 IKE 协商的时候，会从序号最小的 IKE 提议进行匹配，如果匹配则直接使用，否则继续查找。

【描述】

ike proposal 命令用来定义一个 IKE 提议。**undo ike proposal** 命令用来删除一个 IKE 提议。

缺省情况下，系统提供一条缺省的 IKE 提议，此缺省的 IKE 提议具有最低的优先级。

在系统视图下，使用此命令后，将进入 IKE 提议视图。在 IKE 提议视图下，可以使用 **authentication-method** 、 **encryption-algorithm** 、 **dh** 、 **authentication-algorithm** 和 **sa duration** 命令为 IKE 提议定义一系列的参数，包括认证方法、加密算法、认证算法、DH 组标识和生存周期。

缺省的提议具有缺省的参数，如下：

```
Encryption algorithm: DES-CBC
Authentication algorithm: HMAC-SHA1
Authentication method: Pre-Shared Key
DH group ID: MODP_768
SA duration: 86400 seconds
```

可以为进行 IKE 协商的每一端配置多条 IKE 提议，在协商时，将从优先级最高的提议开始，匹配双方都相同的提议。匹配的原则是：协商双方具有相同的加密算法、认证算法、认证方法和 DH 组标识，存活时间是由协商发起方决定的，两端不需要匹配。

相关配置可参考命令 **authentication-method**，**encryption-algorithm**，**dh**，**authentication-algorithm**，**sa duration**，**display ike proposal**。

【举例】

以下命令定义了一个 IKE 提议 10。

```
[H3C] ike proposal 10
[H3C-ike-proposal-10] authentication-algorithm md5
[H3C-ike-proposal-10] authentication-method pre-share
[H3C-ike-proposal-10] sa duration 5000
```

4.1.17 ike sa keepalive-timer interval

【命令】

ike sa keepalive-timer interval *seconds*

undo ike sa keepalive-timer interval

【视图】

系统视图

【参数】

seconds：指定通过 ISAKMP SA 向对端发送 Keepalive 报文的时间间隔。可以设定为 20 到 28800 之间的一个值。

【描述】

ike sa keepalive-timer interval 命令用来配置通过 ISAKMP SA 向对端发送 Keepalive 报文的时间间隔，**undo ike sa keepalive-timer interval** 命令用来使此功能失效。

缺省情况下，此功能无效。

配置通过 ISAKMP SA 向对端发送 Keepalive 报文的时间间隔。IKE 通过此报文维护 ISAKMP SA 的隧道状态。一般在对端使用命令 **ike sa keepalive-timer timeout** 配置了超时时间时，必须在本端配置此 Keepalive 报文发送时间间隔。当对端在配置的超时时间到后，如果对端的 ISAKMP SA 无 TIMEOUT 标记，则将其标记为 TIMEOUT，当对端再收到本端 keepalive-timer 时间到后发送的 keepalive 报文，将清除 TIMEOUT 标记；如果对端的 ISAKMP SA 已带有 TIMEOUT 标记，说明在超时时间内未收到 Keepalive 报文，则删除该 ISAKMP SA 以及对应的 IPsec SA。所以，在配置时，需使配置的超时时间比 Keepalive 报文发送时间长。

相关配置可参考命令 **ike sa keepalive-timer timeout**。

【举例】

配置本端向对端发送 Keepalive 报文的时间间隔为 20 秒。

```
[H3C] ike sa keepalive-timer interval 20
```

4.1.18 ike sa keepalive-timer timeout

【命令】

ike sa keepalive-timer timeout *seconds*

undo ike sa keepalive-timer timeout

【视图】

系统视图

【参数】

seconds：指定 ISAKMP SA 等待对端发送 Keepalive 报文的超时时间。可以设定为 20 到 28800 之间的一个值。

【描述】

ike sa keepalive-timer timeout 命令用来配置一个 ISAKMP SA 等待 Keepalive 报文的超时时间，**undo ike sa keepalive-timer timeout** 命令用来使此功能失效。

缺省情况下，此功能无效。

配置等待对端发送 Keepalive 报文的超时时间。IKE 通过此报文维护该条 ISAKMP SA 的链路状态。当对端在配置的超时时间到后，如果对端的 ISAKMP SA 无 TIMEOUT 标记，则将其标记为 TIMEOUT，当对端再收到本端 keepalive-timer 时间到后发送的 keepalive 报文，将清除 TIMEOUT 标记；如果对端的 ISAKMP SA 已带有 TIMEOUT 标记，说明在超时时间内未收到 Keepalive 报文，则删除该 ISAKMP SA 以及对应的 IPsec SA。所以在配置时，需使配置的超时时间比 Keepalive 报文发送时间长。

在网络上，一般不会出现超过连续三次的报文丢失，所以，配置超时时间时，可以采用对端配置的 Keepalive 报文发送时间间隔的三倍。

相关配置可参考命令 **ike sa keepalive-timer interval**。

【举例】

配置本端等待对端发送 Keepalive 报文的超时时间为 20 秒。

```
[H3C] ike sa keepalive-timer timeout 20
```

4.1.19 ike sa nat-keepalive-timer interval

【命令】

ike sa nat-keepalive-timer interval *seconds*

undo ike sa nat-keepalive-timer interval

【视图】

系统视图

【参数】

seconds：IKE 对等体发送 NAT Keepalive 报文的时间间隔，范围为 5～300，单位为秒。

【描述】

ike sa nat-keepalive-timer interval 命令用来配置 IKE 对等体发送 NAT Keepalive 报文的时间间隔，**undo ike sa nat-keepalive-timer interval** 命令用来恢复发送 NAT Keepalive 报文的时间间隔为缺省值。

当配置此命令时，要确保配置的时间间隔小于 NAT 转换的超时时间。

缺省情况下，IKE 对等体发送 NAT Keepalive 报文的时间间隔为 20 秒。

【举例】

配置 IKE 对等体发送 NAT Keepalive 报文的时间间隔为 30 秒。

```
[H3C] ike sa nat-keepalive-timer interval 30
```

4.1.20 local

【命令】

local { **multi-subnet** | **single-subnet** }

undo local

【视图】

ike-peer 视图

【参数】

multi-subnet：指定多子网类型。

single-subnet：指定单子网类型。

【描述】

local 命令用来配置 IKE 协商时的子网类型，**undo local** 命令用来恢复缺省的子网类型。

此命令用于与 NETSCREEN 设备互通时使用。

缺省情况下，子网类型为单子网类型。

【举例】

配置 IKE 协商时的子网类型为多子网类型。

```
[H3C-ike-peer-xhy] local multi-subnet
```

4.1.21 local-address

【命令】

local-address *ip-address*

undo local-address

【视图】

ike-peer 视图

【参数】

ip-address：IKE 协商时的本端网关的 IP 地址。

【描述】

local-address 命令用来配置 IKE 协商时的本端网关的 IP 地址，**undo local-address** 命令用来取消本端网关的 IP 地址。

一般情况下 **local-address** 不需要配置，只有当用户需要指定特殊的本端网关地址时才需要配置此命令。

【举例】

配置本端网关 IP 地址为 1.1.1.1。

```
[H3C-ike-peer-xhy] local-address 1.1.1.1
```

4.1.22 nat traversal

【命令】

nat traversal

undo nat traversal

【视图】

ike-peer 视图

【参数】

无

【描述】

nat traversal 命令用于配置 IPsec/IKE 的 NAT 穿越功能，**undo nat traversal** 命令用来取消 IPsec/IKE 的 NAT 穿越功能。

此命令适用于 IPsec/IKE 组建的 VPN 隧道中加入了 NAT 网关的情况。

为了节省 IP 地址空间，ISP 经常会在公网中加入 NAT 网关，以便于将私有 IP 地址分配给用户，此时可能会导致 IPsec/IKE 隧道的两端一端为公网地址，另一端为私网地址，所以必须在隧道两端配置 NAT 穿越，保证隧道能够正常协商建立。

【举例】

```
[H3C] ike peer new_peer
[H3C-ike-peer-new_peer] nat traversal
```

4.1.23 pre-shared-key

【命令】

pre-shared-key *key*

undo pre-shared-key

【视图】

ike-peer 视图

【参数】

key：指定的身份认证字，取值范围为 1～128 个字符。

【描述】

pre-shared-key 命令用于配置 IKE 协商所使用的身份认证字，**undo pre-shared-key** 命令用来取消 IKE 协商所使用的身份认证字。

【举例】

配置 IKE 协商所使用的身份认证字为 abcde。

```
[H3C] ike peer new_peer
[H3C-ike-peer-new_peer] pre-shared-key abcde
```

4.1.24 peer

【命令】

peer { **multi-subnet** | **single-subnet** }

undo peer

【视图】

ike-peer 视图

【参数】

multi-subnet：指定多子网类型。

single-subnet：指定单子网类型。

【描述】

peer 命令用来配置 IKE 协商时的子网类型，**undo peer** 命令用来恢复缺省的子网类型。

本命令用于与 NETSCREEN 设备互通时使用。

缺省情况下，子网类型为单子网类型。

【举例】

配置 IKE 协商时的子网类型为多子网类型。

```
[H3C-ike-peer-xhy] peer multi-subnet
```

4.1.25 remote-address

【命令】

remote-address *low-ip-address* [*high-ip-address*]

undo remote-address

【视图】

ike-peer 视图

【参数】

low-ip-address：起始 IP 地址。

high-ip-address：结束 IP 地址。

【描述】

remote-address 命令用来配置对端网关设备的 IP 地址，**undo remote-address** 命令用来删除对端网关设备的 IP 地址。

当 IKE 协商的发起端使用地址进行协商时（即配置了 **id-type ip**），发起端会发送自己的 IP 地址给对端来标识自己的身份，而响应端使用 **remote-address** *low-ip-address* [*high-ip-address*]来验证发起端。若响应端只配置了 *low-ip-address* 时，*low-ip-address* 应与发起端上 **local-address** 命令所配的 IP 地址保持一致；若响应端配置了 *low-ip-address* 和 *high-ip-address*，即配置了一个地址范围时，此地址范围应包含发起端上 **local-address** 命令所配置的 IP 地址。IKE 协商的发起端不能配置 **remote-address** 为地址范围。

【举例】

配置对端网关设备 IP 地址为 10.0.0.1。

```
[H3C] ike peer new_peer
[H3C-ike-peer-new_peer] remote-address 10.0.0.1
```

4.1.26 remote-name

【命令】

remote-name *name*

undo remote-name

【视图】

ike-peer 视图

【参数】

name：指定 IKE 协商时对端的名称，取值范围为 1～32 字符。

【描述】

remote-name 命令用来配置对端网关的名称，**undo remote-name** 命令用来删除配置的对端网关的名称。

当 IKE 协商的发起端使用网关名称进行协商时（即配置了 **id-type name**），发起端会发送自己名称给对端来标识自己的身份，而对端使用 **remote-name** *name* 来验证发起端，故此时 *name* 应与发起端上 **ike local-name** 命令所配置的名称保持一致。

【举例】

```
[H3C] ike peer new_peer
[H3C-ike-peer-new_peer] remote-name beijing
```

4.1.27 reset ike sa

【命令】

reset ike sa [*connection-id*]

【视图】

用户视图

【参数】

connection-id：指定要删除的安全隧道的连接 ID 号。如果未指定此参数，所有的阶段 1 的 SA 都会被删除。

【描述】

reset ike sa 命令用来删除 IKE 建立的安全隧道。

如果未指定 *connection-id*，所有阶段 1 的 SA 都会被删除。删除本地的安全隧道时，如果阶段 1 的 ISAKMP SA 还存在，将在此安全通道的保护下，向对端发送删除消息，通知对方清除相应的安全联盟。

IKE 使用了两个阶段的 ISAKMP：第一阶段建立 IKE 安全联盟，即 ISAKMP SA；第二阶段使用这个已经建立的 ISAKMP SA 为 IPsec 协商安全联盟，即建立 IPsec SA。

相关配置可参考命令 **display ike sa**。

【举例】

删除连接号为 2 的安全通道。

```
<H3C> display ike sa
    Total IKE phase-1 SAs:  1
    connection-id  peer            flag        phase   doi
  ----------------------------------------------------------
        1          172.16.2.1      RD            1     IPSEC
        2          172.16.2.1      RD            2     IPSEC

  flag meaning
  RD--READY ST--STAYALIVE RL--REPLACED FD--FADING TO--TIMEOUT
<H3C> reset ike sa 2
<H3C> display ike sa
    Total IKE phase-1 SAs:  1
    connection-id  peer            flag        phase   doi
  ----------------------------------------------------------
        1          172.16.2.1      RD            1     IPSEC

  flag meaning
  RD--READY ST--STAYALIVE RL--REPLACED FD--FADING TO--TIMEOUT
```

⚠ 注意：

如果先删除阶段 1 的 SA，那么在删除阶段 2 的 SA 时，就无法通知对方清除相应的 SA。

4.1.28 sa duration

【命令】

sa duration *seconds*

undo sa duration

【视图】

IKE 提议视图

【参数】

seconds：指定 ISAKMP SA 的生存周期，单位为秒，范围为 60～604800。SA 的生存周期超时时 ISAKMP SA 将自动更新。

【描述】

sa duration 命令用来指定一个 IKE 提议的 ISAKMP SA 生存周期，**undo sa duration** 命令用来设置 ISAKMP SA 生存周期为缺省值。

缺省情况下，生存周期为 86400 秒（一天）。

在设定的生存周期超时前，会提前协商另一个 SA 来替换旧的 SA。在新的 SA 还没有协商完之前，依然使用旧的 SA；在新的 SA 建立后，将立即使用新的 SA，而旧的 SA 在存活时间超时时，被自动清除。

相关配置可参考命令 **ike proposal**，**display ike proposal**。

【举例】

指定 IKE 提议 10 的 ISAKMP SA 生存周期 600 秒（10 分钟）。

```
[H3C] ike proposal 10
[H3C-ike-proposal-10] sa duration 600
```

第5章 动态 VPN 配置命令

5.1 动态 VPN 配置命令

5.1.1 algorithm-suite

【命令】

algorithm-suite *suite-number*

undo algorithm-suite

【视图】

dvpn-class 视图

【参数】

suite-number：Client 注册过程中使用的算法套件，取值范围为 1～12，缺省值为 1。

1 DES_MD5_DHGROUP1

2 DES_MD5_DHGROUP2

3 DES_SHA1_DHGROUP1

4 DES_SHA1_DHGROUP2

5 3DES_MD5_DHGROUP1

6 3DES_MD5_DHGROUP2

7 3DES_SHA1_DHGROUP1

8 3DES_SHA1_DHGROUP2

9 AES128_MD5_DHGROUP1

10 AES128_MD5_DHGROUP2

11 AES128_SHA1_DHGROUP1

12 AES128_SHA1_DHGROUP2

【描述】

algorithm-suite 命令用来配置客户端注册过程使用的算法套件，**undo algorithm-suite** 命令用来恢复缺省的客户端注册使用的算法套件。

缺省情况下客户端使用的算法套件为 1，即加密算法为 DES、验证算法为 MD5，使用 DH-gropp1 算法进行密钥协商。

【举例】

设置注册过程使用的加密算法为 AES，验证算法使用 SHA1，使用 DH-gropp1 算法进行密钥协商。

```
[H3C-dvpn-class-abc] algorithm-suite 11
```

5.1.2 authentication-client method

【命令】

authentication-client method { **none** | { **chap** | **pap** } [**domain** *isp-name*] }

【视图】

dvpn-policy 视图

【参数】

pap：表示 Server 使用 PAP 对 Client 进行验证。

none：表示 Server 不需要对 Client 进行验证。

chap：表示 Server 使用 CHAP 对 Client 进行验证。

domain *isp-name*：表示 Server 对 Client 采用域认证。

【描述】

authentication-client method 命令用来配置使用该策略的 DVPN 服务器对客户端进行身份验证的方法。目前支持 none、CHAP、和 PAP 三种认证方式。

缺省情况下，不对客户端进行验证。

【举例】

设置 DVPN 策略，Server 对 Client 进行 CHAP 验证。

```
[H3C-dvpn-policy-abc] authentication-client method chap
```

5.1.3 authentication-server method

【命令】

authentication-server method { **none** | **pre-share** }

【视图】

dvpn-class 视图

【参数】

none：表示 Client 不需要对 Server 进行验证。

pre-share：表示 Client 使用预共享密钥对 Server 进行验证。

【描述】

authentication-server method 命令用来配置客户端对其需要接入的服务器端进行身份验证。

缺省情况下，客户端不要求对服务器进行身份验证。

【举例】

设置 Client 使用 pre-share 方式对 Server 进行验证。

```
[H3C-dvpn-class-abc] authentication-server method pre-share
```

5.1.4 data algorithm-suite

【命令】

data algorithm-suite *suite-number*

undo data algorithm-suite

【视图】

dvpn-policy 视图

【参数】

suite-number：会话数据加密使用的算法套件，即 IPsec SA 使用的算法套件，取值范围为 0～12，缺省值为 1。

0 Without protection

1 DES_MD5_DHGROUP1

2 DES_MD5_DHGROUP2

3 DES_SHA1_DHGROUP1

4 DES_SHA1_DHGROUP2

5 3DES_MD5_DHGROUP1

6 3DES_MD5_DHGROUP2

7 3DES_SHA1_DHGROUP1

8 3DES_SHA1_DHGROUP2

9 AES128_MD5_DHGROUP1

10 AES128_MD5_DHGROUP2

11 AES128_SHA1_DHGROUP1

12 AES128_SHA1_DHGROUP2

【描述】

data algorithm-suite 命令用来配置转发数据的 IPsec SA 使用的算法套件。**undo data algorithm-suite** 命令用来恢复 IPsec SA 的算法套件为缺省值。

缺省情况下 IPsec SA 使用的算法套件为 1，即加密算法为 DES、验证算法为 MD5、使用 DH-gropp1 算法进行密钥协商。

【举例】

设置不对报文进行加密保护，即算法套件 0。

```
[H3C-dvpn-policy-abc] data algorithm-suite 0
```

5.1.5 data ipsec-sa duration

【命令】

data ipsec-sa duration time-based *time-interval*

undo data ipsec-sa duration time-based

【视图】

dvpn-policy 视图

【参数】

time-interval：DVPN 数据加密的 IPsec SA 的生存周期，取值范围为 180～604800 秒，缺省值为 3600 秒。

【描述】

data ipsec-sa duration time-based 命令用来配置 DVPN 的数据通信使用的加密 IPsec SA 的生存周期，**undo data ipsec-sa duration time-based** 命令用来恢复 IPsec SA 的生存周期为缺省值。

缺省情况下 IPsec SA 的生存周期为 3600 秒。

【举例】

设置 IPsec SA 的生存周期为 86400 秒。

```
[H3C-dvpn-policy-abc] data ipsec-sa duration time-based 86400
```

5.1.6 debugging dvpn

【命令】

debugging dvpn { **all** | **error** | **event** { **all** | **misc** | **register** | **session** } | **hexadecimal** | **packet** { **all** | **control** | **data** | **ipsec** } }

undo debugging dvpn { **all** | **error** | **event** { **all** | **register** | **session** | **misc** } | **hexadecimal** | **packet** { **all** | **control** | **data** | **ipsec** } }

【视图】

用户视图

【参数】

all：打开所有调试信息；

error：打开 DVPN 错误调试信息；

event：打开 DVPN 的事件调试开关，包括 register、session、misc 事件；

hexadecimal：16 进制报文显示调试开关；

packet：打开 DVPN 的报文调试开关，包括 control 控制报文、data 数据报文及 ipsec 报文。

【描述】

debugging dvpn 命令用来打开 DVPN 的调试信息开关。**undo debugging dvpn** 命令用来关闭 DVPN 调试信息开关。

缺省情况下，DVPN 调试信息开关是关闭的。

【举例】

打开 DVPN 的注册事件调试开关。

```
<H3C> debugging dvpn event register
```

5.1.7 display dvpn ipsec-sa

【命令】

display dvpn ipsec-sa { **all** | **dvpn-id** *dvpn-id* [**private-ip** *private-ip*] }

【视图】

所有视图

【参数】

all：表示所有 IPsec SA 的信息。

dvpn-id *dvpn-id*：指定 *dvpn-id*。取值范围为 1～65535。

private-ip *private-ip*：指定私网 IP 地址。

【描述】

display dvpn ipsec-sa 命令用来显示指定的 IPsec SA 的信息。

【举例】

显示 DVPN 1 的 IPsec SA 信息。

```
<H3C> display dvpn ipsec-sa dvpn-id 1

  ---------------------------
```

```
Session dvpn-id : 1
Session local   : 10.0.0.3
Session remote  : 10.0.0.2
sa mode         : DVPN
----------------------------

[Inbound ESP SAs]
 spi : 1549550209 (0x5c5c4281)
 authentication-algorithm : ESP-AUTH-MD5
 encryption-algorithm : ESP-ENCRYPT-3DES

 life duration(bytes/sec): 0/180
 remaining life duration(bytes/sec): 0/102

[Outbound ESP SAs]
 spi : 2421434273 (0x905427a1)
 authentication-algorithm : ESP-AUTH-MD5
 encryption-algorithm : ESP-ENCRYPT-3DES

 life duration(bytes/sec): 0/180
 remaining life duration(bytes/sec): 0/102
```

5.1.8 display dvpn map

【命令】

display dvpn map { **all** | **dvpn-id** d*vpn-id* | **public-ip** *public-ip* }

【视图】

所有视图

【参数】

all：表示所有的 Map 信息。

dvpn-id *dvpn-id*：指定 dvpn-id。取值范围为 1～65535。

public-ip *public-ip*：指定公网 IP 地址。

【描述】

display dvpn map 命令用来显示指定 DVPN 的 Map 信息。

显示信息包括私网地址、公网地址、端口号、DVPN 连接状态、DVPN 连接类型和客户端标识。

【举例】

显示系统当前的所有 Map 信息。

```
[H3C] display dvpn map all
  vpn-id     private-ip    public-ip     port      state   type    client-id
------------------------------------------------------------------------
       1     10.0.0.2      211.1.1.2     9876   SUCCESS  C->S     70433124
       2     11.0.0.2      211.1.1.2     9876   SUCCESS  C->S     70432548
```

5.1.9 display dvpn session

【命令】

display dvpn session { **all** | **dvpn-id** d*vpn-id* [**private-ip** *private-ip*] }

【视图】

所有视图

【参数】

dvpn-id：指定 dvpn-id。

private-IP：指定私网 IP 地址（指 Tunnel 口的 IP 地址）。

【描述】

display dvpn session 命令用来显示当前节点所拥有的全部 session 信息。

【举例】

显示 DVPN 2 的所有的 session 信息。

```
<H3C> display dvpn session dvpn-id 2
  vpn-id       private-ip        public-ip    port     state  type
 ------------------------------------------------------------
       2         11.0.0.2        211.1.1.2    9876   SUCCESS   C->S
       2         11.0.0.4      211.1.1.100   12289   SUCCESS   C->C
```

5.1.10 display dvpn info

【命令】

display dvpn info { **dvpn-id** d*vpn-id* | **global** }

【视图】

所有视图

【参数】

dvpn-id：指定 dvpn-id。取值范围为 1～65535。

global：DVPN 全局配置信息。

【描述】

display dvpn info 命令用来显示指定 DVPN 的配置信息以及当前的运行信息。

可以使用 **display dvpn info global** 显示系统当前 DVPN 的全局配置信息和运行信息。

【举例】

显示 DVPN 1 的所有信息。

```
[H3C] display dvpn info dvpn-id 1
  ------------------------------------------------
  DVPN Domain 1 Information
  ------------------------------------------------
  type             : client
  register type  : Undistributed | Forward
  session number : 1

  server           : server0
    server state      : active
    server public IP  : 211.1.1.2
    algorithm suite   : DES_MD5_DHGROUP1

  session encryption flag        : Need encryption
  data encryption flag            : Need encryption
  authentication server method   : none

  session algorithm suite        : AES128_SHA1_DHGROUP1
  session setup time              : 10
  session idle time               : 300
  session keepalive time         : 10
  data algorithm suite            : 3DES_MD5_DHGROUP2
  data ipsecsa duration time     : 180
  data ipsecsa duration byte     : 0

  input packets                     : 17160
  input dropped packets          : 0
  output packets                    : 87
  output direct send packets     : 42
  output error dropped packets   : 3
  output send ipsec packets       : 42
  output send ipsec fail packets : 0
```

5.1.11 display dvpn online-user

【命令】

display dvpn online-user

【视图】

所有视图

【参数】

无

【描述】

display dvpn online-user 命令用来显示 DVPN 用户的在线信息。当 Server 对 Client 进行身份验证时，可以通过该命令查看目前已经通过 AAA 验证接入到 DVPN 域的用户信息。

【举例】

显示 DVPN 的在线用户信息。

```
<H3C> dis dvpn online-user
  username    : dvpnuser@dvpn
  authen-type : CHAP
  DVPN total online-user count : 1
```

5.1.12 dvpn class

【命令】

dvpn class *dvpn-class-name*

undo dvpn class *dvpn-class-name*

【视图】

系统视图

【参数】

dvpn-class-name：创建的 *dvpn-class* 的名称，以字符串方式表示，字符串的最大长度为 31 个字符。

【描述】

dvpn class 命令用来创建一个 dvpn-class，并进入该视图。**undo dvpn class** 命令用来删除 dvpn-class。

dvpn-class 视图可以配置目的 Server 的地址，注册使用的用户名、密码等。当该 dvpn-class 已经被接口应用，不能被直接删除。

缺省情况下，没有配置任何 dvpn-class。

【举例】

创建一个名为“abc”的 dvpn-class。

```
[H3C] dvpn class abc
```

5.1.13 dvpn client register-dumb

【命令】

dvpn client register-dumb *time*

undo dvpn client register-dumb

【视图】

系统视图

【参数】

time：客户端连续注册失败后的静默时间，单位为秒，取值范围为 60～3600。

【描述】

dvpn client register-dumb 命令用来设置客户端连续注册失败达到最大次数时进入静默状态的时间，即多长时间后进行下一次注册。**undo dvpn client register-dumb** 命令用来恢复客户端静默的时间间隔为缺省值。

缺省情况下，静默时间为 300 秒。

【举例】

设置客户端进行注册失败后的静默时间为 600 秒。

```
[H3C] dvpn client register-dumb 600
```

5.1.14 dvpn client register-interval

【命令】

dvpn client register-interval *time-interval*

undo dvpn client register-interval

【视图】

系统视图

【参数】

time-interval：客户端进行注册的时间间隔，单位为秒，取值范围为 3～60。

【描述】

dvpn client register-interval 命令用来设置客户端进行注册的时间间隔。**undo dvpn client register-interval** 命令用来恢复客户端进行注册的时间间隔为缺省值。

DVPN 客户端向服务器发起注册请求时，在一定的时间间隔内，若客户端注册不成功，客户端将重新发起注册请求。在达到失败的最大次数时，若仍不成功，DVPN 客户端将进入 dumb 状态。

缺省情况下，客户端进行注册的时间间隔为 10 秒。

【举例】

设置客户端进行注册的时间间隔为 20 秒。

```
[H3C] dvpn client register-interval 20
```

5.1.15 dvpn client register-retry

【命令】

dvpn client register-retry *times*

undo dvpn client register-retry

【视图】

系统视图

【参数】

times：客户端连续进行注册的最大次数，取值范围为 1～6。

【描述】

dvpn client register-retry 命令用来设置客户端连续进行注册的最大次数；**undo dvpn client register-retry** 命令用来恢复客户端连续进行注册的最大次数为缺省值。

缺省情况下，最大次数为 3 次。

【举例】

设置客户端连续进行注册的最大次数为 6 次。

```
[H3C] dvpn client register-retry 6
```

5.1.16 dvpn dvpn-id

【命令】

dvpn dvpn-id *dvpn-id*

undo dvpn dvpn-id

【视图】

Tunnel 接口视图

【参数】

dvpn-id：接口所属的 DVPN 域编号，取值范围为 1～65535。

【描述】

dvpn dvpn-id 命令用来配置 Tunnel 接口所属的 DVPN 域，在 Tunnel 接口封装为 UDP DVPN 时有效，**undo dvpn dvpn-id** 命令用来删除 Tunnel 接口指定的 DVPN 的标识。

缺省情况下，Tunnel 接口没有指定任何 DVPN 标识。

相关配置请参考命令 **tunnel-protocol udp dvpn**。

【举例】

设置 Tunnel 接口所属的 DVPN 域标示为 100。

```
[H3C] interface tunnel 0
[H3C-Tunnel0] tunnel-protocol udp dvpn
[H3C-Tunnel0] dvpn dvpn-id 100
```

5.1.17 dvpn interface-type

【命令】

dvpn interface-type { **client** | **server** }

undo dvpn interface-type

【视图】

Tunnel 接口视图

【参数】

client：表示接口类型为 Client。

server：表示接口类型为 Server。

【描述】

dvpn interface-type 命令用来指定了 Tunnel 接口的接口类型。**undo dvpn interface-type** 命令用来恢复 Tunnel 接口的缺省类型。

缺省情况下，接口类型为 Client。

【举例】

设置 Tunnel 接口为 Server 类型。

```
[H3C-Tunnel0] dvpn interface-type server
```

5.1.18 dvpn policy（系统视图）

【命令】

dvpn policy *dvpn-policy-name*

undo dvpn policy *dvpn-policy-name*

【视图】

系统视图

【参数】

dvpn-polciy-name：创建的 *dvpn-policy* 的名称，以字符串方式表示，字符串的最大长度为 31 个字符。

【描述】

dvpn policy 命令用来创建一个 dvpn-policy，并进入该视图。**undo dvpn policy** 命令用来删除 dvpn-policy。

dvpn-policy 视图用来配置对 Client 的身份的认证方式，会话使用的加密算法套件、转发数据使用的算法套件、以及各种时间参数等各种 DVPN 策略。如果一个 dvpn-policy 已经被接口使用，则需要删除接口的应用才可以删除该 dvpn-policy。

缺省情况下，没有配置任何 dvpn-policy。

【举例】

创建一个名为“abc”的 dvpn-policy。

```
[H3C] dvpn policy abc
```

5.1.19 dvpn policy（Tunnel 接口视图）

【命令】

dvpn policy *dvpn-policy-name*

undo dvpn policy *dvpn-policy-name*

【视图】

Tunnel 接口视图

【参数】

policy-class-name：本接口使用的 dvpn-policy 的名称。

【描述】

dvpn policy 命令用来配置作为 Server 端的 Tunnel 接口使用的 dvpn-policy 名称。**undo dvpn policy** 命令用来删除 Tunnel 接口使用的 dvpn-policy。

dvpn-policy 是一个包含 DVPN 会话使用的算法、以及各种时间定时器的时间设置等信息的数据结构，该结构通过系统视图下的 **dvpn policy** 命令创建。

每个接口最多应用一个 dvpn-policy；如果需要应用新的 dvpn-policy，则必须删除原有的 dvpn-policy；另外一个 dvpn-Policy 可以被多个接口同时使用。

只有配置为 Server 模式的 Tunnel 接口才能够使用 **dvpn-policy**。

缺省情况下，Tunnel 接口没有应用 dvpn-policy。

相关配置请参考命令 **dvpn interface-type**。

【举例】

设置 Tunnel 接口应用的 policy“abc”。

```
[H3C-Tunnel0] dvpn interface-type server
[H3C-Tunnel0] dvpn policy abc
```

5.1.20 dvpn register-type

【命令】

dvpn register-type { **forward** | **undistributed** } *
undo dvpn register-type { **forward** | **undistributed** } *

【视图】

Tunnel 接口视图

【参数】

forward：DVPN 服务器转发从此客户端发送的数据包。

undistributed：不允许服务器向其它客户端发布本客户端的注册信息。

【描述】

dvpn register-type 命令用来配置 Client 向 Server 注册时的附加信息类型。**undo dvpn register-type** 命令用来取消所配置的 Client 向 Server 注册时的附加信息类型。

Server 可以根据指定的类型确定是否发送重定向报文。

只有配置为 Client 模式的 Tunnle 接口才能够配置 **dvpn register-type** 命令。

相关配置请参考命令 **dvpn interface-type**。

在缺省情况下，系统没有设置这里两个标志。

【举例】

设置注册的类型为不允许 Server 向其他节点发布本 Client 的信息。

```
[H3C-Tunnel0] dvpn register-type undistributed
```

5.1.21 dvpn security

【命令】

dvpn security acl *acl-number*

undo dvpn security acl

【视图】

Tunnel 接口视图

【参数】

acl-number：接口进行 IPsec 加密数据流判断的 ACL 的编号，取值范围为 3000～3999。

【描述】

dvpn security acl 命令用来配置 Tunnel 接口的 IPsec 加密数据流匹配的 ACL，**undo dvpn security acl** 命令用来删除 Tunnel 接口指定的 IPsec 加密数据流匹配的 ACL。

DVPN 进行数据转发时，需要进行相应的 ACL 的匹配判断，对于被 ACL 拒绝的数据报文不进行 IPsec 处理，否则进行 IPsec 加密保护。

缺省情况下，对接口的所有数据进行 IPsec 加密。

📖 说明：

dvpn security acl 需要与 **acl** 以及 **rule** 命令配合使用，当 **rule** 命令匹配的关键字为 **deny** 时，表示对于 **rule** 命令 **deny** 掉的数据报文不进行 IPsec 加密，若 **rule** 命令匹配的关键字为 **permit**，对于该配置则无实际意义。

【举例】

设置 Tunnel 接口 IPsec 加密数据流的 ACL 为 3100。

```
[H3C-Tunnel0] dvpn security acl 3100
```

5.1.22 dvpn server

【命令】

dvpn server *dvpn-class-name*

undo dvpn server *dvpn-class-name*

【视图】

Tunnel 接口视图

【参数】

dvpn-class-name：接口使用的 dvpn-class 的名称。

【描述】

dvpn server 命令用来配置 Tunnel 接口使用的 dvpn-class 名称，**undo dvpn server** 命令用来删除 Tunnel 接口使用的 dvpn-class。

dvpn-class 是一个包含 Server 端公网 IP 地址、私网（Tunnel）IP 地址、注册用户名密码等信息的数据结构，该结构通过系统视图下的 **dvpn class** 命令创建。

目前每个接口最多支持一个 DVPN Server,，同时一个 dvpn-class 只允许被一个接口使用。

缺省情况下，Tunnel 接口没有配置 dvpn-class。

【举例】

设置 Tunnel 接口使用 dvpn-class“abc”。

```
[H3C-Tunnel0] dvpn server abc
```

5.1.23 dvpn server authentication-client method

【命令】

dvpn server authentication-client method { **none** | { **chap** | **pap** } [**domain** *isp-name*] }

【视图】

系统视图

【参数】

none：表示 Server 不需要对 Client 进行验证。

pap：表示 Server 使用 pap 对 Client 进行验证。

chap：表示 Server 使用 chap 对 Client 进行验证。

domain *isp-name*：表示 Server 对 Client 采用域认证。

【描述】

dvpn server authentication-client method 命令用来设置服务器端默认对客户端的身份认证方式。

如果客户端注册时不指定需要接入的 DVPN，则会使用默认的身份认证方式对客户端进行认证。目前支持 none、CHAP、和 PAP 三种认证方式。

Client 在 Server 进行注册过程中，会根据配置确定使用 DVPN 域的策略确定对 Client 使用的认证方式，如果没有对应的策略则使用全局配置的验证方式对 Client 进行身份验证。

缺省情况下，服务器不对客户端进行验证。

【举例】

设置服务器端默认使用 CHAP 对客户端进行身份认证。

```
[H3C] dvpn server authentication-client method chap
```

5.1.24 dvpn server map age-time

【命令】

dvpn server map age-time *time*

undo dvpn server map age-time

【视图】

系统视图

【参数】

time：服务器 Map 的超时时间，单位为秒，取值范围为 10～180。

【描述】

dvpn server map age-time 命令用来设置服务器端的注册不成功的 Map 的超时时间。**undo dvpn server map age-time** 命令用来设置服务器端 Map 超时时间为缺省值。

当服务器端的 Map 在指定的超时时间内仍注册不成功时，将删除该 Map。

缺省情况下，超时时间为 30 秒。

【举例】

设置服务器端 Map 超时时间为 60 秒。

```
[H3C] dvpn server map age-time 60
```

5.1.25 dvpn server pre-shared-key

【命令】

dvpn server pre-shared-key *key*

undo dvpn server pre-shared-key

【视图】

系统视图

【参数】

key：设置的 Server 的身份密钥信息，以字符串方式表示，字符串的最大长度为 127 个字符。

【描述】

dvpn server pre-shared-key 命令用来设置服务器的身份标识的预共享密钥信息。**undo dvpn server pre-shared-key** 命令用来清除服务器的预共享密钥。

缺省情况下，服务器没有设置预共享密钥。

【举例】

设置服务器身份标示的密钥为“123”。

```
[H3C] dvpn server pre-shared-key 123
```

5.1.26 dvpn service enable

【命令】

dvpn service enable

undo dvpn service enable

【视图】

系统视图

【参数】

无

【描述】

dvpn service enable 命令用来使能设备的 DVPN 功能，**undo dvpn service enable** 命令用来禁止设备的 DVPN 功能。

缺省情况下，关闭 DVPN 功能。

【举例】

使能 DVPN 功能。

```
[H3C] dvpn service enable
```

5.1.27 local-user

【命令】

local-user *username* **password** { **simple** | **cipher** } *password*

undo local-user

【视图】

dvpn-class 视图

【参数】

username：Client 的用户名，长度为 1～80 个字符的字符串。

password：Client 的用户口令。

simple：表示不加密显示口令。

cipher：表示加密显示口令。

【描述】

local-user 命令用来配置 Client 的用户名和密码，**undo local-user** 命令用来取消已经配置的用户名和密码。

【举例】

设置 Client 进行身份认证的用户名 user、密码为 test。

```
[H3C-dvpn-class-abc] local-user user password simple test
```

5.1.28 public-ip

【命令】

public-ip *ip-address*

undo public-ip

【视图】

dvpn-class 视图

【参数】

ip-address：指定的 Server 的公网 IP 地址。

【描述】

public-ip 命令用来配置指定的 Server 端的公网 IP 地址，**undo public-ip** 命令用来删除指定的 Server 端的公网 IP 地址。

缺省情况下，没有配置 Server 端的公网 IP 地址。

【举例】

指定 Server 的公网 IP 地址为 61.18.3.66。

```
[H3C-dvpn-class-abc] public-ip 61.18.3.66
```

5.1.29 pre-shared-key

【命令】

pre-shared-key *key*

undo pre-shared-key

【视图】

dvpn-class 视图

【参数】

key：设置的 Server 的身份密钥信息，以字符串方式表示，字符串的最大长度为 127 个字符。

【描述】

pre-shared-key 命令用来设置客户端需要对服务器进行身份认证的的预共享密钥，**undo pre-shared-key** 命令用来清除客户端设置的服务器的预共享密钥。

【举例】

设置客户端的服务器的共享密钥为“123”。

```
[H3C-dvpn-class-abc] pre-shared-key 123
```

5.1.30 private-ip

【命令】

private-ip *ip-address*

undo private-ip

【视图】

dvpn-class 视图

【参数】

ip-address：指定的 Server 端的私网 IP 地址（即 Tunnel 接口的 IP 地址）。

【描述】

private-ip 命令用来配置指定 Server 的私网 IP 地址，**undo private-ip** 命令用来删除指定 Server 的私网 IP 地址。

缺省情况下，没有配置 Server 端的私网 IP 地址。

【举例】

指定 Server 的私网（Tunnel）IP 地址为 192.168.0.1。

```
[H3C-Dvpn-class-abc] private-ip 192.168.0.1
```

5.1.31 reset dvpn all

【命令】

reset dvpn all *dvpn-id*

【视图】

用户视图

【参数】

dvpn-id：指定的 DVPN 的标识。

【描述】

reset dvpn all 命令用来清除指定 DVPN 的所有运行信息，对指定的 DVPN 进行初始化。

【举例】

重置 DVPN 2。

```
<H3C> reset dvpn all 2
```

5.1.32 reset dvpn map

【命令】

reset dvpn map *public-ip port* [*client-id*]

【视图】

用户视图

【参数】

public-ip：公网 IP 地址。

port：指定的端口号，取值范围为 1～65535。

client-id：Client 端的 ID。取值范围为 1～4294967295。

【描述】

reset dvpn map 命令用来清除指定的 Map。

如果已经建立了会话连接，则同时会清除相关的会话连接。如果该 Map 为 Client 注册使用的 Map，则会清除使用该 Map 进行注册的 DVPN Client 的所有的会话。

【举例】

清除地址为 10.0.0.2，端口号位 9876，client-id 为 123456 的 Map。

```
<H3C> reset dvpn map 10.0.0.2 9876 123456
```

5.1.33 reset dvpn session

【命令】

reset dvpn session *dvpn-id private-ip*

【视图】

用户视图

【参数】

dvpn-id：指定的 DVPN 的标识 ID。取值范围为 1～65535。

private-ip：私网 IP 地址。

【描述】

reset dvpn session 命令用来清除指定的 session，如果该 session 为 Client 注册过程建立的 session，则会清除使用该 DVPN Client 的所有的 session。

【举例】

清除 DVPN 2 域中私网地址为 10.0.0.2 的 session。

```
<H3C> reset dvpn session 2 10.0.0.2
```

5.1.34 reset dvpn statistics

【命令】

reset dvpn statistics

【视图】

用户视图

【参数】

无

【描述】

reset dvpn statistics 命令用来清除 DVPN 的所有统计信息。

【举例】

清除 DVPN 的统计信息。

```
<H3C> reset dvpn statistics
```

5.1.35 session algorithm-suite

【命令】

session algorithm-suite *suite-number*

undo session algorithm-suite

【视图】

dvpn-policy 视图

【参数】

suite-number：会话控制报文加密保护使用的算法套件，取值范围为 0～12。

0 Without protection

1 DES_MD5_DHGROUP1

2 DES_MD5_DHGROUP2

3 DES_SHA1_DHGROUP1

4 DES_SHA1_DHGROUP2

5 3DES_MD5_DHGROUP1

6 3DES_MD5_DHGROUP2

7 3DES_SHA1_DHGROUP1

8 3DES_SHA1_DHGROUP2

9 AES128_MD5_DHGROUP1

10 AES128_MD5_DHGROUP2

11 AES128_SHA1_DHGROUP1

12 AES128_SHA1_DHGROUP2

【描述】

session algorithm-suite 命令用来配置会话使用的算法套件，**undo session algorithm-suite** 命令用来恢复算法套件的缺省设置。

缺省情况下，会话控制报文使用的算法套件为 1，即加密算法为 DES，验证算法为 MD5，密钥协商算法为 DHGROUP1。

【举例】

设置不对会话控制报文进行加密保护，即使用套件 0。

```
[H3C-dvpn-policy-abc] session algorithm-suite 0
```

5.1.36 session idle-time

【命令】

session idle-time *time*

undo session idle-time

【视图】

dvpn-policy 视图

【参数】

time：会话的空闲超时时间，单位为秒，取值范围为 60～86400。

【描述】

session idle-time 命令用来配置会话的空闲超时时间，**undo session idle-time** 命令用来恢复会话空闲超时时间的缺省设置。

如果会话在空闲超时时间内没有数据传输，该会话会被自动删除。

缺省情况下，空闲超时时间为 300 秒。

【举例】

设置会话空闲超时时间为 180 秒。

```
[H3C-dvpn-policy-abc] session idle-time 180
```

5.1.37 session keepalive-interval

【命令】

session keepalive-interval *time-interval*

undo session keepalive-interval

【视图】

dvpn-policy 视图

【参数】

time-interval：保持定时器的时间间隔，单位为秒，取值范围为 5～300。

【描述】

session keepalive-interval 命令用来配置 DVPN 会话状态的保持连接定时器的时间间隔，**undo session keepalive-interval** 命令用来恢复保持连接定时器的缺省值。

Keepalive 用来保持会话的连接状态。当会话建立成功后，主动方会定时发送 Keepalive 报文，被动端接收到 Keepalive 报文会回应 Keepalive-ack 报文。被动端不会主动发送 Keepalive 报文。

缺省情况下，时间间隔为 10 秒。

【举例】

设置会话状态的保持连接时间间隔为 30 秒。

```
[H3C-dvpn-policy-abc] session keepalive-interval 30
```

5.1.38 session setup-interval

【命令】

session setup-interval *time-interval*

undo session setup-interval

【视图】

dvpn-policy 视图

【参数】

time-interval：会话建立请求定时器的时间间隔，单位为秒，取值范围为 5～60。

【描述】

session setup-interval 命令用来配置会话建立请求（Setup Request）的时间间隔，每次超时将重新发送会话建立请求报文。**undo session setup-interval** 命令用来恢复会话建立请求定时器的缺省值。

当 Client 端发送一个会话建立请求之后，在没有收到对端的应答之前，如果定时器超时则再向对端节点发送会话建立请求报文。

缺省情况下，时间间隔 10 秒。

【举例】

设置会话建立请求的时间间隔为 30 秒。

```
[H3C-dvpn-policy-abc] session setup-interval 30
```

5.1.39 tunnel-protocol dvpn

【命令】

tunnel-protocol udp dvpn

【视图】

Tunnel 接口视图

【参数】

udp dvpn：Tunnel 接口采用 UDP DVPN 封装格式建立 Tunnel。

【描述】

tunnel-protocol udp dvpn 命令用来配置 Tunnel 接口的封装格式，设置 Tunnel 接口采用 DVPN 方式，接口将变成 Multipoint 属性，NBMA 类型。

缺省情况下，Tunnel 接口封装为 GRE 模式。

【举例】

设置 Tunnel 接口为 UDP DVPN 封装格式。

```
[H3C-Tunnel0] tunnel-protocol udp dvpn
```

第6章 BGP/MPLS VPN 配置命令

6.1 BGP/MPLS VPN 配置命令

6.1.1 apply access-vpn vpn-instance

【命令】

apply access-vpn vpn-instance [*vpn-name1 vpn-name2 …*]

undo apply access-vpn vpn-instance [*vpn-name1 vpn-name2 …*]

【视图】

route-policy 视图

【参数】

vpn-name：已经配置的 VPN 实例的名称，最多可以取六个值。

【描述】

apply access-vpn vpn-instance 命令用来在策略路由使能后满足 route-policy 的条件情况下，指定报文依次在 *vpn-name1*，*vpn-name2*，*vpn-name3*，*vpn-name4*，*vpn-name5*，*vpn-name6*(如果它们都存在)中查找私网转发路由并进行相应的转发。

undo apply access-vpn vpn-instance 命令用来取消该功能。

【举例】

指定已经配置的 VPN 实例。

```
[H3C-route-policy] apply access-vpn vpn-instance vpn1
```

6.1.2 apply mpls-label

【命令】

apply mpls-label

undo apply mpls-label

【视图】

Route-policy 视图

【参数】

无

【描述】

apply mpls-label 命令用来配置为满足 route-policy 过滤条件的公网路由分配 MPLS 标签，**undo apply mpls-label** 命令用来取消此配置。

缺省情况下，公网路由不带标签。

相关配置请参考命令 **if-match mpls-label**。

【举例】

定义一条 apply 子句，为满足 route-policy 过滤条件的路由分配标签。

```
[H3C-route-policy] apply mpls-label
```

6.1.3 description

【命令】

description *vpn-instance-description*

undo description

【视图】

vpn-instance 视图

【参数】

vpn-instance-descriptio：指定 VPN 实例的描述信息。

【描述】

description 命令用来为指定 VPN 实例配置描述信息。**undo description** 命令用来删除该 VPN 实例的描述。

【举例】

给出 VPN 的描述信息。

```
[H3C-vpn-vpna] description vpna
```

6.1.4 display bgp routing label

【命令】

display bgp routing label

【视图】

所有视图

【参数】

无

【描述】

display bgp routing label 命令用来查看 BGP 路由表中的路由信息及标签信息。

对于不带标签的普通 IPv4 路由，显示标签为空。

如果使用 **display bgp routing** *address* [*mask*]命令查看 BGP 路由信息，当路由带标签时，也将会显示出来。

【举例】

查看 BGP 路由信息。

```
<H3C> display bgp routing label
Flags:   # - valid       ^ - active      I - internal
          D - damped      H - history     S - aggregate suppressed
                                          In/out
    Dest/Mask          Next-Hop        Label
--------------------------------------------------------------
#^  9.0.0.1/32         0.0.0.0        1024/-
```

查看具体的 BGP 路由信息。

```
<H3C> display bgp routing 9.0.0.1
BGP routing table entry information of 9.0.0.1/32
Age          : 00:00:32
From         : local
State        : valid, sourced, active,
Nexthop      : 0.0.0.0
Origin       : INC
As-path      : (null)
Med          : 1563
In/Out label :   1024/-
```

6.1.5 display bgp vpnv4

【命令】

display bgp vpnv4 { **all** | **route-distinguisher** *rd-value* | **vpn-instance** *vpn-instance-name* } { **group** [*group-name*] | **network** | **peer** [*ip-address1* | **verbose**] | **routing** [*ip-address2* | **statistic**] [**label**] [**as-path-acl** *as-path-acl* | **cidr** | **community** [*community-number* | **no-advertise** | **no-export** | **no-export-subconfed** | **whole-match**] | **community-list** *community-list* [**whole-match**] | **different-origin-as** | **peer** *ip-address1* [**advertised** | **received**] | **regular-expression** *text*] }

【视图】

所有视图

【参数】

all：显示全部 VPNv4 数据库，包括 group、network、peer、routing 等信息。

route-distinguisher *rd-value*：显示匹配路由标识（RD）网络层可达性信息（NLRI）。

vpn-instance *vpn-instance-name*：显示与指定名称的 vpn-instance 关联的网络层可达性信息（NLRI）。

group：显示有关 BGP 对等体组的信息。

group-name：peer 的对等体组名。

network：显示由 BGP 通告的网络。

peer：显示 peer 的信息。

ip-address1：peer 的 IP 地址。

verbose：显示 peer 的详细信息。

routing：显示 bgp 路由。

ip-address2：显示指定目的地址的路由信息。

statistic：显示路由的统计信息。

label：显示指定标签的路由信息。

as-path-acl *as-path-acl*：显示指定 as-path 的路由信息。

cidr：显示无类域内路由信息。

community：显示指定团体的路由信息。

aa:nn：团体号。

no-advertise：不向任何对等体通告的路由。

no-export：不向自治系统外部通告，但发布给其它子自治系统的路由。

no-export-subconfed：不在本地自治系统外通告的路由。

whole-match：与指定团体精确匹配的路由。

different-origin-as：显示非源起于本地自治系统的路由。

advertised：显示所有发布到 peer 的路由。

received：显示所有从 peer 接收到的路由。

regular-expression *text*：显示匹配正则表达式的路由。

【描述】

display bgp vpnv4 命令用来显示 BGP 数据库中 VPNv4 信息。

【举例】

显示 BGP VPNV4 所有路由信息。

```
[H3C] display bgp vpnv4 all routing
Flags:   # - valid       ^ - active      I - internal
         D - damped      H - history     S - aggregate suppressed
In/out     As
    Dest/mask     Next-hop     Med Local-pref   label    path
    Route Distinguisher:1.1.1.1:1 (VPN instance:v1)
#^  1.0.0.0       0.0.0.0                      1024/-

  Routes total: 49194533
```

6.1.6 display ip routing-table vpn-instance

【命令】

display ip routing-table vpn-instance *vpn-instance-name* [**statistics** |[*ip-address*] [**verbose**]]

【视图】

所有视图

【参数】

vpn-instance-name：分配给 vpn-instance 的名字。

ip-address：显示指定地址的信息。

verbose：显示详细信息。

statistics：显示所有路由的摘要信息。

【描述】

display ip routing-table vpn-instance 命令用来显示 vpn-instance 的 IP 路由表中的指定信息。

【举例】

显示与 vpn-instance 相关联的 IP 路由表。

```
[H3C] display ip routing-table vpn-instance vpn-instance1
Routing Table:  vpn-instance1   RD:   1233:11
Destination/Mask ProtoPre Metric    Nexthop           Interface
192.1.1.0/24  Direct   0    0      192.1.1.1 GigabitEthernet1/0/0
192.1.1.1/32  Direct   0    0      127.0.0.1         InLoopBack0
192.1.1.255/32    Direct   0    0      127.0.0.1         InLoopBack0
```

6.1.7 display ip vpn-instance

【命令】

display ip vpn-instance [*vpn-instance-name* | **verbose**]

【视图】

所有视图

【参数】

vpn-instance-name：分配给 vpn-instance 的名字。

verbose：显示详细信息。

【描述】

display ip vpn-instance 命令用来显示 vpn-instance 相关信息，包括该 VPN 实例的 RD，描述以及与之关联的接口等信息。

【举例】

显示 vpn-instance vpn1 的相关信息。

```
[H3C] display ip vpn-instance vpn1
VPN-Instance : vpn1
   No description
   Route-Distinguisher :    100:6
   Interfaces :
     Ethernet0/0/0.101
```

6.1.8 display mpls l3vpn-lsp

【命令】

display mpls l3vpn-lsp [**vpn-instance** *vpn-instance-name*] [**transit** | **egress** | **ingress**] [**include** *text* | **verbose**]

【视图】

所有视图

【参数】

transit: ASBR VPN 的标签交换路径。

egress：出口 VPN 的标签交换路径。

ingress：入口 VPN 的标签交换路径。

vpn-instance: VPN 路由/转发 vpn-instance 的名称。

include *text*: 表示只匹配包含指定 FEC 的字符串。

verbose: 显示详细信息。

【描述】

display mpls l3vpn-lsp 命令用来显示 mpls l3vpn 标签交换路径 vpn-instance 相关的信息。

【举例】

显示 mpls l3vpn 标签交换路径 vpn-instance 相关的信息。

```
<H3C> display mpls l3vpn-lsp transit
----------------------------------------------------------------------LSP
Information: L3vpn Transit Lsp
----------------------------------------------------------------------

TOTAL:  0 Record(s) Found.
```

显示 mpls l3vpn 标签交换路径相关信息。

```
<H3C> display mpls l3vpn-lsp include h3c
```

6.1.9 display ospf sham-link

【命令】

display ospf sham-link

【视图】

所有视图

【参数】

无

【描述】

display ospf sham-link 命令用来显示配置的 sham link。

相关命令可参考命令 **sham-link**。

【举例】

显示配置的 sham-link。

```
<H3C> display ospf sham-link
OSPF Process 1 with Router ID 1.1.1.1
                                Sham Links
  Sham-link 3.3.3.3  -> 5.5.5.5, State: Down
     Area: 0.0.0.1
Cost: 1 State: Down    Type: Sham
```

```
Timers: Hello 10, Dead 40, Poll 0, Retransmit 5, Transmit Delay 1
```

6.1.10 domain-id

【命令】

domain-id { *id-number* | *id-addr* }

undo domain-id

【视图】

OSPF 协议视图

【参数】

id-number：标识 VPN 实例的 domain-id，取值范围为 0～4294967295 的整数，缺省为 0。

id-addr：VPN 实例 domain-id 的 IP 地址形式，缺省为 0.0.0.0。

【描述】

domain-id 命令用来配置 domain-id，**undo domain-id** 命令用来恢复缺省值。

由于对于标准的 BGP/OSPF 互操作而言，当在 PE 上配置引入 BGP 路由到 OSPF 中时，该路由的原 OSPF 属性无法恢复，则这些 BGP VPN IP 路由将以 OSPF 的 ASE LSA（第 5 类 LSA）发布到 CE 上，造成与 OSPF 从其他路由域引入的路由无法区分开。为了区分真正引入的外部路由与 OSPF 自己域的路由，需要在远端引入 BGP 路由到 OSPF 时恢复这些属性。为了实现这个目的，我们可以为每一个 OSPF 域配置一个 Domain ID。domain-id 在 OSPF 路由引入到 BGP/VPN 中时被附加到 BGP/VPN 路由上，借助 BGP/VPN 路由进行传递。然后对端 PE 在引入 BGP 路由时，针对这些扩展团体属性，填写所生成 LSA 的相关值。这样在收到 BGP VPN IP 路由时，如果 domain id 相同，则是来自同一 VPN 实例的路由。

缺省情况下，domain-id 为 0。

⚠ 注意：

配置 domain-id 后，不会马上起作用，只有在 reset ospf 后才会起作用。

【举例】

为 OSPF 进程 100 配置 domain-id 100。

```
[H3C-ospf-100] domain-id 100
[H3C-ospf-100] domain-id 0.0.0.100
```

6.1.11 if-match mpls-label

【命令】

if-match mpls-label

undo if-match mpls-label

【视图】

Route-policy 视图

【参数】

无

【描述】

if-match mpls-label 命令用来配置只匹配带 MPLS 标签的公网路由，**undo if-match mpls-label** 命令用来取消此匹配规则。

相关配置请参考命令 **apply mpls-label**。

【举例】

定义一条 if-match 子句，允许带标签的路由通过该 if-match 子句的过滤。

```
[H3C-route-policy] if-match mpls-label
```

6.1.12 import-route ospf

【命令】

import-route { **ospf** | **ospf-ase** | **ospf-nssa** } [*process-id*] [**med** *value* | **route-policy** *route-policyname*]

undo import-route { **ospf** | **ospf-ase** | **ospf-nssa** } [*process-id*]

【视图】

BGP 协议的单播、多播和 MBGP 的 VPN-instance 地址族视图

【参数】

process-id：OSPF 的进程号，如果没有配置进程号，默认的进程号为 1。

ospf：表示只引入 OSPF 进程 processid 发现 ASE 内部路由作为外部路由信息。

ospf-ase 表示只引入 OSPF 进程 processid 发现的 OSPF-ASE 类型的路由作为外部路由信息。

ospf-nssa 表示只引入 OSPF 进程 processid 发现 OSPF-NSSA 类型的路由作为外部路由信息。

med *value*：表示路由的花费值。

route-policyname：表示路由策略 route-policy 的名字。

【描述】

import-route ospf 命令用来配置引入 OSPF 路由，**undo import-route ospf** 命令用来取消引入 OSPF 路由。

⚠ 注意：

如果没有配置进程号，默认的进程号为 1

【举例】

配置引入进程号为 100 的 OSPF 路由

```
[H3C] ip vpn-instance sphinx
[H3C-vpn-sphinx] route-distinuisher 168.168.55.1:85
[H3C-vpn-sphinx] quit
[H3C] bgp 352
[H3C-bgp] ip vpn-instance sphinx
[H3C-bgp-af-vpn-instance] import-route ospf 100
```

6.1.13 ip binding vpn-instance

【命令】

ip binding vpn-instance *vpn-instance-name*

undo ip binding vpn-instance *vpn-instance-name*

【视图】

接口（含子接口）视图

【参数】

vpn-instance-name：分配给 vpn-instance 的名字。

【描述】

ip binding vpn-instance 命令用来将一个接口或子接口与一个 vpn-instance 关联起来，**undo ip binding vpn-instance** 命令用来取消 vpn-instance 与端口的关联。

缺省情况下，使用全局路由表。

在接口上执行该命令会清除接口的 IP 地址，所以接口的 IP 地址需要重新配置。

【举例】

将 Ethernet0/0/0 与 vpn 实例 vpn1 绑定。

```
[H3C] interface Ethernet0/0/0
```

```
[H3C-Ethernet0/0/0] ip binding vpn-instance vpn1
```

6.1.14 ip route-static vpn-instance

【命令】

ip route-static vpn-instance *vpn-instance-name1 vpn-instance-name2 …destination-address* { *mask* | *mask-length* } { *interface-type interface-number* [*nexthop-address*] | **vpn-instance** *vpn-nexthop-name vpn-nexthop-address* | *nexthop-address* [**public**] } [**preference** *preference-value*] [**reject** | **blackhole**]

undo ip route-static vpn-instance *vpn-instance-name1 vpn-instance-name2 … ip-address* { *mask* | *mask-length* } { *interface-type interface-number* | **vpn-instance** *vpn-nexthop-name vpn-nexthop- address* | *nexthop-address* [**public**] } [**preference** *preference-value*]

【视图】

系统视图

【参数】

vpn-name：VPN 实例的名称，最多可以取六个值。

destination-address：表示静态路由的目的地址。

mask：掩码。

mask-length：掩码长度。由于要求 32 位掩码中的“1”必须是连续的，因此点分十进制格式的掩码也可以用掩码长度 *mask-length* 来代替（掩码长度是掩码中连续“1”的位数）。

interface-type interface-number：表示该静态路由的出接口类型及接口号，可以指定公网或者其他 vpn-instance 下面的接口作为该静态路由的出接口。

vpn-name-nexthop：用于指定该静态路由下一跳所在的 vpn-instance。

nexthop-address：用于指定该静态路由的下一跳 IP 地址。

public：表示该路由的下一跳为公网 IP 地址。

preference-value：指定优先级。

reject：配置路由为不可达路由。

blackhole：配置路由为黑洞路由。

【描述】

ip route-static vpn-instance 命令用来配置静态路由，可以指定一个该私网下面的接口作为静态路由的出接口；在多角色主机应用背景下，用于配置一个私网下面的

静态路由，该静态路由的出接口可以是另外一个私网或者公网的接口。**undo ip route-static vpn-instance** 命令用来取消静态路由的配置。

【举例】

配置静态路由，该静态路由的目的地址为 100.1.1.1，下一跳地址为 1.1.1.2。

```
[H3C] ip route-static vpn-instance vpn1 100.1.1.1 16 vpn-instance vpn1 1.1.1.2
```

6.1.15 ip vpn-instance

【命令】

ip vpn-instance *vpn-instance-name*

undo ip vpn-instance *vpn-instanc-name*

【视图】

系统视图，路由协议视图（BGP、RIP）

【参数】

vpn-instance-name：分配给 vpn-instance 的名字。

【描述】

ip vpn-instance 命令用来创建并配置一个 vpn 实例，**undo ip vpn-instance** 命令用来删除指定 vpn 实例。

缺省情况下，没有定义 vpn-instance，没有输入或输出列表与 vpn-instance 相关联，没有路由映射（route-map）与 vpn-instance 相关联。

使用 **ip vpn-instance** 创建一个名为 *vpn-name* 的 vpn-instance。

【举例】

创建 vpn 实例 VPN1。

```
[H3C] ip vpn-instance vpn1
[H3C-vpn-vpn1]
```

6.1.16 ipv4-family

【命令】

ipv4-family { **multicast** | **vpn-instance** *vpn-instance-name* | **vpnv4** [**unicast**] }

undo ipv4-family { **multicast** | **vpn-instance** *vpn-instance-name* | **vpnv4** [**unicast**] }

【视图】

BGP 视图

【参数】

multicast：使用该参数将进入 MBGP 的组播地址族视图。

vpn-instance *vpn-instance-name*：将指定的 vpn-instance 实例与 MBGP 地址族进行关联，使用该参数将进入 MBGP 的 vpn-instance 地址族视图。

vpnv4: 使用该参数将进入 MBGP 的 vpnv4 的地址族视图。

unicast：使用 VPNv4 单播地址。

【描述】

ipv4-family multicast 命令用来进入使用 MBGP 的组播地址族视图，**undo ipv4-family multicast** 命令用来删除指定的组播地址族视图的配置。

ipv4-family vpn-instance 命令用于进入 MBGP 的 vpn-instance 地址族视图。

执行 **undo ipv4-family vpn-instance** *vpn-instance-name* 命令将取消指定 vpn-instance 实例与 MBGP 地址族的关联，退回到 BGP 单播视图。

ipv4-family vpnv4 命令用来进入 MBGP 的 VPNv4 地址族视图，**undo ipv4-family vpnv4** 命令用来删除 MBGP 的 VPNv4 地址族视图的配置。

缺省情况下，配置 VPNv4 地址族时使用单播地址。

缺省情况下，配置 MBGP 地址族时使用单播地址。

使用此命令进入地址族视图，在这个视图下，可以为 BGP 配置地址族相关的参数。

相关配置可参考命令 **peer enable**。

【举例】

将指定的 vpn-instance 实例与 MBGP 地址族关联，进入 MBGP 的 vpn-instance 地址族视图，必须先配置 vpn-instance 才能进行该项配置。

```
[H3C] bgp 100
[H3C–bgp] ipv4-family vpn-instance abc
[H3C-bgp-af-vpn-instance]
```

进入 VPNv4 地址族视图。

```
[H3C] bgp 100
[H3C-bgp] ipv4-family vpnv4 unicast
[H3C-bgp-af-vpn]
```

6.1.17 ospf vpn-instance

【命令】

ospf *process-id* [**router-id** *router-id-number*] **vpn-instance** *vpn-instance-name*

undo ospf *process-id*

【视图】

系统视图

【参数】

process-id：OSPF 进程号。如果不指定进程号，将使用缺省进程号 1。

router-id-number：OSPF 进程的 router id。可选参数。

vpn-instance-name：OSPF 进程绑定的 VPN 实例。

【描述】

ospf 命令用来启动 OSPF 进程，**undo ospf** 命令用来关闭 OSPF 进程。

用户在启动 OSPF 进程后，就可在该协议视图下进行 OSPF 的相关配置。

缺省情况下，系统缺省不运行 OSPF 协议。

Comware 支持 OSPF 多进程，可以在一台安全网关上通过指定不同的进程号启动多个 OSPF 进程。

建议用户在启动 OSPF 进程时，使用命令中的参数 router-id 指定进程的 router-id，如果在一台安全网关上启动了多个进程，建议为不同的进程指定不同的 router-id。

如果要启动一个不指定 router id 的属于公网的 OSPF 进程，则必须满足下列两个条件之一：

- RM 配置了 router id
- 存在一个接口配置了地址

如果启动 OSPF 进程没有指定 router id，并且进程要绑定 VPN 实例，那么 VPN 实例中必须存在一个接口配置了 IP 地址。

如果要将进程绑定到 VPN 实例，必须指定 VPN 实例名。

一个 VPN 实例可以包含多个进程 process。例如：对一个实例 vpn1，可以配置 ospf 1 vpn-instance vpn1、ospf 2 vpn-instance vpn1、ospf 3 vpn-instance vpn1 等多个命令，实例 vpn1 将包含 OSPF 进程 1、2、3 等。

一个进程只能属于一个实例。如果已配置了 ospf 1 vpn-instance vpn1，则不能再配置 ospf 1 vpn-instance vpn2，否则将提示错误 Wrong configuration. Process 1 has been bound to vpn-instance VPN-INSTANCE1 。如果先配置 ospf 1，再配置 ospf 1 vpn-instance vpn1，则提示错误 Wrong configuration. Process 1 has been running in public domain；

如果先配置 ospf 1 vpn-instance vpn1，再配置命令 ospf 1 时将进入 ospf 1 vpn-instance vpn1 模式中。即在该情况下，命令 ospf 1 和 ospf 1 vpn-instance vpn1 等价。

不同 OSPF 进程绑定的 VPN 实例不同，那么不同进程的网络地址允许相同或包含。但是同一个 VPN 实例中，不同的 OSPF 进程之间，网络地址不允许相同或包含。否则，后配的命令不能生效，并给出提示:Network already set in OSPF process xx。即：如果在进程 100 中使能 network 10.1.0.0 0.0.255.255，那么在其余的 OSPF 进程中使能 network 10.1.0.0 0.0.255.255，或 network 10.1.1.0 0.0.0.255，或 network 10.0.0.0 0.255.255.255 都将失败。

OSPF 进程绑定 VPN 实例后，OSPF 默认路由器是 PE 路由器。执行 **display ospf process-id brief** 命令将显示 PE router，connected to VPN backbone。

⚠ 注意：

- 在一台安全网关上所运行的 OSPF 进程数不超过 1024，每个 VPN 实例中启动的进程数不超过 10 个。
- 如果 OSPF 进程绑定的 VPN 实例不存在，那么命令配置不成功，给出提示错误 Specified vpn instance not configured。
- 如果删除了 VPN 实例，那么相关的所有 OSPF 进程将全部删除。即如果 VPN 实例 vpn1 包含 OSPF 进程 1、2、3，当删除 VPN 实例 vpn1 时，OSPF 进程 1、2、3 同时被删除。

相关配置可参考命令 **network**。

【举例】

启动进程号为 100 的 OSPF 进程，指定进程的 router id 是 2.2.2.2，同时绑定 VPN 实例 vpn1。

```
[H3C] ospf 100 router-id 2.2.2.2 vpn-instance vpn1
[H3C-ospf-100]
```

6.1.18 peer default-route-advertise

【命令】

peer *group-name* **default-route-advertise**

undo peer *group-name* **default-route-advertise**

【视图】

BGP 视图，MBGP 的 IPv4-family 视图

【参数】

group-name：对等体组的名称。

【描述】

peer default-route-advertise 命令用来设置对等体（组）引入缺省路由，**undo peer default-route-advertise** 命令用来取消已有的设置。

缺省情况下，对等体（组）不引入缺省路由。

该命令不需要在路由表中存在缺省路由，而是无条件地向对等体发送一个下一跳为自身的缺省路由。

【举例】

设置对等体（组）test 引入缺省路由。

```
[H3C-bgp] peer test default-route-advertise
```

6.1.19 peer label-route-capability

【命令】

peer *group-name* **label-route-capability**

undo peer *group-name* **label-route-capability**

【视图】

BGP 视图

【参数】

group-name：对等体组的名称。

【描述】

peer label-route-capability 命令用来使能对等体处理带标签的 IPv4 路由的能力，**undo peer label-route-capability** 命令用来去使能对等体处理带标签的 IPv4 路由的能力，

缺省情况下，BGP 对等体不能处理带标签的 IPv4 路由。

【举例】

使能 IBGP 对等体组和 EBGP 对等体组处理带标签的 IPv4 路由的能力。

```
[H3C-bgp] group ibgp internal
[H3C-bgp] peer ibgp label-route-capability
[H3C-bgp] group ebgp external
[H3C-bgp] peer ebgp label-route-capability
```

6.1.20 peer next-hop-invariable

【命令】

peer *group-name* **next-hop-invariable**

undo peer *group-name* **next-hop-invariable**

【视图】

BGP 视图、BGP-VPNv4 子地址族视图、BGP VPN 实例视图、BGP-IPv4 组播子地址族视图

【参数】

group-name：对等体组的名称。

【描述】

peer next-hop-invariable 命令用来配置向 EBGP 对等体发送路由时，不改变路由的下一跳。**undo peer next-hop-invariable** 命令用来恢复缺省配置。

缺省情况下，BGP Speaker 在向 EBGP 对等体发送路由时，会将路由的下一跳改为自己。

peer next-hop-invariable 命令一般用于采用 Multihop MP-BGP 跨域 VPN 方式，并且使用路由反射器 RR（Route Reflector）通告 VPNv4 路由的组网应用。跨域的 RR 之间通告 VPNv4 路由时，配置不改变路由的下一跳。

【举例】

配置向 EBGP 对等体发送 VPNv4 路由时，不改变路由的下一跳。

```
[H3C-bgp] group ebgp external
[H3C-bgp] ipv4-family vpnv4
[H3C-bgp-af-vpn] peer ebgp enable
[H3C-bgp-af-vpn] peer ebgp next-hop-invariable
```

6.1.21 policy vpn-target

【命令】

policy vpn-target

undo policy vpn-target

【视图】

BGP-VPNv4 子地址族视图

【参数】

无

【描述】

policy vpn-target 命令用来配置是否对接收的路由信息进行 VPN-target 扩展团体属性的过滤，**undo policy vpn-target** 命令用来取消该过滤功能。

缺省情况下，对接收的路由信息进行 VPN-target 扩展团体属性的过滤。

【举例】

对接收的路由信息进行 VPN-target 扩展团体属性的过滤。

```
[H3C-bgp-af-vpn] policy vpn-target
```

6.1.22 route-distinguisher

【命令】

route-distinguisher *route-distinguisher*

【视图】

MBGP 的 vpn-instance 视图

【参数】

route-distinguisher：为一个 IPv4 前缀添加一个 8 字节的值，构成一个 VPN IPv4 前缀。

【描述】

route-distinguisher 命令用来配置 MPLS VPN 的 RD。一个 vpn-instance 只有配置了 RD 才能起作用。

一个路由标识（RD）为一个 VPN 创建路由和转发表，并指定缺省的路由标识。将 RD 添加到一个特定的 IPv4 前缀的开始，使之成为全局唯一的 VPN IPv4 前缀。

RD 或者是与自治系统号(ASN)相关的，在这种情况下，RD 是由一个自治系统号和一个任意的数组成；或者是与 IP 地址相关的，在这种情况下，RD 是由一个 IP 地址和一个任意的数组成。

有以下格式：

16 位自治系统号（此处可以取 0）：32 位用户自定义数，例如：101：3。

32 位 IP 地址（此处可以取 0.0.0.0）：16 位用户自定义数，例如：192.168.122.15：1。

【举例】

配置 MPLS VPN 的 RD。

```
[H3C] ip vpn-instance vpn-instance_blue
[H3C-vpn-vpn-instance_blue] route-distinguisher 100:3
[H3C] ip vpn-instance vpn-instance_red
[H3C-vpn-vpn-instance_red] route-distinguisher 173.13.0.12:200
```

6.1.23 route-tag

【命令】

route-tag *tag-number*

undo route-tag

【视图】

OSPF 协议视图

【参数】

tag-number：标识 VPN 引入路由的 tag 值，取默认值时前面两个字节为固定的 0xD000，后面的两个字节为本端 BGP 的 AS 号，比如本端 BGP AS 号为 100，则其默认的 tag 十进制值为 3489661028。该值的取值范围为 0～4294967295 的整数。

【描述】

route-tag 命令用来配置标识 VPN 引入路由的 tag 值，**undo route-tag** 命令用来恢复缺省值。

如果同一个 VPN site 链接了多个 PE，那么从 MPLS/BGP 学到的路由，被一个 PE 路由器通过 5 类或 7 类 LSA 向 VPN site 发布时，可能被另一个 PE 路由器收到，造成路由环。为了防止路由环，应配置 Route-tag，且同一 VPN 域的 PE 最好配置相同的 route-tag，该路由标记被包含在第 5/7 类的 LSA 中。route–tag 不在 BGP 的扩展团体属性中传递，所以实际上只是本地概念，只在收到 BGP 路由并且产生 OSPF LSA 的 PE 路由器上配置并起作用。

route-tag 在 OSPF 视图下进行配置，不同的进程之间可配置相同的 route-tag。通过 route-tag 命令设置的 tag 和其它命令设置的 tag 没有区别，但是有优先级的差别：

(1) import-route 命令配置的 tag 优先级最高；

(2) route-tag 命令配置的 tag 优先级其次；

(3) default tag 命令配置的 tag 优先级最低。

如果收到的 type5、type7 LSA 中包含的 tag 与自己的 tag 相同，则在进行路由计算时忽略该 LSA。

⚠ 注意：

配置 route-tag 后，不会马上起作用，只有在 reset ospf 后才会起作用。

相关配置可参考命令 **import-route**，**default**。

【举例】

为 OSPF 进程 100 配置 route-tag 为 100。

```
[H3C-ospf-100] route-tag 100
OSPF: Process 100's route tag has been changed
OSPF: Reload or use 'reset ospf' command for this to take effect
```

6.1.24 routing-table limit

【命令】

routing-table limit *threshold-value* { *warn-threshold* | **syslog-alert**}

undo routing-table limit

【视图】

VPN 实例视图

【参数】

threshold-value：最大路由数门限值。当到达预设的最大路由数门限值后拒绝增加路由，取值为 1 到 1000。

warn-threshold: 告警门限百分比。当到达预设的最大路由数×告警门限百分比后，产生告警信息，取值为 1 到 100。

syslog-alert：当最大路由数超过门限值（*threshold-value*）时，允许增加路由，仅发出 SYSLOG 错误消息。

【描述】

routing-table limit 命令用来限制一个 vpn-instance 中最大路由数，**undo routing-table limit** 命令用来取消最大路由数限制。

使用 **routing-table limit** 命令，必须进入 vpn-instance 子视图。在这个视图中，创建一个 vpn-instance 路由表，同时以下面一种格式分配一个路由标识(RD)：

16 位自治系统号(ASN)：32 位用户自定义号，例如：100:1

32 位 IP 地址：16 位用户自定义号，例如：172.1.1.1:1

然后为一个 vpn-instance 创建一个 vpn-target 扩展团体，并且为 **vpn-target** 指定入口，出口，或者同时这两个参数。这些参数可以为一个安全网关配置目的 VPN 扩展团体的入口，出口路由信息。

【举例】

配置 vpn-instance vpn1 中最大路由数为 1000。

```
[H3C] ip vpn-instance vpn1
[H3C-vpn-vpn1] route-distinguisher 100:1
[H3C-vpn-vpn1] vpn-target 100:1 import-extcommunity
[H3C-vpn-vpn1] routing-table limit 1000 syslog-alert
```

6.1.25 sham-link

【命令】

sham-link *source-addr destination-addr* [**cost** *cost-value*] [**dead** *seconds*] [**hello** *seconds*] [**md5** *keyid key seconds*] [**retransimit** *seconds*] [**simple** *passwor*] [**trans-delay** *seconds*]

undo sham-link *source-addr destination-addr*

【视图】

OSPF 区域视图

【参数】

source-addr：sham-link 的源地址，为一个 32 位掩码的 loopback 接口地址。

destination-addr：sham-link 的目的地址，为一个 32 位掩码的 loopback 接口地址。

cost-vlaue：经过 sham link 的开销，取值范围为 1～65535，缺省为 1。

password：指定接口的明文验证字，最多 8 个字符。该值必须与 sham link 邻居的验证字相一致。

keyid：指定接口的 MD5 验证字标识符。*keyid* 的取值范围为 1～255。它必须与 sham link 邻居的验证字标识符相等。

key：指定接口的验证字。*keyid* 的取值范围为 1～255，*key* 是最多 16 个字符的字符串。它必须与 sham link 邻居的验证字相等。当用户使用 **display current-configuration** 命令显示系统信息时，系统以 24 个字符的 cipher 密文形式显示配置的 md5 验证字。系统也支持直接输入长度为 24 个字符的 cipher 密文形式验证字。

dead *seconds*：指定死亡定时器的时间间隔，取值范围为 1～8192 秒，缺省值为 40 秒。该值必须 sham link 邻居路由器的 **dead** *seconds* 值相等。

hello *seconds*：指定在接口上发送 Hello 报文的时间间隔，取值范围为 1～8192 秒，缺省值为 10 秒。该值必须与 sham link 邻居路由器上的 **hello** *seconds* 值相等。

retransmit *seconds*：指定在接口上重传 LSA 报文的时间间隔，取值范围为 1～8192 秒，缺省值为 5 秒。

trans-delay *seconds*：指定在接口上延迟发送 LSA 报文的时间间隔，取值范围为 1～8192 秒，缺省值为 1 秒。

【描述】

sham-link 命令用来配置一条 sham link，**undo sham-link** 命令用来删除 sham link。

在 OSPF 的 PE-CE 连接中，假定同一个 OSPF 区域中有两个站点（这两个站点属于同一个 VPN），每一个站点都连接到了不同的 PE 路由器上，并且两个站点之间还存在一条区域内的 OSPF 链路(backdoor)。此时尽管可能会有其他一些路由通过

PE 路由器连接两个站点的，但这些路由会以区域间路由的形式出现，这样 OSPF 会优先考虑经过 backdoor 链路的路由。但在一些时候，人们希望优先考虑经过 VPN 骨干的路由，这时候就需要在 PE 路由器之间建立 sham link 链路，使经过 VPN 骨干的路由成为 OSPF 区域内部优先级最高的路由。

在 VPN PE 间配置 sham-link，将其视为 OSPF 区域内的一条 link。其中源和目的地址均为 32 位掩码的 loopback 接口地址，且该 loopback 接口需在 VPN 实例中绑定，并通过 BGP 引入直连路由引入到 BGP 中。在 sham link 的配置命令中，各可选参数的配置是按追加方式进行的。这些可选参数不能单独进行 undo。

⚠ 注意：

- sham link 的源和目的地址均为 32 位掩码的 loopback 接口地址，且该 loopback 接口需在 VPN 实例中绑定，并通过 BGP 引入直连路由引入到 BGP 中。
- 配置的 sham link 的源和目的地址不能够相同。
- 在不同 OSPF 进程中不能配置相同的 sham link。
- 在一个 OSPF 进程中，最多只能配置 50 条 sham link。

【举例】

配置一条 sham-link，其源地址为 1.1.1.1，目的地址为 2.2.2.2：

```
[H3C-ospf-100-area-0.0.0.1] sham-link 1.1.1.1 2.2.2.2 cost 100
```

6.1.26 vpn-instance-capability simple

【命令】

vpn-instance-capability simple

undo vpn-instance-capability

【视图】

OSPF 协议视图

【参数】

无。

【描述】

vpn-instance-capability simple 命令用来配置安全网关变为 Multi-VPN-Instance CE，**undo vpn-instance-capability** 命令用来取消该配置。

OSPF 多实例通常运行在 PE 路由器上，对于运行 OSPF 多实例的 CE 路由器，通常称之为 Multi-VPN-Instance CE。Multi-VPN-Instance CE 与 PE 虽然都支持多实例，但是 Multi-VPN-Instance CE 不需要具有 BGP/OSPF 互操作功能。

OSPF 进程绑定 VPN 实例后，OSPF 默认路由器是 PE 路由器。配置该命令，将取消对 PE 路由器的默认，安全网关变为 Multi-VPN-Instance CE。配置该命令后，OSPF 进程将重新建立所有的邻居；路由计算时不检测 DN 比特和 route tag，关闭 PE 路由上的路由环路检测功能，防止路由丢失；同时禁止 BGP/OSPF 互操作功能，节省系统资源。

执行 **display ospf brief** 命令可以看到提示信息：

```
Multi-VPN-Instance enable on CE router。
```

⚠ 注意：

配置命令后，OSPF 进程将重新建立所有的邻居。

【举例】

配置 OSPF 进程 100 为 Multi-VPN-Instance CE。

```
[H3C-ospf-100] vpn-instance-capability simple
```

恢复 OSPF 进程 100 为 PE。

```
[H3C-ospf-100] undo vpn-instance-capability
```

6.1.27 vpn-target

【命令】

vpn-target *vpn-target-ext-community* [**import-extcommunity** | **export-extcommunity** | **both**]

undo vpn-target *vpn-target-ext-community* [**import-extcommunity** | **export-extcommunity** | **both**]

【视图】

VPN 实例视图

【参数】

import-extcommunity：从目标 VPN 扩展团体来的入口路由信息。

export-extcommunity：到目标 VPN 扩展团体去的出口路由信息。

both：导入入口和出口路由信息到目标 VPN 扩展团体。

vpn-target-ext-community：添加 vpn-target 扩展团体属性到 vpn-instance 的入口，出口，或者两者（入口和出口）的 vpn-target 扩展团体列表中。

【描述】

vpn -target 命令用来为 vpn-instance 创建 vpn-target 扩展团体，**undo vpn -target** 命令用来取消 vpn-target 扩展团体属性。

缺省情况下，缺省值为 **both**。

vpn-target 命令为指定的 vpn-instance 创建入口和出口 vpn-target 扩展团体列表。为每个目标团体执行一次这个命令。得到的承载特定 vpn-target 扩展团体的路由被导入到所有 vpn-instance 中，这些 vpn-instance 配置了扩展团体作为入口 vpn-target。vpn-target 指定了一个目标 VPN 扩展团体。像 RD 一样，一个扩展团体或者是由一个自治系统号和一个任意的数组成，或者是由一个 IP 地址和一个任意的数组成。

有以下格式：

16 位自治系统号(ASN)：32 位用户自定义数，例如：101：3

32 位 IP 地址：16 位用户自定义数，例如：192.168.122.15：1

【举例】

为 vpn-instance 创建 vpn-target 扩展团体。

```
[H3C] ip vpn-instance vpn-instance_blue
[H3C-vpn-vpn-instance_blue] vpn-target 1000:1 both
[H3C-vpn-vpn-instance_blue] vpn-target 1000:2 export-extcommunity
[H3C-vpn-vpn-instance_blue] vpn-target 173.27.0.130:2 import-extcommunity
```

目 录

第 1 章 AAA及RADIUS/HWTACACS协议配置命令 1-1
1.1 AAA配置命令 1-1
1.1.1 access-limit 1-1
1.1.2 accounting 1-1
1.1.3 accounting optional 1-2
1.1.4 authentication 1-3
1.1.5 authentication super hwtacacs-scheme 1-4
1.1.6 authorization 1-5
1.1.7 display connection 1-5
1.1.8 display domain 1-7
1.1.9 display local-user 1-8
1.1.10 domain 1-9
1.1.11 ip pool 1-11
1.1.12 level 1-12
1.1.13 local-user 1-12
1.1.14 local-user password-display-mode 1-13
1.1.15 password 1-14
1.1.16 scheme 1-15
1.1.17 service-type 1-16
1.1.18 service-type dvpn 1-17
1.1.19 service-type ftp 1-17
1.1.20 service-type ppp 1-18
1.1.21 state 1-18
1.1.22 super authentication-mode 1-19
1.2 RADIUS协议配置命令 1-20
1.2.1 accounting optional 1-20
1.2.2 data-flow-format 1-20
1.2.3 debugging local-server 1-21
1.2.4 debugging radius 1-22
1.2.5 display local-server statistics 1-23
1.2.6 display radius scheme 1-23
1.2.7 display radius statistics 1-25
1.2.8 display stop-accounting-buffer 1-29
1.2.9 key 1-30
1.2.10 local-server 1-31
1.2.11 nas-ip 1-32
1.2.12 primary accounting 1-32
1.2.13 primary authentication 1-33
1.2.14 radius scheme 1-34
1.2.15 radius nas-ip 1-35
1.2.16 radius trap 1-36

1.2.17 reset radius statistics 1-36
1.2.18 reset stop-accounting-buffer 1-37
1.2.19 retry 1-38
1.2.20 retry realtime-accounting 1-38
1.2.21 retry stop-accounting 1-39
1.2.22 secondary accounting 1-40
1.2.23 secondary authentication 1-41
1.2.24 server-type 1-42
1.2.25 state 1-42
1.2.26 stop-accounting-buffer enable 1-43
1.2.27 timer quiet 1-44
1.2.28 timer realtime-accounting 1-45
1.2.29 timer response-timeout 1-46
1.2.30 user-name-format 1-46
1.3 HWTACACS协议配置命令 1-47
1.3.1 data-flow-format 1-47
1.3.2 debugging hwtacacs 1-48
1.3.3 display hwtacacs scheme 1-49
1.3.4 display stop-accounting-buffer 1-51
1.3.5 hwtacacs nas-ip 1-52
1.3.6 hwtacacs scheme 1-53
1.3.7 key 1-53
1.3.8 nas-ip 1-54
1.3.9 primary accounting 1-55
1.3.10 primary authentication 1-55
1.3.11 primary authorization 1-56
1.3.12 reset hwtacacs statistics 1-57
1.3.13 reset stop-accounting-buffer 1-57
1.3.14 retry stop-accounting 1-58
1.3.15 secondary accounting 1-59
1.3.16 secondary authentication 1-59
1.3.17 secondary authorization 1-60
1.3.18 stop-accounting-buffer enable 1-61
1.3.19 timer quiet 1-61
1.3.20 timer realtime-accounting 1-62
1.3.21 timer response-timeout 1-63
1.3.22 user-name-format 1-64
第 2 章 访问控制列表配置命令 2-1
2.1 访问控制列表配置命令 2-1
2.1.1 acl 2-1
2.1.2 acl counter 2-2
2.1.3 description 2-2
2.1.4 display acl 2-3
2.1.5 reset acl counter 2-3
2.1.6 rule 2-4

2.1.7 rule comment 2-8
2.2 时间段配置命令 2-9
2.2.1 display time-range 2-9
2.2.2 time-range 2-10
第 3 章 NAT配置命令 3-1
3.1 NAT配置命令 3-1
3.1.1 connection-limit default 3-1
3.1.2 connection-limit default amount 3-1
3.1.3 connection-limit enable 3-2
3.1.4 connection-limit policy 3-3
3.1.5 debugging connection-limit 3-3
3.1.6 debugging nat 3-4
3.1.7 display connection-limit policy 3-4
3.1.8 display connection-limit statistics 3-5
3.1.9 display nat 3-6
3.1.10 display nat connection-limit 3-8
3.1.11 limit 3-9
3.1.12 nat address-group 3-10
3.1.13 nat aging-time 3-11
3.1.14 nat alg 3-12
3.1.15 nat connection-limit-policy 3-13
3.1.16 nat dns-map 3-13
3.1.17 nat match factor-all 3-14
3.1.18 nat outbound *acl-number* 3-15
3.1.19 nat outbound interface 3-16
3.1.20 nat outbound static 3-17
3.1.21 nat overlapaddress 3-17
3.1.22 nat server 3-18
3.1.23 nat session refresh-speed 3-21
3.1.24 nat static 3-21
3.1.25 nat static inside 3-22
3.1.26 reset nat 3-23
第 4 章 防火墙配置命令 4-1
4.1 包过滤防火墙配置命令 4-1
4.1.1 debugging firewall packet-filter 4-1
4.1.2 debugging firewall packet-filter fragments-inspect events 4-2
4.1.3 display firewall fragment 4-2
4.1.4 display firewall packet-filter statistics 4-3
4.1.5 firewall packet-filter default 4-3
4.1.6 firewall packet-filter enable 4-4
4.1.7 firewall packet-filter fragments-inspect 4-4
4.1.8 firewall packet-filter fragments-inspect { high | low } 4-5
4.1.9 firewall packet-filter *acl-number* 4-6
4.1.10 reset firewall packet-filter statistics 4-7

4.2 状态防火墙配置命令 4-7
4.2.1 aging-time 4-7
4.2.2 aspf-policy 4-8
4.2.3 debugging aspf 4-9
4.2.4 debugging aspf http 4-10
4.2.5 detect 4-11
4.2.6 detect http 4-12
4.2.7 display aspf all 4-13
4.2.8 display aspf interface 4-14
4.2.9 display aspf policy 4-15
4.2.10 display aspf session 4-15
4.2.11 display aspf statistics 4-17
4.2.12 display firewall session aging-time 4-18
4.2.13 display firewall session table 4-18
4.2.14 display port-mapping 4-19
4.2.15 firewall aspf 4-20
4.2.16 firewall session aging-time 4-21
4.2.17 firewall session aging-time default 4-22
4.2.18 log enable 4-22
4.2.19 port-mapping 4-23
4.2.20 reset aspf session 4-24
4.2.21 reset aspf statistic http 4-24
4.2.22 reset firewall session table 4-25
4.3 黑名单配置命令 4-25
4.3.1 debugging firewall blacklist 4-25
4.3.2 display firewall blacklist 4-26
4.3.3 firewall blacklist 4-27
4.4 MAC和IP地址绑定配置命令 4-28
4.4.1 debugging firewall mac-binding 4-28
4.4.2 display firewall mac-binding 4-28
4.4.3 firewall mac-binding 4-30
4.4.4 firewall mac-binding enable 4-30
4.4.5 reset firewall mac-binding 4-31
4.5 区域配置命令 4-31
4.5.1 add interface 4-31
4.5.2 display interzone 4-32
4.5.3 display zone 4-32
4.5.4 set priority 4-33
4.5.5 firewall interzone 4-34
4.5.6 firewall zone 4-34
4.5.7 firewall zone name 4-35
第 5 章 面向对象管理配置命令 5-1
5.1 对象管理配置命令 5-1
5.1.1 acl name 5-1

5.1.2 add 5-1
5.1.3 debugging object dns 5-2
5.1.4 display acl 5-3
5.1.5 display object address 5-3
5.1.6 display object address-group 5-4
5.1.7 display object predefined service 5-4
5.1.8 display object service 5-5
5.1.9 display object service-group 5-5
5.1.10 object address 5-6
5.1.11 object address-group 5-7
5.1.12 object refresh dns 5-7
5.1.13 object service 5-8
5.1.14 object service-group 5-9
5.1.15 reset acl counter 5-10
5.1.16 rule 5-10
5.2 对象引用配置命令 5-12
5.2.1 firewall packet-filter *acl-name* 5-12
5.2.2 nat outbound *acl-name* 5-12
第 6 章 透明防火墙配置命令 6-1
6.1 透明防火墙配置命令 6-1
6.1.1 acl number 6-1
6.1.2 bridge vlanid-transparent-transmit enable 6-1
6.1.3 debugging firewall eff 6-2
6.1.4 debugging firewall transparent-mode eth-forwarding 6-4
6.1.5 debugging firewall transparent-mode ip-forwarding 6-5
6.1.6 display firewall ethernet-frame-filter 6-7
6.1.7 display firewall mode 6-8
6.1.8 display firewall transparent-mode address-table 6-8
6.1.9 display firewall transparent-mode config 6-9
6.1.10 display firewall transparent-mode traffic 6-10
6.1.11 firewall arp-learning enable 6-12
6.1.12 firewall ethernet-frame-filter 6-12
6.1.13 firewall mode 6-13
6.1.14 firewall system-ip 6-14
6.1.15 firewall transparent-mode aging-time 6-15
6.1.16 firewall transparent-mode transmit 6-15
6.1.17 firewall unknown-mac 6-16
6.1.18 firewall unknown-mac broadcast 6-17
6.1.19 firewall unknown-mac multicast 6-17
6.1.20 firewall unknown-mac unicast 6-18
6.1.21 reset firewall ethernet-frame-filter 6-19
6.1.22 reset firewall transparent-mode address-table 6-19
6.1.23 reset firewall transparent-mode traffic 6-20
6.1.24 rule 6-20

第 7 章 混合模式配置命令 7-1
7.1 网桥配置命令 7-1
7.1.1 acl number 7-1
7.1.2 bridge aging-time 7-1
7.1.3 bridge bridge-set enable 7-2
7.1.4 bridge bridging 7-3
7.1.5 bridge enable 7-3
7.1.6 bridge firewall unknown-mac 7-4
7.1.7 bridge firewall unknown-mac broadcast 7-5
7.1.8 bridge firewall unknown-mac multicast 7-5
7.1.9 bridge firewall unknown-mac unicast 7-6
7.1.10 bridge learning 7-7
7.1.11 bridge mac-address 7-7
7.1.12 bridge permit 7-8
7.1.13 bridge vlanid-transparent-transmit enable 7-9
7.1.14 bridge-set 7-10
7.1.15 bridge-set fast-forwarding 7-10
7.1.16 debugging bridge eth-forwarding 7-11
7.1.17 debugging bridge ip-forwarding 7-12
7.1.18 debugging firewall eff 7-13
7.1.19 display bridge address-table 7-15
7.1.20 display bridge information 7-16
7.1.21 display bridge traffic 7-17
7.1.22 display firewall ethernet-frame-filter 7-19
7.1.23 display interface bridge-template 7-20
7.1.24 firewall ethernet-frame-filter 7-21
7.1.25 interface bridge-template 7-21
7.1.26 mac-address 7-22
7.1.27 reset bridge address-table 7-23
7.1.28 reset bridge traffic 7-23
7.1.29 reset firewall ethernet-frame-filter 7-24
7.1.30 rule 7-24
第 8 章 PKI配置命令 8-1
8.1 PKI域配置命令 8-1
8.1.1 ca identifier 8-1
8.1.2 certificate request entity 8-1
8.1.3 certificate request from 8-2
8.1.4 certificate request mode 8-3
8.1.5 certificate request polling 8-3
8.1.6 certificate request url 8-4
8.1.7 crl check disable 8-5
8.1.8 crl update-period 8-5
8.1.9 crl url 8-6
8.1.10 ldap-server 8-6
8.1.11 pki domain 8-7

8.1.12 root-certificate fingerprint 8-8
8.2 PKI实体配置命令 8-8
8.2.1 fqdn 8-8
8.2.2 common-name 8-9
8.2.3 country 8-9
8.2.4 ip 8-10
8.2.5 locality 8-11
8.2.6 organization 8-11
8.2.7 organization-unit 8-12
8.2.8 state 8-12
8.2.9 pki entity 8-13
8.3 PKI证书操作命令 8-13
8.3.1 pki delete-certificate 8-13
8.3.2 pki import-certificate 8-14
8.3.3 pki request-certificate 8-14
8.3.4 pki retrieval-certificate 8-15
8.3.5 pki retrieval-crl 8-16
8.3.6 pki validate-certificate 8-16
8.4 PKI显示与调试命令 8-17
8.4.1 debugging pki 8-17
8.4.2 display pki certificate 8-21
8.4.3 display pki crl 8-23
第 9 章 SSL配置命令 9-1
9.1 SSL服务器策略配置命令 9-1
9.1.1 ciphersuite 9-1
9.1.2 client-verify 9-2
9.1.3 close-mode 9-2
9.1.4 debugging ssl server 9-3
9.1.5 display ssl server-policy 9-4
9.1.6 handshake timeout 9-5
9.1.7 pki-domain 9-5
9.1.8 session 9-6
9.1.9 ssl server-policy 9-7
9.2 SSL加密卡配置命令 9-7
9.2.1 debugging ssl card 9-7
9.2.2 display interface ssl-card 9-8
9.2.3 shutdown 9-9
9.2.4 use ssl-card 9-9
9.3 基于证书属性访问控制策略配置命令 9-10
9.3.1 attribute 9-10
9.3.2 display pki certificate access-control-policy 9-11
9.3.3 display pki certificate attribute-group 9-12
9.3.4 pki certificate access-control-policy 9-12
9.3.5 pki certificate attribute-group 9-13

9.3.6 rule 9-13
9.4 SSL Proxy配置命令 9-14
9.4.1 debugging ssl proxy 9-14
9.4.2 display ssl proxy 9-15
9.4.3 display ssl-proxy session 9-16
9.4.4 port 9-16
9.4.5 reset ssl proxy statistic 9-17
9.4.6 reset ssl-proxy session 9-17
9.4.7 server ip 9-18
9.4.8 ssl proxy 9-18
9.4.9 ssl proxy server 9-19
9.4.10 ssl-server-policy 9-20
第 10 章 Web和邮件过滤配置命令 10-1
10.1 Web过滤配置命令 10-1
10.1.1 debugging firewall url-filter host 10-1
10.1.2 debugging firewall url-filter parameter 10-1
10.1.3 debugging firewall webdata-filter 10-2
10.1.4 display firewall url-filter host 10-3
10.1.5 display firewall url-filter parameter 10-3
10.1.6 display firewall url-filter parameter counter detail 10-4
10.1.7 display firewall webdata-filter 10-5
10.1.8 firewall url-filter host acl-number 10-5
10.1.9 firewall url-filter host add 10-6
10.1.10 firewall url-filter host clear 10-7
10.1.11 firewall url-filter host default 10-7
10.1.12 firewall url-filter host delete 10-8
10.1.13 firewall url-filter host enable 10-8
10.1.14 firewall url-filter host ip-address 10-9
10.1.15 firewall url-filter host save-file 10-9
10.1.16 firewall url-filter host load-file 10-10
10.1.17 firewall url-filter parameter add 10-10
10.1.18 firewall url-filter parameter add-default 10-11
10.1.19 firewall url-filter parameter clear 10-12
10.1.20 firewall url-filter parameter delete 10-12
10.1.21 firewall url-filter parameter enable 10-13
10.1.22 firewall url-filter parameter load-file 10-14
10.1.23 firewall url-filter parameter save-file 10-14
10.1.24 firewall webdata-filter add 10-15
10.1.25 firewall webdata-filter clear 10-16
10.1.26 firewall webdata-filter delete 10-16
10.1.27 firewall webdata-filter enable 10-16
10.1.28 firewall webdata-filter load-file 10-17
10.1.29 firewall webdata-filter save-file 10-18
10.1.30 reset firewall url-filter host counter 10-18
10.1.31 reset firewall url-filter parameter counter 10-19

10.1.32 reset firewall webdata-filter counter 10-19
10.2 邮件过滤配置命令 10-20
10.2.1 debugging firewall smtp-filter 10-20
10.2.2 display firewall smtp-filter 10-20
10.2.3 firewall smtp-filter attach add 10-21
10.2.4 firewall smtp-filter attach clear 10-22
10.2.5 firewall smtp-filter attach delete 10-22
10.2.6 firewall smtp-filter attach enable 10-23
10.2.7 firewall smtp-filter attach load-file 10-23
10.2.8 firewall smtp-filter attach save-file 10-24
10.2.9 firewall smtp-filter content add 10-24
10.2.10 firewall smtp-filter content clear 10-25
10.2.11 firewall smtp-filter content delete 10-25
10.2.12 firewall smtp-filter content enable 10-26
10.2.13 firewall smtp-filter content load-file 10-27
10.2.14 firewall smtp-filter content save-file 10-27
10.2.15 firewall smtp-filter rcptto add 10-28
10.2.16 firewall smtp-filter rcptto clear 10-29
10.2.17 firewall smtp-filter rcptto default 10-29
10.2.18 firewall smtp-filter rcptto delete 10-30
10.2.19 firewall smtp-filter rcptto enable 10-30
10.2.20 firewall smtp-filter rcptto load-file 10-31
10.2.21 firewall smtp-filter rcptto save-file 10-31
10.2.22 firewall smtp-filter subject add 10-32
10.2.23 firewall smtp-filter subject clear 10-32
10.2.24 firewall smtp-filter subject delete 10-33
10.2.25 firewall smtp-filter subject enable 10-33
10.2.26 firewall smtp-filter subject load-file 10-34
10.2.27 firewall smtp-filter subject save-file 10-34
10.2.28 reset firewall smtp-filter counter 10-35
第 11 章 攻击防范配置命令 11-1
11.1 攻击防范配置命令 11-1
11.1.1 debugging firewall defend 11-1
11.1.2 display firewall defend flag 11-1
11.1.3 display firewall tcp-proxy session 11-2
11.1.4 firewall defend all 11-4
11.1.5 firewall defend arp-flood 11-4
11.1.6 firewall defend arp-spoofing 11-5
11.1.7 firewall defend fraggle 11-5
11.1.8 firewall defend frag-flood 11-6
11.1.9 firewall defend icmp-flood 11-7
11.1.10 firewall defend icmp-flood enable 11-8
11.1.11 firewall defend icmp-redirect 11-8
11.1.12 firewall defend icmp-unreachable 11-9
11.1.13 firewall defend ip-fragment 11-9

11.1.14 firewall defend ip-spoofing 11-10
11.1.15 firewall defend ip-sweep 11-10
11.1.16 firewall defend land 11-11
11.1.17 firewall defend large-icmp 11-12
11.1.18 firewall defend ping-of-death 11-12
11.1.19 firewall defend port-scan 11-13
11.1.20 firewall defend route-record 11-14
11.1.21 firewall defend smurf 11-14
11.1.22 firewall defend source-route 11-15
11.1.23 firewall defend syn-flood 11-15
11.1.24 firewall defend syn-flood enable 11-16
11.1.25 firewall defend tcp-flag 11-17
11.1.26 firewall defend teardrop 11-18
11.1.27 firewall defend tracert 11-18
11.1.28 firewall defend udp-flood 11-19
11.1.29 firewall defend udp-flood enable 11-20
11.1.30 firewall defend winnuke 11-20
11.1.31 firewall tcp-proxy 11-21
第 12 章 IDS联动配置命令 12-1
12.1 IDS联动配置命令 12-1
12.1.1 ids-acl enable 12-1
12.1.2 display ids 12-1
12.1.3 display ids-acl 12-2
12.1.4 debugging ids-acl 12-3
第 13 章 报文统计与日志配置命令 13-1
13.1 报文统计配置命令 13-1
13.1.1 display firewall statistic 13-1
13.1.2 display firewall statistic system defend 13-3
13.1.3 display firewall statistic system flow-percent 13-4
13.1.4 firewall statistic system connect-number 13-5
13.1.5 firewall statistic system enable 13-6
13.1.6 firewall statistic system flow-percent 13-6
13.1.7 firewall statistic warning-level drop 13-7
13.1.8 reset firewall statistic ip 13-8
13.1.9 reset firewall statistic system 13-8
13.1.10 reset firewall statistic zone 13-9
13.1.11 statistic connect-number ip 13-9
13.1.12 statistic connect-number zone 13-11
13.1.13 statistic connect-speed ip 13-12
13.1.14 statistic connect-speed zone 13-13
13.1.15 statistic enable 13-14
13.2 SMTP客户端配置命令 13-14
13.2.1 debugging smtpc 13-14
13.2.2 display smtpc 13-15

13.2.3 smtpc administrator mail 13-16
13.2.4 smtpc trigger time 13-16
13.3 DNS客户端配置命令 13-17
13.3.1 debugging dnsc 13-17
13.3.2 display dnsc 13-17
13.3.3 dnsc server 13-18
13.3.4 dnsc cache 13-19
13.4 日志配置命令 13-19
13.4.1 debugging flowlog 13-19
13.4.2 firewall binary-log host 13-20
13.4.3 firewall log-time 13-21
13.4.4 firewall nat log-type 13-21
13.4.5 firewall session log-threshold 13-22
13.4.6 firewall session log-type 13-23
13.4.7 session log enable 13-24
13.4.8 reset firewall log-buf 13-24

第1章 AAA 及 RADIUS/HWTACACS 协议配置命令

1.1 AAA 配置命令

1.1.1 access-limit

【命令】

access-limit { **disable** | **enable** *max-user-number* }

undo access-limit

【视图】

ISP 域视图

【参数】

disable：表示不对当前 ISP 域可容纳的接入用户数作限制。

enable *max-user-number*：表示当前 ISP 域可容纳接入用户数的最大值，取值范围为 1～7072。

【描述】

access-limit 命令用来指定当前 ISP 域可容纳接入用户数的最大值。**undo access-limit** 命令用来恢复缺省设置。

缺省情况下，不对当前 ISP 域可容纳的接入用户数作限制。

由于接入用户之间会发生资源的争用，因此适当地配置该值可以使属于当前 ISP 域的用户获得可靠的性能保障。

【举例】

指定 ISP 域“mydomain.net”最多可容纳 500 个接入用户。

```
[H3C-isp-mydomain.net] access-limit enable 500
```

1.1.2 accounting

【命令】

accounting { **hwtacacs-scheme** *hwtacacs-scheme-name* | **radius-scheme** *radius-scheme-name* | **none** }

undo accounting

【视图】

ISP 域视图

【参数】

hwtacacs-scheme *hwtacacs-scheme-name*：指定计费使用 HWTACACS 方案。

radius-scheme *radius-scheme-name*：指定计费使用 RADIUS 方案。

none：不计费。

【描述】

accounting 命令用来配置当前 ISP 域使用的计费方案。**undo accounting** 命令用来删除 ISP 域使用的计费方案。

缺省情况下，系统没有配置计费方案。

accounting 命令为当前 ISP 域指定引用的 RADIUS/HWTACACS 方案时，所引用的 RADIUS/HWTACACS 方案必须是已经设置好的。

在域视图下，如果配置了 **accounting** 命令，则采用该命令中引用的计费方案进行计费；否则使用 **scheme** 命令中引用的方案进行计费。

相关配置可参考命令 **scheme**，**radius scheme**，**hwtacacs scheme**。

【举例】

指定当前 ISP 域 h3c163.net 引用的 RADIUS 计费方案为 **radius**。

```
[H3C-isp-h3c163.net] accounting radius-scheme radius
```

设置 ISP 域 h3c 引用的为 HWTACACS 计费方案为 hwtac。

```
[H3C-isp-h3c] accounting hwtacacs-scheme hwtac
```

1.1.3 accounting optional

【命令】

accounting optional

undo accounting optional

【视图】

ISP 域视图

【参数】

无

【描述】

accounting optional 命令用来打开计费可选开关，**undo accounting optional** 命令用来关闭计费可选开关。

系统缺省为关闭计费可选开关。

当没有可用的计费服务器或与计费服务器通信失败时，若配置了 **accounting optional** 命令，则用户可以继续使用网络资源，否则用户将被切断。这个命令经常被用于只认证不计费的情况。

【举例】

打开名为 mydomain.net 的域用户的计费可选开关。

```
[H3C] domain mydomain.net
[H3C-isp-mydomain.net] accounting optional
```

1.1.4 authentication

【命令】

authentication { **hwtacacs-scheme** *hwtacacs-scheme-name* [**local**] | **radius-scheme** *radius-scheme-name* [**local**] | **local** | **none** }

undo authentication

【视图】

ISP 域视图

【参数】

hwtacacs-scheme *hwtacacs-scheme-name*：指定认证使用的 HWTACACS 方案。

radius-scheme *radius-scheme-name*：指定认证使用的 RADIUS 方案。

local：指定认证使用本地认证方案。

none：不认证。

【描述】

authentication 命令用来配置当前 ISP 域使用的认证方案。**undo authentication** 命令用来恢复域缺省的认证方案。

缺省情况下，系统认证方案为 local。

当使用 **authentication** 命令为当前 ISP 域指定引用的 RADIUS/HWTACACS 方案时，所引用的 RADIUS/HWTACACS 方案必须是已经设置好的。

如果配置了 **authentication radius-scheme** *radius-scheme-name* **local** 或 **authentication hwtacacs-scheme** *hwtacacs-scheme-name* **local**，则 **local** 为 RADIUS 服务器或 TACACS 服务器没有正常响应后的备选认证方案。即当 RADIUS

服务器或 TACACS 服务器有效时，不使用本地认证；当 RADIUS 服务器或 TACACS 服务器无效时，使用本地认证。

如果 **local** 作为第一方案，那么只能采用本地认证，不能再同时采用 RADIUS 或 HWTACACS 方案。**none** 与 **local** 的使用情况相同。

在域视图下，如果配置了 **authentication** 命令，则采用该命令中引用的认证方案进行认证；否则使用 **scheme** 命令中引用的方案进行认证。

相关配置可参考命令 **scheme**，**radius scheme**，**hwtacacs scheme**。

【举例】

指定当前 ISP 域 h3c163.net 引用的 RADIUS 认证方案为 **radius**。

```
[H3C-isp-h3c163.net] authentication radius-scheme radius
```

设置 ISP 域 h3c 引用的 RADIUS 认证方案为 rd，并采用 local 作为备选认证方案。

```
[H3C-isp-h3c] authentication radius-scheme rd local
```

设置 ISP 域 h3c 引用的 HWTACACS 认证方案为 hwtac，并采用 local 作为备选认证方案。

```
[H3C-isp-h3c] authentication hwtacacs-scheme hwtac local
```

1.1.5 authentication super hwtacacs-scheme

【命令】

authentication super hwtacacs-scheme *hwtacacs-scheme-name*

undo authentication super hwtacacs-scheme

【视图】

ISP 域视图

【参数】

hwtacacs-scheme-name：指定 HWTACACS 方案名称。

【描述】

authentication super hwtacacs-scheme 命令用来设置域的 super 认证方案。

undo authentication super 命令用来取消域的 super 认证方案。

缺省情况下，未配置 super 认证方案。

【举例】

配置 system 域的 super 认证方案为 sup。

```
[H3C] domain system
[H3C-isp-system] authentication super hwtacacs-scheme sup
```

1.1.6 authorization

【命令】

authorization { **hwtacacs-scheme** *hwtacacs-scheme-name* | **none** }

undo authorization

【视图】

ISP 域视图

【参数】

hwtacacs-scheme *hwtacacs-scheme-name*：指定授权使用的 HWTACACS 方案。

none：不需要授权，即不需要授权也可以提供服务。

【描述】

authorization 命令用来配置当前 ISP 域使用的授权方案。**undo authorization** 命令用来恢复域缺省的授权方案。

缺省情况下，系统授权方案为 local。

当使用 **authorization** 命令为当前 ISP 域指定引用的 RADIUS/HWTACACS 方案时，所引用的 RADIUS/HWTACACS 方案必须是已经设置好的。

在域视图下，如果配置了 **authorization** 命令，则采用该命令中引用的授权方案进行授权；否则使用 **scheme** 命令中引用的方案进行授权。

相关配置可参考命令 **scheme**，**radius scheme**，**hwtacacs scheme**。

【举例】

设置 ISP 域 h3c 引用的 HWTACACS 授权方案为 hwtac。

```
[H3C-isp-h3c] authorization hwtacacs-scheme hwtac
```

1.1.7 display connection

【命令】

display connection [**domain** *isp-name* | **ip** *ip-address* | **mac** *mac-address* | **radius-scheme** *radius-scheme-name* | **hwtacacs-scheme** *hwtacacs-scheme-name* | **ucibindex** *ucib-index* | **user-name** *user-name*]

【视图】

所有视图

【参数】

domain *isp-name*：显示某个 ISP 域下的全部用户连接。其中，*isp-name* 为 ISP 域名，为不超过 24 个字符的字符串。指定的 ISP 域必须已经存在。

ip *ip-address*：显示某个 IP 地址为 *ip-address* 的所有用户连接。

mac *mac-address*：显示某个 MAC 地址为 *mac-address* 的用户连接。其中，*mac-address* 为点分十六进制格式（即如 X-X-X 的样式）。

radius-scheme *radius-scheme-name*：显示名称为 *radius-scheme-name* 的 RADIUS 方案的所有用户连接。*radius-scheme-name* 为不超过 32 个字符的字符串。

hwtacacs-scheme *hwtacacs-scheme-name*：显示名称为 *hwtacacs-scheme-name* 的 HWTACACS 方案的所有用户连接。*hwtacacs-scheme-name* 为不超过 32 个字符的字符串。

ucibindex *ucib-index*：显示某个连接索引号为 *ucib-index* 的用户连接。其中，*ucib-index* 的取值范围为 0～7071。

user-name *user-name*：显示某个用户名为 *user-name* 的用户连接。其中，用户名的格式为 *pure-username@domain*。*pure-username* 为纯用户名，不超过 55 个字符；*domain* 为域名，不超过 24 个字符。

【描述】

display connection 命令用来显示所有或指定的用户连接的相关信息。根据输出的信息，可以帮助诊断与排除用户连接方面的故障。

缺省情况下，显示所有用户连接的相关信息。

【举例】

显示所有用户 system 连接的相关信息。

```
<H3C> display connection domain system
Index=0   ,Username=hfx@system
 IP=188.188.188.3

 Total 1 connections matched, 1 listed.
```

表1-1 display connection 显示信息描述表

域名	解释
Index	索引号
Username	用户名
IP	该用户的 IP 地址

1.1.8 display domain

【命令】

display domain [*isp-name*]

【视图】

所有视图

【参数】

isp-name：ISP 域名。为不超过 24 个字符的字符串。所指定的 ISP 域必须已经存在。

【描述】

display domain 命令用来显示指定 ISP 域的配置信息或所有 ISP 域的概要信息。

若不指定域名，则显示系统中所有 ISP 域的概要信息。

display domain 命令可以输出指定 ISP 域的配置信息或所有 ISP 域的概要信息。在指定显示某个 ISP 域的配置信息时，输出内容和格式与 **display domain** 命令的输出完全一致。根据输出的信息，可以帮助诊断与排除与 ISP 域有关的故障。

相关配置可参考命令 **access-limit**，**domain**，**scheme**，**state**，**display domain**。

【举例】

显示系统中所有 ISP 域的概要信息。

```
<H3C> display domain
0  Domain = system
   State = Active
   Scheme = LOCAL
   Access-limit = Disable
   Domain User Template:
Default Domain Name: system
Total 1 domain(s).1 listed.
```

表1-2 display domain 显示信息描述表

域名	解释
Domain	域名及序号
State	该域用户的状态（Active/Block）
Scheme	该域用户的认证方案（Local/Radius/Tacacs）
Access-limit	对该域用户能够同时接入用户的数量是否进行限制（Disable/Enable）

1.1.9 display local-user

【命令】

display local-user [**domain** *isp-name* | **service-type** { **telnet** | **ssh** | **terminal** | **dvpn** | **ftp** | **ppp** } | **state** { **active** | **block** } | **user-name** *user-name*]

【视图】

所有视图

【参数】

domain *isp-name*：显示属于某个 ISP 域的全部本地用户。其中，*isp-name* 为 ISP 域名，为不超过 24 个字符的字符串。指定的 ISP 域必须已经存在。

service-type：根据用户类型显示本地用户。其中，**telent** 为 telnet 用户；**ssh** 为 SSH 用户；**terminal** 为从 Console 口、AUX 口登录的终端用户；**ftp** 指定用户为 FTP 类型；**ppp** 为 PPP 用户；**dvpn** 为 DVPN 用户。

state { **active** | **block** }：显示处于某种状态的本地用户。其中，**active** 表示系统允许用户请求网络服务；**block** 表示系统不允许用户请求网络服务。

user-name *user-name*：显示用户名为 *user-name* 的本地用户。其中，*user-name* 为用户名，为不超过 80 个字符的字符串，字符串中不能包括“/”、“:”、“*”、“?”、“<”以及“>”等字符，并且“@”出现的次数不能多于 1 次，纯用户名（“@”以前部分，即用户标识）不能超过 55 个字符。

【描述】

display local-user 命令用来显示所有或指定的本地用户的相关信息。根据输出的信息，可以帮助诊断和排除与本地用户有关的故障。

缺省情况下，显示所有本地用户的相关信息。

相关配置可参考命令 **local-user**。

【举例】

显示所有本地用户的相关信息。

```
<H3C> display local-user
The contents of local user admin:
 State:          Active            ServiceType Mask: T
 Idle-cut:       Disable
 Access-limit:   Disable           Current AccessNum: 0
 Bind location:  Disable
 Vlan ID:        Disable
 IP address:     Disable
 MAC address:    Disable
```

```
 User Privilege: 3

The contents of local user ftpuser:
 State:          Active            ServiceType Mask: F
 Idle-cut:       Disable
 Access-limit:   Disable           Current AccessNum: 0
 Bind location:  Disable
 Vlan ID:        Disable
 IP address:     Disable
 MAC address:    Disable
 FTP Directory:  flash:

Total 2 local user(s) Matched, 2 listed.
ServiceType Mask Meaning: A--PAD  C--Terminal  D--DVPN  F--FTP  P--PPP  S--SSH
T--Telnet
```

对上述显示信息的各项解释如下表所示。

表1-3 display local-user 显示信息描述表

域名	解释
State	该用户的状态（active/block）
ServiceType Mask	服务类型的缩写
Idle-cut	闲置切断开关
Access-Limit	接入用户连接数限制
Current AccessNum	当前接入用户的数量
Bind location	是否与端口捆绑
VLAN ID	用户所属的 VLAN
IP address	用户的 IP 地址
MAC address	用户的 MAC 地址
FTP Directory	授权给 FTP 用户的路径
User Privilege	用户级别

1.1.10 domain

【命令】

domain { *isp-name* | **default** { **disable** | **enable** *isp-name* } }

undo domain *isp-name*

【视图】

系统视图

【参数】

isp-name：ISP 域名。为不超过 24 个字符的字符串，且不能包括“/”、“:”、“*”、“?”、“<”以及“>”等字符。

default：配置缺省的 ISP 域。系统缺省的 ISP 域为 system，用户可以使用该命令手工配置缺省域。系统缺省的 ISP 域为 system。

disable：禁止配置的缺省 ISP 域，此时不带域的用户将被拒绝。如果配置了发送给 RADIUS 服务器的用户不携带域名，此时就不会被拒绝。

enable：使能配置的缺省 ISP 域，此时不带域的用户名在发往 AAA 服务器前将被加上缺省的 ISP 域名。如果配置了发送给 RADIUS 服务器的用户不携带域名，此时不带域的用户名也不会加上缺省的域名。

【描述】

domain 命令用来创建一个 ISP 域，或者进入已创建 ISP 域的视图，**undo domain** 命令用来删除指定的 ISP 域。

缺省情况下，系统中使用的域为“system”，该域不可以删除，但是可以修改其属性。通过 **display domain** 命令可以查看缺省域 system 的设置。

ISP 域即 ISP 用户群，一个 ISP 域即是由同属于一个 ISP 的用户构成的用户群。一般说来，在“userid@isp-name”形式（例如 gw20010608@mydomain.net）的用户名中，“@”后的“isp-name”（如例中的“mydomain.net”）即为 ISP 域的域名。在 AAA 服务器对用户进行接入控制时，对于用户名为“userid@isp-name”形式的 ISP 用户，系统就将把“userid”作为用于身份认证的用户名，把“isp-name”作为域名。

引入 ISP 域的设置是为了支持多 ISP 的应用环境：在这种环境中，同一个接入设备接入的有可能是不同 ISP 的用户。由于各 ISP 用户的用户属性（例如用户名及密码构成、服务类型/权限等）有可能各不相同，因此有必要通过设置 ISP 域的方法把它们区别开。在 ISP 域视图下，可以为每个 ISP 域配置包括 AAA 方案（使用的 RADIUS 方案等）在内的一整套单独的 ISP 域属性。

对于防火墙来说，每个接入用户都属于一个 ISP 域。系统中最多可以配置 16 个 ISP 域。

使用此命令时，如果指定的 ISP 域不存在，系统将会创建一个新的 ISP 域，所有的 ISP 域在创建后即处于 **active** 状态。

相关配置可参考命令 **access-limit**，**scheme**，**state**，**display domain**。

【举例】

创建一个新的 ISP 域“mydomain.net”，并进入其视图。

```
[H3C] domain mydomain.net
New Domain added.
[H3C-isp-mydomain.net]
```

1.1.11 ip pool

【命令】

ip pool *pool-number low-ip-address* [*high-ip-address*]

undo ip pool *pool-number*

【视图】

系统视图、ISP 域视图

【参数】

pool-number：地址池编号，取值范围为 0～99。

low-ip-address 和 *high-ip-address*：分别为地址池的起始和结束 IP 地址。一个地址池中起始 IP 和结束 IP 地址之间的地址数不能超过 1024。如果在定义 IP 地址池时不指定结束 IP 地址，则该地址池中只有一个 IP 地址，即起始 IP 地址。

【描述】

命令 **ip pool** 用来定义为 PPP 用户分配 IP 地址的本地地址池，命令 **undo ip pool** 用来删除指定的本地地址池。

缺省情况下，没有配置本地 IP 地址池。

在系统视图下，配置 IP 地址池，通过在接口视图下使用命令 **remote address** 为 PPP 用户分配 IP 地址。

在 ISP 域视图下，配置的 IP 地址池用于为相应的 ISP 域所属的 PPP 用户分配 IP 地址。这主要用于通过某接口接入的 PPP 用户较多，而接口所能分配的地址不够用的情况。例如，运行 PPPoE 协议的 Ethernet 接口，最多可以接入 4095 个用户，但在该 Ethernet 接口的 Virtual Template 上，只能配置一个地址池，而一个地址池最多只有 1024 个地址，这显然不能满足要求。通过配置 ISP 域的地址池，可以为 ISP 的 PPP 用户分配地址，从而解决接口地址池中地址不够的问题。

相关配置可参考命令 **remote address**。

【举例】

配置本地 IP 地址池 0，地址范围为 129.102.0.1 到 129.102.0.10。

```
[H3C] domain mydomain.net
```

```
[H3C-isp-mydomain.net] ip pool 0 129.102.0.1 129.102.0.10
```

1.1.12 level

【命令】

level *level*

undo level

【视图】

本地用户视图

【参数】

level：指定用户的优先级。*level* 为整数，取值范围 0~3。

【描述】

level 命令用来设置用户的优先级，**undo level** 命令用来恢复用户缺省的优先级。

缺省情况下，用户的优先级为 0。

相关配置可参考命令 **local user**。

🕮 **说明：**

如果配置的认证方式为不认证或采用 password 认证，则用户登录到系统后所能访问的命令级别由用户界面的优先级确定。对于使用 RSA 认证的用户，其所能访问的命令级别由用户界面的优先级确定。如果配置的认证方式需要用户名和口令，则用户登录系统后所能访问的命令级别由用户的优先级确定。

【举例】

设置用户 myuser 的级别为 3。

```
[H3C-luser-myuser] level 3
```

1.1.13 local-user

【命令】

local-user *user-name*

undo local-user *user-name* [**service-type** | **level**]

undo local-user all [**service-type** { **ftp** | **ppp** | **ssh** | **telnet** | **terminal** }]

【视图】

系统视图

【参数】

user-name：本地用户名。为不超过 80 个字符的字符串，字符串中不能包括“/”、“:”、“*”、“?”、“<”以及“>”等字符，并且“@”出现的次数不能多于 1 次，纯用户名（“@”以前部分，即用户标识）不能超过 55 个字符。用户名区分大小写，输入 UserA 和 usera，系统视为不同用户。

service-type：服务类型。

all：所有的用户。

ftp：服务类型为 FTP。

ppp：服务类型为 PPP。

ssh：服务类型为 SSH。

telnet：服务类型为 Telnet。

terminal：终端服务类型。

【描述】

local-user 命令用来添加本地用户并进入本地用户视图，**undo local-user** *user-name* 命令用来删除本地用户或本地用户的相关属性，**undo local-user all** 命令用来删除所有本地用户或指定类型的本地用户。

缺省情况下，无本地用户。

相关配置可参考命令 **display local-user**。

【举例】

添加名称为 myuser 的本地用户。

```
[H3C] local-user myuser
[H3C-luser-myuser]
```

1.1.14 local-user password-display-mode

【命令】

local-user password-display-mode { **cipher-force** | **auto** }

undo local-user password-display-mode

【视图】

系统视图

【参数】

cipher-force：强制 cipher 方式，即所有接入用户的密码显示方式必须采用密文方式。

auto：自动方式，即接入用户的密码显示方式可以由用户自己通过 **password** 命令来设置。

【描述】

local-user password-display-mode 命令用来设置所有本地用户密码的显示方式，**undo local-user password-display-mode** 命令用来恢复缺省的本地用户密码显示方式。

当采用 **cipher-force** 方式后，即使用户通过 **password** 命令指定密码显示方式为明文显示（即 **simple** 方式）后，也不起作用。

缺省情况下，所有接入用户的密码显示方式 **auto**。

相关配置可参考命令 **display local-user， password**。

【举例】

强制所有接入用户采用密码密文方式显示。

```
[H3C] local-user password-display-mode cipher-force
```

1.1.15 password

【命令】

password { **simple** | **cipher** } *password*

undo password

【视图】

本地用户视图

【参数】

simple：表示密码为明文。

cipher：表示密码为密文。

password：表示设置的密码。

当采用 **simple** 明文密码时，*password* 为明文验证字，长度为 1～63 个字符。

当采用 **cipher** 密文密码时，*password* 为密文验证字。如果以明文形式输入，长度为 1～63 个字符，如：1234567；如果以密文形式输入，长度必须为 24、64 或 88，并且必须是密文形式，如：_(TT8F]Y\5SQ=^Q`MAF4<1!!。

【描述】

password 命令用来设置本地用户的密码，**undo password** 命令用来取消本地用户的密码。

需要注意的是，当采用 **local-user password-display-mode cipher-force** 命令后，即使用户通过 **password** 命令指定密码显示方式为明文显示（即 **simple** 方式）后，也不起作用。

相关配置可参考命令 **display local-user**。

【举例】

设置名称为 myuser 的用户采用明文加密方式，密码为 20030422。

```
[H3C-luser-myuser] password simple 20030422
```

1.1.16 scheme

【命令】

scheme { **radius-scheme** *radius-scheme-name* [**local**] | **hwtacacs-scheme** *hwtacacs-scheme-name* [**local**] | **local** | **none** }

undo scheme [**radius-scheme** | **hwtacacs-scheme** | **none**]

【视图】

ISP 域视图

【参数】

radius-scheme-name：RADIUS 方案名，为不超过 32 个字符的字符串。

hwtacacs-scheme-name：HWTACACS 方案名，为不超过 32 个字符的字符串。

local：本地认证。

none：不进行认证。

【描述】

scheme 命令用来配置当前 ISP 域使用的 AAA 方案。**undo scheme** 命令用来恢复域缺省的 AAA 方案。

系统缺省使用的 AAA 方案为 **local**。

scheme 命令为当前 ISP 域指定引用的 RADIUS/HWTACACS 方案。所指定引用的 RADIUS/HWTACACS 方案必须是已经设置好的。

如果配置了 **radius-scheme** *radius-scheme-name* **local** 或 **hwtacacs-scheme** *hwtacacs-scheme-name* **local**，则 **local** 为 **radius server** 或 **tacacs server** 没有正常响应后的备选认证方案。即当 RADIUS 服务器或 TACACS 服务器有效时，不使用本地认证；当 RADIUS 服务器或 TACACS 服务器无效时，使用本地认证。

如果 **local** 作为第一方案，那么只能采用本地认证，不能再同时采用 RADIUS 或 HWTACACS 方案。

如果 **none** 作为第一方案，那么将不采用认证，且不能再同时采用 RADIUS 或 HWTACACS 方案。

当对 FTP 用户进行验证时，不能使用 none 认证，因为 Comware 实现的 FTP 服务器不支持匿名用户登录。

如果配置 **scheme none**，则用户登录到系统后所拥有的级别为 level 0。

相关配置可参考命令 **radius scheme**，**hwtacacs scheme**。

【举例】

指定当前 ISP 域“mydomain.net”引用的 RADIUS 方案为“rd”。

```
[H3C-isp-mydomain.net] scheme radius rd
```

设置 ISP 域 mydomain 引用的方案为 RADIUS 方案“rd”，并采用 local 作为备选认证方案。

```
[H3C-isp-mydomain] scheme radius-scheme rd local
```

设置 ISP 域 mydomain 引用的方案为 HWTACACS 方案“hwtac”，并采用 local 作为备选认证方案。

```
[H3C-isp-mydomain] scheme hwtacacs-scheme hwtac local
```

1.1.17 service-type

【命令】

service-type { **telnet** | **ssh** | **terminal** }* [**level** *level*]

undo service-type { **telnet** | **ssh** | **terminal** }*

【视图】

本地用户视图

【参数】

telnet：授权用户可以使用 Telnet 服务。

ssh：授权用户可以使用 SSH 服务。

terminal：授权用户可以使用 terminal 服务（即从 Console 口、AUX 口登录）。

level *level*：指定用户的优先级。*level* 为整数，取值范围 0～3。

【描述】

service-type 命令用来设置用户可以使用的服务类型，**undo service-type** 命令用来删除用户可以使用的服务类型。

缺省情况下，系统不对用户授权任何服务。

相关配置可参考命令 **service-type ppp**，**service-type ftp**，**service-type dvpn**。

【举例】

设置用户可以使用 Telnet 服务。

```
[H3C-luser-myuser] service-type telnet
```

1.1.18 service-type dvpn

【命令】

service-type dvpn

undo service-type dvpn

【视图】

本地用户视图

【参数】

无

【描述】

service-type dvpn 命令用来授权用户可以使用 DVPN 服务，**undo service-type dvpn** 命令用来取消用户可以使用 DVPN 服务。

缺省情况下，用户未被授权使用 DVPN 服务。

【举例】

授权用户可以使用 DVPN 服务。

```
[H3C-luser-myuser] service-type dvpn
```

1.1.19 service-type ftp

【命令】

service-type ftp [**ftp-directory** *directory*]

undo service-type ftp [**ftp-directory**]

【视图】

本地用户视图

【参数】

ftp-directory *directory*：授权 FTP 用户可以访问的目录。

【描述】

service-type ftp 命令用来授权用户可以使用 FTP 服务和 FTP 用户可以访问的目录，**undo service-type ftp** 命令用来取消用户可以使用 FTP 服务和恢复对 FTP 用

户授权的缺省目录。

缺省情况下，系统不对用户授权任何服务；若授权 FTP 服务，缺省授权使用根目录 flash:/。缺省情况下，系统不支持 FTP 匿名用户访问。

【举例】

授权用户可以使用 FTP。

```
[H3C-luser-myuser] service-type ftp
```

1.1.20 service-type ppp

【命令】

service-type ppp

undo service-type ppp

【视图】

本地用户视图

【参数】

无

【描述】

service-type 命令用来授权用户可以使用 PPP 服务，**undo service-type** 命令用来取消用户可以使用 PPP 服务。

缺省情况下，系统不对用户授权任何服务。

【举例】

设置用户可以使用 PPP 服务。

```
[H3C-luser-pppuser] service-type ppp
```

1.1.21 state

【命令】

state { **active** | **block** }

【视图】

ISP 域视图，本地用户视图

【参数】

active：指定当前 ISP 域（ISP 域视图）/当前本地用户（本地用户视图）处于“活动”状态，即系统允许该域下的用户（ISP 域视图）/当前本地用户（本地用户视图）

请求网络服务。

block：指定当前 ISP 域（ISP 域视图）/当前本地用户（本地用户视图）处于“挂起”状态，即系统不允许该域下的用户（ISP 域视图）/当前本地用户（本地用户视图）请求网络服务。

【描述】

state 命令用来设置当前 ISP 域/当前本地用户的状态。

缺省情况下，当一个 ISP 域被创建以后，其状态为 **active**（ISP 域视图）。

当一个本地用户被创建以后，其状态为 **active**（本地用户视图）。

在 ISP 域视图下，每个 ISP 域有两个状态：active 或 block。当指示某个 ISP 域处于 active 状态时，允许该域下的用户请求网络服务；当指示某个 ISP 域处于 block 状态时，不允许该域下的用户请求网络服务，但是不影响已经在线的用户。本地用户视图下同理。

相关配置可参考命令 **domain**。

【举例】

设置当前 ISP 域“mydomain.net”处于“挂起”状态，其下的接入用户不能再请求网络服务。

```
[H3C-isp-mydomain.net] state block
```

设置用户 myuser 处于“挂起”状态。

```
[H3C-user-myuser] state block
```

1.1.22 super authentication-mode

【命令】

super authentication-mode { **super-password** | **scheme** }*

undo super authentication-mode

【视图】

用户界面视图

【参数】

super-password：采用 super-password 进行认证。

scheme：采用用户配置方案进行认证。

【描述】

super authentication-mode 命令用来配置 super 认证方式，**undo super authentication-mode** 命令用来恢复 super 认证方式为缺省值。

缺省情况下，采用 super-password 认证。

【举例】

配置 console 用户采用 scheme 认证方式。

```
<H3C> system-view
[H3C] user-interface console 0
[H3C-ui-con0] super authentication-mode scheme
```

1.2 RADIUS 协议配置命令

1.2.1 accounting optional

【命令】

accounting optional

undo accounting optional

【视图】

RADIUS 域视图

【参数】

无

【描述】

accounting optional 命令用来打开计费可选开关，**undo accounting optional** 命令用来关闭计费可选开关。

系统缺省为关闭计费可选开关。

当没有可用的计费服务器或与计费服务器通信失败时，若配置了 **accounting optional** 命令，则用户可以继续使用网络资源，否则用户将被切断。这个命令经常被用于只认证不计费的情况。

【举例】

打开 RADIUS 方案“newscheme”的计费可选开关。

```
[H3C-radius-newscheme] accounting optional
```

1.2.2 data-flow-format

【命令】

data-flow-format data { **byte** | **giga-byte** | **kilo-byte** | **mega-byte** } **packet** { **giga-packet** | **kilo-packet** | **mega-packet** | **one-packet** }

undo data-flow-format

【视图】

RADIUS 视图

【参数】

data：设置数据的单位。

byte：数据单位为字节。

giga-byte：数据单位千兆字节。

kilo-byte：数据单位为千字节。

mega-byte：数据单位为兆字节。

packet：设置数据包的单位。

giga-packet：数据包的单位为“giga-packet”。

kilo-packet：数据包的单位为“kilo-packet”。

mega-packet：数据包的单位为“mega-packet”。

one-packet：数据包的单位为“one-packet”。

【描述】

data-flow-format 命令用来配置发送到 RADIUS 服务器的数据流的单位。**undo data-flow-format** 命令用来恢复发送到 RADIUS 服务器的数据流的单位为缺省设置。

缺省情况下，数据的单位为 byte，数据包的单位为 one-packet。

相关配置可参考命令 **display radius**。

【举例】

设置发往 RADIUS 服务器的数据流的单位为千字节，数据包的单位为 kilo-packet

```
[H3C-radius-myradius] data-flow-format data kilo-byte packet kilo-packet
```

1.2.3 debugging local-server

【命令】

debugging local-server { **all** | **error** | **event** | **packet** }

undo debugging local-server { **all** | **error** | **event** | **packet** }

【视图】

用户视图

【参数】

all：所有调试开关。

error：错误调试开关。

event：事件调试开关。

packet：报文调试开关。

【描述】

debugging local-server 命令用来打开本地 RADIUS 认证服务器的调试开关，**undo debugging local-server** 命令用来关闭本地 RADIUS 认证服务器的调试开关。

缺省情况下，关闭本地 RADIUS 认证服务器的调试开关。

【举例】

打开本地 RADIUS 认证服务器的调试开关

```
<H3C> debugging local-server all
*0.9045238 H3C LS/8/EVENT-MSG:Message  received. MessageType = 1
*0.9045238 H3C LS/8/PACKET:Packet Received,Code = 1
*0.9045239 H3C LS/8/PACKET:Packet Send auth pkt ,Code = 2
```

1.2.4 debugging radius

【命令】

debugging radius packet

undo debugging radius packet

【视图】

用户视图

【参数】

packet：打开报文调试开关。

【描述】

debugging radius 命令用来使能 RADIUS 协议的调试功能。**undo debugging radius** 命令用来禁止 RADIUS 协议的调试功能。

缺省情况下，禁止 RADIUS 协议的调试功能。

【举例】

使能 RADIUS 协议的报文调试功能。

```
<H3C> debugging radius packet
```

1.2.5 display local-server statistics

【命令】

display local-server statistics

【视图】

所有视图

【参数】

无

【描述】

display local-server statistics 命令用来显示本地 RADIUS 认证服务器的统计信息。

相关配置可参考命令 **local-server**。

【举例】

显示本地 RADIUS 认证服务器的统计信息。

```
<H3C> display local-server statistics
The localserver packet statistics:
Receive:                  82          Send:                     61
Discard:                  21          Receive Packet Error:     0
Auth Receive:             82          Auth Send:                61
Acct Receive:             0           Acct Send:                0
```

1.2.6 display radius scheme

【命令】

display radius scheme [*radius-scheme-name*]

【视图】

所有视图

【参数】

radius-scheme-name：RADIUS 方案名，为不超过 32 个字符的字符串。此项如果为空，则显示所有 RADIUS 方案的配置信息。

【描述】

display radius scheme 命令用来显示所有或指定 RADIUS 方案的配置信息或统计信息。

缺省情况下，显示所有 RADIUS 方案的配置信息。

相关配置可参考命令 **radius scheme**。

【举例】

显示所有 RADIUS 方案的配置信息。

```
<H3C> display radius scheme
------------------------------------------------------------------
SchemeName  = system                    Index=0    Type=extended
Primary Auth IP  =127.0.0.1        Port=1645   State=active
Primary Acct IP  =127.0.0.1        Port=1646   State=active
Second  Auth IP  =0.0.0.0          Port=1812   State=block
Second  Acct IP  =0.0.0.0          Port=1813   State=block
Auth Server Encryption Key= Not configured
Acct Server Encryption Key= Not configured
Accounting method = required
TimeOutValue(in second)=3 RetryTimes=3 RealtimeACCT(in minute)=12
Permitted send realtime PKT failed counts       =5
Retry sending times of noresponse acct-stop-PKT =500
Quiet-interval(min)                             =5
Username format                                 =without-domain
Data flow unit                                  =Byte
Packet unit                                     =One Packet

------------------------------------------------------------------
Total 1 RADIUS scheme(s). 1 listed
```

表1-4 Radius 服务器配置信息描述表

域名	描述
SchemeName	RADIUS 方案的名称
Index	RADIUS 方案的索引号
Type	RADIUS 服务器的类型
Primary Auth IP/ Port/ State	主认证服务器 IP 地址/接入端口号/该服务器目前状态
Primary Acct IP/ Port/ State	主计费服务器 IP 地址/接入端口号/该服务器目前状态
Second Auth IP/ Port/ State	备认证服务器 IP 地址/接入端口号/该服务器目前状态
Second Acct IP/ Port/ State	备计费服务器 IP 地址/接入端口号/该服务器目前状态
Auth Server Encryption Key	认证服务器的共享密钥
Acct Server Encryption Key	计费服务器的共享密钥
TimeOutValue (seconds)	RADIUS 服务器响应超时定时器时长
Permitted send realtime PKT failed counts	允许发送的实时计费请求无响应报文的最大次数

域名	描述
Retry sending times of noresponse acct-stop-PKT	缓存的停止计费请求报文的最大重发次数
Quiet-interval(min)	主服务器恢复激活状态的时间
Username format	用户名的格式
Data flow unit	数据流的单位
Packet unit	数据包的单位

1.2.7 display radius statistics

【命令】

display radius statistics

【视图】

所有视图

【参数】

无

【描述】

display radius statistics 命令用来显示 RADIUS 报文的统计信息。根据显示的信息，可以帮助诊断与排除 RADIUS 相关故障。

相关配置可参考命令 **radius scheme**。

【举例】

显示 RADIUS 报文的统计信息。

```
<H3C> display radius statistics
state statistic(total=1048):
     DEAD=1047     AuthProc=0        AuthSucc=0
AcctStart=0         RLTSend=0         RLTWait=1
 AcctStop=0          OnLine=1            Stop=0
 StateErr=0

Received and Sent packets statistic:
Sent PKT total  :38       Received PKT total:2
Resend Times     Resend total
1                12
2                12
Total            24
```

```
RADIUS received packets statistic:
Code= 2,Num=1       ,Err=0
Code= 3,Num=0       ,Err=0
Code= 5,Num=1       ,Err=0
Code=11,Num=0       ,Err=0

Running statistic:
RADIUS received messages statistic:
Normal auth request             , Num=13      , Err=0       , Succ=13
EAP auth request                , Num=0       , Err=0       , Succ=0
Account request                 , Num=1       , Err=0       , Succ=1
Account off request             , Num=0       , Err=0       , Succ=0
PKT auth timeout                , Num=36      , Err=12      , Succ=24
PKT acct_timeout                , Num=0       , Err=0       , Succ=0
Realtime Account timer          , Num=0       , Err=0       , Succ=0
PKT response                    , Num=2       , Err=0       , Succ=2
EAP reauth_request              , Num=0       , Err=0       , Succ=0
PORTAL access                   , Num=0       , Err=0       , Succ=0
Update ack                      , Num=0       , Err=0       , Succ=0
PORTAL access ack               , Num=0       , Err=0       , Succ=0
Session ctrl pkt                , Num=0       , Err=0       , Succ=0
RADIUS sent messages statistic:
Auth accept                     , Num=0
Auth reject                     , Num=0
EAP auth replying               , Num=0
Account success                 , Num=0
Account failure                 , Num=0
Cut req                         , Num=0
RecError_MSG_sum:0        SndMSG_Fail_sum :0
Timer_Err       :0        Alloc_Mem_Err   :0
State Mismatch  :0        Other_Error     :0

No-response-acct-stop packet =0
Discarded No-response-acct-stop packet for buffer overflow =0
```

表1-5 display radius statistics 显示信息描述表

域名	描述
state statistic(total=1048) DEAD=1047 AuthProc=0 AuthSucc=0 AcctStart=0 RLTSend=0 RLTWait=1 AcctStop=0 OnLine=1 Stop=0 StateErr=0	状态统计信息

域名	描述
Received and Sent packets statistic: Sent PKT total :38 Received PKT total:2 Resend Times Resend total 1 12 2 12 Total 24 RADIUS received packets statistic: Code= 2,Num=1 ,Err=0 Code= 3,Num=0 ,Err=0 Code= 5,Num=1 ,Err=0 Code=11,Num=0 ,Err=0	收发包统计信息： 共发送包数：38 共接收包数：2 重发次数： 重发包总数： 1 12 2 12 总共 24 RADIUS 接收报文统计信息： Code= 2,Num=1 ,Err=0 收到 1 个认证回应包，没有错误包 Code= 3,Num=0 ,Err=0 收到 1 个认证拒绝包，没有错误包 Code= 5,Num=1 ,Err=0 收到 1 个计费回应包，没有错误包 Code=11,Num=0 ,Err=0 收到一个 Access-Challenge（EAP 认证）包，么有错误包

域名	描述
Running statistic: RADIUS received messages statistic: Normal auth request , Num=13 , Err=0 , Succ=13 EAP auth request , Num=0 , Err=0 , Succ=0 Account request , Num=1 , Err=0 , Succ=1 Account off request , Num=0 , Err=0 , Succ=0 PKT auth timeout , Num=36 , Err=12 , Succ=24 PKT acct_timeout , Num=0 , Err=0 , Succ=0 Realtime Account timer , Num=0 , Err=0 , Succ=0 PKT response , Num=2 , Err=0 , Succ=2 EAP reauth_request , Num=0 , Err=0 , Succ=0 PORTAL access , Num=0 , Err=0 , Succ=0 Update ack , Num=0 , Err=0 , Succ=0 PORTAL access ack , Num=0 , Err=0 , Succ=0 Session ctrl pkt , Num=0 , Err=0 , Succ=0 RADIUS sent messages statistic: Auth accept , Num=0 Auth reject , Num=0 EAP auth replying , Num=0 Account success , Num=0 Account failure , Num=0 Cut req , Num=0 RecError_MSG_sum:0 SndMSG_Fail_sum :0 Timer_Err :0 Alloc_Mem_Err :0 State Mismatch :0 Other_Error :0	RADIUS 接收信息统计： 正常认证请求 数目＝13，错误＝0，成功＝0 EAP 认证请求 数目＝0，错误＝0，成功＝0 计费请求 数目＝0，错误＝0，成功＝0 计费停止请求 数目＝0，错误＝0，成功＝0 认证超时 数目＝36，错误＝0，成功＝0 计费超时 数目＝0，错误＝0，成功＝0 实时计费次数 数目＝0，错误＝0，成功＝0 回复包 数目＝2，错误＝0，成功＝2 EAP 重认证请求 数目＝0，错误＝0，成功＝0 PORTAL 接入认证请求 数目＝13，错误＝0，成功＝0 升级包 数目＝0，错误＝0，成功＝0 会话控制包 认证请求 数目＝0，错误＝0，成功＝0 RADIUS 发送信息统计 认证通过， 数目＝0 认证拒绝， 数目＝0 计费成功， 数目＝0 计费失败， 数目＝0 EAP 认证回应，数目＝0 计费成功，数目＝0 计费失败，数目＝0 删除请求，数目＝0 接收错误信息数：0 发送信息失败数：0 时间错误 ：0 分配内存错误：0 状态不匹配：0 其他错误：0

域名	描述
No-response-acct-stop packet =0	无响应的停止计费报文数为 0
Discarded No-response-acct-stop packet for buffer overflow =0	由于缓存溢出而丢弃的无响应停止计费报文数为 0

1.2.8 display stop-accounting-buffer

【命令】

display stop-accounting-buffer { **radius-scheme** *radius-scheme-name* | **session-id** *session-id* | **time-range** *start-time stop-time* | **user-name** *user-name* }

【视图】

所有视图

【参数】

radius-scheme *radius-scheme-name*：根据 RADIUS 方案名显示暂存的停止计费请求报文。其中，*radius-scheme-name* 为 RADIUS 方案名，为不超过 32 个字符的字符串，且不能包括“/”、“:”、“*”、“?”、“<”以及“>”等字符。

session-id *session-id*：根据会话 ID 显示暂存的停止计费请求报文。其中，*session-id* 为会话 ID，为不超过 50 个字符的字符串。

time-range *start-time stop-time*：根据停止计费请求时刻显示暂存的停止计费请求报文。其中，*start-time* 为请求时间段的起始时间；*stop-time* 为请求时间段的结束时间，格式为 hh:mm:ss-mm/dd/yyyy（时:分:秒-月/日/年）或 hh:mm:ss-yyyy/mm/dd（时:分:秒-年/月/日）。

user-name *user-name*：根据用户名显示暂存的停止计费请求报文。

【描述】

display stop-accounting-buffer 命令用来显示缓存在防火墙系统中的停止计费请求报文。可以选择显示发往某个 RADIUS 方案的报文；也可以根据用户会话的 session-id 或用户名来显示报文；还可以指定一个时间段，显示那些发起停止计费请求的时刻处于指定时间段内的报文。根据显示的报文信息，可以帮助诊断与排除 RADIUS 相关故障。

在发送停止计费请求报文而 RADIUS 服务器没有响应时，系统会缓存该报文，然后以一定的次数重新发送，具体发送的次数由 **retry stop-accounting** 命令设置。

相关配置可参考命令 **reset stop-accounting-buffer**，**stop-accounting-buffer enable**， **retry stop-accounting**。

【举例】

显示从 2002 年 8 月 31 日 0 点 0 分 0 秒到 2002 年 8 月 31 日 23 点 59 分 59 秒期间内系统缓存的停止计费请求报文。

```
<H3C> display stop-accounting-buffer time-range 0:0:0-08/31/2002
23:59:59-08/31/2002
Total find 0 record
```

1.2.9 key

【命令】

key { **accounting** | **authentication** } *string*

undo key { **accounting** | **authentication** }

【视图】

RADIUS 视图

【参数】

accounting：设置/删除 RADIUS 计费报文的共享密钥。

authentication：设置/删除 RADIUS 认证/授权报文的共享密钥。

string：密钥。为不超过 16 个字符的字符串。

【描述】

key 命令用来设置 RADIUS 认证/授权或计费报文的共享密钥，**undo key** 命令用来恢复相应的共享密钥为缺省设置。

RADIUS 客户端（即防火墙）与 RADIUS 服务器使用 MD5 算法来加密交互的 RADIUS 报文，双方通过设置共享密钥来验证报文的合法性。只有在密钥一致的情况下，双方才能彼此接收对方发来的报文并作出响应。因此，必须保证：防火墙上设置的共享密钥与 RADIUS 服务器上的完全一样。在认证/授权服务器与计费服务器不相同且这两台服务器中的共享密钥也不同时，必须分别设置认证/授权报文和计费报文的共享密钥。

缺省情况下，认证/授权报文和计费报文均未配置密钥。

相关配置可参考命令 **primary accounting**，**primary authentication**，**radius scheme**。

【举例】

将 RADIUS 方案“myradius”的认证/授权报文的共享密钥设置为“hello”。

```
[H3C-radius-myradius] key authentication hello
```

将 RADIUS 方案“myradius”的计费报文的共享密钥设置为“ok”。

```
[H3C-radius-myradius] key accounting ok
```

1.2.10 local-server

【命令】

local-server nas-ip *ip-address* **key** *password*

undo local-server nas-ip *ip-address*

【视图】

系统视图

【参数】

nas-ip *ip-address*：设置接入服务器的 NAS-IP 地址，地址采用点分十进制格式。

key *password*：设置本地服务器的共享密钥，*password* 为密钥，为不超过 16 个字符的字符串。

【描述】

local-server 命令用来设置本地 RADIUS 认证服务器的相关参数，**undo local-server** 命令用来删除设置的本地 RADIUS 认证服务器。

缺省情况下，系统创建了一个 NAS-IP 为 127.0.0.1、无缺省密钥的本地 RADIUS 认证服务器。

需要注意以下几点：

- 设备除了支持传统的作为 RADIUS 客户端的服务——即分别采用认证/授权服务器、计费服务器的方式进行用户的认证管理外，还提供了本地简单 RADIUS 服务器端功能（包括认证和授权），称之为本地 RADIUS 认证服务器功能。
- 采用本地 RADIUS 认证服务器功能时，其认证/授权服务的 UDP 端口号必须为 1645，计费服务的 UDP 端口号为 1646。
- 用此命令配置的报文加密密钥（key password）必须和在 RADIUS 方案视图下用命令 key authentication 配置的认证/授权报文加密密钥一致。
- 包括系统缺省创建的本地 RADIUS 认证服务器在内，设备最多支持 16 个本地 RADIUS 认证服务器。

相关配置可参考命令 **radius scheme**，**state**。

【举例】

设置本地 RADIUS 认证服务器的 IP 地址为 10.110.1.2、登录密码为 aabbcc。

```
[H3C] local-server nas-ip 10.110.1.2 key aabbcc
```

1.2.11 nas-ip

【命令】

nas-ip *ip-address*

undo nas-ip

【视图】

RADIUS 视图

【参数】

ip-address：IP 地址，点分十进制形式。

【描述】

nas-ip 命令用来设置 NAS（防火墙）发送 RADIUS 报文使用的源 IP 地址，这样发送到 RADIUS 服务器的所有报文携带相同的源 IP 地址。**undo nas-ip** 命令用来删除配置。

指定发送 RADIUS 报文使用的源地址，可以避免物理接口故障时从服务器返回的报文不可达。一般推荐使用 loopback 接口地址。

缺省情况下，报文的源 IP 地址是发送端口的 IP 地址。

相关配置可参考命令 **radius nas-ip**。

【举例】

配置 NAS（防火墙）发送 RADIUS 报文使用的源 IP 地址为 10.1.1.1。

```
[H3C] radius scheme test1
[H3C-radius-test1] nas-ip 10.1.1.1
```

1.2.12 primary accounting

【命令】

primary accounting *ip-address* [*port-number*]

undo primary accounting

【视图】

RADIUS 视图

【参数】

ip-address：IP 地址，为点分十进制格式。缺省情况下，在 system 方案中，主计费服务器的 IP 地址为 127.0.0.1，新创建的 RADIUS 方案中的主计费服务器的 IP 地址均为 0.0.0.0。

port-number：UDP 端口号。取值范围为 1～65535。缺省情况下，在 system 方案中，主计费服务的 UDP 端口号为 1646，新创建的 RADIUS 方案中的主计费服务的 UDP 端口号为 1813。

【描述】

primary accounting 命令用来设置主 RADIUS 计费服务器的 IP 地址和端口号，**undo primary accounting** 命令用来将主 RADIUS 计费服务器的 IP 地址和端口号恢复为缺省值。

当创建一个新的 RADIUS 方案之后，需要对属于此方案的 RADIUS 服务器的 IP 地址和 UDP 端口号进行设置，这些服务器包括认证/授权和计费服务器，而每种服务器又有主服务器和备服务器的区别。在实际组网环境中，上述参数的设置需要根据具体需求来决定。但是必须至少设置一个认证/授权服务器和一个计费服务器。同时在配置过程中，请保证防火墙上的 RADIUS 服务端口设置与 RADIUS 服务器上的端口设置保持一致。

在计费成功后，计费更新以及计费停止报文都会发往计费成功时使用的服务器上，即使此服务器不可用，也不会发生主备切换。只有在最开始的认证、授权、计费过程中才会发生切换，成功后将不再切换。

相关配置可参考命令 **key**，**radius scheme**，**state**。

【举例】

设置 RADIUS 方案“myradius”的主计费服务器的 IP 地址为 10.110.1.2，使用 UDP 端口 1813 提供 RADIUS 计费服务。

```
[H3C-radius-myradius] primary accounting 10.110.1.2 1813
```

1.2.13 primary authentication

【命令】

primary authentication *ip-address* [*port-number*]

undo primary authentication

【视图】

RADIUS 视图

【参数】

ip-address：IP 地址，为点分十进制格式。缺省情况下，在 system 方案中，主认证/授权服务器的 IP 地址为 127.0.0.1，新创建的 RADIUS 方案中的主认证/授权服务器的 IP 地址均为 0.0.0.0。

port-number：UDP 端口号。取值范围为 1～65535。缺省情况下，在 system 方案中，主认证/授权服务的 UDP 端口号为 1645，新创建的 RADIUS 方案中的主认证/授权服务的 UDP 端口号为 1812。

【描述】

primary authentication 命令用来设置主 RADIUS 认证/授权的 IP 地址和端口号，**undo primary authentication** 命令用来将主 RADIUS 认证/授权的 IP 地址和端口号恢复为缺省值。

当创建一个新的 RADIUS 方案之后，需要对属于此方案的 RADIUS 服务器的 IP 地址和 UDP 端口号进行设置，这些服务器包括认证/授权和计费服务器，而每种服务器又有主服务器和备服务器的区别。 在实际组网环境中，上述参数的设置需要根据具体需求来决定。但是必须至少设置一个认证/授权服务器和一个计费服务器。同时在配置过程中，请保证防火墙上的 RADIUS 服务端口设置与 RADIUS 服务器上的端口设置保持一致。

相关配置可参考命令 **key**，**radius scheme**，**state**。

【举例】

设置 RADIUS 方案“myradius”的主认证/授权服务器的 IP 地址为 10.110.1.1，使用 UDP 端口 1812 提供 RADIUS 认证/授权服务。

```
[H3C-radius-myradius] primary authentication 10.110.1.1 1812
```

1.2.14 radius scheme

【命令】

radius scheme *radius-scheme-name*

undo radius scheme *radius-scheme-name*

【视图】

系统视图

【参数】

radius-scheme-name：RADIUS 方案名，为不超过 32 个字符的字符串。

【描述】

radius scheme 命令用来创建 RADIUS 方案并进入其视图，**undo radius scheme** 命令用来删除指定的 RADIUS 方案。

缺省情况下，系统中已创建了一个名为“system”的 RADIUS 方案，其各项属性均为缺省值，该方案不可以修改。可以用 **display radius** 命令来查看缺省 RADIUS 方案 system 的设置。

RADIUS 协议的配置是以 RADIUS 方案为单位进行的。每个 RADIUS 方案至少须指明 RADIUS 认证/授权/计费服务器的 IP 地址、UDP 端口号以及 RADIUS 客户端（防火墙）与之交互所需的一些参数。因此，在进行其它 RADIUS 协议配置之前，必须先创建 RADIUS 方案并进入其视图。

一个 RADIUS 方案可以同时被多个 ISP 域引用。

undo radius scheme 命令虽然可以用来删除指定的 RADIUS 方案，但是不能删除缺省的 RADIUS 方案。注意：当有使用 RADIUS 方案的用户在线时不允许删除。

相关配置可参考命令 **key**，**retry realtime-accounting**，**scheme**，**timer realtime-accounting**，**stop-accounting-buffer enable**，**retry stop-accounting**，**server-type**，**state**，**user-name-format**，**retry**，**display radius**，**display radius statistics**。

【举例】

创建名为“myradius”的 RADIUS 方案并进入其视图。

```
[H3C] radius scheme myradius
[H3C-radius-myradius]
```

1.2.15 radius nas-ip

【命令】

radius nas-ip *ip-address*

undo radius nas-ip

【视图】

系统视图

【参数】

ip-address：指定的源 IP 地址，应该为本机的地址，禁止配置全 0 地址、D 类地址、以及 127 网段地址。

【描述】

radius nas-ip 命令用来指定 NAS 发送 RADIUS 报文使用的源地址。**undo radius nas-ip** 命令用来恢复缺省状态。

指定发送 RADIUS 报文使用的源地址，可以避免物理接口故障时从服务器返回的报文不可达。一般推荐使用 loopback 接口地址。

缺省情况下，不指定源地址，即以发送报文的接口地址作为源地址。

本命令只能指定一个源地址，新配置的源地址会覆盖原有的源地址。

相关配置可参考命令 **nas-ip**。

【举例】

配置防火墙发送 RADIUS 报文使用的源地址为 129.10.10.1。

```
[H3C] radius nas-ip 129.10.10.1
```

1.2.16 radius trap

【命令】

radius trap { **authentication-server-down** | **accounting-server-down** }

undo radius trap { **authentication-server-down** | **accounting-server-down** }

【视图】

系统视图

【参数】

authentication-server-down：RADIUS 认证服务器状态变为 down；

accounting-server-down：RADIUS 计费服务器状态变为 down。

【描述】

radius trap 命令用来使能 RADIUS 服务器状态变为 down 时发送 trap 报文的功能，**undo radius trap** 用来关闭 RADIUS 服务器状态变为 down 时发送 trap 报文的功能。

缺省情况下，关闭该功能。

【举例】

使能 RADIUS 认证服务器状态变为 down 时发送 trap 报文的功能。

```
[H3C] radius trap authentication-server-down
```

1.2.17 reset radius statistics

【命令】

reset radius statistics

【视图】

用户视图

【参数】

无

【描述】

reset radius statistics 命令用来清除 RADIUS 协议的统计信息。

相关配置请参考命令 **display radius**。

【举例】

清除 RADIUS 协议的统计信息。

```
<H3C> reset radius statistics
```

1.2.18 reset stop-accounting-buffer

【命令】

reset stop-accounting-buffer { **radius-scheme** *radius-scheme-name* | **session-id** *session-id* | **time-range** *start-time stop-time* | **user-name** *user-name* }

【视图】

用户视图

【参数】

radius-scheme *radius-scheme-name*：根据 RADIUS 方案名删除暂存的停止计费请求报文。其中，*radius-scheme-name* 为 RADIUS 方案名，为不超过 32 个字符的字符串。

session-id *session-id*：根据会话 ID 删除暂存的停止计费请求报文。其中，*session-id* 为会话 ID，为不超过 50 个字符的字符串。

time-range *start-time stop-time*：根据停止计费请求时刻删除暂存的停止计费请求报文。其中，*start-time* 为请求时间段的起始时间；*stop-time* 为请求时间段的结束时间，格式为 *hh:mm:ss-mm/dd/yyyy*（时:分:秒-月/日/年）或 *hh:mm:ss-yyyy/mm/dd*（时:分:秒-年/月/日）。

user-name *user-name*：根据用户名删除暂存的停止计费请求报文。

【描述】

reset stop-accounting-buffer 命令用来删除那些缓存的、没有得到响应的停止计费请求报文。在发送停止计费请求报文而 RADIUS 服务器没有响应时，防火墙系统会缓存该报文，然后以一定的次数重新发送，具体发送的次数由 **retry stop-accounting** 命令设置。

可以选择删除某个 RADIUS 方案的报文；也可以根据用户会话的 session-id 或用户名来删除报文；还可以指定一个时间段，删除那些发起停止计费请求的时刻处于指定时间段内的报文。

相关配置可参考命令 **stop-accounting-buffer enable,retry stop-accounting**，**display stop-accounting-buffer**。

【举例】

删除用户“user0001@mydomain.net”缓存在系统中的停止计费请求报文。

```
<H3C> reset stop-accounting-buffer user-name user0001@mydomain.net
```

删除从 2002 年 8 月 31 日 0 点 0 分 0 秒到 2002 年 8 月 31 日 23 点 59 分 59 秒期间内系统缓存的停止计费请求报文。

```
<H3C> reset stop-accounting-buffer time-range 0:0:0-08/31/2002
23:59:59-08/31/2002
```

1.2.19 retry

【命令】

retry *retry-times*

undo retry

【视图】

RADIUS 视图

【参数】

retry-times：最大传送次数，取值范围为 1～20。缺省情况下，RADIUS 请求报文的最大传送次数为 3 次。

【描述】

retry 命令用来设置 RAIUDS 请求报文的最大传送次数，**undo retry** 命令用来将 RAIUDS 请求报文的最大传送次数恢复为缺省值。

由于 RADIUS 协议采用 UDP 报文来承载数据，因此其通信过程是不可靠的。如果 RADIUS 服务器在响应超时定时器规定的时长内没有响应 NAS，则 NAS 有必要向 RADIUS 服务器重传 RADIUS 请求报文。假设最大传送次数为 N，则如果累计的传送次数超过（N-[N/2]）次而主 RADIUS 服务器仍旧没有响应，则 NAS 将认为其与当前 RADIUS 服务器的通信已经中断，并将转而向其它的 RADIUS 服务器发送请求报文。

根据网络状况合理的设置重发次数可以提高系统的响应速度。

相关配置可参考命令 **radius scheme**。

【举例】

设置在 RADIUS 方案“myradius”下，RAIUDS 请求报文的最大传送次数为 5 次。

```
[H3C-radius-myradius] retry 5
```

1.2.20 retry realtime-accounting

【命令】

retry realtime-accounting *retry-times*

undo retry realtime-accounting

【视图】

RADIUS 视图

【参数】

retry-times：允许实时计费请求无响应的最大次数，取值范围为 1～255。缺省情况下，最多允许 5 次实时计费请求无响应。

【描述】

retry realtime-accounting 命令用来设置允许实时计费请求无响应的最大次数。**undo retry realtime-accounting** 命令用来恢复允许实时计费请求无响应的最大次数为缺省值。

RADIUS 服务器通常通过连接超时定时器来判断用户是否在线。如果 RADIUS 服务器长时间收不到 NAS 传来的实时计费报文，它会认为线路或设备故障并停止对用户记帐。为了配合 RADIUS 服务器的这种特性，有必要在不可预见的故障条件下在 NAS 端尽量与 RADIUS 服务器同步切断用户连接。防火墙提供对连续实时计费请求无响应次数限制的设置——在 NAS 向 RADIUS 服务器发出的实时计费请求没有得到响应的次数超过所设定的限度时，NAS 将切断用户连接。

假设 RADIUS 服务器的应答超时时长为 T（假设定义为 3 秒），NAS 的实时计费间隔为 t（假设定义为 12 分钟），则 NAS 的实时计费请求无响应的最大次数为 *retry-times*（假设定义为 5 次），则其含义为：NAS 每隔 12 分钟发起一次记费请求，如果 3 秒钟得不到回应就重新发起一次请求，如果 5 次发送都没有回应就认为该次实时记费失败。一般情况下，T 乘以 *retry-times* 应该小于 t。

相关配置可参考命令 **radius scheme**，**timer realtime-accounting**。

【举例】

设置 RADIUS 方案“myradius”最多允许 10 次实时计费请求无响应。

```
[H3C-radius-myradius] retry realtime-accounting 10
```

1.2.21 retry stop-accounting

【命令】

retry stop-accounting *retry-times*

undo retry stop-accounting

【视图】

RADIUS 视图

【参数】

retry-times：缓存的停止计费请求报文的最大重发次数，取值范围为 10～65535。缺省情况下，取值为 500。

【描述】

retry stop-accounting 命令用来指示当出现没有得到响应的停止计费请求时，将该报文存入防火墙缓存后，停止计费请求报文的最大重发次数。**undo retry stop-accounting** 命令用来恢复停止计费请求报文的最大重发次数为缺省值。

由于停止计费请求报文涉及到话单结算，并最终影响收费多少，对用户和 ISP 都有比较重要的影响，因此 NAS 应该尽最大努力把它发送给 RADIUS 计费服务器。所以，如果 RADIUS 计费服务器对防火墙发出的停止计费请求报文没有响应，防火墙应将其缓存在本机上，然后重新发送直到 RADIUS 计费服务器产生响应，或者在重新发送的次数达到指定的次数限制后将其丢弃。

相关配置可参考命令 **reset stop-accounting-buffer**，**radius scheme**，**display stop-accounting-buffer**。

【举例】

指示对于 RADIUS 方案“myradius”中的服务器，防火墙系统最多可以将缓存的停止计费请求报文重发 1000 次。

```
[H3C-radius-myradius] retry stop-accounting 1000
```

1.2.22 secondary accounting

【命令】

secondary accounting *ip-address* [*port-number*]

undo secondary accounting

【视图】

RADIUS 视图

【参数】

ip-address：IP 地址，为点分十进制格式。缺省情况下，备计费服务器的 IP 地址均为 0.0.0.0。

port-number：UDP 端口号。取值范围为 1～65535。缺省情况下，计费服务的 UDP 端口号为 1813。

【描述】

secondary accounting 命令用来设置备 RADIUS 计费服务器的 IP 地址和端口号，**undo secondary accounting** 命令用来将备 RADIUS 计费服务器的 IP 地址和端口号恢复为缺省值。

具体的描述请参见 **primary accounting** 命令的描述部分。

相关配置可参考命令 **key**，**radius scheme**，**state**。

【举例】

设置 RADIUS 方案“myradius”的备计费服务器的 IP 地址为 10.110.1.1、使用 UDP 端口 1813 提供 RADIUS 计费服务。

```
[H3C-radius-myradius] secondary accounting 10.110.1.1 1813
```

1.2.23 secondary authentication

【命令】

secondary authentication *ip-address* [*port-number*]

undo secondary authentication

【视图】

RADIUS 视图

【参数】

ip-address：IP 地址，为点分十进制格式。缺省情况下，备认证/授权的 IP 地址均为 0.0.0.0。

port-number：UDP 端口号。取值范围为 1～65535。缺省情况下，认证/授权服务的 UDP 端口号为 1812。

【描述】

secondary authentication 命令用来设置备 RADIUS 认证/授权或计费服务器的 IP 地址和端口号，**undo secondary authentication** 命令用来将备 RADIUS 认证/授权或计费服务器的 IP 地址和端口号恢复为缺省值。

具体的描述请参见 **primary authentication** 命令的描述部分。

相关配置可参考命令 **key**，**radius scheme**，**state**。

【举例】

设置 RADIUS 方案“myradius”的备认证/授权服务器的 IP 地址为 10.110.1.2、使用 UDP 端口 1812 提供 RADIUS 认证/授权服务。

```
[H3C-radius-myradius] secondary authentication 10.110.1.2 1812
```

1.2.24 server-type

【命令】

server-type { **extended** | **standard** }

undo server-type

【视图】

RADIUS 视图

【参数】

extended：指定扩展类型的 RADIUS 服务器，即要求 RADIUS 客户端（防火墙）和 RADIUS 服务器按照各厂商私有 RADIUS 协议的规程和报文格式进行交互。

standard：指定 Standard 类型的 RADIUS 服务器，即要求 RADIUS 客户端（防火墙）和 RADIUS 服务器按照标准 RADIUS 协议（RFC 2138/2139 或更新）的规程和报文格式进行交互。

【描述】

server-type 命令用来指定防火墙系统支持的 RADIUS 服务器类型。**undo server-type** 命令用来恢复 RADIUS 服务器类型为 **standard**。

缺省情况下，system 方案中的 RADIUS 服务器的类型为 **extended**，新创建的 RADIUS 方案中的 RADIUS 服务器的类型为 **standard**。

相关配置可参考命令 **radius scheme**。

【举例】

将 RADIUS 方案“newscheme”的 RADIUS 服务器类型设置为 standard。

```
[H3C-radius-newscheme] server-type standard
```

1.2.25 state

【命令】

state { **primary** | **secondary** } { **accounting** | **authentication** } { **block** | **active** }

【视图】

RADIUS 视图

【参数】

primary：指示设置主 RADIUS 服务器的状态。

secondary：指示设置备 RADIUS 服务器的状态。

accounting：指示设置 RADIUS 计费服务器的状态。

authentication：指示设置 RADIUS 认证/授权服务器的状态。

block：指示 RADIUS 服务器的状态为 **block**，即处于宕机状态。

active：指示 RADIUS 服务器的状态为 **active**，即处于正常工作状态。

【描述】

state 命令用来设置 RADIUS 服务器的状态。

缺省情况下，system 方案中的主认证/授权服务器和主计费服务器的状态为 **active**，备认证/授权服务器和备计费服务器的状态为 **block**；新创建的 RADIUS 方案中各 RADIUS 服务器的状态均为 **block**。

对于某个 RADIUS 方案中的主、备服务器（无论是认证/授权服务器还是计费服务器），当主服务器因故障而导致其与 NAS 的通信中断时，NAS 会主动地转而与备服务器交互报文。当主服务器恢复正常后，NAS 却不会立即恢复与其通信，而是继续与备服务器通信；直到备服务器也出现故障后，NAS 才能再转而恢复与主服务器交互报文。为了使 NAS 在主服务器故障排除后迅速恢复与其通信，需要通过 **state** 命令手工将主服务器的状态设为 **active**。

当主服务器与备服务器的状态都为 **active** 或都为 **block** 时，NAS 将只把报文发送到主服务器上。

相关配置可参考命令 **radius scheme**，**primary authentication**，**secondary authentication**，**primary accounting**，**secondary accounting**。

【举例】

将 RADIUS 方案“myradius”的备认证服务器的状态设置为 active。

```
[H3C-radius-myradius] state secondary authenticaiton active
```

1.2.26 stop-accounting-buffer enable

【命令】

stop-accounting-buffer enable

undo stop-accounting-buffer enable

【视图】

RADIUS 视图

【参数】

无

【描述】

stop-accounting-buffer enable 命令用来允许在防火墙上缓存没有得到响应的停止计费请求报文。**undo stop-accounting-buffer enable** 命令用来禁止在防火墙上

缓存没有得到响应的停止计费请求报文。

缺省情况下，允许防火墙缓存没有得到响应的停止计费请求报文。

由于停止计费请求报文涉及到话单结算、并最终影响收费多少，对用户和 ISP 都有比较重要的影响，因此 NAS 应该尽最大努力把它发送给 RADIUS 计费服务器。所以，如果 RADIUS 计费服务器对防火墙发出的停止计费请求报文没有响应，防火墙应将其缓存在本机上，然后重新发送直到 RADIUS 计费服务器产生响应，或者在重新发送的次数达到指定的次数限制后将其丢弃。

相关配置可参考命令 **reset stop-accounting-buffer**，**radius scheme** ，**display stop-accounting-buffer**。

【举例】

指示对于 RADIUS 方案“myradius”中的服务器，防火墙系统能够缓存没有得到响应的停止计费请求报文。

```
[H3C-radius-myradius] stop-accounting-buffer enable
```

1.2.27 timer quiet

【命令】

timer quiet *minutes*

undo timer quiet

【视图】

RADIUS 视图

【参数】

minutes：取值范围为 1～255，单位为分钟。缺省情况下，主服务器恢复激活状态前需要等待 5 分钟。

【描述】

timer quiet 命令用来设置主服务器恢复激活状态的时间。**undo timer quiet** 命令用来恢复缺省配置。

相关配置可参考命令 **display radius**。

【举例】

设置主服务器恢复激活状态的时间为 10 分钟。

```
[H3C] radius scheme test1
[H3C-radius-test1] timer quiet 10
```

1.2.28 timer realtime-accounting

【命令】

timer realtime-accounting *minutes*

undo timer realtime-accounting

【视图】

RADIUS 视图

【参数】

minutes：实时计费的时间间隔，单位为分钟，取值范围为 3～60，必须为 3 的倍数。

【描述】

timer realtime-accounting 命令用来设置实时计费的时间间隔，**undo timer realtime-accounting** 命令用来将实时计费的时间间隔恢复为缺省值。

为了对用户实施实时计费，有必要设置实时计费的时间间隔。在设置了该属性以后，每隔设定的时间，NAS 会向 RADIUS 服务器发送一次在线用户的计费信息。

实时计费间隔的取值对 NAS 和 RADIUS 服务器的性能有一定的相关性要求——取值越小，对 NAS 和 RADIUS 服务器的性能要求越高。建议当用户量比较大（≥1000）时，尽量把该间隔的值设置得大一些。以下是实时计费间隔与用户量之间的推荐比例关系：

表1-6 实时计费间隔与用户量之间的推荐比例关系

用户数	实时计费间隔（分钟）
1～99	3
100～499	6
500～999	12
≥1000	≥15

缺省情况下，实时计费的时间间隔为 12 分钟。

相关配置可参考命令 **retry realtime-accounting**，**radius scheme**。

【举例】

将 RADIUS 方案“myradius”的实时计费的时间间隔设置为 51 分钟。

```
[H3C-radius-myradius] timer realtime-accounting 51
```

1.2.29 timer response-timeout

【命令】

timer *seconds*

undo timer

timer response-timeout *seconds*

undo timer response-timeout

【视图】

RADIUS 视图

【参数】

seconds：RADIUS 服务器应答超时时间，单位为秒，取值范围为 1～10。

【描述】

timer 和 **timer response-timeout** 命令用来设置 RADIUS 服务器应答超时时间，**undo timer** 和 **undo timer response-timeout** 命令用来将 RADIUS 服务器应答超时时间恢复为缺省值。

如果在 RADIUS 请求报文（认证/授权请求或计费请求）传送出去一段时间后，NAS 还没有得到 RADIUS 服务器的响应，则有必要重传 RADIUS 请求报文，以保证用户确实能够得到 RADIUS 服务，这段时间被称为 RADIUS 服务器响应超时时长，防火墙中用于控制这个时长的定时器就被称为 RADIUS 服务器响应超时定时器，**timer** 和 **timer response-timeout** 命令就是用来设置这个定时器时长的。

根据网络状况，合理地设置这个定时器的时长，有利于提高系统性能。

缺省情况下，RADIUS 服务器应答超时时间为 3 秒。

相关配置可参考命令 **radius scheme**，**retry**。

【举例】

将 RADIUS 方案“myradius”的响应超时定时器设置为 5 秒。

```
[H3C-radius-myradius] timer response-timeout 5
```

1.2.30 user-name-format

【命令】

user-name-format { **with-domain** | **without-domain** }

【视图】

RADIUS 视图

【参数】

with-domain：指定发送给 RADIUS 服务器的用户名带域名。

without-domain：指定发送给 RADIUS 服务器的用户名不带域名。

【描述】

user-name-format 命令用来设置发送给 RADIUS 服务器的用户名格式。

缺省情况下，在 system 方案中，NAS 发送给 RADIUS 服务器的用户名不携带 ISP 域名；在新创建的 RADIUS 方案中，NAS 发送给 RADIUS 服务器的用户名携带有 ISP 域名。

接入用户通常以“userid@isp-name”的格式命名，“@”后面的部分为 ISP 域名，防火墙就是通过该域名来决定将用户归于哪个 ISP 域的。但是，有些较早期的 RADIUS 服务器不能接受携带有 ISP 域名的用户名，在这种情况下，有必要将用户名中携带的域名去除后再传送给 RADIUS 服务器。因此，防火墙提供此命令以指定发送给 RADIUS 服务器的用户名是否携带有 ISP 域名。

📖 说明：

如果指定某个 RADIUS 方案不允许用户名中携带有 ISP 域名，那么请不要在两个乃至两个以上的 ISP 域中同时设置使用该 RADIUS 方案，否则，会出现虽然实际用户不同（在不同的 ISP 域中）、但 RADIUS 服务器认为用户相同（因为传送到它的用户名相同）的错误。

相关配置可参考命令 **radius scheme**。

【举例】

指定发送给 RADIUS 方案“myradius”中 RADIUS 服务器的用户名不得携带域名。

```
[H3C-radius-myradius] user-name-format without-domain
```

1.3 HWTACACS 协议配置命令

1.3.1 data-flow-format

【命令】

data-flow-format data { **byte** | **giga-byte** | **kilo-byte** | **mega-byte** }

data-flow-format packet { **giga-packet** | **kilo-packet** | **mega-packet** | **one-packet** }

undo data-flow-format { **data** | **packet** }

【视图】

HWTACACS 视图

【参数】

data：设置数据的单位。

byte：数据单位为比特。

giga-byte：数据单位千兆字节。

kilo-byte：数据单位为千字节。

mega-byte：数据单位为兆字节。

packet：设置数据包的单位。

giga-packet：数据包的单位为“giga-packet”。

kilo-packet：数据包的单位为“kilo-packet”。

mega-packet：数据包的单位为“mega-packet”。

one-packet：数据包的单位为“one-packet”。

【描述】

data-flow-format 命令用来配置发送到 TACACS 服务器的数据流的单位。**undo data-flow-format** 命令用来恢复发送到 TACACS 服务器的数据流的单位为缺省设置。

缺省情况下，数据的单位为 byte，数据包的单位为 one-packet。

相关配置可参考命令 **display hwtacacs**。

【举例】

设置发往 TACACS 服务器的数据流的单位为千字节，数据包的单位为 kilo-packet。

```
[H3C-hwtacacs-mytacacs] data-flow-format data kilo-byte
[H3C-hwtacacs-mytacacs] data-flow-format packet kilo-packet
```

1.3.2 debugging hwtacacs

【命令】

debugging hwtacacs { **all** | **error** | **event** | **message** | **receive-packet** | **send-packet** }

undo debugging hwtacacs { **all** | **error** | **event** | **message** | **receive-packet** | **send-packet** }

【视图】

用户视图

【参数】

all：HWTACACS 协议的所有调试功能。

error：错误调试功能。

event：事件调试功能。

message：消息调试功能。

receive-packet：对接收到的报文的调试功能。

send-packet：对发送报文的调试功能。

【描述】

debugging hwtacacs 命令用来使能 HWTACACS 协议的调试功能。**undo debugging hwtacacs** 命令用来禁止 HWTACACS 协议的调试功能。

缺省情况下，禁止 HWTACACS 协议的调试功能。

【举例】

使能 HWTACACS 协议的事件调试功能。

```
<H3C> debugging hwtacacs event
```

1.3.3 display hwtacacs scheme

【命令】

display hwtacacs scheme [*hwtacacs-scheme-name* [**statistics**]]

【视图】

所有视图

【参数】

hwtacacs-scheme-name：HWTACACS 方案名，字符串形式，长度为 1～32，不区分大小写。此项如果为空，则显示所有 HWTACACS 方案的配置信息。

statistics：显示 HWTACACS 报文的详细统计信息。

【描述】

display hwtacacs scheme 命令用来查看所有或指定 HWTACACS 方案的配置信息。

不带任何参数的情况下，显示所有 HWTACACS 方案的配置信息。

相关配置请参考命令 **hwtacacs scheme**。

【举例】

查看所有 HWTACACS 方案 gy 的配置情况。

```
<H3C> display hwtacacs scheme gy
-------------------------------------------------------------------------
HWTACACS-server template name   : gy
  Primary-authentication-server   : 172.31.1.11:49
  Primary-authorization-server    : 172.31.1.11:49
  Primary-accounting-server       : 172.31.1.11:49
  Secondary-authentication-server : 0.0.0.0:0
  Secondary-authorization-server  : 0.0.0.0:0
  Secondary-accounting-server     : 0.0.0.0:0
  Current-authentication-server   : 172.31.1.11:49
  Current-authorization-server    : 172.31.1.11:49
  Current-accounting-server       : 172.31.1.11:49
  Source-IP-address               : 0.0.0.0
  key authentication              : 790131
  key authorization               : 790131
  key accounting                  : 790131
  Quiet-interval(min)             : 5
  Response-timeout-Interval(sec)  : 5
  Domain-included                 : No
  Traffic-unit                    : B
  Packet traffic-unit             : one-packet
```

表1-7 display hwtacacs scheme 显示信息描述表

域名	描述
HWTACACS-server template name	HWTACACS 服务器组名（即 HWTACACS 方案名）
Primary-authentication-server	主认证服务器 IP 地址及端口号
Primary-authorization-server	主授权服务器 IP 地址及端口号
Primary-accounting-server	主计费服务器 IP 地址及端口号
Secondary-authentication-server	备认证服务器 IP 地址及端口号
Secondary-authorization-server	备授权服务器 IP 地址及端口号
Secondary-accounting-server	备计费服务器 IP 地址及端口号
Current-authentication-server	当前认证服务器 IP 地址及端口号
Current-authorization-server	当前授权服务器 IP 地址及端口号
Current-accounting-server	当前计费服务器 IP 地址及端口号
Source-IP-address	路由器发送 HWTACACS 报文使用的源 IP 地址
key authentication	HWTACACS 认证服务器共享密钥
key authorization	HWTACACS 授权服务器共享密钥
key accounting	HWTACACS 计费服务器共享密钥

域名	描述
Quiet-interval(min)	主服务器恢复激活状态的等待时间
Response-timeout-Interval(sec)	TACACS 服务器应答超时时间
Domain-included	发送给 TACACS 服务器的用户名为含域名的格式
Traffic-unit	流量单位： B：数据单位为字节。 GB：数据单位千兆字节。 KB：数据单位为千字节。 MB：数据单位为兆字节。
Packet traffic-unit	数据包的单位： **giga-packet**：数据包的单位为千兆“giga-packet”。 **kilo-packet**：数据包的单位为千“kilo-packet”。 **mega-packet**：数据包的单位为兆“mega -packet”。 **one-packet**：数据包的单位为 1 包“one -packet”。

1.3.4 display stop-accounting-buffer

【命令】

display stop-accounting-buffer hwtacacs-scheme *hwtacacs-scheme-name*

【视图】

所有视图

【参数】

hwtacacs-scheme *hwtacacs-scheme-name*：根据 HWTACACS 方案名显示暂存的停止计费请求报文。其中，*hwtacacs-scheme-name* 为 HWTACACS 方案名，为不超过 32 个字符的字符串。

【描述】

display stop-accounting-buffer 命令用来显示缓存在防火墙上的停止计费请求报文。

相关配置可参考命令 **reset stop-accounting-buffer**，**stop-accounting-buffer enable**，**retry stop-accounting**。

【举例】

显示为 HWTACACS 方案“mytacacs”缓存的停止计费请求报文。

```
<H3C> display stop-accounting-buffer hwtacacs-scheme mytacacs
------------------------------------------------------------
NO. SendTime      IP Address                          Template
```

```
  1       10     172.31.1.27                              h3c
------------------------------------------------------------
Whole accounting stop packet to resend:1
```

表1-8 display stop-accounting-buffer 显示信息描述表

域名	描述
NO.	停止计费请求报文的序号
SendTime	停止计费报文已发送次数
IP Address	TACACS 服务器 IP 地址
Template	hwtacacs 认证方案名

1.3.5 hwtacacs nas-ip

【命令】

hwtacacs nas-ip *ip-address*

undo hwtacacs nas-ip

【视图】

系统视图

【参数】

ip-address：指定的源 IP 地址，应该为本机的地址，禁止配置全 0 地址、D 类地址、以及 127 网段地址。

【描述】

hwtacacs nas-ip 命令用来指定 NAS 发送 HWTACACS 报文使用的源地址。**undo hwtacacs nas-ip** 命令用来恢复缺省状态。

指定发送 HWTACACS 报文使用的源地址，可以避免物理接口故障时从服务器返回的报文不可达。一般推荐使用 loopback 接口地址。

缺省情况下，不指定源地址，即以发送报文的接口地址作为源地址。

本命令只能指定一个源地址，新配置的源地址会覆盖原有的源地址。

【举例】

配置防火墙发送 HWTACACS 报文使用的源地址为 129.10.10.1。

```
[H3C] hwtacacs nas-ip 129.10.10.1
```

1.3.6 hwtacacs scheme

【命令】

hwtacacs scheme *hwtacacs-scheme-name*

undo hwtacacs scheme *hwtacacs-scheme-name*

【视图】

系统视图

【参数】

hwtacacs-scheme-name：HWTACACS 方案名称，字符串形式，长度为 1～32。

【描述】

hwtacacs scheme 命令用来进入 HWTACACS 视图，如果指定的 HWTACACS 方案名不存在，则同时创建一个新的 HWTACACS 方案。**undo hwtacacs scheme** 命令用来删除一个 HWTACACS 方案。

【举例】

创建名为 test1 的 HWTACACS 方案并进入相应的 HWTACACS 方案视图。

```
[H3C] hwtacacs scheme test1
[H3C-hwtacacs-test1]
```

1.3.7 key

【命令】

key { **accounting** | **authentication** | **authorzation** } *string*

undo key { **accounting** | **authentication** | **authorzation** }

【视图】

HWTACACS 视图

【参数】

accounting：计费服务器的共享密钥。

authentication：认证服务器的共享密钥。

authorzation：授权服务器的共享密钥。

string：密钥。为不超过 16 个字符的字符串。

【描述】

key 命令用来设置 HWTACACS 认证、授权、计费服务器的共享密钥。**undo key** 命令用来删除配置。

缺省情况下，TACACS 服务器没有密钥。

TACACS 客户端（即防火墙）与 TACACS 服务器使用 MD5 算法来加密交互的 HWTACACS 报文，双方通过设置共享密钥来验证报文的合法性。只有在密钥一致的情况下，双方才能彼此接收对方发来的报文并作出响应。因此，必须保证防火墙上设置的共享密钥与 TACACS 服务器上的完全一样。在认证/授权服务器与计费服务器不相同且这两台服务器中的共享密钥也不同时，必须分别设置认证/授权报文和计费报文的共享密钥。

相关配置可参考命令 **display hwtacacs**。

【举例】

配置 HWTACACS 计费服务器共享密钥为 hello。

```
[H3C] hwtacacs scheme test1
[H3C-hwtacacs-test1] key accounting hello
```

1.3.8 nas-ip

【命令】

nas-ip *ip-address*

undo nas-ip

【视图】

HWTACACS 视图

【参数】

ip-address：IP 地址，点分十进制形式。

【描述】

nas-ip 命令用来设置 NAS（防火墙）发送 HWTACACS 报文使用的源 IP 地址，这样发送到 TACACS 服务器的所有报文携带相同的源 IP 地址。**undo nas-ip** 命令用来删除配置。

指定发送 HWTACACS 报文使用的源地址，可以避免物理接口故障时从服务器返回的报文不可达。一般推荐使用 loopback 接口地址。

缺省情况下，报文的源 IP 地址是发送端口的 IP 地址。

相关配置可参考命令 **display hwtacacs**。

【举例】

配置 NAS（防火墙）发送 HWTACACS 报文使用的源 IP 地址为 10.1.1.1。

```
[H3C] hwtacacs scheme test1
[H3C-hwtacacs-test1] nas-ip 10.1.1.1
```

1.3.9 primary accounting

【命令】

primary accounting *ip-address* [*port*]

undo primary accounting

【视图】

HWTACACS 视图

【参数】

ip-address：服务器的 IP 地址，点分十进制格式。必须是合法的单播地址。

port：服务器的端口号，取值范围为 1～65535，缺省端口号为 49。

【描述】

primary accounting 命令用来配置 HWTACACS 主计费服务器。**undo primary accounting** 命令用来删除配置的 HWTACACS 主计费服务器。

缺省情况下，HWTACACS 计费服务器的 IP 地址为 0.0.0.0。

主计费服务器和备用计费服务器的 IP 地址不能相同，否则将提示配置不成功。

如果多次执行此命令，新的配置将覆盖原来的配置。

只有当没有活跃的、用于发送计费报文的 TCP 连接使用该计费服务器时，才允许删除该服务器。删除服务器只对之后的报文有效。

在计费成功后，计费更新以及计费停止报文都会发往计费成功时使用的服务器上，即使此服务器不可用，也不会发生主备切换。只有在最开始的认证、授权、计费过程中才会发生切换，成功后将不再切换。

【举例】

配置主计费服务器。

```
[H3C] hwtacacs scheme test1
[H3C-hwtacacs-test1] primary accouting 10.163.155.12 49
```

1.3.10 primary authentication

【命令】

primary authentication *ip-address* [*port*]

undo primary authentication

【视图】

HWTACACS 视图

【参数】

ip-address：服务器的 IP 地址，点分十进制格式。必须是合法的单播地址。

port：服务器的端口号，取值范围为 1～65535，缺省端口号为 49。

【描述】

primary authentication 命令用来配置 HWTACACS 认证服务器。**undo primary authentication** 命令用来删除配置的认证服务器。

缺省情况下，HWTACACS 认证服务器的 IP 地址为 0.0.0.0。

主认证服务器和备用认证服务器的 IP 地址不能相同，否则将提示配置不成功。

如果多次执行此命令，新的配置将覆盖原来的配置。

只有当没有活跃的、用于发送认证报文的 TCP 连接使用该认证服务器时，才允许删除该服务器。删除服务器只对之后的报文有效。

相关配置可参考命令 **display hwtacacs**。

【举例】

配置主认证服务器。

```
[H3C] hwtacacs scheme test1
[H3C-hwtacacs-test1] primary authentication 10.163.155.13 49
```

1.3.11 primary authorization

【命令】

primary authorization *ip-address* [*port*]

undo primary authorization

【视图】

HWTACACS 视图

【参数】

ip-address：服务器的 IP 地址，点分十进制格式。必须是合法的单播地址。

port：服务器的端口号，取值范围为 1～65535，缺省端口号为 49。

【描述】

primary authorization 命令用来配置 HWTACACS 主授权服务器。**undo primary authorization** 命令用来删除配置的主授权服务器。

缺省情况下，HWTACACS 授权服务器的 IP 地址为 0.0.0.0。

对于所有类型的用户，如果配置了 TACACS 认证，但没有配置 TACACS 授权服务器，则用户无法登录。

主授权服务器和备用授权服务器的 IP 地址不能相同，否则将提示配置不成功。

如果多次执行此命令，新的配置将覆盖原来的配置。

只有当没有活跃的、用于发送授权报文的 TCP 连接使用该授权服务器，才允许删除该服务器。删除服务器只对之后的报文有效。

相关配置可参考命令 **display hwtacacs**。

【举例】

配置主授权服务器。

```
[H3C] hwtacacs scheme test1
[H3C-hwtacacs-test1] primary authorization 10.163.155.13 49
```

1.3.12 reset hwtacacs statistics

【命令】

reset hwtacacs statistics{ **accounting** | **authentication** | **authorization** | **all** }

【视图】

用户视图

【参数】

accounting：清除所有 HWTACACS 协议关于计费的统计信息。

authentication：清除所有 HWTACACS 协议关于认证的统计信息。

authorization：清除所有 HWTACACS 协议关于授权的统计信息。

all：清除所有统计信息。

【描述】

reset hwtacacs statistics 命令用来清除 HWTACACS 协议的统计信息。

相关配置请参考命令 **display hwtacacs**。

【举例】

清除所有 HWTACACS 协议的统计信息。

```
<H3C> reset hwtacacs statistics all
```

1.3.13 reset stop-accounting-buffer

【命令】

reset stop-accounting-buffer hwtacacs-scheme *hwtacacs-scheme-name*

【视图】

用户视图

【参数】

hwtacacs-scheme *hwtacacs-scheme-name*：根据 HWTACACS 方案名删除暂存的停止计费请求报文。其中，*hwtacacs-scheme-name* 为 HWTACACS 方案名，为不超过 32 个字符的字符串。

【描述】

reset stop-accounting-buffer 命令用来清除那些在防火墙上缓存的、没有得到响应的停止计费请求报文。

相关配置可参考命令 **stop-accounting-buffer enable**，**retry stop-accounting**，**display stop-accounting-buffer**。

【举例】

删除 HWTACACS 方案“mytacacs”缓存在系统中的停止计费请求报文。

```
<H3C> reset stop-accounting-buffer hwtacacs-scheme mytacacs
```

1.3.14 retry stop-accounting

【命令】

retry stop-accounting *retry-times*

undo retry stop-accounting

【视图】

HWTACACS 视图

【参数】

retry-times：停止计费报文传送的最大次数，取值范围为 1～300。

【描述】

retry stop-accounting 命令用来使能停止计费报文重传功能，并配置停止计费报文传送的最大次数。**undo retry stop-accounting** 命令用来恢复停止计费报文传送次数为缺省值。

缺省情况下，使能停止计费报文重传功能，可传送报文的最大次数为 100。

相关配置可参考命令 **reset stop-accounting-buffer**，**hwtacacs scheme**，**display stop-accounting-buffer**。

【举例】

使能停止计费报文重发功能，每次可重发 50 个报文。

```
[H3C-hwtacacs-test] retry stop-accounting 50
```

1.3.15 secondary accounting

【命令】

secondary accounting *ip-address* [*port*]

undo secondary accounting

【视图】

HWTACACS 视图

【参数】

ip-address：服务器的 IP 地址，点分十进制格式，必须是合法的单播地址。

port：服务器的端口号，取值范围为 1～65535，缺省端口号为 49。

【描述】

secondary accounting 命令用来配置 HWTACACS 备计费服务器。**undo secondary accounting** 命令用来删除配置的 HWTACACS 备计费服务器。

缺省情况下，HWTACACS 计费服务器的 IP 地址为 0.0.0.0。

主计费服务器和备用计费服务器的 IP 地址不能相同，否则将提示配置不成功。

如果多次执行此命令，新的配置将覆盖原来的配置。

只有当没有活跃的、用于发送计费报文的 TCP 连接使用该计费服务器时，才允许删除该服务器。

【举例】

配置备计费服务器。

```
[H3C] hwtacacs scheme test1
[H3C-hwtacacs-test1] secondary accouting 10.163.155.12 49
```

1.3.16 secondary authentication

【命令】

secondary authentication *ip-address* [*port*]

undo secondary authentication

【视图】

HWTACACS 视图

【参数】

ip-address：服务器的 IP 地址，点分十进制格式。必须是合法的单播地址。

port：服务器的端口号，取值范围为 1～65535，缺省端口号为 49。

【描述】

secondary authentication 命令用来配置 HWTACACS 备认证服务器。**undo secondary authentication** 命令用来删除配置的备认证服务器。

缺省情况下，HWTACACS 认证服务器的 IP 地址为 0.0.0.0。

主认证服务器和备用认证服务器的 IP 地址不能相同，否则将提示配置不成功。

如果多次执行此命令，新的配置将覆盖原来的配置。

只有当没有活跃的、用于发送认证报文的 TCP 连接使用该认证服务器时，才允许删除该服务器。

相关配置可参考命令 **display hwtacacs**。

【举例】

配置备认证服务器。

```
[H3C] hwtacacs scheme test1
[H3C-hwtacacs-test1] secondary authentication 10.163.155.13 49
```

1.3.17 secondary authorization

【命令】

secondary authorization *ip-address* [*port*]

undo secondary authorization

【视图】

HWTACACS 视图

【参数】

ip-address：服务器的 IP 地址，点分十进制格式。必须是合法的单播地址。

port：服务器的端口号，取值范围为 1～65535，缺省端口号为 49。

【描述】

secondary authorization 命令用来配置 HWTACACS 备授权服务器。**undo secondary authorization** 命令用来删除配置的备授权服务器。

缺省情况下，HWTACACS 授权服务器的 IP 地址为 0.0.0.0。

主授权服务器和备用授权服务器的 IP 地址不能相同，否则将提示配置不成功。

如果多次执行此命令，新的配置将覆盖原来的配置。

只有当没有活跃的、用于发送授权报文的 TCP 连接使用该授权服务器，才允许删除该服务器。

相关配置可参考命令 **display hwtacacs**。

【举例】

配置备授权服务器。

```
[H3C] hwtacacs scheme test1
[H3C-hwtacacs-test1] secondary authorization 10.163.155.13 49
```

1.3.18 stop-accounting-buffer enable

【命令】

stop-accounting-buffer enable

undo stop-accounting-buffer enable

【视图】

HWTACACS 视图

【参数】

无

【描述】

stop-accounting-buffer enable 命令用来允许在防火墙上缓存没有得到响应的停止计费请求报文。**undo stop-accounting-buffer enable** 命令用来禁止在防火墙上缓存没有得到响应的停止计费请求报文。

缺省情况下，允许防火墙缓存没有得到响应的停止计费请求报文。

此命令的具体描述请参见 RADIUS 方案中的 **stop-accounting-buffer enable** 命令。

【举例】

指示对于 HWTACACS 方案“mytacacs”中的服务器，防火墙系统能够缓存没有得到响应的停止计费请求报文。

```
[H3C-hwtacacs-mytacacs] stop-accounting-buffer enable
```

1.3.19 timer quiet

【命令】

timer quiet *minutes*

undo timer quiet

【视图】

HWTACACS 视图

【参数】

minutes：取值范围为 1～255，单位为分钟。缺省情况下，主服务器恢复激活状态前需要等待 5 分钟。

【描述】

timer quiet 命令用来设置主服务器恢复激活状态的时间。**undo timer quiet** 命令用来恢复缺省配置。

相关配置可参考命令 **display hwtacacs**。

【举例】

设置主服务器恢复激活状态的时间为 10 分钟。

```
[H3C] hwtacacs scheme test1
[H3C-hwtacacs-test1] timer quiet 10
```

1.3.20 timer realtime-accounting

【命令】

timer realtime-accounting *minutes*

undo timer realtime-accounting

【视图】

HWTACACS 视图

【参数】

minutes：实时计费的时间间隔，单位为分钟，取值范围为 3～60，必须为 3 的倍数。

【描述】

timer realtime-accounting 命令用来设置实时计费的时间间隔，**undo timer realtime-accounting** 命令用来将实时计费的时间间隔恢复为缺省值。

为了对用户实施实时计费，有必要设置实时计费的时间间隔。在设置了该属性以后，每隔设定的时间，NAS 会向 TACACS 服务器发送一次在线用户的计费信息。

实时计费间隔的取值对 NAS 和 TACACS 服务器的性能有一定的相关性要求——取值越小，对 NAS 和 TACACS 服务器的性能要求越高。建议当用户量比较大（≥1000）时，尽量把该间隔的值设置得大一些。以下是实时计费间隔与用户量之间的推荐比例关系：

表1-9 实时计费间隔与用户量之间的推荐比例关系

用户数	实时计费间隔（分钟）
1～99	3
100～499	6
500～999	12
≥1000	≥15

缺省情况下，实时计费的时间间隔为 12 分钟。

【举例】

将 HWTACACS 方案“mytacacs”的实时计费的时间间隔设置为 51 分钟。

```
[H3C-hwtacacs-mytacacs] timer realtime-accounting 51
```

1.3.21 timer response-timeout

【命令】

timer response-timeout *seconds*

undo timer response-timeout

【视图】

HWTACACS 视图

【参数】

seconds：取值范围为 1～300，单位为秒。

【描述】

timer response-timeout 命令用来设置 TACACS 服务器应答超时时间。**undo timer response-timeout** 命令用来恢复缺省配置。

缺省情况下，TACACS 服务器应答超时时间为 5 秒。

📖 说明：

由于 HWTACACS 是基于 TCP 实现的，因此，服务器应答超时或 TCP 超时都可能导致与 TACACS 服务器的连接断开。

相关配置可参考命令 **display hwtacacs**。

【举例】

配置 TACACS 服务器应答超时时间为 30 秒。

```
[H3C] hwtacacs scheme test1
[H3C-hwtacacs-test1] timer response-timeout 30
```

1.3.22 user-name-format

【命令】

user-name-format { **with-domain** | **without-domain** }

【视图】

HWTACACS 视图

【参数】

with-domain：指定发送给 TACACS 服务器的用户名带域名。

without-domain：指定发送给 TACACS 服务器的用户名不带域名。

【描述】

user-name-format 命令用来设置发送给 TACACS 服务器的用户名格式。

缺省情况下，HWTACACS 方案默认发送给 TACACS 服务器的用户名携带有 ISP 域名。

接入用户通常以“userid@isp-name”的格式命名，“@”后面的部分为 ISP 域名，防火墙就是通过该域名来决定将用户归于哪个 ISP 域的。但是，有些较早期的 TACACS 服务器不能接受携带有 ISP 域名的用户名，在这种情况下，有必要将用户名中携带的域名去除后再传送给 TACACS 服务器。因此，防火墙提供此命令以指定发送给 TACACS 服务器的用户名是否携带有 ISP 域名。

📖 **说明：**

如果指定某个 HWTACACS 方案不允许用户名中携带有 ISP 域名，那么请不要在两个乃至两个以上的 ISP 域中同时设置使用该 HWTACACS 方案，否则，会出现虽然实际用户不同（在不同的 ISP 域中）、但 TACACS 服务器认为用户相同（因为传送到它的用户名相同）的错误。

相关配置可参考命令 **hwtacacs scheme**。

【举例】

指定发送给 HWTACACS 方案“mytacacs”的用户不得携带域名。

```
[H3C-hwtacacs-mytacacs] user-name-format without-domain
```

第2章 访问控制列表配置命令

2.1 访问控制列表配置命令

2.1.1 acl

【命令】

acl number *acl-number* [**match-order** { **config** | **auto** }]

undo acl { **number** *acl-number* | **all** }

【视图】

系统视图

【参数】

number *acl-number*：访问控制列表的序号。1000～1999 为基于接口的访问控制列表，2000～2999 为基本访问控制列表（basic），3000～3999 为高级访问控制列表（advanced），4000～4999 为基于 MAC 地址的访问控制列表。

match-order：指定规则的配置顺序。

config：指定匹配该规则时按用户的配置顺序。

auto：指定匹配该规则时系统自动排序（按“深度优先”的顺序）。

all：所有的 ACL。

【描述】

命令 **acl** 用于创建一个访问控制列表并进入 ACL 视图，命令 **undo acl** 用于删除访问控制列表。

一个访问控制列表是由 **permit** 和 **deny** 语句组成的一系列的规则列表，若干个规则构成一个访问控制列表。在配置访问控制列表的规则之前，首先需要创建一个访问控制列表。

【举例】

创建一个序号为 2000 的基本 ACL。

```
[H3C] acl number 2000
[H3C-acl-basic-2000]
```

2.1.2 acl counter

【命令】

acl counter { **enable** | **disable** }

【视图】

系统视图

【参数】

enable：使能 ACL 计数器。

disable：关闭 ACL 计数器。

【描述】

acl counter 命令用来使能或关闭 ACL 计数器。

缺省情况下，使能 ACL 计数器。

相关配置可参考命令 **reset acl counter**。

【举例】

关闭 ACL 计数器。

```
[H3C] acl counter disable
```

2.1.3 description

【命令】

description *text*

undo description

【视图】

ACL 视图

【参数】

text：ACL 的描述，描述内容最长为 127 个字符。

【描述】

description 命令用来为 ACL 添加描述，**undo description** 命令用来删除 ACL 的描述。

【举例】

为编号为 2001 的基本 ACL 添加描述。

```
[H3C-acl-basic-2001] description Deny HTTP from host 10.0.0.1
```

2.1.4 display acl

【命令】

display acl { **all** | *acl-number* }

【视图】

所有视图。

【参数】

all：所有的 ACL。

acl-number：特定编号的 ACL。

【描述】

命令 **display acl** 用来显示配置的访问控制列表的规则。

默认情况下，规则的匹配顺序为 **config**（配置顺序），**display** 命令将不会显示该匹配顺序；而如果匹配顺序为 **auto** 时，**display** 命令则会显示出该顺序。

【举例】

显示 ACL 2000 的规则的内容。

```
[H3C-acl-basic-2000] display acl 2000
Basic ACL  2000, 2 rules
Acl's step is 1
 rule 1 permit (0 times matched)
 rule 2 permit source 1.1.1.1 0 (0 times matched)
```

2.1.5 reset acl counter

【命令】

reset acl counter { **all** | *acl-number* }

【视图】

用户视图

【参数】

acl-number：特定编号的 ACL。

all：所有的 ACL。

【描述】

命令 **reset acl counter** 用来清除访问控制列表的统计信息。

相关配置可参考命令 **acl counter**。

【举例】

清除访问控制列表 2000 的统计信息。

```
<H3C> reset acl counter 2000
```

2.1.6 rule

【命令】

(1) 增加/删除一个基本访问控制列表的规则

rule [*rule-id*] { **permit** | **deny** } [**source** { *sour-addr sour-wildcard* | **any** }] [**time-range** *time-name*] [**logging**] [**fragment**] [**vpn-instance** *vpn-instance-name*]

undo rule *rule-id* [**source**] [**time-range**] [**logging**] [**fragment**] [**vpn-instance**]

(2) 增加/删除一个高级访问控制列表的规则

rule [*rule-id*] { **permit** | **deny** } *protocol* [**source** { *sour-addr sour-wildcard* | **any** }] [**destination** { *dest-addr dest-wildcard* | **any** }] [**source-port** *operator port1* [*port2*]] [**destination-port** *operator port1* [*port2*]] [**icmp-type** { *icmp-message* |*icmp-type icmp-code*}] [**dscp** *dscp*] [**established**] [**precedence** *precedence*] [**tos** *tos*] [**time-range** *time-name*] [**logging**] [**fragment**] [**vpn-instance** *vpn-instance-name*]

undo rule *rule-id* [**source**] [**destination**] [**source-port**] [**destination-port**] [**icmp-type**] [**dscp**] [**precedence**] [**tos**] [**time-range**] [**logging**] [**fragment**] [**vpn-instance**]

(3) 增加/删除一个基于接口的访问控制列表的规则

rule [*rule-id*] { **permit** | **deny** } **interface** { *interface-type interface-number* | **any** } [**time-range** *time-name*] [**logging**]

undo rule *rule-id* [**time-range**] [**logging**]

(4) 增加/删除一个以太网 MAC 地址的访问控制列表的规则

rule [*rule-id*] { **deny** | **permit** } [**type** *type-code type-mask* | **lsap** *lsap-code lsap-mask*] [**source-mac** *sour-addr sour-mask*] [**dest-mac** *dest-addr dest-mask*] [**time-range** *time-name*] [**logging**]

undo rule *rule-id* [**time-range**] [**logging**]

【视图】

ACL 视图

【参数】

使用命令 **rule** 为 ACL 增加一个规则的时候，参数说明如下：

rule-id：可选参数，ACL 的规则编号，范围为 0～65534。当指定了编号，如果与编号对应的规则已经存在，则会部分覆盖旧的规则，相当于编辑一个已经存在的 ACL 规则。故建议用户当编辑一个已存在编号的规则时，先将旧的规则删除，再创建新的规则，否则配置结果可能与预期的效果不同。如果与编号对应的规则不存在，则使用指定的编号创建一个新的规则。如果不指定编号，表示增加一个新规则，系统自动会为这个规则分配一个编号。

deny：表示拒绝符合条件的数据包。

permit：表示允许符合条件的数据包。

protocol：用名字或数字表示的 IP 承载的协议类型。数字范围为 1～255；用名字表示时，可以选取：gre、icmp、igmp、ip、ipinip、ospf、tcp、udp。

source：可选参数，指定 ACL 规则的源地址信息。如果不配置，表示报文的任何源地址都匹配。

sour-addr：数据包的源地址，点分十进制表示。

sour-wildcard：源地址通配符，点分十进制表示。

destination：可选参数，指定 ACL 规则的目的地址信息。如果不配置，表示报文的任何目的地址都匹配。

dest-addr：数据包的目的地址，点分十进制表示。

dest-wildcard：目的地址通配符，点分十进制表示。

any：表示所有源地址或目的地址，作用与源或目的地址是 0.0.0.0，通配符是 255.255.255.255 相同。

icmp-type：可选参数，指定 ICMP 报文的类型和消息码信息，仅仅在报文协议是 ICMP 的情况下有效。如果不配置，表示任何 ICMP 类型的报文都匹配。

icmp-type：ICMP 包可以依据 ICMP 的消息类型进行过滤。取值为 0～255 的数字。

icmp-code：依据 ICMP 的消息类型进行过滤的 ICMP 包也可以依据消息码进行过滤。取值为 0～255 的数字。

icmp-message：ICMP 包可以依据 ICMP 消息类型名字或 ICMP 消息类型和码的名字进行过滤。

source-port：可选参数，指定 UDP 或者 TCP 报文的源端口信息，仅仅在规则指定的协议号是 TCP 或者 UDP 有效。如果不指定，表示 TCP/UDP 报文的任何源端口信息都匹配。

destination-port：可选参数，指定 UDP 或者 TCP 报文的目的端口信息，仅仅在规则指定的协议号是 TCP 或者 UDP 时有效。如果不指定，表示 TCP/UDP 报文的任何目的端口信息都匹配。

operator：可选参数。比较源或者目的地址的端口号的操作符，名字及意义如下：lt（小于），gt（大于），eq（等于），neq（不等于），range（在范围内）。只有 range 需要两个端口号做操作数，其他的只需要一个端口号做操作数。

port1、*port2*：可选参数。TCP 或 UDP 的端口号，用名字或数字表示，数字的取值范围为 0～65535。

dscp *dscp*：指定 DSCP 字段（IP 报文中的 DS 字节）。此参数与 **precedence**、**tos** 互斥。

established：匹配所有标志为 ACK 或 RST 的 TCP 报文（特征是 ACK 或者 RST 标志已置位）。包括 SYN+ACK、ACK、FIN+ACK、RST、RST+ACK 等几种报文。此选项可以匹配那些已经建立的 TCP 会话的流量，即过滤掉始发的 TCP 会话请求。使用此选项时，建议关闭快速转发功能，有关快速转发的描述请参见本手册的“网络层协议”部分。

precedence *precedence*：可选参数，数据包可以依据优先级字段进行过滤。取值为 0～7 的数字或名称。此参数与 **dscp** 互斥。

tos *tos*：可选参数，数据包可以依据服务类型字段进行过滤。取值为 0～15 的数字或名称。此参数与 **dscp** 互斥。

logging：可选参数，是否对符合条件的数据包做日志。日志内容包括访问控制列表规则的序号、数据包通过或被丢弃、IP 承载的上层协议类型、源/目的地址、源/目的端口号、数据包的数目。目前支持此选项的业务只有包过滤防火墙（在接口下被 **firewall packet-filter** 命令引用）。

time-range *time-name*：配置这条访问控制规则生效的时间段。

fragment：指定该规则是否仅对非首片分片报文有效。当包含此参数时，表示该规则仅对非首片分片报文有效。

vpn-instance：可选参数，指定报文是属于哪个 VPN 实例的。如果没有指定，该规则对所有 VPN 实例中的报文都有效；如果指定了，则表示该规则仅仅对指定的 VPN 实例中的报文有效。

vpn-instance-name：指定具体的 VPN 实例的名字，该实例名字必须是一个已经存在的 VPN 实例名字。

interface *interface-type interface-number*：指定数据包的接口信息。**any** 代表所有的接口。

type：数据帧的类型。

type-code：数据帧的类型值，一个 16 比特的十六进制数，对应Ethernet_II类型和Ethernet_SNAP类型帧中的type-code域。关于*type-code*的值请参考 表 7-5。

type-mask：类型通配符，是一个 16 比特的十六进制数，用于指定屏蔽位。

lsap：数据帧的 LSAP。

lsap-code：数据帧的封装格式的值，是一个 16 比特的十六进制数。

lsap-mask：Lsap 值的通配符，是一个 16 比特的十六进制数，用于指定屏蔽位。

source-mac：源 MAC 地址。

sour-addr：源 MAC 地址，格式为 xxxx-xxxx-xxxx，用来匹配一个分组的源地址。

sour-mask：源 MAC 地址的通配符。

dest-mac：目的 MAC 地址。

dest-addr：目的 MAC 地址，格式为 xxxx-xxxx-xxxx，用来匹配一个分组的源地址。

dest-mask：目的 MAC 地址的通配符。

使用命令 **undo rule** 删除规则的时候，参数说明如下：

rule-id：ACL 规则编号，必须是一个已经存在的 ACL 规则编号。如果 *rule-id* 后面不指定参数，则将这个 ACL 规则完全删除。否则，只是删除对应 ACL 规则的部分信息。

source：可选参数，仅仅删除编号对应的 ACL 规则的源地址部分的信息设置。

destination：可选参数，仅仅删除编号对应的 ACL 规则的目的地址部分的信息设置。

source-port：可选参数，仅仅删除编号对应的 ACL 规则的源端口部分的信息设置，仅仅在规则的协议号是 TCP 或者 UDP 的情况下有效。

destination-port：可选参数，仅仅删除编号对应的 ACL 规则的目的端口部分的信息设置，仅仅在规则的协议号是 TCP 或者 UDP 的情况下有效。

icmp-type：可选参数，仅仅删除编号对应的 ACL 规则 ICMP 类型和消息码部分的信息设置，仅仅在规则的协议号是 ICMP 的情况下有效。

dscp：可选参数，仅仅删除编号对应的 ACL 规则的 DSCP 设置。

precedence：可选参数，仅仅删除编号对应的 ACL 规则的 precedence 的相关设置。

tos：可选参数，仅仅删除编号对应的 ACL 规则的 ToS 的相关设置。

time-range：可选参数，仅仅删除编号对应的 ACL 规则的生效时间段的设置。

logging：可选参数，仅仅删除编号对应的 ACL 规则对符合条件的数据包做日志的设置。

fragment：可选参数，仅仅删除编号对应的 ACL 规则仅对非首片分片报文有效的设置。

vpn-instance：可选参数，仅仅删除编号对应的 ACL 规则中关于 VPN 实例的设置。

【描述】

命令 **rule** 用来在对应的 ACL 视图下，增加一个规则。命令 **undo rule** 用来删除一个规则。

在删除一条规则时，需要指定规则的编号，如果不知道规则的编号，可以使用命令 **display acl** 来查看。

【举例】

创建 ACL 3001，增加一条规则，禁止接收和发送 RIP 报文。

```
[H3C] acl number 3001
[H3C-acl-adv-3001] rule deny udp destination-port eq rip
```

增加一条规则，允许从 129.9.0.0 网段的主机向 202.38.160.0 网段的主机发送 WWW 报文。

```
[H3C-acl-adv-3001] rule permit tcp source 129.9.0.0 0.0.255.255 destination
202.38.160.0 0.0.0.255 destination-port eq www
```

增加一条规则，禁止从 129.9.0.0 网段内的主机建立与 202.38.160.0 网段内的主机的 WWW 端口（80）的连接，并对违反此规则的事件作日志。

```
[H3C-acl-adv-3001] rule deny tcp source 129.9.0.0 0.0.255.255 destination
202.38.160.0 0.0.0.255 destination-port eq www logging
```

增加一条规则，允许从 129.9.8.0 网段内的主机建立与 202.38.160.0 网段内的主机的 WWW 端口（80）的连接。

```
[H3C-acl-adv-3001] rule permit tcp source 129.9.8.0 0.0.0.255 destination
202.38.160.0 0.0.0.255 destination-port eq www
```

增加一条规则，禁止从一切主机建立与 IP 地址为 202.38.160.1 的主机的 Telnet（23）的连接。

```
[H3C-acl-adv-3001] rule deny tcp destination 202.38.160.1 0 destination-port
eq telnet
```

增加一条规则，禁止从 129.9.8.0 网段内的主机建立与 202.38.160.0 网段内的主机的端口号大于 128 的 UDP（用户数据报协议）连接。

```
[H3C-acl-adv-3001] rule deny udp source 129.9.8.0 0.0.0.255 destination
202.38.160.0 0.0.0.255 destination-port gt 128
```

2.1.7 rule comment

【命令】

rule *rule-id* **comment** *text*

undo rule *rule-id* **comment**

【视图】

ACL 视图

【参数】

rule-id：已创建的 ACL 规则的编号。

comment *text*：ACL 规则的注释，注释内容最长为 127 个字符。

【描述】

rule comment 命令用来为 ACL 规则添加注释，**undo rule comment** 命令用来删除 ACL 规则的描述。

【举例】

为编号为 7 的 ACL 规则添加注释。

```
[H3C-acl-adv-3001] rule 7 comment Allow FTP from any source to host 172.16.0.1
```

2.2 时间段配置命令

2.2.1 display time-range

【命令】

display time-range { **all** | *time-name* }

【视图】

所有视图

【参数】

time-name：时间段的名称。

all：所有配置的时间段。

【描述】

命令 **display time-range** 用来显示当前时间段的配置和状态，对于当前处在激活状态的时间段将显示 active，对于非激活状态显示 inactive。

注意，由于系统更新 ACL 状态有一个误差，大约 1 分钟，而 **display time-range** 会采用当前时间对其进行判断，所以有可能出现 **display time-range** 看到一个时间段已经激活，而引用它的 ACL 没有激活，这种情况是正常的。

【举例】

显示名字为 worktime 的时间段。

```
< H3C> display time-range worktime
Current time is 10:47:58 Nov/21/2005 Monday

Time-range : worktime ( Active )
```

```
08:30 to 18:00 working-day
```

2.2.2 time-range

【命令】

time-range *time-name* { *start-time* **to** *end-time days-of-the-week* [**from** *start-time start-date*] [**to** *end-time end-date*] | **from** *start-time start-date* [**to** *end-time end-date*] | **to** *end-time end-date* }

undo time-range *time-name* [*start-time* **to** *end-time days-of-the-week* [**from** *start-time start-date*] [**to** *end-time end-date*] | **from** *start-time start-date* [**to** *end-time end-date*] | **to** *end-time end-date*]

【视图】

系统视图

【参数】

time-name：时间段的名字，不能大于 32 个字符，且必须以字母 a-z，A-Z 开头。

start-time：一个时间范围的开始时间，格式为 hh:mm，小时和分钟之间使用“:”分隔，hh 的范围为 0～24，mm 的范围为 0～59，当 hh 配置为 24 时，mm 只能配置为 0。对于绝对时间段，当配置 24:00 时，配置结果将显示为第二天的 00:00。

end-time：一个时间范围的结束时间，格式为 hh:mm，小时和分钟之间使用“:”分隔，hh 的范围为 0～24，mm 的范围为 0～59，当 hh 配置为 24 时，mm 只能配置为 0。对于绝对时间段，当配置 24:00 时，配置结果将显示为第二天的 00:00。

days-of-the-week：表示配置的时间范围在每周几有效，可以输入如下参数：

数字（0～6）；

星期日到星期六（Sunday，Monday，Tuesday，Wednesday，Thursday，Friday，Saturday）；

工作日（Working-day），包括从星期一到星期五五天；

休息日（Off-day），包括星期六和星期天；

所有日子（Daily)，包括一周七天。

start-date：表示起始日期，输入格式为 MM/DD/YYYY。DD 可以输入 1～31 之间的数字，MM 需要输入 1～12 之间的数字，YYYY 使用 4 位输入，范围为 1970～2100。

end-date：表示结束日期，输入格式为 MM/DD/YYYY。DD 可以输入 1～31 之间的数字，MM 需要输入 1～12 之间的数字，YYYY 使用 4 位输入，范围为 1970～2100。

【描述】

命令 **time-range** 用来定义一个时间段，描述一个特殊的时间范围。命令 **undo time-range** 用来删除一个时间段。

时间段可以分为如下几种：

- 绝对时间段

例如：

配置时间段，从 2003 年 4 月 1 日 20:00 起，到 2003 年 12 月 10 日 20:00 之间有效。

```
[H3C] time-range test from 20:00 04/01/2003 to 20:00 12/10/2003
```

此时查看配置只有一条单独的绝对时间段：

```
[H3C] display time-range test
Current time is 19:41:22 Jan/1/2000 Saturday

Time-range : test ( Inactive )
From 20:00 Apr/1/2003 to 20:00 Dec/10/2003
```

- 周期时间段

例如：

配置时间段，在每天的 12:00 到 17:00 之间有效。

```
[H3C] time-range  test 12:00 to 17:00 daily
```

此时查看配置只有一条周期时间段：

```
[H3C] display time-range test
Current time is 19:44:25 Jan/1/2000 Saturday

Time-range : test ( Inactive )
12:00 to 17:00 daily
```

- 在绝对时间段内生效的周期时间段

例如：

配置时间段，从 2003 年 4 月 1 日 20:00 起，到 2003 年 12 月 10 日 20:00 之间，在每个周末的下午 14:00 到 16:00 之间有效。

```
[H3C] time-range test 14:00 to 16:00 off-day from 20:00 04/01/2003 to 20:00
12/10/2003
```

此时查看配置其实是由一条单独的周期时间段和一条单独的绝对时间段组成的：

```
[H3C] display time-range test
Current time is 18:39:49 Jan/1/2000 Saturday

Time-range : test ( Inactive )
 14:00 to 16:00 off-day
 From 20:00 Apr/1/2003 to 20:00 Dec/10/2003
```

- 复合时间段

复合时间段是由若干条周期时间段和（或）绝对时间段组成，比如：

```
[H3C] time test 16:30 to 18:00 daily from 01:00 01/01/2000 to 23:00 01/10/2000
[H3C] time test 18:00 to 21:30 daily from 23:00 01/10/2000 to 23:00 02/01/2000
[H3C] display time-range test
Current time is 18:29:37 Jan/1/2000 Saturday

Time-range : test ( Active )
 16:30 to 18:00 daily
 18:00 to 21:30 daily
 From 01:00 Jan/1/2000 to 23:00 Jan/10/2000
 From 23:00 Jan/10/2000 to 23:00 Feb/1/2000
```

实际的有效时间是从 2000 年 1 月 1 日 01:00 到 2000 年 2 月 1 日 23:00 期间每天的 16:30 到 21:30。而不只是从 2000 年 1 月 1 日 01:00 到 2000 年 1 月 10 日 23:00 期间的 16:30 到 18:00，和从 2000 年 1 月 10 日 23:00 到 2000 年 2 月 1 日 23:00 期间的 18:00 到 21:30 有效。

总之，复合时间段与各子时间段之间的关系是：如果没有周期时间段，则为所有的绝对时间段的并集；如果有周期时间段，则为所有的绝对时间段的并集与所有周期时间段的并集的交集。

【举例】

配置时间段，在 2003 年 1 月 1 日 0:0 生效，并永远有效。

```
[H3C] time-range test from 0:0 1/1/2003
```

配置时间段，从 2003 年 4 月 1 日 20:00 起，到 2003 年 12 月 10 日 20:00 之间，在每个周末的下午 14:00 到 16:00 之间有效。

```
[H3C] time-range test 14:00 to 16:00 off-day from 20:00 04/01/2003 to 20:00
12/10/2003
```

配置时间段，在周一到周五每天 8:00 到 18:00 生效。

```
[H3C] time-range test 8:00 to 18:00 working-day
```

配置时间段，在周末下午 14:00 到 18:00 生效。

```
[H3C] time-range test 14:00 to 18:00 off-day
```

第3章 NAT 配置命令

3.1 NAT 配置命令

3.1.1 connection-limit default

【命令】

connection-limit default { **permit** | **deny** }

undo connection-limit default { **permit** | **deny** }

【视图】

系统视图

【参数】

permit：进行限制，上下限使用系统默认值。

deny：不进行限制。

【描述】

connection-limit default 命令用来设置在查不到限制策略时的动作。

undo connection-limit default 命令用来取消设置的动作。

connection-limit default 命令可重复配置，后一个配置将覆盖前一个配置。

缺省情况下，在未查找到限制策略时不对连接数进行限制。

【举例】

设置在查不到限制策略时进行连接数限制。

```
[H3C] connection-limit default permit
```

3.1.2 connection-limit default amount

【命令】

connection-limit default amount { **upper-limit** *upper-limit* | **lower-limit** *lower-limit* }*

undo connection-limit default amount { **upper-limit** | **lower-limit** }*

【视图】

系统视图

【参数】

upper-limit：设置缺省上限。

upper-limit：缺省上限值，取值范围是 1～4294967295。

lower-limit：设置缺省下限。

lower-limit：缺省下限值，取值范围是 0～4294967295。

【描述】

connection-limit default amount 命令用来设置连接数限制的缺省阈值。

undo connection-limit default amount 命令用来取消设置的阈值。

缺省情况下，上限为 50，下限为 20。

【举例】

设置连接数限制的缺省阈值，上限为 100，下限为 20。

```
[H3C] connection-limit default amount upper-limit 100 lower-limit 20
```

3.1.3 connection-limit enable

【命令】

connection-limit enable

undo connection-limit enable

【视图】

系统视图

【参数】

无

【描述】

connection-limit enable 命令用来使能连接数限制功能。

undo connection-limit enable 命令用来关闭连接数限制功能。

缺省情况下，连接数限制功能处于关闭状态。

【举例】

使能连接数限制功能。

```
[H3C] connection-limit enable
```

3.1.4 connection-limit policy

【命令】

connection-limit policy *policy-number*

undo connection-limit policy { *policy-number* | **all** }

【视图】

系统视图

【参数】

policy-number：连接数限制策略编号，范围为 0～19。

all：删除策略时使用，删除所有策略。

【描述】

connection-limit policy 命令用来创建连接数限制策略并进入策略视图。

undo connection-limit policy 命令用来删除连接数限制策略。

【举例】

创建一个编号为 10 的连接数限制策略。

```
[H3C] connection-limit policy 10
```

3.1.5 debugging connection-limit

【命令】

debugging connection-limit

undo debugging connection-limit

【视图】

用户视图

【参数】

无

【描述】

debugging connection-limit 命令用来打开连接数限制的调试功能。

undo debugging connection-limit 命令用来关闭连接数限制的调试功能。

缺省情况下，关闭连接数限制的调试功能。

【举例】

打开连接数限制的调试功能。

```
<H3C> debugging connection-limit
```

3.1.6 debugging nat

【命令】

debugging nat { **alg** | **event** | **packet** } [**interface** *interface-type interface-number*]

undo debugging nat { **alg** | **event** | **packet** } [**interface** *interface-type interface-number*]

【视图】

用户视图

【参数】

alg：打开应用协议地址转换信息开关。

event：打开地址转换事件调试信息开关。

packet：打开地址转换数据包调试信息开关。

interface：打开指定接口的地址转换数据包调试信息开关。

【描述】

debugging nat 命令用来打开 NAT 信息调试开关，**undo debugging nat** 命令用来关闭 NAT 信息调试开关。

【举例】

打开地址转换的事件调试信息开关。

```
<H3C> debugging nat event
```

3.1.7 display connection-limit policy

【命令】

display connection-limit policy { *policy-number* | **all** }

【视图】

任意视图

【参数】

policy-number：要显示的策略编号，范围为 0~255。

all：显示所有的策略。

【描述】

display connection-limit policy 命令用来显示连接数限制策略。

【举例】

显示编号为 1 的策略。

```
[H3C] display connection-limit policy 1
```

3.1.8 display connection-limit statistics

【命令】

display connection-limit statistics [**source** *source-addr source-mask*] [**destination** *destination-addr destination-mask*] [**destination-port** { { **eq** | **neq** | **gt** | **lt** } *destination-port* | **range** *destination-port1 destination-port2* }] [**vpn-instance** *vpn-name*]

【视图】

任意视图

【参数】

source：指定源 IP 地址。

source-addr：源 IP 地址。

source-mask：源 IP 地址的掩码。

destination：指定目的 IP 地址。

destination-addr：目的 IP 地址。

destination-mask：目的 IP 地址掩码。

destination-port：指定目的端口号。

eq：显示目的端口号等于指定端口号的服务的连接数。

neq：显示目的端口号不等于指定端口号的服务的所有连接数。

gt：显示目的端口号大于指定端口号的服务的所有连接数。

lt：显示目的端口号小于指定端口号的服务的所有连接数。

range：显示目的端口号在指定范围内的服务的所有连接数。

destination-port：目的端口号。

destination-port1、*destination-port2*：按端口范围显示时的参数，分别表示服务端口的上下限。

vpn-instance：指定 VPN 实例。

vpn-name：VPN 实例的名称。

【描述】

display connection-limit statistics 命令用来显示连接数限制信息。

用户可以通过此命令，灵活的查看所关心的连接数信息。当该命令后面不接其他参数时，将显示所有的连接数信息。

【举例】

显示所有的连接数限制信息。

```
[H3C] display connection-limit statistics
```

3.1.9 display nat

【命令】

display nat { **address-group** | **aging-time** | **all** | **outbound** | **server** | **statistics** | **static** | **session** [**vpn-instance** *vpn-instance-name*] [**source** { **global** *global-addr* | **inside** *inside-addr* }] }

【视图】

所有视图

【参数】

address-group：表示显示地址池的信息。

aging-time：显示地址转换连接的有效时间。

all：表示显示所有的关于地址转换的信息。

outbound：表示显示配置的地址转换的信息。

server：表示显示内部服务器的信息。

statistics：显示当前的地址转换记录统计数据。

static：显示静态地址转换信息。

session：表示显示当前激活的连接信息。

vpn-instance *vpn-instance-name*：只显示指定 VPN 内的 NAT 转换表项。若没有该值，将显示所有私网内的 NAT 转换表项。

source global *global-addr*：只显示 NAT 转换后地址为 *global-addr* 的转换表项。

source inside *inside-addr*：只显示内部地址为 *inside-addr* 的 NAT 转换表项。

【描述】

display nat 命令显示用户对地址转换的配置，用户可以根据该命令的输出信息验证地址转换的配置是否正确。

【举例】

显示所有的关于地址转换的信息。

```
<H3C> display nat all
NAT address-group information:
    1: from 11.1.1.1      to  11.1.1.20
    2: from 22.1.1.1      to  22.1.1.20
NAT outbound information:
   Ethernet0/0/0: acl(2011)-NAT address-group(1) [no-pat]
   Ethernet0/0/0: acl(2022)-NAT address-group(2) [no-pat]
NAT static table information:
  No static tables have been configured
Server in private network information:
  There are currently 2 internal servers
  Interface:  Ethernet0/0/0, Protocol:  6(tcp),
     [global]  201.119.11.3:   8080        [local]     5.5.5.5:    80(www)
  Interface:  Ethernet0/0/0, Protocol:  6(tcp),
     [global]  201.119.11.3:   2121        [local]     5.5.5.5:    21(ftp)
NAT dns-map information:
  No dns-map have been configured
NAT aging-time value information:
       tcp ---- aging-time value is  86400 (seconds)
       udp ---- aging-time value is    300 (seconds)
      icmp ---- aging-time value is     60 (seconds)
      pptp ---- aging-time value is  86400 (seconds)
       dns ---- aging-time value is     60 (seconds)
   tcp-fin ---- aging-time value is     60 (seconds)
   tcp-syn ---- aging-time value is     60 (seconds)
  ftp-ctrl ---- aging-time value is   7200 (seconds)
  ftp-data ---- aging-time value is    300 (seconds)
NAT server-group information:
  No server-groups have been configured
```

如上信息表示：

配置了两个地址池：1、2 地址范围分别是 11.1.1.1 到 11.1.1.20 和 22.1.1.1 到 22.1.1.20。

在 Ethernet0/0/0 配置了 2 个地址转换关联：ACL 规则 2011 与地址池 1 关联，进行一对一方式的地址转换；ACL 规则 2022 与地址池 2 关联，进行一对一方式的地址转换。

在 Ethernet0/0/0 配置了 2 个内部服务器：http://202.119.11.3:8080 的 www 服务器，内部地址是 5.5.5.5；ftp://202.119.11.3:2121 的 FTP 服务器，内部的地址是 5.5.5.5。

显示 NAT 的转换信息。

```
<H3C> display nat session
There are currently 40001 NAT sessions:

Protocol      GlobalAddr  Port      InsideAddr  Port        DestAddr  Port
       -  192.168.100.10   ---     192.168.1.5   ---             ---   ---
                 status: NOPAT,        TTL: 00:04:00,       Left: 00:04:00
       6  192.168.100.10  1024     192.168.1.5  1024   192.168.100.1  1025
                 status: NOPAT,        TTL: 00:01:00,       Left: 00:00:59
       6  192.168.100.10  2048     192.168.1.5  2048   192.168.100.1  2049
                 status: NOPAT,        TTL: 00:01:00,       Left: 00:01:00
       6  192.168.100.10  1025     192.168.1.5  1025   192.168.100.1  1026
                 status: NOPAT,        TTL: 00:01:00,       Left: 00:00:59
```

📖 **说明：**

当使用 No-PAT 转换方式时，通过 **display nat session** 命令查看 NAT 表项时，针对每个内网地址发起的多个连接转换，相应的会有多个 No-PAT 表项，如以上显示信息所示。这样保证了只有从内网向外网发起的连接才会被转换，对于由外网发起的连接将不被转换，提高了网络安全性。

3.1.10 display nat connection-limit

【命令】

display nat connection-limit [**source** *source-addr source-wildcard*] [**destination** *destination-addr destination-wildcard*] [**destination-port** { { **eq** | **neq** | **gt** | **lt** } *destination-port* | **range** *destination-port1 destination-port2* }] [**vpn-instance** *vpn-name*]

【视图】

任意视图

【参数】

nat：显示 NAT 创建的连接数信息。

source：指定源 IP 地址。

source-addr：源 IP 地址。

source-wildcard：源 IP 地址的掩码。

destination：指定目的 IP 地址。

destination-addr：目的 IP 地址。

destination-wildcard：目的 IP 地址掩码。

destination-port：指定目的端口号。

eq：显示目的端口号等于指定端口号的服务的连接数。

neq：显示目的端口号不等于指定端口号的服务的所有连接数。

gt：显示目的端口号大于指定端口号的服务的所有连接数。

lt：显示目的端口号小于指定端口号的服务的所有连接数。

range：显示目的端口号在指定范围内的服务的所有连接数。

destination-port：目的端口号。

destination-port1、*destination-port2*：按端口范围显示时的参数，分别表示服务端口的上下限。

vpn-instance：指定 VPN 实例。

vpn-name：VPN 实例的名称。

【描述】

display nat connection-limit 命令用来显示与 NAT 相关的连接数限制信息。

用户可以通过此命令，灵活的查看所关心的连接数信息。当该命令后面没有接任何参数时，将显示所有与 NAT 相关的连接数限制信息。

【举例】

显示所有与 NAT 相关的连接数限制信息。

```
[H3C] display nat connection-limit
```

3.1.11 limit

【命令】

limit *limit-id* **acl** *acl-number* [{ **per-source** | **per-destination** | **per-service** }* **amount** *upper-limit lower-limit*]

undo limit *limit-id*

【视图】

连接数限制策略视图

【参数】

limit-id：连接数限制策略的子规则编号，范围为 0～255。

acl：指定 ACL。连接数限制策略使用 ACL 来指定需要进行限制的连接的特征。使用 ACL 能够指定几乎所有特征的连接。

acl-number：指定的 ACL 编号，范围为 2000～3999。

per-source：指定按每个源地址方式分别进行限制。

per-destination：指定按每个目的地址方式分别进行限制。

per-service：指定按每个服务（目的端口）方式分别进行限制。

amount：标识配置的是连接数的限制，而非速率的限制。以后增加速率限制时方便添加速率标识。

upper-limit、*lower-limit*：指定此子规则的连接数上下限。此参数的作用是，当连接特征符合指定的规则时，使用这两个值对连接的建立进行限制。*upper-limit* 的取值范围是 1～4294967295，*lower-limit* 的取值范围是 0～4294967295。当连接数到达上限时，禁止新连接建立。此时，只有当连接数降低到小于等于下限时，才允许建立新连接。

【描述】

limit 命令用来在对应的连接数限制策略下创建规则。

undo limit 命令用来在对应的连接数限制策略下删除规则。

当某条规则已经与 NAT 绑定时，用户不能对该规则进行修改和删除，如果用户需要修改或删除该规则，必须先解除该规则与 NAT 的绑定。

通过定义连接限制策略规则的 ACL，不但可以限制 TCP 连接数量，也可以限制非 TCP 流量（如：UDP、ICMP）。如果只对 TCP 连接进行限制，需要在 ACL 中明确指定。

【举例】

在策略 1 下创建一个规则，使用 ACL3000，连接数上限为 100，下限为 10，对源地址进行限制。

```
[H3C] connection-limit policy 1
[H3C-connection-limit-policy-1] limit 0 acl 3000 per-source amount 100 10
```

3.1.12 nat address-group

【命令】

nat address-group *group-number start-addr end-addr*

undo nat address-group *group-number*

【视图】

系统视图

【参数】

group-number：地址池的编号，范围为 0～31 的整数。

start-addr：地址池的开始 IP 地址。

end-addr：地址池的结束 IP 地址。

【描述】

nat address-group 命令用来配置地址池，**undo nat address-group** 命令用来删除地址池。

地址池表示了一些外部 IP 地址的集合，如果 *start-addr* 和 *end-addr* 相同，表示只有一个地址。

⚠ 注意：

- 地址池长度（地址池中包含的所有地址个数）不能超过 255 个地址。
- 当某个地址池已经和某个访问控制列表关联进行地址转换，是不允许删除这个地址池的。
- NAT 地址池中的地址不应包含公网主机已使用的地址，否则会造成地址冲突。

【举例】

配置一个从 202.110.10.10 到 202.110.10.15 的地址池，地址池号为 1。

```
[H3C] nat address-group 1 202.110.10.10 202.110.10.15
```

3.1.13 nat aging-time

【命令】

nat aging-time { **default** | { **dns** | **ftp-ctrl** | **ftp-data** | **icmp** | **pptp** | **tcp** | **tcp-fin** | **tcp-syn** | **udp** } *seconds* }

【视图】

系统视图

【参数】

default：设置地址转换有效时间为系统缺省默认值。

dns：DNS 协议地址转换有效时间，缺省为 60 秒。

ftp-ctrl：FTP 协议控制链路地址转换有效时间，缺省为 7200 秒。

ftp-data：FTP 协议数据链路地址转换有效时间，缺省为 300 秒。

icmp：ICMP 协议地址转换有效时间，缺省为 60 秒。

pptp：PPTP 协议地址转换有效时间，缺省为 86400 秒。

tcp：TCP 协议地址转换有效时间，缺省为 86400 秒。

tcp-fin：TCP 协议 FIN 或 RST 连接地址转换有效时间，缺省为 60 秒。

tcp-syn：TCP 协议 SYN 连接地址转换有效时间，缺省为 60 秒。

udp：UDP 地址转换有效时间，缺省为 300 秒。

seconds：为一个时间值，单位为秒，取值范围为 10～86400（即 24 小时）。

【描述】

nat aging-time 命令用来设置地址转换连接的有效时间。

该命令设置地址转换连接的有效时间，针对不同的协议类型设定不同的时间。单位为秒。ALG 的默认老化时间和对应的应用有关，同时为防止攻击，首包老化时间设置为 5 秒。

【举例】

设定 TCP 协议的连接有效时间为 240 秒。

```
[H3C] nat aging-time tcp 240
```

3.1.14 nat alg

【命令】

nat alg { **dns** | **ftp** | **h323** | **ils** | **msn** | **nbt** | **pptp** | **tns** }

undo nat alg { **dns** | **ftp** | **h323** | **ils** | **msn** | **nbt** | **pptp** | **tns** }

【视图】

系统视图

【参数】

dns：支持 DNS 协议。

ftp：支持 FTP 协议。

h323：支持 H.323 协议。

ils：支持 ILS 协议。

msn：支持 MSN 协议。

nbt：支持 NBT 协议。

pptp：支持 PPTP 协议。

tns：支持 SQLNET 协议。

【描述】

nat alg 命令用来使能地址转换应用层网关功能，**undo nat alg** 命令用来禁用地址转换应用层网关功能。

缺省情况下，使能地址转换应用层网关功能。

【举例】

使能地址转换应用层网关功能，使 NAT 支持 FTP 应用。

```
[H3C] nat alg ftp
```

3.1.15 nat connection-limit-policy

【命令】

nat connection-limit-policy *policy-number*

undo nat connection-limit-policy *policy-number*

【视图】

系统视图

【参数】

policy-number：与 NAT 绑定的连接数限制策略编号，范围为 0～19。

【描述】

nat connection-limit-policy 命令用来指定与 NAT 绑定的连接数限制策略。

undo nat connection-limit-policy 命令用来取消与 NAT 绑定的连接数限制策略。

缺省情况下，策略和 NAT 未进行绑定。

nat connection-limit-policy 命令可重复配置，后面的配置将覆盖前面的配置。

【举例】

将策略 1 与 NAT 绑定。

```
[H3C] nat connection-limit-policy 1
```

3.1.16 nat dns-map

【命令】

nat dns-map *domain-name global-addr global-port* [**tcp** | **udp**]

undo nat dns-map *domain-name*

【视图】

系统视图

【参数】

domain-name：可被外部 DNS 服务器正确解析的合法域名。

global-addr：提供给外部网络访问的 IP 地址（一个合法的 IP 地址）。

global-port：提供给外部网络访问的服务的端口号。

tcp：表示 IP 协议承载的协议类型是 TCP。

udp：表示 IP 协议承载的协议类型是 UDP。

【描述】

nat dns-map 命令用来配置一条域名到外部 IP 地址、端口号、协议类型的映射，**undo nat dns-map** 命令用来删除一条域名到外部 IP 地址、端口号、协议类型的映射。

此命令用于配置内部服务器的“域名-外部 IP 地址、端口、协议类型”的映射，使内部主机在内部无 DNS 服务器的情况下，可以使用不同的域名区别并访问对应的内部服务器。

缺省情况下，未配置此类映射，此时内部主机的域名请求被外部 DNS 服务器解析得到外部 IP 地址后，只能映射到一台内部服务器上，无法实现内部主机使用不同的域名区别并访问其对应的内部服务器的功能。

最多允许配置 64 条映射。

【举例】

配置一条域名到外部 IP 地址、端口号、协议类型的映射。

```
[H3C] nat dns-map www.abc.com 202.112.0.1 80 tcp
```

3.1.17 nat match factor-all

【命令】

nat match factor-all

undo nat match factor-all

【视图】

系统视图

【参数】

无

【描述】

nat match factor-all 命令用来配置报文匹配方式为五元组匹配，**undo nat match factor-all** 命令用来配置报文匹配方式为三元组匹配。

缺省情况下，报文匹配方式为五元组匹配。

当匹配方式为三元组匹配时，创建的 UDP 协议的 NAT 表项将不包括目的地址和目的端口。

【举例】

配置报文匹配方式为三元组匹配。

```
[H3C] undo nat match factor-all
```

3.1.18 nat outbound *acl-number*

【命令】

nat outbound *acl-number* [**address-group** *group-number* [**no-pat**]]

undo nat outbound *acl-number* [**address-group** *group-number* [**no-pat**]]

【视图】

接口视图

【参数】

address-group：表示使用地址池的方式配置地址转换，如果不指定地址池，则直接使用该接口的 IP 地址作为转换后的地址，即 easy-ip 特性。

no-pat：表示使用多对多的地址转换，只转换数据包的地址而不转换端口信息。

acl-number：访问控制列表的索引值，范围为 2000～3999（可以使用高级 ACL）。

group-number：一个已经定义的地址池的编号。

【描述】

nat outbound *acl-number* 命令用来将一个访问控制列表 ACL 和一个地址池关联起来，表示 *acl-number* 中规定的地址可以使用地址池 *group-number* 进行地址转换，**undo nat outbound** *acl-number* 命令用来删除相应的地址转换。

通过配置访问控制列表和地址池的关联，将符合访问控制列表中的数据报文的源地址进行地址转换，选用地址池中的某个地址或者直接使用接口的 IP 地址进行转换。可以在同一个接口上配置不同的地址转换关联。使用对应的 **undo** 命令可以将相应的地址转换关联删除。该接口一般情况应该是和 ISP 连接，是内部网络的出口。

该命令如果不带 **address-group** 参数，即使用 **nat outbound** *acl-number* 命令，则实现了 easy-ip 的特性，地址转换时，使用接口的 IP 地址作为转换后的地址，利用访问控制列表控制哪些地址可以进行地址转换。

【举例】

允许 10.110.10.0/24 网段的主机进行地址转换，选用 202.110.10.10 到 202.110.10.12 之间的地址作为转换后的地址。假设 Ethernet 0/0/0 口连接 ISP。

```
[H3C] acl number 2001
[H3C-acl-basic-2001] rule permit source 10.110.10.0 0.0.0.255
[H3C-acl-basic-2001] rule deny
```

配置地址池。

```
[H3C] nat address-group 1 202.110.10.10 202.110.10.12
```

允许地址转换，使用地址池 1 中的地址进行地址转换。在转换的时候使用 TCP/UDP 的端口信息，使用如下配置。

```
[H3C-Ethernet0/0/0] nat outbound 2001 address-group 1
```

删除对应配置。

```
[H3C-Ethernet0/0/0] undo nat outbound 2001 address-group 1
```

如果使用一对一的地址转换（不使用 TCP/UDP 的端口信息进行地址转换），可以使用如下配置。

```
[H3C-Ethernet0/0/0] nat outbound 2001 address-group 1 no-pat
```

删除对应配置。

```
[H3C-Ethernet0/0/0] undo nat outbound 2001 address-group 1 no-pat
```

如果直接使用 Ethernet 0/0/0 口的 IP 地址，可以使用如下的配置。

```
[H3C-Ethernet0/0/0] nat outbound 2001
```

删除对应配置。

```
[H3C-Ethernet0/0/0] undo nat outbound 2001
```

3.1.19 nat outbound interface

【命令】

nat outbound *acl-number* **interface** *interface-type interface-number*

undo nat outbound *acl-number* **interface** *interface-type interface-number*

【视图】

接口视图

【参数】

acl-number：访问控制列表的索引值，范围为 2000～3999。

interface *interface-type interface-number*：指定接口类型及接口号，目前只支持指定 loopback 接口。

【描述】

nat outbound interface 命令将一个访问控制列表 ACL 和一个指定接口关联起来，并用使用指定接口地址作为转换后的地址，即将匹配访问控制列表的数据报文的源地址转换为指定接口的 IP 地址。**undo nat outbound interface** 命令用来删除访问控制列表和其他接口地址关联，即取消地址转换。

目前仅支持使用指定的 loopback 接口地址作为转换后的地址。

【举例】

使用 loopback0 接口地址作为转换后地址

```
[H3C] interface loopback0
[H3C-LoopBack0] ip address 202.38.160.106
```

```
[H3C-LoopBack0] quit
[H3C] acl number 2000
[H3C-acl-basic-2000] rule permit source 10.110.12.0 0.0.0.255
[H3C-acl-basic-2000] quit
[H3C] interface ethernet3/0/0
[H3C-Ethernet3/0/0] nat outbound 2000 interface loopback 0
```

3.1.20 nat outbound static

【命令】

nat outbound static

undo nat outbound static

【视图】

接口视图

【参数】

无

【描述】

nat outbound static 用来使 **nat static** 命令配置的 NAT 静态转换表项在接口上生效。**undo nat outbound static** 命令用来禁止在接口上配置的 NAT 静态转换表项生效。

【举例】

配置使 Ethernet0/0/0 接口上的 NAT 静态转换表项生效。

```
[H3C-Ethernet0/0/0] nat outbound static
```

3.1.21 nat overlapaddress

【命令】

nat overlapaddress *number overlappool-startaddress temppool-startaddress* { **pool-length** *pool-length* | **address-mask** *mask* }

undo nat overlapaddress *number*

【视图】

系统视图

【参数】

number：地址池对编号，取值范围为 0～7。

overlappool-startaddress：重叠地址池起始地址，各重叠地址池的地址不能有交集。

temppool-startaddress：临时地址池起始地址，各临时地址池的地址不能有交集。临时地址池里面的地址应该与内网及外网地址都不重叠。建议选择私网地址段，避免与公网地址重叠。

pool-length：地址池长度，以十进制表示。相互关联的重叠地址池与临时地址池长度相等，地址一一对应。

mask：地址池对应的子网掩码。

【描述】

nat overlapaddress 命令用于配置一个重叠地址池到一个临时地址池的映射。**undo nat overlapaddress** 命令用于取消已配置的映射。

📖 说明：

重叠地址池与临时地址池一一对应，转换规则为：

临时地址 = 临时地址池首地址 + （重叠地址 – 重叠地址池首地址）

重叠地址 = 重叠地址池首地址 + （临时地址 – 临时地址池首地址）

【举例】

配置一个从 171.69.100.0 到 192.168.0.0 的映射，地址池对编号为 0。

```
[H3C] nat overlapaddress 0 171.69.100.0 192.168.0.0 address-mask 24
```

3.1.22 nat server

【命令】

nat server [**vpn-instance** *vpn-instance-name*] **protocol** *pro-type* **global** { *global-addr* | **current-interface** | **interface** *type number* } [*global-port*] **inside** *host-addr* [*host-port*]

nat server [**vpn-instance** *vpn-instance-name*] **protocol** *pro-type* **global** { *global-addr* | **current-interface** | **interface** *type number* } *global-port1 global-port2* **inside** *host-addr1 host-addr2 host-port*

undo nat server [**vpn-instance** *vpn-instance-name*] **protocol** *pro-type* **global** { *global-addr* | **current-interface** | **interface** *type number* } [*global-port*] **inside** *host-addr* [*host-port*]

undo nat server [**vpn-instance** *vpn-instance-name*] **protocol** *pro-type* **global** { *global-addr* | **current-interface** | **interface** *type number* } *global-port1 global-port2* **inside** *host-addr1 host-addr2 host-port*

【视图】

接口视图

【参数】

vpn-instance-name：内部服务器所属 VPN 的虚拟路由转发实例。如果不设置该值，表示内部服务器属于一个普通的私网，不属于某一个 MPLS VPN。

global-addr：提供给外部访问的 IP 地址（一个合法的 IP 地址）。

global-port：提供给外部访问的服务的端口号。若忽略的话，将和 *host-port* 的值一致。

current-interface：使用安全网关当前公网接口的地址作为 NAT Server 的公网地址。

interface *type number*：指定使用其他接口的地址作为 NAT Server 的公网地址。目前仅支持 LoopBack 接口，且必须已在防火墙中配置。

host-addr：服务器在内部局域网的 IP 地址。

host-port：服务器提供的服务端口号，范围为 0～65535，常用的端口号可以用关键字代替。如：www 服务端口为 80，同时可以使用 **www** 代替。ftp 服务端口号为 21，同时可以使用 **ftp** 代替。如果为零，表示任何类型的服务都提供，可以用 **any** 关键字代替。如果没有配置这个参数，则表示是 **any** 的情况，相当于 *global-addr* 和 *host-addr* 之间有一个静态的连接。当 *host-port* 是 **any** 时候，*global-port* 也必须是 **any**，否则是非法配置。

global-port1、*global-port2*：通过两个端口指定一个端口范围，和内部的主机的地址范围构成一种对应关系。*global-port2* 必须大于 *global-port1*。

host-addr1、*host-addr2*：定义一组连续的地址范围，和前面定义的端口范围构成一一对应的关系。*host-addr2* 必须大于 *host-addr1*。该地址范围的数量必须和 *global-port1*、*global-port2* 定义的端口数量相同。

pro-type：表示 IP 协议承载的协议类型，可以使用协议号，也可用关键字代替。如：**icmp**（协议号为 1）、**tcp**（协议号为 6）、**udp**（协议号为 17）。

【描述】

nat server 命令用来定义一个内部服务器的映射表，用户可以通过 *global-addr* 和 *global-port* 定义的地址端口来访问地址和端口分别为 *host-addr* 和 *host-port* 的内部服务器。**undo nat server** 命令用来取消映射表。

通过该命令可以配置一些内部网络提供给外部使用的服务器，内部服务器可以位于普通的私网内，也可以位于 MPLS VPN 内。例如 www、ftp、telnet、pop3、dns 等等。

在一个接口下最多可以配置 256 条内部服务器转换命令，一个接口下最多可以配置 4096 个内部服务器，系统一共可以最多配置 1024 个内部服务器转换命令。如果配置端口范围的 nat server（即通过配置 *global-port1*、*global-port2* 指定一个端口范

围，和内部主机的地址范围构成一种对应关系），则对应配置多少端口，即为多少个内部服务器。

如果 *global-port* 和 *inside-port* 都为 0、any 或未配置的话，则内网服务器可以通过该配置访问公网，但发起访问的协议必须与配置的协议相同。

当使用端口范围配置 FTP 服务器的 NAT Server 时，内部端口号不能配置为 20 和 21；当不使用端口范围配置 FTP 服务器的 NAT Server 时，内部端口号不能配置为 20。

由于 TFTP 协议的特殊性，当配置 TFTP 服务器的 NAT Server 时，还应对内部的 TFTP 服务器配置相应的 **nat outbound** 命令。

配置该命令的接口应该是和 ISP 连接的，是内部网络的出口。

【举例】

指定局域网内部的 WWW 服务器的 IP 地址是 10.110.10.10，内部的 FTP 服务器的 IP 地址是 10.110.10.11，希望外部通过 http:// 202.110.10.10:8080 可以访问 web，通过 ftp://202.110.10.10 可以连接 FTP 站点。假设 Ethernet 0/0/0 和 ISP 连接。

```
[H3C-Ethernet0/0/0] nat server protocol tcp global 202.110.10.10 8080 inside 10.110.10.10 www
[H3C-Ethernet0/0/0] nat server protocol tcp global 202.110.10.10 inside 10.110.10.11 ftp
```

指定一个内部的主机 10.110.10.12，希望外部网络的主机可以利用 ping 202.110.10.11 命令 ping 通它。

```
[H3C-Ethernet0/0/0] nat server protocol icmp global 202.110.10.11 inside 10.110.10.12
```

用以下命令可以删除 WWW 服务器。

```
[H3C-Ethernet0/0/0] undo nat server protocol tcp global 202.110.10.10 8080 inside 10.110.10.10 www
```

用以下面命令可以删除内部的 FTP 服务器。

```
[H3C-Ethernet0/0/0] undo nat server protocol tcp global 202.110.10.11 8080 inside 10.110.10.11 ftp
```

指定一个外部地址 202.110.10.10，从端口 1001～1100 分别映射主机 10.110.10.1～10.110.10.100 的 telnet 服务。202.110.10.10:1001 访问 10.110.10.1，202.110.10:1002 访问 10.110.10.2。

```
[H3C-Ethernet0/0/0] nat server protocol tcp global 202.110.10.10 1001 1100 inside 10.110.10.1 10.110.10.100 telnet
```

指定使用 Dialer 0 接口获取的 IP 地址作为 NAT Server 的公网地址。

```
[H3C-Dialer0] nat server protocol tcp global current-interface 5000 inside 10.0.0.10 5000
```

3.1.23 nat session refresh-speed

【命令】

nat session refresh-speed level *level-value*

undo nat session refresh-speed

【视图】

系统视图

【参数】

level-value：地址转换表项的老化刷新速度等级，取值范围为 1～5，级别越高速度越快。

【描述】

nat session refresh-speed 命令用来调整地址转换表项的老化刷新速度等级。

undo nat session refresh-speed 命令用来恢复缺省等级。

缺省情况下，SecPath1000 的等级为 2，SecBlade 的等级为 3，其它 SecPath 安全网关设备的等级为 1。

【举例】

调整地址转换表项的老化刷新速度等级为 5 级。

```
[H3C] nat session refresh-speed level 5
```

3.1.24 nat static

【命令】

nat static *ip-addr1 ip-addr2*

undo nat static *ip-addr1 ip-addr2*

【视图】

系统视图

【参数】

ip-addr1：内部主机私有 IP 地址。

ip-addr2：全局 IP 地址。

【描述】

nat static 命令用来配置从内部地址到外部地址的一对一转换。**undo nat static** 命令用来删除已经配置的 NAT 一对一转换。

【举例】

配置内部私有 IP 地址到外部全局 IP 地址的一对一转换。

```
[H3C] nat static 192.168.1.1 2.2.2.2
```

3.1.25 nat static inside

【命令】

nat static inside ip *inside-address* **global ip** *global-address*

nat static inside ip *inside-start-address inside-end-address* **global ip** *global-address mask*

undo nat static inside ip *inside-address*

undo nat static inside ip *inside-address* **global ip** *global-address*

undo nat static inside ip *inside-start-address inside-end-address* [**global ip** *global-address mask*]

【视图】

系统视图

【参数】

inside-address：指定的静态表项需要转换的内网的地址。

inside-start-address：指定的静态表项需要转换的内网的起始地址。

inside- end-address：指定的静态表项需要转换的内网的结束地址。

global-address：指定的静态表项转化后的公网的网段地址。

mask：公网网段地址对应的子网掩码。

【描述】

nat static inside 命令用来配置网段转换静态表项的信息，使用该静态表项进行 NAT 转换时，只进行网段地址的转换，而保持主机地址不变。**undo nat static inside** 命令用来删除已经配置的静态表项。

其中 *global-address* 可以输入任何的地址，配置的 *global-address* 结果会根据输入的 *mask* 和掩码的长度对输入的 *global-address* 进行计算。

nat static inside 和 **nat static** 配置会创建两种不同的 NAT 静态表项，在具体的配置中，两种 NAT 静态表项不存在冲突即可。

缺省情况为没有配置任何静态表项。

【举例】

指定静态表项，将 10.1.1.1 到 10.1.1.100 保持主机地址不变 NAT 转换为 211.1.1.0 网段地址。

```
[H3C] nat static inside ip 10.1.1.1 10.1.1.100 global ip 211.1.1.0
255.255.255.0
```

3.1.26 reset nat

【命令】

reset nat { **log-entry** | **session** }

【视图】

用户视图

【参数】

log-entry：清除 NAT 日志缓冲区。

session：清除地址转换表信息。

【描述】

reset nat 命令用来清除内存中地址转换的映射表，释放动态分配的用于存放映射表的内存。

【举例】

清除 NAT 日志缓冲区。

```
<H3C> reset nat log-entry
```

清除地址转换表信息。

```
<H3C> reset nat session
```

第4章 防火墙配置命令

4.1 包过滤防火墙配置命令

4.1.1 debugging firewall packet-filter

【命令】

debugging firewall packet-filter { { **all** | **icmp** | **tcp** | **udp** | **fragments-inspect** | **others** } [**interface** *type number*] | **denied** | **permitted** }

undo debugging firewall packet-filter { { **all** | **icmp** | **tcp** | **udp** | **fragments-inspect** | **others** } [**interface** *type number*] | **denied** | **permitted** }

【视图】

用户视图

【参数】

all：有关全部的调试信息。

icmp：有关 ICMP 包过滤的调试信息。

tcp：有关 TCP 包过滤的调试信息。

udp：有关 UDP 包过滤的调试信息。

fragments-inspect：有关分片报文调试信息。

others：除了 ICMP、TCP、UDP 外其它所有类型的报文调试信息。

interface *type number*：经过该接口的相应数据包的调试信息，没有这个参数时，表示显示所有接口的调试信息。

denied：有关被禁止的数据包的调试信息。

permitted：有关被允许的数据包的调试信息。

【描述】

debugging firewall packet-filter 命令用来打开防火墙包过滤调试信息开关，**undo debugging firewall packet-filter** 命令用来关闭防火墙包过滤调试信息开关。

缺省设置是关闭包过滤防火墙全部调试信息开关。

相关配置可参考命令 **display debugging**。

【举例】

打开有关 UDP 包过滤的调试信息。

```
<H3C> debugging firewall packet-filter udp
```

4.1.2 debugging firewall packet-filter fragments-inspect events

【命令】

debugging firewall packet-filter fragments-inspect events

undo debugging firewall packet-filter fragments-inspect events

【视图】

用户视图

【参数】

无

【描述】

debugging firewall packet-filter fragments-inspect events 命令用来打开分片报文的检测事件信息的调试开关，**undo debugging firewall packet-filter fragments-inspect events** 命令用来关闭分片报文的检测事件信息的调试开关。

缺省情况下，关闭分片报文的检测事件信息的调试开关。

【举例】

打开分片报文的检测事件信息的调试开关。

```
<H3C> debugging firewall packet-filter fragments-inspect events
```

4.1.3 display firewall fragment

【命令】

display firewall fragment

【视图】

所有视图

【参数】

无

【描述】

display firewall fragment 命令用来显示防火墙的分片表。

【举例】

显示防火墙的分片表。

```
<H3C> display firewall fragment
```

4.1.4 display firewall packet-filter statistics

【命令】

display firewall packet-filter statistics { **all** | **interface** *type number* | **fragments-inspect** }

【视图】

所有视图

【参数】

all：表示显示所有接口的过滤报文统计信息。

interface *type number*：接口类型及接口号，表示显示某接口的过滤报文统计信息。

fragments-inspect：显示分片报文检测统计信息。

【描述】

display firewall packet-filter statistics 命令用来显示包过滤防火墙的统计信息。

【举例】

显示分片报文检测信息。

```
[H3C] display firewall packet-filter statistics fragments-inspect
  Fragments inspection is enabled.
  The high-watermark for clamping is 10000.
  The low-watermark for clamping is 1000.
  Current records for fragments inspection is 0.
```

4.1.5 firewall packet-filter default

【命令】

firewall packet-filter default { **permit** | **deny** }

【视图】

系统视图

【参数】

permit：默认过滤规则为允许。

deny：默认过滤规则为禁止。

【描述】

firewall packet-filter default 命令用来设置包过滤防火墙的缺省过滤方式为“允许”或“禁止”。

当防火墙工作在透明模式下，若缺省过滤方式为 deny，除了绑定编号为 4000～4999 的以太帧 ACL 外，还需要绑定编号为 1000～1999 的接口 ACL，才能正常转发报文。

系统缺省为拒绝任何报文通过。

【举例】

设置防火墙缺省过滤规则为允许。

```
[H3C] firewall packet-filter default permit
```

4.1.6 firewall packet-filter enable

【命令】

firewall packet-filter enable

undo firewall packet-filter enable

【视图】

系统视图

【参数】

无

【描述】

firewall packet-filter enable 命令用来启用包过滤防火墙功能，命令 **undo firewall packet-filter enable** 用来关闭包过滤防火墙功能。

缺省情况下，SecPath 系列防火墙启用包过滤防火墙功能，SecPath 系列安全网关禁止包过滤防火墙功能。

【举例】

禁止防火墙包过滤防火墙功能。

```
[H3C] undo firewall packet-filter enable
```

4.1.7 firewall packet-filter fragments-inspect

【命令】

firewall packet-filter fragments-inspect

undo firewall packet-filter fragments-inspect

【视图】

系统视图

【参数】

无

【描述】

firewall packet-filter fragments-inspect 命令用来打开分片报文检测开关，**undo firewall packet-filter fragments-inspect** 命令用来关闭分片报文检测开关。

缺省情况下，分片检测开关为关闭。

此命令是实现精确匹配的前提。只有打开分片检测开关，才能进行分片报文的精确匹配。这时，包过滤防火墙将记录分片报文的状态，根据高级 ACL 规则对三层（IP 层）以外的信息进行精确匹配。

包过滤防火墙对分片报文的状态记录需要消耗系统资源。如果不使用精确匹配模式，则可以关闭此功能，以提高系统运行效率，减小系统开销。

只有打开了分片报文检测开关，精确匹配模式才能真正有效。

相关配置可参考命令 **firewall packet-filter**（接口视图）。

【举例】

打开分片检测开关。

```
[H3C] firewall packet-filter fragments-inspect
```

4.1.8 firewall packet-filter fragments-inspect { high | low }

【命令】

firewall packet-filter fragments-inspect { **high** | **low** } { **default** | *number* }

undo firewall packet-filter fragments-inspect { **high** | **low** }

【视图】

系统视图

【参数】

high *number*：指定上限分片状态记录数目，取值范围是 100～10000。

low *number*：指定下限分片状态记录数目，取值范围是 100～10000。

default：记录分片状态的缺省数目。上限分片状态记录数目（**high**）缺省值为 2000。下限分片状态记录数目（**low**）缺省值为 1500。

【描述】

firewall packet-filter fragments-inspect { **high** | **low** }命令用来配置分片报文检测的上、下门限值，**undo firewall packet-filter fragments-inspect** { **high** | **low** }命令用来恢复上、下门限值为缺省值。

如果打开分片检测开关，应用精确匹配过滤后，包过滤的执行效率会略微降低，配置的匹配项目越多，效率降低越多。因此，需要设定门限值（最大允许上、下限域值）。当记录状态数达到上限时，将删除最先保存的状态项直至下限值。

下限值必须小于或等于上限值。

相关配置可参考命令 **display firewall packet-filter statistics fragments-inspect**，**firewall packet-filter fragments-inspect**。

【举例】

配置检测上限 3000，下限为缺省值。

```
[H3C] firewall packet-filter fragments-inspect high 3000
[H3C] firewall packet-filter fragments-inspect low default
```

4.1.9 firewall packet-filter *acl-number*

【命令】

firewall packet-filter *acl-number* { **inbound** | **outbound** } [**match-fragments** { **normally** | **exactly** }]

undo firewall packet-filter *acl-number* { **inbound** | **outbound** }

【视图】

接口视图

【参数】

acl-number：ACL 的序号。

inbound：过滤从接口收到的数据包。

outbound：过滤从接口发送的数据包。

match-fragments：指定分片的匹配模式，只有高级访问控制列表有此参数。

normally：标准匹配模式，此模式为缺省模式，只有高级访问控制列表有此参数。

exactly：精确匹配模式，只有高级访问控制列表有此参数。

【描述】

firewall packet-filter *acl-number* 命令用来将访问控制列表应用到相应的接口上，**undo firewall packet-filter** *acl-number* 命令用来删除相应的设置。

基于接口的访问控制列表（即序号为 1000 到 1999 的 ACL）只能用参数 **outbound**。

接口访问控制列表用来匹配从特定接口接收到的报文，然后允许或拒绝匹配的报文从某接口（包括接收报文的接口）发送出去。

Comware 平台的包过滤提供了对分片报文过滤的功能，可以对所有的分片报文进行三层（IP 层）的匹配过滤（例如基于源、目的 IP 地址）；同时，对于包含扩展信息

的高级 ACL 规则（例如包含 TCP/UDP 端口号，ICMP 类型等），提供标准匹配和精确匹配两种匹配方式。标准匹配即三层信息的匹配，匹配将忽略三层以外的信息；精确匹配则对所有的高级 ACL 的过滤规则进行匹配，这就要求防火墙必须记录首片分片报文的状态以获得完整的后续分片的匹配信息。

缺省的模式为标准匹配方式。

只有在启用包过滤防火墙功能后，在接口上应用的访问控制列表才能生效。

相关配置可参考命令 **acl**，**display acl**，**firewall packet-filter enable**，**firewall packet-filter fragments-inspect**。

【举例】

在接口 Ethernet1/0/0 应用访问控制列表 3001，过滤接口发送的报文。

```
[H3C-Ethernet1/0/0] firewall packet-filter 3001 outbound
```

4.1.10 reset firewall packet-filter statistics

【命令】

reset firewall packet-filter statistics { **all** | **interface** *type number* }

【视图】

用户视图

【参数】

all：表示清除所有接口的过滤报文统计信息。

interface：表示清除某接口的过滤报文统计信息。

type number：接口类型及接口号。

【描述】

reset firewall packet-filter statistics 命令用来清除包过滤防火墙的统计信息。

【举例】

清除接口 Ethernet 1/0/0 的接口过滤报文统计信息。

```
<H3C> reset firewall packet-filter statistics interface Ethernet1/0/0
```

4.2 状态防火墙配置命令

4.2.1 aging-time

【命令】

aging-time { **syn** | **fin** | **tcp** | **udp** } *seconds*

undo aging-time { **syn** | **fin** | **tcp** | **udp** }

【视图】

ASPF 策略视图

【参数】

seconds：用于指定在检测到 SYN 和 FIN 报文或者 TCP 和 UDP 协议时，会话表项的空闲超时时间的缺省值。

【描述】

aging-time 命令用来配置 TCP 的 SYN 状态等待超时值、FIN 状态等待超时值，以及 TCP 和 UDP 会话表项空闲状态超时值的缺省值，**undo aging-time** 命令用来恢复超时缺省值。

在超时时间以内，系统会保留所建立的连接和会话。

缺省情况下，SYN、FIN、TCP、UDP 的超时时间分别为 30s、30s、3600s 和 30s。

相关配置可参考命令 **display aspf all**，**display aspf policy**，**display aspf session**，**display aspf interface**。

【举例】

配置 TCP 的 SYN 状态等待时间超时值为 20 秒。

```
[H3C-aspf-policy-1] aging-time syn 20
```

配置 TCP 的 FIN 状态等待时间超时值为 10 秒。

```
[H3C-aspf-policy-1] aging-time fin 10
```

配置 TCP 空闲时间超时值为 3000 秒。

```
[H3C-aspf-policy-1] aging-time tcp 3000
```

设置 UDP 空闲超时值为 110 秒。

```
[H3C-aspf-policy-1] aging-time udp 110
```

4.2.2 aspf-policy

【命令】

aspf-policy *aspf-policy-number*

undo aspf-policy *aspf-policy-number*

【视图】

系统视图

【参数】

aspf-policy-number：ASPF 策略号，范围为 1～99。

【描述】

命令 **aspf-policy** 用来定义一个 ASPF 策略。对于一个已定义的 ASPF 策略，可通过策略号对该策略进行引用。

【举例】

定义一个 ASPF 策略，并进入该 ASPF 策略视图。

```
[H3C] aspf-policy 1
[H3C-aspf-policy-1]
```

4.2.3 debugging aspf

【命令】

debugging aspf { **all** | **verbose** | **events** | **ftp** | **h323** | **rtsp** | **session** | **smtp** | **sqlnet** | **tcp** | **timers** | **udp** }

undo debugging aspf { **all** | **verbose** | **events** | **ftp** | **h323** | **rtsp** | **session** | **smtp** | **sqlnet** | **tcp** | **timers** | **udp** }

【视图】

用户视图

【参数】

all：所有 ASPF 调试开关。

verbose：详细功能调试开关。

events：事件调试开关。

ftp：FTP 检测信息调试开关。

h323：H.323 检测信息调试开关。

rtsp：RTSP 检测信息调试开关。

session：会话信息调试开关。

smtp：SMTP 检测信息调试开关。

sqlnet：SQLNET 检测信息调试开关。

tcp：TCP 检测信息调试开关。

timers：计时器信息调试开关。

udp：UDP 检测信息调试开关。

【描述】

debugging aspf 命令用来打开 ASPF 调试信息开关，**undo debugging aspf** 命令用来关闭 ASPF 调试信息开关。

缺省情况下，关闭 ASPF 全部调试信息开关。

相关配置可参考命令 **display aspf all**，**display aspf policy**，**display aspf session**，**display aspf interface**。

【举例】

打开 ASPF 所有的调试开关。

```
<H3C> debugging aspf all
```

4.2.4 debugging aspf http

【命令】

debugging aspf http { **java-blocking** | **activex-blocking** } { **all** | **error** | **event** | **filter** | **packet** }

undo debugging aspf http { **java-blocking** | **activex-blocking** } { **all** | **error** | **event** | **filter** | **packet** }

【视图】

用户视图

【参数】

java-blocking：Java Applet 阻断调试开关。

activex-blocking：ActiveX 控件阻断调试开关。

all：所有调试功能。

error：错误调试功能。

event：事件调试功能。

filter：过滤调试功能。

packet：报文调试功能。

【描述】

debugging aspf http java-blocking 命令用来打开 HTTP 检测的 Java Applet 阻断调试开关，**undo debugging aspf http java-blocking** 命令用来关闭 HTTP 检测的 Java Applet 阻断调试开关。

debugging aspf http activex-blocking 命令用来打开 HTTP 检测的 ActiveX 控件阻断调试开关，**undo debugging aspf http activex-blocking** 命令用来关闭 HTTP 检测的 ActiveX 控件阻断调试开关。

缺省情况下，未打开 HTTP 检测的 Java Applet 阻断和 ActiveX 控件阻断调试开关。

【举例】

打开 Java Applet 阻断功能的所有调试开关。

```
<H3C> debugging aspf http java-blocking all
```

4.2.5 detect

【命令】

detect *protocol* [**acl** *number*] [**aging-time** *seconds*]

undo detect *protocol* [**acl** *number*]

【视图】

ASPF 策略视图

【参数】

protocol：ASPF 支持的协议名称。应用层协议包括：FTP、HTTP、H323、SMTP、SNMP、RTSP、SQLNET；传输层协议包括：TCP、UDP。

number：ACL 编号，范围为 1000～3999。当 *protocol* 为 FTP、SMTP 和 SNMP 时，支持 **acl** 选项。

seconds：配置协议空闲的超时时间，取值范围是 5～43200 秒，应用层协议的超时时间缺省值为 3600 秒。基于 TCP 协议的超时时间缺省值为 3600 秒；基于 UDP 协议的超时时间缺省值为 30 秒。

【描述】

detect 命令用来为应用层协议指定 ASPF 策略，**undo detect** 命令用来取消所做的配置。

当协议类型为 HTTP 时，允许 Java Applet 阻断和 ActiveX 控件阻断。

如果同时配置了应用层协议检测和通用 TCP/UDP 检测，应用层协议检测优先于通用 TCP/UDP 检测。

ASPF 使用超时时间去管理协议的会话状态信息，以便决定何时终结一个会话状态信息的管理或删除一个不能正常建立的会话。设置超时时间是一个全局的配置，适用于所有的会话，可以保护系统资源不被恶意占用。

相关配置可参考命令 **display aspf all**，**display aspf policy**，**display aspf session**，**display aspf interface**。

【举例】

配置对 FTP 协议指定 ASPF 策略，策略号为 1。

```
[H3C] aspf-policy 1
[H3C-aspf-policy-1] detect ftp
```

4.2.6 detect http

【命令】

detect http [**java-blocking** [*acl-number1*] | **activex-blocking** [*acl-number2*]]* [**aging-time** *seconds*]

undo detect http [**java-blocking** | **activex-blocking**]*

【视图】

ASPF 策略视图

【参数】

java-blocking：阻断 Java Applet。

acl-number1：基本访问控制列表（ACL）号，取值范围是 2000～2999。若不指定，则表示阻断所有的 Jave Applet。

activex-blocking：阻断 ActiveX 控件。

acl-number2：基本访问控制列表（ACL）号，取值范围是 2000～2999。若不指定，则表示阻断所有的 ActiveX 控件。

seconds：配置协议空闲的超时时间，取值范围是 5～43200 秒，应用层协议的超时时间缺省值为 3600 秒。基于 TCP 协议的超时时间缺省值为 3600 秒；基于 UDP 协议的超时时间缺省值为 30 秒。

【描述】

detect http 命令用来配置检测 HTTP 协议，并且可以配置对 Jave Applet 和 ActiveX 控件进行阻断，**undo detect http** 命令用来取消检测 HTTP。

目前 Java 阻断功能只能过滤 HTTP 请求中以“.class”为后缀的 Java 请求。

缺省情况下，不对 HTTP 进行检测。

【举例】

配置 ASPF 策略，检测 HTTP，并阻断所有的 ActiveX 控件和来自服务器 10.1.1.1 的 Java Applet。

```
[H3C] acl number 2000
[H3C-acl-basic-2000] rule permit source 10.1.1.1 0
[H3C-acl-basic-2000] rule deny source any
[H3C-acl-basic-2000] quit
[H3C] aspf-policy 1
[H3C-aspf-policy-1] detect http activex-blocking java-blocking 2000
```

4.2.7 display aspf all

【命令】

display aspf all

【视图】

所有视图

【参数】

无

【描述】

display aspf all 命令用来显示所有的 ASPF 策略和会话信息。

【举例】

下面是 **display aspf all** 命令的输出信息。

```
[H3C] display aspf all
[ASPF Policy Configuration]
  Policy Number 1:
    Log:                 disable
    SYN timeout:         30    s
    FIN timeout:         30    s
    TCP timeout:         3600  s
    UDP timeout:         30    s
    Detect Protocols:
      h323 timeout 3600
      rtsp timeout 3600
      http  timeout 3600
      smtp timeout 3600
      ftp  timeout 3600
      tcp  timeout 3600
      udp  timeout 30

[Interface Configuration]
   Interface                     InboundPolicy   OutboundPolicy
 ----------------------------------------------------------------
   Ethernet0/0/1                 none            1
```

表4-1 ASPF 配置信息显示描述表

域名	描述
Log	表示是否开会话日志功能
SYN timeout	TCP 连接的 SYN 状态超时值为 30 秒
FIN timeout	TCP 连接的 FIN 状态超时值为 5 秒
TCP timeout	TCP 会话的空闲时间超时值为 3600 秒
UDP timeout	UDP 会话的空闲时间超时值为 30 秒
Detect Protocols	ASPF 策略所检测的协议
InboundPolicy	入方向的 ASPF 策略
OutboundPolicy	出方向的 ASPF 策略

4.2.8 display aspf interface

【命令】

display aspf interface

【视图】

所有视图

【参数】

无

【描述】

display aspf interface 命令用来显示接口上配置的 ASPF 策略。

【举例】

下面是 **display aspf interface** 的输出。

```
[H3C] display aspf interface
[Interface Configuration]
   Interface                      InboundPolicy   OutboundPolicy
 ----------------------------------------------------------------
   Ethernet0/0/1                  none            1
```

表4-2 ASPF 接口配置信息显示描述表

域名	描述
InboundPolicy	入方向的 ASPF 策略
OutboundPolicy	出方向的 ASPF 策略

4.2.9 display aspf policy

【命令】

display aspf policy *aspf-policy-number*

【视图】

所有视图

【参数】

aspf-policy-number：ASPF 策略号，范围为 1～99。

【描述】

display aspf policy 命令用来显示一个特定 ASPF 策略。

【举例】

显示策略号为 1 的 ASPF 策略的配置信息。

```
[H3C] display aspf policy 1
[ASPF Policy Configuration]
  Policy Number 1:
    Log:                 disable
    SYN timeout:         30    s
    FIN timeout:         30    s
    TCP timeout:         3600  s
    UDP timeout:         30    s
    Detect Protocols:
      h323 timeout 3600
      rtsp timeout 3600
      http  timeout 3600
      smtp timeout 3600
      ftp  timeout 3600
      tcp  timeout 3600
      udp  timeout 30
```

以上显示信息中的描述请参见 表 4-1。

4.2.10 display aspf session

【命令】

display aspf session [**verbose**]

【视图】

所有视图

【参数】

verbose：显示会话表项的详细信息。

【描述】

display aspf session 命令用来显示 ASPF 的会话。

display aspf session 命令和 **display firewall session table** 命令显示的是两个会话表，这两个会话表的默认老化时间是不同的。对于同一条数据流，有可能在 ASPF 会话表中仍然存在，而在防火墙会话表中已经老化不存在，反之亦然。

【举例】

显示当前 ASPF 会话的相关信息。

```
[H3C] display aspf session

Total session number:2
Syn-list session number:0
Fin-list session munber:0


There are 2 ASPF sessions:

[Established Sessions]
Session Initiator             Responder             Application     Status
------------------------------------------------------------------------------
2637F904 172.16.1.2:20        192.168.1.2:1027     ftp-data       TCP_READY
263A2A04 192.168.1.2:1025     172.16.1.2:21       ftp           FTP_CONXN_UP
```

显示当前 ASPF 会话的详细信息。

```
[H3C] display aspf session verbose

Total session number:2
Syn-list session number:0
Fin-list session munber:0


There are 2 ASPF sessions:

 [Session 0x263A30C4]
   Initiator: 172.16.1.2:20          Responder: 192.168.1.2:1029
   Application protocol: ftp-data    Status: TCP_READY
   Transport protocol: 6             Port: 1029
   Child: 0x0                        Parent: 0x263A2A04
   Interface: GigabitEthernet0/1     Direction: inbound
```

```
  Timeout 01:00:00                  Time left 00:59:55
  Initiator Bytes/Packets sent: 0/0
  Responder Bytes/Packets sent: 9058/21
  Initiator tcp SeqNumber/AckNumber: 0/0
  Responder tcp SeqNumber/AckNumber: 2509472405/1518475561
[Session 0x263A2A04]
  Initiator: 192.168.1.2:1025       Responder: 172.16.1.2:21
  Application protocol: ftp         Status: FTP_CONXN_UP
  Transport protocol: 6             Port: 21
  Child: 0x263A30C4                 Parent: 0x0
  Interface: GigabitEthernet0/1     Direction: outbound
  Timeout 01:00:00                  Time left 00:59:55
  Initiator Bytes/Packets sent: 1302/26
  Responder Bytes/Packets sent: 1387/22
  Initiator tcp SeqNumber/AckNumber: 3350738362/3348472065
  Responder tcp SeqNumber/AckNumber: 3348472011/3350738362
```

4.2.11 display aspf statistics

【命令】

display aspf statistics

【视图】

任意视图

【参数】

无

【描述】

display aspf statistics 命令用来显示 ASPF 的统计信息。

【举例】

显示 ASPF 的统计信息。

```
<H3C> display aspf statistics
ASPF Syn list full occur times:0
ASPF Hash list full occur times:0
ASPF Tacl list full occur times:0
ASPF Session table full occur times:0
ASPF Fin list error occur times:0
```

4.2.12 display firewall session aging-time

【命令】

display firewall session aging-time

【视图】

所有视图

【参数】

无

【描述】

display firewall session aging-time 命令用来显示所有协议的会话超时时间。

相关配置命令请参考 **firewall session aging-time**，**firewall session aging-time default**。

【举例】

显示所有协议的会话超时时间。

```
[H3C] display firewall session aging-time
Firewall aging-time value information:
       tcp ---- aging-time value is    240 (seconds)
       udp ---- aging-time value is     40 (seconds)
      icmp ---- aging-time value is     20 (seconds)
    finrst ---- aging-time value is     10 (seconds)
       syn ---- aging-time value is      5 (seconds)
  fragment ---- aging-time value is      5 (seconds)
     h.323 ---- aging-time value is    600 (seconds)
       ftp ---- aging-time value is    600 (seconds)
       ras ---- aging-time value is    600 (seconds)
      http ---- aging-time value is    240 (seconds)
      smtp ---- aging-time value is     40 (seconds)
      rtsp ---- aging-time value is    240 (seconds)
    telnet ---- aging-time value is    240 (seconds)
   netbios ---- aging-time value is    240 (seconds)
```

4.2.13 display firewall session table

【命令】

display firewall session table [**verbose**] [**source** *ip-address*] [**destination** *ip-address*]

【视图】

所有视图

【参数】

verbose：显示详细信息。

source *ip-address*：会话的源 IP 地址。

destination *ip-address*：会话的目的 IP 地址。

【描述】

display firewall session table 命令用来显示防火墙的会话表。

display firewall session table 命令和 **display aspf session** 命令显示的是两个会话表，这两个会话表的默认老化时间是不同的。对于同一条数据流，有可能在 ASPF 会话表中仍然存在，而在防火墙会话表中已经老化不存在，反之亦然。

防火墙会话老化后将会有一个 timeout 状态，从 timeout 状态到会话被删除会有一定的时间间隔，该时间间隔因实际组网应用而异。

【举例】

显示防火墙的会话表。

```
[H3C] display firewall session table
Total session number: 12
HTTP:192.168.4.1:80<--192.168.4.8:3391
HTTP:192.168.4.1:80<--192.168.4.8:3392
HTTP:192.168.4.1:80<--192.168.4.8:3387
NBT datagram:192.168.4.255:138<--192.168.4.8:138
HTTP:192.168.4.1:80<--192.168.4.8:3396
NBT name:192.168.4.255:137<--192.168.4.8:137
HTTP:192.168.4.1:80<--192.168.4.8:3389
HTTP:192.168.4.1:80<--192.168.4.8:3398
HTTP:192.168.4.1:80<--192.168.4.8:3397
HTTP:192.168.4.1:80<--192.168.4.8:3393
HTTP:192.168.4.1:80<--192.168.4.8:3390
HTTP:192.168.4.1:80<--192.168.4.8:3395
```

4.2.14 display port-mapping

【命令】

display port-mapping [*application-name* | **port** *port-number*]

【视图】

所有视图

【参数】

application-name：指定用于端口映射的应用的名称。可选的应用有：FTP、HTTP、H.323、SMTP、RTSP。

port-number：端口号，范围为 0～65535。

【描述】

命令 **display port-mapping** 用来显示用户定义的端口映射情况。

相关配置可参考命令 **port-mapping**。

【举例】

显示端口映射的所有信息。

```
[H3C] display port-mapping
  SERVICE    PORT       ACL        TYPE
 -------------------------------------------------
  ftp          21                   system defined
  smtp         25                   system defined
  http         80                   system defined
  rtsp        554                   system defined
  h323       1720                   system defined
  sqlnet     1521                   system defined
```

4.2.15 firewall aspf

【命令】

firewall aspf *aspf-policy-number* { **inbound** | **outbound** }

undo firewall aspf *aspf-policy-number* { **inbound** | **outbound** }

【视图】

接口视图

【参数】

aspf-policy-number：在接口上使用的 ASPF 策略号。

inbound：对接口的入方向的报文应用 ASPF 策略。

outbound：对接口的出方向的报文应用 ASPF 策略。

【描述】

firewall aspf 命令用来在一个接口的指定方向上应用 ASPF 策略，**undo firewall aspf** 命令用来删除该接口的指定方向上应用的 ASPF 策略。

对 ASPF 策略，有两个概念：内部接口和外部接口。如果防火墙连接了内部网和 Internet，并且防火墙要通过部署 ASPF 来保护内部网的服务器，则防火墙上与内部网连接的接口就是内部接口，与 Internet 相连的接口就是外部接口。

【举例】

接口 ethernet1/0/0 的出方向上配置 ASPF 防火墙功能。

```
[H3C-Ethernet1/0/0] firewall aspf 1 outbound
```

4.2.16 firewall session aging-time

【命令】

firewall session aging-time { **fin-rst** | **fragment** | **ftp** | **h323** | **http** | **icmp** | **netbios** | **ras** | **rtsp** | **smtp** | **syn** | **tcp** | **telnet** | **udp** } { **default** | *seconds* }

【视图】

系统视图

【参数】

default：设置协议的超时时间为缺省值。

seconds：协议的超时时间，单位为“秒”。

各种协议的缺省超时时间如下：

fin-rst：10 秒

fragment：5 秒

ftp：3600 秒

h323：10800 秒

http：600 秒

icmp：20 秒

netbios：240 秒

ras：1200 秒

rtsp：14400 秒

smtp：600 秒

syn：5 秒

tcp：14400 秒

telnet：14400 秒

udp：120 秒

【描述】

firewall session aging-time 命令用来设置各种协议的会话表的超时时间。

请勿将 syn 的超时时间配置为与 fin-rst 或 tcp 的超时时间相同，否则表项的时间更新会失败。

相关配置命令请参考 **firewall session aging-time default**，**display firewall session aging-time**。

【举例】

设置 HTTP 协议的超时时间为 1200 秒。

```
[H3C] firewall session aging-time http 1200
```

4.2.17 firewall session aging-time default

【命令】

firewall session aging-time default

【视图】

系统视图

【参数】

无

【描述】

firewall session aging-time default 命令用来将所有协议的超时时间恢复到缺省值。

相关配置命令请参考 **firewall session aging-time**，**display firewall session aging-time**。

【举例】

设置所有协议的超时时间为缺省值。

```
[H3C] firewall session aging-time default
```

4.2.18 log enable

【命令】

log enable

undo log enable

【视图】

ASPF 策略视图

【描述】

log enable 命令用来使能 ASPF 的会话日志功能，**undo log enable** 命令用来关闭日志功能。

缺省情况下，关闭会话日志功能。

ASPF 提供了增强的会话日志功能。可以对所有的连接进行记录，记录包括连接的时间、源地址、目的地址、使用的端口和传输的字节数。

相关配置可参考命令 **display aspf all**，**display aspf policy**，**display aspf session**，**display aspf interface**。

【举例】

使能 ASPF 会话日志功能。

```
[H3C-aspf-policy-1] log enable
```

4.2.19 port-mapping

【命令】

port-mapping *application-name* **port** *port-number* [**acl** *acl-number*]

undo port-mapping [*application-name* **port** *port-number* [**acl** *acl-number*]]

【视图】

系统视图

【参数】

application-name：应用协议的名称。可选的应用协议有：FTP、HTTP、H.323、SMTP、RTSP、SQLNET。

port-number：端口号范围为 0～65535。

acl-number：基本访问列表号，范围为 2000～2999。

【描述】

port-mapping 命令用来建立端口到应用层协议的映射，**undo port-mapping** 命令用来删除端口映射项。

当配置监听非标准端口的应用层协议检测时（如 HTTP 监听的端口号为 8080，而非标准的端口号 80），需使用此命令配置相应的端口映射，以使 ASPF 状态检测正常工作。

有两类映射机制：通用端口映射和基于基本访问控制列表（ACL）的主机端口映射。

通用端口映射是将用户自定义端口号和应用层协议建立映射关系；例如：将 8080 端口映射为 HTTP 协议，这样所有目标端口是 8080 的 TCP 报文被认为是 HTTP 报文。基于基本访问控制列表（ACL）的主机端口映射是对来自某些特定主机的报文建立自定义端口号和应用协议的映射，例如：将去往 1.1.0.0 网段的使用 8080 端口的 TCP 报文映射为 HTTP 报文。主机的范围由基本的 ACL 指定。

相关配置可参考命令 **display port-mapping**。

【举例】

设置 FTP 协议使用端口 3456。

```
[H3C] port-mapping ftp port 3456
```

4.2.20 reset aspf session

【命令】

reset aspf session

【视图】

用户视图

【参数】

无

【描述】

reset aspf session 命令用来清除 ASPF 的会话信息。

【举例】

清除 ASPF 的会话信息。

```
<H3C> reset aspf session
```

4.2.21 reset aspf statistic http

【命令】

reset aspf statistic http [**java-blocking** | **activex-blocking**]

【视图】

用户视图

【参数】

java-blocking：清除 HTTP 的 Java 阻断的统计信息。

activex-blocking：清除 HTTP 的 ActiveX 阻断的统计信息。

【描述】

reset aspf statistic http 命令用来清除 HTTP 的 Java 阻断和 ActiveX 阻断的统计信息。

若不指定参数，则同时清除 Java 阻断和 ActiveX 阻断的统计信息。

【举例】

清除 Java 阻断的统计信息。

```
<H3C> reset aspf statistic http java-blocking
```

4.2.22 reset firewall session table

【命令】

reset firewall session table

【视图】

用户视图

【参数】

无

【描述】

reset firewall session table 命令用来清除防火墙的会话表信息。

【举例】

清除防火墙的会话表信息。

```
<H3C> reset firewall session table
```

4.3 黑名单配置命令

4.3.1 debugging firewall blacklist

【命令】

debugging firewall blacklist { **all** | **item** | **packet** }

undo debugging firewall blacklist { **all** | **item** | **packet** }

【视图】

用户视图

【参数】

all：显示全部调试信息。

item：显示黑名单表项变化调试信息。

packet：显示报文中黑名单表项调试信息。

【描述】

debugging firewall blacklist 命令用来打开防火墙黑名单功能调试开关， **undo debugging firewall blacklist** 命令用来关闭防火墙黑名单功能调试信息开关。

缺省情况关闭防火墙全部调试信息开关。

相关配置可参考命令 **display debugging**。

【举例】

打开黑名单表项的全部调试信息。

```
<H3C> debugging firewall blacklist all
```

4.3.2 display firewall blacklist

【命令】

display firewall blacklist { **enable** | **item** [*sour-addr*] }

【视图】

所有视图

【参数】

enable：显示黑名单功能运行状况。

item *sour-addr*：显示黑名单表项内容。*sour-addr* 为表项的 IP 地址。

【描述】

display firewall blacklist 命令用来显示防火墙黑名单功能的运行状况和黑名单表项信息。参数 **item** [*sour-addr*]显示黑名单表项信息。如果不指定 IP 地址，显示当前全部黑名单表项的概要信息。如果指定了要显示的 IP 地址，显示特定黑名单表项的详细信息。

【举例】

显示全部黑名单表项概要信息。

```
<H3C> display firewall blacklist item
Firewall blacklist item :
 Current manual insert items : 3
 Current automatic insert items : 0
 Need aging items : 2
```

```
 IP Address      Insert reason    Insert time            Age time(minutes)

--------------------------------------------------------------------------
 10.10.2.2       Manual           2005/11/21 10:39:49     Permanent
 192.168.1.1     Manual           2005/11/21 10:38:48     15
 10.0.0.1        Manual           2005/11/21 10:39:04     30
```

显示特定黑名单表项详细信息。

```
<H3C> display firewall blacklist item 192.168.1.1
Firewall blacklist item : 192.168.1.1
 Insert reason : Manual
 Insert time : 2005/11/21 10:38:48
 Age action : Aging
 Age time : 15 minutes
```

显示黑名单表项的运行状况。

```
<H3C> display firewall blacklist enable
Blacklist is Enabled
```

4.3.3 firewall blacklist

【命令】

firewall blacklist { **enable** | *sour-addr* [**timeout** *minutes*] }

undo firewall blacklist [**enable** | *sour-addr*]

【视图】

系统视图

【参数】

enable：使能黑名单功能。

sour-addr：指定添加到黑名单的 IP 地址。

timeout *minutes*：指定超时时间。*minutes* 取值范围为 1～1000，以分钟为单位。

【描述】

firewall blacklist 命令用来添加黑名单表项内容，也可以用来使能黑名单功能。**undo firewall blacklist** 命令用来删除黑名单表项内容，也可以用来禁止黑名单功能。

如果没有设置 **timeout** 参数，表示此黑名单表项不进行老化，超时时间在黑名单的日志信息和 debug 信息中将显示为 0。

【举例】

在黑名单表项中插入一条 IP 地址为 192.168.10.10 的黑名单表项，老化时间为 100 分钟。

```
[H3C] firewall blacklist 192.168.10.10 timeout 100
```

使能黑名单功能。

```
[H3C] firewall blacklist enable
```

4.4 MAC 和 IP 地址绑定配置命令

4.4.1 debugging firewall mac-binding

【命令】

debugging firewall mac-binding { **all** | **item** | **packet** }

undo debugging firewall mac-binding { **all** | **item** | **packet** }

【视图】

用户视图

【参数】

all：显示全部调试信息。

item：显示地址绑定表项变化调试信息。

packet：显示报文中地址绑定表项调试信息。

【描述】

debugging firewall mac-binding 命令用来打开防火墙地址绑定功能调试开关，**undo debugging firewall mac-binding** 命令用来关闭防火墙地址绑定功能调试信息开关。

缺省情况关闭防火墙全部调试信息开关。

相关配置可参考命令 **display debugging**。

【举例】

打开地址绑定表项全部调试信息。

```
<H3C> debugging firewall mac-binding all
```

4.4.2 display firewall mac-binding

【命令】

display firewall mac-binding { **enable** | **item** [*ip-addr*] [**statistic**] }

【视图】

所有视图

【参数】

enable：显示地址绑定功能运行状况。

item：显示地址绑定表项内容。

ip-addr：显示指定 IP 地址的表项内容。

statistic：显示地址绑定功能的统计信息。

【描述】

display firewall mac-binding 命令用来显示防火墙地址绑定功能的运行状况和地址绑定表项信息。参数 **item** [*ip-addr*]显示地址绑定表项信息。如果不指定 IP 地址，显示当前全部地址绑定表项的概要信息。如果指定了要显示的 IP 地址，显示特定地址绑定表项的详细信息。

【举例】

显示全部地址绑定表项概要信息。

```
<H3C> display firewall mac-binding item
Firewall mac-binding item(s) :
Current items:2
 192.168.1.1      00e0-0f0c-1149
 20.202.16.5      0adc-0e0f-23ed
```

显示特定地址绑定表项详细信息。

```
<H3C> display firewall mac-binding item 192.168.1.1
Firewall mac-binding item(s) :
 192.168.1.1      00e0-0f0c-1149
```

显示地址绑定表项的运行状况。

```
<H3C> display firewall mac-binding enable
Mac-binding is Disabled
```

显示地址绑定功能的统计信息。

```
<H3C> display firewall mac-binding item statistic
Firewall Mac-binding item(s) :
      IP Address       Mac                 True Pkts          False Pkts
     192.168.1.2  000f-1f73-fec5                   0                  57
```

4.4.3 firewall mac-binding

【命令】

firewall mac-binding *ip-addr mac-addr*

undo firewall mac-binding [*ip-addr*]

【视图】

系统视图

【参数】

ip-addr：指定地址绑定对的 IP 地址。

mac-addr：指定地址绑定对的 MAC 地址。

【描述】

firewall mac-binding 命令用来添加 MAC 地址绑定条目。**undo firewall mac-binding** 命令用来删除 MAC 地址绑定条目，若 **undo firewall mac-binding** 命令使用 *ip-addr* 参数，表示删除特定的绑定条目，否则将删除所有绑定条目。

【举例】

在地址绑定表项中插入一条 IP 地址为 192.168.10.10，MAC 地址为 00e0-0000-0001 的地址绑定条目。

```
[H3C] firewall mac-binding 192.168.10.10 00e0-0000-0001
```

使能地址绑定功能。

```
[H3C] firewall mac-binding enable
```

4.4.4 firewall mac-binding enable

【命令】

firewall mac-binding enable

undo firewall mac-binding enable

【视图】

系统视图

【参数】

enable：使能地址绑定功能。

【描述】

firewall mac-binding enable 命令用来使能 MAC 地址绑定功能，**undo firewall mac-binding enable** 命令用来关闭 MAC 地址绑定功能。

【举例】

使能 MAC 地址绑定功能。

```
[H3C] firewall mac-binding enable
```

4.4.5 reset firewall mac-binding

【命令】

reset firewall mac-binding item [*ip-addr*] **statistic**

【视图】

用户视图

【参数】

item：MAC 和 IP 地址绑定表项。

ip-addr：清除指定 IP 地址的绑定信息。

statistic：MAC 和 IP 地址绑定的统计信息。

【描述】

reset firewall mac-binding 命令用来清除 MAC 和 IP 地址绑定的统计信息。

【举例】

清除所有 MAC 和 IP 地址绑定的统计信息。

```
<H3C> reset firewall mac-binding item statistic
```

4.5 区域配置命令

4.5.1 add interface

【命令】

add interface *interface-type interface-number*

undo add interface *interface-type interface-number*

【视图】

区域视图

【参数】

interface-type interface-number：指定接口类型及接口号。

【描述】

add interface 命令用来将接口加入到安全区域，**undo add interface** 命令用来将接口从安全区域中删除。

将接口加入到一个安全区域中前，这个接口不能已经属于其它的区域，否则需要先将此接口从其它区域中删除，即一个接口只能属于一个安全区域。

缺省情况下，所有安全区域中未添加任何接口。

若要实现防火墙和其它设备的互通，必须将相应的接口添加到某一安全区域中。

【举例】

将 Trust 区域接口 GigabitEthernet0/1 加入到 DMZ 区域。

```
[H3C] firewall zone trust
[H3C-zone-trust] undo add interface GigabitEthernet 0/1
[H3C-zone-trust] quit
[H3C] firewall zone DMZ
[H3C-zone-DMZ] add interface GigabitEthernet 0/1
```

4.5.2 display interzone

【命令】

display interzone [*zone1 zone2*]

【视图】

任意视图

【参数】

zone1 zone2：指定两个安全区域名称，即显示安全区域 *zone1* 和 *zone2* 的区域间配置。

【描述】

display interzone 命令用来显示安全区域间的配置信息。

若不指定参数，则显示所有区域间的配置信息。

【举例】

显示安全区域 trust 和 untrust 的区域间配置信息。

```
<H3C> display interzone trust untrust
```

4.5.3 display zone

【命令】

display zone [*zone-name*] [**interface** | **priority**]

【视图】

所有视图

【参数】

zone-name：安全区域的名称。系统预先定义了 4 个安全区域：Trust、Untrust、DMZ 和 Local。

interface：显示安全区域所包含的接口。

priority：显示安全区域的优先级。

【描述】

display zone 命令用来显示安全区域所包含的接口以及安全区域的优先级。

【举例】

显示所有安全区域的优先级。

```
<H3C> display zone priority
local
 priority is 100
#
trust
 priority is 85
#
untrust
 priority is 5
#
DMZ
 priority is 50
#
```

4.5.4 set priority

【命令】

set priority *number*

【视图】

区域视图

【参数】

number：区域的优先级数值，范围为 1～100。

【描述】

set priority 命令用来设置安全区域的优先级，优先级数值越高，表示此区域的安全性越高。

系统预定义了 4 个安全区域：Local、Trust、Untrust 和 DMZ。这些区域的优先级是不能被更改的。**set priority** 命令只能用来设置和修改新建的区域的优先级。

不同安全区域之间没有访问限制，且安全区域不支持策略配置，若需要访问控制，请在安全区域中的相应接口进行配置。

缺省情况下，Local 区域的优先级为 100，Trust 区域的优先级为 85，Untrust 区域的优先级为 5，DMZ 区域的优先级为 50。

【举例】

设置区域 newzone 的优先级为 70。

```
[H3C] firewall zone newzone
[H3C-zone-newzone] set priority 70
```

4.5.5 firewall interzone

【命令】

firewall interzone *zone1 zone2*

【视图】

系统视图

【参数】

zone1：安全区域名。

zone2：安全区域名。

【描述】

firewall interzone 命令用来进入区域间视图。

【举例】

进入 Trust 区域和 Untrust 区域的区域间视图。

```
[H3C] firewall interzone trust untrust
[H3C-interzone-trust-untrust]
```

4.5.6 firewall zone

【命令】

firewall zone *zonename*

【视图】

系统视图

【参数】

zonename：安全区域名。

【描述】

firewall zone 命令用来进入安全区域视图。

【举例】

进入 DMZ 区域视图。

```
[H3C] firewall zone DMZ
[H3C-zone-DMZ]
```

4.5.7 firewall zone name

【命令】

firewall zone name *zonename*

undo firewall zone name *zonename*

【视图】

系统视图

【参数】

zonename：安全区域名。

【描述】

firewall zone name 命令用来创建新的安全区域，**undo firewall zone name** 命令用来删除新建的安全区域。

缺省情况下，系统预先定义了 4 个安全区域：Trust、Untrust、DMZ 和 Local，这些安全区域是不能被删除的。

【举例】

创建一个新的名为 newzone 的安全区域。

```
[H3C] firewall zone name newzone
[H3C-zone-newzone]
```

第5章 面向对象管理配置命令

5.1 对象管理配置命令

5.1.1 acl name

【命令】

acl name *acl-name*

undo acl name *acl-name*

【视图】

系统视图

【参数】

acl-name：流对象名称，长度为 1～31 个字符，字符串必须以字母开头。

【描述】

acl name 命令用来创建流对象并进入流对象视图。**undo acl name** 命令用来删除流对象。

系统将通常的五元组简化为流对象，一个流对象中可以包括地址（组）对象、服务（组）对象和时间段对象三类对象信息，方便用户记忆所配置的规则的用途，再通过在不同的应用中引用流对象，可以简化配置管理任务。

缺省情况下，未创建流对象。

相关配置可参考命令 **rule**。

【举例】

创建流对象 http。

```
[H3C] acl name http
[H3C-acl-name-http]
```

5.1.2 add

【命令】

add *object-name*

undo add *object-name*

【视图】

地址组对象视图/服务组对象视图

【参数】

object-name：地址对象名或服务对象名，长度为 1～31 个字符。

【描述】

add 命令用来将地址对象添加到地址组对象中或将服务对象添加到服务组对象中。**undo add** 命令用来将地址对象或服务对象从地址组对象或服务组对象中删除。

缺省情况下，地址组/服务组对象中未添加地址/服务对象。

相关配置可参考命令 **object address-group**，**object service-group**，**object address**，**object service**。

【举例】

在地址组对象 test 中添加地址对象 webserver。

```
[H3C] object address-group test
[H3C-obj-addr-group-test] add webserver
```

5.1.3 debugging object dns

【命令】

debugging object dns

undo debugging object dns

【视图】

用户视图

【参数】

无

【描述】

debugging object dns 命令用来打开地址对象的 DNS 解析调试信息开关。**undo debugging object dns** 命令用来关闭调试信息开关。

缺省情况下，关闭调试信息开关。

【举例】

打开地址对象的 DNS 解析调试开关。

```
<H3C> debugging object dns
```

5.1.4 display acl

【命令】

display acl { **all** | **name** *acl-name* }

【视图】

任意视图

【参数】

acl-name：指定流对象，长度为 1～31 个字符。

【描述】

display acl name 命令用来显示流对象信息。**display acl all** 命令用来显示所有的流对象信息和编号型的访问控制列表。

相关配置可参考命令 **acl name**。

【举例】

显示流对象 http-flow 的信息。

```
<H3C> display acl name http-flow
Flow object  Name:http-flow, 1 rule
Acl's step is 10
 rule 0 permit source addrtest1 destination addrtest2 service www logging (0
times matched)
```

5.1.5 display object address

【命令】

display object address [*object-name*]

【视图】

任意视图

【参数】

object-name：指定地址对象，长度为 1～31 个字符。

【描述】

display object address 命令用来显示地址对象信息。

若不指定参数，则显示所有的地址对象。

相关配置可参考命令 **object address**。

【举例】

显示所有的地址对象信息。

```
<H3C> display object address
 Total address object number: 2
 Name                            IP/Domain
-------------------------------------------------------------
 addrtest1                       192.168.1.1      255.255.255.255
 addrtest2                       10.1.1.1         255.255.255.255
```

5.1.6 display object address-group

【命令】

display object address-group [*object-group-name*]

【视图】

任意视图

【参数】

object-group-name：指定地址组对象，长度为 1～31 个字符。

【描述】

display object address-group 命令用来显示地址组对象信息。

若不指定参数，则显示所有的地址组对象。

相关配置可参考命令 **object address-group**。

【举例】

显示地址组对象 test 的信息。

```
<H3C> display object address-group test
 Total address-group member number:  2
 Name                            IP/Domain
-------------------------------------------------------------
 addrtest1                       192.168.1.1      255.255.255.255
 addrtest2                       10.1.1.1         255.255.255.255
```

5.1.7 display object predefined service

【命令】

display object predefined service

【视图】

任意视图

【参数】

无

【描述】

display object predefined service 命令用来显示系统预先定义的服务对象。

系统预先定义了多个服务对象，用户可以直接在服务组对象和流对象中引用这些服务对象。

【举例】

显示系统预先定义的服务对象。

```
<H3C> display object predefined service
```

5.1.8 display object service

【命令】

display object service [*object-name*]

【视图】

任意视图

【参数】

object-name：指定服务对象，长度为 1～31 个字符。

【描述】

display object service 命令用来显示服务对象信息。

若不指定参数，则显示所有的服务对象。

相关配置可参考命令 **object service**。

【举例】

显示所有的服务对象。

```
<H3C> display object service
 Total service object number:  1
 Name                      Protocol  Src-port/Icmp-type  Dst-port/Icmp-code
-------------------------------------------------------------------------------
test                          6            1024-65535         2048-2058
```

5.1.9 display object service-group

【命令】

display object service-group [*object-group-name*]

【视图】

任意视图

【参数】

object-group-name：指定服务组对象，长度为 1～31 个字符。

【描述】

display object service 命令用来显示服务组对象信息。

若不指定参数，则显示所有的服务组对象。

相关配置可参考命令 **object service-group**。

【举例】

显示服务组对象 srvgrp。

```
<H3C> display object service-group srvgrp
 Total service-group member number:  3
 Name                      Protocol  Src-port/Icmp-type  Dst-port/Icmp-code
-------------------------------------------------------------------------
 bgp                            6               0-65535         179-179
 test                           6            1024-65535         2048-2058
 www                            6               0-65535          80-80
```

5.1.10 object address

【命令】

object address *object-name* { *address mask* | *domain-name* }

undo object address *object-name*

【视图】

系统视图

【参数】

object-name：地址对象名，长度为 1～31 个字符。

address：指定地址对象对应的 IP 地址。

mask：指定 IP 地址的掩码或掩码长度。

domain-name：指定地址对象对应的域名，长度为 1～60 个字符。

【描述】

object address 命令用来创建地址对象。**undo object address** 命令用来删除地址对象。

系统支持创建 IP 地址和域名两种类型的地址对象。

缺省情况下，未创建地址对象。

相关配置可参考命令 **object address-group**，**add**，**acl name**。

【举例】

创建域名类型的地址对象 mysite。

```
[H3C] object address mysite www.mysite.net
```

创建 IP 地址类型的地址对象 webserver。

```
[H3C] object address webserver 192.168.1.1 24
```

5.1.11 object address-group

【命令】

object address-group *object-group-name*

undo object address-group *object-group-name*

【视图】

系统视图

【参数】

object-group-name：地址组对象名，长度为 1～31 个字符。

【描述】

object address-group 命令用来创建地址组对象并进入地址组对象视图。**undo object address-group** 命令用来删除地址组对象。

在创建地址组对象后，用户可以将系统中已经存在的地址对象添加到地址组对象中，同一地址对象可以被添加到不同的地址组对象中。

缺省情况下，未创建地址组对象。

相关配置可参考命令 **object address**，**add**，**acl name**。

【举例】

创建地址组对象 test。

```
[H3C] object address-group test
[H3C-obj-addr-group-test]
```

5.1.12 object refresh dns

【命令】

object refresh dns

【视图】

系统视图

【参数】

无

【描述】

object refresh dns 命令用来更新域名地址对象中引用的域名的信息。

当域名对应的地址更新后，可以使用此命令及时更新域名地址对象中引用的域名的信息。

相关配置命令可参考 **object address**。

【举例】

更新域名地址对象中引用的域名的信息。

```
[H3C] object refresh dns
```

5.1.13 object service

【命令】

object service *object-name* **protocol** { **tcp** | **udp** } [**src-port** *src-port1* **to** *src-port2*] [**dst-port** *dst-port1* **to** *dst-port2*]

object service *object-name* **protocol icmp type** *icmp-type* **code** *icmp-code*

object service *object-name* **protocol** *protocol-number*

undo object service *object-name*

【视图】

系统视图

【参数】

object-name：服务对象名，长度为 1～31 个字符。

tcp：指定服务对象的类型为 TCP。

udp：指定服务对象的类型为 UDP。

src-port1 **to** *src-port2*：当服务对象为 TCP 和 UDP 类型时，指定源端口的范围，端口号取值范围为 0～65535。若 *src-port1* 等于 *src-port2*，则表示一个指定的端口。

dst-port1 **to** *dst-port2*：当服务对象为 TCP 和 UDP 类型时，指定目的端口的范围，端口号取值范围为 0～65535。若 *dst-port1* 等于 *dst-port2*，则表示一个指定的端口。

icmp：指定服务对象的类型为 ICMP。

icmp-type：当服务对象为 ICMP 类型时，指定 ICMP 类型。

icmp-code：当服务对象为 ICMP 类型时，指定 ICMP 代码。

protocol-number：当服务对象为其它协议类型时指定协议号。

【描述】

object service 命令用来创建服务对象。**undo object service** 命令用来删除服务对象。

系统支持 ICMP、TCP、UDP 和其它协议的对象配置和管理。通过将协议号、源端口、目的端口、ICMP 消息类型简化为服务对象，简化了配置管理的工作。

缺省情况下，系统预先定义了多个服务对象，用户可以直接在服务组对象和流对象中引用这些服务对象。可以通过 **display object predefined service** 命令查看预定义的服务对象。

相关配置可参考命令 **object service-group**，**add**，**acl name**。

【举例】

创建 UDP 服务对象 myapp，源端口为 1024～65535，目的端口为 20000。

```
[H3C] object service myapp protocol udp src-port 1024 to 65535 dst-port 20000
to 20000
```

5.1.14 object service-group

【命令】

object service-group *object-group-name*

undo object service-group *object-group-name*

【视图】

系统视图

【参数】

object-group-name：服务组对象名，长度为 1～31 个字符。

【描述】

object service-group 命令用来创建服务组对象并进入服务组对象视图。**undo object service-group** 命令用来删除服务组对象。

在创建服务组对象后，用户可以将系统中已经存在的服务对象添加到服务组对象中，同一服务对象可以被添加到不同的服务组对象中。

缺省情况下，未创建服务组对象。

相关配置可参考命令 **object service**，**add**，**acl name**。

【举例】

创建服务组对象 test。

```
[H3C] object service-group test
[H3C-obj-srv-group-test]
```

5.1.15 reset acl counter

【命令】

reset acl counter { **all** | **name** *acl-name* }

【视图】

用户视图

【参数】

acl-name：指定流对象，长度为 1～31 个字符。

【描述】

reset acl counter name 命令用来清除流对象下流规则的匹配统计信息。**reset acl counter all** 用来清除所有流对象下流规则的匹配统计信息和编号型访问控制列表的匹配统计信息。

【举例】

清除流对象 http-flow 的匹配统计信息。

```
<H3C> reset acl counter name http-flow
```

5.1.16 rule

【命令】

rule [*rule-id*] { **permit** | **deny** } [**source** { *src-name* | *src-group-name* }] [**destination** { *dst-name* | *dst-group-name* }] [**service** { *srv-name* | *srv-group-name* }] [**time-range** *time-name*] [**logging**]

undo rule *rule-id* [**source**] [**destination**] [**service**] [**time-range**] [**logging**]

【视图】

流对象视图

【参数】

rule-id：流规则的编号，范围为 0～65534。当指定了编号，如果此编号的规则已存在，则会在原有定义的基础上叠加新定义的规则，相当于编辑一个已经存在的规则。如果此编号的规则不存在，则使用指定的编号创建一个新的规则。如果不指定编号，

表示增加一个新规则，系统自动会为这个规则分配一个编号，编号分配根据当前最大编号累加，累加步长为 10。

deny：表示拒绝符合条件的数据包。

permit：表示允许符合条件的数据包。

source：指定流规则的源地址对象（组）信息。如果不配置，表示报文的任何源地址都匹配。

src-name：指定源地址对象。

src-group-name：指定源地址组对象。

destination：指定流规则的目的地址对象（组）信息。如果不配置，表示报文的任何目的地址都匹配。

dst-name：指定目的地址对象名称。

dst-group-name：指定目的地址组对象。

service：指定服务对象（组）信息。

srv-name：指定服务对象。

srv-group-name：指定服务组对象。

time-range *time-name*：指定时间段对象名称。

logging：对符合匹配条件的数据包进行日志记录。目前支持此选项的业务只有包过滤防火墙（在接口下被 **firewall packet-filter** 命令引用）。

【描述】

rule 命令用来在流对象中添加流规则。**undo rule** 命令用来删除流规则。

一个流对象中可以添加多条流规则，系统将根据配置的流规则对数据流进行过滤。

缺省情况下，流对象中未添加流规则。

相关配置可参考命令 **acl name**，**object address**，**object address-group**，**object service**，**object service-group**。

【举例】

添加流规则，允许 srctest 到 dsttest 的 HTTP 数据流。

```
[H3C] acl name test
[H3C-acl-name-test] rule permit source srctest destination dsttest service
http
```

5.2 对象引用配置命令

5.2.1 firewall packet-filter *acl-name*

【命令】

firewall packet-filter *acl-name* { **inbound** | **outbound** }

undo firewall packet-filter *acl-name* { **inbound** | **outbound** }

【视图】

接口视图

【参数】

acl-name：指定流对象，长度为 1～31 个字符。

inbound：过滤从接口收到的数据包。

outbound：过滤从接口发送的数据包。

【描述】

firewall packet-filter *acl-name* 命令用来将流对象应用到包过滤防火墙中。**undo firewall packet-filter** *acl-name* 命令用来取消上述配置。

在包过滤防火墙中，可以通过引用流对象对数据流进行过滤。

缺省情况下，流对象未应用到包过滤防火墙中。

相关配置可参考命令 **acl name**。

【举例】

在 Ethernet 0/0/0 接口的入方向应用流对象 http-flow。

```
[H3C] interface Ethernet 0/0/0
[H3C-Ethernet0/0/0] firewall packet-filter http-flow inbound
```

5.2.2 nat outbound *acl-name*

【命令】

nat outbound *acl-name* [**address-group** *group-number* [**no-pat**]]

undo nat outbound *acl-name* [**address-group** *group-number* [**no-pat**]]

【视图】

接口视图

【参数】

acl-name：指定流对象，长度为 1～31 个字符。

address-group：表示使用地址池的方式配置地址转换，如果不指定地址池，则直接使用该接口的 IP 地址作为转换后的地址，即 easy-ip 特性。

group-number：一个已经定义的地址池的编号。

no-pat：表示使用多对多的地址转换，只转换数据包的地址而不转换端口信息。

【描述】

nat outbound *acl-name* 命令用来将流对象应用到 NAT 中。**undo nat outbound** *acl-name* 命令用来取消上述配置。

在 NAT 应用中，可以通过引用流对象对指定的数据流进行地址转换。

缺省情况下，未将流对象应用到 NAT 中。

相关配置可参考命令 **acl name**。

【举例】

在 Ethernet 0/0/0 接口上将流对象 http-flow 应用到 NAT 中。

```
[H3C] interface Ethernet 0/0/0
[H3C-Ethernet0/0/0] nat outbound http-flow
```

第6章 透明防火墙配置命令

📖 说明：

仅 SecPath F100-C 防火墙和 SecPath F100-S 防火墙支持透明防火墙。

6.1 透明防火墙配置命令

6.1.1 acl number

【命令】

acl number *acl-number*

undo acl { **number** *acl-number* | **all** }

【视图】

系统视图

【参数】

number *acl-number*：基于 MAC 地址的访问控制列表的序号，范围为 4000～4999。

all：删除所有的 ACL，包括那些基于接口的访问控制列表，基本访问控制列表和高级访问控制列表。

【描述】

acl number 命令用来创建访问控制列表，**undo acl** 命令用来删除一个已经存在的访问控制列表。

缺省情况下，系统未定义任何基于 MAC 地址的访问控制列表。

关于访问控制列表的其它命令请参考 2.1.1 和 2.1.6 。

【举例】

创建一个编号为 4009 的基于 MAC 地址的访问控制列表。

```
[H3C] acl number 4009
```

6.1.2 bridge vlanid-transparent-transmit enable

【命令】

bridge vlanid-transparent-transmit enable

undo bridge vlanid-transparent-transmit enable

【视图】

接口视图

【参数】

无

【描述】

bridge vlanid-transparent-transmit enable 命令用来使能 VLAN ID 透传功能。**undo bridge vlanid-transparent-transmit enable** 命令用来关闭 VLAN ID 透传功能。

VLAN ID 透传是指接口直接转发报文，不对该报文中的 VLAN ID 做任何处理。即使出接口上有 VLAN ID 的情况下，也不会改变报文原有的 VLAN ID。

当以太网子接口配置 VLAN ID 后，该子接口只会接收这个 VLAN 的数据，这就决定了该桥组负责传输哪些 VLAN 的数据。

在使能 VLAN ID 透传功能以后，系统不对报文的 VLAN ID 做任何处理，两端相连的交换机可以看成是直接相连的。为了正常通信，用户需要给两端交换机的 trunk 口配置相同的 VLAN ID。

⚠ 注意：

如果某个接口启用 VLAN 透传，那么这个接口对应的物理接口和相应的子接口必须配置基于接口的访问控制列表以过滤从本接口收到的报文，防止报文又被转发回去。

缺省情况下，关闭 VLAN ID 透传功能。

【举例】

在 GigabitEthernet 0/0 接口上使能 VLAN ID 透传功能。

```
[H3C] interface GigabitEthernet 0/0
[H3C-GigabitEthernet0/0] bridge vlanid-transparent-transmit enable
```

6.1.3 debugging firewall eff

【命令】

debugging firewall eff [**interface** *interface-type interface-number*]

undo debugging firewall eff [**interface** *interface-type interface-number*]

【视图】

用户视图

【参数】

interface *interface-type interface-number*：特定接口的调试信息。

【描述】

debugging firewall eff 命令用来打开以太帧过滤的调试开关，**undo debugging firewall eff** 命令用来关闭以太帧过滤的调试开关。

缺省情况下，关闭以太帧过滤的调试开关。

【举例】

打开以太帧过滤的调试开关。

```
<H3C> debugging firewall eff
 Ethernet-frame-filter's debugging is on
<H3C>
*0.1350738 H3C EFF/8/DEBUGGING:
 OutBound List 4001, deny the frame with the following head :
 dest-mac is 000f-1f7e-fec5,sour-mac is 00e0-fc36-a7a9, type is 0800
*0.1350739 H3C BRIDGE/8/DEBUGGING:
Discard a frame for the filter on outport ; received from interface GigabitEther
net0/1;and try to send to interface GigabitEthernet0/0, with following frame
head :
00 0f 1f 7e fe c5 00 e0 fc 36 a7 a9 08 00
*0.1352740 H3C EFF/8/DEBUGGING:
 OutBound List 4001, deny the frame with the following head :
 dest-mac is 000f-1f7e-fec5,sour-mac is 00e0-fc36-a7a9, type is 0800
*0.1352740 H3C BRIDGE/8/DEBUGGING:
Discard a frame for the filter on outport ; received from interface GigabitEther
net0/1;and try to send to interface GigabitEthernet0/0, with following frame
head :
00 0f 1f 7e fe c5 00 e0 fc 36 a7 a9 08 00
*0.1352925 H3C EFF/8/DEBUGGING:
 InBound List 4001, deny the frame with the following head :
 dest-mac is ffff-ffff-ffff,sour-mac is 000f-1f7e-fec5, type is 0806
*0.1352925 H3C BRIDGE/8/DEBUGGING:
Discard a frame for the filter on inport ; received from interface GigabitEthern
et0/0, with following frame head :
ff ff ff ff ff ff 00 0f 1f 7e fe c5 08 06
*0.1354741 H3C EFF/8/DEBUGGING:
 OutBound List 4001, deny the frame with the following head :
 dest-mac is 000f-1f7e-fec5,sour-mac is 00e0-fc36-a7a9, type is 0800
*0.1354741 H3C BRIDGE/8/DEBUGGING:
Discard a frame for the filter on outport ; received from interface GigabitEther
```

```
net0/1;and try to send to interface GigabitEthernet0/0, with following frame
head :
00 0f 1f 7e fe c5 00 e0 fc 36 a7 a9 08 00
*0.1356742 H3C EFF/8/DEBUGGING:
 OutBound List 4001, deny the frame with the following head :
 dest-mac is 000f-1f7e-fec5,sour-mac is 00e0-fc36-a7a9, type is 0800
*0.1356742 H3C BRIDGE/8/DEBUGGING:
Discard a frame for the filter on outport ; received from interface GigabitEther
net0/1;and try to send to interface GigabitEthernet0/0, with following frame
head :
00 0f 1f 7e fe c5 00 e0 fc 36 a7 a9 08 00
```

6.1.4 debugging firewall transparent-mode eth-forwarding

【命令】

debugging firewall transparent-mode eth-forwarding [**interface** *interface-type interface-number*]

undo debugging firewall transparent-mode eth-forwarding [**interface** *interface-type interface-number*]

【视图】

用户视图

【参数】

interface *interface-type interface-number*：特定接口的调试信息。

【描述】

debugging firewall transparent-mode eth-forwarding 命令用来打开透明防火墙的以太帧转发调试开关，**undo debugging firewall transparent-mode eth-forwarding** 命令用来关闭透明防火墙的以太帧转发调试开关。

当不指定接口时，则打开或关闭所有接口的以太帧转发调试开关。

缺省情况下，关闭透明防火墙的以太帧转发调试开关。

【举例】

打开透明防火墙的以太帧转发调试开关。

```
<H3C> debugging firewall transparent-mode eth-forwarding
The Transparent-mode eth-forwarding Debugging  is on
*0.695514 H3C BRIDGE/8/DEBUGGING:
Forward a frame; received from interface GigabitEthernet0/0;and try to send
to interface GigabitEthernet0/1, with following frame head :
00 e0 fc 36 a7 a9 00 0f 1f 7e fe c5 08 00
```

```
*0.695514 H3C BRIDGE/8/DEBUGGING:
Forward a frame; received from interface GigabitEthernet0/1;and try to send
to interface GigabitEthernet0/0, with following frame head :
00 0f 1f 7e fe c5 00 e0 fc 36 a7 a9 08 00
*0.696515 H3C BRIDGE/8/DEBUGGING:
Forward a frame; received from interface GigabitEthernet0/0;and try to send
to interface GigabitEthernet0/1, with following frame head :
00 e0 fc 36 a7 a9 00 0f 1f 7e fe c5 08 00
*0.696515 H3C BRIDGE/8/DEBUGGING:
Forward a frame; received from interface GigabitEthernet0/1;and try to send
to interface GigabitEthernet0/0, with following frame head :
00 0f 1f 7e fe c5 00 e0 fc 36 a7 a9 08 00
*0.696582 H3C BRIDGE/8/DEBUGGING:
Forward a frame; received from interface GigabitEthernet0/1;and try to send
to interface GigabitEthernet0/0, with following frame head :
00 0f 1f 7e fe c5 00 e0 fc 36 a7 a9 08 00
*0.696582 H3C BRIDGE/8/DEBUGGING:
Forward a frame; received from interface GigabitEthernet0/0;and try to send
to interface GigabitEthernet0/1, with following frame head :
00 e0 fc 36 a7 a9 00 0f 1f 7e fe c5 08 00
*0.696584 H3C BRIDGE/8/DEBUGGING:
Forward a frame; received from interface GigabitEthernet0/1;and try to send
to interface GigabitEthernet0/0, with following frame head :
00 0f 1f 7e fe c5 00 e0 fc 36 a7 a9 08 00
*0.696584 H3C BRIDGE/8/DEBUGGING:
Forward a frame; received from interface GigabitEthernet0/0;and try to send
to interface GigabitEthernet0/1, with following frame head :
00 e0 fc 36 a7 a9 00 0f 1f 7e fe c5 08 00
```

6.1.5 debugging firewall transparent-mode ip-forwarding

【命令】

debugging firewall transparent-mode ip-forwarding

undo debugging firewall transparent-mode ip-forwarding

【视图】

用户视图

【参数】

无

【描述】

debugging firewall transparent-mode ip-forwarding 命令用来打开透明防火墙的 IP 报文转发调试开关，**undo debugging firewall transparent-mode ip-forwarding** 命令用来关闭透明防火墙的 IP 报文转发调试开关。

缺省情况下，关闭透明防火墙的 IP 报文转发调试开关。

【举例】

打开透明防火墙的 IP 报文转发调试开关。

```
<H3C> debugging firewall transparent-mode ip-forwarding
 The Transparent-mode Ip-forwarding Debugging  is on
<H3C>
*0.11355193 H3C FWTP/8/rcv_ip:Receive an IP packet
    interface: GigabitEthernet0/0
    source_ip_addr : 192.168.3.6
    source_port : 33073
    destination_ip_addr : 192.168.3.8
    destination_port : 52128
    protocol : 1

*0.11355193 H3C FWTP/8/sndto_secur:Send an IP packet to security module
    source_ip_addr : 192.168.3.6
    source_port : 17664
    destination_ip_addr : 192.168.3.8
    destination_port : 60
    protocol : 1
    return value:0

*0.11355193 H3C FWTP/8/snd_ip:Send an IP packet
    interface: GigabitEthernet0/1
    source_ip_addr : 192.168.3.6
    source_port : 0
    destination_ip_addr : 192.168.3.8
    destination_port : 1
    protocol : 1

*0.11355193 H3C FWTP/8/rcv_ip:Receive an IP packet
    interface: GigabitEthernet0/1
    source_ip_addr : 192.168.3.8
    source_port : 33073
    destination_ip_addr : 192.168.3.6
    destination_port : 52128
```

```
    protocol : 1
*0.11355193 H3C FWTP/8/sndto_secur:Send an IP packet to security module
    source_ip_addr : 192.168.3.8
    source_port : 17664
    destination_ip_addr : 192.168.3.6
    destination_port : 60
    protocol : 1
    return value:0

*0.11355193 H3C FWTP/8/snd_ip:Send an IP packet
    interface: GigabitEthernet0/0
    source_ip_addr : 192.168.3.8
    source_port : 0
    destination_ip_addr : 192.168.3.6
    destination_port : 1
    protocol : 1
```

6.1.6 display firewall ethernet-frame-filter

【命令】

display firewall ethernet-frame-filter { **all** | **interface** *interface-type interface-number* }

【视图】

所有视图

【参数】

all：所有接口的以太帧过滤的统计信息。

interface *interface-type interface-number*：特定接口的以太帧过滤的统计信息。

【描述】

display firewall ethernet-frame-filter 命令用来显示以太帧过滤的统计信息。

【举例】

显示所有接口的以太帧过滤的统计信息。

```
<H3C> display firewall ethernet-frame-filter all
  Interface: GigabitEthernet0/1
  In-bound Policy: acl 4000
  From 2099-08-02 5:55:05  to 2099-08-02 5:55:41
     11 packets, 668 bytes, 100% permitted,
     0 packets, 0 bytes, 0% denied,
     0 packets, 0 bytes, 0% permitted default,
```

```
    0 packets, 0 bytes, 0% denied default,
  Totally 11 packets, 668 bytes, 100% permitted,
  Totally 0 packets, 0 bytes, 0% denied.
  Out-bound Policy: acl 4000
  From 2099-08-02 5:55:07  to 2099-08-02 5:55:41
    0 packets, 0 bytes, 0% permitted,
    0 packets, 0 bytes, 0% denied,
    0 packets, 0 bytes, 0% permitted default,
    0 packets, 0 bytes, 100% denied default,
  Totally 0 packets, 0 bytes, 0% permitted,
  Totally 0 packets, 0 bytes, 100% denied.
```

6.1.7 display firewall mode

【命令】

display firewall mode

【视图】

所有视图

【参数】

无

【描述】

display firewall mode 命令用来显示当前防火墙的工作模式。

【举例】

显示当前防火墙的工作模式。

```
<H3C> display firewall mode
 Firewall mode: transparent
```

6.1.8 display firewall transparent-mode address-table

【命令】

display firewall transparent-mode address-table [**interface** *interface-type interface-number* | **mac** *mac-address*]

【视图】

所有视图

【参数】

interface *interface-type interface-number*：与指定接口相关联的 MAC 地址信息。

mac *mac-address*：特定 MAC 地址条目的信息。

【描述】

display firewall transparent-mode address-table 命令用来显示透明防火墙的 MAC 地址表信息。

【举例】

显示透明防火墙的 MAC 地址表信息。

```
<H3C> display firewall transparent-mode address-table
 The total of the address-items is 2
 Mac-address    Flag   Aging-time   Receive       Send Interface-name
 00e0-fc36-a7a9  PD    00:01:41         23         13  GigabitEthernet0/1
 000f-1f7e-fec5  PD    00:03:28        121         12  GigabitEthernet0/0
 Flag meaning:  P--PERMIT   N--DENY  D--DYNAMIC  S--STATIC
```

6.1.9 display firewall transparent-mode config

【命令】

display firewall transparent-mode config

【视图】

所有视图

【参数】

无

【描述】

display firewall transparent-mode config 命令用来显示透明防火墙的配置信息。

【举例】

显示透明防火墙的配置信息。

```
<H3C> display firewall transparent-mode config
 Firewall transparent-info:
  ARP learning     : enable
  System IP address: 169.0.0.1
  System IP mask   : 255.0.0.0
  Unknown-mac:
    Unicast IP packet  : arp
    broadcast IP packet: drop
    Multicast IP packet: drop
```

6.1.10 display firewall transparent-mode traffic

【命令】

display firewall transparent-mode traffic [**interface** *interface-type interface-number*]

【视图】

所有视图

【参数】

interface *interface-type interface-number*：特定接口的流量信息。

【描述】

display firewall transparent-mode traffic 命令用来显示透明防火墙的流量信息。

【举例】

显示透明防火墙的流量信息。

```
<H3C> display firewall transparent-mode traffic
 system error  is 0,inport error  is 0,
 outport error is 0 ,other error is 0

the total statistic :
 Input:
         860 total, 0 bpdu, 750 single,
         0 multi, 110 broadcast;
         860 ip,0 ipx, 0 other protocol;
         860 eth2, 0 snap,
         0 dlsw, 0 other,
         0 vlan;
 Output:
         747 total, 0 bpdu, 747 single,
         0 multi, 0 broadcast;
         747 ip, 0 ipx, 0 other protocol;
         747 eth2, 0 snap,
         0 dlsw, 0 other,
         0 vlan;
 Send way:
         0 broadcast, 0 fast, 747 other
 Discard:
         0 by inport state,
         0 for local frame ,
         0 by mac table,
```

```
        0 by inport filter,
        0 by outport filter,
        113 by ip filter ,
        0 other

the statistic of interface GigabitEthernet0/1
 Input:
        376 total, 0 bpdu, 375 single,
        0 multi, 1 broadcast;
        376 ip,0 ipx, 0 other protocol;
        376 eth2, 0 snap,
        0 dlsw, 0 other,
        0 vlan;
 Output:
        374 total, 0 bpdu, 374 single,
        0 multi, 0 broadcast;
        374 ip, 0 ipx, 0 other protocol;
        374 eth2, 0 snap,
        0 dlsw, 0 other,
        0 vlan;
 Send way:
        0 broadcast, 0 fast, 374 other
 Discard:
        0 by inport state,
        0 for local frame ,
        0 by mac table,
        0 by inport filter,
        0 by outport filter,
        3 by ip filter ,
        0 other

the statistic of interface GigabitEthernet0/0
 Input:
        484 total, 0 bpdu, 375 single,
        0 multi, 109 broadcast;
        484 ip,0 ipx, 0 other protocol;
        484 eth2, 0 snap,
        0 dlsw, 0 other,
        0 vlan;
 Output:
        373 total, 0 bpdu, 373 single,
        0 multi, 0 broadcast;
        373 ip, 0 ipx, 0 other protocol;
```

```
        373 eth2, 0 snap,
        0 dlsw, 0 other,
        0 vlan;
Send way:
        0 broadcast, 0 fast, 373 other
Discard:
        0 by inport state,
        0 for local frame ,
        0 by mac table,
        0 by inport filter,
        0 by outport filter,
        110 by ip filter ,
        0 other
```

6.1.11 firewall arp-learning enable

【命令】

firewall arp-learning enable

undo firewall arp-learning enable

【视图】

系统视图

【参数】

无

【描述】

firewall arp-learning enable 命令用来启用工作在透明模式下的防火墙的动态 ARP 表项学习功能，**undo firewall arp-learning enable** 命令用来关闭透明防火墙的 ARP 学习功能。

缺省情况下，当防火墙工作在透明模式下时，防火墙自动启用动态 ARP 表项学习功能。

【举例】

启用防火墙的 ARP 学习功能。

```
[H3C] firewall arp-learning enable
```

6.1.12 firewall ethernet-frame-filter

【命令】

firewall ethernet-frame-filter *acl-number* { **inbound** | **outbound** }

undo firewall ethernet-frame-filter { **inbound** | **outbound** }

【视图】

以太网接口视图

【参数】

acl-number：基于 MAC 地址的 ACL 编号，范围为 4000～4999。

inbound：过滤从接口接收的帧。

outbound：过滤从接口发送的帧。

【描述】

firewall ethernet-frame-filter 命令用来将基于 MAC 地址的 ACL 应用到接口上，**undo firewall ethernet-frame-filter** 命令用来从接口上删除基于 MAC 地址的 ACL。

要将基于 MAC 地址的访问控制列表应用到接口上，防火墙必须工作在透明模式下，否则系统会提示错误信息。

当防火墙工作在透明模式下时，对于报文进行二层的过滤之后还要进行三层的过滤。

缺省情况下，未在接口上应用任何基于 MAC 地址的 ACL。

【举例】

在以太网接口 GigabitEthernet 0/1 的入方向上应用编号为 4009 的基于 MAC 地址的 ACL。

```
[H3C-GigabitEthernet0/1] firewall ethernet-frame-filter 4009 inbound
```

6.1.13 firewall mode

【命令】

firewall mode { **route** | **transparent** }

undo firewall mode

【视图】

系统视图

【参数】

route：配置防火墙工作在路由模式下。

transparent：配置防火墙工作在透明模式下。

【描述】

firewall mode 命令用来配置防火墙的工作模式，**undo firewall mode** 命令用来将防火墙恢复到工作在缺省模式下。

缺省情况下，防火墙工作在路由模式。

当防火墙工作在路由模式下时，其所有接口都工作在第三层，即可以为接口配置 IP 地址等第三层属性。当防火墙工作在透明模式下时，其所有接口都将工作在第二层，即转换为交换端口，且不能为接口配置 IP 地址等第三层属性。

【举例】

配置防火墙工作在透明模式。

```
[H3C] firewall mode transparent
 Set system ip address successfully.
 All the Interfaces's ip addresses have been deleted.
 The mode is set successfully.
```

从以上显示的系统提示信息可以看出，防火墙已经工作在透明模式下，且所有接口上的 IP 地址已经被删除。

6.1.14 firewall system-ip

【命令】

firewall system-ip *ip-address* [*mask*]

undo firewall system-ip

【视图】

系统视图

【参数】

ip-address：防火墙的系统 IP 地址。

mask：系统 IP 地址的子网掩码。若不指定掩码，系统则使用默认的分类子网掩码。

【描述】

firewall system-ip 命令用来配置防火墙的系统 IP 地址，**undo firewall system-ip** 命令用来将系统 IP 地址设置为防火墙缺省的系统 IP 地址。

缺省情况下，防火墙的系统 IP 地址为 169.0.0.1/8。

当防火墙工作在透明模式下时，其所有接口都将工作在第二层，即转换为交换端口，且不能为接口配置 IP 地址等第三层属性。此时若要对防火墙进行管理或使其提供网络服务，防火墙必须拥有 IP 地址，可以为防火墙配置系统 IP 地址以解决此问题。当防火墙被配置为工作在透明模式下时，若系统中不存在 Loopback0 接口，则系统会为防火墙创建一个地址为 169.0.0.1/8 的 Loopback0 接口，此地址将为缺省的系统 IP 地址；若系统中已存在 Loopback0 接口，Loopback0 接口的地址将被设为系统 IP 地址。当修改 Loopback0 接口的地址或删除 Loopback0 接口时，系统 IP 地址也会被修改或删除，可以使用此命令修改系统 IP 地址。

当防火墙工作在路由模式下时，不能配置系统 IP 地址。

【举例】

配置防火墙的系统 IP 地址

```
[H3C] firewall mode transparent
 Set system ip address successfully.
 All the Interfaces's ip addresses have been deleted.
 The mode is set successfully.
[H3C] firewall system-ip 10.1.1.5 255.255.255.0
 Set system ip address successfully.
```

6.1.15 firewall transparent-mode aging-time

【命令】

firewall transparent-mode aging-time *seconds*

undo firewall transparent-mode aging-time

【视图】

系统视图

【参数】

seconds：MAC 地址转发表的老化时间，范围为 10～1000000，单位为“秒”。

【描述】

firewall transparent-mode aging-time 命令用来配置 MAC 地址转发表的老化时间，**undo firewall transparent-mode aging-time** 命令用来恢复 MAC 地址转发表的老化时间为缺省值。

缺省情况下，MAC 地址转发表的老化时间为 300 秒。

【举例】

配置 MAC 地址转发表的老化时间为 1800 秒。

```
[H3C] firewall transparent-mode aging-time 1800
```

6.1.16 firewall transparent-mode transmit

【命令】

firewall transparent-mode transmit { **bpdu** | **dlsw** | **ipx** }

undo firewall transparent-mode transmit { **bpdu** | **dlsw** | **ipx** }

【视图】

系统视图

【参数】

bpdu：Bridge Protocol Data Unit，桥协议数据单元。

dlsw：Data Link Switching，数据链路交换。

ipx：Internetwork Packet Exchange，网际报文交换。

【描述】

firewall transparent-mode transmit 命令用来配置允许通过的报文类型，**undo firewall transparent-mode transmit** 命令用来配置拒绝通过的报文类型。

缺省情况下，防火墙不允许这些类型的报文通过。

【举例】

配置允许 BPDU 通过透明防火墙。

```
[H3C] firewall transparent-mode transmit bpdu
```

6.1.17 firewall unknown-mac

【命令】

firewall unknown-mac { **drop** | **flood** }

undo firewall unknown-mac

【视图】

系统视图

【参数】

drop：直接丢弃该未知目的 MAC 地址的 IP 单播、组播和广播报文。

flood：将此未知目的 MAC 地址的 IP 单播、组播和广播报文在除接收接口外的其它所有接口（接口必须属于某一安全区域）上泛洪。待收到响应报文后，则保存其 MAC 地址信息，后续报文将使用该 MAC 地址进行转发。

【描述】

firewall unknown-mac 命令用来配置防火墙对未知目的 MAC 地址的单播、组播和广播报文的处理方式，**undo firewall unknown-mac** 命令用来恢复缺省处理方式。

缺省情况下，防火墙对未知目的 MAC 地址的单播、组播和广播报文的处理方式为 **flood**。

相关配置请参考命令 **firewall unknown-mac unicast**，**firewall unknown-mac multicast**，**firewall unknown-mac broadcast**。

【举例】

配置防火墙丢弃未知目的 MAC 地址的 IP 报文。

```
[H3C] firewall unknown-mac drop
```

6.1.18 firewall unknown-mac broadcast

【命令】

firewall unknown-mac broadcast { **drop** | **flood** }

undo firewall unknown-mac broadcast

【视图】

系统视图

【参数】

drop：直接丢弃广播 IP 报文。

flood：将广播 IP 报文在除接收接口外的其它所有接口（接口必须属于某一安全区域）上泛洪。待收到响应报文后，保存其 MAC 地址信息。

【描述】

firewall unknown-mac broadcast 命令用来配置防火墙对广播 IP 报文的处理方式，**undo firewall unknown-mac broadcast** 命令用来恢复对广播 IP 报文的缺省处理方式。

缺省情况下，防火墙泛洪广播 IP 报文，即按照 **flood** 的方式进行处理。

【举例】

配置防火墙丢弃广播 IP 报文。

```
[H3C] firewall unknown-mac broadcast drop
```

6.1.19 firewall unknown-mac multicast

【命令】

firewall unknown-mac multicast { **drop** | **flood** }

undo firewall unknown-mac multicast

【视图】

系统视图

【参数】

drop：直接丢弃组播 IP 报文。

flood：将组播 IP 报文在除接收接口外的其它所有接口（接口必须属于某一安全区域）上泛洪。待收到响应报文后，保存其 MAC 地址信息。

【描述】

firewall unknown-mac multicast 命令用来配置防火墙对组播 IP 报文的处理方式，**undo firewall unknown-mac multicast** 命令用来恢复对组播 IP 报文的缺省处理方式。

缺省情况下，防火墙泛洪组播 IP 报文，即按照 **flood** 的方式进行处理。

【举例】

配置防火墙丢弃组播 IP 报文。

```
[H3C] firewall unknown-mac multicast drop
```

6.1.20 firewall unknown-mac unicast

【命令】

firewall unknown-mac unicast { **drop** | **arp** | **flood** }

undo firewall unknown-mac unicast

【视图】

系统视图

【参数】

drop：直接丢弃该未知目的 MAC 地址的 IP 报文。

arp：在除接收到该报文的接口外的其它所有接口（接口必须属于某一安全区域）上广播 ARP 请求报文，并且丢弃原来的未知 MAC 地址的 IP 报文。收到 ARP 响应报文后，保存 MAC 地址和接口的对应关系。

flood：将此未知目的 MAC 地址的 IP 报文在除接收接口外的其它所有接口（接口必须属于某一安全区域）上泛洪。待收到响应报文后，则保存其 MAC 地址信息，后续报文将使用该 MAC 地址进行转发。

【描述】

firewall unknown-mac unicast 命令用来配置防火墙对未知目的 MAC 地址的 IP 单播报文的处理方式，**undo firewall unknown-mac unicast** 命令用来恢复对未知目的 MAC 地址的 IP 单播报文的缺省处理方式。

缺省情况下，防火墙对未知目的 MAC 地址的单播 IP 报文按照 **flood** 方式进行处理。

【举例】

配置防火墙丢弃未知目的 MAC 地址的 IP 单播报文。

```
[H3C] firewall unknown-mac unicast drop
```

6.1.21 reset firewall ethernet-frame-filter

【命令】

reset firewall ethernet-frame-filter { **all** | **interface** *interface-type interface-number* }

【视图】

用户视图

【参数】

all：所有接口上的以太帧的过滤信息。

interface *interface-type interface-number*：特定接口上的以太帧的过滤信息。

【描述】

reset firewall ethernet-frame-filter 命令用来清除以太帧的过滤信息。

【举例】

清除所有接口上的以太帧过滤信息。

```
<H3C> reset firewall ethernet-frame-filter all
```

6.1.22 reset firewall transparent-mode address-table

【命令】

reset firewall transparent-mode address-table [**interface** *interface-type interface-number*]

【视图】

用户视图

【参数】

interface *interface-type interface-number*：与特定接口关联的 MAC 地址信息。

【描述】

reset firewall transparent-mode address-table 命令用来清除 MAC 地址表中的信息。

【举例】

清除与接口 GigabitEthernet 0/1 相关联的 MAC 地址信息。

```
<H3C> reset firewall transparent-mode address-table interface
```

```
GigabitEthernet0/1
```

6.1.23 reset firewall transparent-mode traffic

【命令】

reset firewall transparent-mode traffic [**interface** *interface-type interface-number*]

【视图】

用户视图

【参数】

interface *interface-type interface-number*：特定接口的流量统计信息。

【描述】

reset firewall transparent-mode traffic 命令用来清除透明防火墙的流量统计信息。

【举例】

清除透明防火墙的流量统计信息。

```
<H3C> reset firewall transparent-mode traffic
```

6.1.24 rule

【命令】

rule [*rule-id*] { **permit** | **deny** } [**type** *type-code type-wildcard* | **lsap** *lsap-code lsap-wildcard*] [**source-mac** *sour-addr source-wildcard*] [**dest-mac** *dest-addr dest-wildcard*] [**time-range** *time-name*] [**logging**]

undo rule *rule-id* [**time-range**] [**logging**]

【视图】

基于 MAC 地址的 ACL 视图

【参数】

rule-id：ACL 的规则编号，范围为 0～65534。当指定了编号，如果与编号对应的规则已经存在，则会部分覆盖旧的规则，相当于编辑一个已经存在的 ACL 规则。故建议用户当编辑一个已存在编号的规则时，先将旧的规则删除，再创建新的规则，否则配置结果可能与预期的效果不同。如果与编号对应的规则不存在，则使用指定的编号创建一个新的规则。如果不指定编号，表示增加一个新规则，系统自动会为这个规则分配一个编号。

permit：表示允许符合条件的数据包。

deny：表示拒绝符合条件的数据包。

type：数据帧的类型。

type-code：数据帧的类型，一个 16 比特的十六进制数，对应Ethernet_II类型和Ethernet_SNAP类型帧中的type-code域。关于*type-code*的值请参考 表 7-5。

type-mask：类型掩码，是一个 16 比特的十六进制数，用于指定屏蔽位。

lsap：数据帧的封装格式。

lsap-code：数据帧的封装格式的值，是一个 16 比特的十六进制数。

lsap-mask：lsap 值的掩码，是一个 16 比特的十六进制数，用于指定屏蔽位。

source-mac：源 MAC 地址。

sour-addr：源 MAC 地址，格式为 xxxx-xxxx-xxxx，用来匹配一个分组的源地址。

sour-mask：源 MAC 地址的掩码。

dest-mac：目的 MAC 地址。

dest-addr：目的 MAC 地址，格式为 xxxx-xxxx-xxxx，用来匹配一个分组的源地址。

dest-mask：目的 MAC 地址的掩码。

logging：对符合条件的数据包记录日志。目前支持此选项的业务只有包过滤防火墙（在接口下被 **firewall packet-filter** 命令引用）。

time-range *time-name*：配置这条访问控制规则生效的时间段。

【描述】

rule 命令用来添加一个 ACL 规则，**undo rule** 命令用来删除 ACL 规则。

缺省情况下，未创建任何 ACL 规则。

【举例】

配置一条拒绝任何以太网帧的规则。

```
[H3C] acl number 4009
[H3C-acl-ethernetframe-4009] rule deny
```

表6-1 以太网类型域值表

以太网类型域值（16 进制值）	描述
0000-05DC	IEEE802.3 Length Field
0101-01FF	Experimental
200	XEROX PUP (see 0A00)
201	PUP Addr Trans (see 0A01)
400	Nixdorf
600	XEROX NS IDP

以太网类型域值（16 进制值）	描述
660	DLOG
661	DLOG
800	Internet IP (IPv4)
801	X.75 Internet
802	NBS Internet
803	ECMA Internet
804	Chaosnet
805	X.25 Level 3
806	ARP
807	XNS Compatability
081C	Symbolics Private
0888-088A	Xyplex
900	Ungermann-Bass net debugr
0A00	Xerox IEEE802.3 PUP
0A01	PUP Addr Trans
0BAD	Banyan Systems
1000	Berkeley Trailer nego
1001-100F	Berkeley Trailer encap/IP
1600	Valid Systems
4242	PCS Basic Block Protocol
5208	BBN Simnet
6000	DEC Unassigned (Exp.)
6001	DEC MOP Dump/Load
6002	DEC MOP Remote Console
6003	DEC DECNET Phase IV Route
6004	DEC LAT
6005	DEC Diagnostic Protocol
6006	DEC Customer Protocol
6007	DEC LAVC, SCA
6008-6009	DEC Unassigned
6010-6014	3Com Corporation
7000	Ungermann-Bass download
7002	Ungermann-Bass dia/loop
7020-7029	LRT

以太网类型域值（16 进制值）	描述
7030	Proteon
7034	Cabletron
8003	Cronus VLN
8004	Cronus Direct
8005	HP Probe
8006	Nestar
8008	AT&T
8010	Excelan
8013	SGI diagnostics
8014	SGI network games
8015	SGI reserved
8016	SGI bounce server
8019	Apollo Computers
802E	Tymshare
802F	Tigan, Inc.
8035	Reverse ARP
8036	Aeonic Systems
8038	DEC LANBridge
8039-803C	DEC Unassigned
803D	DEC Ethernet Encryption
803E	DEC Unassigned
803F	DEC LAN Traffic Monitor
8040-8042	DEC Unassigned
8044	Planning Research Corp.
8046	AT&T
8047	AT&T
8049	ExperData
805B	Stanford V Kernel exp.
805C	Stanford V Kernel prod.
805D	Evans & Sutherland
8060	Little Machines
8062	Counterpoint Computers
8065	Univ. of Mass. @ Amherst
8066	Univ. of Mass. @ Amherst

以太网类型域值（16 进制值）	描述
8067	Veeco Integrated Auto.
8068	General Dynamics
8069	AT&T
806A	Autophon
806C	ComDesign
806D	Computgraphic Corp.
806E-8077	Landmark Graphics Corp.
807A	Matra
807B	Dansk Data Elektronik
807C	Merit Internodal
807D-807F	Vitalink Communications
8080	Vitalink TransLAN III
8081-8083	Counterpoint Computers
809B	Appletalk
809C-809E	Datability
809F	Spider Systems Ltd.
80A3	Nixdorf Computers
80A4-80B3	Siemens Gammasonics Inc.
80C0-80C3	DCA Data Exchange Cluster
80C4	Banyan Systems
80C5	Banyan Systems
80C6	Pacer Software
80C7	Applitek Corporation
80C8-80CC	Intergraph Corporation
80CD-80CE	Harris Corporation
80CF-80D2	Taylor Instrument
80D3-80D4	Rosemount Corporation
80D5	IBM SNA Service on Ether
80DD	Varian Associates
80DE-80DF	Integrated Solutions TRFS
80E0-80E3	Allen-Bradley
80E4-80F0	Datability
80F2	Retix
80F3	AppleTalk AARP (Kinetics)

以太网类型域值（16 进制值）	描述
80F4-80F5	Kinetics
80F7	Apollo Computer
80FF-8103	Wellfleet Communications
8107-8109	Symbolics Private
8130	Hayes Microcomputers
8131	VG Laboratory Systems
8132-8136	Bridge Communications
8137-8138	Novell, Inc.
8139-813D	KTI
8148	Logicraft
8149	Network Computing Devices
814A	Alpha Micro
814C	SNMP
814D	BIIN
814E	BIIN
814F	Technically Elite Concept
8150	Rational Corp
8151-8153	Qualcomm
815C-815E	Computer Protocol Pty Ltd
8164-8166	Charles River Data System
817D-818C	Protocol Engines
818D	Motorola Computer
819A-81A3	Qualcomm
81A4	ARAI Bunkichi
81A5-81AE	RAD Network Devices
81B7-81B9	Xyplex
81CC-81D5	Apricot Computers
81D6-81DD	Artisoft
81E6-81EF	Polygon
81F0-81F2	Comsat Labs
81F3-81F5	SAIC
81F6-81F8	VG Analytical
8203-8205	Quantum Software
8221-8222	Ascom Banking Systems

以太网类型域值（16 进制值）	描述
823E-8240	Advanced Encryption Syste
827F-8282	Athena Programming
8263-826A	Charles River Data System
829A-829B	Inst Ind Info Tech
829C-82AB	Taurus Controls
82AC-8693	Walker Richer & Quinn
8694-869D	Idea Courier
869E-86A1	Computer Network Tech
86A3-86AC	Gateway Communications
86DB	SECTRA
86DE	Delta Controls
86DF	ATOMIC
86E0-86EF	Landis & Gyr Powers
8700-8710	Motorola
8A96-8A97	Invisible Software
9000	Loopback
9001	3Com(Bridge) XNS Sys Mgmt
9002	3Com(Bridge) TCP-IP Sys
9003	3Com(Bridge) loop detect
FF00	BBN VITAL-LanBridge cache
FF00-FF0F	ISC Bunker Ramo

第7章 混合模式配置命令

📖 **说明：**

仅 SecPath F1000-A 防火墙、SecPath F1000-S 防火墙、SecPath F1000-C 防火墙、SecPath F100-A 防火墙、SecPath F100-A-SI 防火墙、SecPath F100-M 防火墙和 SecPath F100-E 防火墙、SecPath F100-C-EI 防火墙、SecPath F100-C II 防火墙即新一代 F100-C 支持混合模式。

7.1 网桥配置命令

7.1.1 acl number

【命令】

acl number *acl-number*

undo acl { **number** *acl-number* | **all** }

【视图】

系统视图

【参数】

number *acl-number*：基于 MAC 地址的访问控制列表的序号，范围为 4000～4999。

all：删除所有的 ACL，包括那些基于接口的访问控制列表、基本访问控制列表和高级访问控制列表。

【描述】

acl number 命令用来创建访问控制列表，**undo acl** 命令用来删除一个已经存在的访问控制列表。

缺省情况下，系统未定义任何基于 MAC 地址的访问控制列表。

【举例】

创建一个编号为 4009 的基于 MAC 地址的访问控制列表。

```
[H3C] acl number 4009
```

7.1.2 bridge aging-time

【命令】

bridge aging-time *seconds*

undo bridge aging-time

【视图】

系统视图

【参数】

seconds：动态地址表的老化时间，取值范围为 10～1000000 秒，缺省为 300 秒。

【描述】

bridge aging-time 命令用来配置动态地址表的老化时间，**undo bridge aging-time** 命令用来恢复动态地址表老化时间的缺省值。

📖 说明：

当桥组学习到一个 MAC 地址时，如果 MAC 地址在地址表中不存在，则会创建一个新的地址表项，并初始老化定时器：

- 若在老化定时器超时前未收到来自此 MAC 地址的报文，等到老化定时器超时时，将删除此地址表项。
- 若在老化定时器超时前收到了来自此 MAC 地址的报文，等到老化定时器超时时，系统将重新初始老化定时器。

【举例】

配置动态地址表的老化时间为 500 秒。

```
[H3C] bridge aging-time 500
```

7.1.3 bridge bridge-set enable

【命令】

bridge *bridge-set* **enable**

undo bridge *bridge-set* **enable**

【视图】

系统视图

【参数】

bridge-set：网桥组编号，取值范围为 1～255。

【描述】

bridge *bridge-set* **enable** 命令用来使能桥组的桥接功能，**undo bridge** *bridge-set* **enable** 命令用来禁止桥组的桥接功能。

缺省情况下，禁止桥组的桥接功能。

只有使能桥组的桥接功能，桥组的配置才能生效。

【举例】

使能桥组 1 的桥接功能。

```
[H3C] bridge 1 enable
```

7.1.4 bridge bridging

【命令】

bridge *bridge-set* **bridging** { **ip** | **ipx** }

undo bridge *bridge-set* **bridging** { **ip** | **ipx** }

【视图】

系统视图

【参数】

bridge-set：网桥组号，取值范围为 1～255。

ip：IP 协议。

ipx：IPX 协议。

【描述】

bridge bridging 命令用来激活在指定网桥组上对网络层协议的桥接功能，**undo bridge bridging** 命令用来取消在指定网桥组上对网络层协议的桥接。

缺省情况下，激活桥接功能。

当在桥组内禁止 IP 和 IPX 协议的桥接功能后，对于需要进行桥接转发的 IP 和 IPX 报文，将会把其丢弃。

【举例】

禁止对 IP 协议的桥接功能。

```
[H3C] undo bridge 1 bridging ip
```

激活 IP 的桥接功能。

```
[H3C] bridge 1 bridging ip
```

7.1.5 bridge enable

【命令】

bridge enable

undo bridge enable

【视图】

系统视图

【参数】

无

【描述】

bridge enable 命令用来使能网桥功能，**undo bridge enable** 命令用来禁止网桥功能。

当存在已使能的桥组时，不能使用 **undo bridge enable** 命令来禁用网桥功能，需要先通过 **undo bridge** *bridge-set* **enable** 命令删除桥组。

缺省情况下，系统禁止网桥功能。

只有使能网桥功能，网桥的配置才能生效。

【举例】

使能网桥功能。

```
[H3C] bridge enable
```

7.1.6 bridge firewall unknown-mac

【命令】

bridge *bridge-set* **firewall unknown-mac** { **drop** | **flood** }

undo bridge *bridge-set* **firewall unknown-mac**

【视图】

系统视图

【参数】

bridge-set：网桥组编号，取值范围为 1～255。

drop：直接丢弃该未知目的 MAC 地址的 IP 单播、组播和广播报文。

flood：将此未知目的 MAC 地址的 IP 单播、组播和广播报文在除接收接口外的其它所有接口（接口必须属于某一安全区域）上泛洪。待收到响应报文后，则保存其 MAC 地址信息，后续报文将使用该 MAC 地址进行转发。

【描述】

bridge firewall unknown-mac 命令用来配置防火墙对未知目的 MAC 地址的单播、组播和广播 IP 报文的处理方式，**undo bridge firewall unknown-mac** 命令用来恢复缺省处理方式。

缺省情况下，防火墙对未知目的 MAC 地址的 IP 单播、组播和广播报文的处理方式为 **flood**。

相关配置请参考命令 **bridge firewall unknown-mac unicast**，**bridge firewall unknown-mac multicast**，**bridge firewall unknown-mac broadcast**。

【举例】

配置防火墙泛洪丢弃目的 MAC 地址的 IP 报文。

```
[H3C] bridge 1 firewall unknown-mac drop
```

7.1.7 bridge firewall unknown-mac broadcast

【命令】

bridge *bridge-set* **firewall unknown-mac broadcast** { **drop** | **flood** }

undo bridge *bridge-set* **firewall unknown-mac broadcast**

【视图】

系统视图

【参数】

bridge-set：网桥组编号，取值范围为 1～255。

drop：直接丢弃广播 IP 报文。

flood：将广播 IP 报文在除接收接口外的其它所有接口（接口必须属于某一安全区域）上泛洪。待收到响应报文后，保存其 MAC 地址信息。

【描述】

bridge firewall unknown-mac broadcast 命令用来配置防火墙对广播 IP 报文的处理方式，**undo bridge firewall unknown-mac broadcast** 命令用来恢复对广播 IP 报文的缺省处理方式。

缺省情况下，防火墙泛洪广播 IP 报文，即按照 **flood** 的方式进行处理。

【举例】

配置防火墙丢弃广播 IP 报文。

```
[H3C] bridge 1 firewall unknown-mac broadcast drop
```

7.1.8 bridge firewall unknown-mac multicast

【命令】

firewall unknown-mac multicast { **drop** | **flood** }

undo firewall unknown-mac multicast

【视图】

系统视图

【参数】

bridge-set：网桥组编号，取值范围为 1～255。

drop：直接丢弃组播 IP 报文。

flood：将组播 IP 报文在除接收接口外的其它所有接口（接口必须属于某一安全区域）上泛洪。待收到响应报文后，保存其 MAC 地址信息。

【描述】

bridge firewall unknown-mac multicast 命令用来配置防火墙对组播 IP 报文的处理方式，**undo bridge firewall unknown-mac multicast** 命令用来恢复对组播 IP 报文的缺省处理方式。

缺省情况下，防火墙泛洪组播 IP 报文，即按照 **flood** 的方式进行处理。

【举例】

配置防火墙丢弃组播 IP 报文。

```
[H3C] firewall unknown-mac multicast drop
```

7.1.9 bridge firewall unknown-mac unicast

【命令】

bridge *bridge-set* **firewall unknown-mac unicast** { **drop** | **arp** | **flood** }

undo bridge *bridge-set* **firewall unknown-mac unicast**

【视图】

系统视图

【参数】

bridge-set：网桥组编号，取值范围为 1～255。

drop：直接丢弃该未知目的 MAC 地址的 IP 报文。

arp：在除接收到该报文的接口外的其它所有接口（接口必须属于某一安全区域）上广播 ARP 请求报文，并且丢弃原来的未知 MAC 地址的 IP 报文。收到 ARP 响应报文后，保存 MAC 地址和接口的对应关系。

flood：将此未知目的 MAC 地址的 IP 报文在除接收接口外的其它所有接口（接口必须属于某一安全区域）上泛洪。待收到响应报文后，则保存其 MAC 地址信息，后续报文将使用该 MAC 地址进行转发。

【描述】

bridge firewall unknown-mac unicast 命令用来配置防火墙对未知目的 MAC 地址的 IP 单播报文的处理方式，**undo bridge firewall unknown-mac unicast** 命令用来恢复对未知目的 MAC 地址的 IP 单播报文的缺省处理方式。

缺省情况下，防火墙对未知目的 MAC 地址的单播 IP 报文按照 **flood** 方式进行处理。

【举例】

配置防火墙丢弃未知目的 MAC 地址的 IP 单播报文。

```
[H3C] bridge 1 firewall unknown-mac unicast drop
```

7.1.10 bridge learning

【命令】

bridge *bridge-set* **learning**

undo bridge *bridge-set* **learning**

【视图】

系统视图

【参数】

bridge-set：接口所属网桥组的编号，取值范围为 1～255。

【描述】

bridge learning 命令用来允许动态学习地址，**undo bridge learning** 命令用来禁止动态学习地址，即只使用静态地址表项进行转发。

缺省情况下，允许动态学习地址。

动态地址表项不需要手工维护，当网络拓扑结构有变化时能自动刷新。

当禁止动态学习地址功能后，先前地址表中通过动态学习的表项仍然会存在，并可以进行数据转发。当地址表项老化或手动将其清除后，动态表项才会被删除。

【举例】

允许动态学习 MAC 地址。

```
[H3C] bridge 1 learning
```

7.1.11 bridge mac-address

【命令】

bridge *bridge-set* **mac-address** *mac-address* { **permit interface** *interface-type interface-number* | **deny** }

undo bridge *bridge-set* **mac-address** *mac-address* [**interface** *interface-type interface-number*]

【视图】

系统视图

【参数】

bridge-set：接口所属的网桥组编号，取值范围为 1～255。

mac-address：以太网 MAC 地址，格式为 xxxx-xxxx-xxxx，用来匹配一个以太网目的 MAC 地址。

deny：丢弃目的地址为指定地址的帧。

permit：转发目的地址为指定地址的帧。

interface：指定一个出接口。

interface-type：接口类型。

interface-number：接口编号。

【描述】

bridge mac-address 命令用来手工配置网桥静态地址表项，**undo bridge mac-address** 命令用来删除静态地址表项。

一般情况下，网桥根据获取的 MAC 地址和接口的对应关系自动生成动态地址映射表项，但也可以由管理员手工配置静态地址映射表项，且静态地址映射表项永远不会老化。

【举例】

配置接口 Ethernet0/0/0 可转发 MAC 地址为 0000-0000-0111 的帧。

```
[H3C] bridge 1 mac-address 0000-0000-0111 permit interface Ethernet 0/0/0
```

7.1.12 bridge permit

【命令】

bridge permit { **bpdu** | **dlsw** | **ipx** }

undo bridge permit { **bpdu** | **dlsw** | **ipx** }

【视图】

系统视图

【参数】

bpdu：Bridge Protocol Data Unit，桥协议数据单元。

dlsw：Data Link Switching，数据链路交换。

ipx：Internetwork Packet Exchange，网际报文交换。

【描述】

bridge permit 命令用来配置允许通过的报文类型，**undo bridge permit** 命令用来配置拒绝通过的报文类型。

缺省情况下，允许 BPDU、DLSw 和 IPX 报文通过。

【举例】

配置禁止 BPDU 通过网桥。

```
[H3C] undo bridge permit bpdu
```

7.1.13 bridge vlanid-transparent-transmit enable

【命令】

bridge vlanid-transparent-transmit enable

undo bridge vlanid-transparent-transmit enable

【视图】

接口视图

【参数】

无

【描述】

bridge vlanid-transparent-transmit enable 命令用来使能 VLAN ID 透传功能。**undo bridge vlanid-transparent-transmit enable** 命令用来关闭 VLAN ID 透传功能。

VLAN ID 透传是指通过对加入桥组设备的出接口配置支持 VLAN ID 透传，使接口直接转发报文，不对该报文中的 VLAN ID 做任何处理。

通过 VLAN ID 透传，可以使加入桥组的非以太出接口也能转发带有 VLAN ID 的报文，而不会因此丢失 VLAN ID，并且即使加入桥组设备的出接口上有 VLAN ID 的情况下，也不会改变报文原有的 VLAN ID，从而实现不同 VLAN 的隔离。

当以太网子接口配置 VLAN ID 后，该子接口只会接收这个 VLAN 的数据，这就决定了该桥组负责传输哪些 VLAN 的数据。

在使能了 VLAN ID 透传功能以后，系统不对报文的 VLAN ID 做任何处理，两端相连的交换机可以看成是直接相连的。为了正常通信，用户需要给两端交换机的 trunk 口配置相同的 VLAN ID。

缺省情况下，关闭 VLAN ID 透传功能。

【举例】

在 Ethernet 0/0/0 接口上使能 VLAN ID 透传功能。

```
[H3C] interface Ethernet 0/0/0
[H3C-Ethernet0/0/0] bridge vlanid-transparent-transmit enable
```

7.1.14 bridge-set

【命令】

bridge-set *bridge-set*

undo bridge-set *bridge-set*

【视图】

接口视图

【参数】

bridge-set：网桥组编号，取值范围为 1～255。

【描述】

bridge-set 命令用来将接口加入到网桥组中，**undo bridge set** 命令用来将接口从网桥组中删除。

缺省情况下，未将任何接口加入网桥组。

对网桥而言，只有属于同一个网桥组的接口之间才能进行桥接。

接口加入桥组后，在接口上配置的三层属性将不生效。

同一桥组中的接口若要互相通信，需将接口加入到安全区域中；不同桥组中的接口若要互相通信，只需将 bridge-template 接口加入到安全区域中。

需要注意的是，如果网桥组所对应的桥模板已经使能 VRRP，则不允许非以太网类型的接口加入网桥组。

【举例】

将接口 Ethernet0/0/0 加入到网桥组 1 中。

```
[H3C] interface Ethernet0/0/0
[H3C-Ethernet0/0/0] bridge-set 1
```

7.1.15 bridge-set fast-forwarding

【命令】

bridge-set fast-forwarding [**inbound** | **outbound**]

undo bridge-set fast-forwarding [**inbound** | **outbound**]

【视图】

接口视图

【参数】

无

【描述】

bridge-set fast-forwarding 命令用来打开网桥的快速转发功能，undo **bridge-set fast-forwarding** 命令用来关闭网桥的快速转发功能。

缺省情况下，关闭网桥的快速转发功能。

【举例】

打开接口 Ethernet0/0/0 的网桥快速转发功能。

```
[H3C-Ethernet0/0/0] bridge-set fast-forwarding
```

7.1.16 debugging bridge eth-forwarding

【命令】

debugging bridge eth-forwarding [**interface** *interface-type interface-number*]

undo debugging bridge eth-forwarding [**interface** *interface-type interface-number*]

【视图】

用户视图

【参数】

interface-type：接口类型。

interface-number：接口编号。

【描述】

debugging bridge 命令用来打开网桥的以太帧转发调试信息开关，**undo debugging bridge** 命令用来关闭调试信息开关。

【举例】

打开网桥的以太帧转发调试信息开关。

```
<H3C> debugging bridge eth-forwarding
```

7.1.17 debugging bridge ip-forwarding

【命令】

debugging bridge ip-forwarding

undo debugging bridge ip-forwarding

【视图】

用户视图

【参数】

无

【描述】

debugging bridge ip-forwarding 命令用来打开网桥的 IP 转发调试开关，**undo** 命令用来关闭网桥的 IP 转发调试开关。

缺省情况下，关闭网桥的 IP 转发调试开关。

【举例】

打开网桥的 IP 转发调试开关。

```
<H3C> debugging bridge ip-forwarding
*0.11355193 H3C FWTP/8/rcv_ip:Receive an IP packet
    interface: Ethernet0/0/0
    source_ip_addr : 192.168.3.6
    source_port : 33073
    destination_ip_addr : 192.168.3.8
    destination_port : 52128
    protocol : 1

*0.11355193 H3C FWTP/8/sndto_secur:Send an IP packet to security module
    source_ip_addr : 192.168.3.6
    source_port : 17664
    destination_ip_addr : 192.168.3.8
    destination_port : 60
    protocol : 1
    return value:0

*0.11355193 H3C FWTP/8/snd_ip:Send an IP packet
    interface: Ethernet0/0/0
    source_ip_addr : 192.168.3.6
    source_port : 0
    destination_ip_addr : 192.168.3.8
```

```
    destination_port : 1
    protocol : 1

*0.11355193 H3C FWTP/8/rcv_ip:Receive an IP packet
    interface: Ethernet0/0/0
    source_ip_addr : 192.168.3.8
    source_port : 33073
    destination_ip_addr : 192.168.3.6
    destination_port : 52128
    protocol : 1

*0.11355193 H3C FWTP/8/sndto_secur:Send an IP packet to security module
    source_ip_addr : 192.168.3.8
    source_port : 17664
    destination_ip_addr : 192.168.3.6
    destination_port : 60
    protocol : 1
    return value:0

*0.11355193 H3C FWTP/8/snd_ip:Send an IP packet
    interface: Ethernet0/0/0
    source_ip_addr : 192.168.3.8
    source_port : 0
    destination_ip_addr : 192.168.3.6
    destination_port : 1
    protocol : 1
```

7.1.18 debugging firewall eff

【命令】

debugging firewall eff [**interface** *interface-type interface-number*]

undo debugging firewall eff [**interface** *interface-type interface-number*]

【视图】

用户视图

【参数】

interface *interface-type interface-number*：特定接口的调试信息。

【描述】

debugging firewall eff 命令用来打开以太帧过滤的调试开关，**undo debugging firewall eff** 命令用来关闭以太帧过滤的调试开关。

缺省情况下，关闭以太帧过滤的调试开关。

【举例】

打开以太帧过滤的调试开关。

```
<H3C> debugging firewall eff
 Ethernet-frame-filter's debugging is on
<H3C>
*0.1350738 H3C EFF/8/DEBUGGING:
 OutBound List 4001, deny the frame with the following head :
 dest-mac is 000f-1f7e-fec5,sour-mac is 00e0-fc36-a7a9, type is 0800
*0.1350739 H3C BRIDGE/8/DEBUGGING:
Discard a frame for the filter on outport ; received from interface GigabitEther
net0/1;and try to send to interface GigabitEthernet0/0, with following frame
head :
00 0f 1f 7e fe c5 00 e0 fc 36 a7 a9 08 00
*0.1352740 H3C EFF/8/DEBUGGING:
 OutBound List 4001, deny the frame with the following head :
 dest-mac is 000f-1f7e-fec5,sour-mac is 00e0-fc36-a7a9, type is 0800
*0.1352740 H3C BRIDGE/8/DEBUGGING:
Discard a frame for the filter on outport ; received from interface GigabitEther
net0/1;and try to send to interface GigabitEthernet0/0, with following frame
head :
00 0f 1f 7e fe c5 00 e0 fc 36 a7 a9 08 00
*0.1352925 H3C EFF/8/DEBUGGING:
 InBound List 4001, deny the frame with the following head :
 dest-mac is ffff-ffff-ffff,sour-mac is 000f-1f7e-fec5, type is 0806
*0.1352925 H3C BRIDGE/8/DEBUGGING:
Discard a frame for the filter on inport ; received from interface GigabitEthern
et0/0, with following frame head :
ff ff ff ff ff ff 00 0f 1f 7e fe c5 08 06
*0.1354741 H3C EFF/8/DEBUGGING:
 OutBound List 4001, deny the frame with the following head :
 dest-mac is 000f-1f7e-fec5,sour-mac is 00e0-fc36-a7a9, type is 0800
*0.1354741 H3C BRIDGE/8/DEBUGGING:
Discard a frame for the filter on outport ; received from interface GigabitEther
net0/1;and try to send to interface GigabitEthernet0/0, with following frame
head :
00 0f 1f 7e fe c5 00 e0 fc 36 a7 a9 08 00
*0.1356742 H3C EFF/8/DEBUGGING:
 OutBound List 4001, deny the frame with the following head :
 dest-mac is 000f-1f7e-fec5,sour-mac is 00e0-fc36-a7a9, type is 0800
*0.1356742 H3C BRIDGE/8/DEBUGGING:
```

```
Discard a frame for the filter on outport ; received from interface GigabitEther
net0/1;and try to send to interface GigabitEthernet0/0, with following frame
head :
00 0f 1f 7e fe c5 00 e0 fc 36 a7 a9 08 00
```

7.1.19 display bridge address-table

【命令】

display bridge address-table [**bridge-set** *bridge-set* | **interface** *interface-type interface-number* | **mac** *mac-address*] [**dynamic** | **static**]

【视图】

任意视图

【参数】

bridge-set：桥组号，取值范围为 1～255。

interface-type：接口类型。

interface-number：接口编号。

mac-address：MAC 地址，形式为 xxxx-xxxx-xxxx 的一组十六进制数。

dynamic：进行动态地址筛选。

static：进行静态地址筛选。

【描述】

display bridge address-table 命令用来显示 MAC 地址转发表的信息。

【举例】

显示桥组 1 中的 MAC 地址表项。

```
[H3C] display bridge address-table bridge-set 1
 The total of the address-items is 2
 Mac-address     Set  Flag  Aging-time   Receive      Send   Interface-name
 0001-0001-0001   1    PD   00:04:40         15         15   Ethernet0/0/1
 0002-0002-0002   1    PD   00:04:40         15         15   Ethernet0/0/0
 Flag meaning:  P--PERMIT   N--DENY  D--DYNAMIC  S--STATIC
```

该显示信息主要内容解释如下表。

表7-1 display bridge address-table 命令输出信息描述

主要字段	描述
Mac-Address	MAC 地址
Set	桥组编号

主要字段	描述
Flag	有四种取值分别为：P--PERMIT N--DENY D--DYNAMIC S--STATIC P：表示 MAC 地址过滤采用“允许”规则 N：表示 MAC 地址过滤采用“拒绝”规则 D：表示该表项是动态表项 S：表示该表项是静态表项
Aging-time	转发表项的剩余生存时间
Receive	接收此源 MAC 地址的报文计数
Send	转发此目的 MAC 地址的报文计数
Interface-name	出接口名

7.1.20 display bridge information

【命令】

display bridge information [**bridge-set** *bridge-set*]

【视图】

任意视图

【参数】

bridge-set：桥组号，取值范围为 1～255。

【描述】

display bridge information 命令用来显示网桥模块中所有或指定桥组的信息。

【举例】

显示所有桥组的信息。

```
[H3C] display bridge information
 Bridge module is activated,2 port take part in bridge module at all;
 Address table has 2 item, with  0 static one; life cycle is 300 (s).

Bridge set 1 :
  configure :bridge 1 enable;
             bridging ip, bridging ipx;
             bridge 1 learning
 Unknown-mac: Unicast IP packet  :flood
              broadcast IP packet: flood
              Multicast IP packet: flood
```

```
  interface :total 2 interface(s) in the set
            Ethernet0/0/0 : up
            Ethernet0/0/1 : up
```

该显示信息主要内容解释如下表。

表7-2 display bridge information 命令输出信息描述

主要字段	描述
Configure	该部分显示了桥组的配置属性，比如桥组 1 的 configure 部分显示了它能桥接 IP 包和 IPX 包，以及能进行动态 MAC 地址学习
Unknown-mac	该部分显示了对于未知目的 MAC 地址的单播 IP 报文、广播 IP 报文和组播 IP 报文的处理方式。
interface	该部分显示了本桥组所包含的接口及他们各自的状态，比如桥组 1 说明了其中有 2 个接口参与桥接：Ethernet0/0/0 和 Ethernet0/0/1，它们的状态都是 up。注意在表示接口的状态时：up 表示接口处于活动状态，down 则表示接口处于非活动状态，只有当接口状态处于 up 时，桥组才能完成桥接的功能

7.1.21 display bridge traffic

【命令】

display bridge traffic [**bridge-set** *bridge-set* | **interface** *interface-type interface-number*]

【视图】

任意视图

【参数】

bridge-set：桥组号，取值范围为 1～255。

interface-type：接口类型。

Interface-number：接口编号。

【描述】

display bridge traffic 命令用来显示桥组中接口的流量统计数据。

【举例】

显示 Ethernet0/0/0 接口的流量信息。

```
[H3C] display bridge traffic interface Ethernet0/0/0
the statistic of interface Ethernet0/0/0
 Input:
         46 total, 0 bpdu, 16 unicast,
         0 multi, 30 broadcast;
```

```
        46 ip,0 ipx, 0 other protocol;
        0 eth2, 0 snap,
        0 dlsw,
        0 vlan,
        0 other;
Output:
        15 total, 0 bpdu, 15 unicast,
        0 multi, 0 broadcast;
        15 ip, 0 ipx, 0 other protocol;
        0 eth2, 0 snap,
        0 dlsw,
        0 vlan,
        0 other;
Send way:
        0 broadcast, 0 fast, 0 other
Discard:
        0 by inport state,
        0 for local frame ,
        0 by mac table,
        0 by inport filter,
        0 by outport filter,
        0 by ip filter ,
        0 other
```

该显示信息主要内容解释如下表。

表7-3 display bridge traffic 命令输出信息描述

主要字段	描述
Input	表示该接口输入报文的种类和数量，“10 total, 1 bpdu, 2 single,”表示总共被输入了 10 个数据包，其中 1 个 BPDU 报文，2 个单播报文
Output	表示该接口输出报文的种类和数量
Send way	表示发送数据的方式
Discard	表示报文被丢弃的原因和数量
0 by inport state	由于入接口的状态异常而丢弃帧的数量
0 for local frame	由于出接口等于入接口而丢弃帧的数量
0 by mac table	由于 MAC 转发表中配置的禁止表项而丢弃帧的数量
0 by inport filter	由于入接口上配置的过滤规则而丢弃帧的数量
0 by outport filter	由于出接口上配置的过滤规则而丢弃帧的数量

主要字段	描述
0 by ip filter	由于 IP 层配置的过滤规则而丢弃帧的数量
0 other	由于其他原因而丢弃帧的数量

7.1.22 display firewall ethernet-frame-filter

【命令】

display firewall ethernet-frame-filter { **all** | **interface** *interface-type interface–number* }

【视图】

任意视图

【参数】

interface-type：接口类型。

interface-number：接口编号。

all：所有接口上的以太帧过滤统计信息。

【描述】

display firewall ethernet-frame-filter 命令用来查看接口上的以太帧过滤统计信息。

【举例】

显示 Ethernet0/0/0 接口上的以太帧过滤统计信息。

```
[H3C] display firewall ethernet-frame-filter interface Ethernet0/0/0
Interface: Ethernet0/0/0
  In-bound Policy: acl 4000
        From 2003-06-07 14:46:59  to 2003-06-07 16:16:23
             0 packets, 0 bytes, 0% permitted,
             0 packets, 0 bytes, 0% denied,
             0 packets, 0 bytes, 0% permitted default,
             0 packets, 0 bytes, 0% denied default,
       Totally 0 packets, 0 bytes, 0% permitted,
       Totally 0 packets, 0 bytes, 0% denied.
  Out-bound Policy: acl 4000
       From 2003-06-07 15:59:23  to 2003-06-07 16:16:23
             0 packets, 0 bytes, 0% permitted,
             0 packets, 0 bytes, 0% denied,
             0 packets, 0 bytes, 0% permitted default,
```

```
        0 packets, 0 bytes, 0% denied default,
    Totally 0 packets, 0 bytes, 0% permitted,
    Totally 0 packets, 0 bytes, 0% denied.
```

7.1.23 display interface bridge-template

【命令】

display interface bridge-template *interface-number*

【视图】

任意视图

【参数】

interface-number：接口编号。

【描述】

display interface bridge-template 命令用来显示 bridge-template 接口的状态。

【举例】

显示接口 bridge-template1 的状态。

```
<H3C> display interface bridge-template 1
Bridge-template1 current state :UP
Line protocol current state :UP
Description : Bridge-template1 Interface
The Maximum Transmit Unit is 1500
Internet Address is 2.0.0.1/30
IP Sending Frames' Format is PKTFMT_ETHNT_2, Hardware address is
000f-e207-f301
    47881 packets input, 5937028 bytes, 0 drops
    3 packets output, 156 bytes, 0 drops
```

表7-4 display interce bridge-template 命令显示信息表

选项	意义
Bridge-template1 current state :UP	bridge-template 接口的状态
Line protocol current state :UP	链路协议状态
Description : Bridge-template1 Interface	接口描述
The Maximum Transmit Unit is 1500	最大传输单元值
Internet Address is 2.0.0.1/30	接口 IP 地址
IP Sending Frames' Format is PKTFMT_ETHNT_2, Hardware address is 000f-e207-f301	帧格式和 MAC 地址

选项	意义
47881 packets input, 5937028 bytes, 0 drops 3 packets output, 156 bytes, 0 drops	接口接收和发送的数据统计

7.1.24 firewall ethernet-frame-filter

【命令】

firewall ethernet-frame-filter *acl-number* { **inbound** | **outbound** }

undo firewall ethernet-frame-filter { **inbound** | **outbound** }

【视图】

以太网接口视图

【参数】

acl-number：基于 MAC 地址的 ACL 编号，范围为 4000～4999。

inbound：过滤从接口接收的帧。

outbound：过滤从接口发送的帧。

【描述】

firewall ethernet-frame-filter 命令用来将基于 MAC 地址的 ACL 应用到接口上，**undo firewall ethernet-frame-filter** 命令用来从接口上删除基于 MAC 地址的 ACL。

要将基于 MAC 地址的访问控制列表应用到接口上，接口必须被加入到桥组中，否则系统会提示错误信息。

对于桥组中的接口，报文进行二层的过滤之后还要进行三层的过滤。

缺省情况下，未在接口上应用任何基于 MAC 地址的 ACL。

【举例】

在以太网接口 Ethernet0/0/1 的入方向上应用编号为 4009 的基于 MAC 地址的 ACL。

```
[H3C] interface Ethernet0/0/1
[H3C-Ethernet0/0/1] bridge-set 1
[H3C-Ethernet0/0/1] firewall ethernet-frame-filter 4009 inbound
```

7.1.25 interface bridge-template

【命令】

interface bridge-template *bridge-set*

undo interface bridge-template *bridge-set*

【视图】

系统视图

【参数】

bridge-set：网桥组编号，取值范围为 1～255。

【描述】

interface bridge-template 命令用来创建 bridge-template 接口，并将指定的网桥组连接到路由的网络中。**undo interface bridge-template** 命令用来删除 bridge-template 接口。

对于每个网桥组来说，只能有一个 bridge-template 接口。

【举例】

创建接口 bridge-template 1 。

```
[H3C] interface bridge-template 1
[H3C-Bridge-template1]
```

7.1.26 mac-address

【命令】

mac-address *H-H-H*

undo mac-address

【视图】

bridge-template 接口视图

【参数】

H-H-H：MAC 地址。

【描述】

mac-address 命令用来手工配置 bridge-template 接口的 MAC 地址，**undo mac-address** 命令用来取消手工配置的 bridge-template 接口的 MAC 地址。

缺省情况下，bridge-template 接口使用的是自动生成的 MAC 地址。

【举例】

手工配置 bridge-template 1 接口的 MAC 地址为 123-234-345。

```
[H3C-Bridge-template1] mac-address 123-234-345
```

7.1.27 reset bridge address-table

【命令】

reset bridge address-table [**bridge-set** *bridge-set* | **interface** *interface-type interface-number*]

【视图】

用户视图

【参数】

bridge-set：网桥组编号，取值范围为 1～255。

interface-type：接口类型。

interface-number：接口编号。

【描述】

reset bridge address-table 命令用来清除转发表中所有或者指定桥组或者指定接口的动态地址表项。

【举例】

清除转发表中所有关于网桥组 1 的动态表项。

```
<H3C> reset bridge address-table bridge-set 1
```

7.1.28 reset bridge traffic

【命令】

reset bridge traffic [**bridge-set** *bridge-set* | **interface** *interface-type interface-number*]

【视图】

用户视图

【参数】

bridge-set：桥组号，取值范围为 1～255。

interface-type：接口类型。

interface-number：接口编号。

【描述】

reset bridge traffic 命令用来清除桥组中接口上的流量统计数据。

【举例】

清除桥组 1 的流量统计信息。

```
<H3C> reset bridge traffic bridge-set 1
```

7.1.29 reset firewall ethernet-frame-filter

【命令】

reset firewall ethernet-frame-filter { **all** | **interface** *interface-type interface-number* }

【视图】

用户视图

【参数】

all：所有接口上的以太帧的过滤信息。

interface *interface-type interface-number*：特定接口上的以太帧的过滤信息。

【描述】

reset firewall ethernet-frame-filter 命令用来清除以太帧的过滤信息。

【举例】

清除所有接口上的以太帧过滤信息。

```
<H3C> reset firewall ethernet-frame-filter all
```

7.1.30 rule

【命令】

rule [*rule-id*] { **permit** | **deny** } [**type** *type-code type-wildcard* | **lsap** *lsap-code lsap-wildcard*] [**source-mac** *sour-addr source-wildcard*] [**dest-mac** *dest-addr dest-wildcard*] [**time-range** *time-name*] [**logging**]

undo rule *rule-id* [**time-range**] [**logging**]

【视图】

基于 MAC 地址的 ACL 视图

【参数】

rule-id：ACL 的规则编号，范围为 0～65534。当指定了编号，如果与编号对应的规则已经存在，则会部分覆盖旧的规则，相当于编辑一个已经存在的 ACL 规则。故建议用户在编辑一个已存在编号的规则时，先将旧的规则删除，再创建新的规则，否则配置结果可能与预期的效果不同。如果与编号对应的规则不存在，则使用指定的

编号创建一个新的规则。如果不指定编号，表示增加一个新规则，系统自动会为这个规则分配一个编号。

permit：表示允许符合条件的数据包。

deny：表示拒绝符合条件的数据包。

type：数据帧的类型。

type-code：数据帧的类型值，一个 16 比特的十六进制数，对应Ethernet_II类型和Ethernet_SNAP类型帧中的type-code域。关于*type-code*的值请参考 表 7-5。

type-mask：类型掩码，是一个 16 比特的十六进制数，用于指定屏蔽位。

lsap：数据帧的封装格式。

lsap-code：数据帧的封装格式的值，是一个 16 比特的十六进制数。

lsap-mask：lsap 值的掩码，是一个 16 比特的十六进制数，用于指定屏蔽位。

source-mac：源 MAC 地址。

sour-addr：源 MAC 地址，格式为 xxxx-xxxx-xxxx，用来匹配一个分组的源地址。

sour-mask：源 MAC 地址的掩码。

dest-mac：目的 MAC 地址。

dest-addr：目的 MAC 地址，格式为 xxxx-xxxx-xxxx，用来匹配一个分组的源地址。

dest-mask：目的 MAC 地址的掩码。

logging：对符合条件的数据包记录日志。目前支持此选项的业务只有包过滤防火墙（在接口下被 **firewall packet-filter** 命令引用）。

time-range *time-name*：配置这条访问控制规则生效的时间段。

【描述】

rule 命令用来添加一个 ACL 规则，**undo rule** 命令用来删除 ACL 规则。

缺省情况下，未创建任何 ACL 规则。

【举例】

配置一条拒绝任何以太网帧的规则。

```
[H3C] acl number 4009
[H3C-acl-ethernetframe-4009] rule deny
```

表7-5 以太网类型域值表

以太网类型域值（16 进制值）	描述
0000-05DC	IEEE802.3 Length Field
0101-01FF	Experimental
200	XEROX PUP (see 0A00)

以太网类型域值（16 进制值）	描述
201	PUP Addr Trans (see 0A01)
400	Nixdorf
600	XEROX NS IDP
660	DLOG
661	DLOG
800	Internet IP (IPv4)
801	X.75 Internet
802	NBS Internet
803	ECMA Internet
804	Chaosnet
805	X.25 Level 3
806	ARP
807	XNS Compatability
081C	Symbolics Private
0888-088A	Xyplex
900	Ungermann-Bass net debugr
0A00	Xerox IEEE802.3 PUP
0A01	PUP Addr Trans
0BAD	Banyan Systems
1000	Berkeley Trailer nego
1001-100F	Berkeley Trailer encap/IP
1600	Valid Systems
4242	PCS Basic Block Protocol
5208	BBN Simnet
6000	DEC Unassigned (Exp.)
6001	DEC MOP Dump/Load
6002	DEC MOP Remote Console
6003	DEC DECNET Phase IV Route
6004	DEC LAT
6005	DEC Diagnostic Protocol
6006	DEC Customer Protocol
6007	DEC LAVC, SCA
6008-6009	DEC Unassigned
6010-6014	3Com Corporation

以太网类型域值（16 进制值）	描述
7000	Ungermann-Bass download
7002	Ungermann-Bass dia/loop
7020-7029	LRT
7030	Proteon
7034	Cabletron
8003	Cronus VLN
8004	Cronus Direct
8005	HP Probe
8006	Nestar
8008	AT&T
8010	Excelan
8013	SGI diagnostics
8014	SGI network games
8015	SGI reserved
8016	SGI bounce server
8019	Apollo Computers
802E	Tymshare
802F	Tigan, Inc.
8035	Reverse ARP
8036	Aeonic Systems
8038	DEC LANBridge
8039-803C	DEC Unassigned
803D	DEC Ethernet Encryption
803E	DEC Unassigned
803F	DEC LAN Traffic Monitor
8040-8042	DEC Unassigned
8044	Planning Research Corp.
8046	AT&T
8047	AT&T
8049	ExperData
805B	Stanford V Kernel exp.
805C	Stanford V Kernel prod.
805D	Evans & Sutherland
8060	Little Machines

以太网类型域值（16 进制值）	描述
8062	Counterpoint Computers
8065	Univ. of Mass. @ Amherst
8066	Univ. of Mass. @ Amherst
8067	Veeco Integrated Auto.
8068	General Dynamics
8069	AT&T
806A	Autophon
806C	ComDesign
806D	Computgraphic Corp.
806E-8077	Landmark Graphics Corp.
807A	Matra
807B	Dansk Data Elektronik
807C	Merit Internodal
807D-807F	Vitalink Communications
8080	Vitalink TransLAN III
8081-8083	Counterpoint Computers
809B	Appletalk
809C-809E	Datability
809F	Spider Systems Ltd.
80A3	Nixdorf Computers
80A4-80B3	Siemens Gammasonics Inc.
80C0-80C3	DCA Data Exchange Cluster
80C4	Banyan Systems
80C5	Banyan Systems
80C6	Pacer Software
80C7	Applitek Corporation
80C8-80CC	Intergraph Corporation
80CD-80CE	Harris Corporation
80CF-80D2	Taylor Instrument
80D3-80D4	Rosemount Corporation
80D5	IBM SNA Service on Ether
80DD	Varian Associates
80DE-80DF	Integrated Solutions TRFS
80E0-80E3	Allen-Bradley

以太网类型域值（16 进制值）	描述
80E4-80F0	Datability
80F2	Retix
80F3	AppleTalk AARP (Kinetics)
80F4-80F5	Kinetics
80F7	Apollo Computer
80FF-8103	Wellfleet Communications
8107-8109	Symbolics Private
8130	Hayes Microcomputers
8131	VG Laboratory Systems
8132-8136	Bridge Communications
8137-8138	Novell, Inc.
8139-813D	KTI
8148	Logicraft
8149	Network Computing Devices
814A	Alpha Micro
814C	SNMP
814D	BIIN
814E	BIIN
814F	Technically Elite Concept
8150	Rational Corp
8151-8153	Qualcomm
815C-815E	Computer Protocol Pty Ltd
8164-8166	Charles River Data System
817D-818C	Protocol Engines
818D	Motorola Computer
819A-81A3	Qualcomm
81A4	ARAI Bunkichi
81A5-81AE	RAD Network Devices
81B7-81B9	Xyplex
81CC-81D5	Apricot Computers
81D6-81DD	Artisoft
81E6-81EF	Polygon
81F0-81F2	Comsat Labs
81F3-81F5	SAIC

以太网类型域值（16 进制值）	描述
81F6-81F8	VG Analytical
8203-8205	Quantum Software
8221-8222	Ascom Banking Systems
823E-8240	Advanced Encryption Syste
827F-8282	Athena Programming
8263-826A	Charles River Data System
829A-829B	Inst Ind Info Tech
829C-82AB	Taurus Controls
82AC-8693	Walker Richer & Quinn
8694-869D	Idea Courier
869E-86A1	Computer Network Tech
86A3-86AC	Gateway Communications
86DB	SECTRA
86DE	Delta Controls
86DF	ATOMIC
86E0-86EF	Landis & Gyr Powers
8700-8710	Motorola
8A96-8A97	Invisible Software
9000	Loopback
9001	3Com(Bridge) XNS Sys Mgmt
9002	3Com(Bridge) TCP-IP Sys
9003	3Com(Bridge) loop detect
FF00	BBN VITAL-LanBridge cache
FF00-FF0F	ISC Bunker Ramo

第8章 PKI 配置命令

8.1 PKI 域配置命令

8.1.1 ca identifier

【命令】

ca identifier *name*

undo ca identifier

【视图】

PKI 域视图

【参数】

name：本设备信任的 CA 标识符。长度范围为 1～63 个字符。

【描述】

ca identifier 命令用来指定本设备信任的 CA，将本设备与名称为 *name* 的 CA 进行绑定。**undo ca identifier** 命令用来删除本设备信任的 CA。

缺省情况下，未指定本设备信任的 CA。

在未删除该 CA 之前，该设备证书的申请、获取、撤消及查询均是通过该 CA 执行。

【举例】

指定本设备信任的 CA 的名称。

```
[H3C-pki-domain-1] ca identifier new-ca
```

8.1.2 certificate request entity

【命令】

certificate request entity *entity-name*

undo certificate request entity

【视图】

PKI 域视图

【参数】

entity-name：申请证书所用的实体名称，该名称必须与 **pki entity** 命令定义的名称

保持一致。长度范围为 1～15 个字符。

【描述】

certificate request entity 命令用来指定申请证书所用的实体名称，**undo certificate request entity** 命令用来取消申请证书所用的实体名称。

缺省情况下，未指定设备申请证书所使用的实体名称。

相关命令请参考 **pki entity**。

【举例】

指定设备申请证书时使用实体“en”。

```
[H3C-pki-domain-1] certificate request entity en
```

8.1.3 certificate request from

【命令】

certificate request from { **ca** | **ra** }

undo certificate request from

【视图】

PKI 域视图

【参数】

ca：表示实体从 CA 注册申请证书。

ra：表示实体从 RA 注册申请证书。

【描述】

certificate request from 命令用来为实体指定是通过 CA 还是 RA 注册申请证书。**undo certificate request from** 命令用来删除所选定的证书注册受理机构。

RA 是 CA 证书发放管理的延伸，它负责证书申请者的信息录入、审核以及证书发放等工作，但其并无证书的签发功能。在一些小的 PKI 系统中，RA 的职能可由 CA 来完成，而不设立独立运行的 RA。

缺省情况下，未指定本设备证书申请的注册受理机构。PKI 安全策略推荐使用 RA 作为注册审理机构。

【举例】

指定实体从 CA 注册申请证书。

```
[H3C-pki-domain-1] certificate request from ca
```

8.1.4 certificate request mode

【命令】

certificate request mode { **manual** | **auto** [**key-length** *key-length* | **password** { **simple** | **cipher** } *password*]* }

undo certificate request mode

【视图】

PKI 域视图

【参数】

manual：表示用手工方式申请证书。

auto：表示用自动方式申请证书。

key-length：指定 RSA 密钥长度，最小长度为 512 位，最大长度为 2048 位。

simple：指定密码以明文形式显示。

cipher：指定密码以加密形式显示。

password：指定吊销证书时使用的密码，长度为 1～31 个字符。

【描述】

certificate request mode 命令用来指定证书申请是手工发起，还是自动发起。**undo certificate request mode** 命令用来恢复证书申请方式为缺省值。

如果是自动方式，则在本地没有自己的证书时自动向注册机构进行申请，而且在证书快要过期时自动申请新的证书。如果为手工方式，则需要手工完成各项证书申请工作。

缺省情况下，证书申请为手工方式。

相关命令请参考 **pki request-certificate**。

【举例】

指定证书申请为自动发起方式。

```
[H3C-pki-domain-1] certificate request mode auto
```

8.1.5 certificate request polling

【命令】

certificate request polling { **interval** *minutes* | **count** *count* }

undo certificate request polling { **interval** | **count** }

【视图】

PKI 域视图

【参数】

minutes：指定两次查询之间的时间间隔。单位分钟，取值范围为 5～168 分钟，缺省为 20 分钟。

count：重试次数。取值范围为 1～100，缺省为 5。

【描述】

certificate request polling 命令用来指定两次状态查询之间的时间间隔以及重传次数。**undo certificate request polling** 命令用来恢复缺省参数。

在发送证书申请后，如果 CA 采用手工验证申请，会需要很长时间才能发布证书，客户端需要定期发送状态查询，以便在证书签发后能及时获取到证书。

相关命令请参考 **display pki certificate**。

【举例】

指定两次状态查询之间的时间间隔和查询重试次数。

```
[H3C-pki-domain-1] certificate request polling interval 15
[H3C-pki-domain-1] certificate request polling count 40
```

8.1.6 certificate request url

【命令】

certificate request url *string*

undo certificate request url

【视图】

PKI 域视图

【参数】

string：表示证书申请的注册机构服务器位置 URL。长度范围为 1～127 个字符。内容包括服务器位置及 CA 的 CGI 命令接口脚本位置，格式为 *http://server_location /ca_script_location*。其中 *server_location* 以 IP 地址表示，目前不支持使用服务器名称表示。

【描述】

certificate request url 命令用来指定本设备通过 SCEP 协议进行证书申请的服务器位置 URL，SCEP 是专门用于与认证权威机构进行通信的协议。**undo certificate request url** 命令用来删除设置的证书申请的服务器位置。

缺省情况下，未指定证书申请机构的服务器位置 URL。

【举例】

指定证书申请的服务器位置。

```
[H3C-pki-domain-1] certificate request url http://169.254.0.100/certsrv/mscep/mscep.dll
```

8.1.7 crl check disable

【命令】

crl check disable

undo crl check disable

【视图】

PKI 域视图

【参数】

无

【描述】

crl check disable 命令用来禁止 CRL 检查，**undo crl check disable** 命令用来使能 CRL 检查。

缺省情况下，使能 CRL 检查。

【举例】

禁止 CRL 检查。

```
[H3C-pki-domain-1] crl check disable
```

8.1.8 crl update-period

【命令】

crl update-period *hours*

undo crl update-period

【视图】

PKI 域视图

【参数】

hours：指定更新周期，范围为 1～720，单位为“小时”。

【描述】

crl update-period 指定 CRL 的更新周期，CRL 的更新周期是指本地从 CRL 存储服务器上下载 CRL 的时间间隔。**undo crl update-period** 命令用来恢复 CRL 更新周期为缺省值。

缺省情况下，更新周期为 0 小时，根据 CRL 的有效期进行更新。

【举例】

指定 CRL 的更新周期为 20 小时。

```
[H3C-pki-domain-1] crl update-period 20
```

8.1.9 crl url

【命令】

crl url { *url-string* | **scep** }

undo crl url

【视图】

PKI 域视图

【参数】

url-string：表示 CRL 的发布点位置，长度范围为 1～127 个字符。格式为 *http://server_location* 或 *ldap://server_location*，其中 *server_location* 以 IP 地址表示，目前不支持使用服务器名称表示。

scep：使用 SCEP 获取 CRL。

【描述】

crl url 命令用来设置 CRL 发布点位置 URL。**undo crl url** 命令用来撤消该 URL。

缺省情况下，未指定 CRL 发布点位置 URL。

【举例】

指定 CRL 库的 URL 位置。

```
[H3C-pki-domain-1] crl url http://192.168.19.2/certenroll/win2000.crl
```

8.1.10 ldap-server

【命令】

ldap-server ip *ip-address* [**port** *port-num*] [**version** *version-number*]

undo ldap-server

【视图】

PKI 域视图

【参数】

ip-address：LDAP 服务器的 IP 地址。

port-num：LDAP 服务器的端口号。取值范围 1～65535，缺省为 389。

version-number：LDAP 版本号。可取值为 2 或 3，缺省为 2。

【描述】

ldap-server ip 命令用来设置 LDAP 服务器地址及端口。**undo ldap-server** 命令用来撤消 LDAP 服务器地址及端口。

缺省情况下，未指定 LDAP 服务器。

【举例】

指定 LDAP 服务器的位置。

```
[H3C-pki-domain-1] ldap-server ip 169.254.0 30
```

8.1.11 pki domain

【命令】

pki domain *name*

undo pki domain *name*

【视图】

系统视图

【参数】

name：该参数为本设备指定 PKI 域，用于表示本设备是属于哪一个 PKI 域，供其它命令引用时指定。长度范围为 1～15 个字符。

【描述】

pki domain 命令用来创建 PKI 域并进入 PKI 域视图。**undo pki domain** 命令用来删除指定的 PKI 域。

缺省情况下，未创建 PKI 域。

【举例】

创建并进入 PKI 域视图。

```
[H3C] pki domain 1
[H3C-pki-domain-1]
```

8.1.12 root-certificate fingerprint

【命令】

root-certificate fingerprint { **md5** | **sha1** } *string*

undo root-certificate fingerprint

【视图】

PKI 域视图

【参数】

md5：使用 MD5 指纹。

sha1：使用 SHA1 指纹。

string：指定所使用的指纹。当选择 MD5 指纹时，*string* 必须为 32 个字符，并且以 16 进制的形式输入；当选择 SHA1 指纹时，*string* 必须为 40 个字符，并且以 16 进制的形式输入。

【描述】

root-certificate fingerprint 命令用来配置验证 CA 根证书时所使用的指纹，**undo root-certificate fingerprint** 命令用来取消配置的指纹。

缺省情况下，未配置验证 CA 根证书时使用的指纹。

【举例】

配置验证 CA 根证书时使用的 MD5 指纹。

```
[H3C-pki-domain-1] root-certificate fingerprint md5
12EF53FA355CD23E12EF53FA355CD23E
```

配置验证 CA 根证书时使用的 SHA1 指纹。

```
[H3C-pki-domain-1] root-certificate fingerprint sha1
D1526110AAD7527FB093ED7FC037B0B3CDDDAD93
```

8.2 PKI 实体配置命令

8.2.1 fqdn

【命令】

fqdn *name-str*

undo fqdn

【视图】

PKI 实体视图

【参数】

name-str：实体的 FQDN 名。长度范围为 1～127 个字符。

【描述】

fqdn 命令用来指定实体的 FQDN 名称。**undo fqdn** 命令用来删除实体的 FQDN 名称。

缺省情况下，未指定实体的 FQDN。

FQDN（Fully Qualified Domain Name）是实体在网络中的唯一标识，如 Email 地址，可被解析为 IP 地址，一般形式为：user.domain。

【举例】

配置实体的 FQDN。

```
[H3C-pki-entity-1] fqdn secpath.myentity.com
```

8.2.2 common-name

【命令】

common-name *name-str*

undo common-name

【视图】

PKI 实体视图

【参数】

name-str：实体的通用名称。长度范围为 1～31 个字符。

【描述】

common-name 命令用来指定实体的通用名。**undo common-name** 命令用来删除实体的通用名。

缺省情况下，未指定实体通用名。

【举例】

配置实体的通用名。

```
[H3C-pki-entity-1] common-name pkisecpath
```

8.2.3 country

【命令】

country *country-code-str*

undo country

【视图】

PKI 实体视图

【参数】

country-code-str：2 字节国家代码。

【描述】

country 命令用来指定实体所属的国家代码，代码用标准的 2 字符代码。例如，中国为“CN”。**undo country** 命令用来删除实体所属的国家代码。

缺省情况下，未指定实体所属国家代码。

【举例】

配置实体所属的国家代码。

```
[H3C-pki-entity-1] country CN
```

8.2.4 ip

【命令】

ip *ip-address*

undo ip

【视图】

PKI 实体视图

【参数】

ip-address：实体的 IP 地址。IP 地址为点分十进制形式，如 A.B.C.D。

【描述】

ip 命令用来指定实体的 IP 地址。**undo ip** 命令用来删除实体的 IP 地址。

缺省情况下，未指定实体 IP 地址。

【举例】

配置实体的 IP 地址。

```
[H3C-pki-entity-1] ip 161.12.2.3
```

8.2.5 locality

【命令】

locality *locality-str*

undo locality

【视图】

PKI 实体视图

【参数】

locality-str：地理区域的名称。长度范围为 1～31 个字符。

【描述】

locality 命令用来指定实体所在的地理区域的名称，比如城市名称。**undo locality** 命令用来删除实体所在的地理区域的名称。

缺省情况下，未指定实体所在的地理区域。

【举例】

配置实体所在的地理区域的名称。

```
[H3C-pki-entity-1] locality Beijing
```

8.2.6 organization

【命令】

organization *org-str*

undo organization

【视图】

PKI 实体视图

【参数】

org-str：组织名称。长度范围为 1～31 个字符。

【描述】

organization 命令用来指定实体所属组织的名称。**undo organization** 命令用来删除实体所属组织的名称。

缺省情况下，未指定实体所属组织。

【举例】

配置实体所属组织名称。

```
[H3C-pki-entity-1] organization h3c
```

8.2.7 organization-unit

【命令】

organization-unit *org-unit-str*

undo organization-unit

【视图】

PKI 实体视图

【参数】

org-unit-str：组织部门的名称。长度范围为 1～31 个字符。

【描述】

organization-unit 命令用来指定实体所属的组织部门的名称。**undo organization-unit** 命令用来删除实体所属的组织部门的名称。

缺省情况下，未指定实体所属部门。

【举例】

配置实体所属组织部门名称。

```
[H3C-pki-entity-1] organization-unit soft plat
```

8.2.8 state

【命令】

state *state-str*

undo state

【视图】

PKI 实体视图

【参数】

state-str：州或省的名称。长度范围为 1～31 个字符。

【描述】

state 命令用来指定实体所属的州或省的名称。**undo state** 命令用来删除此配置。

缺省情况下，未指定实体所在州或省。

【举例】

配置实体所在省。

```
[H3C-pki-entity-1] state Beijing
```

8.2.9 pki entity

【命令】

pki entity *name-str*

undo pki entity *name-str*

【视图】

所有视图

【参数】

name-str：本设备唯一的标识字符串，用于被引用时指定。长度范围为 1～15 个字符。

【描述】

pki entity 命令用来指定 PKI 实体的名称并进入 PKI 实体视图，**undo pki entity** 命令用来删除此实体的名称及其名字空间下所有配置。

在 PKI 实体视图下可配置实体的各种属性值。*name-str* 只是用来方便被其它命令引用，不用于证书的相关字段。

缺省情况下，未指定实体名称。

【举例】

进入 PKI 实体视图。

```
[H3C] pki entity en
[H3C-pki-entity-en]
```

8.3 PKI 证书操作命令

8.3.1 pki delete-certificate

【命令】

pki delete-certificate { **local** | **ca** } **domain** *domain-name*

【视图】

系统视图

【参数】

local：表示删除存储在本地的所有本地证书。

ca：表示删除存储在本地的所有 CA 证书。

domain-name：指定待删除证书所在的 PKI 域。

【描述】

pki delete-certificate 命令用来删除本地存储的证书。

【举例】

删除 PKI 域“cer”中的本地证书。

```
[H3C] pki delete-certificate local domain cer
```

8.3.2 pki import-certificate

【命令】

pki import-certificate { **local** | **ca** } **domain** *domain-name* { **der** | **p12** | **pem** } [**filename** *filename*]

【视图】

系统视图

【参数】

local：表示本地证书。

ca：表示 CA 证书。

domain-name：证书所在的 PKI 域。

der：指定证书文件格式为 DER 编码。

p12：指定证书文件格式为 P12 编码。

pem：指定证书文件格式为 PEM 编码。

filename：证书的文件名，文件名长度为 1～127 个字符。

【描述】

pki import-certificate 命令用来导入已有的 CA 证书或本地证书。

相关命令请参考 **pki domain**。

【举例】

导入 CA 证书，证书文件格式为 PEM 编码。

```
[H3C] pki import-certificate ca domain cer pem
```

8.3.3 pki request-certificate

【命令】

pki request-certificate domain *domain-name* [*password*] [**pkcs10** [**filename**

filename]]

【视图】

系统视图

【参数】

domain-name：是包含证书申请中 CA 或 RA 等信息的域名。该名称是使用 **pki domain** 命令配置的。

password：在证书撤销时需要提供的密码，可选，长度为 1～31 个字符。

pkcs10：在终端上显示出 BASE64 编码的 PKCS#10 证书请求，该信息可用于带外方式（如电话、磁盘、电子邮件等）的证书请求，可选。

filename：将 PKCS#10 证书请求保存到名为 *filename* 的文件。

【描述】

pki request-certificate 命令为已经生成的 RSA 密钥对通过 SCEP 协议向 CA 申请证书。当 SCEP 出现异常无法正常通信时，可以使用可选参数 **pkcs10** 打印出本地的证书请求信息（base64 格式），用户保存该信息，并通过带外方式将该信息发送给 CA 进行证书请求。

此命令不被保存在配置中。

相关命令请参考 **pki domain**。

【举例】

手工申请证书，并在终端上显示 PKCS#10 证书请求。

```
[H3C] pki request-certificate domain 1 pkcs10
```

8.3.4 pki retrieval-certificate

【命令】

pki retrieval-certificate { **local** | **ca** } **domain** *domain-name*

【视图】

系统视图

【参数】

local：表示下载本地证书。

ca：表示下载 CA 的证书。

domain-name：是包含证书申请中 CA 或 RA 等信息的域名。该域名是使用 **pki domain** 命令配置的。

【描述】

pki retrieval-certificate 命令用来从证书发布服务器上下载证书。

相关命令请参考 **pki domain**。

【举例】

从证书发布服务器上获取证书。

```
[H3C] pki retrieval-certificate ca domain 1
```

8.3.5 pki retrieval-crl

【命令】

pki retrieval-crl domain *domain-name*

【视图】

系统视图

【参数】

domain-name：是包含证书申请中 CA 或 RA 等信息的域名。该域名是使用 **pki domain** 命令配置的。

【描述】

pki retrieval-crl 命令用来从 CRL 发布服务器上获取最新的 CRL。下载 CRL 目的是验证当前证书的合法性。

相关命令请参考 **pki domain**。

【举例】

获取 CRL。

```
[H3C] pki retrieval-crl domain 1
```

8.3.6 pki validate-certificate

【命令】

pki validate-certificate { **local** | **ca** } **domain** *domain-name*

【视图】

系统视图

【参数】

local：表示验证本地证书。

ca：表示验证 CA 的证书。

domain-name：指明待验证证书所在的域。该域名是使用 **pki domain** 命令配置的。

【描述】

pki validate-certificate 命令用来检查一个证书的有效性。证书验证的核心就是检查 CA 在证书上的签名，并确定证书仍在有效期内，而且未被废除。由于人们相信 CA 不会发行伪造证书，所以含有它的真实签名的任何证书都可通过验证。

相关命令请参考 **pki domain**。

【举例】

验证 CA 证书。

```
[H3C] pki validate-certificate ca domain 1
```

8.4 PKI 显示与调试命令

8.4.1 debugging pki

【命令】

debugging pki { **all** | **request** | **retrieval** | **verify** | **error** }

undo debugging pki { **all** | **request** | **retrieval** | **verify** | **error** }

【视图】

用户视图

【参数】

all：打开所有的调试开关。

request：证书申请过程的调试开关。

retrieval：证书获取过程的调试开关。

verify：证书验证过程的调试开关。

error：错误发生的调试开关。

【描述】

debugging pki 命令用来打开 PKI 调试信息开关。**undo debugging pki** 命令用来关闭 PKI 调试开关。

在设备使用过程中可能会出现意想不到的问题，所以采用调试命令可以进行有选择性的调试信息打印输出，为网络管理员和开发人员监控网络运行情况和诊断网络故障提供了强有力的支持。

缺省情况下，关闭所有 PKI 调试开关。

【举例】

打开 PKI 证书操作发生错误时的调试开关。

```
<H3C> debugging pki error
<H3C> system-view
[H3C] pki delete-certificate ca domain 1
[H3C] pki request-certificate domain 1
Certificate enroll failed!
Cannot get the CA/RA certificate when creating the x509 Request
```

打开 PKI 证书获取过程的调试开关。

```
<H3C> debugging pki retrieval
<H3C> system-view
[H3C] pki retrieval-certificate local domain 1
Retrievaling CA/RA certificates. Please wait a while......
We receive 3 certificates.
The trusted CA's finger print is:
    MD5  fingerprint:74C9 B71D 406B DDB3 F74A 96BC E05B 40E9
SHA1 fingerprint:770E 2937 4E32 ACD4 4ACC 7CF1 0FF0 6FB8 6C34 E24A
Is the finger print correct?(Y/N):y
Saving the CA/RA certificate to flash.....................Done!
```

打开 PKI 证书申请过程的调试开关。

```
<H3C> debugging pki request
<H3C> system-view
[H3C] pki request-certificate 1
Create PKCS#10 request: token seen: CN=pki test
Create PKCS#10 request: CN=pki test added
Create PKCS#10 request: subject dn set to '/CN=pki test'

Certificate Request:
   …..

dir_name:certsrv/mscep/mscep.dll
host_name:169.254.0.100
SCEP transaction id: 58D41D0C5A7B1E21C5F4A008B580B1A1
PKCS#7 envelope: creating inner PKCS#7
PKCS#7 envelope: data payload size: 297 bytes

data payload:
….
PKCS#7 envelope: successfully encrypted payload
PKCS#7 envelope: size 667 bytes
PKCS#7 envelope: creating outer PKCS#7
```

```
PKCS#7 envelope: signature added successfully
PKCS#7 envelope: adding signed attributes
PKCS#7 envelope: adding string attribute transId
PKCS#7 envelope: adding string attribute messageType
PKCS#7 envelope: adding octet attribute senderNonce
PKCS#7 envelope: PKCS#7 data written successfully
PKCS#7 envelope: applying base64 encoding
PKCS#7 envelope: base64 encoded payload size: 2145 bytes
SCEP send message:IP = 0xa9fe0064
SCEP send message: Server returned status code
Valid response from server
PKCS#7 develope: reading outer PKCS#7
PKCS#7 develope: PKCS#7 payload size: 1872 bytes
PKCS#7 develope: PKCS#7 contains 1276 bytes of enveloped data
PKCS#7 develope: verifying signature
PKCS#7 develope: signature ok
PKCS#7 develope: finding signed attributes
PKCS#7 develope: finding attribute transId
PKCS#7 develope: allocating 32 bytes for attribute
PKCS#7 develope: reply transaction id: 58D41D0C5A7B1E21C5F4A008B580B1A1

PKCS#7 develope: finding attribute messageType
PKCS#7 develope: allocating 1 bytes for attribute
PKCS#7 develope: reply message type is good
PKCS#7 develope: finding attribute senderNonce
PKCS#7 develope: allocating 16 bytes for attribute

PKCS#7 develope: senderNonce in reply: :

a6341944 28d9b544 a4755d9a ba320d35
PKCS#7 develope: finding attribute recipientNonce
PKCS#7 develope: allocating 16 bytes for attribute

PKCS#7 develope: recipientNonce in reply: :

b98da9c3 20b638c5 634f4924 65f804d9
PKCS#7 develope: finding attribute pkiStatus
PKCS#7 develope: allocating 1 bytes for attribute
PKCS#7 develope: pkistatus SUCCESS
PKCS#7 develope: reading inner PKCS#7
PKCS#7 develope: decrypting inner PKCS#7
PKCS#7 develope: PKCS#7 payload size: 1003 bytes
PKI Get the Signed Certificates:
```

```
  subject: / CN=pki test
  issuer:
/emailAddress=myca@h3c.com/C=CN/ST=Beijing/L=Beijing/O=hw3c/OU=bjs/
CN=myca
Key usage: general purpose
```

打开 PKI 证书验证过程的调试开关。

```
<H3C> debugging pki verify
<H3C> system-view
[H3C] pki validate-certificate local domain 1
Verify certificate......
        Serial Number:
            101E266A 00000000 006B
        Issuer:
            emailAddress=myca@h3c.com
            C=CN
            ST=Beijing
            L=Beijing
            O=hw3c
            OU=bjs
            CN=myca
        Subject:
            C=CN
            ST=bei jing
            O=hua wei - 3com
            CN=pki test
Verify result: ok
```

表8-1 debuging pki 调试信息的域描述

域	描述
Create PKCS#10 request	实体请求信息格式封装成 PKCS#10 格式
PKCS#7 envelope	数据封装为 PKCS#7 加密格式
inner PKCS#7	PKCS#7 数据报文的加密处理
outer PKCS#7	PKCS#7 数据报文的签名处理
PKCS#7 develope	PKCS#7 加密报文解包
host_name	注册服务器主机名称
dir_name	注册服务器 CGI 脚本目录
data payload	数据载荷
token seen	实体 DN 信息
pkistatus	PKI 证书操作状态

域	描述
SUCCESS	成功
FAILURE	失败
PENDING	等待处理
fingerprint	指纹，一般指 CA 的签名
base64 encoded	一种数据编码方式
x509 Request	X509 证书请求（证书格式为 X509 标准）
Key usage	密钥用途(一般为加密、签名和通用)
Issuer	证书颁发者
Subject	证书请求实体
SCEP send message	实体通过 SCEP 协议向 CA 发出证书操作报文
Signed Certificates	经 CA 签名的证书

8.4.2 display pki certificate

【命令】

display pki certificate { { **local** | **ca** } **domain** *domain-name* | **request-status** }

【视图】

所有视图

【参数】

local：表示显示本地的证书。

ca：表示显示 CA 的证书。

request-status：表示显示证书申请后的状态。

domain-name：指明待验证证书所在的域。该域名是使用 **pki domain** 命令配置的，可选。

【描述】

display pki certificate 命令用来显示和查看证书的内容。

相关命令请参考 **pki retrieval-certificate**、**pki domain**、**certificate request polling**。

【举例】

显示本地证书。

```
[H3C] display pki certificate local domain 1
```

```
Data:
        Version: 3 (0x2)
        Serial Number:
            10B7D4E3 00010000 0086
        Signature Algorithm: md5WithRSAEncryption
        Issuer:
            emailAddress=myca@h3c.com
            C=CN
            ST=Beijing
            L=Beijing
            O=hw3c
            OU=bjs
            CN=new-ca
        Validity
            Not Before: Jan 13 08:57:21 2004 GMT
            Not After : Jan 20 09:07:21 2005 GMT
        Subject:
            C=CN
            ST=beijing
            L=beijing
            CN=pki test
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
            RSA Public Key: (512 bit)
                Modulus (512 bit):
                    00D41D1F …
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Subject Alternative Name:
            DNS:hyf.h3c.com
            …          …
    Signature Algorithm: md5WithRSAEncryption
        A3A5A447 4D08387D …
```

表8-2 证书显示的内容描述

域	描述
Version	证书版本号
Serial Number	证书序列号
Signature Algorithm	签名算法
Issuer	证书颁发者
Validity	证书有效期

域	描述
Subject	证书申请实体
Subject Public Key Info	申请实体公钥信息
X509v3 extensions	X509（版本 3）格式证书扩展属性
X509v3 CRL Distribution Points	X509（版本 3）格式 CRL 发布点

8.4.3 display pki crl

【命令】

display pki crl domain *domain-name*

【视图】

所有视图

【参数】

domain-name：指明待验证证书所在的域。该域名是使用 **pki domain** 命令配置的，可选。

【描述】

display pki crl 命令用来显示和查看存储在本地的 CRL。

相关命令请参考 **pki retrieval-crl**，**pki domain**。

【举例】

显示 CRL。

```
[H3C] display pki crl domain 1
 Certificate Revocation List (CRL):
        Version 2 (0x1)
        Signature Algorithm: sha1WithRSAEncryption
        Issuer:
            C=CN
            O=h3c
            OU=soft
            CN=A Test Root
        Last Update: Jan  5 08:44:19 2004 GMT
        Next Update: Jan  5 21:42:13 2004 GMT
        CRL extensions:
            X509v3 CRL Number:            2
            X509v3 Authority Key Identifier:
            keyid:0F71448E E075CAB8 ADDB3A12 0B747387 45D612EC
```

```
Revoked Certificates:
Serial Number: 05a234448E…
Revocation Date: Sep  6 12:33:22 2004 GMT
CRL entry extensions:……
Serial Number: 05a278445E…
Revocation Date: Sep  7 12:33:22 2004 GMT
CRL entry extensions:…
```

表8-3 CRL 显示的内容描述

域	描述
Version	CRL 版本号
Signature Algorithm	CRL 采用的签名算法
Issuer	颁发该 CRL 的 CA
Last Update	上次更新时间
Next Update	下次更新时间
CRL extensions	CRL 扩展属性
CRL Number	CRL 列表中撤消证书的数量
Authority Key Identifier	发布该无效证书(即 CRL)的 CA
Revoked Certificates	撤销的证书
Serial Number	撤销证书的序列号
Revocation Date	撤销日期

第9章 SSL 配置命令

9.1 SSL 服务器策略配置命令

9.1.1 ciphersuite

【命令】

ciphersuite { **rsa_rc4_128_md5** | **rsa_rc4_128_sha** | **rsa_des_cbc_sha** | **rsa_3des_ede_cbc_sha** | **rsa_aes_128_cbc_sha** | **rsa_aes_256_cbc_sha** } *

undo ciphersuite [**rsa_rc4_128_md5** | **rsa_rc4_128_sha** | **rsa_des_cbc_sha** | **rsa_3des_ede_cbc_sha** | **rsa_aes_128_cbc_sha** | **rsa_aes_256_cbc_sha**] *

【视图】

SSL 服务器策略视图

【参数】

rsa_rc4_128_md5：密钥交换算法采用 RSA、加密算法采用 128 位的 RC4 算法、MAC 算法采用 MD5。

rsa_rc4_128_sha：密钥交换算法采用 RSA、加密算法采用 128 位的 RC4 算法、MAC 算法采用 SHA。

rsa_des_cbc_sha：密钥交换算法采用 RSA、加密算法采用 DES_CBC 算法、MAC 算法采用 SHA。

rsa_3des_ede_cbc_sha：密钥交换算法采用 RSA、加密算法采用 3DES_EDE_CBC 算法、MAC 算法采用 SHA。

rsa_aes_128_cbc_sha：密钥交换算法采用 RSA、加密算法采用 128 位 AES_CBC 算法、MAC 算法采用 SHA。

rsa_aes_256_cbc_sha：密钥交换算法采用 RSA、加密算法采用 256 位 AES_CBC 算法、MAC 算法采用 SHA。

【描述】

ciphersuite 命令用来配置服务器端 SSL 策略中使用的加密套件，**undo ciphersuite** 命令用来撤销已经配置的加密套件。

在使用 **undo ciphersuite** 命令时，如果不提供参数，表示撤销所有已配置的加密套件，恢复为上述六种都支持。

缺省情况下，6 种加密套件都支持。

【举例】

指定服务器支持的加密套件为 RSA_RC4_128_MD5 和 RSA_RC4_128_SHA。

```
[H3C-ssl-server-policy-policy1] ciphersuite rsa_rc4_128_md5 rsa_rc4_128_sha
```

从原来指定的服务器支持的加密套件（RSA_RC4_128_MD5 和 RSA_RC4_128_SHA）中删除 RSA_RC4_128_MD5 套件。

```
[H3C-ssl-server-policy-policy1] undo ciphersuite rsa_rc4_128_md5
```

9.1.2 client-verify

【命令】

client-verify enable

undo client-verify enable

【视图】

SSL 服务器策略视图

【参数】

无

【描述】

client-verify enable 命令用来在服务器端设定在握手过程中需要进行基于证书的 SSL 客户端认证。

undo client-verify enable 命令用来在服务器端设定在握手过程中不需要进行基于证书的 SSL 客户端认证。

缺省情况下，服务器端在握手过程中不需要进行基于证书的 SSL 客户端认证。

【举例】

设定握手过程要求用户认证。

```
[H3C-ssl-server-policy-policy1] client-verify enable
```

9.1.3 close-mode

【命令】

close-mode wait

undo close-mode wait

【视图】

SSL 服务器策略视图

【参数】

无

【描述】

close-mode wait 命令用来配置服务器的 SSL 关闭模式为 wait 关闭模式，即发送 close-notify 警告消息给客户端后，等待客户端的 close-notify 警告消息。

undo close-mode wait 命令用来撤销 wait 关闭模式。

仅当使用硬件加密时，配置 **close-mode wait** 命令后，服务器的关闭模式才为 wait 模式；当使用软件加密时，此命令不生效。

缺省情况下，服务器发送 close-notify 警告消息给客户端，在关闭会话前并不等待客户端的 close-notify 警告。

【举例】

设定关闭模式为等待 close-notify 消息。

```
[H3C-ssl-server-policy-policy1] close-mode wait
```

设定关闭模式为不等待 close-notify 消息。

```
[H3C-ssl-server-policy-policy1] undo close-mode wait
```

9.1.4 debugging ssl server

【命令】

debugging ssl server { **all** | **event** | **packet** | **error** | **process** | **misc** }

undo debugging ssl server { **all** | **event** | **packet** | **error** | **process** | **misc** }

【视图】

用户视图

【参数】

all：输出 SSL 模块的所有调试信息。

event：输出事件调试信息。

packet：输出报文的调试信息。

error：输出错误调试信息。

process：输出处理过程调试信息。

misc：输出其它种类的调试信息。

【描述】

debugging ssl server 命令用来打开 SSL 服务器的调试开关，**undo debugging ssl**

server 命令用来关闭 SSL 服务器的调试开关。

缺省情况下，未打开调试开关。

【举例】

打开 SSL 服务器的报文调试开关。

```
<H3C> debugging ssl server packet
```

9.1.5 display ssl server-policy

【命令】

display ssl server-policy { *policy-name* | **all** }

【视图】

所有视图

【参数】

policy-name：SSL 服务器策略名。

all：表示所有的策略。

【描述】

display ssl server-policy 命令用来显示一个名为 *policy-name* 的 SSL 服务器策略配置或所有 SSL 服务器策略配置。

【举例】

显示名为 policy1 的策略配置。

```
[H3C] display ssl server-policy policy1
ssl-policy: policy1
        pki-domain:
        ciphersuite:
                rsa_rc4_128_md5
                rsa_rc4_128_sha
                rsa_des_cbc_sha
                rsa_3des_ede_cbc_sha
                rsa_aes_128_cbc_sha
                rsa_aes_256_cbc_sha
        handshake timeout: 3600
        close-mode: wait disabled
        session timeout: 3600
        session cachesize: 2000
        client-verify: disabled
```

9.1.6 handshake timeout

【命令】

handshake timeout *time*

undo handshake timeout

【视图】

SSL 服务器策略视图

【参数】

time：握手连接的超时时间，单位为秒，范围为 180～7200。

【描述】

handshake timeout 命令用来配置服务器端 SSL 握手连接的保持时间。

undo handshake timeout 命令用来撤销原来设置的时间，并恢复为缺省值。

缺省情况下，保持时间为 3600 秒。

【举例】

设定握手超时时间为 3000 秒。

```
[H3C-ssl-server-policy-policy1] handshake timeout 3000
```

撤销原来设定的握手超时时间 3000 秒，恢复为缺省的 3600 秒。

```
[H3C-ssl-server-policy-policy1] undo handshake timeout
```

9.1.7 pki-domain

【命令】

pki-domain *pki-name*

undo pki-domain

【视图】

SSL 服务器策略视图

【参数】

pki-name：PKI 域的域名。

【描述】

pki-domain 命令用来为服务器端指定 SSL 握手时使用的 PKI 域，在握手过程中服务器将发送该域的证书。

undo pki-domain 命令用来撤销已设置的 PKI 域。

缺省情况下，未指定 PKI 域。

【举例】

指定服务器使用的 PKI 域为 h3c-domain。

```
[H3C-ssl-server-policy-policy1] pki-domain h3c-domain
```

撤销服务器所使用的 PKI 域。

```
[H3C-ssl-server-policy-policy1] undo pki-domain
```

9.1.8 session

【命令】

session { **timeout** *time* | **cachesize** *size* } *

undo session { **timeout** | **cachesize** } *

【视图】

SSL 服务器策略视图

【参数】

time：会话缓存的超时时间，单位为秒，范围为 1800～72000。

size：会话缓存空间的大小，单位为单元个数，范围为 1000～10000 个单元。

【描述】

session timeout 命令用来配置会话缓存中单元的保存时间，它指定会话单元在缓存中保存时间值为 *time*，会话单元只有在超时后才会从缓存中清除。如果会话缓存中没有空间，将拒绝新加入的连接。**session cachesize** 用来指定会话缓存的空间大小。

undo session 命令用来撤销原来设定的会话缓存保存时间和会话缓存大小，并分别恢复为缺省值。

缺省情况下，会话缓存的超时时间为 3600 秒，缓存空间的大小为 2000 个单元。

【举例】

设定会话的超时时间为 7200 秒，会话缓存为 3000 个单元。

```
[H3C-ssl-server-policy-policy1] session timeout 7200 cachesize 3000
```

撤销设定的会话的超时时间和会话缓存大小，并恢复为缺省值。

```
[H3C-ssl-server-policy-policy1] undo session timeout cachesize
```

9.1.9 ssl server-policy

【命令】

ssl server-policy *policy_name*

undo ssl server-policy { *policy_name* | **all** }

【视图】

系统视图

【参数】

policy_name：SSL 服务器策略的名称。

all：所有 SSL 服务器策略。

【描述】

ssl server-policy 命令用来定义一个名为 *policy_name* 的 SSL 服务器策略，输入命令后，同时进入 SSL 服务器策略视图。

undo ssl server-policy 命令用来删除 SSL 服务器策略。

缺省情况下，未配置 SSL 服务器策略。

【举例】

定义名为 policy1 的 SSL 服务器策略。

```
[H3C] ssl server-policy policy1
```

删除名为 policy1 的 SSL 服务器策略。

```
[H3C] undo ssl server-policy policy1
```

9.2 SSL 加密卡配置命令

9.2.1 debugging ssl card

【命令】

debugging ssl card { **all** | **event** | **packet** | **error** | **process** | **misc** }

undo debugging ssl card { **all** | **event** | **packet** | **error** | **process** | **misc** }

【视图】

用户视图

【参数】

all：输出 SSL 模块的所有调试信息。

event：输出模块处理过程中事件的调试信息。

packet：输出有关报文内容的调试信息。

error：输出模块处理过程中产生错误的调试信息。

process：输出模块处理过程中函数调用的调试信息。

misc：输出其它种类的调试信息。

【描述】

debugging ssl card 命令用来打开 SSL 加密卡的调试开关，**undo debugging ssl card** 命令用来关闭 SSL 加密卡的调试开关。

缺省情况下，关闭 SSL 加密卡的调试开关。

【举例】

打开 SSL 加密卡的所有调试开关。

```
<H3C> debugging ssl card all
```

9.2.2 display interface ssl-card

【命令】

display interface ssl-card [*slot-id*]

【视图】

所有视图

【参数】

slot-id：SSL 加密卡的槽位号。

【描述】

display interface ssl-card 命令用来显示 SSL 加密卡的统计信息。

【举例】

显示 SSL 加密卡 1/0 的统计信息。

```
<H3C> display interface ssl-card 1/0
Description : Ssl-Card1/0 Interface
Driver Status : READY
    Last 5 seconds input rate 0.00 bytes/sec, 0.00 packets/sec
    Last 5 seconds output rate 0.00 bytes/sec, 0.00 packets/sec
    Input : 0 bytes, 0 packets, 0 drops
    Output: 0 bytes, 0 packets
```

9.2.3 shutdown

【命令】

shutdown

undo shutdown

【视图】

SSL 加密卡接口视图

【参数】

无

【描述】

shutdown 命令用来关闭加密卡，禁止加密卡的使用，**undo shutdown** 命令用来使能加密卡，启动加密卡的使用。

缺省情况下，加密卡为使能状态。

【举例】

禁止使用加密卡 SSL Card1/0。

```
[H3C-Ssl-Card1/0] shutdown
```

使能加密卡 1/0。

```
[H3C-Ssl-Card1/0] undo shutdown
```

9.2.4 use ssl-card

【命令】

use ssl-card *slot-id*

undo use ssl-card

【视图】

服务器端 SSL 策略视图

【参数】

slot-id：SSL 加密卡的槽位号。

【描述】

use ssl-card 命令用来指定 SSL 服务器策略所使用的加密卡，**undo use ssl-card** 命令用来取消 SSL 服务器策略使用的加密卡。

缺省情况下，未配置使用加密卡。

【举例】

为 SSL 服务器策略 policy1 配置使用加密卡。

```
[H3C-ssl-server-policy-policy1] use ssl-card 1/0
```

删除 policy1 所使用的加密卡，设置 ploicy1 使用软件加密。

```
[H3C-ssl-server-policy-policy1] undo use ssl-card
```

9.3 基于证书属性访问控制策略配置命令

9.3.1 attribute

【命令】

attribute *id* { **subject-name** | **issuer-name** } **dn** { **ctn** | **nctn** } *attribute-value*

attribute *id* **alt-subject-name fqdn** { **equ** | **nequ** | **ctn** | **nctn** } *attribute-value*

attribute *id* **alt-subject-name ip** { **equ** | **nequ** } *attribute-value*

undo attribute { *id* | **all** }

【视图】

证书属性过虑组视图

【参数】

id：证书属性过虑条件序号。

subject-name：证书主题名。

issuer-name：证书颁发者名称。

alt-subject-name：证书主题扩展名。

dn：证书主题名或者颁发者的 DN。

fqdn：证书主题名、颁发者名称、主题扩展名的 FQDN 值。

ip：证书主题名、颁发者名称、主题扩展名的 IP 值。

equ：相等操作符。

nequ：不等操作符。

ctn：包含操作符。

nctn：不包含符。

attribute-value：证书属性值字符串。

all：所有证书属性过虑条件。

【描述】

attribute 命令用来配置证书属性过滤条件，**undo attribute** 命令用来删除一个或者所有证书属性过虑条件。

缺省情况下，未配置任何证书属性过滤条件。

【举例】

为 subject-name 属性的 DN 值创建一个过滤条件，该条件表示，DN 值必须包含字符串 abc。

```
[H3C-cert-attribute-group-mygroup] attribute 1 subject-name dn ctn abc
```

为 alt-subject-name 属性的 IP 值创建一个过滤条件，该条件表示 IP 值必须不等于 10.165.87.154。

```
[H3C-cert-attribute-group-mygroup] attribute 3 alt-subject-name ip nequ
10.165.87.154
```

9.3.2 display pki certificate access-control-policy

【命令】

display pki certificate access-control-policy { *policy-name* | **all** }

【视图】

所有视图

【参数】

policy-name：基于证书属性的访问控制策略名。

all：所有基于证书属性的访问控制策略。

【描述】

display pki certificate access-control-policy 命令用来显示一个或者所有已经配置的基于证书属性访问的控制策略。

【举例】

显示一个名为 mypolicy 的的访问控制策略。

```
<H3C> display pki certificate access-control-policy mypolicy
access-control-policy name: mypolicy
 rule 1 deny mygroup1
 rule 2 permit mygroup2
```

9.3.3 display pki certificate attribute-group

【命令】

display pki certificate attribute-group { *group-name* | **all** }

【视图】

所有视图

【参数】

group-name：证书属性过虑组。

all：所有证书属性过虑组。

【描述】

display pki certificate attribute-group 命令用来显示一个或者所有已经配置的证书属性过滤组信息。

【举例】

显示一个名为 mygroup 的属性过滤组信息。

```
<H3C> display pki certificate attribute-group mygroup
attribute group name: mygroup
 attribute 1 subject-name dn ctn abc
 attribute 2 alt-subject-name fqdn nctn H3C
```

9.3.4 pki certificate access-control-policy

【命令】

pki certificate access-control-policy *policy-name*

undo pki certificate access-control-policy { *policy-name* | **all** }

【视图】

系统视图

【参数】

policy-name：基于证书属性的访问控制策略名称。

all：所有证书属性的访问控制策略。

【描述】

pki certificate access-control-policy 命令用来创建一个证书属性访问控制策略。

undo pki certificate access-control-policy 命令用来删除一个或者所有证书属性访问控制策略。

缺省情况下，未配置基于证书属性的访问控制策略。

【举例】

创建一个名称为 mypolicy 的访问控制策略

```
[H3C] pki certificate access-control-policy mypolicy
```

删除一个名称为 mypolicy 的访问控制策略

```
[H3C] undo pki certificate access-control-policy mypolicy
```

删除所有访问控制策略

```
[H3C] undo pki certificate access-control-policy all
```

9.3.5 pki certificate attribute-group

【命令】

pki certificate attribute-group *group-name*

undo pki certificate attribute-group { *group-name* | **all** }

【视图】

系统视图

【参数】

group-name：证书属性过虑组。

all：所有属性过虑组。

【描述】

pki certificate attribute-group 命令用来创建一个证书属性过滤组。

undo pki certificate attribute-group 命令用来删除一个或者所有证书属性过滤组。

缺省情况下，未配置证书属性过滤组。

【举例】

创建一个名为 mygroup 证书属性过滤组，并且进入证书属性过滤组视图。

```
[H3C] pki certificate attribute-group mygroup
[H3C-cert-attribute-group-mygroup]
```

9.3.6 rule

【命令】

rule [*id*] { **permit** | **deny** } *group-name*

undo rule { *id* | **all** }

【视图】

基于证书属性的访问控制策略配置视图

【参数】

id：基于证书属性的访问控制规则序号。

permit：若规则被验证匹配，则允许客户端访问服务器资源。

deny：若规则被验证匹配，则不允许客户端访问服务器资源。

group-name：规则所关联的证书属性过虑组名称。

all：所有控制规则。

【描述】

rule 命令用来添加一个访问控制规则。

undo rule 命令用来删除一个或者所有访问控制规则。

缺省情况下，未配置访问控制规则。

【举例】

添加一条访问控制规则，该规则表示，当 mygroup 验证匹配时，允许客户端访问服务器资源。

```
[H3C-cert-acp-mypolicy] rule 1 permit mygroup
```

删除序号为 1 的访问控制规则。

```
[H3C-cert-acp-mypolicy] undo rule 1
```

删除所有访问控制规则。

```
[H3C-cert-acp-mypolicy] undo rule all
```

9.4 SSL Proxy 配置命令

9.4.1 debugging ssl proxy

【命令】

debugging ssl proxy { **all** | **event** | **packet** | **error** | **process** | **misc** }

undo debugging ssl proxy { **all** | **event** | **packet** | **error** | **process** | **misc** }

【视图】

用户视图

【参数】

all：输出 SSL 模块的所有调试信息。

event：输出模块处理过程中事件的调试信息。

packet：输出有关报文内容的调试信息。

error：输出模块处理过程中产生错误的调试信息。

process：输出模块处理过程中函数调用的调试信息。

misc：输出其它种类的调试信息。

【描述】

debugging ssl proxy 命令用来打开 SSL Proxy 的调试开关，**undo debugging ssl proxy** 命令用来关闭 SSL Proxy 的调试开关。

缺省情况下，关闭 SSL Proxy 的调试开关。

【举例】

打开 SSL Proxy 的错误调试开关。

```
<H3C> debugging ssl proxy error
```

9.4.2 display ssl proxy

【命令】

display ssl proxy { **all** | *ssl-proxy-name* }

【视图】

所有视图

【参数】

all：所有配置的 SSL Proxy。

ssl-proxy-name：SSL Proxy 策略名称。

【描述】

display ssl proxy 命令用来显示当前 SSL Proxy 的配置和状态。

【举例】

显示名为 myproxy 的 SSL Proxy 的配置信息和状态。

```
[H3C] display ssl proxy myproxy
SSL proxy policy name: myproxy
        Port: 443
        Target server configuration:
           Server IP: 10.165.87.168  Port:80
        SSL server policy: ssl_policy
        Certificate access-control-policy: ssl_cert_acp
```

```
Debugging : off
Operation status : Running
Current number of connection is 1
Connection status:
            Remote Address     Connid          State
          10.165.87.148:443        2           Established(client)
          10.165.87.147:80         3           Established(server)
SSL statistics:
          1 items in the session cache
          2 server accepts
          2 server accepts that finished
          0 session cache hits
          0 session cache misses
          0 session cache timeouts
          0 cache full overflows (500 allowed)
```

9.4.3 display ssl-proxy session

【命令】

display ssl-proxy session [**statistics**]

【视图】

所有视图

【参数】

statistics：显示 SSL Proxy 的会话统计信息。

【描述】

display ssl-proxy session 命令用来显示 SSL Proxy 的会话信息。

【举例】

显示 SSL Proxy 的会话信息。

```
<H3C> display ssl-proxy session
```

9.4.4 port

【命令】

port *port-number*

undo port

【视图】

SSL Proxy 配置视图

【参数】

port-number：指定 SSL Proxy 的端口号，取值范围为 2000～50000。

【描述】

port 命令用来定义 SSL Proxy 服务器使用的端口号。

undo port 命令用来恢复 SSL Proxy 服务器使用的端口号为缺省值。

缺省情况下，SSL Proxy 服务器使用的端口号为 443。

【举例】

配置名为 test 的 SSL Proxy 服务使用的端口号是 4443。

```
[H3C-sslproxy-test] port 4443
```

9.4.5 reset ssl proxy statistic

【命令】

reset ssl proxy statistic

【视图】

用户视图

【参数】

无

【描述】

reset ssl proxy statistic 命令用来清空 SSL Proxy 服务的连接统计信息。

【举例】

清空 SSL Proxy 服务的连接统计信息。

```
<H3C> reset ssl proxy statistic
```

9.4.6 reset ssl-proxy session

【命令】

reset ssl-proxy session

【视图】

用户视图

【参数】

无

【描述】

reset ssl-proxy session 命令用来清除 SSL Proxy 的会话。

【举例】

清除 SSL Proxy 的会话。

```
<H3C> reset ssl-proxy session
```

9.4.7 server ip

【命令】

server ip *ip-address* **port** *port-number*

undo server ip *ip-address*

【视图】

SSL Proxy 配置视图

【参数】

ip：指定目标服务器的地址信息。

ip-address：IP 地址，点分十进制表示。

port：指定目标服务器的端口信息。

port-number：用数字表示，数字的取值范围为 1～65535。

【描述】

server ip 命令用来定义 SSL Proxy 的目标服务器的 IP 地址和端口号，**undo server ip** 用来删除已配置的目标服务器。

缺省情况下，未配置目标服务器。

【举例】

配置名为 test 的 SSL Proxy 服务连接的目标服务器地址是 6.100.100.120，端口号是 80。

```
[H3C-sslproxy-test] server ip 6.100.100.120 port 80
```

9.4.8 ssl proxy

【命令】

ssl proxy *ssl-proxy-name*

undo ssl proxy { *ssl-proxy-name* | **all** }

【视图】

系统视图

【参数】

ssl-proxy-name：SSL Proxy 服务的名称。

all：所有的 SSL Proxy 服务。

【描述】

ssl proxy 命令用于创建一个 SSL Proxy 服务并进入 SSL Proxy 视图。

undo ssl proxy 命令用于删除 SSL Proxy 服务。

缺省情况下，未创建 SSL Proxy 服务。

【举例】

创建一个名为 test 的 SSL Proxy 服务。

```
[H3C] ssl proxy test
```

删除一个名为 test 的 SSL Proxy 服务。

```
[H3C] undo ssl proxy test
```

9.4.9 ssl proxy server

【命令】

ssl proxy server *ssl-proxy-name* **enable**

undo ssl proxy server *ssl-proxy-name* **enable**

【视图】

系统视图

【参数】

ssl-proxy-name：SSL Proxy 服务名称。

【描述】

ssl proxy server 命令用来使用名为 *ssl-proxy-name* 的 SSL Proxy 服务策略启动 SSL Proxy 服务器。

undo ssl proxy server 命令用来停止使用 *ssl-proxy-name* 的 SSL Proxy 服务策略启动的 SSL Proxy 服务器。

缺省情况下，未使用任何 SSL Proxy 服务策略启动 SSL Proxy 服务器。

【举例】

使用名为 myproxy 的 SSL Proxy 服务策略启动 SSL Proxy 服务器。

```
[H3C] ssl proxy server myproxy enable
```

停止使用名为 myproxy 的 SSL Proxy 服务策略启动的 SSL Proxy 服务器。

```
[H3C] undo ssl proxy server myproxy enable
```

9.4.10 ssl-server-policy

【命令】

ssl-server-policy *policy-name*

undo ssl-server-policy

【视图】

SSL Proxy 配置视图

【参数】

policy-name：SSL 服务器策略的名称。

【描述】

ssl-server-policy 命令用来指定 SSL Proxy 使用的 SSL 服务器策略。

undo ssl-server-policy 命令用来取消指定的 SSL 服务器策略。

缺省情况下，未指定 SSL 服务器策略。

【举例】

给名为 test 的 SSL Proxy 服务指定名为 server_policy 的 SSL 服务器策略。

```
[H3C-sslproxy-test] ssl-server-policy server_policy
```

第10章 Web 和邮件过滤配置命令

10.1 Web 过滤配置命令

10.1.1 debugging firewall url-filter host

【命令】

debugging firewall url-filter host { **all** | **filter** | **packet** | **event** | **error** }

undo debugging firewall url-filter host { **all** | **filter** | **packet** | **event** | **error** }

【视图】

用户视图

【参数】

all：所有调试功能。

filter：过滤包调试功能。

packet：报文调试功能。

event：事件调试功能。

error：错误调试功能。

【描述】

debugging firewall url-filter host 命令用来打开 Web 地址过滤的调试功能，**undo debugging firewall url-filter host** 命令用来关闭调试功能。

缺省情况下，关闭调试功能。

【举例】

打开 Web 地址过滤的所有调试功能。

```
<H3C> debugging firewall url-filter host all
```

10.1.2 debugging firewall url-filter parameter

【命令】

debugging firewall url-filter parameter { **all** | **error** | **event** | **filter** | **packet** }

undo debugging firewall url-filter parameter { **all** | **error** | **event** | **filter** | **packet** }

【视图】

用户视图

【参数】

all：所有调试功能。

filter：过滤包调试功能。

packet：报文调试功能。

event：事件调试功能。

error：错误调试功能。

【描述】

debugging firewall url-filter parameter 命令用来打开 SQL 注入攻击防范的调试功能，**undo debugging firewall url-filter parameter** 命令用来关闭 SQL 注入攻击防范的调试功能。

缺省情况下，关闭调试功能。

【举例】

打开 SQL 注入攻击防范的错误调试功能。

```
<H3C> debugging firewall url-filter parameter error
```

10.1.3 debugging firewall webdata-filter

【命令】

debugging firewall webdata-filter { **all** | **filter** | **packet** | **event** | **error** }

undo debugging firewall webdata-filter { **all** | **filter** | **packet** | **event** | **error** }

【视图】

用户视图

【参数】

all：所有调试功能。

filter：过滤包调试功能。

packet：报文调试功能。

event：事件调试功能。

error：错误调试功能。

【描述】

debugging firewall webdata-filter 命令用来打开 Web 内容过滤的调试功能，**undo**

debugging firewall webdata-filter 命令用来关闭调试功能。

缺省情况下，关闭调试功能。

【举例】

打开 Web 内容过滤的所有调试功能。

```
<H3C> debugging firewall webdata-filter all
```

10.1.4 display firewall url-filter host

【命令】

display firewall url-filter host { **enable** | **all** | **item** *url-address* | **item-all** }

【视图】

所有视图

【参数】

enable：显示 Web 地址过滤的使能信息。

all：显示所有的 Web 地址过滤信息。

item *url-address*：显示具体的过滤地址条目的统计信息。

Item-all：显示所有过滤地址条目的统计信息。

【描述】

display firewall url-filter host 命令用来显示 Web 地址过滤的信息。

【举例】

显示 Web 地址过滤的信息。

```
[H3C] display firewall url-filter host all
Url host filter is enabled.
Default method : permit.
No ACL configed to be Matched
Deny http requeset when the URL is ip address ,No acl selected to be Matched
Url host filter has loaded file "flash:/urlfilter" , there are 2 item(s) in
filter now( 2 Added,0 Loaded).
Packet(s) blocked.
Packet(s) allowed.
```

10.1.5 display firewall url-filter parameter

【命令】

display firewall url-filter parameter { **enable** | **all** | **item** *keywords* | **item-all** }

【视图】

所有视图

【参数】

enable：显示 SQL 注入攻击防范的使能信息。

all：显示所有的 SQL 注入攻击防范的过滤信息。

item *keywords*：显示具体的过滤关键字条目的统计信息。

Item-all：显示所有的过滤关键字条目的统计信息。

【描述】

display firewall url-filter parameter 命令用来显示 SQL 注入攻击的过滤信息。

【举例】

显示所有 SQL 注入攻击的过滤信息。

```
[H3C] display firewall url-filter parameter all
Url parameter filter is enabled.
 Url parameter filter has loaded file "flash:/SQLfilter" , there are 9 item(s)
in filter now( 9 Added,0 Loaded).
Packet(s) blocked    :0.
 Packet(s) allowed    :0.
```

10.1.6 display firewall url-filter parameter counter detail

【命令】

display firewall url-filter parameter counter detail

【视图】

所有视图

【参数】

无

【描述】

display firewall url-filter parameter counter detail 命令用来详细显示每个关键字所匹配的次数。

【举例】

显示每个关键字所匹配的次数。

```
[H3C] display firewall url-filter parameter counter detail
KeyWord             MatchedTimes
```

```
 ----------------------------------------
 ^select^            0
 ^insert^            0
 ^update^            0
 ^delete^            0
 ^drop^              0
 --                  0
 '                   0
 ^exec^              0
 %27                 0
```

10.1.7 display firewall webdata-filter

【命令】

display firewall webdata-filter { **enable** | **all** | **item** *keywords* | **item-all** }

【视图】

所有视图

【参数】

enable：显示 Web 内容过滤的使能信息。

all：显示所有的 Web 内容过滤信息。

item *keywords*：显示具体的过滤关键字条目的统计信息。

Item-all：显示所有的过滤关键字条目的统计信息。

【描述】

display firewall webdata-filter 命令用来显示 Web 内容过滤的信息。

【举例】

显示 Web 内容过滤的信息。

```
[H3C] display firewall webdata-filter all
 Webdata-filter is enabled.
 Webdata-filter has loaded file "flash:/webdatafilter" , there are 1 item(s)
in filter now ( 0 Added,0 Loaded).
Packet(s) blocked.
 Packet(s) allowed.
```

10.1.8 firewall url-filter host acl-number

【命令】

firewall url-filter host acl-number *number*

undo firewall url-filter host acl-number

【视图】

系统视图

【参数】

number：基本访问控制列表的编号，范围为 2000～2999。

【描述】

firewall url-filter host acl-number 命令用来配置防火墙通过使用 ACL 对目标 URL 为 IP 地址的 Web 请求进行过滤，**undo firewall url-filter host acl-number** 命令用来取消配置的过滤规则。

使用此命令只能引用一个 ACL 规则，随后配置的规则将覆盖原先的配置。

缺省情况下，未配置任何过滤规则。

【举例】

配置仅允许目标 IP 地址为符合编号 2001 的 ACL 规则的 Web 请求通过。

```
[H3C] acl number 2001
[H3C-acl-basic-2001] rule deny source 200.1.1.0 0.0.0.255
[H3C-acl-basic-2001] rule permit
[H3C-acl-basic-2001] quit
[H3C] firewall url-filter host acl-number 2001
```

10.1.9 firewall url-filter host add

【命令】

firewall url-filter host add { **permit** | **deny** } *url-address*

【视图】

系统视图

【参数】

permit：表示操作行为为允许。

deny：表示操作行为为拒绝。

url-address：添加的 URL 过滤地址。

【描述】

firewall url-filter host add 命令用来添加 Web 过滤地址，并设置对其的过滤行为。

用户添加的网址地址最长允许 128 个字符，否则视为非法地址，不予添加。如果输入*.sina.com 为匹配网址，则系统将匹配 www.sina.com、news.sina.com 等，而不

匹配 www.sina.com.cn。不支持以下的地址格式：*.*.com.cn、news.*.com、sina.com.*。

缺省情况下，未添加任何过滤地址。

【举例】

添加允许地址为 www.163.com 的过滤条目。

```
[H3C] firewall url-filter host add permit www.163.com
```

10.1.10 firewall url-filter host clear

【命令】

firewall url-filter host clear

【视图】

系统视图

【参数】

无

【描述】

firewall url-filter host clear 命令用来清除所有过滤地址条目。

【举例】

清除所有过滤地址条目。

```
[H3C] firewall url-filter host clear
```

10.1.11 firewall url-filter host default

【命令】

firewall url-filter host default { **permit** | **deny** }

【视图】

系统视图

【参数】

permit：配置默认过滤操作为允许。

deny：配置默认过滤操作为拒绝。

【描述】

firewall url-filter host default 命令用来允许或者拒绝未与管理员配置的网址发生匹配的数据报通过。

缺省情况下，允许未发生匹配的数据报通过。

【举例】

配置默认过滤行为为允许。

```
[H3C] firewall url-filter host default permit
```

10.1.12 firewall url-filter host delete

【命令】

firewall url-filter host delete *url-address*

【视图】

系统视图

【参数】

url-address：删除的过滤地址。

【描述】

firewall url-filter host delete 命令用来删除 Web 过滤地址。

【举例】

删除地址为 www.163.com 的过滤条目。

```
[H3C] firewall url-filter host delete www.163.com
```

10.1.13 firewall url-filter host enable

【命令】

firewall url-filter host enable

undo firewall url-filter host enable

【视图】

系统视图

【参数】

无

【描述】

firewall url-filter host enable 命令用来使能 Web 地址过滤功能，**undo firewall url-filter host enable** 命令用来关闭 Web 地址过滤功能。

缺省情况下，关闭 Web 地址过滤功能。

开启 Web 地址过滤功能之前要先配置 ASPF 策略，**detect http**，**detect tcp**，才能使 Web 地址过滤功能生效。

对于监听非标准端口的 HTTP 协议，必须使用 **port-mapping** 命令正确的配置端口映射，这样 Web 地址过滤功能才能生效。

有关ASPF配置命令请参见 4.2 状态防火墙配置命令。

【举例】

使能 Web 地址过滤功能。

```
[H3C] firewall url-filter host enable
```

10.1.14 firewall url-filter host ip-address

【命令】

firewall url-filter host ip-address { **permit** | **deny** }

【视图】

系统视图

【参数】

permit：允许目标 URL 为 IP 地址的 Web 请求通过。

deny：拒绝目标 URL 为 IP 地址的 Web 请求通过。

【描述】

firewall url-filter host ip-address 命令用来配置防火墙是否允许目标 URL 为 IP 地址的 Web 请求通过。

缺省情况下，防火墙将阻止目标 URL 为 IP 地址的 Web 请求通过。

【举例】

配置允许目标 URL 为 IP 地址的 Web 请求通过。

```
[H3C] firewall url-filter host ip-address permit
```

10.1.15 firewall url-filter host save-file

【命令】

firewall url-filter host save-file *file-name*

【视图】

系统视图

【参数】

file-name：保存的过滤文件名。

【描述】

firewall url-filter host save-file 命令用来保存 Web 地址过滤文件。

【举例】

保存名为 urlfilter 的 Web 地址过滤文件。

```
[H3C] firewall url-filter host save-file urlfilter
```

10.1.16 firewall url-filter host load-file

【命令】

firewall url-filter host load-file *file-name*

undo firewall url-filter host load-file

【视图】

系统视图

【参数】

file-name：装载的过滤文件名。

【描述】

firewall url-filter host load-file 命令用来装载 Web 地址过滤文件，**undo firewall url-filter host load-file** 命令用来卸载 Web 地址过滤文件。

如果要使 Web 地址过滤文件中的条目生效并对地址进行过滤，必须将其装载。

【举例】

装载名为 urlfilter 的 Web 地址过滤文件。

```
[H3C] firewall url-filter host load-file urlfilter
```

10.1.17 firewall url-filter parameter add

【命令】

firewall url-filter parameter add *keywords*

undo firewall url-filter parameter add *keywords*

【视图】

系统视图

【参数】

keywords：出现在 HTTP 命令中的关键字。

【描述】

firewall url-filter parameter add 命令用来添加 SQL 注入攻击过滤的关键字。若指定的关键字出现在 HTTP 命令中，防火墙将阻止此 HTTP 请求。

用户可以根据自己的需要，将一些表名、字段、以及一些系统的和自定义的存储过程名作为关键字。

缺省情况下，未添加任何关键字。

过滤关键字最长支持 128 个字符。关键字过滤支持模糊查找，即允许向过滤关键字文件中添加带“*”、“^”、“?”和“ ”（空格）的关键字。“?”和“ ”（空格）可以通过文件进行加载或以 Web 管理方式输入，不能通过命令行输入。

“*”表示最少 0 个到最多 2 个任意中文字符或最少 0 个到最多 4 个任意英文字符。其不能出现在开头和结尾的位置，不能和“^”以及“?”相邻。为避免“*”带来的误判断，管理员应谨慎添加带“*”的过滤关键字。不允许一个关键字中出现两个以上的“*”。过滤词汇文件格式如：test1、te*st2；不允许：te**st、t*es*t、*test。

“^”只能出现在关键字的开头和结尾的位置，最多允许出现两个。例如：^hello，它可以匹配以 hello 开头的字符串，如 helloworld、hello，但其不匹配 ahelloworld；you^可以匹配以 you 结尾的字符串，如 thankyou、you，但其不匹配 thankyour、your。

“?”代表一个字符，如果是汉字这要用“??”。“?”可以出现多个，并可以连续出现。其可以出现在随意的位置，但不能和“*”相邻。如果出现在开始和结尾的位置，则一定要和“^”相邻。“?”只能通过文件加载，不能通过命令行输入。

用户可以通过命令行和文件的形式加载带空格“ ”的关键字。空格的个数和位置没有限制，一个空格可以匹配连续的几个空格。

相关配置命令请参考 **firewall url-filter parameter add-default**。

【举例】

若数据库中含有一个用户自定义的存储过程“sp_additem”，若要阻止对此存储过程的操作，可以将含有此存储过程名的 HTTP 命令进行阻止。

```
[H3C] firewall url-filter parameter add sp_additem
```

10.1.18 firewall url-filter parameter add-default

【命令】

firewall url-filter parameter add-default

【视图】

系统视图

【参数】

无

【描述】

firewall url-filter parameter add-default 命令用来添加系统缺省定义的过滤关键字：^select^、^insert^、^update^、^delete^、^drop^、--、'、^exec^和%27，方便了用户的输入，也防止用户无意中删除了某些关键字，或者不恰当地使用了 **firewall url-filter parameter clear** 命令时可以很快地恢复缺省配置。

缺省情况下，未添加任何过滤关键字。

【举例】

添加系统缺省的过滤关键字。

```
[H3C] firewall url-filter parameter add-default
 Success to add 9 keys!
```

10.1.19 firewall url-filter parameter clear

【命令】

firewall url-filter parameter clear

【视图】

系统视图

【参数】

无

【描述】

firewall url-filter parameter clear 命令用来清除所有过滤关键字。

【举例】

清除所有过滤关键字。

```
[H3C] firewall url-filter parameter clear
```

10.1.20 firewall url-filter parameter delete

【命令】

firewall url-filter parameter delete *keywords*

【视图】

系统视图

【参数】

keywords：删除的过滤关键字。

【描述】

firewall url-filter parameter delete 命令用来删除一个以添加的过滤关键字。

【举例】

删除过滤关键字^select^

```
[H3C] firewall url-filter parameter delete ^select^
```

10.1.21 firewall url-filter parameter enable

【命令】

firewall url-filter parameter enable

undo firewall url-filter parameter enable

【视图】

系统视图

【参数】

无

【描述】

firewall url-filter parameter enable 命令用来使能 SQL 注入攻击防范功能，**undo** 命令用来关闭 SQL 注入攻击防范功能。

缺省情况下，关闭 SQL 注入攻击防范功能。

开启 SQL 注入攻击防范功能之前要先配置 ASPF 策略，**detect http**，**detect tcp**，才能使 SQL 注入攻击防范功能生效。

对于监听非标准端口的 HTTP 协议，必须使用 **port-mapping** 命令正确的配置端口映射，这样 SQL 注入攻击防范功能才能生效。

有关ASPF配置命令请参见 4.2 状态防火墙配置命令。

【举例】

使能 SQL 注入攻击防范功能。

```
[H3C] firewall url-filter parameter enable
```

10.1.22 firewall url-filter parameter load-file

【命令】

firewall url-filter parameter load-file *file-name*

undo firewall url-filter parameter load-file

【视图】

系统视图

【参数】

file-name：装载的过滤文件名。

【描述】

firewall url-filter parameter load-file 命令用来装载 SQL 注入攻击过滤文件，**undo firewall url-filter parameter load-file** 命令用来卸载 SQL 注入攻击过滤文件。

【举例】

装载名为 sqlfilter 的 SQL 注入攻击过滤文件。

```
[H3C] firewall url-filter parameter load-file sqlfilter
```

10.1.23 firewall url-filter parameter save-file

【命令】

firewall url-filter parameter save-file *file-name*

【视图】

系统视图

【参数】

file-name：保存的过滤文件名。

【描述】

firewall url-filter parameter save-file 命令用来保存 SQL 注入攻击过滤文件。

【举例】

保存名为 sqlfilter 的 SQL 注入攻击过滤文件。

```
[H3C] firewall url-filter parameter save-file sqlfilter
```

10.1.24 firewall webdata-filter add

【命令】

firewall webdata-filter add *keywords*

【视图】

系统视图

【参数】

keywords：添加的过滤关键字。

【描述】

firewall webdata-filter add 命令用来添加 Web 内容过滤关键字。

过滤关键字最长支持 128 个字符。关键字过滤支持模糊查找，即允许向过滤关键字文件中添加带“*”、“^”、“?”和“ ”（空格）的关键字。“?”和“ ”（空格）可以通过文件进行加载或以 Web 管理方式输入，不能通过命令行输入。

“*”表示最少 0 个到最多 2 个任意中文字符或最少 0 个到最多 4 个任意英文字符。其不能出现在开头和结尾的位置，不能和“^”以及“?”相邻。为避免“*”带来的误判断，管理员应谨慎添加带“*”的过滤关键字。不允许一个关键字中出现两个以上的“*”。过滤词汇文件格式如：test1、te*st2；不允许：te**st、t*es*t、*test。

“^”只能出现在关键字的开头和结尾的位置，最多允许出现两个。例如：^hello，它可以匹配以 hello 开头的字符串，如 helloworld、hello，但其不匹配 ahelloworld；you^可以匹配以 you 结尾的字符串，如 thankyou、you，但其不匹配 thankyour、your。

“?”代表一个字符，如果是汉字这要用“??”。“?”可以出现多个，并可以连续出现。其可以出现在随意的位置，但不能和“*”相邻。如果出现在开始和结尾的位置，则一定要和“^”相邻。“?”只能通过文件加载，不能通过命令行输入。

用户可以通过命令行和文件的形式加载带空格“ ”的关键字。空格的个数和位置没有限制，一个空格可以匹配连续的几个空格。

缺省情况下，未添加任何过滤关键字。

注意：

添加的 Web 内容过滤关键字不能为 HTML 语言的标记，例如<head>、<html>、<title>、<script>等等，否则合法的网页可能会被过滤掉。

【举例】

添加包含关键字“music”的过滤条目。

```
[H3C] firewall webdata-filter add music
```

10.1.25 firewall webdata-filter clear

【命令】

firewall webdata-filter clear

【视图】

系统视图

【参数】

无

【描述】

firewall webdata-filter clear 命令用来清除所有内容关键字条目。

【举例】

清除所有内容关键字条目。

```
[H3C] firewall webdata-filter clear
```

10.1.26 firewall webdata-filter delete

【命令】

firewall webdata-filter delete *keywords*

【视图】

系统视图

【参数】

keywords：删除的过滤关键字。

【描述】

firewall webdata-filter delete 命令用来删除 Web 内容过滤关键字。

【举例】

删除包含关键字“music”的过滤条目。

```
[H3C] firewall webdata-filter delete music
```

10.1.27 firewall webdata-filter enable

【命令】

firewall webdata-filter enable

undo firewall webdata-filter enable

【视图】

系统视图

【参数】

无

【描述】

firewall webdata-filter enable 命令用来使能 Web 内容过滤功能，**undo firewall webdata-filter enable** 命令用来关闭 Web 内容过滤功能。

缺省情况下，关闭 Web 内容过滤功能。

开启 Web 内容过滤功能之前要先配置 ASPF 策略，**detect http**，**detect tcp**，才能使 Web 内容过滤功能生效。

对于监听非标准端口的 HTTP 协议，必须使用 **port-mapping** 命令正确的配置端口映射，这样 Web 内容过滤功能才能生效。

有关ASPF配置命令请参见 4.2 状态防火墙配置命令。

【举例】

使能 Web 内容过滤功能。

```
[H3C] firewall webdata-filter enable
```

10.1.28 firewall webdata-filter load-file

【命令】

firewall webdata-filter load-file *file-name*

undo firewall webdata-filter load-file

【视图】

系统视图

【参数】

file-name：装载的过滤文件名。

【描述】

firewall webdata-filter load-file 命令用来装载 Web 内容过滤文件，**undo firewall webdata-filter load-file** 命令用来卸载 Web 内容过滤文件。

如果要使 Web 内容过滤文件中的条目生效并对内容进行过滤，必须将其装载。

Web 内容过滤的真正目的是过滤掉包含非法内容的 HTTP 回应报文。一旦 HTTP 回应报文包含需要过滤的内容，则报文将被过滤。

【举例】

装载名为 webdatafilter 的 Web 内容过滤文件。

```
[H3C] firewall webdata-filter load-file webdatafilter
```

10.1.29 firewall webdata-filter save-file

【命令】

firewall webdata-filter save-file *file-name*

【视图】

系统视图

【参数】

file-name：保存的过滤文件名。

【描述】

firewall webdata-filter save-file 命令用来保存 Web 内容过滤文件。

【举例】

保存名为 webdatafilter 的 Web 内容过滤文件。

```
[H3C] firewall webdata-filter save-file webdatafilter
```

10.1.30 reset firewall url-filter host counter

【命令】

reset firewall url-filter host counter

【视图】

用户视图

【参数】

无

【描述】

reset firewall url-filter host counter 命令用来清除 Web 地址过滤的统计信息。

【举例】

清除 Web 地址过滤的统计信息。

```
<H3C> reset firewall url-filter host counter
```

10.1.31 reset firewall url-filter parameter counter

【命令】

reset firewall url-filter parameter counter

【视图】

用户视图

【参数】

无

【描述】

reset firewall url-filter parameter counter 命令用来清除 SQL 注入攻击防范的统计信息。

【举例】

清除 SQL 注入攻击防范的统计信息。

```
<H3C> reset firewall url-filter parameter counter
```

10.1.32 reset firewall webdata-filter counter

【命令】

reset firewall webdata-filter counter

【视图】

用户视图

【参数】

无

【描述】

reset firewall webdata-filter counter 命令用来清除 Web 内容过滤的统计信息。

【举例】

清除 Web 内容过滤的统计信息。

```
<H3C> reset firewall webdata-filter counter
```

10.2 邮件过滤配置命令

10.2.1 debugging firewall smtp-filter

【命令】

debugging firewall smtp-filter

undo debugging firewall smtp-filter

【视图】

用户视图

【参数】

无

【描述】

debugging firewall smtp-filter 命令用来打开邮件过滤的调试功能，**undo debugging firewall smtp-filter** 命令用来关闭调试功能。

缺省情况下，关闭调试功能。

【举例】

打开邮件过滤的调试功能。

```
<H3C> debugging firewall smtp-filter
```

10.2.2 display firewall smtp-filter

【命令】

display firewall smtp-filter { **all** | { **rcptto** | **subject** | **content** | **attach** } { **item** *string* | **item-all** } }

【视图】

所有视图

【参数】

all：显示所有的邮件过滤信息。

rcptto：显示邮件地址过滤信息。

subject：显示邮件主题过滤信息。

content：显示邮件内容过滤信息

attach：显示邮件附件过滤信息。

item *string*：显示具体的过滤关键字条目的统计信息。

Item-all：显示所有的过滤关键字条目的统计信息。

【描述】

display firewall smtp-filter 命令用来显示邮件过滤信息。

【举例】

显示所有邮件过滤的信息。

```
[H3C] display firewall smtp-filter all
 Smtp-filter rcptto is enabled.
 Default method: deny.
 Rcptto has Loaded file "flash:/rcpttofilter", there are 1 item(s) in filter
now( 5 Added,0 Loaded).
Packet(s) blocked    :0.

 Packet(s) allowed    :0.

 Smtp-filter subject is enabled.
 Subject has Loaded file "flash:/subjectfilter", there are 1 item(s) in filter
now( 7 Added,0 Loaded).
Packet(s) blocked    :0.

 Smtp-filter content is enabled.
 Content has Loaded file "flash:/contentfilter", there are 1 item(s) in filter
now( 5 Added,0 Loaded).
Packet(s) blocked    :0.

 Smtp-filter attach is enabled.
 Attach has Loaded file "flash:/attachfilter", there are 1 item(s) in filter
now( 6 Added,0 Loaded).
Packet(s) blocked    :0.
```

10.2.3 firewall smtp-filter attach add

【命令】

firewall smtp-filter attach add *file-name*

【视图】

系统视图

【参数】

file-name：添加的附件文件名。

【描述】

firewall smtp-filter attach add 命令用来添加过滤附件名。

过滤附件名最长支持 128 个字符。系统允许用户添加两种形式的过滤附件名，一种是完全的文件名，另外一种是“*.ext”形式的文件名。对于第二种则只过滤附件扩展名而不比较扩展名前的文件名。允许过滤文件中同时存在*.exe 和 abc.exe 这样的文件名，当用户取消*.exe 格式的文件名过滤后，abc.exe 过滤继续起作用。

缺省情况下，未添加过滤附件名。

【举例】

添加包含附件名为“virus.exe”的过滤条目。

```
[H3C] firewall smtp-filter attach add virus.exe
```

10.2.4 firewall smtp-filter attach clear

【命令】

firewall smtp-filter attach clear

【视图】

系统视图

【参数】

无

【描述】

firewall smtp-filter attach clear 命令用来清除所有过滤附件名。

【举例】

清除所有过滤附件名条目。

```
[H3C] firewall smtp-filter attach clear
```

10.2.5 firewall smtp-filter attach delete

【命令】

firewall smtp-filter attach delete *file-name*

【视图】

系统视图

【参数】

file-name：删除的附件文件名。

【描述】

firewall smtp-filter attach delete 命令用来删除过滤附件名。

【举例】

删除附件名为“virus.exe”的过滤条目。

```
[H3C] firewall smtp-filter attach delete virus.exe
```

10.2.6 firewall smtp-filter attach enable

【命令】

firewall smtp-filter attach enable

undo firewall smtp-filter attach enable

【视图】

系统视图

【参数】

无

【描述】

firewall smtp-filter attach enable 命令用来使能邮件附件过滤功能，**undo firewall smtp-filter attach enable** 命令用来关闭邮件附件过滤功能。

当使用邮件附件过滤时，被过滤的邮件的附件名长度不能超过 128 个字符。

缺省情况下，关闭邮件附件过滤功能。

开启邮件附件过滤功能之前要先配置 ASPF 策略，**detect smtp**，**detect tcp**，才能使邮件附件过滤功能生效。

对于监听非标准端口的 SMTP 协议，必须使用 **port-mapping** 命令正确的配置端口映射，这样邮件附件过滤功能才能生效。

有关ASPF配置命令请参见 4.2 状态防火墙配置命令。

【举例】

使能邮件附件过滤功能。

```
[H3C] firewall smtp-filter attach enable
```

10.2.7 firewall smtp-filter attach load-file

【命令】

firewall smtp-filter attach load-file *file-name*

undo firewall smtp-filter attach load-file

【视图】

系统视图

【参数】

file-name：装载的过滤文件名。

【描述】

firewall smtp-filter attach load-file 命令用来装载邮件附件过滤文件，**undo firewall smtp-filter attach load-file** 命令用来卸载邮件附件过滤文件。

如果要使邮件附件过滤文件中的条目生效并对附件进行过滤，必须将其装载。

【举例】

装载名为 attachfilter 的邮件附件过滤文件。

```
[H3C] firewall smtp-filter attach load-file attachfilter
```

10.2.8 firewall smtp-filter attach save-file

【命令】

firewall smtp-filter attach save-file *file-name*

【视图】

系统视图

【参数】

file-name：保存的过滤文件名。

【描述】

firewall smtp-filter attach save-file 命令用来保存邮件附件过滤文件。

【举例】

保存名为 attachfilter 的邮件附件过滤文件。

```
[H3C] firewall smtp-filter attach save-file attachfilter
```

10.2.9 firewall smtp-filter content add

【命令】

firewall smtp-filter content add *content-keywords*

【视图】

系统视图

【参数】

content-keywords：添加的内容过滤关键字。

【描述】

firewall smtp-filter content add 命令用来添加内容过滤关键字。

过滤关键字最长支持 128 个字符。关键字过滤支持模糊查找，即允许向过滤关键字文件中添加带 “*”的关键字，“*”表示最少 0 个到最多 2 个任意中文字符或最少 0 个到最多 4 个任意英文字符。为避免“*”带来的误判断，管理员应谨慎添加带“*”的过滤关键字。*只允许出现在关键字的中间。不允许一个关键字中出现两个以上的“*”。过滤词汇文件格式如：test1、te*st2；不允许：te**st、t*es*t。

缺省情况下，未添加内容过滤关键字。

【举例】

添加包含内容关键字“abcde”的过滤条目。

```
[H3C] firewall smtp-filter content add abcde
```

10.2.10 firewall smtp-filter content clear

【命令】

firewall smtp-filter content clear

【视图】

系统视图

【参数】

无

【描述】

firewall smtp-filter content clear 命令用来清除所有内容过滤关键字条目。

【举例】

清除所有过滤关键字条目。

```
[H3C] firewall smtp-filter content clear
```

10.2.11 firewall smtp-filter content delete

【命令】

firewall smtp-filter content delete *content-keywords*

【视图】

系统视图

【参数】

content-keywords：删除的内容过滤关键字。

【描述】

firewall smtp-filter content delete 命令用来删除邮件内容过滤关键字。

【举例】

删除内容关键字为“abcde”的过滤条目。

```
[H3C] firewall smtp-filter content delete abcde
```

10.2.12 firewall smtp-filter content enable

【命令】

firewall smtp-filter content enable

undo firewall smtp-filter content enable

【视图】

系统视图

【参数】

无

【描述】

firewall smtp-filter content enable 命令用来使能邮件内容过滤功能，**undo firewall smtp-filter content enable** 命令用来关闭邮件内容过滤功能。

缺省情况下，关闭邮件内容过滤功能。

开启邮件内容过滤功能之前要先配置 ASPF 策略，**detect smtp**，**detect tcp**，才能使邮件内容过滤功能生效。

对于监听非标准端口的 SMTP 协议，必须使用 **port-mapping** 命令正确的配置端口映射，这样邮件内容过滤功能才能生效。

有关ASPF配置命令请参见 4.2 状态防火墙配置命令。

【举例】

使能邮件内容过滤功能。

```
[H3C] firewall smtp-filter content enable
```

10.2.13 firewall smtp-filter content load-file

【命令】

firewall smtp-filter content load-file *file-name*

undo firewall smtp-filter content load-file

【视图】

系统视图

【参数】

file-name：装载的过滤文件名。

【描述】

firewall smtp-filter content load-file 命令用来装载邮件内容过滤文件，**undo firewall smtp-filter content load-file** 命令用来卸载邮件内容过滤文件。

如果要使邮件内容过滤文件中的条目生效并对内容进行过滤，必须将其装载。

【举例】

装载名为 subjectfilter 的邮件地址过滤文件。

```
[H3C] firewall smtp-filter content load-file contentfilter
```

10.2.14 firewall smtp-filter content save-file

【命令】

firewall smtp-filter content save-file *file-name*

【视图】

系统视图

【参数】

file-name：保存的过滤文件名。

【描述】

firewall smtp-filter content save-file 命令用来保存邮件内容过滤文件。

【举例】

保存名为 contentfilter 的邮件内容过滤文件。

```
[H3C] firewall smtp-filter content save-file contentfilter
```

10.2.15 firewall smtp-filter rcptto add

【命令】

firewall smtp-filter rcptto add { **permit** | **deny** } *mail-address*

【视图】

系统视图

【参数】

permit：表示操作行为为允许。

deny：表示操作行为为拒绝。

mail-address：添加的过滤地址。

【描述】

firewall smtp-filter rcptto add 命令用来添加邮件过滤地址，并设置对其的过滤行为。

邮件地址最长允许 128 个字符（含 用户名、@符和其后的域名）。电子邮件地址用户名部分要么是完整的用户名称，要么是*，不允许出现用户名称和*同时出现的邮件地址。

邮件地址可以是下面几种格式：

test@h3c.com：表示该地址需要进行精确匹配

*@h3c.com：表示只匹配@后面的主机名部分，忽略前面的用户名

@.sina.com：表示将类似 mail.sina.com 和 smtp.sina.com 的主机名都匹配，而不匹配 sina.com 和 smtp.sina.com.cn

不支持以下的地址格式：*@*.*.com.cn、*@news.*.com、*@163.*，即“*”只能出现在@前后。

系统对邮件地址进行检查时，先检查域名部分，找到与当前域名最匹配的一项或几项，然后按照配置的先后顺序对用户名进行检查。当找到一个匹配项后即按照设定的操作进行处理。

缺省情况下，未添加邮件过滤地址。

【举例】

添加允许收件人地址为 163.com 域中的所有地址“*@163.com”的过滤条目。

```
[H3C] firewall smtp-filter rcptto add permit *@163.com
```

10.2.16 firewall smtp-filter rcptto clear

【命令】

firewall smtp-filter rcptto clear

【视图】

系统视图

【参数】

无

【描述】

firewall smtp-filter rcptto clear 命令用来清除所有邮件过滤地址条目。

【举例】

清除所有邮件过滤地址条目。

```
[H3C] firewall smtp-filter rcptto clear
```

10.2.17 firewall smtp-filter rcptto default

【命令】

firewall smtp-filter rcptto default { **permit** | **deny** }

【视图】

系统视图

【参数】

permit：配置默认过滤操作为允许。

deny：配置默认过滤操作为拒绝。

【描述】

firewall smtp-filter rcptto default 命令用来允许或者拒绝未与管理员配置的邮件地址发生匹配的数据报通过。

缺省情况下，允许未发生匹配的数据报通过。

【举例】

配置默认过滤行为为允许。

```
[H3C] firewall smtp-filter rcptto default permit
```

10.2.18 firewall smtp-filter rcptto delete

【命令】

firewall smtp-filter rcptto delete *mail-address*

【视图】

系统视图

【参数】

mail-address：删除的邮件过滤地址。

【描述】

firewall smtp-filter rcptto delete 命令用来删除邮件过滤地址。

【举例】

删除地址为“*@163.com”的过滤条目。

```
[H3C] firewall smtp-filter rcptto delete *@163.com
```

10.2.19 firewall smtp-filter rcptto enable

【命令】

firewall smtp-filter rcptto enable

undo firewall smtp-filter rcptto enable

【视图】

系统视图

【参数】

无

【描述】

firewall smtp-filter rcptto enable 命令用来使能邮件地址过滤功能，**undo firewall smtp-filter rcptto enable** 命令用来关闭邮件地址过滤功能。

缺省情况下，关闭邮件地址过滤功能。

开启邮件地址过滤功能之前要先配置 ASPF 策略，**detect smtp**，**detect tcp**，才能使邮件地址过滤功能生效。

对于监听非标准端口的 SMTP 协议，必须使用 **port-mapping** 命令正确的配置端口映射，这样邮件地址过滤功能才能生效。

有关ASPF配置命令请参见 4.2 状态防火墙配置命令。

【举例】

使能邮件地址过滤功能。

```
[H3C] firewall smtp-filter rcptto enable
```

10.2.20 firewall smtp-filter rcptto load-file

【命令】

firewall smtp-filter rcptto load-file *file-name*

undo firewall smtp-filter rcptto load-file

【视图】

系统视图

【参数】

file-name：装载的过滤文件名。

【描述】

firewall smtp-filter rcptto load-file 命令用来装载邮件地址过滤文件，**undo firewall smtp-filter rcptto load-file** 命令用来卸载邮件地址过滤文件。

如果要使邮件地址过滤文件中的条目生效并对地址进行过滤，必须将其装载。

【举例】

装载名为 rcpttofilter 的邮件地址过滤文件。

```
[H3C] firewall smtp-filter rcptto load-file rcpttofilter
```

10.2.21 firewall smtp-filter rcptto save-file

【命令】

firewall smtp-filter rcptto save-file *file-name*

【视图】

系统视图

【参数】

file-name：保存的过滤文件名。

【描述】

firewall smtp-filter rcptto save-file 命令用来保存邮件地址过滤文件。

【举例】

保存名为 rcpttofilter 的邮件地址过滤文件。

```
[H3C] firewall smtp-filter rcptto save-file rcpttofilter
```

10.2.22 firewall smtp-filter subject add

【命令】

firewall smtp-filter subject add *mail-subject*

【视图】

系统视图

【参数】

mail-subject：添加的过滤主题。

【描述】

firewall smtp-filter subject add 命令用来添加邮件过滤主题。

过滤关键字最长支持 128 个字符。关键字过滤支持模糊查找，即允许向过滤关键字文件中添加带“*”的关键字，“*”表示最少 0 个到最多 2 个任意中文字符或最少 0 个到最多 4 个任意英文字符。为避免“*”带来的误判断，管理员应谨慎添加带“*”的过滤关键字。*只允许出现在关键字的中间。不允许一个关键字中出现两个以上的“*”。过滤词汇文件格式如：test1、te*st2；不允许：te**st、t*es*t。

缺省情况下，未添加过滤主题。

【举例】

添加包含主题“Hi”的过滤条目。

```
[H3C] firewall smtp-filter subject add Hi
```

10.2.23 firewall smtp-filter subject clear

【命令】

firewall smtp-filter subject clear

【视图】

系统视图

【参数】

无

【描述】

firewall smtp-filter subject clear 命令用来清除所有过滤主题条目。

【举例】

清除所有过滤主题条目。

```
[H3C] firewall smtp-filter subject clear
```

10.2.24 firewall smtp-filter subject delete

【命令】

firewall smtp-filter subject delete *mail-subject*

【视图】

系统视图

【参数】

mail-subject：删除的过滤主题。

【描述】

firewall smtp-filter subject delete 命令用来删除邮件过滤主题。

【举例】

删除主题为“Hi”的过滤条目。

```
[H3C] firewall smtp-filter subject delete Hi
```

10.2.25 firewall smtp-filter subject enable

【命令】

firewall smtp-filter subject enable

undo firewall smtp-filter subject enable

【视图】

系统视图

【参数】

无

【描述】

firewall smtp-filter subject enable 命令用来使能邮件主题过滤功能，**undo firewall smtp-filter subject enable** 命令用来关闭邮件主题过滤功能。

当使用邮件主题过滤时，被过滤的邮件的主题长度不能超过 512 个字符。

缺省情况下，关闭邮件主题过滤功能。

开启邮件主题过滤功能之前要先配置 ASPF 策略，**detect smtp**，**detect tcp**，才能使邮件主题过滤功能生效。

对于监听非标准端口的 SMTP 协议，必须使用 **port-mapping** 命令正确的配置端口映射，这样邮件主题过滤功能才能生效。

有关ASPF配置命令请参见 4.2 状态防火墙配置命令。

【举例】

使能邮件主题过滤功能。

```
[H3C] firewall smtp-filter subject enable
```

10.2.26 firewall smtp-filter subject load-file

【命令】

firewall smtp-filter subject load-file *file-name*

undo firewall smtp-filter subject load-file

【视图】

系统视图

【参数】

file-name：装载的过滤文件名。

【描述】

firewall smtp-filter subject load-file 命令用来装载邮件主题过滤文件，**undo firewall smtp-filter subject load-file** 命令用来卸载邮件主题过滤文件。

如果要使邮件主题过滤文件中的条目生效并对主题进行过滤，必须将其装载。

【举例】

装载名为 subjectfilter 的邮件主题过滤文件。

```
[H3C] firewall smtp-filter subject load-file subjectfilter
```

10.2.27 firewall smtp-filter subject save-file

【命令】

firewall smtp-filter subject save-file *file-name*

【视图】

系统视图

【参数】

file-name：保存的过滤文件名。

【描述】

firewall smtp-filter subject save-file 命令用来保存邮件主题过滤文件。

【举例】

保存名为 subjectfilter 的邮件主题过滤文件。

```
[H3C] firewall smtp-filter subject save-file subjectfilter
```

10.2.28 reset firewall smtp-filter counter

【命令】

reset firewall smtp-filter [**rcptto** | **subject** | **content** | **attach**] **counter**

【视图】

用户视图

【参数】

rcptto：邮件地址过滤。

subject：邮件主题过滤。

content：邮件内容过滤。

attach：邮件附件过滤。

【描述】

reset firewall smtp-filter counter 命令用来清除邮件过滤的统计信息。

【举例】

清除邮件地址过滤的统计信息。

```
<H3C> reset firewall smtp-filter rcptto counter
```

第11章 攻击防范配置命令

11.1 攻击防范配置命令

11.1.1 debugging firewall defend

【命令】

debugging firewall defend { **all** | **arp-flood** | **arp-spoofing** | **ip-spoofing** | **land** | **smurf** | **fraggle** | **frag-flood** | **winnuke** | **syn-flood** | **icmp-flood** | **udp-flood** | **icmp-redirect** | **icmp-unreachable** | **ip-sweep** | **port-scan** | **source-route** | **route-record** | **tracert** | **ping-of-death** | **teardrop** | **tcp-flag** | **ip-fragment** | **large-icmp** }

undo debugging firewall defend { **all** | **arp-flood** | **arp-spoofing** | **ip-spoofing** | **land** | **smurf** | **fraggle** | **frag-flood** | **winnuke** | **syn-flood** | **icmp-flood** | **udp-flood** | **icmp-redirect** | **icmp-unreachable** | **ip-sweep** | **port-scan** | **source-route** | **route-record** | **tracert** | **ping-of-death** | **teardrop** | **tcp-flag** | **ip-fragment** | **large-icmp** }

【视图】

用户视图

【参数】

各参数：表示启动或关闭指定攻击防范功能的调试开关。

【描述】

debugging firewall defend 命令用来打开攻击防范功能的调试开关，**undo debugging firewall defend** 命令用来关闭攻击防范功能的调试开关。

系统缺省为关闭各攻击防范功能的调试开关。

相关配置可参考命令 **display debugging**。

【举例】

对 SYN Flood 攻击防范功能进行调试。

```
<H3C> debugging firewall defend syn-flood
```

11.1.2 display firewall defend flag

【命令】

display firewall defend flag

【视图】

所有视图

【参数】

无

【描述】

display firewall defend flag 命令用来显示防火墙上已启用的攻击防范类型。

【举例】

显示防火墙采用的攻击防范的类型信息。

```
<H3C> display firewall defend flag
The attack defend flag is:
 ip-spoofing        land               smurf              fraggle
 winnuke            icmp-redirect      icmp-unreachable   source-route
 route-record       tracert            ping-of-death      tcp-flag
 ip-fragment        large-icmp         teardrop           ip-sweep
 port-scan          syn-flood          udp-flood          icmp-flood
 arp-spoofing       arp-flood          frag-flood
```

11.1.3 display firewall tcp-proxy session

【命令】

display firewall tcp-proxy session [**zone** *zone-name* **| ip** *ip-address*]

【视图】

所有视图

【参数】

zone：安全区域的名称，显示指定安全区域的 TCP 代理的会话信息。

ip-address：IP 地址，显示指定 IP 地址的 TCP 代理的会话信息。

【描述】

display firewall tcp-proxy session 命令用来显示 TCP 代理的会话信息，若不指定参数，则显示所有的 TCP 代理会话信息。

【举例】

显示所有的 TCP-Proxy 会话信息。

```
<H3C> display firewall tcp-proxy session
Firewall Tcp-proxy session table information:
```

```
 State:2
 SrcZone:trust                        SrcIP&SrcPort:1.0.0.1       1025
 DestZone:untrust                         DestIP&DestPort:2.0.0.1       1026
 State:4
 SrcZone:untrust                      SrcIP&SrcPort:2.0.0.3          1028
 DestZone:trust                        DestIP&DestPort:1.0.0.2       1026
 State:6
 SrcZone:untrust                      SrcIP&SrcPort:2.0.0.5          1032
 DestZone:trust                        DestIP&DestPort:1.0.0.6       1028
 State:2
 SrcZone:trust                        SrcIP&SrcPort:1.0.0.3          1035
 DestZone:untrust                     DestIP&DestPort:2.0.0.8        1045
```

显示指定安全区域的 TCP-Proxy 会话信息。

```
<H3C> display firewall tcp-proxy session zone trust
Firewall Tcp-proxy session table information for destination zone trust:
State:4
 SrcZone:untrust                      SrcIP&SrcPort:2.0.0.3          1028
 DestZone:trust                        DestIP&DestPort:1.0.0.2       1026
 State:6
 SrcZone:untrust                      SrcIP&SrcPort:2.0.0.5          1032
 DestZone:trust                        DestIP&DestPort:1.0.0.6       1028
```

显示指定目的 IP 的 TCP-Proxy 会话信息。

```
<H3C> display firewall tcp-proxy session ip 2.0.0.1
Firewall Tcp-proxy session table information for destination IP 2.0.0.1:
State:2
 SrcZone:trust                        SrcIP&SrcPort:1.0.0.1       1025
 DestZone:untrust                         DestIP&DestPort:2.0.0.1       1026
```

表11-1 display firewall tcp-proxy session 命令显示信息描述表

字段	描述
SrcZone	源安全区域名
SrcIP	源 IP 地址
SrcPort	源端口号
DestZone	目的安全区域名
DestIP	目的 IP 地址
DestPort	目的端口号
State	TCP-Proxy 会话状态值

11.1.4 firewall defend all

【命令】

firewall defend all

undo firewall defend all

【视图】

系统视图

【参数】

无

【描述】

firewall defend all 命令用来打开所有的攻击防范功能，**undo firewall defend all** 命令用来关闭所有的攻击防范功能。

缺省情况下，关闭任何攻击防范功能。

【举例】

打开所有攻击防范功能。

```
[H3C] firewall defend all
```

11.1.5 firewall defend arp-flood

【命令】

firewall defend arp-flood [**max-rate** *rate-number*]

undo firewall defend arp-flood [**max-rate**]

【视图】

系统视图

【参数】

max-rate *rate-number*：设定收到的 ARP 包速率的阈值，即一秒钟出现 ARP 包的总数，超过该阈值将视为攻击。*rate-number* 的默认值为 100 包/秒，取值范围为 1～1,000,000 包/秒。

【描述】

firewall defend arp-flood 命令用来打开 arp_flood 攻击防范功能，**undo firewall defend arp-flood** 命令用来关闭 arp_flood 攻击防范功能。

缺省情况下，关闭 ARP Flood 攻击防范功能。

【举例】

打开 ARP Flood 攻击防范功能。

```
[H3C] firewall defend arp-flood
```

11.1.6 firewall defend arp-spoofing

【命令】

firewall defend arp-spoofing [**loose**]

undo firewall defend arp-spoofing [**loose**]

【视图】

系统视图

【参数】

loose：使用宽松检测模式。

【描述】

firewall defend arp-spoofing 命令用来打开 ARP 欺骗攻击防范功能，并使用非宽松检测模式；**firewall defend arp-spoofing loose** 命令用来打开 ARP 欺骗攻击防范功能，并使用宽松检测模式。

undo firewall defend arp-spoofing 命令用来关闭 ARP 欺骗攻击防范功能；**undo firewall defend arp-spoofing loose** 命令用来取消宽松检测，使用非宽松检测模式。

ARP 欺骗攻击防范有两种模式，一种为宽松检测模式，一种为非宽松检测模式。当使用非宽松检测（即不配置 **loose** 选项）时，防火墙会将目的 MAC 地址为单播地址的 ARP 请求视为攻击报文，并将其丢弃。若使用宽松检测（即配置 **loose** 选项），目的 MAC 地址为单播地址的 ARP 请求不被视为攻击报文，且不进行丢弃。

缺省情况下，关闭 ARP 欺骗攻击防范功能。

【举例】

打开 ARP 欺骗攻击防范功能，并使用非宽松检测模式。

```
[H3C] firewall defend arp-spoofing
```

11.1.7 firewall defend fraggle

【命令】

firewall defend fraggle

undo firewall defend fraggle

【视图】

系统视图

【参数】

无

【描述】

firewall defend fraggle 命令用来打开 Fraggle 攻击防范功能，**undo firewall defend fraggle** 命令用来关闭 Fraggle 攻击防范功能。

系统缺省为关闭 Fraggle 攻击防范功能。

【举例】

打开 Fraggle 攻击防范功能。

```
[H3C] firewall defend fraggle
```

11.1.8 firewall defend frag-flood

【命令】

firewall defend frag-flood [**max-identical-rate** *max-identical-rate*] [**max-total-rate** *max-total-rate*]

undo firewall defend frag-flood [**max-identical-rate**] [**max-total-rate**]

【视图】

系统视图

【参数】

max-identical-rate：最大相同分片报文速率，范围为 1～10,000，缺省值为 50。

max-total-rate：最大分片报文速率，范围为 1～10,000，缺省值为 100。

【描述】

firewall defend frag-flood 命令用来打开 Frag Flood 攻击防范功能，**undo firewall defend frag-flood** 命令用来关闭 Frag Flood 攻击防范功能。

对于目的地为防火墙自身的分片报文攻击，防火墙只告警，但不丢弃报文。否则，防火墙将告警，并丢弃报文。

缺省情况下，关闭 Frag Flood 攻击防范功能。

【举例】

打开 Frag Flood 攻击防范功能。

```
[H3C] firewall defend frag-flood
```

11.1.9 firewall defend icmp-flood

【命令】

firewall defend icmp-flood { **ip** *ip-address* | **zone** *zone-name* } [**max-rate** *rate-number*]

undo firewall defend icmp-flood [**ip** [*ip-address* [**max-rate**]] | **zone** [*zone-name* [**max-rate**]]]

【视图】

系统视图

【参数】

ip *ip-address*：设定受保护的主机 IP 地址。如果 **undo** 形式只列出 **ip** 而不指定具体 *ip-address*，则关闭对所有已配置了 IP 保护的主机进行 ICMP Flood 检测。

zone *zone-name*：设定受保护的安全区域名，此参数表示对安全区域内的所有 IP 地址使能 ICMP Flood 攻击检测功能。如果 **undo** 形式只列出 **zone** 而不指定具体安全区域名 *zone-name*，则关闭对所有已配置了保护的安全区域进行 ICMP Flood 检测。

max-rate *rate-number*：设定连接特定目的 IP 的 ICMP 包速率的阈值，即一秒钟出现 ICMP 包的总数，超过该阈值将视为攻击。*rate-number* 的默认值为 1000 包/秒，取值范围为 1～1,000,000 包/秒。

【描述】

firewall defend icmp-flood 命令用来使能 ICMP Flood 攻击检测功能，该命令可选择对指定 IP 或指定安全区域进行保护；**undo firewall defend icmp-flood** 命令用来关闭 ICMP Flood 攻击检测功能。

ICMP Flood 的 IP 配置的优先级比安全区域配置的优先级高。如果对特定 IP 配置开启 ICMP Flood 攻击防范功能，同时也对该 IP 所在的安全区域内的所有 IP 配置开启了防范功能，则该 IP 的各检测参数以 IP 配置为准；若此时取消 IP 配置，则该 IP 的各检测参数以安全区域配置为准。

系统缺省为关闭 ICMP Flood 攻击检测功能。

除使用命令 **firewall defend icmp-flood** 外，使能 ICMP Flood 攻击检测功能还需使用命令 **firewall defend icmp-flood enable** 打开全局开关，并开启受保护 IP 或安全区域入方向的 IP 统计功能。

【举例】

打开对 Trust 安全区域内所有 IP 的 ICMP Flood 攻击检测的开关，设定 ICMP 包连接速率的阈值为 500 包/秒。

```
[H3C] firewall defend icmp-flood zone trust max-rate 500
```

11.1.10 firewall defend icmp-flood enable

【命令】

firewall defend icmp-flood enable

undo firewall defend icmp-flood enable

【视图】

系统视图

【参数】

无

【描述】

firewall defend icmp-flood enable 命令用来打开 ICMP Flood 攻击检测功能；**undo firewall defend icmp-flood enable** 命令用来关闭 ICMP Flood 攻击检测功能。

系统缺省为关闭 ICMP Flood 攻击检测功能。

【举例】

打开 ICMP Flood 攻击检测功能。

```
[H3C] firewall defend icmp-flood enable
```

11.1.11 firewall defend icmp-redirect

【命令】

firewall defend icmp-redirect

undo firewall defend icmp-redirect

【视图】

系统视图

【参数】

无

【描述】

firewall defend icmp-redirect 命令用来打开 ICMP 重定向报文攻击防范功能，**undo firewall defend icmp-redirect** 命令用来关闭 ICMP 重定向报文攻击防范功能。

系统缺省为关闭 ICMP 重定向报文攻击防范功能。

【举例】

打开 ICMP 重定向报文攻击防范功能。

```
[H3C] firewall defend icmp-redirect
```

11.1.12 firewall defend icmp-unreachable

【命令】

firewall defend icmp-unreachable

undo firewall defend icmp-unreachable

【视图】

系统视图

【参数】

无

【描述】

firewall defend icmp-unreachable 命令用来打开ICMP不可达报文攻击防范功能，**undo firewall defend icmp-unreachable** 命令用来关闭 ICMP 不可达报文攻击防范功能。

系统缺省为关闭 ICMP 不可达报文攻击防范功能。

【举例】

打开 ICMP 不可达报文攻击防范功能。

```
[H3C] firewall defend icmp-unreachable
```

11.1.13 firewall defend ip-fragment

【命令】

firewall defend ip-fragment

undo firewall defend ip-fragment

【视图】

系统视图

【参数】

无

【描述】

firewall defend ip-fragment 命令用来打开 IP 分片报文检测功能，**undo firewall**

defend ip-fragment 命令用来关闭 IP 分片报文检测功能。

系统缺省为关闭 IP 分片报文检测功能。

【举例】

打开 IP 分片报文检测功能。

```
[H3C] firewall defend ip-fragment
```

11.1.14 firewall defend ip-spoofing

【命令】

firewall defend ip-spoofing

undo firewall defend ip-spoofing

【视图】

系统视图

【参数】

无

【描述】

firewall defend ip-spoofing 命令用来打开 IP 欺骗防范功能，**undo firewall defend ip-spoofing** 命令用来关闭 IP 欺骗防范功能。

系统缺省为关闭 IP 欺骗防范功能。

📖 **说明：**

IP 欺骗攻击防范功能不能在透明模式下应用。

【举例】

打开 IP 欺骗防范功能。

```
[H3C] firewall defend ip-spoofing
```

11.1.15 firewall defend ip-sweep

【命令】

firewall defend ip-sweep [**max-rate** *rate-number*] [**blacklist-timeout** *minutes*]

undo firewall defend ip-sweep

【视图】

系统视图

【参数】

max-rate *rate-number*：设定从同一源地址向外发送报文的目的地址变化速率的阈值。*rate-number* 默认值为 4000 次/秒，取值范围为 1～10,000 次/秒。

blacklist-timeout *minutes*：将攻击源 IP 加入黑名单并设定其在黑名单内的保持时间，*minutes* 取值范围为 0～1000 分钟，默认值为 0，表示不加入黑名单。建议将此值设置为大于 2 分钟。

【描述】

firewall defend ip-sweep 命令用来打开地址扫描攻击防范功能，**undo firewall defend ip-sweep** 命令用来关闭地址扫描攻击防范功能。

加入黑名单的老化时间应该大于防火墙会话的超时时间（使用命令 **firewall session aging-time** 设置），否则会导致攻击通过防火墙。必须使能防火墙的黑名单功能后，此命令设置的黑名单功能才能生效。

缺省情况下为关闭地址扫描攻击防范功能。

此命令只有在配置了相关源 IP 或安全区域出方向的 IP 统计功能才起作用。

相关配置命令请参考 **firewall blacklist**。

【举例】

打开地址扫描攻击防范功能，设定扫描速率的阈值为 1000，加入黑名单的时间为 5 分钟，并使能黑名单功能。

```
[H3C] firewall defend ip-sweep max-rate 1000 blacklist-timeout 5
[H3C] firewall blacklist enable
```

11.1.16 firewall defend land

【命令】

firewall defend land

undo firewall defend land

【视图】

系统视图

【参数】

无

【描述】

firewall defend land 命令用来打开 Land 攻击防范功能，**undo firewall defend land** 命令用来关闭 Land 攻击防范功能。

系统缺省为关闭 Land 攻击防范功能。

【举例】

打开 Land 攻击防范功能。

```
[H3C] firewall defend land
```

11.1.17 firewall defend large-icmp

【命令】

firewall defend large-icmp [*length*]

undo firewall defend large-icmp

【视图】

系统视图

【参数】

length：允许通过的 ICMP 报文的最大长度，*length* 的默认值为 4000 字节，取值范围为 28～65535 字节。

【描述】

firewall defend large-icmp 命令用来打开超大 ICMP 报文攻击检测功能，**undo firewall defend large-icmp** 命令用来关闭超大 ICMP 报文攻击检测功能。

系统缺省为关闭超大 ICMP 报文攻击检测功能。

【举例】

打开超大 ICMP 报文攻击检测功能，设定允许报文长度小于 4000 字节的 ICMP 报文通过。

```
[H3C] firewall defend large-icmp 4000
```

11.1.18 firewall defend ping-of-death

【命令】

firewall defend ping-of-death

undo firewall defend ping-of-death

【视图】

系统视图

【参数】

无

【描述】

firewall defend ping-of-death 命令用来打开 ping-of-death 攻击检测功能，**undo firewall defend ping-of-death** 命令用来关闭 ping-of-death 攻击检测功能。

系统缺省为关闭 ping-of-death 攻击检测功能。

【举例】

打开 ping-of-death 攻击检测功能。

```
[H3C] firewall defend ping-of-death
```

11.1.19 firewall defend port-scan

【命令】

firewall defend port-scan [**max-rate** *rate-number*] [**blacklist-timeout** *minutes*]

undo firewall defend port-scan

【视图】

系统视图

【参数】

max-rate *rate-number*：设定从同一源地址向外发送报文的目的端口变化速率的阈值。*rate-number* 默认值为 4000 次/秒，取值范围为 1～10,000 次/秒。

blacklist-timeout *minutes*：将攻击源 IP 加入黑名单并设定其在黑名单内的保持时间，*minutes* 取值范围为 0～1000 分钟，默认值为 0，表示不加入黑名单。建议将此值设置为大于 2 分钟。

【描述】

firewall defend port-scan 命令用来打开端口扫描攻击防范功能，**undo firewall defend port-scan** 命令用来关闭端口扫描攻击防范功能。

加入黑名单的老化时间应该大于防火墙会话的超时时间（使用命令 **firewall session aging-time** 设置），否则会导致攻击通过防火墙。必须使能防火墙的黑名单功能后，此命令设置的黑名单功能才能生效。

缺省情况下为关闭端口扫描攻击防范功能。

此命令只有在配置了相关源 IP 或安全区域出方向的 IP 统计功能后才起作用。

相关配置命令请参考 **firewall blacklist**。

【举例】

打开端口扫描攻击防范功能，设定扫描速率的阈值为 1000，加入黑名单的时间为 5 分钟，并使能黑名单功能。

```
[H3C] firewall defend port-scan max-rate 1000 blacklist-timeout 5
[H3C] firewall blacklist enable
```

11.1.20 firewall defend route-record

【命令】

firewall defend route-record

undo firewall defend route-record

【视图】

系统视图

【参数】

无

【描述】

firewall defend route-record 命令用来打开带路由记录选项报文攻击防范功能，**undo firewall defend route-record** 命令用来关闭带路由记录选项报文攻击防范功能。

系统缺省为关闭带路由记录选项报文攻击防范功能。

【举例】

打开带路由记录选项报文攻击防范功能。

```
[H3C] firewall defend route-record
```

11.1.21 firewall defend smurf

【命令】

firewall defend smurf

undo firewall defend smurf

【视图】

系统视图

【参数】

无

【描述】

firewall defend smurf 命令用来打开 Smurf 攻击防范功能，**undo firewall defend smurf** 命令用来关闭 Smurf 攻击防范功能。

系统缺省为关闭 Smurf 攻击防范功能开关。

【举例】

打开 Smurf 攻击防范功能。

```
[H3C] firewall defend smurf
```

11.1.22 firewall defend source-route

【命令】

firewall defend source-route

undo firewall defend source-route

【视图】

系统视图

【参数】

无

【描述】

firewall defend source-route 命令用来打开带源路由选项报文攻击防范功能，**undo firewall defend source-route** 命令用来关闭带源路由选项报文攻击防范功能。

系统缺省为关闭带源路由选项报文攻击防范功能。

【举例】

打开带源路由选项报文攻击防范功能。

```
[H3C] firewall defend source-route
```

11.1.23 firewall defend syn-flood

【命令】

firewall defend syn-flood { **ip** *ip-address* | **zone** *zone-name* } [**max-rate** *rate-number*] [**tcp-proxy**]

undo firewall defend syn-flood [**ip** [*ip-address* [**max-rate**] [**tcp-proxy**]] | **zone** [*zone-name* [**max-rate**] [**tcp-proxy**]]]

【视图】

系统视图

【参数】

ip *ip-address*：设定受保护的主机 IP 地址。如果 **undo** 形式只列出 **ip** 而不指定具体 *ip-address*，则关闭对所有已配置了 IP 保护的主机进行 SYN Flood 检测。

zone *zone-name*：设定受保护的安全区域名，此参数表示对安全区域内的所有 IP 地址使能 SYN Flood 攻击检测功能。如果 **undo** 形式只列出 **zone** 而不指定具体安全区域名 *zone-name*，则关闭对所有已配置了保护的安全区域进行 SYN Flood 检测。

max-rate *rate-number*：设定连接特定目的 IP 的 SYN 包速率的阈值，即一秒钟出现 SYN 包的总数，超过该阈值将视为攻击。*rate-number* 的默认值为 1000 包/秒，取值范围为 1～1,000,000 包/秒。

tcp-proxy：启动 TCP 代理。当检测到受保护主机受到 SYN Flood 攻击时，TCP 代理自动启动；当不再受到攻击时，TCP 代理自动关闭。

【描述】

firewall defend syn-flood 命令用来使能 SYN Flood 攻击检测功能，该命令可选择对指定 IP 或指定安全区域进行保护；**undo firewall defend syn-flood** 命令用来关闭 SYN Flood 攻击检测功能。

SYN Flood 的 IP 配置的优先级比安全区域配置的优先级高。如果对特定 IP 配置开启 SYN Flood 攻击防范功能，同时也对该 IP 所在的安全区域内的所有 IP 配置开启了防范功能，则该 IP 的各检测参数以 IP 配置为准；若此时取消 IP 配置，则该 IP 的各检测参数以安全区域配置为准。

若要对 SYN Flood 攻击进行防范，则必须配置 TCP 代理。

系统缺省为关闭 SYN Flood 攻击检测功能。

除使用命令 **firewall defend syn-flood** 外，使能 SYN Flood 攻击检测功能还需使用命令 **firewall defend syn-flood enable** 打开全局开关，并开启受保护 IP 或安全区域入方向的 IP 统计功能。

【举例】

打开对 Trust 安全区域内所有 IP 的 SYN Flood 攻击检测的开关，设定 SYN 包连接速率的阈值为 100 包/秒，并启动 TCP 代理功能。

```
[H3C] firewall defend syn-flood zone trust max-rate 100 tcp-proxy
```

11.1.24 firewall defend syn-flood enable

【命令】

firewall defend syn-flood enable

undo firewall defend syn-flood enable

【视图】

系统视图

【参数】

无

【描述】

firewall defend syn-flood enable 命令用来打开 SYN Flood 攻击检测功能，**undo firewall defend syn-flood enable** 命令用来关闭 SYN Flood 攻击检测功能。

系统缺省为关闭 SYN Flood 攻击检测功能。

【举例】

打开 SYN Flood 攻击检测功能。

```
[H3C] firewall defend syn-flood enable
```

11.1.25 firewall defend tcp-flag

【命令】

firewall defend tcp-flag

undo firewall defend tcp-flag

【视图】

系统视图

【参数】

无

【描述】

firewall defend tcp-flag 命令用来打开 TCP 报文标志合法性检测功能，**undo firewall defend tcp-flag** 命令用来关闭 TCP 报文标志合法性检测功能。

系统缺省为关闭 TCP 报文标志合法性检测功能。

【举例】

打开 TCP 报文标志合法性检测功能。

```
[H3C] firewall defend tcp-flag
```

11.1.26 firewall defend teardrop

【命令】

firewall defend teardrop [**teardrop-loose**]

undo firewall defend teardrop [**teardrop-loose**]

【视图】

系统视图

【参数】

teardrop-loose：使用宽松检测模式。

【描述】

firewall defend teardrop 命令用来打开 teardrop 攻击检测功能，并使用非宽松检测模式；**firewall defend teardrop teardrop-loose** 命令用来打开 teardrop 攻击检测功能，并使用宽松检测模式。

undo firewall defend teardrop 命令用来关闭 teardrop 攻击检测功能；**undo firewall defend teardrop teardrop-loose** 命令用来取消宽松检测，使用非宽松检测模式。

系统缺省为关闭 teardrop 攻击检测功能。

【举例】

打开 teardrop 攻击检测功能，并使用非宽松检测模式。

```
[H3C] firewall defend teardrop
```

11.1.27 firewall defend tracert

【命令】

firewall defend tracert

undo firewall defend tracert

【视图】

系统视图

【参数】

无

【描述】

firewall defend tracert 命令用来打开 tracert 报文攻击防范功能，**undo firewall defend tracert** 命令用来关闭 tracert 报文攻击防范功能。

系统缺省为关闭 tracert 报文攻击防范功能。

【举例】

打开 tracert 报文攻击防范功能。

```
[H3C] firewall defend tracert
```

11.1.28 firewall defend udp-flood

【命令】

firewall defend udp-flood { **ip** *ip-address* | **zone** *zone-name* } [**max-rate** *rate-number*]

undo firewall defend udp-flood [**ip** [*ip-address* [**max-rate**]] | **zone** [*zone-name* [**max-rate**]]]

【视图】

系统视图

【参数】

ip *ip-address*：设定受保护的主机 IP 地址。如果 **undo** 形式只列出 **ip** 而不指定具体 *ip-address*，则关闭对所有已配置了 IP 保护的主机进行 UDP Flood 检测。

zone *zone-name*：设定受保护的安全区域名，此参数表示对安全区域内的所有 IP 地址使能 UDP Flood 攻击检测功能。如果 **undo** 形式只列出 **zone** 而不指定具体安全区域名 *zone-name*，则关闭对所有已配置了保护的安全区域进行 UDP Flood 检测。

max-rate *rate-number*：设定连接特定目的 IP 的 UDP 包速率的阈值，即一秒钟出现 UDP 包的总数，超过该阈值将视为攻击，*rate-number* 的默认值为 1000 包/秒，取值范围为 1～1,000,000 包/秒。

【描述】

firewall defend udp-flood 命令用来使能 UDP Flood 攻击检测功能，该命令可选择对指定 IP 或指定安全区域进行保护，**undo firewall defend udp-flood** 命令用来关闭 UDP Flood 攻击检测功能。

UDP Flood 的 IP 配置的优先级比安全区域配置的优先级高。如果对特定 IP 配置开启 UDP Flood 攻击防范功能，同时也对该 IP 所在的安全区域内的所有 IP 配置开启了防范功能，则该 IP 的各检测参数以 IP 配置为准；若此时取消 IP 配置，则该 IP 的各检测参数以安全区域配置为准。

系统缺省为关闭 UDP Flood 攻击检测功能。

除使用命令 **firewall defend udp-flood** 外，使能 UDP Flood 攻击检测功能还需使用命令 **firewall defend udp-flood enable** 打开全局开关，并开启受保护 IP 或安全区域入方向的 IP 统计功能。

【举例】

打开对 Trust 安全区域内所有 IP 的 UDP Flood 攻击检测的开关，设定 UDP 包连接速率的阈值为 500 包/秒。

```
[H3C] firewall defend udp-flood zone trust max-rate 500
```

11.1.29 firewall defend udp-flood enable

【命令】

firewall defend udp-flood enable

undo firewall defend udp-flood enable

【视图】

系统视图

【参数】

无

【描述】

firewall defend udp-flood enable 命令用来打开 UDP Flood 攻击检测功能，**undo firewall defend udp-flood enable** 命令用来关闭 UDP Flood 攻击检测功能。

系统缺省为关闭 UDP Flood 攻击检测功能。

【举例】

打开 UDP Flood 攻击检测功能。

```
[H3C] firewall defend udp-flood enable
```

11.1.30 firewall defend winnuke

【命令】

firewall defend winnuke

undo firewall defend winnuke

【视图】

系统视图

【参数】

无

【描述】

firewall defend winnuke 命令用来打开 WinNuke 攻击防范功能，**undo firewall defend winnuke** 命令用来关闭 WinNuke 攻击防范功能。

系统缺省为关闭 WinNuke 攻击防范功能。

【举例】

打开 WinNuke 攻击防范功能。

```
[H3C] firewall defend winnuke
```

11.1.31 firewall tcp-proxy

【命令】

firewall tcp-proxy { **ip** *ip-address* | **zone** *zone-name* }

undo firewall tcp-proxy { **ip** *ip-address* | **zone** *zone-name* }

【视图】

系统视图

【参数】

ip *ip-address*：设定受保护的主机 IP 地址。

zone *zone-name*：设定受保护的安全区域名。

【描述】

firewall tcp-proxy 命令用来配置为特定主机或安全区域启用 TCP 代理，**undo firewall tcp-proxy** 命令用来配置为特定主机或安全区域关闭 TCP 代理。

缺省情况下，未对任何 IP 地址或安全区域启用 TCP 代理。

📖 **说明：**

如果在配置 SYN Flood 攻击时也启用了 TCP 代理（参见命令 **firewall defend syn-flood**），则在此处的配置优先于 SYN Flood 攻击中的配置，即无论是否受到 SYN Flood 攻击，都启用 TCP 代理，对目的主机或目的安全区域进行保护。

【举例】

为 Trust 区域中的所有主机启用 TCP 代理。

```
[H3C] firewall tcp-proxy zone trust
```

第12章 IDS 联动配置命令

12.1 IDS 联动配置命令

12.1.1 ids-acl enable

【命令】

ids-acl enable

undo ids-acl enable

【视图】

接口视图

【参数】

无

【描述】

ids-acl enable 命令用来允许在接口下发 IDS 联动的 ACL 规则，**undo ids-acl enable** 命令用来取消在接口下发 IDS 联动的 ACL 规则。

可以在以太网接口和 Dialer 接口下发 IDS 联动的 ACL 规则。

缺省情况下，不在任何接口下发 IDS 联动规则。

【举例】

在接口 GigabitEthernet 0/0 下发 IDS 联动的 ACL 规则。

```
[H3C] interface GigabitEthernet 0/0
[H3C-GigabitEthernet0/0] ids-acl enable
```

12.1.2 display ids

【命令】

display ids { **all** | **controlled-interface** | **name** *name* | **source** *ip-addr* | **destination** *ip-addr* }

【视图】

所有视图

【参数】

all：显示所有 IDS 联动信息内容。

controlled-interface：显示当前使能 IDS 联动的 ACL 规则下发的接口列表。

name *name*：显示指定名称的 IDS 联动信息。

source *ip-addr*：显示指定源 IP 地址的 IDS 联动信息。

destination *ip-addr*：显示指定目的 IP 地址的 IDS 联动信息。

【描述】

display ids 命令用来显示 IDS 联动信息。

【举例】

显示所有 IDS 联动信息。

```
<H3C> display ids all
Port list under IDS control is:
      GigabitEthernet0/0
Number of items 4, running items 4
ACL rules created by IDS is:
    1   Name 00000000000000000000000000001111
        Action deny,  time 12000,  curtime 11740
        Smac any,  sip 1.1.1.1,  swild 255.255.255.255,  sport 1234,  prot 6
        Dmac any,  dip 2.2.2.2,  dwild 255.255.255.255,  dport 444,  prot 6
        Interface(s) all, direction all
    2   Name 00000000000000000000000000001112
        Action deny,  time 12000,  curtime 11790
        Smac any,  sip any,  swild 0.0.0.0,  sport 0,  prot any
        Dmac any,  dip any,  dwild 0.0.0.0,  dport 0,  prot any
        Interface(s) all, direction inbound
    3   Name 00000000000000000000000000001113
        Action deny,  time 12000,  curtime 11820
        Smac any,  sip 5.5.5.5,  swild 255.255.255.255,  sport 0,  prot any
        Dmac any,  dip any,  dwild 0.0.0.0,  dport 0,  prot any
        Interface(s) all, direction all
    4   Name 00000000000000000000000000001114
        Action deny,  time 12000,  curtime 11860
        Smac any,  sip 3.3.3.3,  swild 255.255.255.255,  sport 0,  prot 1
        Dmac any,  dip 4.4.4.4,  dwild 255.255.255.255,  dport 0,  prot 1
        Interface(s) all, direction all
Number of items 4, running items 4
```

12.1.3 display ids-acl

【命令】

display ids-acl { **all** | **name** *name* }

【视图】

所有视图

【参数】

all：显示所有 IDS 联动信息生成的 ACL 规则。

name *name*：显示指定名称的 IDS 联动信息生成的 ACL 规则。

【描述】

display ids-acl 命令用来显示 IDS 联动信息生成的 ACL 规则。

【举例】

显示所有 IDS 联动信息生成 ACL 规则。

```
<H3C> display ids-acl all

(Total ACL number is 7)

Interface: GigabitEthernet0/0
IDS_ACL Direction: InBound
 rule 0 deny tcp source 1.1.1.1 0 source-port eq 1234 destination 2.2.2.2 0
destination-port eq 444 (0 times matched)
 rule 1 deny ip (0 times matched)
 rule 2 deny ip source 5.5.5.5 0 (0 times matched)
 rule 3 deny icmp source 3.3.3.3 0 destination 4.4.4.4 0 (0 times matched)
IDS_ACL Direction: OutBound
 rule 0 deny tcp source 1.1.1.1 0 source-port eq 1234 destination 2.2.2.2 0
destination-port eq 444 (0 times matched)
 rule 1 deny ip source 5.5.5.5 0 (0 times matched)
 rule 2 deny icmp source 3.3.3.3 0 destination 4.4.4.4 0 (0 times matched)
```

12.1.4 debugging ids-acl

【命令】

debugging ids

undo debugging ids

【视图】

用户视图

【参数】

无

【描述】

debugging ids 命令用来打开 IDS 联动功能的调试开关，**undo debugging ids** 命令用来关闭 IDS 联动功能的调试开关。

【举例】

打开 IDS 联动功能的调试开关。

```
<H3C> debugging ids
```

第13章 报文统计与日志配置命令

13.1 报文统计配置命令

13.1.1 display firewall statistic

【命令】

display firewall statistic { **system** | **zone** *zone-name* { **inzone** | **outzone** } | **ip** { *ip-address* { **source-ip** | **destination-ip** | **both** } | **which** } }

【视图】

所有视图

【参数】

system：显示防火墙系统的统计信息。

zone *zone-name*：显示安全区域的统计信息，*zone-name* 是安全区域名称。

ip *ip-address*：显示 IP 地址的统计信息，*ip-address* 为指定的 IP 地址。

inzone：指定安全区域的入方向的统计信息。

outzone：指定安全区域的出方向的统计信息。

source-ip：源地址表的统计信息。

destination-ip：目的地址表的统计信息。

which：显示 IP 地址。

【描述】

display firewall statistic 命令用来显示通过防火墙模块处理的系统统计信息，或者显示通过防火墙模块处理的基于指定安全区域的入/出方向统计信息，或者显示通过防火墙模块处理的某 IP 地址在源/目的地址表的统计信息。

【举例】

显示系统全局统计信息。

```
<H3C> display firewall statistic system
Firewall system statistic information:
       TotalBootCon,             787,  Total connection(s) since last reboot
        CurTotalCon,                   4,  Current total connection(s)
       MaxSessSpeed,                   9,  Peak session speed(num/s)
       CurSessSpeed,                   0,  Current session speed(num/s)
```

```
          CurTcpSess,                2,  Total current TCP session(s)
          CurUdpSess,                2,  Total current UDP session(s)
         CurIcmpSess,                0,  Total current ICMP session(s)
          CurFtpSess,                0,  Current FTP session(s)
         CurHttpSess,                0,  Current Http session(s)
         CurH323Sess,                0,  Current H.323 session(s)
         CurRtspSess,                0,  Current RTSP session(s)
         CurSmtpSess,                0,  Current SMTP session(s)
           CurFrgTbls                0,  Current frag table number
       CurTcpproxySess,              0,  Total current TCP-Proxy session(s)
          RcvSynPkts,              724,  TCP SYN packet(s) received
          RcvFinPkts,              929,  TCP FIN packet(s) received
       RcvSynAckPkts,              578,  TCP SYNACK packet(s) received
          RcvRstPkts,              358,  TCP RST packet(s) received
         RcvIcmpPkts,               10,  Received ICMP packet(s)
         RcvIcmpOcts,              840,  Received ICMP byte(s)
        PassIcmpPkts,               10,  Passed ICMP packet(s)
        PassIcmpOcts,              840,  Passed ICMP byte(s)
          RcvTcpPkts,            11732,  Received TCP packet(s)
          RcvTcpOcts,          3288722,  Received TCP byte(s)
         PassTcpPkts,            11729,  Passed TCP packet(s)
         PassTcpOcts,          3288578,  Passed TCP byte(s)
          RcvUdpPkts,             2675,  Received UDP packet(s)
          RcvUdpOcts,           225437,  Received UDP byte(s)
         PassUdpPkts,             2535,  Passed UDP packet(s)
         PassUdpOcts,           211363,  Passed UDP byte(s)
          RcvEtcPkts,                0,  Received Etc packet(s)
          RcvEtcOcts,                0,  Received Etc byte(s)
         PassEtcPkts,                0,  Passed Etc packet(s)
         PassEtcOcts,                0,  Passed Etc byte(s)
         RcvFragPkts,                0,  Received frag packet(s)
         RcvFragOcts,                0,  Received frag byte(s)
          RcvFtpPkts,                0,  Received FTP packet(s)
          RcvFtpOcts,                0,  Received FTP byte(s)
         RcvSmtpPkts,                0,  Received SMTP packet(s)
         RcvSmtpOcts,                0,  Received SMTP byte(s)
         RcvHttpPkts,             7934,  Received Http packet(s)
         RcvHttpOcts,          3096083,  Received Http byte(s)
         RcvH323Pkts,                0,  Received H.323 packet(s)
         RcvH323Octs,                0,  Received H.323 byte(s)
         RcvRtspPkts,                0,  Received RTSP packet(s)
         RcvRtspOcts,                0,  Received RTSP byte(s)
         BlsDscdPkts,                0,  Black list discard packet(s)
```

```
 BlsDscdOcts,                0,  Black list discard byte(s)
SessDscdPkts,              0,  Failed session table discard packet(s)
SessDscdOcts,              0,  Failed session table discard byte(s)
   TotalPkts,             14417,  Received Total packet(s)
   TotalOcts,           3514999,  Received Total byte(s)
```

📖 **说明：**

- 以上显示信息中的报文均是指通过防火墙检测的报文。
- **display firewall statistic** 命令显示的统计信息是指自统计功能使能后的统计信息，不包括统计功能使能前的信息。如 **display firewall statistic system** 命令中显示的 CurTotalCon 表示自系统统计功能使能后的系统连接数，与系统当前的 session 数可能不一致；**display firewall statistic zone trust inzone** 命令中显示的 CurTotalCon 表示自 trust 区域的入域统计功能使能后的该域的连接数。
- **display firewall statistic system** 命令中显示的收到的报文是指防火墙所有安全域出方向的报文总和，包括从本地域发出的报文；该命令中显示的通过的报文是指防火墙所有安全域入方向的报文总和，包括发往本地域的报文。

13.1.2 display firewall statistic system defend

【命令】

display firewall statistic system defend

【视图】

所有视图

【参数】

无

【描述】

display firewall statistic system defend 命令用来显示收到的各种类型攻击的报文数目或攻击次数。

【举例】

显示收到的各种类型攻击的报文数目或攻击次数。

```
<H3C> display firewall statistic system defend
  Display firewall defend statistic:
                      IP-spoofing,           0 time(s)
                             Land,           0 time(s)
                            Smurf,           0 time(s)
                          Fraggle,           0 time(s)
                          Winnuke,           0 time(s)
```

```
                          SYN-flood,           0 time(s)
                          UDP-flood,           0 time(s)
                         ICMP-flood,           0 time(s)
                       ICMP-redirect,          0 time(s)
                     ICMP-unreachable,         0 time(s)
                             IP-sweep,         0 time(s)
                   Source-route attack,        0 time(s)
                   Route-record attack,        0 time(s)
                              Tracert,         0 time(s)
                        Ping-of-death,         0 time(s)
                             Teardrop,         0 time(s)
                              Tcp-flag,        0 time(s)
                           IP-fragment,        0 time(s)
                            Large-icmp,        0 time(s)
    Too much Half Con of SYN Flood,            0 time(s)
                         ARP-spoofing,         0 time(s)
                            ARP-flood,         0 time(s)
                           Frag-flood,         0 time(s)
                         TCP port-scan,        0 time(s)
                         UDP port-scan,        0 time(s)
                          Other attack,        0 time(s)
                                 total,        0 time(s)
```

13.1.3 display firewall statistic system flow-percent

【命令】

display firewall statistic system flow-percent [**default**]

【视图】

所有视图

【参数】

default：报文流量百分比的缺省值。

【描述】

display firewall statistic system flow-percent 命令用来显示报文流量的百分比信息。

【举例】

显示报文流量百分比信息。

```
<H3C> display firewall statistic system flow-percent
```

```
Current tcp percent:   75
Current udp percent:   15
Current icmp percent:  5
Current alternation:   25
Current time interval: 60 minutes
```

13.1.4 firewall statistic system connect-number

【命令】

firewall statistic system connect-number { **tcp** | **udp** } **high** *high-value* **low** *low-value*

undo firewall statistic system connect-number { **tcp** | **udp** }

【视图】

系统视图

【参数】

tcp：TCP 连接。

udp：UDP 连接。

high *high-value*：上限阈值，基于系统的 TCP 和 UDP 连接的上限阈值范围为 1～500000，缺省值为 500000。

low *low-value*：下限阈值，基于系统的 TCP 和 UDP 连接的下限阈值范围为 1～500000，缺省值为 450000。

【描述】

firewall statistic system connect-number 命令用来设置基于系统的 TCP 连接和 UDP 连接总数的上限阈值和下限阈值。**undo firewall statistic system connect-number** 命令用来恢复缺省值。

基于系统的连接数阈值没有方向，指的是系统的总的连接数。当连接数大于上限阈值时，表明发生异常情况，输出日志告警；当连接数小于下限阈值时，表明系统恢复正常。

注意：**firewall statistic system connect-number** 命令在系统视图下使用，用于配置系统相关的阈值；**statistic connect-number** 命令在安全区域视图下使用，用于配置安全区域或 IP 地址相关的阈值。

【举例】

设置基于系统的 TCP 连接总数的上限阈值是 120000，下限阈值是 60000。

```
[H3C] firewall statistic system connect-number tcp high 120000 low 60000
```

13.1.5 firewall statistic system enable

【命令】

firewall statistic system enable

undo firewall statistic system enable

【视图】

系统视图

【参数】

无

【描述】

firewall statistic system enable 命令用来使能全局统计功能，**undo firewall statistic system enable** 命令用来禁止全局统计功能。

缺省情况下，使能全局统计功能。

【举例】

使能全局统计功能。

```
[H3C] firewall statistic system enable
```

13.1.6 firewall statistic system flow-percent

【命令】

firewall statistic system flow-percent tcp *tcp-percent* **udp** *udp-percent* **icmp** *icmp-percent* **alternation** *alternation-percent* [**time** *time-value*]

undo firewall statistic system flow-percent

【视图】

系统视图

【参数】

tcp-percent：TCP 报文所占的百分比比率，取值范围是 0～100，缺省值是 75。

udp-percent：UDP 报文所占的百分比比率，取值范围是 0～100，缺省值是 15。

icmp-percent：ICMP 报文所占的百分比比率，取值范围是 0～100，缺省值是 5。

alternation-percent：各种报文所允许的百分比的波动范围，取值范围是 0～25，缺省值是 25。

time-value：进行检测计算的时间周期（单位：分钟），取值范围是 0～6000，缺省值是 60 分钟。

【描述】

firewall statistic system flow-percent 命令用来设置不同类型的报文在正常情况下一定时间内所占的百分比以及允许的变动范围。**undo firewall statistic system flow-percent** 命令用来恢复缺省值。

如果某类型（TCP、UDP、ICMP 或其他）报文百分比超过配置的上限阈值（加波动范围）或低于配置的下限阈值（减波动范围），则系统输出日志告警。

TCP、UDP、ICMP 三种报文所占百分比需要同时被配置，并且三种报文所占百分比之和必须小于或等于 100%；如果 TCP、UDP、ICMP 三种报文百分比之和超过 100%，则命令不会生效。

此告警信息是基于系统当前的统计值，如果当前系统统计信息没有被清除，此告警信息会按照配置的时间间隔定时进行输出。

【举例】

配置 TCP、UDP、ICMP 和其它报文分别所占的百分比分别为 50、25、15，允许波动 10%。

```
[H3C] firewall statistic system flow-percent tcp 50 udp 25 icmp 15 alternation 10
```

13.1.7 firewall statistic warning-level drop

【命令】

firewall statistic warning-level drop

undo firewall statistic warning-level drop

【视图】

系统视图

【参数】

无。

【描述】

firewall statistic warning-level drop 命令用来设置防火墙连接数量和连接速率监控的告警级别为输出告警信息，并丢弃报文。

undo firewall statistic warning-level drop 命令用来设置防火墙连接数量和连接速率监控的告警级别为仅输出告警信息。

告警级别分为两种，一种为“告警”，是指当连接数量和连接速率超过设置的上限阈值时，仅输出告警信息；另一种为“丢弃”，是指当连接数量或连接速率超过设

置的上限阈值时，输出告警信息，并且丢弃后续报文。仅当连接数量或连接速率恢复到设置的下限阈值时，不再丢弃报文。

该命令仅对基于安全区域和 IP 的统计功能有效，对于系统统计功能无效。

缺省情况下，告警级别为仅输出告警信息。

相关配置命令可参考 **statistic connect-number ip**，**statistic connect-number zone**，**statistic connect-speed ip**，**statistic connect-speed zone**。

【举例】

设置告警级别为输出告警信息，并丢弃报文。

```
[H3C] firewall statistic warning-level drop
```

13.1.8 reset firewall statistic ip

【命令】

reset firewall statistic ip *ip-address* { **source-ip** | **destination-ip | both** }

【视图】

用户视图

【参数】

ip *ip-address*：清除指定 IP 地址的统计信息。

source-ip：清除源地址表表项。

destination-ip：清除目的地址表表项。

【描述】

reset firewall statistic ip 用来清除源/目的地址表中的统计数据。

如果指定的 IP 地址不存在，则命令无效果。

【举例】

清除指定 IP 地址 1.1.1.1 在源地址表中的统计信息。

```
<H3C> reset firewall statistic ip 1.1.1.1 source-ip
```

13.1.9 reset firewall statistic system

【命令】

reset firewall statistic system [**defend** | **current**]

【视图】

用户视图

【参数】

defend：清除攻击防范信息。

current：清除当前连接数。

【描述】

reset firewall statistic system 命令用来清除全局统计信息或全局攻击防范信息。

【举例】

清除全局统计信息。

```
<H3C> reset firewall statistic system
```

13.1.10 reset firewall statistic zone

【命令】

reset firewall statistic zone *zone-name* { **inzone** | **outzone** }

【视图】

用户视图

【参数】

zone *zone-name*：清除基于安全区域统计信息，*zone-name* 是指定安全区域的名称。

inzone：安全区域入方向。

outzone：安全区域出方向。

【描述】

reset firewall statistic zone 用来清除当前安全区域的入/出方向的统计数据。

如果指定的安全区域不存在，则命令无效果。

【举例】

清除 Trust 安全区域在出方向的统计信息。

```
<H3C> reset firewall statistic zone trust outzone
```

13.1.11 statistic connect-number ip

【命令】

statistic connect-number ip outzone { **tcp** | **udp** } **high** *high-limit* **low** *low-limit*

statistic connect-number id *id* **ip outzone** { **tcp** | **udp** } **high** *high-limit* **low** *low-limit* **acl-number** *acl-number*

undo statistic connect-number [**id** *id*] **ip outzone** { **tcp** | **udp** }

statistic connect-number ip inzone { **tcp** | **udp** } **high** *high-limit* **low** *low-limit*

undo statistic connect-number ip inzone { **tcp** | **udp** }

【视图】

安全区域视图

【参数】

id *id*：规则的编号，范围为 1～99。

ip：基于 IP 的阈值。

inzone：安全区域的入方向。

outzone：安全区域的出方向。

tcp：TCP 连接。

udp：UDP 连接。

high *high-value*：基于 IP 地址的 TCP 和 UDP 连接的上限阈值，范围为 1～500000，缺省值为 500000。

low *low-value*：基于 IP 地址的 TCP 和 UDP 连接的下限阈值，范围为 1～450000，缺省值为 450000。

acl-number *acl-number*：指定基本 ACL 的编号，范围为 2000～2999。通过指定 ACL 可以控制对哪些 IP 地址进行限制。

【描述】

statistic connect-number ip 命令用来设置基于 IP 地址的某一方向上发起的 TCP 连接和 UDP 连接总数的上限阈值和下限阈值。**undo statistic connect-number ip** 命令用来恢复缺省值。

基于 IP 地址的连接数阈值则要根据数据包流向相对安全区域的方向分别进行设置。当连接数量超过设定的阈值上限或恢复到阈值下限时，系统将根据 **firewall statistic warning-level** 命令的设置采取相应操作。

相关配置命令可参考 **firewall statistic warning-level**。

【举例】

设置向 Untrust 安全区域的入方向发起 TCP 连接总数的基于 IP 地址的上限阈值为 5000，下限阈值为 500。

```
[H3C-zone-untrust] statistic connect-number ip inzone tcp high 5000 low 500
```

13.1.12 statistic connect-number zone

【命令】

statistic connect-number zone { **inzone** | **outzone** } { **tcp** | **udp** } **high** *high-limit* **low** *low-limit*

undo statistic connect-number zone { **inzone** | **outzone** } { **tcp** | **udp** }

【视图】

安全区域视图

【参数】

zone：基于安全区域的阈值。

inzone：安全区域的入方向。

outzone：安全区域的出方向。

tcp：TCP 连接。

udp：UDP 连接。

high *high-value*：基于安全区域的TCP和UDP连接的上限阈值，范围为1～500000，缺省值为 500000。

low *low-value*：基于安全区域的 TCP 和 UDP 连接的下限阈值，范围为 1～500000，缺省值为 450000。

【描述】

statistic connect-number zone 命令用来设置基于安全区域的某一方向上发起的 TCP 连接和 UDP 连接总数的上限阈值和下限阈值。**undo statistic connect-number zone** 命令用来恢复缺省值。

基于安全区域的连接数阈值则要根据数据包流向相对安全区域的方向分别进行设置。当连接数超过设定的阈值上限或恢复到阈值下限时，系统将根据 **firewall statistic warning-level** 命令的设置采取相应操作。

相关配置命令可参考 **firewall statistic warning-level**。

【举例】

设置向 Untrust 安全区域的入方向发起 TCP 连接总数的基于安全区域的上限阈值为 25000，下限阈值为 10000。

```
[H3C-zone-untrust] statistic connect-number zone inzone tcp high 25000 low
10000
```

13.1.13 statistic connect-speed ip

【命令】

statistic connect-speed ip outzone { **tcp** | **udp** } **high** *high-limit* **low** *low-limit*

statistic connect-speed id *id* **ip outzone** { **tcp** | **udp** } **high** *high-limit* **low** *low-limit* **acl-number** *acl-number*

undo statistic connect-speed [**id** *id*] **ip outzone** { **tcp** | **udp** }

statistic connect-speed ip inzone { **tcp** | **udp** } **high** *high-limit* **low** *low-limit*

undo statistic connect-speed ip inzone { **tcp** | **udp** }

【视图】

安全区域视图

【参数】

id *id*：规则的编号，范围为 1～99。

ip：基于 IP 的阈值。

inzone：安全区域的入方向。

outzone：安全区域的出方向。

tcp：TCP 连接。

udp：UDP 连接。

high *high-value*：基于 IP 地址的 TCP 和 UDP 连接速率的上限阈值，范围为 1～10000，缺省值为 10000。

low *low-value*：基于 IP 地址的 TCP 和 UDP 连接速率的下限阈值，范围为 1～10000，缺省值为 9000。

acl-number *acl-number*：指定基本 ACL 的编号，范围为 2000～2999。通过指定 ACL 可以控制对哪些 IP 地址进行限制。

【描述】

statistic connect-speed ip 命令用来设置基于 IP 地址的某一方向上发起的 TCP 连接和 UDP 连接速率（每秒）的上限阈值和下限阈值。**undo statistic connect-speed ip** 命令用来恢复缺省值。

连接速率阈值是数据包相对安全区域的流向，基于 IP 地址来分别设定的。当连接速率超过设定的阈值上限或恢复到阈值下限时，系统将根据 **firewall statistic warning-level** 命令的设置采取相应操作。

相关配置命令可参考 **firewall statistic warning-level**。

【举例】

设置向 Untrust 安全区域的入方向发起 TCP 连接速率的基于 IP 地址的上限阈值为 5000，下限阈值为 500。

```
[H3C-zone-untrust] statistic connect-speed ip inzone tcp high 5000 low 500
```

13.1.14 statistic connect-speed zone

【命令】

statistic connect-speed zone { **inzone** | **outzone** } { **tcp** | **udp** } **high** *high-value* **low** *low-value*

undo statistic connect-speed zone { **inzone** | **outzone** } { **tcp** | **udp** }

【视图】

安全区域视图

【参数】

zone：基于安全区域的阈值。

inzone：安全区域的入方向。

outzone：安全区域的出方向。

tcp：TCP 连接。

udp：UDP 连接。

high *high-value*：基于安全区域的 TCP 和 UDP 连接速率的上限阈值，范围为 1～10000，缺省值为 10000。

low *low-value*：基于安全区域的 TCP 和 UDP 连接速率的下限阈值，范围为 1～10000，缺省值为 9000。

【描述】

statistic connect-speed zone 命令用来设置基于安全区域的某一方向上发起的 TCP 连接和 UDP 连接速率（每秒）的上限阈值和下限阈值。**undo statistic connect-speed zone** 命令用来恢复缺省值。

连接速率阈值是数据包相对安全区域的流向，基于安全区域来分别设定的。当连接速率超过设定的阈值上限或恢复到阈值下限时，系统将根据 **firewall statistic warning-level** 命令的设置采取相应操作。

相关配置命令可参考 **firewall statistic warning-level**。

【举例】

设置向 Trust 安全区域的入方向发起 TCP 连接速率（每秒）的基于安全区域的上限阈值为 2500，下限阈值为 1000。

```
[H3C-zone-trust] statistic connect-speed zone inzone tcp high 2500 low 1000
```

13.1.15 statistic enable

【命令】

statistic enable { **ip** | **zone** } { **inzone** | **outzone** }

undo statistic enable { **ip** | **zone** } { **inzone** | **outzone** }

【视图】

安全区域视图

【参数】

inzone：基于安全区域或基于 IP 统计入方向数据包，入方向数据包是指目的地址为本安全区域的数据包。如果基于 IP 进行统计，则数据包只根据目的地址进行统计。

outzone：基于安全区域或基于 IP 统计出方向数据包，出方向数据包是指源地址为本安全区域的数据包。如果基于 IP 进行统计，则数据包只根据源地址进行统计。

【描述】

statistic enable 命令用来使能基于安全区域和 IP 的统计功能，**undo statistic enable** 命令用来禁止基于安全区域和 IP 的统计功能。

缺省情况下，禁止基于安全区域和 IP 的统计功能。

【举例】

在 Trust 安全区域上配置基于 IP 地址的统计功能，对入安全区域方向数据包进行统计（只统计其目的地址）。

```
[H3C-zone-trust] statistic enable ip inzone
```

在 Untrust 安全区域上配置基于安全区域的统计功能，对出安全区域方向数据包进行统计。

```
[H3C-zone-trust] statistic enable zone outzone
```

13.2 SMTP 客户端配置命令

13.2.1 debugging smtpc

【命令】

debugging smtpc

undo debugging smtpc

【视图】

用户视图

【参数】

无

【描述】

debugging smtpc 命令用来打开 SMTP 客户端的调试开关，**undo debugging smtpc** 命令用来关闭 SMTP 客户端的调试开关。

缺省情况下，关闭 SMTP 客户端的调试开关。

【举例】

打开 SMTP 客户端的调试开关。

```
<H3C> debugging smtpc
```

13.2.2 display smtpc

【命令】

display smtpc [**administrator** | **trigger**]

【视图】

所有视图

【参数】

administrator：显示邮件收件人信息。

trigger：显示邮件触发时间信息。

【描述】

display smtpc 命令用来显示 SMTP 客户端的配置信息。

【举例】

显示邮件的收件人信息。

```
<H3C> display smtpc administrator
  The following mail address configured:
         administrator@secpath.com
         admin@ms.com
```

显示邮件触发时间信息。

```
<H3C> display smtpc trigger
```

```
The following trigger time configured:

        10:30   12:00   15:15   17:30
```

13.2.3 smtpc administrator mail

【命令】

smtpc administrator mail *mail-address*

undo smtpc administrator { **all** | **mail** *mail-address* }

【视图】

系统视图

【参数】

mail-address：邮件的收件人地址。

all：所有收件人地址。

【描述】

smtpc administrator mail 命令用来配置邮件的收件人地址，**undo smtpc administrator** 命令用来删除邮件的收件人地址。

添加的收件人地址必须符合 SMTP 邮件地址的格式。通过多次执行此命令，可以添加多个收件人地址，最多可配置 5 个。

缺省情况下，未配置邮件的收件人地址。

【举例】

添加邮件的收件人地址 administrator@secpath.com

```
[H3C] smtpc administrator mail administrator@secpath.com
```

13.2.4 smtpc trigger time

【命令】

smtpc trigger time *hh:mm*

undo smtpc trigger { **all** | **time** *hh:mm* }

【视图】

系统视图

【参数】

hh:mm：定时邮件的触发时间，范围为 00:00～23:59。

all：所有已配置的触发时间。

【描述】

smtpc trigger time 命令用来配置每日定时邮件的触发时间点，**undo smtpc trigger** 命令用来取消配置的邮件触发时间点。

通过多次执行此命令，可以添加多个触发时间点，最多可配置 5 个。

缺省情况下，未配置邮件的触发时间点。

【举例】

配置在 17:30 发送定时邮件。

```
[H3C] smtpc trigger time 17:30
```

13.3 DNS 客户端配置命令

13.3.1 debugging dnsc

【命令】

debugging dnsc

undo debugging dnsc

【视图】

用户视图

【参数】

无

【描述】

debugging dnsc 命令用来打开 DNS 客户端的调试开关，**undo debugging dnsc** 命令用来关闭 DNS 客户端的调试开关。

缺省情况下，关闭 DNS 客户端的调试开关。

【举例】

打开 DNS 客户端的调试开关。

```
<H3C> debugging dnsc
```

13.3.2 display dnsc

【命令】

display dnsc { **server** | **cache** }

【视图】

所有视图

【参数】

server：显示配置的 DNS 服务器。

cache：显示 DNS 缓存条目。

【描述】

display dnsc 命令用来显示 DNS 客户端的配置信息。

【举例】

显示配置的 DNS 服务器。

```
<H3C> display dnsc server
  10.1.1.1
  10.1.1.2
  10.1.1.3
  Total 3 dns server is configured.
```

13.3.3 dnsc server

【命令】

dnsc server ip *ip-address*

undo dnsc server { **all** | **ip** *ip-address* }

【视图】

系统视图

【参数】

ip *ip-address*：DNS 服务器的 IP 地址。

all：所有 DNS 服务器。

【描述】

dnsc server 命令用来配置 DNS 服务器，**undo dnsc server** 命令用来删除配置的 DNS 服务器。

缺省情况下，未配置 DNS 服务器。

【举例】

配置 DNS 服务器的 IP 地址为 10.1.1.3。

```
[H3C] dnsc server ip 10.1.1.3
```

13.3.4 dnsc cache

【命令】

dnsc cache add domain *domain-name* **type** { **a** | **mx** } **ip** *ip-address* **ttl** *ttl*

dnsc cache delete domain *domain-name* **type** { **a** | **mx** }

undo dnsc cache { **all** | **domain** *domain-name* **type** { **a** | **mx** } }

【视图】

系统视图

【参数】

add：添加 DNS 缓存条目。

delete：删除 DNS 缓存条目。

domain *domain-name*：域名，长度为 3～255 个字符。

type：缓存条目的类型。

a：主机（A）记录。

mx：邮件交换记录（Mail Exchange）。

ip *ip-address*：域名对应的 IP 地址。

ttl *ttl*：缓存条目的生存周期，范围为 0～3600，单位为分钟（m）。

all：所有缓存条目。

【描述】

dnsc cache add 命令用来添加 DNS 缓存条目，**dnsc cache delete** 命令和 **undo dnsc cache** 命令用来删除 DNS 缓存条目。

缺省情况下，未配置 DNS 缓存条目。

【举例】

添加类型为 MX 的缓存条目。

```
[H3C] dnsc cache add domain h3c.com type mx ip 1.1.1.1 ttl 600
```

13.4 日志配置命令

13.4.1 debugging flowlog

【命令】

debugging flowlog { **packet** | **error** | **event** | **all** }

undo debugging flowlog { **packet** | **error** | **event** | **all** }

【视图】

用户视图

【参数】

packet：流日志报文调试功能。

error：流日志错误调试功能。

event：流日志事件调试功能。

all：流日志所有调试功能。

【描述】

debugging flowlog 命令用来打开流日志的调试开关。

undo debugging flowlog 命令用来关闭流日志的调试开关。

缺省情况下，关闭流日志调试功能。

【举例】

打开流日志错误调试功能。

```
<H3C> debugging flowlog error
```

13.4.2 firewall binary-log host

【命令】

firewall binary-log host *ip-address* [*port-number*]

undo firewall binary-log host

【视图】

系统视图

【参数】

ip-address：二进制流日志主机的 IP 地址。

port-number：二进制流日志主机接收流日志所使用的端口号，范围为 0～65535，缺省为 9002。

【描述】

firewall binary-log host 命令用来设置二进制流日志主机的 IP 地址。

undo firewall binary-log host 命令用来取消二进制流日志主机的配置。

缺省情况下，未配置二进制流日志主机的 IP 地址。

【举例】

指定二进制流日志主机的 IP 地址和端口。

```
[H3C] firewall binary-log host 2.2.2.2 9023
```

13.4.3 firewall log-time

【命令】

firewall { **defend** | **statistic** | **http** | **ftp | snmp | smtp** } **log-time** *time*

undo firewall { **defend** | **statistic** | **http** | **ftp | snmp | smtp** } **log-time**

【视图】

系统视图

【参数】

defend：攻击防范信息。

statistic：流量统计信息。

http：HTTP 过滤信息。

ftp：FTP 过滤信息。

snmp：SNMP 过滤信息。

smtp：SMTP 过滤信息。

time：日志缓冲区的扫描时间，单位秒，范围 1～65535。

【描述】

firewall log-time 命令用来设置日志缓冲区的扫描时间。

undo firewall log-time 命令恢复日志缓冲区扫描时间的缺省值。

缺省情况下，日志缓冲区的扫描时间为 30 秒。

【举例】

设置攻击防范日志缓冲区的扫描时间为 100 秒。

```
[H3C] firewall defend log-time 100
```

13.4.4 firewall nat log-type

【命令】

firewall nat log-type { **syslog** | **binary** }

undo firewall nat log-type

【视图】

系统视图

【参数】

syslog：设置 NAT 流日志的日志格式为 syslog 格式。

binary：设置 NAT 流日志的日志格式为 binary 格式。

【描述】

firewall nat log-type 命令用来设置 NAT 流日志的日志格式。

undo firewall nat log-type 命令用来将 NAT 流日志的日志格式恢复为缺省值。

缺省情况下，NAT 流日志的日志格式为 syslog 格式。

【举例】

设置 NAT 流日志格式为 binary 格式。

```
[H3C] firewall nat log-type binary
```

13.4.5 firewall session log-threshold

【命令】

firewall session log-threshold { **time** *value* | **mega-byte** *value* | **mega-packet** *value* }

undo firewall session log-threshold { **time** | **mega-byte** | **mega-packet** }

【视图】

系统视图

【参数】

time *value*：指定防火墙流日志统计的时间阈值，单位为分钟，取值范围为 1～600。当某条流的生存时间到达此阈值时，将会对此流进行日志统计。

mega-byte *value*：指定防火墙流日志统计的字节数阈值，单位为 MByte，取值范围为 1～4095。当某条流所传输的字节数到达此阈值时，将会对此流进行日志统计。

mega-packet *value*：指定防火墙流日志统计的报文数阈值，单位为 MPacket，取值范围为 1～4095。当某条流所传输的报文数到达此阈值时，将会对此流进行日志统计。

【描述】

firewall session log-threshold 命令用来指定防火墙流日志统计的各项阈值。

undo firewall session log-threshold 命令用来将防火墙流日志统计的各项阈值恢复为缺省值。

对于同一条数据流，在达到任意一种类型的阈值时，系统就会对此流进行日志统计。

缺省情况下，防火墙流日志统计的时间阈值为 600 分钟，字节数阈值为 4095 MByte，报文数阈值为 4095 MPacket。

【举例】

设置流日志统计时间阈值为 10 分钟。

```
[H3C] firewall session log-threshold time 10
```

设置流日志统计字节数阈值为 10 Mbyte。

```
[H3C] firewall session log-threshold mega-byte 10
```

设置流日志统计报文数阈值为 1 Mpacket。

```
[H3C] firewall session log-threshold mega-packet 1
```

13.4.6 firewall session log-type

【命令】

firewall session log-type { **syslog** | **binary** }

undo firewall session log-type

【视图】

系统视图

【参数】

syslog：设置防火墙流日志的日志格式为 syslog 格式。

binary：设置防火墙流日志的日志格式为 binary 格式。

【描述】

firewall session log-type 命令用来指定防火墙流日志的日志格式。

undo firewall session log-type 命令用来恢复防火墙流日志格式为缺省值。

防火墙流日志暂时只支持以二进制格式发送。

缺省情况下，防火墙流日志的日志格式为 syslog 格式。

【举例】

指定防火墙流日志格式为二进制格式。

```
[H3C] firewall session log-type binary
```

13.4.7 session log enable

【命令】

session log enable [**acl-number** *acl-number*]

undo session log enable

【视图】

域间视图

【参数】

acl-number：通过指定基本访问控制列表或高级访问控制列表的编号，配置域间流日志收集规则，访问控制列表编号范围为 2000～3999。

【描述】

session log enable 命令用来在防火墙不同的安全区域间开启流日志功能。

undo session log enable 命令用来关闭安全区域间的流日志功能。

缺省情况下，关闭域间流日志功能。

【举例】

进入防火墙域间视图，并使能域间流日志功能。

```
[H3C] firewall interzone trust untrust
[H3C-interzone-trust-untrust] session log enable
```

13.4.8 reset firewall log-buf

【命令】

reset firewall log-buf { **session** | **defend** | **statistic** | **http** | **ftp | snmp | smtp** }

【视图】

用户视图

【参数】

session：清除 NAT/ASPF 流的日志缓冲区。

defend：清除攻击防范的日志缓冲区。

statistic：清除流量监控的日志缓冲区。

http：清除 HTTP 过滤信息。

ftp：清除 FTP 过滤信息。

snmp：清除 SNMP 过滤信息。

smtp：清除 SMTP 过滤信息。

【描述】

reset firewall log-buf 命令用来清除日志缓冲区的内容。

【举例】

清除 NAT/ASPF 流的日志缓冲区内容。

```
<H3C> reset firewall log-buf session
```

目 录

第 1 章 VRRP配置命令 1-1
1.1 VRRP配置命令 1-1
1.1.1 debugging vrrp 1-1
1.1.2 display vrrp 1-1
1.1.3 vrrp authentication-mode 1-2
1.1.4 vrrp ping-enable 1-3
1.1.5 vrrp un-check ttl 1-4
1.1.6 vrrp vrid preempt-mode 1-4
1.1.7 vrrp vrid priority 1-5
1.1.8 vrrp vrid timer advertise 1-6
1.1.9 vrrp vrid track 1-6
1.1.10 vrrp vrid virtual-ip 1-7
第 2 章 双机热备配置命令 2-1
2.1 双机热备配置命令 2-1
2.1.1 ad-interval 2-1
2.1.2 debugging rdmp 2-2
2.1.3 display rdo 2-3
2.1.4 display rdo *rdo-id* 2-4
2.1.5 display rdo sync-modules 2-6
2.1.6 ha-interface 2-7
2.1.7 priority 2-8
2.1.8 rdo 2-9
2.1.9 scp batch-sync 2-10
2.1.10 vif 2-11

第1章 VRRP 配置命令

1.1 VRRP 配置命令

1.1.1 debugging vrrp

【命令】

debugging vrrp { **packet** | **state** }

undo debugging vrrp { **packet** | **state** }

【视图】

用户视图

【参数】

packet：VRRP 报文调试功能。

state：VRRP 状态调试功能。

【描述】

debugging vrrp 命令用来使能 VRRP 的调试功能，**undo debugging vrrp** 命令用来禁止 VRRP 的调试功能。

缺省情况下，VRRP 的调试功能被禁止。

【举例】

使能 VRRP 的报文调试功能。

```
<H3C> debugging vrrp packet
```

1.1.2 display vrrp

【命令】

display vrrp [**interface** *type number* [*virtual-router-ID*]]

【视图】

所有视图

【参数】

interface *type number*：接口类型和接口号。

virtual-router-ID：备份组号。

【描述】

display vrrp 命令用来显示 VRRP 的状态信息。

可以查看当前 VRRP 的状态信息和配置参数。如果不指定接口和备份组号，则显示该防火墙上所有备份组的状态信息；如果只指定接口，则显示该接口上的所有备份组的状态信息；如果指定接口和备份组号，则显示该备份组的状态信息。

【举例】

显示防火墙上的全部备份组信息。

```
<H3C> display vrrp
Virtual Ip Ping : Disable
   Ethernet1/0/0 | Virtual Router 1
          state : Initialize
     Virtual IP : 22.2.2.2
Config Priority : 100
   Run Priority : 100
        Preempt : YES   Delay Time : 0
          Timer : 1
      Auth Type : NONE

   Ethernet2/0/0 | Virtual Router 1
          state : Initialize
     Virtual IP : 1.1.11.1
Config Priority : 100
   Run Priority : 100
        Preempt : YES   Delay Time : 0
          Timer : 1
      Auth Type : NONE
```

1.1.3 vrrp authentication-mode

【命令】

vrrp authentication-mode { **md5** *key* | **simple** *key* }

undo vrrp authentication-mode

【视图】

接口视图

【参数】

simple：表示进行明文字符认证。

md5：表示利用 MD5 算法进行密文认证。

key：认证字。当采用 **simple** 认证方式时，*key* 为明文验证字，长度为 1～8 个字符；当采用 **md5** 认证方式时，*key* 为 MD5 密文验证字，如果以明文形式输入，长度为 1～8 个字符，如：1234567；如果以密文形式输入，长度必须为 24，并且必须是密文形式，如：_(TT8F]Y\5SQ=^Q`MAF4<1!!。

【描述】

vrrp authentication-mode 命令用来设置 VRRP 备份组的认证方式和认证字。**undo vrrp authentication-mode** 命令用来取消 VRRP 备份组的认证。

缺省情况下，不进行认证。

这条命令是为一个接口上的所有 VRRP 备份组设置认证方式和认证字，这是由于协议规定一个接口上的备份组应当使用相同的认证方式和认证字。另外，加入同一备份组的成员也应该设置相同的认证方式和认证字。

认证方式和认证字的设置，认证字区分大小写。

【举例】

设置接口 Ethernet 1/0/0 上所有 VRRP 备份组的认证方式和认证字。

```
[H3C-Ethernet1/0/0] vrrp authentication-mode simple vrrppwd
```

1.1.4 vrrp ping-enable

【命令】

vrrp ping-enable

undo vrrp ping-enable

【视图】

系统视图

【参数】

无

【描述】

vrrp ping-enable 命令用来使备份组的虚拟 IP 地址可以被 ping 通，**undo vrrp ping-enable** 命令用来恢复为缺省情况，使备份组的虚拟 IP 地址不能被 ping 通。

缺省情况下，虚拟备份组的 IP 地址不能被 ping 通。

需要注意的是，本命令需要在配置备份组之前使用。在防火墙上创建了备份组之后，系统将不允许再使用本命令和命令的 **undo** 形式。

【举例】

使备份组的虚拟 IP 地址可以被 ping 通。

```
[H3C] vrrp ping-enable
```

1.1.5 vrrp un-check ttl

【命令】

vrrp un-check ttl

undo vrrp un-check ttl

【视图】

接口视图

【参数】

无

【描述】

vrrp un-check ttl 命令用来取消检查 VRRP 报文的 TTL 值。**undo vrrp un-check ttl** 命令用来恢复检查 VRRP 报文中的 TTL 值。

协议中规定 VRRP 报文的 TTL 值必须为 255，如果备份防火墙收到报文后，检查到 TTL 值不等于 255，就将其丢弃。

缺省情况下，需要检查 VRRP 报文的 TTL 值。

【举例】

取消检查 VRRP 报文的 TTL 值。

```
[H3C-Ethernet0/0/0] vrrp un-check ttl
```

1.1.6 vrrp vrid preempt-mode

【命令】

vrrp vrid *virtual-router-ID* **preempt-mode** [**timer delay** *delay-value*]

undo vrrp vrid *virtual-router-ID* **preempt-mode**

【视图】

接口视图

【参数】

virtual-router-ID：VRRP 备份组号，范围为 1～255。

delay-value：延迟时间，单位为秒，范围为 0～255。

【描述】

vrrp vrid preempt-mode 命令用来设置备份组中防火墙的抢占方式和延迟时间，**undo vrrp vrid preempt-mode** 命令用来取消备份组的抢占方式。

如果需要优先级高的防火墙能够主动的抢占成为 Master，就需要将这台防火墙设置为抢占方式。如果需要将抢占的时间延长，还可以设置延迟时间。当设置为不抢占时，延迟时间会自动被置为 0 秒。

缺省情况下，为抢占方式，延迟时间为 0 秒。

【举例】

设置抢占。

```
[H3C-Ethernet1/0/0] vrrp vrid 1 preempt-mode
```

设置抢占的延迟时间。

```
[H3C-Ethernet1/0/0] vrrp vrid 1 preempt-mode timer delay 5
```

设置不抢占。

```
[H3C-Ethernet1/0/0] undo vrrp vrid 1 preempt-mode
```

1.1.7 vrrp vrid priority

【命令】

vrrp vrid *virtual-router-ID* **priority** *priority-value*

undo vrrp vrid *virtual-router-ID* **priority**

【视图】

接口视图

【参数】

virtual-router-ID：VRRP 备份组号，范围为 1～255。

priority-value：优先级的值，可配置的范围最小值为 1，最大值为 254。

【描述】

vrrp vrid priority 命令用来设置防火墙在备份组中的优先级。**undo vrrp vrid priority** 命令用来将优先级恢复为缺省值。

优先级决定防火墙在备份组中的地位，优先级越高，越有可能成为 Master。优先级 0 是系统保留为特殊用途来使用的，255 则是系统保留给 IP 地址拥有者的。

缺省情况下，优先级为 100。

【举例】

设置防火墙在备份组 1 中的优先级为 150。

```
[H3C-Ethernet1/0/0] vrrp vrid 1 priority 150
```

1.1.8 vrrp vrid timer advertise

【命令】

vrrp vrid *virtual-router-ID* **timer advertise** *adver-interval*

undo vrrp vrid *virtual-router-ID* **timer advertise**

【视图】

接口视图

【参数】

virtual-router-ID：VRRP 备份组号，范围为 1～255。

adver-interval：备份组中的 Master 发送 VRRP 报文的间隔时间，单位为秒，取值范围从 1 到 255。

【描述】

vrrp vrid timer advertise 命令用来设置备份组的定时器。**undo vrrp vrid timer advertise** 命令用来恢复为缺省值。

用户可以通过这条命令来设置 Master 发送 VRRP 报文的间隔时间。

缺省情况下，定时器的值为 1 秒。

【举例】

设置备份组 1 的 Master 发送 VRRP 报文的间隔时间为 5 秒。

```
[H3C-Ethernet1/0/0] vrrp vrid 1 timer advertise 5
```

1.1.9 vrrp vrid track

【命令】

vrrp vrid *virtual-router-ID* **track** *interface-type interface-number* [**reduced** *priority-reduced*]

undo vrrp vrid *virtual-router-ID* **track** [*interface-type interface-number*]

【视图】

接口视图

【参数】

virtual-router-ID：VRRP 备份组号，范围为 1～255。

interface-type interface-number：被监视的接口类型及接口号。

priority-reduced：运行优先级降低的数额，范围为 1～255。

【描述】

vrrp vrid track 命令用来设置监视接口。**undo vrrp vrid track** 命令用来取消监视指定接口。

VRRP 的监视接口功能，更好的扩充了备份功能，即不仅在防火墙出现故障时提供备份功能，而且在某网络接口 DOWN 掉时，也可以实现备份功能。配置命令后，如果被监视接口 DOWN 掉，则防火墙的运行优先级就会降低，备份组内的其它成员的运行优先级就会变成最高的运行优先级，从而成为新的 Master，实现备份功能。当防火墙为 IP 地址拥有者时，不允许对其进行监视接口的配置。

缺省情况下，运行优先级降低的数额为 10。

【举例】

设置监视接口 Ethernet 0/0/0。

```
[H3C-Ethernet1/0/0] vrrp vrid 1 track Ethernet0/0/0 reduced 50
```

取消监视接口 Ethernet 0/0/0。

```
[H3C-Ethernet1/0/0] undo vrrp vrid 1 track Ethernet0/0/0
```

1.1.10 vrrp vrid virtual-ip

【命令】

vrrp vrid *virtual-router-ID* **virtual-ip** *virtual-address*

undo vrrp vrid *virtual-router-ID* **virtual-ip** *virtual-address*

【视图】

接口视图

【参数】

virtual-router-ID：VRRP 备份组号，范围为 1～255。

virtual-address：虚拟 IP 地址。

【描述】

vrrp vrid virtual-ip 命令用来创建一个备份组，并添加虚拟 IP 地址，**undo vrrp vrid** 命令用来删除备份组。

缺省情况下，系统无备份组。

用户可以通过这条命令来创建一个备份组，也可以向一个已经存在的备份组中添加虚拟 IP 地址，一个备份组最多可以添加 16 个虚拟 IP 地址。用户还可以通过 **undo vrrp vrid** *virtual-router-ID* 命令来删除一个已经存在的备份组，或者用 **undo vrrp vrid** *virtual-router-ID* **virtual-ip** *virtual-address* 命令删除备份组中的某个虚拟地址。如果备份组中的地址被删除完，则系统也会自动将这个备份组删除。

【举例】

创建一个备份组。

```
[H3C-Ethernet1/0/0] vrrp vrid 1 virtual-ip 10.10.10.10
```

向一个已经存在的备份组添加虚拟 IP 地址。

```
[H3C-Ethernet1/0/0] vrrp vrid 1 virtual-ip 10.10.10.11
```

删除一个虚拟 IP 地址。

```
[H3C-Ethernet1/0/0] undo vrrp vrid 1 virtual-ip 10.10.10.10
```

第2章 双机热备配置命令

2.1 双机热备配置命令

2.1.1 ad-interval

【命令】

ad-interval *time-value*

undo ad-interval

【视图】

RDO 视图

【参数】

time-value：通告时间间隔，单位为秒，取值范围为 1～255。

【描述】

ad-interval 命令用来指定 RDO 的通告时间间隔，**undo ad-interval** 命令用来恢复 RDO 的通告时间间隔为缺省值。

缺省情况下，RDO 的通告时间间隔为 3 秒。

- 一个 RDO 中的主设备会定期发送抑制报文，通知备份设备自己处于正常工作的状态，并且通告自己的优先级。
- 备份设备根据通告时间间隔确定收到抑制报文的超时时间，如果连续三次超时未收到抑制报文则认为 Master 已经出现故障，并进行状态切换。
- 本端和对端需设置相同的通告间隔。
- 由于不同型号产品的硬件性能差异，以及设备在实际应用中的业务量大小等因素，双机热备中的备机在批量备份与恢复过程中可能会不能及时处理主机发来的通告报文，从而导致主备设备无法达到稳定同步状态，发生主备频繁切换的异常现象，可以通过配置更大的通告时间间隔来避免此现象。建议用户配置的通告时间间隔大于或等于 3 秒，以防止上述问题发生。
- 当实际应用中存在较大流量或较多会话，或配置文件较大时，建议用户增加通告时间间隔，以保证双机热备功能正常运行。

【举例】

设置 RDO 1 的通告时间间隔为 5 秒。

```
[H3C] rdo 1
[H3C-rdo1] ad-interval 5
```

恢复 RDO 的通告时间间隔为缺省值。

```
[H3C] rdo 1
[H3C-rdo1] undo ad-interval
```

2.1.2 debugging rdmp

【命令】

debugging rdmp { **all** | **core** { **error** | **event** | **packet** | **all** } | **fwd** { **error** | **event** | **packet** | **all** } | **scp** *scp-id* { **batch** | **realtime** | **timing** | **event** | **all** } | **sync** { **aspf-backup** | **aspf-restore** | **cfg-backup** | **cfg-restore** | **nat-backup** | **nat-restore** | **all** } }

undo debugging rdmp { **all** | **core** { **error** | **event | packet** | **all** } | **fwd** { **error** | **event** | **packet** | **all** } | **scp** *scp-id* { **batch** | **realtime** | **timing** | **event** | **all** } | **sync** { **aspf-backup** | **aspf-restore** | **cfg-backup** | **cfg-restore** | **nat-backup** | **nat-restore** | **all** } }

【视图】

用户视图

【参数】

all：所有调试信息开关。

core：CORE 模块的调试信息开关。

error：错误调试信息开关。

event：事件调试信息开关。

packet：报文调试信息开关。

fwd：FWD 模块的调试信息开关。

scp：SCP 模块的调试信息开关。

scp-id：SCP 的 ID 号，取值范围为 1～2。

batch：批量备份调试信息开关。

realtime：实时备份调试信息开关。

timing：定时备份调试信息开关。

sync：SYNC 模块的调试信息开关。

aspf-backup：ASPF 的数据备份调试信息开关。

aspf-restore：ASPF 的数据恢复调试信息开关。

cfg-backup：配置命令的数据备份调试开关。

cfg-restore：配置命令的数据恢复调试开关。

nat-backup：NAT 的数据备份调试开关。

nat-restore：NAT 的数据恢复调试开关。

【描述】

debugging rdmp 命令用来打开双机热备的调试信息开关，**undo debugging rdmp** 命令用来关闭双机热备的调试信息开关。

缺省情况下，关闭双机热备的全部调试信息开关。

相关配置可参考命令 **display rdo**。

【举例】

打开双机热备的所有调试信息开关。

```
<H3C> debugging rdmp all
```

关闭双机热备 CORE 模块的的事件调试信息开关。

```
<H3C> undo debugging rdmp core event
```

2.1.3 display rdo

【命令】

display rdo

【视图】

任意视图

【参数】

无

【描述】

display rdo 命令用来显示双机热备所有 RDO 的全局信息，包括已使能的 RDO 的 ID 号、RDO 的状态、当前实时优先级、状态协商接口名、SCP 的使能状态和 SCP 的当前状态。

相关配置可参考命令 **rdo** *rdo-id*。

【举例】

显示 RDO 的全局信息。

```
<H3C> display rdo

ID  Status    Priority  HA Interface             Enable(SCP)  Status(SCP)
--------------------------------------------------------------------------
```

```
1    backup    90        Ethernet0/0/1              Yes          Sync(s4)
```

如上信息表示：RDO 1 已使能，RDO 1 的状态为备份状态，实时优先级为 90，状态协商接口为 Ethernet0/0/1，SCP 1 已使能，SCP 1 的当前状态为稳定同步状态。

表2-1 双机热备全局信息描述表

域名	描述
ID	RDO 的 ID 号
Status	RDO 的当前状态，包括 inactive、init、master、backup、bachsync
Priority	RDO 的实时优先级
HA Interface	状态协商接口，用来在互为主备的两台防火墙之间传输协商报文以及备份数据
Enable(SCP)	SCP 的使能状态
Status(SCP)	SCP 当前状态。 备机状态包括 Idle(s0)、WaitInsAck(s1)、WaitSyncAck(s2)、BatchSync(s3)、Sync(s4) 主机状态包括 Idle(m0)、WaitInsReq(m1)、WaitSyncReq(m2)、WaitSyncAck(m3)、BatchSync(m4)、Sync(m5)

2.1.4 display rdo *rdo-id*

【命令】

display rdo *rdo-id*

【视图】

任意视图

【参数】

rdo-id：RDO 的 ID 号，取值范围为 1～2。

【描述】

display rdo *rdo-id* 命令用来显示双机热备 RDO 的详细信息，包括 RDO 的当前状态、静态优先级、实时优先级、认证模式、虚拟接口、SCP 的使能状态、当前状态、状态上下文、模块上下文、同步模块列表等。

相关配置可参考命令 **rdo** *rdo-id*。

【举例】

显示 RDO 1 的详细信息。

```
<H3C> display rdo 1

RDO 1 information:
```

```
  Status: master
  Static priority: 100
  Runtime priority: 90
  HA interface: Ethernet0/0/1
  Advertisement interval: 3000 ms
  VIF 1
    Interface: Ethernet0/0/0
    Virtual IP: 192.168.0.80
    Virtual MAC: 005e-0000-1101
    Reduced value: 10

SCP Instance information:
  ID: 1, Enable: Yes, Master: Yes, Current State: WaitInsReq(m1), Flags: 0
  Fsm Context:
    BatchSync Group: 0
    Batch Backup one turn: 0
    Batch Sent one turn: 0
    Data Count of Retrans Buffer: 0
    Current Data Identifer: 0
  Module Context:
    Data Count of Sync Queue: 0
    Realtime Data Buffer Length: 0
    Current BatchBackup Module: NONE
```

如上信息表示：RDO 1 的当前状态为主状态，静态优先级为 100，实时优先级为 90，状态协商接口为 Ethernet0/0/1，通告时间间隔为 3000ms，虚拟接口 1 绑定在接口 Ethernet0/0/0 上，虚拟 IP 地址为 192.168.0.80，虚拟 MAC 地址为 005e-0000-1101，权值为 10；SCP 1 已使能，协商为 Master，当前状态为稳定同步状态等。

表2-2 双机热备 RDO 信息描述表

域名	描述
Status	RDO 的当前状态，包括 inactive、init、master、backup、bachsync
Static priority	RDO 的静态优先级，指设备接口全部 UP 的状态下 RDO 的优先级。
Runtime Priority	RDO 的实时优先级，指根据静态优先级与设备接口状态计算得出的优先级，在主备协商中实时优先级高的设备为主。
HA Interface	状态协商接口，用来在互为主备的两台防火墙之间传输协商报文以及备份数据
Advertisement interval	通告时间间隔，指主机发送抑制报文的时间间隔
VIF	虚拟接口
Interface	虚拟接口绑定的实际接口

域名	描述
Virtual IP	虚拟 IP 地址
Virtual MAC	虚拟 MAC 地址
Reduce value	权值，用于动态更新实时优先级
ID	SCP 的 ID 号
Enable	SCP 是否已使能
Master	SCP 是否协商为主
Current State	SCP 的当前状态 备机包括 Idle(s0)、WaitInsAck(s1)、WaitSyncAck(s2)、BatchSync(s3)、Sync(s4) 主机包括 Idle(m0)、WaitInsReq(m1)、WaitSyncReq(m2)、WaitSyncAck(m3)、BatchSync(m4)、Sync(m5)
Flags	调试信息开关标志，0 为关闭，1 为开启
BatchSync Group	批量同步组
Batch Backup one turn	批量备份数目
Batch Sent one turn	批量发送数目
Data Count of Retrans Buffer	重传缓存中数据数目
Current Data Identifer	当前数据标号
Data Count of Sync Queue	同步队列中数据数目
Realtime Data Buffer Length	实时数据缓冲长度
Current BatchBackup Module	当前批量备份模块

2.1.5 display rdo sync-modules

【命令】

display rdo sync-modules

【视图】

任意视图

【参数】

无

【描述】

display rdo sync-modules 命令用来显示双机热备同步模块的信息，包括各同步模块的优先级与组标志。

【举例】

显示双机热备同步模块的信息。

```
<H3C> display rdo sync-modules
Sync module list:
    CFGT: Priority:  80, Group: 22020096
    BLST: Priority:  60, Group: 235339776
    SESS: Priority:  60, Group: 235339776
    ASPF: Priority:  50, Group: 235339776
    NATT: Priority:  50, Group: 34078720
  End
```

如上信息表示：双机热备的同步模块包括配置模块、防火墙黑名单模块、防火墙会话表模块、ASPF 模块和 NAT 模块以及各同步模块的优先级和组标志。

表2-3 双机热备同步模块信息描述表

域名	描述
Sync module list	同步模块列表，显示已注册的同步模块信息
Priority	同步模块优先级，优先级高的模块在批量备份时先备份
Group	同步模块组标志，表示同步模块的组 ID 号

2.1.6 ha-interface

【命令】

ha-interface interface *interface-name* [**peer-mac** *mac-address*]

undo ha-interface

【视图】

RDO 视图

【参数】

interface *interface-name*：指定本端的 HA 接口。

peer-mac *mac-address*：对端 HA 接口的 MAC 地址。

【描述】

ha-interface 命令用来配置本端的 HA 接口和对端 HA 接口的 MAC 地址，**undo ha-interface** 命令用来删除 HA 接口配置。

缺省情况下，未配置本端 HA 接口。

当配置了本端 HA 接口，但未使用 **peer-mac** 参数指定对端 HA 接口的 MAC 地址时，缺省为广播 MAC 地址 FFFF-FFFF-FFFF。

双机热备的协商报文和业务同步数据都使用 HA 接口进行传输，这些报文不同于普通报文，因此防火墙的防火墙模块（如黑名单、包过滤等）对这些报文不起作用。

HA 接口必须为物理接口。

如果 HA 接口的物理状态为 DOWN 时，RDO 状态在设备重新启动后会停止在 Init 状态。因此，请在双机热备环境中，始终保持 HA 接口的物理状态为 UP。

如果 HA 接口的物理状态为 DOWN 时，会导致主备设备的状态都为 Master，这时两台设备都将响应 ARP 报文，进行数据转发，导致业务不能正常运行。因此，请在双机热备环境中，始终保持 HA 接口的物理状态为 UP。

HA 接口不能与实际的业务接口复用。

主备设备间的 HA 接口需使用线缆直接相连。

【举例】

配置 Ethernet 0/0/0 为本端 HA 接口，并指定对端 HA 接口的 MAC 地址。

```
[H3C] rdo 1
[H3C-rdo1] ha-interface interface Ethernet 0/0/0 peer-mac 0001-0001-0001
```

2.1.7 priority

【命令】

priority *value*

undo priority

【视图】

RDO 视图

【参数】

value：RDO 的静态优先级，指设备接口全部 UP 的状态下 RDO 的优先级，取值范围为 1～255。

【描述】

priority 命令用来配置 RDO 的静态优先级，**undo priority** 命令用来将 RDO 的静态优先级恢复为缺省值。

缺省情况下，RDO 的静态优先级为 100。

系统根据静态优先级、接口状态与权值计算出 RDO 的实时优先级。在状态协商过程中，实时优先级数值高的为主设备。实时优先级的计算公式为：

RDO 的实时优先级 = RDO 静态优先级 – 所有 DOWN 状态的 VIF 的权值。

若本端和对端的实时优先级相等，则根据双方 HA 接口的 MAC 地址确定主备关系，MAC 地址大的为 Master。

【举例】

设置 RDO 1 的静态优先级为 150。

```
[H3C] rdo 1
[H3C-rdo1] priority 150
```

恢复 RDO 1 的静态优先级为缺省值。

```
[H3C] rdo 1
[H3C-rdo1] undo priority
```

2.1.8 rdo

【命令】

rdo *rdo-id*

undo rdo *rdo-id*

【视图】

系统视图

【参数】

rdo-id：RDO 的 ID 号，取值范围为 1～2。

【描述】

rdo 命令用来创建指定 ID 号的 RDO 或进入指定 RDO 视图，**undo rdo** 命令用来删除指定的 RDO。

缺省情况下，未创建任何 RDO。

在 RDO 视图下可以配置本端 HA 接口、RDO 的通告时间间隔、静态优先级、虚拟接口等配置参数。

⚠ 注意：

- 不能删除正在批量备份的 RDO。
- 当防火墙工作在网桥模式下时，如果配置了 RDO，请将 RDO 的相关命令配置完整（如虚拟接口、本端 HA 接口），否则防火墙将不能转发数据。

【举例】

创建 RDO 1，并进入 RDO 视图。

```
[H3C] rdo 1
[H3C-rdo1]
```

删除 RDO 1。

```
[H3C] undo rdo 1
```

2.1.9 scp batch-sync

【命令】

scp batch-sync { **all** | **config** }

【视图】

系统视图

【参数】

all：手动批量备份配置命令和动态备份信息。

config：只手动批量备份配置命令。

【描述】

scp batch-sync 命令用来手动批量备份配置命令和动态备份信息。

- 当两台互为主备的设备的所有 RDO 都处于稳定同步状态时，可以在配置主设备上使用此命令实现从 Master 向 Backup 的批量备份。所谓配置主设备，就是指用户配置的第一个主状态的 RDO 所在的设备。
- 使用 **scp batch-sync all** 命令批量备份的内容与设备重新启动时自动批量备份的内容相同，包括配置命令和动态备份信息。
- 使用 **scp batch-sync config** 命令则仅批量备份配置命令。

需要注意的是：

- **scp batch-sync config** 命令只能使用在没有数据业务、仅需要同步配置的情况；

- 在有数据业务的情况下，同步配置命令会清除备机的状态信息，如果此时需要同步配置，应该执行 **scp batch-sync all** 命令。

【举例】

手动批量备份配置命令。

```
[H3C] scp batch-sync config
```

手动批量备份配置命令与动态备份信息。

```
[H3C] scp batch-sync all
```

2.1.10 vif

【命令】

vif *vif-id* **interface** *type number* **virtual-ip** *ip-address* [**virtual-mac** *mac-address*] [**reduce** *value-reduced*]

vif *vif-id* **interface** *type number* [**reduce** *value-reduced*]

undo vif *vif-id*

【视图】

RDO 视图

【参数】

vif-id：虚拟接口的序号，取值范围为 1～128。

type number：虚拟接口所绑定的实际物理接口或 Bridge-template 接口。

ip-address：虚拟接口的虚拟 IP 地址。

mac-address：虚拟接口的虚拟 MAC 地址。

value-reduced：权值，不能大于静态优先级，取值范围为 1～254，缺省值为 10。

【描述】

vif 命令用来配置虚拟接口，**undo vif** 命令用来删除虚拟接口。

缺省情况下，未创建虚拟接口。

- VIF 是虚拟设备中处理业务数据的实体，它绑定的接口的状态会直接影响到设备 RDO 的状态。每个 RDO 和真实设备一样拥有多个虚拟接口（VIF）用来处理业务，必须为每个虚拟接口指定其对应的真实的接口。
- 两个互为主备的防火墙监视的接口所对应的虚拟接口 ID 必须相同，该虚拟接口的虚拟 IP 地址与虚拟 MAC 地址也必须相同。
- 虚拟 IP 地址必须与虚拟接口所绑定的接口的真实 IP 地址在同一网段，且为合法的单播地址，不能与虚拟接口所绑定的接口的真实 IP 地址相同。

- 虚拟 MAC 地址的默认格式为：00-5e-00-00-{ rdo-id :0001}-{ vif-id }。其中 rdo-id 为当前 RDO 的 ID 号，占高 4 位；vif-id 为当前虚拟接口的 ID 号。例如 RDO 1 的 VIF1 的默认虚拟 MAC 地址为 00-5e-00-00-11-01。虚拟 MAC 地址不能与绑定的接口的真实 MAC 地址相同。
- 权值用于动态更新实时优先级，不能大于静态优先级，并且一个 RDO 下每个绑定接口的权值总和不能大于或等于对应 RDO 的静态优先级。RDO 的实时优先级 = RDO 静态优先级 – 所有 DOWN 状态的 VIF 的权值。
- 工作在路由模式的双机热备使用 **vif** 命令的第一条命令，必须配置虚拟 IP 地址。
- 工作在网桥模式的双机热备使用 **vif** 命令的第二条命令，不能配置虚拟 IP 地址和虚拟 MAC 地址。
- 在批量备份过程中不要删除虚拟接口。
- 在指定虚拟接口已配置的情况下，必须先删除该虚拟接口再重新配置。
- 一个 RDO 的多个虚拟接口不能重复绑定在同一个接口上。

【举例】

设置互为主备的两台防火墙 RDO 1 的虚拟接口 1。

```
[H3C1] rdo 1
[H3C1-rdo1] vif 1 interface Ethernet 0/0/1 virtual-ip 192.16.0.1 virtual-mac
00-5e-00-00-11-22
[H3C2] rdo 1
[H3C2-rdo1] vif 1 interface Ethernet 0/0/1 virtual-ip 192.16.0.1 virtual-mac
00-5e-00-00-11-22
```

目 录

第 1 章 流量监管和流量整形配置命令 1-1
1.1 流量监管配置命令 1-1
1.1.1 display qos car interface 1-1
1.1.2 display qos carl 1-2
1.1.3 qos car 1-2
1.1.4 qos carl 1-4
1.2 流量整形配置命令 1-5
1.2.1 display qos gts interface 1-5
1.2.2 qos gts 1-5
1.3 物理接口限速配置命令 1-6
1.3.1 display qos lr interface 1-6
1.3.2 qos lr 1-7
第 2 章 拥塞管理配置命令 2-1
2.1 FIFO队列配置命令 2-1
2.1.1 qos fifo queue-length 2-1
2.2 优先队列配置命令 2-1
2.2.1 display qos pq interface 2-1
2.2.2 display qos pql 2-2
2.2.3 qos pq 2-3
2.2.4 qos pql default-queue 2-3
2.2.5 qos pql inbound-interface 2-4
2.2.6 qos pql protocol 2-5
2.2.7 qos pql queue 2-6
2.3 定制队列配置命令 2-7
2.3.1 display qos cq interface 2-7
2.3.2 display qos cql 2-8
2.3.3 qos cq 2-8
2.3.4 qos cql default-queue 2-9
2.3.5 qos cql inbound-interface 2-10
2.3.6 qos cql protocol 2-10
2.3.7 qos cql queue 2-12
2.3.8 qos cql queue serving 2-12
2.4 加权公平队列配置命令 2-13
2.4.1 display qos wfq interface 2-13
2.4.2 qos wfq 2-14
2.5 基于类的队列配置命令 2-14
2.5.1 car 2-14
2.5.2 classifier behavior 2-16
2.5.3 debugging qos cbq 2-16

2.5.4 display qos cbq interface 2-17
2.5.5 display qos policy 2-17
2.5.6 display qos policy interface 2-19
2.5.7 display traffic behavior 2-21
2.5.8 display traffic classifier 2-22
2.5.9 gts 2-22
2.5.10 if-match { destination-mac | source-mac } 2-23
2.5.11 if-match acl 2-24
2.5.12 if-match any 2-24
2.5.13 if-match classifier 2-25
2.5.14 if-match dscp 2-26
2.5.15 if-match inbound-interface 2-27
2.5.16 if-match ip-precedence 2-28
2.5.17 if-match protocol 2-29
2.5.18 if-match rtp 2-29
2.5.19 qos apply policy 2-30
2.5.20 qos max-bandwidth 2-31
2.5.21 qos policy 2-31
2.5.22 queue af 2-32
2.5.23 queue ef 2-33
2.5.24 queue wfq 2-34
2.5.25 queue-length 2-34
2.5.26 remark dscp 2-35
2.5.27 remark ip-precedence 2-37
2.5.28 traffic behavior 2-37
2.5.29 traffic classifier 2-38
2.5.30 wred 2-39
2.5.31 wred dscp 2-39
2.5.32 wred ip-precedence 2-41
2.5.33 wred weighting-constant 2-42
2.6 实时传输协议队列的配置命令 2-42
2.6.1 display qos rtpq interface 2-42
2.6.2 qos reserved-bandwidth 2-43
2.6.3 qos rtpq 2-44
第 3 章 DAR配置命令 3-1
3.1 DAR配置命令 3-1
3.1.1 dar max-session-count 3-1
3.1.2 dar protocol 3-1
3.1.3 dar protocol-rename 3-2
3.1.4 dar protocol-statistic 3-3
3.1.5 debugging dar 3-4
3.1.6 display dar information 3-4
3.1.7 display dar protocol 3-5
3.1.8 display dar protocol-rename 3-7
3.1.9 display dar protocol-statistic 3-8

3.1.10 if-match protocol 3-9
3.1.11 if-match protocol http 3-10
3.1.12 if-match protocol rtp 3-10
3.1.13 reset dar protocol-statistic 3-11
3.1.14 reset dar session 3-12
第 4 章 WRED配置命令 4-1
4.1 WRED配置命令 4-1
4.1.1 display qos wred interface 4-1
4.1.2 qos wred 4-2
4.1.3 qos wred dscp 4-2
4.1.4 qos wred ip-precedence 4-3
4.1.5 qos wred weighting-constant 4-4
第 5 章 MPLS QoS配置命令 5-1
5.1 MPLS QoS配置命令 5-1
5.1.1 if-match mpls-exp 5-1
5.1.2 qos cql protocol mpls exp 5-1
5.1.3 qos pql protocol mpls exp 5-2
5.1.4 remark mpls-exp 5-3

第1章 流量监管和流量整形配置命令

1.1 流量监管配置命令

1.1.1 display qos car interface

【命令】

display qos car interface [*interface-type interface-number*]

【视图】

所有视图

【参数】

interface-type：接口类型。

interface-number：接口编号。

【描述】

display qos car interface 命令用来显示 CAR 在指定接口上的参数设置情况和运行统计信息。

如不指定接口，将显示所有接口的 CAR 参数设置情况和运行统计信息。

【举例】

显示 CAR 在各接口上的参数设置情况和运行统计信息。

```
[H3C] display qos car interface
Interface: Ethernet1/0/0
Direction: Inbound
Rule(s): If-match  CARL   1
CIR  8000(bps),   CBS  15000(bit),  EBS  0(bit)
Conform Action:  remark ip-precedence 3 and pass
Exceed Action:   remark ip-precedence 4 and continue
Conformed:     0/0 (Packets/Bytes)
Exceeded:  0/0 (Packets/Bytes)
Direction: Outbound
Rule(s): If-match ACL   2001
CIR  8000(bps),   CBS  15000(bit),  EBS  0(bit)
Conform Action: pass
Exceed Action:  discard
Conformed:     0/0(Packets/Bytes)
```

```
Exceeded:       0/0(Packets/Bytes)
```

1.1.2 display qos carl

【命令】

display qos carl [*carl-index*]

【视图】

所有视图

【参数】

carl-index：CAR 列表的号码，取值范围为 1～199。

【描述】

display qos carl 命令用来显示 CAR 列表的某条规则或所有规则。

如不指定 *carl-index*，将显示所有的 CAR 列表的规则。

【举例】

显示列表号为 1 的 CAR 规则。

```
[H3C] display qos carl 1
Current CARL Configuration:
List  Params
-------------------------------------------------------
1     Precedence 1 2
```

1.1.3 qos car

【命令】

qos car { **inbound** | **outbound** } { **any** | **acl** *acl-number* | **carl** *carl-index* } **cir** *committed-information-rate* **cbs** *committed-burst-size* **ebs** *excess-burst-size* **green** *action* **red** *action*

undo qos car { **inbound** | **outbound** } { **any** | **acl** *acl-number* | **carl** *carl-index* } **cir** *committed-information-rate* **cbs** *committed-burst-size* **ebs** *excess-burst-size*

【视图】

接口视图

【参数】

inbound：对接口接收到的数据包进行限速。

outbound：对接口发送的数据包进行限速。

any：对所有的 IP 数据包进行限速。

acl *acl-number*：对匹配访问控制列表（ACL）的数据包进行限速。*acl- number* 为访问控制列表编号，取值范围 2000～3999。

carl *carl-index*：对匹配 CAR 列表的数据包进行限速。*carl-index* 为承诺访问速率列表编号，取值范围 1～199。

cir *committed-information-rate*：承诺信息速率，取值范围是 8000～155000000bps。CIR 不能超过 CBS×20。

cbs *committed-burst-size*：承诺突发尺寸，实际平均速率在承诺速率以内时的突发流量，取值范围为 15000～155000000bit。

ebs *excess-burst-size*：超出突发尺寸，取值范围为 0～155000000bit。

green：数据流量符合承诺速率时对数据包采取的动作。

red：数据流量不符合承诺速率时对数据包采取的动作。

action：对数据包采取的动作，有以下几种：

- **continue**：继续由下一个 CAR 策略处理。
- **discard**：丢弃数据包。
- **pass**：发送数据包。
- **remark-prec-continue** *new-precedence*：设置新的 IP 优先级 *new-precedence*，并继续由下一个 CAR 策略处理，取值范围 0～7。
- **remark-prec-pass** *new-precedence*：设置新的 IP 优先级 *new-precedence*，并发送数据包到目的地址，取值范围 0～7。
- **remark-mpls-exp-continue** *new-mpls-exp*：设置新的 MPLS EXP 值 *new-mpls-exp*，并继续由下一个 CAR 策略处理，取值范围 0～7。
- **remark-mpls-exp-pass** *new-mpls-exp*：设置新的 MPLS EXP 值 *new-mpls-exp*，并发送数据包到目的地址，取值范围 0～7。

【描述】

qos car 命令用来在某个接口实施 CAR 策略，**undo qos car** 命令用来删除接口上的某个 CAR 策略。

该命令只对 IP 数据包进行处理，对其它的数据包不进行处理。

该命令的重复执行将在接口上配置多个 CAR 策略，策略的执行顺序与配置的先后顺序一致。

【举例】

在接口 Ethernet1/0/0 的出方向上对满足 CARL 规则 1 的报文进行流量监管。报文正常流量为 38400bps，在第一时间可以有 2 倍于正常流量的突发流量通过，以后速率小于等于 38400bit 时正常发送，大于 38400bit 时，报文优先级改为 0 并发送。

```
[H3C-Ethernet1/0/0] qos car outbound carl 1 cir 38400 cbs 76800 ebs 0 green
pass red remark-prec-pass 0
```

1.1.4 qos carl

【命令】

qos carl *carl-index* { **precedence** *precedence-value* | **dscp** *dscp-value* | **mac** *mac-address* }

undo qos carl *carl-index*

【视图】

系统视图

【参数】

carl：承诺访问速率列表。

carl-index：CAR 列表号码，取值范围为 1～199。

precedencee-value：优先级，取值范围为 0～7。

dscp-value：DSCP 的值，取值范围为 0-63。

mac-address：16 进制的 MAC 地址。对于 **car inbound** 来说是源 MAC 地址，对于 **car outbound** 来说是目的 MAC 地址。

【描述】

qos carl 命令用来创建或修改 CAR 自身的规则列表，**undo qos carl** 命令用来删除 CAR 列表。

可以选择基于优先级或基于 MAC 地址建立 CAR 列表。

对于不同的 *carl-index*，该命令的重复执行将创建多个 CAR 列表，对于同一个 *carl-index*，该命令的重复执行将修改 CAR 列表的参数。

可以配置多个 **precedence** 值，最多可指定 8 个；如果指定了多个相同的 **precedence** 值，系统默认为一个；多个不同的 **precedence** 值是或的关系。

【举例】

下面的命令将配置 CAR 规则 1 为报文优先级 1 和 7。

```
[H3C] qos carl 1 precedence 1 7
```

1.2 流量整形配置命令

1.2.1 display qos gts interface

【命令】

display qos gts interface [*interface-type interface-number*]

【视图】

所有视图

【参数】

interface-type：接口类型。

interface-number：接口号。

【描述】

display qos gts interface 命令用来显示某个接口或所有接口的 TS 配置情况和统计信息。

如不指定接口，将显示所有接口的 TS 配置情况和运行统计信息。

【举例】

显示所有接口的 TS 配置情况和统计信息。

```
[H3C] display qos gts interface
Interface: Ethernet1/0/0
  Rule(s): If-match Any
 CIR 64000 (bps), CBS 32000 (bit), EBS 0 (bit)
 Queue Length: 50 (Packet)
 Queue Size  : 13 (Packet)
 Passed   : 723/979860 (Packets/Bytes)
 Discarded: 0/0 (Packets/Bytes)
 Delayed  : 723/979860 (Packets/Bytes)
```

1.2.2 qos gts

【命令】

qos gts { **any** | **acl** *acl-number* } **cir** *committed-information-rate* [**cbs** *committed-burst-size* [**ebs** *excess-burst-size* [**queue-length** *queue-length*]]]

undo qos gts { **any** | **acl** *acl-number* }

【视图】

接口视图

【参数】

any：对所有的 IP 数据包进行流量整形。

acl *acl-number*：对匹配访问控制列表 ACL 的数据包进行流量整形。*acl-number* 为访问控制列表编号，取值范围 2000～3999。

cir *committed-information-rate*：承诺信息速率，取值范围为 8000～155000000bps。

cbs *committed-burst-size*：承诺突发尺寸，取值范围为 15000～155000000bit。当 CIR 小于 30000 时，缺省值为 15000；当 CIR 大于 30000 时，缺省值为 CIR/2。

ebs *excess-burst-size*：超出突发尺寸，取值范围为 0～155000000bit，缺省取值为 0，即只采用一个令牌桶监管。

queue-length *queue-length*：缓存队列的最大长度，取值范围为 1～1024，缺省取值为 50。

【描述】

qos gts 命令用来为某一类别的流或所有流设置整形参数，并开始整形，**undo qos gts** 命令用来取消对某一类流或所有流的整形设置。

qos gts acl 用来为符合某一 ACL 的流设置整形参数，使用不同的 ACL 可以为不同的流设置整形参数。

qos gts any 用来为所有的流设置整形参数。

qos gts 命令的重复使用将替代原先的设置。

qos gts acl 不能和 **qos gts any** 同时使用。

【举例】

下面的命令将在接口 Ethernet1/0/0 上对满足 ACL 规则 2001 的报文进行流量整形。正常流量为 38400bps，在第一时间可以有 2 倍于正常流量的突发流量通过，以后速率小于等于 38400bps 的流量时正常发送，速率大于 38400bps 时，将进入队列缓存，缓存队列长度为 100。

```
[H3C-Ethernet1/0/0] qos gts acl 2001 cir 38400 cbs 76800 ebs 0 queue-length
100
```

1.3 物理接口限速配置命令

1.3.1 display qos lr interface

【命令】

display qos lr interface [*interface-type interface-number*]

【视图】

所有视图

【参数】

interface-type：接口类型。

interface-number：接口号。

【描述】

display qos lr interface 命令用来显示接口的 LR 配置情况和统计信息。

如不指定接口，将显示所有接口的 LR 配置情况和运行统计信息。

【举例】

显示所有接口的 LR 配置情况和统计信息。

```
[H3C] display qos lr interface
Interface: Ethernet1/0/0
CIR  8000 (bps),   CBS  15000 (bit),   EBS  0 (bit)
Pass:  0/0 (Packets/Bytes)
Delay    :  0/0 (Packets/Bytes)
Active Shaping   :  NO
```

1.3.2 qos lr

【命令】

qos lr cir *committed-information-rate* [**cbs** *committed-burst-size* [**ebs** *excess-burst-size*]]

undo qos lr

【视图】

接口视图

【参数】

cir *committed-information-rate*：承诺信息速率，取值范围为 8000～155000000bps。

cbs *committed-burst-size*：承诺突发尺寸，取值范围为 15000～155000000bit。当 CIR 小于 30000 时，缺省值为 15000；当 CIR 大于 30000 时，缺省值为 CIR/2。

ebs *excess-burst-size*：超出突发尺寸，取值范围为 0～155000000bit，缺省为 0，即只采用一个令牌桶监管。

【描述】

qos lr 命令用来限制接口的向外发送数据的速率，**undo qos lr** 命令用来取消限制。

【举例】

下面的命令将对接口 Ethernet0/0/0 发出的报文进行限速。

```
[H3C-Ethernet0/0/0] qos lr cir 38400 cbs 76800 ebs 0
```

第2章 拥塞管理配置命令

2.1 FIFO 队列配置命令

2.1.1 qos fifo queue-length

【命令】

qos fifo queue-length *queue-length*

undo qos fifo queue-length

【视图】

接口视图

【参数】

queue-length：队列的长度限制，取值范围为 1～1024，队列的缺省长度限制为 75。

【描述】

qos fifo 命令用来设定 FIFO 队列的长度限制，**undo qos fifo** 命令用来恢复队列长度的缺省值。

相关配置可参考命令 **display interface**。

【举例】

下面命令把 FIFO 的队列长度设置为 100。

```
[H3C-Ethernet1/0/0] qos fifo queue-length 100
```

2.2 优先队列配置命令

2.2.1 display qos pq interface

【命令】

display qos pq interface [*interface-type interface-number*]

【视图】

所有视图

【参数】

interface-type：接口类型。

interface-number：接口号。

【描述】

display qos pq interface 命令用来显示接口的优先队列配置情况和统计信息。

如不指定接口，将显示所有接口的优先队列配置情况和统计信息。

相关配置可参考命令 **qos pq**。

【举例】

显示 Ethernet 0/0/0 接口优先队列配置情况和统计信息。

```
[H3C] display qos pq interface ethernet 0/0/0
Interface: Ethernet0/0/0
Output queue : (Protocol queue : Size/Length/Discards) 0/500/0
Output queue : (Priority queuing : PQL 2 Size/Length/Discards)
Top:  0/20/0    Middle:  0/40/0    Normal:  0/60/0    Bottom:  0/80/0
```

2.2.2 display qos pql

【命令】

display qos pql [*pql-index*]

【视图】

所有视图

【参数】

pql-index：优先列表的序号。

【描述】

display qos pql 命令用来显示优先列表的内容。

使用缺省配置的项不被显示。

相关配置可参考命令 **qos pq pql**，**qos pq**。

【举例】

显示优先列表。

```
[H3C] display qos pql
Current PQL Configuration:
List  Queue   Params
-------------------------------------------------------
1     Top     Protocol ip less-than 1000
2     Normal  Length 60
2     Bottom  Length 40
```

```
3     Middle  Inbound-interface Ethernet5/0/0
```

2.2.3 qos pq

【命令】

qos pq pql *pql-index*

undo qos pq

【视图】

接口视图

【参数】

pql：采用指定的优先队列列表中定义的参数。

pql-index：优先队列的组号，取值范围为 1～16。

【描述】

qos pq 命令用来在接口上应用优先队列调度机制，**undo qos pq** 命令用来将接口的拥塞管理策略恢复到 FIFO。

缺省情况下，各接口拥塞管理策略为 FIFO。

一个接口只能应用一组优先列表。

可以为优先列表的组配置多条分类规则。在进行流分类的时候，系统沿规则链进行匹配，如果匹配上某规则则进入相应的队列，匹配结束；如果数据包不与任何规则匹配，则进入缺省队列。

相关配置可参考命令 **qos pq**，**qos pql**，**display qos pq interface**，**display qos pql**，**display interface**。

【举例】

将第 12 组优先列表应用到 Ethernet 0/0/0 上。

```
[H3C-Ethernet0/0/0] qos pq pql 12
```

2.2.4 qos pql default-queue

【命令】

qos pql *pql-index* **default-queue** { **top** | **middle** | **normal** | **bottom** }

undo qos pql *pql-index* **default-queue**

【视图】

系统视图

【参数】

pql-index：优先队列的组号，取值范围为 1～16。

top、**middle**、**normal**、**bottom**：对应 PQ 的四个队列，优先级依次降低。缺省情况下，队列为 **normal**。

【描述】

qos pql default-queue 命令用来将那些无对应规则的包指定到一个缺省队列。**undo qos pql default-queue** 命令用来取消配置，恢复缺省值。

进行流分类时，如果数据包不与任何规则匹配，则进入缺省队列。

对于同一个 *pql-index*，该命令重复使用将设定新的缺省队列。

相关配置可参考命令 **display qos pql**。

【举例】

将优先列表中第 12 组中无对应规则的包的缺省队列设定为 bottom。

```
[H3C] qos pql 12 default-queue bottom
```

2.2.5 qos pql inbound-interface

【命令】

qos pql *pql-index* **inbound-interface** *interface-type interface-number* **queue** { **top** | **middle** | **normal** | **bottom** }

undo qos pql *pql-index* **inbound-interface** *interface-type interface-number*

【视图】

系统视图

【参数】

pql-index：优先队列的组号，取值范围为 1～16。

interface-type：接口的类型。

interface-number：接口的编号。

top、**middle**、**normal**、**bottom**：对应 PQ 的四个队列，优先级依次降低。

【描述】

qos pql inbound-interface 命令用来建立基于接口的分类规则，**undo qos pql inbound-interface** 命令用来删除相应的分类规则。

缺省情况下，不配置任何分类规则。

该命令按报文输入的接口进行匹配。对于同一个 *pql-index*，该命令可以重复使用，为来自不同接口的报文建立不同的分类规则。

相关配置可参考命令 **qos pql default-queue**，**qos pql protocol**，**qos pql queue**，**qos pq**。

【举例】

指定规则 12，使得来自 Ethernet1/0/0 的报文进入 middle 队列。

```
[H3C] qos pql 12 inbound-interface Ethernet1/0/0 queue middle
```

2.2.6 qos pql protocol

【命令】

qos pql *pql-index* **protocol ip** [*queue-key key-value*] **queue** { **top** | **middle** | **normal** | **bottom** }

undo qos pql *pql-index* **protocol ip** [*queue-key key-value*]

【视图】

系统视图

【参数】

pql-index：优先队列的组号，取值范围为 1～16。

top、**middle**、**normal**、**bottom**：对应 PQ 的四个队列，优先级依次降低。

ip：指定协议为 IP。

当协议为 IP 时，*queue-key* 和 *key-value* 的取值见下表：

表2-1 协议为 IP 时的 queue-key 和 key-value 的取值

queue-key	key-value	意义
acl	*access-list-number*（2000～3999）	符合某访问控制列表定义的 IP 报文就进 入队列
fragments	空	只要是分片的 IP 报文就进入队列
greater-than	长度值（0～65535）	链路层数据报的长度大于某个计数值则报文进入队列
less-than	长度值（0～65535）	链路层数据报的长度小于某个计数值则报文进入队列
tcp	端口号（0～65535）	只要 IP 报文的源或目的 TCP 端口号为指定的端口号，就进入队列
udp	端口号（0~65535）	只要 IP 报文的源或目的 UDP 端口号为指定的端口号，就进入队列
-	-	所有 IP 报文进入队列

当 *queue-key* 指定为 tcp 或 udp 时，*key-value* 的值既可以直接使用端口名称，也可以使用相关端口号。两者的匹配关系请在指定 *key-value* 的位置处键入“？”而获知。

【描述】

qos pql protocol 命令用来建立基于协议的分类规则，**undo qos pql protocol** 命令用来删除相应的分类规则。

缺省情况下，不配置任何规则。

系统是以规则被配置的顺序来匹配数据包，如果发现数据包与某个规则匹配，便结束整个查找过程。

对于同一个 *pql-index*，该命令可以重复使用，为数据包建立多种分类规则。

相关配置可参考命令 **display qos pql**。

【举例】

指定 PQ 规则 1，使满足 ACL 为 3100 规则定义的 IP 报文进入 top 队列。

```
[H3C] qos pql 1 protocol ip acl 3100 queue top
```

2.2.7 qos pql queue

【命令】

qos pql *pql-index* **queue** { **top** | **middle** | **normal** | **bottom** } **queue-length** *queue-length*

undo qos pql *pql-index* **queue** { **top** | **middle** | **normal** | **bottom** } **queue-length**

【视图】

系统视图

【参数】

pql-index：优先队列的组号，取值范围为 1～16。

queue-length：为不同级别优先级队列组的长度值，取值范围为 1～1,024 个报文。

各优先级队列组长度的缺省值如下：

顶层队列的缺省长度值为 20；

中间队列的缺省长度值为 40；

一般队列的缺省长度值为 60；

底层队列的缺省长度值为 80。

【描述】

qos pql queue 命令用来设置 PQ 各队列的长度（所能容纳的数据包个数），**undo qos pql queue** 命令用来恢复各队列长度的缺省值。

如果队列满，新来的数据包就要被丢弃。

相关配置可参考命令**qos pql default-queue，qos pql inbound-interface，qos pql protocol，qos pq**。

【举例】

指定优先列表第 10 组 top 队列的长度为 10。

```
[H3C] qos pql 10 queue top queue-length 10
```

2.3 定制队列配置命令

2.3.1 display qos cq interface

【命令】

display qos cq interface [*interface-type interface-number*]

【视图】

所有视图

【参数】

interface-type：接口类型。

interface-number：接口号。

【描述】

display qos cq interface 命令用来显示接口的定制队列配置情况和统计信息。

如果不指定接口，将显示所有接口的 CQ 配置情况和统计信息。

相关配置可参考命令 **qos cq**。

【举例】

显示接口 Ethernet 2/0/0 的定制队列配置情况和统计信息。

```
[H3C] display qos cq interface Ethernet 2/0/0
Interface: Ethernet2/0/0
Output queue : (Protocol queuing : Size/Length/Discards) 0/500/0
Output queue : (Custom queuing : CQL 6 Size/Length/Discards)
 0:   0/  20/0             1:   0/  20/0             2:   0/  20/0
 3:   0/  20/0             4:   0/  20/0             5:   0/  20/0
 6:   0/  20/0             7:   0/  20/0             8:   0/  20/0
 9:   0/  20/0            10:   0/  20/0            11:   0/  20/0
12:   0/  20/0            13:   0/  20/0            14:   0/  20/0
15:   0/  20/0            16:   0/  20/0
```

2.3.2 display qos cql

【命令】

display qos cql [*cql-index*]

【视图】

所有视图

【参数】

cql-index：定制列表的序号。

【描述】

display qos cql 命令用来显示定制列表的内容。

如果为缺省值，则不被显示。

相关配置可参考命令 **qos cq**，**qos cql**。

【举例】

显示定制列表。

```
[H3C] display qos cql
Current CQL Configuration:
List  Queue  Params
2     3      Protocol ip fragments
3     0      Length 100
3     1      Inbound-interface Ethernet0
```

2.3.3 qos cq

【命令】

qos cq cql *cql-index*

undo qos cq

【视图】

接口视图

【参数】

cql-index：定制列表的组号，取值范围为 1～16。

【描述】

qos cq 命令用来在接口上应用定制队列，**undo qos cq** 命令用来将接口的拥塞管理策略恢复到 FIFO。

缺省情况下，接口拥塞管理策略为 FIFO。

一个接口只能应用一组定制队列。

我们可以为定制列表的组配置多条分类规则。在进行流分类的时候，系统沿规则链进行匹配，如果匹配上某规则则进入相应的队列，匹配结束；如果数据包不与任何规则匹配，则进入缺省队列。

相关配置可参考命令 **qos cql default-queue**，**qos cql inbound-interface**，**qos cql protocol**，**qos cql queue serving**，**qos cql queue queue-length**。

【举例】

将定制列表的第 5 组应用到 Ethernet 0/0/0 上。

```
[H3C-Ethernet0/0/0] qos cq cql 5
```

2.3.4 qos cql default-queue

【命令】

qos cql *cql-index* **default-queue** *queue-number*

undo qos cql *cql-index* **default-queue**

【视图】

系统视图

【参数】

cql-index：定制列表的组号，取值范围为 1～16。

queue-number：队列号，取值范围为 0～16，缺省队列号为 1。

【描述】

qos cql default-queue 命令用来为那些无对应规则的包指定一个缺省队列，**undo qos cql default-queue** 命令用来取消配置，恢复缺省值。

在进行流分类的时候，如果数据包不与任何规则匹配，则进入缺省队列。

相关配置可参考命令 **qos cql inbound-interface**，**qos cql protocol**，**qos cql queue serving**，**qos cql queue queue-length**，**qos cq**

【举例】

指定定制列表第 5 组的缺省队列为 2。

```
[H3C] qos cql 5 default-queue 2
```

2.3.5 qos cql inbound-interface

【命令】

qos cql *cql-index* **inbound-interface** *interface-type interface-number* **queue** *queue-number*

undo qos cql *cql-index* **inbound-interface** *interface-type interface-number*

【视图】

系统视图

【参数】

cql-index：定制列表的组号，取值范围为 1～16。

Interface-type：接口类型。

interface-number：接口号。

queue-number：队列号，取值范围为 0～16。

【描述】

qos cql inbound-interface 命令用来建立基于接口的分类规则，**undo qos cql inbound-interface** 命令用来删除相应的分类规则。

缺省情况下，不配置任何分类规则。

该命令按报文输入的接口进行匹配。对于同一个 *cql-index*，该命令可以重复使用，为来自不同接口的报文建立不同的分类规则。

相关配置可参考命令 **qos cql default-queue**，**qos cql protocol**，**qos cql queue serving**，**qos cql queue**。

【举例】

指定了一条规则使得来自于 Ethernet1/0/0 的报文进队列 3。

```
[H3C] qos cql 5 inbound-interface Ethernet1/0/0 queue 3
```

2.3.6 qos cql protocol

【命令】

qos cql *cql-index* **protocol ip** [*queue-key key-value*] **queue** *queue-number*

undo qos cql *cql-index* **protocol ip** [*queue-key key-value*]

【视图】

系统视图

【参数】

cql-index：定制列表的组号，取值范围为 1～16。

queue-number：队列号，取值范围为 0～16。

ip：指定协议为 **IP**。

当协议为 **IP** 时，*queue-key* 和 *key-value* 的取值见下表：

表2-2 协议为 IP 时的 queue-key 和 key-value 的取值

queue-key	key-value	意义
acl	*access-list-number*（2000~3999）	符合某访问控制列表定义的 IP 报文就进入队列
fragments	空	只要是分片的 IP 报文就进入队列
greater-than	长度值（0~65535）	链路层数据报长度大于某个计数值则报文进入队列
less-than	长度值（0~65535）	链路层数据报长度小于某个计数值则报文进入队列
tcp	端口号（0~65535）	只要 IP 报文的源或目的 TCP 端口号为指定的端口号，就进入队列
udp	端口号（0~65535）	只要 IP 报文的源或目的 UDP 端口号为指定的端口号，就进入队列
-	-	所有 IP 报文进入队列

当 *queue-key* 指定为 tcp 或 udp 时，*key-value* 的值既可以直接使用端口名称，也可以使用相关端口号。两者的匹配关系请在指定 key-value 的位置处键入“？”而获知。

【描述】

qos cql protocol 命令用来配置基于协议的分类规则，**undo qos cql protocol** 命令用来删除相应的分类规则。

系统是以规则被配置的顺序来匹配数据包，如果发现数据包与某个规则匹配，便结束整个查找过程。

对于同一个 *cql-index*，该命令可以重复使用，为 IP 数据包建立多种分类规则。

缺省情况下，不配置任何分类规则。

相关配置可参考命令 **qos cql default-queue**，**qos cql inbound-interface**，**qos cql queue**，**qos cq cql**。

【举例】

指定 CQ 规则 5，使得匹配访问控制列表 3100 的 IP 报文进入队列 3。

```
[H3C] qos cql 5 protocol ip acl 3100 queue 3
```

2.3.7 qos cql queue

【命令】

qos cql *cql-index* **queue** *queue-number* **queue-length** *queue-length*

undo qos cql *cql-index* **queue** *queue-number* **queue-length**

【视图】

系统视图

【参数】

cql-indexr：定制列表的组号，取值范围为 1～16。

queue-number：队列号，取值范围为 0～16。

queue-length：队列的最大长度，取值范围为 1～1024，缺省值为 20。

【描述】

qos cql queue 命令用来设置各队列的长度（所能容纳的数据包个数），**undo qos cql queue** 命令用来恢复队列长度的缺省值。

如果队列满，新来的数据包就要被丢弃。

相关配置可参考命令 **qos cql default-queue**，**qos cql inbound-interface**，**qos cql protocol**，**qos cql queue serving**，**qos cq**。

【举例】

指定定制列表第 5 组队列 4 的长度为 40。

```
[H3C] qos cql 5 queue 4 queue-length 40
```

2.3.8 qos cql queue serving

【命令】

qos cql *cql-index* **queue** *queue-number* **serving** *byte-count*

undo qos cql *cql-index* **queue** *queue-number* **serving**

【视图】

系统视图

【参数】

cql-index：定制列表的组号，取值范围为 1～16。

queue-number：队列号，取值范围为 0～16。

byte-count：队列每次轮询所发送数据包的字节数，取值范围是 1～16777215，缺省值为 1500 字节。

【描述】

qos cql queue serving 命令用来设置各队列每次轮询所发送数据包的字节数，**undo qos cql queue serving** 命令用来恢复发送数据包数的缺省值。

相关配置可参考命令 **qos cql default-queue**，**qos cql inbound-interface**，**qos cql protocol**，**qos cql queue queue-length**，**qos cq**。

【举例】

指定定制列表中的第 5 组队列 2，每次轮询所发送的字节数为 1400。

```
[H3C] qos cql 5 queue 2 serving 1400
```

2.4 加权公平队列配置命令

2.4.1 display qos wfq interface

【命令】

display qos wfq interface [*interface-type interface-number*]

【视图】

所有视图

【参数】

interface-type：接口类型。

interface-number：接口号。

【描述】

display qos wfq interface 命令用来显示接口的加权公平队列配置情况和统计信息。

如不指定接口，将显示所有接口的加权公平队列配置情况和统计信息。

相关配置可参考命令 **qos wfq**。

【举例】

显示接口 ethernet 1/0/0 的加权公平队列配置情况和统计信息。

```
[H3C] display qos wfq interface ethernet 1/0/0
Interface: Ethernet1/0/0
Output queue : (Protocol queuing : Size/Length/Discards) 0/500/0
Output queue : (Weighted Fair queuing : Size/Length/Discards)  0/64/0
Hashed by IP Precedence
Hashed queues :  0/0/256 (Active/Max active/Total)
```

2.4.2 qos wfq

【命令】

qos wfq [**precedence** | **dscp**] [**queue-length** *max-queue-length* [**queue-number** *total-queue-number*]]

undo qos wfq

【视图】

接口视图

【参数】

precedence：按照 IP 优先级进行流分类，缺省情况下使用 IP 优先级进行流分类。

dscp：按照 DSCP 值进行流分类。

max-queue-length：队列的最大长度，即每个队列中数据包的最大个数，超出后数据包将被丢弃，取值范围为 1～1024，缺省值为 64。

total-queue-number：队列的总数目，可取的值为：16、32、64、128、256、512、1024、2048、4096，缺省值为 256。

【描述】

qos wfq 命令用来在接口上应用加权公平队列或修改加权平均队列的参数，**undo qos wfq** 命令用来恢复缺省拥塞管理机制 FIFO。

当接口没有应用 WFQ 策略时，使用该命令可以在接口上应用 WFQ 策略，同时可指定 WFQ 的参数。如果接口已经应用了 WFQ 策略，使用该命令可以修改 WFQ 的参数。

相关配置可参考命令 **display interface**，**display qos wfq interface**。

【举例】

在接口 Ethernet 0/0/0 上应用 WFQ，并设置队列长度为 100，总队列个数设置为 512 个。

```
[H3C-Ethernet0/0/0] qos wfq queue-length 100 queue-number 512
```

2.5 基于类的队列配置命令

2.5.1 car

【命令】

car cir *committed-information-rate* [**cbs** *committed-burst-size* **ebs** *excess-burst-size*] [**green** *action* [**red** *action*]]

undo car

【视图】

流行为视图

【参数】

cir：承诺信息速率。

committed-information-rate：流量的平均速率，取值范围为 8000～155000000bps。

cbs *committee-burst-size*：承诺突发尺寸，每个时间间隔可发送的位数，取值范围为 15000～155000000bit，缺省值为 1500。

ebs *excess-burst-size*：超出突发尺寸，取值范围为 0～155000000bit，缺省值为 0。

green：数据包的流量符合承诺速率时对数据包采取的动作，缺省值为 **pass**。

red：数据包的流量不符合承诺速率时对数据包采取的动作，缺省值为 **discard**。

action：对数据包采取的动作，有以下几种：

- **discard**：丢弃数据包。
- **remark-dscp-pass** *new-dscp*：设置新的 DSCP 值 new-dscp，并发送，取值范围为 0～63。
- **remark-prec-pass** *new-precedence*：设置新的 IP 优先级 new-precedence，并发送，取值范围为 0～7。
- **remark-mpls-exp-pass** *new-exp*：设置新 MPLS 报文的 EXP 域，并发送，取值范围为 0～7。
- **pass**：发送数据包。

【描述】

car 命令用来为流行为配置使用流量监管，**undo car** 命令用来取消流量监管配置。

接口上应用的策略中使用 **car** 时，可以应用到接口的入或出方向。

接口上应用配置了 CAR 的策略将导致原有的 **qos car** 命令失效。

如果多次使用该命令在同一个流行为上配置，最后一次的配置将覆盖前面的配置。

相关配置可参考命令 **qos policy**，**traffic behavior**，**classfier behavior**。

【举例】

为流行为配置使用流量监管。报文正常流量为 38400bps，在第一时间可以有 2 倍于正常流量的突发流量通过，以后速率小于等于 38400bit 时正常发送，大于 38400bit 时，报文优先级改为 0 并发送。

```
[H3C] traffic behavior database
[H3C-behavior-database] car cir 38400 cbs 76800 ebs 0 green pass red
remark-prec-pass 0
```

2.5.2 classifier behavior

【命令】

classifier *tcl-name* **behavior** *behavior-name*

undo classifier *tcl-name*

【视图】

策略视图

【参数】

tcl-name：必须是已定义的类名，可以是系统定义或用户定义类。

behavior–name：必须是已定义的行为名，可以是系统定义或用户定义行为。

【描述】

classifier behavior 命令用来在策略中为类指定采用的行为，**undo classifier** 命令用来取消指定类在策略中的使用。

策略下每个类只能与一个动作关联。

对缺省类不能使用 **undo** 命令。

相关配置可参考命令 **qos policy**。

【举例】

在策略 mypolicy 中为类 database 指定采用的行为 test。

```
[H3C] qos policy mypolicy
[H3C-qospolicy-mypolicy] classifier database behavior test
```

2.5.3 debugging qos cbq

【命令】

debugging qos cbq { **af** | **ef** | **be** }

undo debugging qos cbq { **af** | **ef** | **be** }

【视图】

用户视图

【参数】

af：打开 AF 队列调试开关。

ef：打开 EF 队列调试开关。

be：打开 BE 队列调试开关。

【描述】

debugging qos cbq 命令用来打开基于类的队列的调试开关，**undo debugging qos cbq** 命令用来关闭基于类的队列的调试开关。

缺省情况下，关闭基于类的队列的调试开关。

【举例】

打开 AF 队列的调试开关。

```
<H3C> debugging qos cbq af
```

2.5.4 display qos cbq interface

【命令】

display qos cbq interface [*interface-type interface-number*]

【视图】

所有视图

【参数】

interface-type：接口类型。

interface-number：接口号。

【描述】

display qos cbq interface 命令用来显示指定接口或所有接口的基于类的队列配置信息和运行情况。

【举例】

```
[H3C] display qos cbq interface Ethernet1/0/0
Interface: Ethernet1/0/0
Output queue : (Protocol queue : Size/Length/Discards) 0/500/0
Output queue : (Class Based Queuing : Size/Discards)  0/0
    Queue Size: 0/0/0 (EF/AF/BE)
    BE queues:  0/0/256 (Active/Max active/Total)
    AF queues:  1 (Allocated)
    Bandwidth(Kbps): 30% / 80000 (Available/Max reserve)
```

2.5.5 display qos policy

【命令】

display qos policy { **system-defined** | **user-defined** } [*policy-name* [**classifier** *tcl-name*]]

【视图】

所有视图

【参数】

system-defined：系统预定义策略。

user-defined：用户定义策略。

policy-name：策略名，如果未指定，则显示所有系统预定义策略或所有用户定义策略的配置信息。

tcl-name：策略中的类名。

【描述】

display qos policy 命令用来显示指定策略或所有策略中指定类或所有类及与类关联的行为的配置信息。

【举例】

```
[H3C] display qos policy user-defined
User Defined QoS Policy Information:
Policy: test

 Classifier: default-class
   Behavior: be
    -none-

 Classifier: myclassifier
   Behavior: mybehavior
    Marking:
      Remark IP Precedence 3
    Committed Access Rate:
      CIR 20000 (bps), CBS 15000 (bit), EBS 0 (bit)
      Conform Action: pass
      Exceed  Action: discard
    Expedited Forwarding:
      Bandwidth 50 (Kbps) CBS 1500 (Bytes)

 Classifier: database
   Behavior: database
    Assured Forwarding:
      Bandwidth 30 (Kbps)
      Discard Method: Tail
      Queue Length  : 64 (Packets)
    General Traffic Shape:
```

```
    CIR 30000 (bps), CBS 15000 (bit), EBS 0 (bit)
    Queue length 50 (Packets)
  Marking:
    Remark IP Precedence 2
```

2.5.6 display qos policy interface

【命令】

display qos policy interface [*interface-type interface-number*] [**inbound** | **outbound**]

【视图】

所有视图

【参数】

interface-type：接口类型。

interface-number：接口号。

【描述】

display qos policy interface 命令用来显示指定接口或所有接口上策略的配置信息和运行情况。

对标记 MPLS EXP 报文数的统计值统计的是安全网关对数据包的临时标记，最终是否标记在 MPLS EXP 域，取决于该数据包从安全网关输出时是否是 MPLS 报文

【举例】

```
[H3C] display qos policy interface Ethernet 2/0/0
  Interface: Ethernet2/0/0
  Direction: Outbound
  Policy: test
   Classifier: default-class
     Matched : 0/0 (Packets/Bytes)
     Rule(s) : if-match any
     Behavior: be
     Default Queue:
      Flow Based Weighted Fair Queuing
        Max number of hashed queues: 256
        Matched  : 0/0 (Packets/Bytes)
        Enqueued : 0/0 (Packets/Bytes)
        Discarded: 0/0 (Packets/Bytes)
        Discard Method: Tail

   Classifier: myclassifier
```

```
  Matched : 0/0 (Packets/Bytes)
  Operator: AND
  Rule(s) : if-match ip-precedence 5
  Behavior: mybehavior
   Marking:
     Remark IP Precedence 3
     Remarked: 0 (Packets)
   Committed Access Rate:
     CIR 20000 (bps), CBS 15000 (bit), EBS 0 (bit)
     Conform Action: pass
     Exceed  Action: discard
     Conformed: 0/0 (Packets/Bytes)
     Exceeded : 0/0 (Packets/Bytes)
   Expedited Forwarding:
     Bandwidth 50 (Kbps), CBS 1500 (Bytes)
     Matched  : 0/0 (Packets/Bytes)
     Enqueued : 0/0 (Packets/Bytes)
     Discarded: 0/0 (Packets/Bytes)
Classifier: database
  Matched : 0/0 (Packets/Bytes)
  Operator: AND
  Rule(s) : if-match acl 3131
            if-match inbound interface Ethernet2/0/0
  Behavior: database
   General Traffic Shape:
     CIR 30000 (bps), CBS 15000 (bit), EBS 0 (bit)
     Queue Length: 50 (Packets)
     Queue size  : 0 (Packets)
     Passed   :  0/0 (Packets/Bytes)
     Discarded:  0/0 (Packets/Bytes)
     Delayed  :  0/0 (Packets/Bytes)
   Marking:
     Remark IP Precedence 2
     Remarked: 0 (Packets)
   Assured Forwarding:
     Bandwidth 30 (Kbps)
     Matched  : 0/0 (Packets/Bytes)
     Enqueued : 0/0 (Packets/Bytes)
     Discarded: 0/0 (Packets/Bytes)
```

2.5.7 display traffic behavior

【命令】

display traffic behavior { **system-defined** | **user-defined** } [*behavior-name*]

【视图】

所有视图

【参数】

system-defined：系统预定义行为。

user-defined：用户定义行为。

behavior-name：行为名，如果未指定行为名，则显示所有系统预定义行为或所有用户定义行为的信息。

【描述】

display traffic behavior 命令用来显示防火墙配置的流行为信息。

【举例】

```
[H3C] display traffic behavior user-defined
User Defined Behavior Information:
  Behavior: test
    Assured Forwarding:
      Bandwidth 30 (Kbps)
      Discard Method: Tail
      Queue Length  : 64 (Packets)
    General Traffic Shape:
      CIR 30000 (bps), CBS 15000 (bit), EBS 0 (bit)
      Queue length 50 (Packets)
    Marking:
      Remark IP Precedence 2
  Behavior: mybehavior
    Marking:
      Remark IP Precedence 3
    Committed Access Rate:
      CIR 20000 (bps), CBS 15000 (bit), EBS 0 (bit)
      Conform Action: pass
      Exceed  Action: discard
    Expedited Forwarding:
      Bandwidth 50 (Kbps) CBS 1500 (Bytes)
```

2.5.8 display traffic classifier

【命令】

display traffic classifier { **system-defined** | **user-defined** } [*tcl-name*]

【视图】

所有视图

【参数】

system-defined：系统预定义类。

user-defined：用户定义类。

tcl-name：类名，如果未指定类名，则显示所有系统预定义类或所有用户定义类的信息。

【描述】

display traffic classifier 命令用来显示防火墙配置的类信息。

【举例】

```
[H3C] display traffic classifier user-defined
User Defined Classifier Information:
 Classifier: myclassifier
  Operator: AND
  Rule(s) : if-match ip-precedence 5

 Classifier: database
  Operator: AND
  Rule(s) : if-match acl 3131
            if-match inbound-interface Ethernet2/0/0
```

2.5.9 gts

【命令】

gts cir *committed-information-rate* [**cbs** *committed-burst-size* [**ebs** *excess-burst-size* [**queue-length** *queue-length*]]]

undo gts

【视图】

流行为视图

【参数】

cir *committed-information-rate*：承诺信息速率，取值范围为 8000～155000000bps。

cbs *committed-burst-size*：承诺突发尺寸，取值范围为 15000～155000000bit。当 CIR 小于 30000 时，缺省值为 15000；当 CIR 大于 30000 时，缺省值为 CIR/2。

ebs *excess-burst-size*：超出突发尺寸，取值范围为 0～155000000bit，缺省为 0。

queue-length：队列的最大长度，取值范围为 1～1024，缺省为 50。

【描述】

gts 命令用来为流行为配置流量整形，**undo gts** 命令用来取消流量整形配置。

接口上应用的策略中使用 **gts** 时，只能应用到接口的出方向。

接口上应用配置了 TS 的策略将导致原有的 **qos gts** 命令失效。

如果多次使用该命令在同一个流行为上配置，最后一次的配置将覆盖前面的配置。

相关配置可参考命令 **qos policy**，**traffic behavior**，**classifier behavior**。

【举例】

为流行为配置使用 TS，正常流量为 38400bps，在第一时间可以有 2 倍于正常流量的突发流量通过，以后速率小于等于 38400bit 的流量时正常发送，速率大于 38400bit 时，将进入队列缓存，缓存队列长度为 100。

```
[H3C] traffic behavior database
[H3C-behavior-database] gts cir 38400 cbs 76800 ebs 0 queue-length 100
```

2.5.10 if-match { destination-mac | source-mac }

【命令】

if-match [**not**] { **destination-mac** | **source-mac** } *mac-address*

undo if-match [**not**] { **destination-mac** | **source-mac** } *mac-address*

【视图】

类视图

【参数】

mac-address：MAC 地址。

not：不匹配该类。

【描述】

if-match { **destination-mac** | **source-mac** }命令用来定义目的或源 MAC 地址匹配规则，**undo if-match** { **destination-mac** | **source-mac** }命令用来删除目的或源 MAC 地址匹配规则。

目的 MAC 地址匹配规则只对出方向的策略有意义，并且只对以太类型的接口有意义。

源 MAC 地址匹配规则只对入方向的策略有意义，并且只对以太类型的接口有意义。

相关配置可参考命令 **traffic classifier**。

【举例】

定义类 class1 的匹配规则为：匹配目的 MAC 地址为 0050-ba27-bed3 的报文。

```
[H3C] traffic classifier class1
[H3C-classifier-class1] if-match destination-mac 0050-ba27-bed3
```

定义类 class2 的匹配规则为：匹配源 MAC 地址为 0050-ba27-bed2 的报文。

```
[H3C] traffic classifier class2
[H3C-classifier-class2] if-match source-mac 0050-ba27-bed2
```

2.5.11 if-match acl

【命令】

if-match [**not**] **acl** *access-list-number*

undo if-match [**not**] **acl** *access-list-number*

【视图】

类视图

【参数】

access-list-number：ACL 号。

not：不匹配该类。

【描述】

if-match acl 命令用来定义 ACL 匹配规则，**undo if-match acl** 命令用来删除 ACL 匹配规则。

相关配置可参考命令 **traffic classifier**。

【举例】

定义类匹配 ACL3101。

```
[H3C] traffic classifier class1
[H3C-classifier-class1] if-match acl 3101
```

2.5.12 if-match any

【命令】

if-match [**not**] **any**

undo if-match [**not**] **any**

【视图】

类视图

【参数】

not：不匹配该类。

【描述】

if-match any 命令用来定义匹配所有数据包的规则，**undo if-match any** 命令用来删除匹配所有数据包的规则。

相关配置可参考命令 **traffic classifier**。

【举例】

定义匹配所有数据包的规则。

```
[H3C] traffic classifier class1
[H3C-classifier-class1] if-match any
```

2.5.13 if-match classifier

【命令】

if-match [**not**] **classifier** *tcl-name*

undo if-match [**not**] **classifier** *tcl-name*

【视图】

类视图

【参数】

tcl-name：类名。

not：不匹配该类。

【描述】

if-match classifier 命令用来定义 QoS 类匹配规则，**undo if-match classifier** 命令用来删除 QoS 类匹配规则。

如果类匹配的规则之间既有逻辑与，又有逻辑或的关系，采用本匹配方法可以解决。

例如，需要定义 classA，满足以下关系：规则 1 & 规则 2 | 规则 3，可以这样定义：

traffic classifier classB operator and

if-match 规则 1

if-match 规则 2

traffic classifier classA operator or

if-match 规则 3

if-match classifier classB

相关配置可参考命令 **traffic classifier**。

【举例】

定义类 class2，要求引用 class1。

定义类 class2 的匹配规则，需要引用 class1，所以先配置 class1。class1 规则为：匹配 IP 优先级为 5。

```
[H3C] traffic classifier class1
[H3C-classifier-class1] if-match ip-precedence 5
```

定义类 class2，匹配规则为 class1，并且目的 MAC 地址为 0050-BA27-BED3 的报文。

```
[H3C] traffic classifier class2
[H3C-classifier-class2] if-match classifier class1
[H3C-classifier-class2] if-match destination-mac 0050-BA27-BED3
```

2.5.14 if-match dscp

【命令】

if-match [**not**] **dscp** { *dscp-value* }

undo if-match [**not**] **dscp** { *dscp-value* }

【视图】

类视图

【参数】

dscp-value：DSCP 的值，取值范围为 0-63，或可以是如下关键字 **ef**，**af11**，**af12**，**af13**，**af21**，**af22**，**af23**，**af31**，**af32**，**af33**，**af41**，**af42**，**af43**，**cs1**，**cs2**，**cs3**，**cs4**，**cs5**，**cs7** 或 **default**。

表2-3 DSCP 关键字与值的对应表

关键字	DSCP 值（二进制）	DSCP 值（十进制）
ef	101110	46
af11	001010	10
af12	001100	12
af13	001110	14
af21	010010	18
af22	010100	20
af23	010110	22

关键字	DSCP 值（二进制）	DSCP 值（十进制）
af31	011010	26
af32	011100	28
af33	011110	30
af41	100010	34
af42	100100	36
af43	100110	38
cs1	001000	8
cs2	010000	16
cs3	011000	24
cs4	100000	32
cs5	101000	40
cs6	110000	48
cs7	111000	56
default	000000	0

not：不匹配该类。

【描述】

if-match dscp 命令用来定义 DSCP 匹配规则，**undo if-match dscp** 命令用来删除 DSCP 匹配规则。

一个类下可配置多条这样的命令，不覆盖。每条命令在配置后，*dscp-value* 将自动按照从小到大的顺序排序。删除时指定的所有 DSCP 值必须与规则中的完全相同才会删除，顺序可不一样。

一条命令可以配置多个 DSCP 值，最多可指定 8 个；如果指定了多个相同的 DSCP 值，系统默认为一个；多个不同的 DSCP 值是或的关系。

相关配置可参考命令 **traffic classifier**。

【举例】

定义类 class1 的匹配规则为：匹配 DSCP 值为 1 或 6 或 9 的报文。

```
[H3C] traffic classifier class1
[H3C-classifier-class1] if-match dscp 1 6 9
```

2.5.15 if-match inbound-interface

【命令】

if-match [**not**] **inbound-interface** *interface-type interface-number*

undo if-match [**not**] **inbound-interface** *interface-type interface-number*

【视图】

类视图

【参数】

interface-type：接口类型。

interface-number：接口号。

not：不匹配该类。

【描述】

if-match inboud-interface 命令用来定义类的入接口匹配规则，**undo if-match inboud-interface** 命令用来删除类的入接口匹配规则。

定义该匹配规则时，指定接口必须存在。如果接口为动态接口，在该接口删除后，该规则被删除。

支持接口类型：以太网接口、VT 等。

相关配置可参考命令 **traffic classifier**。

【举例】

定义类匹配从 Ethernet1/0/0 进入的报文。

```
[H3C] traffic classifier class1
[H3C-classifier-class1] if-match inbound-interface Ethernet1/0/0
```

2.5.16 if-match ip-precedence

【命令】

if-match [**not**] **ip-precedence** { *ip-precedence-value* }

undo if-match [**not**] **ip-precedence**

【视图】

类视图

【参数】

ip-precedence-value：IP 优先级的值，取值范围为 0～7。

not：不匹配该类。

【描述】

if-match ip-precedence 命令用来定义 IP 优先级匹配规则，**undo if-match ip-precedence** 命令用来删除 IP 优先级匹配规则。

命令在配置后，IP 优先级的值将自动按照从小到大的顺序排序。

可以配置多个 IP 优先级值，最多可指定 8 个；如果指定了多个相同的 IP 优先级值，系统默认为一个；多个不同的 IP 优先级值是或的关系。

相关配置可参考命令 **traffic classifier**。

【举例】

定义类 class1 的匹配规则为：匹配 IP 优先级值为 1 或 6 的报文。

```
[H3C] traffic classifier class1
[H3C-classifier-class1] if-match ip-precedence 1 6
```

2.5.17 if-match protocol

【命令】

if-match [**not**] **protocol** *protocol-name*

undo if-match [**not**] **protocol** *protocol-name*

【视图】

protocol-name：协议名，取值为 IP。

not：不匹配该类。

【参数】

类视图

【描述】

if-match protocol 命令用来定义协议匹配规则，**undo if-match protocol** 命令用来删除协议匹配规则。

相关配置可参考命令 **traffic classifier**。

【举例】

定义类匹配 ip 协议的报文。

```
[H3C] traffic classifier class1
[H3C-classifier-class1] if-match protocol ip
```

2.5.18 if-match rtp

【命令】

if-match [**not**] **rtp start-port** *starting-port-number* **end-port** *end-port-number*

undo if-match [**not**] **rtp start-port** *starting-port-number* **end-port** *end-port-number*

【视图】

类视图

【参数】

starting-port-number：起始 RTP 端口号，取值范围为 2000～65535。

end-port-number：RTP 目的端口号范围，取值范围为 2000～65535。

not：不匹配该类。

【描述】

if-match rtp 命令用来定义 RTP 协议端口匹配规则，**undo if-match rtp** 命令用来删除 RTP 协议端口匹配规则。

该命令用于匹配落在指定 RTP 端口号范围内的 RTP 报文，即匹配所有在 *starting-port-number* 与 end-*port-number* 之间的偶数 UDP 端口号的报文。 一个类下如果多次重复使用该命令，最后一个将覆盖前面的。

相关配置可参考命令 **traffic classifier**。

【举例】

定义类 class1 的匹配规则为：匹配 RTP 端口号在 16384 和 32767 之间的偶数 UDP 端口号的报文。

```
[H3C] traffic classifier class1
[H3C-classifier-class1] if-match rtp start-port 16384 end-port 32767
```

2.5.19 qos apply policy

【命令】

qos apply policy *policy-name* { **inbound** | **outbound** }

undo qos apply policy { **inbound** | **outbound** }

【视图】

接口视图

【参数】

inbound：入方向。

outbound：出方向。

policy-name：策略名。

【描述】

qos apply policy 命令用来在接口应用关联的策略，**undo qos apply policy** 命令用来删除关联的策略。

【举例】

将策略 mypolicy 应用到接口 Ethernet1/0/0 的出方向上。

```
[H3C-Ethernet1/0/0] qos apply policy mypolicy outbound
```

2.5.20 qos max-bandwidth

【命令】

qos max-bandwidth *bandwidth*

undo qos max-bandwidth

【视图】

接口视图

【参数】

bandwidth：接口的可用带宽，单位 Kbps，范围为 1～1000000。缺省情况下，对于物理接口，其取值为物理接口实际的波特率或速率；对于虚拟接口模板（Virtual Template）、VE 等逻辑接口，取值为 64Kbps。

【描述】

qos max-bandwidth 命令用来配置 CBQ 中报文入队列进行带宽检查时使用的最大接口带宽，并非指物理接口的实际带宽。**undo qos max-bandwidth** 命令用来取消带宽配置。

如果接口上同时配置了 LR 和百分比类型的 CBQ，请将此命令中设置的带宽与 LR 的限制速率保持一致。

建议该值小于物理接口或逻辑链路的实际可用带宽。

【举例】

下面命令把 Virtual-Template 1 的带宽设置为 128kbps。

```
[H3C-Virtual-Template1] qos max-bandwidth 128
```

2.5.21 qos policy

【命令】

qos policy *policy-name*

undo qos policy *policy-name*

【视图】

系统视图

【参数】

policy-name：策略名。

【描述】

qos policy 命令用来定义一个策略并进入策略视图，**undo qos policy** 命令用来删除一个策略。

如果某接口应用了该策略，则不允许删除该策略，需要先在应用的接口上取消对该策略的应用，然后再使用 **undo qos policy** 删除该策略。

策略名 *policy-name* 不允许为系统预定义策略。系统预定义的策略为 default。

相关配置可参考命令 **classifier behavior**，**qos apply policy**。

【举例】

定义一个名为 mypolicy 的策略。

```
[H3C] qos policy mypolicy
[H3C-qospolicy-mypolicy]
```

2.5.22 queue af

【命令】

queue af bandwidth { *bandwidth* | **pct** *percentage* }

undo queue af

【视图】

流行为视图

【参数】

bandwidth：带宽，取值范围 8～1000000，单位 Kbps。

percentage：可用带宽的百分比，取值范围 1～100。

【描述】

queue af 命令用来配置类进行确保转发（Assured-forwarding），并配置类可确保的最小带宽，**undo queue af** 命令用来取消配置。

当在策略下将类与 queue af 所属行为关联时，必须满足：

- 同一个策略下为确保转发（queue af）和加速转发（queue ef）的类指定的带宽之和必须不大于该策略所应用接口的可用带宽；
- 同一个策略下为确保转发（queue af）和加速转发（queue ef）的类指定的带宽百分比之和必须不大于 100；

- 同一个策略下确保转发（queue af）和加速转发（queue ef）的类的带宽的配置必须都采用相同的值的类型，比如都采用绝对值形式，或者都采用百分比形式。

相关配置可参考命令 **qos policy**，**traffic behavior**，**classfier behavior**。

【举例】

为行为 database 配置确保转发，并且确保最小带宽为 200Kbit/s。

```
[H3C] traffic behavior database
[H3C-behavior-database] queue af bandwidth 200
```

2.5.23 queue ef

【命令】

queue ef bandwidth { *bandwidth* [**cbs** *committed-burst-size*] | **pct** *percentage* [**cbs_ratio** *ratio*] }

undo queue ef

【视图】

流行为视图

【参数】

bandwidth：带宽，取值范围 8～1000000，单位 Kbps。

percentage：可用带宽的百分比，取值范围 1～100。

committed-burst-size：指定允许的突发量，单位是字节，取值范围 32～2000000 字节，缺省值为 bandwidth*25。

ratio：允许的突发量的百分比，取值范围为 25～500。

【描述】

queue ef 命令用来配置加速转发（Expedited-forwarding），报文进入绝对优先队列，并配置至少保证的最大带宽，**undo queue ef** 命令用来取消配置。

该命令在流行为视图下不能与 **queue af**，**queue-length**，**wred** 同时使用。

在策略下，缺省类 default-class 不能与 **queue ef** 所属 **behavior** 关联。

同一个策略下为确保转发（queue af）和加速转发（queue ef）的类指定的带宽之和必须不大于该策略所应用接口的可用带宽；

同一个策略下为确保转发（queue af）和加速转发（queue ef）的类指定的带宽百分比之和必须不大于 100；

同一个策略下确保转发（queue af）和加速转发（queue ef）的类的带宽的配置必须都采用相同的值的类型，比如都采用绝对值形式，或者都采用百分比形式。相关配置可参考命令 **qos policy**，**traffic behavior**，**classifier behavior**。

【举例】

配置报文进入优先队列，最大带宽为 200Kbit/s，*burst* 缺省计算为 5000byte。

```
[H3C] traffic behavior database
[H3C-behavior-database] queue ef bandwidth 200 cbs 5000
```

2.5.24 queue wfq

【命令】

queue wfq [**queue-number** *total-queue-number*]

undo queue wfq

【视图】

流行为视图

【参数】

total-queue-number：公平队列的数目，可取的值为 16、32、64、128、256、512、1024、2048、4096，即 2 的幂数，缺省为 64。

【描述】

queue wfq 命令用来为缺省类配置采用公平队列，**undo queue wfq** 命令用来取消配置。

配置了该命令的行为仅仅可以与缺省类关联使用，另外，该命令还可以搭配 **queue-length** 或 **wred** 使用。

相关配置可参考命令 **qos policy**，**traffic behavior**，**classifir behavior**。

【举例】

为缺省类配置使用 WFQ，队列数为 16。

```
[H3C] traffic behavior test
[H3C-behaviro-test] queue wfq queue-number 16
[H3C] qos policy mypolicy
[H3C-qospolicy-mypolicy] classifier default-class behavior test
```

2.5.25 queue-length

【命令】

queue-length *queue-length*

undo queue-length

【视图】

流行为视图

【参数】

queue-length：队列最大阈值，取值范围为 1～512，缺省为尾部丢弃方式，队列长度为 64。

【描述】

queue-length 命令用来配置最大队列长度，丢弃方式为尾部丢弃，**undo queue-length** 命令用来取消该配置。

该命令必须在配置了 **queue af** 或 **queue wfq** 后使用。

配置 **queue-length** 后，若执行 **undo queue af** 和 **undo queue wfq** 命令，则 **queue-length** 也同时被取消，反之亦然。

配置 **queue-length** 后，若用 **wred** 命令配置为随机丢弃方式，则 **queue-length** 也被取消，反之亦然。

缺省情况下，为尾部丢弃方式。

相关配置可参考命令 **qos policy**，**traffic behavior**，**classifier behavior**。

【举例】

配置尾部丢弃，队列长度最大为 16。

```
[H3C] traffic behavior database
[H3C-behavior-database] queue af bandwidth 200
[H3C-behavior-database] queue-length 16
```

2.5.26 remark dscp

【命令】

remark dscp *dscp-value*

undo remark dscp

【视图】

流行为视图

【参数】

dscp-value：DSCP 值，取值范围为 0～63，或可以是如下关键字 **ef**，**af11**，**af12**，**af13**，**af21**，**af22**，**af23**，**af31**，**af32**，**af33**，**af41**，**af42**，**af43**，**cs1**，**cs2**，**cs3**，**cs4**，**cs5**，**cs7** 或 **default**。

表2-4 DSCP 关键字与值的对应表

关键字	DSCP 值（二进制）	DSCP 值（十进制）
ef	101110	46
af11	001010	10
af12	001100	12
af13	001110	14
af21	010010	18
af22	010100	20
af23	010110	22
af31	011010	26
af32	011100	28
af33	011110	30
af41	100010	34
af42	100100	36
af43	100110	38
cs1	001000	8
cs2	010000	16
cs3	011000	24
cs4	100000	32
cs5	101000	40
cs6	110000	48
cs7	111000	56
default	000000	0

【描述】

remark dscp 命令用来为类配置标记报文的 DSCP 值，**undo remark dscp** 命令用来取消标记报文的 DSCP 值。

相关配置可参考命令 **qos policy**，**traffic behavior**，**classifier behavior**。

【举例】

配置标记报文的 DSCP 值为 6。

```
[H3C] traffic behavior database
[H3C-behavior-database] remark dscp 6
```

2.5.27 remark ip-precedence

【命令】

remark ip-precedence *ip-precedence-value*

undo remark ip-precedence

【视图】

流行为视图

【参数】

ip-precedence-value：标记的 IP 优先级，取值范围为 0～7。

【描述】

remark ip-precedence 命令用来配置标记报文的 IP 优先级，**undo remark ip-precedence** 命令用来取消标记报文的 IP 优先级

相关配置可参考命令 **qos policy**，**traffic behavior**，**classifier behavior**。

【举例】

配置标记报文的 IP 优先级值为 6。

```
[H3C] traffic behavior database
[H3C-behavior-database] remark ip-precedence 6
```

2.5.28 traffic behavior

【命令】

traffic behavior *behavior–name*

undo traffic behavior *behavior–name*

【视图】

系统视图

【参数】

behavior–name：流行为名。

【描述】

traffic behavior 命令用来定义一个流行为并进入流行为视图，**undo traffic behavior** 命令用来删除一个流行为。

行为名 *behavior–name* 不能为系统预定义的流行为名。系统预定义的流行为有 ef、af、be 等。

相关配置可参考命令 **qos policy**，**qos apply policy**，**classifier behavior**。

【举例】

定义一个名为 behavior1 的流行为。

```
[H3C] traffic behavior behavior1
[H3C-behavior-behavior1]
```

2.5.29 traffic classifier

【命令】

traffic classifier *tcl-name* [**operator** { **and** | **or** }]

undo traffic classifier *tcl-name*

【视图】

系统视图

【参数】

and：指定类下的规则之间是逻辑与的关系，即数据包必须匹配全部规则才属于该类。

or：指定类下的规则之间是逻辑或的关系，即数据包只要匹配其中任何一个规则就属于该类。

tcl-name：类名。

【描述】

traffic classifier 命令用来定义一个类并进入类视图，**undo traffic classifier** 命令用来删除一个类。

缺省情况下为 **operator and**。

类名 *tcl-name* 不允许为系统预定义类。系统预定义的类如下：

default-class、ef、af1、af2、af3、af4、ip-prec0、ip-prec1、ip-prec2、ip-prec3、ip-prec4、ip-prec5、ip-prec6、ip-prec7、mpls-exp0、mpls-exp1、mpls-exp2、mpls-exp3、mpls-exp4、mpls-exp5、mpls-exp6、mpls-exp7。

相关配置可参考命令 **qos policy**，**qos apply policy**，**classifier behavior**。

【举例】

定义一个名为 class1 的类。

```
[H3C] traffic classifier class1
[H3C-classifier-class1]
```

2.5.30 wred

【命令】

wred [**dscp** | **ip-precedence**]

undo wred

【视图】

流行为视图

【参数】

dscp：表明在为一个包计算丢弃概率时使用的是 DSCP 值。

ip-precedence：表明在为一个包计算丢弃概率时使用的是 IP 优先级值，作为缺省配置。

【描述】

wred 命令用来配置丢弃方式为加权随机早期检测，**undo wred** 命令用来取消该配置。

该命令必须在配置了 **queue af** 和 **queue wfq** 后使用。**wred** 和 **queue-length** 这两个命令不能同时有效。取消该配置时将删除 WRED 相关的其他配置。当接口上应用了配置 WRED 的策略后，原有的接口级的 WRED 配置失效。

与缺省类 default-class 关联的行为，只能配 **ip-precedence**。

相关配置可参考命令 **qos policy**，**traffic behavior**，**classifier behavior**。

【举例】

配置采用加权早期检测方式，丢弃概率以 IP 优先级计算。

```
[H3C] traffic behavior database
[H3C-behavior-database] wred
```

2.5.31 wred dscp

【命令】

wred dscp *dscp-value* **low-limit** *low-limit* **high-limit** *high-limit* [**discard-probability** *discard-prob*]

undo wred dscp *dscp-value*

【视图】

流行为视图

【参数】

dscp-value：DSCP 值，取值范围为 0～63，或可以是如下关键字：**ef**，**af11**，**af12**，**af13**，**af21**，**af22**，**af23**，**af31**，**af32**，**af33**，**af41**，**af42**，**af43**，**cs1**，**cs2**，**cs3**，**cs4**，**cs5**，**cs6**，**cs7** 或 **default**。

表2-5 DSCP 关键字与值的对应表

关键字	DSCP 值（二进制）	DSCP 值（十进制）
ef	101110	46
af11	001010	10
af12	001100	12
af13	001110	14
af21	010010	18
af22	010100	20
af23	010110	22
af31	011010	26
af32	011100	28
af33	011110	30
af41	100010	34
af42	100100	36
af43	100110	38
cs1	001000	8
cs2	010000	16
cs3	011000	24
cs4	100000	32
cs5	101000	40
cs6	110000	48
cs7	111000	56
default	000000	0

low-limit：下限，取值范围为 1～1024，缺省值为 10。

high-limit：上限，取值范围为 1～1024，缺省值为 30。

discard-prob：丢弃概率的分母，取值范围为 1～255，缺省值为 10。

【描述】

wred dscp 命令用来设置 WRED 各 DSCP 的下限、上限和丢弃概率分母，**undo wred dscp** 命令用来取消该配置。

需已用 **wred** 使能了基于 DSCP 的 WRED 丢弃方式。

取消 **wred** 配置，**wred dscp** 配置同时被取消。

取消 **queue af** 或 **queue wfq** 配置，丢弃参数的配置同时被取消。

相关配置可参考命令 **qos policy**，**traffic behavior**，**classifier behavior**。

【举例】

设置 DSCP 为 3 的报文的队列下限为 20，上限为 40，丢弃概率分母为 15。

```
[H3C] traffic behavior database
[H3C-behavior-database] wred dscp
[H3C-behavior-database] wred dscp 3 low-limit 20 high-limit 40
discard-probability 15
```

2.5.32 wred ip-precedence

【命令】

wred ip-precedence *precedence* **low-limit** *low-limit* **high-limit** *high-limit* [**discard-probability** *discard-prob*]

undo wred ip-precedence *precedence*

【视图】

流行为视图

【参数】

precedence：IP 报文的优先级，取值范围为 0～7。

low-limit：下限，取值范围为 1～1024，缺省值为 10。

high-limit：上限，取值范围为 1～1024，缺省值为 30。

discard-prob：丢弃概率的分母，取值范围为 1～255，缺省值为 10。

【描述】

wred ip-precedence 命令用来设置 WRED 各优先级的下限、上限和丢弃概率分母，**undo wred ip-precedence** 命令用来取消配置。

缺省情况下，已使能基于 IP 优先级的 WRED 丢弃方式。

取消 **wred** 配置，**wred ip-precedence** 配置同时被取消。

取消 **queue af** 或 **queue wfq** 配置，丢弃参数的配置同时被取消。

相关配置可参考命令 **qos policy**，**traffic behavior**, **classifier behavior**。

【举例】

设置优先级为 3 的报文的队列下限为 20，上限为 40，丢弃概率分母为 15。

```
[H3C] traffic behavior database
[H3C-behaviro-database] wred
[H3C-behavior-database] wred ip-precedence 3 low-limit 20 high-limit 40
discard-probability 15
```

2.5.33 wred weighting-constant

【命令】

wred weighting-constant *exponent*

undo wred weighting-constant

【视图】

流行为视图

【参数】

exponent：指数，取值范围 1～16，缺省为 9。

【描述】

wred weighting-constant 命令用来设置 WRED 计算平均队列长度的指数，**undo wred weighting-constant** 命令用来取消配置。

需配置了 **queue af** 或 **queue wfq**，并已用 **wred** 使能了 WRED 丢弃方式。

如果取消 **wred** 配置，**wred weighting-constant** 配置同时被取消。

相关配置可参考命令 **qos policy**，**traffic behavior**，**classifier behavior**。

【举例】

配置计算平均队列长度的指数为 6。

```
[H3C] traffic behavior database
[H3C-behavior-database] queue af bandwidth 200
[H3C-behavior-database] wred ip-precedence
[H3C-behavior-database] wred weighting-constant 6
```

2.6 实时传输协议队列的配置命令

2.6.1 display qos rtpq interface

【命令】

display qos rtpq interface [*interface-type interface-number*]

【视图】

所有视图

【参数】

interface-type：接口类型。

interface-number：接口编号。

【描述】

display qos rtpq interface 命令用来显示当前 IP RTP Priority 的队列信息，包括当前的 RTP 队列长度和 RTP 报文的丢包数，显示所有接口的 RTP 队列配置情况和统计信息。

【举例】

例如显示当前 IP RTP Priority 的队列信息：

```
[H3C] display qos rtpq interface Ethernet 2/0/0
Interface: Ethernet2/0/0
Output queue : (RTP queuing : Size/Max/Outputs/Discards)  0/0/0/0
```

2.6.2 qos reserved-bandwidth

【命令】

qos reserved-bandwidth pct *percentage*

undo qos reserved-bandwidth

【视图】

接口视图

【参数】

percentage：是预留带宽占可用带宽的百分比，取值范围为 1～100，缺省值为 80。

【描述】

qos reserved-bandwidth 命令用来设置最大预留带宽占可用带宽的百分比，**undo qos reserved-bandwidth** 命令用来恢复缺省的配置。

为 QoS 队列分配带宽时，考虑到部分带宽用于控制协议报文、2 层帧头等，通常配置的带宽不大于带宽的 75％。

建议慎重使用该命令修改最大预留带宽。

相关配置可参考命令 **qos rtpq**。

【举例】

设置为 RTP 队列的应用分配的最大预留带宽为可用带宽的 80%。

```
[H3C-Ethernet1/0/0] qos reserved-bandwidth pct 80
```

2.6.3 qos rtpq

【命令】

qos rtpq start-port *start-port-number* **end-port** *end-port-number* **bandwidth** *bandwidt*h [**cbs** *committed-burst-size*]

undo qos rtpq

【视图】

接口视图

【参数】

start-port-number：指定发起 RTP 报文的起始 UDP 端口号

end-port-number：指定发起 RTP 报文的终止 UDP 端口号。

bandwidth：RTP 队列所占用的带宽，为最大预留带宽的一部分，单位是 kbps。

committed-burst-size：指定允许的突发量，取值范围 1500～2000000 字节。

【描述】

qos rtpq 命令用来启动接口下 RTP 队列特性，为某个 UDP 目的端口范围的 RTP 报文保留一个实时业务，**undo qos rtpq** 命令用来关闭本接口的 RTP 队列特性。

缺省情况下，不启动 RTP 队列特性。

该命令主要应用于对时延敏感的应用，如实时语音传输。**qos rtpq** 命令为语音业务提供最优先服务。

在配置 *bandwidth* 参数时，通常应该将其设置为比此实时业务所需的带宽总量要大一些，以预防突发流量的冲击。

但是实时协议队列的带宽不能超过总有效带宽的 75%，如果需要配置带宽大于 75%，需要先执行 **qos reserved-bandwidth** 来改变缺省的最大保留带宽值。

另外，需要为 2 层报文头预留 25％的空间，这是因为带宽分配考虑了数据载荷加上 IP、UDP 和 RTP 报文头，但没有考虑 2 层的帧头。

相关配置可参考命令 **qos reserved-bandwidth**。

【举例】

配置接口 Ethernet 1/0/0 下启动 RTP 队列特性，起始端口号为 16384，终止端口为 32767，RTP 报文占用 64Kbit/s 的带宽，如果输出接口拥塞，进入 RTP 队列。

```
[H3C-Ethernet1/0/0] qos rtpq start-port 16384 end-port 32767 bandwidth 64
```

第3章 DAR 配置命令

3.1 DAR 配置命令

3.1.1 dar max-session-count

【命令】

dar max-session-count *count*

undo dar max-session-count

【视图】

系统视图

【参数】

count：DAR 可识别的最大连接数目，取值范围与产品型号相关，请以实际产品为准。

【描述】

dar max-session-count 命令用来配置 DAR 可识别的最大连接数。**undo dar max-session-count** 命令用来恢复 DAR 可识别的最大连接数的缺省值。

当有大量的数据流经设备时，若 DAR 对其进行一一识别，将会消耗大量的系统资源，从而影响其它功能模块的正常工作。为了避免这种现象，用户可以对 DAR 能够识别的最大连接数目进行限制，以节省宝贵的系统资源。当连接数目超过设定的最大阈值时，DAR 将不再对其进行识别，直接将其标记为无法识别报文。

【举例】

设置 DAR 可识别的最大连接数为 1000。

```
<H3C> system-view
[H3C] dar max-session-count 1000
```

3.1.2 dar protocol

【命令】

dar protocol *protocol-name* { **tcp** | **udp** } **port** { *portvalue* | **range** *port-min port-max* }*

undo dar protocol *protocol-name* { **tcp** | **udp** } **port**

【视图】

系统视图

【参数】

protocol-name：应用协议名称，其中包括十个用户预定义协议 **user-defined01**、**user-defined02**、……、**user-defined10**。初始状态的用户预定义协议是没有指定端口号的，只有指定了端口号以后才会生效。同时用户预定义协议也可以使用 **dar protocol-rename** 命令来更改名称。

tcp：基于 TCP 协议。

udp：基于 UDP 协议。

portvalue：协议的端口号，取值范围 1～65535，且不能与 DAR 特性中其他应用协议已设置的端口号冲突。最多可以输入 16 个端口号，用空格分隔。

range *port-min port-max*：设置端口号的范围，*port-min* 表示范围内的最小端口号，*port-max* 表示范围内的最大端口号。最大端口号和最小端口号之间的差值要小于等于 1000，即 *port-max* – *port-min* ≤ 1000。端口号范围内不能含有 DAR 特性中其他应用协议已设置的匹配端口。

【描述】

dar protocol 命令用来配置 DAR 应用协议的端口号。**undo dar protocol** 命令用来恢复 DAR 应用协议的端口号为缺省值。

该命令支持同时设置应用协议的端口号和端口范围。

缺省情况下，各协议均有其缺省的端口号，其中十个用户预定义协议无端口号。

【举例】

设置 RTP 协议的端口号为 36000、36001 和 40000～41000。

```
<H3C> system-view
[H3C] dar protocol rtp udp port 36000 36001 range 40000 41000
```

3.1.3 dar protocol-rename

【命令】

dar protocol-rename *old-name user-defined-name*

undo dar protocol-rename *user-defined-name*

【视图】

系统视图

【参数】

old-name：用户预定义协议的初始名称，初始名称为 user-defined01、user-defined02、……、user-defined10。

user-defined-name：用户预定义协议的新名称，长度为 1～14 个字符。新的名称不能与已存在的协议名称冲突，而且不能为 all、total、tcp、udp、ip 或 user-defined01、user-defined02、……、user-defined10。

【描述】

dar protocol-rename 命令用来重命名用户预定义协议的名称。**undo dar protocol-rename** 命令用来恢复用户预定义协议的缺省名称。

缺省情况下，初始名称为 user-defined01、user-defined02、……、user-defined10。

【举例】

将用户预定义协议 user-defined01 的名称改为 hello。

```
<H3C> system-view
[H3C] dar protocol-rename user-defined01 hello
```

将用户预定义协议 user-defined01 的名称恢复为缺省名称。

```
<H3C> system-view
[H3C] undo dar protocol-rename hello
```

3.1.4 dar protocol-statistic

【命令】

dar protocol-statistic [**flow-interval** *time*]

undo dar protocol-statistic

【视图】

以太网接口视图

【参数】

flow-interval *time*：设置平均速率和最大速率的统计时间，取值范围为 1～30，单位为分钟，缺省为 5 分钟。

【描述】

dar protocol-statistic 命令用来使能 DAR 的报文统计功能。**undo dar protocol-statistic** 命令用来关闭 DAR 的报文统计功能。

通过使能 DAR 的报文统计功能，用户可以及时对各个接口上的应用协议的报文个数、数据流量、以及流量的历史平均速率和历史最大速率进行监控，便于对数据流实施相应的策略。

缺省情况下，关闭 DAR 的报文统计功能。

【举例】

使能接口 Ethernet 0/0/0 的 DAR 报文统计功能，并设置统计时间为 7 分钟。

```
<H3C> system-view
[H3C] interface Ethernet 0/0/0
[H3C-Ethernet0/0/0] dar protocol-statistic flow-interval 7
```

3.1.5 debugging dar

【命令】

debugging dar { **packet** | **event** | **error** | **all** }

undo debugging dar { **packet** | **event** | **error** | **all** }

【视图】

用户视图

【参数】

packet：DAR 的报文调试信息开关。

event：DAR 的事件调试信息开关。

error：DAR 的错误调试信息开关。

all：DAR 的所有调试信息开关。

【描述】

debugging dar 命令用来打开 DAR 的调试信息开关。**undo debugging dar** 命令用来关闭 DAR 的调试信息开关。

缺省情况下，关闭 DAR 的调试信息开关。

【举例】

打开 DAR 的报文调试信息开关。

```
<H3C> debugging dar packet
```

3.1.6 display dar information

【命令】

display dar information

【视图】

任意视图

【参数】

无

【描述】

display dar information 命令用来查看 DAR 特性模块的信息。

显示信息包括可识别的最大连接数和已监视的连接数。

【举例】

查看 DAR 特性模块的信息。

```
<H3C> display dar information
Max session count       : 8192
Watched session count   : 1000
```

3.1.7 display dar protocol

【命令】

display dar protocol { **all** | *protocol-name* }

【视图】

任意视图

【参数】

all：查看所有协议的信息。

protocol-name：应用协议的名称。

【描述】

display dar protocol 命令用来查看 DAR 协议的相关信息。

【举例】

查看所有协议的信息。

```
<H3C> display dar protocol all
Protocol       TCP/UDP  Port
-------------- -------- -----------
bgp            tcp      179
               udp      179
citrix         tcp      1494
               udp      1604
cuseeme        tcp      7648 7649
               udp      7648 7649 24032
dhcp           udp      67 68
```

```
dns             tcp      53
                udp      53
exchange        tcp      135
finger          tcp      79
ftp             tcp      21
gopher          tcp      70
                udp      70
http            tcp      80
imap            tcp      143 220
                udp      143 220
irc             tcp      194
                udp      194
kerberos        tcp      88 749
                udp      88 749
l2tp            udp      1701
ldap            tcp      389
                udp      389
mgcp            tcp      2427 2428 2727
                udp      2427 2727
napster         tcp      6699 8875 8888 7777 6700 6666 6677 6688 4444 5555
netbios         tcp      137 138 139
                udp      137 138 139
netshow         tcp      1755
nfs             tcp      2049
                udp      2049
nntp            tcp      119
                udp      119
notes           tcp      1352
                udp      1352
novadigm        tcp      3460 3461 3462 3463 3464 3465
                udp      3460 3461 3462 3463 3464 3465
ntp             tcp      123
                udp      123
pcanywhere      tcp      65301 5631
                udp      22 5632
pop3            tcp      110
                udp      110
pptp            tcp      1723
printer         tcp      515
                udp      515
rcmd            tcp      512 513 514
rip             udp      520
rsvp            udp      1698 1699
```

```
rtsp            tcp      554
sip             tcp      5060
                udp      5060
skinny          tcp      2000 2001 2002
smtp            tcp      25
snmp            tcp      161 162
                udp      161 162
socks           tcp      1080
sqlnet          tcp      1521
sqlserver       tcp      1433
ssh             tcp      22
streamwork      udp      1558
sunrpc          tcp      111
                udp      111
syslog          udp      514
telnet          tcp      23
vdolive         tcp      7000
winmx           tcp      6699
xwindows        tcp      6000 6001 6002 6003
```

3.1.8 display dar protocol-rename

【命令】

display dar protocol-rename

【视图】

任意视图

【参数】

无

【描述】

display dar protocol-rename 命令用来查看用户预定义协议的重命名信息。

【举例】

查看用户预定义协议的重命名信息，其中 user-defined01 协议已被重命名为 merry，其它协议未被重命名。

```
<H3C> display dar protocol-rename
Old Name        User Defined Name
--------------- ---------------
user-defined01   merry
user-defined02
```

```
user-defined03
user-defined04
user-defined05
user-defined06
user-defined07
user-defined08
user-defined09
user-defined10
```

3.1.9 display dar protocol-statistic

【命令】

display dar protocol-statistic [**protocol** *protocol-name* | **top** *top-number* | **all**] [**interface** *type number*] [**direction** { **in** | **out** }]

【视图】

任意视图

【参数】

protocol *protocol-name*：应用协议的名称。

top *top-number*：查询流量最大的 *top-number* 个协议的报文，取值范围为 1～16。

all：查看所有的协议报文。

interface *type number*：查看指定的接口。

direction：指定查看的流量的方向，缺省为双向。

in：查看入方向的流量。

out：查看出方向的流量。

【描述】

display dar protocol-statistic 命令用来查看 DAR 的报文统计信息。

【举例】

查看 Ethernet0/0/0 接口 DAR 的报文统计信息。

```
<H3C> display dar protocol-statistic all
Interface: Ethernet0/0/0
Port     In/Out  Packet Count  Byte Count      Bit Rate    Max Bit Rate
                                                in 5 min     in 5 min
                                                 (bps)       (bps)
-------- ------ ------------- --------------- ------------ -----------
ftp       IN    33            1034            23           44
          OUT   10            650             0            0
```

```
http        IN    24          948          11          20
bgp         IN    1           72           10          12
Total       IN    58          2054         44          76
            OUT   10          650          0           0
```

3.1.10 if-match protocol

【命令】

if-match [**not**] **protocol** *protocol-name*

undo if-match [**not**] **protocol** *protocol-name*

【视图】

类视图

【参数】

protocol-name：匹配协议的名称，可以为：**bgp**、**bittorrent**、**citrix**、**cuseeme**、**dhcp**、**dns**、**edonkey**、**egp**、**eigrp**、**exchange**、**fasttrack**、**finger**、**ftp**、**gnutella**、**gopher**、**gre**、**h323**、**http**、**icmp**、**igmp**、**imap**、**ip**、**ipinip**、**ipsec**、**irc**、**kerberos**、**l2tp**、**ldap**、**mgcp**、**napster**、**netbios**、**netshow**、**nfs**、**nntp**、**notes**、**novadign**、**ntp**、**pcanywhere**、**pop3**、**pptp**、**printer**、**rcmd**、**rip**、**rsvp**、**rtcp**、**secure-ftp**、**secure-http** 、 **secure-imap** 、 **secure-irc** 、 **secure-ldap** 、 **secure-nntp** 、**secure-pop3**、**secure-telnet**、**sip**、**skinny**、**smtp**、**snmp**、**socks**、**sqlnet**、**sqlserver**、**ssh**、**streamwork**、**sunrpc**、**syslog**、**telnet**、**tftp**、**vdolive**、**winmx**、**xwindows**、**unknown-tcp**、**unknown-udp**、**unknown-others**、**user-defined01**、**user-defined02**、……、**user-defined10**（如果 **user-defined01**～**user-defined10** 被改了名字，则为修改后的名字）。其中 **unknown-tcp** 为不可识别的 TCP 协议报文，**unknown-udp** 为不可识别的 UDP 协议报文，**unknown-others** 为不可识别的其它 IP 协议报文。**user-defined01**、**user-defined02**、……、**user-defined10** 为用户预定义协议报文，在没有使用 **dar protocol** 命令为其分配端口号前是无效的。

【描述】

if-match protocol 命令用来定义协议匹配规则。**undo if-match protocol** 命令用来删除协议匹配规则。

缺省情况下，未配置协议匹配规则。

【举例】

定义类 smtp-class，配置规则匹配 SMTP 协议。

```
<H3C> system-view
[H3C] traffic classifier smtp-class
[H3C-classifier-smtp-class] if-match protocol smtp
```

3.1.11 if-match protocol http

【命令】

if-match [**not**] **protocol http** [**url** *url-string* | **host** *hostname-string* | **mime** *mime-type*]

undo if-match [**not**] **protocol http** [**url** *url-string* | **host** *hostname-string* | **mime** *mime-type*]

【视图】

类视图

【参数】

url：根据 HTTP 报文中的 URL 进行匹配。

url-string：在 HTTP 报文中进行匹配的 URL，支持“*”和“#”通配符，长度为 1～32 字符的字符串。

host：根据 HTTP 报文中的 hostname 进行匹配。

hostname-string：HTTP 报文中进行匹配的 hostname，支持“*”和“#”通配符，长度为 1～32 字符的字符串。

mime：根据 HTTP 报文中的 MIME 类型进行匹配。

mime-type：在 HTTP 报文中进行匹配的 MIME 类型，支持“*”和“#”通配符，长度为 1～32 字符的字符串。

【描述】

if-match protocol http 命令用来配置 HTTP 协议的匹配规则。**undo if-match protocol http** 命令用来删除 HTTP 协议的匹配规则。

缺省情况下，未配置 HTTP 协议的匹配规则。

【举例】

定义类 http-class，配置匹配规则为匹配 hostname 为*.abc.com 的 HTTP 报文。

```
<H3C> system-view
[H3C] traffic classifier http-class
[H3C-classifier-http-class] if-match protocol http host *.abc.com
```

3.1.12 if-match protocol rtp

【命令】

if-match [**not**] **protocol rtp** [**payload-type** { **audio** | **video** | *payload-string* }*]

undo if-match [**not**] **protocol rtp** [**payload-type** { **audio** | **video** | *payload-string* }*]

【视图】

类视图

【参数】

payload-type：对载荷类型进行匹配。

audio：对音频 RTP 载荷类型进行匹配。

video：对视频 RTP 载荷类型进行匹配。

payload-string：在 RTP 报文中进行匹配的载荷类型，取值范围是 0～127。可以同时配置多个值，每个值之间用空格分隔，最多可以同时配置 16 个值。

【描述】

if-match protocol rtp 命令用来配置 RTP 协议的匹配规则。**undo if-match protocol rtp** 命令用来删除 RTP 协议的匹配规则。

若不指定载荷类型，表示匹配所有 RTP 报文。

缺省情况下，未配置 RTP 协议的匹配规则。

【举例】

定义类 rtp-class1，配置匹配规则为匹配载荷类型为视频的 RTP 报文。

```
<H3C> system-view
[H3C] traffic classifier rtp-class1
[H3C-classifier-rtp-class1] if-match protocol rtp payload-type video
```

定义类 rtp-class2，配置匹配规则为匹配载荷类型为 0、1、4、5、6、10、或 64 的 RTP 报文。

```
<H3C> system-view
[H3C] traffic classifier rtp-class2
[H3C-classifier-rtp-class2] if-match protocol rtp payload-type 0 1 4 5 6 10
64
```

3.1.13 reset dar protocol-statistic

【命令】

reset dar protocol-statistic { { **protocol** *protocol-name* | **interface** *type number* }* | **all** }

【视图】

用户视图

【参数】

protocol *protocol-name*：清除指定协议的统计信息。

interface *type number*：清除指定接口的统计信息。

all：清除所有统计信息。

【描述】

reset dar protocol-statistic 命令用来清除 DAR 的协议统计信息，即将统计的结果重置为 0。

【举例】

清除以太网接口 Ethernet 0/0/1 的 FTP 协议的统计信息。

```
<H3C> reset dar protocol-statistic protocol ftp interface Ethernet 0/0/1
```

清除所有协议的统计信息。

```
<H3C> reset dar protocol-statistic all
```

3.1.14 reset dar session

【命令】

reset dar session

【视图】

用户视图

【参数】

无

【描述】

reset dar session 命令用来清除所有的会话连接缓存信息。

【举例】

清除会话连接缓存信息。

```
<H3C> reset dar session
```

第4章 WRED 配置命令

4.1 WRED 配置命令

4.1.1 display qos wred interface

【命令】

display qos wred interface [*interface-type interface-number*]

【视图】

所有视图

【参数】

interface-type：接口类型。

interface-number：接口号。

【描述】

display qos wred interface 命令用来显示接口的 WRED 配置情况和统计信息。

如果不指定接口，将显示所有接口的 WRED 配置情况和统计信息。

【举例】

显示指定接口的 WRED 配置情况和统计信息。

```
[H3C] display qos wred interface Ethernet0/0/0
Interface: Ethernet0/0/0
 Current WRED configuration:
 Exponent: 9 (1/512)
 Precedence Low     High    Discard      Random      Tail
            Limit   Limit   Probability  Discard     Discard
 ------------------------------------------------------------
 0          10      30      10           0           0
 1          10      30      10           0           0
 2          10      30      10           0           0
 3          10      30      10           0           0
 4          10      30      10           0           0
 5          10      30      10           0           0
 6          10      30      10           0           0
 7          10      30      10           0           0
```

4.1.2 qos wred

【命令】

qos wred [**ip-precedence** | **dscp**]

undo qos wred

【视图】

接口视图

【参数】

dscp：表明在为一个包计算丢弃概率时使用的是 DSCP 值。

ip-precedence：表明在为一个包计算丢弃概率时使用的是 IP 优先级值，作为缺省配置。

【描述】

qos wred 命令用来在接口上应用加权随机早期检测 WRED，**undo qos wred** 命令用来恢复缺省的丢弃方法。

缺省情况下，队列丢弃方法为尾丢弃。

接口视图下的 WRED 只能和 WFQ 共同使用，不能单独使用或和其它的队列共同使用。所以在一个接口上使能 WRED 前，需要确保接口上应用的是 WFQ。

相关配置可参考命令 **qos wfq**，**qos wred**，**display qos wred interface**。

【举例】

以下命令将在 Ethernet0/0/0 接口上使用加权随机早期检测。（假设已在接口上应用了 WFQ）。

```
[H3C-Ethernet0/0/0] qos wred
```

4.1.3 qos wred dscp

【命令】

qos wred dscp *dscp-value* **low-limit** *low-limit* **high-limit** *high-limit* **discard-probability** *discard-prob*

undo qos wred dscp *dscp-value*

【视图】

接口视图

【参数】

dscp-value：DSCP 值，取值范围为 0～63，或可以是如下关键字：**ef**，**af11**，**af12**，**af13**，**af21**，**af22**，**af23**，**af31**，**af32**，**af33**，**af41**，**af42**，**af43**，**cs1**，**cs2**，**cs3**，**cs4**，**cs5**，**cs6**，**cs7** 或 **default**。

low-limit：下限，取值范围为 1～1024，缺省值为 10。

high-limit：上限，取值范围为 1～1024，缺省值为 30。

discard-prob：丢弃概率的分母，取值范围为 1～255，缺省值为 10。

【描述】

qos wred dscp 命令用来设置 WRED 各 DSCP 的下限、上限和丢弃概率分母，**undo qos wred dscp** 命令用来恢复缺省值。

必须先使用 **qos wred** 在接口上应用 WRED，才可以配置 WRED 的参数。阈值限制的是平均队列长度。

相关配置可参考命令 **qos wred**，**display qos wred interface**。

【举例】

设置 DSCP 为 3 的报文的队列下限为 20，上限为 40，丢弃概率分母为 15。

```
[H3C-Ethernet0/0/0] qos wred dscp 3 low-limit 20 high-limit 40
discard-probability 15
```

4.1.4 qos wred ip-precedence

【命令】

qos wred ip-precedence *ip-precedence* **low-limit** *low-limit* **high-limit** *high-limit* **discard-probability** *discard-prob*

undo qos wred ip-precedence *ip-precedence*

【视图】

接口视图

【参数】

ip-precedence：IP 报文的优先级，取值范围为 0～7。

low-limit：优先级的 WRED 下限，取值范围为 1～1024，*low-limit* 的缺省值分别为 10。

high-limit：优先级的 WRED 上限，取值范围为 1～1024，*high-limit* 的缺省值为 30。

discard-prob：丢弃概率的分母，取值范围为 1～255，缺省值为 10。

【描述】

qos wred ip-precedence 命令用来设置 WRED 各优先级的下限、上限和丢弃概率分母，**undo qos wred ip-precedence** 命令用来恢复缺省值。

必须先使用 **qos wred** 在接口上应用 WRED，才可以配置 WRED 的参数。阈值限制的是平均队列长度。

相关配置可参考命令 **qos wred**，**display qos wred interface**。

【举例】

在接口上设置优先级为 3 的报文的队列下限为 20，上限为 40，丢弃概率分母为 15。

```
[H3C-Ethernet0/0/0] qos wred ip-precedence 3 low-limit 20 high-limit 40
discard-probability 15
```

4.1.5 qos wred weighting-constant

【命令】

qos wred weighting-constant *exponent*

undo qos wred weighting-constant

【视图】

接口视图

【参数】

exponent：计算平均队列长度的指数，取值范围为 1～16，缺省值为 9。

【描述】

qos wred weighting-constant 命令用来设置 WRED 计算平均队列长度的指数，**undo qos wred weighting-constant** 命令用来恢复缺省值。

必须先使用 **qos wred** 在接口上应用 WRED，才可以配置 WRED 的参数。

相关配置可参考命令 **qos wred**，**display qos wred interface**。

【举例】

以下命令将在 Ethernet1/0/0 接口上配置计算平均队列长度的指数为 6。（假设已在接口上使能了 WRED）。

```
[H3C-Ethernet0/0/0] qos wred weighting-constant 6
```

第5章 MPLS QoS 配置命令

5.1 MPLS QoS 配置命令

5.1.1 if-match mpls-exp

【命令】

if-match [**not**] **mpls-exp** { *mpls-experimental-value* }

undo if-match [**not**] **mpls-exp**

【视图】

类视图

【参数】

mpls-experimental-value：EXP 值，取值范围 0～7。

【描述】

if-match mpls-exp 命令用来定义匹配 mpls 的 exp 域的规则，**undo if-match mpls-exp** 命令用来删除匹配 mpls 的 exp 域的规则。

在该命令中 MPLS 的 EXP 值可指定多个，最多可指定 8 个，如果指定了多个相同的值，只取一个，多个不同的值是或的关系。一个类下如果多次重复使用该命令，最后一个将覆盖前面的。命令在配置后，EXP 将自动按照从小到大的顺序排序。

相关配置可参考命令 **traffic classifier**。

【举例】

定义类匹配 exp 为 3 或 4 的报文。

```
[H3C-classifier-database] if-match mpls-exp 3 4
```

5.1.2 qos cql protocol mpls exp

【命令】

qos cql *cql-index* **protocol mpls exp** *mpls-experimental-number* **queue** *queue-number*

undo qos cql *cql-index* **protocol mpls exp** *mpls-experimental-number*

【视图】

系统视图

【参数】

cql-index：定制列表的组号，取值范围为 1～16。

mpls-experimental-number：MPLS 报文的 EXP 域，取值范围为 0～7。

queue-number：队列号，取值范围为 0～16。

【描述】

qos cql protocol mpls exp 命令用来配置基于协议 MPLS 的分类规则，根据 MPLS EXP 值配置定制列表，并使匹配的分组进入不同的定制队列。**undo qos cql protocol mpls exp** 命令用来删除相应的分类规则。

系统是以规则被配置的顺序来匹配数据包，如果发现数据包与某个规则匹配，便结束整个查找过程。

对于同一个 *cql-index*，本命令可以重复使用，为 IP 数据包建立多种分类规则。

相关配置可参考命令 **qos cql protocol**。

【举例】

配置基于协议 MPLS 的分类规则，MPLS 的 EXP 值为 1。

```
[H3C] qos cql 10 protocol mpls exp 1
```

5.1.3 qos pql protocol mpls exp

【命令】

qos pql *pql-index* **protocol mpls exp** *mpls-experimental-value* **queue** { **top** | **middle** | **normal** | **bottom** }

undo qos pql *pql-index* **protocol mpls exp** *mpls-experimental-value*

【视图】

系统视图

【参数】

pql-index：优先列表的序号，取值范围为 1～16。

mpls-experimental-value：MPLS 报文的 EXP 域，取值范围为 0～7。

queue top | **middle** | **normal** | **bottom**：高/中/正常/低优先队列。

【描述】

qos pql protocol mpls exp 命令用来建立基于协议 MPLS 的分类规则，根据 MPLS EXP 值配置优先列表，并使匹配的分组进入不同的优先队列。**undo qos pql protocol mpls exp** 命令用来删除相应的分类规则。

系统是以规则被配置的顺序来匹配数据包，如果发现数据包与某个规则匹配，便结束整个查找过程。

对于同一个 *pql-index*，本命令可以重复使用，为 IP 数据包建立多种分类规则。

相关配置可参考命令 **qos pql protocol**。

【举例】

建立基于协议 MPLS 的分类规则，设置 MPLS 的 EXP 值为 5。

```
[H3C] qos pql 10 protocol mpls exp top 5
```

5.1.4 remark mpls-exp

【命令】

remark mpls-exp *mpls-experimental-value*

undo remark mpls-exp

【视图】

流行为视图

【参数】

mpls-experimental-value：预设置的 MPLS 的 EXP 值，取值范围为 0～7。

【描述】

remark mpls-exp 命令用来配置标记报文的 MPLS 的 EXP 值，**undo remark mpls-exp** 命令用来配置取消标记报文的 MPLS 的 EXP 值。

相关配置可参考命令 **traffic classifier**，**qos policy**，**classifier behavior**。

【举例】

配置标记报文的 MPLS 的 EXP 值为 0。

```
[H3C] qos policy h3c
[H3C] traffic behavior database
[H3C-behavior-database] remark mpls-exp 0
```

附录A 命令总索引

本命令索引包括手册中所出现的全部命令，按字母序排列，左边为命令行，右边为该命令所在的功能模块和页码。

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

A

abr-summary	04-路由协议命令	3-1
access-limit	07-安全命令	1-1
accounting	07-安全命令	1-1
accounting commands scheme	01-基础配置命令	6-1
accounting domain	03-网络层协议命令	5-4
accounting optional	07-安全命令	1-2
accounting optional	07-安全命令	1-20
acl	01-基础配置命令	6-1
acl	07-安全命令	2-1
acl counter	07-安全命令	2-2
acl name	07-安全命令	5-1
acl number	07-安全命令	6-1
acl number	07-安全命令	7-1
add	07-安全命令	5-1
add interface	07-安全命令	4-31
ad-interval	08-可靠性命令	2-1
aggregate	04-路由协议命令	4-1
aging-time	07-安全命令	4-7
ah authentication-algorithm	06-VPN 命令	3-1
algorithm-suite	06-VPN 命令	5-1
allow l2tp	06-VPN 命令	1-1
apply access-vpn vpn-instance	06-VPN 命令	6-1
apply as-path	04-路由协议命令	5-1
apply community	04-路由协议命令	5-1
apply cost	04-路由协议命令	5-2

apply cost-type	04-路由协议命令	5-3
apply default output-interface	03-网络层协议命令	7-1
apply ip-address default next-hop	03-网络层协议命令	7-1
apply ip-address next-hop	03-网络层协议命令	7-2
apply ip-precedence	03-网络层协议命令	7-3
apply local-preference	04-路由协议命令	5-3
apply mpls-label	06-VPN 命令	6-1
apply origin	04-路由协议命令	5-4
apply output-interface	03-网络层协议命令	7-4
apply tag	04-路由协议命令	5-5
area	04-路由协议命令	3-2
arp check enable	03-网络层协议命令	2-1
arp send-gratuitous-arp	03-网络层协议命令	2-1
arp static	03-网络层协议命令	2-2
arp-proxy enable	03-网络层协议命令	2-3
asbr-summary	04-路由协议命令	3-2
ascii	01-基础配置命令	5-20
aspf-policy	07-安全命令	4-8
async mode	01-基础配置命令	13-16
attribute	07-安全命令	9-10
authentication	07-安全命令	1-3
authentication super hwtacacs-scheme	07-安全命令	1-4
authentication-algorithm	06-VPN 命令	4-1
authentication-client method	06-VPN 命令	5-2
authentication-method	06-VPN 命令	4-1
authentication-mode	01-基础配置命令	6-2
authentication-mode	04-路由协议命令	3-3
authentication-server method	06-VPN 命令	5-2
authorization	07-安全命令	1-5
auto-execute command	01-基础配置命令	6-3

B

bgp	04-路由协议命令	4-2
bims boot request	01-基础配置命令	9-3

bims device-id	01-基础配置命令	9-3
bims enable	01-基础配置命令	9-4
bims interval	01-基础配置命令	9-4
bims ip address	01-基础配置命令	9-5
bims request	01-基础配置命令	9-6
bims sharekey	01-基础配置命令	9-6
bims source ip-address	01-基础配置命令	9-7
bims specify-time	01-基础配置命令	9-7
bims-server	03-网络层协议命令	5-4
binary	01-基础配置命令	5-21
boot bootrom	01-基础配置命令	5-1
bridge aging-time	07-安全命令	7-1
bridge bridge-set enable	07-安全命令	7-2
bridge bridging	07-安全命令	7-3
bridge enable	07-安全命令	7-3
bridge firewall unknown-mac	07-安全命令	7-4
bridge firewall unknown-mac broadcast	07-安全命令	7-5
bridge firewall unknown-mac multicast	07-安全命令	7-5
bridge firewall unknown-mac unicast	07-安全命令	7-6
bridge learning	07-安全命令	7-7
bridge mac-address	07-安全命令	7-7
bridge permit	07-安全命令	7-8
bridge vlanid-transparent-transmit enable	07-安全命令	6-1
bridge vlanid-transparent-transmit enable	07-安全命令	7-9
bridge-set	07-安全命令	7-10
bridge-set fast-forwarding	07-安全命令	7-10
broadcast-limit link	01-基础配置命令	13-25
bye	01-基础配置命令	5-21
bye	01-基础配置命令	11-31

C

ca identifier	07-安全命令	8-1
car	09-QoS 命令	2-14
cd	01-基础配置命令	5-1

cd	01-基础配置命令	5-22
cd	01-基础配置命令	11-32
cdup	01-基础配置命令	5-22
cdup	01-基础配置命令	11-32
certificate request entity	07-安全命令	8-1
certificate request from	07-安全命令	8-2
certificate request mode	07-安全命令	8-3
certificate request polling	07-安全命令	8-3
certificate request url	07-安全命令	8-4
checkzero	04-路由协议命令	2-1
ciphersuite	07-安全命令	9-1
classifier behavior	09-QoS 命令	2-16
client-verify	07-安全命令	9-2
clock datetime	01-基础配置命令	1-1
clock summer-time	01-基础配置命令	1-1
clock timezone	01-基础配置命令	1-2
close	01-基础配置命令	5-23
close-mode	07-安全命令	9-2
command-alias enable	01-基础配置命令	1-19
command-alias mapping	01-基础配置命令	1-20
command-privilege	01-基础配置命令	1-3
common-name	07-安全命令	8-9
compare-different-as-med	04-路由协议命令	4-3
confederation id	04-路由协议命令	4-3
confederation nonstandard	04-路由协议命令	4-4
confederation peer-as	04-路由协议命令	4-5
connection-limit default	07-安全命令	3-1
connection-limit default amount	07-安全命令	3-1
connection-limit enable	07-安全命令	3-2
connection-limit policy	07-安全命令	3-3
copy	01-基础配置命令	5-2
count	01-基础配置命令	4-1
country	07-安全命令	8-9
cpu-usage cycle	01-基础配置命令	1-4

crl check disable	07-安全命令	8-5
crl update-period	07-安全命令	8-5
crl url	07-安全命令	8-6

D

dampening	04-路由协议命令	4-5
dar max-session-count	09-QoS 命令	3-1
dar protocol	09-QoS 命令	3-1
dar protocol-rename	09-QoS 命令	3-2
dar protocol-statistic	09-QoS 命令	3-3
data algorithm-suite	06-VPN 命令	5-3
data ipsec-sa duration	06-VPN 命令	5-4
databits	01-基础配置命令	6-4
datafill	01-基础配置命令	4-1
data-flow-format	07-安全命令	1-20
data-flow-format	07-安全命令	1-47
datasize	01-基础配置命令	4-2
debugging	01-基础配置命令	2-1
debugging	01-基础配置命令	5-23
debugging arp packet	03-网络层协议命令	2-3
debugging aspf	07-安全命令	4-9
debugging aspf http	07-安全命令	4-10
debugging bgp	04-路由协议命令	4-6
debugging bims all	01-基础配置命令	9-1
debugging bridge eth-forwarding	07-安全命令	7-11
debugging bridge ip-forwarding	07-安全命令	7-12
debugging connection-limit	07-安全命令	3-3
debugging dar	09-QoS 命令	3-4
debugging detect-group	01-基础配置命令	3-1
debugging dhcp client	03-网络层协议命令	5-43
debugging dhcp relay	03-网络层协议命令	5-46
debugging dhcp server	03-网络层协议命令	5-5
debugging dns	03-网络层协议命令	2-9
debugging dnsc	07-安全命令	13-17

debugging dvpn	06-VPN 命令	5-4
debugging encrypt-card host	06-VPN 命令	3-42
debugging firewall blacklist	07-安全命令	4-25
debugging firewall defend	07-安全命令	11-1
debugging firewall eff	07-安全命令	6-2
debugging firewall eff	07-安全命令	7-13
debugging firewall mac-binding	07-安全命令	4-28
debugging firewall packet-filter	07-安全命令	4-1
debugging firewall packet-filter fragments-inspect events	07-安全命令	4-2
debugging firewall smtp-filter	07-安全命令	10-20
debugging firewall transparent-mode eth-forwarding	07-安全命令	6-4
debugging firewall transparent-mode ip-forwarding	07-安全命令	6-5
debugging firewall url-filter host	07-安全命令	10-1
debugging firewall url-filter parameter	07-安全命令	10-1
debugging firewall webdata-filter	07-安全命令	10-2
debugging flowlog	07-安全命令	13-19
debugging hwping	01-基础配置命令	4-3
debugging hwtacacs	07-安全命令	1-48
debugging ids-acl	07-安全命令	12-3
debugging ike	06-VPN 命令	4-2
debugging ike dpd	06-VPN 命令	3-2
debugging ip	03-网络层协议命令	6-1
debugging ip urpf	03-网络层协议命令	2-17
debugging ipsec	06-VPN 命令	3-2
debugging l2tp	06-VPN 命令	1-2
debugging local-server	07-安全命令	1-21
debugging modem	01-基础配置命令	12-1
debugging mpls ldp	05-MPLS 命令	2-1
debugging mpls lspm	05-MPLS 命令	1-1
debugging nat	07-安全命令	3-4
debugging ntp-service	01-基础配置命令	7-1
debugging object dns	07-安全命令	5-2
debugging ospf	04-路由协议命令	3-4
debugging physical	01-基础配置命令	13-1

debugging pki	07-安全命令	8-17
debugging ppp { all | cbcp | ccp | scp }	02-用户接入命令	1-1
debugging ppp { chap | compression | pap | vjcomp packet }	02-用户接入命令	1-2
debugging ppp { core | ip | ipcp | lcp | lqc | mp }	02-用户接入命令	1-3
debugging ppp compression iphc rtp	02-用户接入命令	1-13
debugging ppp compression iphc tcp	02-用户接入命令	1-13
debugging pppoe-client	02-用户接入命令	3-1
debugging qos cbq	09-QoS 命令	2-16
debugging radius	07-安全命令	1-22
debugging rdmp	08-可靠性命令	2-2
debugging rip	04-路由协议命令	2-2
debugging smtpc	07-安全命令	13-14
debugging snmp-agent	01-基础配置命令	8-1
debugging ssh client	01-基础配置命令	11-7
debugging ssh server	01-基础配置命令	11-7
debugging ssl card	07-安全命令	9-7
debugging ssl proxy	07-安全命令	9-14
debugging ssl server	07-安全命令	9-3
debugging tcp event	03-网络层协议命令	6-2
debugging tcp md5	03-网络层协议命令	6-3
debugging tcp packet	03-网络层协议命令	6-4
debugging telnet	01-基础配置命令	11-1
debugging tunnel	06-VPN 命令	2-1
debugging udp packet	03-网络层协议命令	6-5
debugging udp-helper	03-网络层协议命令	3-1
debugging vrrp	08-可靠性命令	1-1
debugging vty	01-基础配置命令	6-4
default cost	04-路由协议命令	2-2
default cost	04-路由协议命令	3-5
default interval	04-路由协议命令	3-6
default limit	04-路由协议命令	3-6
default local-preference	04-路由协议命令	4-8
default med	04-路由协议命令	4-9
default tag	04-路由协议命令	3-7

default type	04-路由协议命令	3-7
default-cost	04-路由协议命令	3-8
default-route imported	04-路由协议命令	4-7
default-route-advertise	04-路由协议命令	3-9
delete	01-基础配置命令	5-3
delete	01-基础配置命令	5-24
delete	01-基础配置命令	11-33
delete static-routes all	04-路由协议命令	1-13
description	01-基础配置命令	4-3
description	01-基础配置命令	13-2
description	06-VPN 命令	6-2
description	07-安全命令	2-2
destination	06-VPN 命令	2-1
destination-ip	01-基础配置命令	4-4
destination-port	01-基础配置命令	4-4
detach	01-基础配置命令	5-4
detect	01-基础配置命令	13-17
detect	07-安全命令	4-11
detect http	07-安全命令	4-12
detect-group	01-基础配置命令	3-1
detect-list	01-基础配置命令	3-2
dh	06-VPN 命令	4-3
dhcp enable	03-网络层协议命令	5-1
dhcp relay release	03-网络层协议命令	5-47
dhcp select （接口视图）	03-网络层协议命令	5-1
dhcp select interface（系统视图）	03-网络层协议命令	5-2
dhcp server accounting domain（接口视图）	03-网络层协议命令	5-8
dhcp server accounting domain（系统视图）	03-网络层协议命令	5-7
dhcp server bims-server （接口视图）	03-网络层协议命令	5-8
dhcp server bims-server （系统视图）	03-网络层协议命令	5-9
dhcp server detect	03-网络层协议命令	5-3
dhcp server dns-list （接口视图）	03-网络层协议命令	5-10
dhcp server dns-list（系统视图）	03-网络层协议命令	5-11
dhcp server domain-name（接口视图）	03-网络层协议命令	5-11

dhcp server domain-name（系统视图）	03-网络层协议命令	5-12
dhcp server expired （接口视图）	03-网络层协议命令	5-13
dhcp server expired（系统视图）	03-网络层协议命令	5-14
dhcp server forbidden-ip	03-网络层协议命令	5-14
dhcp server ip-pool	03-网络层协议命令	5-15
dhcp server nbns-list （系统视图）	03-网络层协议命令	5-16
dhcp server nbns-list（接口视图）	03-网络层协议命令	5-17
dhcp server netbios-type（接口视图）	03-网络层协议命令	5-18
dhcp server netbios-type（系统视图）	03-网络层协议命令	5-18
dhcp server option（接口视图）	03-网络层协议命令	5-20
dhcp server option（系统视图）	03-网络层协议命令	5-19
dhcp server ping	03-网络层协议命令	5-21
dhcp server static-bind	03-网络层协议命令	5-22
dhcp server voice-config（接口视图）	03-网络层协议命令	5-22
dhcp server voice-config（系统视图）	03-网络层协议命令	5-24
dialer bundle	02-用户接入命令	3-2
dialer enable-circular	02-用户接入命令	3-1
dialer user	02-用户接入命令	3-4
dialer-group	02-用户接入命令	3-2
dialer-rule	02-用户接入命令	3-3
dir	01-基础配置命令	5-5
dir	01-基础配置命令	5-24
dir	01-基础配置命令	11-33
disconnect	01-基础配置命令	5-25
display acl	07-安全命令	2-3
display acl	07-安全命令	5-3
display arp	03-网络层协议命令	2-4
display aspf all	07-安全命令	4-13
display aspf interface	07-安全命令	4-14
display aspf policy	07-安全命令	4-15
display aspf session	07-安全命令	4-15
display aspf statistics	07-安全命令	4-17
display bgp group	04-路由协议命令	4-9
display bgp network	04-路由协议命令	4-10

display bgp paths	04-路由协议命令	4-11
display bgp peer	04-路由协议命令	4-12
display bgp routing	04-路由协议命令	4-15
display bgp routing as-path-acl	04-路由协议命令	4-16
display bgp routing cidr	04-路由协议命令	4-18
display bgp routing community	04-路由协议命令	4-19
display bgp routing community-list	04-路由协议命令	4-20
display bgp routing dampened	04-路由协议命令	4-21
display bgp routing different-origin-as	04-路由协议命令	4-22
display bgp routing flap-info	04-路由协议命令	4-23
display bgp routing label	06-VPN 命令	6-2
display bgp routing peer	04-路由协议命令	4-25
display bgp routing peer dampened	04-路由协议命令	4-26
display bgp routing peer regular-expression	04-路由协议命令	4-27
display bgp routing regular-expression	04-路由协议命令	4-28
display bgp routing statistic	04-路由协议命令	4-29
display bgp vpnv4	06-VPN 命令	6-3
display bootp client	03-网络层协议命令	4-1
display bridge address-table	07-安全命令	7-15
display bridge information	07-安全命令	7-16
display bridge traffic	07-安全命令	7-17
display brief interface	01-基础配置命令	13-2
display channel	01-基础配置命令	2-12
display clipboard	01-基础配置命令	1-4
display clock	01-基础配置命令	1-5
display command-alias	01-基础配置命令	1-21
display connection	07-安全命令	1-5
display connection-limit policy	07-安全命令	3-4
display connection-limit statistics	07-安全命令	3-5
display cpu-usage	01-基础配置命令	1-5
display cpu-usage history	01-基础配置命令	1-7
display current-configuration	01-基础配置命令	5-38
display dar information	09-QoS 命令	3-4
display dar protocol	09-QoS 命令	3-5

display dar protocol-rename	09-QoS 命令	3-7
display dar protocol-statistic	09-QoS 命令	3-8
display debugging	01-基础配置命令	2-2
display debugging ospf	04-路由协议命令	3-10
display detect-group	01-基础配置命令	3-3
display device	01-基础配置命令	2-2
display dhcp client	03-网络层协议命令	5-43
display dhcp relay address	03-网络层协议命令	5-47
display dhcp relay statistics	03-网络层协议命令	5-48
display dhcp server conflict	03-网络层协议命令	5-25
display dhcp server expired	03-网络层协议命令	5-26
display dhcp server free-ip	03-网络层协议命令	5-27
display dhcp server ip-in-use	03-网络层协议命令	5-27
display dhcp server statistics	03-网络层协议命令	5-29
display dhcp server tree	03-网络层协议命令	5-30
display diagnostic-information	01-基础配置命令	2-3
display dns domain	03-网络层协议命令	2-12
display dns dynamic-host	03-网络层协议命令	2-13
display dns server	03-网络层协议命令	2-12
display dnsc	07-安全命令	13-17
display domain	07-安全命令	1-7
display dvpn info	06-VPN 命令	5-7
display dvpn ipsec-sa	06-VPN 命令	5-5
display dvpn map	06-VPN 命令	5-6
display dvpn online-user	06-VPN 命令	5-9
display dvpn session	06-VPN 命令	5-7
display encrypt-card fast-switch	06-VPN 命令	3-43
display fib	03-网络层协议命令	6-5
display fib acl	03-网络层协议命令	6-6
display fib begin	03-网络层协议命令	6-7
display fib ip-prefix	03-网络层协议命令	6-8
display fib longer	03-网络层协议命令	6-9
display fib statistics	03-网络层协议命令	6-10
display firewall blacklist	07-安全命令	4-26

display firewall defend flag	07-安全命令	11-1
display firewall ethernet-frame-filter	07-安全命令	6-7
display firewall ethernet-frame-filter	07-安全命令	7-19
display firewall fragment	07-安全命令	4-2
display firewall mac-binding	07-安全命令	4-28
display firewall mode	07-安全命令	6-8
display firewall packet-filter statistics	07-安全命令	4-3
display firewall session aging-time	07-安全命令	4-18
display firewall session table	07-安全命令	4-18
display firewall smtp-filter	07-安全命令	10-20
display firewall statistic	07-安全命令	13-1
display firewall statistic system defend	07-安全命令	13-3
display firewall statistic system flow-percent	07-安全命令	13-4
display firewall tcp-proxy session	07-安全命令	11-2
display firewall transparent-mode address-table	07-安全命令	6-8
display firewall transparent-mode config	07-安全命令	6-9
display firewall transparent-mode traffic	07-安全命令	6-10
display firewall url-filter host	07-安全命令	10-3
display firewall url-filter parameter	07-安全命令	10-3
display firewall url-filter parameter counter detail	07-安全命令	10-4
display firewall webdata-filter	07-安全命令	10-5
display ftp source-ip	01-基础配置命令	5-25
display ftp-server	01-基础配置命令	5-15
display ftp-server source-ip	01-基础配置命令	5-16
display ftp-user	01-基础配置命令	5-15
display history-command	01-基础配置命令	1-8
display hwping	01-基础配置命令	4-5
display hwtacacs scheme	07-安全命令	1-49
display icmp statistics	03-网络层协议命令	6-11
display ids	07-安全命令	12-1
display ids-acl	07-安全命令	12-2
display ike dpd	06-VPN 命令	3-3
display ike peer	06-VPN 命令	4-4
display ike proposal	06-VPN 命令	4-4

display ike sa	06-VPN 命令	4-5
display info-center	01-基础配置命令	2-14
display interface	01-基础配置命令	13-3
display interface bridge-template	07-安全命令	7-20
display interface encrypt	06-VPN 命令	3-44
display interface ethernet	01-基础配置命令	13-11
display interface looback	01-基础配置命令	13-28
display interface null	01-基础配置命令	13-29
display interface ssl-card	07-安全命令	9-8
display interface tunnel	06-VPN 命令	2-2
display interface virtual-template	01-基础配置命令	13-26
display interzone	07-安全命令	4-32
display ip as-path-acl	04-路由协议命令	4-30
display ip community-list	04-路由协议命令	4-30
display ip fast-forwarding cache	03-网络层协议命令	6-12
display ip host	03-网络层协议命令	2-8
display ip interface	03-网络层协议命令	1-1
display ip interface	03-网络层协议命令	6-13
display ip interface brief	03-网络层协议命令	6-14
display ip ip-prefix	04-路由协议命令	5-6
display ip policy	03-网络层协议命令	7-4
display ip policy setup	03-网络层协议命令	7-5
display ip policy statistic	03-网络层协议命令	7-6
display ip routing-table	04-路由协议命令	1-1
display ip routing-table acl	04-路由协议命令	1-2
display ip routing-table *ip-address*	04-路由协议命令	1-3
display ip routing-table *ip-address1 ip-address2*	04-路由协议命令	1-5
display ip routing-table ip-prefix	04-路由协议命令	1-6
display ip routing-table protocol	04-路由协议命令	1-7
display ip routing-table radix	04-路由协议命令	1-9
display ip routing-table statistics	04-路由协议命令	1-9
display ip routing-table verbose	04-路由协议命令	1-10
display ip routing-table vpn-instance	04-路由协议命令	1-12
display ip routing-table vpn-instance	06-VPN 命令	6-5

display ip socket	03-网络层协议命令	6-15
display ip statistics	03-网络层协议命令	6-16
display ip vpn-instance	06-VPN 命令	6-6
display ipsec fragment buffer-chain	06-VPN 命令	3-4
display ipsec fragment statistics	06-VPN 命令	3-5
display ipsec policy	06-VPN 命令	3-6
display ipsec policy-template	06-VPN 命令	3-9
display ipsec proposal	06-VPN 命令	3-10
display ipsec sa	06-VPN 命令	3-11
display ipsec statistics	06-VPN 命令	3-14
display ipsec tunnel	06-VPN 命令	3-15
display l2tp session	06-VPN 命令	1-3
display l2tp tunnel	06-VPN 命令	1-4
display l2tp user	06-VPN 命令	1-5
display local-server statistics	07-安全命令	1-23
display local-user	07-安全命令	1-8
display logbuffer	01-基础配置命令	2-15
display logbuffer summary	01-基础配置命令	2-17
display memory	01-基础配置命令	1-9
display memory	04-路由协议命令	6-1
display mpls fast-forwarding cache	05-MPLS 命令	1-2
display mpls interface	05-MPLS 命令	1-2
display mpls l3vpn-lsp	06-VPN 命令	6-6
display mpls ldp	05-MPLS 命令	2-2
display mpls ldp buffer-info	05-MPLS 命令	2-2
display mpls ldp interface	05-MPLS 命令	2-3
display mpls ldp lsp	05-MPLS 命令	2-4
display mpls ldp peer	05-MPLS 命令	2-4
display mpls ldp remote	05-MPLS 命令	2-5
display mpls ldp session	05-MPLS 命令	2-5
display mpls lsp	05-MPLS 命令	1-3
display mpls static-lsp	05-MPLS 命令	1-3
display mpls statistics	05-MPLS 命令	1-4
display nat	07-安全命令	3-6

display nat connection-limit	07-安全命令	3-8
display ntp-service sessions	01-基础配置命令	7-2
display ntp-service status	01-基础配置命令	7-3
display ntp-service trace	01-基础配置命令	7-4
display object address	07-安全命令	5-3
display object address-group	07-安全命令	5-4
display object predefined service	07-安全命令	5-4
display object service	07-安全命令	5-5
display object service-group	07-安全命令	5-5
display ospf abr-asbr	04-路由协议命令	3-10
display ospf asbr-summary	04-路由协议命令	3-11
display ospf brief	04-路由协议命令	3-13
display ospf cumulative	04-路由协议命令	3-14
display ospf error	04-路由协议命令	3-16
display ospf interface	04-路由协议命令	3-19
display ospf lsdb	04-路由协议命令	3-20
display ospf nexthop	04-路由协议命令	3-22
display ospf peer	04-路由协议命令	3-23
display ospf request-queue	04-路由协议命令	3-25
display ospf retrans-queue	04-路由协议命令	3-26
display ospf routing	04-路由协议命令	3-27
display ospf sham-link	06-VPN 命令	6-7
display ospf vlink	04-路由协议命令	3-28
display pki certificate	07-安全命令	8-21
display pki certificate access-control-policy	07-安全命令	9-11
display pki certificate attribute-group	07-安全命令	9-12
display pki crl	07-安全命令	8-23
display port-mapping	07-安全命令	4-19
display ppp access-control	06-VPN 命令	1-6
display ppp compression iphc rtp	02-用户接入命令	1-14
display ppp compression iphc tcp	02-用户接入命令	1-14
display ppp compression stac-lzs	02-用户接入命令	1-15
display pppoe-client session	02-用户接入命令	3-5
display pppoe-server session	02-用户接入命令	2-1

display qos car interface	09-QoS 命令	1-1
display qos carl	09-QoS 命令	1-2
display qos cbq interface	09-QoS 命令	2-17
display qos cq interface	09-QoS 命令	2-7
display qos cql	09-QoS 命令	2-8
display qos gts interface	09-QoS 命令	1-5
display qos lr interface	09-QoS 命令	1-6
display qos policy	09-QoS 命令	2-17
display qos policy interface	09-QoS 命令	2-19
display qos pq interface	09-QoS 命令	2-1
display qos pql	09-QoS 命令	2-2
display qos rtpq interface	09-QoS 命令	2-42
display qos wfq interface	09-QoS 命令	2-13
display qos wred interface	09-QoS 命令	4-1
display radius scheme	07-安全命令	1-23
display radius statistics	07-安全命令	1-25
display rdo	08-可靠性命令	2-3
display rdo *rdo-id*	08-可靠性命令	2-4
display rdo sync-modules	08-可靠性命令	2-6
display rip	04-路由协议命令	2-3
display rip interface	04-路由协议命令	2-4
display rip routing	04-路由协议命令	2-5
display rmon alarm	01-基础配置命令	10-1
display rmon event	01-基础配置命令	10-2
display rmon eventlog	01-基础配置命令	10-3
display rmon history	01-基础配置命令	10-3
display rmon prialarm	01-基础配置命令	10-5
display rmon statistics	01-基础配置命令	10-6
display route-policy	04-路由协议命令	5-6
display rsa local-key-pair public	01-基础配置命令	11-8
display rsa peer-public-key	01-基础配置命令	11-10
display saved-configuration	01-基础配置命令	5-41
display schedule reboot	01-基础配置命令	2-5
display sftp source-ip	01-基础配置命令	11-34

display smtpc	07-安全命令	13-15
display snmp-agent	01-基础配置命令	8-1
display snmp-agent community	01-基础配置命令	8-2
display snmp-agent group	01-基础配置命令	8-3
display snmp-agent mib-view	01-基础配置命令	8-4
display snmp-agent statistics	01-基础配置命令	8-5
display snmp-agent sys-info	01-基础配置命令	8-7
display snmp-agent usm-user	01-基础配置命令	8-8
display ssh server	01-基础配置命令	11-10
display ssh server-info	01-基础配置命令	11-25
display ssh user-information	01-基础配置命令	11-12
display ssh2 source-ip	01-基础配置命令	11-26
display ssh-server source-ip	01-基础配置命令	11-11
display ssl proxy	07-安全命令	9-15
display ssl server-policy	07-安全命令	9-4
display ssl-proxy session	07-安全命令	9-16
display startup	01-基础配置命令	5-44
display stop-accounting-buffer	07-安全命令	1-29
display stop-accounting-buffer	07-安全命令	1-51
display tcp statistics	03-网络层协议命令	6-17
display tcp status	01-基础配置命令	11-1
display tcp status	03-网络层协议命令	6-19
display telnet source-ip	01-基础配置命令	11-2
display telnet-server source-ip	01-基础配置命令	11-3
display tftp source-ip	01-基础配置命令	5-35
display this	01-基础配置命令	5-44
display time-range	07-安全命令	2-9
display traffic behavior	09-QoS 命令	2-21
display traffic classifier	09-QoS 命令	2-22
display trapbuffer	01-基础配置命令	2-18
display udp statistics	03-网络层协议命令	6-20
display udp-helper server	03-网络层协议命令	3-1
display user-interface	01-基础配置命令	6-5
display users	01-基础配置命令	6-6

display version	01-基础配置命令	1-9
display virtual-access	01-基础配置命令	13-27
display vlan interface	01-基础配置命令	13-18
display vlan interface	02-用户接入命令	4-1
display vlan max-packet-process	01-基础配置命令	13-18
display vlan max-packet-process	02-用户接入命令	4-1
display vlan statistics vid	01-基础配置命令	13-19
display vlan statistics vid	02-用户接入命令	4-2
display vrrp	08-可靠性命令	1-1
display zone	07-安全命令	4-32
dns domain	03-网络层协议命令	2-11
dns resolve	03-网络层协议命令	2-10
dns server	03-网络层协议命令	2-10
dnsc cache	07-安全命令	13-19
dnsc server	07-安全命令	13-18
dns-list	03-网络层协议命令	5-33
dns-proxy enable	03-网络层协议命令	2-15
domain	07-安全命令	1-9
domain-id	06-VPN 命令	6-8
domain-name	03-网络层协议命令	5-33
dpd	06-VPN 命令	3-16
duplex	01-基础配置命令	13-12
dvpn class	06-VPN 命令	5-9
dvpn client register-dumb	06-VPN 命令	5-10
dvpn client register-interval	06-VPN 命令	5-10
dvpn client register-retry	06-VPN 命令	5-11
dvpn dvpn-id	06-VPN 命令	5-11
dvpn interface-type	06-VPN 命令	5-12
dvpn policy（Tunnel 接口视图）	06-VPN 命令	5-13
dvpn policy（系统视图）	06-VPN 命令	5-13
dvpn register-type	06-VPN 命令	5-14
dvpn security	06-VPN 命令	5-15
dvpn server	06-VPN 命令	5-15
dvpn server authentication-client method	06-VPN 命令	5-16

dvpn server map age-time	06-VPN 命令	5-17
dvpn server pre-shared-key	06-VPN 命令	5-17
dvpn service enable	06-VPN 命令	5-18

E

enable snmp trap updown	01-基础配置命令	8-9
encapsulation-mode	06-VPN 命令	3-16
encrypt-card backuped	06-VPN 命令	3-45
encrypt-card fast-switch	06-VPN 命令	3-45
encryption-algorithm	06-VPN 命令	4-6
esp authentication-algorithm	06-VPN 命令	3-17
esp encryption-algorithm	06-VPN 命令	3-18
exchange-mode	06-VPN 命令	4-7
execute	01-基础配置命令	5-6
exit	01-基础配置命令	11-34
expired	03-网络层协议命令	5-34

F

file prompt	01-基础配置命令	5-6
filename	01-基础配置命令	4-7
filter-policy export	04-路由协议命令	2-6
filter-policy export	04-路由协议命令	3-29
filter-policy export	04-路由协议命令	4-31
filter-policy export	04-路由协议命令	5-7
filter-policy import	04-路由协议命令	2-7
filter-policy import	04-路由协议命令	3-30
filter-policy import	04-路由协议命令	4-31
filter-policy import	04-路由协议命令	5-7
firewall arp-learning enable	07-安全命令	6-12
firewall aspf	07-安全命令	4-20
firewall binary-log host	07-安全命令	13-20
firewall blacklist	07-安全命令	4-27
firewall defend all	07-安全命令	11-4
firewall defend arp-flood	07-安全命令	11-4

firewall defend arp-spoofing	07-安全命令	11-5
firewall defend frag-flood	07-安全命令	11-6
firewall defend fraggle	07-安全命令	11-5
firewall defend icmp-flood	07-安全命令	11-7
firewall defend icmp-flood enable	07-安全命令	11-8
firewall defend icmp-redirect	07-安全命令	11-8
firewall defend icmp-unreachable	07-安全命令	11-9
firewall defend ip-fragment	07-安全命令	11-9
firewall defend ip-spoofing	07-安全命令	11-10
firewall defend ip-sweep	07-安全命令	11-10
firewall defend land	07-安全命令	11-11
firewall defend large-icmp	07-安全命令	11-12
firewall defend ping-of-death	07-安全命令	11-12
firewall defend port-scan	07-安全命令	11-13
firewall defend route-record	07-安全命令	11-14
firewall defend smurf	07-安全命令	11-14
firewall defend source-route	07-安全命令	11-15
firewall defend syn-flood	07-安全命令	11-15
firewall defend syn-flood enable	07-安全命令	11-16
firewall defend tcp-flag	07-安全命令	11-17
firewall defend teardrop	07-安全命令	11-18
firewall defend tracert	07-安全命令	11-18
firewall defend udp-flood	07-安全命令	11-19
firewall defend udp-flood enable	07-安全命令	11-20
firewall defend winnuke	07-安全命令	11-20
firewall ethernet-frame-filter	07-安全命令	6-12
firewall ethernet-frame-filter	07-安全命令	7-21
firewall interzone	07-安全命令	4-34
firewall log-time	07-安全命令	13-21
firewall mac-binding	07-安全命令	4-30
firewall mac-binding enable	07-安全命令	4-30
firewall mode	07-安全命令	6-13
firewall nat log-type	07-安全命令	13-21
firewall packet-filter *acl-name*	07-安全命令	5-12

firewall packet-filter *acl-number*	07-安全命令	4-6
firewall packet-filter default	07-安全命令	4-3
firewall packet-filter enable	07-安全命令	4-4
firewall packet-filter fragments-inspect	07-安全命令	4-4
firewall packet-filter fragments-inspect { high | low }	07-安全命令	4-5
firewall session aging-time	07-安全命令	4-21
firewall session aging-time default	07-安全命令	4-22
firewall session log-threshold	07-安全命令	13-22
firewall session log-type	07-安全命令	13-23
firewall smtp-filter attach add	07-安全命令	10-21
firewall smtp-filter attach clear	07-安全命令	10-22
firewall smtp-filter attach delete	07-安全命令	10-22
firewall smtp-filter attach enable	07-安全命令	10-23
firewall smtp-filter attach load-file	07-安全命令	10-23
firewall smtp-filter attach save-file	07-安全命令	10-24
firewall smtp-filter content add	07-安全命令	10-24
firewall smtp-filter content clear	07-安全命令	10-25
firewall smtp-filter content delete	07-安全命令	10-25
firewall smtp-filter content enable	07-安全命令	10-26
firewall smtp-filter content load-file	07-安全命令	10-27
firewall smtp-filter content save-file	07-安全命令	10-27
firewall smtp-filter rcptto add	07-安全命令	10-28
firewall smtp-filter rcptto clear	07-安全命令	10-29
firewall smtp-filter rcptto default	07-安全命令	10-29
firewall smtp-filter rcptto delete	07-安全命令	10-30
firewall smtp-filter rcptto enable	07-安全命令	10-30
firewall smtp-filter rcptto load-file	07-安全命令	10-31
firewall smtp-filter rcptto save-file	07-安全命令	10-31
firewall smtp-filter subject add	07-安全命令	10-32
firewall smtp-filter subject clear	07-安全命令	10-32
firewall smtp-filter subject delete	07-安全命令	10-33
firewall smtp-filter subject enable	07-安全命令	10-33
firewall smtp-filter subject load-file	07-安全命令	10-34
firewall smtp-filter subject save-file	07-安全命令	10-34

firewall statistic system connect-number	07-安全命令	13-5
firewall statistic system enable	07-安全命令	13-6
firewall statistic system flow-percent	07-安全命令	13-6
firewall statistic warning-level drop	07-安全命令	13-7
firewall system-ip	07-安全命令	6-14
firewall tcp-proxy	07-安全命令	11-21
firewall transparent-mode aging-time	07-安全命令	6-15
firewall transparent-mode transmit	07-安全命令	6-15
firewall unknown-mac	07-安全命令	6-16
firewall unknown-mac broadcast	07-安全命令	6-17
firewall unknown-mac multicast	07-安全命令	6-17
firewall unknown-mac unicast	07-安全命令	6-18
firewall url-filter host acl-number	07-安全命令	10-5
firewall url-filter host add	07-安全命令	10-6
firewall url-filter host clear	07-安全命令	10-7
firewall url-filter host default	07-安全命令	10-7
firewall url-filter host delete	07-安全命令	10-8
firewall url-filter host enable	07-安全命令	10-8
firewall url-filter host ip-address	07-安全命令	10-9
firewall url-filter host load-file	07-安全命令	10-10
firewall url-filter host save-file	07-安全命令	10-9
firewall url-filter parameter add	07-安全命令	10-10
firewall url-filter parameter add-default	07-安全命令	10-11
firewall url-filter parameter clear	07-安全命令	10-12
firewall url-filter parameter delete	07-安全命令	10-12
firewall url-filter parameter enable	07-安全命令	10-13
firewall url-filter parameter load-file	07-安全命令	10-14
firewall url-filter parameter save-file	07-安全命令	10-14
firewall webdata-filter add	07-安全命令	10-15
firewall webdata-filter clear	07-安全命令	10-16
firewall webdata-filter delete	07-安全命令	10-16
firewall webdata-filter enable	07-安全命令	10-16
firewall webdata-filter load-file	07-安全命令	10-17
firewall webdata-filter save-file	07-安全命令	10-18

firewall zone	07-安全命令	4-34
firewall zone name	07-安全命令	4-35
flow-control	01-基础配置命令	6-7
flow-control	01-基础配置命令	13-13
flow-interval	01-基础配置命令	13-5
format	01-基础配置命令	5-7
fqdn	07-安全命令	8-8
free user-interface	01-基础配置命令	6-8
frequency	01-基础配置命令	4-8
ftp	01-基础配置命令	5-26
ftp server enable	01-基础配置命令	5-16
ftp source-interface	01-基础配置命令	5-26
ftp source-ip	01-基础配置命令	5-27
ftp timeout	01-基础配置命令	5-18
ftp update	01-基础配置命令	5-19
ftp-operation	01-基础配置命令	4-8
ftp-server source-interface	01-基础配置命令	5-17
ftp-server source-ip	01-基础配置命令	5-18

G

gateway-list	03-网络层协议命令	5-35
get	01-基础配置命令	5-28
get	01-基础配置命令	11-35
gratuitous-arp-learning enable	03-网络层协议命令	2-5
gratuitous-arp-sending enable	03-网络层协议命令	2-6
gre checksum	06-VPN 命令	2-4
gre key	06-VPN 命令	2-4
group	04-路由协议命令	4-32
gts	09-QoS 命令	2-22

H

ha-interface	08-可靠性命令	2-7
handshake timeout	07-安全命令	9-5
header	01-基础配置命令	1-10

help	01-基础配置命令	11-35
history-command max-size	01-基础配置命令	6-8
history-records	01-基础配置命令	4-9
host-route	04-路由协议命令	2-8
hotkey	01-基础配置命令	1-12
http-operation	01-基础配置命令	4-9
hwping	01-基础配置命令	4-10
hwping-agent enable	01-基础配置命令	4-11
hwping-agent max-requests	01-基础配置命令	4-11
hwping-server enable	01-基础配置命令	4-22
hwping-server tcpconnect	01-基础配置命令	4-23
hwping-server udpecho	01-基础配置命令	4-23
hwtacacs nas-ip	07-安全命令	1-52
hwtacacs scheme	07-安全命令	1-53

I

icmp redirect send	03-网络层协议命令	6-21
idle-timeout	01-基础配置命令	6-9
ids-acl enable	07-安全命令	12-1
id-type	06-VPN 命令	4-8
if-match { destination-mac | source-mac }	09-QoS 命令	2-23
if-match acl	03-网络层协议命令	7-6
if-match acl	04-路由协议命令	5-8
if-match acl	09-QoS 命令	2-24
if-match any	09-QoS 命令	2-24
if-match as-path	04-路由协议命令	5-9
if-match classifier	09-QoS 命令	2-25
if-match community	04-路由协议命令	5-10
if-match cost	04-路由协议命令	5-10
if-match dscp	09-QoS 命令	2-26
if-match inbound-interface	09-QoS 命令	2-27
if-match interface	04-路由协议命令	5-11
if-match ip next-hop	04-路由协议命令	5-12
if-match ip-precedence	09-QoS 命令	2-28

if-match ip-prefix	04-路由协议命令	5-13
if-match mpls-exp	09-QoS 命令	5-1
if-match mpls-label	06-VPN 命令	6-9
if-match packet-length	03-网络层协议命令	7-7
if-match protocol	09-QoS 命令	2-29
if-match protocol	09-QoS 命令	3-9
if-match protocol http	09-QoS 命令	3-10
if-match protocol rtp	09-QoS 命令	3-10
if-match rtp	09-QoS 命令	2-29
if-match tag	04-路由协议命令	5-13
ike dpd	06-VPN 命令	3-19
ike encrypt-card dh-computation disabled	06-VPN 命令	4-9
ike local-name	06-VPN 命令	4-9
ike next-payload check disabled	06-VPN 命令	4-10
ike peer	06-VPN 命令	4-10
ike proposal	06-VPN 命令	4-11
ike sa keepalive-timer interval	06-VPN 命令	4-13
ike sa keepalive-timer timeout	06-VPN 命令	4-13
ike sa nat-keepalive-timer interval	06-VPN 命令	4-14
ike-peer	06-VPN 命令	4-11
import-route	04-路由协议命令	2-9
import-route	04-路由协议命令	3-31
import-route	04-路由协议命令	4-33
import-route ospf	06-VPN 命令	6-9
info-center channel	01-基础配置命令	2-19
info-center console channel	01-基础配置命令	2-20
info-center enable	01-基础配置命令	2-20
info-center logbuffer	01-基础配置命令	2-21
info-center loghost	01-基础配置命令	2-22
info-center loghost source	01-基础配置命令	2-23
info-center monitor channel	01-基础配置命令	2-24
info-center snmp channel	01-基础配置命令	2-24
info-center source	01-基础配置命令	2-25
info-center timestamp	01-基础配置命令	2-27

info-center timestamp loghost	01-基础配置命令	2-28
info-center trapbuffer	01-基础配置命令	2-28
insulate	01-基础配置命令	13-6
interface	01-基础配置命令	13-8
interface { ethernet | gigabitethernet }	01-基础配置命令	13-19
interface bridge-template	07-安全命令	7-21
interface dialer	01-基础配置命令	13-22
interface dialer	02-用户接入命令	3-7
interface encrypt	06-VPN 命令	3-46
interface loopback	01-基础配置命令	13-29
interface null	01-基础配置命令	13-30
interface tunnel	06-VPN 命令	2-5
interface virtual-template	01-基础配置命令	13-27
interface virtual-template	06-VPN 命令	1-7
interval-time	06-VPN 命令	3-20
ip	07-安全命令	8-10
ip address	03-网络层协议命令	1-1
ip address bootp-alloc	03-网络层协议命令	4-2
ip address dhcp-alloc	03-网络层协议命令	5-45
ip address ppp-negotiate	03-网络层协议命令	1-3
ip address unnumbered	03-网络层协议命令	1-3
ip as-path-acl	04-路由协议命令	4-34
ip binding vpn-instance	06-VPN 命令	6-10
ip community-list	04-路由协议命令	4-35
ip fast-forwarding	03-网络层协议命令	6-22
ip host	03-网络层协议命令	2-8
ip http acl	01-基础配置命令	2-32
ip http shutdown	01-基础配置命令	2-33
ip ip-prefix	04-路由协议命令	5-14
ip local policy route-policy	03-网络层协议命令	7-8
ip policy route-policy	03-网络层协议命令	7-8
ip pool	07-安全命令	1-11
ip relay address	03-网络层协议命令	5-49
ip relay address cycle	03-网络层协议命令	5-50

ip relay address interface	03-网络层协议命令	5-50
ip route-static	04-路由协议命令	1-14
ip route-static detect-group	01-基础配置命令	3-7
ip route-static vpn-instance	06-VPN 命令	6-11
ip tcp vjcompress	02-用户接入命令	1-16
ip urpf	03-网络层协议命令	2-16
ip vpn-instance	06-VPN 命令	6-12
ipsec card-proposal	06-VPN 命令	3-47
ipsec fragment-chain	06-VPN 命令	3-20
ipsec fragment-chain timeout	06-VPN 命令	3-21
ipsec policy（接口视图）	06-VPN 命令	3-21
ipsec policy（系统视图）	06-VPN 命令	3-22
ipsec policy-template	06-VPN 命令	3-24
ipsec proposal	06-VPN 命令	3-25
ipsec sa global-duration	06-VPN 命令	3-26
ipv4-family	04-路由协议命令	4-58
ipv4-family	06-VPN 命令	6-12
ipv4-family vpn-instance	04-路由协议命令	2-10
ipv4-family vpnv4	04-路由协议命令	4-59

J

jitter-interval	01-基础配置命令	4-12
jitter-packetnum	01-基础配置命令	4-12

K

keepalive	06-VPN 命令	2-6
key	07-安全命令	1-30
key	07-安全命令	1-53

L

l2tp enable	06-VPN 命令	1-8
l2tp-auto-client enable	06-VPN 命令	1-8
l2tp-group	06-VPN 命令	1-9
l2tpmoreexam enable	06-VPN 命令	1-9

language-mode	01-基础配置命令	1-13
lcd	01-基础配置命令	5-28
ldap-server	07-安全命令	8-6
level	07-安全命令	1-12
limit	07-安全命令	3-9
link-protocol ppp	02-用户接入命令	1-4
local	06-VPN 命令	4-15
local-address	06-VPN 命令	4-15
locality	07-安全命令	8-11
local-server	07-安全命令	1-31
local-user	06-VPN 命令	5-19
local-user	07-安全命令	1-12
local-user password-display-mode	07-安全命令	1-13
lock	01-基础配置命令	1-14
log enable	07-安全命令	4-22
log-peer-change	04-路由协议命令	3-32
log-peer-change	04-路由协议命令	4-36
loopback	01-基础配置命令	13-17
loopback (Ethernet/Gigabitethernet Interface)	01-基础配置命令	13-14
ls	01-基础配置命令	5-29
ls	01-基础配置命令	11-36
lsp-trigger	05-MPLS 命令	1-6

M

mac-address	07-安全命令	7-22
mandatory-chap	06-VPN 命令	1-10
mandatory-lcp	06-VPN 命令	1-11
max-packet-process	01-基础配置命令	13-20
max-packet-process	02-用户接入命令	4-2
memory	04-路由协议命令	6-3
memory auto-establish disable	04-路由协议命令	6-2
memory auto-establish enable	04-路由协议命令	6-3
mkdir	01-基础配置命令	5-8
mkdir	01-基础配置命令	5-29

mkdir	01-基础配置命令	11-37
modem	01-基础配置命令	6-10
modem	01-基础配置命令	12-1
modem auto-answer	01-基础配置命令	6-10
modem auto-answer	01-基础配置命令	12-2
modem timer answer	01-基础配置命令	6-11
more	01-基础配置命令	5-8
move	01-基础配置命令	5-9
mpls	05-MPLS 命令	1-6
mpls ldp	05-MPLS 命令	2-6
mpls ldp enable	05-MPLS 命令	2-6
mpls ldp hops-count	05-MPLS 命令	2-7
mpls ldp loop-detect	05-MPLS 命令	2-8
mpls ldp password	05-MPLS 命令	2-8
mpls ldp path-vectors	05-MPLS 命令	2-9
mpls ldp remote-peer	05-MPLS 命令	2-10
mpls ldp reset-session	05-MPLS 命令	2-10
mpls ldp timer	05-MPLS 命令	2-11
mpls ldp timer targeted-hello	05-MPLS 命令	2-12
mpls ldp timer targeted-session-hold	05-MPLS 命令	2-12
mpls ldp transport-ip	05-MPLS 命令	2-13
mpls lsr-id	05-MPLS 命令	1-7
mtu	01-基础配置命令	13-9
multi-path-number	04-路由协议命令	3-33

N

nas-ip	07-安全命令	1-32
nas-ip	07-安全命令	1-54
nat address-group	07-安全命令	3-10
nat aging-time	07-安全命令	3-11
nat alg	07-安全命令	3-12
nat connection-limit-policy	07-安全命令	3-13
nat dns-map	07-安全命令	3-13
nat match factor-all	07-安全命令	3-14

nat outbound *acl-name*	07-安全命令	5-12
nat outbound *acl-number*	07-安全命令	3-15
nat outbound interface	07-安全命令	3-16
nat outbound static	07-安全命令	3-17
nat overlapaddress	07-安全命令	3-17
nat server	07-安全命令	3-18
nat session refresh-speed	07-安全命令	3-21
nat static	07-安全命令	3-21
nat static inside	07-安全命令	3-22
nat traversal	06-VPN 命令	4-16
naturemask-arp	03-网络层协议命令	2-7
nbns-list	03-网络层协议命令	5-35
netbios-type	03-网络层协议命令	5-36
network	03-网络层协议命令	5-37
network	04-路由协议命令	2-10
network	04-路由协议命令	3-34
network	04-路由协议命令	4-37
nslookup type	03-网络层协议命令	2-14
nssa	04-路由协议命令	3-34
ntp-service access	01-基础配置命令	7-5
ntp-service authentication enable	01-基础配置命令	7-6
ntp-service authentication-keyid	01-基础配置命令	7-6
ntp-service broadcast-client	01-基础配置命令	7-7
ntp-service broadcast-server	01-基础配置命令	7-7
ntp-service in-interface disable	01-基础配置命令	7-8
ntp-service max-dynamic-sessions	01-基础配置命令	7-9
ntp-service multicast-client	01-基础配置命令	7-9
ntp-service multicast-server	01-基础配置命令	7-10
ntp-service refclock-master	01-基础配置命令	7-11
ntp-service reliable authentication-keyid	01-基础配置命令	7-11
ntp-service source-interface	01-基础配置命令	7-12
ntp-service unicast-peer	01-基础配置命令	7-13
ntp-service unicast-server	01-基础配置命令	7-14

O

object address	07-安全命令	5-6
object address-group	07-安全命令	5-7
object refresh dns	07-安全命令	5-7
object service	07-安全命令	5-8
object service-group	07-安全命令	5-9
open	01-基础配置命令	5-30
option	01-基础配置命令	3-4
option	03-网络层协议命令	5-38
organization	07-安全命令	8-11
organization-unit	07-安全命令	8-12
ospf	04-路由协议命令	3-35
ospf authentication-mode	04-路由协议命令	3-36
ospf cost	04-路由协议命令	3-37
ospf dr-priority	04-路由协议命令	3-38
ospf mib-binding	04-路由协议命令	3-38
ospf mtu-enable	04-路由协议命令	3-39
ospf network-type	04-路由协议命令	3-40
ospf timer dead	04-路由协议命令	3-41
ospf timer hello	04-路由协议命令	3-41
ospf timer poll	04-路由协议命令	3-42
ospf timer retransmit	04-路由协议命令	3-43
ospf trans-delay	04-路由协议命令	3-43
ospf vpn-instance	06-VPN 命令	6-13

P

parity	01-基础配置命令	6-11
passive	01-基础配置命令	5-30
password	01-基础配置命令	4-13
password	07-安全命令	1-14
peer	04-路由协议命令	2-11
peer	04-路由协议命令	3-44
peer	06-VPN 命令	4-17

peer advertise-community	04-路由协议命令	4-37
peer allow-as-loop	04-路由协议命令	4-38
peer as-number	04-路由协议命令	4-38
peer as-path-acl	04-路由协议命令	4-39
peer connect-interface	04-路由协议命令	4-40
peer default-route-advertise	04-路由协议命令	4-40
peer default-route-advertise	06-VPN 命令	6-15
peer description	04-路由协议命令	4-41
peer ebgp-max-hop	04-路由协议命令	4-42
peer enable	04-路由协议命令	4-42
peer enable	04-路由协议命令	4-60
peer filter-policy	04-路由协议命令	4-43
peer group	04-路由协议命令	4-44
peer ip-prefix	04-路由协议命令	4-45
peer label-route-capability	06-VPN 命令	6-16
peer next-hop-invariable	06-VPN 命令	6-16
peer next-hop-local	04-路由协议命令	4-46
peer password	04-路由协议命令	4-46
peer public-as-only	04-路由协议命令	4-47
peer reflect-client	04-路由协议命令	4-48
peer route-policy	04-路由协议命令	4-48
peer route-update-interval	04-路由协议命令	4-49
peer shutdown	04-路由协议命令	4-50
peer timer	04-路由协议命令	4-50
peer-public-key end	01-基础配置命令	11-12
pfs	06-VPN 命令	3-27
ping	01-基础配置命令	2-5
pki certificate access-control-policy	07-安全命令	9-12
pki certificate attribute-group	07-安全命令	9-13
pki delete-certificate	07-安全命令	8-13
pki domain	07-安全命令	8-7
pki entity	07-安全命令	8-13
pki import-certificate	07-安全命令	8-14
pki request-certificate	07-安全命令	8-14

pki retrieval-certificate	07-安全命令	8-15
pki retrieval-crl	07-安全命令	8-16
pki validate-certificate	07-安全命令	8-16
pki-domain	07-安全命令	9-5
policy vpn-target	06-VPN 命令	6-17
port	07-安全命令	9-16
port-mapping	07-安全命令	4-23
ppp access-control enable	06-VPN 命令	1-11
ppp access-control match-fragments	06-VPN 命令	1-12
ppp authentication-mode	02-用户接入命令	1-4
ppp chap password	02-用户接入命令	1-5
ppp chap user	02-用户接入命令	1-6
ppp compression iphc	02-用户接入命令	1-16
ppp compression iphc rtp-connections	02-用户接入命令	1-17
ppp compression iphc tcp-connections	02-用户接入命令	1-18
ppp compression stac-lzs	02-用户接入命令	1-18
ppp ipcp dns	02-用户接入命令	1-6
ppp ipcp dns admit-any	02-用户接入命令	1-7
ppp ipcp dns request	02-用户接入命令	1-9
ppp ipcp remote-address forced	02-用户接入命令	1-8
ppp lqc	02-用户接入命令	1-10
ppp pap local-user	02-用户接入命令	1-11
ppp timer negotiate	02-用户接入命令	1-11
pppoe-client	02-用户接入命令	3-7
pppoe-server bind virtual-template	02-用户接入命令	2-2
pppoe-server log-information off	02-用户接入命令	2-3
pppoe-server max-sessions local-mac	02-用户接入命令	2-3
pppoe-server max-sessions remote-mac	02-用户接入命令	2-4
pppoe-server max-sessions total	02-用户接入命令	2-4
preference	04-路由协议命令	2-12
preference	04-路由协议命令	3-45
preference	04-路由协议命令	4-51
pre-shared-key	06-VPN 命令	4-17
pre-shared-key	06-VPN 命令	5-20

primary accounting	07-安全命令	1-32
primary accounting	07-安全命令	1-55
primary authentication	07-安全命令	1-33
primary authentication	07-安全命令	1-55
primary authorization	07-安全命令	1-56
priority	08-可靠性命令	2-8
private-ip	06-VPN 命令	5-20
probe-failtimes	01-基础配置命令	4-14
promiscuous	01-基础配置命令	13-14
proposal	06-VPN 命令	3-28
protocol inbound	01-基础配置命令	6-12
protocol inbound	01-基础配置命令	11-13
public-ip	06-VPN 命令	5-19
public-key-code begin	01-基础配置命令	11-14
public-key-code end	01-基础配置命令	11-14
put	01-基础配置命令	5-31
put	01-基础配置命令	11-37
pwd	01-基础配置命令	5-10
pwd	01-基础配置命令	5-31
pwd	01-基础配置命令	11-38

Q

qos apply policy	09-QoS 命令	2-30
qos car	09-QoS 命令	1-2
qos carl	09-QoS 命令	1-4
qos cq	09-QoS 命令	2-8
qos cql default-queue	09-QoS 命令	2-9
qos cql inbound-interface	09-QoS 命令	2-10
qos cql protocol	09-QoS 命令	2-10
qos cql protocol mpls exp	09-QoS 命令	5-1
qos cql queue	09-QoS 命令	2-12
qos cql queue serving	09-QoS 命令	2-12
qos fifo queue-length	09-QoS 命令	2-1
qos gts	09-QoS 命令	1-5

qos lr	09-QoS 命令	1-7
qos max-bandwidth	09-QoS 命令	2-31
qos policy	09-QoS 命令	2-31
qos pq	09-QoS 命令	2-3
qos pql default-queue	09-QoS 命令	2-3
qos pql inbound-interface	09-QoS 命令	2-4
qos pql protocol	09-QoS 命令	2-5
qos pql protocol mpls exp	09-QoS 命令	5-2
qos pql queue	09-QoS 命令	2-6
qos reserved-bandwidth	09-QoS 命令	2-43
qos rtpq	09-QoS 命令	2-44
qos wfq	09-QoS 命令	2-14
qos wred	09-QoS 命令	4-2
qos wred dscp	09-QoS 命令	4-2
qos wred ip-precedence	09-QoS 命令	4-3
qos wred weighting-constant	09-QoS 命令	4-4
queue af	09-QoS 命令	2-32
queue ef	09-QoS 命令	2-33
queue wfq	09-QoS 命令	2-34
queue-length	09-QoS 命令	2-34
quit	01-基础配置命令	1-15
quit	01-基础配置命令	5-32
quit	01-基础配置命令	11-26
quit	01-基础配置命令	11-38

R

radius nas-ip	07-安全命令	1-35
radius scheme	07-安全命令	1-34
radius trap	07-安全命令	1-36
rdo	08-可靠性命令	2-9
reboot	01-基础配置命令	2-7
reflect between-clients	04-路由协议命令	4-52
reflector cluster-id	04-路由协议命令	4-52
refresh bgp	04-路由协议命令	4-53

remark dscp	09-QoS 命令	2-35
remark ip-precedence	09-QoS 命令	2-37
remark mpls-exp	09-QoS 命令	5-3
remote address	03-网络层协议命令	1-4
remote-address	06-VPN 命令	4-18
remotehelp	01-基础配置命令	5-32
remote-ip	05-MPLS 命令	2-14
remote-name	06-VPN 命令	4-18
remove	01-基础配置命令	11-39
remove slot	01-基础配置命令	2-8
rename	01-基础配置命令	5-10
rename	01-基础配置命令	5-33
rename	01-基础配置命令	11-39
reset	04-路由协议命令	2-12
reset acl counter	07-安全命令	2-3
reset acl counter	07-安全命令	5-10
reset arp	03-网络层协议命令	2-7
reset aspf session	07-安全命令	4-24
reset aspf statistic http	07-安全命令	4-24
reset bgp	04-路由协议命令	4-54
reset bgp dampening	04-路由协议命令	4-56
reset bgp flap-info	04-路由协议命令	4-55
reset bgp group	04-路由协议命令	4-55
reset bridge address-table	07-安全命令	7-23
reset bridge traffic	07-安全命令	7-23
reset counters interface	01-基础配置命令	13-10
reset counters interface encrypt	06-VPN 命令	3-48
reset dar protocol-statistic	09-QoS 命令	3-11
reset dar session	09-QoS 命令	3-12
reset dhcp relay statistics	03-网络层协议命令	5-51
reset dhcp server conflict	03-网络层协议命令	5-38
reset dhcp server ip-in-use	03-网络层协议命令	5-39
reset dhcp server statistics	03-网络层协议命令	5-39
reset dns dynamic-host	03-网络层协议命令	2-15

reset dvpn all	06-VPN 命令	5-21
reset dvpn map	06-VPN 命令	5-21
reset dvpn session	06-VPN 命令	5-22
reset dvpn statistics	06-VPN 命令	5-22
reset encrypt-card fast-switch	06-VPN 命令	3-48
reset encrypt-card sa	06-VPN 命令	3-49
reset encrypt-card statistics	06-VPN 命令	3-49
reset encrypt-card syslog	06-VPN 命令	3-50
reset firewall ethernet-frame-filter	07-安全命令	6-19
reset firewall ethernet-frame-filter	07-安全命令	7-24
reset firewall log-buf	07-安全命令	13-24
reset firewall mac-binding	07-安全命令	4-31
reset firewall packet-filter statistics	07-安全命令	4-7
reset firewall session table	07-安全命令	4-25
reset firewall smtp-filter counter	07-安全命令	10-35
reset firewall statistic ip	07-安全命令	13-8
reset firewall statistic system	07-安全命令	13-8
reset firewall statistic zone	07-安全命令	13-9
reset firewall transparent-mode address-table	07-安全命令	6-19
reset firewall transparent-mode traffic	07-安全命令	6-20
reset firewall url-filter host counter	07-安全命令	10-18
reset firewall url-filter parameter counter	07-安全命令	10-19
reset firewall webdata-filter counter	07-安全命令	10-19
reset hwtacacs statistics	07-安全命令	1-57
reset ike sa	06-VPN 命令	4-19
reset ip fast-forwarding cache	03-网络层协议命令	6-23
reset ip routing-table statistics protocol	04-路由协议命令	1-13
reset ip statistics	03-网络层协议命令	6-23
reset ipsec fragment buffer-chain	06-VPN 命令	3-29
reset ipsec fragment statistics	06-VPN 命令	3-29
reset ipsec sa	06-VPN 命令	3-29
reset ipsec statistics	06-VPN 命令	3-31
reset l2tp session	06-VPN 命令	1-13
reset l2tp tunnel	06-VPN 命令	1-13

reset l2tp user	06-VPN 命令	1-14
reset logbuffer	01-基础配置命令	2-29
reset mpls fast-forwarding cache	05-MPLS 命令	1-8
reset mpls statistics	05-MPLS 命令	1-8
reset nat	07-安全命令	3-23
reset ospf	04-路由协议命令	3-45
reset ppp compression iphc	02-用户接入命令	1-19
reset ppp compression stac-lzs	02-用户接入命令	1-19
reset pppoe-client	02-用户接入命令	3-9
reset pppoe-server	02-用户接入命令	2-5
reset radius statistics	07-安全命令	1-36
reset recycle-bin	01-基础配置命令	5-11
reset saved-configuration	01-基础配置命令	5-45
reset ssl proxy statistic	07-安全命令	9-17
reset ssl-proxy session	07-安全命令	9-17
reset stop-accounting-buffer	07-安全命令	1-37
reset stop-accounting-buffer	07-安全命令	1-57
reset tcp statistics	03-网络层协议命令	6-24
reset trapbuffer	01-基础配置命令	2-29
reset udp statistics	03-网络层协议命令	6-24
reset vlan statistics vid	01-基础配置命令	13-21
reset vlan statistics vid	02-用户接入命令	4-3
retry	01-基础配置命令	3-5
retry	07-安全命令	1-38
retry realtime-accounting	07-安全命令	1-38
retry stop-accounting	07-安全命令	1-39
retry stop-accounting	07-安全命令	1-58
return	01-基础配置命令	1-15
rip	04-路由协议命令	2-13
rip authentication-mode	04-路由协议命令	2-13
rip input	04-路由协议命令	2-14
rip metricin	04-路由协议命令	2-15
rip metricout	04-路由协议命令	2-16
rip output	04-路由协议命令	2-16

rip split-horizon	04-路由协议命令	2-17
rip version	04-路由协议命令	2-17
rip work	04-路由协议命令	2-18
rmdir	01-基础配置命令	5-12
rmdir	01-基础配置命令	5-33
rmdir	01-基础配置命令	11-40
rmon alarm	01-基础配置命令	10-7
rmon event	01-基础配置命令	10-8
rmon history	01-基础配置命令	10-9
rmon prialarm	01-基础配置命令	10-9
rmon statistics	01-基础配置命令	10-11
root-certificate fingerprint	07-安全命令	8-8
route-distinguisher	06-VPN 命令	6-18
route-policy	03-网络层协议命令	7-9
route-policy	04-路由协议命令	5-15
router id	04-路由协议命令	3-46
route-tag	06-VPN 命令	6-19
routing-table limit	06-VPN 命令	6-20
rsa local-key-pair create	01-基础配置命令	11-15
rsa local-key-pair destroy	01-基础配置命令	11-16
rsa peer-public-key	01-基础配置命令	11-17
rule	07-安全命令	2-4
rule	07-安全命令	5-10
rule	07-安全命令	6-20
rule	07-安全命令	7-24
rule	07-安全命令	9-13
rule comment	07-安全命令	2-8

S

sa authentication-hex	06-VPN 命令	3-31
sa duration	06-VPN 命令	3-33
sa duration	06-VPN 命令	4-20
sa encryption-hex	06-VPN 命令	3-34
sa spi	06-VPN 命令	3-35

sa string-key	06-VPN 命令	3-36
save	01-基础配置命令	5-46
schedule reboot at	01-基础配置命令	2-9
schedule reboot delay	01-基础配置命令	2-10
scheme	07-安全命令	1-15
scp batch-sync	08-可靠性命令	2-10
screen-length	01-基础配置命令	6-13
script-string	01-基础配置命令	12-3
secondary accounting	07-安全命令	1-40
secondary accounting	07-安全命令	1-59
secondary authentication	07-安全命令	1-41
secondary authentication	07-安全命令	1-59
secondary authorization	07-安全命令	1-60
security acl	06-VPN 命令	3-38
send	01-基础配置命令	6-13
sendpacket passroute	01-基础配置命令	4-15
send-trap	01-基础配置命令	4-14
server ip	07-安全命令	9-18
server-type	07-安全命令	1-42
service-type	07-安全命令	1-16
service-type dvpn	07-安全命令	1-17
service-type ftp	07-安全命令	1-17
service-type ppp	07-安全命令	1-18
session	07-安全命令	9-6
session algorithm-suite	06-VPN 命令	5-23
session idle-time	06-VPN 命令	1-14
session idle-time	06-VPN 命令	5-24
session keepalive-interval	06-VPN 命令	5-24
session log enable	07-安全命令	13-24
session setup-interval	06-VPN 命令	5-25
set authentication password	01-基础配置命令	6-14
set priority	07-安全命令	4-33
sftp	01-基础配置命令	11-40
sftp server enable	01-基础配置命令	11-31

sftp source-interface	01-基础配置命令	11-41
sftp source-ip	01-基础配置命令	11-42
sham-link	06-VPN 命令	6-21
shell	01-基础配置命令	6-15
shutdown	01-基础配置命令	13-10
shutdown	07-安全命令	9-9
silent-interface	04-路由协议命令	3-47
smtpc administrator mail	07-安全命令	13-16
smtpc trigger time	07-安全命令	13-16
snmp-agent	01-基础配置命令	8-10
snmp-agent community	01-基础配置命令	8-10
snmp-agent group	01-基础配置命令	8-11
snmp-agent local-engineid	01-基础配置命令	8-13
snmp-agent mib-view	01-基础配置命令	8-13
snmp-agent packet max-size	01-基础配置命令	8-14
snmp-agent sys-info	01-基础配置命令	8-14
snmp-agent target-host	01-基础配置命令	8-15
snmp-agent trap enable	01-基础配置命令	8-17
snmp-agent trap enable encrypt-card	06-VPN 命令	3-51
snmp-agent trap enable ldp	05-MPLS 命令	1-9
snmp-agent trap enable lsp	05-MPLS 命令	1-10
snmp-agent trap enable ospf	04-路由协议命令	3-48
snmp-agent trap life	01-基础配置命令	8-18
snmp-agent trap queue-size	01-基础配置命令	8-18
snmp-agent trap source	01-基础配置命令	8-19
snmp-agent usm-user	01-基础配置命令	8-20
source	06-VPN 命令	2-6
source-interface	01-基础配置命令	4-16
source-ip	01-基础配置命令	4-16
source-port	01-基础配置命令	4-17
speed	01-基础配置命令	6-16
speed	01-基础配置命令	13-15
spf-schedule-interval	04-路由协议命令	3-49
ssh authentication-type default	01-基础配置命令	11-18

ssh client assign rsa-key	01-基础配置命令	11-27
ssh client first-time enable	01-基础配置命令	11-27
ssh server authentication-retries	01-基础配置命令	11-18
ssh server compatible-ssh1x enable	01-基础配置命令	11-19
ssh server rekey-interval	01-基础配置命令	11-20
ssh server timeout	01-基础配置命令	11-20
ssh user	01-基础配置命令	11-22
ssh user assign	01-基础配置命令	11-23
ssh user authentication-type	01-基础配置命令	11-24
ssh user service-type	01-基础配置命令	11-24
ssh2	01-基础配置命令	11-28
ssh2 source-interface	01-基础配置命令	11-29
ssh2 source-ip	01-基础配置命令	11-30
ssh-server source-interface	01-基础配置命令	11-21
ssh-server source-ip	01-基础配置命令	11-21
ssl proxy	07-安全命令	9-18
ssl proxy server	07-安全命令	9-19
ssl server-policy	07-安全命令	9-7
ssl-server-policy	07-安全命令	9-20
start l2tp	06-VPN 命令	1-15
start l2tp tunnel	06-VPN 命令	1-16
start-script	01-基础配置命令	12-5
startup saved-configuration	01-基础配置命令	5-46
state	07-安全命令	1-18
state	07-安全命令	1-42
state	07-安全命令	8-12
static-bind { mac-address | client-identifier }	03-网络层协议命令	5-41
static-bind ip-address	03-网络层协议命令	5-40
static-lsp egress	05-MPLS 命令	1-10
static-lsp ingress	05-MPLS 命令	1-11
static-lsp transit	05-MPLS 命令	1-12
statistic connect-number ip	07-安全命令	13-9
statistic connect-number zone	07-安全命令	13-11
statistic connect-speed ip	07-安全命令	13-12

statistic connect-speed zone	07-安全命令	13-13
statistic enable	07-安全命令	13-14
stop-accounting-buffer enable	07-安全命令	1-43
stop-accounting-buffer enable	07-安全命令	1-61
stopbits	01-基础配置命令	6-17
stub	04-路由协议命令	3-50
summary	04-路由协议命令	2-19
summary	04-路由协议命令	4-56
super	01-基础配置命令	1-16
super authentication-mode	07-安全命令	1-19
super password	01-基础配置命令	1-17
sysname	01-基础配置命令	1-18
system-view	01-基础配置命令	1-18

T

tcp mss	03-网络层协议命令	6-24
tcp timer fin-timeout	03-网络层协议命令	6-25
tcp timer syn-timeout	03-网络层协议命令	6-26
tcp window	03-网络层协议命令	6-26
telnet	01-基础配置命令	11-3
telnet source-interface	01-基础配置命令	11-4
telnet source-ip	01-基础配置命令	11-5
telnet-server source-interface	01-基础配置命令	11-5
telnet-server source-ip	01-基础配置命令	11-6
terminal debugging	01-基础配置命令	2-30
terminal logging	01-基础配置命令	2-30
terminal monitor	01-基础配置命令	2-31
terminal trapping	01-基础配置命令	2-32
test-enable	01-基础配置命令	4-18
test-failtimes	01-基础配置命令	4-19
test-type	01-基础配置命令	4-17
tftp	01-基础配置命令	5-35
tftp source-interface	01-基础配置命令	5-37
tftp source-ip	01-基础配置命令	5-38

tftp-server acl	01-基础配置命令	5-36
timeout	01-基础配置命令	4-19
time-out	06-VPN 命令	3-39
timer hold	02-用户接入命令	1-12
timer keep-alive hold	04-路由协议命令	4-57
timer loop	01-基础配置命令	3-5
timer quiet	07-安全命令	1-44
timer quiet	07-安全命令	1-61
timer realtime-accounting	07-安全命令	1-45
timer realtime-accounting	07-安全命令	1-62
timer response-timeout	07-安全命令	1-46
timer response-timeout	07-安全命令	1-63
timer wait	01-基础配置命令	3-6
time-range	07-安全命令	2-10
timers	04-路由协议命令	2-20
tos	01-基础配置命令	4-20
tracert	01-基础配置命令	2-11
traffic behavior	09-QoS 命令	2-37
traffic classifier	09-QoS 命令	2-38
traffic-share-across-interface	04-路由协议命令	2-21
transform	06-VPN 命令	3-39
ttl	01-基础配置命令	4-20
ttl expiration	05-MPLS 命令	1-13
ttl propagate	05-MPLS 命令	1-13
tunnel authentication	06-VPN 命令	1-17
tunnel avp-hidden	06-VPN 命令	1-17
tunnel flow-control	06-VPN 命令	1-18
tunnel keepstanding	06-VPN 命令	1-18
tunnel local	06-VPN 命令	3-41
tunnel name	06-VPN 命令	1-19
tunnel password	06-VPN 命令	1-20
tunnel remote	06-VPN 命令	3-41
tunnel timer hello	06-VPN 命令	1-20
tunnel-protocol dvpn	06-VPN 命令	5-25

tunnel-protocol gre	06-VPN 命令	2-7

U

udp-helper enable	03-网络层协议命令	3-2
udp-helper port	03-网络层协议命令	3-2
udp-helper server	03-网络层协议命令	3-3
undelete	01-基础配置命令	5-13
undo synchronization	04-路由协议命令	4-57
upgrade	01-基础配置命令	5-14
use encrypt-card	06-VPN 命令	3-51
use ssl-card	07-安全命令	9-9
user	01-基础配置命令	5-34
user privilege	01-基础配置命令	6-17
user-interface	01-基础配置命令	6-18
username	01-基础配置命令	4-21
user-name-format	07-安全命令	1-46
user-name-format	07-安全命令	1-64

V

validate-source-address	04-路由协议命令	2-21
verbose	01-基础配置命令	5-34
vif	08-可靠性命令	2-11
virtualbaudrate	01-基础配置命令	13-22
vlan-type dot1q	01-基础配置命令	13-21
vlan-type dot1q	02-用户接入命令	4-3
vlink-peer	04-路由协议命令	3-50
voice-config	03-网络层协议命令	5-41
vpninstance	01-基础配置命令	4-22
vpn-instance-capability simple	06-VPN 命令	6-22
vpn-target	06-VPN 命令	6-23
vrbd	01-基础配置命令	1-19
vrrp authentication-mode	08-可靠性命令	1-2
vrrp ping-enable	08-可靠性命令	1-3
vrrp un-check ttl	08-可靠性命令	1-4

vrrp vrid preempt-mode	08-可靠性命令	1-4
vrrp vrid priority	08-可靠性命令	1-5
vrrp vrid timer advertise	08-可靠性命令	1-6
vrrp vrid track	08-可靠性命令	1-6
vrrp vrid track detect-group	01-基础配置命令	3-8
vrrp vrid virtual-ip	08-可靠性命令	1-7

W

wred	09-QoS 命令	2-39
wred dscp	09-QoS 命令	2-39
wred ip-precedence	09-QoS 命令	2-41
wred weighting-constant	09-QoS 命令	2-42

X

Y

Z