



S1720&S2700&S3700&S5700&S6700数据配置规范

版本	基于V200R007C00产品文档
修订	2016年12月9日 v1.0



目录

S1720&S2700&S3700&S5700&S6700数据配置规范	1
1 系统基本配置规范	7
1.1 配置设备名称.....	7
1.2 配置Banner.....	7
1.3 配置设备时间.....	8
1.4 配置NTP.....	8
1.5 配置VTY用户界面	9
1.6 空闲时间	10
1.7 配置访问控制列表.....	10
1.8 配置VTY用户界面的telnet用户.....	11
1.9 配置VTY用户界面的SSH用户	11
1.10 配置AAA.....	12
1.11 查看系统状态.....	13
1.12 查看设备版本.....	14
1.13 查看设备文件.....	14
1.14 备份设备文件.....	14



1.15	清空配置	15
1.16	检测LLDP链路.....	15
2	ACL配置规范	16
2.1	配置基本ACL.....	16
2.2	配置高级ACL.....	16
2.3	配置二层ACL.....	17
2.4	配置用户自定义ACL.....	17
2.5	配置用户ACL.....	17
2.6	配置高级ACL.....	18
2.7	配置命名型ACL.....	19
3	接口配置	19
3.1	接口基本配置规范.....	19
3.2	Eth-Trunk接口配置规范.....	19
3.3	接口MTU（超大帧处理）	20
4	生成树	20
4.1	MSTP配置	20
4.2	VBST配置	21



5	硬件相关操作	22
5.1	复位设备以及查看状态.....	22
5.2	主备倒换	22
5.3	修改温度告警阈值.....	23
5.4	修改风扇调速温度阈值.....	23
6	ICMP报文防攻击配置.....	23
6.1	全局ICMP报文防攻击配置.....	23
6.2	接口ICMP报文防攻击配置.....	24
7	IP路由配置.....	24
7.1	ECMP负载分担配置.....	24
7.2	OSPF.....	25
7.2.1	OSPF基本配置规范	25
7.2.2	OSPF路由聚合	26
7.2.3	ECMP负载分担配置.....	27
7.2.4	OSPF维护查看命令	27
7.3	静态路由	28
7.3.1	静态路由基本配置规范.....	28



7.3.2	路由表维护查看命令.....	28
8	BFD.....	29
8.1	静态标识符自协商BFD.....	29
8.1.1	静态多跳BFD配置规范.....	29
8.1.2	配置接口绑定静态单跳BFD.....	29
8.2	动态BFD配置.....	30
8.2.1	BFD和接口状态联动的配置规范.....	30
8.3	BFD维护查看命令.....	30
9	VRRP.....	31
10	IP QoS.....	32
10.1	CAR限速配置（针对不同流做限速的配置规范：使用流策略进行限速）.....	32
10.2	接口拥塞管理（PQ/WRR/DRR调度）.....	33
10.3	QOS默认模板查询命令.....	33
11	策略路由.....	34
11.1	策略路由基本配置规范.....	34
11.2	流策略配置(三层流量去除DSCP优先级).....	34
12	CPU保护.....	36



12.1	基本配置规范.....	36
12.2	本机防攻击	37
13	NQA（网络质量检查）	37
14	镜像	38
14.1	端口镜像	38
14.2	流镜像	38
15	堆叠	40
15.1	业务口堆叠	40
15.2	堆叠卡堆叠	41
15.3	双主检测（V200R002版本及之前版本）	42
15.4	多主检测（V200R003版本及之后版本）	44
16	日志告警	45
16.1	Info-center信息中心设置	45
16.2	SNMP配置	46



1 系统基本配置规范

1.1 配置设备名称

命令	说明
< HUAWEI> system-view [HUAWEI] sysname Switch [Switch]	//进入用户视图 //配置设备名称为Switch //设备名称显示为Switch

1.2 配置 Banner

命令	说明
header login information "WARNING!!! Authorized access only, all of your done will be recorded! disconnect IMMEDIATELY if you are not an authorised user!" header shell information "welcome!"	//配置当用户在登录设备认证过程中, 激活终端连接时显示的标题信息。 //配置当用户成功登录到设备上, 已经建立了会话时显示的标题信息。



1.3 配置设备时间

命令	说明
clock timezone Beijing add 08:00:00	//配置设备所在时区为Beijing, 相对UTC时间偏移8小时
clock datetime 0:0:0 2015-01-01	//配置设备当前日期和时间2015年1月1日0时0分0秒（用户视图下执行）

1.4 配置 NTP

命令	说明
# vlan batch 100 # acl number 2000 description This acl is used restrict ntp server rule 10 permit source 10.1.1.1 0 rule 20 permit source 10.1.2.1 0 rule 100 deny # interface vlanif100 ip address 100.10.1.1 255.255.255.0	//创建VLAN供NTP引用 //创建ACL供NTP引用



# ntp-service authentication enable ntp-service authentication-keyid 42 authentication-mode hmac-sha256 cipher huawei123 ntp-service reliable authentication-keyid 42 ntp-service refclock-master ntp-service source-interface vlanif100 ntp-service unicast-server 10.1.1.1 authentication-keyid 42 preference ntp-service unicast-server 10.1.2.1 authentication-keyid 42 ntp-service access peer 2000 #	//启用NTP认证 //配置NTP认证密钥ID号为42，采用 HMAC-SHA256算法，密钥为huawei123，以密 文显示 //指定ID号为42的NTP认证密钥为可信的密钥 //设置本地时钟作为NTP主时钟 //指定NTP所有输出报文都用VLANIF100的IP 地址为源IP //指定10.1.1.1为优先选择的NTP SERVER //指定10.1.2.1为备用NTP SERVER //设置允许匹配ACL 2000号中的peer可以对本 地设备进行时间请求、查询控制、时间同步
---	---

1.5 配置 VTY 用户界面

命令	说明
aaa local-user user1 password irreversible-cipher Huawei@123 local-user user1 privilege level 15 local-user user1 service-type telnet # user-interface maximum-vty 15	//创建AAA本地用户，其中用户的密码在配置文 件中以密文显示 //设置用户的接入类型 //配置通过VTY用户界面登录的用户最大数目，



user-interface vty 0 14 authentication-mode aaa protocol inbound telnet	S12700最大支持15 //进入0~14的VTY用户界面视图 //配置VTY用户界面的验证方式为AAA //指定VTY用户界面所支持的协议为Telnet
---	--

1.6 空闲时间

命令	说明
user-interface console 0 idle-timeout 15 0 # user-interface vty 0 14 idle-timeout 15 0	//设置用户界面断连的超时时间为15分0秒，即用户没有输入命令的时间

1.7 配置访问控制列表

命令	说明
acl number 2001 description This acl is used restrict telnet users rule 10 permit source 10.136.135.1 0 rule 20 permit source 10.136.136.1 0 rule 3000 deny source any # user-interface vty 0 14	//配置ACL，此处以使用基本ACL限制用户通过Telnet登录权限为例 //规则10允许网段为10.136.135.1子网掩码为32的报文 //规则3000拒绝任意源地址的报文 //进入0~14的VTY用户界面视图



authentication-mode aaa acl 2001 inbound	//配置VTY用户界面的验证方式为AAA //配置VTY用户界面登录控制列表为2001
---	--

1.8 配置 VTY 用户界面的 telnet 用户

命令	说明
aaa local-user user1 password irreversible-cipher Huawei@123 local-user user1 service-type telnet local-user user1 privilege level 15 # user-interface vty 0 14 authentication-mode aaa protocol inbound telnet user privilege level 15 history-command max-size 20 idle-timeout 20 0 screen-length 30	//配置AAA本地用户的用户名和密码 //配置用户的接入类型为Telnet //配置本地用户的用户级别为15, 该命令优先级低于VTY用户界面的 user privilege level 15 //还需要配置 telnet server enable , 使能Telnet服务器功能, 该命令不会在配置文件中显示 //设置VTY用户通过AAA认证登陆 //指定VTY用户界面所支持的协议为Telnet //配置VTY用户界面的用户级别为15 //配置终端属性

1.9 配置 VTY 用户界面的 SSH 用户

命令	说明
rsa local-key-pair create # user-interface vty 0 14	//生成本地RSA主机密钥对和服务器密钥对



authentication-mode aaa protocol inbound ssh user privilege level 15 # aaa local-user user2 password irreversible-cipher Huawei@456 local-user user2 service-type ssh # stelnet server enable ssh user client001 ssh user client001 authentication-type password ssh user client001 service-type stelnet ssh user client002 ssh user client002 assign rsa-key rsakey001 ssh user client002 authentication-type rsa ssh user client002 service-type stelnet	//设置VTY用户通过AAA认证登陆 //指定VTY用户界面所支持的协议为SSH //配置VTY用户界面的用户级别为15 //配置AAA本地用户 //使能SSH服务器功能 //创建SSH用户client001 //配置用户通过password认证方式登录 //配置用户的接入类型为STelnet //创建SSH用户client002 //为用户分配RSA公钥rsakey001 //配置用户通过RSA认证方式登录 //配置用户的接入类型为STelnet
---	---

1.10 配置 AAA

命令	说明
hwtacacs-server template temp1 hwtacacs-server authentication 202.96.96.86 hwtacacs-server authentication 202.101.172.38 secondary hwtacacs-server authorization 202.96.96.86 hwtacacs-server authorization 202.101.172.38 secondary	//创建HWTACACS服务器模板 //配置HWTACACS认证服务器的地址 //配置HWTACACS备用认证服务器的地址 //配置HWTACACS授权服务器的地址 //配置HWTACACS备用授权服务器的地址



<pre>hwtacacs-server accounting 202.96.96.86 hwtacacs-server accounting 202.101.172.38 secondary hwtacacs-server shared-key huawei@1234 undo hwtacacs-server user-name domain-included # aaa authentication-scheme sch1 authentication-mode hwtacacs local authorization-scheme sch1 authorization-mode hwtacacs local accounting-scheme sch1 accounting-mode hwtacacs accounting start-fail online domain huawei authentication-scheme sch1 authorization-scheme sch1 accounting-scheme sch1 hwtacacs-server temp1</pre>	<p>//配置HWTACACS计费服务器的地址</p> <p>//配置HWTACACS备用计费服务器的地址</p> <p>//设置HWTACACS服务器的共享密钥</p> <p>//设置HWTACACS服务器的用户名不包含域名（如果HWTACACS服务器不接受包含域名的用户名，需要配置该命令）</p> <p>//配置认证方案</p> <p>//先使用HWTACACS认证，无响应时转为本地认证</p> <p>//配置授权方案</p> <p>//先使用HWTACACS授权，无响应时转为本地授权</p> <p>//配置计费方案</p> <p>//使用HWTACACS计费</p> <p>//如果开始计费失败仍允许用户上线。如果不需要计费建议不配置计费方案，否则需要配置该命令使用户上线</p> <p>//配置用户登录时使用域huawei</p> <p>//把域和某个特定的认证、计费和授权方案关联后，该域就可以用该方案对用户进行认证、计费和授权</p>
--	---

1.11 查看系统状态



命令	说明
display device	//查看所有在位设备的基本信息, 包括电源模块和风扇模块的信息
display switchover state	//查看系统是否满足主备倒换的条件
display health	//查看系统健康状态: 包含设备的电压信息、温度信息、电源信息、风扇信息、CPU及内存占用率信息以及存储介质使用信息
display current-configuration	//查看系统当前配置

1.12 查看设备版本

命令	说明
display version	//查看系统版本信息
display patch-information	//查看当前所有的补丁信息

1.13 查看设备文件

命令	说明
dir	//显示设备存储设备中的指定文件或目录的信息

1.14 备份设备文件

命令	说明
----	----



display startup	//查看与本次及下次启动相关的系统软件、配置文件名和PAF、License文件、补丁文件
save	//保存设备当前配置 (设备作FTP客户端时), 在用户视图下执行命令
ftp 10.11.0.24	//登录FTP服务器
put vrpcfg.zip	//将文件放入ftp服务器

1.15 清空配置

命令	说明
reset saved-configuration reboot	//清除配置, 恢复成出厂配置重启设备。请慎重执行此命令, 建议在技术支持人员指导下使用。

1.16 检测 LLDP 链路

命令	说明
lldp enable	//全局LLDP使能
snmp-agent trap enable feature-name lldptrap	//使能LLDP告警
reset lldp statistics [interface <i>interface-type</i> <i>interface-number</i>]	//清除全局或接口LLDP报文的统计信息 (用户视图)



lldp clear neighbor [interface <i>interface-type</i> <i>interface-number</i>]	//清除全局或接口邻居信息（用户视图）
display lldp neighbor [interface <i>interface-type</i> <i>interface-number</i>]	//查看全局或接口邻居信息
display lldp statistics [interface <i>interface-type</i> <i>interface-number</i>]	//查看全局或接口LLDP报文的统计信息

2 ACL 配置规范

2.1 配置基本 ACL

命令	说明
time-range ftp-access 14:00 to 18:00 off-day time-range ftp-access from 00:00 2015/1/1 to 23:59 2015/12/31 # acl number 2001 rule 5 permit source 172.16.105.0 0.0.0.255 rule 10 permit source 172.16.107.0 0.0.0.255 time-range ftp-access rule 15 deny	//配置基本ACL，基于时间段限制用户

2.2 配置高级 ACL

命令	说明
acl number 3001 rule 5 deny ip source 10.1.1.0 0.0.0.255 destination 10.1.2.0 0.0.0.255 acl number 3002 rule 5 deny ip source 10.1.2.0 0.0.0.255 destination 10.1.1.0 0.0.0.255	//配置高级ACL，基于网段限制用户



2.3 配置二层 ACL

命令	说明
acl number 4000 rule 5 deny source-mac 00e0-f201-0101	//配置二层ACL，基于源MAC限制用户

2.4 配置用户自定义 ACL

命令	说明
acl number 5000 rule 5 deny 0x0180c200 0xffffffff 14	// 配置用户自定义ACL，基于特定规则限制用户

2.5 配置用户 ACL

命令	说明
authentication unified-mode # ucl-group 1 name group_m ucl-group 2 name group_r ucl-group 3 name group_it # acl number 6001 rule 5 deny ip source ucl-group name group_m destination ucl-group name group_r	将NAC配置模式切换成统一模式。传统模式与统一模式相互切换后，必须重启设备，新配置模式的各项功能才能生效。缺省情况下，NAC配置模式为统一模式。 //创建UCL组 //配置关联UCL组的用户ACL



<pre>rule 10 deny ip source ucl-group name group_r destination ucl-group name group_m rule 15 deny ip source ucl-group name group_m destination ucl-group name group_it rule 20 deny ip source ucl-group name group_it destination ucl-group name group_m # aaa authentication-scheme abc authentication-mode radius service-scheme service-scheme1 ucl-group name group_m service-scheme service-scheme2 ucl-group name group_r service-scheme service-scheme3 ucl-group name group_it domain abc11 authentication-scheme abc radius-server rd1 # traffic-filter inbound acl 6001 #</pre>	<p>//创建业务方案并在业务方案中分别应用UCL组,实现网络权限的分组控制</p> <p>//配置基于用户ACL对报文进行过滤</p>
--	--

2.6 配置高级 ACL

命令	说明
<pre>acl ipv6 number 3001 rule 0 deny ipv6 source FC01::2/128 destination FC01::/64</pre>	//配置高级ACL6，对IPv6报文进行过滤



2.7 配置命名型 ACL

命令	说明
acl name test1 3276 rule 5 permit ip source 218.109.5.69 0	//配置命名型ACL

3 接口配置

3.1 接口基本配置规范

命令	说明
# interface gigabitethernet 0/0/1 combo-port copper # interface gigabitethernet 0/0/2 eth-trunk 1	//配置接口工作模式为电口模式 //将当前以太网接口加入Eth-Trunk接口

3.2 Eth-Trunk 接口配置规范

命令	说明
# interface Eth-Trunk1 port link-type trunk undo port trunk allow-pass vlan 1	//配置接口的链路类型 //将接口退出VLAN1



port trunk allow-pass vlan 2 110 130 150 160 170 180 510 mode lacp #	//配置接口加入的VLAN //配置Eth-Trunk工作模式为LACP模式
--	---

3.3 接口 MTU（超大帧处理）

命令	说明
interface GigabitEthernet 0/0/1 jumboframe enable 5000 # interface Vlanif 100 mtu 1492	//配置接口允许通过的最大帧长为5000字节 //设置接口的最大传输单元为1492。VLANIF接口下mtu的取值必须小于该VLAN下的物理端口jumboframe的取值

4 生成树

4.1 MSTP 配置

命令	说明
# stp instance 1 root primary stp instance 2 root secondary # stp region-configuration region-name RG1	//配置设备在指定生成树实例中的优先级 //配置MST域的域名



instance 1 vlan 2 to 10 instance 2 vlan 11 to 20 active region-configuration # interface Eth-Trunk1 port link-type trunk undo port trunk allow-pass vlan 1 port trunk allow-pass vlan 2 to 20 mode lacp # interface GigabitEthernet 0/0/1 port link-type access port default vlan 2 stp edged-port enable #	//配置多生成树实例和VLAN的映射关系 //激活MST域的配置 //配置设备互联接口的链路类型 //将接口退出VLAN1 //配置接口加入的VLAN //配置连接终端接口的链路类型 //配置连接终端接口的缺省VLAN //配置连接终端的接口为边缘端口
---	---

4.2 VBST 配置

命令	说明
# stp mode vbst # stp vlan 30 root secondary stp vlan 10 20 root primary #	//配置设备的生成树协议工作模式为VBST //配置设备在指定生成树中的优先级



<pre>interface Eth-Trunk1 port link-type trunk undo port trunk allow-pass vlan 1 port trunk allow-pass vlan 10 20 30 # interface GigabitEthernet 0/0/1 port link-type access port default vlan 10 stp edged-port enable #</pre>	<p>//配置设备互联接口加入的VLAN</p> <p>//配置连接终端的接口为边缘端口</p>
---	--

5 硬件相关操作

5.1 复位设备以及查看状态

命令	说明
reset slot 1	//复位堆叠ID为1的设备
display device	//查看设备的部件类型及状态信息

5.2 主备倒换

命令	说明
----	----



slave switchover enable	//使能主备倒换
slave switchover	//强制进行主备倒换（按照设备提示输入“Y”）

5.3 修改温度告警阈值

命令	说明
temperature threshold slot all lower-limit 20 upper-limit 45	//设置堆叠中所有设备的温度告警阈值为下限20℃，上限45℃

5.4 修改风扇调速温度阈值

命令	说明
set fan speed-adjust threshold minus 10	//将风扇转速的温度阈值降低10℃

6 ICMP 报文防攻击配置

6.1 全局 ICMP 报文防攻击配置

命令	说明
icmp unreachable drop	//使能丢弃目的不可达ICMP报文功能。缺省未使能
icmp port-unreachable send	//使能设备的ICMP端口不可达报文的发送功能。缺省已使能
icmp protocol-unreachable send	//使能ICMP协议不可达报文的发送功能。缺省已使能



6.2 接口 ICMP 报文防攻击配置

命令	说明
interface vlanif 10 icmp redirect send icmp ttl-exceeded send icmp host-unreachable send	//使能ICMP重定向报文发送功能。缺省已使能 //使能ICMP TTL超时报文发送功能。缺省已使能 //使能ICMP主机不可达报文发送功能。缺省已使能

7 IP 路由配置

7.1 ECMP 负载分担配置

对于IPv4及ECMP，可以分别配置负载分担模式，以下步骤可不选、选择其一或多选，请根据网络转发报文的实际情况选择。

命令	说明
load-balance-profile a ipv4 field sip protocol # ecmp load-balance sip #	//配置负载分担模板 //配置指定负载分担模板中IPv4报文负载分担方式 //配置等价路由基于源IP地址进行负载分担



7.2 OSPF

7.2.1 OSPF 基本配置规范

命令	说明
ospf 1 router-id 10.1.1.1 area 0.0.0.0 network 192.168.0.0 0.0.0.255 area 0.0.0.1 network 192.168.1.0 0.0.0.255	//配置OSPF基本功能
ospf 1 area 0.0.0.1 network 192.168.1.0 0.0.0.255 stub	//配置STUB区域
ospf 1 area 0.0.0.2 nssa	//配置NSSA区域
ospf 1 import-route direct	//配置OSPF引入其他路由
interface Vlanif20 ospf cost 5	//配置OSPF的接口开销



bfd # ospf 1 bfd all-interfaces enable ospf 1 default-route-advertise always ospf 1 area 0.0.0.3 nssa default-route-advertise interface Vlanif100 ip address 100.10.1.1 255.255.255.0 ospf enable 1 area 0.0.0.0	//配置OSPF与BFD联动，需要在设备的邻居设备上 也进行同样配置 //在OSPF普通区域发布缺省路由 //在 OSPF NSSA 区域发布缺省路由 //使能接口VLANIF100到OSPF指定区域
---	--

7.2.2 OSPF 路由聚合

命令	说明
ospf 100 area 0 network 36.42.10.0 0.0.0.255 network 36.42.110.0 0.0.0.255 abr-summary 36.42.0.0 255.255.0.0	//配置ABR路由聚合。将OSPF 100的区域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向其它区域发布



ospf 100 asbr-summary 10.2.0.0 255.255.0.0 not-advertise tag 2 cost 100	//配置ASBR路由聚合
--	--------------

7.2.3 ECMP 负载分担配置

命令	说明
ospf 100 maximum load-balancing 2 nexthop 10.0.0.3 weight 1	//配置最大等价路由数量，缺省情况为16 //配置OSPF的负载分担优先级，weight值越小，优先级越高

7.2.4 OSPF 维护查看命令

命令	说明
display ospf peer display ospf routing display ospf interface display ospf lsdb display ospf error	//查看OSPF邻居 //查看OSPF路由表 //查看OSPF接口以及接口状态 //查看OSPF的LSDB //查看OSPF的协议错误信息



7.3 静态路由

7.3.1 静态路由基本配置规范

命令	说明
ip route-static 0.0.0.0 0.0.0.0 10.1.4.2	//配置缺省静态路由
ip route-static 10.1.1.0 255.255.255.0 10.1.4.1	//配置静态路由
ip route-static 1.0.0.0 255.0.0.0 10.1.6.1 preference 3	//配置静态路由的优先级值，默认60
ip route-static 1.0.0.0 255.0.0.0 10.1.7.1 preference 3 track bfd-session sess1	//配置静态路由绑定BFD会话session（需先创建sess1）
ip route-static 1.0.0.0 255.0.0.0 vpn-instance vpn1 2.2.2.2	//配置静态黑洞路由
ip route-static vpn-instance vpn2 1.0.0.0 255.0.0.0 3.3.3.3	//配置静态global路由的下一跳在vpn里面
ip route-static vpn-instance vpn2 1.0.0.0 255.0.0.0 vpn-instance vpn1 3.3.3.3	//配置静态vpn路由的下一跳是在另外一个vpn里面
ipv6 route-static :: 0 vlanif20 fc00:0:0:2010::2	//配置缺省静态IPv6路由
ipv6 route-static fc00:0:0:2001:: 64 vlanif20 fc00:0:0:2010::1	//配置静态IPv6路由
ipv6 route-static default-preference 70	//配置缺省静态路由并设置其优先级

7.3.2 路由表维护查看命令

命令	说明
display ip routing-table [verbose]	//查看路由表
display ip routing-table vpn-instance vpn1 [verbose]	//查看vpn路由
display fib	//查看设备的FIB表
display router id	//查看本路由的router-id



8 BFD

8.1 静态标识符自协商 BFD

8.1.1 静态多跳 BFD 配置规范

命令	说明
bfd # bfd atoc bind peer-ip 10.2.1.2 discriminator local 10 discriminator remote 20 commit # ip route-static 10.2.2.0 24 10.1.1.2 track bfd-session atoc	//全局打开bfd功能，缺省情况下为关闭状态 //创建名为atoc的多跳BFD会话，检测到对端IP地址为10.2.1.2的多跳链路 //配置BFD会话的本地标识符为10，远端标识符为20 //提交BFD会话配置 //静态路由绑定BFD会话，检测下一跳状态

8.1.2 配置接口绑定静态单跳 BFD

命令	说明
bfd # bfd atod bind peer-ip 10.1.1.6 interface vlanif 100 discriminator local 1	//创建名称为atob的BFD会话，对从本端接口VLANIF100到对端IP地址为10.1.1.6的单跳链路进行检



discriminator remote 2 wtr 5 commit	测 //配置BFD会话等待恢复时间，即UP后5分钟再上报恢复事件，避免上层应用震荡 (两端配置要对应，还需要配置相应的路由)
---	--

8.2 动态 BFD 配置

8.2.1 BFD 和接口状态联动的配置规范

命令	说明
bfd # bfd atob bind peer-ip default-ip interface GigabitEthernet0/0/1 discriminator local 10 discriminator remote 20 process-interface-status commit #	//创建检测接口物理状态的BFD会话atob //配置BFD会话与绑定的接口进行状态联动

8.3 BFD 维护查看命令

命令	说明
display bfd configuration all	//查看BFD会话配置信息



display bfd session all	//查看BFD会话信息
display bfd interface	//查看使能BFD的接口信息
display bfd statistics session all	//查看BFD会话的统计信息

9 VRRP

命令	说明
VRRP主设备: # interface Vlanif100 ip address 10.1.1.1 255.255.255.0 vrrp vrid 1 virtual-ip 10.1.1.111 vrrp vrid 1 priority 120 # VRRP备设备: # interface Vlanif100 ip address 10.1.1.2 255.255.255.0 vrrp vrid 1 virtual-ip 10.1.1.111 #	//创建VRRP备份组并为备份组指定虚拟IP地址 //配置设备在VRRP备份组中的优先级



10 IP QoS

10.1 CAR 限速配置（针对不同流做限速的配置规范：使用流策略进行限速）

命令	说明
acl number 2001 rule 5 permit source 1.1.1.1 0 acl number 2002 rule 5 permit source 1.1.1.2 0 # traffic classifier class1 if-match acl 2001 traffic classifier class2 if-match acl 2002 # traffic behavior behavior1 car cir 5000 cbs 10000 pbs 10000 traffic behavior behavior2 car cir 2000 cbs 10000 pbs 10000 # traffic policy policy1 classifier class1 behavior behavior1 classifier class2 behavior behavior2 # interface GigabitEthernet 0/0/1	//使用ACL匹配流量 //定义流分类 //定义car这个限速流行为 //流分类和流行为组成流量策略 //在接口入方向应用流量策略，限制发往设备的流量



traffic-policy policy1 inbound interface GigabitEthernet 2/0/0 qos lr cir 200 outbound	//流量出方向进行流量整形，限制端口带宽为20%
--	--------------------------

10.2 接口拥塞管理（PQ/WRR/DRR 调度）

命令	说明
interface gigabitethernet 0/0/1 qos lr inbound cir 20000 cbs 375000	//配置入方向接口限速
interface GigabitEthernet 0/0/1 qos wrr qos queue 2 wrr weight 20 qos queue 4 wrr weight 5 qos queue 5 wrr weight 50	//配置端口队列调度方式为WRR //配置队列2、4、5比例分别为20：5：50，当报文超过端口转发car值的时候，队列2、4、5转发按照比例转发，优先保证PQ队列的转发
display qos configuration interface GigabitEthernet 0/0/1	//查询端口的调度情况

10.3 QOS 默认模板查询命令

命令	说明
display diffserv domain	//显示DiffServ域的详细配置信息



11 策略路由

11.1 策略路由基本配置规范

不指定出接口，使用指定的下一跳去查FIB表，查找成功则根据查到的表项转发；否则再使用报文中的目的IP地址去查FIB表，查找成功则根据查到的表项转发；否则丢弃。

命令	说明
acl number 2003 rule 0 permit source 50.1.1.0 0.0.0.255 # traffic classifier c1 operator or precedence 5 if-match acl 2003 # traffic behavior b1 redirect ip-nexthop 10.0.0.1 # traffic policy aaa classifier c1 behavior b1 # interface GigabitEthernet 2/0/0 traffic-policy aaa inbound	//用ACL匹配流量 //用流分类匹配ACL //创建将报文重定向到单个下一跳IP地址的动作 //将流分类和对应的流行为进行绑定 //在接口inbound方向应用流策略

11.2 流策略配置(三层流量去除 DSCP 优先级)

命令	说明
----	----



traffic classifier ISR operator or if-match vlan 400 if-match vlan 401 # traffic behavior ISR remark dscp default # traffic policy ISR classifier ISR behavior ISR # interface GigabitEthernet 0/0/1 traffic-policy ISR inbound # traffic-policy ISR global inbound display traffic classifier user-defined display traffic behavior user-defined display traffic policy global display traffic-policy applied-record	//配置流分类 //配置流行为 //将流分类和对应的流行为进行绑定 //将流策略ISR应用到接口的入方向上 //在全局入方向上应用该策略 //查看已配置的流分类 //查看已配置的流行为 //查看全局应用的流策略 //查看流策略的应用记录
--	--

12 CPU 保护

12.1 基本配置规范

命令	说明
acl number 2001	
rule 5 permit source 10.1.1.0 0.0.0.255	
acl number 2002	
rule 5 permit source 10.2.2.0 0.0.0.255	
acl number 2003	
rule 5 permit source 10.3.3.0 0.0.0.255	
#	
cpu-defend policy 10	//创建本机防攻击策略
blacklist 2 acl 2001	//创建黑名单，未匹配的其他流都进黑名单
whitelist 2 acl 2002	//创建白名单，优先处理匹配白名单特征的报文
user-defined-flow 2 acl 2001	//创建用户自定义流，将符合此特征的数据流进行上送限制
car user-defined-flow 1 cir 5000 cbs 940000	//对指定用户自定义流设置速率限制
car packet-type arp-request cir 120 cbs 22560	//对指定类型的报文设置速率限制
linkup-car packet-type ftp cir 1000 cbs 100000	//配置建立FTP连接时FTP报文的承诺信息速率为1000kbit/s，承诺突发尺寸为100000bytes
auto-defend enable	//使能攻击溯源功能
auto-defend alarm enable	//使能攻击溯源告警功能
auto-defend action deny	//使能攻击溯源的惩罚功能，并指定惩罚措施为丢弃
auto-port-defend protocol arp-request threshold 40	//配置端口防攻击可以防范的报文类型为ARP Request
auto-port-defend whitelist 1 interface GigabitEthernet0/0/1	//配置网络侧接口GE0/0/1为端口防攻击白名单，避免网络侧的



# display cpu-defend configuration slot X	协议报文得不到CPU及时处理而影响正常业务 //查看接口板CPU-defend配置
--	--

12.2 本机防攻击

匹配顺序为：白名单whitelist，黑名单blacklist

命令	说明
acl number 2001 rule 5 permit source 1.1.1.0 0.0.0.255 cpu-defend policy test1 blacklist 1 acl 2001 car packet-type arp-reply cir 64 cbs 33000 auto-defend enable auto-defend action deny auto-defend alarm enable auto-defend trace-type source-mac source-ip source-portvlan auto-defend protocol all cpu-defend-policy test1	//创建一个ACL，匹配源IP //创建一个cpu-defend保护策略 //配置黑名单 //配置arp-reply报文上送CPU的速率限制 //配置攻击溯源检查功能 //配置攻击溯源惩罚措施为丢弃攻击报文 //使能攻击溯源告警功能 //默认配置，使能auto-defend之后，默认是基于源MAC、源IP、 端口+vlan的溯源，可根据需要自行修改 //全局应用防攻击策略

13 NQA（网络质量检查）

命令	说明
----	----



nqa test-instance test1 10 test-type icmp destination-address ipv4 122.224.187.154 source-address ipv4 122.224.187.153 probe-failtimes 2 test-failtimes 3 frequency 1 interval seconds 60 probe-count 10 start now	//创建NQA测试例 //配置ICMP类型的NQA测试样例 //配置NQA测试例的目的地址 //配置NQA测试的源IP地址 //配置在NQA测试中，连续探测失败的次数 //配置在NQA测试中，连续测试失败的次数 //配置NQA测试例的自动执行测试间隔 //配置NQA测试例的报文的时间间隔 //probe-count命令配置NQA测试例的测试探针数目 //启动测试
---	---

14 镜像

14.1 端口镜像

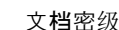
命令	说明
observe-port 1 interface GigabitEthernet 0/0/1 interface GigabitEthernet 0/0/2 port-mirroring to observe-port 1 both	//配置本地镜像的观测端口 //配置本地镜像的镜像端口，将镜像端口入方向和出方向的报文都镜像到观察端口

14.2 流镜像

命令	说明
----	----



observe-port 1 interface GigabitEthernet 0/0/1 # acl 4001 rule permit 8021p 6 # traffic-mirror inbound acl 4001 to observe-port 1 # traffic classifier c1 if-match 8021p 6 # traffic behavior b1 mirroring to observe-port 1 # traffic policy p1 classifier c1 behavior b1 # interface gigabitethernet 0/0/2 traffic-policy p1 inbound	//配置本地镜像的观察端口 //创建二层ACL，配置的规则是匹配802.1p优先级为6的报文 //将所有端口入方向（即接收报文方向）802.1p优先级为6的报文复制到观察端口GE0/0/1 //创建流分类c1，并配置流分类规则是匹配802.1p优先级为6的报文 //创建流行为b1，并配置动作为流镜像 // 创建流策略，并将流分类和流行为绑定到流策略上 //将端口 GE0/0/2 入方向 802.1p 优先级为 6 的报文复制到观察端口 GE0/0/1
---	---



15.1 业务口堆叠

第 40 页, 共 47 页



<pre>[HUAWEI] sysname SwitchB [SwitchB] interface stack-port 0/1 [SwitchB-stack-port0/1] port interface gigabitethernet 0/0/27 enable Warning: Enabling stack function may cause configuration loss on the interface. Continue? [Y/N]:y Info: This operation may take a few seconds. Please wait. [SwitchB-stack-port0/1] quit [SwitchB] interface stack-port 0/2 [SwitchB-stack-port0/2] port interface gigabitethernet 0/0/28 enable Warning: Enabling stack function may cause configuration loss on the interface. Continue? [Y/N]:y Info: This operation may take a few seconds. Please wait. [SwitchB-stack-port0/2] quit [SwitchB] quit <SwitchB> save 将SwitchA、SwitchB下电，使用SFP+电缆连接后再上电。 display stack</pre>	<pre>//创建逻辑堆叠端口 //配置指定业务接口为堆叠物理成员端口，并将堆叠物理成员端 口加入逻辑堆叠口 //按照设备提示输入“Y” //保存设备配置 //查看堆叠系统的堆叠信息</pre>
--	---

15.2 堆叠卡堆叠

命令	说明
<pre>SwitchA: <HUAWEI> system-view [HUAWEI] sysname SwitchA</pre>	



<pre>[SwitchA] stack slot 0 priority 200 [SwitchA] quit <SwitchA> save SwitchB: <HUAWEI> system-view [HUAWEI] sysname SwitchB [SwitchB] stack slot 0 renumber 1 [SwitchB] quit <SwitchB> save 将SwitchA、SwitchB下电，使用线缆连接各堆叠端口并上电。 display stack</pre>	<pre>//配置SwitchA的堆叠ID，堆叠优先级为200 //保存设备配置 //配置SwitchB的堆叠ID //保存设备配置 //查看堆叠系统的堆叠信息</pre>
---	--

15.3 双主检测（V200R002 版本及之前版本）

配置采用直连方式双主检测：

命令	说明
<pre>interface GigabitEthernet0/0/5 dual-active detect mode direct # interface GigabitEthernet1/0/5 dual-active detect mode direct</pre>	<pre>//配置接口GigabitEthernet0/0/5采用直连方式双主检测功能 //配置接口GigabitEthernet1/0/5采用直连方式双主检测功能</pre>



配置代理方式双主检测:

命令	说明
堆叠系统上: interface Eth-Trunk1 dual-active detect mode relay # interface GigabitEthernet0/0/5 eth-trunk 1 # interface GigabitEthernet1/0/5 eth-trunk 1	//在堆叠系统上, 配置Eth-Trunk1的代理方式双主检测功能 //GigabitEthernet0/0/5加入到Eth-Trunk1中 //GigabitEthernet1/0/5加入到Eth-Trunk1中
代理设备上: # interface Eth-Trunk1 dual-active relay # interface GigabitEthernet0/0/1 eth-trunk 1 # interface GigabitEthernet0/0/2 eth-trunk 1	//在代理设备上, 配置Eth-Trunk1的代理方式双主检测功能 //GigabitEthernet0/0/1加入到Eth-Trunk1中 //GigabitEthernet0/0/2加入到Eth-Trunk1中



15.4 多主检测（V200R003 版本及之后版本）

配置采用直连方式多主检测：

命令	说明
interface GigabitEthernet0/0/5 mad detect mode direct # interface GigabitEthernet1/0/5 mad detect mode direct	//配置接口GigabitEthernet0/0/5采用直连方式多主检测功能 //配置接口GigabitEthernet1/0/5采用直连方式多主检测功能

配置代理方式多主检测：代理设备为一台交换机

命令	说明
堆叠系统上： interface Eth-Trunk1 mad detect mode relay # interface GigabitEthernet0/0/5 eth-trunk 1 # interface GigabitEthernet1/0/5 eth-trunk 1 代理设备上： # interface Eth-Trunk1	//在堆叠系统上，配置Eth-Trunk1的代理方式多主检测功能 //GigabitEthernet0/0/5加入到Eth-Trunk1中 //GigabitEthernet1/0/5加入到Eth-Trunk1中



mad relay	//在代理设备上，配置Eth-Trunk1的代理方式多主检测功能
#	
interface GigabitEthernet0/0/1	
eth-trunk 1	//GigabitEthernet0/0/1加入到Eth-Trunk1中
#	
interface GigabitEthernet0/0/2	
eth-trunk 1	//GigabitEthernet0/0/2加入到Eth-Trunk1中

配置代理方式多主检测：两套堆叠系统互为代理

命令	说明
在每个堆叠系统上： mad domain 1 # interface Eth-Trunk5 mad detect mode relay mad relay	//配置堆叠系统MAD域值为1，设备支持两套堆叠系统互为代理进行多主检测，此时必须通过配置保证两套堆叠系统的MAD域值不同。 //配置Eth-Trunk5的代理方式多主检测功能 //在Eth-Trunk5上启用代理功能

16 日志告警

16.1 Info-center 信息中心设置

命令	说明
info-center enable	//使能信息中心功能。缺省已使能



info-center logbuffer display info-center	//使能Log信息向Log缓冲区的发送功能,缺省未使能 //查看信息中心输出方向的配置信息
info-center logfile channel 9 info-center channel 0 name execonsole info-center filter-id bymodule-alias MD CMD_PRI_REARRG info-center loghost 202.38.160.1 channel channel6	//配置向日志文件输出信息的通道 //将0号通道命名为execonsole //配置通过模块名和助记符进行过滤 //向IP地址为202.38.160.1的日志主机发送信息,所使用的通道为channel6
info-center loghost source loopback 1023	//设置Loopback1023的IP地址为日志消息报文的源地址
info-center source bfd channel snmpagent log level warning	//将SNMP agent通道输出BFD模块的Log信息,且允许输出信息的最低级别为warning
display channel 1	//显示信息通道1中Log、Trap和Debug信息是否允许从指定的信息通道通过和允许通过信息的级别
display logbuffer	//查看日志缓存
display alarm all	//查看告警
display logfile logfile/log.log	//查看保存在本地日志文件里面的日志

16.2 SNMP 配置

命令	说明
snmp-agent	//使能SNMP Agent功能
snmp-agent udp-port 1057	//配置SNMP端口号



snmp-agent sys-info version v2c v3 snmp-agent trap enable snmp-agent target-host trap address udp-domain 1.1.1.1 params securityname Switchv2 snmp-agent trap enable feature-name snmp trap-name coldstart snmp-agent trap enable feature-name bfd trap-name hwbfdsessreachlimit snmp-agent group v3 admin privacy write-view allextisis acl 2001 snmp-agent usm-user v3 u1 group g1 snmp-agent usm-user v3 u1 authentication-mode sha snmp-agent target-host trap address udp-domain 10.1.1.1 params securityname nms2-admin v3 snmp-agent sys-info contact call Operator at 010-12345678 display info-center display snmp-agent target-host	//配置启用SNMPv2c和SNMPv3版本 //配置Trap功能 //设置接收Trap消息的目的地 //打开SNMP的coldstart的告警开关 //使能交换机发送BFD特性的hwbfdsessreachlimit告警 //指定团体名对应的读写视图是allextisis、对用户进行访问控制 //配置SNMPv3用户，用户名u1，所属组名g1，鉴别方式sha，加密方式aes128 //配置告警功能 //配置管理远联系方式 //查看SNMP Agent输出信息所使用的通道 //查看SNMP Agent输出网管的信息。
--	---