S7700&S9700&S12700数据配置规范

版本	基于V200R007C00产品文档
修订	2016年1月28日 初稿v1.0

目录

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 clock datetime 0:0:0 2015-01-01	//配置设备所在时区为Beijing，相对UTC时间偏移8小时 //配置设备当前日期和时间为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
#
	
	//创建VLAN供NTP引用
	
	//创建ACL供NTP引用

interface vlanif100
ip address 100.10.1.1 255.255.255.0
#
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
	
	//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

#
user-interface maximum-vty 15
 	
user-interface vty 0 14
  authentication-mode aaa
  protocol inbound telnet
	
	//配置通过VTY用户界面登录的用户最大数目，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
	//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

#
user-interface vty 0 14
  authentication-mode aaa
  acl 2001 inbound
	
	//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
	//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	//生成本地RSA主机密钥对和服务器密钥对

#	
user-interface vty 0 14	
authentication-mode aaa	//设置VTY用户通过AAA认证登陆
protocol inbound ssh	//指定VTY用户界面所支持的协议为SSH
user privilege level 15	//配置VTY用户界面的用户级别为15
#	
aaa	
local-user user2 password irreversible-cipher Huawei@456	//配置AAA本地用户
local-user user2 service-type ssh	
#	
stelnet server enable	//使能SSH服务器功能
ssh user client001	//创建SSH用户client001
ssh user client001 authentication-type password	//配置用户通过password认证方式登录
ssh user client001 service-type stelnet	//配置用户的接入类型为STelnet
ssh user client002	//创建SSH用户client002
ssh user client002 assign rsa-key rsakey001	//为用户分配RSA公钥rsakey001
ssh user client002 authentication-type rsa	//配置用户通过RSA认证方式登录
ssh user client002 service-type stelnet	//配置用户的接入类型为STelnet

1.10 配置 AAA

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

hwtacacs-server authorization 202.96.96.86	//配置HWTACACS授权服务器的地址
hwtacacs-server authorization 202.101.172.38 secondary	//配置HWTACACS备用授权服务器的地址
hwtacacs-server accounting 202.96.96.86	//配置HWTACACS计费服务器的地址
hwtacacs-server accounting 202.101.172.38 secondary	//配置HWTACACS备用计费服务器的地址
hwtacacs-server shared-key huawei@1234	//设置HWTACACS服务器的共享密钥
undo hwtacacs-server user-name domain-included	//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）
#	
aaa	
authentication-scheme sch1	//配置认证方案
authentication-mode hwtacacs local	//先使用HWTACACS认证，无响应时转为本地认证
authorization-scheme sch1	//配置授权方案
authorization-mode hwtacacs local	//先使用HWTACACS授权，无响应时转为本地授权
accounting-scheme sch1	//配置计费方案
accounting-mode hwtacacs	//使用HWTACACS计费
accounting start-fail online	//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**
domain huawei	//配置用户登录时使用域huawei
authentication-scheme sch1 authorization-scheme sch1 accounting-scheme sch1 hwtacacs-server temp1	//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

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 *interface-type interface-number*]	//清除全局或接口LLDP报文的统计信息（用户视图）
lldp clear neighbor [interface *interface-type interface-number*]	//清除全局或接口邻居信息（用户视图）
display lldp neighbor [interface *interface-type interface-number*]	//查看全局或接口邻居信息
display lldp statistics [interface *interface-type interface-number*]	//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	//配置高级ACL，基于网段限制用户

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	

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	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

<table>
<tr><td><pre>#</pre></td><td></td></tr>
<tr><td><pre>acl number 6001
 rule 5 deny ip source ucl-group name group_m destination ucl-group name group_r
 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</pre></td><td>//配置关联UCL组的用户ACL</td></tr>
<tr><td><pre>#</pre></td><td></td></tr>
<tr><td><pre>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</pre></td><td>//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</td></tr>
<tr><td><pre>#</pre></td><td></td></tr>
<tr><td><pre>traffic-filter inbound acl 6001</pre></td><td>//配置基于用户ACL对报文进行过滤</td></tr>
<tr><td><pre>#</pre></td><td></td></tr>
</table>

2.6 配置高级 ACL

命令	**说明**

acl ipv6 number 3001 rule 0 deny ipv6 source FC01::2/128 destination FC01::/64	//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 1/0/1
undo portswitch
ip address 10.10.10.10 255.255.255.0
#
interface gigabitethernet 1/0/1
combo-port copper
#
interface 40GE 1/0/0
eth-trunk 1
	
	//将接口切换为三层模式
	//配置IP地址
	
	//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

批注 [薛小芹1]: 新增

命令	说明

#
interface Eth-Trunk1
port link-type trunk
undo port trunk allow-pass vlan 1
port trunk allow-pass vlan 2 110 130 150 160 170 180 510
mode lacp
#
	
	//配置接口的链路类型
	//将接口退出VLAN1
	//配置接口加入的VLAN
	//配置Eth-Trunk工作模式为LACP模式

3.3 40GE 接口和 10GE 接口的拆分与合并

命令	说明

<Switch> **system-view**
[Switch] **interface 40ge 1/0/1**
[Switch-40GE1/0/1] **port split**
Warning: This command will take effect only after resetting the board. 40GE1/0/0 will not be changed. 40GE1/0/1-40GE1/0/7 will be split up into XGE, and the port configuration will be lost when the port type is changed! Continue? [Y/N]: **y**
Info: Succeeded in setting the configuration.
[Switch -40GE1/0/1] **quit**
	
	//进入40GE接口端口视图
	//将当前40GE接口拆分为四个10GE接口
	//提示是否执行，确定输入“Y”
	
	//重启接口板后，端口拆分生效

[Switch] **quit** <Switch> **reset slot 1** Caution!!! Confirm to reset slot 1 ? [Y/N]:**y** Info: The board[1] reset success.	
<Switch> **system-view** [Switch] **interface xgigabitethernet 1/0/1** [Switch-XGigabitEthernet1/0/1] **undo port split** Warning: This operation will cause all configuration on the port lose. The configuration will take effect after the board is reset. Continue? [Y/N]:**y** [Switch-XGigabitEthernet1/0/1] **quit** [Switch] **quit**	//进入拆分后的四个10GE接口中的任意一个接口视图 //将四个10GE接口合并成一个40GE接口
<Switch> **reset slot 1** Caution!!! Confirm to reset slot 1 ? [Y/N]:**y** Info: The board[1] reset success.	//重启接口板后，端口合并生效
<Switch> **display port split**	//查看设备中拆分接口的当前状态

3.4 接口 MTU（超大帧处理）

命令	说明
interface GigabitEthernet 1/0/0 jumboframe enable 5000 #	//配置接口允许通过的最大帧长为5000字节

interface Vlanif 100 mtu 1492	//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

批注 [薛小芹2]: 新增

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
instance 1 vlan 2 to 10
instance 2 vlan 11 to 20
active region-configuration
#
	
	//配置设备在指定生成树实例中的优先级
	
	//配置MST域的域名
	//配置多生成树实例和VLAN的映射关系
	
	//激活MST域的配置

4.2 VBST 配置

命令	说明
# stp mode vbst	 //配置设备的生成树协议工作模式为VBST

#
stp vlan 30 root secondary
stp vlan 10 20 root primary
#
interface Eth-Trunk1
  port link-type trunk
  undo port trunk allow-pass vlan 1
  port trunk allow-pass vlan 10 20 30
#
	
	//配置设备在指定生成树中的优先级
	
	//配置接口加入的VLAN

5 硬件相关操作

5.1 接口卡、单板上下电以及查看状态

命令	说明
power on slot 1	//给1号槽位单板上电，对于主用和备用主控板该命令无效
power off slot 1	//给1号槽位单板下电，对于主用和备用主控板该命令无效
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 slave switchover	//使能主备倒换 //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 1 lower-limit 20 upper-limit 45	//设置单板1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 icmp port-unreachable send	//使能丢弃目的不可达ICMP报文功能。缺省未使能 //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 vlan 10	
icmp redirect send	//使能ICMP重定向报文发送功能。缺省已使能
icmp ttl-exceeded send	//使能ICMP TTL超时报文发送功能。缺省已使能
icmp host-unreachable send	//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	//配置负载分担模板

ipv4 field sip protocol
#
ecmp load-balance sip
#
ecmp-profile prof1
ipv4 field sip protocol
#
ecmp load-balance enhanced profile prof1
	//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
	
	//配置ECMP模板
	//指定IPv4报文负载分担方式，根据IPv4报文的源IP地址和协议号进行负载分担
	//应用ECMP模板

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
 	
ospf 1
area 0.0.0.1
network 192.168.1.0 0.0.0.255
stub
	//配置OSPF基本功能
	
	//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	//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
ospf 1 default-route-advertise always	//在OSPF普通区域发布缺省路由

ospf 1
  area 0.0.0.3
  nssa default-route-advertise
	//在 OSPF NSSA 区域发布缺省路由

interface Vlanif100
  ip address 100.10.1.1 255.255.255.0
  ospf enable 1 area 0.0.0.0
	//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	//配置最大等价路由数量，缺省情况为16
nexthop 10.0.0.3 weight 1	//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	//查看OSPF邻居
display ospf routing	//查看OSPF路由表
display ospf interface	//查看OSPF接口以及接口状态
display ospf lsdb	//查看OSPF的LSDB
display ospf error	//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
ipv6 route-static fc00:0:0:2001:: 64 vlanif20 fc00:0:0:2010::1
ipv6 route-static default-preference 70
	//配置缺省静态IPv6路由
	//配置静态IPv6路由
	//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]
display ip routing-table vpn-instance vpn1 [verbose]
display fib 1
display router id
	//查看路由表
	//查看vpn路由
	//查看slot1的FIB表
	//查看本路由的router-id

8 路由策略 ip prefix 和 route-map

8.1 IP-PREFIX 配置规范

命令	说明

ip ip-prefix p1 permit 10.0.0.0 8 greater-equal 17 less-equal 18
 	
ip ip-prefix p3 index 10 deny 0.0.0.0 8 match-network
ip ip-prefix p3 index 20 permit 0.0.0.0 0 less-equal 32
ip ip-prefix default-routing index 10 permit 0.0.0.0 0
	//配置名为p1的地址前缀列表，只允许10.0.0.0/8网段内，掩码长度在17到18之间的路由通过
	//配置名为p3的地址前缀列表，拒绝0.0.0.1～0.255.255.255范围内的所有路由通过，允许其他路由通过
	（一个ip-prefix有多个规则index组成，和命名的ACL类似，它只能匹配路由，不能匹配数据报文）

8.2 常用路由策略配置规范

命令	说明
route-policy policy1 permit node 10	//配置路由策略
if-match ip-prefix p1	//设置一个基于IP地址前缀列表的匹配规则
apply cost 100	//设置路由的开销
ospf	//创建并运行OSPF进程
import-route isis 1 route-policy policy1	//引入其他路由协议学习到的路由信息
route-policy p2 permit node 40	//匹配所有，直接执行apply
apply cost 0	//修改路由的cost
acl 2002	//创建ACL
rule 5 permit source any	
#	
ip as-path-filter 2 permit _200_300	//创建AS路径过滤器
#	
ip community-filter 1 permit 100:200	//创建团体属性过滤器
#	
ip rd-filter 1 permit 100:1	//创建RD属性过滤器
#	
route-policy p3 permit node 40	//多个if-match是“与”关系，都必须匹配才能执行动作
if-match acl 2002	//匹配ACL

if-match as-path-filter 2	//匹配AS-PATH
if-match community-filter 1	//匹配团体属性
if-match cost 8	//匹配路由开销
if-match mpls-label	//匹配是否带MPLS标签
if-match rd-filter 1	//匹配RD属性
if-match route-type nssa-external-type1	//匹配路由类型，OSPF NSSA的外部路由
if-match tag 8	//匹配tag
if-match ip next-hop ip-prefix p1	//匹配路由下一跳
if-match ip route-source acl 2000	//匹配路由更新源地址（ACL2000需先创建）
apply as-path 200 10.10 additive	//修改BGP AS-PATH，追加指定AS号
apply as-path 300 overwrite	//修改BGP AS-PATH，覆盖指定AS号
apply as-path none overwrite	//清空BGP AS-PATH
apply community internet	//修改BGP的团体属性
apply community no-advertise	
apply community no-export	
apply community no-export-subconfed	
apply tag 100	//修改路由信息标记
apply cost 120	//修改路由的开销值
apply cost-type type-1	/修改路由的开销类型
apply isis LEVEL-1	//设置引入到IS-IS中的路由的Level级别
apply preference 90	//修改路由优先级
apply ip-address next-hop 192.168.1.8	//修改下一跳
route-policy export-other-routing2ospf permit node 10	
if-match ip-prefix export-other-routing2ospf	
apply cost 5	//两个apply都要执行

apply cost-type type-1	
	（以下策略中引用的如IPv4地址前缀列表、ACL需要先创建）
route-policy default2allIBGP permit node 10	//这个策略default2allIBGP有多个node，node之间是“或”关系，匹配一个节点则本策略即执行完成，跳出
if-match ip-prefix default-routing	
apply ip-address next-hop 10.1.2.1	//修改路由下一跳
#	
route-policy default2allIBGP deny node 20	//本节点是deny模式，即匹配了规则，这个策略就不执行了，一般排除某些路由不要对它做策略
if-match ip-prefix small_net_23_32	
if-match ip next-hop acl small_net_neighbor	//匹配下一跳地址
#	
route-policy default2allIBGP deny node 30	
if-match ip-prefix small_net_25_32	
if-match ip next-hop acl small_net_new_neighbor	
#	
route-policy default2allIBGP permit node 40	
if-match ip next-hop acl neighbor_2	
apply ip-address next-hop X.X.X.X	
#	
route-policy default2allIBGP permit node 50	
if-match ip next-hop acl NET-ISP_neighbor	
apply ip-address next-hop X.X.X.X	
#	
route-policy default2allIBGP permit node 60	
if-match ip next-hop acl NET-ISP_neighbor	
apply ip-address next-hop X.X.X.X	

#	

9 BFD

9.1 静态标识符自协商 BFD

9.1.1 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
#
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（在配置文件中不显示）
	
	//静态路由绑定BFD会话，检测下一跳状态

批注 [薛小芹3]: 待确认

9.1.2 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
discriminator remote 2
wtr 5
commit
	//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）

9.2 动态 BFD 配置

9.2.1 BFD 和 OSPF 联动的配置规范

命令	说明

bfd
#
ospf 1
bfd all-interfaces enable
interface vlanif 100
ospf bfd block
interface vlanif 100
ospf bfd enable
ospf bfd min-rx-interval 400 detect-multiplier 4
	//在OSPF进程下使能BFD特性
	//阻止指定接口创建BFD会话
	//在VLANIF100接口上使能BFD特性，并指定最小接收间隔为400ms，本地检测倍数为4

9.3 BFD 维护查看命令

命令	说明
display bgp bfd session all	//查看BGP建立的BFD会话信息
display ospf bfd session all	//查看使能BFD特性邻居的信息
display isis bfd session all	//查看BFD特性动态会话的信息
display isis bfd interface	//查看使能BFD特性的ISIS接口信息
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

10 VRRP

批注 [薛小芹4]: 新增

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
	
	//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

vrrp vrid 1 virtual-ip 10.1.1.111 #	

11 IP QoS

11.1 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
#
	//使用ACL匹配流量
	
	//定义流分类

traffic classifier class1 if-match acl 2001 traffic classifier class2 if-match acl 2002 #	 //定义car这个限速流行为
traffic behavior behavior1 car cir 5000 cbs 10000 pbs 10000 traffic behavior behavior2 car cir 2000 cbs 10000 pbs 10000 #	 //流分类和流行为组成流量策略
traffic policy policy1 classifier class1 behavior behavior1 classifier class2 behavior behavior2	

#
interface GigabitEthernet 1/0/0
  traffic-policy policy1 inbound
interface GigabitEthernet 2/0/0
  qos lr cir 200 outbound
	//在接口入方向应用流量策略，限制发往设备的流量
	
	//流量出方向进行流量整形，限制端口带宽为20%

11.2 接口拥塞管理（PQ/WRR/DRR 调度）

命令	说明

qos car qoscar1 cir 10000 cbs 10240
interface gigabitethernet 1/0/1
  qos car inbound qoscar1
 	
qos car qoscar1 cir 10000 kbps 10240
interface GigabitEthernet 1/0/0
  qos drr
  qos queue 2 drr weight 20
  qos queue 4 drr weight 5
  qos queue 5 drr weight 50
display qos configuration interface GigabitEthernet 1/0/0
	//配置入方向接口限速
	
	//配置端口流量整形带宽为10000kbit/s，承诺突发尺寸为10240byte
	//配置端口队列调度方式为WRR
	//配置wfq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
	//查询端口的调度情况

11.3 QOS 默认模板查询命令

命令	说明

display diffserv domain	//显示默认DiffServ域的详细配置信息

12 策略路由

12.1 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
	
	//通过流策略将流分类和流行为匹配
	
	//在接口inbound方向，应用流策略

12.2 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 2/0/0
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

13 CPU 保护

13.1 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 GigabitEthernet1/0/0	//配置网络侧接口GE1/0/0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

13.2 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

14 NQA（网络质量检查）

命令	说明

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

15 镜像

15.1 端口镜像

命令	说明
observe-port 1 interface GigabitEthernet 1/0/0	//配置本地镜像的观测端口
interface GigabitEthernet 1/0/0 port-mirroring to observe-port 1 both	//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

15.2 流镜像

命令	说明

	配置基于ACL的流镜像。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GE1/0/2
observe-port 1 interface GigabitEthernet 1/0/2	//配置本地镜像的观察端口
#	
acl 4001 rule permit 8021p 6	//创建二层ACL，配置的规则是匹配802.1p优先级为6的报文
traffic-mirror inbound acl 4001 to observe-port 1	
#	
traffic classifier c1 if-match 8021p 6	//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
#	
traffic behavior b1 mirroring to observe-port 1	//创建流行为b1，并配置动作为流镜像
#	
traffic policy p1 classifier c1 behavior b1	// 创建流策略，并将流分类和流行为绑定到流策略上
#	
interface gigabitethernet 2/0/1 traffic-policy p1 inbound	//将端口 GE2/0/1 入方向 802.1p 优先级为 6 的报文复制到观察端口 GE1/0/2

16 集群

批注 [薛小芹5]: 新增

16.1 业务口集群

命令	说明

SwitchA:
<HUAWEI> **system-view**
[HUAWEI] **sysname SwitchA**
[SwitchA] **set css mode lpu**
[SwitchA] **set css id 1**
[SwitchA] **set css priority 100**
 	
SwitchB:
<HUAWEI> **system-view**
[HUAWEI] **sysname SwitchB**
[SwitchB] **set css mode lpu**
[SwitchB] **set css id 2**
[SwitchB] **set css priority 10**
 	
SwitchA:
[SwitchA] interface css-port 1
[SwitchA-css-port1] port interface xgigabitethernet 1/0/1 to xgigabitethernet 1/0/2 enable
[SwitchA-css-port1] quit
[SwitchA] interface css-port 2
	
	//配置SwitchA的集群连接方式为集群卡连接
	//配置SwitchA的集群ID为1
	//配置SwitchA的集群优先级为100
	
	//配置SwitchB的集群连接方式为集群卡连接
	//配置SwitchB的集群ID为2
	//配置SwitchB的集群优先级为10
	
	//配置SwitchA的业务口XGE1/0/1～XGE1/0/2为集群物理成员端口并加入集群端口1。
	
	//配置SwitchA的业务口XGE2/0/1～XGE2/0/2为集群物理成员

[SwitchA-css-port2] port interface xgigabitethernet 2/0/1 to xgigabitethernet 2/0/2 enable [SwitchA-css-port2] quit	端口并加入集群端口2。
SwitchB: [SwitchB] interface css-port 1 [SwitchB-css-port1] port interface xgigabitethernet 1/0/1 to xgigabitethernet 1/0/2 enable [SwitchB-css-port1] quit	//配置SwitchB的业务口XGE1/0/1～XGE1/0/2为集群物理成员端口并加入集群端口1
[SwitchB] interface css-port 2 [SwitchB-css-port2] port interface xgigabitethernet 2/0/1 to xgigabitethernet 2/0/2 enable [SwitchB-css-port2] quit	//配置SwitchB的业务口XGE2/0/1～XGE2/0/2为集群物理成员端口并加入集群端口2。
[SwitchA] **css enable** Warning: The CSS configuration will take effect only after the system is rebooted. The next CSS mode is CSS card. Reboot now? [Y/N]:**y**	//使能SwitchA的集群功能，配置完成后必须立即重启使配置生效 //按照设备提示输入“Y”
[SwitchB] **css enable** Warning: The CSS configuration will take effect only after the system is rebooted. The next CSS mode is CSS card. Reboot now? [Y/N]:**y**	//使能SwitchB的集群功能，配置完成后必须立即重启使配置生效 //按照设备提示输入“Y”
display css status	//查看集群状态

16.2 集群口集群

命令	说明

SwitchA：
<HUAWEI> **system-view**
[HUAWEI] **sysname SwitchA**
[SwitchA] **set css mode css-card**
[SwitchA] **set css id 1**
[SwitchA] **set css priority 100**
 	
SwitchB：
<HUAWEI> **system-view**
[HUAWEI] **sysname SwitchB**
[SwitchB] **set css mode css-card**
[SwitchB] **set css id 2**
[SwitchB] **set css priority 10**
 	
[SwitchA] **css enable**
Warning: The CSS configuration will take effect only after the system is rebooted. The next CSS mode is CSS card. Reboot now? [Y/N]:**y**
 	
[SwitchB] **css enable**
Warning: The CSS configuration will take effect only after the system is rebooted. The next CSS mode is CSS card. Reboot now? [Y/N]:**y**
 	
display css status
	
	//配置SwitchA的集群连接方式为集群卡连接
	//配置SwitchA的集群ID为1
	//配置SwitchA的集群优先级为100
	
	//配置SwitchB的集群连接方式为集群卡连接
	//配置SwitchB的集群ID为2
	//配置SwitchB的集群优先级为10
	
	//使能SwitchA的集群功能，配置完成后必须立即重启使配置生效
	//按照设备提示输入“Y”
	
	//使能SwitchB的集群功能，配置完成后必须立即重启使配置生效
	//按照设备提示输入“Y”
	
	//查看集群状态

16.3 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

interface GigabitEthernet1/1/0/5
  dual-active detect mode direct
#
interface GigabitEthernet 2/1/0/5
  dual-active detect mode direct
	
	//配置接口GigabitEthernet1/1/0/5采用直连方式双主检测功能
	
	//配置接口GigabitEthernet2/1/0/5采用直连方式双主检测功能

配置代理方式双主检测：

命令	说明

集群系统上：
interface Eth-Trunk1
  dual-active detect mode relay
#
interface GigabitEthernet1/5/0/1
  eth-trunk 1
#
interface GigabitEthernet2/5/0/1
  eth-trunk 1
 	
代理设备上：
#
interface Eth-Trunk1
	
	//在集群系统上，配置Eth-Trunk1的代理方式双主检测功能
	
	//GigabitEthernet1/5/0/1加入到Eth-Trunk1中
	
	//GigabitEthernet2/5/0/1加入到Eth-Trunk1中

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

16.4 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 GigabitEthernet1/2/0/0
mad detect mode direct
#
interface GigabitEthernet2/10/0/0
mad detect mode direct
	
	//配置接口GigabitEthernet1/2/0/0采用直连方式多主检测功能
	
	//配置接口GigabitEthernet2/10/0/0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
集群系统上： interface Eth-Trunk1 mad detect mode relay	 //在集群系统上，配置Eth-Trunk1的代理方式多主检测功能

#
interface GigabitEthernet1/2/0/5
  eth-trunk 1
#
interface GigabitEthernet2/9/0/5
  eth-trunk 1
 	
代理设备上：
#
interface Eth-Trunk1
  mad relay
#
interface GigabitEthernet0/0/1
  eth-trunk 1
#
interface GigabitEthernet0/0/2
  eth-trunk 1
	
	//GigabitEthernet1/2/0/5加入到Eth-Trunk1中
	
	//GigabitEthernet2/9/0/5加入到Eth-Trunk1中
	
	//在代理设备上，配置Eth-Trunk1的代理方式多主检测功能
	
	//GigabitEthernet0/0/1加入到Eth-Trunk1中
	
	//GigabitEthernet0/0/2加入到Eth-Trunk1中

配置代理方式多主检测：两套集群系统互为代理

命令	说明

在每个集群系统上：
mad domain 1
#
interface Eth-Trunk5
  mad detect mode relay
	
	//配置集群系统MAD域值为1，设备支持两套集群系统互为代理进行多主检测，此时必须通过配置保证两套集群系统的MAD域值不同。
	//配置Eth-Trunk5的代理方式多主检测功能

mad relay	//在Eth-Trunk5上启用代理功能

17 日志告警

17.1 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	//使能Log信息向Log缓冲区的发送功能，缺省未使能
display info-center	//查看信息中心输出方向的配置信息
info-center logfile channel 9	//配置向日志文件输出信息的通道
info-center channel 0 name execconsole	//将0号通道命名为execconsole
info-center filter-id bymodule-alias MD CMD_PRI_REARRG	//配置通过模块名和助记符进行过滤
info-center loghost 202.38.160.1 channel channel6	//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

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