### 华为路由与交换配置命令

**前言：**

1.蓝色字体表示命令行命令，正式执行时不要复制前面的> # []号，> # []号只是提示符

2.绿色字体表示注释，有时注释太多就不用绿色表示了

3.注意：本文档的所有操作请先在在测环境进行实践，请不要直接在真实的服务器中操作！

**版权声明**：

本文档以开源的形式发布，所有条款如下：

1. 无担保：作者不保证文档内容的准确无误，亦不承担由于使用此文档所导致的任何后果

2. 自由使用：任何人可以出于任何目的而自由地 阅读/链接/打印/转载/引用/再创作 此文档，无需任何附加条件

若您 阅读/链接/打印/转载/引用/再创作 本文档，则说明接受以上2个条款。

作者：李茂福

时间：2022年7月10日

**章0、安装华为eNSP模拟器**

首先，到华为官网下载**eNSP模拟器**的安装包，然后在安装eNSP之前，要先安装三个依赖软件：

**WinPcap**

**Wireshark**

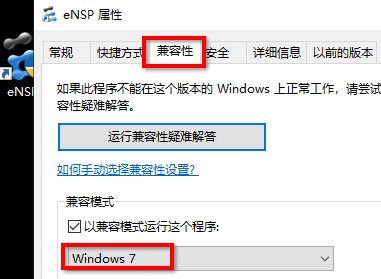
**Oracle VM VirtualBox**

所以一共是要准备4个软件包，如果找不到下载的资源，可以联系作者：[sysyear@163.com](mailto:sysyear@163.com)

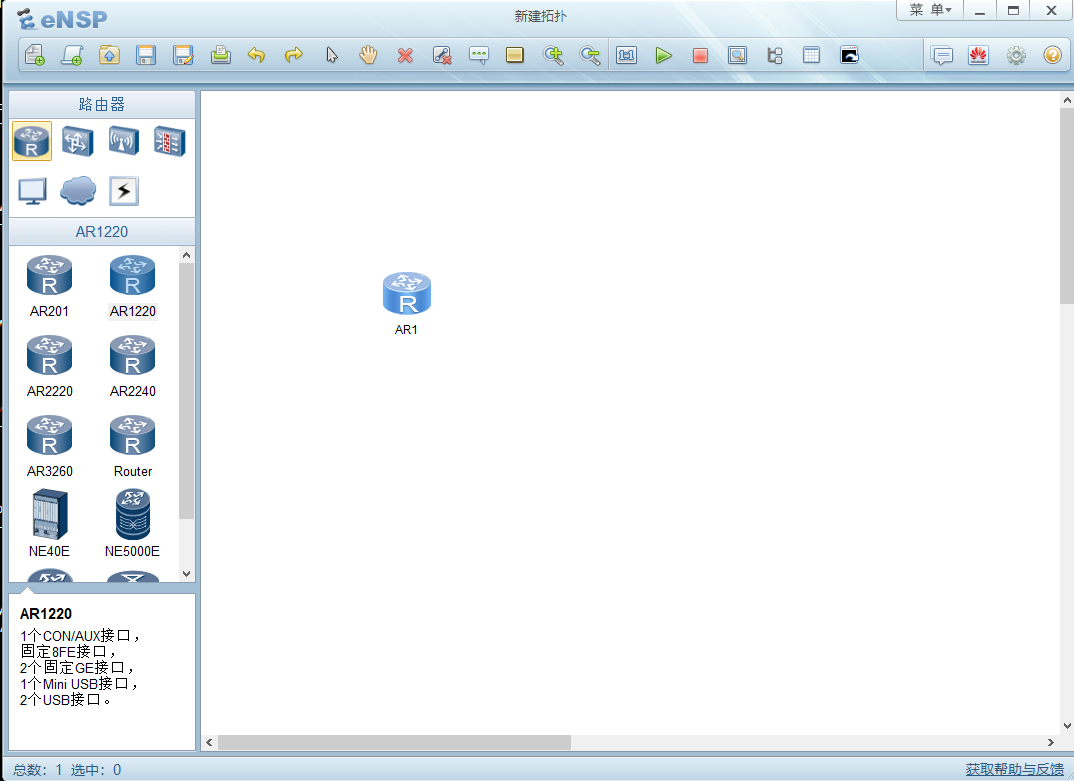
安装的过程就不多介绍了，装好eNSP模拟器后，找到它的图标：



点击右键，设置属性，将其兼容性改为Windows7，确定。这一步很重要，有时路由器不能正常启动就是因为没有以win7的兼容性来运行程序。



然后再双击图标，运行软件。



上图为eNSP的主界面，可以在左边拖入路由器或交换机等设备，放到右边的工作区里。

然后右击选择启动，再双击设备的图标就可以进入命令行了。具体的用法这里也不介绍了

本教程主要是教配置命令

如果有实体硬件设备，那最好是用真实的设备去测试。注意：不要在生产环境中做测试！！

**章n、设备登录管理**

**★设备基础信息查看**

<HUAWEI> disp elabel #查看设备电子标签

[Board Properties]

BoardType=S5735S-L24T4S-A

BarCode=21980109152SL1604582

Item=98010915

Description=Data Communication,S5735S-L24T4S-A,S5735S-L24T4S-A,S5735S-L24T4S-A (24\*10/100/1000BASE-T ports, 4\*GE SFP ports, AC power)

Manufactured=2020-02-12

VendorName=Huawei

IssueNumber=00

CLEICode=

BOM=

Model=S5735S-L24T4S-A

/$ElabelVersion=4.0

<HUAWEI> disp esn #查看设备序列号，用于申请license

ESN of slot 0: 21980109152SL1604582

<HUAWEI> disp bridge mac-address #查看设备网桥mac，同vlanif接口mac

System bridge MAC address: 60d7-5574-fd76

<HUAWEI> disp version #查看设备版本信息

Huawei Versatile Routing Platform Software

VRP (R) software, Version 5.170 (S5735 V200R021C00SPC100)

Copyright (C) 2000-2021 HUAWEI TECH Co., Ltd.

HUAWEI S5735S-L24T4S-A Routing Switch uptime is 0 week, 0 day, 0 hour, 59 minutes

ES5D2T28S022 0(Master) : uptime is 0 week, 0 day, 0 hour, 58 minutes

DDR Memory Size : 1024 M bytes

FLASH Total Memory Size : 512 M bytes

FLASH Available Memory Size : 306 M bytes

Pcb Version : VER.B

MAB Version : 0

BootROM(1st) Version : 0000.0121

BootROM(2nd) Version : 0000.0200

BootLoad Version : 0215.0000

CPLD Version : 0108

Software Version : VRP (R) Software, Version 5.170 (V200R021C00SPC100)

FLASH Version : 0000.0000

<HUAWEI> disp license #查看License许可信息

**★带内管理（console本地登录）**

①**仅使用密码登录console**

<Huawei> #刚开始进入的是一般模式

<Huawei> system-view #在一般模式下输入system-view进入系统配置模式

Enter system view, return user view with Ctrl+Z.

[Huawei] user-interface console 0 #进入console接口的配置界面

[Huawei-ui-console0] authentication-mode password #验证模式为仅密码

Please configure the login password (maximum length 16):123456

#如果是路由器，则要求立即输入密码，交换机则不会要求立即输入密码

[Huawei-ui-console0]user privilege level 15

#设置console登录的权限级别，15为管理员级别（6800及以上型号管理级别为3，）

[Huawei-ui-console0]set authentication password cipher 12pass6

#如果是交换机则要配置这行，设置console登录密码为12pass6

[Huawei-ui-console0]

②**使用 用户名和密码登录**

[Huawei] user-interface console 0

[Huawei-ui-console0]authentication-mode aaa #使用aaa认证登录，需要配置aaa

[Huawei-ui-console0]

**★aaa表示：**

**A**uthentication认证，**A**uthorization授权，**A**ccounting计费或Admission准入 的缩写

在交换机里表示使用 用户密码认证

**★虚拟终端vty数量**

[Huawei]

[HUAWEI] user-interface maximum-vty ?

INTEGER<0-15> The maximum number of VTY users, the default value is 5

[HUAWEI] user-interface maximum-vty 5 #最大终端数量为5（0到4）

Info: VTY0-4 VTYs are available, and VTY 16 to VTY 20 are reserved for the NMS.

**★带外管理（ssh远程登录）**

①**Telnet仅密码登录**

[Huawei] telnet server enable #开启telnet服务

Error: TELNET server has been enabled

[Huawei] user-interface vty 0 4 #进入vty接口配置

[Huawei-ui-vty0-4] authentication-mode password #验证模式为仅密码

Please configure the login password (maximum length 16): 12xx56

#如果是路由器，则要求立即输入密码，交换机则不会要求立即输入密码

[Huawei-ui-vty0-4] user privilege level 15

[Huawei-ui-vty0-4] set authentication password cipher 12xx56 #如果是交换机要配这条

[Huawei-ui-vty0-4] protocol inbound telnet #允许telnet登录

[Huawei-ui-vty0-4]

②**Telnet用户名和密码登录**

[Huawei-ui-vty0-4] user-interface vty 0 4

[Huawei-ui-vty0-4] authentication-mode aaa

[Huawei-ui-vty0-4] protocol inbound telnet #允许telnet登录

[Huawei-ui-vty0-4]

**★禁用telnet服务**

[Huawei] telnet server disable

[Huawei] telnet ipv6 server disable

③**SSH用户名和密码登录**

[Huawei] rsa local-key-pair create #创建rsa密钥

The key name will be: Host

% RSA keys defined for Host already exist.

Confirm to replace them? (y/n)[n]: y #输入y确定

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]:2048 #推荐用2048位的密钥

Generating keys...

.........................+++

.........+++

[Huawei] user-interface vty 0 4

[Huawei-ui-vty0-4] authentication-mode aaa

[Huawei-ui-vty0-4] protocol inbound ssh

#允许ssh登录，如果要允许telnet和ssh都能登录，则设置为 protocol inbound all

[Huawei-ui-vty0-4] acl 3011 inbound #设置允许远程访问的acl，可选

[Huawei-ui-vty0-4] quit

[Huawei] stelnet server enable #开启ssh服务

Info: Succeeded in starting the STELNET server.

[Huawei] sftp server enable #开启sftp服务，可选

[Huawei] ssh user admin authentication-type password

#添加ssh用户 **admin**，但该用户可能还未创建

Error: Username does not exist

先到下一节创建一个帐号

创建好了再回来：

[Huawei] ssh user admin authentication-type password #添加ssh登录用户 admin

[Huawei] ssh user admin service-type all #ssh用户服务类型为所有(sftp,stenlet)

[Huawei] ssh server cipher aes256\_ctr aes128\_ctr #至少要有aes128\_ctr

[Huawei] ssh server hmac sha2\_256

[Huawei] ssh server dh-exchange min-len 1024 #密钥交换材料长度

[Huawei] ssh server publickey rsa rsa\_sha2\_256 rsa\_sha2\_512 #至少要有 rsa

[Huawei] ssh server key-exchange dh\_group14\_sha256 dh\_group15\_sha512 dh\_group16\_sha512 dh\_group\_exchange\_sha256 #至少要有dh\_group14\_sha256

[Huawei] ssh server-source -i MEth 0/0/1 #指定ssh服务监听接口，一般为管理口

Warning: SSH server source configuration will take effect in the next login. Continue? [Y/N]:y

[Huawei] ssh server-source all-interface #也可设置监听所有接口

[Huawei] ssh server port 22 #设置ssh监听tcp端口号，默认22

[Huawei] ssh ipv4 server port 22 #较新型号设置ssh端口号方法

[Huawei] ssh authorization-type default aaa

[Huawei] ssh authentication-type default password

**★aaa创建用户（及密码策略）**

[Huawei] aaa #进入aaa配置界面

[HUAWEI-aaa] undo local-user policy security-enhance #关闭密码安全策略

[Huawei-aaa] local-user admin password cipher xxx #创建用户admin密码为xxx

[Huawei-aaa] local-user admin privilege level 15

#用户权限级别为15,管理员级别，6800及以上型号为 local-user admin level 3

[Huawei-aaa] local-user admin service-type telnet terminal ssh http

#用户的服务类型 telnet, terminal, ssh, http 登录用户

[Huawei-aaa]

**#如果关闭不了密码安全策略，则可设置：**

[HUAWEI-aaa] local-aaa-user password policy administrator #密码策略设置

[HUAWEI-aaa-lupp-admin] password history record number 0

# **0**表示不记录历史密码，改密码时就不会对比历史记录了，默认5

[HUAWEI-aaa-lupp-admin] undo password alert original #初次登录不提示改密码

[HUAWEI-aaa-lupp-admin] password expire 0 #0天，密码永不过期，默认90天

**#账号操作：**

[Huawei]aaa

[Huawei-aaa]undo local-user cof #删除帐号

[Huawei-aaa]

[Huawei-aaa]local-user cof state block #锁定帐号，锁定后该帐号无法再使用

[Huawei-aaa]local-user cof state active #解锁帐号，解锁后该帐号又可以使用了

[Huawei-aaa]

**★查看当前登录用户及踢除某用户**

[HUAWEI] display users [all]

User-Intf Delay Type Network Address AuthenStatus AuthorcmdFlag

+ 0 CON 0 00:00:00 pass no Username : admin

[HUAWEI] quit

<HUAWEI> kill user-interface console 0 #踢除con 0用户

<HUAWEI> kill user-interface vty 0 #踢除vty 0用户

**★登录超时设置**

[Huawei] user-interface vty 0 4

[Huawei-ui-vty0-4] idle-timeout 15 #空闲15分钟则自动登出，默认10分钟

[Huawei-ui-vty0-4]

**★终端信息设置**

**★关闭console终端信息输出**

<Huawei> undo terminal monitor

Info: Current terminal monitor is off.

<HUAWEI> undo terminal debugging

<Huawei>

**★终端显示行数**

<USG6300E>screen-length ?

INTEGER<0-512> Display the number of lines on a screen (the value 0

indicates none split screen, and the default value is 24)

<USG6300E> screen-length 0 temporary # 0表示一次性显示完，不分页

Info: The configuration takes effect on the current user terminal interface only.

[USG6300E] user-interface console 0

[USG6300E-ui-console0] screen-length 24 #console登录时分页显示，一页24行

[USG6300E] user-interface vty 0 4

[USG6300E-ui-vty0-4] screen-length 0 #vty远程登录时不分页显示

**★查看历史执行命令**

[USG6300E] disp history-command all-users

**★提交/清空候选配置**

#较高型号的设备，如6800及以上系列，默认配置模式下输入的配置是未提交（未生效）的，此时shell提示符前面有个\*星号，必须输入commit后才生效

[\*HUAWEI] display configuration candidate changes #查看当前未提交的配置

[HUAWEI] refresh configuration candidate #清除当前未提交的配置

**★查看配置**

<HUAWEI> disp saved-configuration #查看保存的配置

<HUAWEI> disp current-configuration #查看当前运行的配置

<HUAWEI> disp current-configuration interface vlan1 #查看接口上的配置

**★保存配置**

[Huawei]quit

<Huawei> save #配置完毕一定要记得保存配置，在一般模式下保存

The current configuration will be written to the device. #默认保存到vrpcfg.zip

Are you sure to continue? (y/n)[n]: y #输入y确定

It will take several minutes to save configuration file, please wait.......

Configuration file had been saved successfully

Note: The configuration file will take effect after being activated

<Huawei>

<Huawei>save xxx.cfg #保存到指定的文件名xxx.cfg

<Huawei>

[HUAWEI] configuration file auto-save interval 30 delay 5

#定时自动保存配置，30分钟，延迟5分钟

**★文件目录操作**

<HUAWEI> pwd #查看当前所在路径

flash:

<HUAWEI> cd ? #查看可进入的根路径

STRING The total length of absolute path is 64,the length of single

directory is 15

flash: Device name

<HUAWEI> cd flash: #进入flash:

<HUAWEI> dir #查看当前路径下的文件及子目录

<HUAWEI> mkdir back #在当前路径下创建一个子目录，名为 back

<HUAWEI> cd back #进入名为back的子目录

<HUAWEI> save back-xxx.cfg #保存配置到当前路径下，名为back-xxx.cfg

<HUAWEI> dir

Directory of flash:/back/

Idx Attr Size(Byte) Date Time FileName

0 -rw- 3,160 Jul 11 2022 23:22:53 back-xxx.cfg

<HUAWEI> copy back-xxx.cfg flash:/back-yyy.cfg #复制文件

Copy flash:/back/back-xxx.cfg to flash:/back-yyy.cfg?[Y/N]: y

100% complete.

<HUAWEI> unzip xxx.zip #解压某.zip文件

<HUAWEI> tail fileName 1000 #查看文件内容，显示最后1000行，默认显示10

<HUAWEI> delete back-xxx.cfg #删除文件

Delete flash:/back/back-xxx.cfg?[Y/N]: y

Info: Deleting file flash:/back/back-xxx.cfg...succeeded.

<HUAWEI> undelete xxx.cfg #恢复文件，默认删除文件时是会放到回收站的

<HUAWEI> reset recycle-bin #清空回收站

**★启动文件选择**

<Huawei> display startup #查看启动文件

<Huawei> startup saved-configuration vrpcfg.zip #指定启动时使用的配置文件

This operation will take several minutes, please wait....

Info: Succeeded in setting the file for booting system

<Huawei> startup system-software xxxxxx.cc #指定启动时使用的系统镜像文件

<HUAWEI> startup patch xxx.pat #指定启动时加载的补丁包

**★加载系统补丁**

<HUAWEI> patch load xxx.pat all [run] #加载补丁包

<HUAWEI> patch active all #激活补丁包

<HUAWEI> patch run all #运行补丁包

<HUAWEI> patch delete all #删除补丁包

**★license操作**

<HUAWEI> display esn #查看设备序列号

ESN of slot 0: 21980109152SL1604582

<HUAWEI> license verify xxxx.dat #验证许可文件 xxxx.dat

<HUAWEI> license active xxxx.dat #激活许可

<HUAWEI> display license #查看当前设备的许可信息

**★恢复出厂配置**

<Huawei> save back-old-xxx.cfg #一定要先备份原来的配置！

<Huawei> disp startup #查看当前启动文件

<Huawei> reset saved-configuration #重置配置文件

Warning: The action will delete the saved configuration in the device.

The configuration will be erased to reconfigure. Continue? [Y/N]: y #确定清除配置

Warning: Now clearing the configuration in the device.

Info: Succeeded in clearing the configuration in the device.

<Huawei> reboot #配置文件重置后，得重启系统才恢复出厂的运行状态

Info: The system is now comparing the configuration, please wait.

Warning: All the configuration will be saved to the configuration file for the n

ext startup:, Continue?[Y/N]: n #这里问是否要保存配置，**不保存**

Info: If want to reboot with saving diagnostic information, input 'N' and then e

xecute 'reboot save diagnostic-information'.

System will reboot! Continue?[Y/N]: y #确定要重启

<Huawei>#######

**初始化账号**：

s5735 账号 admin 密码 admin@huawei.com

ar2220 默认console密码： admin@huawei

**★设置系统时间**

[Huawei] undo ntp-service enable #不使用ntp，或者使用以下命令：  
[HUAWEI] ntp-service disable #不使用ntp

[HUAWEI] ntp-service ipv6 disable

Warning: NTP IPv4 service will be disabled. Continue?[Y/N] y

Info:Stop the NTP service successfully

[Huawei]quit

<Huawei> clock timezone **cst** add 08:00:00 #先配置时区，时区名称可自定义，如cst

<Huawei> clock datetime 22:55:00 2022-07-11 #再配置 时间 日期

<Huawei>

<HUAWEI> display clock #查看当前系统时间

2022-07-11 22:55:08+08:00

Monday

Time Zone(cst) : UTC+08:00

<HUAWEI>

**★SSH客户端**

[Huawei]

[Huawei] ssh client first-time enable #初次使用stelnet客户端要初始化客户端的密钥

[Huawei] stelnet 10.1.1.1 #使用stelnet远程登录到10.1.1.1

Please input the username: admin #输入用户名

Trying 10.1.1.1 ...

Press CTRL+K to abort

Connected to 10.1.1.1 ...

The server is not authenticated. Continue to access it? [Y/N] : y #确认

Save the server's public key? [Y/N] : y #确认

The server's public key will be saved with the name 10.1.1.1. Please wait...

Enter password: #输入密码

Info: The max number of VTY users is 5, and the number

of current VTY users on line is 1.

The current login time is 2019-12-03 09:41:47.

<S5700> #远程登录成功

<S5700> quit #退出登录

**★LLDP**

在

**★SNMP**

[Huawei]snmp-agent //开启snmp代理功能

[Huawei]snmp-agent community read public123 acl 2002 //可用acl指定允许的管理站

[Huawei]snmp-agent sys-info version all //指定snmp版本，v1, v2c, v3, all

[Huawei]snmp-agent sys-info location XXbuilding

[Huawei]snmp-agent sys-info contact coflee-18912345678

[Huawei]snmp-agent trap enable //开启trap功能

Warning: All switches of SNMP trap/notification will be open. Continue? [Y/N]:y

[Huawei]snmp-agent target-host trap address udp-domain 10.1.1.252 udp-port 162 params securityname prtgxx v2c

#设置trap参数，管理主机ip,trap端口号，团体字及版本

**章n、文件传输**

**★TFTP客户端**

[Huawei] tftp client-source -a 10.1.1.1 #指定tftp客户端的源ip

Info: Succeeded in setting the source address of the TFTP client to 10.1.1.1.

[Huawei]quit

<Huawei> tftp 10.1.1.254 put vrpcfg.zip s5700\_cfg.zip

#上传配置文件vrpcfg.zip到tftp服务器10.1.1.254，存储文件名为s5700\_cfg.zip

Info: Transfer file in binary mode.

Uploading the file to the remote TFTP server. Please wait...

<HUAWEI> tftp -a 192.168.2.104 192.168.2.102 put src.file dst.filename

#上传时直接指定tftp客户端ip（-a）

**★FTP服务器**

把交换机或路由器当作FTP服务器

[Huawei] ftp server enable #开启ftp服务器

Info: Succeeded in starting the FTP server.

[Huawei] aaa #进入aaa配置模式

[Huawei-aaa] local-user cof password cipher 12xx56 #创建用户cof作为ftp用户

Info: Add a new user.

[Huawei-aaa] local-user cof service-type ftp #用户仅用户ftp服务

[Huawei-aaa] local-user cof ftp-directory flash:/ #用户的ftp家目录为flash:/

[Huawei-aaa]quit

[Huawei]

**★FTP客户端**

<Huawei> ftp -a 10.1.1.2 10.1.1.1 #指定源ip为10.1.1.2,服务器ip为10.1.1.1

Trying 10.1.1.1 ...

Connected to 10.1.1.1.

220 FTP service ready.

User(10.1.1.1:(none)): cof #输入ftp用户名

331 Password required for cof.

Enter password: #输入密码

230 User logged in #成功登录

[Huawei-ftp] dir #查看服务器上的文件列表

200 Port command okay.

150 Opening ASCII mode data connection for \*.

drwxrwxrwx 1 noone nogroup 0 Aug 06 2015 src

-rwxrwxrwx 1 noone nogroup 538 Dec 03 09:31 vrpcfg.zip

226 Transfer complete.

FTP: 194 byte(s) received in 0.160 second(s) 1.21Kbyte(s)/sec.

[Huawei-ftp] get vrpcfg.zip s5700.zip #下载文件，上传为 put srcxx dstxxx

200 Port command okay.

150 Opening ASCII mode data connection for vrpcfg.zip.

226 Transfer complete.

FTP: 538 byte(s) received in 0.150 second(s) 3.58Kbyte(s)/sec.

[Huawei-ftp]quit

221 Server closing.

**章n、端口操作**

**★端口速率及模式**

[Huawei] int g0/0/3

[Huawei-GigabitEthernet0/0/3] undo negotiation auto

#手动指定端口参数时要先关闭自协商

[Huawei-GigabitEthernet0/0/3] duplex full #信道模式为全双工

[Huawei-GigabitEthernet0/0/3] speed 1000 #速率为1000M

[Huawei-GigabitEthernet0/0/3] combo-port copper #光电复用口指定为电口，光口为fiber

**#有的新型号设备配置方式为：**

[Huawei-GigabitEthernet0/0/3] negotiation disable #关闭自协商

[Huawei-GigabitEthernet0/0/3] port mode ge #设置速率为1000M

**★查看接口ip及状态**

<Huawei>dis ip int brief #查看接口的up/down状态及接口上的ip

\*down: administratively down

^down: standby

(l): loopback

(s): spoofing

The number of interface that is UP in Physical is 2

The number of interface that is DOWN in Physical is 2

The number of interface that is UP in Protocol is 2

The number of interface that is DOWN in Protocol is 2

Interface IP Address/Mask Physical Protocol

GigabitEthernet0/0/0 unassigned down down

GigabitEthernet0/0/1 10.1.1.2/24 up up

GigabitEthernet0/0/2 unassigned down down

NULL0 unassigned up up(s)

<Huawei>

**★二层口设置为三层口（保留vlan）**

[Huawei] vlan reserved for main-interface 4030 to 4063 #设置保留vlan

[Huawei] int eth-trunk 2 #或者int g0/0/2

[Huawei-Eth-Trunk2] undo portswitch #设置为3层口

**★清空某端口上的所有配置**

[HUAWEI] interface GigabitEthernet0/0/17 #先进入端口配置模式

[HUAWEI-GigabitEthernet0/0/17] clear configuration this

Warning: All configurations of the interface will be cleared, and its state will be shutdown. Continue? [Y/N] : y

[HUAWEI] clear configuration interface GigabitEthernet0/0/18 #直接清空

Warning: All configurations of the interface will be cleared, and its state will be shutdown. Continue? [Y/N] : y

**★端口拆分split**

[Huawei] port split mode mode2 slot 1 #mode1,mode2,mode3

<Huawei> reboot #重启后才生效

[Huawei] port split dimension int 100GE1/0/5 split-type 4\*25GE

#将5号口拆分为4个25GE的口，使用1分4线缆

ce8850拆分模式：

|  |  |
| --- | --- |
| mode1 | 所有端口都不可拆分 |
| mode2 | 不可拆分端口：1-4，17-20，33-36，49-52  不可使用的端口：12-16，28-32，44-48，60-64  其余**可拆分**：5-11，21-27，37-43，53-59 |
| mode3 | 不可拆分端口：1-8，17-24，33-40，49-56  不可使用的端口：15-16，31-32，47-48，63-64  其余**可拆分**：9-14，25-30，41-46，57-62 |

**★DDM光口/VCT电口检测**

[Huawei] disp transceiver interface g0/0/1 #显示端口的光功率等信息

[HUAWEI] disp transceiver interface GigabitEthernet0/0/26 verbose

#显示端口的光功率等详细信息

[HUAWEI] int g0/0/23 #先进入目标端口

[HUAWEI-GigabitEthernet0/0/23] virtual-cable-test #vct电口检测

Warning: The command will stop service for a while. Continue? [Y/N]: y

Info: This operation may take a few seconds. Please wait for a moment..done.

Pair A length: Unknown

Pair B length: Unknown

Pair C length: Unknown

Pair D length: Unknown

Pair A state: Ok

Pair B state: Ok

Pair C state: Ok

Pair D state: Ok

Info: The test result is only for reference.

**★端口组操作**

创建一个端口组，并把一些端口放入此组，便于同时对这组端口进行端口相关的操作

[HUAWEI] port-group 1 #创建一个端口组，组号 1

[HUAWEI-port-group-1] group-member g0/0/4 to g0/0/8 #加入成员端口

[HUAWEI-port-group-1]

[HUAWEI-port-group-1] disp this

#

port-group 1

group-member GigabitEthernet0/0/4

group-member GigabitEthernet0/0/5

group-member GigabitEthernet0/0/6

group-member GigabitEthernet0/0/7

group-member GigabitEthernet0/0/8

#

**★端口聚合**

[Huawei] int Eth-Trunk 1 #创建聚合口1

[Huawei-Eth-Trunk1] mode lacp #聚合模式为lacp，或者为：manual

[Huawei-Eth-Trunk1] mode manual load-balance #与lacp二选一

[Huawei-Eth-Trunk1]quit

[Huawei] int g0/0/20

[Huawei-GigabitEthernet0/0/20] eth-trunk 1 #将g0/0/20指定为聚合口1的成员端口

Info: This operation may take a few seconds. Please wait for a moment...done.

[Huawei-GigabitEthernet0/0/20]quit

[Huawei] int g0/0/21

[Huawei-GigabitEthernet0/0/21] eth-trunk 1 #将g0/0/21指定为聚合口1的成员端口

Info: This operation may take a few seconds. Please wait for a moment...done.

[Huawei-GigabitEthernet0/0/21] quit

[Huawei] int eth-trunk 1

[HUAWEI-Eth-Trunk1] trunkport g0/0/2 #直接在聚合口里添加物理成员口

[Huawei-Eth-Trunk1] load-balance src-dst-ip #负载均衡模式

[Huawei-Eth-Trunk1]

[Huawei-Eth-Trunk1] port link-type trunk #聚合口指定为trunk，也可为access

[Huawei-Eth-Trunk1] port trunk allow-pass vlan all

**★端口安全（mac地址绑定及过滤）**

端口安全是对进入端口的报文源mac地址进行过滤

[Huawei] int g0/0/9

[Huawei-GigabitEthernet0/0/9] port-security enable #开启端口安全

[Huawei-GigabitEthernet0/0/9] port-security protect-action protect

#保护模式，也可设置为shutdown

[Huawei-GigabitEthernet0/0/9] port-security max-mac-num 10

#最多允许学习10个mac地址，默认动态学习，

#可设置为sticky模式，学习到的mac不会老化

[Huawei-GigabitEthernet0/0/9] port-security mac-address sticky #sticky模式

[Huawei-GigabitEthernet0/0/9] port-security mac-address sticky 0026-ab03-9f04 vlan 1

#手工添加一条不会老化的mac地址

[Huawei-GigabitEthernet0/0/9]

★端口安全保护动作：

|  |  |
| --- | --- |
| protect | 只丢弃源MAC地址不存在的报文，不上报告警 |
| restrict | 丢弃源MAC地址不存在的报文并上报告警 |
| shutdown | 接口状态被置为error-down，并上报告警 |

[Huawei] error-down auto-recovery cause port-security interval 300

#设置端口因保护关闭的自动恢复时间，300秒，不设置则不会自动恢复shutdown的端口

[Huawei] display mac-address sticky vlan 1 #查看sticky mac表项

[Huawei] display trapbuffer #查看trap告警信息

**★IP和MAC绑定（可绑到端口上）**

[Huawei] user-bind static ip-address 10.1.1.92 mac-address 4c1f-cc6f-0f33 [ int g0/0/3 ]

Info: 1 static user-bind item(s) added. #添加一条静态的ip和mac绑定条目

[Huawei] vlan 1

[Huawei-vlan1] ip source check user-bind enable #在相应vlan上开启ip-mac检查

[Huawei-vlan1]quit

**★端口环路检测**

[Huawei] loopback-detect packet-interval 20 #端口环路检测周期，20秒检测一次

[Huawei] int g0/0/10

[Huawei-GigabitEthernet0/0/10] loopback-detect recovery-time 180

#设置端口恢复时间180秒，默认为3倍interval时间，不能低于3倍interval时间

[Huawei-GigabitEthernet0/0/10] loopback-detect enable #在端口上开启

[Huawei-GigabitEthernet0/0/10] loopback-detect packet vlan 1 to 20

#检测的vlan，有数量限制，一般为32个vlan

[Huawei-GigabitEthernet0/0/10] loopback-detect action shutdown #惩戒动作

[Huawei-GigabitEthernet0/0/10]quit

[Huawei]

[Huawei]loopback-detect enable #在全局上开启，所有端口都开启

**★端口error-down自动恢复**

[HUAWEI] error-down auto-recovery cause bpdu-protection interval 300 #300秒

[HUAWEI] error-down auto-recovery cause ?

as-not-ready The AS is not in service

auto-defend Auto-defend punishing function

bpdu-protection Specify BPDU protection function

efm-remote-failure Dying-gasp, link-fault, critical-event, or timeout

efm-threshold-event Error-frame, error-code, or error-frame-second event

error-statistics Specify CRC error-packet statistics exceed threshold

protection function

link-flap Specify link flap protection function

mac-address-flapping MAC address flapping protection function

port-security Port security protection function

storm-control Storm-control punishing function

transceiver-power-low Specify transceiver power low protection function

**★广播抑制**

[Huawei]int g0/0/3

[Huawei-GigabitEthernet0/0/3] storm-control interval 180 #惩戒时间180秒

[Huawei-GigabitEthernet0/0/3] storm-control action block

#惩戒动作为block阻塞，或者error-down

[Huawei-GigabitEthernet0/0/3] storm-control enable log #开启日志

[Huawei-GigabitEthernet0/0/3] storm-control broadcast min-rate 1000 max-rate 1200

#广播包速率限制为1000 pps最大允许1200 包每秒

[Huawei-GigabitEthernet0/0/3]

[Huawei] error-down auto-recovery cause storm-control interval 180

或者新型号配置方式：

[Huawei-GigabitEthernet2/0/20] storm suppression multicast pts 1000

[Huawei-GigabitEthernet2/0/20] storm suppression broadcast 5

[Huawei-GigabitEthernet2/0/20] storm suppression multicast cir 100 kpbs ？？

**★端口镜像**

[Huawei] observe-port 1 int g0/0/3 #观察口，被镜像的数据流向此端口

[Huawei] int g0/0/2

[Huawei-GigabitEthernet0/0/2] port-mirroring to observe-port 1 both

#设置端口为被镜像口，镜像的数据为both（包含inbound和outbound）

[Huawei-GigabitEthernet0/0/2]quit

[Huawei]

[Huawei] dis port-mirroring #查看端口镜像情况

Port-mirror:

----------------------------------------------------------------------

Mirror-port Direction Observe-port

----------------------------------------------------------------------

GigabitEthernet0/0/2 Both GigabitEthernet0/0/3

----------------------------------------------------------------------

[Huawei]

[Huawei] disp observe-port #查看 观察口

----------------------------------------------------------------------

Index : 1

Untag-packet : No

Forwarding : Yes

Dynamic-alloc : No

Interface : GigabitEthernet0/0/3

**章n、VLAN及STP操作**

**★创建vlan及查看vlan**

[Huawei]vlan 10 #创建vlan 10（建议业务vlan为2到4000）

[Huawei-vlan10] description kefu #描述信息

[Huawei-vlan10] quit

[Huawei]

[Huawei] vlan batch 100 101 102 #批量创建vlan

Info: This operation may take a few seconds. Please wait for a moment...done.

[Huawei]

[Huawei] vlan batch 20 to 30 #批量创建vlan区间（20到30共11个vlan）

Info: This operation may take a few seconds. Please wait for a moment...done.

[Huawei]

[Huawei] disp vlan summary #查看vlan汇总情况

static vlan:

Total 16 static vlan.

1 10 20 to 30 100 to 102

[Huawei] disp port vlan #查看各端口对应的vlan

Port Link Type PVID Trunk VLAN List

-------------------------------------------------------------------------------

Eth-Trunk1 access 1 -

GigabitEthernet2/0/1 auto 1 1-4094

GigabitEthernet2/0/2 auto 1 1-4094

GigabitEthernet2/0/19 trunk 1 1-4094

GigabitEthernet2/0/20 trunk 20 1-2 20 22-23

[Huawei] vlan 10

[Huawei-vlan10] management-vlan

#设置vlan10为管理vlan（可选），管理vlan不能添加端口

[Huawei-vlan10]quit

[Huawei] int vlanif 10 #创建SVI三层虚拟接口

[Huawei-Vlanif10] ip address 10.18.1.1 255.255.255.0 #配置ip

[Huawei-Vlanif10] quit

**★二层口模式（access, trunk）**

[Huawei] int GigabitEthernet 0/0/5

[Huawei-GigabitEthernet0/0/5] port link-type access #设置端口类型为access

[Huawei-GigabitEthernet0/0/5] port default vlan 20 #将端口加入vlan20

[Huawei-GigabitEthernet0/0/5]quit

[Huawei] interface GigabitEthernet 0/0/1

[Huawei-GigabitEthernet0/0/1] port link-type trunk #设置端口为trunk口

[Huawei-GigabitEthernet0/0/1] port trunk pvid vlan 1 #native vlan为1

[Huawei-GigabitEthernet0/0/1] port trunk allow-pass vlan all

#华为的trunk口默认只允许vlan1通过，要手动指定允许通过的vlan

[Huawei-GigabitEthernet0/0/1]quit

[Huawei]

**★vlan-mapping（vlan转换）**

[Huawei-GigabitEthernet2/0/19] qinq vlan-translation enable

[Huawei-GigabitEthernet2/0/19] port vlan-mapping vlan 20 map-vlan 22

#将入站的vlan tag 20改为22，出站自动将22转换回20

**★STP**

[Huawei] stp enable

[Huawei] stp mode stp #stp模式为STP（**默认mstp**）可设为stp,rstp,mstp

#在STP/RSTP中，建议手动配置根桥和备份根桥

[Huawei] stp root primary #指定为根桥

[Huawei] stp root secondary #其他再选一台指定为备份根桥

[Huawei] stp priority 61440 # 0~61440，默认32768，可为 0, 4096, 8192,12288 ...

#设置桥优先级，必须为4096的倍数，如果已设置为根桥/备份根桥 则不能再手动指定桥优先级

#对于网络中部分性能低、网络层次低的交换设备，不适合作为根桥设备，一般会配置其优先级以保证该设备不会成为根桥。

#未指定根桥时，将想要成为根桥的设备优先级可配置为4096，指定根桥时，可将其他设备优先级设置为61440

[Huawei]int g0/0/3

[Huawei-GigabitEthernet0/0/3] stp port priority 240 #设置端口的优先级，16的倍数

# 0~240，默认128，可为0, 16, 32, 48...

#将环路中的某交换设备的端口阻塞从而破除环路，可将其端口优先级设置比缺省值大，使得在选举过程中成为被阻塞的端口。**似乎不生效**！！建议配置端口开销

[Huawei-GigabitEthernet0/0/3] **stp cost 200000** #手动指定端口开销

#存在环路的网络环境中，对于链路速率值相对较小的端口，建议将其路径开销值配置相对较大，以使其在生成树算法中被选举成为阻塞端口（反之则设置小值为根端口）

[Huawei] dis stp brief #查看stp基本情况

MSTID Port Role STP State Protection

0 GigabitEthernet0/0/1 DESI FORWARDING NONE

0 GigabitEthernet0/0/3 DESI FORWARDING NONE #根桥

[Huawei2] disp stp brief

MSTID Port Role STP State Protection

0 GigabitEthernet2/0/11 ALTE DISCARDING NONE

0 GigabitEthernet2/0/13 ROOT FORWARDING NONE #设置了小值开销

0 GigabitEthernet2/0/15 DESI FORWARDING NONE

[Huawei2] int GigabitEthernet2/0/15 #进入端口

[Huawei2-GigabitEthernet2/0/15] stp disable #端口关闭stp协议（不连接交换机的口）

[Huawei2] disp stp int g2/0/11 #查看端口stp信息（开头含网桥stp信息）

CIST RegRoot/IRPC : 61440.60d7-5574-d552 / 0 #本网桥id

Designated Bridge/Port : 0.60d7-5574-fd76 / 128.12 #根桥id及本设备根/指定端口id

\*桥ID == 优先级 + MAC地址 #越小越优先

\*根端口 本交换机中 到根桥的路径开销最小的端口（一台非根桥设备上只有一个根端口）

\*为一对交换机间选指定端口，一条链路（2台交换机之间的）的2个端口，谁到根桥开销小，谁就是指定端口（一台设备可有多个指定端口）

**★网桥优先级和端口优先级**

网桥优先级和端口优先级都是值越小越优先

网桥优先级默认32768，端口默认优先级128，路径开销算法默认802.1t

**★STP端口开销表**

|  |  |  |  |
| --- | --- | --- | --- |
| 端口速率 | 802.1D旧版 | 802.1D-1998开销 | 802.1T/2001开销 |
| 10M | 100 | 100 | 2,000,000 |
| 100M | 10 | 19 | 200,000 |
| 1G | 1 | 4 | 20,000 |
| 10G | 1 | 2 | 2,000 |
| 100G |  |  | 200 |

**★指定端口开销算法**

[HUAWEI] stp pathcost-standard dot1t

[HUAWEI]stp pathcost-standard ?

dot1d-1998 IEEE 802.1D-1998

dot1t IEEE 802.1T #默认

legacy Legacy

**★超时设置**

Forward Delay Time默认15秒，

Hello Time默认2秒

Max Age Time默认20秒

**★RSTP**

基础配置同STP

[Huawei] stp enable

[Huawei] stp mode rstp #stp模式为**RSTP**（**默认mstp**）可设为stp,rstp,mstp

#在STP/RSTP中，建议手动配置根桥和备份根桥

[Huawei] stp root primary #指定为根桥

[Huawei] stp root secondary #其他再选一台指定为备份根桥

[Huawei] stp priority 61440 # 0~61440，默认32768，可为 0, 4096, 8192,12288 ...

#设置桥优先级，必须为4096的倍数，如果已设置为根桥/备份根桥 则不能再手动指定桥优先级

#对于网络中部分性能低、网络层次低的交换设备，不适合作为根桥设备，一般会配置其优先级以保证该设备不会成为根桥。

#未指定根桥时，将想要成为根桥的设备优先级可配置为4096，指定根桥时，可将其他设备优先级设置为61440

**★RSTP边缘端口配置**

[Huawei1] int GigabitEthernet1/0/23

[Huawei1-GigabitEthernet1/0/23] stp edged-port enable #设置为边缘端口

[Huawei1-GigabitEthernet1/0/23] stp bpdu-filter enable #开启bpdu报文过滤

#配置为边缘端口后，端口仍然会发送BPDU报文，这可能导致BPDU报文发送到其他网络，使其他网络产生震荡。因此可以配置边缘端口的BPDU报文过滤功能，使边缘端口不处理、不发送BPDU报文。

**★开启BPDU保护功能**

[Huawei1] stp bpdu-protection

[Huawei1] error-down auto-recovery cause bpdu-protection interval 180

#开启bpdu保护后，如果边缘端口收到bpdu报文入站，则error-down，可配置error-down自动恢复

**★开启TC保护功能**

[Huawei1] stp tc-protection interval 10 #默认为hello time时间，2秒

[Huawei1] stp tc-protection threshold 5 #默认为1个报文

#如果在单位时间内，交换设备在收到TC BPDU报文数量大于配置的阈值，那么设备只会处理阈值指定的次数。

**★开启根保护功能**

[Huawei1] int g1/0/18 #仅在指定端口上配置

[Huawei1-GigabitEthernet1/0/18] stp root-protection

#开启根保护的端口不可以再配置环路保护

#根保护功能只能在指定端口上配置生效

**★开启环路保护**

[Huawei1] int g1/0/20 #交换机的根端口及Alternate端口上都要开启

[Huawei1-GigabitEthernet1/0/20] stp loop-protection

#开启环路保护的端口不可再配置根保护

#环路保护功能只能在根端口或Alternate端口上配置生效

**★RSTP点对点链路**

与点对点链路相连的两个端口如果为根端口或者指定端口，则端口可以通过传送同步报文（Proposal报文和Agreement报文）快速迁移到转发状态，减少了不必要的转发延迟时间。

[Huawei2] int GigabitEthernet2/0/15 #进入端口

[Huawei2-GigabitEthernet2/0/15] stp point-to-point force-true #配置为点对点链路

**★端口不使用增强的快速迁移机制**

[Huawei1] int g1/0/18 #进入参与stp协议计算的端口

[Huawei1-GEt1/0/18] stp no-agreement-check #端口使用普通的快速迁移方式，默认使用增强的快速迁移机制

[Huawei1] display stp topology-change #查看stp拓扑变化统计信息

CIST topology change information

Number of topology changes : 3

Time since last topology change : 0 days 0h:18m:13s

Topology change initiator(notified) :GigabitEthernet1/0/13

Topology change last received from :60d7-5574-d552

Number of generated topologychange traps : 2

Number of suppressed topologychange traps: 0

**★STP/RSTP超时时间**

[Huawei2] disp stp global #先查看STP全局配置信息

Protocol Status : Enabled

Bpdu-filter default : Disabled

Tc-protection : Enabled

Tc-protection threshold : 1

Tc-protection interval : 2s

Edged port default : Disabled

Pathcost-standard : Dot1t

Timer-factor : 3 # 默认3

Transmit-limit : 6

Bridge-diameter : 7 #直径7

-------[CIST Global Info][Mode RSTP]-------

CIST Bridge : 61440.60d7-5574-d552 #本网桥id

Config Times :Hello 2s MaxAge 20s FwDly 15s MaxHop 20

Active Times :Hello 2s MaxAge 20s FwDly 15s MaxHop 20

CIST Root/ERPC :0 .60d7-5574-fd76 / 2000

CIST RegRoot/IRPC :61440.60d7-5574-d552 / 0

CIST RootPortId :16.14 (GigabitEthernet2/0/13) #本设备的根端口

BPDU-Protection :Disabled

TC or TCN received :252

TC count per hello :0

STP Converge Mode :Normal

Share region-configuration :Enabled

Time since last TC :0 days 0h:4m:1s

Number of TC :92

Last TC occurred :GigabitEthernet2/0/13

[Huawei1] stp bridge-diameter 7 #设置stp网络直径，2~7，默认7，值越大表示网络直径越大

值为2时：

Active Times :Hello 2s MaxAge 10s FwDly 7s MaxHop 20

值为3时：

Active Times :Hello 2s MaxAge 12s FwDly 9s MaxHop 20

**默认值7时**：

Active Times :Hello 2s MaxAge 20s FwDly 15s MaxHop 20

★如果设备在超时时间（超时时间＝Hello Time **×** 3 **×** Timer Factor）内没有收到上游设备发送的BPDU，则生成树会重新进行计算。

[Huawei2] stp timer-factor 3 # 1~10，默认3倍

\*建议配置网络直径，而不是直接修改超时时间

\*根交换设备的Hello Time、Forward Delay以及Max Age三个时间参数取值之间应该满足如下公式，否则网络会频繁震荡：

• 2 × (Forward Delay － 1 second) >= Max Age

• Max Age >= 2 × (Hello Time + 1 second)

[Huawei1] stp timer forward-delay 1500 #15秒，单位10毫秒，取值400~3000

[Huawei1] stp timer hello 200 #2秒，单位10毫秒，取值100~1000

[Huawei1] stp timer max-age 2000 #20秒，单位10毫秒，取值600~4000

**★华为与思科互通rstp**

[Huawei1-GigabitEthernet1/0/18] stp compliance dot1s

#在自适应模式下，本端口收到对端的报文，本端能够解析且转发此报文

[Huawei1-GigabitEthernet1/0/18] stp config-digest-snoop

#使能摘要侦听功能可以使交换机的BPDU报文密钥与其他设备制造商设备的BPDU报文密钥一致。

•如果其他厂商设备运行标准的STP/RSTP协议，交换机均可与之对接。

•如果其他厂商设备运行非标准STP/RSTP协议（cisco的pvst除外），部分交换机可在端口下配置stp disable、bpdu enable、l2protocol-tunnel enable命令实现与该厂商设备STP/RSTP报文透传。

•对cisco设备，如果起了pvst，交换机现有版本无法参与协商计算，但是可以透传报文

**★MSTP**

[Huawei] stp enable

[Huawei] stp mode mstp

[Huawei] stp region-configuration //进入mstp配置模式

[Huawei-mst-region] region-name mstp1 //设置mstp域名为mstp1

[Huawei-mst-region] revision-level 1 //设置修定级别为1

[Huawei-mst-region] instance 1 vlan 1 to 3 //实例与vlan绑定

[Huawei-mst-region] instance 2 vlan 9 to 11

[Huawei-mst-region] active region-configuration //激活mstp域配置

Info: This operation may take a few seconds. Please wait for a moment...done.

[Huawei-mst-region]

[Huawei] stp instance 1 priority 4096 //设置本交换机的实例1的桥优先级

[Huawei] stp instance 0 root primary //将本交换机指定为实例0的根

[Huawei] dis stp region-configuration //查看mstp域配置

Oper configuration

Format selector :0

Region name :mstp1

Revision level :1

Instance VLANs Mapped

0 4 to 8, 12 to 4094

1 1 to 3

2 9 to 11

[Huawei]

[Huawei]int g0/0/2

[Huawei-GigabitEthernet0/0/2]stp edged-port enable //设置为边缘端口

[Huawei-GigabitEthernet0/0/2]quit

[Huawei]int g0/0/3

[Huawei-GigabitEthernet0/0/3]stp loop-protection //非根桥的上联口开启环路保护

[Huawei-GigabitEthernet0/0/3]quit

[Huawei]int g0/0/4

[Huawei-GigabitEthernet0/0/4]stp root-protection //根桥上指定端口保护

[Huawei-GigabitEthernet0/0/4]quit

[Huawei]stp bpdu-protection //全局下所有边缘端口开启BPDU防护

**章n、DHCP配置**

**★DHCP服务器**

[Huawei]dhcp enable //开启dhcp服务

Info: The operation may take a few seconds. Please wait for a moment.done.

[Huawei]int vlanif 1

[Huawei-Vlanif1]ip addr 10.1.1.1 255.255.255.0 //先配置vlanif的IP

[Huawei-Vlanif1]dhcp select global //dhcp使用本地全局的

[Huawei-Vlanif1]quit

[Huawei]ip pool vlan1 //创建地址池vlan1

Info:It's successful to create an IP address pool.

[Huawei-ip-pool-vlan1]gateway-list 10.1.1.1 //网关为10.1.1.1

[Huawei-ip-pool-vlan1]network 10.1.1.0 mask 255.255.255.0 //配置网络

[Huawei-ip-pool-vlan1]excluded-ip-address 10.1.1.2 10.1.1.10 //排除地址，不分配10.1.1.2~10

[Huawei-ip-pool-vlan1]lease day 5 hour 4 minute 0 //租期为5天4小时0分钟

[Huawei-ip-pool-vlan1]dns-list 10.1.1.20 114.114.114.114 //dns列表

[Huawei-ip-pool-vlan1]static-bind ip-address 10.1.1.99 mac-address 1418-7709-2fd8

//给目标mac分配固定的IP地址

[Huawei-ip-pool-vlan1]quit

[Huawei]dis dhcp statistics //查看dhcp报文收发情况

[Huawei]dis ip pool name vlan1 //查看地址池vlan1的信息，IP分配情况等

Pool-name : vlan1

... ...

VPN instance : --

-----------------------------------------------------------------------------

Start End Total Used Idle(Expired) Conflict Disable

-----------------------------------------------------------------------------

10.1.1.1 10.1.1.254 253 1 243(0) 0 9

-----------------------------------------------------------------------------

[Huawei]

<Huawei>reset ip pool name vlan1 ? //收回分配的IP地址，可以是某个范围，也可

X.X.X.X Start IP address //以是全部收回

all All IP address

conflict Conflict IP address

expired Expired IP address

used Used IP address

执行命令dhcp server bootfile bootfile，配置DHCP客户端的启动配置文件名称。

缺省情况下，未配置DHCP客户端的启动配置文件名称。

5.执行命令dhcp server sname sname，配置DHCP客户端获取启动配置文件的服务器名称。

缺省情况下，未配置DHCP客户端获取启动配置文件的服务器名称。

6.执行命令dhcp server next-server ip-address，指定客户端获取IP地址后下一步使用的文件服务器IP地址。

缺省情况下，DHCP服务器未指定客户端下一步使用的文件服务器IP地址。

•基于全局方式：

1.执行命令system-view，进入系统视图。

2.执行命令ip pool ip-pool-name，进入全局地址池视图。

3.执行命令bootfile bootfile，配置DHCP客户端的启动配置文件名称。

缺省情况下，未配置DHCP客户端的启动配置文件名称。

4.执行命令sname sname，配置DHCP客户端获取启动配置文件的服务器名称。

缺省情况下，未配置DHCP客户端获取启动配置文件的服务器名称。

5.（可选）执行命令next-server ip-address ，配置客户端自动获取IP地址后下一步使用的文件服务器地址。

缺省情况下，未配置客户端自动获取IP地址后下一步使用的文件服务器地址。

**★DHCP中继**

[Huawei]int vlan1

[Huawei-Vlanif1]dhcp select relay //配置DHCP模式为中继

[Huawei-Vlanif1]dhcp relay server-ip 10.2.2.33 //配置中继服务器

**★DHCP保存地址分配信息**

[Huawei]dhcp server database enable //开启保存地址分配信息的服务

Info: The operation may take a few seconds, please wait.

done.

[Huawei]dhcp server database recover //使用单一文件保存

[Huawei]dhcp server database write-delay 300 //每分配一个地址后延迟300秒再保存

[Huawei]dis dhcp server database //查看database信息

Status: enable

Recover from files after reboot: enable

File saving lease items: flash:/dhcp/lease.txt //分配信息保存的文件

File saving conflict items: flash:/dhcp/conflict.txt //地址冲突信息保存的文件

Save Interval: 300 (seconds)

[Huawei]

**★DHCP Snooping**

[Huawei]dhcp snooping enable //开启dhcp snooping

[Huawei]int g0/0/1

[Huawei-GigabitEthernet0/0/1]dhcp snooping enable //接口上开启

[Huawei-GigabitEthernet0/0/1]dhcp snooping trusted //上联口一定要设置为信任口

[Huawei-GigabitEthernet0/0/1]quit

[Huawei]int g0/0/xxx //所有下联口，接终端机的，都要开启dhcp snooping

[Huawei-GigabitEthernet0/0/3]dhcp snooping enable

[Huawei-GigabitEthernet0/0/3]quit

[Huawei]vlan 1

[Huawei-vlan1]ip source check user-bind enable //在vlan上应用ip-mac绑定过滤策略

//只有由交换机分配的ip和对应的mac包才允许进入

Info: Add permit rule for dynamic snooping bind-table, please wait a minute!done.

[Huawei-vlan1]

**章n、ARP及MAC相关命令**

**★ARP操作**

<Huawei> dis arp #查看ARP表

# IP地址 MAC地址 过期时间（分钟） 类型 接口 vpn实例 vlan

IP ADDRESS MAC ADDRESS EXPIRE(M) TYPE INTERFACE VPN-INSTANCE VLAN

------------------------------------------------------------------------------

10.1.1.1 4c1f-ccb2-5fd9 I - Vlanif1

10.1.1.3 4c1f-cc28-6616 20 D-0 GE0/0/1 1

10.1.1.2 4c1f-cc6f-0dba 20 D-0 GE0/0/2 1

------------------------------------------------------------------------------

Total:3 Dynamic:2 Static:0 Interface:1

<Huawei>

[Huawei] arp static 10.1.1.3 4c1f-cc28-6616 #添加静态arp条目

[Huawei]

[Huawei] int vlan 1

[Huawei-Vlanif1] arp-proxy enable #在vlan接口上开启arp代理

[Huawei-Vlanif1] arp-proxy enable anyway #在vlan接口上开启arp代理

[Huawei-Vlanif1]

[Huawei] arp gratuitous-arp send enable #开启免费arp功能

[Huawei] arp gratuitous-arp send interval 20 #免费arp发包周期为20秒

[Huawei]

[Huawei] arp speed-limit source-mac maximum 50 #限制arp发包速率为50个每秒

[Huawei] arp speed-limit source-mac 4c1f-cc28-6616 maximum 5

#限制指定源mac的arp发包速率

[Huawei]

[Huawei] int vlan 1

[Huawei-Vlanif1] arp expire-time 180 #设置arp老化时间为180秒，默认是20分钟

[Huawei-Vlanif1] arp time-out 30 #设置arp老化时间为30秒（新设备配置方式）

#如果配置为30秒，则需要全局开启：

[Huawei] arp constant-send enable

[Huawei] arp ip-conflict-detect enable #开启ip地址冲突检测

**★MAC操作**

[Huawei] dis mac-address #查看mac地址表

MAC address table of slot 0:

MAC Address VLAN/VSI/BD Learned-From Type

-------------------------------------------------------------------------------

60d7-5574-fd76 1/-/- GE2/0/15 sticky

94c6-915c-9bff 1/-/- GE2/0/23 dynamic

Total matching items on slot 0 displayed = 2

[Huawei]

[Huawei] mac-address aging-time 300 #设置mac老化时间，默认为300秒

[Huawei] mac-address static 4c1f-cc28-6616 g0/0/3 vlan 1 #添加静态mac条目

[Huawei]

[Huawei] mac-address blackhole 4c1f-cc28-992f vlan 1 #黑洞mac

[Huawei]

**章n、访问控制及Qos流量控制**

**★ACL访问控制列表**

**★ACL编号及基础配置**

|  |  |  |
| --- | --- | --- |
| acl number | 类型 | 匹配对象 |
| 2000~2999 | 基本acl | 源ip |
| 3000~3999 | 扩展acl | 源ip，目的ip，tcp/udp的源port，目的port，IP上层协议号 |
| 4000~4999 | 二层acl | mac地址，vlanID |

★默认最后有一条permit any，记得必要时请在末尾一条rule添加deny any

[Huawei]acl number 2000 //创建基本acl

[Huawei-acl-basic-2000]rule 1 permit source 10.1.1.0 0.0.0.255 //匹配源网段，反掩码

[Huawei-acl-basic-2000]rule 10 permit source 10.1.2.22 0 //匹配源ip，掩码为0

[Huawei-acl-basic-2000]quit

[Huawei]acl number 3000 //创建扩展 acl

[Huawei-acl-adv-3000]rule 1 permit ip source 10.1.1.0 0.0.0.255 destination

10.18.0.0 0.0.255.255 //ip地址只能用反掩码

[Huawei-acl-adv-3000]rule 5 permit tcp source 10.0.0.0 0.255.255.255 source-port

eq 40 destination any destination-port range 10 99

[Huawei-acl-adv-3000]quit

[Huawei]acl number 4000 //创建二层acl

[Huawei-acl-L2-4000]rule 1 permit source-mac 4c1f-cc28-6616 ffff-ffff-ffff //匹配mac

destination-mac 4c1f-cc28-6617 ffff-ffff-ffff //使用正掩码

[Huawei-acl-L2-4000]quit

[Huawei]int g0/0/9

[Huawei-GigabitEthernet0/0/9]traffic-filter inbound acl 2000 //应用acl到接口上

[Huawei-GigabitEthernet0/0/9]quit

**★ACL时间**

[Huawei]time-range time1 from 18:00 2019/12/04 to 23:00 2019/12/06 //匹配一段时间

[Huawei]time-range time2 10:00 to 15:30 daily //匹配一个周期，每天的某个时段

[Huawei]time-range time3 15:00 to 19:30 ? //也可以是指定的星期几

<0-6> Day of the week(0 is Sunday)

Fri Friday

Mon Monday

Sat Saturday

Sun Sunday

Thu Thursday

Tue Tuesday

Wed Wednesday

daily Every day of the week

off-day Saturday and Sunday

working-day Monday to Friday

★ACL应用注意事项

**★Qos限速策略**

[Huawei]traffic classifier class1 //定义流类

[Huawei-classifier-class1]if-match any //匹配数据，可以是所有数据，也可用acl限定

[Huawei-classifier-class1]quit

[Huawei]traffic behavior behav1 //定义流行为

[Huawei-behavior-behav1]car cir 1000 cbs 150000 pbs 200000 //单位:Kbit/s, byte/s,byte/s

[Huawei-behavior-behav1]quit

[Huawei]traffic policy policy1 //定义流策略

[Huawei-trafficpolicy-policy1]classifier class1 behavior behav1 //策略使用的流类及流行为

[Huawei-trafficpolicy-policy1]quit

[Huawei]

[Huawei]int g0/0/3

[Huawei-GigabitEthernet0/0/3]traffic-policy policy1 inbound //在接口上使用策略

[Huawei-GigabitEthernet0/0/3]traffic-policy policy1 outbound //2个方向上都可应用

[Huawei-GigabitEthernet0/0/3]quit

<Huawei>dis traffic-policy applied-record policy1 //查看策略的应用情况

-------------------------------------------------

Policy Name: policy1

Policy Index: 2

Classifier:class1 Behavior:behav1

-------------------------------------------------

\*interface GigabitEthernet0/0/3

traffic-policy policy1 inbound

slot 0 : success

\*interface GigabitEthernet0/0/3

traffic-policy policy1 outbound

slot 0 : success

-------------------------------------------------

Policy total applied times: 2.

<Huawei>

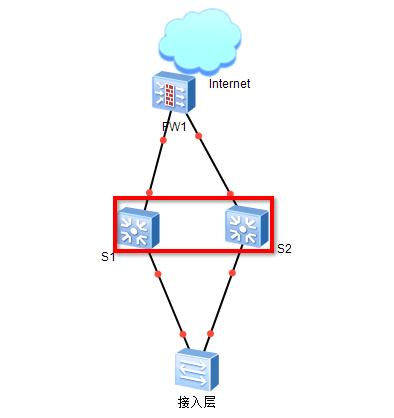
**★流量统计**

在

**34. VRRP（要配合mstp）**

VRRP只有advertisment报文，报文传播使用组播地址224.0.0.18，报文封装在IP报文中，上层协议号为118，Virtual Router的mac地址为0000-5E00-01-vrid

优先级默认为100，越大越优先



拓扑如上图

S1（10.10.1.1）和S2（10.10.1.2）虚拟成一个网关（10.10.1.254）vlan10

S1上的配置如下（S2上的配置省略）

[Huawei]vrrp virtual-ip ping enable //允许ping虚拟网关，必须在配置vrrp之前开启

[Huawei]int vlan 10

[Huawei-Vlanif10]ip add 10.10.1.1 255.255.255.0

[Huawei-Vlanif10]vrrp vrid 10 virtual-ip 10.10.1.254 //虚拟网关ip

[Huawei-Vlanif10]vrrp vrid 10 priority 120 //优先级为120，目的是让其成为master

[Huawei-Vlanif10]vrrp vrid 10 track int g0/0/24 reduced 30

//如果上联口断了则降低优先级，减30，变成备份的

[Huawei-Vlanif10]vrrp vrid 10 preempt-mode timer delay 5 //抢占延迟时间设为5秒

[Huawei-Vlanif10]vrrp vrid 10 preempt-mode disable //或者 关闭抢占模式

[Huawei-Vlanif10]quit

[Huawei]vrrp gratuitous-arp timeout 30 //设置vrrp的免费arp发送周期，30秒

[Huawei]dis vrrp brief //查看vrrp信息

VRID State Interface Type Virtual IP

----------------------------------------------------------------

10 Initialize Vlanif10 Normal 10.10.1.254

----------------------------------------------------------------

Total:1 Master:0 Backup:0 Non-active:1

[Huawei]

**章n、路由配置**

**★vpn实例（VRF虚拟路由表）**

vpn-instance == Virtual Routing Forwarding

[AR2220-R2] ip vpn-instance vpn22 #创建vpn实例，名为vpn22

[AR2220-R2-vpn-instance-vpn22] description vpn22-manager

[AR2220-R2-vpn-instance-vpn22] ipv4-family

[AR2220-R2-vpn-instance-vpn22-af-ipv4] route-distinguisher 22:10 # RD

[AR2220-R2-vpn-instance-vpn22-af-ipv4] vpn-target 22:10 export-extcommunity # eRT

[AR2220-R2-vpn-instance-vpn22-af-ipv4] vpn-target 22:10 import-extcommunity # iRT

[AR2220-R2] int GigabitEthernet0/0/0 #进入三层接口

[AR2220-R2-GigabitEthernet0/0/0] ip binding vpn-instance vpn22

#三层口绑定vpn实例，所有ip相关配置都会清空

[AR2220-R2-GigabitEthernet0/0/0] ip add 22.22.22.1 24 #重新配置ip地址

[AR2220-R2-GigabitEthernet0/0/0] quit

[Huawei] int Vlanif 22 #进入vlanif接口

[Huawei-Vlanif22] ip binding vpn-instance vpn22 #三层口绑定vpn实例

[Huawei] disp ip routing-table #查看默认路由表（public）

[Huawei] disp ip routing-table vpn-instance vpn22 #查看指定的vpn实例路由表

**★静态路由配置**

[Huawei]ip route-static 10.19.0.0 255.255.0.0 10.1.1.2 preference 30 #配置静态路由

[Huawei] #目的网络 子网掩码 下一跳地址 路由优先级

[Huawei]dis ip routing-table #查看路由表

Route Flags: R - relay, D - download to fib

------------------------------------------------------------------------------

Routing Tables: Public

Destinations : 5 Routes : 5

Destination/Mask Proto Pre Cost Flags NextHop Interface

10.1.1.0/24 Direct 0 0 D 10.1.1.1 Vlanif1

10.1.1.1/32 Direct 0 0 D 127.0.0.1 Vlanif1

**10.19.0.0/16** Static 30 0 RD 10.1.1.2 Vlanif1

127.0.0.0/8 Direct 0 0 D 127.0.0.1 InLoopBack0

127.0.0.1/32 Direct 0 0 D 127.0.0.1 InLoopBack0

**★单臂路由**

[Huawei]int g0/0/2.10

[Huawei-GigabitEthernet0/0/2.10]dot1q termination vid 10

[Huawei-GigabitEthernet0/0/2.10]ip add 192.168.10.254 255.255.255.0

[Huawei-GigabitEthernet0/0/2.10]arp broadcast enable

[Huawei-GigabitEthernet0/0/2.10]quit

[Huawei]int g0/0/2.20

[Huawei-GigabitEthernet0/0/2.20]dot1q termination vid 20

[Huawei-GigabitEthernet0/0/2.20]ip add 192.168.20.254 255.255.255.0

[Huawei-GigabitEthernet0/0/2.20]arp broadcast enable

[Huawei-GigabitEthernet0/0/2.20]quit

[Huawei]

**★黑洞路由**

[Huawei] ip route-static 10.255.255.0 255.255.255.0 NULL 0

**★RIP**

[Huawei]rip 1 #开启rip进程1

[Huawei-rip-1]version 2 #版本为v2

[Huawei-rip-1]undo summary #关闭路由自动汇总

[Huawei-rip-1]preference 50 #设置路由优先级

[Huawei-rip-1]network 10.0.0.0 #宣告网段

[Huawei-rip-1]import-route ospf 1 cost 5 #路由引入（重分布）

[Huawei-rip-1]default-route originate cost 2 #引入默认路由（0.0.0.0）

[Huawei-rip-1]silent-interface g0/0/2 #rip进程里指定 静默接口

[Huawei-rip-1]quit

[Huawei]int g0/0/1

[Huawei-GigabitEthernet0/0/1]rip authentication-mode md5 nonstandard plain xxxx 1

#设置rip端口验证

**★OSPF**

[Huawei]ospf router-id 10.1.1.252 1 #开启ospf进程1，同时指定router-id

Info: The configuration succeeded. You need to restart the OSPF process to valid

ate the new router ID.

[Huawei-ospf-1]

[Huawei-ospf-1]area 0

[Huawei-ospf-1-area-0.0.0.0]network 10.1.1.0 0.0.0.255 #在区域0宣告网段

[Huawei-ospf-1-area-0.0.0.0]quit

[Huawei-ospf-1]area 1

[Huawei-ospf-1-area-0.0.0.1]network 10.2.2.0 0.0.0.255 #在区域1宣告网段

[Huawei-ospf-1-area-0.0.0.1]quit

[Huawei-ospf-1]area 0

[Huawei-ospf-1-area-0.0.0.0]authentication-mode md5 1 cipher xxxx #区域0开启区域验证

[Huawei-ospf-1-area-0.0.0.0]quit

[Huawei-ospf-1]import-route rip 1 cost 20000 #路由引入（重分布）

[Huawei-ospf-1]default-route-advertise cost 20000 #引入默认路由（0.0.0.0）

[Huawei-ospf-1]area 1

[Huawei-ospf-1-area-0.0.0.1]vlink-peer 10.2.2.33 #虚链路对端

[Huawei-ospf-1-area-0.0.0.1]quit

[Huawei]dis ospf peer brief #查看ospf邻居及相关信息

[Huawei]dis ospf lsdb #查看ospf链路状态数据库

**★BGP**

在

**★策略路由**

[Huawei]traffic classifier class2 //定义流类

[Huawei-classifier-class2]if-match acl 2000 //匹配acl，该acl匹配目标流量

[Huawei-classifier-class2]quit

[Huawei]traffic behavior behav2 //定义流行为

[Huawei-behavior-behav2]redirect ip-nexthop 10.1.1.1 //指定下一跳

[Huawei-behavior-behav2]quit

[Huawei]traffic policy policy2 //定义流策略

[Huawei-trafficpolicy-policy2]classifier class2 behavior behav2 //匹配相应的类和行为

[Huawei-trafficpolicy-policy2]quit

[Huawei]int g0/0/1

[Huawei-GigabitEthernet0/0/1]traffic-policy policy2 inbound //在接口上应用策略

[Huawei-GigabitEthernet0/0/1]quit

[Huawei]dis traffic-policy applied-record //查看策略应用情况

-------------------------------------------------

Policy Name: policy2

Policy Index: 0

Classifier:class2 Behavior:behav2

-------------------------------------------------

\*interface GigabitEthernet0/0/1

traffic-policy policy2 inbound

slot 0 : success

-------------------------------------------------

**★路由策略**

在

**章n、Vxlan配置**

在

**41. PPP**

[Huawei]int s4/0/1

[Huawei-Serial4/0/1]virtualbaudrate 2048000 //设置串口波特率

[Huawei-Serial4/0/1]physical-mode async //串口传输模式设为异步的

[Huawei-Serial4/0/1]physical-mode sync //也可设为同步的（默认是同步的）

[Huawei-Serial4/0/1]link-protocol ppp //封装协议为ppp

[Huawei-Serial4/0/1]ppp authentication-mode chap //ppp使用chap

[Huawei-Serial4/0/1]ppp chap user cof //ppp用户名

[Huawei-Serial4/0/1]ppp chap password cipher xxxxx //ppp用户密码

[Huawei-Serial4/0/1]quit

[Huawei-Serial4/0/1]ppp authentication-mode pap //ppp使用pap

[Huawei-Serial4/0/1]ppp pap local-user cof password cipher xxxx

[Huawei-Serial4/0/1]quit

**42. DNS**

[Huawei]dns resolve //开启dns解析

[Huawei]dns server 8.8.8.8 //设置dns服务器

[Huawei]dns proxy enable //开启dns代理

[Huawei]ip host xx.com 10.1.1.33 //添加本地解析项

[Huawei]ip host ff.com 10.1.1.22

[Huawei]

[Huawei]ping xx.com //测试

PING xx.com (10.1.1.33): 56 data bytes, press CTRL\_C to break

**43. NAT**

**①静态NAT：**一对一映射，映射的公网IP不可与出接口的ip相同

[Huawei]int g0/0/1

[Huawei-GigabitEthernet0/0/1]ip add 100.1.1.1 255.255.255.0 //接口配置公网ip

[Huawei-GigabitEthernet0/0/1]nat server global 100.1.1.2 inside 10.1.1.45 //配置ip转换

[Huawei-GigabitEthernet0/0/1]nat static enable //开启静态NAT

[Huawei-GigabitEthernet0/0/1]quit

**②端口复用PAT**

[Huawei]acl number 2009

[Huawei-acl-basic-2009]rule 1 permit source 10.1.1.0 0.0.0.255 //acl匹配内网网段

[Huawei-acl-basic-2009]quit

[Huawei]int g0/0/1

[Huawei-GigabitEthernet0/0/1]nat outbound 2009 //出接口上应用nat，

//内网ip转换为出接口的ip

[Huawei-GigabitEthernet0/0/1]quit

[Huawei]

**③端口映射**

[Huawei]int g0/0/1

[Huawei-GigabitEthernet0/0/1]nat static protocol tcp global current-interface 8888

inside 10.1.1.22 80

//将外网的接口ip:8888转为内网的10.1.1.22:80

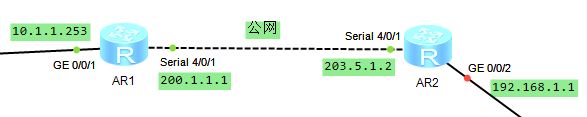
[Huawei-GigabitEthernet0/0/1]nat static protocol tcp global 100.1.1.5 9999 inside 10.1.1.35 443

//将外网的100.1.1.5:9999转为内网的10.1.1.35:443

[Huawei]dis nat session all //查看nat会话情况

**44. IPsec VPN（站到站）**

前提：2端的路由器都要有去往对端内网网段的路由，且要有缺省路由指向网关。



拓扑图如上，AR1的内网为10.1.1.0/24，出接口ip为200.1.1.1，网关200.1.1.2

AR2的内网为192.168.1.0/24，出接口ip203.5.1.2，网关203.5.1.3

**AR1上的配置如下：（AR2的类似）**

**0.配置出接口ip及路由**

[Huawei]int s4/0/1

[Huawei-Serial4/0/1]ip add 200.1.1.1 255.255.255.0

[Huawei-Serial4/0/1]quit

[Huawei]ip route-static 0.0.0.0 0.0.0.0 200.1.1.2

[Huawei]

**1.配置acl匹配目标流**

[Huawei]acl num 3000

[Huawei-acl-adv-3000]rule 1 permit ip source 10.1.1.0 0.0.0.255 destination

192.168.1.0 0.0.0.255

[Huawei-acl-adv-3000]quit

**2.配置ipsec提议**

[Huawei]ipsec proposal pro1 //创建ipsec安全提议

[Huawei-ipsec-proposal-pro1]esp authentication-algorithm sha1 //消息摘要算法

[Huawei-ipsec-proposal-pro1]esp encryption-algorithm aes-128 //数据加密算法

[Huawei-ipsec-proposal-pro1]encapsulation-mode tunnel //使用隧道模式

[Huawei-ipsec-proposal-pro1]quit

**3.配置ike提议**

[Huawei]ike proposal 5

[Huawei-ike-proposal-5]authentication-algorithm sha1

[Huawei-ike-proposal-5]encryption-algorithm aes-cbc-128

[Huawei-ike-proposal-5]authentication-method pre-share

**4.配置ike对端**

[Huawei]ike peer peer1 v1

[Huawei-ike-peer-peer1]pre-shared-key cipher xxxx

[Huawei-ike-peer-peer1]remote-address 203.5.1.2

[Huawei-ike-peer-peer1]ike-proposal 5

[Huawei-ike-peer-peer1]quit

**5.配置ipsec策略**

[Huawei]ipsec policy ipsecp1 10 isakmp

[Huawei-ipsec-policy-isakmp-ipsecp1-10]ike-peer peer1

[Huawei-ipsec-policy-isakmp-ipsecp1-10]proposal pro1

[Huawei-ipsec-policy-isakmp-ipsecp1-10]security acl 3000

**6.出接口上应用ipsec策略**

[Huawei]int s4/0/1

[Huawei-Serial4/0/1]ipsec policy ipsecp1

[Huawei-Serial4/0/1]quit

[Huawei]dis ike proposal //查看ike提议

[Huawei]dis ipsec proposal //查看ipsec提议

[Huawei]dis ike peer //查看ike对端

[Huawei]dis ipsec statistics esp //查看ipsec统计情况

**45. L2TP VPN**

**1.先添加一个用户，用于l2tp拨号的（也可用radius验证）**

[Huawei]aaa

[Huawei-aaa]local-user coflee password cipher xxxx

Info: Add a new user.

[Huawei-aaa]local-user coflee service-type ppp

[Huawei-aaa]quit

**2.配置拨号后的地址池**

[Huawei]ip pool lns

Info: It's successful to create an IP address pool.

[Huawei-ip-pool-lns]network 192.168.33.0 mask 255.255.255.0

[Huawei-ip-pool-lns]gateway-list 192.168.33.1

[Huawei-ip-pool-lns]dns-list 8.8.8.8

[Huawei-ip-pool-lns]quit

**3.配置虚拟接口模板**

[Huawei]int Virtual-Template 1

Dec 5 2019 11:22:41-08:00 Huawei %%01IFPDT/4/IF\_STATE(l)[0]:Interface Virtual-T

emplate1 has turned into UP state.

[Huawei-Virtual-Template1]ip add 192.168.33.1 255.255.255.0

[Huawei-Virtual-Template1]ppp authentication chap

[Huawei-Virtual-Template1]remote address pool lns

[Huawei-Virtual-Template1]quit

[Huawei]

**4.配置l2tp vpn**

[Huawei]l2tp enable

[Huawei]l2tp-group 1

[Huawei-l2tp1]tunnel name LNS

[Huawei-l2tp1]undo tunnel authentication

[Huawei-l2tp1]allow l2tp Virtual-Template 1

[Huawei-l2tp1]quit

**46. PPPoe服务器**

**1.配置虚拟接口模板**

[Huawei]int Virtual-Template 2

Dec 5 2019 11:30:10-08:00 Huawei %%01IFPDT/4/IF\_STATE(l)[1]:Interface Virtual-T

emplate2 has turned into UP state.

[Huawei-Virtual-Template2]ppp authentication-mode chap call-in domain xxx.com

[Huawei-Virtual-Template2]remote address pool pppoe1

[Huawei-Virtual-Template2]ip address unnumbered interface g0/0/2

[Huawei-Virtual-Template2]quit

**2.配置ip地址池**

[Huawei]ip pool pppoe1

Info: It's successful to create an IP address pool.

[Huawei-ip-pool-pppoe1]network 10.1.1.0 mask 255.255.255.0

[Huawei-ip-pool-pppoe1]gateway-list 10.1.1.1

[Huawei-ip-pool-pppoe1]dns-list 8.8.8.8

[Huawei-ip-pool-pppoe1]quit

**3.配置用户认证（使用radius）**

[Huawei]radius-server template rds //创建radius-server模板

Info: Create a new server template.

[Huawei-radius-rds]radius-server shared-key cipher xxxx

[Huawei-radius-rds]radius-server authentication 10.1.1.99 1645 //指定验证服务器及端口

[Huawei-radius-rds]radius-server accounting 10.1.1.99 1645 //指定计费服务器及端口

[Huawei-radius-rds]quit

[Huawei]aaa

[Huawei-aaa]authentication-scheme rdsAuth //创建验证方案

Info: Create a new authentication scheme.

[Huawei-aaa-authen-rdsAuth]authentication-mode radius //验证模式用radius

[Huawei-aaa-authen-rdsAuth]quit

[Huawei-aaa]accounting-scheme rdsAcct //创建计费方案

Info: Create a new accounting scheme.

[Huawei-aaa-accounting-rdsAcct]accounting-mode radius

[Huawei-aaa-accounting-rdsAcct]quit

[Huawei-aaa]domain xxx.com //创建域

Info: Success to create a new domain.

[Huawei-aaa-domain-xxx.com]authentication-scheme rdsAuth

[Huawei-aaa-domain-xxx.com]accounting-scheme rdsAcct

[Huawei-aaa-domain-xxx.com]radius-server rds

[Huawei-aaa-domain-xxx.com]quit

[Huawei-aaa]quit

[Huawei]

[Huawei]domain xxx.com admin //指定该域为默认的，缺省的域，当用户拨号时若

//不指定域名，则缺省为该域，然后使用该域的验证方案和计费方案，即radius

**4.接口上应用**

[Huawei]int g0/0/2

[Huawei-GigabitEthernet0/0/2]pppoe-server bind virtual-template 2

[Huawei-GigabitEthernet0/0/2]mtu 1492 //因为pppoe报文占8字节开销

[Huawei-GigabitEthernet0/0/2]quit

[Huawei]dis pppoe-server session all //查看pppoe会话情况

**47. PPPoe客户端**

[Huawei]int Dialer 1 //创建拨号接口1

Dec 5 2019 11:46:45-08:00 Huawei %%01IFPDT/4/IF\_STATE(l)[2]:Interface Dialer1 h

as turned into UP state.

[Huawei-Dialer1]link-potocol ppp

[Huawei-Dialer1]ppp chap user cof

[Huawei-Dialer1]ppp chap password cipher xxx

[Huawei-Dialer1]ip address ppp-negotiate

[Huawei-Dialer1]dialer user cof //该用户名同ppp用户

[Huawei-Dialer1]dialer bundle 1

[Huawei-Dialer1]dialer timer idle 300

INFO: The configuration will become effective after link reset.

[Huawei-Dialer1]dialer-group 1

[Huawei-Dialer1]quit

[Huawei]int g0/0/1

[Huawei-GigabitEthernet0/0/1]pppoe-client dial-bundle-number 1

//出接口上配置为pppoe拨号

[Huawei-GigabitEthernet0/0/1]quit

[Huawei]ip route-static 0.0.0.0 0.0.0.0 Dialer 1 //缺省路由下一跳指向拨号接口1

**48. NQA（network quality analysis）**

[Huawei]nqa test-instance admin isp1 //创建nqa探测实例isp1

[Huawei-nqa-admin-isp1]test-type icmp

[Huawei-nqa-admin-isp1]destination-address ipv4 200.1.1.2 //探测目标ip

[Huawei-nqa-admin-isp1]frequency 20 //每20秒探测一次

[Huawei-nqa-admin-isp1]probe-count 2 //每次发2个icmp包

[Huawei-nqa-admin-isp1]interval seconds 4 //每个icmp包时间间隔为4秒

[Huawei-nqa-admin-isp1]timeout 2 //ping超时2秒

[Huawei-nqa-admin-isp1]start now //立即启动nqa探测

[Huawei-nqa-admin-isp1]undo start //关闭nqa

[Huawei-nqa-admin-isp1]start now

[Huawei-nqa-admin-isp1]quit

[Huawei]dis nqa results //#查看nqa结果

[Huawei]dis nqa history //查看nqa历史情况

**nqa一般可以应用在缺省路由和路由策略上**，相关的命令如下：

[Huawei]ip route-static 0.0.0.0 0.0.0.0 10.1.1.2 track nqa admin isp1 //isp1为nqa实例

[Huawei]ip route-static 0.0.0.0 0.0.0.0 20.1.1.2 track nqa admin isp2 //#isp2为nqa实例

//当nqa检测到某个网关ping不通时，就会联动通知路由器取消某条路由或策略

[Huawei]traffic behavior be1

[Huawei-behavior-be1]redirect ip-nexthop 10.1.1.2 track nqa admin isp1

[Huawei-behavior-be1]quit

[Huawei]traffic behavior be2

[Huawei-behavior-be2]redirect ip-nexthop 20.1.1.2 track nqa admin isp2

[Huawei-behavior-be2]quit

**章n、iStack堆叠（虚拟化）**

在

**#设备1**

[HUAWEI] interface stack-port 0/1 #创建堆叠逻辑口（slot-id / stack-port号1-2）

[HUAWEI-stack-port0/1] port interface GigabitEthernet0/0/13 to GigabitEthernet0/0/14 enable

#加入物理成员口（S6720-EI、S6720S-EI设备上的XGE端口从左边开始，每4个为一组（例如，1～4为一组，2～5不能作为一组，即每组最后一个端口的编号为4的倍数），如果将每组内的任意一个接口配置为堆叠物理成员端口，则同组内的另外三个端口下的配置将会丢失，且不能作为普通的业务口来使用）

Warning: Enabling stack function may cause config loss on the interface. Continue? [Y/N]: y

[HUAWEI-stack-port0/1]quit

[HUAWEI] stack slot 0 renumber 1 #设置当前slot id为1，重启后生效

Warning: All the configurations related to the slot ID will be lost after the slot ID is modified.

Do not frequently modify the slot ID because it will make the stack split. Continue? [Y/N]: y

[HUAWEI] stack slot 0 priority 255 #设备当前设备堆叠优先级，1~255，默认100，越大越优先；当前仍为slot 0

Warning: Do not frequently modify the priority because it will make the stack split. Continue? [Y/N]: y

[HUAWEI]quit

<HUAWEI>save

<HUAWEI>reboot

<HUAWEI> disp stack configuration #查看堆叠配置

---------------Configuration on slot 1 Begin---------------

stack enable

stack slot 0 renumber 1

stack slot 1 priority 255

stack reserved-vlan 4093

stack timer mac-address switch-delay 10

interface stack-port 1/1

port interface GigabitEthernet1/0/13 enable

port interface GigabitEthernet1/0/14 enable

interface stack-port 1/2

---------------Configuration on slot 1 End-----------------

**#设备2**

[HUAWEI] interface stack-port 0/2 #创建堆叠逻辑口（stack-port号要和邻居不同）

[HUAWEI-stack-port0/2] port interface GigabitEthernet0/0/13 to GigabitEthernet0/0/14 enable

#加入物理成员口

Warning: Enabling stack function may cause config loss on the interface. Continue? [Y/N]: y

[HUAWEI-stack-port0/2]quit

[HUAWEI] stack slot 0 renumber 2 #设置当前slot id为2，重启后生效

Warning: All the configurations related to the slot ID will be lost after the slot ID is modified.

Do not frequently modify the slot ID because it will make the stack split. Continue? [Y/N]: y

[HUAWEI] stack slot 0 priority 200 #设备当前设备堆叠优先级，1~255，默认100，越大越优先；当前仍为slot 0

Warning: Do not frequently modify the priority because it will make the stack split. Continue? [Y/N]: y

[HUAWEI]quit

<HUAWEI>save

<HUAWEI>reboot

重启后再接线

<HUAWEI> disp stack configuration #查看堆叠配置

<HUAWEI> disp stack #查看堆叠信息

Stack mode: Service-port

Stack topology type: Link

Stack system MAC: 60d7-5574-fd76

MAC switch delay time: 10 min

Stack reserved VLAN: 4093

Slot of the active management port: --

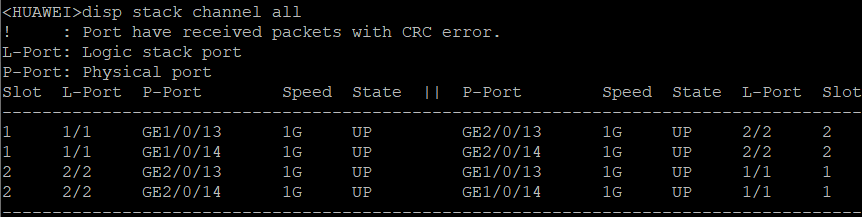
Slot Role MAC Address Priority Device Type

-------------------------------------------------------------

1 Master 60d7-5574-fd76 255 S5735S-L24T4S-A

2 Standby 60d7-5574-d552 200 S5735S-L24T4S-A

<HUAWEI> disp stack channel all #查看stack通道（物理口信息）



**★成员重新加入堆叠集群时会自动重启！**

比如堆叠口断开时，成员退出了堆叠，再连接上时，相当于重新加入集群，重新加入集群的这台设备会自动重启

**★stack物理成员口退出逻辑口**

[switch2] inter stack-port 2/1

[switch2-stack-port2/1] shutdown interface GigabitEthernet2/0/13 to GigabitEthernet2/0/14

[switch2-stack-port2/1] undo port interface GigabitEthernet2/0/13 to GigabitEthernet2/0/14 enable

Warning: Deleting member ports may cause stack split and a loss of all config on the interface. Continue? [Y/N]: y

**★堆叠创建后的配置文件**

<HUAWEI>dir ?

/all List all files

/all-filesystems List files on all filesystems

STRING [drive][path][file name]

flash: Device name #master设备的磁盘

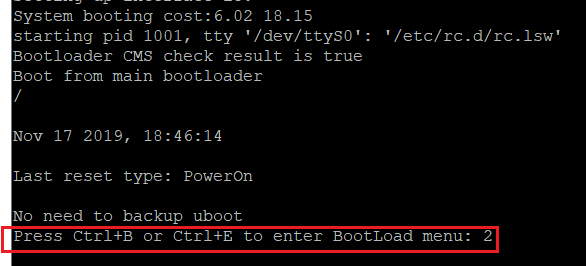
slot2#flash: Device name #standby设备的磁盘

<cr>

**章n、维护模式**

**★恢复密码（保留原配置）**

1.开机或重启设备时，出现Press Ctrl+B or Ctrl+E to xxx字符提示时立即按下 Ctrl键和B键，进入BootRom模式



2.输入BootRom密码：

一般新型号设备密码为 Admin@huawei.com ,旧型号密码为 Admin@huawei

或者是 huawei 或者是 9300

3.进入BootRom后，根据提示输入 6 （清除console密码），yes确定。

The default password is used now. Change the password.

BootLoad Menu

1. Boot with default mode

2. Enter startup submenu

3. Enter ethernet submenu

4. Enter filesystem submenu

5. Enter password submenu

6. Clear password for console user

7. Reboot

(Press Ctrl+E to enter diag menu)

Enter your choice(1-7): 6

Note: Clear password for console user? Yes or No(Y/N): y

Clear password for console user successfully.

Note: Choose "1. Boot with default mode" to boot, then set a new password.

Enter your choice(1-7): 1

或者：

Enter Password: \*\*\*\*\*\*\*\*\*\*\*\*

Default Password,Please Set New Password.

Main Menu

1. Default Startup

2. Serial Menu

3. Network Menu

4. Startup Select

5. File Manager

6. Reboot

7. Password Manager

Enter your choice(1-7): 7

PassWord Menu

1. Modify the menu password

2. Clear the console login password

0. Return

Enter your choice(0-2): 2

Clear the console login password Succeed!

PassWord Menu

1. Modify the menu password

2. Clear the console login password

0. Return

Enter your choice(0-2): 0

Main Menu

1. Default Startup

2. Serial Menu

3. Network Menu

4. Startup Select

5. File Manager

6. Reboot

7. Password Manager

Enter your choice(1-7): 1

4.再输入1（以默认模式进入系统），不要选择 Reboot（重启），不然还是要密码

5.以默认模式进入系统后，一般不要求输入密码，这时我们可以重新配置管理员密码，保存即可。

★有的设备要求配置console登录的初始密码

Please configure the login password (8-16)

Enter Password:

Confirm Password:

Warning: The authentication mode was changed to password authentication and the user level was changed to 15 on con0 at the first user login.

**初始化账号**：

s5735 账号 admin 密码 admin@huawei.com

ar2220默认console密码： admin@huawei

**★维护模式传文件**

在

**章n、防火墙配置**

在

**★创建用户**

[USG6300E] aaa #进入aaa界面

[USG6300E-aaa] manager-user admin #创建一个名为admin的用户

[USG6300E-aaa-manager-user-admin] password cipher passwdxxx #设置密码

[USG6300E-aaa-manager-user-admin] service-type terminal ssh web #账号服务类型

[USG6300E-aaa-manager-user-admin] level 15 #权限级别

[USG6300E-aaa-manager-user-admin] quit

[USG6300E-aaa] bind manager-user admin role system-admin #绑定管理员角色

[USG6300E-aaa] manager-user password valid-days 0 #密码过期时间，单位天

设置为0时表示永不过期，默认90天，设置为0后，初次登录不用强制改密码

**★接口安全域**

[USG6300E] disp zone #查看防火墙的安全域

2022-07-19 21:24:32.550 #默认有以下4个安全域

local

trust

untrust

dmz

#

[USG6300E] firewall zone name internalxx #创建自定义的安全域，名称为internalxx

[USG6300E-zone-internalxx] set priority 80 #设置安全域优先级，1~100

[USG6300E-zone-internalxx] add interface GigabitEthernet0/0/1 #将接口加入安全域

**★安全域流量放通**

[USG6300E] disp security-policy rule all #查看安全策略

★防火墙本地接口上的ip监听的服务（含路由服务）认为自己处于local的安全域，所以假如这个接口配置到了trust安全域，从trust访问此接口上的ip的某服务（如http,ssh,ping,ospf,bgp等），也算是从trust到local，从本地ip访问到外部 则算是从local到trust

[USG6300E] security-policy #进入安全策略配置界面

[USG6300E-policy-security] rule name sec-policy-internalxx-local

#创建一条策略，名为 sec-policy-trust-local

[USG6300E-xx] source-zone internalxx #源安全域

[USG6300E-xx] source-zone local #源安全域

[USG6300E-xx] destination-zone local #目的安全域

[USG6300E-xx] destination-zone internalxx #目的安全域

[USG6300E-xx] source-address 9.9.9.0 0.0.0.255 #源ip网段，反掩码

[USG6300E-xx] destination-address 9.9.9.0 0.0.0.255 #目的ip网段，反掩码

[USG6300E-xx] action permit #匹配后的动作为permit，也可配置为deny

[USG6300E] disp security-policy rule all

2022-07-19 21:41:34.380

Total:2

RULE ID RULE NAME STATE ACTION HITS

-------------------------------------------------------------------------------

2 sec-policy-internalxx-local enable permit 2

0 default enable deny 331

**#有条默认的rule deny所有**

**★接口管理服务配置**

[USG6300E] interface GigabitEthernet0/0/1

[USG6300E-GigabitEthernet0/0/1] ip add 9.9.9.33 255.255.255.0 #配置ip

[USG6300E-GigabitEthernet0/0/1] service-manage ping permit #允许icmp服务

[USG6300E-GigabitEthernet0/0/1] service-manage https permit #允许https服务

[USG6300E-GigabitEthernet0/0/1] service-manage ssh permit #允许ssh服务

[USG6300E-GigabitEthernet0/0/1] service-manage all permit #允许所有服务

**★开启web服务**

#默认开启以下三行配置

web-manager security version tlsv1.1 tlsv1.2 # TLS版本

web-manager enable

web-manager security enable

#

按前面几小节操作即可：

①创建管理员账号并开启web服务类型

②接口配置ip并加入某个安全域

③接口安全域与local安全域放通流量

④接口管理服务开启https与ssh

# https web界面默认8443端口号

如： https://9.9.9.33:8443



