### 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测环境进行实践，请不要直接在真实的服务器中操作！

4.本文档出现的所有设备序列号及其他信息均为作者个人在二手市场购买来专用于实验目的的，不涉及泄露任何公司生产环境的相关信息。

**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/分发/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/分发/再创作 本文档，则说明接受以上2个条款。

作者：李茂福

时间：2024-06-27

**★第0章、安装华为eNSP模拟器及基础配置**

**★安装eNSP**

先到华为官网下载**eNSP模拟器**安装包（官网已下架此软件，民间流传的最新版本为eNSP\_1.3.00.100\_Setup.exe）

然后要先安装以下三个依赖的软件：（先装依赖软件，最后再安装eNSP）

**WinPcap** 官网下载地址： https://www.winpcap.org/install/default.htm

**Wireshark** 官网下载地址： https://www.wireshark.org/#download

**Oracle VM VirtualBox** 官网下载地址： https://www.virtualbox.org/wiki/Downloads 建议用5.2.x版本

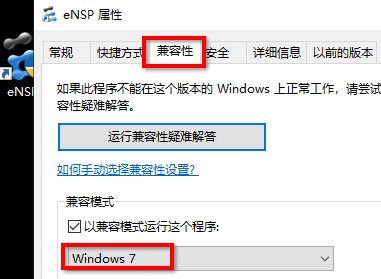
（https://download.virtualbox.org/virtualbox/5.2.44/VirtualBox-5.2.44-139111-Win.exe）

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

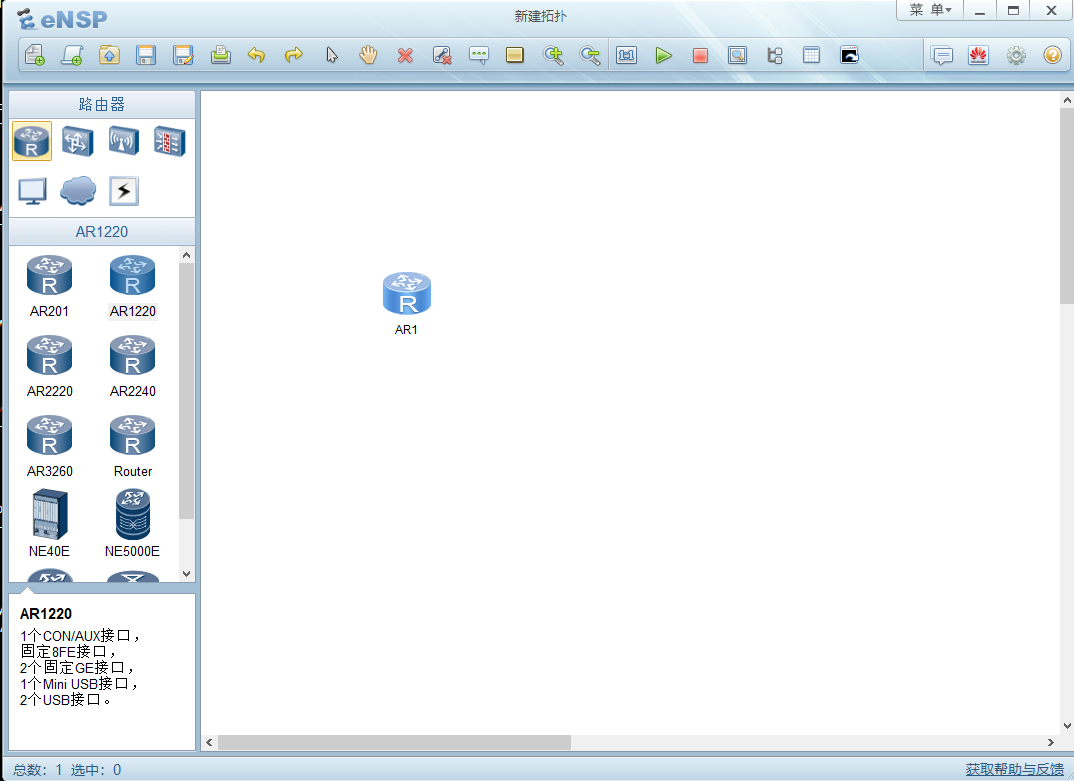
安装的过程就不多介绍了，双击安装，一路Next，装好eNSP模拟器后，找到它的图标：



点击右键，设置属性，将其兼容性改为Windows7，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（有些高级特性命令是在实体设备上配置的）

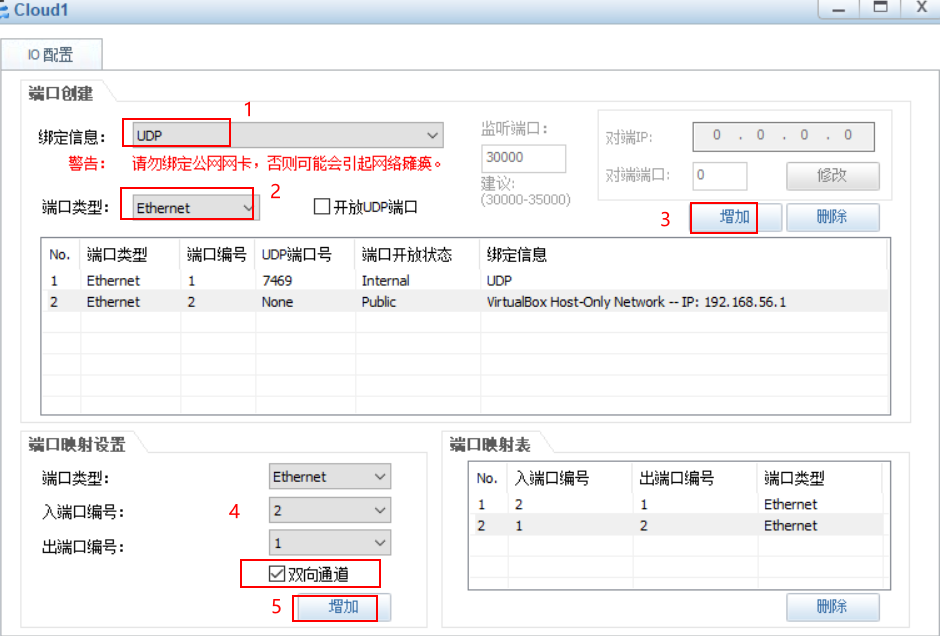
如果有实体硬件设备，那最好是用真实的设备去测试。注意：不要在生产环境中做测试！！

**★宿主机与模拟设备通信**

让宿主机能通过网络访问到eNSP里的模拟设备，在拓扑中添加一朵云（cloud设备）

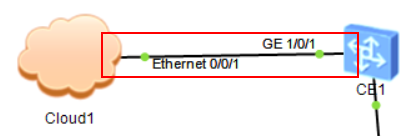


双击云，进行配置，创建2个端口，先创建UDP(Ethernet)，再创建一个ethernet（绑定端口为宿主机上的网卡（如VirtualBox Host-Only Network）



最后添加双向通道映射，入端口为2号，出端口为1号（顺序不可错了）

这时，可以将Cloud设备与其他模拟交换机/路由器连接了



宿主机（个人电脑）的“VirtualBox Host-Only Network”这块网卡配置一个和交换机同网段的ip即可通信

**★第1章、设备基础信息操作**

**★设备基础信息查看**

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

ESN of slot 0: 21980109152SL1604582 #此设备是作者个人在二手市场购买的，正式环境的序列号不可泄露

<HUAWEI> disp esn int #查看端口的（光模块）

<HUAWEI> disp esn all #查看所有，含电源，风扇

<HUAWEI> disp elabel #查看设备电子标签

[Board Properties]

BoardType=S5735S-L24T4S-A

BarCode=21980109152SL1604582

Manufactured=2020-02-12

Model=S5735S-L24T4S-A

<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)

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

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)

<HUAWEI> disp license #查看License许可信息

<HUAWEI> disp device slot 1/7 #查看slot板卡信息

**★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

**★提交/清空候选配置**

#较高型号的设备，如6800及以上系列，为了安全起见，默认配置模式下输入的配置是未提交（未生效）的，此时命令提示符前面有个\*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（此时命令提示符前没有\*号）

如果想让执行的命令立即生效，可进入system-view时加个参数immediately：

<Huawei> system-view immediately #进入立即生效的命令配置界面

[HUAWEI] #此时执行的任何配置命令都是立即生效的

**★保存配置**

[Huawei] return #返回到<>一般模式

<Huawei> save #配置完毕**一定要记得保存配置**，在一般模式下保存；默认保存到vrpcfg.zip

The current configuration will be written to the device.

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> unzip xxx.zip xxx.cfg #解压某.zip文件解压后文件名为xxx.cfg，有的设备必须指定解压后文件名

<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

**★安装模块**

在官网下载相应版本的mod模块文件，然后使用ftp/tftp上传到设备上

> install-module S5735S-L\_V200R022C00SPC500\_WEAKEA.mod

Error: The file hda1:/$\_install\_mod/usg6300e\_v600r007c20spc600\_weakea.mod does not exist on the main board.

在根目录下，直接安装不行，它默认是要到hda1:/$\_install\_mod/子目录下去找组件，所以先复制到此子目录下

> copy S5735S-L\_V200R022C00SPC500\_WEAKEA.mod flash:/$\_install\_mod/S5735S-L\_V200R022C00SPC500\_WEAKEA.mod

> install-module S5735S-L\_V200R022C00SPC500\_WEAKEA.mod

**★license操作**

<HUAWEI> display esn #查看设备序列号

ESN of slot 0: 21980109152SL1604582 #记录下此序列号，然后去找代理商申请相关许可

<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>####### #重启中

**初始化账号及密码**：

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

**★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

**★第2章、设备登录管理配置**

**★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console**

[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

**★带外管理（telnet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接口配置界面，0到4表示开启5条vty线路

[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使用用户名和密码登录**

[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（不建议使用不安全的连接方式，应当禁止telnet服务）**

[Huawei] telnet server disable

[Huawei] telnet ipv6 server disable

**★带外管理（ssh远程登录）**

**SSH用户名和密码登录**

[Huawei] rsa local-key-pair create #创建系统的rsa密钥，6800及以上可以不手动创建

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及以上位数的密钥

Generating keys...

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

[Huawei] user-interface vty 0 4 #进入vty配置界面

[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] user privilege level 15 #有这条配置后，再通过ssh-key密钥方式登录就有管理级别权限

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

[Huawei-ui-vty0-4] quit

先到下一节（aaa创建用户）创建一个帐号；创建好了再继续：

[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 #输入y确定

[Huawei] ssh server-source all-interface #也可设置监听所有接口（与上面一条二选一）

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

Warning: It expandes the range of accessed Ip.

[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

先指定监听的源ip或源端口，再开启ssh服务：

[Huawei] stelnet server enable #开启ssh服务

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

[Huawei] ssh server hmac sha2\_256 #一般只用这个

[Huawei] ssh server dh-exchange min-len 2048 #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\_group\_exchange\_sha256 dh\_group16\_sha512

#至少要有dh\_group14\_sha256

[Huawei] ssh authorization-type default aaa

[Huawei] ssh authentication-type default password

[Huawei] ssh user admin authentication-type password #添加ssh登录用户admin（认证方式还可为all）

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

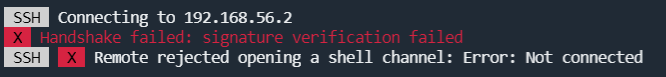
[Huawei] sftp server enable #开启sftp服务，可选

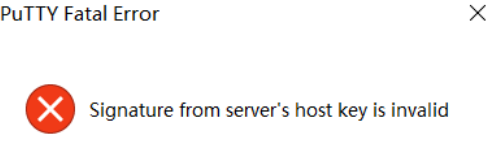
[Huawei] sftp server default-directory flash: #登录sftp后的默认路径

[Huawei] ssh user admin sftp-directory flash: #指定用户的sftp默认路径

**★ssh远程连接失败（不支持ecc）**

[Huawei] ssh server publickey ecc dsa rsa #有些型号的设备默认是3个都有，但优先进行ecc密钥认证，失败则不再尝试其他算法，一般客户端工具只支持dsa和rsa，如果登录不上，请把ecc去除。报错情况一般如下：





**★虚拟终端vty数量限制**

[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）可根据实际需求设置

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

**★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

**★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 #关闭增强型密码安全策略

[Huawei-aaa] local-user policy password expire 90 prompt 7 #密码90天过期，提前7天提醒用户

[Huawei-aaa] local-user authentication lock times 3 15 #密码输错3次锁定15分钟

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

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

#用户权限级别为15（管理员级别），6800及以上型号最高只有3级，设置如下：

[Huawei-aaa] 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，则尝试使用以下设置：**

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

[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 #初次登录不提示用户更改密码

[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（用户名为cof）

[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]

**★用户命令权限级别管理**

默认情况下，权限级别按0～3级进行注册（6800及更高版本）说明如下：

|  |  |  |
| --- | --- | --- |
| level | 说明 | 包含命令 |
| 0 | 参观级 | 网络诊断命令，如ping tracert telnet |
| 1 | 监控级 | 系统维护命令，含display等命令（在某些高版本设备中display命令为管理级level3的命令） |
| 2 | 配置级 | 业务配置命令 |
| 3 | 管理级 | 用于繁育基本运行的命令，如文件系统、ftp、tftp下载以及debugging命令 |

高级别权限包含了所有低级别的权限（如level 2包含了level 0、level 1的所有权限）

低版本的设备（比6800低的）默认是0～15级的权限，如果想让所有设备使用相同的命令级别，可按如下配置：

[Huawei] command-privilege level rearrange #将命令级别批量提升（0-3级别类型提升为0-15级别类型）

命令级别提升后，原命令等级0、1、2、3升级为0、1、10、15级。2～9级和11～14级的命令级别中没有命令行。用户可以单独调整需要的命令行到这些级别中，以实现用户权限的精细化管理。

或者都用0～3级别：

[Huawei] undo command-privilege level rearrange #将命令级别批量降级（0-15级别类型降级为0-3级别类型）

★使用command-privilege命令可配置不同权限级别的用户可以执行哪些命令

**例如：**新建一个测试账号cof，其权限level为0

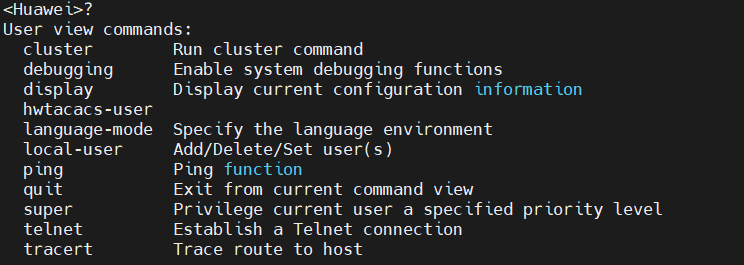
[Huawei] aaa

[Huawei-aaa] local-user cof password cipher xxxxxx

[Huawei-aaa] local-user cof privilege level 0

[Huawei-aaa] local-user cof service-type terminal ssh

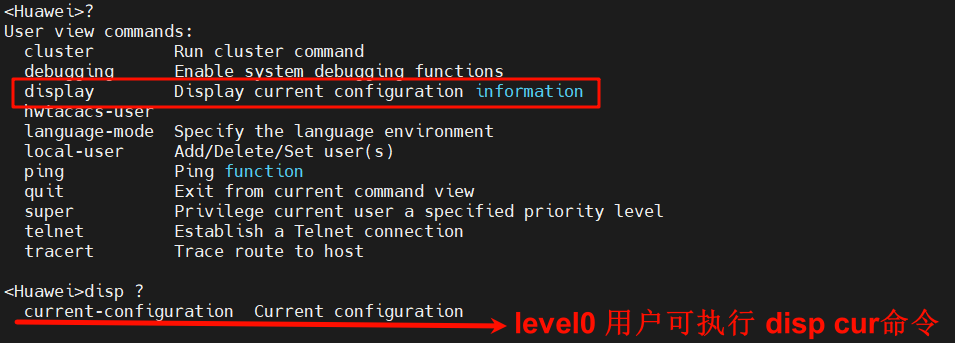
level 0的用户级别，远程登录设备之后，其默认可执行的命令只有以下几个：



★添加指定命令到level0级别

[Huawei] command-privilege level 0 view shell display current-configuration

然后cof用户可执行的命令就多了一条：



**★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]

**★用户登录提示语**

[Huawei] header login information "xxxxxxxx"

**★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

**★使用ssh密钥登录设备**

ssh协议支持使用账号密码的方式登录，也支持使用rsa密钥登录，只需要将rsa公钥放到交换机/路由器设备上，然后用户在终端使用私钥登录此设备

首先在用户电脑上生成rsa密钥对，并将公钥输出为二进制对应的十六进制字符，命令如下：

# ssh-keygen -t rsa -b 2048 -C "admin@switch5700" -P "" -f ~/sshkey-switch

#直接生成key文件及公钥.pub文件，**无需交互**，-C指定密钥的描述信息，-P指定加密密钥的密码，-f指定生成的文件名，sshkey-switch为私钥，sshkey-switch.pub为公钥

# ssh-keygen -e -m pem -f ~/sshkey-switch.pub | egrep -v 'BEGIN|END' | base64 -d | xxd -ps -u

3082010A0282010100BB3F60E40490EB7A77169CC15EF0299E59A5A8FEE0

7334A8EDFA70BE874B6BB8C54E76289908B8E618C8D0DA1CCCB32A32AB88

590522288DA4EC79F30B2A19A512D488458A6778E62848C863920D0BE642

B7F4FA5AC9C9BF0DD33FA0536430CE1A8A994D25B9732222DE8E613D4447

2AB277E6C6D78C804C9DFF3CE94E305167BC2D2C7A8078730BACAD7A566F

EF2CD2749ADE1C90278708CE072A1BD6A597874C270F84F542401B23ED84

C01E90010473597E2728B90C0E0F31A1D8A1E13CDC39B89909EF352BEB4D

846FCE39EA21DD587CD2796A4F29CB5A5C0AD0C1A135BC72852EBDA8D0FE

EB0F3916B697010091A56ECF0F9A48F11135EB94A47C21BFE70203010001

然后将公钥导入到交换机/路由器设备中

[Huawei] rsa peer-public-key rsa\_pubkey\_01 #创建一个名为rsa\_pubkey\_01的rsa公钥

[Huawei-rsa-public-key] public-key-code begin #接下来，将公钥的十六进制字符一行一行地复制粘贴

（旧版本的系统只能以十六进制形式导入公钥）

[Huawei-rsa-key-code]3082010A0282010100BB3F60E40490EB7A77169CC15EF0299E59A5A8FEE0

[Huawei-rsa-key-code]7334A8EDFA70BE874B6BB8C54E76289908B8E618C8D0DA1CCCB32A32AB88

[Huawei-rsa-key-code]590522288DA4EC79F30B2A19A512D488458A6778E62848C863920D0BE642

[Huawei-rsa-key-code]B7F4FA5AC9C9BF0DD33FA0536430CE1A8A994D25B9732222DE8E613D4447

[Huawei-rsa-key-code]2AB277E6C6D78C804C9DFF3CE94E305167BC2D2C7A8078730BACAD7A566F

[Huawei-rsa-key-code]EF2CD2749ADE1C90278708CE072A1BD6A597874C270F84F542401B23ED84

[Huawei-rsa-key-code]C01E90010473597E2728B90C0E0F31A1D8A1E13CDC39B89909EF352BEB4D

[Huawei-rsa-key-code]846FCE39EA21DD587CD2796A4F29CB5A5C0AD0C1A135BC72852EBDA8D0FE

[Huawei-rsa-key-code]EB0F3916B697010091A56ECF0F9A48F11135EB94A47C21BFE70203010001

[Huawei-rsa-key-code]

[Huawei-rsa-key-code] public-key-code end #退出

[Huawei-rsa-public-key] peer-public-key end #退出

[Huawei]

[Huawei] ssh user admin assign rsa-key rsa\_pubkey\_01 #设置admin用户使用指定的rsa公钥做认证

[Huawei] ssh user admin authentication-type password-rsa #允许admin用户使用密码及rsa密钥登录（先验证密钥，再输入密码（2次认证）

[Huawei] ssh user admin authentication-type all #允许admin用户使用任意方式认证

[Huawei] disp rsa peer-public-key name rsa\_pubkey\_01 #查看公钥内容

=====================================

Key name: rsa\_pubkey\_01

Key address:

=====================================

Key Code:

30820109

02820100

BB3F60E4 0490EB7A 77169CC1 5EF0299E 59A5A8FE E07334A8 EDFA70BE 874B6BB8

C54E7628 9908B8E6 18C8D0DA 1CCCB32A 32AB8859 0522288D A4EC79F3 0B2A19A5

12D48845 8A6778E6 2848C863 920D0BE6 42B7F4FA 5AC9C9BF 0DD33FA0 536430CE

1A8A994D 25B97322 22DE8E61 3D44472A B277E6C6 D78C804C 9DFF3CE9 4E305167

BC2D2C7A 8078730B ACAD7A56 6FEF2CD2 749ADE1C 90278708 CE072A1B D6A59787

4C270F84 F542401B 23ED84C0 1E900104 73597E27 28B90C0E 0F31A1D8 A1E13CDC

39B89909 EF352BEB 4D846FCE 39EA21DD 587CD279 6A4F29CB 5A5C0AD0 C1A135BC

72852EBD A8D0FEEB 0F3916B6 97010091 A56ECF0F 9A48F111 35EB94A4 7C21BFE7

0203

010001

**★高版本系统支持以OpenSSH公钥字符串的形式导入**

[~HUAWEI] rsa peer-public-key rsa\_pubkey\_02 encoding-type ?

der DER encoded public key # der就是旧版本默认支持的，十六进制形式

openssh OpenSSH encoded public key

pem PEM encoded public key

[Huawei] rsa peer-public-key rsa\_pubkey\_02 encoding-type openssh

[\*Huawei-rsa-public-key] public-key-code begin #接下来，将公钥内容复制粘贴（可换行输入）

[\*HUAWEI-rsa-public-key-rsa-key-code] ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQC7P2D

kBJDrencWnMFe8CmeWaWo/uBzNKjt+nC+h0truMVOdiiZCLjmGMjQ2hzMsyoyq4hZBSIojaTsefMLKhm

lEtSIRYpneOYoSMhjkg0L5kK39Ppaycm/DdM/oFNkMM4aiplNJblzIiLejmE9REcqsnfmxteMgEyd/zz

pTjBRZ7wtLHqAeHMLrK16Vm/vLNJ0mt4ckCeHCM4HKhvWpZeHTCcPhPVCQBsj7YTAHpABBHNZficouQw

ODzGh2KHhPNw5uJkJ7zUr602Eb8456iHdWHzSeWpPKctaXArQwaE1vHKFLr2o0P7rDzkWtpcBAJGlbs8

PmkjxETXrlKR8Ib/n admin@switch5700

[\*HUAWEI-rsa-public-key-rsa-key-code]

[\*HUAWEI-rsa-public-key-rsa-key-code] public-key-code end

[\*HUAWEI-rsa-public-key] peer-public-key end

[\*HUAWEI] commit

[~HUAWEI] disp rsa peer-public-key name rsa\_pubkey\_02 #查看公钥内容

=====================================

Key name: rsa\_pubkey\_02

Encoding type: OPENSSH

=====================================

Key Code:

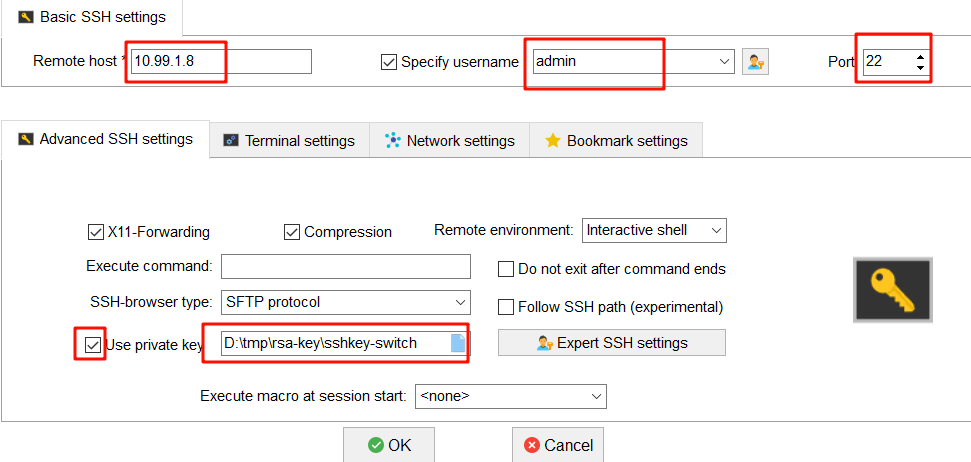
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQC7P2DkBJDrencWnMFe8CmeWaWo/uBzNKjt+nC+h0tr

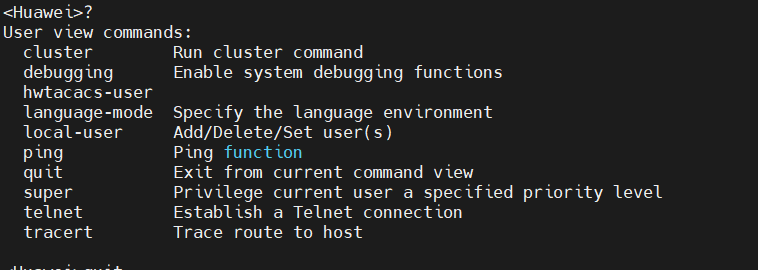
uMVOdiiZCLjmGMjQ2hzMsyoyq4hZBSIojaTsefMLKhmlEtSIRYpneOYoSMhjkg0L5kK39Ppaycm/DdM/

oFNkMM4aiplNJblzIiLejmE9REcqsnfmxteMgEyd/zzpTjBRZ7wtLHqAeHMLrK16Vm/vLNJ0mt4ckCeH

CM4HKhvWpZeHTCcPhPVCQBsj7YTAHpABBHNZficouQwODzGh2KHhPNw5uJkJ7zUr602Eb8456iHdWHzS

eWpPKctaXArQwaE1vHKFLr2o0P7rDzkWtpcBAJGlbs8PmkjxETXrlKR8Ib/n rsa-key





但是，使用rsa密钥登录的权限不够，原因是在配置ssh远程登录界面里未指定用户权限级别：

[Huawei] user-interface vty 0 4

[Huawei-ui-vty0-4] disp this

user-interface con 0

user-interface vty 0 4

authentication-mode aaa

protocol inbound all

需要添加一条配置：

[Huawei-ui-vty0-4] user privilege level 15 #有这条配置后，再通过ssh-key密钥方式登录就有管理级别权限

**★LLDP**

LLDP（Link Layer Discovery Protocol）是IEEE 802.1ab中定义的链路层发现协议。LLDP是一种标准的二层发现方式，可以将本端设备的管理地址、设备标识、接口标识等信息组织起来，并发布给自己的邻居设备，邻居设备收到这些信息后将其以标准的管理信息库MIB（Management Information Base）的形式保存起来，以供网络管理系统查询及判断链路的通信状况

[Huawei] lldp enable #全局开启lldp功能

[Huawei] lldp management-address 9.9.9.33 #设置lldp管理地址，即领居发现我时，显示我的ip地址

[Huawei] int g0/0/1

[Huawei-GigabitEthernet0/0/1] lldp enable #接口上开启lldp

Info: LLDP on the port is already enabled.

[Huawei] disp lldp neighbor #查看lldp邻居（所有网口）

[Huawei] disp lldp neighbor interface g0/0/1 #查看指定接口的lldp邻居

**★syslog日志服务配置**

[Huawei] info-center enable #全局开启信息中心服务

[Huawei] info-center channel 6 name syslog1 #重命名通道名称，1~9

[Huawei] info-center filter-id bymodule-alias xxx #过滤不需要输出的日志模块

[Huawei] info-center timestamp log date precision-time millisecond #配置时间戳精度

[Huawei] info-center local log-counter disable #关闭log信息的计数功能

[Huawei] info-center source default channel 6 log level informational

#source default 允许输出信息的模块为所有模块

[Huawei] info-center loghost 192.x.x.x source-ip 192.x.x.y channel 6 language english

#设置日志服务器为192.x.x.x；信息级别为informational，输出语言为英文

<> display channel #查看通道状态

<> disp logbuffer #查看log日志缓存

**★SNMP**

★v2c配置

[Huawei] snmp-agent #开启snmp代理功能

[Huawei] snmp-agent local-engineid xxxxxxxx

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

[Huawei] snmp-agent sys-info location XXbuilding

[Huawei] snmp-agent sys-info contact coflee-1x912345678

[Huawei] snmp-agent community read *publicxxxx* acl 2002 #可用acl指定允许的管理站

[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

[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 protocol source-interface Meth0/0/0

★v3配置

[Huawei] snmp-agent

[Huawei] snmp-agent local-engineid xxxxxxxx

[Huawei] snmp-agent sys-info location R09/22U

[Huawei] snmp-agent sys-info version v3

[Huawei] snmp-agent mib-view included iso-view iso

[Huawei] snmp-agent group v3 snmpgrp privacy read-view iso-view write-view notify-view acl 2001

[Huawei] snmp-agent usm-user v3 v3userxx

[Huawei] snmp-agent usm-user v3 v3userxx snmpgrp authentication-mode sha2-256 passwdxx1 \

privacy-mode aes128 passwdxx2

[Huawei] snmp-agent usm-user v3 v3userxx acl 2001

[Huawei] snmp-agent acl 2001

[Huawei] snmp-agent target-host [host-name *trapHostxx* ] trap address udp-domain 10.1.1.252 \

udp-port 162 params securityname *trapsecurityxxxx* v3 privacy

[Huawei] snmp-agent trap source Meth0/0/0

[Huawei] snmp-agent trap enable

[Huawei] snmp-agent protocol source-interface Meth0/0/0

[Huawei] undo snmp-agent protocol source-status all-interface

[Huawei] undo snmp-agent protocol source-status ipv6 all-interface

[Huawei] undo snmp-agent proxy protocol source-status all-interface

[Huawei] undo snmp-agent proxy protocol source-status ipv6 all-interface

★注意：

#以下2行写法要求输入加密后的密文

snmp-agent usm-user v3 v3userxx authentication-mode sha2-256 cipher xxxxxxxxx

snmp-agent usm-user v3 v3userxx privacy-mode aes128 cipher xxxxxxxxx

#以下写法可以写明文密码，执行后会自动加密（比上面多加了个组名）

snmp-agent usm-user v3 v3 userxx snmpgrp authentication-mode sha2-256 passwdxx privacy-mode aes128 passwdxx

**★NETCONF**

作为新一代的网络设备的配置管理协议，NETCONF使用YANG作为它的数据建模语言。用户可以使用这套机制增加、修改、删除网络设备的配置，获取网络设备的配置和状态信息。通过NETCONF协议，网络设备可以提供规范的应用程序编程接口API（Application Programming Interface），应用程序可以直接使用这些API，向网络设备发送和获取配置。

NETCONF是基于SSH和TCP协议的设备管理协议，使用XML来传输配置信息。默认时，netconf下发的配置立即生效，但不会保存到配置文件中，设备重启会丢失下发的配置，需要手动保存一下设备配置。

**★s5700系列配置netconf**

**首先创建api类型的aaa账号**

[HUAWEI] aaa

[HUAWEI-aaa] local-user service password cipher passwdxxxx #创建一个名为service的账号

[HUAWEI-aaa] local-user service privilege level 15

[HUAWEI-aaa] local-user service service-type api #服务类型必须为api

Warning: This command may cause a configuration conflict in NETCONF mode. Continue? [Y/N]:y

[HUAWEI] netconf #开启netconf功能

Warning: Enabling NETCONF will cause LNP to be disabled and STP to be enabled. Continue? [Y/N]:y

Info: NETCONF is being enabled. Please wait..........................................

[HUAWEI-netconf] source ip 10.99.2.55 port ?

INTEGER<830,55552-55807> Port number. The default value is 830.

[HUAWEI-netconf] source ip 10.99.2.55 port 830 #指定监听的源ip和端口号

[HUAWEI-netconf] user service assign rsa public-key rsa\_pubkey\_02 #使用密钥认证（可选）

[HUAWEI-netconf] rsa local-key-pair create

Warning: RSA keys already exist. Continue? [Y/N]:y

**★CE12800系列配置netconf**

**首先创建ssh类型的aaa账号**

[HUAWEI] aaa

[HUAWEI-aaa] local-user service password cipher passwdxxxx #创建一个名为service的账号

[HUAWEI-aaa] local-user service level 3

[HUAWEI-aaa] local-user service service-type ssh #服务类型为ssh也行

[~HUAWEI] snetconf server enable

[~HUAWEI] ssh user service authentication-type password

[~HUAWEI] ssh user service service-type snetconf

[~HUAWEI] netconf

[~HUAWEI-netconf] protocol inbound ssh port 830

**★编写python脚本**

使用netconf协议连接设备并下发配置

from ncclient import manager  
from ncclient import xml\_  
  
set\_interface = """  
 <edit-config>  
 <target>  
 <running/>  
 </target>  
 <config>  
 <if:interfaces xmlns:if="urn:ietf:params:xml:ns:yang:ietf-interfaces">  
 <if:interface>  
 <if:name>GigabitEthernet0/0/3</if:name>  
 <if:description>port description xxx</if:description>  
 <if:type xmlns:iana-if-type="urn:ietf:params:xml:ns:yang:iana-if-type">iana-if-type:ethernetCsmacd</if:type>  
 <if:enabled>true</if:enabled>  
 <if:link-up-down-trap-enable>disabled</if:link-up-down-trap-enable>  
 </if:interface>  
 </if:interfaces>  
 </config>  
 </edit-config>  
"""  
  
def netconf():  
 manager.connect(host="10.99.2.55", port=830, username="service", password="passwdxxxx",  
 allow\_agent=False, hostkey\_verify=False,  
 device\_params={"name": "huaweiyang"}).rpc(xml\_.to\_ele(set\_interface))  
 print("netconf设置成功")  
  
if \_\_name\_\_ == '\_\_main\_\_':  
 netconf()

执行脚本后，查看交换机配置：

[HUAWEI] disp cur int g0/0/3

interface GigabitEthernet0/0/3

description port description xxx

undo shutdown

undo enable snmp trap updown

★配置接口ip地址

from ncclient import manager  
from ncclient import xml\_  
  
# NETCONF发送XML数据，配置设备接口IP地址  
set\_interface = """  
 <config>  
 <ethernet xmlns="http://www.huawei.com/netconf/vrp" content-version="1.0" format-version="1.0">  
 <ethernetIfs>  
 <ethernetIf operation="merge">  
 <ifName>GE1/0/2</ifName>  
 <l2Enable>disable</l2Enable>  
 </ethernetIf>  
 </ethernetIfs>  
 </ethernet>  
 <ifm xmlns="http://www.huawei.com/netconf/vrp" content-version="1.0" format-version="1.0">  
 <interfaces>  
 <interface operation="merge">  
 <ifName>GE1/0/2</ifName>  
 <ifDescr>Config by NETCONF</ifDescr>  
 <ifmAm4>  
 <am4CfgAddrs>  
 <am4CfgAddr operation="create">  
 <subnetMask>255.255.255.0</subnetMask>  
 <addrType>main</addrType>  
 <ifIpAddr>192.168.3.1</ifIpAddr>  
 </am4CfgAddr>  
 </am4CfgAddrs>  
 </ifmAm4>  
 </interface>  
 </interfaces>  
 </ifm>  
 </config>  
"""  
  
if \_\_name\_\_ == '\_\_main\_\_':  
 # 创建NETCONF连接  
 m = manager.connect(host="192.168.56.2", # 设备IP地址或主机名  
 port=830, # 连接的端口，默认为830  
 username="service", # 登录用户名  
 password="Centos123", # 登录密码  
 hostkey\_verify=False, # 禁用主机密钥验证  
 device\_params={'name': "huawei"}, # 指定设备类型为华为，这会影响连接过程中的一些行为和参数设置  
 allow\_agent=False, # 禁用NETCONF agent，设置为False表示不使用NETCONF agent  
 look\_for\_keys=False) # 禁用密钥查找，设置为False表示不自动查找密钥  
 # 通过NETCONF连接对象m，执行编辑配置的操作，目标是运行中的配置，并传入要应用的配置set\_interface  
 m.edit\_config(target='running', config=set\_interface)

**★OPS**

开放可编程系统OPS（Open Programmability System）是指设备通过提供统一的应用程序接口RESTful API（Representational State Transfer Application Programming Interface）来开放系统，使得系统具备可编程能力，可以运行python脚本实现用户自定义的功能。

首先编写一个简单的python测试脚本，例如 ops\_demo\_01.py，内容如下：

#!/usr/bin/env python  
# -\*- coding: utf-8 -\*-  
  
import sys  
  
if \_\_name\_\_ == "\_\_main\_\_":  
 print(sys.getdefaultencoding()) # 查看python默认字符编码  
 print(sys.version\_info) # 查看python版本信息

使用ftp/tftp协议将测试脚本文件上传到交换机设备

<HUAWEI> ftp 10.99.2.1

Trying 10.99.2.1 ...

Press CTRL+K to abort

Connected to 10.99.2.1.

220-FileZilla Server 1.4.1

220 Please visit https://filezilla-project.org/

User(10.99.2.1:(none)):ftpuser1

331 Please, specify the password.

Enter password:

230 Login successful.

[ftp] get ops\_demo\_01.py

200 PORT command successful.

150 Starting data transfer.

226 Operation successful

FTP: 220 byte(s) received in 0.033 second(s) 6.51Kbyte(s)/sec.

[ftp] quit

221 Goodbye.

<HUAWEI> ops install file ops\_demo\_01.py #安装ops脚本，默认安装到 flash:/$\_user 目录下

<HUAWEI> disp ops script #查看已安装的ops脚本

<HUAWEI> ops run python ops\_demo\_01.py #运行指定的脚本（一次性的）用于测试脚本是否正常

确认脚本正常后，需要使用python脚本助手进行注册，才能被自动触发（可以是定时器触发，也可是满足其他指定的事件而触发）

★s5735等低版本的设备，不能run脚本，只能使用python脚本助手进行注册运行

（S5735 V200R021C00SPC100 内置的python解释器版本为 3.8.5），有的设备内置的python版本为2.7.x，需要事先确认再去写ops脚本。

需要在ops脚本里实现2个固定名称的函数：

|  |  |
| --- | --- |
| ops\_condition(ops) | 定义订阅处理函数ops\_condition。该函数在配置脚本助手的时候调用，用于订阅事件，由设备内置的框架脚本\_frame.py调度执行 |
| ops\_execute(ops) | 定义执行处理函数ops\_execute。该函数在脚本事件执行的时候调用，用于执行动作，由设备内置的框架脚本\_frame.py调度执行 |

示例脚本ops\_test\_05.py内容：

#!/usr/bin/env python  
# -\*- coding: utf-8 -\*-  
  
import ops  
  
def ops\_condition(ops):  
 # 定义订阅处理函数ops\_condition。该函数用于订阅事件，在配置脚本助手时由设备内置的框架脚本\_frame.py调度执行  
 status, err\_str = ops.timer.cron("t1", "\*/5 \* \* \* \*") # 订阅一个定时器，以t1标识，每5分钟  
 # 对于ops.timer.cron接口，status返回值为0表示该API执行成功，1表示该API执行失败。  
 # 第二个返回值err\_str仅当第一个返回值status为1时返回，为字符串形式，描述执行失败的原因。  
 return 0 # 返回值为0时，ops\_condition函数执行成功  
  
def ops\_execute(ops):  
 # 定义执行处理函数ops\_execute。该函数用于执行动作，在脚本事件执行时由设备内置的框架脚本\_frame.py调度执行  
 value, descri\_str = ops.terminal.write("test alarm generated", vty="all") # 向终端输出信息  
 return 0 # 返回值为0时，ops\_execute函数执行成功

将脚本上传到设备，过程省略

<HUAWEI> ops install file ops\_test\_05.py

<HUAWEI> system-view

[HUAWEI] ops #进入ops配置界面

[HUAWEI-ops] script-assistant python ops\_test\_05.py #配置python脚本助手，注册ops脚本里的事件

Info: Executing user script... Please wait...

Info: The script assistant ops\_test\_05.py is installed on the device successfully.

然后每隔5分钟都会在tty输出信息：



[HUAWEI] disp ops assistant current

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

Assistant State Condition

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

ops\_test\_05.py ready timer

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

[HUAWEI] disp ops assistant history

Assistant history information

Name :ops\_test\_05.py

Running information

Trigger condition :timer

Trigger event name :t1

Trigger time :2024-06-26 20:51:00

Execute start time :2024-06-26 20:51:00

Execute end time :2024-06-26 20:51:01

Execute result :normal

[HUAWEI] ops #进入ops配置界面

[HUAWEI-ops] shutdown script-assistant ops\_test\_05.py #停止指定脚本的python脚本助手

[HUAWEI-ops] disp ops assistant current

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

Assistant State Condition

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

ops\_test\_05.py shutdown timer

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

[HUAWEI-ops] assistant scheduler suspend #关闭ops维护助手功能

[HUAWEI-ops] disp ops assistant current

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

Assistant State Condition

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

ops\_test\_05.py suspend timer

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

[HUAWEI-ops] undo assistant scheduler suspend #重新开启ops维护助手功能（默认就是开启状态）

[HUAWEI-ops] undo script-assistant python ops\_test\_05.py #删除指定的python脚本助手

<HUAWEI> ops uninstall file ops\_test\_05.py #卸载ops脚本（前提是先删除指定的python脚本助手）

Info: The script file flash:/$\_user/ops\_test\_05.py is uninstalled from the device successfully.

其他的订阅事件api，可参考官方文档的“设备管理配置”→“OPS配置”→“OPS API列表”

**★第3章、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

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.

[Huawei-ftp] put srcxx dstxxx #上传文件

**★第4章、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

**#或者：**

[Huawei-100GE1/0/1] device transceiver 100GBASE-FIBER

[Huawei-100GE1/0/1] negotiation disable

[Huawei-100GE1/0/1] fec mode rs #手动指定fec模式，使用铜缆时

★有的型号将每4个口分为一组，同一组内的口必须为同一速率，比如1-4，5-8，9-12，13-16，17-20，21-24各自为一组，一旦将同一组内某个口设置为xx速率，则同一组内其他口都会变为xx速率

★有的型号100G光口不支持40G的速率，比如CE6881

★有的型号个别口不支持低速率的光模块，比如CE6881的10G口，有部分口（13-16，25-18）就不支持插1000兆的光模块

**★查看接口ip及状态**

<Huawei> disp 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>

**★接口流量统计时间设置**

[Huawei] set flow-stat interval 60 #设置接口的流量统计时间间隔，单位秒

[Huawei] undo set flow-stat interval #恢复默认时间间隔，300秒

**★二层口设置为三层口（保留vlan）**

有些型号的交换机（如CE6800及更高系列的）二层口设置为三层口时，需要先配置保留vlan

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

[Huawei] int eth-trunk 2 #聚合口，或者用物理口int g0/0/2都可以

[Huawei-Eth-Trunk2] undo portswitch #设置为3层口（路由口）

**★交换机三层子接口配置vlan**

[Huawei] int g0/0/2.2

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

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

**★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 #清空本端口上的所有配置

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 #配置模式下直接清空

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

**★端口拆分port-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

#再使用1分4线缆插入此端口，使用拆分后的口：

[Huawei] interface 100GE1/0/5:1 #使用拆分后的第一个子接口（25GE）

[Huawei] interface 100GE1/0/5:2

[Huawei] interface 100GE1/0/5:3

[Huawei] interface 100GE1/0/5:4

以CE8800系列为示例，其拆分模式为：

|  |  |
| --- | --- |
| 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 （作为单个口使用）  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 （作为单个口使用）  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 |

不同型号的设备对端口的拆分支持情况不尽相同，需要事先查阅官方产品文档

**★DDM光口功率检测**

（Digital Diagnostic Monitoring）数字诊断检测是由SFF Committee制定，遵循SFF-8472多源协议定义的标准参数，规范了光模块和网络设备的软硬件所需遵循的标准数值或范围。

实时测量参数：工作电压、工作温度、接收光功率、发射光功率和激光器偏置电流

[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 #查看端口的光功率等详细信息

[Huawei] disp interface GigabitEthernet0/0/1 transceiver verbose #显示指定端口的光功率信息

[Huawei] disp interface transceiver brief #显示端口的光功率等信息；详细信息用 verbose

**★VCT电口检测**

（virtual-cable-test）VCT是利用TDR（Time Domain Reflectometry-时域反射测试）来检测网络线缆的物理状态。

TDR检测原理类似于雷达，它工作方式是通过主动向导线发射一个脉冲信号并检测所发送的脉冲信号的反射结果来检测电缆故障。当发送的脉冲信号通过电缆的末端或电缆的故障点时，就会引起部分或全部的脉冲能量被反射回来到达原来的发送源，VCT技术根据测量脉冲信号在导线中的传输获得信号到达故障点或返回的时间，然后根据公式将相应时间换算为距离值。通过VCT可以检测电缆状态、故障距离是否极性交换、插入信号衰减、返回信号衰减等。

[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port-group**

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Eth-Trunk**

★lacp模式

[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] lacp timeout fast #设置lacp短超时（发送周期1秒，超时3秒）

#默认为lacp timeout slow，发送周期30秒，超时90秒，链路2端的超时时间可以不一致

★manual模式

[Huawei] int Eth-Trunk 1 #创建聚合口1

[Huawei-Eth-Trunk1] mode manual load-balance #手工模式，与lacp二选一，默认为load-balance

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

[Huawei-Eth-Trunk1] quit

★成员口加入聚合口

[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

★聚合口里直接添加成员口

[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]

[Huawei-Eth-Trunk1] port link-type trunk #聚合口指定为trunk，也可为access（在聚合口做配置）

[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，学习到的mac不会老化

[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]

★端口安全保护模式：

|  |  |
| --- | --- |
| 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）**

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

#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

**★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 kbps

**★端口error-down自动恢复**

[HUAWEI] error-down auto-recovery cause bpdu-protection interval 300 #300秒后自动恢复为up

[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

**★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），也可只镜像某一方向的，如inbound

[Huawei-GigabitEthernet0/0/2]quit

[Huawei] disp port-mirroring #查看端口镜像情况

Port-mirror:

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

Mirror-port(被镜像) Direction Observe-port（观察口）

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

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

observe-port group 2 #观察组，被镜像的数据流向此组里的所有端口

group-member GE1/0/1

group-member GE1/0/2

#

interface Eth-trunk 1 #在聚合口上做镜像

port-mirroring observe-port group 2 inbound

port-mirroring observe-port group 2 outbound

#

**★第5章、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 #此vlan的描述信息

[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（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

**★删除某个vlan**

int 目标接口

undo port trunk allow-pass vlan 71 #首先在trunk口里undo要排除的vlan（不允许此vlan通过）

#

undo vlan 71 #删除目标vlan

#

commit

#

**★trunk口新增一个允许通过的vlan**

port trunk allow-pass vlan 22 23 24 58 33 #在原有配置上追加一个33，

port trunk allow-pass vlan 33 #华为设备可直接添加要新增的那个vlan，原有配置不会被清空

**★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，出站时自动将22转换回20

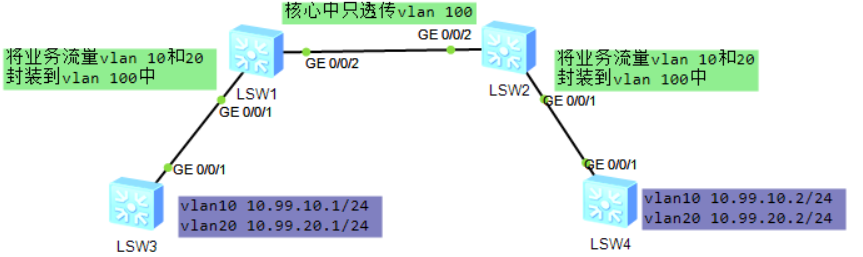
**★QinQ（vlan透传）**

802.1Q-in-802.1Q是在802.1Q标签报文的基础上再增加一层802.1Q的Tag来达到隔离VLAN的功能

基本QinQ：对进入二层QinQ接口的所有帧都加上相同的外层vlan Tag。

灵活QinQ：根据不同的内层Tag或符合流分类规则的帧，加上不同的外层vlan Tag，对业务流量进行精细划分。

**①基本QinQ配置：**



LSW3的GE 0/0/1为trunk口，允许vlan 10 20 通过

LSW4的GE 0/0/1为trunk口，允许vlan 10 20 通过

现在想在核心（LSW1、LSW2）上把业务vlan 10, 20封装起来，封装到vlan 100中进行透明传输（以便和核心上的vlan 10, 20隔离开来）

核心的GE 0/0/2只放通vlan 100，配置省略

LSW1和LSW2的GE 0/0/1配置如下：

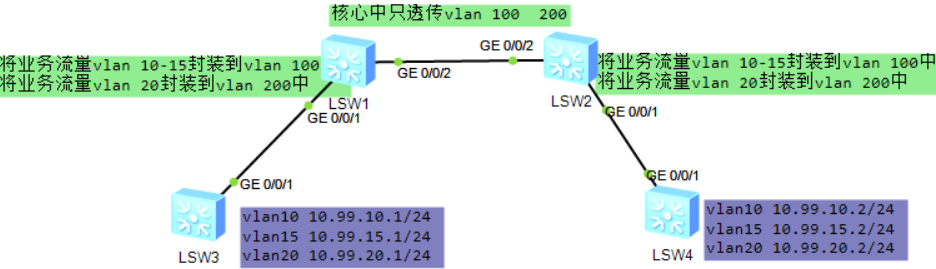
[Huawei] int g0/0/1

[Huawei-GigabitEthernet0/0/1] port link-type dot1q-tunnel

[Huawei-GigabitEthernet0/0/1] port default vlan 100 #流量入站时带上外层vlan tag 100，出站时自动剥离

[Huawei-GigabitEthernet0/0/1] quit

**②灵活QinQ配置：**



LSW3的GE 0/0/1为trunk口，允许vlan 10 15 20 通过

LSW4的GE 0/0/1为trunk口，允许vlan 10 15 20 通过

现在想在核心（LSW1、LSW2）上把业务vlan 10, 15, 20封装起来，

将vlan 10, 15封装到vlan 100中进行透明传输；将vlan 20封装到vlan 200中进行透明传输

核心的GE 0/0/2只放通vlan 100 200，配置省略

LSW1和LSW2的GE 0/0/1配置如下：

[Huawei] int g0/0/1

[Huawei-GigabitEthernet0/0/1] port link-type hybrid

[Huawei-GigabitEthernet0/0/1] port hybrid untagged vlan 100 200 #流量出站时自动剥离100,200的tag

[Huawei-GigabitEthernet0/0/1] qinq vlan-translation enable

[Huawei-GigabitEthernet0/0/1] port vlan-stacking vlan 10 to 15 stack-vlan 100 #将10-15封装到100

[Huawei-GigabitEthernet0/0/1] port vlan-stacking vlan 20 stack-vlan 200 #将20封装到100

[Huawei-GigabitEthernet0/0/1] quit

**★Mux VLAN（主次vlan）**

mux VLAN可实现一个大的广播域的分隔以及各广播域内流量的灵活控制

mux将某个大的广播域分隔为主vlan（Principal）及次vlan（Subordinate）

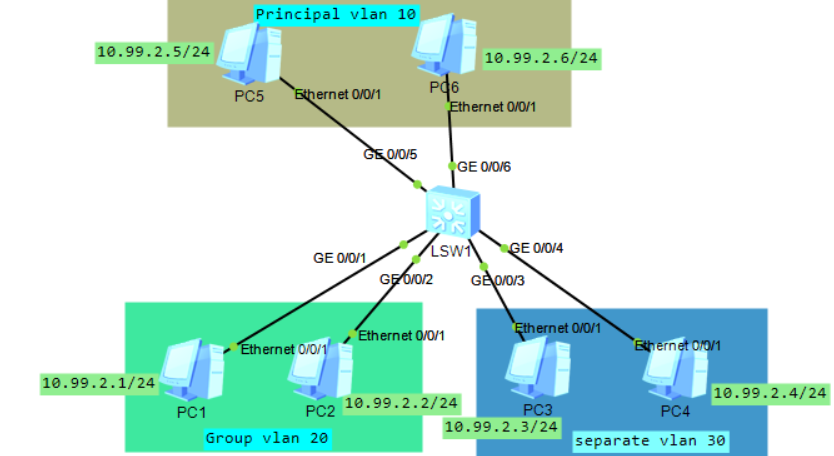
次vlan又分为Group VLAN（互通型从VLAN）和Separate VLAN（隔离型从VLAN）

加入Principal VLAN（主VLAN）的端口，可以与MUX VLAN内的所有端口进行通信

加入Group VLAN（互通型从VLAN）的端口，可以与Principal VLAN的端口互通以及同组内端口互通

加入Separate VLAN（隔离型从VLAN）的端口，可以与Principal VLAN的端口互通（同组内端口不能互通）

拓扑图：



[Huawei] vlan batch 10 20 30

[Huawei] vlan 10

[Huawei-vlan10] mux-vlan

[Huawei-vlan10] subordinate group 20

[Huawei-vlan10] subordinate separate 30

[Huawei] interface GigabitEthernet 0/0/1

[Huawei-GigabitEthernet0/0/1] port link-type access

[Huawei-GigabitEthernet0/0/1] port default vlan 20

[Huawei-GigabitEthernet0/0/1] port mux-vlan enable

[Huawei] interface GigabitEthernet 0/0/2

[Huawei-GigabitEthernet0/0/2] port link-type access

[Huawei-GigabitEthernet0/0/2] port default vlan 20

[Huawei-GigabitEthernet0/0/2] port mux-vlan enable

[Huawei] interface GigabitEthernet 0/0/3

[Huawei-GigabitEthernet0/0/3] port link-type access

[Huawei-GigabitEthernet0/0/3] port default vlan 30

[Huawei-GigabitEthernet0/0/3] port mux-vlan enable

[Huawei] interface GigabitEthernet 0/0/4

[Huawei-GigabitEthernet0/0/4] port link-type access

[Huawei-GigabitEthernet0/0/4] port default vlan 30

[Huawei-GigabitEthernet0/0/4] port mux-vlan enable

[Huawei] interface GigabitEthernet 0/0/5

[Huawei-GigabitEthernet0/0/5] port link-type access

[Huawei-GigabitEthernet0/0/5] port default vlan 10

[Huawei-GigabitEthernet0/0/5] port mux-vlan enable

[Huawei] interface GigabitEthernet 0/0/6

[Huawei-GigabitEthernet0/0/6] port link-type access

[Huawei-GigabitEthernet0/0/6] port default vlan 10

[Huawei-GigabitEthernet0/0/6] port mux-vlan enable

[Huawei] disp vlan

The total number of vlans is : 4

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

U: Up; D: Down; TG: Tagged; UT: Untagged;

MP: Vlan-mapping; ST: Vlan-stacking;

#: ProtocolTransparent-vlan; \*: Management-vlan;

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

VID Type Ports

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

1 common UT:GE0/0/7(D) GE0/0/8(D) GE0/0/9(D) GE0/0/10(D)

GE0/0/11(D) GE0/0/12(D) GE0/0/13(D) GE0/0/14(D)

GE0/0/15(D) GE0/0/16(D) GE0/0/17(D) GE0/0/18(D)

GE0/0/19(D) GE0/0/20(D) GE0/0/21(D) GE0/0/22(D)

GE0/0/23(D) GE0/0/24(D)

10 mux UT:GE0/0/5(U) GE0/0/6(U)

20 mux-sub UT:GE0/0/1(U) GE0/0/2(U)

30 mux-sub UT:GE0/0/3(U) GE0/0/4(U)

**★Super VLAN（vlan聚合）**

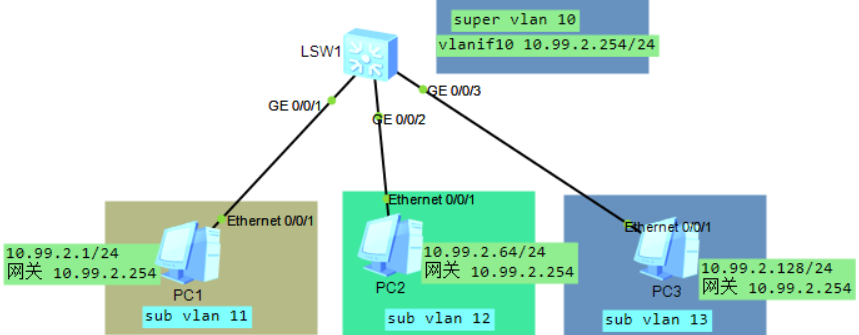
super vlan也叫VLAN Aggregation（vlan聚合）

如果每个vlan都要划分一个三层网段的话，会造成ip浪费，或者划分不出这么多数量的子网，这时可以让多个vlan使用同一个ip子网网段（只在二层上隔离，三层上是互通的）

vlan聚合分为2种类型vlan：

super vlan为管理vlan，可配置三层接口，配置网关ip地址（不可加入端口）需要使能Proxy ARP功能

sub vlan为业务vlan，只可加入业务端口，不可起三层接口，各sub vlan端口之间是二层隔离的，共用一个super vlan的网关



[Huawei] vlan batch 10 to 13

[Huawei] vlan 10

[Huawei-vlan10] aggregate-vlan #将vlan 10设置为super vlan

[Huawei-vlan10] access-vlan 11 to 13 #设置sub vlan

[Huawei-vlan10] quit

[Huawei] int vlanif 10

[Huawei-Vlanif10] ip addr 10.99.2.254 24 #super vlan配置三层接口网关地址

[Huawei-Vlanif10] arp-proxy inner-sub-vlan-proxy enable #开启arp代理功能???

#高版本交换机配置命令为 arp proxy inter-vlan enable

[Huawei] interface GigabitEthernet 0/0/1

[Huawei-GigabitEthernet0/0/1] port link-type access

[Huawei-GigabitEthernet0/0/1] port default vlan 11

[Huawei] interface GigabitEthernet 0/0/2

[Huawei-GigabitEthernet0/0/2] port link-type access

[Huawei-GigabitEthernet0/0/2] port default vlan 12

[Huawei] interface GigabitEthernet 0/0/3

[Huawei-GigabitEthernet0/0/3] port link-type access

[Huawei-GigabitEthernet0/0/3] port default vlan 13

[Huawei] disp vlan

The total number of vlans is : 5

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

U: Up; D: Down; TG: Tagged; UT: Untagged;

MP: Vlan-mapping; ST: Vlan-stacking;

#: ProtocolTransparent-vlan; \*: Management-vlan;

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

VID Type Ports

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

1 common UT:GE0/0/4(D) GE0/0/5(D) GE0/0/6(D) GE0/0/7(D)

GE0/0/8(D) GE0/0/9(D) GE0/0/10(D) GE0/0/11(D)

GE0/0/12(D) GE0/0/13(D) GE0/0/14(D) GE0/0/15(D)

GE0/0/16(D) GE0/0/17(D) GE0/0/18(D) GE0/0/19(D)

GE0/0/20(D) GE0/0/21(D) GE0/0/22(D) GE0/0/23(D)

GE0/0/24(D)

10 super

11 sub UT:GE0/0/1(U)

12 sub UT:GE0/0/2(U)

13 sub UT:GE0/0/3(U)

**★STP（生成树协议）**

生成树协议的作用是防止二层环路，最早使用的是stp协议，后来演进为rstp、mstp等，现在建议在正式环境中只使用MSTP协议，不建议使用STP/RSTP了，本小节仅供学习原理使用。

[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，默认128，16的倍数

# 0~240，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] disp 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

[HUAWEI] stp pathcost-standard dot1t

**★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，现在建议在正式环境中只使用MSTP协议，不建议使用STP/RSTP了，本小节仅供学习原理使用。

[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 #配置为MSTP模式

[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 #默认所有未指定的vlan处于instance 0

[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] disp 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] disp stp region-configuration digest #查看mstp域配置的md5消息摘要

Oper configuration

Format selector :0

Region name :mstp1

Revision level :1

Digest :0xCBEA249445F4933BA4ADE3DFE74D536A #只有域配置消息摘要相同的交换机才处于同一个mstp区域中

[Huawei] disp stp global #查看mstp全局信息

<Huawei1> disp stp brief #查看各实例各端口角色状态

MSTID Port Role STP State Protection

0 GigabitEthernet1/0/7 ROOT FORWARDING NONE

0 GigabitEthernet1/0/11 ALTE DISCARDING NONE

0 GigabitEthernet1/0/17 ALTE DISCARDING NONE

1 GigabitEthernet1/0/7 DESI FORWARDING NONE

1 GigabitEthernet1/0/17 DESI FORWARDING NONE

2 GigabitEthernet1/0/11 ROOT FORWARDING NONE

#可知这台交换机在mst实例1为根桥，实例0和2为指定桥

[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 #指定桥的根端口开启环路保护

[Huawei-GigabitEthernet0/0/3] quit

[Huawei] int g0/0/4

[Huawei-GigabitEthernet0/0/4] stp root-protection #指定端口上的根保护

[Huawei-GigabitEthernet0/0/4] quit

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

**★第6章、ARP及MAC相关命令**

**★ARP操作**

<Huawei> disp 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> reset arp dynamic ip 10.1.1.99 #清除某个动态arp记录（因为老化时间默认20分钟太久了）

<Huawei> reset arp dynamic ip 10.1.22.99 vpn-instance xxx #清除某个动态arp记录

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

[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] 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] 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] 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）

[Huawei] arp constant-send enable #如果arp老化时间配置为30秒，则需要全局开启constant-send

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

**★MAC操作**

[Huawei] disp 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]

**★第7章、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 #创建一个名为vlan1的地址池

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] disp dhcp statistics #查看dhcp报文收发情况

[Huawei] disp 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，也可以是全部收回

X.X.X.X Start IP address

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。

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。

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（本交换机收到的dhcp请求报文交给中继服务器处理）

**★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] disp 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（上联口接dhcp server）

[Huawei-GigabitEthernet0/0/1] quit

[Huawei] int g0/0/3 #所有下联口，接终端机的，都要开启dhcp snooping（防止有终端伪装为dhcp server）

[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绑定过滤策略后，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.

**★第8章、ACL访问控制及Qos流量控制**

**★ACL访问控制列表**

**①ACL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 |

★华为的设备，缺省时最后有一条规则是permit any，必要时请在末尾添加一条规则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（或者0.0.0.0）

[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] rule 10 permit vpn-instance vpn实例名称 其他配置 #配置vpn实例

[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 destination-mac 4c1f-cc28-6617

ffff-ffff-ffff #匹配mac，使用正掩码，全f表示匹配单个mac

[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

**②ACL应用时间**

首先要确认交换机时间和现实的时间同步

[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

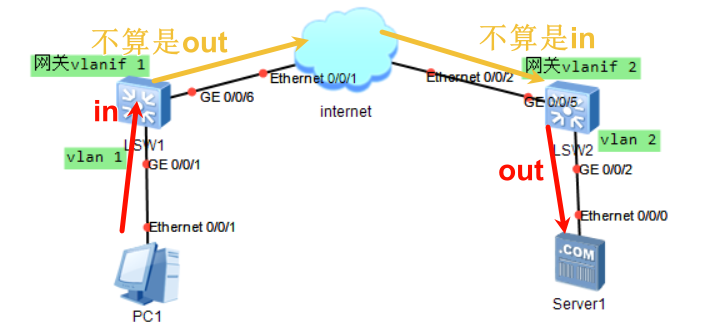
daily Every day of the week

off-day Saturday and Sunday

working-day Monday to Friday

**★ACL应用注意事项**

在交换机上应用acl时，关于in / out方向的解释：



假如接入vlan 1的PC1（ip为10.1.1.1）要访问外部某服务器Server1，

PC1发来的报文要先发给网关vlanif 1，则在LSW1设备上对于vlanif 1而言就是入站（可在in方向做acl）

而vlanif 1收到报文后，要走路由层转发给下一跳设备，★int vlanif 1把报文交给路由层处理的话，不能算是out

★报文经过路由转发到LSW2设备时不能算是in入站（收到的报文是从路由层转来的，不算in）

vlanif 2把外部转来的报文发给本vlan里的主机Server1时，才算out出站（可在out方向做acl）

所以：

从本vlan下的主机发报文给本vlanif算in方向，从vlanif发报文给本vlan下的主机算out方向。

而经过路由转发的报文，不论是发过来，还是发出去，都不能算是in/out方向

同理，如果报文只是经过此vlan的某2个端口，不发给此vlan的vlanif接口的话，就没有in，也没有out，在vlanif上无法做acl的匹配。而大多数交换机只支持在vlanif接口上应用acl访问控制列表，所以这种情况就没法控制了。

而有些高级型号的设备支持在端口上应用acl，直接在端口上应用in/out方向的访问策略，这时的in就是进入交换机的流量，out就是从交换机发出的流量。不考虑是否经过vlanif处理了。

**★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 #匹配 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> disp 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**

有时需要在交换机上查看是否有某个源ip/目的ip的报文经过，可以使用流量统计功能

# 先创建acl 3001，匹配ip source destination

[Huawei] traffic classifier class2 #定义流类

[Huawei-classifier-class1] if-match acl 3001 #匹配数据，用acl限定

[Huawei-classifier-class1] quit

[Huawei] traffic behavior behav2 #定义流行为

[Huawei-behavior-behav1] statistics enable #流量统计

[Huawei-behavior-behav1] quit

[Huawei] traffic policy policy2 #定义流策略

[Huawei-trafficpolicy-policy1] classifier class2 behavior behav2 precedence 5 #匹配流类及流行为

[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> disp traffic-policy applied-record policy1 #查看策略的应用情况

<Huawei> disp traffic-policy statistics interface g0/0/3 #查看流量匹配统计情况

**★抓包**

<> disp qos queue statistics interface G1/0/1 #看队列流量统计，只能看出方向的

<> reset qos queue statistics interface G1/0/1 #清空统计

<> capture-packet interface g1/0/2 destination terminal packet-len 64 packet-num 20

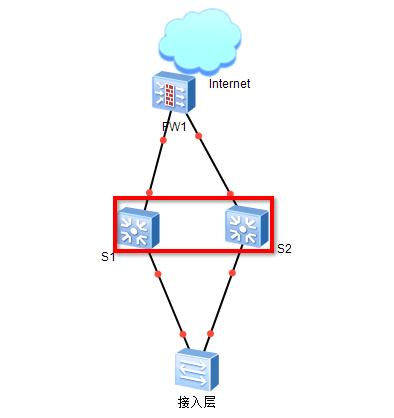
#每个包抓取前64字节，共抓20个包

**★第9章、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，vrrp报文封装在IP报文中，上层协议号为118

Virtual Router（虚拟ip）对应的mac地址为0000-5E00-01-vrid

vrrp设备优先级默认为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 #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] disp vrrp brief #查看vrrp信息

VRID State Interface Type Virtual IP

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

10 Initialize Vlanif10 Normal 10.10.1.254

**★第10章、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 #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

#目的网络 子网掩码 下一跳地址 路由优先级

[Huawei] ip route-static vpn-instance xxxx 10.19.0.0 24 10.1.1.2 #配置vpn实例的静态路由

[Huawei] ip route-static ...... track nqa admin xx #与nqa联动

[Huawei] disp ip routing-table [ vpn-instance xxxx] #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

[Huawei] disp ip routing-table limit #查看路由限制

**★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**

Routing Information Protocol距离矢量路由选择协议

[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），cost最大15，16表示不可达

[Huawei-rip-1] default-route originate cost 2 #引入默认路由（0.0.0.0/0）

[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 xxx 1 #设置rip接口验证

[Huawei-GigabitEthernet0/0/1] rip authentication-mode md5 usual plain xxx 1 #设置rip接口验证

[Huawei-GigabitEthernet0/0/1] rip authentication-mode simple plain xxx #设置rip接口验证

#水平分割

从某接口学到的路由不再从此接口发出

#毒性逆转

从某接口学到路由后，将该路由度量值设置为16后再发回此接口

**★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] bandwidth-reference 100000 #修改参考带宽为100G

[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，使用反掩码

[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，使用反掩码

[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 #引入RIP路由（路由重分布）

#引入的外部路由显示为O\_AES，优先级150，默认cost为1

[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

#接口开销

#接口认证

int g0/0/1

ospf authentication-mode simple plain 123xxxx

ospf authentication-mode md5 1 plain 123xxx

#参考带宽

cost = 100M / 接口带宽 #参考为100M

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

[Huawei] disp ospf lsdb #查看ospf链路状态数据库

**★BGP**

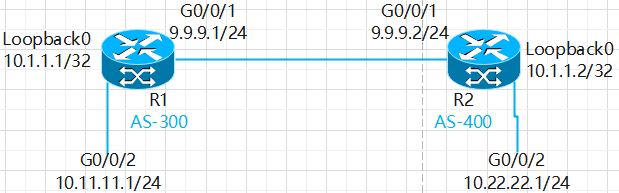
AS（Autonomous System）在2009年1月之前，使用2字节的AS号，即1到65535，

公有AS号为1~64511，私有AS号为64512~65535

在2009年1月后，IANA决定使用4字节长度的AS号，范围65536到4294967295

**★eBGP**

拓扑图：



\*首先配置好各接口ip，过程省略

[AR2220-R1] bgp 300 #开启bgp进程，本设备as号为300

[AR2220-R1-bgp] router-id 10.1.1.1 #手动指定route id

[AR2220-R1-bgp] timer keepalive 10 hold 30 #

[AR2220-R1-bgp] timer connect-retry 3 #重连时间，秒

[AR2220-R1-bgp] peer 9.9.9.2 as-number 400 #配置邻居及指定邻居的as号

[AR2220-R1-bgp] peer x.x.x.x allow-as-loop #允许接收路由信息中带有一次本as号的路由

[AR2220-R1-bgp] ipv4-family unicast #进入ipv4路由配置界面

[AR2220-R1-bgp-af-ipv4] network 10.1.1.1 32 #手动宣告网段/ip

[AR2220-R1-bgp-af-ipv4] network 10.11.11.0 24 #手动宣告的网段必须处于活跃状态

[AR2220-R1-bgp-af-ipv4] network 9.9.9.0 24 #发布的子网掩码必须和接口上的一致

[AR2220-R1-bgp-af-ipv4] maximum load-balancing ebgp 8 #配置ecmp等价路由为最多8条，

#ecmp等价路由数目根据设备型号而定，有的一般最大只可设置为8，有的也可设置为32，64

#ECMP（Equal-Cost Multiple Path）等成本负载分担，指到达同一目的地址有多条等价链路，流量在这些等价链路上平均分配，要求为同一路由协议生成的多条路由，这些路由的优先级和度量都相同

#UCMP（Unequal-Cost Multiple Path）非等成本负载分担，是指到达同一目的地址有多条带宽不同的等价链路，流量根据带宽按比例分担到各条链路上。

#ECMP支持逐流及逐包的负载分担方式，UCMP仅支持逐流的方式（即根据五元组去做hash确定走哪条链路）

#逐包方式为rr均匀轮询方式

[AR2220-R2]bgp 400

[AR2220-R2-bgp]peer 9.9.9.1 as-number 300

[AR2220-R2-bgp] ipv4-family unicast

[AR2220-R2-bgp-af-ipv4]network 10.1.1.2 32

[AR2220-R2-bgp-af-ipv4]network 10.22.22.0 24

[AR2220-R2-bgp-af-ipv4]network 9.9.9.0 24

[AR2220-R2-bgp-af-ipv4]maximum load-balancing ebgp 8

#查看：

[AR2220-R1] disp bgp peer #查看bgp邻居

Status codes: \* - Dynamic

BGP local router ID : 192.168.1.1

Local AS number : 300

Total number of peers : 1 Peers in established state : 1

Peer V AS MsgRcvd MsgSent OutQ Up/Down State PrefRcv

9.9.9.2 4 400 7 8 0 00:02:25 Established 3

[AR2220-R1] disp bgp routing-table #查看bgp学习到的路由

BGP Local router ID is 192.168.1.1

Status codes: \* - valid, > - best, d - damped,

h - history, i - internal, s - suppressed, S - Stale

Origin : i - IGP, e - EGP, ? - incomplete

Total Number of Routes: 6

Network NextHop MED LocPrf PrefVal Path/Ogn

\*> 9.9.9.0/24 0.0.0.0 0 0 i

9.9.9.2 0 0 400i

\*> 10.1.1.1/32 0.0.0.0 0 0 i

\*> 10.1.1.2/32 9.9.9.2 0 0 400i

\*> 10.11.11.0/24 0.0.0.0 0 0 i

\*> 10.22.22.0/24 9.9.9.2 0 0 400i

[AR2220-R1] disp ip routing-table protocol bgp #查看bgp生效的路由

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

BGP routing table status : <Active>

Destinations : 2 Routes : 2

Destination/Mask Proto Pre Cost Flags NextHop Interface

10.1.1.2/32 EBGP 255 0 D 9.9.9.2 GigabitEthernet0/0/1

10.22.22.0/24 EBGP 255 0 D 9.9.9.2 GigabitEthernet0/0/1

[AR2220-R1] ping -a 10.11.11.1 10.22.22.1

PING 10.22.22.1: 56 data bytes, press CTRL\_C to break

Reply from 10.22.22.1: bytes=56 Sequence=1 ttl=255 time=1 ms

Reply from 10.22.22.1: bytes=56 Sequence=2 ttl=255 time=1 ms

Reply from 10.22.22.1: bytes=56 Sequence=3 ttl=255 time=1 ms

**★bfd联动**

[AR2220-R1] bfd #先全局使能bfd

[AR2220-R1] bgp 100

[AR2220-R1-bgp] peer 9.9.9.2 bfd enable

[AR2220-R1-bgp] peer 9.9.9.2 bfd min-tx-interval 1000 min-rx-interval 1000

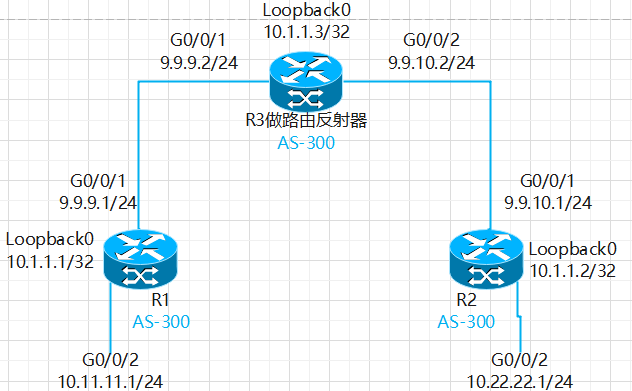
**★引入直连路由**

[AR2220-R1-bgp] ipv4-family unicast #进入ipv4路由配置界面

[AR2220-R1-bgp-af-ipv4] import-route direct #引入直连路由

**★iBGP路由反射**

拓扑图：



\*首先配置好各接口ip，过程省略

# R1（R2省略）

bgp 300

router-id 10.1.1.1

peer 9.9.9.2 as-number 300

ipv4-family unicast

network 10.1.1.1 255.255.255.255

network 10.11.11.0 255.255.255.0

# R3做路由反射器

（iBGP水平分割规则限制：某路由器学习自一个iBGP对等体的路由信息不会再更新发送给其他iBGP邻居，当其他邻居之间没有建立邻居关系时，路由信息没法传递过去，要在中间的路由器配置RouteReflect，配置路由反射后，会把ibgp邻居发来的路由信息再发给其他ibgp邻居）

bgp 300

router-id 10.1.1.3

group rr\_inter\_1 internal #创建对等体组（把同类对端都放入此组，方便配置）

peer rr\_inter\_1 reflect-client #使此组内的路由器进行路由反射

peer 9.9.9.1 group rr\_inter\_1 #将9.9.9.1对端放入rr\_inter\_1组内

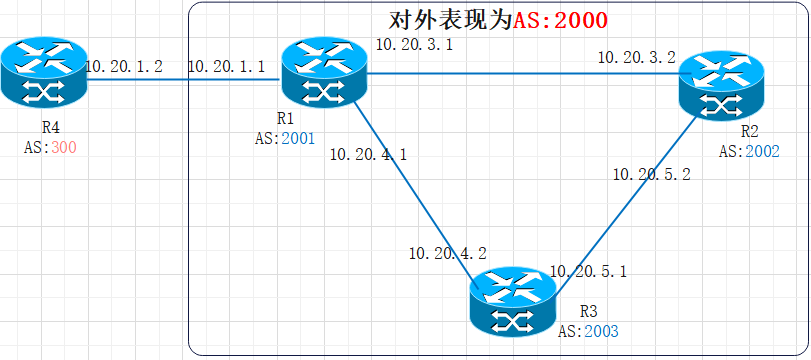
peer 9.9.10.1 group rr\_inter\_1 # iBGP对等体组不需要配置AS号

ipv4-family unicast

network 10.1.1.3 255.255.255.255

reflector cluster-id 1

**★iBGP联盟**



**R1为ASBR，配置如下：**

bgp 2001

router-id x.x.x.x

confederation id 2000 #对外表现为as 2000

confederation peer-as 2002 2003

peer 10.20.3.2 as-number 2002

peer 10.20.4.2 as-number 2003

peer 10.20.2.2 as-number 300

ipv4-family unicast

peer 10.20.3.2 next-hop-local #配置这条之后，R2到外部都要经过R1

peer 10.20.4.2 next-hop-local #配置这条之后，R3到外部都要经过R1

**R2配置：**

bgp 2002

router-id x.x.x.x

confederation id 2000

confederation peer-as 2001 2003

peer 10.20.3.1 as-number 2001

peer 10.20.5.1 as-number 2003

**R4配置：**

bgp 300

peer 10.20.1.1 as-number 2000 #将R1视为as 2000

**★路由策略**

路由策略的操作对象是路由信息，主要实现路由过滤和路由属性设置等功能，通过改变路由属性（包括可达性）来改变网络流量所经过的路径

一条route-policy可有多个node组成，一条node匹配通过后，不再匹配剩下的node

一条node中可if-match匹配多个目标，各if-match之间为AND关系，各条if-match都通过才认为通过此node

（即node之间为OR关系，同一node内的各if-match为AND关系）

[] route-policy 1 permit node 1

if-match acl 2001

if-match ip-prefix xxxx

**★策略路由**

# 策略路由的操作对象是数据包，在路由表已经产生的情况下，不按照路由表进行转发，而是根据需要按照某种策略改变数据包的转发路径

[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] disp 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

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

**★分布式网关引入arp主机路由**

spine-leaf组网中，leaf层配置分布式网关，引入arp主机路由，所有leaf层设备都一样的配置

interface Vlanif10

ip address 192.168.10.1 255.255.255.0

mac-address 0000-0000-0001 #如果一台终端连接多个接入层网关时，要求所有接入层网关的mac地址相同

arp timeout 60

arp proxy anyway enable #开启arp代理

arp delete trigger link-down enable #当接口down时，删除其上的所有arp

arp direct-route enable #引入直连路由

arp direct-route preference 1 #引入的直连路由优先级设置为1，默认255

arp smart-discover enable #开启arp智能探测，每秒发128个arp请求报文（本网段）

#

arp smart-discover interval 10 count 64 #全局设置为每10秒突发64个arp请求包

#如果网段包含的主机数量过多，如16位的地址段，则不建议开启arp smart-discover，会产生大量的arp包

ip ip-prefix arp-host-prefix1 index 10 permit 0.0.0.0 32 greater-equal 32 less-equal 32

#创建一个名为arp-host-prefix1的ip前缀规则，匹配32位的主机路由

route-policy arp-host-router1 permit node 10 #创建路由策略

if-match ip-prefix arp-host-prefix1 #匹配ip-prefix

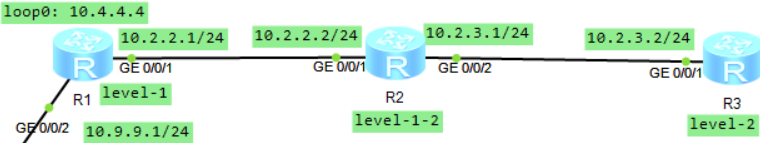
apply community 10:10 #应用团体属性（非必须，可用于路由策略的控制）

bgp 100

ipv4-family unicast

import-route direct route-policy arp-host-router1 #引入直连路由时做相应的匹配限制

**★IS-IS**



**各设备的systemID不能相同！**

**R1配置**

isis 1 #1为进程id，可配置为1-65535，默认1，仅本地有效，一台路由器可启动多个isis进程

is-level level-1 #指定level，默认为level-1-2

cost-style wide #设置is-is设备接收和发送路由的开销类型

network-entity 49.0002.1111.1111.1111.00 #设置isis网络实体名称（NET）

is-name ar1 #在LSP中带上此xx名称方便查看维护

import-route direct level-1 #引入直连路由

#

interface GigabitEthernet0/0/1

ip address 10.2.2.1 255.255.255.0

isis enable 1 #在接口上使能isis进程1

isis circuit-level level-1

isis authentication-mode md5 cipher passxx #配置接口MD5验证

#

interface GigabitEthernet0/0/2

ip address 10.9.9.1 255.255.255.0

#

interface LoopBack0

ip address 10.4.4.4 255.255.255.255

#

**R2配置**

isis 1

cost-style wide

network-entity 49.0002.1111.1111.1112.00 #设置isis网络实体名称，同一个level-1区域号要求相同

is-name ar2

#

interface GigabitEthernet0/0/1

ip address 10.2.2.2 255.255.255.0

isis enable 1

isis circuit-level level-1

isis authentication-mode md5 cipher passxx #配置接口MD5验证

#

interface GigabitEthernet0/0/2

ip address 10.2.3.1 255.255.255.0

isis enable 1

isis circuit-level level-2

#

**R3配置**

isis 1

is-level level-2

cost-style wide

network-entity 49.0003.1111.1111.1113.00

is-name ar3

#

interface GigabitEthernet0/0/1

ip address 10.2.3.2 255.255.255.0

isis enable 1

isis circuit-level level-2

#

<Huawei> disp isis peer #查看isis邻居

Peer information for ISIS(1)

System Id Interface Circuit Id State HoldTime Type PRI

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

ar1 GE0/0/1 ar1.01 Up 9s L1 64

ar3 GE0/0/2 ar2.02 Up 28s L2 64

Total Peer(s): 2

<Huawei> disp isis lsdb #查看isis链路状态数据库

**★IGMP**

待更新

<Huawei> disp igmp routing-table #查看IGMP路由表

<Huawei> disp multicast routing-table #查看组播路由表

<Huawei> disp multicast forwarding-table #查看组播转发表

**★PIM**

待更新

<Huawei> disp pim routing-table #查看PIM路由表

<Huawei> disp multicast routing-table #查看组播路由表

<Huawei> disp multicast forwarding-table #查看组播转发表

**★MPLS**

LSR（Label Switch Router）标签交换路由器

LER（Label Edge Router）标签边界路由器

FEC（转发等价类）

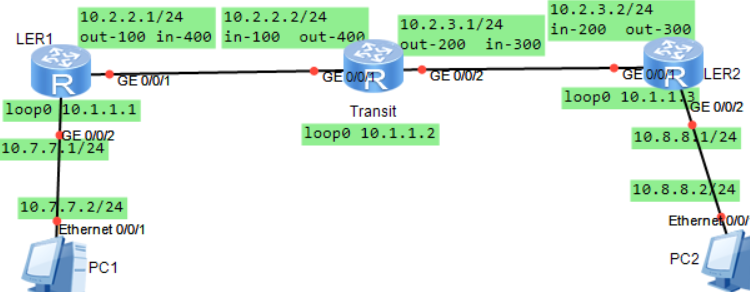
LSP（标签转发路径）mpls报文经过的路径，路径起始lsr称为入站LER，最后一个lsr称为出站LER；可以静态创建一条LSP，也可动态创建；一条LSP途经各跳路由器时，在路由器上的label id可不一样，只要能将报文送达目的地即可，和vlan类似，中间经过的vlan id可不一样，只要将报文送达目标主机即可。

不过：一条LSP的流量是单向的，要想双方可达，需要建立一来一回共2条LSP

LDP（标签分发协议）用于动态建立LSP，在RFC3036中被定义

**★静态LSP**

一条LSP在各结点上面对应的label值可不一样，一条LSP流量是单向的



LER1配置：

mpls lsr-id 10.1.1.1 #指定mpls的LSR-ID，一般使用loop口的ip，必须手工配置，没有缺省的

mpls #全局开启mpls

int g0/0/1

ip addr 10.2.2.1 24

mpls #LSP经过的接口上开启mpls

#

static-lsp ingress lsp1 destination 10.8.8.0 24 nexthop 10.2.2.2 out-label 100

static-lsp egress lsp2 incomming-ingerface g0/0/1 in-label 400

Transit配置：

#省略mpls全局及接口相关配置

static-lsp transit lsp1 incomming-interface g0/0/1 in-label 100 nexthop 10.2.3.2 out-label 200

static-lsp transit lsp2 incomming-interface g0/0/2 in-label 300 nexthop 10.2.2.1 out-label 400

LER2配置：

#省略mpls全局及接口相关配置

static-lsp ingress lsp2 destination 10.7.7.0 24 nexthop 10.2.3.1 out-label 300

static-lsp egress lsp1 incomming-interface g0/0/0 in-label 200

★说明：

在LER1和LER2上要求配置到2边客户侧的路由，在transit上不需要配置2端pc的路由，根据mpls label进行转发

ingress负责将匹配到的报文打上mpls label（根据destination目的网段及nexthop下一跳ip进行匹配）

egress负责将 入接口的匹配上的in-label流量 剥去mpls label，再进行普通路由转发

disp mpls static-lsp #查看lsp状态

**★动态lsp（LDP协议）**

1.LSP数据总是从源发往目的，由上游发往下游

2.在lsp路径倒数第2跳弹出mpls label，即离目的路由器的前一个路由器上把目标流量的mpls label剥去，这样当流量传到最后一跳路由器时直接进行普通路由转发，无需再在最后一跳进行mpls label剥离工作，减轻负担

LDP报文基于TCP，封装在646/tcp里（hello报文是封装在udp里，发送目标地址224.0.0.2，每5秒周期发送）

LDP传输地址是用于建立tcp连接的，默认同LSR-ID的ip（可在其他三层接口上指定其为ldp传输地址）

int g0/0/1

mpls ldp transport-address interface #指定使用此接口的ip为传输地址

★LDP标签发布方式

①DU（Downstream Unsolicited）下游自主模式，当建立完ldp会话后，下游主动向上游发布标签映射通告报文

②DoD（Downstream On Demand）下游按需要，触发方式，在收到上游lsp的标签请求报文后，才会发送上游需要的标签映射信息给上游

华为路由器默认使用DU下游自主模式，但只发布32位掩码路由的标签映射信息

★LDP标签分配的控制方式

①独立控制方式，中间路由器在没有收到下游lsr发来的标签信息时，就可向上游发布

②有序控制方式，中间路由器必须收到下游lsr发来的标签信息时，才可向上游发布，（华为路由器默认）

独立控制方式下，中间结点标签通告较自由，但无法保证到目标网络的lsp是连续的，容易发生lsp断裂情况

有序控制方式下，标签通告受到一定的限制，建立lsp效率会受到一定影响，但确保了整条lsp是连续的

★标签的保持方式

①保守方式（conservative retention mode）对于特定的一条FEC，即使从多个LDP邻居都收到了标签映射，该lsr只会将最优的标签保留下来

②自由方式（liberal retention mode）lsr会保存所有收到的标签映射，即使有些标签没有对应的路由或没有下一跳，优点是当网络发生故障时可以立即使用新的标签计算出新的LSP路径，收敛较快

mpls ldp

label-retention conservative #修改标签的默认保留方式为conservative

华为设备默认为： DU+有序+自由

★LDP和IGP路由同步

当主备链路切换时，IGP路由协议收敛速度要快于LDP协议的，这会导致旧的LSP被删除，而新的LSP未建立好，导致业务中断一会，一般在5s左右，开启LDP和IGP同步后，会在链路切换之前抑制igp邻居关系的建立，先建立新的LSP（旧的LSP仍保留），新的LSP建立完成后，再切换链路删除旧的LSP

int g0/0/1

ospf ldp-sync #配置osp和LDP同步

★在MPLS骨干网内部不建议对路由进行汇总，否则会导致LSP不连续

★动态LSP建立配置

只需要在全局启动mpls及mpls ldp，再在骨干网接口上启用mpls ldp即可

mpls lsr-id 10.1.1.1 #指定mpls的LSR-ID，一般使用loop口的ip，必须手工配置，没有缺省的

mpls #全局开启mpls

mpls ldp #全局开启mpls ldp

#

int g0/0/1

ip addr 10.2.2.1 24

mpls #LSP经过的接口上开启mpls

mpls ldp #LSP经过的接口上开启mpls ldp

#

disp mpls ldp session #查看ldp邻居会话状态

disp mpls lsp #查看lsp转发表，默认只学到32位掩码的标签映射，可用lsp-trigger引入其他路由

#同一条路由对应2条标签，有NULL的，有非空的，如果本地接收到去往目标前缀的报文时，使用入标签为NULL的那条lsp，如果接收到带有标签的mpls报文，则使用不带NULL的那条lsp

ip ip-prefix 1 permit 10.22.22.0 24 #创建一条ip前缀匹配

#

mpls

lsp-trigger ip-prefix 1 #将此ip前缀匹配的路由在ldp中宣告

disp mpls lsp include 10.22.22.0 24 verbose #查看lsp转发表中关于此路由的详细情况

★LDP标签过滤

ip ip-prefix 1 permit 10.22.22.0 24 #创建一条ip前缀匹配

#

mpls

inbound peer 10.2.2.1 fec ip-prefix 1 #配置ldp inbound策略，只接收匹配的标签映射

**★MPLS VPN**

**VPN解决的问题：**

①不同的用户可使用重叠（相同）的ip地址段，在转发时互不干扰，路由表隔离开来

②用户的ip地址不暴露在外网上，是以隧道的方式传递的（将用户流量封装在外网流量之上）

**VPN隧道分类：**

①pptp/l2tp/vxlan这些是将用户的二层流量（mac帧）封装在外网的udp报文之上，也称为二层隧道协议

②ipsec这种是将用户的三层流量（ip报文）封装在外网的ip报文之上，也称为三层隧道协议

③mpls vpn这种是在用户的三层流量之前插入一个mpls Label，在外网上只根据mpls label进行转发，也称为第二层之上和第三层之下的隧道技术

外网是指不属于用户内部网络的网络，是用来承载用户内部网络流量并打通用户不同站点之间的通信

**★mpls vpn相关概念**

**①vpn-instance（vpn实例，VRF）**

不同的用户可能会使用相同的网段，当一台CE接入路由器连接多个用户网络为多个用户提供服务时，会导致路由冲突，这时可以将不同的用户流量隔离起来，单独使用一套路由转发表，就不会冲突了，这些路由转发称为VRF（VPN Routing and Forwarding table）然后在宣告这些不同的路由转发表信息时得带上一些额外的信息去区分不同的用户

在mpls vpn里，不同的用户VRF数据出站时会打上不同的mpls label

**②RD（Route Distinguisher）**

同一个用户在不同站点的流量所属的vpn实例，打上相同的一个标签，这个标签称为RD，全局有效，同一个用户的所有站点vpn实例的RD全局唯一且相同，不同用户的RD互不相同

RD字段有8字节，2字节的类型，6字节的RD值，RD值可写为xx:yy（有2种情况）

类型0: ASN:yy #ASN表示as号，2字节，yy表示服务提供商自己分配给用户vpn实例的一个id，4字节

类型1: IP-addr:yy #ip-addr使用4字节，yy表示服务提供商自己分配给用户vpn实例的一个id，4字节

**③RT（Route Target）**

也称为VPN-Target，用于在用户VRF里进行路由引入与导出的控制的，如果一个用户的不同站点间需要互相学习路由，则需要使用相同的RT，或者说站点的eRT要与iRT匹配，才会引入此路由

RT字段有8字节，2字节的类型，6字节的RT值，RT值可写为xx:yy （xx和yy不可同时为0）

RT是BGP扩展团体属性，有2种类型

类型值0x0002： 2字节AS：4字节id

类型值0x0102： 4字节ip：2字节id

一条vpn路由可带多个RT值，可灵活地控制不同站点间路由的引入

**基本配置：**

ip vpn-instance vpnxx #创建一个名为vpnxx的vpn实例（vrf）

ipv4-family

route-distinguisher 10:22 #配置RD，全局有效，一个vpn实例只可有一个RD

vpn-target 10:22 export-extcommunity #eRT全局有效，

vpn-target 10:22 import-extcommunity # iRT，RT可有多个

#

mpls lsr-id x.x.x.x

mpls

mpls ldp

#

int g0/0/1 #客户网络流量入口

ip binding vpn-instance vpnxx #绑定到vpn实例，绑定后接口上的所有ip配置会被清空，需要重新配置ip

ip addr 172.16.1.1 24

#

bgp 1000 #创建BGP进程，所有vpn实例相关信息借助bgp去传输

router-id y.y.y.y

peer x.x.x.x as-number 1000

peer x.x.x.x connect-interface loopback0

ipv4-family unicast #普通的ipv4路由宣告

undo synchronization

network ........

ipv4-family vpnv4 #vpn实例，配置路由策略及对等体

policy vpn-target #表示在vpn实例间引入路由时需要匹配eRT和iRT

peer x.x.x.x enable #只和这些对等体之间交换vpn相关信息

ipv4-family vpn-instance vpnxx #在bgp里宣告vpn实例的路由信息

network 172.16.1.0 24

xxxxx #宣告本vpn里其他的路由

#

#

disp ip routing-table vpn-instance vpnxx #查看vpn实例对应的路由表

**★第11章、Vxlan配置**

NVE概念：Network Virtualization Edge网络虚拟化边缘节点，负责vxlan数据的封装与解封装，NVE视图里可配置多个vxlan隧道

**★静态vxlan**

bridge-domain 10 #创建一个二层广播域，相当于vlan，本地有效

vxlan vni 1010 #指定vxlan的id，全局唯一

#

int g1/0/2.1 mode l2 #一个子接口为一个业务vlan，可配置多个子接口

encapsulation dot1q vid 10 #encap untag为不打tag

bridge-domain 10 #关联vxlan二层广播域

#

int Nve1 #创建nve接口，用于封装解封装vxlan载荷数据

source 10.10.1.22 #选用本设备的一个loopback接口的ip

vni 1010 head-end peer-list 10.10.1.33 #指定对端的nve接口ip

vni 2020 head-end peer-list 10.10.1.44

#

int Vbdif10 #创建vxlan二层广播域对应的三层接口，相当于vlan if

ip addr 192.168.10.1 255.255.255.0

#

disp vxlan peer [ vni 1010 ]

disp vxlan vni 1010

disp vxlan tunnel

disp bridge-domain 10 [ brief ]

**★evpn-vxlan**

使用evpn进行vxlan隧道的自动发现与建立

首先配置各设备互连口的ip，这里省略

①规划3个loopback接口ip

# leaf 1

interface LoopBack 0 # Loop0的ip用作bgp路由器id

description for\_bgp\_router\_id

ip address 10.10.1.1 32

#

interface LoopBack 1 # Loop1的ip用作evpn bgp实例的路由器id

description for\_evpn\_router\_id

ip address 10.10.1.2 32

#

interface LoopBack 2 # Loop2的ip用作nve接口的ip

description for\_vxlan\_nve\_id

ip address 10.10.1.3 32

#

commit

#

②配置普通路由协议，如bgp或ospf，本例使用eBGP

# leaf 1

bgp 100

router-id 10.10.1.1

peer 10.2.1.2 as-number 200

ipv4-family unicast

network 10.10.1.1 32

network 10.10.1.2 32

network 10.10.1.3 32

#

commit

③配置VXLAN隧道模式并使能VXLAN的ACL扩展功能（仅CE12800）

ip tunnel mode vxlan

assign forward nvo3 acl extend enable

#

assign forward nvo3 f-linecard compatibility enable

#配置非增强模式下防止VXLAN流量不通功能

commit

③创建bridge-domain和vxlan业务接入口

bridge-domain 10

vxlan vni 10

#

commit

#

int g1/0/2.1 mode l2 #同一接口可配置多个子接口，此时可根据封装的vid来区别

encapsulation dot1q vid 10

#根据vlan tag10来区别，要求入站的数据包带有vlan tag 10，encapsulation untag为匹配不打tag的流量

bridge-domain 10 #将此子接口划入BD 10

#

commit

④开启evpn功能（使能EVPN作VXLAN控制平面）所有结点都开启

evpn-overlay enable #开启evpn之后，才可在bgp里配置evpn相关命令

commit

⑤创建vpn实例（vrf）

ip vpn-instance vpn10

vxlan vni 5010

ipv4-family

route-distinguisher 10:1 #RD

vpn-target 10:5010 export-extcommunity #eRT

vpn-target 10:5010 import-extcommunity #iRT

#

commit

⑥创建evpn实例

# leaf 1

bridge-domain 10

evpn

route-distinguisher 10:2 #evpn的RD

vpn-target 10:3 #iRT,eRT

vpn-target 10:5010 export-extcommunity #新增一个eRT

#

commit

⑦创建vxlan三层网关（分布式网关）

# leaf 1

interface Vbdif10

ip binding vpn-instance vpn10

ip address 192.168.10.1 255.255.255.0

arp timeout 60

arp proxy anyway enable

mac-address 0000-0000-0001

arp direct-route enable

arp direct-route preference 1 #将引入的arp路由优先级改为1，必须比eBGP的优先级高才会生效

#

commit

⑧leaf之间建立BGP EVPN对等体关系，发布IRB路由，发布IP前缀路由

#一般一台路由设备只允许开启一个bgp实例，华为设备为evpn bgp**额外支持**一个bgp实例

#当然了，evpn也可配置在普通的bgp实例下，为了区分开来，方便管理，建议在另一bgp实例里配置

#**在单独的evpn bgp实例里，只能用iBGP**，如果有必要，请配置Route-Reflect路由反射

bgp 100.500 instance evpnxx

router-id 10.10.1.2

peer 10.10.2.2 as-number 100.500

peer 10.10.2.2 connect-interface LoopBack1

l2vpn-family evpn

policy vpn-target

peer 10.10.2.2 enable

y

peer 10.10.2.2 advertise irb

ipv4-family vpn-instance vpn10

import-route direct

advertise l2vpn evpn

#

commit

⑨创建头端复制，nve封装接口

interface Nve1

source 10.10.1.3

vni 10 head-end peer-list protocol bgp

#

commit

**★vlan-vxlan-mpls概念对照**

vlan,vxlan,mpls的某些概念有互通之处

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
|  | ID | id字段长度 | id号范围 | 区域概念 | 二层转发表 | 三层接口 | 信息交换协议 |
| vlan | vlanid | 12 bit | 0-4095 | vlan | FIB | vlanif | gvrp,vtp |
| vxlan | vni | 24 bit | 16M | bridge-domain | 无 | vbdif | evpn-bgp |
| mpls | mpls label | 20 bit | 1M | vpn-instance | LFIB | 无 | ldp-bgp |

**★第12章、网络连通性检测**

**★NQA网络质量检测**

Network Quality Analysis网络质量检测，一般用于检测出口网关的连通性，应用在静态路由上

[Huawei] nqa test-instance admin isp1 #创建名为isp1的nqa探测实例

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

[Huawei-nqa-admin-isp1] destination-address ipv4 200.1.1.2 #探测目标ip，一般为上行出口网关ip

[Huawei-nqa-admin-isp1] source-address ipv4 200.1.1.1 #探测时使用的源ip

[Huawei-nqa-admin-isp1] **frequency** 10 #每10秒进行一次nqa探测

[Huawei-nqa-admin-isp1] probe-count 3 #每次nqa探测发3个icmp包

[Huawei-nqa-admin-isp1] interval seconds 3 #每个icmp包时间间隔为3秒

[Huawei-nqa-admin-isp1] timeout 2 #ping超时2秒，默认为3秒

[Huawei-nqa-admin-isp1] vpn-instance xxxx #绑定vpn实例（vrf），可选

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

[Huawei-nqa-admin-isp1] undo start #结束探测，再次启动nqa后才会恢复路由优先级，不支持抢占

[Huawei-nqa-admin-isp1] start now

[Huawei-nqa-admin-isp1] quit

★说明：frequency的值表示一次nqa探测周期，而不是发包的频率，frequency的值要满足以下要求：

frequency > interval \* ( probeCount - 1 ) + timeout #不满足时直接返回no result，探测失败

例如：interval为3秒，probe-count为3，timeout为2，则**frequency**要大于 (3\*(3-1)+2)即8秒

[Huawei] disp nqa results #查看nqa结果

[Huawei] disp nqa history #查看nqa历史情况

**nqa一般可以应用在静态路由和策略路由上**，

**★nqa和静态路由联动**

[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 20.2.1.2 track nqa admin isp2 # isp2为nqa实例

#当nqa检测到某个网关ping不通时，就会通知路由模块取消某条路由或策略

**★nqa和策略路由联动**

[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 20.2.1.2 track nqa admin isp2

[Huawei-behavior-be2] quit

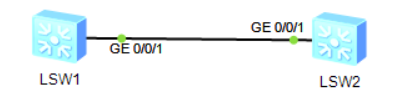
**★BFD双向转发检测**

Bidirectional Forwarding Detection双向转发检测是一种通用的快速故障检测协议，用于检测网络转发连通状况

一般的网络协议都有发送hello报文进行连通性检测，但其超时时间都比较长（几秒钟以上）这对于某此业务而言时间太长了，而BFD可以实现毫秒级的快速检测连通状态的能力。当BFD发现其检测的链路不通时就会立即通知其服务的上层协议，让上层协议及时处理（而不用等上层协议的hello超时）。

**★BFD单跳检测二层链路**

拓扑如下：



检测交换机之间的直连线路是否连通，直连端口为二层口（无ip）

**LSW1配置：**

[Huawei] interface GigabitEthernet 0/0/1

[Huawei-GigabitEthernet0/0/1] port link-type access

[Huawei-GigabitEthernet0/0/1] port default vlan 1

[Huawei-GigabitEthernet0/0/1] quit

[Huawei] bfd

[Huawei-bfd] quit

[Huawei] bfd s1\_to\_s2 bind peer-ip default-ip interface GigabitEthernet 0/0/1

[Huawei-bfd-session-s1\_to\_s2] discriminator local 1 #取值1-8191

[Huawei-bfd-session-s1\_to\_s2] discriminator remote 2

**LSW2配置：**

[Huawei] interface GigabitEthernet 0/0/1

[Huawei-GigabitEthernet0/0/1] port link-type access

[Huawei-GigabitEthernet0/0/1] port default vlan 1

[Huawei-GigabitEthernet0/0/1] quit

[Huawei] bfd

[Huawei-bfd] quit

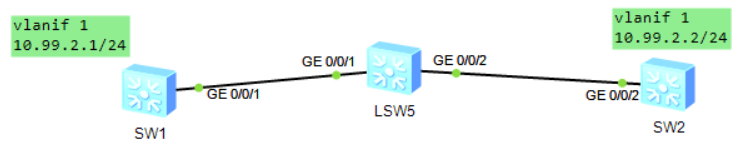
[Huawei] bfd s2\_to\_s1 bind peer-ip default-ip interface GigabitEthernet 0/0/1

[Huawei-bfd-session-s2\_to\_s1] discriminator local 2 #取值1-8191

[Huawei-bfd-session-s2\_to\_s1] discriminator remote 1

[Huawei] disp bfd session all verbose #查看bfd会话

**★BFD单跳检测三层链路**



**SW1配置**

[Huawei] int vlanif 1

[Huawei-Vlanif1] ip add 10.99.2.1 24

[Huawei-Vlanif1] qui

[Huawei] bfd

[Huawei-bfd] quit

[Huawei] bfd s1\_to\_s2 bind peer-ip 10.99.2.2 interface vlanif 1

[Huawei-bfd-session-s1\_to\_s2] discriminator local 1 #取值1-8191

[Huawei-bfd-session-s1\_to\_s2] discriminator remote 2

**SW2配置**

[Huawei] int vlanif 1

[Huawei-Vlanif1] ip add 10.99.2.2 24

[Huawei-Vlanif1] qui

[Huawei] bfd

[Huawei-bfd] quit

[Huawei] bfd s2\_to\_s1 bind peer-ip 10.99.2.1 interface vlanif 1

[Huawei-bfd-session-s2\_to\_s1] discriminator local 2 #取值1-8191

[Huawei-bfd-session-s2\_to\_s1] discriminator remote 1

[Huawei] disp bfd session all verbose #查看bfd会话

**★BFD与静态路由联动**

[Huawei] ip route-static 0.0.0.0 0.0.0.0 10.99.2.2 track bfd-session s1\_to\_s2

#当bfd检测到某个网关不通时，就会通知路由模块取消某条路由或策略

**★BFD与OSPF联动**

**★BFD与ISIS联动**

**★BFD与BGP联动**

**★BFD与VRRP联动**

**★第13章、NAT地址转换**

**交换机不支持NAT地址转换功能，需要使用路由器去配置**

**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（dNAT）**

[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] disp nat session all #查看nat会话情况

**★第14章、隧道技术**

**★GRE隧道**

Generic Routing Encapsulation通用路由封装协议，GRE封装在IPv4报文中，ipv4上层协议号为47

GRE头部最短4字节，最长16字节，头部之后为被封装的ip报文

解封装过程：网络层发现IP头的协议号为47则剥离IP头部，将剩下的部分交给GRE模块，GRE模块剥离GRE头部后，剩下的内层IP数据包交给网络层继续处理



R1配置：

int Tunnel0/0/0

ip addr 10.12.1.1 255.255.255.252

tunnel-protocol gre

source 200.1.1.1

destination 200.2.2.2

R2配置：

int Tunnel0/0/0

ip addr 10.12.1.2 255.255.255.252

tunnel-protocol gre

source 200.2.2.2

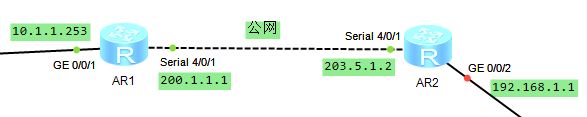
destination 200.1.1.1

disp ip int brief #可见Tunnel0/0/0状态为up

#之后，2边可配置去往对端的路由，下一跳为对端Tunnel的ip

**★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] disp ike proposal #查看ike提议

[Huawei] disp ipsec proposal #查看ipsec提议

[Huawei] disp ike peer #查看ike对端

[Huawei] disp ipsec statistics esp #查看ipsec统计情况

**★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

**★第15章、其他**

**★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

**★PPP**

[Huawei] int s4/0/1

[Huawei-Serial4/0/1] virtualbaudrate 2048000 #设置串口波特率为2M

[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

**★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] disp pppoe-server session all #查看pppoe会话情况

**★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

**★第16章、iStack堆叠（虚拟化）**

本章节以S5735型号交换机为例

不同型号交换机配置不太一样，需要查看相应的产品配置手册，但大概思路是一致的

**#交换机1**

[HUAWEI] interface stack-port 0/1 #创建堆叠逻辑口（slot-id/stack-port，slot-id为0，stack-port取值为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，未重启时当前仍为slot 0

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 #当前设备堆叠优先级，1~255，默认100，越大越优先

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

**#交换机2**

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

[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

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: --

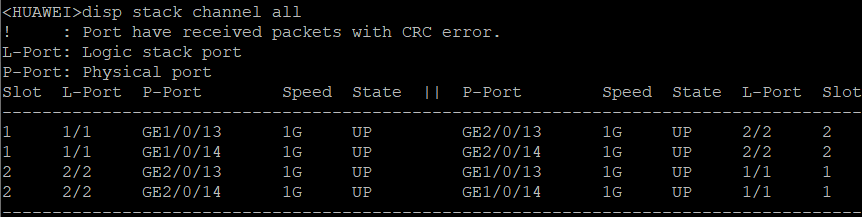
Slot Role MAC Address Priority Device Type

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

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（堆叠口网线拔掉后），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，所以要确保堆叠线不松动

**★stack物理成员口退出逻辑口**

[switch2] interface 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>

★有些高级系列型号设备堆叠后，堆叠口可以配置crc校验，链路中出现坏包，丢包时shutdown此接口，切换到备份链路上

# interface g1/0/1

port crc-statistics trigger error-down

#

trap-threshold crc-statistics #配置crc错误报文告警阈值和告警时间间隔

# error-down auto-recovery cause crc-statistics interval #接口自动恢复

# display error-down recovery #查看接口自动恢复信息

为了防止堆叠线故障，出现2个主设备，需要配置双活检测，在Eth-Trunk聚合口上配置

# dual-active detect mode relay

# disp dual-active

**★退出堆叠**

[Huawei1] reset stack configuration

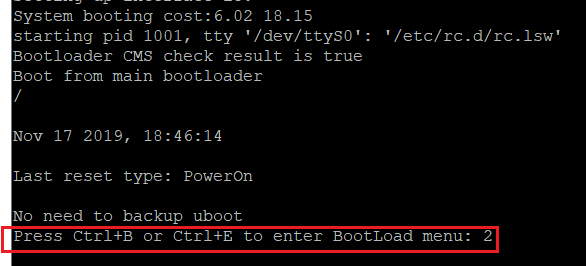
Warning: This operation will clear all stack configurations and may lead to the loss of the slot ID configuration and cause the device to reset immediately. Are you sure you want to continue? [Y/N]: y

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

**★第17章、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

其他可能的界面：

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.

**初始化账号密码**：

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

**★第18章、防火墙配置**

**★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

**★防火墙三层子接口打vlan**

interface Eth-Trunk1.100

vlan-type dot1q 100

ip addresss 10.1.1.2 24

**★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（创建放通策略）**

[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 #创建一条名为sec-policy-trust-local的策略

[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

Total:2

RULE ID RULE NAME STATE ACTION HITS

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

2 sec-policy-internalxx-local enable permit 2

0 default enable deny 331

**#最后有条默认的rule deny所有**

**★新增一条策略**

#首先创建源ip地址集；address-set 名称长度为1-63字符，若有空格，需要用""引号括起来（长度不含引号）

ip address-set policy-test-srcip type object

description policy-test-srcip

address 0 10.88.0.0 mask 16

address 1 10.99.1.2 mask 32

quit

#创建目的ip地址集；address-set 名称长度为1-63字符，若有空格，需要用""引号括起来（长度不含引号）

ip address-set policy-test-destip type object

description policy-test-destip

address 0 172.16.33.0 mask 24

quit

#创建目的端口集；service-set 名称长度为1-63字符，若有空格，需要用""引号括起来（长度不含引号）

ip service-set policy-test-service type object

description policy-test-service

service 0 protocol tcp source-port 0 to 65535 destination-port 443

service 1 protocol udp source-port 0 to 65535 destination-port 123

quit

#新增一条策略；rule name策略名长度为1-32字符，若有空格，需要用""引号括起来（长度不含引号）

security-policy

rule name policy-test

source-address address-set policy-test-srcip

destination-address address-set policy-test-destip

service policy-test-service

policy logging #记录策略命中日志

session logging #记录会话日志

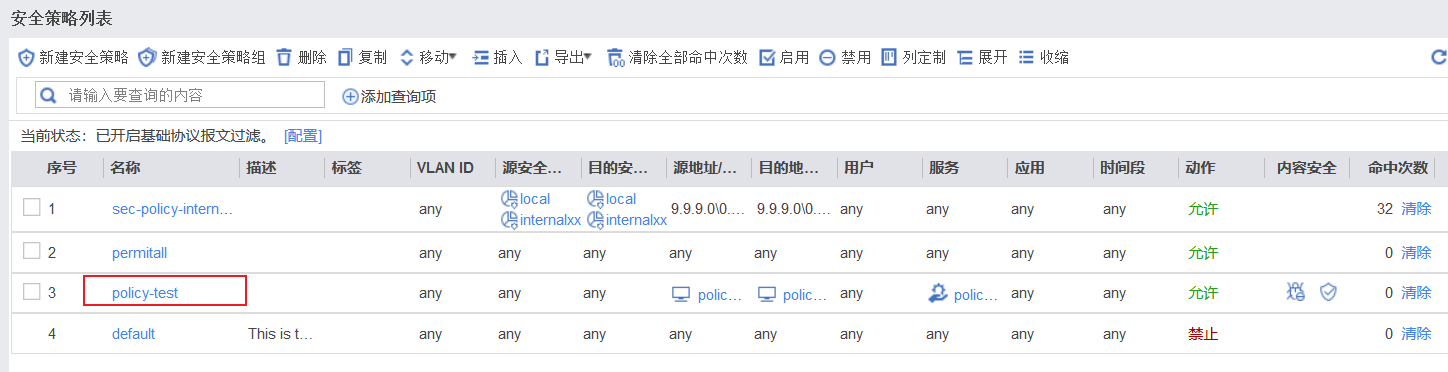
profile av default #反病毒

profile ips default #入侵防御

action permit

quit

#默认情况下，新增的策略放在末尾（default之前）



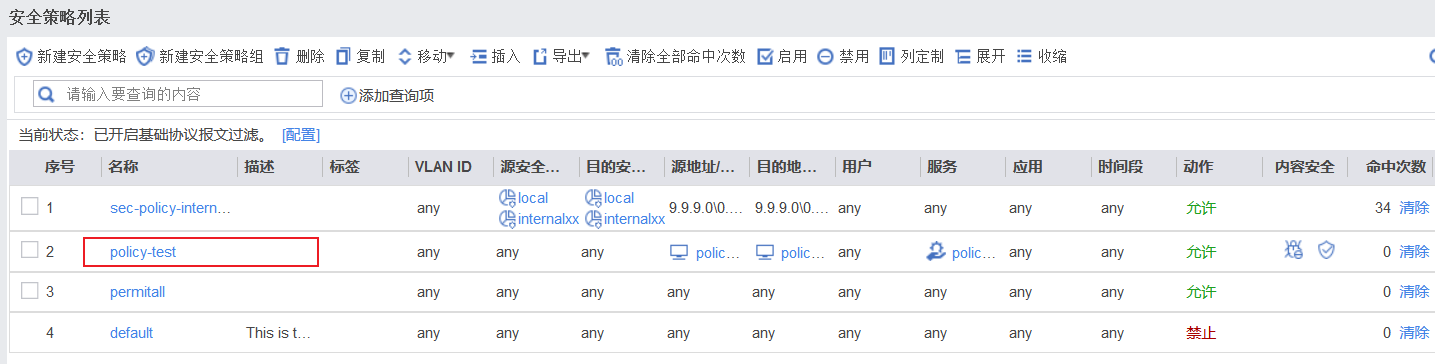
#移动新增的策略到某条策略之后

security-policy

rule move policy-test after sec-policy-internalxx-local

quit

#



**★ASPF多通道协议设置**

ASPF（Application SpecificPacket Filter）针对应用层的特殊包过滤技术（基于应用层包过滤），其原理是检测通过设备的报文的应用层协议信息，记录临时协商的数据连接，使得某些在安全策略中没有明确定义要放行的报文也能够得到正常转发。

Application Layer Gateway 应用层网关技术能对多通道协议进行应用层报文信息的解析和地址转换，将载荷中需要进行地址转换的IP地址和端口或者需特殊处理的字段进行相应的转换和处理，从而保证应用层通信的正确性。

主动模式穿越SNAT主要用于FTP服务器部署在公网，客户端需要通过SNAT转换访问服务器。

此时需要借助ALG技术才可以完成穿越防火墙。

ASPF和ALG功能使用的是同一个配置，只是不同场景下FW对报文的处理不同，因而叫法不同。非NAT场景下叫ASPF，NAT场景下叫ALG

策略→ASPF配置



**★设置TCP最大报文长度**

tcp-mss，默认为1460，如果有vpn流量经过，则承载的数据可能会因为此tcp-mss过大，而导致报文被丢弃。

因为vpn隧道2端设备不知道自己的流量会经过vpn，所以将tcp-mss设置为默认值1460，vpn本身有外部的报文信息开销，导致1460字节长度的数据封装在vpn隧道传输时，无法通过防火墙（1460数据加vpn开销，大于了tcp-mss）

此时若将vpn经过的防火墙tcp-mss设置小一点（减去vpn的报文开销），比如1360，则经过vpn的流量都能正常经过防火墙（防火墙把这些流量分片了）



**★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





**★安装弱安全组件**

有些防火墙默认安全要求较高，导致ssh服务默认只支持ecc密钥，没有rsa密钥，所以大多数shell终端无法通过ssh远程登录这些防火墙

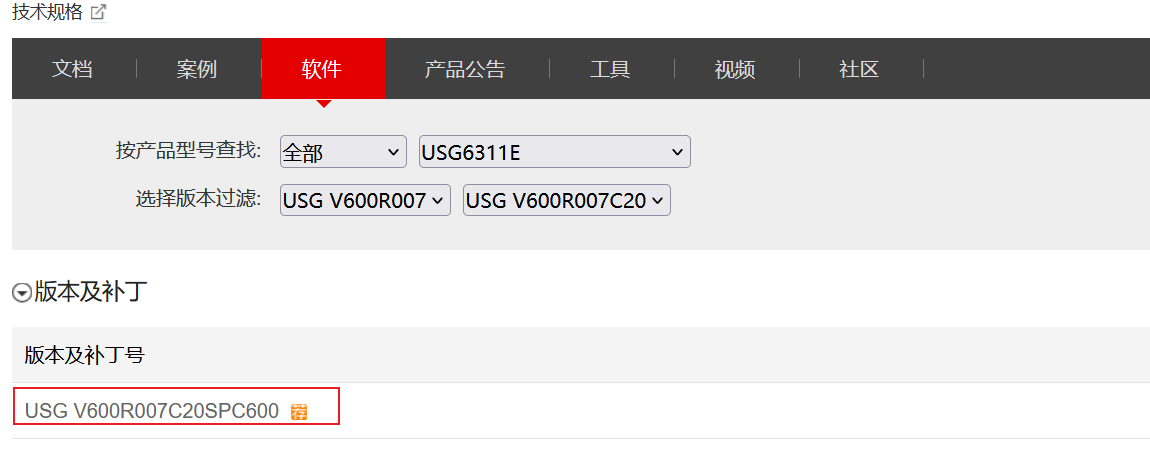
[USG6300E] ssh server publickey ?

ecc ECC public key algorithm

可以安装防火墙弱安全组件，使其支持rsa密钥

到华为官网查找目标型号的软件：

https://support.huawei.com/enterprise/zh/security/usg-pid-22914752/software



首先要注册产品，才能下载相应产品的软件：

https://support.huawei.com/enterprisemysupport/mysupport#click=productreg





下载组件版本和当前系统版本要保持一致，不一致的先升级系统版本，

点击组件名称，进入下载页



点击直接下载

下载后，使用ftp/tftp上传到防火墙上

> install-module usg6300e\_v600r007c20spc600\_weakea.mod

Error: The file hda1:/$\_install\_mod/usg6300e\_v600r007c20spc600\_weakea.mod does not exist on the main board.

在根目录下，直接安装不行，它默认是要到hda1:/$\_install\_mod/子目录下去找组件，所以先复制到此子目录下

> copy usg6300e\_v600r007c20spc600\_weakea.mod hda1:/$\_install\_mod/usg6300e\_v600r007c20spc600\_weakea.mod

> install-module usg6300e\_v600r007c20spc600\_weakea.mod

/---------------------------------------------------------------------------------\

| Warning: The weak encryption algorithm component package is being loaded, |

| which brings security risks to the device. Therefore, confirm that you need to |

| use the weak encryption algorithm before the installation. In addition, if the |

| device is deployed in a hot standby environment, ensure that this component |

| is loaded on both devices to prevent exceptions. |

\---------------------------------------------------------------------------------/

Continue?[Y/N]: y.

Info: Installing the module hda1:/$\_install\_mod/usg6300e\_v600r007c20spc600\_weakea.mod.........

Info: Succeeded in MOD Install..

Info: Succeeded in installing the module on the master board.

Info: The slot 11 does not have module to be installed......

[USG6300E] ssh server publickey ? #安装完弱安全组件后，就支持rsa了

dsa DSA public key algorithm

ecc ECC public key algorithm

rsa RSA public key algorithm

rsa\_sha2\_256

rsa\_sha2\_512

**★防火墙HA双机热备配置**

HRP协议是华为自己开发的协议，主要是在VGMP协议的基础上进行扩展得到的；VGMP是华为的私有协议，主要是用来管理VRRP的，VGMP也是华为的私有协议，是在VRRP的基础上进行扩展得到的。不管是VGMP的报文，还是HRP的报文，都是VRRP的报文，只是防火墙在识别这些报文的时候能根据自己定义的字段能判断出是VGMP的报文，HRP的报文，或者是普通的VRRP的报文。

在Eudemon防火墙上，hrp的作用主要是备份防火墙的会话表，备份防火墙的servermap表，备份防火墙的黑名单，备份防火墙的配置，以及备份ASPF模块中的公私网地址映射表和上层会话表等。

两台防火墙正确配置VRRP，VGMP，以及HRP之后，将会形成主备关系，这个时候防火墙的命令行上会自动显示防火墙状态是主还是备，如果命令行上有HRP\_M的标识，表示此防火墙和另外一台防火墙进行协商之后抢占为主防火墙，如果命令行上有HRP\_S的标识，表示此防火墙和另外一台防火墙进行协商之后抢占为备防火墙。防火墙的主备状态只能在两台防火墙之间进行协商，并且协商状态稳定之后一定是一台为主状态另外一台为备状态，不可能出现两台都为主状态或者都是备状态的。

★FW1

hrp enable #使能HRP之后防火墙将形成主备状态

undo hrp preempt enable #关闭抢占功能

hrp device active #主墙

hrp mirror config enable #开启 配置快速备份 功能

hrp interface Eth-Trunk0 remote 10.99.255.1 #添加防火墙配置会话备份通道，即防火墙心跳口

hrp track interface g0/0/1 #对目标链路进行监控，若目标链路down了，则优先级减2，若有vrrp，则优先级减去（2+vrrp组数量\*2）

hrp track interface Eth-Trunk1 #对目标链路进行监控，若目标链路down了，则优先级减去（此聚合口的成员口数量\*2）

hrp track vlan 100 #对目标vlan接口进行监控，若目标链路down了，则优先级减去（此vlan的端口数量\*2）

hrp authentication-key xxxx

★FW2

hrp enable

undo hrp preempt enable

hrp device standby #备墙

hrp mirror config enable

hrp interface Eth-Trunk0 remote 10.99.255.2 #添加防火墙配置会话备份通道，即防火墙心跳口

hrp track interface Eth-Trunk1

hrp track interface Eth-Trunk2

hrp authentication-key xxxx

#

display hrp #显示当前hrp的状态信息

display hrp verbose #显示当前hrp的详细状态信息

其他配置：

hrp configuration check acl #检查主备防火墙两端的ACL的配置是否一致

display hrp configuration check acl #查看两边的配置是否一致。

hrp configuration check hrp #检查主备防火墙两端的 HRP的配置是否一致

display hrp configuration check hrp #查看两边的配置是否一致

hrp interface Ethernet 1/0/0 high-availability #配置防火墙的高可用性接口。主要是用来实现防火墙的会话快速备份，如果不配置high-availability 会话快速备份的命令将不能使能

hrp mirror session enable #会话快速备份使能命令，此命令使能之后防火墙上对新建的会话或者是刷新的会话立即备份到对端防火墙上，在配置high-availability 之后才能配置此命令。

hrp mirror packet enable #报文搬迁使能命令，此命令使能之后，如果ICMP的应答报文或者是TCP的ACK报文在其中一台防火墙上找不到会话，会把报文搬迁到另外一台防火墙上，如果在另外一台防火墙上找到会话，报文根据会话转发，如果找不到会话，直接丢弃。此功能现在保留，但是基本上不再使用，因为防火墙会话快速备份使能之后会话在建立或者是刷新的时候马上就能备份到对端防火墙上，并且报文搬迁占用比较多的带宽，所以这个命令推荐不使用

hrp auto-sync connection-status #防火墙连接状态备份命令。防火墙会话备份不分防火墙是主防火墙或者是备防火墙，使能了次命令后，防火墙都能把自己建立的会话或者是刷新的会话备份到对端防火墙上。此命令行在防火墙hrp enable 执行之后就默认使能了

hrp auto-sync config #防火墙配置备份命令。防火墙上使能此命令后，在主防火墙上配置的命令行如 ACL，域等都可以自动备份到备防火墙上，保证命令行能实时同步。此命令行在hrp enable之后就默认使能了，此时在备防火墙上是默认不能配置 ACL等配置的，但是如果需要单独配置，执行undo hrp auto-sync config就可以在备防火墙上配置此命令行了，主防火墙上执行ACL等配置发送到备防火墙上不会备执行，如果在主防火墙上执行此命令，主防火墙上将不把配置发送到备防火墙上执行

hrp auto-sync config batch-backup #防火墙配置批量备份使能命令。使能此命令，在防火墙发生主备倒换之后，新的主防火墙备自动把配置备份到新的备防火墙上。此命令默认是不使能的，现在也不推荐使用，因为批量备份将消耗大量的 CPU资源，可能在执行批量备份的时候影响某些业务

hrp sync config #防火墙配置批量备份命令。执行此命令后主防火墙能把自己的配置发送到备防火墙上执行，此命令行在用户视图下使用，在使能了hrp之后才能使用。此命令默认是也不推荐使用，因为批量备份将消耗大量的CPU资源，可能在执行批量备份的时候影响某些业务。

hrp sync connection-status #手工同步连接状态信息命令，会进行会话，黑名单，地址转换表，以及ARP表等的备份等，同时对于Eudemon 1000来说还会刷新备份的通道

**★硬件Bypass功能**

#FW提供Bypass接口对来实现硬件Bypass功能。当FW下电或者重启时，Bypass接口对将设备的上下游设备直接相连，使流量直接通过设备，而不做检测和拦截等任何处理，保证业务不中断；当故障排除后，所有流量恢复由设备处理后再发送，保证业务的安全性。

firewall feature-bypass bandwidth-policy enable level 2 priority 1

firewall feature-bypass ddos enable level 2 priority 2

**★其他（软件、文档、序列号查询）**

**★设备软件下载地址**

https://support.huawei.com/enterprise/zh/switches/cloudengine-s5735s-h24s4xc-a-pid-251695484/software?offeringId=6691579

**★设备序列号查询维保信息**

https://support.huawei.com/enterprise/ecareWechat



**★防火墙病毒库升级**

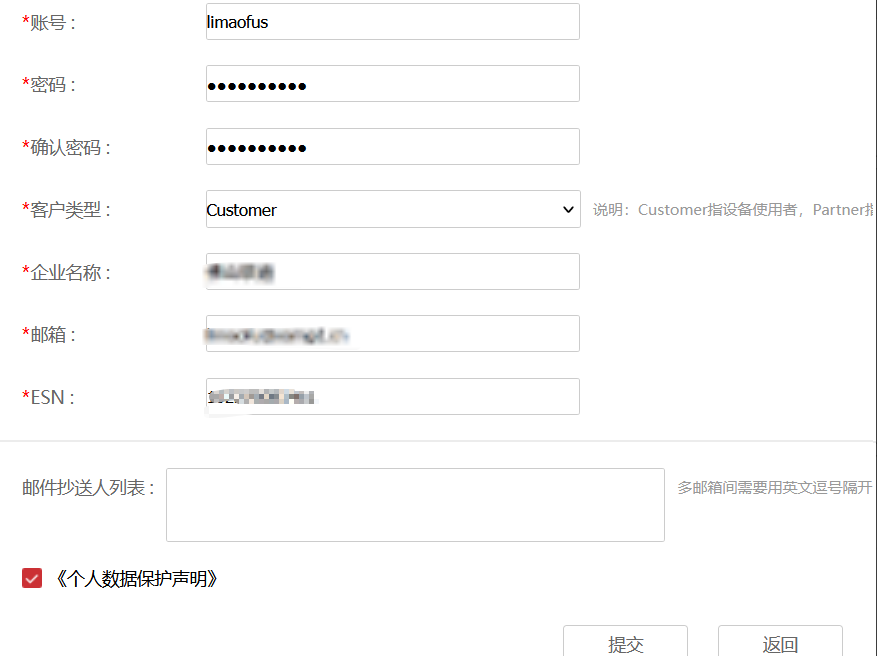
系统→升级中心，如果防火墙无法访问外网，可以点击本地升级，导入下载好的更新包

特征库更新包下载地址：

https://isecurity.huawei.com/sec/web/freesignature.do#



要先注册账号：



账号名 limaofus

密码 xxxxxxx





反病毒特征库： AV\_H30010004\_2023050600.zip 128,438KB

IPS引擎： IPS\_H20011000\_2023050407\_offline.zip 4,430KB

业务感知特征库： SA\_H30071000\_2023042800.zip 3,790KB

防火墙 系统→升级中心，点击本地升级





若防火墙建立HA，则主备2台都要各自升级

**★附录、hccn\_tool命令**

华为atlas设备的npu网卡默认在操作系统里无法显示，不可用ip addr或ifconfig命令操作，

得安装npu驱动后再使用hccn\_tool命令操作

参考地址： https://support.huawei.com/enterprise/zh/doc/EDOC1100257828/eead0d2f