### 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：2024-10-29

**★第0章、安装华为eNSP模拟器**

**★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

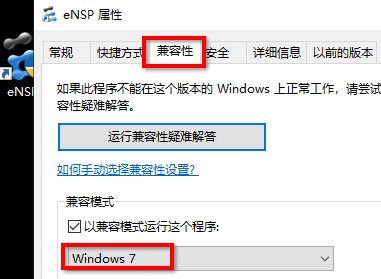
（https://download.virtualbox.org/virtualbox/5.2.44/VirtualBox-5.2.44-139111-Win.exe）

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)

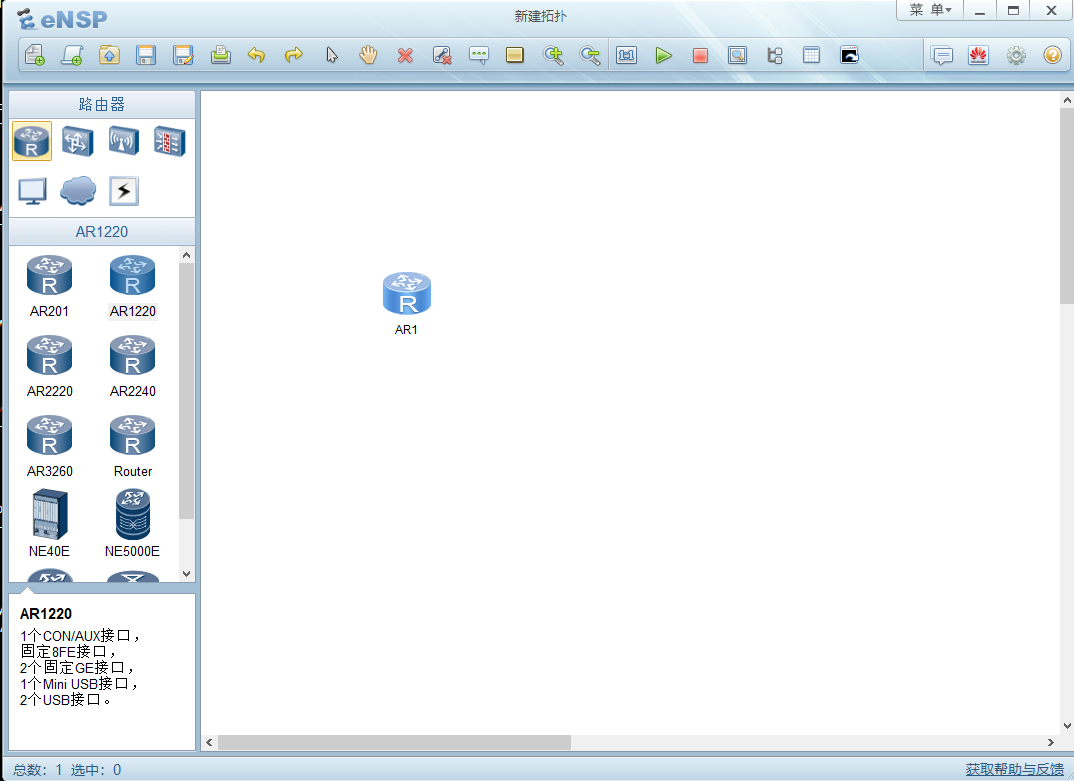
安装的过程就不多介绍了，双击安装，一路Next，装好eNSP模拟器后，找到它的图标：



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）

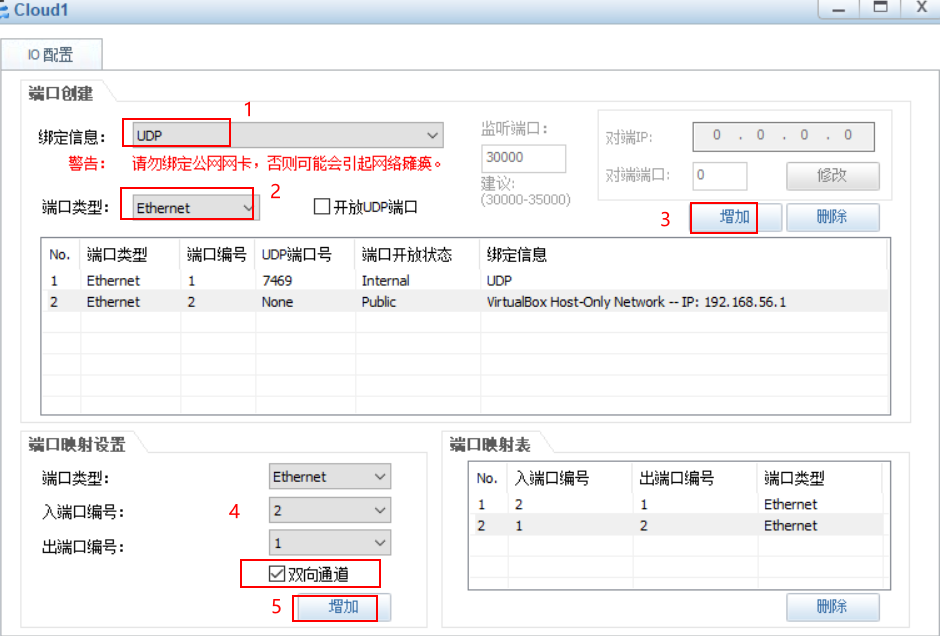
如果有实体硬件设备，那最好是用真实的设备去测试。注意：不要在生产环境中做测试！！

**★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）

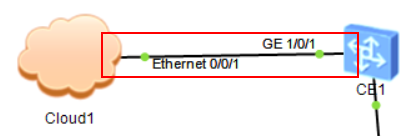


双击云，进行配置，创建2个端口，先创建UDP(Ethernet)，再创建一个ethernet（绑定端口为宿主机上的网卡（如VirtualBox Host-Only Network）



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

<HUAWEI> delete /unreserved s5735\_back\_config.cfg #永久删除文件，不放入回收站

Warning: The contents of file flash:/s5735\_back\_config.cfg cannot be recycled. Continue? [Y/N]:y

Info: Deleting file flash:/s5735\_back\_config.cfg...succeeded.

<HUAWEI> fixdisk flash: #修复文件系统

Fix disk flash: will take long time if needed.

% Fix disk flash: completed.

**★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 flash:/$\_install\_mod/S5735S-L\_V200R022C00SPC500\_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flash:/$\_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

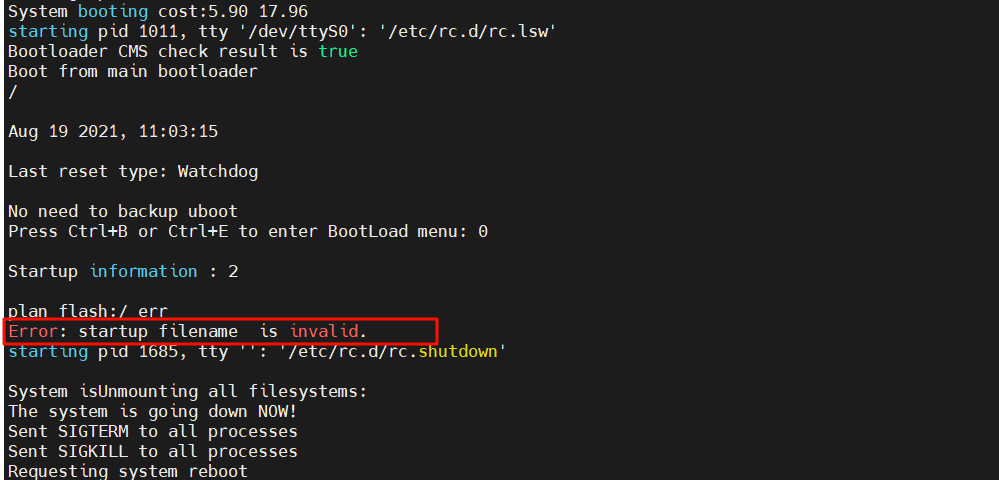
**★格式化flash**

<HUAWEI> format flash: #格式化flash（相当于格式化系统盘，里面的所有文件都会被清除，谨慎操作）

All data(include configuration and system startup file) on flash: will be lost , proceed with format ? [Y/N]:y

........................................................................................................................................................会一直输入...，可断电重启

格式化flash后，重启设备时会报错



提示startup filename无效，因为bootrom里记录了启动系统文件及配置文件，而flash已被格式化了，没有任何文件

可重启设备时按下Ctrl+B进入bootrom模式上传需要的文件

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): 2 #输入2，进入startup子菜单

Startup Configuration Submenu

**1. Display startup configuration**

2. Modify startup configuration

3. Return to main menu

Enter your choice(1-3): 1 #输入1查看bootrom里记录的重启配置文件名

Current startup configuration

startup type : Flash

startup file :

configuration file: back-yyy.cfg

patch package : s5735s-l-v200r021sph012.pat

Last time startup state : Success

Latest successful startup configuration #记录以下3个文件名，接下来需要下载以下文件

startup file : s5735-l-v200r021c00spc100.cc

configuration file: back-yyy.cfg

patch package : s5735s-l-v200r021sph012.pat

Startup Configuration Submenu

1. Display startup configuration

2. Modify startup configuration

**3. Return to main menu**

Enter your choice(1-3): 3 #输入3返回上一级菜单

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): 3 #输入3进入ethernet子菜单

ETHERNET SUBMENU

1. Download file to Flash through ethernet interface

**2. Modify ethernet interface boot parameter**

3. Return to main menu

Enter your choice(1-3): 2 #输入2设置要下载的文件名、下载时使用的协议参数

BOOTLINE SUBMENU

1. Set TFTP protocol parameters

**2. Set FTP protocol parameters**

3. Set SFTP protocol parameters

4. Return to ethernet menu

Enter your choice(1-4): 2 #输入2使用ftp协议下载指定的文件，以及设置ftp账号密码等参数

Warning: FTP is not a secure protocol. SFTP is recommended.

'.' = clear field; '-' = go to previous field; 'Ctrl+D' = quit

Load File name : s5735\_back\_config.cfg . #如果已有配置参数，输入.点号再回车，可消除此项配置

Switch IP address : 192.168.2.2 .

Server IP address : .192.168.2.1

FTP User Name : .cof

FTP User Password :

Starting to write BOOTLINE into flash ... done

BOOTLINE SUBMENU

1. Set TFTP protocol parameters

**2. Set FTP protocol parameters**

3. Set SFTP protocol parameters

4. Return to ethernet menu

Enter your choice(1-4): 2 #再重新输入2进行参数设置

Warning: FTP is not a secure protocol. SFTP is recommended.

'.' = clear field; '-' = go to previous field; 'Ctrl+D' = quit

Load File name : s5735-l-v200r021c00spc100.cc #先下载系统文件

Switch IP address : 192.168.2.2

Server IP address : 192.168.2.1

FTP User Name : cof

FTP User Password :

Starting to write BOOTLINE into flash ... done

BOOTLINE SUBMENU

1. Set TFTP protocol parameters

2. Set FTP protocol parameters

3. Set SFTP protocol parameters

4. Return to ethernet menu

Enter your choice(1-4): 4

ETHERNET SUBMENU

1. Download file to Flash through ethernet interface

2. Modify ethernet interface boot parameter

3. Return to main menu

Enter your choice(1-3): 1 #输入1开始下载文件

Use ftp to download file : s5735-l-v200r021c00spc100.cc , please wait for a moment.

...................

Download file successfully. #提示下载成功，再按此步骤下载其他配置文件，所有文件都下载完成后，可返回上一级菜单，重启设备

ETHERNET SUBMENU

1. Download file to Flash through ethernet interface

2. Modify ethernet interface boot parameter

3. Return to main menu

Enter your choice(1-3):3 #返回上一级菜单

BootLoad Menu

1. Boot with default mode

2. Enter startup submenu

3. Enter ethernet submenu

4. Enter filesystem submenu

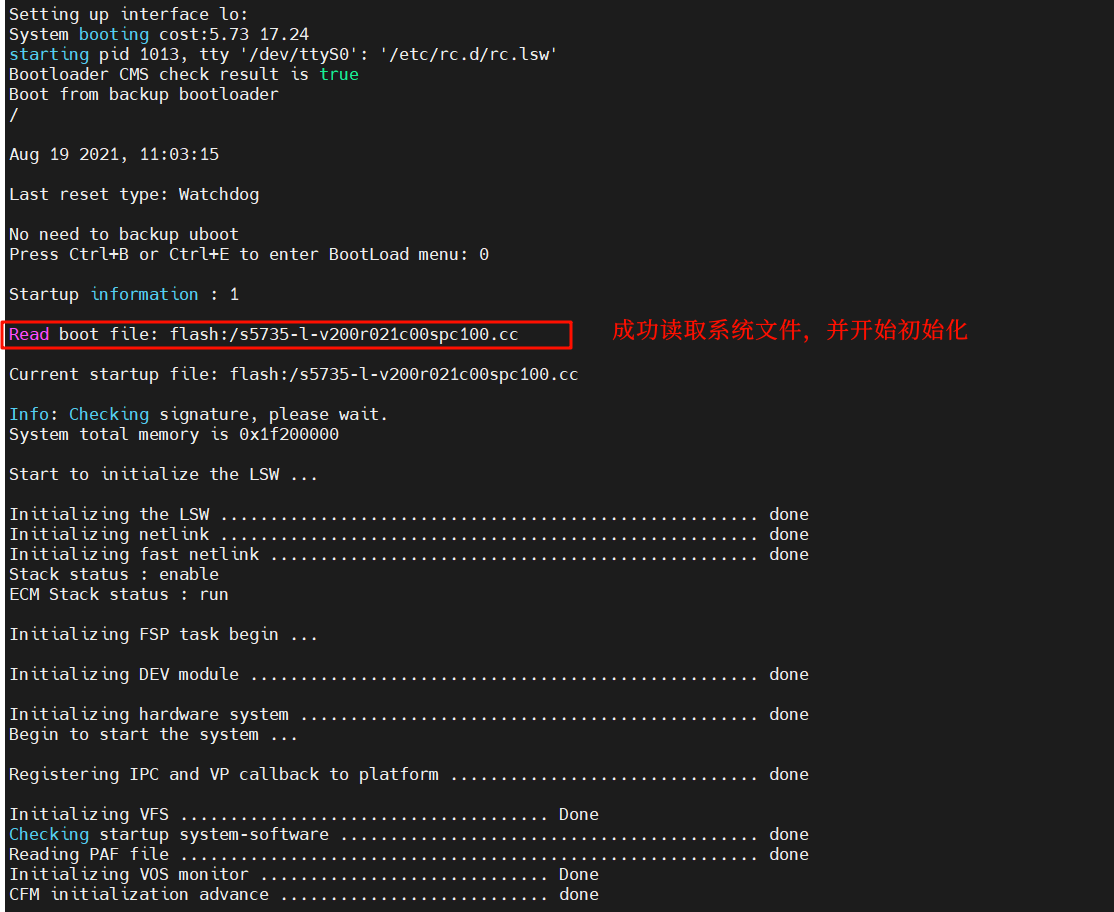
5. Enter password submenu

6. Clear password for console user

7. Reboot

(Press Ctrl+E to enter diag menu)

Enter your choice(1-7): 7 #重启设备



**★设置系统时间**

**①手动配置时间**

[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 #不使用ntp

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

**②使用ntp（客户端）**

[Huawei] undo ntp-service disable #使用ntp，开启ntp客户端

[Huawei] undo ntp-service ipv6 disable #使用ntp，开启ntp客户端

[Huawei] ntp-service source-interface Vlanif1 #指定同步ntp时使用的源接口

[Huawei] ntp-service unicast-server 10.99.4.1 #指定上级ntp-server地址

[HUAWEI] disp ntp-service status #查看ntp同步状态

clock status: synchronized

clock stratum: 15

reference clock ID: 10.99.4.1

nominal frequency: 100.0000 Hz

actual frequency: 100.0000 Hz

clock precision: 2^15

clock offset: 0.0000 ms

root delay: 21.98 ms

root dispersion: 4.24 ms

peer dispersion: 0.00 ms

reference time: 09:54:55.457 UTC Aug 11 2024(EA6308EF.7506CCA2)

synchronization state: clock set

[HUAWEI] disp clock #查看当前系统时间

2024-08-11 17:56:22+08:00

Sunday

Time Zone(cst) : UTC+08:00

**★配置为ntp服务端**

[HUAWEI] ntp-service refclock-master 5 #设置本ntp服务端的服务层次为5

[HUAWEI] undo ntp-service server disable #开启ntp服务端功能

[HUAWEI] undo ntp-service ipv6 server disable #开启ntp服务端功能（ipv6）

[HUAWEI] disp ntp-service status #查看ntp同步状态

clock status: synchronized

clock stratum: 5

reference clock ID: LOCAL(0)

nominal frequency: 100.0000 Hz

actual frequency: 100.0000 Hz

clock precision: 2^15

clock offset: 0.0000 ms

root delay: 0.00 ms

root dispersion: 12.57 ms

peer dispersion: 10.00 ms

reference time: 10:04:40.882 UTC Aug 11 2024(EA630B38.E1E29B6B)

synchronization state: clock set

**★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

**★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）

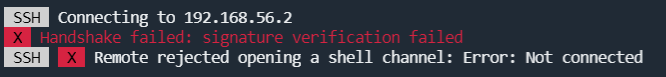
[Huawei] sftp server enable #开启sftp服务，可选

[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

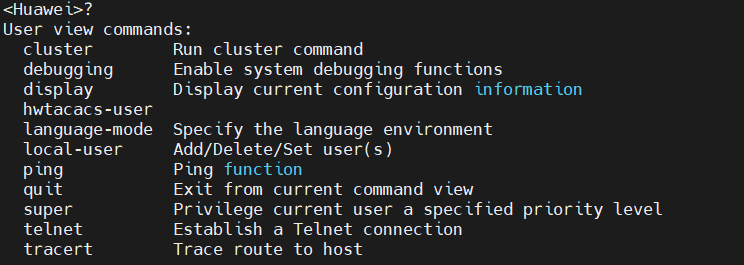
[Huawei] aaa

[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:

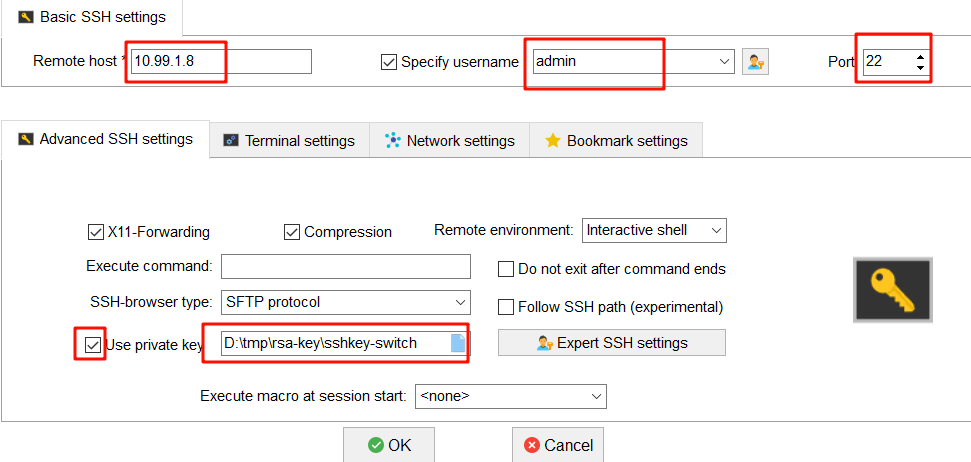
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQC7P2DkBJDrencWnMFe8CmeWaWo/uBzNKjt+nC+h0tr

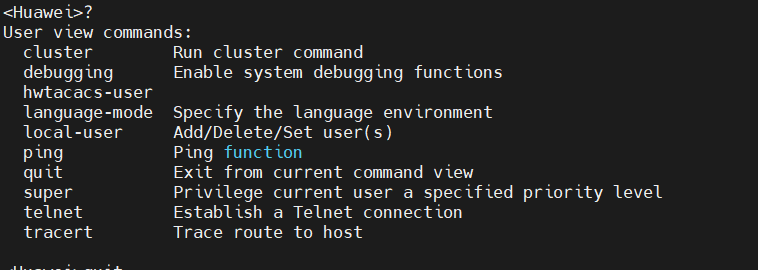
uMVOdiiZCLjmGMjQ2hzMsyoyq4hZBSIojaTsefMLKhmlEtSIRYpneOYoSMhjkg0L5kK39Ppaycm/DdM/

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

**★cpu-defend攻击防护**

[HUAWEI] acl number 4001

[HUAWEI-acl-L2-4001] rule 5 permit source-mac 0C11-2222-3333

[HUAWEI-acl-L2-4001] quit

[HUAWEI] cpu-defend policy cpu\_defend\_temp1 #创建攻击防护策略

[HUAWEI-cpu-defend-policy-cpu\_defend\_temp1] whitelist 1 acl 4001 #白名单（一律处理匹配的报文）

[HUAWEI-cpu-defend-policy-cpu\_defend\_temp1] blacklist 1 acl 4002 #黑名单（一律丢弃匹配的报文）

[HUAWEI-cpu-defend-policy-cpu\_defend\_temp1] auto-defend enable #开启攻击溯源检查功能（默认开启）

[HUAWEI-cpu-defend-policy-cpu\_defend\_temp1] auto-defend threshold 60 #阈值默认60

[HUAWEI-cpu-defend-policy-cpu\_defend\_temp1] car packet-type arp-request cir 128 cbs 131072

Warning: Improper parameter settings may affect stable operating of the system. Use this command under assistance of Huawei engineers. Continue? [Y/N]:y

[HUAWEI-cpu-defend-policy-cpu\_defend\_temp1] car packet-type dhcp-client cir 128 cbs 131072

Warning: Improper parameter settings may affect stable operating of the system. Use this command under assistance of Huawei engineers. Continue? [Y/N]:y

[HUAWEI-cpu-defend-policy-cpu\_defend\_temp1] car packet-type icmp cir 128 cbs 131072

Warning: Improper parameter settings may affect stable operating of the system. Use this command under assistance of Huawei engineers. Continue? [Y/N]:y

# Cir单位是Kbps Cbs单位是Byte

[HUAWEI-cpu-defend-policy-cpu\_defend\_temp1] quit

[HUAWEI] cpu-defend-policy cpu\_defend\_temp1 global #应用攻击防护策略

[HUAWEI] disp cpu-defend policy cpu\_defend\_temp1

Related slot : <0>

Configuration :

Whitelist 1 ACL number : 4001

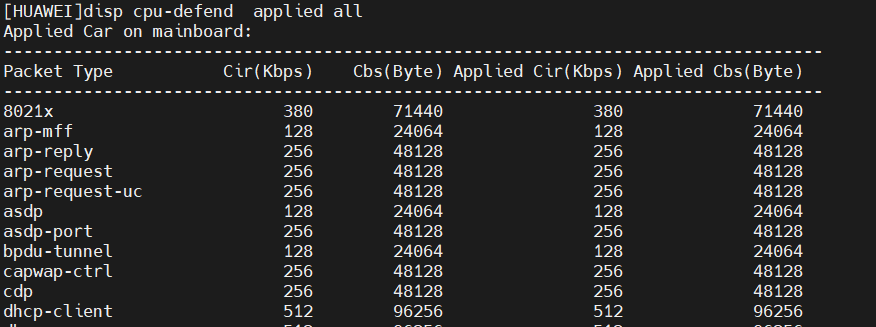
Blacklist 1 ACL number : 4002

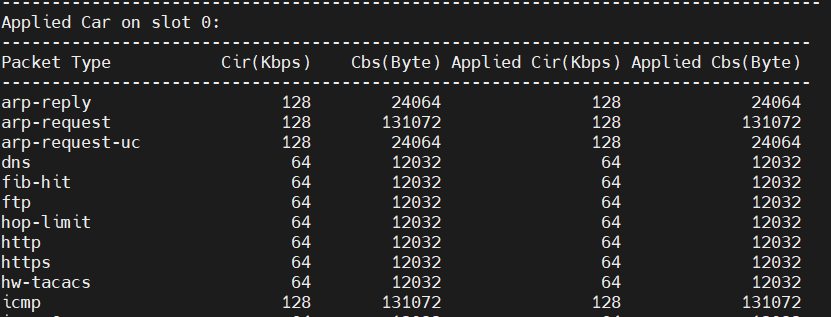
Car packet-type arp-request : CIR(128) CBS(131072)

Car packet-type dhcp-client : CIR(128) CBS(131072)

Car packet-type icmp : CIR(128) CBS(131072)

[HUAWEI] disp cpu-defend applied all #查看生效的防护情况





[HUAWEI] disp auto-defend configuration #查看攻击溯源配置信息

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

Name : cpu\_defend\_temp1

Related slot : <0>

auto-defend : enable

auto-defend attack-packet sample : 5

auto-defend threshold : 60 (pps)

auto-defend trace-type : source-mac source-ip

auto-defend protocol : arp icmp dhcp igmp tcp telnet 8021x nd dhcpv6 mld icmpv6

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

**★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配置管理协议，NETCONF使用YANG作为它的数据建模语言（类似于SNMP使用MIB一样）。用户可以通过NETCONF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。有了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”

#!/usr/bin/env python  
# -\*- coding: utf-8 -\*-  
  
import traceback  
import httplib  
  
  
# Python 2.x中的"httplib"模块在Python 3.x中变成了"http.client"，目前交换机内置python 2.x  
# import http.client  
  
  
class OPSConnection(object):  
 *"""Make an OPS connection instance."""* def \_\_init\_\_(self, host, port=80):  
 *"""初始化类，创建一个HTTP连接"""* self.host = host  
 self.port = port  
 self.headers = {  
 "Content-type": "text/xml",  
 "Accept": "text/xml"  
 }  
 self.conn = None  
  
 def close(self):  
 *"""关闭HTTP连接"""* self.conn.close()  
  
 def create(self, uri, req\_data):  
 *"""创建设备资源操作"""* ret = self.rest\_call("POST", uri, req\_data)  
 return ret  
  
 def get(self, uri, req\_data=None):  
 *"""查询设备资源操作"""* ret = self.rest\_call("GET", uri, req\_data)  
 return ret  
  
 def delete(self, uri, req\_data):  
 *"""删除设备资源操作"""* ret = self.rest\_call("DELETE", uri, req\_data)  
 return ret  
  
 def set(self, uri, req\_data):  
 *"""修改设备资源操作"""* ret = self.rest\_call("PUT", uri, req\_data)  
 return ret  
  
 def rest\_call(self, method, uri, req\_data):  
 *""" REST call"""* print('| - - - - - - - - - - - - - - - request: - - - - - - - - - - - - - - -|')  
 print('%s %s HTTP/1.1\n' % (method, uri))  
 if req\_data == None:  
 body = ""  
 else:  
 body = req\_data  
 print(body)  
 if self.conn:  
 self.conn.close()  
 self.conn = httplib.HTTPConnection(self.host, self.port)  
 # self.conn = http.client.HTTPConnection(self.host, self.port)  
 self.conn.request(method, uri, body, self.headers)  
 response = self.conn.getresponse()  
 response.status = httplib.OK # stub code  
 # response.status = http.client.OK #stub code  
 ret = (response.status, response.reason, response.read())  
 print('| - - - - - - - - - - - - - - - response: - - - - - - - - - - - - - - -|')  
 print('HTTP/1.1 %s %s\n\n%s' % ret)  
 print('| - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -|')  
 return ret  
  
  
def get\_startup\_info(ops\_conn):  
 # 指定系统启动信息的URI。URI为Restful API中定义的管理对象，不同的管理对象有不同的URI  
 uri = "/cfg/startupInfos/startupInfo"  
 # 指定发送的请求内容。该部分内容与URI相对应，不同的URI对应不同的请求内容  
 req\_data = """  
 <?xml version="1.0" encoding="UTF-8"?>  
 <startupInfo>  
 </startupInfo>  
 """  
 ret, \_, rsp\_data = ops\_conn.get(uri, req\_data)  
 if ret != httplib.OK:  
 return None  
 return rsp\_data  
  
  
def clear\_startup\_info(ops\_conn):  
 uri = "/cfg/clearStartup"  
 req\_data = """  
 <?xml version="1.0" encoding="UTF-8"?>  
 <clearStartup>  
 </clearStartup>  
 """  
 ret, \_, rsp\_data = ops\_conn.create(uri, req\_data)  
 if ret != httplib.OK:  
 return None  
 else:  
 return ret  
  
  
def main():  
 # host表示环路地址，当前RESTful API为设备内部调用，即取值为"localhost"。  
 host = "localhost"  
 try:  
 ops\_conn = OPSConnection(host) # 建立HTTP连接  
 rsp\_data1 = get\_startup\_info(ops\_conn) # 调用获取系统启动信息的函数  
 # rsp\_data2 = clear\_startup\_info(ops\_conn) # 清空系统启动配置信息  
 rsp\_data3 = get\_startup\_info(ops\_conn)  
 ops\_conn.close() # 关闭HTTP连接  
 except:  
 errinfo = traceback.format\_exc()  
 print(errinfo)  
 return  
  
  
if \_\_name\_\_ == "\_\_main\_\_":  
 main()

**★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（ipv4）

\*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>

<Huawei> disp ipv6 int brief #查看接口的up/down状态及接口上的ip（ipv6）

\*down: administratively down

!down: FIB overload down

(l): loopback

(s): spoofing

Interface Physical Protocol VPN

Vlanif1 up up --

[IPv6 Address] FD00:1234::FF02

Vlanif2 up up --

[IPv6 Address] FD88:1299::FF02

<HUAWEI> ping ipv6 FD00:1234::FF01 #ping ipv6

PING FD00:1234::FF01 : 56 data bytes, press CTRL\_C to break

Reply from FD00:1234::FF01

bytes=56 Sequence=1 hop limit=64 time=29 ms

<HUAWEI> ping ipv6 FE80::727B:E8FF:FE64:7CDF -i vlanif 1 #ping ipv6链路本地地址时需要指定三层接口

PING FE80::727B:E8FF:FE64:7CDF : 56 data bytes, press CTRL\_C to break

Reply from FE80::727B:E8FF:FE64:7CDF

bytes=56 Sequence=1 hop limit=64 time=17 ms

**★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Port-Mirroring**

[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(镜像口) 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

#

**★匹配具体流量并镜像到观察口（流镜像）：**

[Huawei] observe-port interface GigabitEthernet 0/0/2 #观察口，被镜像的数据流向此端口

[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] quit

[Huawei] traffic classifier class3 #定义流类

[Huawei-classifier-class3] if-match acl 2000 #匹配acl，该acl匹配目标流量

[Huawei-classifier-class3] quit

[Huawei] traffic behavior behav3 #定义流行为

[Huawei-behavior-behav3] mirror to observe-port #镜像到观察口

[Huawei-behavior-behav3] quit

[Huawei] traffic policy policy3 #定义流策略

[Huawei-trafficpolicy-policy3] classifier class3 behavior behav3 #匹配相应的类和行为

[Huawei-trafficpolicy-policy3] quit

[Huawei] int g0/0/1

[Huawei-GigabitEthernet0/0/1] traffic-policy policy3 inbound #在接口上应用策略

[Huawei-GigabitEthernet0/0/1] quit

**★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

**★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

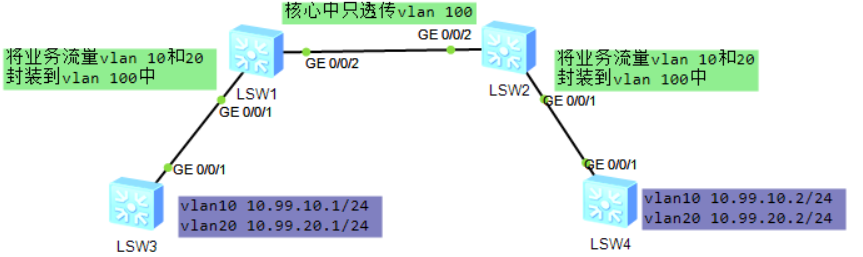
**★QinQ（vlan透传）**

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：

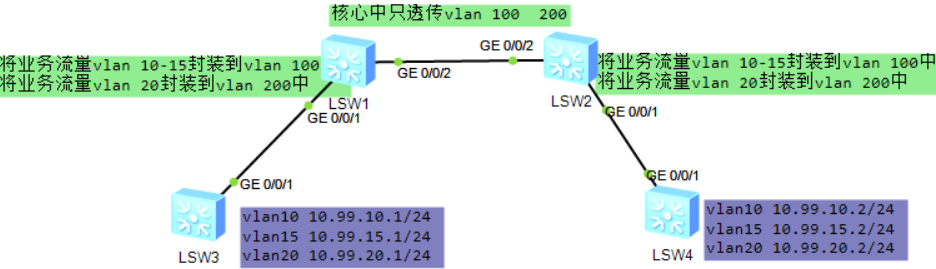
[Huawei] int g0/0/1

[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）**

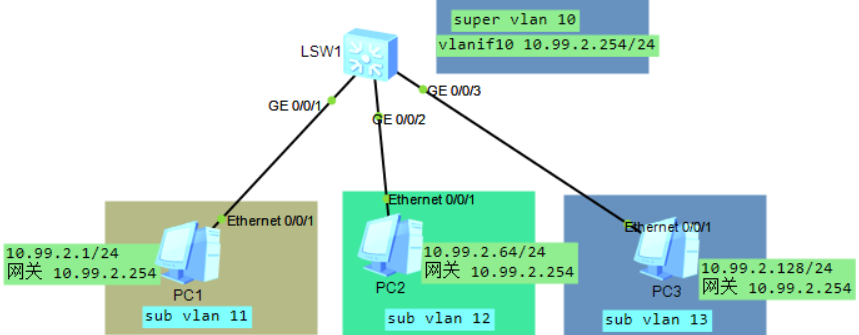
super vlan也叫VLAN Aggregation（vlan聚合）

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，不再建议使用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（华为设备**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（优先级为0）

[Huawei] stp root secondary #其他再选一台指定为备份根桥（优先级为4096）

[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，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，必须为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。

[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 #进入接口配置界面

[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(Half) 18(Full) | 200 000 |
| 1000M | 1 | 4 | 20 000 |
| 10G | 1 | 2 | 2 000 |
| 40G | 1 | 1 | 500 |
| 100G | 1 | 1 | 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（快速生成树协议）**

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（多生成树协议）**

[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 #指定端口上开启根保护

[Huawei-GigabitEthernet0/0/4] quit

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

**★VBST（基于vlan的生成树协议）**

VBST（VLAN-Based Spanning Tree）是华为私有协议，基于vlan的生成树协议，可在每个vlan上运行STP或RSTP

VBST协议中BID（Bridge-ID）长8字节，由桥优先级（Bridge Priority）、VLAN ID与桥MAC地址构成。

桥优先级数值+VLAN ID占据前面16位，后面的48位是MAC地址。

\*桥ID == （优先级 + VLAN ID） 及 MAC地址 #越小越优先

在VBST网络中，桥ID最小的设备会被选举为根桥。

VBST通过在VLAN内传递VBST报文来确定网络拓扑结构。VBST报文基于STP/RSTP报文，但相对STP/RSTP报文，VBST报文在源MAC地址字段和协议长度字段之间加入了四字节的802.1q Tag

VBST报文目的mac地址为0100-0CCC-CCCD

VBST报文中的Data字段依据对接设备填充标准RSTP/STP报文的Data内容，默认填充标准RSTP报文

**VBST与标准协议STP/RSTP互通**

|  |  |
| --- | --- |
| Trunk口 | VBST设备和RSTP设备对接时，在VLAN1内，VBST设备使用标准的RSTP报文与对端交互，其他VLAN内使用填充RSTP Data的VBST报文与对端交互  VBST设备和STP设备对接时，在VLAN1内，VBST设备使用标准的STP报文与对端交互，其他VLAN内使用填充STP Data的VBST报文与对端交互 |
| Access口 | VBST设备将只根据此端口所在的VLAN使用标准的STP报文（对接STP设备）或RSTP报文（对接RSTP设备）与对端交互。这样，拓扑计算将按照STP/RSTP协议进行，STP/RSTP协议不区分VLAN，所以最终形成一棵各VLAN共享的生成树 |

**VBST与思科PVST协议互通**

|  |  |
| --- | --- |
| Trunk口 | VBST设备和Rapid PVST+设备对接时，在VLAN1中，VBST设备使用标准的RSTP报文与对端交互（也会同时发填充RSTP Data的VBST报文），其他VLAN内使用RSTP Data填充的VBST报文与对端交互。  VBST设备和PVST+设备对接时，在VLAN1中，VBST设备使用标准的STP报文与对端交互（也会同时发填充STP Data的VBST报文），其他VLAN内使用STP Data填充的VBST报文与对端交互。  VBST设备和PVST设备对接时，报文交互跟VBST与PVST+对接类似。区别在于，在VLAN1中，VBST设备和PVST设备之间只发送填充STP Data的VBST报文交互。 |
| Access口 | VBST设备将只根据此端口所在VLAN使用标准的STP（对接PVST/PVST+设备）或RSTP（对接Rapid PVST+设备）报文与对端交互。这样，拓扑计算将按照STP/RSTP协议进行，由于STP/RSTP协议不区分VLAN，所以最终形成一棵各VLAN共享的生成树 |

[Huawei] stp enable

[Huawei] stp mode vbst

[Huawei] stp vlan 10 root primary #将设备设置为vlan 10的根桥

[Huawei] stp vlan 20 root secondary #将设备设置为vlan 20的备份根桥

[Huawei] stp vlan 30 priority 61440 #指定设备在vlan 30的桥优先级

[Huawei] int g0/0/4

[HUAWEI-GigabitEthernet0/0/4] stp vlan 10 port priority 16 #配置端口在指定vlan中的优先级

[HUAWEI-GigabitEthernet0/0/4] stp vlan 10 cost 20000 #配置端口在指定vlan中的端口开销

[HUAWEI-GigabitEthernet0/0/4] stp vlan 20 cost 40000

[HUAWEI] disp stp vlan 10 brief #查看vlan 10情况

VLAN-ID Port Role STP State Protection

10 GigabitEthernet0/0/5 DESI FORWARDING NONE

[HUAWEI] disp stp vlan 20 #查看vlan 20情况

-------[VLAN 20 Global Info][Mode VBST]-------

Bridge ID :4116 .60d7-5574-fd76 # 桥ID中的4116==优先级4096 + VLAN 20

Bridge Diameter :7

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

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

Root ID / RPC :4116 .60d7-5574-fd76 / 0 (This bridge is the root)

RootPortId :0.0

Root Type :Secondary

[HUAWEI] int g0/0/22

[HUAWEI-GigabitEthernet0/0/22] stp edged-port enable #配置为边缘端口

[HUAWEI-GigabitEthernet0/0/22] stp bpdu-filter enable #过滤bpdu报文

#某端口配置为边缘端口后，默认仍然会发送BPDU报文，这可能导致BPDU报文发送到其他网络，引起其他网络产生震荡。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

**★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]

**★IPv6-ND**

<HUAWEI> disp ipv6 neighbors brief #查看ipv6邻居

D-Dynamic,S-Static,R-Remote

I-INCMP,R-REACH,S-STALE,D-DELAY,P-PROBE

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

IPv6 Address Link-layer State Type Interface

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

FD00:1234::12 707b-e8bb-13b4 R D GE1/0/1

FD00:1234::FF01 707b-e864-7cdf S D GE1/0/1

FD00:1234::FFFF 0000-5e00-0201 S D GE1/0/1

FE80::727B:E8FF:FE64:7CDF 707b-e864-7cdf R D GE1/0/1

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

Total: 4 Dynamic: 4 Static: 0 Remote: 0

<HUAWEI> reset ipv6 neighbors Vlanif 1 #清除ipv6邻居信息

**★第7章、DHCP配置**

**★DHCP服务配置**

[Huawei] dhcp enable #开启dhcp服务

[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

[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] bootfile undionly.kpxe #使用此引导文件

[Huawei-ip-pool-vlan1] next-server 10.99.1.2 #引导文件从这个地址获取

[Huawei-ip-pool-vlan1] option 43 hex HHHHHHHH #下发option 43配置，还可为其他option，以及使用ascii或hex格式配置数据

[Huawei-ip-pool-vlan1] quit

**#配置ip地址冲突探测**

[Huawei] dhcp server ping packet 2 #下发ip配置之前先对要下发的地址进行ping检测是否已存在

[Huawei] dhcp server ping timeout 2000 #ping检测超时，默认500毫秒

**#配置DHCP报文限速**

[Huawei] int vlanif 1

[Huawei-Vlanif1] dhcp check dhcp-rate enable #开启dhcp报文限速功能

[Huawei-Vlanif1] dhcp check dhcp-rate 50 #将dhcp报文限制为50pps，默认是100pps

[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

**★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请求报文交给指定的dhcp服务器处理（单播转发））

[Huawei-GE0/0/1.100] arp broadcast enable #在子接口上配置dhcp中继时需开启此功能，终结子接口的ARP广播功能

**★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

[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 #接终端设备的端口上开启dhcp snooping

[Huawei-GigabitEthernet0/0/3] dhcp snooping sticky-mac #根据DHCP Snooping绑定表生成静态MAC表项

[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访问控制及流量控制**

**★ACL访问控制列表**

**①ACL编号及基础应用（traffic-filter）**

|  |  |  |
| --- | --- | --- |
| 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，起到流量过滤的作用

[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

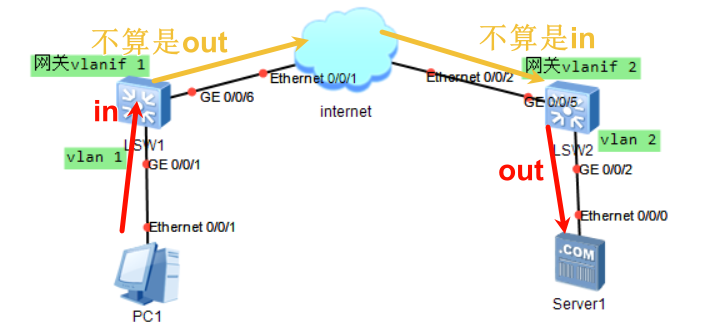
daily Every day of the week

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。

**★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

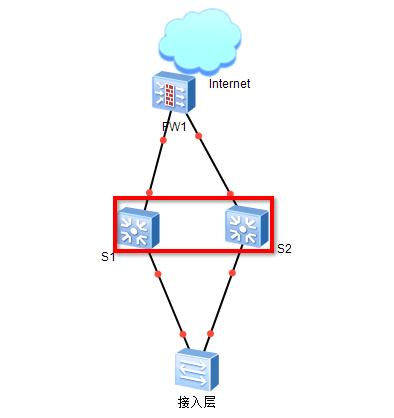
**★第9章、设备高可用配置**

**★VRRP（虚拟路由冗余协议）**

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 vlanif 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

**★VRRPv3**

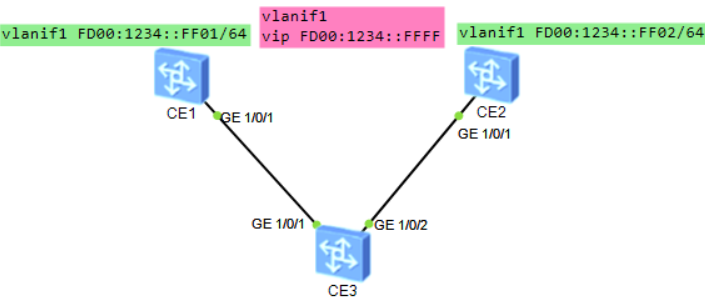
ipv4的VRRP版本为v2，VRRPv3支持ipv4及ipv6

advertisment报文源地址使用链路本地地址FE80::xxxx

advertisment报文目的地址使用组播地址FF02::12，vrrp报文封装在IPv6中，Next Header为112

ipv6虚拟ip对应的mac地址为0000-5E00-02-vrid

**★实验：VRRPv3-ipv6\_ce12800**



**CE1配置：**

interface Vlanif1

ipv6 enable

ipv6 address FD00:1234::FF01/64

vrrp6 vrid 1 virtual-ip FE80::1 link-local #vrrp6中第1个vip必须是链路本地地址

vrrp6 vrid 1 virtual-ip FD00:1234::FFFF #唯一本地地址的vip

vrrp6 vrid 1 priority 120 #默认优先级为100，越大越优先

vrrp6 vrid 1 preempt disable

#

**CE2配置：**

interface Vlanif1

ipv6 enable

ipv6 address FD00:1234::FF02/64

vrrp6 vrid 1 virtual-ip FE80::1 link-local

vrrp6 vrid 1 virtual-ip FD00:1234::FFFF

vrrp6 vrid 1 preempt disable

#

**CE1查看：**

<HUAWEI> disp vrrp6 1 verbose #查看vrrp6的vrid 1的详情

Vlanif1 | Virtual Router 1

State : Master

Virtual IP : FE80::1

FD00:1234::FFFF

Master IP : FE80::727B:E8FF:FE64:7CDF #VRRP宣告报文中使用此ip为源地址

PriorityRun : 120

PriorityConfig : 120

MasterPriority : 120

Preempt : NO

Hold Multiplier : 3

TimerRun : 100cs

TimerConfig : 100cs

Virtual MAC : 0000-5e00-0201

Check Hop Limit : YES

Config Type : Normal

Create Time : 2024-08-10 22:05:53

Last Change Time : 2024-08-10 22:06:15

**CE2查看：**

<HUAWEI> disp ipv6 neighbors brief

D-Dynamic,S-Static,R-Remote

I-INCMP,R-REACH,S-STALE,D-DELAY,P-PROBE

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

IPv6 Address Link-layer State Type Interface

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

FD00:1234::FF01 707b-e864-7cdf R D GE1/0/1

FD00:1234::FFFF 0000-5e00-0201 R D GE1/0/1

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

Total: 2 Dynamic: 2 Static: 0 Remote: 0

**★iStack堆叠（设备虚拟化）**

本章节以S5735型号交换机为例

不同型号交换机具体的配置命令不太一样，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 g0/0/13 to g0/0/14 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，即从第1个口开始按顺序每4个口为一组），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 #输入y确认

[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 #输入y确认

[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 #输入y确认

[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: --

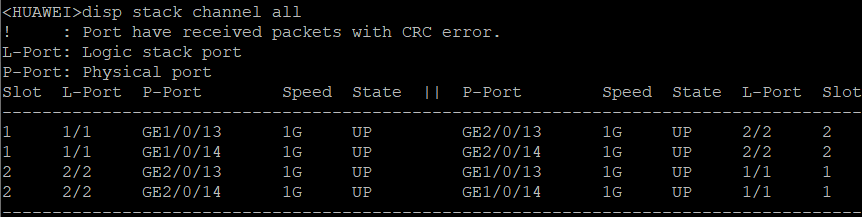
Slot Role MAC Address Priority Device Type

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

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

[HUAWEI] stack timer mac-address switch-delay 10 #设置堆叠系统mac地址切换时间，默认10分钟，配置为0表示不切换mac地址

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

**★直连接口多主检测**

由于MAD报文是BPDU报文，如果直连检测链路上存在中间设备，则中间设备上需要配置转发BPDU报文

接口配置直连方法多主检测功能后，STP端口状态会变成Discarding，会影响数据报文的转发和某些协议报文的上送，所以不要在此接口上再配置其他业务

直连检测方式只能配置于二层以太物理端口上，且端口必须为UP状态

[HUAWEI] int Eth-Trunk 1

[HUAWEI-Eth-Trunk1] mad detect mode direct

**★代理多主检测**

堆叠成员设备都连到一台代理交换机上

堆叠成员交换机侧配置：

[HUAWEI] int Eth-Trunk 1

[HUAWEI-Eth-Trunk1] mad detect mode relay

代理交换机侧配置：

[HUAWEI] int Eth-Trunk 1

[HUAWEI-Eth-Trunk1] mad relay

多主检测发现堆叠分裂，分裂后的多个堆叠系统之间会进行相互竞争，为防止相同的MAC地址、IP地址引起网络振荡，竞争失败的堆叠系统内成员交换机的所有业务端口会被关闭，以减少对网络的影响。

堆叠分裂后，MAD冲突处理机制使用MAD报文进行MAD竞争，竞争结果为堆叠系统处于Detect状态或者Recovery状态：

Detect：竞争成功，堆叠系统将处于正常工作状态

Recovery：竞争失败，堆叠系统将状态处于禁用状态，关闭除手动配置的保留端口以外的其它所有物理端口

如果有部分端口仅做报文透传功能，出现堆叠分裂后，这部分端口不会影响网络运行。用户如果希望保留这些端口的业务，可以通过命令将这些端口配置为保留端口。堆叠分裂后，多主检测功能不会关闭保留端口的业务。

缺省情况下，堆叠物理成员端口为保留端口，其它所有业务口均为非保留端口。

堆叠分裂后，用于双主检测的端口也会被关闭

[HUAWEI] mad exclude interface g0/0/8 to g0/0/9 #配置为保留端口

[HUAWEI] mad exclude interface g0/0/12 #可配置多条

[HUAWEI] disp mad verbose #查看mad双主检测情况

Current MAD domain: 0

Current MAD status: Detect

Mad direct detect interfaces configured:

Mad relay detect interfaces configured:

Excluded ports(configurable):

GigabitEthernet0/0/8

GigabitEthernet0/0/9

GigabitEthernet0/0/12

Excluded ports(can not be configured):

**★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....

**★M-LAG跨设备端口聚合**

M-LAG（Multichassis Link Aggregation Group）即跨设备链路聚合组，是一种横向虚拟化技术，将双归接入的两台设备在逻辑上虚拟成一台设备。M-LAG本身提供了一个没有环路的二层拓扑同时实现冗余备份，极大的简化了组网及配置。

V-STP（Virtual Spanning Tree Protocol）是二层拓扑管理特性，其核心思想是将两台设备的STP协议虚拟成一台设备的STP协议，对外呈现为一台设备进行STP协议计算，v-stp仅支持stp或rstp模式

stp mode rstp

stp v-stp enable

stp bridge-address 0000-0000-0001

stp bpdu-protection

stp tc-protection

#

ip vpn-instance vpn\_DAD

ipv4-family

route-distinguisher 99:10

vpn-target 99:10 export-extcommunity

vpn-target 99:10 import-extcommunity

#

interface Eth-Trunk0 #DAD口配置（Dual Active Detection双主检测）

description M-LAG\_DAD-port

undo portswitch

ip binding vpn-instance vpn\_DAD

ip address 10.99.9.1 255.255.255.252

mode lacp-static

m-lag unpaired-port reserved #在peer-link故障但双主检测正常时不被Error-Down，主备设备上相同的接口都要配置；该命令不支持在peer-link接口、M-LAG成员口下配置

trunkport GE1/0/1

trunkport GE1/0/2

#

dfs-group 1

priority 150 #默认优先级为100，需要将主备设备的优先级设置为不同的值

source ip vpn-instance vpn\_DAD 10.99.9.1 peer 10.99.9.2

dual-active detection enhanced enable

#dual-active detection source ip 10.99.9.1 vpn-instance vpn\_DAD peer 10.99.9.2 #上面2行合为一行

vbdif mac-address advertise disable

authentication-mode hmac-sha256 password xxxxx #指定dfs-group同步报文所使用的验证模式及口令

m-lag up-delay 240 auto-recovery interval 0 #设置延迟up时间为240秒，延迟自动恢复时间为0秒，默认up-delay为240秒，auto-recovery interval为0秒

#

interface Eth-Trunk1 #peer-link口配置

stp enable #peer-link口在v-stp模式下要开启stp，根桥模式下要关闭stp

mode lacp-static #为了提高M-LAG的可靠性，必须配置为静态LACP模式

peer-link 1 #配置为peer-link接口

port vlan exclude 10 to 20 #配置peer-link口不允许通过的vlan，peer-link口为二层口，默认允许所有vlan通过。如果有配置vlanif三层口ip做双主检测，建议将此vlan从peer-link排除出去，防止心跳检测失效

trunkport GE1/0/3

trunkport GE1/0/4

#

**#业务口配置（接服务器）**

#

interface Eth-Trunk2

mode lacp-static

port link-type access

port default vlan 10

dfs-group 1 m-lag 2 #m-lag后面的数字，在主备2台设备上的相同聚合口上要保持一致

trunkport GE1/0/7

trunkport GE1/0/8

#

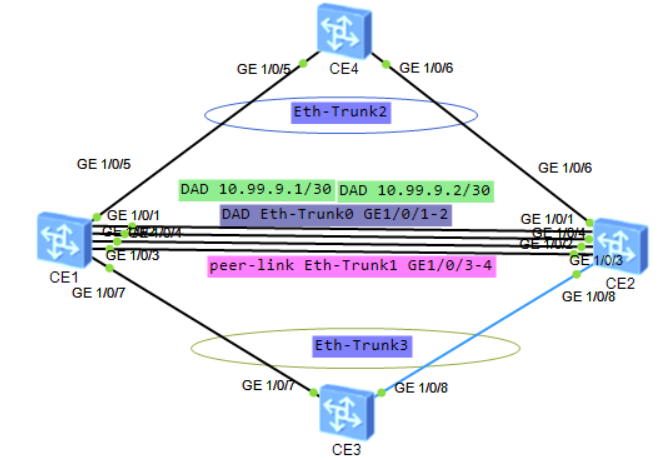
#查看

display dfs-group 1 m-lag #查看DFS Group编号为1的M-LAG信息

display dfs-group 1 node 1 m-lag brief #查看node1的m-lag信息

★如果配置了m-lag，且在主备2台设备上配置了vrrp，则主备2边的vrrp状态都是Master（主），这是正常的

**★实验：M-LAG\_ce12800（模拟器中ce6800/12800不支持m-lag）**



**★第10章、路由配置**

**★vpn实例（VRF虚拟路由转发表）**

vpn-instance <==> Virtual Routing Forwarding

将一台路由器划分为几个不同的虚拟路由器使用，将不同的接口加入到不同的vpn-instance中，各vpn-instance分别维护一张RIB路由表和FIB转发表

[Huawei] ip vpn-instance vpn\_22 #创建vpn实例，名为vpn\_22

[Huawei-vpn-instance-vpn\_22] description vpn\_22\_manager

[Huawei-vpn-instance-vpn\_22] ipv4-family

[Huawei-vpn-instance-vpn\_22-af-ipv4] route-distinguisher 22:10 # RD

[Huawei-vpn-instance-vpn\_22-af-ipv4] vpn-target 22:10 export-extcommunity # eRT

[Huawei-vpn-instance-vpn\_22-af-ipv4] vpn-target 22:10 import-extcommunity # iRT

[Huawei] int GigabitEthernet0/0/0 #进入三层接口

[Huawei-GigabitEthernet0/0/0] ip binding vpn-instance vpn\_22 #绑定vpn实例，所有ip相关配置都会清空

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

[Huawei-GigabitEthernet0/0/0] quit

[Huawei] int Vlanif 22 #进入vlanif接口

[Huawei-Vlanif22] ip binding vpn-instance vpn\_22 #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 vpn\_22 #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 #配置静态路由并指定优先级

#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 #静态路由与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

静态路由和RIP默认不考虑链路带宽的差异。如果去往某网段的静态路由条目有多条，则默认是开启ECMP等价路由，各链路均匀分担流量负载，当各链路带宽不同时，需要使用UCMP非等成本负载分担，在出接口上都开启UCMP功能，且shutdown/undo shutdown重启接口重新下发FIB表项后才生效，配置如下：

int g1/0/1 #其他出接口都需要进行如下配置

load-balance unequal-cost enable

shutdown

undo shutdown

#

**★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 是内部网关协议的一种，基于距离向量的路由选择协议。RIP中从一个路由器到非直连网络的距离定义为：所经过的路由器数加1

RIP协议的距离也称为跳数（hop count），一条路径最多只允许跳数为15，16则认为不可达

★若设备配置了水平分割或毒性逆转，有类聚合将失效，华为设备默认开启水平分割，所以rip v2的路由器默认不会自动聚合

[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] verify-source #开启rip更新报文源地址检查

[Huawei-rip-1] preference 50 #设置路由优先级

[Huawei-rip-1] network 10.0.0.0 #宣告网段，即使是v2版本，宣告路由时只可配置为主类地址

[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 cipher xxx 1 #设置rip接口验证

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

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

[Huawei-GigabitEthernet0/0/1] rip authentication-mode hmac-sha256 cipher xxx 1 #设置rip接口验证

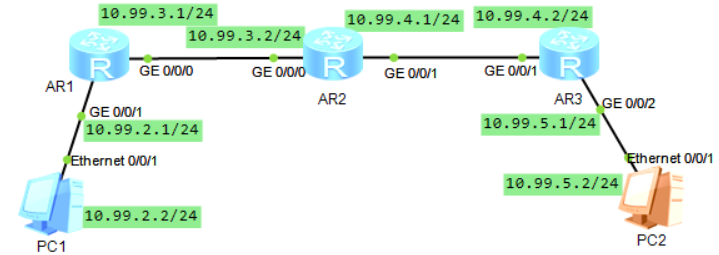
★MD5验证时，nonstandard表示使用基于IETF国际标准的MD5加密方式

usual表示使用基于华为私有的MD5加密方式

**★RIP防环机制**

|  |  |
| --- | --- |
| 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 |
| 最大计数器 | RIP的距离跳数最大有效值15，达到16则表示路由不可达 |
| 触发更新 | 路由表中的某条路由发生变化时，路由器会立刻发送更新报文，不等RIP定时器超时 |

**★实验：rip\_v2\_ar2240（RIPv2基础配置）**



**AR1配置：**

interface GigabitEthernet0/0/0

ip address 10.99.3.1 255.255.255.0

rip authentication-mode hmac-sha256 hmac-sha256 cipher passwdxx 1

#

interface GigabitEthernet0/0/1

ip address 10.99.2.1 255.255.255.0

#

rip 1

undo summary

default-route originate cost 2

version 2

network 10.0.0.0 #配置时只可写有类地址（主类地址）实际上v2发报文时会发送子网信息

silent-interface GigabitEthernet0/0/1

#

**AR2配置：**

interface GigabitEthernet0/0/0

ip address 10.99.3.2 255.255.255.0

rip authentication-mode hmac-sha256 hmac-sha256 cipher passwdxx 1

#

interface GigabitEthernet0/0/1

ip address 10.99.4.1 255.255.255.0

rip authentication-mode hmac-sha256 hmac-sha256 cipher passwdxx 1

#

rip 1

undo summary

version 2

network 10.0.0.0

#

**AR3配置：**

interface GigabitEthernet0/0/1

ip address 10.99.4.2 255.255.255.0

rip authentication-mode hmac-sha256 hmac-sha256 cipher passwdxx 1

#

interface GigabitEthernet0/0/2

ip address 10.99.5.1 255.255.255.0

#

rip 1

undo summary

version 2

network 10.0.0.0

silent-interface GigabitEthernet0/0/2

#

**AR3查看路由表：**

[Huawei] disp ip routing-table

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

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

Routing Tables: Public

Destinations : 13 Routes : 13

Destination/Mask Proto Pre Cost Flags NextHop Interface

0.0.0.0/0 RIP 100 4 D 10.99.4.1 GigabitEthernet0/0/1 #AR1引入的默认

10.99.2.0/24 RIP 100 2 D 10.99.4.1 GigabitEthernet0/0/1

10.99.3.0/24 RIP 100 1 D 10.99.4.1 GigabitEthernet0/0/1

10.99.4.0/24 Direct 0 0 D 10.99.4.2 GigabitEthernet0/0/1

10.99.4.2/32 Direct 0 0 D 127.0.0.1 GigabitEthernet0/0/1

10.99.4.255/32 Direct 0 0 D 127.0.0.1 GigabitEthernet0/0/1

10.99.5.0/24 Direct 0 0 D 10.99.5.1 GigabitEthernet0/0/2

10.99.5.1/32 Direct 0 0 D 127.0.0.1 GigabitEthernet0/0/2

10.99.5.255/32 Direct 0 0 D 127.0.0.1 GigabitEthernet0/0/2

<Huawei> disp rip 1 database

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

Advertisement State : [A] - Advertised

[I] - Not Advertised/Withdraw

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

0.0.0.0/0, cost 4, [A], nexthop 10.99.4.1

10.0.0.0/8, cost 0, ClassfulSumm

10.99.2.0/24, cost 2, [A], nexthop 10.99.4.1

10.99.3.0/24, cost 1, [A], nexthop 10.99.4.1

10.99.4.0/24, cost 0, [A], Rip-interface

10.99.5.0/24, cost 0, [A], Rip-interface

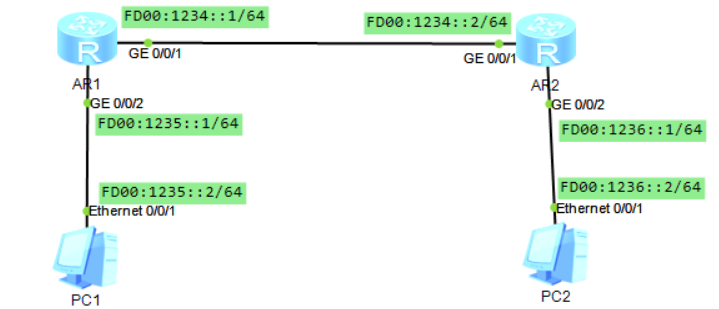
**★RIPng**

RIP Next Generation下一代RIP协议 是内部网关协议的一种，用于ipv6网络

RIPng使用组播地址FF02::9作为目的地址发送报文，源地址使用链路本地地址FE80::/10

RIPng协议报文共有2种（请求报文和响应报文）封装在UDP报文中，目的端口号521（和ripv1/v2不同）

**★实验：ripng\_ar2240（RIPng基础配置）**



**AR1配置：**

ipv6

#

interface GigabitEthernet0/0/1

ipv6 enable

ipv6 address FD00:1234::1/64

ripng 1 enable

#

interface GigabitEthernet0/0/2

ipv6 enable

ipv6 address FD00:1235::1/64

ripng 1 enable

#

ripng 1

**AR2配置：**

ipv6

#

interface GigabitEthernet0/0/1

ipv6 enable

ipv6 address FD00:1234::2/64

ripng 1 enable

#

interface GigabitEthernet0/0/2

ipv6 enable

ipv6 address FD00:1236::1/64

ripng 1 enable

#

ripng 1

**AR1查看：**

[Huawei] disp ipv6 routing-table protocol ripng #查看ripng路由

Public Routing Table : RIPng

Summary Count : 1

RIPng Routing Table's Status : < Active >

Summary Count : 1

Destination : FD00:1236:: PrefixLength : 64

NextHop : FE80::2E0:FCFF:FE8D:46B8 Preference : 100

Cost : 1 Protocol : RIPng

RelayNextHop : :: TunnelID : 0x0

Interface : GigabitEthernet0/0/1 Flags : D

RIPng Routing Table's Status : < Inactive >

Summary Count : 0

<Huawei> disp ripng 1 database verbose

FD00:1234::/64,

GigabitEthernet0/0/1, cost 0, RIPng-interface

EntryID : 0xb3df21f4 Tag : 0

FD00:1235::/64,

GigabitEthernet0/0/2, cost 0, RIPng-interface

EntryID : 0xb1a91b54 Tag : 0

FD00:1236::/64,

via FE80::2E0:FCFF:FE8D:46B8, GigabitEthernet0/0/1, cost 1

EntryID : 0xb1a91bfc Tag : 0

**★OSPF**

OSPF（Open Shortest Path First）开放最短路径优先协议，是一个内部网关协议，用在单一自治系统（Autonomous System）内决策路由，是对链路状态路由协议的一种实现，使用Dijkstra算法来计算最短路径树

OSPF v2用在ipv4网络，RFC 2328以及RFC 1583

OSPF v3支持ipv6网络，RFC 5340

OSPF中的链路代价cost/metric可取值1~65535，OSPF支持负载均衡（到同一目的网络有多条相同代价的路径时）

（华为设备如果要支持ipv4及ipv6，需要同时配置ospfv2及ospfv3两个路由进程）

[Huawei] ospf router-id 10.1.1.252 1 #开启ospf进程1，同时指定router-id。建议为每个osfp进程配置不同的router-id，一般router-id使用loopback环回接口的ip

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，全网设备都改为一致的

[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] abr-summary 10.2.0.0 0.0.255.255 cost 2000 #聚合区域间路由

[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，import-route不能引入其他路由进程中的默认路由

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

[Huawei-ospf-1] asbr-summary 10.3.0.0 255.255.0.0 cost 2000 #聚合引入的外部路由

[Huawei-ospf-1] area 1

[Huawei-ospf-1-area-0.0.0.1] vlink-peer 10.2.2.33 #虚链路对端（邻居的router-id）

[Huawei-ospf-1-area-0.0.0.1] vlink-peer 10.2.2.33 md5 1 cipher xxxx #虚链路对端也配置验证

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

[Huawei-ospf-1] maximum load-balancing 8 #配置路由负载分担

#接口开销

int g0/0/1

ospf cost 500 #到某目的网段的总开销为转发路径上出接口的开销之和

#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(M) #默认参考带宽为100M，对于现在的网络而言太小了，建议用100000M

[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

#配置为stub/nssa区域

[Huawei-ospf-1] area 4

[Huawei-ospf-1-area-0.0.0.4] stub #配置为Stub区域

[Huawei-ospf-1-area-0.0.0.4] stub no-summary #配置为Totally Stub区域

[Huawei-ospf-1-area-0.0.0.4] nssa #配置为NSSA区域

[Huawei-ospf-1-area-0.0.0.4] nssa no-summary #配置为Totally NSSA区域

<Huawei> reset ospf 1 process #复位ospf进程1，相当于重启了此进程

Warning: The OSPF process will be reset. Continue? [Y/N]:y

#引入静态路由时指定开销（使用路由策略）

acl number 2000

rule 10 permit source 10.99.9.4 0

#

route-policy p001\_static\_to\_ospf permit node 10

if-match acl 2000

apply cost 500

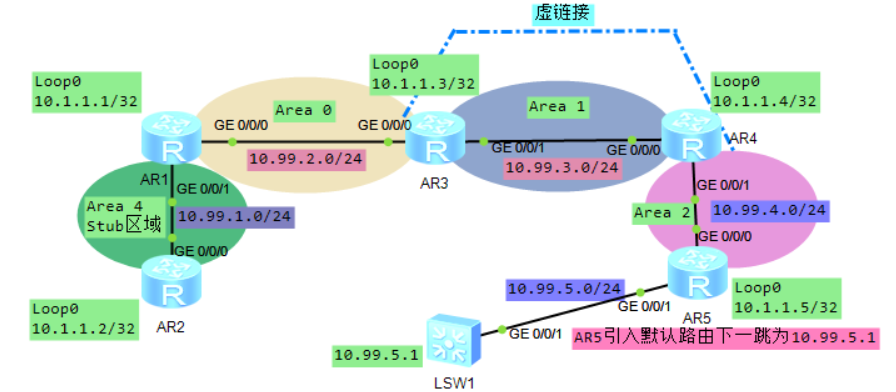
#

ospf 1

import-route static type 2 route-policy p001\_static\_to\_ospf

#

**★实验：ospf\_ar2240（OSPFv2基础配置）**



**AR1配置：**

interface GigabitEthernet0/0/0

ip address 10.99.2.1 255.255.255.0

#

interface GigabitEthernet0/0/1

ip address 10.99.1.1 255.255.255.0

#

interface LoopBack0

description for\_OSPF\_Router-ID

ip address 10.1.1.1 255.255.255.255

#

ospf 1 router-id 10.1.1.1 #router-id使用loopback0环回接口的ip

bandwidth-reference 100000

area 0.0.0.0

authentication-mode md5 1 cipher passwdxx

network 10.99.2.0 0.0.0.255

area 0.0.0.4

authentication-mode md5 1 cipher passwdxx

network 10.1.1.1 0.0.0.0

network 10.99.1.0 0.0.0.255

stub

**AR2配置：**

interface GigabitEthernet0/0/0

ip address 10.99.1.2 255.255.255.0

#

interface LoopBack0

description for\_OSPF\_Router-ID

ip address 10.1.1.2 255.255.255.255

#

ospf 1 router-id 10.1.1.2

bandwidth-reference 100000

area 0.0.0.4

authentication-mode md5 1 cipher passwdxx

network 10.1.1.2 0.0.0.0

network 10.99.1.0 0.0.0.255

stub

**AR3配置：**

interface GigabitEthernet0/0/0

ip address 10.99.2.2 255.255.255.0

#

interface GigabitEthernet0/0/1

ip address 10.99.3.1 255.255.255.0

#

interface LoopBack0

description for\_OSPF\_Router-ID

ip address 10.1.1.3 255.255.255.255

#

ospf 1 router-id 10.1.1.3

bandwidth-reference 100000

area 0.0.0.0

authentication-mode md5 1 cipher passwdxx

network 10.1.1.3 0.0.0.0

network 10.99.2.0 0.0.0.255

area 0.0.0.1

authentication-mode md5 1 cipher passwdxx

network 10.99.3.0 0.0.0.255

vlink-peer 10.1.1.4 md5 1 cipher passwdxx #虚链路对端的route-id

**AR4配置：**

interface GigabitEthernet0/0/0

ip address 10.99.3.2 255.255.255.0

#

interface GigabitEthernet0/0/1

ip address 10.99.4.1 255.255.255.0

#

interface LoopBack0

description for\_OSPF\_Router-ID

ip address 10.1.1.4 255.255.255.255

#

ospf 1 router-id 10.1.1.4

bandwidth-reference 100000

area 0.0.0.1

authentication-mode md5 1 cipher passwdxx

network 10.1.1.4 0.0.0.0

network 10.99.3.0 0.0.0.255

vlink-peer 10.1.1.3 md5 1 cipher passwdxx #虚链路对端的route-id

area 0.0.0.2

authentication-mode md5 1 cipher passwdxx

network 10.99.4.0 0.0.0.255

**AR5配置：**

interface GigabitEthernet0/0/0

ip address 10.99.4.2 255.255.255.0

#

interface GigabitEthernet0/0/1

ip address 10.99.5.2 255.255.255.0

#

interface LoopBack0

description for\_OSPF\_Router-ID

ip address 10.1.1.5 255.255.255.255

#

ospf 1 router-id 10.1.1.5

default-route-advertise cost 20000

bandwidth-reference 100000

area 0.0.0.2

authentication-mode md5 1 cipher passwdxx

network 10.1.1.5 0.0.0.0

network 10.99.4.0 0.0.0.255

#

ip route-static 0.0.0.0 0.0.0.0 10.99.5.1

**AR1查看信息：**

<Huawei> disp ospf abr-asbr

OSPF Process 1 with Router ID 10.1.1.1

Routing Table to ABR and ASBR

RtType Destination Area Cost Nexthop Type

Intra-area 10.1.1.3 0.0.0.0 100 10.99.2.2 ABR

Intra-area 10.1.1.4 0.0.0.0 200 10.99.2.2 ABR

Inter-area 10.1.1.5 0.0.0.0 300 10.99.2.2 ASBR

<Huawei> disp ospf lsdb

OSPF Process 1 with Router ID 10.1.1.1

Link State Database

Area: 0.0.0.0

Type LinkState ID AdvRouter Age Len Sequence Metric

Router 10.1.1.3 10.1.1.3 1183 60 80000010 0

Router 10.1.1.1 10.1.1.1 673 36 80000005 100

Router 10.1.1.4 10.1.1.4 1184 36 80000001 100

Network 10.99.2.2 10.1.1.3 674 32 80000002 0

Sum-Net 10.99.3.0 10.1.1.3 607 28 80000002 100

Sum-Net 10.99.3.0 10.1.1.4 1352 28 80000001 100

Sum-Net 10.99.1.0 10.1.1.1 718 28 80000002 100

Sum-Net 10.99.4.0 10.1.1.4 1352 28 80000001 100

Sum-Net 10.1.1.5 10.1.1.4 1352 28 80000001 100

Sum-Net 10.1.1.4 10.1.1.3 470 28 80000002 100

Sum-Net 10.1.1.4 10.1.1.4 1352 28 80000001 0

Sum-Net 10.1.1.1 10.1.1.1 718 28 80000002 0

Sum-Net 10.1.1.2 10.1.1.1 718 28 80000002 100

Sum-Asbr 10.1.1.5 10.1.1.4 1026 28 80000001 100

Area: 0.0.0.4

Type LinkState ID AdvRouter Age Len Sequence Metric

Router 10.1.1.2 10.1.1.2 984 48 80000009 100

Router 10.1.1.1 10.1.1.1 977 48 80000006 100

Network 10.99.1.2 10.1.1.2 984 32 80000003 0

Sum-Net 0.0.0.0 10.1.1.1 673 28 80000002 1

Sum-Net 10.99.3.0 10.1.1.1 606 28 80000002 200

Sum-Net 10.99.2.0 10.1.1.1 718 28 80000002 100

Sum-Net 10.99.4.0 10.1.1.1 1181 28 80000001 300

Sum-Net 10.1.1.5 10.1.1.1 1181 28 80000001 300

Sum-Net 10.1.1.4 10.1.1.1 469 28 80000002 200

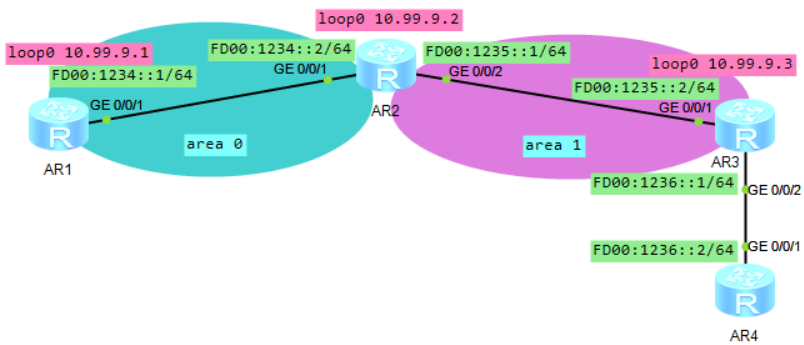
Sum-Net 10.1.1.3 10.1.1.1 673 28 80000002 100

AS External Database

Type LinkState ID AdvRouter Age Len Sequence Metric

External 0.0.0.0 10.1.1.5 849 36 80000001 20000

**★实验：ospf-v3\_ar2240（OSPFv3基础配置）**



ospfv3的router-id也是一个4字节的无符号整数，采用ipv4地址的形式。如果在同一台设备上运行了多个ospfv3进程，必须为每个进程指定不同的router-id

**AR1配置：**

ipv6

#

ospfv3 1

router-id 10.99.9.1 #必须手动指定router-id

bandwidth-reference 100000

#

interface GigabitEthernet0/0/1

ipv6 enable

ipv6 address FD00:1234::1/64

ospfv3 1 area 0.0.0.0 #在接口上配置ospfv3区域

#

interface LoopBack0

ip address 10.99.9.1 255.255.255.255

**AR2配置：**

ipv6

#

ospfv3 1

router-id 10.99.9.2

bandwidth-reference 100000

#

interface GigabitEthernet0/0/1

ipv6 enable

ipv6 address FD00:1234::2/64

ospfv3 1 area 0.0.0.0

#

interface GigabitEthernet0/0/2

ipv6 enable

ipv6 address FD00:1235::1/64

ospfv3 1 area 0.0.0.1

#

interface LoopBack0

ip address 10.99.9.2 255.255.255.255

**AR3配置：**

ipv6

#

ospfv3 1

router-id 10.99.9.3

bandwidth-reference 100000

default-route-advertise cost 2000 #引入默认路由

#

interface GigabitEthernet0/0/1

ipv6 enable

ipv6 address FD00:1235::2/64

ospfv3 1 area 0.0.0.1

#

interface GigabitEthernet0/0/2

ipv6 enable

ipv6 address FD00:1236::1/64

#

interface LoopBack0

ip address 10.99.9.3 255.255.255.255

#

ipv6 route-static :: 0 FD00:1236::2 #配置默认路由到AR4

**AR1查看：**

<Huawei> disp ospfv3 routing #查看ospfv3路由信息

Codes : E2 - Type 2 External, E1 - Type 1 External, IA - Inter-Area,

N - NSSA, U - Uninstalled

OSPFv3 Process (1)

Destination Metric Next-hop

E2 ::/0 2000 via FE80::2E0:FCFF:FEB3:6654, GigabitEthernet0/0/1

FD00:1234::/64 99 directly connected, GigabitEthernet0/0/1

IA FD00:1235::/64 198 via FE80::2E0:FCFF:FEB3:6654, GigabitEthernet0/0/1

**★IS-IS**

Intermediate System-Intermediate System中间系统到中间系统

[Huawei] 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

[Huawei-isis-1] is-level level-1 #指定level，未指定时默认为level-1-2

[Huawei-isis-1] cost-style wide #设置is-is设备接收和发送路由的开销类型

[Huawei-isis-1] network-entity 49.0001.1111.1111.1111.00 #设置isis网络实体名称（NET）

#同一个level-1区域号要求相同

[Huawei-isis-1] is-name ar1 #在LSP中带上此xx名称方便查看维护

[Huawei-isis-1] import-route direct level-1 #引入直连路由

#

[Huawei] interface GigabitEthernet0/0/1

[Huawei-GigabitEthernet0/0/1] ip address 10.99.1.1 255.255.255.0

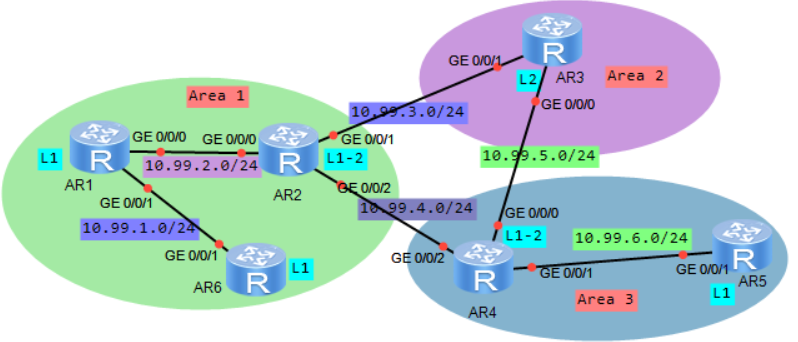
[Huawei-GigabitEthernet0/0/1] isis enable 1 #在接口上使能isis进程1

[Huawei-GigabitEthernet0/0/1] isis circuit-level level-1

[Huawei-GigabitEthernet0/0/1] isis authentication-mode md5 cipher passwdxx #配置接口MD5验证

#

**★实验：isis\_ar2240**



**各设备的systemID不能相同！**

**AR1配置：**

isis 1

is-level level-1

cost-style wide

network-entity 49.0001.1111.1111.1111.00

is-name ar1

import-route direct level-1

#

interface GigabitEthernet0/0/0

ip address 10.99.2.1 255.255.255.0

isis enable 1

isis circuit-leve l level-1

isis authentication-mode md5 cipher passwdxx

#

interface GigabitEthernet0/0/1

ip address 10.99.1.1 255.255.255.0

isis enable 1

isis circuit-level level-1

isis authentication-mode md5 cipher passwdxx

**AR6配置：**

isis 1

is-level level-1

cost-style wide

network-entity 49.0001.1111.1111.6666.00

is-name ar6

import-route direct level-1

#

interface GigabitEthernet0/0/1

ip address 10.99.1.2 255.255.255.0

isis enable 1

isis circuit-level level-1

isis authentication-mode md5 cipher passwdxx

**AR2配置：**

isis 1

cost-style wide

network-entity 49.0001.1111.1111.2222.00

is-name ar2

import-route direct level-1-2

#

interface GigabitEthernet0/0/0

ip address 10.99.2.2 255.255.255.0

isis enable 1

isis authentication-mode md5 cipher passwdxx

#

interface GigabitEthernet0/0/1

ip address 10.99.3.1 255.255.255.0

isis enable 1

isis authentication-mode md5 cipher passwdxx

#

interface GigabitEthernet0/0/2

ip address 10.99.4.1 255.255.255.0

isis enable 1

isis authentication-mode md5 cipher passwdxx

**AR3配置：**

isis 1

is-level level-2

cost-style wide

network-entity 49.0002.1111.1111.3333.00

is-name ar3

import-route direct

#

interface GigabitEthernet0/0/0

ip address 10.99.5.1 255.255.255.0

isis enable 1

isis circuit-level level-2

isis authentication-mode md5 cipher passwdxx

#

interface GigabitEthernet0/0/1

ip address 10.99.3.2 255.255.255.0

isis enable 1

isis circuit-level level-2

isis authentication-mode md5 cipher passwdxx

**AR4配置：**

isis 1

cost-style wide

network-entity 49.0003.1111.1111.4444.00

is-name ar4

import-route direct level-1-2

#

interface GigabitEthernet0/0/0

ip address 10.99.5.2 255.255.255.0

isis enable 1

isis authentication-mode md5 cipher passwdxx

#

interface GigabitEthernet0/0/1

ip address 10.99.6.1 255.255.255.0

isis enable 1

isis authentication-mode md5 cipher passwdxx

#

interface GigabitEthernet0/0/2

ip address 10.99.4.2 255.255.255.0

isis enable 1

isis authentication-mode md5 cipher passwdxx

**AR5配置：**

isis 1

is-level level-1

cost-style wide

network-entity 49.0003.1111.1111.5555.00

is-name ar5

import-route direct level-1

#

interface GigabitEthernet0/0/1

ip address 10.99.6.2 255.255.255.0

isis enable 1

isis circuit-level level-1

isis authentication-mode md5 cipher passwdxx

**AR2查看：**

<Huawei> disp isis peer #查看isis邻居

Peer information for ISIS(1)

System Id Interface Circuit Id State HoldTime Type PRI

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

ar1 GE0/0/0 ar2.01 Up 29s L1 64

ar3 GE0/0/1 ar2.02 Up 22s L2 64

ar4 GE0/0/2 ar2.03 Up 30s L2(L1L2) 64

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

Database information for ISIS(1)

Level-1 Link State Database

LSPID Seq Num Checksum Holdtime Length ATT/P/OL

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

ar1.00-00 0x00000008 0x1942 542 93 0/0/0

ar2.00-00\* 0x0000000a 0xbd7e 442 94 1/0/0

ar2.01-00\* 0x00000002 0x57af 442 54 0/0/0

ar6.00-00 0x00000007 0xd87f 871 70 0/0/0

ar6.01-00 0x00000003 0xec0a 871 54 0/0/0

Total LSP(s): 5

\*(In TLV)-Leaking Route, \*(By LSPID)-Self LSP, +-Self LSP(Extended),

ATT-Attached, P-Partition, OL-Overload

Level-2 Link State Database

LSPID Seq Num Checksum Holdtime Length ATT/P/OL

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

ar2.00-00\* 0x0000000e 0xd625 442 113 0/0/0

ar2.02-00\* 0x00000002 0x5071 442 54 0/0/0

ar2.03-00\* 0x00000002 0x4955 442 54 0/0/0

ar3.00-00 0x00000009 0x7dca 692 93 0/0/0

ar4.00-00 0x0000000e 0xea1a 880 105 0/0/0

ar4.02-00 0x00000002 0x1d1c 880 54 0/0/0

Total LSP(s): 6

<Huawei> disp ip routing-table protocol isis #查看isis学习到的路由

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

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

Public routing table : ISIS

Destinations : 3 Routes : 4

ISIS routing table status : <Active>

Destinations : 3 Routes : 4

Destination/Mask Proto Pre Cost Flags NextHop Interface

10.99.1.0/24 ISIS-L1 15 20 D 10.99.2.1 GigabitEthernet0/0/0

10.99.5.0/24 ISIS-L2 15 20 D 10.99.3.2 GigabitEthernet0/0/1 #2条等价路径

ISIS-L2 15 20 D 10.99.4.2 GigabitEthernet0/0/2

10.99.6.0/24 ISIS-L2 15 20 D 10.99.4.2 GigabitEthernet0/0/2

**AR6查看：**

<Huawei> disp ip routing-table protocol isis #查看isis学习到的路由，level-2的路由引入为默认路由

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

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

Public routing table : ISIS

Destinations : 4 Routes : 4

ISIS routing table status : <Active>

Destinations : 4 Routes : 4

Destination/Mask Proto Pre Cost Flags NextHop Interface

0.0.0.0/0 ISIS-L1 15 20 D 10.99.1.1 GigabitEthernet0/0/1 #非level-1的路由

10.99.2.0/24 ISIS-L1 15 20 D 10.99.1.1 GigabitEthernet0/0/1

10.99.3.0/24 ISIS-L1 15 30 D 10.99.1.1 GigabitEthernet0/0/1

10.99.4.0/24 ISIS-L1 15 30 D 10.99.1.1 GigabitEthernet0/0/1

**★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及BFD联动**

eBGP路由器邻居分别属于不同的AS系统，eBGP各路由器之间会相互发送学习到的路由信息

[AR2220-R1] bfd #先全局使能bfd

[AR2220-R1] bgp 300 #开启bgp进程，本设备as号为300（2字节的AS号）

#如果要使用4字节的AS号，则按2字节为一组，中间用.点号分隔，比如 5000:100这种形式

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

[AR2220-R1-bgp] timer keepalive 10 hold 30 #消息报文周期为10秒，30秒为最大超时

[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，

#邻居只需要路由可达即可，不一定非得是直连网段的ip

[AR2220-R1-bgp] peer 9.9.9.2 password cipher passwdxx #配置MD5认证密码

[AR2220-R1-bgp] peer 9.9.9.2 bfd enable #和邻居之间使能bfd

[AR2220-R1-bgp] peer 9.9.9.2 bfd min-tx-interval 1000 min-rx-interval 1000 #周期为1000毫秒

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

#默认情况下，为了防止AS间产生环路，当收到eBGP对等体发送的路由时，会将带有本地AS号的路由丢弃

[AR2220-R1-bgp] peer x.x.x.x next-hop-local #向iBGP对等体通告路由时，把下一跳属性设置为自身的tcp连接源地址，默认情况下本路由器把收到的eBGP路由通告给iBGP对待体时不会改变其next-hop属性

[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] aggregate 10.1.1.0 24 detail-suppressed #聚合路由

[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] import-route direct #引入直连路由

[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

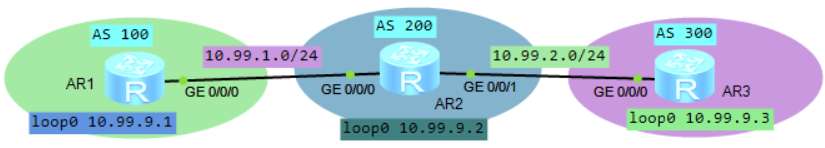
**#查看**

[AR2220-R1] disp bgp peer #查看bgp邻居

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

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

**★实验：eBGP\_ar2240**



**AR1配置：**

bfd

#

interface GigabitEthernet0/0/0

ip address 10.99.1.1 255.255.255.0

#

interface LoopBack0

ip address 10.99.9.1 255.255.255.255

#

bgp 100

router-id 10.99.9.1

timer keepalive 10 hold 30

timer connect-retry 3

peer 10.99.1.2 as-number 200

peer 10.99.1.2 bfd min-tx-interval 100 min-rx-interval 100

peer 10.99.1.2 bfd enable

ipv4-family unicast

undo synchronization #默认

network 10.99.1.0 255.255.255.0

network 10.99.9.1 255.255.255.255

maximum load-balancing ebgp 8

peer 10.99.1.2 enable #根据前面配置的peer对等体信息自动生成的

**AR2配置：**

bfd

#

interface GigabitEthernet0/0/0

ip address 10.99.1.2 255.255.255.0

#

interface GigabitEthernet0/0/1

ip address 10.99.2.1 255.255.255.0

#

interface LoopBack0

ip address 10.99.9.2 255.255.255.255

#

bgp 200

router-id 10.99.9.2

timer keepalive 10 hold 30

timer connect-retry 3

peer 10.99.1.1 as-number 100

peer 10.99.1.1 bfd min-tx-interval 100 min-rx-interval 100

peer 10.99.1.1 bfd enable

peer 10.99.2.2 as-number 300

peer 10.99.2.2 bfd min-tx-interval 100 min-rx-interval 100

peer 10.99.2.2 bfd enable

ipv4-family unicast

undo synchronization

import-route direct

peer 10.99.1.1 enable

peer 10.99.2.2 enable

**AR3配置：**

bfd

#

interface GigabitEthernet0/0/0

ip address 10.99.2.2 255.255.255.0

#

interface LoopBack0

ip address 10.99.9.3 255.255.255.255

#

bgp 300

router-id 10.99.9.3

timer keepalive 10 hold 30

timer connect-retry 3

peer 10.99.2.1 as-number 200

peer 10.99.2.1 bfd min-tx-interval 100 min-rx-interval 100

peer 10.99.2.1 bfd enable

ipv4-family unicast

undo synchronization

import-route direct

peer 10.99.2.1 enable

**AR2上查看：**

<Huawei> disp bgp peer #查看bgp邻居

BGP local router ID : 10.99.9.2

Local AS number : 200

Total number of peers : 2 Peers in established state : 2

Peer V AS MsgRcvd MsgSent OutQ Up/Down State Pre fRcv

10.99.1.1 4 100 79 82 0 00:12:38 Established 2

10.99.2.2 4 300 47 50 0 00:07:16 Established 2

<Huawei> disp ip routing-table protocol bgp #查看bgp路由（生效的）

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

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

Public routing table : BGP

Destinations : 2 Routes : 2

BGP routing table status : <Active>

Destinations : 2 Routes : 2

Destination/Mask Proto Pre Cost Flags NextHop Interface

10.99.9.1/32 EBGP 255 0 D 10.99.1.1 GigabitEthernet0/0/0

10.99.9.3/32 EBGP 255 0 D 10.99.2.2 GigabitEthernet0/0/1

BGP routing table status : <Inactive>

Destinations : 0 Routes : 0

<Huawei> disp bfd session all #查看bfd会话

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

Local Remote PeerIpAddr State Type InterfaceName

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

8192 8192 10.99.1.1 Up D\_IP\_IF GigabitEthernet0/0/0

8193 8192 10.99.2.2 Up D\_IP\_IF GigabitEthernet0/0/1

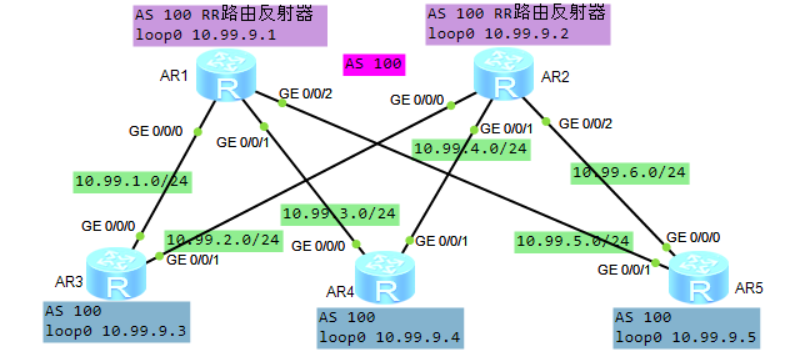
--------------------------------------------------------------------------------

Total UP/DOWN Session Number : 2/0

**★iBGP及路由反射**

为了防止AS内产生环路（iBGP水平分割规则限制），BGP设备不会把从iBGP对等体学到的路由通告给其他iBGP对等体，如果要和所有iBGP对等体学习路由信息，需要所有iBGP对等体之间建立全连接，当iBGP对等体数量过多时，会建立相当多的对等体连接导致效率降低，这时可使用BGP路由反射器功能，所有iBGP设备只需要和反射器设备建立对等体连接，路由反射器会将收到的iBGP路由信息发送给其他所有iBGP对等体。

**★实验：iBGP\_route\_reflect\_ar2240**



AR1和AR2做路由反射器

**AR1配置：**

interface GigabitEthernet0/0/0

ip address 10.99.1.1 255.255.255.0

#

interface GigabitEthernet0/0/1

ip address 10.99.3.1 255.255.255.0

#

interface GigabitEthernet0/0/2

ip address 10.99.5.1 255.255.255.0

#

interface LoopBack0

ip address 10.99.9.1 255.255.255.255

#

bgp 100

router-id 10.99.9.1

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

#对等体组配置为internal后，此group不需要再配置as-number，同本bgp的AS号

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

peer 10.99.1.2 group rc\_inter\_1 #将对端放入rc\_inter\_1组内

peer 10.99.3.2 group rc\_inter\_1

peer 10.99.5.2 group rc\_inter\_1

ipv4-family unicast

undo synchronization

reflector cluster-id 1 #配置反射器的cluster-id

import-route direct

peer rc\_inter\_1 enable

#以下是根据前面的配置自动生成的，配置时不需要输入以下命令

peer rc\_inter\_1 reflect-client

peer 10.99.1.2 enable

peer 10.99.1.2 group rc\_inter\_1

peer 10.99.3.2 enable

peer 10.99.3.2 group rc\_inter\_1

peer 10.99.5.2 enable

peer 10.99.5.2 group rc\_inter\_1

**AR2配置：**

interface GigabitEthernet0/0/0

ip address 10.99.2.1 255.255.255.0

#

interface GigabitEthernet0/0/1

ip address 10.99.4.1 255.255.255.0

#

interface GigabitEthernet0/0/2

ip address 10.99.6.1 255.255.255.0

#

interface LoopBack0

ip address 10.99.9.2 255.255.255.255

#

bgp 100

router-id 10.99.9.2

group rc\_inter\_1 internal

peer rc\_inter\_1 reflect-client

peer 10.99.2.2 group rc\_inter\_1

peer 10.99.4.2 group rc\_inter\_1

peer 10.99.6.2 group rc\_inter\_1

ipv4-family unicast

undo synchronization

reflector cluster-id 1

import-route direct

#以下是根据前面的配置自动生成的，配置时不需要输入以下命令

peer rc\_inter\_1 enable

peer rc\_inter\_1 reflect-client

peer 10.99.2.2 enable

peer 10.99.2.2 group rc\_inter\_1

peer 10.99.4.2 enable

peer 10.99.4.2 group rc\_inter\_1

peer 10.99.6.2 enable

peer 10.99.6.2 group rc\_inter\_1

**AR3配置：**

interface GigabitEthernet0/0/0

ip address 10.99.1.2 255.255.255.0

#

interface GigabitEthernet0/0/1

ip address 10.99.2.2 255.255.255.0

#

interface LoopBack0

ip address 10.99.9.3 255.255.255.255

#

bgp 100

router-id 10.99.9.3

group rr\_inter\_1 internal

peer 10.99.1.1 group rr\_inter\_1

peer 10.99.2.1 group rr\_inter\_1

ipv4-family unicast

undo synchronization

import-route direct

maximum load-balancing ibgp 8

#以下是根据前面的配置自动生成的，配置时不需要输入以下命令

peer rr\_inter\_1 enable

peer 10.99.1.1 enable

peer 10.99.1.1 group rr\_inter\_1

peer 10.99.2.1 enable

peer 10.99.2.1 group rr\_inter\_1

**AR4及AR5配置同AR3，这里不列出了。**

**AR3上查看：**

<Huawei> disp bgp peer #查看bgp邻居

BGP local router ID : 10.99.9.3

Local AS number : 100

Total number of peers : 2 Peers in established state : 2

Peer V AS MsgRcvd MsgSent OutQ Up/Down State Pre fRcv

10.99.1.1 4 100 29 27 0 00:20:35 Established 8

10.99.2.1 4 100 27 24 0 00:18:54 Established 8

<Huawei> disp ip routing-table protocol bgp #查看bgp路由（生效的）

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

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

Public routing table : BGP

Destinations : 8 Routes : 14

BGP routing table status : <Active>

Destinations : 8 Routes : 14

Destination/Mask Proto Pre Cost Flags NextHop Interface

10.99.3.0/24 IBGP 255 0 RD 10.99.1.1 GigabitEthernet0/0/0

IBGP 255 0 RD 10.99.4.2 GigabitEthernet0/0/1

10.99.4.0/24 IBGP 255 0 RD 10.99.2.1 GigabitEthernet0/0/1

IBGP 255 0 RD 10.99.3.2 GigabitEthernet0/0/0

10.99.5.0/24 IBGP 255 0 RD 10.99.1.1 GigabitEthernet0/0/0

IBGP 255 0 RD 10.99.6.2 GigabitEthernet0/0/1

10.99.6.0/24 IBGP 255 0 RD 10.99.2.1 GigabitEthernet0/0/1

IBGP 255 0 RD 10.99.5.2 GigabitEthernet0/0/0

10.99.9.1/32 IBGP 255 0 RD 10.99.1.1 GigabitEthernet0/0/0

10.99.9.2/32 IBGP 255 0 RD 10.99.2.1 GigabitEthernet0/0/1

10.99.9.4/32 IBGP 255 0 RD 10.99.3.2 GigabitEthernet0/0/0

IBGP 255 0 RD 10.99.4.2 GigabitEthernet0/0/1

10.99.9.5/32 IBGP 255 0 RD 10.99.5.2 GigabitEthernet0/0/0

IBGP 255 0 RD 10.99.6.2 GigabitEthernet0/0/1

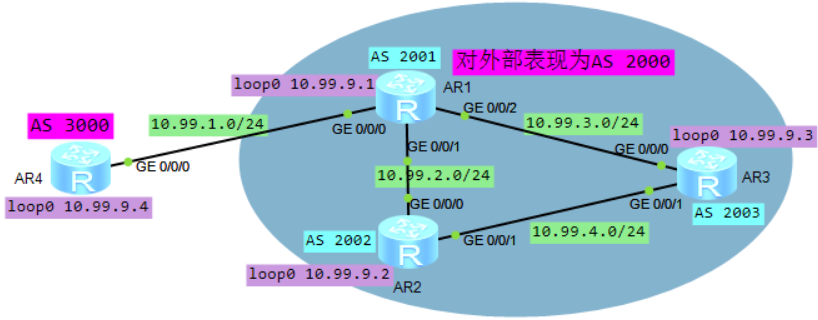
BGP routing table status : <Inactive>

Destinations : 0 Routes : 0

<Huawei> reset bgp 100 #重置bgp连接

**★iBGP联盟**

**★实验：iBGP\_confederation\_ar2240**



**AR1配置：（作为ASBR）**

interface GigabitEthernet0/0/0

ip address 10.99.1.1 255.255.255.0

#

interface GigabitEthernet0/0/1

ip address 10.99.2.1 255.255.255.0

#

interface GigabitEthernet0/0/2

ip address 10.99.3.1 255.255.255.0

#

interface LoopBack0

ip address 10.99.9.1 255.255.255.255

#

bgp 2001

router-id 10.99.9.1

confederation id 2000 #对外表现为一个AS 2000

confederation peer-as 2002 2003

peer 10.99.1.2 as-number 3000

peer 10.99.2.2 as-number 2002

peer 10.99.3.2 as-number 2003

ipv4-family unicast

undo synchronization

import-route direct

peer 10.99.2.2 next-hop-local #配置这条之后，AR2到外部都要经过R1

peer 10.99.3.2 next-hop-local #配置这条之后，AR3到外部都要经过R1

**AR2配置：**

interface GigabitEthernet0/0/0

ip address 10.99.2.2 255.255.255.0

#

interface GigabitEthernet0/0/1

ip address 10.99.4.1 255.255.255.0

#

interface LoopBack0

ip address 10.99.9.2 255.255.255.255

#

bgp 2002

router-id 10.99.9.2

confederation id 2000

confederation peer-as 2001 2003

peer 10.99.2.1 as-number 2001

peer 10.99.4.2 as-number 2003

ipv4-family unicast

undo synchronization

import-route direct

maximum load-balancing ibgp 8

**AR3配置同AR2，这里省略了**

**AR4配置：**

interface GigabitEthernet0/0/0

ip address 10.99.1.2 255.255.255.0

#

interface LoopBack0

ip address 10.99.9.4 255.255.255.255

#

bgp 3000

router-id 10.99.9.4

peer 10.99.1.1 as-number 2000

ipv4-family unicast

undo synchronization

import-route direct

**★ip-prefix匹配**

ACL可以匹配IP地址的前缀，但无法匹配掩码长度，使用P-Prefix可以同时匹配IP地址前缀及掩码长度。

注意：IP-Prefix不能用于流量的过滤（不像ACL那样能直接应用在接口上），只能用于路由信息的过滤（应用于路由策略中）

1、匹配固定长度的前缀

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

2、匹配前缀范围

ip ip-prefix yewu-prefix1 index 10 permit 10.99.0.0 24 greater-equal 24 less-equal 28

#创建一个名为yewu-prefix1的ip前缀规则，前24位要匹配上10.99.0.0/24的路由条目，其子网掩码长度在24到28位之间，这样的路由可被匹配上。

**★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（用于控制平面）

通过路由过滤来控制某些路由信息的传递（接收与发布），

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）

[Huawei] route-policy rp-01 permit node 10 #创建名为rp-01的路由策略

[Huawei-route-policy] if-match acl 2001 #匹配acl

[Huawei-route-policy] if-match ip-prefix xxx-prefix1 #匹配ip-prefix，各if-match都要被匹配通过

[Huawei-route-policy] apply community 10:10 #才会应用团体属性

**★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层设备都一样的网关配置

interface Vlanif10

ip address 192.168.10.1 255.255.255.0 #网关地址

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（仅引入到本设备的路由表中）

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，默认每秒发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

#前面引入的arp主机路由目前仅存在当前设备中，还得在动态路由协议中宣告出去

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 #创建一个名为**arp-host-router1**的路由策略

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

#

**★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

**★第11章、隧道技术**

**ensp模拟器中的AR2240等AR路由器的Tunnel接口起不来，**

**本章节的MPLS相关实验使用NE40E路由器进行配置，**

**VXLAN相关实验只能用CE系列交换机，建议用CE12800交换机进行配置。**

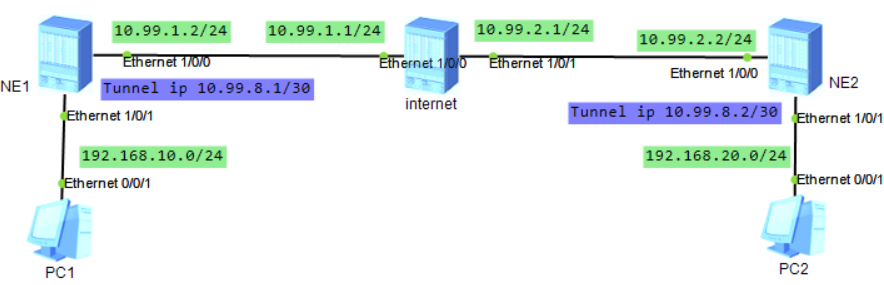
**★GRE隧道**

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

**★实验：GRE\_ne40e**



NE1和NE2之间建立一条gre隧道，隧道2端需要配置ip（同一网段的）

**NE1配置：**

interface Ethernet1/0/0

undo shutdown

ip address 10.99.1.2 255.255.255.0

dcn

dcn mode vlan

binding tunnel gre #出接口需要绑定gre隧道

#

interface Ethernet1/0/1

undo shutdown

ip address 192.168.10.1 255.255.255.0

dcn

dcn mode vlan

#

interface Tunnel0/0/0 #创建隧道接口

ip address 10.99.8.1 255.255.255.252

tunnel-protocol gre #隧道协议为GRE

keepalive #保持连接

keepalive period 10 #保活周期设置为10秒，默认5秒

source 10.99.1.2 #源ip为出接口ip

destination 10.99.2.2 #目的ip为隧道对端设备的出接口ip

#

ip route-static 10.99.2.0 255.255.255.0 10.99.1.1 #普通路由，用于连接到对端的

ip route-static 192.168.20.0 255.255.255.0 Tunnel0/0/0 #业务路由，将目标网段下一跳设置为隧道接口

**NE2配置：**

interface Ethernet1/0/0

undo shutdown

ip address 10.99.2.2 255.255.255.0

dcn

dcn mode vlan

binding tunnel gre

#

interface Ethernet1/0/1

undo shutdown

ip address 192.168.20.1 255.255.255.0

dcn

dcn mode vlan

#

interface Tunnel0/0/0

ip address 10.99.8.2 255.255.255.252

tunnel-protocol gre

keepalive

keepalive period 10

source 10.99.2.2

destination 10.99.1.2

#

ip route-static 10.99.1.0 255.255.255.0 10.99.2.1

ip route-static 192.168.10.0 255.255.255.0 10.99.8.1 #业务路由，目标网段下一跳也可设置为隧道对端ip

**NE1查看：**

[~HUAWEI] display tunnel-info all

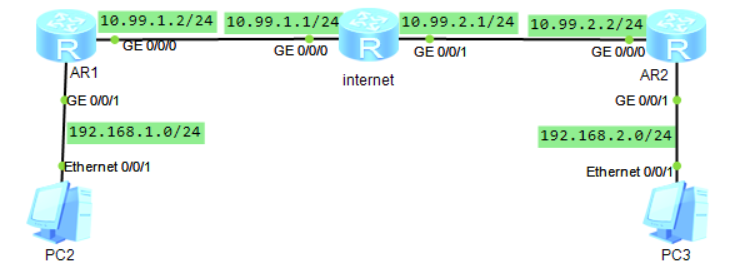
Tunnel ID Type Destination Status

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

0x00000000050000001a gre 10.99.2.2 UP

**★IPsec VPN**

**★实验：IPsec\_VPN\_ar2240**



拓扑图如上，AR1的业务网段为192.168.1.0/24，出接口ip为10.99.1.2，网关10.99.1.1

AR2的业务网段为192.168.2.0/24，出接口ip为10.99.2.2，网关10.99.2.1

internet上没有vpn业务网段相关的路由

**AR1配置：**

acl number 3000 #配置acl匹配目标流（vpn业务流量）

rule 1 permit ip source 192.168.1.0 0.0.0.255 destination 192.168.2.0 0.0.0.255

#

ipsec proposal pro1 #配置ipsec安全提议

esp authentication-algorithm sha1 #消息摘要算法

esp encryption-algorithm aes-128 #数据加密算法

encapsulation-mode tunnel #使用隧道模式（默认）

#

ike proposal 5 #配置ike安全提议

esp authentication-algorithm sha1 #消息摘要算法（默认）

encryption-algorithm aes-cbc-128 #数据加密算法

authentication-method pre-share #认证方式为预共享密码（默认）

#

ike peer peer1 v1 #配置ike对端

pre-shared-key cipher passwdxx

ike-proposal 5

remote-address 10.99.2.2

#

ipsec policy ipsec\_po1 10 isakmp #配置ipsec策略

security acl 3000

ike-peer peer1

proposal pro1

#

interface GigabitEthernet0/0/0 #出接口上应用ipsec策略

ip address 10.99.1.2 255.255.255.0

ipsec policy ipsec\_po1

#

interface GigabitEthernet0/0/1

ip address 192.168.1.1 255.255.255.0

#

ip route-static 0.0.0.0 0.0.0.0 10.99.1.1 #默认路由（或者前往目标vpn业务网段的路由）下一跳要指向出接口网关

**AR2配置：**

acl number 3000

rule 1 permit ip source 192.168.2.0 0.0.0.255 destination 192.168.1.0 0.0.0.255

#

ipsec proposal pro1

esp authentication-algorithm sha1

esp encryption-algorithm aes-128

#

ike proposal 5

encryption-algorithm aes-cbc-128

#

ike peer peer1 v1

pre-shared-key cipher passwdxx

ike-proposal 5

remote-address 10.99.1.2

#

ipsec policy ipsec\_po1 10 isakmp

security acl 3000

ike-peer peer1

proposal pro1

#

interface GigabitEthernet0/0/0

ip address 10.99.2.2 255.255.255.0

ipsec policy ipsec\_po1

#

interface GigabitEthernet0/0/1

ip address 192.168.2.1 255.255.255.0

#

ip route-static 0.0.0.0 0.0.0.0 10.99.2.1

**AR1上查看：**

<Huawei> disp ipsec sa brief

Number of SAs:2

Src address Dst address SPI VPN Protocol Algorithm

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

10.99.2.2 10.99.1.2 1049700406 0 ESP E:AES-128 A:SHA1-96

10.99.1.2 10.99.2.2 4120190158 0 ESP E:AES-128 A:SHA1-96

[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**

L2TP（Layer 2 Tunnel Protocol）二层隧道协议，是将PPP报文封装在L2TP报文里，再封装在1701/UDP里

**L2TP应用场景：**

③Client-Initaited



直接由用户侧发起连接（用户侧充当LAC），LNS侧需要为每个远程用户建立一条隧道，建立L2TP隧道，建立L2TP会话（PPP），最后传输数据

LAC（L2TP Access Concentrator）

LNS（L2TP Network Server）

**会话是有方向的：**

Incomming会话：从LAC到LNS

Outgoing会话：从LNS到LAC

**★实验：L2TP\_VPN\_ar2220（实体设备）**

**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

**★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

**★MPLS**

LSR（Label Switch Router）标签交换路由器

LER（Label Edge Router）标签边界路由器

FEC（Forwarding Equivalence Class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ingress-LER（入站LER），最后一个lsr称为egress-LER（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。

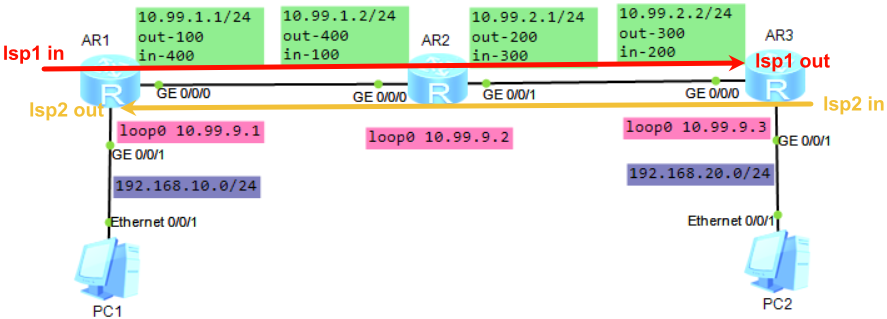
不过：一条LSP的流量是单向的，要想双方可达，需要建立一来一回共2条LSP

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

**实验：mpls\_static\_LSP\_ar2240**



AR1和AR3为LER节点，AR2为Transit节点

在LER（AR1和AR2）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in-label的流量 剥去mpls label，再进行普通路由转发

**AR1配置：**

mpls lsr-id 10.99.9.1 #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

#

interface GigabitEthernet0/0/0

ip address 10.99.1.1 255.255.255.0

mpls #LSP经过的接口上开启mpls

#

interface GigabitEthernet0/0/1

ip address 192.168.10.1 255.255.255.0

#

interface LoopBack0

ip address 10.99.9.1 255.255.255.255

#

ip route-static 192.168.20.0 255.255.255.0 10.99.1.2

#

static-lsp ingress lsp1 destination 192.168.20.0 24 nexthop 10.99.1.2 out-label 100

static-lsp egress lsp2 incoming-interface GigabitEthernet0/0/0 in-label 400

**AR2配置：**

mpls lsr-id 10.99.9.2

mpls

#

interface GigabitEthernet0/0/0

ip address 10.99.1.2 255.255.255.0

mpls

#

interface GigabitEthernet0/0/1

ip address 10.99.2.1 255.255.255.0

mpls

#

interface LoopBack0

ip address 10.99.9.2 255.255.255.255

#

static-lsp transit lsp1 incoming-interface GigabitEthernet0/0/0 in-label 100 nexthop 10.99.2.2 out-label 200

static-lsp transit lsp2 incoming-interface GigabitEthernet0/0/1 in-label 300 nexthop 10.99.1.1 out-label 400

**AR3配置：**

mpls lsr-id 10.99.9.3

mpls

#

interface GigabitEthernet0/0/0

ip address 10.99.2.2 255.255.255.0

mpls

#

interface GigabitEthernet0/0/1

ip address 192.168.20.1 255.255.255.0

#

interface LoopBack0

ip address 10.99.9.3 255.255.255.255

#

ip route-static 192.168.10.0 255.255.255.0 10.99.2.1

#

static-lsp ingress lsp2 destination 192.168.10.0 24 nexthop 10.99.2.1 out-label 300

static-lsp egress lsp1 incoming-interface GigabitEthernet0/0/0 in-label 200

**AR1上查看：**

<Huawei> disp mpls static-lsp #查看静态lsp状态

<Huawei> disp mpls lsp #查看lsp状态

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

LSP Information: STATIC LSP

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

FEC In/Out Label In/Out IF Vrf Name

-/- 400/NULL GE0/0/0/-

192.168.20.0/24 NULL/100 -/GE0/0/0

**AR2上查看：**

<Huawei> disp mpls lsp #查看lsp状态

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

LSP Information: STATIC LSP

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

FEC In/Out Label In/Out IF Vrf Name

-/- 100/200 GE0/0/0/GE0/0/1

-/- 300/400 GE0/0/1/GE0/0/0

**★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保守方式

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ospf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（ingress），使用入标签为NULL的那条lsp，如果接收到带有标签的mpls报文（transit），则使用不带NULL的那条lsp

ip ip-prefix mpls\_yewu\_01 permit 192.168.20.0 24 #创建一条ip前缀匹配

mpls #全局开启mpls

lsp-trigger ip-prefix mpls\_yewu\_01 #将此ip前缀匹配的路由在ldp中宣告

disp mpls lsp include 192.168.20.0 24 verbose #查看lsp转发表中关于此路由的详细情况

★LDP标签过滤

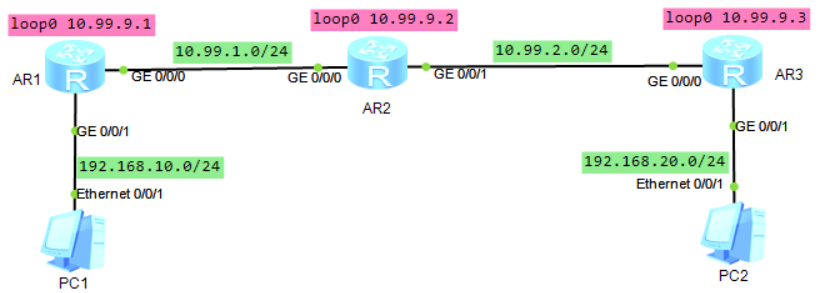
ip ip-prefix xxx permit 10.22.22.0 24 #创建一条ip前缀匹配

#

mpls

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

**实验：mpls\_LDP\_ar2240**



**AR1配置：**

mpls lsr-id 10.99.9.1

mpls #全局开启mpls

lsp-trigger ip-prefix mpls\_yewu\_01 #将此ip前缀匹配的路由在ldp中宣告

#

mpls ldp #全局开启mpls ldp

#

interface GigabitEthernet0/0/0

ip address 10.99.1.1 255.255.255.0

ospf ldp-sync #配置ospf和LDP同步

mpls #LSP经过的接口上开启mpls

mpls ldp #LSP经过的接口上开启mpls ldp

#

interface GigabitEthernet0/0/1

ip address 192.168.10.1 255.255.255.0

#

interface LoopBack0

ip address 10.99.9.1 255.255.255.255

#

ospf 1 router-id 10.99.9.1

bandwidth-reference 100000

area 0.0.0.0

network 10.99.1.0 0.0.0.255

network 10.99.9.1 0.0.0.0

network 192.168.10.0 0.0.0.255

#

ip ip-prefix mpls\_yewu\_01 index 10 permit 192.168.10.0 24 #创建一条ip前缀匹配，匹配业务流量

**AR2配置：**

mpls lsr-id 10.99.9.2

mpls

#

mpls ldp

#

interface GigabitEthernet0/0/0

ip address 10.99.1.2 255.255.255.0

ospf ldp-sync

mpls

mpls ldp

#

interface GigabitEthernet0/0/1

ip address 10.99.2.1 255.255.255.0

ospf ldp-sync

mpls

mpls ldp

#

interface LoopBack0

ip address 10.99.9.2 255.255.255.255

#

ospf 1 router-id 10.99.9.2

bandwidth-reference 100000

area 0.0.0.0

network 10.99.1.0 0.0.0.255

network 10.99.2.0 0.0.0.255

network 10.99.9.2 0.0.0.0

**AR3配置：**

mpls lsr-id 10.99.9.3

mpls

lsp-trigger ip-prefix mpls\_yewu\_01

#

mpls ldp

#

interface GigabitEthernet0/0/0

ip address 10.99.2.2 255.255.255.0

ospf ldp-sync

mpls

mpls ldp

#

interface GigabitEthernet0/0/1

ip address 192.168.20.1 255.255.255.0

#

interface LoopBack0

ip address 10.99.9.3 255.255.255.255

#

ospf 1 router-id 10.99.9.3

bandwidth-reference 100000

area 0.0.0.0

network 10.99.2.0 0.0.0.255

network 10.99.9.3 0.0.0.0

network 192.168.20.0 0.0.0.255

#

ip ip-prefix mpls\_yewu\_01 index 10 permit 192.168.20.0 24

**AR1查看：**

<Huawei> disp mpls ldp session #查看ldp邻居会话状态

LDP Session(s) in Public Network

Codes: LAM(Label Advertisement Mode), SsnAge Unit(DDDD:HH:MM)

A '\*' before a session means the session is being deleted.

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

PeerID Status LAM SsnRole SsnAge KASent/Rcv

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

10.99.9.2:0 Operational DU Passive 0000:00:24 97/97

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

TOTAL: 1 session(s) Found.

<Huawei> disp mpls lsp #查看lsp转发表

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

LSP Information: LDP LSP

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

FEC In/Out Label In/Out IF Vrf Name

10.99.9.2/32 1024/3 -/GE0/0/0

192.168.20.0/24 1026/1026 -/GE0/0/0

192.168.10.0/24 3/NULL -/-

**★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的网络。

**★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（Virtual 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vpn的RD互不相同。

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

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iRT要与收到的路由信息中的eRT匹配，才会引入此路由

RT字段有8字节，其中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）

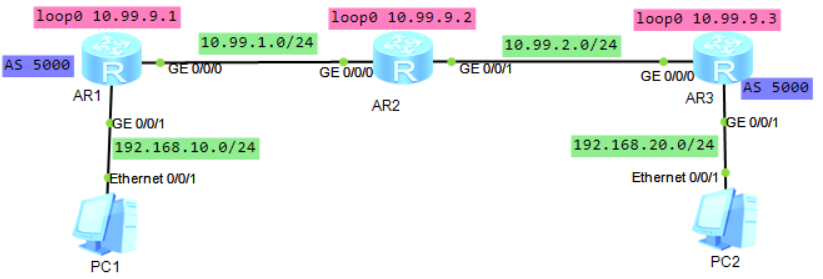
RT是BGP扩展团体属性，有2种类型

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

**实验：mpls\_VPN\_ar2240**



由于模拟器里的AR2240路由器不支持多个BGP实例，所以普通的底层路由协议使用ospf

mpls vpn使用BGP去宣告路由信息，仅AR1和AR3配置bgp实例，且为iBGP，使用Loopback0接口通信

**AR1配置：**

ip vpn-instance vpn100 #创建一个名为vpnxx的vpn实例（vrf）

ipv4-family

route-distinguisher 100:100 #配置RD，全局有效，一个vpn实例只可有一个RD

vpn-target 100:100 export-extcommunity #eRT全局有效

vpn-target 100:100 import-extcommunity # iRT，eRT可有多个

#

mpls lsr-id 10.99.9.1

mpls

#

mpls ldp

#

interface GigabitEthernet0/0/0

ip address 10.99.1.1 255.255.255.0

mpls

mpls ldp

#

interface GigabitEthernet0/0/1 #业务流量入口

ip binding vpn-instance vpn100 #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 address 192.168.10.1 255.255.255.0

#

interface LoopBack0

ip address 10.99.9.1 255.255.255.255

#

bgp 5000 #创建BGP进程，所有vpn实例相关信息借助bgp去传输

router-id 10.99.9.1

peer 10.99.9.3 as-number 5000

peer 10.99.9.3 connect-interface LoopBack0

#

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 10.99.9.3 enable #只和这些对等体之间交换vpn相关信息

#

ipv4-family vpn-instance vpn100 #在bgp里宣告vpn实例的路由信息

network 192.168.10.0 #宣告本vpn里的路由

#

ospf 1 router-id 10.99.9.1 # ospf进程用于普通路由的宣告，比如loopback0的ip宣告

bandwidth-reference 100000

area 0.0.0.0

network 10.99.1.0 0.0.0.255

network 10.99.9.1 0.0.0.0

**AR2配置：（AR2上面没有业务网段的路由）**

mpls lsr-id 10.99.9.2

mpls

#

mpls ldp

#

interface GigabitEthernet0/0/0

ip address 10.99.1.2 255.255.255.0

mpls

mpls ldp

#

interface GigabitEthernet0/0/1

ip address 10.99.2.1 255.255.255.0

mpls

mpls ldp

#

interface LoopBack0

ip address 10.99.9.2 255.255.255.255

#

ospf 1 router-id 10.99.9.2

bandwidth-reference 100000

area 0.0.0.0

network 10.99.1.0 0.0.0.255

network 10.99.2.0 0.0.0.255

network 10.99.9.2 0.0.0.0

**AR3配置：**

ip vpn-instance vpn100

ipv4-family

route-distinguisher 100:100

vpn-target 100:100 export-extcommunity

vpn-target 100:100 import-extcommunity

#

mpls lsr-id 10.99.9.3

mpls

#

mpls ldp

#

interface GigabitEthernet0/0/0

ip address 10.99.2.2 255.255.255.0

mpls

mpls ldp

#

interface GigabitEthernet0/0/1

ip binding vpn-instance vpn100

ip address 192.168.20.1 255.255.255.0

#

interface LoopBack0

ip address 10.99.9.3 255.255.255.255

#

bgp 5000

router-id 10.99.9.3

peer 10.99.9.1 as-number 5000

peer 10.99.9.1 connect-interface LoopBack0

#

ipv4-family vpnv4

policy vpn-target

peer 10.99.9.1 enable

#

ipv4-family vpn-instance vpn100

network 192.168.20.0

#

ospf 1 router-id 10.99.9.3

bandwidth-reference 100000

area 0.0.0.0

network 10.99.2.0 0.0.0.255

network 10.99.9.3 0.0.0.0

**AR1上查看：**

<Huawei> disp ip routing-table vpn-instance vpn100 #查看vpn实例对应的路由表

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

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

Routing Tables: vpn100

Destinations : 5 Routes : 5

Destination/Mask Proto Pre Cost Flags NextHop Interface

192.168.10.0/24 Direct 0 0 D 192.168.10.1 GigabitEthernet0/0/1

192.168.10.1/32 Direct 0 0 D 127.0.0.1 GigabitEthernet0/0/1

192.168.10.255/32 Direct 0 0 D 127.0.0.1 GigabitEthernet0/0/1

192.168.20.0/24 IBGP 255 0 RD 10.99.9.3 GigabitEthernet0/0/0 #下一跳为AR3

255.255.255.255/32 Direct 0 0 D 127.0.0.1 InLoopBack0

<Huawei> disp mpls lsp #查看lsp转发表

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

LSP Information: BGP LSP

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

FEC In/Out Label In/Out IF Vrf Name

192.168.10.0/24 1027/NULL -/- vpn100

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

LSP Information: LDP LSP

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

FEC In/Out Label In/Out IF Vrf Name

10.99.9.1/32 3/NULL -/-

10.99.9.2/32 NULL/3 -/GE0/0/0

10.99.9.2/32 1025/3 -/GE0/0/0

10.99.9.3/32 NULL/1029 -/GE0/0/0 #去往业务网段的流量下一跳为10.99.9.3，这里进行mpls封装

10.99.9.3/32 1026/1029 -/GE0/0/0

**AR2上查看：（transit节点）**

<Huawei> disp mpls lsp #查看lsp转发表

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

LSP Information: LDP LSP

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

FEC In/Out Label In/Out IF Vrf Name

10.99.9.1/32 NULL/3 -/GE0/0/0

10.99.9.1/32 1028/3 -/GE0/0/0

10.99.9.2/32 3/NULL -/-

10.99.9.3/32 NULL/3 -/GE0/0/1

10.99.9.3/32 1029/3 -/GE0/0/1

**★静态MPLS-TE**

MPLS TE（Traffic Engineering）流量工程，把多条LSP联合起来使用，并将这些LSP与一个虚拟隧道接口关联起来，这样的一组LSP称为MPLS TE隧道。

|  |  |
| --- | --- |
| 隧道接口 | 是为实现报文的封装而提供的一种点对点类型的虚拟接口 |
| 隧道标识 | （Tunnel ID）采用十进制数字来唯一标识一条MPLS TE隧道，以便对隧道进行规划和管理 |
| LSP标识 | （LSP ID）采用十进制数字来唯一标识一条LSP，以便对LSP进行规划和管理 |
| CR-LSP | MPLS TE隧道所使用的LSP称为基于一定约束条件建立的LSP，通常简称为CR-LSP（Constraint-based Routed Label Switched Path），这些约束条件可以称为隧道属性。 |

与普通LSP（比如LDP LSP）不同，CR-LSP的建立不仅依赖路由信息，还需要满足其他一些约束条件，这些约束条件包括带宽约束和路径约束两个方面: 1、受限标签路径（CR-LSP） 2、信息如何发布

TE信息的发布主要是依靠现有链路状态路由协议的扩展，包括OSPF TE和IS-IS TE。两种IGP路由协议会自动收集信息发布内容，并对这些信息进行泛洪，发布给MPLS TE网络中的其他节点。

★OSPF TE

OSPF是一种基于链路状态信息的路由协议，具有较强的扩展功能。OSPF定义了第1-5、7类的LSA来传递路由信息，并用于路由计算。但是这几种LSA的固定格式不能够适应MPLS TE的需求，因而出现了Opaque LSA和TE LSA扩展。

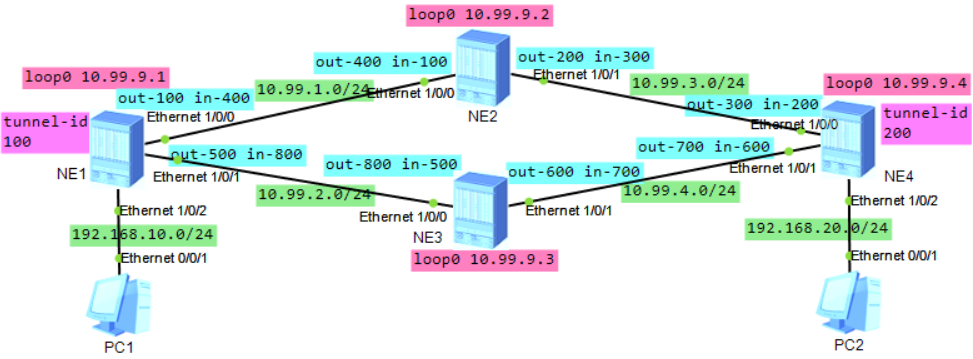
Opaque LSA分为三类，分别为第9、10、11类LSA。

第9类LSA只能在某一个接口上扩散；

第10类LSA只能在某一个区域内扩散；

第11类LSA则与第5类LSA具有相同的扩散范围，可以在除了STUB、NSSA之外的整个自治系统内部扩散。

**实验：mpls\_TE\_static\_ne40e**



**NE1配置：**

mpls lsr-id 10.99.9.1

#

mpls

mpls te

#

interface Ethernet1/0/0

undo shutdown

ip address 10.99.1.1 255.255.255.0

mpls

mpls te

dcn

dcn mode vlan

#

interface Ethernet1/0/1

undo shutdown

ip address 10.99.2.1 255.255.255.0

mpls

mpls te

dcn

dcn mode vlan

#

interface Ethernet1/0/2

undo shutdown

ip address 192.168.10.1 255.255.255.0

dcn mode vlan

#

interface LoopBack0

ip address 10.99.9.1 255.255.255.255

#

interface Tunnel0/0/0

ip address unnumbered interface LoopBack0

tunnel-protocol mpls te

destination 10.99.9.4

mpls te signal-protocol cr-static

mpls te tunnel-id 100

#

ip route-static 192.168.20.0 255.255.255.0 Tunnel0/0/0

#

static-cr-lsp ingress tunnel-interface Tunnel0/0/0 destination 10.99.9.4 nexthop 10.99.2.2 out-label 500 bandwidth ct0 0

#

static-cr-lsp egress lsp2 incoming-interface Ethernet1/0/0 in-label 400

static-cr-lsp egress lsp4 incoming-interface Ethernet1/0/1 in-label 800

#备用配置

static-cr-lsp ingress tunnel-interface Tunnel0/0/0 destination 10.99.9.4 nexthop 10.99.1.2 out-label 100

**NE2配置：**

mpls lsr-id 10.99.9.2

#

mpls

mpls te

#

interface Ethernet1/0/0

undo shutdown

ip address 10.99.1.2 255.255.255.0

mpls

mpls te

dcn

dcn mode vlan

#

interface Ethernet1/0/1

undo shutdown

ip address 10.99.3.1 255.255.255.0

mpls

mpls te

dcn

dcn mode vlan

#

interface LoopBack0

ip address 10.99.9.2 255.255.255.255

#

static-cr-lsp transit lsp1 incoming-interface Ethernet1/0/0 in-label 100 nexthop 10.99.3.2 out-label 200 bandwidth ct0 0

static-cr-lsp transit lsp2 incoming-interface Ethernet1/0/1 in-label 300 nexthop 10.99.1.1 out-label 400 bandwidth ct0 0

**NE3配置：**

mpls lsr-id 10.99.9.3

#

mpls

mpls te

#

interface Ethernet1/0/0

undo shutdown

ip address 10.99.2.2 255.255.255.0

mpls

mpls te

dcn

dcn mode vlan

#

interface Ethernet1/0/1

undo shutdown

ip address 10.99.4.1 255.255.255.0

mpls

mpls te

dcn

dcn mode vlan

#

interface LoopBack0

ip address 10.99.9.3 255.255.255.255

#

static-cr-lsp transit lsp3 incoming-interface Ethernet1/0/0 in-label 500 nexthop 10.99.4.2 out-label 600 bandwidth ct0 0

static-cr-lsp transit lsp4 incoming-interface Ethernet1/0/1 in-label 700 nexthop 10.99.2.1 out-label 800 bandwidth ct0 0

**NE4配置：**

mpls lsr-id 10.99.9.4

#

mpls

mpls te

#

interface Ethernet1/0/0

undo shutdown

ip address 10.99.3.2 255.255.255.0

mpls

mpls te

dcn

dcn mode vlan

#

interface Ethernet1/0/1

undo shutdown

ip address 10.99.4.2 255.255.255.0

mpls

mpls te

dcn

dcn mode vlan

#

interface Ethernet1/0/2

undo shutdown

ip address 192.168.20.1 255.255.255.0

dcn mode vlan

#

interface LoopBack0

ip address 10.99.9.4 255.255.255.255

#

interface Tunnel0/0/0

ip address unnumbered interface LoopBack0

tunnel-protocol mpls te

destination 10.99.9.1

mpls te signal-protocol cr-static

mpls te tunnel-id 200

#

ip route-static 192.168.10.0 255.255.255.0 Tunnel0/0/0

#

static-cr-lsp ingress tunnel-interface Tunnel0/0/0 destination 10.99.9.1 nexthop 10.99.4.1 out-label 700 bandwidth ct0 0

#

static-cr-lsp egress lsp1 incoming-interface Ethernet1/0/0 in-label 200

static-cr-lsp egress lsp3 incoming-interface Ethernet1/0/1 in-label 600

备用配置：

static-cr-lsp ingress tunnel-interface Tunnel0/0/0 destination 10.99.9.1 nexthop 10.99.3.1 out-label 300

**NE1查看：**

<HUAWEI> display tunnel-info all

Tunnel ID Type Destination Status

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

0x000000000300000001 te 10.99.9.4 UP

<HUAWEI> disp mpls te tunnel

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

Ingress LsrId Destination LSPID In/OutLabel R Tunnel-name

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

10.99.9.1 10.99.9.4 0 -/500 I Tunnel0/0/0

- - - 400/- E lsp2

- - - 800/- E lsp4

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

R: Role, I: Ingress, T: Transit, E: Egress

<HUAWEI> disp mpls lsp

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

LSP Information: STATIC CRLSP

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

FEC In/Out Label In/Out IF Vrf Name

10.99.9.4/32 NULL/500 -/Ethernet1/0/1

-/32 400/NULL Ethernet1/0/0/-

-/32 800/NULL Ethernet1/0/1/-

<HUAWEI> disp mpls static-cr-lsp

TOTAL : 3 STATIC CRLSP(S)

UP : 3 STATIC CRLSP(S)

DOWN : 0 STATIC CRLSP(S)

Name FEC I/O Label I/O If Status

Tunnel0/0/0 10.99.9.4/32 NULL/500 -/Ethernet1/0/1 Up

lsp2 -/32 400/NULL Ethernet1/0/0/- Up

lsp4 -/32 800/NULL Ethernet1/0/1/- Up

**NE2查看：**

<HUAWEI> disp mpls static-cr-lsp

TOTAL : 2 STATIC CRLSP(S)

UP : 2 STATIC CRLSP(S)

DOWN : 0 STATIC CRLSP(S)

Name FEC I/O Label I/O If Status

lsp1 -/32 100/200 Ethernet1/0/0/Ethernet1/0/1 Up

lsp2 -/32 300/400 Ethernet1/0/1/Ethernet1/0/0 Up

**★动态MPLS-TE**

**实验：mpls\_TE\_ospf\_ar2240**

**实验：mpls\_TE\_isis\_ar2240**

**★DR-MPLS**

**实验：dr-mpls\_ne40e**

**★VXLAN**

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

**★VxLAN大二层网络隧道**

VxLAN是一种隧道技术，能在三层网络的基础上建立二层以太网络，vxlan的实现方法是将原始的以太网帧加上8字节的vxlan头部，再封装在一个UDP报文里，此报文目的端口为8472/udp，即对端的隧道终端服务监听8472/udp端口。

所以vxlan可以理解为 MAC帧over UDP，Linux内核在3.7.0版本才开始支持vxlan，但linux 3.7发布时，相关的vxlan标准未规定使用哪个端口号，所以大多数厂商使用8472/udp端口，后来IANA分配了4789/udp作为vxlan的目的端口

**VTEP**（Vxlan Tunnel End Point）vxlan隧道终端节点，实现vxlan报文的封装/解封装

**VxLAN头部：**

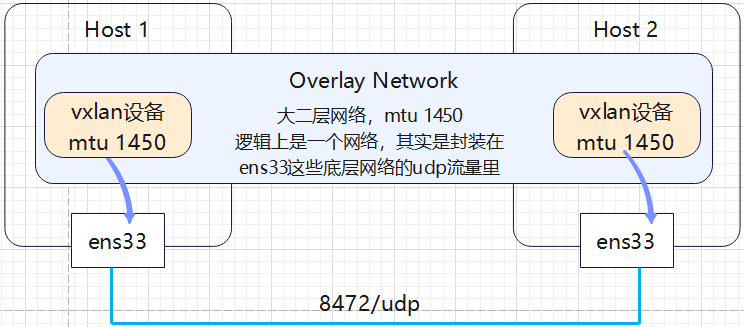
|  |  |  |  |
| --- | --- | --- | --- |
| 8 bit | 24 bit | 24 bit | 8 bit |
| vxlan tag | Reserved | VNI | Reserved |

VNI：（Vxlan Network Identifier），类似于vlan的id，vni区分一个vxlan虚拟overlay网络，vni有24bit，可表示16M个vxlan网络（即16777216个）

vxlan隧道底层网络的mtu如果是1500的话，那么vxlan要求被封装的报文网络mtu为1450

1500 - ( 20+8+8+14 ) = 1450 **所以vxan设备的mtu一般为1450**

20表示ip头，8为udp头，8为vxlan头，14为被封装流量的mac帧头（不带vlan tag）



**★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

#

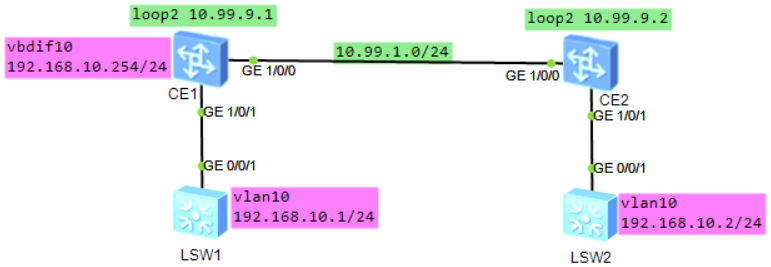
disp vxlan peer [ vni 1010 ]

disp vxlan vni 1010

disp vxlan tunnel

disp bridge-domain 10 [ brief ]

**实验：static\_vxlan\_ce12800**



**CE1配置：**

bridge-domain 10

vxlan vni 1010

#

interface Vbdif10

ip address 192.168.10.254 255.255.255.0

#

interface GE1/0/0

undo portswitch

undo shutdown

ip address 10.99.1.1 255.255.255.0

#

interface GE1/0/1.1 mode l2

encapsulation dot1q vid 10

bridge-domain 10

#

interface LoopBack2

description for\_vxlan\_nve\_id

ip address 10.99.9.1 255.255.255.255

#

interface Nve1

source 10.99.9.1

vni 1010 head-end peer-list 10.99.9.2

#

ip route-static 10.99.9.2 255.255.255.255 10.99.1.2

**CE2配置：**

bridge-domain 10

vxlan vni 1010

#

interface GE1/0/0

undo portswitch

undo shutdown

ip address 10.99.1.2 255.255.255.0

#

interface GE1/0/1.1 mode l2

encapsulation dot1q vid 10

bridge-domain 10

#

interface LoopBack2

description for\_vxlan\_nve\_id

ip address 10.99.9.2 255.255.255.255

#

interface Nve1

source 10.99.9.2

vni 1010 head-end peer-list 10.99.9.1

#

ip route-static 10.99.9.1 255.255.255.255 10.99.1.1

**LSW1配置：**

vlan batch 10

#

interface Vlanif10

ip address 192.168.10.1 255.255.255.0

#

interface GigabitEthernet0/0/1

port link-type trunk

port trunk allow-pass vlan 2 to 4094

**CE1查看：**

<HUAWEI> disp vxlan peer vni 1010

Number of peers : 1

Vni ID Source Destination Type Out Vni ID

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

1010 10.99.9.1 10.99.9.2 static 1010

<HUAWEI> disp vxlan tunnel

Number of vxlan tunnel : 1

Tunnel ID Source Destination State Type Uptime

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

4026531841 10.99.9.1 10.99.9.2 up static 00:14:47

<HUAWEI> disp bridge-domain 10

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

MAC\_LRN: MAC learning; STAT: Statistics; SPLIT: Split-horizon;

BC: Broadcast; MC: Unknown multicast; UC: Unknown unicast;

\*down: Administratively down; FWD: Forward; DSD: Discard;

U: Up; D: Down;

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

BDID Ports

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

10 GE1/0/1.1(U)

BDID State MAC-LRN STAT BC MC UC SPLIT Description

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

10 up enable disable FWD FWD FWD disable

BDID VLANIDs

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

10

**★evpn-vxlan**

EVPN（Ethernet Virtual Private Network）是一种用于二层网络互联的VPN技术。EVPN技术采用类似于BGP/MPLS IP VPN的机制，在BGP协议的基础上定义了一种新的NLRI（Network Layer Reachability Information，网络层可达信息）即EVPN NLRI，EVPN NLRI定义了几种新的BGP EVPN路由类型，用于处在二层网络的不同站点之间的MAC地址学习和发布。

使用evpn进行vxlan隧道的自动发现与建立。EVPN为控制平面，底层数据转发平面使用VXLAN。

**★配置步骤**

1、首先配置各设备互连口的ip，这里省略【所有节点】

2、规划3个loopback接口ip【所有节点】

# leaf 1

interface LoopBack 0 # Loop0的ip用作bgp路由器id（underlay的路由协议）

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\_bgp\_router\_id

ip address 10.10.1.2 32

#

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

description for\_vxlan\_nve\_ip

ip address 10.10.1.3 32

#

commit

3、配置普通路由协议，如bgp或ospf，本例使用eBGP【所有节点】

# leaf 1

bgp 100

router-id 10.10.1.1

peer 10.2.1.2 as-number 200

peer 10.2.1.2 allow-as-loop

ipv4-family unicast

network 10.10.1.1 32

network 10.10.1.2 32

network 10.10.1.3 32

maximum load-balancing ebgp 32

#

commit

4、优化VXLAN网络负载【所有节点】

ip tunnel mode vxlan

assign forward nvo3 acl extend enable #配置VXLAN隧道模式并使能VXLAN的ACL扩展功能

assign forward nvo3 f-linecard compatibility enable #配置非增强模式下防止VXLAN流量不通功能

assign forward nvo3 ecmp hash enable #VXLAN报文通过ECMP等价路由时采用负载均衡效果优化

assign forward nvo3 eth-trunk hash enable #使能VXLAN报文通过聚合口时采用负载均衡效果优化

assign forward nvo3 hash-polarization enhanced enable #使能VXLAN IPv4报文哈希极化增强功能

assign forward nvo3 hash-polarization ipv6 enhanced enable #使能VXLAN IPv6报文哈希极化增强功能

commit

5、创建bridge-domain和vxlan业务接入口【仅leaf节点】

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 #匹配不打tag的流量（同一主接口上只能有一个子接口配置为untag）

bridge-domain 10 #将此子接口划入BD 10

#

commit

6、开启evpn功能（使能EVPN作VXLAN控制平面）【所有节点】

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

commit

7、创建vpn实例（vrf）【仅leaf节点】

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

8、创建evpn实例【仅leaf节点】

# 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

9、创建vxlan三层网关（分布式网关）【仅leaf节点】

# 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

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 #创建一个名为**arp-host-router1**的路由策略

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）

#

commit

10、leaf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**，如有必要，请配置Route-Reflect路由反射

#可以使用Spine节点充当RR反射器

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

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

#

commit

11、创建头端复制，nve封装接口【仅leaf节点】

interface Nve1

source 10.10.1.3

vni 10 head-end peer-list protocol bgp

#

commit

**实验：evpn\_vxlan\_ce12800\_new**



**evpn相关参数规划：**

xxxx表示相应网段对应的vlan号，4位数字，不足4位前面以0填充；本实验中业务vlan配置为1002

vpn实例名称为： vpn\_xxxx

bridge-domain编号为： 2xxxx

|  |  |  |  |
| --- | --- | --- | --- |
|  | vpn-instance | evpn | 说明 |
| vni | 3xxxx | 2xxxx |  |
| RD | 3xxxx:100 | 2xxxx:100 |  |
| iRT | 3xxxx:200 | 2xxxx:200 |  |
| eRT | 3xxxx:200 | 2xxxx:200 3xxxx:200 |  |

**Spine1配置：**

evpn-overlay enable

#

interface GE1/0/0

undo portswitch

undo shutdown

ip address 10.99.1.1 255.255.255.0

#

interface GE1/0/1

undo portswitch

undo shutdown

ip address 10.99.2.1 255.255.255.0

#

interface LoopBack0

description for\_bgp\_router\_id

ip address 10.99.7.1 255.255.255.255

#

interface LoopBack1

description for\_evpn\_bgp\_router\_id

ip address 10.99.8.1 255.255.255.255

#

interface LoopBack2

description for\_vxlan\_nve\_ip

ip address 10.99.9.1 255.255.255.255

#

bgp 100

router-id 10.99.7.1

group exter\_group\_leaf external

peer exter\_group\_leaf as-number 200

peer 10.99.1.2 group exter\_group\_leaf

peer 10.99.2.2 group exter\_group\_leaf

ipv4-family unicast

network 10.99.7.1 255.255.255.255

network 10.99.8.1 255.255.255.255

network 10.99.9.1 255.255.255.255

maximum load-balancing ebgp 32

#

#以下evpn\_bgp路由反射器配置，在模拟器里，不支持配置在evpn的bgp实例上

#bgp 5000 instance evpnxx

# router-id 10.99.8.1

# group evpn\_inter\_group\_leaf internal

# peer 10.99.8.3 group evpn\_inter\_group\_leaf

# peer 10.99.8.4 group evpn\_inter\_group\_leaf

# peer evpn\_inter\_group\_leaf connect-interface LoopBack1

# peer evpn\_inter\_group\_leaf reflect-client

# l2vpn-family evpn

# policy vpn-target

# peer evpn\_inter\_group\_leaf enable

# peer evpn\_inter\_group\_leaf advertise irb

**Spine2配置：**

evpn-overlay enable

#

interface GE1/0/0

undo portswitch

undo shutdown

ip address 10.99.3.1 255.255.255.0

#

interface GE1/0/1

undo portswitch

undo shutdown

ip address 10.99.4.1 255.255.255.0

#

interface LoopBack0

description for\_bgp\_router\_id

ip address 10.99.7.2 255.255.255.255

#

interface LoopBack1

description for\_evpn\_bgp\_router\_id

ip address 10.99.8.2 255.255.255.255

#

interface LoopBack2

description for\_vxlan\_nve\_ip

ip address 10.99.9.2 255.255.255.255

#

bgp 100

router-id 10.99.7.2

group exter\_group\_leaf external

peer exter\_group\_leaf as-number 200

peer 10.99.3.2 group exter\_group\_leaf

peer 10.99.4.2 group exter\_group\_leaf

ipv4-family unicast

network 10.99.7.2 255.255.255.255

network 10.99.8.2 255.255.255.255

network 10.99.9.2 255.255.255.255

maximum load-balancing ebgp 32

#

#以下路由反射器配置，在模拟器里，不支持配置在evpn的bgp实例上

#bgp 5000 instance evpnxx

# router-id 10.99.8.2

# group evpn\_inter\_group\_leaf internal

# peer 10.99.8.3 group evpn\_inter\_group\_leaf

# peer 10.99.8.4 group evpn\_inter\_group\_leaf

# peer evpn\_inter\_group\_leaf connect-interface LoopBack1

# peer evpn\_inter\_group\_leaf reflect-client

# l2vpn-family evpn

# policy vpn-target

# peer evpn\_inter\_group\_leaf enable

# peer evpn\_inter\_group\_leaf advertise irb

**Leaf1配置：**

evpn-overlay enable

#

ip vpn-instance vpn\_1002

ipv4-family

route-distinguisher 31002:100

vpn-target 31002:200 export-extcommunity

vpn-target 31002:200 import-extcommunity

vxlan vni 31002

#

bridge-domain 21002

vxlan vni 21002

evpn

route-distinguisher 21002:100

vpn-target 21002:200 export-extcommunity

vpn-target 31002:200 export-extcommunity

vpn-target 21002:200 import-extcommunity

#

interface Vbdif21002

ip binding vpn-instance vpn\_1002

ip address 192.168.10.1 255.255.255.0

mac-address 0000-0000-0001 #模拟器中给vbdif配置mac地址后，会导致流量不通，实体设备需要配置

arp timeout 60

arp proxy anyway enable

arp direct-route enable

arp direct-route preference 1

#

interface GE1/0/0

undo portswitch

undo shutdown

ip address 10.99.1.2 255.255.255.0

#

interface GE1/0/1

undo portswitch

undo shutdown

ip address 10.99.3.2 255.255.255.0

#

interface GE1/0/2

undo shutdown

#

interface GE1/0/2.1002 mode l2

encapsulation untag

bridge-domain 21002

#

interface LoopBack0

description for\_bgp\_router\_id

ip address 10.99.7.3 255.255.255.255

#

interface LoopBack1

description for\_evpn\_bgp\_router\_id

ip address 10.99.8.3 255.255.255.255

#

interface LoopBack2

description for\_vxlan\_nve\_ip

ip address 10.99.9.3 255.255.255.255

#

interface Nve1

source 10.99.9.3

vni 21002 head-end peer-list protocol bgp

#

bgp 200

router-id 10.99.7.3

group exter\_group\_spine external

peer exter\_group\_spine as-number 100

peer exter\_group\_spine allow-as-loop

peer 10.99.1.1 group exter\_group\_spine

peer 10.99.3.1 group exter\_group\_spine

ipv4-family unicast

network 10.99.7.3 255.255.255.255

network 10.99.8.3 255.255.255.255

network 10.99.9.3 255.255.255.255

maximum load-balancing ebgp 32

#

ipv4-family vpn-instance vpn\_1002

import-route direct route-policy arp-host-router1

maximum load-balancing 32

advertise l2vpn evpn

#

bgp 5000 instance evpnxx

router-id 10.99.8.3

#group evpn\_inter\_group\_spine internal #模拟器不支持在evpn的bgp实例上配置路由反射器

#peer evpn\_inter\_group\_spine connect-interface LoopBack1

#peer 10.99.8.1 group evpn\_inter\_group\_spine

#peer 10.99.8.2 group evpn\_inter\_group\_spine

peer 10.99.8.4 as-number 5000 #由于模拟器不支持，这里直接和另一leaf建立邻居

peer 10.99.8.4 connect-interface LoopBack1

l2vpn-family evpn

policy vpn-target

#peer evpn\_inter\_group\_spine enable

#peer evpn\_inter\_group\_spine advertise irb

peer 10.99.8.4 enable

peer 10.99.8.4 advertise irb

#

route-policy arp-host-router1 permit node 10

if-match ip-prefix arp-host-prefix1

apply community 10:10 #这个comm暂时没用上，先预留

#

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

**Leaf2配置：**

evpn-overlay enable

#

ip vpn-instance vpn\_1002

ipv4-family

route-distinguisher 31002:100

vpn-target 31002:200 export-extcommunity

vpn-target 31002:200 import-extcommunity

vxlan vni 31002

#

bridge-domain 21002

vxlan vni 21002

evpn

route-distinguisher 21002:100

vpn-target 21002:200 export-extcommunity

vpn-target 31002:200 export-extcommunity

vpn-target 21002:200 import-extcommunity

#

interface Vbdif21002

ip binding vpn-instance vpn\_1002

ip address 192.168.10.1 255.255.255.0

mac-address 0000-0000-0001

arp timeout 60

arp proxy anyway enable

arp direct-route enable

arp direct-route preference 1

#

interface GE1/0/0

undo portswitch

undo shutdown

ip address 10.99.2.2 255.255.255.0

#

interface GE1/0/1

undo portswitch

undo shutdown

ip address 10.99.4.2 255.255.255.0

#

interface GE1/0/2

undo shutdown

#

interface GE1/0/2.1002 mode l2

encapsulation untag

bridge-domain 21002

#

interface LoopBack0

description for\_bgp\_router\_id

ip address 10.99.7.4 255.255.255.255

#

interface LoopBack1

description for\_evpn\_bgp\_router\_id

ip address 10.99.8.4 255.255.255.255

#

interface LoopBack2

description for\_vxlan\_nve\_ip

ip address 10.99.9.4 255.255.255.255

#

interface Nve1

source 10.99.9.4

vni 21002 head-end peer-list protocol bgp

#

bgp 200

router-id 10.99.7.4

group exter\_group\_spine external

peer exter\_group\_spine as-number 100

peer exter\_group\_spine allow-as-loop

peer 10.99.2.1 group exter\_group\_spine

peer 10.99.4.1 group exter\_group\_spine

ipv4-family unicast

network 10.99.7.4 255.255.255.255

network 10.99.8.4 255.255.255.255

network 10.99.9.4 255.255.255.255

maximum load-balancing ebgp 32

#

ipv4-family vpn-instance vpn\_1002

import-route direct route-policy arp-host-router1

maximum load-balancing 32

advertise l2vpn evpn

#

bgp 5000 instance evpnxx

router-id 10.99.8.4

peer 10.99.8.3 as-number 5000

peer 10.99.8.3 connect-interface LoopBack1

#group evpn\_inter\_group\_spine internal #模拟器不支持在evpn的bgp实例上配置路由反射器

#peer evpn\_inter\_group\_spine connect-interface LoopBack1

#peer 10.99.8.1 group evpn\_inter\_group\_spine

#peer 10.99.8.2 group evpn\_inter\_group\_spine

l2vpn-family evpn

policy vpn-target

#peer evpn\_inter\_group\_spine enable

#peer evpn\_inter\_group\_spine advertise irb

peer 10.99.8.3 enable

peer 10.99.8.3 advertise irb

#

route-policy arp-host-router1 permit node 10

if-match ip-prefix arp-host-prefix1

apply community 10:10

#

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

**Leaf1查看：**

<HUAWEI> disp vxlan peer

Number of peers : 1

Vni ID Source Destination Type Out Vni ID

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

21002 10.99.9.3 10.99.9.4 dynamic 21002

<HUAWEI> disp vxlan vni 21002

VNI BD-ID State

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

21002 21002 up

<HUAWEI> disp bridge-domain 21002 verbose #查看BD广播域信息

Bridge-domain ID : 21002

Description :

State : Up

MAC Learning : Enable

Statistics : Disable

Broadcast : Forward

Unknown-unicast : Forward

Unknown-multicast : Forward

Split-horizon : Disable

Vxlan Vni : 21002

VSI :

EVPN :

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

Interface State

GE1/0/2.1002 up

<HUAWEI> disp arp

ARP Entry Types: D - Dynamic, S - Static, I - Interface, O - OpenFlow, RD - Redirect

EXP: Expire-time VLAN:VLAN or Bridge Domain

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

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

192.168.10.1 0000-0000-0001 I Vbdif21002 vpn\_1002

192.168.10.2 5489-98a4-5575 1 D/BD21002 10.99.9.4 vpn\_1002

192.168.10.3 5489-98e5-3d8f 1 D/BD21002 GE1/0/2.1002 vpn\_1002

10.99.1.2 3814-0903-0100 I GE1/0/0

10.99.1.1 3814-0901-0100 10 D GE1/0/0

10.99.3.2 3814-0903-0101 I GE1/0/1

10.99.3.1 3814-0902-0100 10 D GE1/0/1

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

Total:7 Dynamic:4 Static:0 Interface:3 OpenFlow:0 Redirect:0

<HUAWEI> disp bgp instance evpnxx evpn peer 10.99.8.4 verbose #查看evpn bgp对等体详细信息

<HUAWEI> disp bgp instance evpnxx evpn all routing-table #查看evpn bgp路由信息

<HUAWEI> disp bgp instance evpnxx evpn peer #查看evpn bgp对等体信息

BGP local router ID : 10.99.8.3

Local AS number : 5000

Total number of peers : 1

Peers in established state : 1

Peer V AS MsgRcvd MsgSent OutQ Up/Down State PrefRcv

10.99.8.4 4 5000 41 36 0 00:20:16 Established 2

**★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 | 0-16M | bridge-domain | 无 | vbdif | evpn-bgp |
| mpls | mpls label | 20 bit | 0-1M | 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（admin, 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

#注意，如果不指定frequency，则只进行一次nqa探测，不会周期探测

[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默认参数：

报文优先级：7（最高级）

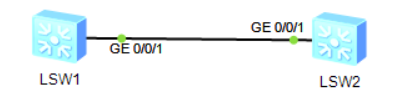
发送间隔：1000毫秒

接收间隔：1000毫秒

本地检测倍数：3

**★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、QoS服务质量**

**★Qos-DiffServ-MQC概念**

QoS服务质量（Quality of Service）是在发生网络拥塞时为不同的业务流量提供不同级别的质量保证，QoS是一个服务方案，当网络中2个主机通信时，只有当其流量经过的网络中所有设备都遵循统一的QoS服务模型时，才能实现端到端的服务质量保证。目前存在多种QoS服务模型，其中应用最广的是差分服务模型（Differentiated Services）

QoS涉及的4个部分：

|  |  |
| --- | --- |
| 流分类和标记 | Classification and Marking 将不同业务类型的流量标记为不同的优先级 |
| 流量监管和整形 | Policing and Shaping 将目标优先级的流量限制为某个特定的带宽，超过带宽的部分流量将被丢弃或缓存，将超过的流量丢弃的技术称为流量监管，将超过的流量缓存的技术称为流量整形 |
| 拥塞管理 | Congestion Management 当发生拥塞时，将报文放入相应的队列中缓存，并采取某种调度算法进行转发 |
| 拥塞避免 | Congestion Avoidance 当发现网络有拥塞加剧的趋势时采取主动丢弃报文的策略来解除网络过载 |

**★DiffServ差分服务模型**

差分服务模型（Differentiated Services）

DiffServ模型的基本原理是将网络中的流量分成多个类，当网络出现拥塞时不同的类会享受不同级别的处理。而同一类的业务在网络中会被聚合起来统一发送，保证相同的时延、抖动、丢包率等QoS指标。

流量入口设备可以通过多种条件灵活地对报文进行分类，对不同的报文设置不同的优先级，而其他设备只需要简单地识别报文中的这些优先级，即可进行资源分配和流量控制。

设备支持的QoS技术都是基于DiffServ服务模型的

QoS技术提供了如下报文分类的方式：

**★复杂流分类（MQC流分类）**

复杂流分类采用复杂的规则，如由五元组（源地址、源端口号、协议号码、目的地址、目的端口号）对报文进行精细的分类，并为同一类报文提供相同的QoS服务。复杂流分类可以通过模块化QoS命令行MQC（Modular QoS Command-Line Interface）中的流分类实现。

MQC包含三个要素，分别是流分类、流行为和流策略，三要素通过下面的方式配合使用完成对流量的处理：

|  |  |
| --- | --- |
| 1.配置流分类 | （traffic classifier）定义报文匹配规则 |
| 2.配置流行为 | （traffic behavior）确定报文处理动作。根据不同的流行为，可以实现不同的QoS功能 |
| 3.配置流策略 | （traffic policy）将配置好的流分类和流行为绑定到一起后在指定接口下应用流策略 |

流分类中各规则之间的关系分为：and或or，缺省情况下的关系为or。

流策略可绑定多个流分类和流行为

**流分类的使用注意事项：**

|  |  |
| --- | --- |
| 1 | 在流分类中匹配带vpn-instance的ACL规则时，会忽略其中的vpn-instance字段，即公网流量和私网流量都会匹配。若需要精确匹配私网流量，请在对应的三层接口上应用流策略 |
| 2 | 在流分类中匹配带外层VLAN ID的ACL规则并叠加了VLAN Mapping功能时：◾入方向匹配的是VLAN Mapping映射后的VLAN ID，出方向匹配的是VLAN Mapping映射前的VLAN ID |
| 3 | 流分类不支持匹配二层子接口的VLAN ID |
| 4 | 若在一个流分类中同时包含if-match any以及其他匹配规则，则实际生效的匹配字段取决于除if-match any外的匹配规则能够匹配到的具体报文类型 |

**流行为的使用注意事项：**

在同一流行为下同时配置重定向与其他流动作时，包含该流行为的流策略生效命中的报文以重定向的生效范围为准。

**流策略的使用注意事项：**

|  |  |
| --- | --- |
| 1 | 在三层主接口下应用的流策略，对三层子接口的流量也能生效 |
| 2 | 在同一接口同一方向下应用2个流策略（假设先应用的流策略是p1，后应用的流策略是p2）的情况下，若去应用先配置的流策略p1，然后再重新应用流策略（可以是p1，也可以是其他的流策略），则流策略p2会失效一段时间，且重新应用的流策略的实际生效时间相对配置提交时间会有延时。 |
| 3 | 当在某一接口下，需要同时匹配同一类报文（如二层报文、IPv4报文、IPv6报文等）的多个字段时，请在该接口下应用1个流策略，并在该流策略中指定多个流分类及其所需的流行为。若需要同时匹配IPv4报文和IPv6报文，请为这两类报文分别创建1个流策略 |

**★简单流分类（QoS优先级分类）**

简单流分类就是指采用简单的规则，根据报文中的某个优先级字段，对报文进行粗略的分类。优先级的概念如下：

|  |  |
| --- | --- |
| 外部优先级 | 又称为报文优先级、QoS优先级，即使用报文中某些特定字段比如VLAN报文的802.1p值、IP报文的DSCP值等记录QoS信息。需要注意的是，设备只可以根据设备内部优先级处理收到的报文，为不同的业务提供不同的QoS服务，所以上述外部优先级在进入设备后会映射为设备内部的优先级。 |
| 内部优先级 | 又称为服务等级（Class of Service）、PHB行为（Per Hop Behavior）、本地优先级，支持8种取值，优先级从高到低依次为CS7、CS6、EF、AF4、AF3、AF2、AF1、BE，与出端口的8个队列从高到低依次对应。因此内部优先级决定了报文在设备内部所属的队列。当针对某一个队列配置QoS业务时，即对所有通过该队列转发的报文都设置了相同的QoS服务。 |
| 丢弃优先级 | 又称为颜色（Color），是指报文在设备内部的丢弃优先级，用于决定当一个队列发生拥塞时报文的丢弃顺序，对内部优先级与队列的映射关系没有影响，丢弃优先级有3种取值，IEEE定义的优先级从低到高依次为Green、Yellow、Red。缺省情况下，丢弃优先级越高，则队列发生拥塞时，对应优先级的报文会被优先丢弃。  然而报文是否会被优先丢弃实际取决于参数的配置。例如，配置WRED丢弃模板中Green最大只能使用50%缓存，Red最大可以使用100%缓存，则队列发生拥塞时，标记为Green的报文将比标记为Red的报文优先丢弃。 |

设备在处理QoS业务时，在端口入方向将报文的外部优先级映射到合适的内部优先级和丢弃优先级，在端口出方向将内部优先级和丢弃优先级映射到外部优先级。

**★调整外部与内部优先级的映射关系的方法：**

|  |  |
| --- | --- |
| 报文重标记配置 | 基于MQC方式，在流行为中使用重标记行为，将报文的优先级或者标志位进行设置，重新定义报文的外部优先级。 |
| 优先级映射配置 | 在DiffServ模型中，设备定义了DiffServ域来管理和记录外部优先级与内部优先级、丢弃优先级之间的映射关系，不同DiffServ域允许有不同的优先级映射关系。优先级映射通过配置DiffServ域来设定不同的优先级映射关系，从而实现不同的QoS服务。 |

**★PHB行为（内部优先级）**

在每一个DS节点上对报文的处理称为PHB。PHB描述了DS节点对报文采用的外部可见的转发行为。PHB可以用优先级来定义，也可以用一些可见的服务特征如报文延迟、抖动或丢包率来定义。PHB只定义了一些外部可见的转发行为，没有指定特定的实现方式。RFC定义了四种标准的PHB：

|  |  |
| --- | --- |
| CS（Class Selector） | 可以细分为CS7和CS6，CS代表的服务等级与网络中使用的IP Precedence相同。在所有标准PHB中，CS的优先级最高。 |
| EF（Expedited Forwarding） | EF被定义为这样的一种转发处理：从任何DS节点发出的信息流速率在任何情况下必须获得等于或大于设定的速率。EF PHB在DS域内不能被重新标记，仅允许在边界节点重新标记。EF流要求低时延、低抖动、低丢包率，对应于实际应用中的视频、语音、会议电视等实时业务。 |
| AF（Assured Forwarding） | 可以细分为AF4、AF3、AF2、AF1  AF的推出是为了满足这样的需求：用户在与ISP订购带宽服务时，允许业务量超出所订购的规格。对不超出所订购规格的流量要求确保转发的质量；对超出规格的流量将降低服务待遇继续转发，而不只是简单地被丢弃。 |
| BE（Best-Effort） | BE对应于传统的IP报文投递服务，只关注可达性，其他方面不做任何要求。任何交换机必须支持BE PHB |

**★TP流量监管**

流量监管（Traffic Policing）是指对进入设备的流量进行监控，确保其没有滥用网络资源。通过监控进入网络的某一流量的规格，限制它在一个允许的范围之内，若某个连接的报文流量过大，就丢弃报文，或重新设置该报文的优先级（比如限制HTTP报文不能占用超过50%的网络带宽），以保护网络资源和运营商的利益不受损害。

运营商之间都签有服务水平协议（SLA），其中包含每种业务流的承诺速率CIR（Committed Information Rate）、峰值速率PIR（Peak Information Rate）、承诺突发尺寸CBS（Committed Burst Size）、峰值突发尺寸PBS（Peak Burst Size）等流量参数，对超出SLA约定的流量报文可指定给予pass（通过）、drop（直接丢弃）或markdown（降级）等处理，此处降级是指降低服务等级（Service Class），或者是提高丢弃等级（Color），即报文在网络拥塞时将被优先丢弃，从而保证在SLA约定范围之内的报文享受到SLA预定的服务。

流量监管采用承诺访问速率CAR（Committed Access Rate）来对流量进行控制。CAR使用令牌桶算法进行流量速率的评估，依据评估结果，实施预先设定好的监管动作。对应于SLA预定的处理动作，流量监管动作包括：

|  |  |
| --- | --- |
| 转发（pass） | 对测量结果不超过CIR的报文通常处理为继续正常转发 |
| 丢弃（discard） | 对测量结果超过PIR的报文通常进行丢弃 |
| 重标记（remark） | 对处于承诺速率（CIR）与峰值速率（PIR）之间的流量通常执行Remark动作，此时的报文不丢弃，而是通过Remark降低优先级进行尽力而为转发 |

**★MQC应用**

**★traffic-policy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>

**★traffic-policy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-class2] if-match acl 3001 #匹配数据，用acl限定

[Huawei-classifier-class2] quit

[Huawei] traffic behavior behav2 #定义流行为

[Huawei-behavior-behav2] statistics enable #流量统计

[Huawei-behavior-behav2] quit

[Huawei] traffic policy policy2 #定义流策略

[Huawei-trafficpolicy-policy2] classifier class2 behavior behav2 precedence 5 #匹配流类及流行为

[Huawei-trafficpolicy-policy2] quit

[Huawei]

[Huawei] int g0/0/3

[Huawei-GigabitEthernet0/0/3] traffic-policy policy2 inbound #在接口上使用策略

[Huawei-GigabitEthernet0/0/3] traffic-policy policy2 outbound #2个方向上都可应用

[Huawei-GigabitEthernet0/0/3] quit

<Huawei> disp traffic-policy applied-record policy2 #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

**★traffic-policy策略路由**

PBR（Policy-Based Routing）策略路由的操作对象是数据包（用于转发平面），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，在数据包进入路由转发层之前进行控制。

[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] quit

[Huawei] traffic classifier class3 #定义流类

[Huawei-classifier-class3] if-match acl 2000 #匹配acl，该acl匹配目标流量

[Huawei-classifier-class3] quit

[Huawei] traffic behavior behav3 #定义流行为

[Huawei-behavior-behav3] redirect ip-nexthop 10.1.1.1 #指定下一跳

[Huawei-behavior-behav3] quit

[Huawei] traffic policy policy3 #定义流策略

[Huawei-trafficpolicy-policy3] classifier class3 behavior behav3 #匹配相应的类和行为

[Huawei-trafficpolicy-policy3] quit

[Huawei] int g0/0/1

[Huawei-GigabitEthernet0/0/1] traffic-policy policy3 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: policy3

Policy Index: 0

Classifier:class3 Behavior:behav3

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

\*interface GigabitEthernet0/0/1

traffic-policy policy3 inbound

slot 0 : success

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

**PBR另一种写法（不使用MQC）：**

policy-based-route pbr\_test1 permit node 10 #创建一条名为pbr\_test1的PBR

if-match acl 2000 #匹配acl

apply ip-address next-hop 10.99.1.2 #指定下一跳ip

#

ip local policy-based-route pbr\_test1 #全局应用此策略路由

# 或者单独应用到某个接口下

int g0/0/0

ip policy-based-route pbr\_test1

[Huawei] disp policy-based-route pbr\_test1 verbose #查看策略路由应用情况

**★traffic-policy重标记报文优先级**

[Huawei] traffic classifier class4 #定义流类

[Huawei-classifier-class4] if-match dscp 36 #匹配ip报文中的dscp

[Huawei-classifier-class4] quit

[Huawei] traffic behavior behav4 #定义流行为

[Huawei-behavior-behav4] remark dscp 46 #重新标记dscp值为46

[Huawei-behavior-behav4] quit

[Huawei] traffic policy policy4 #定义流策略

[Huawei-trafficpolicy-policy4] classifier class4 behavior behav4 #匹配相应的类和行为

[Huawei-trafficpolicy-policy4] quit

[Huawei] int g0/0/1

[Huawei-GigabitEthernet0/0/1] traffic-policy policy4 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

**★traffic-policy流量过滤**

[Huawei] traffic classifier class1 #定义流类

[Huawei-classifier-class1] if-match acl 2000 #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] deny #禁止匹配到的流量通过

[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

为匹配ACL规则的报文指定报文过滤动作时，

如果此ACL中的rule规则配置为permit，则设备对此报文采取的动作由流行为中配置的deny或permit决定；

如果此ACL中的rule规则配置为deny，则无论流行为中配置了deny或permit，此报文都被丢弃。

**★DiffServ应用**

**★DiffServ优先级默认映射关系**

|  |  |  |  |
| --- | --- | --- | --- |
| PHB行为（内部优先级） | 802.1p优先级 | mpls EXP优先级 | DSCP |
| BE | 0 | 0 | 0-7,9,11,13,15,17,19,21,23,25,27,29,  31,33,35,37,39,41-45,47,49-55,57-63 |
| AF1 | 1 | 1 | 8,10,12,14 |
| AF2 | 2 | 2 | 16,18,20,22, |
| AF3 | 3 | 3 | 24,26,28,30, |
| AF4 | 4 | 4 | 32,34,36,38 |
| EF | 5 | 5 | 40,46, |
| CS6 | 6 | 6 | 48 |
| CS7 | 7 | 7 | 56 |

★队列调度算法

|  |  |  |  |
| --- | --- | --- | --- |
| 算法 | 说明 | 优点 | 缺点 |
| FIFO | First In First Out | 实现机制简单，处理速度快 | 不能差别对待各优先级报文 |
| PQ | Priority Queuing | 高优先级报文优先转发 | 低优先级队列可能会出现“饿死”现象 |
| WRR | Weighted Round Robin | 避免了PQ调度算法易出现的“饿死”现象 | 基于报文个数来调度，易出现包长尺寸不同的报文出现不平等调度，低时延业务得不到及时调度 |
| WFQ | Weighted Fair Queuing | 按照权重分配带宽，自动分类，配置简单 | 低时延业务得不到及时调度，无法实现用户自定义分类规则 |
| DRR | Deficit Weighted Round Robin |  |  |
| PQ+WFQ |  | 可保证低时延业务得到及时调度，实现按权重分配带宽 | 无法实现根据用户自定义灵活分类报文的需求 |
| CBQ | Class-Based Queuing | 支持自定义类，为不同的业务定义不同的调度策略 | 涉及复杂流分类，会耗费较多的系统资源 |

★队列装满后的处理方式

|  |  |
| --- | --- |
| 处理方式 | 说明 |
| Tail Drop | 尾丢弃，当某一队列被装满时，后续向该队列发送的报文全部丢弃，易引发TCP全局同步问题 |
| RED | 早期随机检测，在队列未装满前先随机丢弃一部分报文，预先降低一部分tcp连接的速度，避免TCP全局同步问题；无法对流量进行区分丢弃，易造成TCP饿死现象 |
| WRED | 对不同优先级队列设置相应的丢弃策略，对不同的流量进行区分丢弃 |

**★配置拥塞避免和拥塞管理**

1、重标记报文优先级（可选）

参考前面一小节：MQC应用→traffic-policy重标记报文优先级

2、创建diffserv domain并应用到入接口

[Switch] diffserv domain diffserv\_domain\_1

[Switch-dsdomain-ds1] 8021p-inbound 6 phb ef green #映射到5号队列

[Switch-dsdomain-ds1] 8021p-inbound 5 phb af3 yellow #映射到3号队列

[Switch-dsdomain-ds1] 8021p-inbound 2 phb af1 red #映射到1号队列

[Switch-dsdomain-ds1] quit

[Switch] interface gigabitethernet 0/0/3

[Switch-GigabitEthernet0/0/3] trust upstream diffserv\_domain\_1

[Switch-GigabitEthernet0/0/3] trust 8021p inner

[Switch-GigabitEthernet0/0/3] quit

3、创建丢弃模板并应用到出接口

[Switch] drop-profile drop\_profile\_wred\_1

[Switch-drop-wred1] color green low-limit 80 high-limit 100 discard-percentage 10

[Switch-drop-wred1] color yellow low-limit 60 high-limit 80 discard-percentage 20

[Switch-drop-wred1] color red low-limit 40 high-limit 60 discard-percentage 40

[Switch-drop-wred1] quit

[Switch] interface gigabitethernet 0/0/1

[Switch-GigabitEthernet0/0/1] qos wred drop\_profile\_wred\_1

[Switch-GigabitEthernet0/0/1] qos queue 5 wred drop\_profile\_wred\_1

[Switch-GigabitEthernet0/0/1] qos queue 3 wred drop\_profile\_wred\_1

[Switch-GigabitEthernet0/0/1] qos queue 1 wred drop\_profile\_wred\_1

[Switch-GigabitEthernet0/0/1] quit

[Switch] display diffserv domain name diffserv\_domain\_1

[Switch] display drop-profile name drop\_profile\_wred\_1

**创建队列调度模板并应用到出接口**

[Huawei] qos queue-profile queue\_profile\_1

[Huawei-qos-queue-profile-queue\_profile\_1] schedule pq 5 wrr 1 to 3

[Huawei-qos-queue-profile-queue\_profile\_1] quit

[Switch]

[Switch] interface gigabitethernet 0/0/1

[Switch-GigabitEthernet0/0/1] qos queue-profile queue\_profile\_1

[Switch-GigabitEthernet0/0/1] quit

[Huawei] disp qos queue-profile queue\_profile\_1 #查看

Queue-profile: queue\_profile\_1

Queue Schedule Weight Length(Bytes/Packets) GTS(CIR/CBS)

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

1 WRR 10 -/- -/-

2 WRR 10 -/- -/-

3 WRR 10 -/- -/-

5 PQ - -/- -/-

**★智能无损网络配置**

智能无损网络基于PFC机制提供了智能化拥塞控制技术，可以解决传统以太网络拥塞丢包、时延大的约束，为RoCEv2分布式应用提供“无丢包、低时延、高吞吐”的网络环境，满足分布式应用的高性能需求。

**★PFC反压通知↑**

PFC（Priority-based Flow Control）基于优先级的流量控制 也称为Per Priority Pause或CBFC（Class Based Flow Control），是对Pause机制的一种增强。以太网的Pause机制（IEEE 802.3 Annex 31B）也能达到无丢包的要求，原理如下：当下游设备发现接收能力小于上游设备的发送能力时，会主动发Pause帧给上游设备，要求暂停流量的发送，等待一定时间后再继续发送数据。但是以太Pause机制的流量暂停是针对整个接口，即在出现拥塞时会将链路上所有的流量都暂停。

而PFC允许在一条以太网链路上创建8个虚拟通道，并为每条虚拟通道指定一个优先等级，允许单独暂停和重启其中任意一条虚拟通道，同时允许其它虚拟通道的流量无中断通过。这一方法使网络能够为单个虚拟链路创建无丢包类别的服务，使其能够与同一接口上的其它流量类型共存。

当下游设备某个队列缓存消耗过快（收到数据过多）时就会向上游设备发送反压信号（PFC）信号（封装在mac帧中，上层协议类型为0x8808）

设备会为端口上的8个队列设置各自的PFC门限值，当队列已使用的缓存超过PFC门限值时，则向上游发送PFC反压通知报文，通知上游设备停止发包；当队列已使用的缓存降低到PFC门限值以下时，则向上游发送PFC反压停止报文，通知上游设备重新发包，从而最终实现报文的无丢包传输。

设备支持基于802.1p优先级的PFC和基于DSCP优先级的PFC：

（1）基于802.1p优先级的PFC：设备将报文中的802.1p优先级值与端口队列一一对应，即优先级值为0对应0号队列、优先级值为1对应1号队列，以此类推。

（2）基于DSCP优先级的PFC：设备根据配置的DiffServ域将报文中的DSCP优先级映射为内部优先级，内部优先级与端口队列一一对应

**★ECN显式拥塞通知↓**

当设备转发队列中的报文超过ECN门限时，设备会向宿端服务器发送携带ECN标记的报文以告知宿端设备网络中出现拥塞。宿端设备收到携带ECN标记的报文后，会向源端服务器发送**CNP拥塞通知报文**，以通知源端服务器进行流量降速。

传统的ECN（Explicit Congestion Notification）显式拥塞通知采用的是入队列标记方式。入队列标记方式是指报文在入队列时判断队列已使用的缓存是否超过ECN门限，若超过则在入队列的报文中打上ECN拥塞标记（将报文的ECN字段置为11）。再将报文按正常的出队列发出到下游设备，在网络拥堵严重的情况下，这种入队列标记方式容易造成队列拥堵恶化。

**快速ECN**拥塞标记采用的是出队列标记方式。它在报文出队列时判断队列已使用的缓存是否超过ECN门限，若超过则在出队列的报文中打上ECN拥塞标记（将报文的ECN字段置为11）。此时，设备给报文打上ECN拥塞标记与设备将携带ECN拥塞标记的报文转发出去同步进行，从而缩短了携带ECN拥塞标记报文在设备队列中的转发时间，使得宿端服务器能够尽快的收到携带ECN标记的报文。

**★CNP拥塞通知↑**

中间设备向目标主机发送ECN拥塞标记报文后，目标主机会向源主机发送CNP（Congestion Notification Packet）报文以通知源主机进行降速处理。

在中间设备（转发设备）上使能**快速CNP**拥塞通知功能后，转发设备会在转发报文时将报文的信息记录在流表表项中，并在后续收到携带ECN拥塞标记的报文时，基于学习到的流表表项信息向源端服务器发送CNP拥塞通知报文，缩短了拥塞反馈路径，从而及时调整源端服务器的流速，缓解转发设备缓存的拥塞。

即未经过目标主机，中间设备直接向源发送CNP报文，同时目标主机也会发送CNP报文，所以开通快速CNP功能后，可能会导致源主机过度降速。

**★配置过程**

dcb pfc pfc\_01 #创建一个名为pfc\_01的pfc模板

priority 4 #针对优先级4使能PFC优先级流量控制

priority 4 deadlock-detect time 1 #队列4开启pfc死锁检测，100毫秒

priority 4 deadlock-recovery time 1 #队列4 pfc死锁检测恢复时间，100毫秒

#

dcb pfc dscp-mapping enable slot 1 # slot 1上全局开启pfc功能

#

diffserv domain ds1 #创建一个名为ds1的diffserv domain

ip-dscp-inbound 36 phb af4 green #将入站报文中dscp值为36的报文映射为队列4

# IP报文中tos字段共8bit，分为6bit的dscp和2bit的ecn

#

interface 100ge 1/0/2

dcb pfc enable pfc\_01 mode manual #入接口上使能pfc功能，应用pfc\_01这个模板

trust dscp #使能PFC功能基于DSCP映射后的优先级进行反压

trust upstream ds1 #入接口上应用diffserv模板

dcb pfc buffer 3 xoff dynamic 6 hdrm 330 #手工配置无损队列的缓存空间优化功能，将Queue Headroom缓存空间增大为330 cells

#

low-latency fabric #配置低时延网络功能，开启后，需要重启交换机才生效

undo qos buffer auto-configuration enable #关闭无损队列的缓存空间自动优化功能（默认开启）

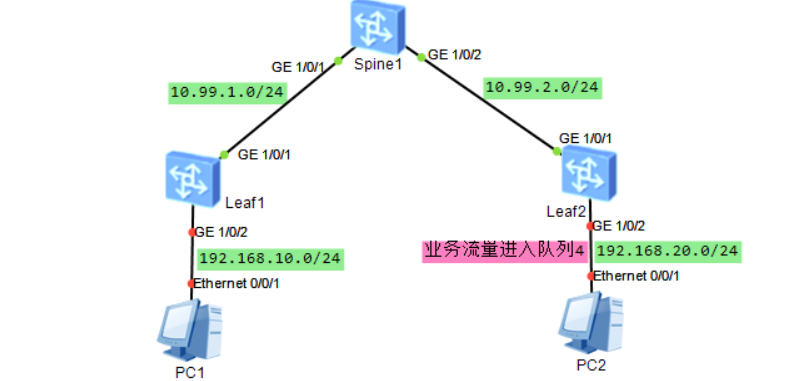
qos dynamic-ecn-threshold target-delay 30 mark-percentage 25 #使能动态ECN门限的无损队列的期望转发时延为30us，ECN标记概率为25

qos fast-cnp enable #使能快速CNP拥塞通知功能

qos fast-cnp aggregate-time 60 #配置设备向源端服务器发送CNP拥塞通知报文的聚合时间为60微秒

#

**实验：dcb\_pfc\_ce12800（模拟器不支持）**

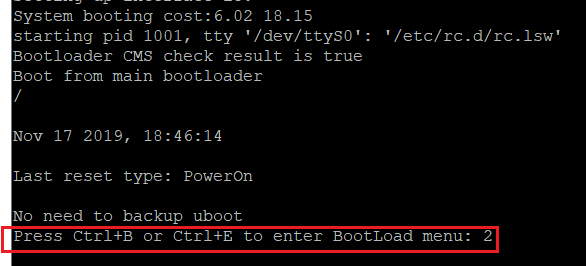


Leaf1配置：

**★第15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.

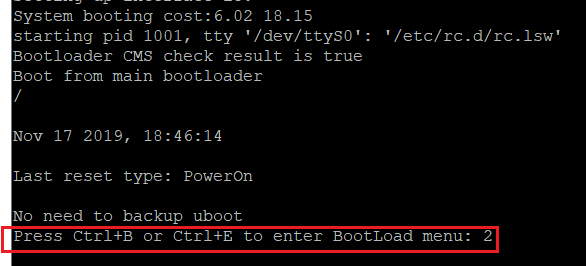
**初始化账号密码**：

s5735 账号 admin 密码 admin@huawei.com

ar2220 默认console密码 admin@huawei

**★维护模式传文件**

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

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): 3 #输入3，进入ethernet子菜单

ETHERNET SUBMENU

1. Download file to Flash through ethernet interface

**2. Modify ethernet interface boot parameter**

3. Return to main menu

Enter your choice(1-3): 2 #输入2，设置使用何种协议进行下载文件（下载到交换机上）

BOOTLINE SUBMENU

1. Set TFTP protocol parameters

**2. Set FTP protocol parameters**

3. Set SFTP protocol parameters

4. Return to ethernet menu

Enter your choice(1-4): 2 #输入2，设置ftp协议相关参数，如交换机的ip，ftp服务端ip以及要下载的文件名

Warning: FTP is not a secure protocol. SFTP is recommended.

'.' = clear field; '-' = go to previous field; 'Ctrl+D' = quit

Load File name : s5735\_back\_config.cfg #要通过ftp下载的文件名

Switch IP address : 192.168.2.2 #设置交换机管理口的ip，管理口ip要和ftp服务端ip在同一网段

Server IP address : 192.168.2.1 #ftp服务端ip

FTP User Name : cof #ftp用户名

FTP User Password : #ftp密码

Starting to write BOOTLINE into flash ... done

BOOTLINE SUBMENU

1. Set TFTP protocol parameters

2. Set FTP protocol parameters

3. Set SFTP protocol parameters

**4. Return to ethernet menu**

Enter your choice(1-4): 4 #输入4回到上一级菜单

ETHERNET SUBMENU

**1. Download file to Flash through ethernet interface**

2. Modify ethernet interface boot parameter

3. Return to main menu

Enter your choice(1-3): 1 #输入1开始下载文件

Use ftp to download file : s5735\_back\_config.cfg , please wait for a moment.

Download file successfully. #出现successfully表示下载文件成功

ETHERNET SUBMENU

1. Download file to Flash through ethernet interface

2. Modify ethernet interface boot parameter

3. Return to main menu

Enter your choice(1-3): 3 #输入3回到上一级菜单，然后可进行其他设置，比如进行startup子菜单设置启动系统文件

**★第16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

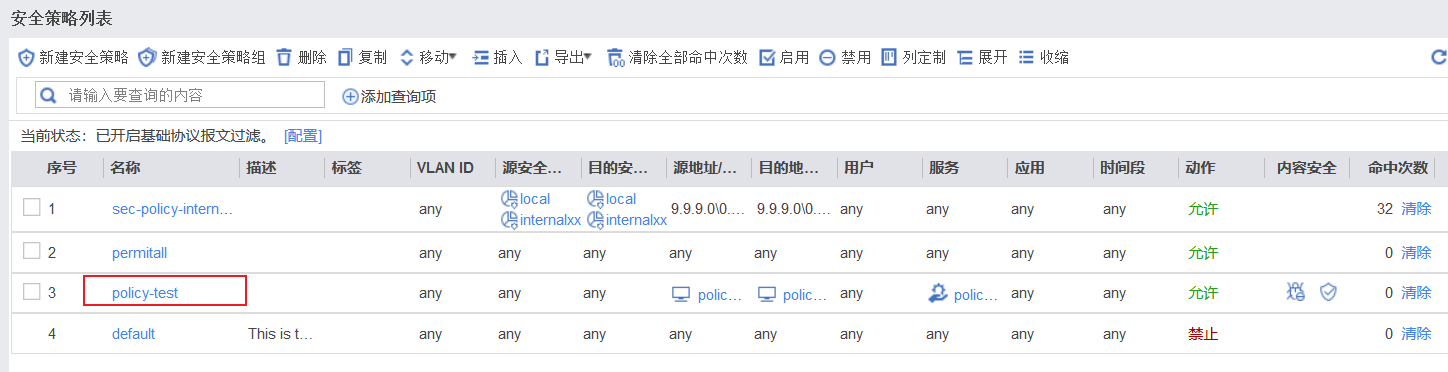
profile av default #反病毒

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

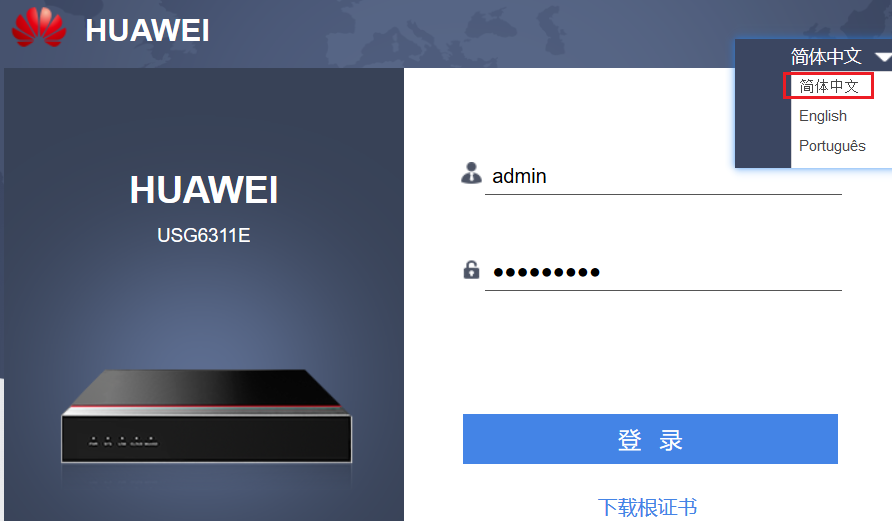
②接口配置ip并加入某个安全域

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**

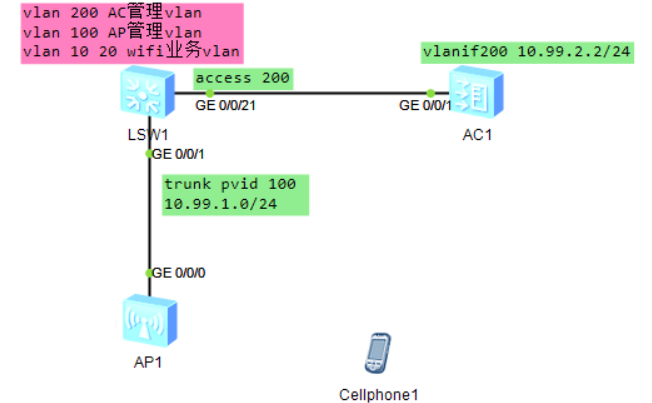
#FW提供Bypass接口对来实现硬件Bypass功能。当FW下电或者重启时，Bypass接口对将设备的上下游设备直接相连，使流量直接通过设备，而不做检测和拦截等任何处理，保证业务不中断；当故障排除后，所有流量恢复由设备处理后再发送，保证业务的安全性。

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

firewall feature-bypass ddos enable level 2 priority 2

**★第17章、WLAN配置**

**实验：WLAN\_AC6605**



**LSW1配置（做dhcp server）：**

vlan batch 10 20 100 200

#

dhcp enable

#

ip pool vlan10

gateway-list 192.168.10.1

network 192.168.10.0 mask 255.255.255.0

#

ip pool vlan20

gateway-list 192.168.20.1

network 192.168.20.0 mask 255.255.255.0

#

ip pool vlan100

gateway-list 10.99.1.1

network 10.99.1.0 mask 255.255.255.0

option 43 sub-option 2 ip-address 10.99.2.2

#

interface Vlanif10

ip address 192.168.10.1 255.255.255.0

dhcp select global

#

interface Vlanif20

ip address 192.168.20.1 255.255.255.0

dhcp select global

#

interface Vlanif100

ip address 10.99.1.1 255.255.255.0

dhcp select global

#

interface Vlanif200

ip address 10.99.2.1 255.255.255.0

#

interface GigabitEthernet0/0/1 #接AP的口

port link-type trunk

port trunk pvid vlan 100

port trunk allow-pass vlan 10 20 100

#

interface GigabitEthernet0/0/21 #接AC的口

port link-type access

port default vlan 200

#

**AC1配置：**

vlan batch 200

#

interface Vlanif200

ip address 10.99.2.2 255.255.255.0

#

ip route-static 0.0.0.0 0.0.0.0 10.99.2.1

#

[AC6605] capwap source interface Vlanif 200

[AC6605] vlan pool vlan\_pool\_Free-Wifi

[AC6605-vlan-pool-vlan\_pool\_Free-Wifi] vlan 10 20

[AC6605-vlan-pool-vlan\_pool\_Free-Wifi] assignment even #vlan分配算法，even或hash

[AC6605-vlan-pool-vlan\_pool\_Free-Wifi] quit

[AC6605] wlan

[AC6605-wlan-view] ssid-profile name ssid\_profile\_Free-Wifi

[AC6605-wlan-ssid-prof-ssid\_profile\_Free-Wifi] ssid Free-Wifi

[AC6605-wlan-ssid-prof-ssid\_profile\_Free-Wifi] quit

[AC6605-wlan-view]

[AC6605-wlan-view] security-profile name sec\_profile\_Free-Wifi

[AC6605-wlan-sec-prof-sec\_profile\_Free-Wifi] security wpa2 psk pass-phrase Paswd\_123 aes

[AC6605-wlan-sec-prof-sec\_profile\_Free-Wifi] quit

[AC6605-wlan-view]

[AC6605-wlan-view] vap-profile name vap\_profile\_Free-Wifi

[AC6605-wlan-vap-prof-vap\_profile\_Free-Wifi] service-vlan vlan-pool vlan\_pool\_Free-Wifi

[AC6605-wlan-vap-prof-vap\_profile\_Free-Wifi] ssid-profile ssid\_profile\_Free-Wifi

[AC6605-wlan-vap-prof-vap\_profile\_Free-Wifi] security-profile sec\_profile\_Free-Wifi

Warning: This action may cause service interruption. Continue?[Y/N] y

[AC6605-wlan-vap-prof-vap\_profile\_Free-Wifi] quit

[AC6605-wlan-view]

[AC6605-wlan-view] regulatory-domain-profile name domain\_cn

[AC6605-wlan-regulate-domain-domain\_cn] country-code CN

[AC6605-wlan-regulate-domain-domain\_cn] quit

[AC6605-wlan-view]

[AC6605-wlan-view] ap-group name ap\_group\_guest

[AC6605-wlan-ap-group-ap\_group\_guest] regulatory-domain-profile domain\_cn

Warning: Modifying the country code will clear channel, power and antenna gain c

onfigurations of the radio and reset the AP. Continue?[Y/N]: y

[AC6605-wlan-ap-group-ap\_group\_guest] vap-profile vap\_profile\_Free-Wifi wlan 1 radio 0 #wlan 1-16

[AC6605-wlan-ap-group-ap\_group\_guest] vap-profile vap\_profile\_Free-Wifi wlan 1 radio 1 #radio 0-2

[AC6605-wlan-ap-group-ap\_group\_guest] quit

[AC6605-wlan-view]

[AC6605-wlan-view] ap auth-mode mac-auth

[AC6605-wlan-view] ap-id 1 ap-mac 00e0-fc29-16e0 #添加AP，id 0-8191

[AC6605-wlan-ap-1] ap-name ap\_3F\_308\_C

[AC6605-wlan-ap-1] ap-group ap\_group\_guest

Warning: This operation may cause AP reset. If the country code changes, it will

clear channel, power and antenna gain configurations of the radio, Whether to c

ontinue? [Y/N]: y

[AC6605-wlan-ap-1] quit

[AC6605-wlan-view] quit

[AC6605]

**AC1查看：**

[AC6605] disp ap all

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

Total AP information:

idle : idle [1]

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

ID MAC Name Group IP Type State STA Uptime

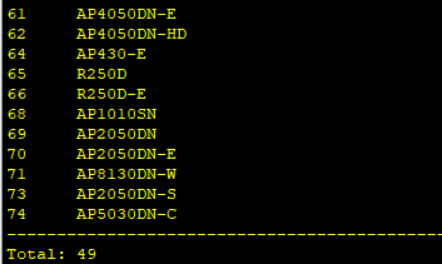
---------------------------------------------------------------------------------------------

1 00e0-fc29-16e0 ap\_3F\_308\_C ap\_group\_guest 10.99.1.254 AP4050DN-E nor 1 1M:25S

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

Total: 1

[AC6605] disp ap-type all #查看支持的AP型号



[AC6605] disp capwap configuration

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

Source interface : vlanif200

Source ip-address : -

Echo interval(seconds) : 25

Echo times : 6

Control priority(server to client) : 7

Control priority(client to server) : 7

Control-link DTLS encrypt : disable

DTLS PSK value : \*\*\*\*\*\*

PSK mandatroy match switch : disable

Control-link inter-controller DTLS encrypt : disable

Inter-controller DTLS PSK value : \*\*\*\*\*\*

IPv6 status : disable

Message-integrity PSK value : \*\*\*\*\*\*

Message-integrity check switch : enable

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

**AP查看mac等信息：**

<Huawei> disp system-information

System Information

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

Serial Number : 210235448310993CB66D

System Time : 2024-10-29 04:09:25

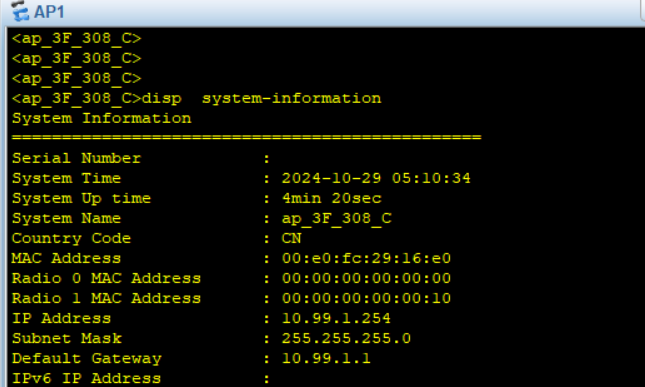
System Up time : 31min 6sec

System Name : Huawei

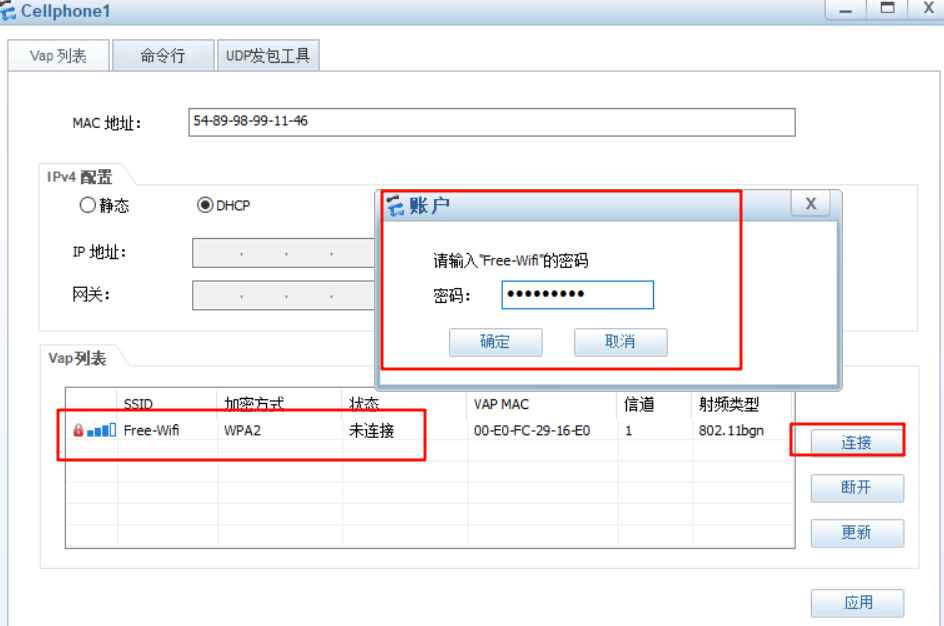
Country Code : US

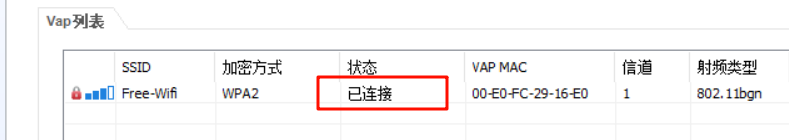
MAC Address : 00:e0:fc:29:16:e0

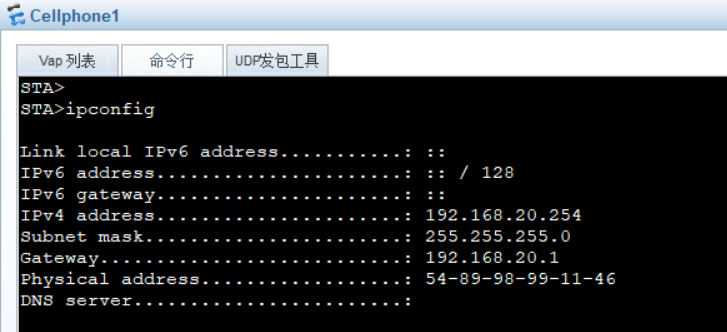
AP上线后，信息自动变更为配置的：

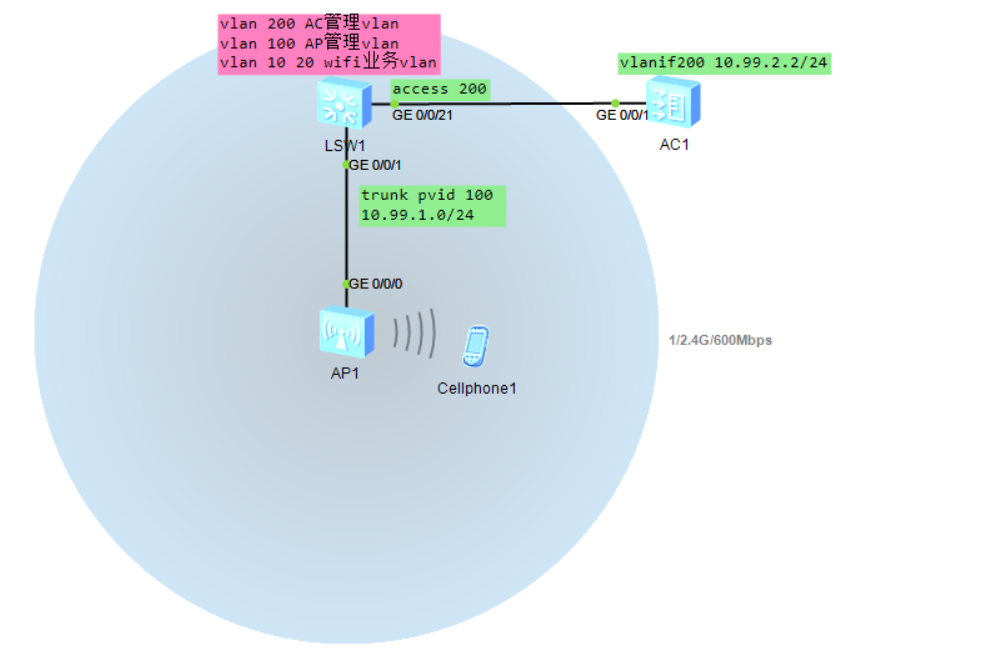


手机连接wifi：









**★附录（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**

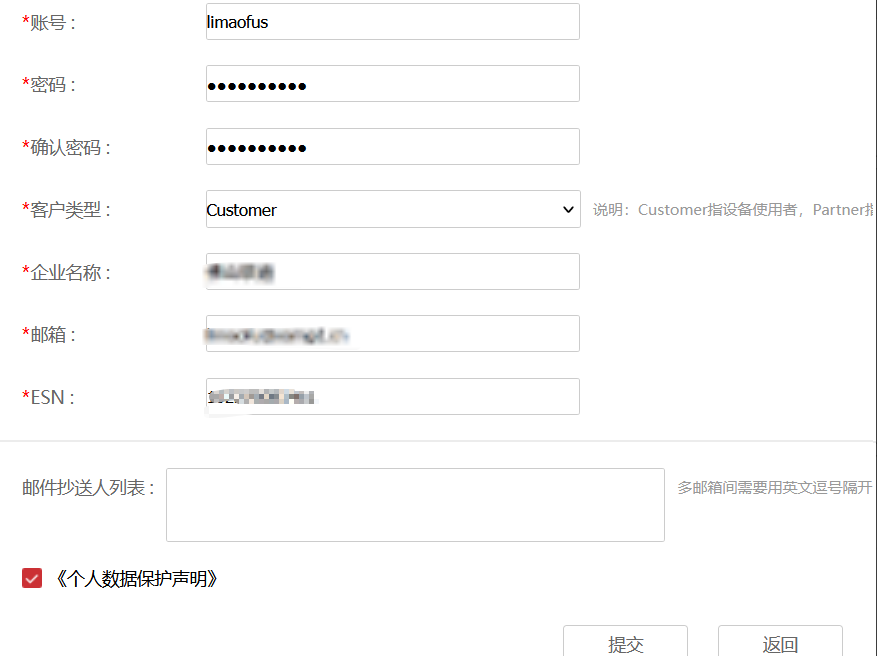
系统→升级中心，如果防火墙无法访问外网，可以点击本地升级，导入下载好的更新包

特征库更新包下载地址：

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



要先注册账号：



注册成功后，再根据目标防火墙的型号去下载相应版本的病毒库特征库等压缩包

**★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