### 思科路由与交换配置命令2.0

**前言：**

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

2.绿色字体表示注释，有时注释太多就不用绿色表示了

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

**版权声明**：

本文档以开源的形式发布，所有条款如下：

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

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

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

作者：李茂福

更新日期：2023-03-04

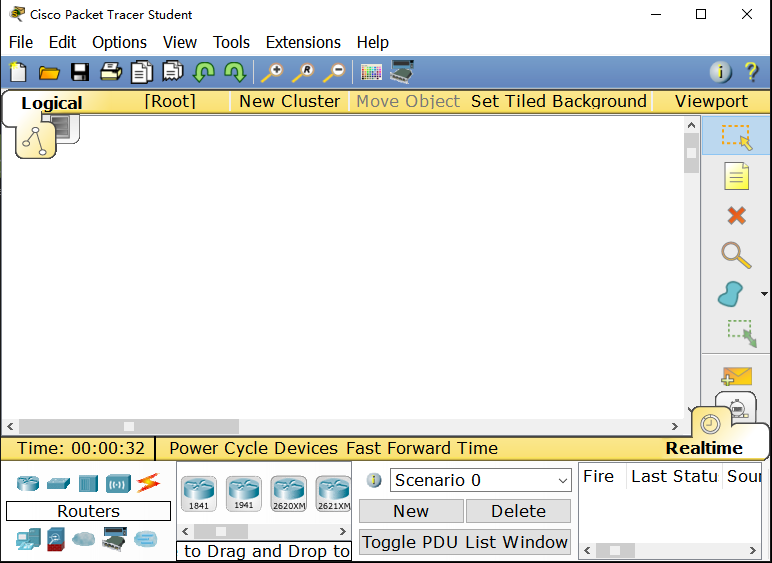
**0.安装思科模拟器**

思科的设备模拟器主要有2个：**GNS3**和**Packet Tracer**

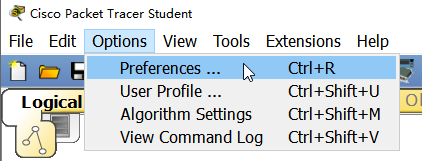
推荐使用Cisco Packet Tracer做交换机方面的配置，其他的配置推荐用GNS3，这两个软件可以到网上下载，然后安装。如果找不到的可以联系作者 sysyear@163.com

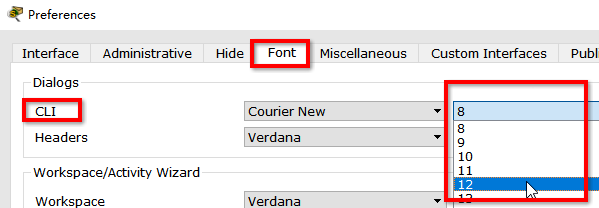


安装完后双击桌面上的图标打开模拟器（Packet Tracer主界面如下图）

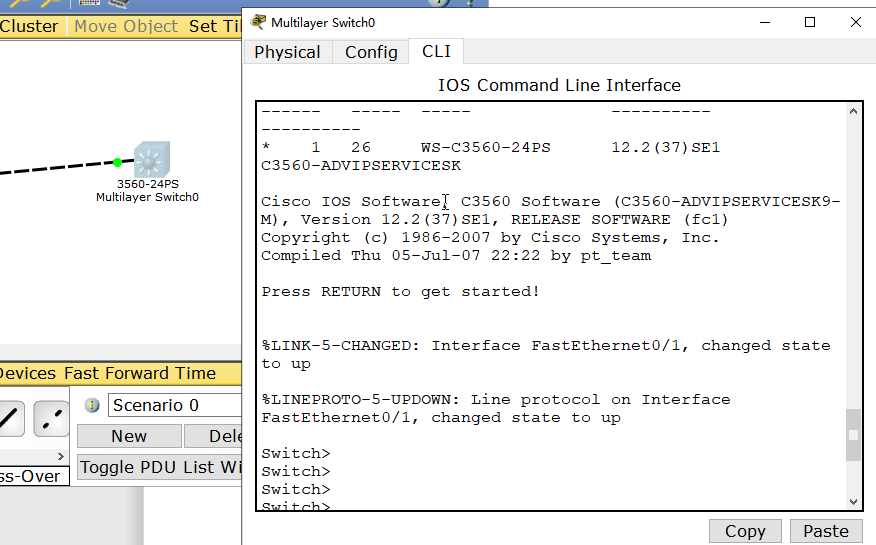


点击左下角的设备图标，拖入设备到主工作区，双击主工作区的图标即可进入命令行配置界面。默认字体太小了，可以设置字体大小：（点击菜单栏的Options，Preferences，Font选项卡里）





设置完字体就可以使用了，双击主工作区的设备图标，会弹出一个界面，点击新界面的CLI选项卡，就是命令行了。



初次进入命令行时会有如下提示：

Would you like to enter the initial configuration dialog? [yes/no]: no

#输入no表示不用系统给的初始化配置

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！！

**交换机的配置**

**1.初识命令行**

Switch> #刚开始进入的是一般模式，提示符为" > "

Switch> #提示符" > "前面的Switch为设备主机名称，可自定义

Switch> enable #输入enable，进入特权用户模式

Switch# #特权用户模式提示符为" # "

Switch# configure terminal #输入configure terminal进入配置模式

Enter configuration commands, one per line. End with CNTL/Z.

Switch(config)# #配置模式提示符前有(config)字样

Switch(config)# exit #输入exit可以退出当前模式

Switch#

Switch(config)# end #无论在何种模式何种配置界面下，输入end都会退出到#特权用户模式中

Switch# show running-config #查看正在运行的配置

Building configuration...

Current configuration : 1125 bytes

!

version 12.2

no service timestamps log datetime msec

no service timestamps debug datetime msec

no service password-encryption

!

hostname Switch #配置有很多行，一页显示不下，可以按空格键翻页

#如果不想看剩下的配置了，可以按Q键退出

Switch# write #确定运行的配置无误后，输入write保存配置

Building configuration...

[OK]

\*先配置一条：

Switch(config)# no ip domain-lookup #配置模式下输入此命令，关闭dns解析，一般路由与交换设备也不需要用到dns解析。关闭它的好处只有一个，那就是：我们在特权模式下输入一条错误（不存在）的命令时，系统不会花几分钟去解析它。不然每次输错命令都得等好几分钟。（系统会把不认识的命令当成域名去解析）需要解析时再打开。

\*路由与交换设备的系统一般都支持命令的简写，只要不产生歧义即可，比如：

Switch# conf t # configure terminal可以简写为conf t

Enter configuration commands, one per line. End with CNTL/Z.

Switch(config)#

Switch# sh r # show running-config可以简写为sh r

Building configuration...

Current configuration : 1145 bytes

!

version 12.2

#输入命令的前几个字母确认无二义后可以按下Tab键补全命令。

#当输错命令时，可以按下Ctrl和W键向前删除一个单词

#在配置命令时，一定要先确定是在哪个模式下进行的配置，看命令行的提示符

**章n、设备登录管理**

**★带内管理（console登录）**

**①仅密码**

Switch# conf ter #进入配置模式

Switch(config)# line con 0 #进入console线路的配置界面

Switch(config-line)# password 123456xx #设置密码

Switch(config-line)# login # login表示使用密码验证

Switch(config-line)# exit

Switch(config)#

**②用户名与密码**

Switch(config)# line con 0

Switch(config-line)# login local #使用本地用户名与密码验证

Switch(config-line)# exit

# 当然还可以使用其他的验证方案，暂时先不讲

# 配置完用户名与密码登录后，一定要记得去创建一个用户，请看下面的章节3.

**★带外管理**

**①Telnet仅密码**

Switch(config)# line vty 0 4 # vty 0~4是telnet登录的vty

Switch(config-line)# password 123xxx

Switch(config-line)# login

Switch(config-line)# exit

**②Telnet用户名与密码**

Switch(config)# line vty 0 4

Switch(config-line)# login local

Switch(config-line)# exit

**③SSH（仅支持用户名与密码的方式）**

Switch(config)# hostname Switch #先配置主机名

Switch(config)# ip domain-name xxx.com #域名也要配置

Switch(config)# crypto key generate rsa #创建rsa密钥

The name for the keys will be: Switch.xxx.com

Choose the size of the key modulus in the range of 360 to 2048 for your

General Purpose Keys. Choosing a key modulus greater than 512 may take

a few minutes.

How many bits in the modulus [512]: 2048 #使用2048位密钥

% Generating 2048 bit RSA keys, keys will be non-exportable...[OK]

Switch(config)# line vty 5 15 # vty 5~15为ssh登录的vty

\*3? 1 0:33:47.953: %SSH-5-ENABLED: SSH 1.99 has been enabled

Switch(config-line)# login local #使用本地的用户名与密码验证

Switch(config-line)# transport input ssh #允许ssh登录

Switch(config-line)# transport input ? #输入命令后空格，再输入问号?

#可以查看允许匹配的参数

all All protocols

none No protocols

ssh TCP/IP SSH protocol

telnet TCP/IP Telnet protocol

Switch(config-line)# transport input all #允许所有远程方式登录

Switch(config-line)#

**★创建用户**

Switch(config)# username coflee privilege 15 secret 0 123xxx #创建用户

#用户名为coflee，权限级别15，密码123xxx

Switch(config)# enable secret 0 123xxx #配置enable密码，必须配置

Switch(config)#

Switch(config)# service password-encryption #开启加密配置文件里的明文

#密码的功能

Switch(config)# exit

Switch# write #记得保存配置

**★登录超时设置**

Switch(config)# line con 0 #进入目标线路（console）

Switch(config-line)# exec-timeout 10 #超时时间10分钟

Switch(config-line)# exit #空闲时间达到10分钟后会断开连接

Switch(config)# line vty 0 15 #进入目标线路（远程）

Switch(config-line)# exec-timeout 15 #超时时间设为15分钟

Switch(config-line)# exi

**★系统时间设置**

Switch(config)# clock timezone cst 8 #先在配置模式下设置时区cst东8区

Switch(config)# exi # 退回特权模式

Switch# clock set 10:30:00 6 Dec 2019 #特权模式下配置时间日期

# 时分秒 日 月 年

Switch#

Switch# show clock #查看系统时间

18:30:3.739 cst Fri Dec 6 2019

Switch#

\*也可用ntp

Switch(config)# ntp authentication-key 1 md5 xxxx

Switch(config)# ntp server 10.1.1.22 key 1

**★重启/定时重启**

Switch# reload #立即重启系统

Proceed with reload? [confirm]y

Switch# reload at 23:30 8 Dec #定时重启，在12月8日的23:30

Reload scheduled for 23:30:00 UTC Sun Dec 8 2019 (in 54 hours and 41 minutes) by console

Reload reason: Reload Command

Proceed with reload? [confirm]y #确定

或者：

Switch# reload in 5:30 #定时重启，在5小时30分钟后

Reload scheduled for 22:20:55 UTC Fri Dec 6 2019 (in 5 hours and 30 minutes) by console

Reload reason: Reload Command

Proceed with reload? [confirm]y #确定

Switch# reload cancel #取消定时重启

**★查看登录的用户**

Switch# show users

Line User Host(s) Idle Location

\* 0 con 0 idle 00:00:00

3 vty 0 cof idle 00:00:03 10.1.1.2

Switch#

Switch# clear line 3 #把3号line（vty 0）的用户踢下线

**★AAA访问控制安全管理机制**

AAA的知识点很多，不过一般用不了那么多，感兴趣的可以研究一下

交换机路由器上运行的AAA是作为客户端运行的，这些交换机路由器也叫网络接入服务器

**aaa命令语法**：

Switch(config)# aaa 控制类型 目标 方案名称 认证类型

**控制类型**：Authentication认证，Authorization授权，Accounting计费

**目标**：login登录，dot1x，exec操作权限，network网络服务，ppp

**方案名称**：default默认的，也可自己命名新的方案，none表示无认证方案

**认证类型**：local本地，radius，tacacs，none不进行认证

例：

配置一条名为**default**的**认证**方案用于**登录**的，使用**本地**的用户名和密码认证

Switch(config)# aaa new-model #首次配置aaa要使用此命令，之后不用

Switch(config)# aaa authentication login default local #配置默认的认证方案

# aaa控制类型 目标 方案名 本地

Switch(config)#

\*配置完该默认（default）方案后，可以应用到远程登录和console登录里

Switch(config)# line con 0

Switch(config-line)# login authentication default #使用默认的认证方案

Switch(config-line)# exit

Switch(config)# line vty 0 4

Switch(config-line)# login authentication default

Switch(config-line)# exit

未完待续，一般也就是用aaa做登录认证和操作权限的授权，详见最后一章节

**★日志输出同步**

\*用console登录时，系统输出的消息有时会打断我们正在输入的命令

Switch(config)# line con 0

Switch(config-line)# logging synchronous #开启日志输出同步，这样就不会

#打断我们正在输入的命令了

Switch(config-line)# exit

\*用远程登录时，看不到console下的消息，

Switch(config)# terminal monitor #开启后就可以在远程登录界面看到

# console输出的消息了，这条命令在模拟器里没有

**★登录访问控制**

Switch(config)# line vty 0 4 #进入目标线路

Switch(config-line)# access-class 1 in #应用acl 1，只允许acl 1里匹配的

#网段或主机来登录本设备

Switch(config-line)# exit

**★登录后导语**

有时需要提醒下一次登录设备的管理员要注意的事项，可以配置一条登录后导语，就是在用户登录系统后，会输出一段话，这段话是由我们配置的。

Switch(config)# banner motd **$** #表示输入的导语以字符$结束，可以换行

Enter TEXT message. End with the character '$'.

Notice, bobo, please do not shutdown G0/0/3,

---- coflee

20191206**$** #以$作为结束标识，回车后退出

Switch(config)# line con 0

Switch(config-line)# motd-banner #在相应的线路开启banner

Switch(config-line)# exit

Switch(config)# line vty 0 15

Switch(config-line)# motd-banner

Switch(config-line)# exit

**★SNMP**

Switch(config)# snmp-server community pubxxx ro

%SNMP-5-WARMSTART: SNMP agent on host Switch is undergoing a warm start

Switch(config)#

**★CDP思科设备发现协议**

Switch(config)# int g0/1

Switch(config-if)# cdp enable #在端口上开启cdp功能

Switch(config-if)# exit

Switch(config)# cdp run #全局开启cdp功能

Switch# show cdp neighbors #查看cdp邻居

Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge

S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone

Device ID Local Intrfce Holdtme Capability Platform Port ID

Switch Gig 1/0/1 133 3650 Gig 1/0/1

Switch Gig 1/0/2 169 3650 Gig 1/0/6

自己这边的端口 邻居的端口

一条记录即为一个邻居设备

Switch# show cdp int g1/0/1 #查看端口上的cdp信息

GigabitEthernet1/0/1 is up, line protocol is up

Sending CDP packets every 60 seconds

Holdtime is 180 seconds

**章n、配置相关操作**

**★查看配置**

Switch# show startup-config #特权模式下查看配置文件

Switch# show running-config #查看正在运行的配置，同show configuration

以上两者的区别是：

|  |  |
| --- | --- |
| startup-config | 保存在设备存储器里的配置文件，对应**flash:/config.text**文件  如果有nvram:/设备，则在此设备下，是flash:/config.text的备份 |
| running-config | 正在运行的配置，在系统内存里，在system:/设备下 |

S3750-1# pwd

nvram:/

S3750-1# dir nvram:/

Directory of nvram:/

506 -rw- 3128 <no date> startup-config

507 ---- 1940 <no date> private-config

1 -rw- 0 <no date> ifIndex-table

2 -rw- 580 <no date> IOS-Self-Sig#3031.cer

S3750-1# dir system:/

Directory of system:/

2 -r-- 0 <no date> default-running-config

4 dr-x 0 <no date> memory

1 -rw- 4465 <no date> running-config

3 dr-x 0 <no date> vfiles

S3750-1(config)# do write #配置模式下默认没有特权模式下的操作命令

Building configuration... #可加上 do 去执行维护查看相关操作

[OK]

S3750-1(config)# do show running-config

S3750-1# show running-config interface vlan 1 #查看int vlan 1的配置

**★清除配置（谨慎操作）**

Switch# erase startup-config #清除配置文件，也可用erase nvram:

Erasing the nvram filesystem will remove all configuration files! Continue? [confirm]y

#输入y，确定

Erase of nvram: complete

%SYS-7-NV\_BLOCK\_INIT: Initialized the geometry of nvram

Switch#

Switch# delete vlan.dat #交换机还要删除vlan数据

Delete filename [vlan.dat]? #这里不要输入任何字符，直接回车

Delete flash:/vlan.dat? [confirm]y

Switch# show startup-config #这时查看配置文件，已经没有了

startup-config **is not** present

Switch#

Switch# show run #但是正在运行的配置还在内存里，所以需要重启系统

#有的教程上写着erase 之后还要write，这是不正确的

#如果这时write，正在运行的配置会保存到flash里

#相当于没有清除配置，所以erase之后直接重启

Building configuration...

Current configuration : 1523 bytes

!

version 12.2

enable secret 5 xxxx

Switch# reload #直接重启系统

Proceed with reload? [confirm]y #输入y，确定

**★直接删除配置文件**

Switch# delete flash:/config.text #直接删除flash里的配置文件

Delete filename [/config.text]? #这里不要输入，直接回车

Delete flash:/config.text? [confirm]y #输入y，确定

#然后可以重启，恢复出厂设置

**★备份配置**

Switch# copy running-config flash: #备份正在运行的配置到flash:/文件里

Destination filename [running-config]? confbak20191206.cfg #保存的文件名

Building configuration...

[OK]

Switch# dir

Directory of flash:/

3 -rw- 8662192 <no date> c3560-advipservicesk9-mz.122-37.SE1.bin

4 -rw- 1523 <no date> confbak20191206.cfg

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

64016384 bytes total (55096850 bytes free)

Switch#

#备份以后，可以在原来的基础上做其他的配置，如果出了问题就可以用备份的文件来恢复。可以参考下一节《启动文件配置》，建议将备份文件上传到ftp/tftp服务器上

**★启动文件配置**

Switch# show boot #查看启动时使用的是哪个系统镜像和配置文件

BOOT path-list : flash:c3750-ipbasek9-mz.122-50.SE4.bin

Config file : flash:/config.text

Private Config file : flash:/private-config.text

Enable Break : no

Manual Boot : no

HELPER path-list :

Auto upgrade : yes

Auto upgrade path :

Timeout for Config

Download: 0 seconds

Config Download

via DHCP: disabled (next boot: disabled)

Switch#

Switch(config)# boot system flash:/xxxxx.bin #指定使用的系统镜像文件

Switch(config)# boot config-file flash:/confback.cfg #指定使用的配置文件

#指定启动文件时一定要带上flash:/，默认是tftp: 会导致系统启动时找不到文件而失败，失败后再次以旧的系统镜像启动，如果旧的文件还在的话

#以上有的命令在模拟器里不支持

**★TFTP客户端**

Switch# copy startup-config tftp: #上传配置到服务器上

Address or name of remote host []? 10.1.1.251 #服务器ip

Destination filename [Switch-confg]? c3650.cfg #存到服务器上的文件名

Writing startup-config....

Switch# copy tftp: flash: #从tftp服务器下载文件到本地的flash上

Source filename []? c3650.cfg #服务器上的文件名

Address or name of remote host []? 10.1.1.251 #服务器ip

Destination filename [c3650.cfg]? bakconf.cfg #存到本地flash里的文件名

Writing c3650.cfg...

**★FTP客户端**

Switch(config)# ip ftp source-interface vlan 1 #指定访问服务器时的源接口

Switch(config)# ip ftp username coflee # ftp用户名

Switch(config)# ip ftp password xxxx # ftp用户密码，明文输入，明文保存

Switch(config)# exit

Switch# copy startup-config ftp: #上传配置到ftp服务器

Address or name of remote host []? 10.1.1.22 #服务器ip

Destination filename [Switch-confg]? c3650.cfg #指定存到服务器上的文件名

Writing startup-config...

**章n、堆叠配置**

**①傻瓜式配置**

1，master设备的stack1和backup设备的stack2相连线（专用堆叠线）

2，先启动master设备，不用做配置

3，后启动backup设备，不用做配置

4，2台设备会自动选举，亮master灯的就是主设备，从设备会同步主设备的配置

从设备原有配置丢失

S3750-7# show switch #查看堆叠设备情况

Switch/Stack Mac Address : 001d.a2f8.3c00

H/W Current

Switch# Role Mac Address Priority Version State

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

1 Member 001b.2b22.6800 1 0 Ready stack2

\*7 Master 001d.a2f8.3c00 15 0 Ready stack1

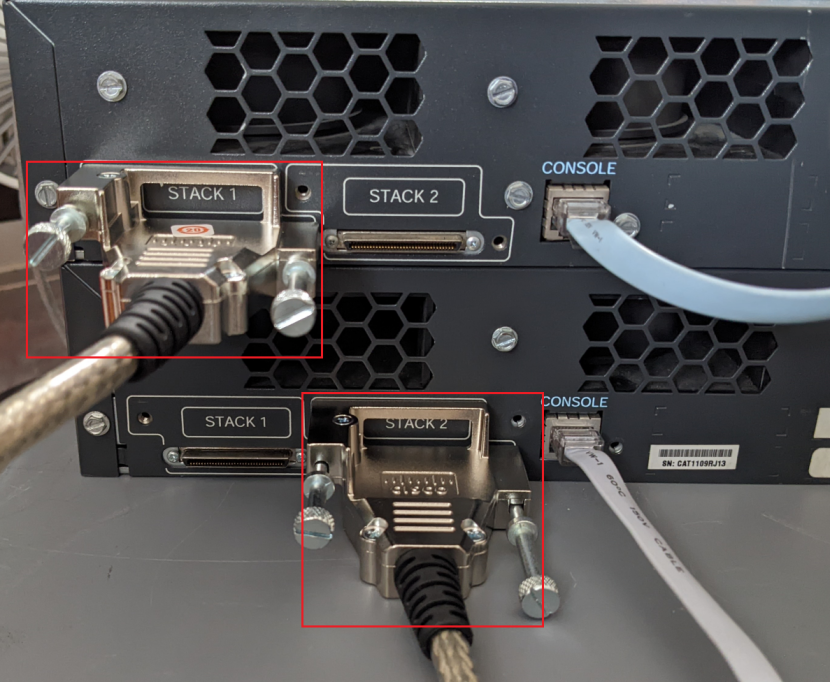
S3750-7# show switch stack-ports #查看堆叠设备的stack堆叠口情况

Switch # Port 1 Port 2

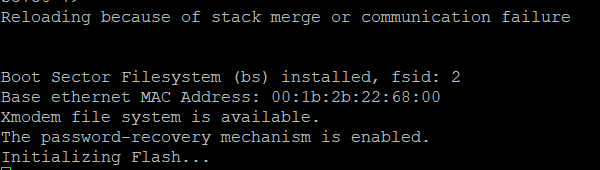
1 Down Ok #1号设备的Port2是接线的

7 Ok Down #7号设备的Port1是接线的

#下图的上面一台设备为switch7，下面一台为switch1



如果堆叠线断开，重新接上，则backup设备会重启！



**★当堆叠形成后，无论从哪台设备的console口登录，显示的都是master设备名称**

堆叠形成后，逻辑设备的mac地址为主设备的mac地址

S3750-1# show switch detail

Switch/Stack Mac Address : 001d.a2f8.3c00

H/W Current

Switch# Role Mac Address Priority Version State

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

\*1 Master 001d.a2f8.3c00 15 0 Ready

2 Member 001b.2b22.6800 12 0 Ready

**②手动配置**

switch(config)# switch 7 renumber 1 #将本设备的编号从7改为1

WARNING: Changing the switch number may result in a

configuration change for that switch.

The interface configuration associated with the old switch

number will remain as a provisioned configuration.

Do you want to continue?[confirm] #直接回车确认

Changing Switch Number 7 to Switch Number 1

New Switch Number will be effective after next reboot #需要重启才生效

switch(config)# switch 1 provision ws-c3750g-24ts #设置设备的型号

switch(config)# switch 1 priority 15 #设置本设备的堆叠优先级，越大越优先

Changing the Switch Priority of Switch Number 1 to 15 #优先级取值可为1~15

Do you want to continue?[confirm] #直接回车确认

New Priority has been set successfully

#再断电重启

#其他设备也类似操作，改下编号及优先级，优先级不要比master的高

#最后要记得接stack堆叠线

S3750-1# show switch neighbors #查看堆叠拓扑情况

Switch # Port 1 Port 2

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

1 2 None

2 None 1

★如果堆叠裂开，成员设备配置信息还在，不会自动删除

如果需要，可手动删除成员switch

S3750-2(config)# no switch 7 provision #将switch 7的配置删除

S3750-2(config)# do write #需要保存

S3750-2# reload #直接重启系统

Proceed with reload? [confirm]y #输入y，确定

S3750-1(config)# no switch 2 provision #如果设备正常上电且在堆叠集群里，无法删除！

%Switch can not be un-provisioned when it is physically present

**章n、端口相关操作**

**★查看接口信息**

Switch# show ip interface brief #查看接口ip及up/down情况

Interface IP-Address OK? Method Status Protocol

FastEthernet0/1 unassigned YES NVRAM up up

FastEthernet0/2 unassigned YES NVRAM down down

Vlan1 10.1.1.1 YES manual administratively down down

Switch# show int vlan1 # 查看具体的某个接口的详细信息

Router# show int f0/0

Switch# show running-config int f0/5 #查看具体端口上的配置

Switch# show running-config interface gigabitEthernet 0/2

**★端口速率**

Switch(config)# int f0/2 #进入目标端口

Switch(config-if)# duplex full #信道工作模式为全双工

Switch(config-if)# bandwidth 100000 #带宽设为100000Kbit/s

Switch(config-if)# speed 100 #速率100M

Switch(config-if)# exit

Switch(config)# int f0/5

**★设置为三层接口(路由口)**

Switch(config-if)# no switchport #设置为路由口

Switch(config-if)# ip add 10.2.2.2 255.255.255.0

Switch(config-if)# exit

**★端口安全**

Switch(config)# int f0/9

Switch(config-if)# switchport mode access #只能在access口上设置

Switch(config-if)# switchport port-security #开启端口安全功能

Switch(config-if)# switchport port-security maximum 20

#最大允许20个mac地址的数据包进入

Switch(config-if)# switchport port-security mac-address 00D0.97A9.1A39

#添加一条动态的记录

Switch(config-if)# switchport port-security mac-address sticky #开启sticky

Switch(config-if)# switchport port-security mac-address sticky 00D0.97A9.1A88

#添加一条sticky记录

Switch(config-if)# switchport port-security violation protect #惩戒动作protect

Switch(config-if)#

Switch(config-if)# exit

Switch(config)# errdisable recovery cause security-violation #开启假死恢复

**★端口聚合**

Switch(config)# int port-channel 1 #创建聚合口

Switch(config-if)# exit

Switch(config)# int range f0/20-21 #选中成员端口20~21

Switch(config-if-range)# channel-group 1 mode on #聚合模式为手动开启

Switch(config-if-range)# no shut

Switch(config-if-range)# exit

Switch(config)# int port-channel 1 #接下来是对聚合口的操作

Switch(config-if)# no shut

Switch(config-if)# switchport trunk encapsulation dot1q

Switch(config-if)# switchport mode trunk

Switch(config-if)# exit

Switch(config)# port-channel load-balance src-dst-mac #设置负载均衡

**★端口假死恢复**

有时我们会在交换机的端口上配置某些策略（比如端口安全，环路检测等），当用户的行为违反策略时，端口会被shutdown，此时的端口称为假死，默认是不会再自动开启该端口了，可以配置假死恢复，让端口再次开启。

Switch(config)# errdisable detect cause ? #查看支持恢复的类型

all Enable error detection on all cases

bpduguard Enable error detection on bpdu-guard

dtp-flap Enable error detection on dtp-flapping

link-flap Enable error detection on linkstate-flapping

pagp-flap Enable error detection on pagp-flapping

rootguard Enable error detection on root-guard

udld Enable error detection on udld

.........

Switch(config)# errdisable detect cause all #可以启用检测所有的类型

Switch(config)# errdisable recovery interval 300 #恢复周期300秒

Switch# show int f0/1 status err-disabled #查看端口假死的原因

**★光模块兼容性**

思科交换机默认只识别自己的光模块，其他厂商的光模块 检测序列号不通过

Switch(config)# int GigabitEthernet7/0/25 #必须进入相应的端口去配置

Switch(config-if)# service unsupported-transceiver #支持不兼容的光模块

#其实就是允许使用非思科的光模块

Switch(config)# int GigabitEthernet7/0/25

Switch(config-if)# no errdisable detect cause gbic-invalid

#关闭由于光模块不兼容而导致的端口死

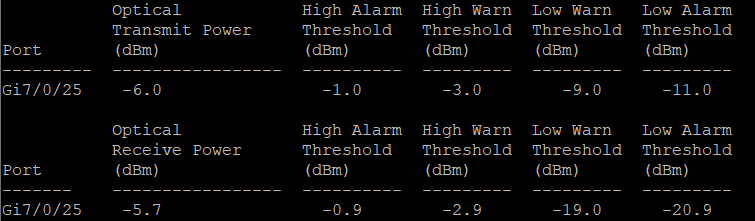
Switch(config)# int GigabitEthernet7/0/25

Switch(config-if)# speed nonegotiate #关闭自协商

Switch# show int transceiver supported-list #查看支持列表

**★DDM/VCT线路检测**

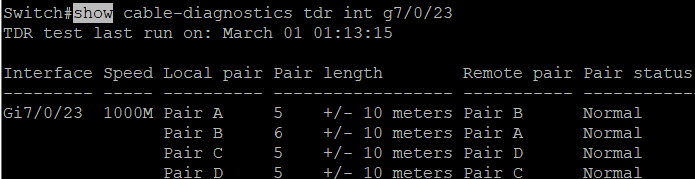
Switch# show int g7/0/25 transceiver detail #查看光口功率等信息



Switch# test cable-diagnostics tdr interface g7/0/23

#先检测，等几秒种，检测时这个端口会down再up

Switch# show cable-diagnostics tdr int g7/0/23 #查看电口线路检测结果



**34. DNS服务**

Switch(config)# ip domain-lookup #开启域名解析

Switch(config)# ip name-server 8.8.8.8 #指定dns服务器

Switch(config)# ip host xxx.com 10.1.1.4 #添加本地静态解析项

Switch(config)# ip dns server #自己作为dns服务器

**★端口镜像SPAN**

Switch(config)# monitor session 1 source int g1/0 both #监控端口tx和rx的流量

Switch(config)# monitor session 1 filter vlan 10 #只监控该vlan的流量

Switch(config)# monitor session 1 destination int g1/0/1

#目的端口，被监控的流量流向此端口，此端口只能接分析设备

Switch# show monitor session 1 #查看端口镜像

**★设置MTU**

Switch(config)# vlan 1

Switch(config-vlan)# mtu 1500

或者：

Switch(config)# int vlan 1

Switch(config-if)# ip mtu 1500

**★广播风暴抑制**

Switch(config-if)# storm-control broadcast level pps 800 #限制发包数

Switch(config-if)# storm-control broadcast level bps 200000 #限制速率

Switch(config-if)# storm-control broadcast level ?

<0.0-100.0> Enter rising threshold

Switch(config-if)# storm-control broadcast level 5 #限制为端口速率的5%

Switch(config-if)# storm-control action block #惩戒动作block,或shutdown

Switch(config)# errdisable recovery cause all #假死恢复

**章n、VLAN及STP操作**

**★创建vlan**

Switch(config)# vlan 10 #创建vlan 10

Switch(config-vlan)# name stuff #命名该vlan为stuff

Switch(config-vlan)# exit

Switch(config)# int vlan 10 #创建svi三层虚拟接口

Switch(config-if)#

Switch(config-if)# ip address 10.1.1.1 255.255.255.0 #配置IP

Switch(config-if)# description xxxxx #描述

Switch(config-if)# shutdown #关闭接口

Switch(config-if)#

administratively down

Switch(config-if)# no shutdown #启用接口

Switch(config-if)#

\*3? 02, 02:24:40.2424: %LINK-5-CHANGED: Interface Vlan10, changed state to up

Switch(config-if)# exit

Switch(config)# int range f0/1-5 #进入一组端口的配置界面

Switch(config-if-range)# switchport mode access #将该组端口设为access口

Switch(config-if-range)# switchport access vlan 10 #加入vlan 10

Switch(config-if-range)#

\*3? 02, 02:26:54.2626: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan10, changed state to up

Switch(config-if-range)# exit

Switch(config)# int f0/24

Switch(config-if)# switchport mode trunk #设置为trunk口

Command rejected: An interface whose trunk encapsulation is "Auto" can not be configured to "trunk" mode. # 三层交换机不能直接设置trunk口

Switch(config-if)# switchport trunk encapsulation dot1q #要先封装dot1q协议

Switch(config-if)# switchport mode trunk #再设置为trunk口

Switch(config-if)# switchport trunk native vlan 1 #设置native vlan（pvid）

Switch(config-if)# switchport allowed vlan 1-20

Switch(config-if)# switchport trunk allowed vlan 1-20 #只允许vlan1~20通过

Switch(config-if)# #思科的trunk口默认允许所有vlan通过

**★思科保留vlan**

VLAN Type SAID MTU Stp BrdgMode Trans1 Trans2

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

1002 fddi 101002 1500 - - 0 0 fddi-default

1003 tr 101003 1500 - - 0 0 token-ring-default

1004 fdnet 101004 1500 ieee - 0 0 fddinet-default

1005 trnet 101005 1500 ibm - 0 0 trnet-default

**★VTP（VLAN Trunk Protocol）**

Switch# vlan database

% Warning: It is recommended to configure VLAN from config mode,

as VLAN database mode is being deprecated. Please consult user

documentation for configuring VTP/VLAN in config mode.

Switch(vlan)# exit

APPLY completed.

Exiting....

Switch# conf t

Switch(config)# vtp domain vtpcom

Changing VTP domain name from NULL to vtpcom

Switch(config)# vtp password xxx

Setting device VLAN database password to xxx

Switch(config)# vtp mode server # vtp模式为server，其他交换机要设置为client

Device mode already VTP SERVER.

Switch(config)#

**★STP端口开销**

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

\*思科c2960,c3750默认使用802.1D-1998开销

Switch(config)# spanning-tree pathcost method long

#设置端口开销算法，long为802.1t，short为802.1d

**★PVST**

d

S2960# show spanning-tree vlan 1 #查看stp的vlan信息

VLAN0001

Spanning tree enabled protocol ieee

Root ID Priority 32769

Address 001b.2b22.6800 #根桥mac

Cost 19

Port 25 (GigabitEthernet0/1) #根端口

Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Bridge ID Priority 32769 (priority 32768 sys-id-ext 1)

Address 0021.d771.1380

Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Aging Time 300

Interface Role Sts Cost Prio.Nbr Type

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

Fa0/1 Altn BLK 200000 128.1 P2p

Fa0/7 Altn BLK 200000 128.7 P2p

Gi0/1 Root FWD 20000 128.25 P2p

S2960# show spanning-tree summary #查看stp概要信息

Switch is in pvst mode

Root bridge for: none

......

S2960(config)# spanning-tree pathcost method long

#设置端口开销算法，long为802.1t，short为802.1d

#配置上行链路，实现备份的上行链路快速恢复（意思就是指定的直连备份的根端口的可以直接恢复，不用经过转换）

spanning-tree uploadfast

配置上行速链路，当接入层或汇聚成的交换机主用的上行链路断开的时候，被阻塞的端口迅速转换到转发状态，不需要经过侦听和学习状态

3.配置速端口，使链接终端的端口快速进入转发状态

spanning-tree portfast

**★Rapid-PVST**

Switch(config)# spanning-tree mode ?

pvst Per-Vlan spanning tree mode

rapid-pvst Per-Vlan rapid spanning tree mode

Switch(config)# spanning-tree mode rapid-pvst #使用rapid-pvst

Switch(config)# spanning-tree vlan 1-10 root primary #指定为vlan1-10的根桥

Switch(config)# spanning-tree vlan 30 priority 4096 #指定vlan30的桥优先级

Switch(config)# int g1/0/1

Switch(config-if)# spanning-tree vlan 1-10 port-priority 16 #设置端口优先级

Switch(config-if)# spanning-tree cost 20 #设置端口路径开销

Switch(config-if)# exit

Switch(config)# int g1/0/3

Switch(config-if)# spanning-tree portfast #设置端口为边缘快速端口

Switch(config)# int g1/0/4

Switch(config-if)# spanning-tree bpduguard enable #开启bpdu防护

Switch(config-if)# exit

error-down自动恢复

Switch# show spanning-tree #查看STP详细信息

**21. ARP相关操作**

Switch# show arp #查看ARP表

Protocol Address Age (min) Hardware Addr Type Interface

Internet 10.1.1.1 - 00D0.97A9.1ABE ARPA Vlan10

Switch# show arp | include 10.1.1. #可以做过滤匹配

Switch(config)# arp 10.1.1.22 00D0.97A9.1A22 arpa #添加静态arp条目

Switch(config)# int vlan 1

Switch(config-if)# arp timeout 180 #在接口上配置arp老化时间，秒

Switch(config-if)# ip proxy-arp #开启代理arp

**22. MAC相关操作**

Switch# show mac-address-table #查看mac表

Switch# show mac-address-table | include 00D0.97A9.1A #仅显示匹配条目

Switch# clear mac-address-table [dynamic] #清空mac表[仅动态的条目]

Switch(config)# mac-address-table static 00D0.97A9.1A22 int f0/1 vlan 1

#添加静态mac条目

Switch(config)# mac-address-table aging-time 300 # mac老化时间

**25. Qos限速**

Switch(config)# mls qos #开启qos

Switch(config)# access-list 10 permit 10.1.1.0 0.0.0.255 # acl匹配目标流

Switch(config)# class-map class1 #定义流类

Switch(config-cmap)# match access-group 10 #匹配acl

Switch(config-cmap)# exit

Switch(config)# policy-map policy1 #定义流策略

Switch(config-pmap)# class class1

Switch(config-pmap-c)# bandwidth 10000 #带宽限制为10000Kbit/s

Switch(config-pmap-c)# shape average 16000000 #整流平均流量，bit/s

Switch(config-pmap-c)# exit

Switch(config)# int f0/3 #应用策略到接口

Switch(config-if)# service-policy output policy1 #仅支持output方向

\*有的设备配置policy时用的不是上面的命令，可能是下面的命令：

Switch(config)# policy-map policy1

Switch(config-pmap)# class class1

Switch(config-pmap-c)# police cir 10000000 10000000 # bit/s，byte/s

\*也可能是下面的命令：

Switch(config)# policy-map policy1

Switch(config-pmap)# class class1

Switch(config-pmap-c)# trust dscp

Switch(config-pmap-c)# policy 10000000 10000000 exceed-action drop # bps, Byte/s

# 一共就这三种命令，思科的设备命令不太统一

Switch# show policy-map int f0/3 #查看策略应用情况

FastEthernet0/3

Service-policy output: policy1

Class-map: class1 (match-all)

0 packets, 0 bytes

5 minute offered rate 0 bps, drop rate 0 bps

Match: access-group 10

Traffic Shaping

Target/Average Byte Sustain Excess Interval Increment

Rate Limit bits/int bits/int (ms) (bytes)

16000000/16000000 500000 2000000 2000000 125 250000

**26. DHCP**

Switch(config)# service dhcp #开启dhcp服务

Switch(config)# ip dhcp pool pxx #创建dhcp地址池

Switch(dhcp-config)# network 10.1.1.0 255.255.255.0 #设置网段

Switch(dhcp-config)# default-router 10.1.1.1 #网关

Switch(dhcp-config)# dns-server 8.8.8.8 # dns

Switch(dhcp-config)# lease 5 4 30 #租期，单位：日，时，分

Switch(dhcp-config)# option 43 hex xxxxxxxx # option 43

Switch(dhcp-config)# exit

Switch(config)# ip dhcp excluded-address 10.1.1.1 10.1.1.10 #排除地址段

Switch(config)#

**保存ip分配信息到ftp服务器上的lease.db.cfg文件中**

Switch(config)# ip dhcp database ftp:# user:pass@10.1.1.252/lease.db.cfg

Switch(config)#

**开启ping检测**

Switch(config)# ip dhcp ping packets 2 #每次分配ip前先ping一下要分配的ip，发2个包

Switch(config)# ip dhcp ping timeout 1000 # Ping超时，毫秒

Switch(config)#

Switch(config)# ip dhcp binding cleanup interval 600 #**清除已过期的ip**，秒

**27.给特定mac分配固定的IP**

Switch(config)# ip dhcp pool pc1 #创建地址池，只有一个ip

Switch(dhcp-config)# host 10.1.1.35 255.255.255.0

Switch(dhcp-config)# client-identifier 0100.D097.A91A.22

#以01开始加上mac地址

Switch(dhcp-config)# default-router 10.1.1.1

Switch(dhcp-config)# dns-server 8.8.8.8

Switch(dhcp-config)# exit

Switch# show dhcp lease #查看dhcp分配的地址情况

Switch# show ip dhcp binding #查看分配的ip及绑定的mac地址

Switch#

**28.DHCP中继**

Switch(config)# int vlan 1

Switch(config-if)# ip helper-address 10.3.3.1

Switch(config-if)# exit

# 要记得先配置去往10.3.3.1的路由

**29. DHCP snooping**

Switch(config)# ip dhcp snooping #开启dhcp snooping

Switch(config)# int f0/24 #上联口

Switch(config-if)# ip dhcp snooping trust #上联口要设为信任口

Switch(config-if)# ip dhcp snooping limit rate 50 #限制dhcp报文速率

Switch(config-if)# exit

Switch(config)# ip dhcp snooping vlan 1-30 #监测的vlan

Switch(config)# ip dhcp snooping verify mac-address #检查mac地址

#入站包的mac地址和ip地址和dhcp服务器中分配的条目吻合时才放行

Switch(config)#

Switch(config)# errdisable recovery cause dhcp-rate-limit #假死恢复

Switch(config)# ip dhcp snooping binding xxxx.xxxx.xxxx vlan 10 ip x.x.x.x int f0/3

Switch(config)# ip dhcp snooping database flash:/dhcpsnooping.db

Switch(config)# ip dhcp snooping database write-delay 100

Switch(config)#

Switch# show ip dhcp snooping binding #查看dhcp snooping绑定情况

Switch# clear ip dhcp snooping binding #清除dhcp snooping绑定条目

**章n、ACL访问控制列表**

每一个acl的末尾都有一条隐含的deny any，每一个ACL都可以有多条规则（rule）

规则的执行顺序是从上到下，匹配一条后立即停止下面规则的匹配

所有的掩码都只能是反掩码的形式

|  |  |  |
| --- | --- | --- |
| acl编号 | 类型 | 匹配对象 |
| 1~99 | 标准ip acl | 源ip |
| 100~199 | 扩展ip acl | 源ip，目的ip，源端口目的端口等，可加时间段 |
| 700~799 | 标准mac acl | 源mac |
| 1100~1199 | 扩展mac acl | 源mac，目的mac等，可加时间段 |

**★标准ACL**

Switch(config)# access-list 1 permit 10.1.1.0 0.0.0.255 #标准数字acl匹配网段

Switch(config)# access-list 2 permit host 10.1.1.3 #标准数字acl匹配单个IP

Switch(config)# access-list 3 permit any #标准数字acl匹配所有ip

Switch(config)# ip access-list standard acl\_1 #标准命名acl

Switch(config-std-nacl)# permit 192.168.0.0 0.0.255.255

Switch(config-std-nacl)# exit

**★扩展ACL**

Switch(config)# access-list 100 permit ip 10.1.1.0 0.0.0.0 192.168.9.0 0.0.0.255

Switch(config)# access-list 101 deny icmp host 10.1.1.33 192.168.9.0 0.0.0.255

Switch(config)# ip access-list extended acl\_ex1 #扩展命名acl

Switch(config-ext-nacl)# permit tcp 10.1.1.0 0.0.0.255 eq 80 192.168.9.0 0.0.0.255 range 20 90 # tcp 源IP 源端口 目的IP 目的端口范围

Switch(config-ext-nacl)# permit tcp host 10.1.1.3 any 192.168.9.0 0.0.0.255 eq ftp

#端口可以为数字，也可为别名

Switch(config-ext-nacl)# exit

**端口别名**对应的端口号：

bootpc 68 bootps 67 domain 53 isakmp 500 snmp 161

ftp 21 pop3 110 smtp 25 telnet 23 www 80

**★MAC ACL**

Switch(config)# mac access-list extended mac\_ex1 #命名扩展mac acl

Switch(config-mac-ext-nacl)# permit host xxxx.xxxx.xxxx any

Switch(config-mac-ext-nacl)# deny xxxx.xxxx.xxxx 0000.0000.00ff any #反掩码

Switch(config-mac-ext-nacl)# exit

Switch(config)# access-list 700 permit xxxx.xxxx.xxxx 0000.0000.0000

#数字标准mac acl

**★ACL时间**

Switch(config)# time-range *time1* #创建acl时间time1

Switch(config-time-range)# periodic Friday 10:30 to Sunday 19:00

#每周的这个时段，循环

Switch(config-time-range)# exit

Switch(config)# time-range *time2* #创建acl时间time2

Switch(config-time-range)# absolute start 11:00 9 Dec 2019 end 23:00 12 Dec 2019

Switch(config-time-range)# #日月年，只在这个时间段执行一次

ACL时间只应用在扩展的acl规则中，在acl规则末尾添加time-range *time1*即可

**在接口上应用ACL**

Switch(config)# int vlan 10 #有的交换机只能应用acl到vlan接口上，

Switch(config-if)# ip access-group 1 in #而不支持应用到物理端口上

**★插入或删除ACL中的某条规则**

\*思科的ACL其实也是有规则（rule）的编号的，只是在大多教程中都不教，因为模拟器中不支持对规则编号的操作

Switch# show ip access-lists acl\_ex1 #先查看ACL的rule

Extended IP access list acl\_ex1

1 permit tcp 10.1.1.0 0.0.0.255 eq www 192.168.9.0 0.0.0.255 range 20 90

2 permit tcp 10.1.1.0 0.0.0.255 eq www 192.168.9.0 0.0.0.255 eq ftp

#开头的数字为rule编号

Switch(config)# ip access-list extended acl\_ex1 #进入acl编辑模式

Switch(config-ext-nacl)# no 1 #删除编号为1的规则

Switch(config-ext-nacl)# 3 permit ip any any #添加一条规则，编号为3

**★ACL应用要点**

ACL访问控制列表，是交换机的基本功能，大多数厂商的交换机的acl是应用在端口上，如g0/0/1之类的物理端口，方向为in或out，很容易理解，配置时不易出错。不过思科的交换机一般都是将acl应用在int vlan 接口上，如int vlan 1之类的，方向为in或out（一般二层交换机只能in）所以容易出错，搞不好会酿成生产事故。

首先思科交换机的acl本身的配置这里就不多说了，只讲1点：它的每个acl的末尾默认是有deny any any的

1.当我们仅配置permit xx xx这一条时，则默认只permit这一条，因为有隐含的

deny any any

2.当我们仅配置deny xx xx这一条时，则默认是无permit的，因为隐含有deny any

3.所以当我们想 只过滤某条访问规则时，写完deny xx xx这条后，得再加上

permit ip any any，不然就全部deny了

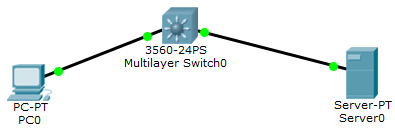
然后讲它的acl在int vlan上的方向问题：

**拓扑如下图**：

3560交换机为三层的，支持in和out方向的应用，作为以下2台计算机的网关

pc0为客户端，ip: 10.1.1.1接入vlan 1，网关10.1.1.254

server 0为服务端，ip: 10.2.2.2接入vlan 2，网关10.2.2.254



交换机上想做一条acl，仅禁止pc0访问server 0的80端口，其他的流量正常通过，该怎么配置呢？

\*\* **ACL配置如下**：

Switch# conf t

Switch(config)# ip access-list extended deny\_80

#创建名为deny\_80的扩展acl

Switch(config-ext-nacl)# deny tcp host 10.1.1.1 host 10.2.2.2 eq 80

#阻止源ip为10.1.1.1，目的ip为10.2.2.2，目的端口80/tcp的报文

Switch(config-ext-nacl)# permit ip any any

#因为末尾隐含为deny any，所以 仅deny某条时，要permit所有

Switch(config-ext-nacl)# exit

Switch(config)#

\*\***应用acl到int vlan接口上**：

Switch(config)# int vlan 1 #进入接口配置界面

Switch(config-if)# ip access-group deny\_80 in #应用acl到in方向

Switch(config-if)#exit

也可这样应用，用在int vlan 2上

Switch(config)# int vlan 2

Switch(config-if)# ip access-group deny\_80 out #应用到out方向

Switch(config-if)#exit

能否同时应用到int vlan 1和int vlan 2上呢？可以，只是没必要做2次匹配，对速度有影响。

**关于in / out方向的解释**：

因为源ip:10.1.1.1发来的报文要先发给网关int vlan 1，所以对于int vlan 1而言就是入站，而且int vlan 1收到报文后，要走路由层，因为目的ip不在本vlan里，int vlan 1把报文发给路由层的话，不算是out，只有发给本vlan里的主机时，才算out

而在int vlan 2那里应用acl时，只能用out，因为它收到的报文是从路由层转来的，不算in，int vlan 2收到报文后，发现目的ip为本vlan里的主机的ip，所以发给本vlan的主机的话，算out方向。

也就是说，如果报文只是经过此vlan的某2个端口，不发给此vlan的int vlan x接口的话，就没有in，也没有out，无法做acl的匹配。

或者说没有经过路由层面的报文，没法应用acl （这也是思科交换机的一大痛点）

二层交换机只能应用到int vlan 接口的in方向，也就是只能对上行流量做匹配

当然，有些较新的思科交换机也是支持应用acl到物理端口上的。这里就不多讲了，和其他品牌的应用原理都一样。

以上就是思科交换机的acl应用到int vlan接口的 注意要点！

**32.日志服务器**

Switch(config)# logging on #开启日志功能

Switch(config)# logging 10.1.1.253 #设置日志服务器（syslog）

Switch(config)# logging source-interface vlan 1 #发数据给服务器时的源IP

Switch(config)# logging trap debugging # trap级别设置为7（debugging）默认为6（information）

Switch(config)# logging buffered 100000

#设置本地的日志存储buff空间大小，单位byte

Switch(config)# service sequence-numbers #发送日志时也带上序号

Switch# show logging #查看日志信息

**37. Xmodem传文件**

通过console线传文件，只支持传文件到交换机上，速度受console的速率限制

Switch# copy xmodem: flash: #从console传文件到交换机的flash上

dst-file-name: c3650.cfg #指定存到flash上的文件名

ccccc

#打印cccc字符时交换机已准备好，此时可以在终端仿真软件上发送Xmodem

Router# copy xmodem: flash: #从console传文件到路由器的flash上

\*\*\*\* WARNING \*\*\*\*

x/ymodem is a slow transfer protocol limited to the current speed

settings of the auxiliary/console ports. The use of the auxilary

port for this download is strongly recommended.

During the course of the download no exec input/output will be

available.

---- \*\*\*\*\*\*\* ----

Proceed? [confirm] y #确定

Source filename []? c3650.cfg #指定目标文件名（终端上的）

Destination filename [c3650.cfg]? bak.cfg #指定存到路由器flash里的文件名

Erase flash: before copying? [confirm] y #确定

Use crc block checksumming? [confirm] y #确定

Max Retry Count [10]: 2 #重传次数，2次

Perform image validation checks? [confirm] y #确定

Xmodem download using crc checksumming with image validation

Continue? [confirm] y #确定

Ready to receive file........... #此时在终端上发送xmodem

**41. HSRP思科路由（网关）冗余协议**

\*要与pvst/rapid-pvst配合

发送hello包的组播地址为224.0.0.2（v1）或224.0.0.102（v2），默认优先级100越大越优先。所有路由器的version应该一致。

虚拟网关mac为0000.0c07.ac-standby编号

Switch(config)# int vlan 1

Switch(config-if)# ip add 10.1.1.1 255.255.255.0

Switch(config-if)# standby version 2 # HSRP版本

Switch(config-if)# standby 1 ip 10.1.1.254 #虚拟网关

Switch(config-if)# standby 1 priority 120 #优先级设为120，变成master

Switch(config-if)# standby 1 preempt delay minimum 5 #抢占延迟最少5秒

Switch(config-if)# standby 1 authentication md5 key-string xxx #备份组验证信息

Switch(config-if)# standby 1 track g1/0/24 30

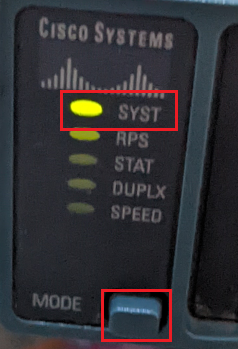
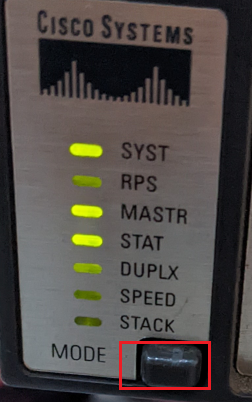
#监测上联口，当上联口不通时优先级降低30，该网关变为备份的

Switch# show standby brief #查看standby信息

**章n、交换机switch模式**

**★进入switch模式**

1.重启设备时长按MODE键（一般位于正面的左边的小按钮）直到SYST指示灯不闪烁，以及console输出switch提示符 则说明进入交换机的switch模式了

2.switch模式指示符为 switch> 或 switch: switch模式下的常用操作有：

**★使用xmodem传文件**

switch> flash\_init #初始化文件系统

switch> load\_helper #加载基本的功能模块

switch> copy xmodem: flash:c3650-xxx.bin #传送系统镜像文件

cccccc #此时可以在终端仿真软件上发送xmodem

switch> set BOOT flash:c3650-xxx.bin #指定以该文件为启动镜像文件

switch> boot #启动系统

**★修改console口波特率**

switch> set BAUD 115200 #设置波特率为115200

switch>unset BAUD #恢复原来的波特率（默认的9600）

switch>

**★交换机恢复密码**

switch> flash\_init

switch> load\_helper

switch> dir flash: #先查看flash: 里的文件列表

switch> rename flash:config.text flash:c3650old.cfg #把默认的配置文件

# 更名为c3650old.cfg，这样系统启动时找不到配置文件就会以出厂设置启动

switch> boot #启动系统

xxxxxxxxxx #此时系统重启中

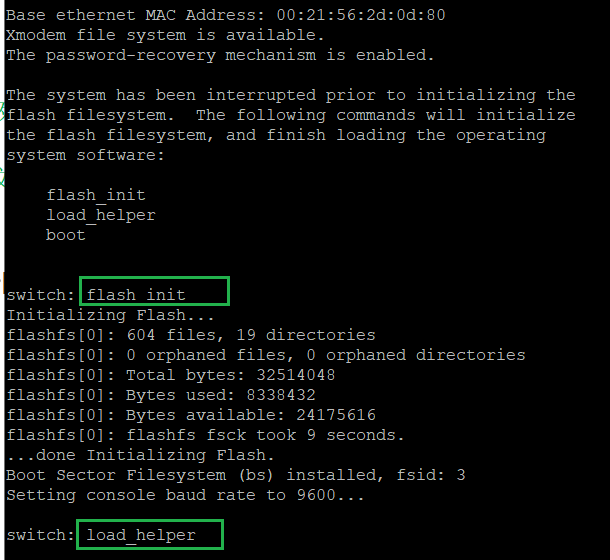
Would you like to enter the initial configuration dialog? [yes/no]: n #否

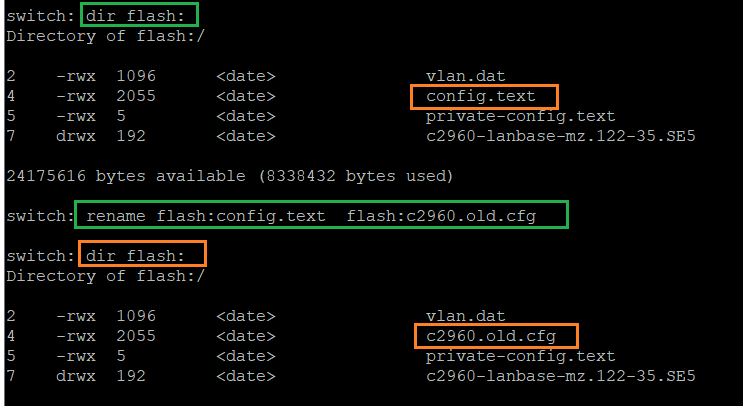
Switch> enable #进入配置模式

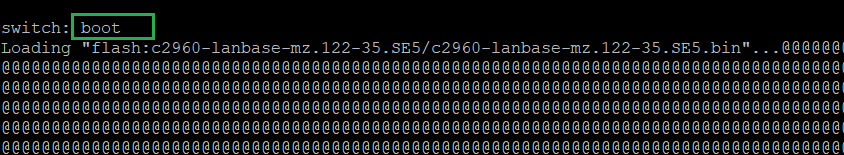
Switch# copy flash:c3650old.cfg system:running-config #加载原配置

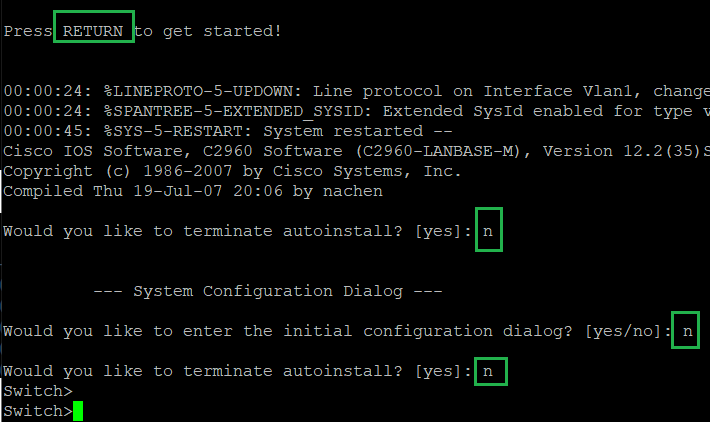
然后重新配置管理员密码 和 enable密码

Switch# write #保存配置即可









**章n、路由器Rommon模式**

Rommon模式也叫维护模式，在Rommon模式下可以传文件到路由器上，也可以恢复密码

重启时按下Ctrl键和Break键 进入Rommon模式。（Break键也叫Pause键）

①Rommon模式下传文件到路由器

rommon 1 >

rommon 1 > IP\_ADDRESS=10.1.1.1 #设置临时的IP地址，只能使用(G)Ethernet0/0端口

rommon 2 > IP\_SUBNET\_MASK=255.255.255.0 #子网掩码

rommon 3 > DEFAULT\_GATEWAY=10.1.1.254 #网关

rommon 4 > TFTP\_SERVER=10.1.1.2 # TFTP服务器IP

rommon 5 > TFTP\_FILE=c3650xx-xx.bin #要下载到路由器上的的文件名

rommon 6 > tftpdnld #开始用tftp下载，下载到路由器上

IP\_ADDRESS: 10.1.1.1

IP\_SUBNET\_MASK: 255.255.255.0

DEFAULT\_GATEWAY: 10.1.1.254

TFTP\_SERVER: 10.1.1.2

TFTP\_FILE: c3650xx-xx.bin

Invoke this command for disaster recovery only.

WARNING: all existing data in all partitions on flash will be lost!

Do you wish to continue? y/n: [n]: y #确定

下载成功后

rommon 7 > boot c3650xx-xx.bin #指定以此系统镜像文件启动

然后系统启动

②**路由器恢复密码**

先重启系统，按下Ctrl键和Break键进入Rommon模式

rommon 1 > confreg 0x2142 # 表示启动时跳过配置文件

rommon 2 > boot # 启动系统

系统启动后，再加载配置文件，再重置密码，保存。

Router> enable

Router# copy startup-config running-config #加载配置文件

Destination filename [running-config]? #这里直接回车

1973 bytes copied in 0.416 secs (4742 bytes/sec)

Router0#

Router0# conf t

Enter configuration commands, one per line. End with CNTL/Z.

Router0(config)# enable password xxxx #重置密码

Router0(config)# username coflee privilege 15 password xxxx #修改用户密码

Router0(config)# config-register 0x2102 #表示启动时加载配置文件

Router0(config)# do write #保存配置

Building configuration...

[OK]

**章n、路由操作**

**★二层交换机设置默认网关**

Switch(config)# ip default-gateway 10.1.1.254

**★三层交换机开启路由转发功能**

Switch(config)# ip routing

**！以下为路由器的操作**

**★静态路由**

Router0(config)# ip route 192.168.0.0 255.255.0.0 10.1.1.2 [int s1/0/1] 20

# 目的网段 子网掩码 下一跳 [出接口] 优先级

Router0# show ip route #查看路由表

9.0.0.0/8 is variably subnetted, 3 subnets, 2 masks

S 9.9.9.0/24 [1/0] via 9.9.10.7

C 9.9.10.0/24 is directly connected, Serial0/0/1

L 9.9.10.5/32 is directly connected, Serial0/0/1

Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP

D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area

N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2

E1 - OSPF external type 1, E2 - OSPF external type 2

i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2

ia - IS-IS inter area, \* - candidate default, U - per-user static route

o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP

a - application route

+ - replicated route, % - next hop override

**★RIP**

Router0(config)# router rip #进入rip配置界面

Router0(config-router)# version 2 #设置版本

Router0(config-router)# no auto-summary #关闭自动汇总

Router0(config-router)# distance 120 #指定路由优先级

Router0(config-router)# network 10.0.0.0 #宣告网段

Router0(config-router)# network 10.1.1.0

Router0(config-router)# passive-interface g0/0/2 #静默接口

Router0(config-router)# redistribute ospf 1 metric 3 #路由引入（重分布）

Router0(config-router)# default-information originate #引入默认路由（0.0.0.0）

Router0(config-router)#

Router0(config)# int g0/0/1

Router0(config-if)# ip rip authentication mode md5 # rip接口验证

Router0(config-if)# ip rip authentication key-chain xxxxx # rip接口验证密码

**★OSPF**

Router0(config)# router ospf 1 #进入osfp配置界面，ospf进程号1

Router0(config-router)# router-id 10.1.1.1 #指定router-id

Router0(config-router)# network 10.1.1.0 0.0.0.255 area 0 #在区域0宣告网段

Router0(config-router)# passive-interface g0/0/2 #静默接口

Router0(config-router)# area 1 virtual-link 10.2.2.2 #虚拟链路对端

Router0(config-router)# redistribute rip metric 20000 [subnets metric-type 1]

#路由引入（重分布）

Router0(config-router)# area 0 authentication message-digest #区域0开启验证

Router0(config-router)# auto-cast reference-bandwidth 1000

#参考带宽改为1000Mb，默认为100M

Router0(config-router)# area 2 stub #设置区域类型

Router0(config)# int g0/0/1

Router0(config-if)# ip ospf authentication message-digest #接口上开启ospf验证

Router0(config-if)# ip ospf message-digest-key 1 md5 xxxx #验证密码

Router0(config-if)# ip ospf priority 2 #设置ospf路由器优先级，用于选举DR

Router0(config-if)# ip ospf cost 10 #设置ospf接口开销

Router0(config-if)# ip ospf network broad #设置接口所处的网络类型

Router0# show ip ospf ? #查看ospf信息

<1-65535> Process ID number

border-routers Border and Boundary Router Information

database Database summary

interface Interface information

neighbor Neighbor list

virtual-links Virtual link information

**★单臂路由**

Router0(config)# int g0/0/0

Router0(config-if)# no shut

Router0(config-if)# exit

Router0(config)# int g0/0/0.1 #开启子接口

Router0(config-subif)# encapsulation dot1q 1 [native] #封装dot1q，vid为1

Router0(config-subif)# ip add 10.10.10.1 255.255.255.0

Router0(config-subif)# exit

Router0(config)# int g0/0/0.2

Router0(config-subif)# encapsulation dot1q 2 #封装dot1q，vid为2

Router0(config-subif)# ip add 10.20.20.1 255.255.255.0

Router0(config-subif)# exit

**★BGP**

在

**49.PPP**

Router0(config)# int s0/1/1

Router0(config-if)# clock rate 200000

#单位波特，设置时钟频率，仅DCE端需要设置（接v35母头线一侧为DCE）

Router0(config-if)# encapsulation ppp #封装ppp协议，也可用hdlc（无需验证）

Router0(config-if)# bandwidth 2000 #单位kbit/s，设置带宽为2000Kbit/s（2M）

Router0(config-if)# ppp authentication pap #使用pap验证

Router0(config-if)# ppp pap sent-username coflee password xxxx

#对端的pap用户名及密码

Router0(config-if)# no shutdown #启用接口

Router0(config-if)#

#要求验证的用户已在对端设备创建，用户名可相同，也可不相同，密码可相同也可不同

Router0(config-if)# ppp authentication chap *default*

#使用chap验证，默认为双向验证，最后的default表示使用默认的验证方案

Router0(config-if)# ppp chap hostname r7 #设置对端的用户，**不能相同**

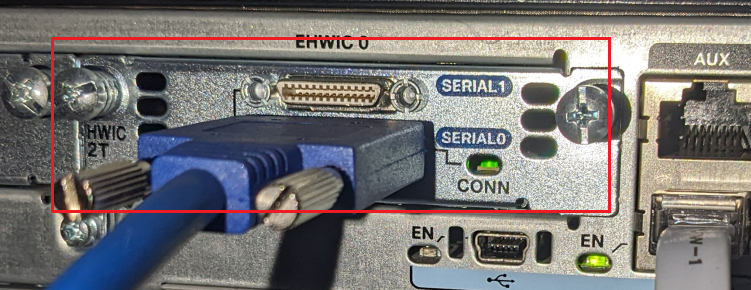
Router0(config-if)# ppp chap password xxxx #密码**双方要相同**

Router0(config-if)# no shutdown #启用接口

#要求验证的用户已在对端设备创建，且密码一致，双方的用户名(hostname)**不能**相同

HWIC 2T扩展卡如下图：（有2个Serial口，使用small serial v26接口）





**50. NAT地址转换**

①静态NAT（一对一）

Router0(config)# int g0/0/1 #内网口

Router0(config-if)# ip nat inside

Router0(config-if)# exit

Router0(config)# int s0/1/1 #外网口

Router0(config-if)# ip nat outside

Router0(config-if)# exit

Router0(config)# ip nat inside source static 10.1.1.55 200.1.1.3

#将内网的10.1.1.55和外网的200.1.1.3对应起来

②动态NAT（多对多，可端口复用）

Router0(config)# int g0/0/1 #内网口

Router0(config-if)# ip nat inside

Router0(config-if)# exit

Router0(config)# int s0/1/1 #外网口

Router0(config-if)# ip nat outside

Router0(config-if)# exit

Router0(config)# ip nat pool pname 200.1.1.5 200.1.1.10 netmask 255.255.255.0

# nat的公网ip范围

Router0(config)# access-list 10 permit 10.1.1.0 0.0.0.255 #匹配内网ip段

Router0(config)# ip nat inside source list 10 pool pname overload

③目的NAT（端口映射）

Router0(config)# ip nat inside source static tcp 10.1.1.22 3389 200.1.1.9 9999

#将外网的200.1.1.9:9999转换为内网的10.1.1.22:3389

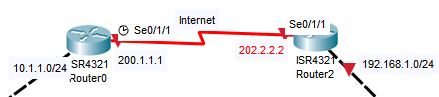
Router0# show ip nat translations #查看nat转换情况

**★GRE Tunnel**

在

**51. IPsec VPN**

前提：两端的路由器都要有去往对端内网网段的路由，且要有缺省路由指向网关。



Router0的公网IP为200.1.1.1，网关200.1.1.254，内网10.1.1.0/24

Router2的公网IP为202.2.2.2，网关202.2.2.254，内网192.168.1.0/24

**Router0的配置如下：**（Router2的类似）

**0.配置出接口IP及路由**

Router0(config)# int s0/1/1

Router0(config-if)# ip add 200.1.1.1 255.255.255.0

Router0(config-if)# exit

Router0(config)# ip route 0.0.0.0 0.0.0.0 200.1.1.254

**1.配置acl匹配目标流**

Router0(config)# ip access-list extended vpn1

Router0(config-ext-nacl)# permit ip 10.1.1.0 0.0.0.255 192.168.1.0 0.0.0.255

Router0(config-ext-nacl)# exit

**2.配置IKE提议**

Router0(config)# crypto isakmp policy 10

Router0(config-isakmp)# authentication pre-share

Router0(config-isakmp)# hash sha #消息摘要算法

Router0(config-isakmp)# encryption aes #加密算法

Router0(config-isakmp)# group 5 # DH密钥交换组

Router0(config-isakmp)# exit

**3.配置IKE对端**

Router0(config)# crypto isakmp key [0] xxxx address 202.2.2.2

**4.配置IPsec交换集**

Router0(config)# crypto ipsec transform-set tranName esp-aes esp-sha-hmac

Router0(cfg-crypto-trans)# mode transport #使用传输模式

Router0(cfg-crypto-trans)# exit

**5.配置vpn map**

Router0(config)# crypto map mapName 10 ipsec-isakmp

Router0(config-crypto-map)# set transform-set tranName #匹配交换集

Router0(config-crypto-map)# set peer 202.2.2.2 #设置对端

Router0(config-crypto-map)# match address vpn1 #匹配目标流

Router0(config-crypto-map)# set pfs group5

**6.接口上应用vpn map**

Router0(config)# int s0/1/1

Router0(config-if)# crypto map mapName

Router0# show crypto isakmp ? #查看对端

policy Show ISAKMP protection suite policy

sa Show ISAKMP Security Associations

Router0# show crypto ipsec ? #查看ipsec相关信息

sa IPSEC SA table

transform-set Crypto transform sets

**52. L2TP VPN**

Router0(config)# aaa new-model

Router0(config)# aaa authentication ppp default group radius #使用radius认证

Router0(config)# radius-server host 10.1.1.33 auth-port 1645 key xxxx

Router0(config)# vpdn enable #开启vpdn

Router0(config)# vpdn-group l2tp1 #创建vpdn组

Router0(config-vpdn)# accept-dialin #允许客户拨号

Router0(config-vpdn-acc-in)# protocol l2tp #使用l2tp协议

Router0(config-vpdn-acc-in)# virtual-template 1 #创建虚拟模板

Router0(config-vpdn-acc-in)# exit

Router0(config-vpdn)# exit

Router0(config)# int virtual-Template 1 #进入虚拟模板配置界面

Router0(config-if)# ip unnumbered g0/0/1 # IP地址共用接口g0/0/1的

Router0(config-if)# peer default ip address pool L2tpPool #给客户端分配的IP池

Router0(config-if)# ppp authentication chap default # ppp使用chap验证

Router0(config-if)# ppp ipcp dns 8.8.8.8 #给客户端分配的dns

Router0(config)# ip local pool L2tpPool 10.8.8.2 10.8.8.250 #定义地址池

Router0(config)#

**53. PPPoe服务器**

Router0(config)# aaa new-model

Router0(config)# aaa authentication ppp default group radius #使用radius认证

Router0(config)# radius-server host 10.1.1.33 auth-port 1645 key xxxx

Router0(config)# vpdn enable

Router0(config)# vpdn-group pppoe1 #创建vpdn组

Router0(config-vpdn)# accept-dialin

Router0(config-vpdn-acc-in)# protocol pppoe #使用pppoe协议

Router0(config-vpdn-acc-in)# virtual-template 2

Router0(config-vpdn-acc-in)# exit

Router0(config)# int virtual-template 2

Router0(config-if)# ip unnumbered g0/0/1

Router0(config-if)# peer default ip address pool pppoePool

Router0(config-if)# ppp authentication chap

Router0(config-if)# ppp ipcp dns 8.8.8.8

Router0(config-if)# ip nat inside

Router0(config-if)# exit

Router0(config)# ip local pool pppoePool 10.1.1.2 10.1.1.200

Router0(config)# int g0/0/1

Router0(config-if)# ip add 10.1.1.1 255.255.255.0

Router0(config-if)# pppoe enable #接口上使能pppoe

Router0# show aaa sessions #查看拨号情况

**55.用户权限设置**

很多教程都没有深入详细地讲解如何给用户分配具体的权限，大多都是教大家在创建用户时指定相应的privilege级别就完事儿了，可能是作者觉得没有必要教。

首先：思科的网络设备对用户操作权限分配的思想是 定义15个等级，然后默认给每个等级授予一定的权限（即能执行的命令），创建用户时，指定其privilege level之后，该用户就有这一级别的权限。

然后我们登录系统时，默认是进入>一般模式，需要输入enable密码才能进入特权用户模式。好像不论是哪个级别的用户输入enable密码后都拥有了管理员权限（最高级别权限），这是怎么回事呢？

先做个实验看看，创建一个用户admin，权限级别为15，登录系统后，查看其权限级别：

Username: admin

Password:

Router0>show privilege #查看当前用户权限

Current privilege level is 1 #显示的级别为1，最低级

\*这是怎么回事儿？

因为我们只是在创建用户时指定其权限级别为level-15，但并没有指定用这个level来给用户授权，所以登录到系统的用户，不论我们指定的权限是哪个level的，其实都是一样的（leve-1），没有区别。然后谁有enable密码，谁就能获得level-15的权限。（说直接点就是没有配置好）

\*我们需要创建一条aaa的授权策略：

Router0(config)# aaa new-model

Router0(config)# aaa authorization exec default local

# exec操作权限授权使用本地授权，即由用户的privilege的level来决定

Router0(config)# line vty 0 4

Router0(config-line)# authorization exec default

#应用到vty上，**模拟器无该命令**，**只能用真实的设备**配置

这时当用户使用远程登录后，默认进入的界面为特权用户界面，

在该界面下show privilege时，看到的是在创建用户时指定的level

然后能执行该level权限下的命令。

\* level高的用户默认是继承level低的权限，就是说如果给level-5指定允许使用命令write，则比level-5高的其他level都有该权限了。

登录系统后可以按下问号?查看自己这个level支持的命令（即拥有的权限）

\*为不同级别的用户分配额外的命令

Router0(config)# privilege exec level 5 configure ter

#表示级别5的用户登录到>一般模式后，可以执行configure ter 命令

Router0(config)# privilege configure all level 7 interface

#表示级别7的用户进入配置模式后，可以执行以interface开头的所有命令

Router0(config)# privilege configure all level 10 ip

#表示级别10的用户进入配置模式后，可以执行以ip开头的所有命令

上面命令中的all表示可以列出后面指定命令的所有子命令。

以此为例可以灵活地分配不同级别的用户能够执行的命令。

\*前面讲到 输入enable密码后都有了管理员权限，这又是怎么一回事呢？

Router0> enable ?

<0-15> Enable level # enable后面还可以接数字，表示level

view Set into the existing view

<cr>

Router0>enable #原来我们在输入enable时，缺省是enable 15的级别，

设置enable密码时默认也是设置的enable 15的密码，所以不论是谁输入enable密码，缺省都是进入了level-15的特权模式。

\*所以正确的做法是为相应的level设置对应的enable密码：

Router0(config)# enable secret level 7 passxxx

Router0(config)# enable secret level 10 passxxx

Router0(config)# enable secret level 15 passxxx

\*然后用户在输入enable时要指定进入哪个level：

Router0>

Router0> enable 7 #进入level-7的特权模式

Password:

Router0#

Router0# show privilege

Current privilege level is 7 #果然是level-7

Router0(config)# ? #进入配置模式后，查看授予的权限（支持的命令）

Configure commands:

do To run exec commands in config mode

end Exit from configure mode

exit Exit from configure mode

interface Select an interface to configure #这就是我们前面给level-7分配的可执行的命令

no Negate a command or set its defaults

Router0(config)#

这下明白是怎么回事了吧。

如果发现权限不够，可以退回到# 特权模式，再输入enable 10或enable 15这些高级别的就行了。

Router0# enable 15 #进入管理员的级别，和enable是一样的

Password:

Router0# show privilege

Current privilege level is 15

如果觉得权限太高不安全，想降几级，可以直接输入disable 5等比当前级别低的数字就行。

Router0# disable 5

**总结：**

1.创建用户时可以给用户指定不同的权限level

2.要想使这个level生效，需要定义aaa的exec的授权方案并在line con 0或line vty 里应用授权

3.为不同的level分配额外的命令

4.设置不同level的enable密码

5.用户登录系统后要进入特权用户模式时，输入enable时须指明要进入的level