思科路由与交换配置命令

说明：

1.本文档没有目录，本文档在发布时为 pdf 文档，有章节书签，可以下载到本地来查看，点击书签进入相应的章节。

2.蓝色的字为配置命令，绿色的字为命令的注释，有时命令太密集时，就不用蓝色标出了。

3.本文档仅为配置命令，相关的理论知识请参考其他文档。

4.有的命令在模拟器里可能不支持，可以下载最新的版本试试，最好是弄一两台真实的设备实践一下。

作者：李茂福

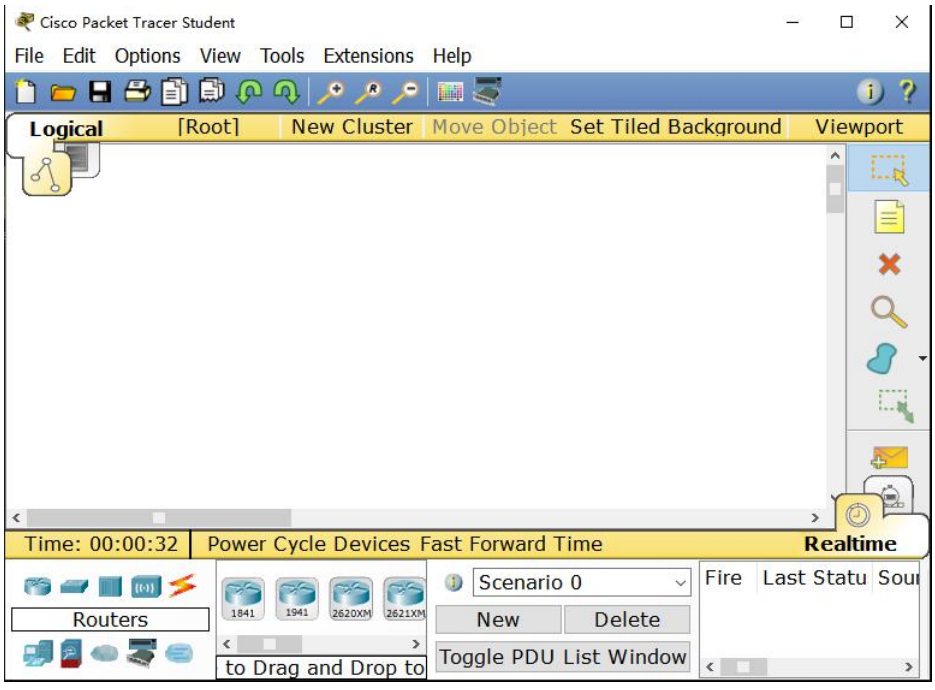
日期：2019 年 12 月 9 日

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**

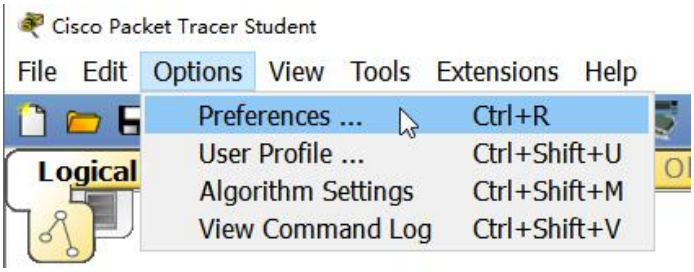
推荐使用 Cisco Packet Tracer 做交换机方面的配置，其他的配置推荐用 GNS3，这两个软件可以到网上下载，然后安装。如果找不到的可以联系作者 sysyear@163.com

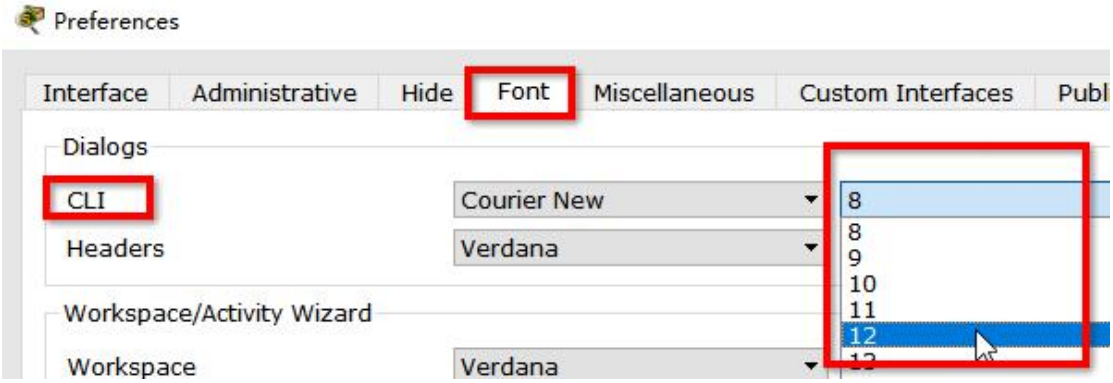
安装完后双击桌面上的图标打开模拟器（Packet Tracer 主界面如下图）



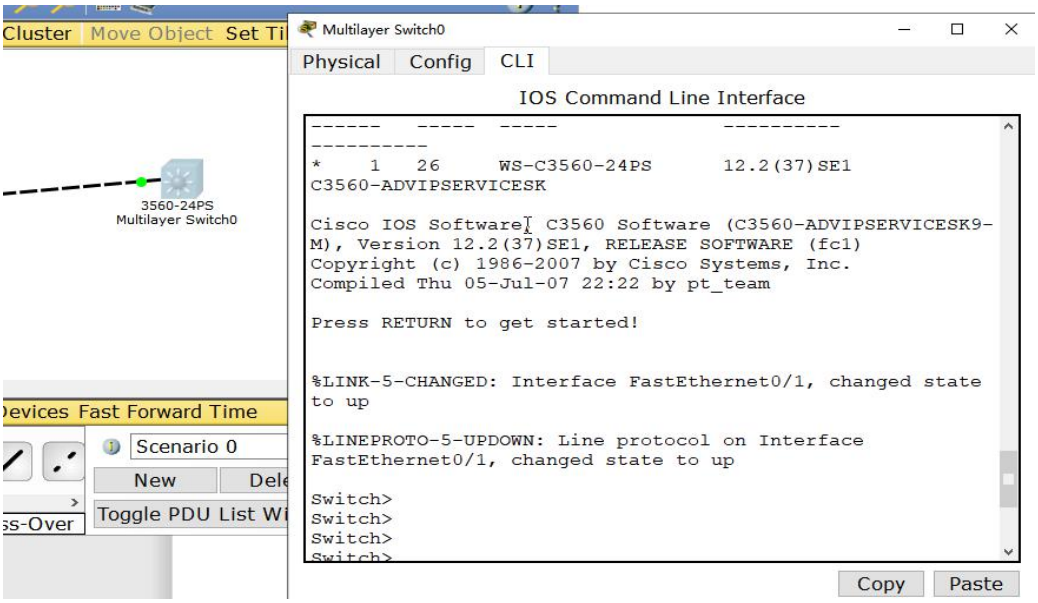
点击左下角的设备图标，拖入设备到主工作区，双击主工作区的图标即可进入命令行配置界面。

但字体太小了，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>
Switch>                    //刚开始进入的是一般模式，提示符为" > "
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
Switch#                            //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]
*别急，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

2.设备登录管理

带内管理（console 本地登录）
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 Switch12　　//先配置主机名
Switch12(config)#ip domain-name xxx.com　　//域名也要配置
Switch12(config)#crypto key generate rsa　　//创建 rsa 密钥
The name for the keys will be: Switch12.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]

Switch12(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
Switch12(config-line)#login local               //使用本地的用户名与密码验证
Switch12(config-line)#transport input ssh       //允许 ssh 登录
Switch12(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
Switch12(config-line)#transport input all       //允许所有远程方式登录
Switch12(config-line)#
```

3.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
```

4.登录超时设置

```
Switch12(config)#line con 0                     //进入目标线路（console）
Switch12(config-line)#exec-timeout 10           //超时时间 10 分钟
Switch12(config-line)#exit                      //空闲时间达到 10 分钟后会断开连接
Switch12(config)#line vty 0 15                  //进入目标线路（远程）
Switch12(config-line)#exec-timeout 15           //超时时间设为 15 分钟
Switch12(config-line)#exi
```

5.系统时间设置

```
Switch12(config)#clock timezone cst 8        //先在配置模式下设置时区 cst 东 8 区
Switch12(config)#exi                         //退回特权模式
Switch12#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
Switch12#
Switch12#show clock            //查看系统时间
18:30:3.739 cst Fri Dec 6 2019
Switch12#
*也可用 ntp
Switch12(config)#ntp authentication-key 1 md5 xxxx
Switch12(config)#ntp server 10.1.1.22 key 1
```

6.定时重启

```
Switch12#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：
Switch12#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

Switch12#reload cancel                       //取消重启
```

7.查看登录的用户

```
Switch12#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

Switch12#
Switch12#clear line 3      //把 3 号 line（vty 0）的用户踢下线
```

8. 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
Switch12(config)#aaa new-model //首次配置 aaa 要使用此命令，之后不用
Switch12(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
Switch12(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
Switch12(config)#line con 0
Switch12(config-line)#login authentication default //使用默认的认证方案
Switch12(config-line)#exit
Switch12(config)#line vty 0 4
Switch12(config-line)#login authentication default
Switch12(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

9.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
Switch12(config)#line con 0
Switch12(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
Switch12(config-line)#exit
*用远程登录时，看不到 console 下的消息，
Switch12(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

10.登录访问控制

```
Switch12(config)#line vty 0 4                  //进入目标线路
Switch12(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
Switch12(config-line)#exit
```

11.配置文件相关操作

```
Switch12#show startup-config          //查看配置文件
Switch12#show running-config          //查看正在运行的配置
```

以上两者的区别是：

startup-config 为保存在设备存储器里的配置文件，对应 **flash:/config.text** 文件

running-config 是正在运行的配置，在系统内存里。

清除配置（谨慎操作）

```
Switch12#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
[OK]
Erase of nvram: complete
%SYS-7-NV_BLOCK_INIT: Initialized the geometry of nvram
Switch12#
Switch12#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

Switch12#show startup-config          //这时查看配置文件，已经没有了
startup-config is not present
Switch12#
Switch12#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 之后立即重启
Building configuration...
Current configuration : 1523 bytes
!
version 12.2
service timestamps log datetime msec
service timestamps debug datetime msec
service password-encryption
!
```

hostname Switch12
!
enable secret 5 1mERr$iVdvDReOoQW.iyI2k9pxs1
Switch12#reload　　//重启系统
Proceed with reload? [confirm]y

直接删除配置文件
Switch12#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
Switch12#copy running-config flash:　　//备份正在运行的配置到文件里
Destination filename [running-config]? confbak20191206.cfg　　//保存的文件名
Building configuration...
[OK]
Switch12#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)
Switch12#
//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。可以参考下一章《启动文件配置》

12.启动文件配置

Switch12#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 :
Config file : flash:/config.text
Private Config file : flash:/private-config.text
Enable Break : no
Manual Boot : no
HELPER path-list :
Auto upgrade : yes
NVRAM/Config file
buffer size: 65536
Switch#
Switch12(config)#boot system flash:/xxxxxxx.bin　　//指定使用的系统镜像文件
Switch12(config)#boot config-file flash:/confback.cfg　　//指定使用的配置文件
//以上有的命令在模拟器里不支持

13.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。

```
Switch12(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

Switch12(config)#line con 0
Switch12(config-line)#motd-banner          //在相应的线路开启 banner
Switch12(config-line)#exit
Switch12(config)#line vty 0 15
Switch12(config-line)#motd-banner
Switch12(config-line)#exit
```

14. SNMP

```
Switch12(config)#snmp-server community pubxxx ro
%SNMP-5-WARMSTART: SNMP agent on host Switch12 is undergoing a warm start
Switch12(config)#
```

15.查看接口信息

```
Switch12#show ip int 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

Switch12# show int vlan1            //查看具体的某个接口的详细信息
Router#show int f0/0
```

16.设置 MTU

```
Switch12(config)#vlan 1
Switch12(config-vlan)#mtu 1500
或者：
Switch12(config)#int vlan 1
Switch12(config-if)#ip mtu 1500
```

17. VLAN 操作

```
Switch12(config)#vlan 10                    //创建 vlan 10
Switch12(config-vlan)#name stuff            //命名该 vlan 为 stuff
Switch12(config-vlan)#exit
Switch12(config)#int vlan 10                //创建 svi
Switch12(config-if)#
*3? 02, 02:24:00.2424: %LINK-5-CHANGED: Interface Vlan10, changed state to up
Switch12(config-if)#ip address 10.1.1.1 255.255.255.0        //配置 IP
Switch12(config-if)#description xxxxx       //描述
Switch12(config-if)#shutdown                //关闭接口
Switch12(config-if)#
*3? 02, 02:24:37.2424: %LINK-5-CHANGED: Interface Vlan10, changed state to
administratively down
Switch12(config-if)#no shutdown             //启用接口
Switch12(config-if)#
*3? 02, 02:24:40.2424: %LINK-5-CHANGED: Interface Vlan10, changed state to up
Switch12(config-if)#exit

Switch12(config)#int range f0/1-5                    //进入一组端口的配置界面
Switch12(config-if-range)#switchport mode access     //将该组端口设为 access 口
Switch12(config-if-range)#switchport access vlan 10  //加入 vlan 10
Switch12(config-if-range)#
*3? 02, 02:26:54.2626: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan10,
changed state to up
Switch12(config-if-range)#exit
Switch12(config)#int f0/24
Switch12(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
Switch12(config-if)#switchport trunk encapsulation dot1q   //要先封装 dot1q 协议
Switch12(config-if)#switchport mode trunk                  //再设置为 trunk 口
Switch12(config-if)#switchport trunk native vlan 1         //设置 native vlan（pvid）
```

```
Switch12(config-if)#switchport allowed vlan 1-20
Switch12(config-if)#switchport trunk allowed vlan 1-20        //只允许 vlan1~20 通过
Switch12(config-if)#                          //思科的 trunk 口默认允许所有 vlan 通过
```

18. VTP

```
Switch12#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.
Switch12(vlan)#exit
APPLY completed.
Exiting....
Switch12#conf t
Switch12(config)#vtp domain vtpcom
Changing VTP domain name from NULL to vtpcom
Switch12(config)#vtp password xxx
Setting device VLAN database password to xxx
Switch12(config)#vtp mode server            //vtp 模式为 server，
                                            //其他交换机要设置为 client
Device mode already VTP SERVER.
Switch12(config)#
```

19.端口操作

```
Switch12(config)#int f0/2           //进入目标端口
Switch12(config-if)#duplex full                 //信道工作模式为全双工
Switch12(config-if)#bandwidth 100000            //带宽设为 100000Kbit/s
Switch12(config-if)#speed 100                   //速率 100M
Switch12(config-if)#exit
Switch12(config)#int f0/5
Switch12(config-if)#no switchport               //设置为路由口
Switch12(config-if)#ip add 10.2.2.2 255.255.255.0
Switch12(config-if)#exit
Switch12#show running-config int f0/5           //查看具体端口上的配置
```

20.广播风暴抑制

```
Switch12(config-if)#storm-control broadcast level pps 800          //限制发包数
Switch12(config-if)#storm-control broadcast level bps 200000       //限制速率
Switch12(config-if)#storm-control broadcast level ?
<0.0-100.0> Enter rising threshold
Switch12(config-if)#storm-control broadcast level 5        //限制为端口速率的 5%
Switch12(config-if)#storm-control action block          //惩戒动作 block,或 shutdown
Switch12(config)#errdisable recovery cause all          //假死恢复
```

21. ARP 相关操作

```
Switch12#show arp                                  //查看 ARP 表
Protocol Address Age (min) Hardware Addr Type Interface
Internet 10.1.1.1 - 00D0.97A9.1ABE ARPA Vlan10
Switch12#show arp | include 10.1.1.          //可以做过滤匹配
Switch12(config)#arp 10.1.1.22 00D0.97A9.1A22 arpa          //添加静态 arp 条目
Switch12(config)#int vlan 1
Switch12(config-if)#arp timeout 180          //在接口上配置 arp 老化时间，秒
Switch12(config-if)#ip proxy-arp             //开启代理 arp
```

22. MAC 相关操作

```
Switch12#show mac-address-table                  //查看 mac 表
Switch12#show mac-address-table | include 00D0.97A9.1A        //仅显示匹配条目
Switch12#clear mac-address-table [dynamic]    //清空 mac 表[仅动态的条目]
Switch12(config)#mac-address-table static 00D0.97A9.1A22 int f0/1 vlan 1
                                                  //添加静态 mac 条目
Switch12(config)#mac-address-table aging-time 300      //mac 老化时间
```

23.端口安全

```
Switch12(config)#int f0/9
Switch12(config-if)#switchport mode access          //只能在 access 口上设置
Switch12(config-if)#switchport port-security        //开启端口安全功能

Switch12(config-if)#switchport port-security maximum 20        //最大允许 20 个
                                                    //mac 地址的数据包进入
Switch12(config-if)#switchport port-security mac-address 00D0.97A9.1A39
                    //添加一条动态的记录
Switch12(config-if)#switchport port-security mac-address sticky       //开启 sticky
Switch12(config-if)#switchport port-security mac-address sticky 00D0.97A9.1A88
                        //添加一条 sticky 记录
Switch12(config-if)#switchport port-security violation protect     //惩戒动作 protect
Switch12(config-if)#
Switch12(config-if)#exit
Switch12(config)#errdisable recovery cause security-violation     //开启假死恢复
```

24.端口聚合

```
Switch12(config)#int port-channel 1                    //创建聚合口
Switch12(config-if)#exit
Switch12(config)#int range f0/20-21                    //选中成员端口 20~21
Switch12(config-if-range)#channel-group 1 mode on      //聚合模式为手动开启
Switch12(config-if-range)#no shut
Switch12(config-if-range)#exit
Switch12(config)#int port-channel 1                    //接下来是对聚合口的操作
Switch12(config-if)#no shut
Switch12(config-if)#switchport trunk encapsulation dot1q
Switch12(config-if)#switchport mode trunk
Switch12(config-if)#exit
Switch12(config)#port-channel load-balance src-dst-mac         //设置负载均衡
```

25. Qos 限速

```
Switch12(config)#mls qos                                    //开启 qos
Switch12(config)#access-list 10 permit 10.1.1.0 0.0.0.255          //acl 匹配目标流
Switch12(config)#class-map class1                           //定义流类
Switch12(config-cmap)#match access-group 10                 //匹配 acl
Switch12(config-cmap)#exit
Switch12(config)#policy-map policy1                         //定义流策略
Switch12(config-pmap)#class class1
Switch12(config-pmap-c)#bandwidth 10000                     //带宽限制为 10000Kbit/s
Switch12(config-pmap-c)#shape average 16000000              //整流平均流量，bit/s
Switch12(config-pmap-c)#exit
Switch12(config)#int f0/3                                   //应用策略到接口
Switch12(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：

```
Switch12(config)#policy-map policy1
Switch12(config-pmap)#class class1
Switch12(config-pmap-c)#police cir 10000000 10000000              //bit/s，byte/s
```

*也可能是下面的命令：

```
Switch12(config)#policy-map policy1
Switch12(config-pmap)#class class1
Switch12(config-pmap-c)#trust dscp
Switch12(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

```
Switch12#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

```
Switch12(config)#service dhcp          //开启 dhcp 服务
Switch12(config)#ip dhcp pool pxx          //创建 dhcp 地址池
Switch12(dhcp-config)#network 10.1.1.0 255.255.255.0      //设置网段
Switch12(dhcp-config)#default-router 10.1.1.1          //网关
Switch12(dhcp-config)#dns-server 8.8.8.8                //dns
Switch12(dhcp-config)#lease 5 4 30                  //租期，单位：日，时，分
Switch12(dhcp-config)#option 43 hex xxxxxxxx       //option 43
Switch12(dhcp-config)#exit
Switch12(config)#ip dhcp excluded-address 10.1.1.1 10.1.1.10    //排除地址段
Switch12(config)#
```

保存 **ip** 分配信息到 **ftp** 服务器上的 **lease.db.cfg** 文件中

```
Switch12(config)#ip dhcp database ftp://user:pass@10.1.1.252/lease.db.cfg
Switch12(config)#
```

开启 **ping** 检测

```
Switch12(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
Switch12(config)#ip dhcp ping timeout 1000          //Ping 超时，毫秒
Switch12(config)#
```

```
Switch12(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

```
Switch12(config)#ip dhcp pool pc1      //创建地址池，只有一个 ip
Switch12(dhcp-config)#host 10.1.1.35 255.255.255.0
Switch12(dhcp-config)#client-identifier 0100.D097.A91A.22
                                       //以 01 开始加上 mac 地址
Switch12(dhcp-config)#default-router 10.1.1.1
Switch12(dhcp-config)#dns-server 8.8.8.8
Switch12(dhcp-config)#exit
```

```
Switch12#show dhcp lease              //查看 dhcp 分配的地址情况
Switch12#show ip dhcp binding         //查看分配的 ip 及绑定的 mac 地址
Switch12#
```

28.DHCP 中继

```
Switch12(config)#int vlan 1
Switch12(config-if)#ip helper-address 10.3.3.1
Switch12(config-if)#exit
//要记得先配置去往 10.3.3.1 的路由
```

29. DHCP snooping

```
Switch12(config)#ip dhcp snooping                    //开启 dhcp snooping
Switch12(config)#int f0/24                           //上联口
Switch12(config-if)#ip dhcp snooping trust           //上联口要设为信任口
Switch12(config-if)#ip dhcp snooping limit rate 50       //限制 dhcp 报文速率
Switch12(config-if)#exit
Switch12(config)#ip dhcp snooping vlan 1-30          //监测的 vlan
Switch12(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
Switch12(config)#
Switch12(config)#errdisable recovery cause dhcp-rate-limit       //假死恢复

Switch12(config)#ip dhcp snooping binding xxxx.xxxx.xxxx vlan 10 ip x.x.x.x int f0/3
Switch12(config)#ip dhcp snooping database flash:/dhcpsnooping.db
Switch12(config)#ip dhcp snooping database write-delay 100
Switch12(config)#
Switch12#show ip dhcp snooping binding        //查看 dhcp snooping 绑定情况
Switch12#clear ip dhcp snooping binding       //清除 dhcp snooping 绑定条目
```

30. 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

①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
```

②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

③MAC 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
```

31.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
```

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
```

33.光模块兼容性

```
Switch(config)#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)#no errdisable detect cause gbic-invalid
                                        //关闭由于光模块不兼容而导致的端口假死
Switch#show int transceiver supported-list      //查看支持列表
```

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
```

35. 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 flash: tftp:                  //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...
```

36. FTP 客户端

```
Switch(config)#ip ftp source-interface vlan 1        //指定访问服务器时的源 ip
Switch(config)#ip ftp username coflee                //ftp 用户名
Switch(config)#ip ftp password xxxx                  //ftp 用户密码
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...
```

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
//出现 cccc 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
```

38. PVST/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          //指定端口优先级
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
Switch#show spanning-tree          //查看 STP 详细信息
```

STP 端口开销表：

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

39.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
```

40. 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
```

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
```

42.交换机 switch 模式

1.重启设备时长按 mode 键（一般位于正面的右边，一个小按钮），直到 sys 指示灯不闪烁，则进入交换机的 switch 模式了
2.switch 模式指示符为 switch>，switch 模式下的常用操作：
①使用 xmodem 传系统镜像文件或配置文件到交换机上

```
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
ccccccc                               //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
```

②修改 console 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>
```

③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
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
```

43.二层交换机设置默认网关

```
Switch(config)#ip default-gateway 10.1.1.254
```

44.三层交换机开启路由转发功能

```
Switch(config)#ip routing
```

路由器的操作，和交换机相同的以下就不列出了

45.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
```

46. 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
```

47. 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
```

48.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
```

49. PPP

```
Router0(config)#int s0/1/1
Router0(config-if)#clock rate 128000           //设置时钟频率
Router0(config-if)#encapsulation ppp           //封装 ppp 协议
Router0(config-if)#bandwidth 128               //设置带宽为 128Kbit
```

```
Router0(config-if)#ppp authentication pap       //使用 pap 验证
Router0(config-if)#ppp pap sent-username coflee password xxxx
                                                //pap 用户名及密码
Router0(config-if)#
Router0(config-if)#ppp authentication chap [callin] coflee          //使用 chap 验证
Router0(config-if)#ppp chap password xxx
```

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
```

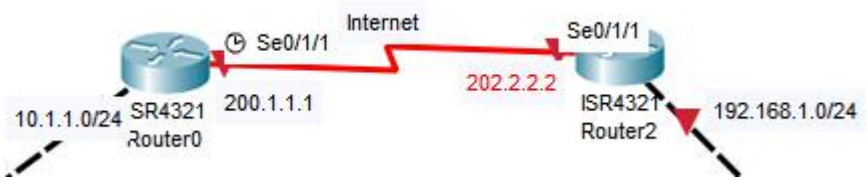
③目的 NAT（端口映射）

```
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
```

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
```

54.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 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              //要传送的文件名
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]
```

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