**第一章　VRP操作基础**   
**1VRP基础**

MiniUsb串口连接交换机的方法

**2eNSP入门**

**3命令行基础(1)**   
eNSP中路由开启后（记住端口）－－－第三方软件连接该路由方法：telnet 127.0.0.1 端口

用户视图（文件）—–系统视图（系统sys）——接口视图（接口 interface GigabitEthernet 0/0/0）——协议视图（路由）

display hotkey 显示功能键   
display clock 显示时间   
clock timezone CST add 8 设置时区（先设时区再设时间）   
clock datetime 设置时间

header login information #   
内容

登录前信息

header shell information 登录后信息（格式同上）Ctrl+] 可以退出查看该信息

用户权限15 命令权限3   
**为console口配置密码：**   
user-interface console 0 ；进入到相应口   
authentication-mode password ；认证模式为passwork   
set authentication password cipher huawei ;设置密码（路由器不需要）

**为vty（telnet）设置密码**   
user-interface vty 0 4   
其它同上   
user privilege level 3；用户命令等级3（管理员）PS：console不用

dis history-command；显示历史命令

**为接口配置2个IP地址**（限路由）   
system-view   
[Huawei]interface gigabitethernet 0/0/0   
[Huawei-GigabitEthernet0/0/0]ip address 10.0.12.1 255.255.255.0   
[Huawei-GigabitEthernet0/0/0]interface loopback 0 ；环回接口（逻辑接口）   
[Huawei-LoopBack0]ip address 1.1.1.1 32

**管理网口配置：**   
注意：华为交换机有单独的管理网口，不占用机器配置表中的网口   
interface MEth0/0/1 //标识有ETH的单独的RJ45网口   
ip address 192.168.5.250 24 //设置管理网口的ip地址和掩码

**汇聚交换机管理IP配置**网关vlanif已在核心交换机内

在汇聚交换机中新加和核心交换机中相同vlanif ，并分配IP（网段同网关）

交换机如何将二层接口转换到三层接口

缺省情况下，交换机的以太网接口工作在二层模式，用户可使用undo portswitch将二层口切换为三层口。

说明：   
交换机在V200R003C00及先前版本，接口切换到三层模式后，不支持配置IP地址。

交换机在V200R005C00版本及后续版本，接口切换到三层模式后，支持配置IP地址。

物理接口是否可以直接配置IP地址

管理接口ETH接口为三层接口，可以直接配IP地址。

业务接口无法直接配IP地址，需要配置Vlanif虚接口，并在该Vlanif下配置IP地址。例如：

[Quidway] vlan 10   
[Quidway-vlan10] quit   
[Quidway] interface vlanif 10   
[Quidway-Vlanif10] ip address 192.168.1.1 24 业务接口也支持在子接口上配置IP地址。

V200R005C00及后续版本，在接口使用命令undo portswitch ，将以太网接口从二层模式切换到三层模式后，支持配置IP地址。

**4.命令行基础(2)**

云配置：udp （入口）1－－－绑定vmware仅主机网卡（出口）2   
要做端口映射   
1－2 双向 2－1 双向

display version   
查看路由器基本信息   
display interface GigabitEthernet 0/0/0   
查看接口状态信息   
display ip interface brief   
查看全部接口的IP简要信息，含IP地址   
display ip routing-table   
查看路由表   
display current-configuration   
查看当前的配置（内存中）   
display saved-configuration   
查看保存的配置（Flash中）   
dir flash:   
查看Flash中的文件   
save   
保存配置文件   
reboot   
重启设备

telnet实验（参照上面命令）   
**3A认证（不同用户不同密码）**   
user-interface vty 0 4   
authentication-mode aaa ；区别password   
user privilege level 15   
－－－－－－－－－－－－－－－－－WEB登陆方式   
aaa   
local-user admin password cipher huawei ;建用户并给密码,已有帐号修改密码   
local-user admin privilege level 15   
local-user admin service-type telnet http ftp ；类型

PS:以前可以用于修改WEB登陆密码

telnet登录后使用dis users 可查看当前登录用户

抓包可以分析出telnet的密码“Follow TCP Stream”

**5.VRP文件系统基础**

cd 改变目录

more 查看文件内容

copy 复制 copy flash:/vrpcfg.zip vrpcfg.zip （拷贝根目录“需加flash”下的配置文件到当前目录）

move 移动

delete 删除

rename 改名

undelete 恢复回收站的文件

pwd显示路径

mkdir 创建目录

rmdir 删除目录

format 格式化

fixdisk 修复文件系统

save 生成cfg.zip

display saved显示保存配置

display cur 显示当前配置

reset saved 删除保存配置 + reboot 第一次Ｎ　　　＝＝＝＝＝＝＝＝＝＝　　设备复位

compare configuration 比较配置文件区别

删除/永久删除文件   
delete /unreserved （dir /all 可查看回收站的文件）   
恢复删除的文件   
undelete   
彻底删除回收站中的文件   
reset recycle-bin

**加载不同的配置文件**   
dis startup ；查看开机信息，其中有加载配置文件的路径   
startup saved-configuration flash:/a.zip ；更改启动配置文件

比较当前配置与下次启动的配置   
compare configuration

**6.VRP系统管理(1)**

路由器做为客户端 :

ftp (FTP服务器地址)

get vrp.cc 下载文件到ftp   
put vrp.zip 上传文件到ftp

TFTP相关   
tftp 10.0.1.184 put（get） vrpcfg.zip

**7.VRP系统管理(2)**

**第二章　静态路由**   
**8.IP路由原理、静态路由基本配置**

**路由的来源：**   
直连路由：链路层发现的路由（direct）   
管理员手工添加：静态路由 （static）   
路由器协议学到的路由：动态路由 （ospf rip）

静态路由特点：   
优：实现简单，精确控制，不占资源   
缺：不适用大型网络，网络变更需要手动改

dis ip routing-table ；查看路由表，直连11条

ip route-static 192.168.23.0 24 Serial 1/0/0 192.168.12.2   
目的 经过（本路由出口） 下一跳（下一路由入口）

交换机写路由时最好省略 “经过”，因为经过的不是接口而是vlan，接口不能直接配IP导致。

ip route-static 10.168.234.232（网络号） 255.255.255.248 GigabitEthernet0/0/1 10.168.234.233（vlanif网关）   
用“子网掩码计算器”：网关+掩码算出“网络号”   
ps：24的掩码算出的是192.168.1.0 （网络号）

**9.静态路由深入分析**   
优先级pre：直连最大0 －－－－OSPF－－－静态   
度量值cost：同一路由下，选择最小开销（多因素）的路径

以上参数，值越小，优先级越高

**匹配原则**：目的地址和路由表的掩码做与，再比较路由中的“目的地址”－－－优先挑掩码大的做匹配

下一跳写法：   
点对点：可以省略下一跳；   
以太网：可以省略出接口；

dis fib ；最终采纳的路由表

递归查询（带R标志）：经过中间多次查询，最终到达目的地址

缺省路由：0.0.0.0 0.0.0.0 网关 ；目的和子网掩码都为0的路由，上互联网都有这条

**10.负载分担、路由备份**   
双线路负载（2条线路同时工作）：平时2条静态方向不同的路由表，可以达到负载的作用；

浮动路由（路由备份，平时只有一条线路工作）：通过其中一条设置成低优先级（添加路由时加preference）的路由，变成浮动（路由表中看不到），出问题才出现

dis ip routing-table 192.168.4.0 verbose ；查看某一目的路由的详细信息

**第三章　RIP**

**11.动态路由协议基础**

常见的动态路由协议有：   
RIP：Routing Information Protocol，路由信息协议。   
OSPF：Open Shortest Path First，开放式最短路径优先。   
ISIS： Intermediate System to Intermediate System，中间系统到中间系统。   
BGP：Border Gateway Protocol，边界网关协议。

分类：   
自治系统内部的路由协议—— IGP：RIPv1/v2、OSPF、ISIS   
自治系统之间的路由协议 —— EGP：BGP

单播，组播

不同路由协议不能直接互相学习，但可以通过路由引入来导入不同的协议

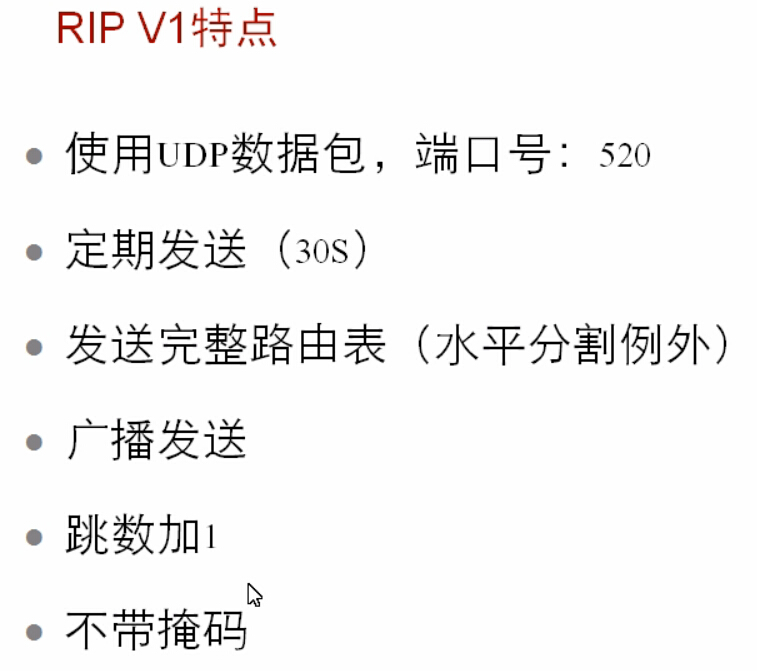
**12.RIP简单介绍及基本配置**

度量值：跳；最多不可以超过15跳

2个路由学习时，更新是一个方向，学回后的路由指向是相反方向

RIP1.0 ： UDP：520端口 工作在应用层

**RIP 基本配置**   
rip   
network 10.0.0.0 ;只支持主类网络 10.0.1.254 必须写成10.0.0.0



rip 1 ；进入相关进程   
silent-interface GigabitEthernet0/0/0 ；静默（关闭）某接口发送

**第四章　OSPF**

**20.OSPF基本原理及基本配置**

开放式最短路径优先（OSPF）   
链路状态路由协议   
无环路   
收敛快   
扩展性好   
支持认证

OSPF报文封装在IP报文中，协议号为89。

OSPF工作原理：路由通过LSA泛洪－－－收集到路由数据库（LSDB）－－－通过SPF算法－－－根据自身算出最短路由 （交换的不是路由表，而是数据库）

hello报文建立邻居关系－－－邻接（同步数据库，full状态）

OSPF区域：分区域为了减小数据大小

配置方法：   
ospf   
area 0；进入到0区域   
network 10.1.1.0 0.0.0.255（代表10.1.1.0网段） ;把该路由器上地址为10.1.1.X 网段的接口应用ospf,有2个方向就要有2个network

同等 10.1.0.0 0.0.255.255 同等 0.0.0.0 255.255.255.255

dis ospf peer brief ；查看ospf邻居信息

**第七章　访问控制列表**

**35.基本ACL介绍**   
ACL是用来实现流识别功能的。   
ACL（Access Control List，访问控制列表）是定义好的一组规则的集合，通常用于:   
标识感兴趣网络流量   
过滤经过路由器的数据包

**分类：**   
基本ACL：2000～2999 报文的源IP地址   
高级ACL：3000～3999 报文的源IP地址、目的IP地址、报文优先级、IP承载的协议类型及特性等三、四层信息

配置ACL的过程：实际上就是告诉路由器允许或者拒绝某些数据包

ACL难点：通配符、语句顺序、方向性

**单台：**   
rule 10 permit source 10.1.1.1 0.0.0.0   
允许来自10.1.1.1主机的IP数据包通过   
rule 10 deny source 10.1.1.2 0.0.0.0   
拒绝自10.1.1.2主机的IP数据包通过

**多台：**   
rule 10 permit source 10.0.0.0 0.255.255.255   
允许来自IP地址为10.×.×.×（即IP地址的第一个字节为10）的主机的数据包通过。

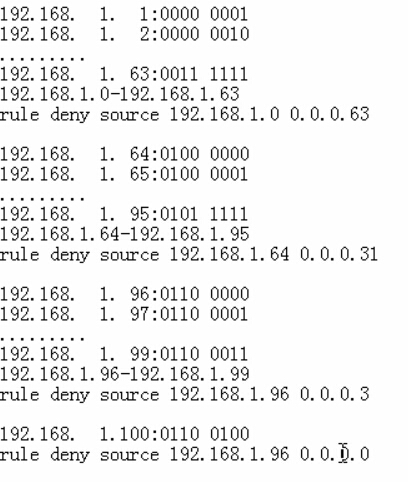
**例子：**

允许来自10.0.0.0/255.255.255.0的IP数据包通过   
rule 5 permit source 10.0.0.0 0.0.0.255 ；掩码位反过来（简单的0和25，复杂）   
复杂255.224.0.0 写的话主是 0.31.255.255 224对应机器数32－1＝31

**特殊的通配符掩码** 0 关心位 255 不关心位X   
1.permit source any   
= permit source 0.0.0.0 255.255.255.255   
= permit   
2.permit source 172.30.16.29 0 某一具体主机   
= permit source 172.30.16.29 0.0.0.0

ACL顺序匹配：一但匹配成功，后面的列表将不再检查（比较苛刻的放前面）   
未命中规则（一条都不匹配）：不同模块处理不一样。如果是转发模块，则转发数据包；如果是telnet模块，则不允许;如果是路由过滤，不允许路由通过。

禁止192.168.1.1－192.168.1.100思路

   
PS：最后一条，96应该是100

**例子：**   
acl 2000   
rule………………..   
int gi0/0/0 ;进入相关接口   
traffic-filter inbound acl 2000 ；应用到相关接口

dis acl 2000 ；查看   
dis traffic-filter applied-record ；查看接口（方向）应用了哪个列表

**36.基本ACL应用案例**

**禁止telnet ：**   
user-interface vty 0 4 ；进到vty   
acl 2999 inbound ；应用到该接口，和物理接口有区别

rule primit ; ACL中加这名是因为，ACL匹配未成功后，telnet模块，不允许通过数据包

telnet -a 10.2.2.1 192.168.12.1 ；－a参数，以指定IP源telnet

**时间控制：**   
time-range work-time 9:0 to 18:00 working-day 6 ；定义“work-time” 星期一到六   
acl 2001   
rule deny time-range worktime ；上班时间不允许上网   
rule permit

禁止学习某路由表；   
rip 1 ； 进到相关rip   
filter-policy（过滤策略） 2000 export ;2000为定义的acl ，export 代表向外发布；import代表我要学习

自动让匹配宽松的放前面，苛刻的放后面   
acl 2200 match-order auto

**37.高级ACL**   
acl number 3000 ;高级   
rule 5 permit tcp destination 172.2.0.250 0 destination-port eq www   
；允许所有机器TCP访问目标机器的www 服务   
rule 10 deny ip destination 172.2.0.250 0 ；拒绝所有的IP协议（包括icmp）访问

traffic-filter inbound acl 3000；进入端口，并应用

**ACL放置位置**

基本ACL尽可能靠近目的   
高级ACL尽可能靠近源

**内可以ping外，外不可以ping内**（ping 分析： 去类型为：echo 回类型为：echo-reply）   
acl number 3000   
rule 5 deny icmp icmp-type echo   
rule 10 permit ip   
traffic-filter inbound acl 3000

**内可以telnet外，外不可以telnet内**（tcp三次握手，第一个包不带ack位）   
rule 8 permit tcp tcp-flag ack ；放行带ack的   
rule 9 deny tcp ；拒绝不带ack的

**第八章　网络地址转换**

**38.静态NAT、动态NAT**

静态nat 和外网地址一一对应，n–n 不能减少公网地址；

**环回口配置**   
int lookback 1   
ip add 192.168.1.1

ip route-static 0.0.0.0 0 gi0/0/1 61.0.0.2 ；要上网的路由需加的路由表

**静态nat配置**   
int gi0/0/1 ；进入外网接口   
nat static global 61.0.0.11（公网IP，不一定是接口IP） inside 192.168.1.1   
特点：发包源IP地址转换 收包目的IP地址转换   
dis nat static ;查看静态nat

**动态nat配置**   
int gi0/0/1 ；进入外网接口   
acl 2000 ;定义acl编号   
rule permit source 192.168.1.0 0.0.0.255 ；地址范围内网   
nat address-group 1 61.0.0.11 61.0.0.20 ；外网地址范围   
nat outbound 2000 address-group 1 no-pat ；先内后外 no-pat 不做端口转换   
特点：100对50 只能节省部分地址   
dis nat session all ;显示 nat 转换情况

**39.PAT、NAT服务器**

**NAPT or PAT （端口地址转换）** ：动态端口转换   
设置同动态NAT   
nat outbound 2000 address-group 1 ；先内后外 与动态NAT区别：no-pat

对网关的配置：

[R3]acl 2000

[R3-acl-basic-2000]rule 5 permit source any

[R3]nat address-group 1 34.1.1.100 34.1.1.100

[R3-GigabitEthernet0/0/2]nat outbound 2000 address-group 1

**Easy IP 配置** （家庭使用，没有固定IP）   
nat outbound 2000 ；只指定源IP

**端口映射**   
nat server protocol tcp global 202.10.10.1 www inside 192.168.1.1 8080

**第一十一章　交换基础、VLAN**

**50.VLAN原理和配置**   
简单vlan配置   
vlan 10 ；创建 valn   
dis vlan   
dis port vlan ；接口vlan状态   
int eth0/0/0   
port link- type access ；接口类型   
port default vlan 10 ；配置

Access端口在收到数据后会添加VLAN Tag，VLAN ID和端口的PVID相同。   
Access端口在转发数据前会移除VLAN Tag。

当Trunk端口收到帧时，如果该帧不包含Tag，将打上端口的PVID；如果该帧包含Tag，则不改变。   
当Trunk端口发送帧时，该帧的VLAN ID在Trunk的允许发送列表中：若与端口的PVID（trunk2端pvid必须相同，默认是1）相同时，则剥离Tag发送；若与端口的PVID不同时，则直接发送。

vlan batch 10 20 30 ; 批量10 to 30 （10，11，12.…………30）

**配置Trunk**   
int gi0/0/1   
port link-type trunk   
port trunk allow-pass vlan all ；允许通过的vlan   
port trunk pvid vlan 1 ；改变pvid ,默认是1

dis port vlan active ;查看trunk接口是否打标记，T or U



PS：取消Trunk   
undo port trunk allow-pass vlan all   
port trunk allow-pass vlan 1   
port link-type access

**51.Hybrid接口**

访端口可以连任何设备

**GVRP**

GVRP [交换机](https://baike.baidu.com/item/%E4%BA%A4%E6%8D%A2%E6%9C%BA)之间能够相互交换 VLAN 配置信息

配置：

Vlan 10

inter g0/0/1

port link-type access

port default vlan 10

首先要在全局启用gvrp

Gvrp

然后在端口（声明为trunk的端口）处启用gvrp

Gvrp

#

interface GigabitEthernet0/0/2

port link-type trunk

port trunk allow-pass vlan 2 to 4094

gvrp

#

**第一十三章　VLAN间路由、VRRP**

**58.单臂路由实现VLAN间路由**

**每个vlan一个物理连接（一条线）**   
交换机与路由2根线（有几个VLAN就有几根线） PS：缺点   
交换机端：该端配置和“客户端口”相同   
路由端：只需配IP（网关）

**单臂路由**

将交换机和路由器之间的链路配置为Trunk链路，并且在路由器上创建子接口以支持VLAN路由。

交换机端：跟路由直连的端口配置trunk   
路由器端：   
[RTA]interface GigabitEthernet0/0/1.1 ；定义子接口   
[RTA-GigabitEthernet0/0/1.1]dot1q termination vid 2 ；分配VLAN   
[RTA-GigabitEthernet0/0/1.1]ip address 192.168.2.254 24 ；配置网关   
[RTA-GigabitEthernet0/0/1.1]arp broadcast enable ；开启ARP广播

**59.三层交换实现VLAN间路由**

2层+路由器 路由配虚拟端口vlan 和网关   
[SWA]interface vlanif 2 ； 2同相关VLAN号   
[SWA-Vlanif2]ip address 192.168.2.254 24 ；网关PS：该地址不能在其它VLAN网段中出现

**复杂模式：三层接二层（带管理）**   
中间设置成trunk，三层也要建和二层相关VLAN，int vlanif放在三层上。

**第一十四章　交换机端口技术**   
**63链路聚合(手工模式)**

[SWA]interface Eth-Trunk 1   
[SWA-Eth-Trunk1]interface GigabitEthernet0/0/1   
[SWA-GigabitEthernet0/0/1]eth-trunk 1   
[SWA-GigabitEthernet0/0/1]interface GigabitEthernet0/0/2   
[SWA-GigabitEthernet0/0/2]eth-trunk 1

dis eth-trunk 1 ；查看链路

PS: trunk端口下做链路聚合方法：先做链路聚合，然后在int eth-trunk 数字下做Trunk

**72.防火墙技术**

按照防火墙实现的方式，一般把防火墙分为如下几类：   
包过滤防火墙：简单，每个包都要检查，缺乏灵活性，策略多影响性能   
代理型防火墙：安全，但不方便，针对性强（http代理），不通用   
状态检测防火墙：基于连接状态，结合以上2种防火墙的优点

只防网络层和传输层，不防应用层（比如网站漏洞）；   
防外不防内；

**防火墙的安全区域：**

Local（100网网）－－－－Trust（85外网）   
－－－－－DMZ（50WEB服务器）   
高可以访问低，低不可以访问高

**配置思路**   
配置安全区域和安全域间。   
将接口加入安全区域。   
配置ACL。   
在安全域间配置基于ACL的包过滤。

**1.在AR2200上配置安全区域和安全域间**   
system-view   
[Huawei] firewall zone trust   
[Huawei-zone-trust] priority 15   
[Huawei-zone-trust] quit   
[Huawei] firewall zone untrust ；取消接口安全域命令 undo zone   
[Huawei-zone-untrust] priority 1   
[Huawei-zone-untrust] quit   
[Huawei] firewall interzone trust untrust ；配置（进入）域间   
[Huawei-interzone-trust-untrust] firewall enable ；开启该域间的防火墙   
[Huawei-interzone-trust-untrust] quit

**2.在AR2200上将接口加入安全区域**   
int gi0/0/1   
zone OUTSIDE ；相关接口加入到相关区域（华为防火墙：如果不加入的话，与之相连的PC不能访问该端口，和路由有区别）

PS：以上另外等价方法   
firewall zone trust ；进入相关区域   
add int gi0/0/1 ；加入相关端口

PS： dis firewall session all ；查看防火墙的所有会话信息

**3.在AR2200上配置ACL** （允许外网可以telnet内网）   
acl 3001   
rule permit tcp destination 192.168.1.100 0 destination-port eq 23 ；允许telnet   
firewall interzone INSIDE OUTSIDE ；进入相关域间   
packet-filter 3001 inbound；应用相关acl

FTP的主动（FTP本身），被动（客户端）模式

内网访问外网FTP，FTP主动模式（PORT）不能传数据（经常外网FTP服务器访问不了，FTP下载软件要改成被动模式），但被动模式（PASV）可以访问

**ASPF配置**工作在应用层，检测http、FTP等，可以为这些协议打开放行通道   
firewall interzone INSIDE OUTSIDE；进入到相关区域   
detect aspf all ；开启检测

**帧中继协议**

**R1**

#

interface Serial0/0/0

link-protocol fr

#

inter s0/0/0.1 p2p

#

interface Serial0/0/0.1

ip address 12.1.1.1 255.255.255.0

#

inter s0/0/0.2 p2mp

#

interface Serial0/0/0.2

fr map ip 134.1.1.3 103 broadcast

fr map ip 134.1.1.4 104 broadcast

ip address 134.1.1.1 255.255.255.0

#

R2

#

interface Serial0/0/0

link-protocol fr

ip address 12.1.1.2 255.255.255.0

#

R3

#

interface Serial0/0/0

link-protocol fr

undo fr inarp

fr map ip 134.1.1.1 301 broadcast

ip address 134.1.1.3 255.255.255.0

#

R4

#

interface Serial0/0/0

link-protocol fr

undo fr inarp

fr map ip 134.1.1.1 401 broadcast

ip address 134.1.1.4 255.255.255.0

#

**PPPoE**

**Server：**

[server]ip pool pppoepool

#

ip pool pppoepool

gateway-list 12.1.1.254

network 12.1.1.0 mask 255.255.255.0

#

[server]aaa

[server-aaa]local-user huawei password cipher Huawei

[server-aaa]local-user huawei service-type ppp

[server]int Virtual-Template 1