

一、网络基础知识

1、什么是计算机网络

硬件方面：通过线缆将网络设备和计算机连接起来；

软件方面：操作系统，应用软件，应用程序通过通信线路互联；

作用：

实现资源共享，信息传递，增加可靠性，提高系统处理能力

2、标准化组织

ISO（国际标准化组织）

IEEE（电气和电子工程师协会）

3、WAN与LAN

WAN（广域网）：

范围：几十到几千千米；

作用：用于连接远距离的计算机网络；

应用：Internet；

LAN(局域网)：

范围：1km左右；

作用：用于连接较短距离内的计算机；

应用：企业网，校园网；

4、网络设备生产厂商

华为；

Cisco(思科)；

5、网络拓扑结构

1》点对点拓扑结构：

两台设备之间有一条单独的连接；

作用：

专用于广域网中连接的两台路由器；

2》星型拓扑：

优点：

易于实现；

易于网络扩展；

易于故障排查；

缺点：

中心节点压力大；
组网成本较高

3》网状拓扑结构：

一个节点与其他节点相连；

优点：

提供冗余性和容错性；

可靠性高；

缺点：

组网成本高；

6、OSI七层模型（理论框架）

应用层：应用程序，准备好数据，向下发送到表示层；

表示层：负责数据形式的表示，比如声音用mp3，加密、压缩；

会话层：负责建立到远端的会话；

传输层：负责将数据拆分成数据段segment，并添加序列号，以及源和目标的端口号。如果需要可靠传输，采用TCP；否则使用UDP；

网络层：负责将数据打包package，添加源和目标的IP地址。网络层重要设备是路由器，负责选择路径，将数据包发往目的地；

数据链路层：负责将数据封装成帧frame，添加源和目标的MAC地址。重要设备是交换机；

物理层：将数据表示成2进制的0和1，叫比特bit，在介质上发送；

7、TCP/IP五层模型（实际应用）

应用层：	上层数据	-----》计算机	HTTP, FTP, TFTP, SMTP, SNMP, DNS
传输层：	数据段	-----》防火墙	TCP, UDP
网络层：	数据包	-----》路由器	ICMP, IGMP, IP, ARP
数据链路层：	数据帧	-----》交换机	VLAN, TRUNK, MSTP
物理层：	比特流	-----》网卡	

8、什么是协议

为了使数据可以在网络上从源传递到目的地，网络上所有设备需要“讲”相同的“语言”；
描述网络通信中“语言”规范的一组规则就是协议；

9、以太网接口

RJ-11:四根线序，连接电话；

RJ-45:八根线序，最常用的规范（廉价稳定）；

RJ-----》描述公用电信，代表网络的接口

10、线序的选择

直通线：线缆两头的线序相同；
交叉线：线缆两头的线序不同；
有交换机时用直通线（一条线连接的两台设备）；
没有交换机时用交叉线（一条线连接的两台设备）；

11、线序类型

T568A：白绿，绿，白橙，蓝，白蓝，橙，白棕，棕
T568B：白橙，橙，白绿，蓝，白蓝，绿，白棕，棕
标准网线（直通线）：
T568A ----- T568A
T568B ----- T568B
交叉网线（交叉线）：
T568A ----- T568B

12、双绞线（网线）

概念：
1》目前使用最广，价格相对便宜的一种传输介质；
2》由两根绝缘铜导线相互缠绕组成，以减少对邻近线的电气干扰；
双绞线的标准：
类型 传输速率
cat5 100Mbps
cat5e 100Mbps
cat6 1000Mbps----->服务器常用
cat7 10000Mbps----->使用需要万兆网卡，少用

13、中继器（物理层设备）

作用：
放大信号；
延长网络传输距离；
网线一般不要超过150米，否则会丢失数据，可以加一个中继器。

14、IP地址

IP地址是网络层地址。低层次设备不能有高层地址，所以IP地址不能配置在二层交换机的端口上：
1》IP地址由32个二进制数构成。总体上可以分为两部分：网络位+主机位；
2》为了方便表示，人为地，将8位换算成10进制数，共4段。4段数字用小数点分隔，称作点分10进制的表示方式；
3》相同的网络，网络部分相同；主机部分一定不同；
4》不同的网络，网络部分一定不同；主机部分可以相同；

子网掩码：
1》用于判定一个IP地址的网络部分和主机部分；
2》网络部分全写为1，主机部分写为0；

3》1对应的部分是网络，0对应的部分是主机；

二层交换机连接的主机处于同一网络；路由器连接不同的网络，路由器的每个端口都是不同网络。

IP地址分类：

A类：1 - 127	网络位+主机位+主机位+主机位	255.0.0.0(掩码)
B类：128 - 191	网络位+网络位+主机位+主机位	255.255.0.0
C类：192 - 223	网络位+网络位+网络位+主机位	255.255.255.0
D类：用于多播，也叫组播		
E类：保留		

私有地址(网段)：

A：10.0.0.0/8	/8表示网络位是8位	10.0.0.1 ~ 10.255.255.255
B：172.16.0.0 - 172.31.0.0/16		176.16.0.1 ~ 176.31.255.255
C：192.168.0.0/16		192.168.0.1 ~ 192.168.255.255

二、交换机（华为设备）

1、基础命令

设备配置时，有不同的视图模式，代表了不同的配置权限等。在不同的视图模式下，可以执行的命令也不相同：

- 1》 用户视图模式：只能执行一些基础配置和查看；
- 2》 系统视图模式：可以执行很多全局生效的配置操作；
- 3》 接口视图模式：配置只对当前接口生效；

配置时，可以按"?"来查看可用的命令。按回车，逐行向下翻，按空格键，逐屏向下翻，按"q"退出；

基础命令：

```
<Huawei>language-mode Chinese    //更改语言为中文
<Huawei>system-view               //进入系统视图
<Huawei>undo info-center enable    //关闭设备日志输出
<Huawei>info-center enable         //开启设备日志输出
[Huawei]sysname sw1               //修改主机名
[sw1]display interface brief       //查看接口的简要信息
[sw1]interface GigabitEthernet 0/0/1    //进入千兆接口0/0/1
[Huawei-GigabitEthernet0/0/1]quit      //返回上一级,按"ctrl+z"或输入return直接返回到用户视图
[sw1]
```

信息不提示命令

```
//取消控制台的错误，日志等各种提示信息
<Huawei>undo terminal debugging
<Huawei>undo terminal monitor
<Huawei>undo terminal logging
```

```

<Huawei>undo terminal trapping
<Huawei>system-view

//华为模拟器10分钟会自动关闭，进入console 0,设置超时为0，永不自动关机
[Huawei]user-interface console 0
[Huawei]idle-timeout 0

//一起执行上述命令，在用户试图下，复制，粘贴
undo terminal debugging
undo terminal monitor
undo terminal logging
undo terminal trapping
system-view
user-interface console 0
idle-timeout 0

```

2、交换机常用命令（设置密码）

```

<sw1>display version      //显示版本
<sw1>system-view          //进入系统视图
[sw1]display current-configuration    //查看当前配置（内存中的配置）

配置密码：
[sw1]aaa      //进入3a模式
//Authentication认证：你是谁
//Athorization授权：你能干什么
//Audit审计：你都干了什么
[sw1-aaa]local-user 用户名 password cipher 密码      //创建加密的密码
[sw1-aaa] quit      //退到系统视图
[sw1]user-interface console 0      //进入控制台接口模式
[sw1-ui-console0]authentication-mode aaa      //启用aaa认证
[sw1-ui-console0]return      //退回到用户视图
<sw1>quit      //退出到最外层，相当于手机锁屏

<sw1>save      //保存，输入y确认保存，再回车，使用默认的文件名
<sw1>reboot      //重启，回答y确认需要重启

<sw1>display saved-configuration      //查看存盘的配置

恢复出厂设置：
<sw1>reset saved-configuration      //回答y，清除已存盘配置
<sw1>reboot      //先回答n，不存盘当前配置，再回答y，重启

自定义控制台会话超时时间（相当于手机锁屏时间）：
[sw1]user-interface console 0
[sw1-ui-console0]idle-timeout 分钟数

```

3、数据链路层解析

以太网MAC地址：

用来识别一个以太网上的某个单独的设备或一组设备；

IP地址 32位(二进制) 十进制 跨网络的数据传递(长距离)；

MAC地址 48位(二进制) 十六进制 同局域网内的数据传递(短距离)；

MAC地址的前24位是供应商标识，后24位是供应商对网卡的唯一编号；

数据传输：

IP地址[1] -----> IP地址[2]

MAC(1) -> MAC(2) -> MAC(2)

单播：一对一的数据传递；

组播：一对多的数据传递；

广播：一对所有的数据传递

以太网帧格式：

数据链路层的协议数据单元

MAC，物理地址，硬件地址-----》说的都是MAC地址；

bit 比特(网速用) 8bit(比特) = 1byte(字节)

byte 字节(存储量) 100Mb(比特) = 12MB(字节)

mtu-----》最大传输单元(1500)，每一帧最大传输1500字节

4、广播域

只接收同样广播消息的节点的集合：

在该集合中的任何一个节点传输一个广播帧，则其他所有能接收到这个帧的节点都被认为是该广播帧的一部分；

交换机的所有接口默认属于同一个广播域；

5、以太网交换机（交换机）

用来连接局域网的主要设备，交换机能够根据以太网帧中的目标地址只能的转发数据，因此交换机工作在数据链路层；

交换机转发原理：

1》初始状态(一无所知)；

2》MAC地址学习(将源地址记录到MAC地址表中)；

3》广播未知数据帧(广播目的地址，接收方回应，交换机记录接收方的源MAC地址到MAC地址表中)

原理过程：

1》学习--》MAC地址表是交换机通过学习接收的数据帧的源MAC地址来形成的；

2》广播--》如果目标地址在MAC地址表中没有，交换机就向除接收到该数据帧的接口外的其他所有接口广播该数据帧；

3》转发--》交换机根据MAC地址表单播转发数据帧；

4》更新--》交换机MAC地址表的老化时间是300秒，交换机如果发现一个帧的源接口和MAC地址表中的源MAC地址的所在接口不同，交换机将MAC地址重新学习到新的接口；-----注意：断电，拔网线，过300秒都会使MAC地址表变化

6、VLAN技术及应用

什么是VLAN：

(虚拟局域网)是物理设备上连接的不受物理位置限制的用户的一个逻辑组；

为什么引入VLAN：

- 1》交换机的所有接口默认属于同一个广播域；
- 2》随着接入设备的增多，网络中广播增多，降低了网络的效率；
- 3》为了分割广播域，引入了VLAN

VLAN的作用：

- 1》广播控制；
- 2》增加安全性；
- 3》提高带宽利用；
- 4》降低延迟

VLAN的最大数量(默认)：4096个(vlan0默认保留，从vlan1开始，vlan1是默认存在的，所有接口默认属于vlan1)

7、配置VLAN

1>查看VLAN

查看VLAN，默认所有接口都处于vlan1

```
[sw1]display vlan
```

2>创建VLAN

```
[sw1]vlan 2      //创建vlan2
[sw1-vlan2]description 企划部    //定义vlan的描述信息
[sw1-vlan2]display this    //查看当前模式下的配置
[sw1]vlan 3 6 8    //创建多个vlan
[sw1]vlan batch 11 to 20    //创建连续的多个vlan
```

3>删除VLAN

```
[sw1]undo vlan 15      //删除单个vlan
[sw1]undo vlan batch 5 7    //同时删除多个vlan
[sw1]undo vlan batch 11 to 14    //删除连续的多个vlan
```

4>将端口加入VLAN

端口模式分为接入和中继：

- 1》接入端口：仅能属于一个VLAN；
- 2》中继端口：不属于任何VLAN，但是可以承载所有VLAN的数据；

access接入类型，一般应用在交换机与PC终端相连的接口上；

将单个端口加入vlan2：

```
[sw1]interface ethernet 0/0/1
[sw1-ethernet0/0/1]port link-type access
[sw1-ethernet0/0/1]port default vlan 2
```

将不连续的端口加入到vlan2,首先创建端口组，再对端口进行配置：

```
[sw1]port-group 1
[sw1-port-group-1]group-member ethernet0/0/2 ethernet0/0/5
[sw1-port-group-1]port link-type access
[sw1-port-group-1]port default vlan 2
```

将连续的端口加入到vlan3

```
[sw1]port-group 1
[sw1-port-group-1]group-member ethernet0/0/3 to ethernet0/0/5
[sw1-port-group-1]port link-type access
[sw1-port-group-1]port default vlan 3
```

8、trunk中继

trunk干道类型，一般应用在交换机和交换机相连的接口上；

特点：

- 1》用在交换机之间，可以实现不同交换机上相同VLAN通信；
- 2》中继链路不属于任何VLAN；
- 3》中继链路可以承载所有VLAN的数据；

```
[sw1]interface GigabitEthernet 0/0/1
[sw1-gigabyte0/0/1]port default vlan 1 //恢复为默认配置
[sw1-gigabyte0/0/1]port link-type trunk //修改接口类型为trunk
[sw1-gigabyte0/0/1]port trunk allow-pass vlan all //允许所有vlan通过
```

9、链路聚合

也叫以太网通道，如果交换机之间只有一条线路，这条链路可能成为网络的瓶颈；

可以在交换机之间再增加额外的链路，使多条链路成为一个逻辑链路；

参与链路聚合的端口需要有相同的状态，如链路类型、速率

```
[sw1]clear configuration GigabitEthernet 0/0/1 //清除g0/0/1的自定义配置
[sw1]interface Eth-trunk 1 //创建Eth-trunk 1端口
[sw1]trunkport GigabitEthernet 0/0/1 0/0/2 //将两个端口加入到Eth-trunk 1中
[sw1]port trunk allow-pass vlan all //允许所有vlan通过这个端口
[sw1]display eth-trunk //查看加入的物理成员接口
[sw1]display interface Eth-trunk //查看聚合后的带宽
[sw1]clear configuration interface g0/0/1 //恢复接口默认配置
```

三、网络层

1、网络层功能

- 1》定义了基于IP协议的逻辑地址；
- 2》连接不同的媒介类型；
- 3》选择数据通过网络的最佳途径

2、ICMP协议（Internet控制消息协议）

ICMP协议通过IP数据报传送，用来发送错误和控制信息；ICMP工作在网络层，用来测试两个IP地址是否可以通信；

ICMP定义了很多信息类型：

- 1》目的不可达；
- 2》TTL超时；
- 3》信息请求；
- 4》信息应答；
- 5》地址请求；
- 6》地址应答

ICMP检测双向通道的连通性；

ping命令使用ICMP协议

3、ARP（地址解析协议）

用来将IP地址解析为MAC地址；

工作方式是广播

```
[root@room8pc16 network]# arp -n //显示本机的arp缓存,linux系统
```

4、三层交换机（华为设备）

三层交换机，既具有二层交换功能，又具有三层路由功能；

配置三层交换机，只要把vlan当成端口，配置IP地址即可；

VLAN端口物理上不存在，所以叫作交换虚拟端口（SVI）。

现有三层交换机S5700一台LSW3，两台二层交换机S3700两台LSW1和LSW2：

```
[Huawei]vlan batch 2 3 //所有交换机上创建vlan2和vlan3
```

在LSW1上，端口1，2加入vlan2；端口3，4加入vlan3：

```
[sw1]port-group 1
[sw1-port-group-1]group-member e0/0/1 e0/0/2
[sw1-port-group-1]port link-type access
[sw1-port-group-1]port default vlan 2
[sw1]port-group 2
[sw1-port-group-2]group-member e0/0/3 e0/0/4
[sw1-port-group-2]port link-type access
[sw1-port-group-2]port default vlan 3
```

在所有交换机之间创建中继链路：

```
[sw1]interface GigabitEthernet 0/0/1
[sw1-gigabyte0/0/1]port link-type trunk
[sw1-gigabyte0/0/1]port trunk allow-pass vlan all
```

三层交换机配置三层交换：

每个VLAN必须是不同网络；

vlan端口的IP地址是该vlan的网关；

```
[sanceng]interface vlanif 2
```

```
[sanceng-vlanif2]ip address 192.168.1.1 24 //24表示网络位有24位
[sanceng]interface vlanif 3
[sanceng-vlanif3]ip address 192.168.3.1 24
[sanceng]display interface vlanif //查看所有虚拟IP
```

网络通信时，发送端判断自己与目标是不是同一网络，如果是则直接发送，如果不是则发送给网关。

5、路由器（华为设备）

路由：

路由，就是选择路径；

选择路由的方式有静态和动态之分。静态是管理员手工配置的，动态路由是通过路由协议自动学习来的。

路由器工作原理：

路由器根据路由表做出数据包的转发决定；

路由表中存储的是最佳路径，而不是全部路径；

路由器如果发现目标地址未知，则丢弃数据包

路由表的形成：

路由器端口配置上IP地址，就会出现到该网络的直连路由；

管理员手工配置静态、缺省路由；

管理员还可以配置路由协议，路由器自动学习路由。

```
[R1]interface GigabitEthernet 0/0/0 //进入千兆端口0/0/0
[R1-gigabyte0/0/0]ip address 192.168.1.1 24 //给端口配置IP地址，24为子网掩码
[R1]interface GigabitEthernet 0/0/1 //进入千兆端口0/0/1
[R1-gigabyte0/0/1]ip address 192.168.2.1 24
[R1]display ip routing-table //查看路由表
```

静态路由配置：

ip route-static 目标网络 掩码长度 下一跳的地址

```
[R1]ip route-static 192.168.3.0 24 192.168.2.2
```

```
[R2]interface GigabitEthernet 0/0/0 //进入千兆端口0/0/0
[R2-gigabyte0/0/0]ip address 192.168.3.1 24
[R2]interface GigabitEthernet 0/0/1
[R2-gigabyte0/0/0]ip address 192.168.2.2 24
[R2]display ip routing-table //查看路由表
//静态路由 ip route-static 目标网络 掩码长度 下一跳的地址
[R2]ip route-static 192.168.1.0 24 192.168.2.1
```

```
[R1]display ip routing-table //查看R1路由表信息
```

```
[R2]display ip routing-table //查看R2的路由表信息
```

6、动态路由协议OSPF

OSPF，全称开放式最短路径优先：

适合大中型网络使用：

OSPF区域：

为了适应大型的网络，OSPF在网络内部划分多个区域；

每个OSPF路由器只维护所在区域的完整链路状态信息；

区域ID：

区域ID可以表示成一个十进制的数字；

也可以表示成一个IP

骨干区域Area 0：

负责区域间路由信息传播

OSPF基本配置：

```
[Huawei]interface GigabitEthernet 0/0/0
```

```
[Huawei-GigabitEthernet0/0/0] ip address 192.168.4.2 24
```

```
[Huawei]interface GigabitEthernet 0/0/1
```

```
[Huawei-GigabitEthernet0/0/0] ip address 192.168.5.254 24
```

```
[Huawei]ospf 1 //启动OSPF路由进程
```

```
[Huawei-ospf-1]area 0 //进入到骨干区域
```

```
[Huawei-ospf-1-area-0.0.0.0]network 192.168.0.0 0.0.0.255
```

//0.0.0.255为255.255.255.0的反掩码,宣告直连接口的网段信息

```
[Huawei]display ip routing-table //查看路由表信息
```

```
[Huawei]display ip interface brief //查看ip接口的简要信息
```

四、传输层概述

1、传输层的作用

网络层提供点到点的连接；

传输层提供端口到端口的连接；

2、传输层的协议

TCP协议：

1>传输控制协议；

2>可靠的，面向连接的协议；

3>传输效率低

应用：FTP(21)，Telnet(23)，SMTP(25)，DNS(53)，HTTP(80)

三次握手：

第一次握手：client向 server发送一个SYN，等待server确认；

第二次握手：server收到数据包后，知道client请求建立连接，给client回复SYN和ACK，确认连接请求；

第三次握手：client收到确认后，发送ACK给server；

四次断开：

即终止TCP连接，就是断开一个TCP连接时，需要客户端和服务端总共发送4个包以确认连接的断开。

第一次断开：client发送一个FIN，用来关闭client到server的数据传送；

第二次断开：server收到FIN后，发送一个ACK给client；

第三次断开：server发送一个FIN，用来关闭server到client的数据传送；

第四次断开：client收到FIN后，发送一个ACK给server；

UDP协议：

1>用户数据报协议；

2>不可靠的，面向无连接的服务；

3>传输效率高

应用：TFTP(69)，DNS(53)，NTP(123)

3、ACL访问控制列表

ACL是应用在路由器接口的指令列表---即规则；

读取第三层，第四层报文头信息；

根据预先定义好的规则对报文进行过滤；

ACL的主要类型：

分类	编号范围	参数(基于什么过滤数据包)
基本ACL	2000-2999	源IP地址
高级ACL	3000-3999	源IP地址，目的IP地址，端口，协议

ACL规则：

每个ACL可以包含多个规则，路由器根据规则对数据流量进行过滤；

匹配即停止；

默认规则是允许；

基本ACL编写的语法：

拒绝规则：rule deny source ip地址或网段 通配符掩码(即反码)

允许规则：rule permit source ip地址或网段 通配符掩码(即反码)

匹配规则：顺序匹配，匹配即停止，无匹配默认允许

案例1（基本ACL）：

-允许PC1(192.168.2.1)访问服务器Server1；

-拒绝其他所有的访问流量；

```
[Huawei]acl 2001
```

```
[Huawei-acl-basic-2001]rule permit source 192.168.2.1 0
```

//0代表全匹配，指匹配到具体的ip地址，1代表不匹配，0.0.0.255指匹配一个网段

```
[Huawei-acl-basic-2001]rule deny source any
```

```
[Huawei]interface GigabitEthernet 0/0/1
```

```
[Huawei-GigabitEthernet0/0/1]undo traffic-filter inbound acl 2000
```

//删除2000的acl规则

```
[Huawei-GigabitEthernet0/0/1]traffic-filter inbound acl 2001 //在接口中应用acl
```

高级ACL编写的语言：

拒绝规则：rule deny 协议(tcp/udp/icmp/ip) source ip地址或网段 反码

destination ip地址或网段 反码 destination-port eq 端口

允许规则: rule permit 协议(tcp/udp/icmp/ip) source ip地址或网段 反码
destination ip地址或网段 反码 destination-port eq 端口

ACL应用到接口: 一个接口一个方向只能应用一个ACL

案例2(高级ACL):

禁止pc2(192.168.2.1)访问pc1(192.168.1.1)的ftp服务, 禁止pc3(192.168.2.2)访问pc1的www服务, 所有主机的其他服务不受限制

```
[Huawei]acl 3000
```

```
[Huawei-acl-adv-3000]rule deny tcp source 192.168.2.1 0 destination  
192.168.1.1 0 destination-port eq 21
```

//0代表全匹配, 指匹配到具体的ip地址, 1代表不匹配, 0.0.0.255指匹配一个网段

```
[Huawei-acl-adv-3000]rule deny tcp source 192.168.2.2 0 destination  
192.168.1.1 0 destination-port eq 80
```

```
[Huawei]interface g0/0/1
```

```
[Huawei-GigabitEthernet0/0/1]traffic-filter inbound acl 3000 //在接口  
中应用acl
```

```
[Huawei]display acl all //查看acl配置信息
```

五、NAT概述

NAT, 网络地址转换;

作用:

通过将内部网络的私有IP地址翻译成全球唯一的公网IP地址, 使内部网络可以连接到互联网等外部网络上。

NAT配置位置:

公司内网或家庭网络与运营商相连的网关设备上;

优点:

- 1》节省公有合法IP地址;
- 2》处理地址重叠;
- 3》安全性;

缺点:

- 1》延迟增大;
- 2》配置和维护的复杂性;

实现方式:

- 1》静态转换;
- 2》Easy IP;

1、私有IP地址分类(网段)

A类 10.0.0.0 ~ 10.255.255.255 //10.0.0.0网段

B类 172.16.0.0 ~ 172.31.255.255 //172.16.0.0网段 ~ 172.31.0.0网段

C类 192.168.0.0 ~ 192.168.255.255 //192.168.0.0网段

2、静态NAT

所谓静态NAT是指公网IP和私网IP的对应关系是静态的，由管理员手工指定后就不会改变了，并且静态NAT实现的是一对一的地址转换；

静态转换是指将内部网络的私有地址转换为公有IP地址；

静态转换是双向的；

第一步：进入内网出公网的接口

```
[Huawei]interface GigabitEthernet 0/0/0
```

```
[Huawei-GigabitEthernet0/0/0] ip address 100.0.0.1 8 //接口0/0/0配置IP地址
```

第二步：允许静态NAT

```
[Huawei-GigabitEthernet0/0/0] nat static enable
```

第三步：配置静态NAT(转换后的公网地址在前，转换前的私网地址在后)

```
[Huawei-GigabitEthernet0/0/0] nat static global 100.0.0.2 inside 192.168.2.1
```

//配置静态nat使192.168.2.1转换为100.0.0.2实现外部网络访问

```
[Huawei-GigabitEthernet0/0/0] nat static global 100.0.0.3 inside 192.168.2.2
```

//配置静态nat使192.168.2.2转换为100.0.0.3实现外部网络访问

```
[Huawei]display nat static //查看静态绑定关系是否成功建立
```

3、Easy-IP

工作方式与NAT一样，转换后的公网IP为路由器出口的公网IP；

动态NAT：实现多个内网私有主机共有一个公有IP上网；

easy-ip是基于出接口的公有IP进行转换的；

动态的NAT传输数据是单向的；

配置步骤：

第一步：定义私网地址池；

第二步：进入公网接口关联私网地址池；

案例：

在路由器上配置Easy IP，使企业内网192.168.2.0/24利用g0/0/0端口的ip，实现外部网络的访问？

第一步：定义私网地址池

```
[Huawei]acl 2000
```

```
[Huawei-acl-basic-2000]rule permit source any
```

//使用acl定义任何内部地址

```
[Huawei-acl-basic-2000]rule permit source 192.168.2.0 0.0.0.255
```

//使用acl定义192.168.2.0网段的内部IP地址

第二步：进入公网接口关联私网地址池

```
[Huawei]interface g0/0/0 //要使用连接外网的那一头的端口
```

```
[Huawei-GigabitEthernet0/0/0] nat outbound 2000 //将ACL和出接口的公有IP关联
```

```
[Huawei]display nat outbound //查看 动态NAT是否 转换成功
```

4、VRRP（虚拟路由冗余协议）

VRRP是通过把几台路由设备联合组成一台虚拟的路由设备，将虚拟路由设备的IP地址作为用户的默认网关实现与外部网络通信。当网关设备发生故障时，VRRP机制能够选举新的网关设备承担数据流量，从而保障网络的可靠通信。

解决的问题：网关的单点故障问题；

VRRP组成员角色：

- 1》主(Master)路由器----实际转发数据的路由器；
- 2》备份(Backup)路由器----进行网关备份的设备(备份不转发数据)；
- 3》虚拟(Virtual)路由器----主要是给PC或者上网终端做网关用的IP；

如何确定虚拟组里面谁是主路由器？

优先级 优先级高的作为主路由器。

VRRP配置步骤：

- 1》配置为VRRP的成员；
- 2》配置VRRP的优先级(默认100)；
- 3》配置VRRP抢占模式(默认开启)；
- 4》查看VRRP信息

案例：

```
<Huawei>system-view      //进入系统视图
[Huawei]interface Vlanif 1  //进入vlan1,给vlan1配置IP地址
[Huawei-Vlanif1]ip address 192.168.1.252 24 //配置世界的接口IP
[Huawei-Vlanif1]vrrp vrid 1 virtual-ip 192.168.1.254 //配置虚拟路由器IP
[Huawei-Vlanif1]vrrp vrid 1 priority 200 //配置优先级为200，选择主路由器
<Huawei>display vrrp      //查看VRRP详细信息
<Huawei>display vrrp brief //查看VRRP简要信息
```