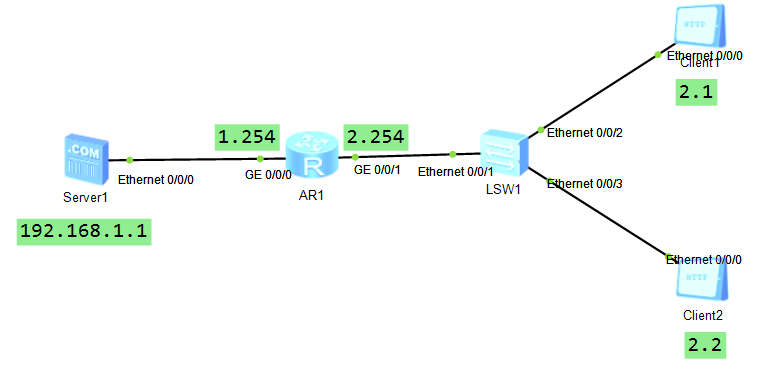
NETWORK 04

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

**使用高级acl**

基本acl 2000~2999 源地址

高级acl 3000~3999 源地址、目标地址、协议、端口



**禁止2.2访问1.1的网站服务，但不影响其他服务**

[Huawei]acl 3000 //创建(进入)acl3000

[Huawei-acl-adv-3000]rule deny tcp source 192.168.2.2 0 destination

192.168.1.1 0 destination-port eq 80 //拒绝2.2访问1.1的tcp的80

端口

[Huawei-acl-adv-3000]in g0/0/1 //进入距离2.2比较近的接口

[Huawei-GigabitEthernet0/0/1]undo traffic-filter inbound //删除原有acl

[Huawei-GigabitEthernet0/0/1]traffic-filter inbound acl 3000 //重新在

接口应用acl3000

禁止2.1访问1.1的ftp服务，但不影响其他服务

[Huawei-acl-adv-3000]rule deny tcp source 192.168.2.1 0 destination

192.168.1.1 0 destination-port eq 21 //拒绝2.1访问1.1的tcp

的21端口

使用acl时，同接口的同方向只能一次应用一个acl列表

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

**nat 网络地址转换，可以将私有地址转换为全球唯一的公有**

**地址**

广域网 外网

局域网 内网

**ip地址 32位**  **拥有 42亿+的数量并且已经枯竭**

**私有ip地址**

**A 10.0.0.0~10.255.255.255**

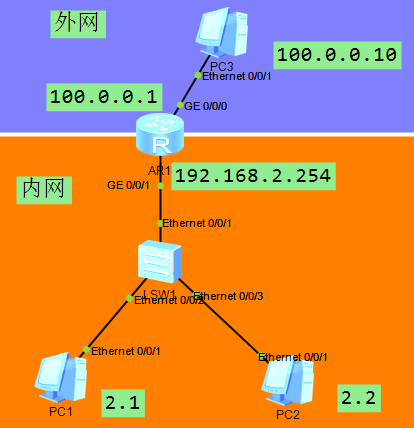
**B 172.16.0.0~172.31.255.255**

**C 192.168.0.0~192.168.255.255**

**nat常见的两种用法：**

**静态转换 1对1 双向通信**

**easy ip 多对1 单向通信**



**首先按图配置ip**

**然后在路由器配置静态nat**

**使用nat前要进入外网接口**

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

//使用静态nat技术，将内部的2.1与外部的公网地址100.0.0.2进行相互

转换然后测试使用192.168.2.1 ping 100.0.0.10可以互通说明地址转换成功

如果配置错误可以用undo删除，比如：

undo nat static global 100.0.0.2 inside 192.168.2.4

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

**在路由器配置easy ip，让所有的内部主机仅仅利用唯一的一个公网地址**

**100.0.0.1访问外网**

[Huawei]acl 2000 //通过acl定义允许访问外网的设备

[Huawei-acl-basic-2000]rule permit source any //这里放行所有设备，如果

将any换成192.168.2.0 0.0.0.255则是仅仅允许2.0网段的设备访问外网

[Huawei-acl-basic-2000]in g0/0/0 //进入0接口(外网接口)

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

//删除已有的静态nat

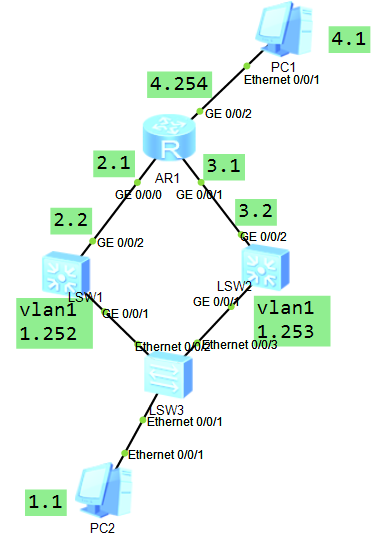
[Huawei-GigabitEthernet0/0/0]undo nat static global 100.0.0.2 inside 192.168.2.1

[Huawei-GigabitEthernet0/0/0]nat outbound 2000 //应用nat (easy ip方式)

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

**vrrp 虚拟路由冗余协议**

**vrrp能够在不改变组网的情况下，将多台路由器虚拟成一个虚拟路由器，通过配置虚拟路由器的IP地址为默认网关，实现网关的备份**



**三层交换机配置，第一台**

[Huawei]sysname sw1 //修改主机名为sw1

[sw1]undo info-center enable //关闭日志

[sw1]in vlan 1 //进入vlan1

[sw1-Vlanif1]ip add 192.168.1.252 24 //配置ip

[sw1]vlan 2 //创建vlan2

[sw1-vlan2]in vlan 2 //进入vlan虚拟接口

[sw1-Vlanif2]ip add 192.168.2.2 24 //配ip

[sw1-Vlanif2]in g0/0/2 //进入要配ip的接口

[sw1-GigabitEthernet0/0/2]port link-type access

[sw1-GigabitEthernet0/0/2]port default vlan 2

**另外一台s5700**

<Huawei>sys

[Huawei]sysname sw2

[sw2]undo info-center enable

[sw2]in vlan 1

[sw2-Vlanif1]ip add 192.168.1.253 24

[sw2]vlan 3 //创建vlan3

[sw2-vlan3]in vlan 3 //进入vlan虚拟接口

[sw2-Vlanif3]ip add 192.168.3.2 24 //配ip

[sw2-Vlanif3]in g0/0/2 //进入要配ip的接口

[sw2-GigabitEthernet0/0/2]port link-type access

[sw2-GigabitEthernet0/0/2]port default vlan 3

**然后分别在路由器与三层交换机上配置ospf**

[Huawei]ospf //在路由器配置ospf

[Huawei-ospf-1]area 0

[Huawei-ospf-1-area-0.0.0.0]network 192.168.2.0 0.0.0.255

[Huawei-ospf-1-area-0.0.0.0]network 192.168.3.0 0.0.0.255

[Huawei-ospf-1-area-0.0.0.0]network 192.168.4.0 0.0.0.255

[sw1]ospf //在sw1配置ospf

[sw1-ospf-1]area 0

[sw1-ospf-1-area-0.0.0.0]network 192.168.1.0 0.0.0.255

[sw1-ospf-1-area-0.0.0.0]network 192.168.2.0 0.0.0.255

[sw2]ospf //在sw2配置ospf

[sw2-ospf-1]area 0

[sw2-ospf-1-area-0.0.0.0]network 192.168.1.0 0.0.0.255

[sw2-ospf-1-area-0.0.0.0]network 192.168.3.0 0.0.0.255

**在两台三层交换机配置vrrp**

[sw1]in vlan 1 //vrrp需要在接口中配置，进入vlan接口

[sw1-Vlanif1]vrrp vrid 1 virtual-ip 192.168.1.254 //开启vrrp功能，组号

是1，虚拟设备的ip是1.254

[sw2]in vlan 1 //另外这台设备配置一样的内容

[sw2-Vlanif1]vrrp vrid 1 virtual-ip 192.168.1.254

[sw2-Vlanif1]display this //查看当前视图配置

<sw1>display vrrp brief //分别在两台三层交换机查看vrrp状态，看

到一台是**Master一台是backup即可**

**VRRP组成员角色**

**主（Master）路由器**

**备份（Backup）路由器**

**虚拟（Virtual）路由器**

如果打算将某个设备定义为主：

in vlan 1

vrrp vrid 1 priority 105 //修改vrrp优先级，默认值

是100，越高越优先成为主

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

练习：

1，NAT的作用是什么，有哪些优点？

2，私有IP地址分类有哪些？

3，NAT常用实现方式有哪些，各有什么特点？

4，VRRP是什么，具体的作用是什么？

5，VRRP中设备的身份有哪些？

6，VRRP通过什么定义路由设备的主备身份？

参考答案

1，NAT的作用是什么，有哪些优点？

通过将内部网络的私网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。

优点有节约公网ip、处理地址重叠(使用相同私网地址的主机不会冲突，可以利用不同的公网ip互通)、增加安全

2，私有IP地址分类有哪些？

A类 10.0.0.0~10.255.255.255

B类 172.16.0.0~172.31.255.255

C类 192.168.0.0~192.168.255.255

3，NAT常用实现方式有哪些，各有什么特点？

静态转换 可以实现1个私网地址对1个公网地址的转换 是双向通讯

Easy IP 可以实现多个私网地址对1个公网地址的转换 是单向通讯

4，VRRP是什么，具体的作用是什么？

vrrp是虚拟路由冗余协议

可以实现网关的冗余备份，可以保障网关设备出现故障的情况下不会对网络造成重大影响。

5，VRRP中设备的身份有哪些？

主(master)路由器，备份(backup)路由器，虚拟(virtual)路由器

6，VRRP通过什么定义路由设备的主备身份？

可以修改优先级来决定