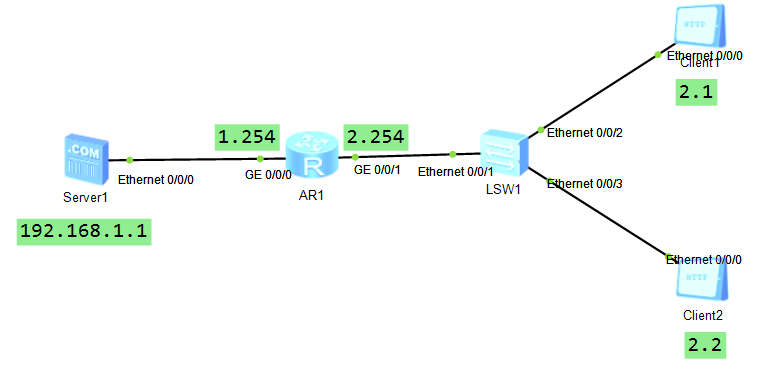
**NETWORK day 04**

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

**使用高级acl限制网络数据**



**禁止2.1访问1.1的ftp**

[Huawei]acl 3000 //创建(进入)acl3000

[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

[Huawei-acl-adv-3000]in g0/0/1 //进入1接口

[Huawei-GigabitEthernet0/0/1]traffic-filter inbound acl 3000 //启用新acl3000

此时测试2.1已经无法访问1.1的ftp，但是可以访问网站

**禁止2.2.访问1.1的网站服务**

[Huawei-GigabitEthernet0/0/1]acl 3000 //重新回到acl3000里

[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

此时测试2.2已经无法访问1.1的网站，但是可以访问ftp

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

**NAT (Network Address Translation)，网络地址转换**

**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的优点**

**节省公有合法IP地址、处理地址重叠、增加安全**

**NAT的缺点**

**延迟增大、配置和维护的复杂性**

**私有ip地址范围**

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

ipv4 32位长度 42亿+

ipv6 128位长度 几乎无限的地址空间

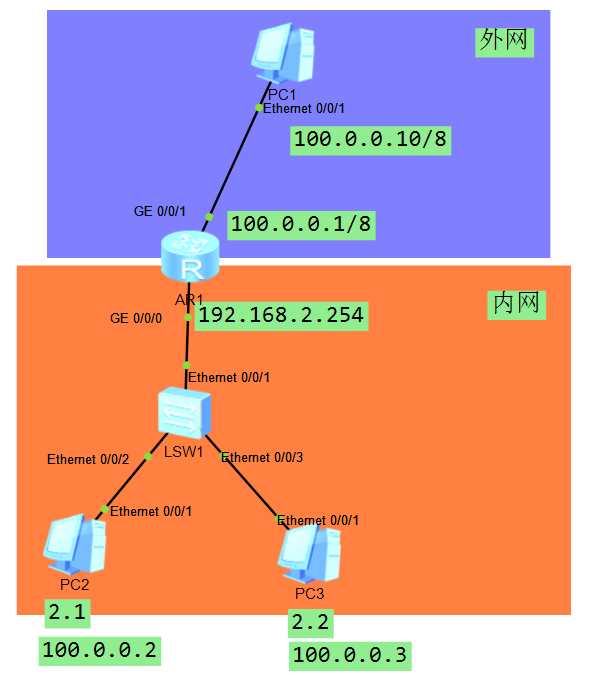
**静态转换 1对1 双向通信 1台内部主机可以利用1个公网ip访问外部网络**

**通常有服务器设备发布服务到外网时使用**

**easy ip 多对1 单向通信 多台内部主机可以利用1个公网ip访问外部网络**

**通常办公室环境使用**

**按图配置地址**



**在路由器配置静态nat**

[Huawei]in g0/0/1 //进入外网接口

[Huawei-GigabitEthernet0/0/1]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

[Huawei-GigabitEthernet0/0/1]nat static global 100.0.0.3 inside 192.168.2.2

之后效果是2.1与2.2可以利用外网地址ping通100.0.0.10

反之，100.0.0.10也可以ping通2.1与2.2的公网地址

[Huawei-GigabitEthernet0/0/1]undo nat static global 100.0.0.3 inside 192.168.2.2 //如

果错误，就删除重新配置

**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

[Huawei-acl-basic-2000]in g0/0/1 //进入1接口

[Huawei-GigabitEthernet0/0/1]undo nat static global 100.0.0.3 inside 192.168.2.2 //删

除已有的静态nat

[Huawei-GigabitEthernet0/0/1]undo nat static global 100.0.0.2 inside 192.168.2.1

[Huawei-GigabitEthernet0/0/1]nat outbound 2000 //应用nat

[Huawei-GigabitEthernet0/0/1]undo nat outbound 2000 //如果nat无效，删除重新

配置即可（属于bug，小概率事件）

之后效果是2.1与2.2可以利用外网地址ping通100.0.0.10

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

**VRRP是虚拟路由冗余协议**

**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**

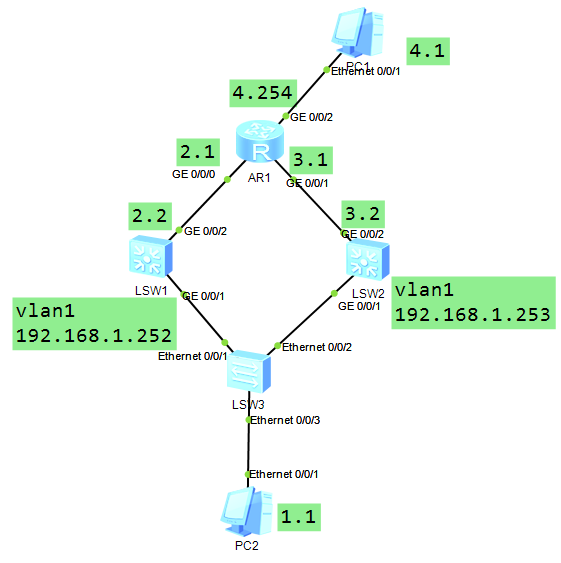
**VRRP组成员角色**

**主（Master）路由器**

**备份（Backup）路由器**

**虚拟（Virtual）路由器**

按图配置ip



<Huawei>sys

[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vlan2接口

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

[sw1-Vlanif2]in g0/0/2 //进入2口

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

[sw1-GigabitEthernet0/0/2]port default vlan 2 //将2口加入vlan2

**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

[sw2-vlan3]in vlan 3

[sw2-Vlanif3]ip add 192.168.3.2 24

[sw2-Vlanif3]in g0/0/2

[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

[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

[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

[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

<sw1>display vrrp brief //查看vrrp状态

[sw2]in vlan 1 //另外这台设备配置一样的内容

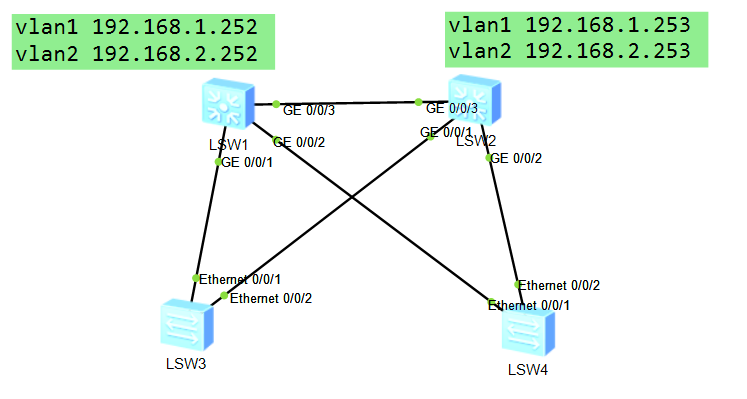
[sw2-Vlanif1]vrrp vrid 1 virtual-ip 192.168.1.254

[sw1-Vlanif1]vrrp vrid 1 priority 105 //修改vrrp优先级，默认值是100，越高

越优先成为主

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

**配置vrrp实现负载均衡**



**1， 所有交换机修改主机名sw1~sw4，所有交换机创建vlan2**

[Huawei]sysname sw1 //第1台s5700交换机（左）

[sw1]vlan 2 //创建vlan2

[Huawei]sysname sw2 //第2台s5700交换机

[sw2]vlan 2

[Huawei]sysname sw3 //第1台s3700交换机（左）

[sw3]vlan 2

[Huawei]sysname sw4 //第2台s3700交换机

[sw4]vlan 2

**按图配置三层交换机的ip**

[sw1]in vlan 1

[sw1-Vlanif1]ip add 192.168.1.252 24

[sw1-Vlanif1]in vlan 2

[sw1-Vlanif2]ip add 192.168.2.252 24

[sw2]in vlan 1

[sw2-Vlanif1]ip add 192.168.1.253 24

[sw2-Vlanif1]in vlan 2

[sw2-Vlanif2]ip add 192.168.2.253 24

**2，将所有链路修改为trunk**

[sw1]port-group 1 //sw1与sw2按照此方式配置（s5700）

[sw1-port-group-1]group-member GigabitEthernet 0/0/1 to

GigabitEthernet 0/0/3

[sw1-port-group-1]port link-type trunk

[sw1-port-group-1]port trunk allow-pass vlan all

[sw3]port-group 1 // sw3与sw4按照此方式配置（s3700）

[sw3-port-group-1]group-member Ethernet 0/0/1 Ethernet 0/0/2

[sw3-port-group-1]port link-type trunk

[sw3-port-group-1]port trunk allow-pass vlan all

**如果要实现vrrp的负载均衡，需要按下列思路进行配置**

Sw1 vlan1主 vlan2备

Sw2 vlan1备 vlan2主

[sw1]in vlan 1

[sw1-Vlanif1]display this //查看vlan1接口的配置，如果vrrp配置已有则无需再配置

[sw1-Vlanif1]vrrp vrid 1 virtual-ip 192.168.1.254 //配置vlan1的vrrp

[sw1-Vlanif1]vrrp vrid 1 priority 105 //为了成为vlan1的主，修改了优先级

[sw1-Vlanif1]in vlan 2

[sw1-Vlanif2]vrrp vrid 2 virtual-ip 192.168.2.254 //vlan2仅仅开启vrrp功能即可

[sw2]in vlan 1

[sw2-Vlanif1]vrrp vrid 1 virtual-ip 192.168.1.254 //vlan1仅仅开启vrrp功能即可

[sw2-Vlanif1]in vlan 2

[sw2-Vlanif2]vrrp vrid 2 virtual-ip 192.168.2.254 //配置vlan2的vrrp

[sw2-Vlanif2]vrrp vrid 2 priority 105 //为了成为vlan2的主，修改了优先级

[sw2-Vlanif2]dis vrrp brief //查看结果，一主一备即可，sw1要与sw2相反

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 服务器环境常用

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 办公室环境常用

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