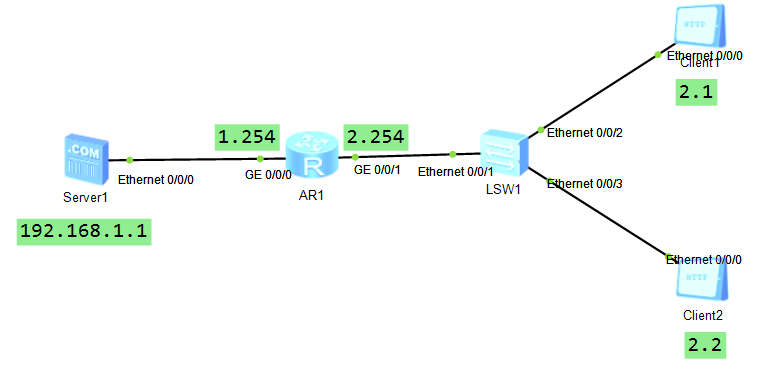
NETWORK day 04

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

**使用高级acl限制网络数据**



**禁止2.1访问1.1的ftp服务，不影响其他数据**

[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，不影响其他数据**

[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。**

**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

**nat的转换方式**

1. 静态转换 双向通信

1对1 1台内部主机可以利用1个公网ip访问外部网络

通常由服务器发布服务到外网时使用

1. easy ip 单向通信

多对1 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

**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，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 g0/0/1 //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

vrrp 虚拟路由冗余协议

[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

display vrrp brief //查看vrrp摘要信息，可以识别主和备

[sw2-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

下课休息 17:20回