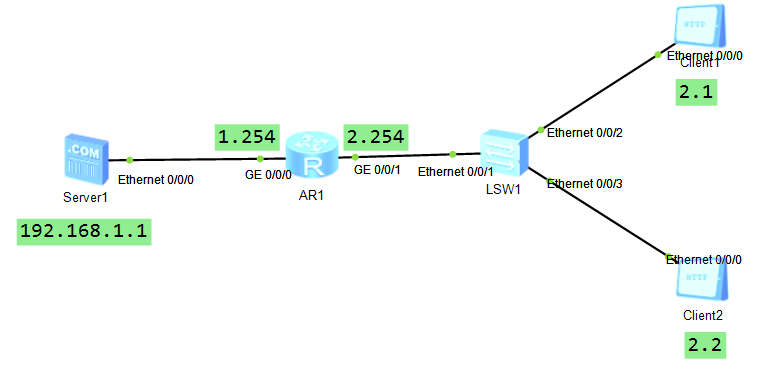
NETWORK day 04

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

**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

下课休息 15:05回