nsd1908_network_day03

路由协议

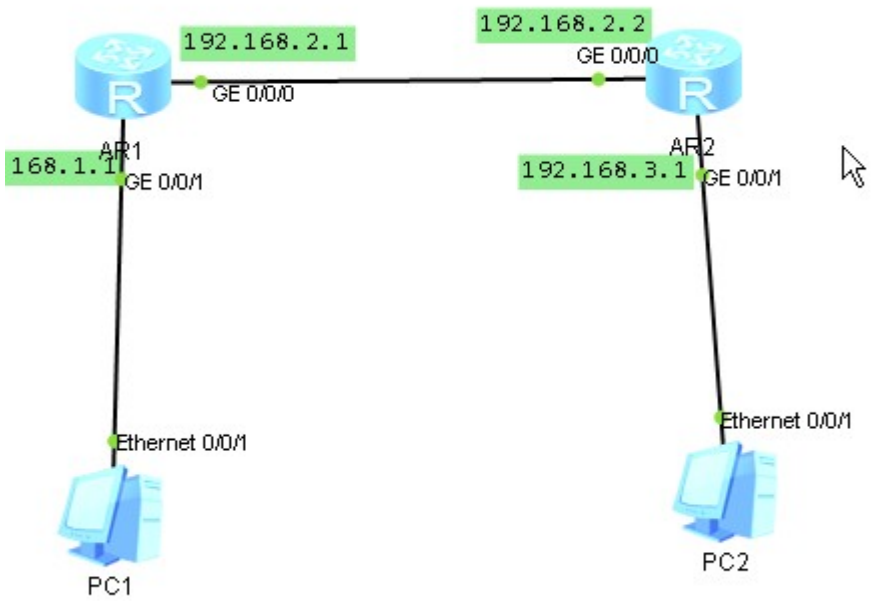
分类

- IGP：内部网关路由协议。最常用的是OSPF
- EGP：外部网关路由协议。互联网上的EGP采用的是BGP（边界网关路由协议）

OSPF：开放最短路径优先

- 在大规模网络环境下，如果每台路由器都要存储全部的信息，将会消耗路由器太多资源。因此，OSPF将网络划分成多个区域。
- 同一个区域内的路由器拥有一致的信息。不同区域可以不一样
- 如果存在多个区域，0区域必须有，是主干区域。
- 非0区域必须和0区域直连

OSPF配置




```
[R1]# int g0/0/1
[R1-gigabyte0/0/1]ip add 192.168.1.1 24
[R1]int g0/0/0
[R1-gigabyte0/0/0]ip add 192.168.2.1 24
[R1]ospf 1   # 1是进程号，从1到65535随便用一个数字即可
[R1-ospf-1]area 0  # 创建0号区域
# 路由器上哪个端口的IP地址以192.168.1.开头，则加入到0区域
[R1-ospf-1-area-0.0.0.0]network 192.168.1.0 0.0.0.255
```

```
# 路由器上哪个端口的IP地址以192.168.2.开头，则加入到0区域
[R1-ospf-1-area-0.0.0.0]network 192.168.2.0 0.0.0.255

[R2]# int g0/0/1
[R2-gigabyte0/0/1]ip add 192.168.3.1 24
[R2]int g0/0/0
[R2-gigabyte0/0/0]ip add 192.168.2.2 24
[R2]ospf 1   # 1是进程号，从1到65535随便用一个数字即可
[R2-ospf-1]area 0  # 创建0号区域
# 路由器上哪个端口的IP地址以192.168.开头，则加入到0区域
[R1-ospf-1-area-0.0.0.0]network 192.168.0.0 0.0.255.255
```

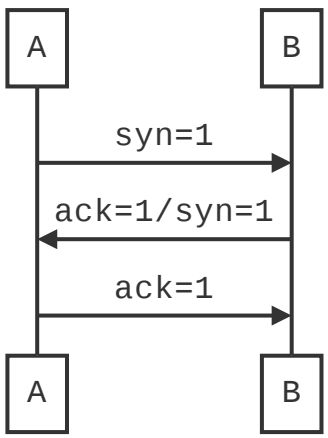
传输层

- 网络层提供点到点的连接
- 传输层帝现端到端的连接，即应用到应用
- 重要的协议有TCP和UDP

TCP

- 传输控制协议
- 可靠的、面向连接的协议

tcp三次握手




```
# yum install -y wireshark-gnome
# 应用程序 -> 互联网 -> wireshark xxxxxx
# 在Interface list中选择要抓取哪块网卡进出的数据包
# 点击绿色鲨鱼qi的开始按钮开始
```

UDP

- 用户数据报协议

- 不可靠的、非面向连接的协议

> 协议和端口号对应的说明文件：/etc/services

ACL：访问控制列表

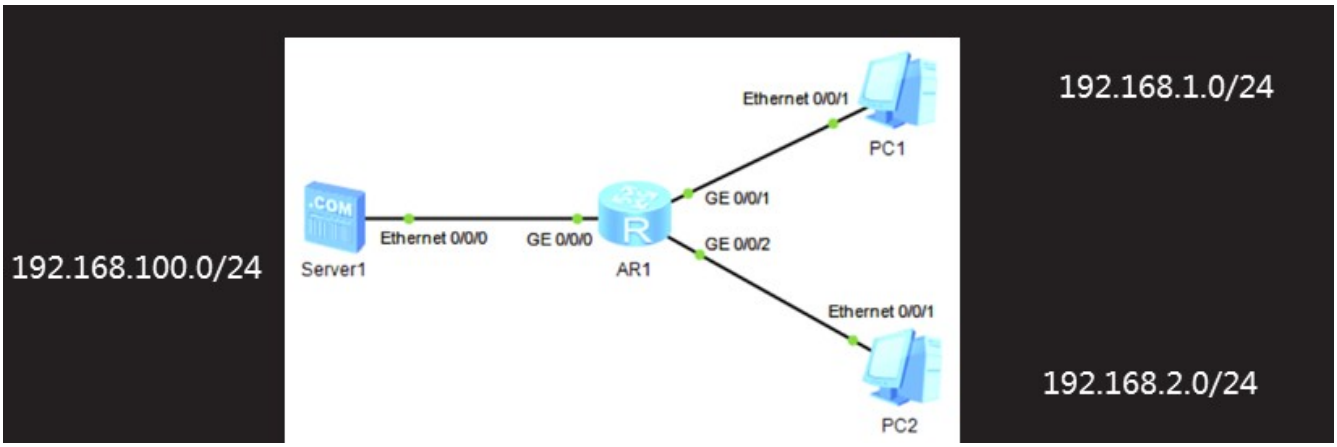
- 简单来说，它可以实现防火墙功能
- ACL原理是，路由器检查数据包的源和目标地址以及端口号，根据提前配置好的规则决定是否放行
- ACL可以分为基本和高级

ACL匹配规则

- 一张表可以有多条规则
- 规则是有顺序的。当检查规则的时候，一旦某一规则匹配立即生效，后续其他规则就不再检查了。
- 如果全部的规则都没有匹配，华为路由器默认允许；思科路由器默认拒绝。
- 应用到路由器端口时，有进方向和出方向。

基本ACL

- 表号从2000到2999
- 只检查数据包的源IP地址

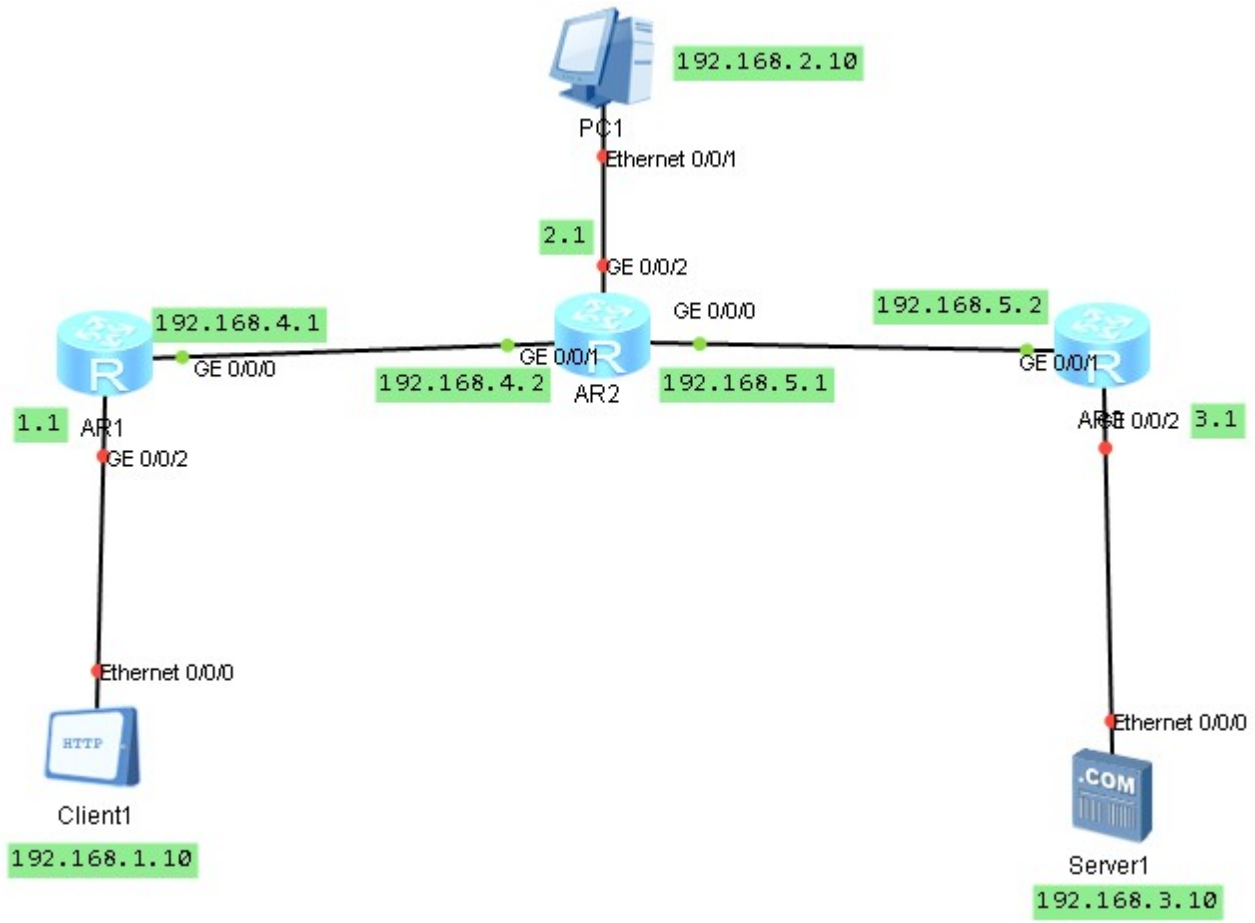


pc1: 192.168.1.10/24 pc2: 192.168.2.20/24 server1: 192.168.100.30

```
[R1]acl 2000
# 只拒绝192.168.1.10这一个IP地址
# 如果拒绝192.168.1.0整个网络，用192.168.1.0 0.0.0.255
[R1-acl-basic-2000]rule 5 deny source 192.168.1.10 0
[R1]int g0/0/0
[R1-gigabyte0/0/0]traffic-filter outbound acl 2000
[R1]display acl all  # 查看所有的acl
```

高级ACL

- 表号从3000到3999
- 可以检查数据包的源、目标地址以及端口号



- 允许client1访问server1的web服务
- 允许client1访问192.168.2.0
- 禁止client访问其他网络

```
# 1. 各设备根据图中要求配置IP地址
# 2. 各设备配置OSPF路由协议，所有设备的配置方法完全相同
[Huawei]ospf 1
[Huawei-ospf-1]area 0
[Huawei-ospf-1-0.0.0.0]network 192.168.0.0 0.0.255.255

# 3. 在R1上配置高级ACL
[R1]acl 3000
[R1-acl-adv-3000]rule 5 permit tcp source 192.168.1.10 0 destination 192.168.3.10 0
destination-port eq 80
[R1-acl-adv-3000]rule 10 permit ip source 192.168.1.10 0 destination 192.168.2.0 0.0.0.255
[R1-acl-adv-3000]rule 10 deny ip source 192.168.1.10 0
# 4. 将ACL应用到g0/0/0的入方向
[R1]int g0/0/0
[R1-gigabyte0/0/0]traffic-filter inbound acl 3000
```

服务器的web配置：

1. 在主机的d盘建立文件夹web
2. web中创建一个文件叫index.html，内容随意

3. 服务器双击后，点击“服务器信息”，地址填d:\web，点击“启动”

客户端访问：http://192.168.3.10/index.html