实验16：访问控制列表（ACL）实验

1.实验内容

根据给定的网络拓扑图搭建硬件实验环境，完成标准及扩展IP访问控制列表（ACL）实验。

2.实验原理

访问控制列表(ACL)是一种基于包过滤的访问控制技术，它可以根据设定的条件对接口上的数据包进行过滤，允许其通过或丢弃。访问控制列表被广泛地应用于路由器和三层交换机，借助于访问控制列表，可以有效地控制用户对网络的访问，从而最大程度地保障网络安全。其功能包括：

- 限制网络流量、提高网络性能。例如，ACL可以根据数据包的协议，指定这种类型的数据包具有更高的优先级，同等情况下可预先被网络设备处理。
- 提供对通信流量的控制手段。
- 提供网络访问的基本安全手段。
- 在网络设备接口处，决定哪种类型的通信流量被转发、哪种类型的通信流量被阻塞。

标准IP访问列表

一个标准IP访问控制列表匹配IP包中的源地址或源地址中的一部分，可对匹配的包采取拒绝或允许两个操作。编号范围是从1到99的访问控制列表是标准IP访问控制列表。

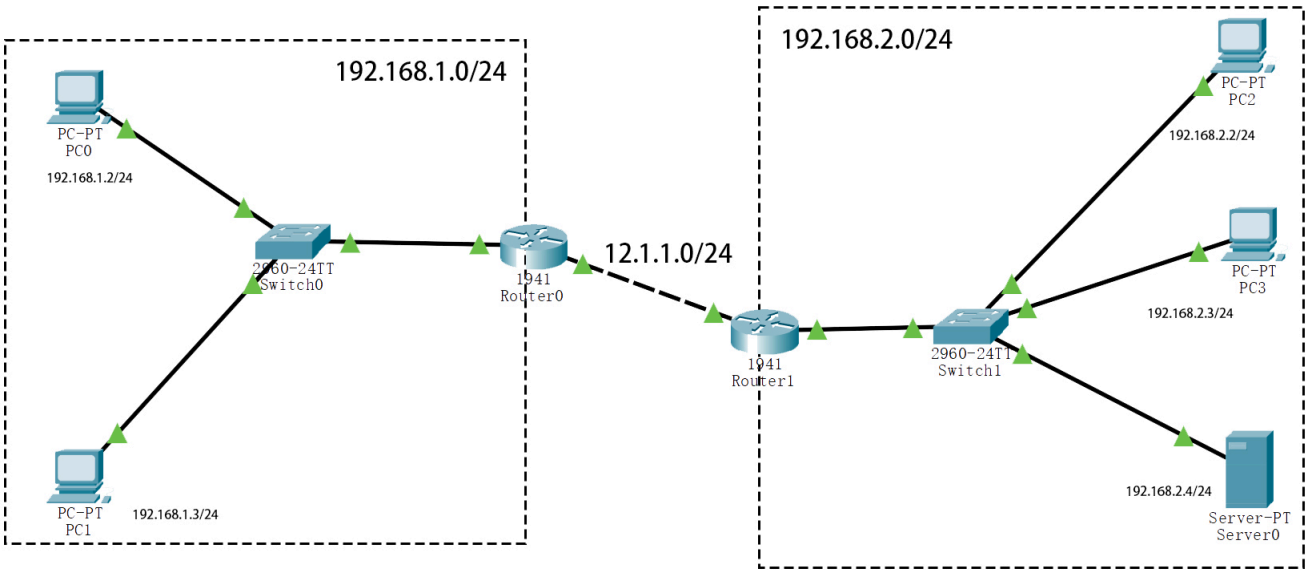
扩展IP访问

扩展IP访问控制列表比标准IP访问控制列表具有更多的匹配项，包括协议类型、源地址、目的地址、源端口、目的端口、建立连接的和IP优先级等。编号范围是从100到199的访问控制列表是扩展IP访问控制列表。

3.实验设备

1941路由器（2台）、2960交换机（2台）、PC（4台）、提供http服务的服务器（1台）、网线（8根）

4.实验拓扑图



5.实验步骤

5.1 连接设备

1）按照拓扑图连接设备，并为PC、服务器及路由器端口配置IP、子网掩码和网关

设备名称	设备ip
PC0	192.168.1.2/24
PC1	192.168.1.3/24
PC2	192.168.2.2/24
PC3	192.168.2.3/24
Server0	192.168.2.4/24

2）在路由器上启用ospf协议，**确保所有PC和服务器相互连通。**

5.2 标准ACL实验

实验目标：

- PC0能够访问PC2和PC3。
- PC1不能访问PC2和PC3。

1）在路由器Router0上，创建基本ACL列表，内容包括：

- 允许所有源地址为PC0的报文。
- 禁止所有源地址为PC1的报文。

2）在PC0和PC1到Router0的入网端口上应用ACL规则。

3）验证是否达成实验目标。

4）使用no+命令，撤销在接口上应用的标准ACL规则。

5.3 扩展ACL实验

实验目标：

- 配置Router0。使得PC0能够访问PC2，不能访问PC3；PC1不能访问PC2，能够访问PC3。
- 配置Router1。使得PC0能够访问Server0的http服务，但是无法ping通server0；PC1能够ping通server0，但是无法访问Server0的http服务。

1）在路由器Router0上，创建扩展ACL列表，内容包括：

- 禁止从PC0发往PC3的报文。
- 禁止从PC1发往PC2的报文。
- 允许任意报文通过。

2）在PC0和PC1到Router0的入网端口上应用扩展ACL规则。

3）在路由器Router1上，创建扩展ACL列表，内容包括：

- 禁止从PC0发往Server0的icmp报文
- 禁止从PC1发往Server0的http报文（使用80端口的tcp报文）
- 允许其他报文通过。

4）在Router1连接到Router0的端口上应用扩展ACL规则。

5）使用ping和telnet命令来验证是否达成实验目标

6.参考命令

 # 配置路由器端口ip

```
Router>enable                                          #启动路由器
Router#configure terminal                  #进入配置界面
Router(config)#interface GigabitEthernet 0/0                #配置端口GigabitEthernet 0/0
Router(config-if)#ip address 192.168.1.1 255.255.255.0        #设置ip为192.168.1.1/24
Router(config-if)#no shutdown        #启动端口
Router(config-if)#exit                          #返回上一层
```

 # 启动OSPF进程，并将192.168.1.0和192.168.3.0网段加入区域0

```
Router(config)#router ospf 1
Router(config-router)#network 192.168.1.0 0.0.0.255 area 0
Router(config-router)#network 192.168.3.0 0.0.0.255 area 0
```

 # 建立一条编号为1的基础ACL规则，内容是允许192.168.1.10的报文，但禁止192.168.1.20的报文

```
Router(config)#ip access-list standard 1
Router(config-std-nacl)#permit host 192.168.1.10
Router(config-std-nacl)#deny host 192.168.1.20
```

 # 在端口0/1上应用编号为1的ACL规则

```
Router(config)#interface GigabitEthernet 0/0
Router(config-if)#ip acc
Router(config-if)#ip access-group 1 in
```

 # 撤销编号为1的ACL规则

```
Router(config-if)#no ip access-group 1 in
```

 # 建立一条编号为100的扩展ACL规则，内容包括

1. 禁止源目的IP10.1.1.2，目的IP为10.1.2.2的报文

2. 允许源目的IP为10.1.1.2发往10.1.3.2的类型为Echo请求的ICMP报文

3. 禁止从10.1.1.2发往任意IP的与FTP（端口21）匹配的TCP数据流

4. 允许其他报文通过

```
Router(config)#ip access-list extended 100
Router(config-ext-nacl)#deny ip host 10.1.1.2 host 10.1.2.2 # host+ip指代具体的源或目的ip
Router(config-ext-nacl)#permit icmp host 10.1.1.2 host 10.1.3.2 echo
Router(config-ext-nacl)#deny tcp host 10.1.1.2 any eq ftp
Router(config-ext-nacl)#deny tcp host 10.1.1.2 any eq 21  # 与上一条等价
Router(config-ext-nacl)#permit ip any any  # any指代任意ip
```

（PC命令）使用telnet尝试访问10.1.1.2的http服务（80端口）

```
telnet 10.1.1.2 80
```