陕西科技大学

路由与交换 实验报告

实验[五]：访问控制列表

学　　生：

班　　级：网络 201

系　　别：计算机系

学　　院：电子信息与人工智能学院

实验五 访问控制列表 预习报告

一、实验目的

掌握 ACL 的配置。

二、实验条件

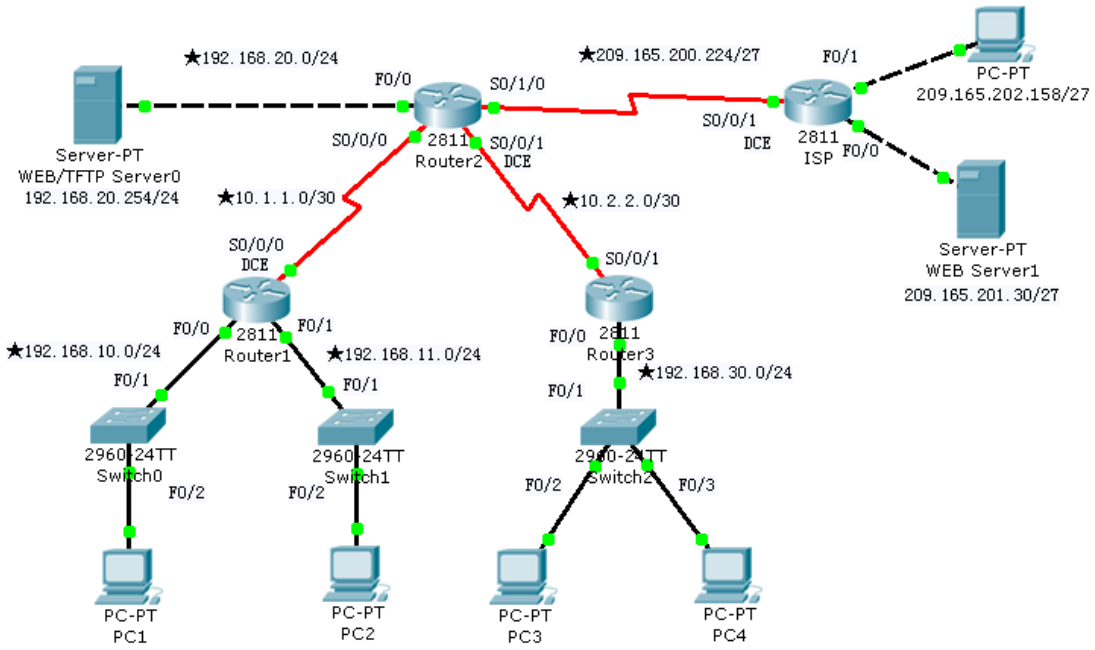
Cisco2621 Switch、Cisco 2950 交换机、PacketTrace 仿真软件、具备 Windows 操作系统的 PC 机

三、实验原理及相关知识

ACL 基本原理

四、实验步骤

网络拓扑结构及地址分配如下。



五、常用路由器查询命令（在特权模式下输入命令）

```
show running-config  //查看运行配置
show access-lists  //查看配置的 ACL
show ip route  //显示整个路由表
copy running-config startup-config  //保存配置
```

实验五 访问控制列表

一、实验目的

掌握 ACL 的配置。

二、实验条件

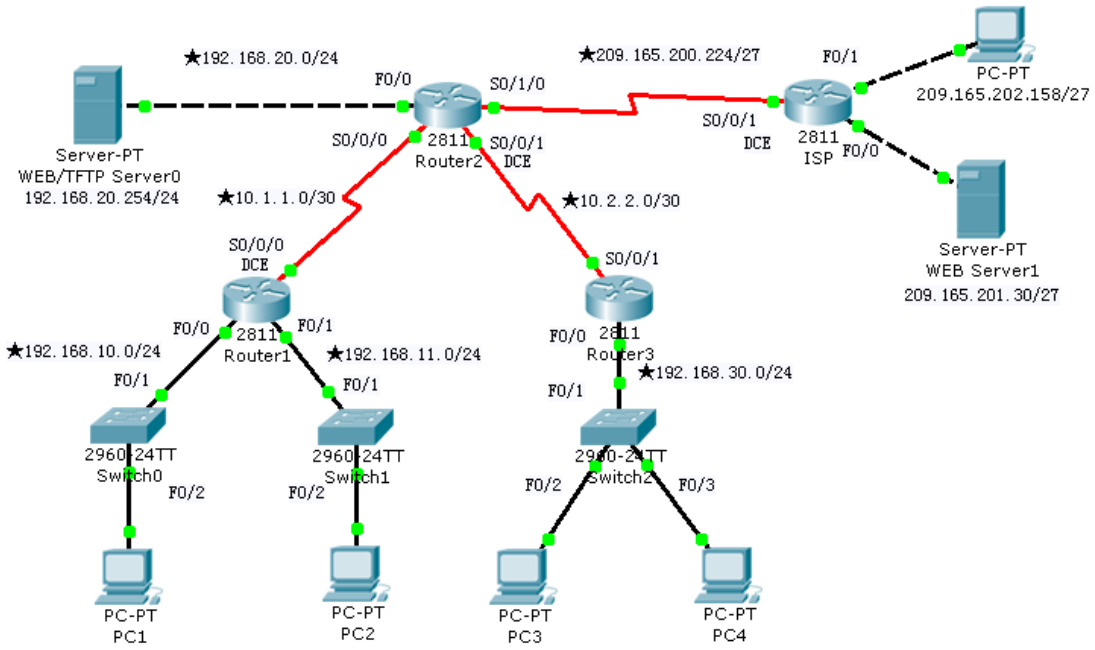
Cisco2621 Switch、Cisco 2950 交换机、PacketTrace 仿真软件、具备 Windows 操作系统的 PC 机

三、实验原理及相关知识

ACL 基本原理

四、实验步骤

网络拓扑结构及地址分配如下。



设备R1（接口 IP地址 子网掩码）	255.255.255.224
Fa0/0 192.168.10.1 255.255.255.0	Fa0/0 209.165.201.1 255.255.255.224
Fa0/1 192.168.11.1 255.255.255.0	Fa0/1 209.165.202.129 255.255.255.224
S0/0/0 10.1.1.1 255.255.255.252	**主机网卡（IP地址 子网掩码）**
设备R2（接口 IP地址 子网掩码）	PC1 网卡 192.168.10.10 255.255.255.0
S0/0/0 10.1.1.2 255.255.255.252	PC2 网卡 192.168.11.10 255.255.255.0
Fa0/0 192.168.20.1 255.255.255.0	PC3 网卡 192.168.30.10 255.255.255.0
S0/1/0 209.165.200.225 255.255.255.224	PC4 网卡 192.168.30.128 255.255.255.0
S0/0/1 10.2.2.1 255.255.255.252	WEB/TFTP Server0 网卡
设备R3（接口 IP地址 子网掩码）	192.168.20.254 255.255.255.0
S0/0/1 10.2.2.2 255.255.255.252	WEB Server1 网卡
Fa0/0 192.168.30.1 255.255.255.0	209.165.201.30 255.255.255.224
设备ISP（接口 IP地址 子网掩码）	Outside Host 网卡
S0/0/1 209.165.200.226	209.165.202.158 255.255.255.224

1．配置网络地址及路由协议，使全网连通。

2．按要求配置标准 ACL，将 ACL 应用于路由器接口并检验和测试 ACL 实施。

⊙ 允许主机192.168.10.10访问外网，禁止网络192.168.10.0访问外网；

⊙ 禁止主机192.168.30.10访问外网，允许网络192.168.30.0访问外网；

⊙ 允许其他访问外网。

⑴配置采用数字编号的标准 ACL

```
Router(config)#ac
Router(config)#access-list 1 per
Router(config)#access-list 1 permit 192.168.10.10 0.0.0.0
Router(config)#ac
Router(config)#access-list 1 de
Router(config)#access-list 1 deny 192.168.10.0 0.0.0.255
Router(config)#ac
Router(config)#access-list 1 de
Router(config)#access-list 1 deny 192.168.30.10 0.0.0.0
Router(config)#ac
Router(config)#access-list 1 pe
Router(config)#access-list 1 permit 0.0.0.0 255.255.255.255
Router(config)#int s0/0/1
Router(config-if)#ip a
Router(config-if)#ip ac
Router(config-if)#ip access-group 1 in
Router(config-if)#ex
```

⑵配置采用命名方式的标准 ACL

```
Router(config)#ac
Router(config)#ip ac
Router(config)#ip access-list ex
Router(config)#ip access-list extended aclQuestion_1
Router(config-ext-nacl)#permit ip 192.168.10.10 0.0.0.0
% Incomplete command.
Router(config-ext-nacl)#per
Router(config-ext-nacl)#permit 192.168.10.10 0.0.0.0
^
% Invalid input detected at '^' marker.
Router(config-ext-nacl)#permit ip 192.168.10.10 0.0.0.0 any any
^
% Invalid input detected at '^' marker.
Router(config-ext-nacl)#permit ip 192.168.10.10 0.0.0.0 any
Router(config-ext-nacl)#deny ip 192.168.10.0 0.0.0.255 any
Router(config-ext-nacl)#deny ip 192.168.30.10 0.0.0.0 any
Router(config-ext-nacl)#permit ip any ant
^
% Invalid input detected at '^' marker.
Router(config-ext-nacl)#permit ip any any
```

```
Router(config-ext-nacl)#show
^
% Invalid input detected at '^' marker.
Router(config-ext-nacl)#show ?
% Unrecognized command
Router(config-ext-nacl)#ex
Router(config)#int s0/0/1
Router(config-if)#ip ac
Router(config-if)#ip access-group ac
Router(config-if)#ip access-group acl
Router(config-if)#ip access-group aclQuestio
Router(config-if)#ip access-group aclQuestion_1 in
Router(config-if)#
%SYS-5-CONFIG_I: Configured from console by console
```

3．按要求配置扩展 ACL，将 ACL 应用于路由器接口并检验和测试 ACL 实施。

⑴为 R1 配置采用数字编号的扩展 ACL

⊙ 对于 192.168.10.0/24 网络，阻止 telnet 访问所有位置，并且阻止通过 TFTP 访问地址为 192.168.20.254 的企业 Web/TFTP Server。允许所有其它访问。

⊙ 对于 192.168.11.0/24 网络，允许通过 TFTP 和 Web 访问地址为 192.168.20.254 的企业 Web/TFTP Server。阻止从 192.168.11.0/24 网络发往 192.168.20.0/24 网络的所有其它流量。

⊙ 允许所有其它访问。

```
Router(config)#ac
Router(config)#access-list 101 deny tcp 192.168.10.0 0.0.0.255 any eq
telnet
Router(config)#ac
Router(config)#access-list 101 de
Router(config)#access-list 101 deny udp 192.168.10.0 0.0.0.255
192.168.20.254 0.0.0.0 eq tf
Router(config)#access-list 101 deny udp 192.168.10.0 0.0.0.255
192.168.20.254 0.0.0.0 eq tftp
Router(config)#ac
Router(config)#access-list 101 pe
Router(config)#access-list 101 permit ip 192.168.10.0 0.0.0.255 any
Router(config)#ac
Router(config)#access-list 101 pe
Router(config)#access-list 101 permit 192.168.11.0 0.0.0.255
192.168.20.254 0.0.0.0 eq tf
Router(config)#access-list 101 permit udp 192.168.11.0 0.0.0.255
192.168.20.254 0.0.0.0 eq tf
Router(config)#access-list 101 permit udp 192.168.11.0 0.0.0.255
192.168.20.254 0.0.0.0 eq tftp
Router(config)#ac
Router(config)#access-list 101 pe
```

```
Router(config)#access-list 101 permit tcp 192.168.11.0 0.0.0.255
192.168.20.254 0.0.0.0 eq 80
Router(config)#ac
Router(config)#access-list 101 de
Router(config)#access-list 101 deny ip 192.168.11.0 0.0.0.255
192.168.20.0 0.0.0.255
Router(config)#acc
Router(config)#access-list pe
Router(config)#access-list 101 pe
Router(config)#access-list 101 permit ip an
Router(config)#access-list 101 permit ip any an
Router(config)#access-list 101 permit ip any any
Router(config)#int ran
Router(config)#int range f0/0-1
Router(config-if-range)#ip ac
Router(config-if-range)#ip access-group 101 in
Router(config-if-range)#
```

⑵为 R3 配置采用命名方式的扩展 ACL

192.168.30.0/24 网络中前一半 IP 地址的访问策略有如下要求：

- ⊙ 拒绝其访问 192.168.20.0/24 网络
- ⊙ 允许其访问所有其它目的地址

对 192.168.30.0/24 网络中的后一半 IP 地址有如下限制：

- ⊙ 拒绝其访问 192.168.20.0/24 网络
- ⊙ 允许其访问 192.168.10.0 和 192.168.11.0
- ⊙ 允许其对所有其它位置的 www 访问

```
Router(config)#ip ac
Router(config)#ip access-list ex
Router(config)#ip access-list extended aclQuestion_3
Router(config-ext-nacl)#deny ip 192.168.30.0 0.0.0.127 192.168.20.0
0.0.0.255
Router(config-ext-nacl)#pe
Router(config-ext-nacl)#permit ip 192.168.30.0 0.0.0.127 any
Router(config-ext-nacl)#deny ip 192.168.30.128 0.0.0.127 192.168.20.0
0.0.0.255
Router(config-ext-nacl)#permi
Router(config-ext-nacl)#permit ip 192.168.30.128 0.0.0.127
192.168.10.0 0.0.1.255
Router(config-ext-nacl)#per
Router(config-ext-nacl)#permit tcp 192.168.30.128 0.0.0.127 any eq 80
Router(config-ext-nacl)#
Router(config-ext-nacl)#ex
Router(config)#int f0/0
Router(config-if)#ip ac
Router(config-if)#ip access-group aclQuestion_3 in
```

Router(config-if)#

五、思考题及其它

⑴访问控制列表的作用是什么？

答：路由器可以根据访问控制列表决定对规则所写的数据包进行转发或者丢弃，从而保证了网络中数据的安全性。

⑵标准 ACL 及扩展 ACL 一般应该放置在网络中什么位置上？

答：标准 ACL 一般放在靠近访问目的地址的位置；扩展 ACL 一般放在接近访问源地址的位置。