实验七　ACL 访问控制列表

实验目的

了解访问控制列表的概念。

掌握访问控制列表的配置方法。

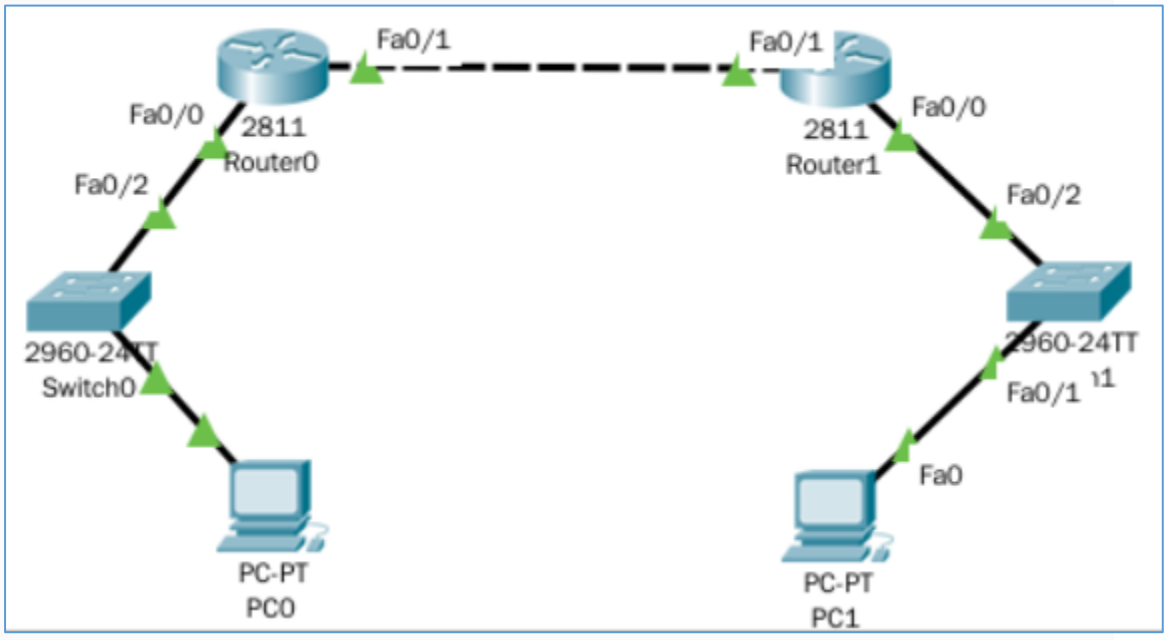
实验原理

访问控制列表(Access Control List,ACL)是控制流入、流出路由器数据包的一种方法。它通过在数据包流入路由器或流出路由器时进行检查、过滤达到流量管理的目的。

访问控制列表不但可以起到控制网络流量、流向的作用，还在很大程度上起到了保护网络设备、服务器的关键作用。作为外网进入受保护的内网的第一道关卡，路由器上的访问控制列表成为保护内网安全的有效手段。

实验条件

拓扑图如下图所示（设备型号及端口如图中所示）：



实验步骤

（1）按照拓扑正确连接设备，配置 IP 地址。

（2）为路由器配置路由。

（3）配置标准 ACL。

（4）配置扩展 ACL。

主机的 IP 地址配置如下表所示。

主机	IP 地址	网关
PC0	10.1.1.2/24	10.1.1.1
PC1	192.168.1.2/24	192.168.1.1

各设备配置如下：

Switch0：

```
Switch>en
Switch#conf t
Switch(config)#int vlan 1
Switch(config-if)#ip address 10.1.1.3 255.255.255.0
Switch(config-if)#no shut
Switch(config-if)#exit
Switch(config)#ip defalut-gateway 10.1.1.1
```

```
Switch(config)#enable password 123
Switch(config)#line vty 0 1
Switch(config-line)#password 123
Switch(config-line)#login local
Switch(config-line)#exit
Switch(config)#username abc password 123
Switch(config)#exit
```

Switch1：

```
Switch>en
Switch#conf t
Switch(config)#int vlan 1
Switch(config-if)#ip address 192.168.1.3 255.255.255.0
Switch(config-if)#no shut
Switch(config-if)#exit
Switch(config)#ip default-gateway 192.168.1.1
Switch(config)#enable password 123
Switch(config)#line vty 0 1
Switch(config-line)#password 123
Switch(config-line)#login local
Switch(config-line)#exit
Switch(config)#username abc password 123
Switch(config)#exit
```

Router0：

```
 Router>enable
Router#configure terminal
Router(config)#interface f0/1
Router(config-if)#no shutdown
Router(config-if)#ip address 200.1.1.1 255.255.255.0
Router(config-if)#exit
Router(config)#interface FastEthernet0/0
Router(config-if)#ip address 10.1.1.1 255.255.255.0
Router(config-if)#no shutdown
Router(config-if)#exit
Router(config)#ip route 192.168.1.0 255.255.255.0 200.1.1.2
Router(config)#exit
```

Router1：

```
Router>enable
Router#configure terminal
Router(config)#interface FastEthernet0/0
Router(config-if)#no shutdown
Router(config-if)#ip address 192.168.1.1 255.255.255.0
Router(config-if)#exit
Router(config)#interface f0/1
Router(config-if)#no shutdown
Router(config-if)#ip address 200.1.1.2 255.255.255.0
Router(config-if)#exit
Router(config)#ip route 10.1.1.0 255.255.255.0 200.1.1.1
```

用 ping 命令测试两个主机之间的连通性。 （截图）

在 PC0 上用 telnet 192.168.1.3 测试交换机 1 是否可以远程登录。（截图）

在 PC1 上用 telnet 10.1.1.3 测试交换机 0 是否可以远程登录。（截图）

在 Router0 上配置标准 ACL，拒绝 192.168.1.0 的网络流入。

```
 Router>en
Router#conf t
Router(config)#access-list 1 deny 192.168.1.0 0.0.0.255
Router(config)#access-list 1 permit any
Router(config)#interface f0/1
Router(config-if)#ip access-group 1 in
```

用 ping 命令再次测试两台主机之间的连通性。（截图）

通过以下命令删除已经配置的 ACL。

```
Router(config)#no access-list 1
Router(config)#int f0/1
Router(config-if)#no ip access-group 1 in
Router(config-if)#exit
```

用 ping 命令第三次测试两台主机之间的连通性。（截图）

在 Router0 上配置扩展 ACL 拒绝 Telnet 数据。

```
 Router(config)#access-list 100 deny tcp host 10.1.1.3 eq telnet host 192.168.1.2
Router(config)#access-list 100 permit ip any any
Router(config)#int f0/0
Router(config-if)#ip access-group 100 in
Router(config-if)#exit
Router(config)#access-list 101 deny tcp host 192.168.1.3 eq telnet host 10.1.1.2
Router(config)#access-list 101 permit ip any any
Router(config)#int f0/1
Router(config-if)#ip access-group 101 in
Router(config-if)#exit
```

在 PC1 上测试 telnet 10.1.1.3 是否可以远程登录交换机。 （截图）

在 PC0 上测试 telnet 192.168.1.3 是否可以远程登录交换机。（截图）