10.2　利用 IP 扩展访问列表实现应用服务的访问限制

【实验名称】

命名的扩展 IP 访问列表。

【实验目的】

掌握在交换机上命名的扩展 IP 访问列表规则及配置。

【背景描述】

你是学校的网络管理员，在 3550-24 交换机上连着学校的提供 WWW 和 FTP 的服务器，另外还连接着学生宿舍楼和教工宿舍楼，学校规定学生只能对服务器进行 FTP 访问，不能进行 WWW 访问，教工则没有此限制。

【技术原理】

IP ACL（IP 访问控制列表或 IP 访问列表）是实现对流经路由器或交换机的数据包根据一定的规则进行过滤。从而提高网络可管理性和安全性。

IP ACL 分为两种：标准 IP 访问列表和扩展 IP 访问列表。标准 IP 访问列表可以根据数据包的源 IP 地址定义规则，进行数据包的过滤。扩展 IP 访问列表可以根据数据包的源 IP、目的 IP、源端口、目的端口、协议来定义规则，进行数据包的过滤。

IP ACL 基于接口进行规则的应用，分为入栈应用和出栈应用。入栈应用是指由外部经该接口进行路由器的数据包进行过滤。出栈应用是指路由器从该接口向外转发数据时进行数据包的过滤。IP ACL 的配置有两种方式：按照编号的访问列表，按照命名的访问列表。标准 IP 访问列表编号范围是 1~99、1300~1999，扩展 IP 访问列表编号范围是 100~199、2000~2699。

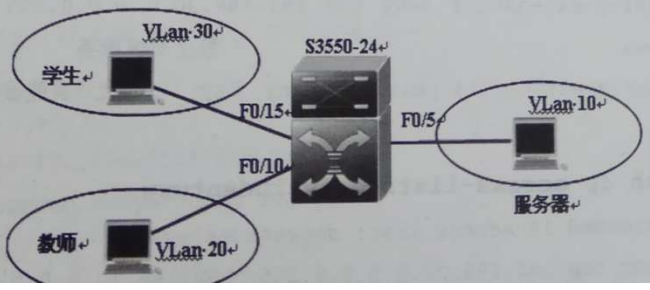
【实现功能】

实现网段间互相访问的安全控制。

【实验设备】

S3550 交换机（1 台）、PC（3 台）、直连线（3 条）

【实验拓扑】



【实验步骤】

步骤1. 基本配置。

```
3550-24(config)#vlan 10
3550-24(config-vlan)#name server
3550-24(config)#vlan 20
3550-24(config-vlan)#name teachers
3550-24(config)#vlan 30
3550-24(config-vlan)#name students
3550-24(config)#interface f0/5
3550-24(config-if)#switchport mode access
3550-24(config-if)#switchport access vlan 10
3550-24(config)#interface f0/10
3550-24(config-if)#switchport mode access
3550-24(config-if)#switchport access vlan 20
3550-24(config)#interface f0/15
3550-24(config-if)#switchport mode access
3550-24(config-if)#switchport access vlan 30
3550-24(config)#int vlan10
3550-24(config-if)#ip add 192.168.10.1 255.255.255.0
3550-24(config-if)#no shutdown
3550-24(config-if)#int vlan 20
3550-24(config-if)#ip add 192.168.20.1 255.255.255.0
3550-24(config-if)#no shutdown
3550-24(config-if)#int vlan 30
3550-24(config-if)#ip add 192.168.30.1 255.255.255.0
3550-24(config-if)#no shutdown
```

步骤2. 配置命名扩展 IP 访问控制列表。

```
3550-24(config)#ip access-list extended denystudentwww
                !定义命名扩展访问列表
3550-24(config-ext-nacl)# deny tcp 192.168.30.0 0.0.0.255  192.168.10.0
0.0.0.255 eq www
                                        ! 禁止 WWW 服务
3550-24(config-ext-nacl)# permit ip any  any      !允许其他服务
```

验证命令：

```
3550-24#sh ip access-lists denystudentwww
        Extended IP access list: denystudentwww
        deny tcp 192.168.30.0 0.0.0.255  192.168.10.0 0.0.0.255 eq www
        permit ip any  any
```

步骤3. 把访问控制列表在接口下应用。

```
3550-24(config)#int vlan 30
3550-24(config-if)#ip access-group denystudentwww in
```

步骤4. 配置 Web 服务器（详见选学实验内容）。

步骤5. 验证测试。

分别在学生网段和教师宿舍网段使用 1 台主机，访问 Web 服务器。测试发现学生网段不能访问网页，教学宿舍网段可以访问网页。

【注意事项】

1、访问控制列表要在接口下应用；

2、要注意 deny 某个网段后要 peimit 其他网段。

【参考配置】

```
3550-24#show run
version 1.0
!
hostname 3550-24
ip access-list extended denystudentwww
 deny tcp 192.168.30.0 0.0.0.255  192.168.10.0 0.0.0.255 eq www
 permit ip any any
interface FastEthernet 0/5
switchport access vlan 10
interface FastEthernet 0/10
 switchport access vlan 20
interface FastEthernet 0/15
 switchport access vlan 30
!
interface Vlan 10
 ip address 192.168.10.1 255.255.255.0
!
interface Vlan 20
 ip address 192.168.20.1 255.255.255.0
!
interface Vlan 30
 ip address 192.168.30.1 255.255.255.0
ip access-group denystudent www in
!
end
```