**标准与扩展ACL**

**1，访问控制列表ACL作用：**

**——读取第三层(网络层)、第四层(传输层)包头信息；**

**——根据预先定义好的规则对包进行过滤；**

**2，访问控制列表的类型：**

**标准访问控制列表：**

**——基于源IP地址过滤数据包；列表号是1~99；应该应用在离目标最近的出方向**

**扩展访问控制列表：**

**——基于源IP地址、目的IP地址、指定协议、端口来过滤数据包；列表号是100~199；**

**——最好应用在离源最近的入口方向**

**命名访问控制列表：**

**——允许在标准和扩展访问控制列表中使用名称代替表号；**

**3，创建标准ACl**

**R(config)# access-list 1 deny 192.168.1.1 0.0.0.0 拒绝单个主机**

**R(config)# access-list 1 permit 192.168.1.0 0.0.0.255 允许一个网段**

**4，将ACL应用于接口**

**R(config-if)# ip access-group 1 {out | in } 出口路由器的对内端口用in；反之用out**

**在接口上取消ACL的应用**

**R(config-if)# no ip access-group 1 {out | in }**

**5，查看访问控制列表：**

**R(config)# show access-lists**

**6，删除ACl**

**R(config)# no access-list 1**

**7，创建扩展ACL**

**语法格式：access-list 表号 拒绝|允许 协议 源IP 目标IP 端口**

**应用1：**

**R(config)# access-list 101 permit ip host 192.168.1.1 host 192.168.2.1**

**R(config)# access-list 101 deny ip any any**

**应用2：**

**R(config)# access-list 101 deny tcp 192.168.1.0 0.0.0.255 192.168.2.0 0.0.0.255 eq 21**

**R(config)# access-list 101 permit ip any any**

**应用3：**

**R(config)# access-list 101 deny icmp 192.168.1.0 0.0.0.255 host 192.168.2.1 echo**

**R(config)# access-list 101 permit ip any any**

**备注点： host 192.168.1.1 = 192.168.1.1 0.0.0.0**

**any = 0.0.0.0 255.255.255.255**

**ip 代表所有的协议**

**将ACL应用于接口**

**R(config-if)# ip access-group 1 {out | in } 出口路由器的对内端口用in；反之用out**

**8，创建命名ACl**

**R(config)# ip access-list {standard | extended} abc**

**备注点： standard 为标准命名ACL； extended为扩展命名ACl； abc为表名**

**R(config-xxx-nacl)# permit ip host 192.168.1.1 host 192.168.2.1**

**R(config-xxx-nacl)# deny ip host 192.168.1.2 host 192.168.2.2 eq 80**

**R(config-xxx-nacl)#deny any**

**插入一条列表**

**R(config-xxx-nacl)# 15 permit host 192.168.1.3 15为序列号**

**9，删除整组ACL**

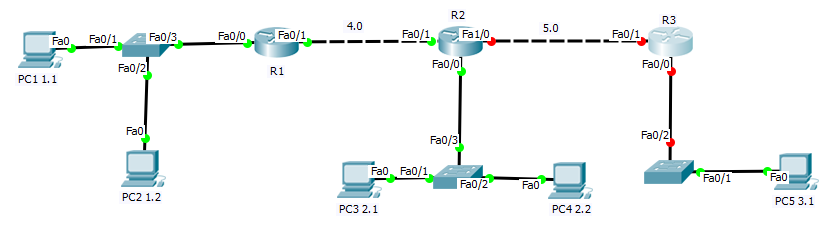
**R(config)# no ip access-list {standard | extended} abc**

**删除组中单一ACl语句**

**R(config-xxx-nacl)# no 序列号**

案例：

通过标准ACL，允许1.0网段访问3.1主机；拒绝2.1主机访问3.1主机所有服务。



配置流程：

1. 配置各个端口的IP；
2. 配置路由表；
3. 设置标准ACL

R2(config)#access-list 1 deny 192.168.1.0 0.0.0.255

R2(config)#access-list 1 deny 192.168.2.1 0.0.0.0

R2(config)#access-list 1 permit any

4，配置端口应用

R2(config)#inter f 0/1

R2(config-if)#ip access-group 1 in

R2(config-if)#inter f 0/0

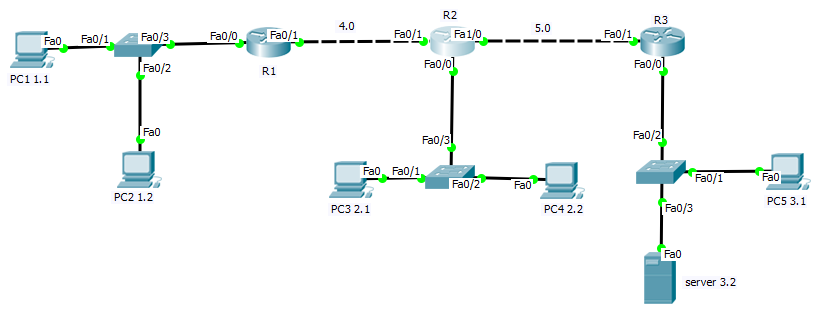
R2(config-if)#ip access-group 1 in

R2(config-if)#inter f 1/0

R2(config-if)#ip access-group 1 out

通过扩展ACL，拒绝1.1主机访问3.2的WEB服务；拒绝2.0网段访问3.0所有服务；

1.0网段可以与2.0网段通信。



把上一个案例ACL给取消：

R2(config)#no access-list 1

配置新的ACL：

R1(config)#access-list 100 deny tcp host 192.168.1.1 host 192.168.3.2 eq 80

R1(config)#access-list 100 permit ip any any

R1(config)#inter f0/0

R1(config-if)#ip access-group 100 in

R2(config)#access-list 100 deny ip 192.168.2.0 0.0.0.255 192.168.3.0 0.0.0.255

R2(config)#access-list 100 permit ip 192.168.2.0 0.0.0.255 192.168.1.0 0.0.0.255

R2(config)#inter f 0/0

R2(config-if)#ip access-group 100 in

命名ACL：允许1.1主机访问3.2主机所有服务；拒绝1.2主机访问所有

R1(config)#ip access-list extended aaa

R1(config-ext-nacl)#permit ip host 192.168.1.1 host 192.168.3.2

R1(config-ext-nacl)#deny ip host 192.168.1.2 any

R1(config-ext-nacl)#permit ip any any

R1(config)#inter f 0/0

R1(config-if)#ip access-group aaa in