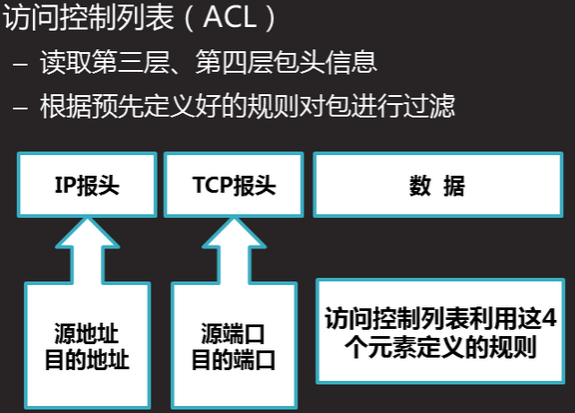
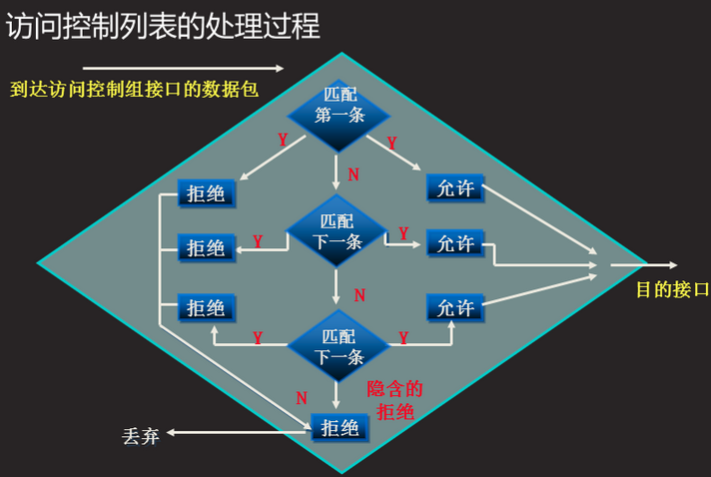
**访问控制列表概述、标准 扩展ACL配置**

**访问控制列表（ACL）**



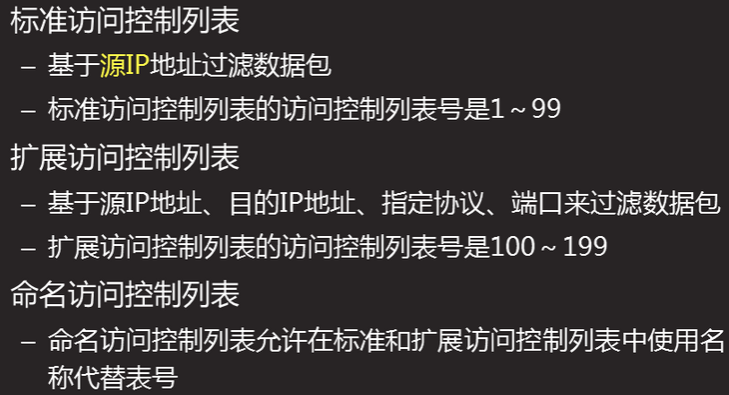
**访问控制列表的处理过程**

**如果匹配第一条规则，则不再往下检查，路由器将决定该数据包允许通过或拒绝通过。**

**如果不匹配第一条规则，则依次往下检查，直到有任何一条规则匹配。**

**如果最后没有任何一条规则匹配，则路由器根据默认的规则将丢弃该数据包。**

**访问控制列表的类型**



**标准访问控制列表的配置**

**1、标准访问控制列表的创建**

**全局：access-list 1 deny 192.168.1.1 0.0.0.0**

**全局：access-list 1 permit 192.168.1.0 0.0.0.255**

**通配符掩码**：也叫做反码。用二进制数0和1表示，如果某位为1，表明这一位不需要进行匹配操作，如果为0表明需要严格匹配。

例：192.168.1.0/24子网掩码是255.255.255.0,其反码可以通过255.255.255.255减去255.255.255.0得到0.0.0.255

**隐含拒绝语句：**

**全局：access-list 1 deny 0.0.0.0 255.255.255.255**

**2、将ACL应用于接口**

**接口模式：ip access-group 列表号 in或out**

注：**access-list 1 deny 192.168.1.1 0.0.0.0或写为**

**access-list 1 deny host 192.168.1.1**

**access-list 1 deny 0.0.0.0 255.255.255.255**

**或写为**

**access-list 1 deny any**

1. **删除已建立的访问控制列表**

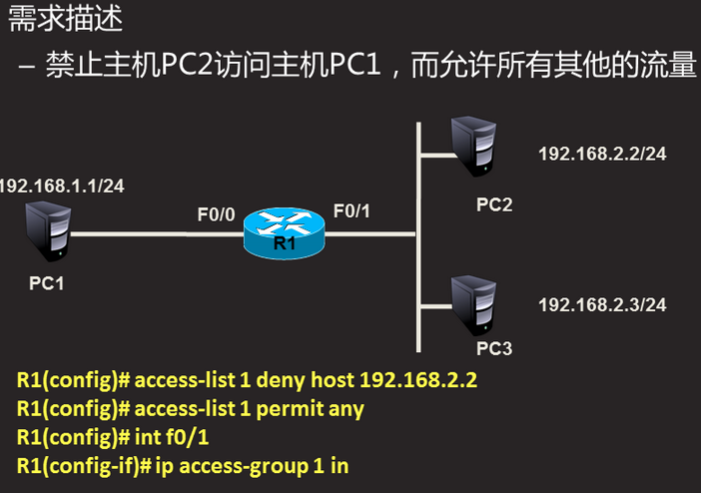
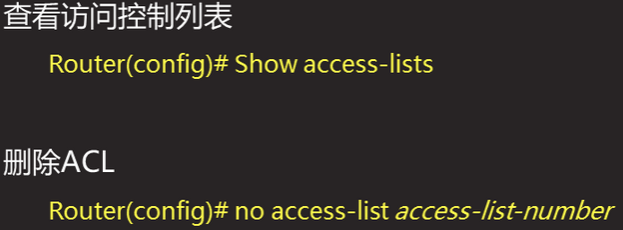
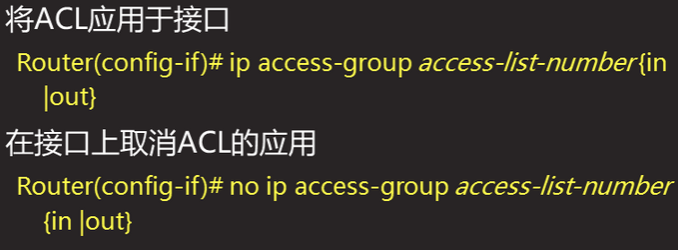
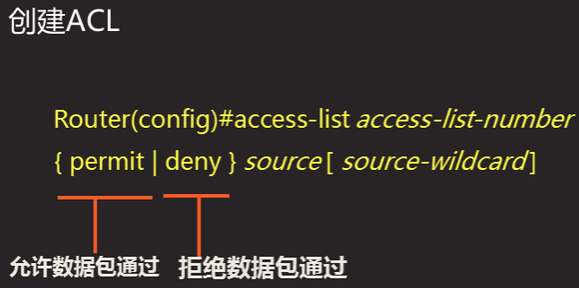
**全局：no access-list 列表号**

1. **接口上取消ACL**

**接口模式：no ip access-group 列表号in 或out**

1. **查看访问控制列表**

**特权：show access-lists**

**扩展访问控制列表**

**1、作用**

**可以根据源IP地址，目的IP地址，指定协议，端口等过滤数据包。**

**2、扩展访问控制列表号:100-199**

**3、eq等于、lt小于、gt大于、neq不等于**

**4、扩展访问控制列表案例：**

**例1：全局： access-list 101 permit ip 192.168.1.0 0.0.0.255 192.168.2.0 0.0.0.255**

**（允许192.168.1.0网络访问192.168.2.0网络的所有服务）**

**全局： access-list 101 deny ip any any**

**（拒绝所有）**

**例2：全局： access-list 101 deny tcp 192.168.1.0 0.0.0.255 host 192.168.2.2 eq 21**

**（拒绝192.168.1.0网段访问192.168.2.2的TCP的21端口）**

**全局：access-list 101 permit ip any any（允许访问所有）**

**例3全局： access-list 101 deny icmp 192.168.1.0 0.0.0.255 host 192.168.2.2 echo**

**（拒绝192.168.1.0 ping 192.168.2.2）**

**5、删除扩展ACL**

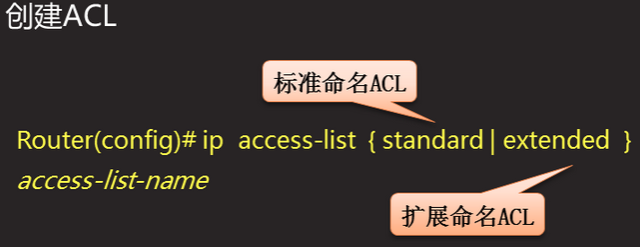
**全局：no access-list 列表号**

**注：扩展与标准ACL不能删除单条ACL语句，只能删除整个ACL。**

1. **扩展ACL应该应用在离源地址最近的路由器上。**

**命名访问控制列表**

1. **命名访问控制列表可以配置标准命名也可配置扩展命名。**



**2、命名访问控列表的ACL语句默第一条为10,第二条为20,依此类推。**

**3、命名ACL可以删除单条ACL语句,而不必删除整个ACL。并且命名ACL语句可以有选择的插入到列表中的某个位置，使得ACL配置更加方便灵活。**



**4、标准命名ACL的配置**

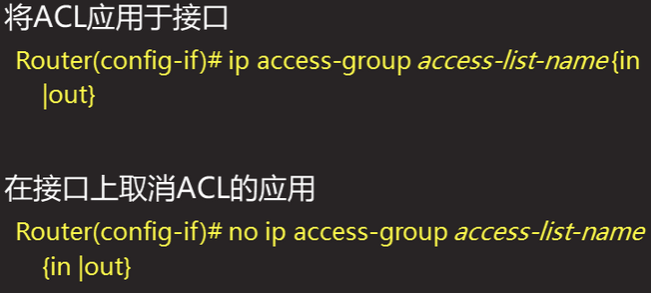
**1）全局:ip access-list standard 名字**

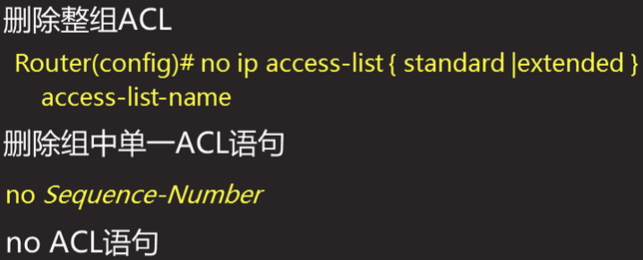
**Permit host 192.168.1.1**

**deny any**

**2)命名ACL应用于接口**

**接口模式：ip access-group 名字 in或out**





**5、扩展命名ACL的配置**

**全局：ip access-list extended 名字**

**deny tcp 192.168.1.0 0.0.0.255 host 192.168.2.2 eq 80**

**（拒绝1.0网段访问2.2的web服务）**

**Permit ip any any**

**/////////////////////////补充：动态路由OSPF///////////////////////**

**OSPF 三张关键的表**： 邻居列表 链路状态数据库 路由表

**七个邻居建立的过程：**down状态、init状态、2-WAY状态、ExStart状态、Exchange状态、Loading状态、Full状态

**OSPF区域**

为了适应大型的网络，OSPF在AS内划分多个区域

每个OSPF路由器只维护所在区域的完整链路状态信息

**区域ID**

区域ID可以表示成一个十进制的数字

也可以表示成一个IP

**骨干区域Area 0**

负责区域间路由信息传播

**非骨干区域**

Router ID

OSPF区域内唯一标识路由器的IP地址

Router ID选取规则

首先，选取路由器loopback接口上数值最高的IP地址

如果没有loopback接口，在物理端口中选取IP地址最高的

也可以使用router-id命令指定Router ID

**DR和BDR的选举方法**

**自动选举DR和BDR**

网段上Router ID最大的路由器将被选举为DR，第二大的将被选举为BDR

**手工选择DR和BDR**

优先级范围是0～255，数值越大，优先级越高，默认为1

如果优先级相同，则需要比较Router ID

如果路由器的优先级被设置为0，它将不参与DR和DBR的选举

**启动OSPF路由进程**

**Router(config)# router ospf *process-id***

**指定OSPF协议运行的接口和所在的区域：**

**Router(config-router)# network *address* *inverse-mask* area *area-id***

**修改接口的优先级（为了指定DR，修改完之后要重启该网段所有的ospf进程或者重启设备）**

**Router(config-if)#ip ospf priority *priority***

**案例**

