Cisco ACL

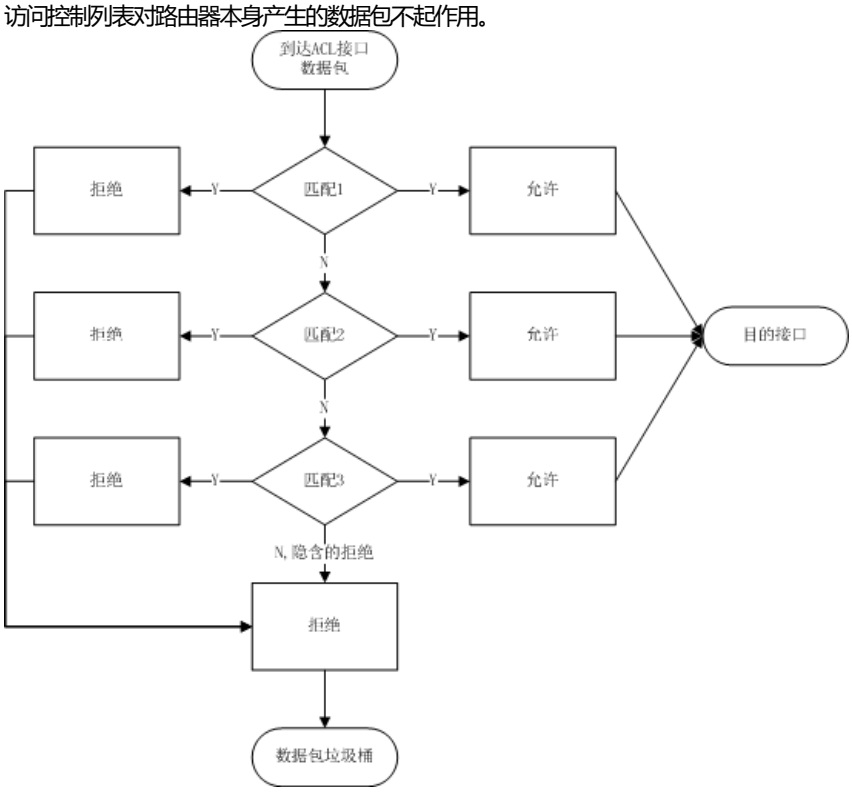
访问控制列表(ACL)是应用在路由器接口的指令列表（即规则）。

ACL基本类型：
1.标准访问控制列表　检查被路由数据包的源地址。表号（1-99）
2.扩展访问控制列表　对数据包的源地址与目标地址均进行检查，也能检查特定的协议，端口号以及其他参数。表号（100-199）
3.基于协议　表号（200-299）
4.基于IPX标准　表号（800-899）
5.基于IPX扩展　表号（900-999）

ACL的定义是基于协议的。

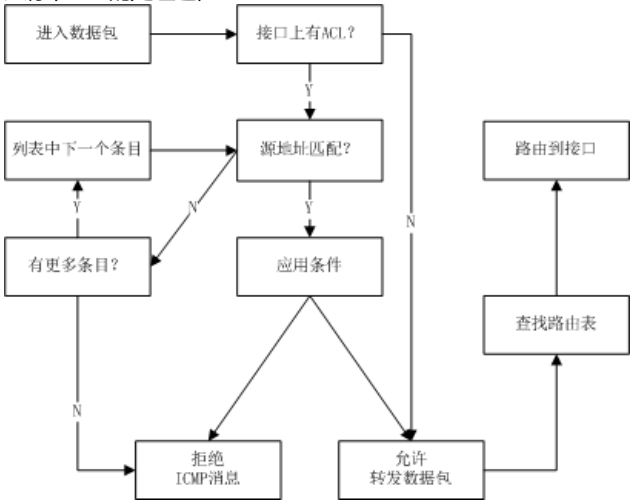
ACL用途
1.提供网络访问的基本安全手段。
2.访问控制列表可用于QoS（Quality of Service，服务质量）对数据流量进行控制。
3.提供对通信流量的控制手段。

访问控制列表对路由器本身产生的数据包不起作用。

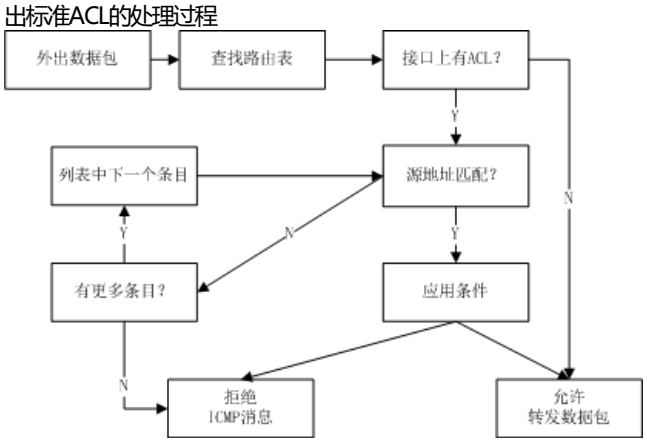


在接口上应用ACL
Router(config-if)#ip access-group *access-list-number* { in | out }

入标准ACL的处理过程



出标准ACL的处理过程



access-list命令：

Router(config)#access-list *access-list-number* { permit | deny } source [source-wildcard] [log]

Router(config)#access-list *access-list-number* { permit | deny } protocol [source source-wildcard destination destination-wildcard] [operator operan] [established] [log]

1.access-list-number　ACL表号

2.source　数据包的源地址

　2.1.主机：192.168.1.12 0.0.0.0

　2.2.子网：192.168.1.0　0.0.0.255

　2.3.所有任何：0.0.0.0 255.255.255.0

3.source-wildcard　用来跟源地址一起决定哪些位需要进行匹配操作。

4.destination　数据包的目的地址

5.destination-wildcard　用来跟目的地址一起决定哪些位需要进行匹配操作。

6.log　生成相应的日志信息。

7.protocol　指定协议类型。

8.operator operan lt(小于),gt(大于),eq(等于),neq(不等于)和一个端口号。

9.established　如果数据包使用一个已建立连接（例如该数据包的ACK位设置了），便可以允许TCP信息量通过。

通配符：

1.any

Router(config)#access-list 1 permit 0.0.0.0 255.255.255.0

Router(config)#access-list 1 permit any

2.host

Router(config)#access-list 1 permit 172.30.16.29 0.0.0.0

Router(config)#access-list 1 permit host 172.30.16.29