访问控制列表实验

金舒原
jinshuyuan@mail.sysu.edu.cn
计算机学院

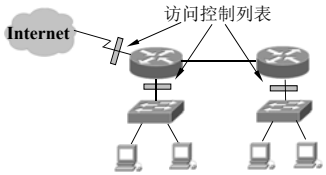
本章内容

- 访问控制列表概述
- 标准访问控制列表及其配置与验证
- 扩展访问控制列表及其配置与验证

访问控制列表概述
ACL(Access Control List)

主要作用是阻止非法用户对资源节点的访问，以及限制特定用户节点的访问权限

- 检查和过滤数据包
- 限制网络流量，提高网络性能
- 限制和减少路由更新的内容
- 提供网络访问的基本安全级别



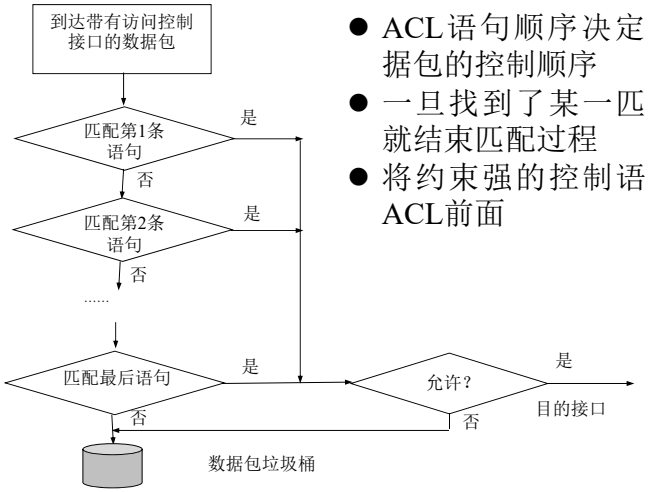
一般将ACL设置在路由器的接口上，对接口的进方向和出方向的数据包进行过滤

* 只能过滤经过路由器的数据包，对路由器本身所产生的数据包不起作用

ACL的工作原理

- 当一个数据包进入路由器的某一个接口时，路由器首先检查该数据包是否可路由或桥接，然后检查是否在入接口上应用了ACL
- 如果有ACL
  - 将该数据包与ACL中的条件语句相比较
  - 若允许通过，则检查路由表决定转发的出接口：出接口若应用了ACL，则按该出口的ACL规则进行过滤，若无则直接输出
  - 若不允许通过，则丢弃
- 若无ACL，则直接检查路由表决定转发的出接口
  - 出接口若应用了ACL，则按该出口的ACL规则进行过滤，若无则直接输出

ACL匹配检查过程



- ACL语句顺序决定了对数据包的控制顺序
- 一旦找到了某一匹配条件就结束匹配过程
- 将约束强的控制语句放在ACL前面

配置访问控制列表需注意的规则

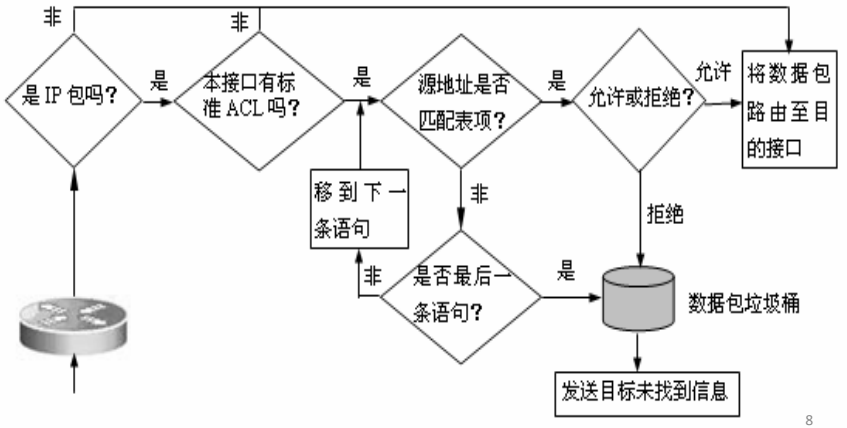
- 配置ACL，应先编辑好列表，再加载到相应的接口上
- ACL中至少要有一条允许语句；所有ACL最后都隐含一条“全部拒绝”的命令
- 配置ACL一般按从特殊到一般的顺序；先拒绝特定主机，再执行一般过滤操作：把最有限制性的语句放在靠前位置，将全部允许或者全部拒绝放置在末行
- 新的列表项会加到ACL的最后；若想改变已应用的ACL，需先删除已存在的整个ACL(不能有选择地删除某个ACL条目）再应用新的ACL
- 并不是ACL的语句越多越好；ACL会消耗路由器资源，影响路由器性能
- 若接口没有配置ACL则该接口会正常处理数据

访问控制列表的类型

- 标准访问控制列表
  - 只能够检查可被路由的数据包的源地址
  - 根据源网络、子网、源主机IP地址来决定对数据包的拒绝或允许
- 扩展访问控制列表
  - 能够检查可被路由的数据包的源地址、目的地址、协议、端口号、其他参数等
  - 配置灵活、精确控制

标准ACL的工作过程

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



标准ACL的配置

1、使用access-list命令创建访问控制列表

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

2、使用ip access-group命令把访问控制列表应用到某端口

（config-if）#ip access-group access-list-number {in|out}

access-list 命令的参数	描　　述
access-list-number	访问控制列表表号，用来指定入口属于哪一个访问控制列表。对于标准ACL来说，是一个从1到99或1300到1999之间的数字
Deny	如果满足条件，则拒绝从该入口来的通信流量
Permit	如果满足条件，则允许从该入口来的通信量
Source	数据包的源地址，可以是网络地址或是主机IP地址
source-wildcard	（可选项）通配符掩码，又称反掩码，用来跟源地址一起决定哪些位需要匹配
Log	（可选项）生成相应的日志消息

标准ACL的配置

例子：在路由器上RTB上配置标准ACL

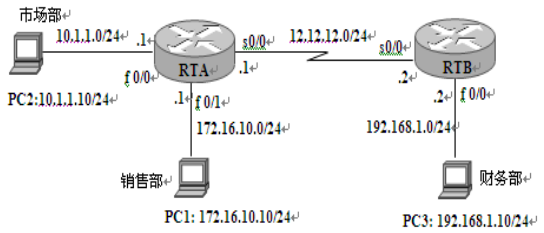
RTB(config)# access-list 1 permit host 172.16.10.10
RTB(config)# access-list 1 deny 172.16.10.0 0.0.0.255
RTB(config)# access-list 1 permit any
RTB(config)# interface s0/0
RTB(config-if)# ip access-group 1 in

标准ACL的配置

- 在通配符掩码中有两种比较特殊，分别是any和host
  - any可以表示任何IP地址，例如
    Router(config) # access-list 10 permit 0.0.0.0 255.255.255.255
    等同于：
    Router (config) # access-list 10 permit any
  - host表示一台主机，例如：
    Router (config) # access-list 10 permit 172.16.30.22 0.0.0.0
    等同于：
    Router (config) # access-list 10 permit host 172.16.30.22
- 删除一个已经建立的标准ACL：在access-list命令前加no
  - Router (config) # no access-list access-list-number
    例如 Router (config) # no access-list 10
- 验证标准ACL
  - show access-lists、show ip interface 等命令

标准ACL应用的例子

某企业销售部、市场部的网络和财务部的网络通过路由器RTA和RTB相连，整个网络配置RIPv2路由协议。要求在RTB上配置标准ACL，允许销售部的主机PC1访问路由器RTB，但拒绝销售部的其他主机访问RTB，允许销售部、市场部网络上所有其他流量访问RTB。



- 在路由器上RTB上配置如下：
  - RTB(config)# access-list 1 permit host 172.16.10.10
  - RTB(config)# access-list 1 deny 172.16.10.0 0.0.0.255
  - RTB(config)# access-list 1 permit any
  - RTB(config)# interface s0/0
  - RTB(config-if)# ip access-group 1 in

验证标准ACL的配置

① show access-lists命令：查看所有访问控制列表内容

- RTB# show access-lists

```
Standard ip access list 1
10 permit 172.16.10.20
20 deny 172.16.10.0, wildcard bits 0.0.0.255 (16 matches)
30 permit any (18 matches)
```

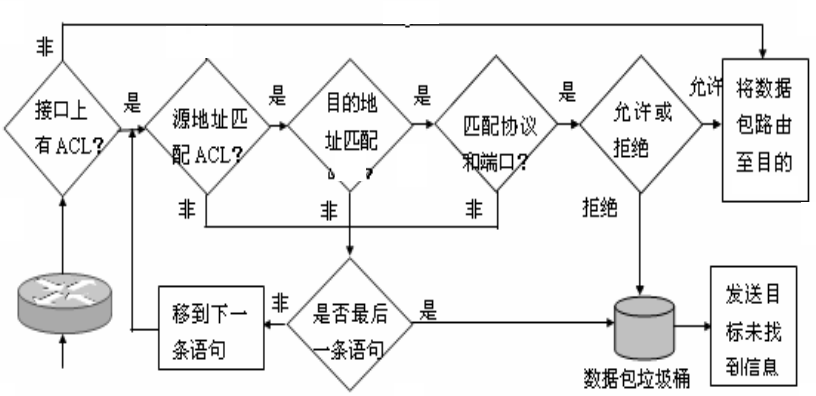
② show ip interface命令：查看ACL作用在IP接口上的信息

- RTB# show ip interface

```
Serial 0/0/0 is up,line protocol is up
Internet address is 12.12.12.12/24
Broadcast address is 255.255.255.255
Address determined by setup command
MTU is 1500 bytes
Helper address is not set
Directed broadcast forwarding is disabled
Outgoing access list is not set
Inbound access list is 1
```


扩展ACL的工作过程

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



配置扩展ACL

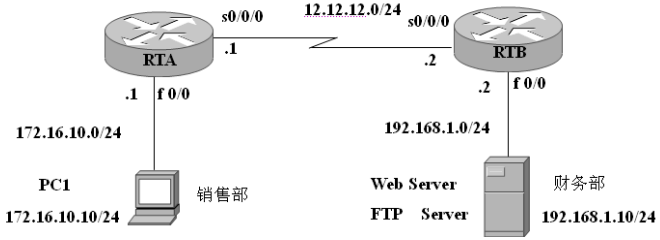
(config)# access-list *access-list-number* {deny | permit} *protocol source* [*source-wildcard destination destination-wildcard*] [*operator operand*] [established]

参 数	描 述
access-list-number	访问控制列表表号，使用一个 100 到 199 或 2000 到 2699 之间的数字来标识一个扩展访问控制列表
deny	如果条件符合就拒绝后面指定的特定地址的通信流量
permit	如果条件符合就允许后面指定的特定地址的通信流量
protocol	用来指定协议类型，如 IP、ICMP、TCP 或 UDP 等
source 和 destination	数据包的源地址和目的地址，可以是网络地址或是主机 IP 地址
source-wildcard	应用于源地址的通配符掩码
destination-wildcard	应用与目的地的通配符掩码位
operator	（可选项）比较源和目的端口，可用的操作符包括 lt（小于）、gt（大于）、eq（等于）、neq（不等于）和 range（包括的范围） 如果操作符位于源地址和源地址通配符之后，那么它必须匹配源端口。如果操作符位于目的地址和目的地址通配符之后，那么它必须匹配目的端口。range 操作符需要两个端口号，其他操作符只需要一个端口号
operand	（可选项）指明 TCP 或 UDP 端口的十进制数字或名字。端口号可以从 0 到 65535
established	（可选项）只针对 TCP 协议，如果数据包使用一个已建连接（例如，具有 ACK 位组），便可允许 TCP 信息量通过

扩展ACL应用的例子

某企业销售部的网络和财务部的网络通过路由器RTA和RTB相连，整个网络配置RIPv2路由协议。要求在RTA上配置扩展ACL，实现以下4个功能：

（1）允许销售部网络172.16.10.0的主机访问WWW Server 192.168.1.10；
（2）拒绝销售部网络172.16.10.0的主机访问FTP Server 192.168.1.10；
（3）拒绝销售部网络172.16.10.0的主机Telnet路由器RTB；
（4）拒绝销售部主机172.16.10.10 Ping路由器RTB。



扩展ACL应用的例子

- 在路由器RTA上配置如下：

```
RTA(config)# access-list 100 permit tcp  172.16.10.0  0.0.0.255 host 192.168.1.10 eq 80
RTA(config)# access-list 100 deny  tcp  172.16.10.0  0.0.0.255 host 192.168.1.10 eq 20
RTA(config)# access-list 100 deny  tcp  172.16.10.0  0.0.0.255 host 192.168.1.10 eq 21
RTA(config)# access-list 100 deny  tcp  172.16.10.0  0.0.0.255 host 12.12.12.2 eq 23
RTA(config)# access-list 100 deny  tcp  172.16.10.0  0.0.0.255 host 192.168.1.2 eq 23
RTA(config)# access-list 100 deny  icmp  host 172.16.10.10  host 12.12.12.2
RTA(config)# access-list 100 deny  icmp  host 172.16.10.10  host 192.168.1.2
RTA(config)# access-list 100 permit  ip  any  any
RTA(config)# interface  f0/0
RTA(config-if)# ip  access-group  100  in
```

- 验证扩展ACL

  使用show access-lists和show ip interface命令，其使用方法与标准ACL相同

访问控制列表实验

- 实验目的
  - 掌握标准访问列表规则及配置
  - 掌握扩展访问列表规则及配置
  - 了解标准访问列表和扩展访问列表的区别
  - 使用基于时间的ACL实现主机对服务器的高级访问控制
- 完成ACL实验（实验描述助教已发大家）
  - 重要信息信需给出截图，注意实验步骤的前后对比

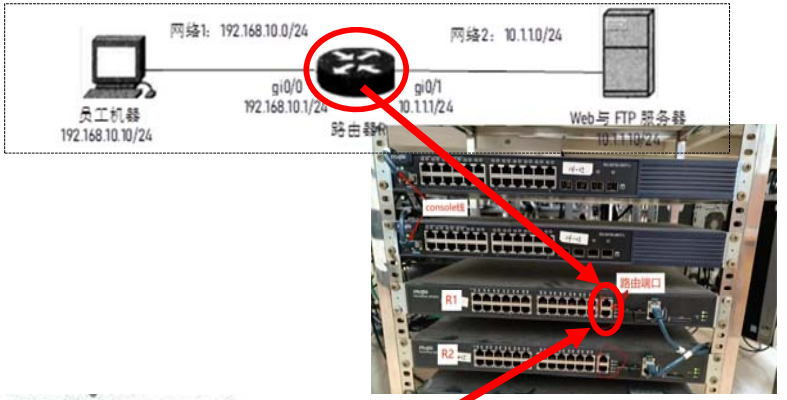
实验拓扑图

访问控制列表实验

【实验内容】

1. 搭建实验拓扑：正确配置员工机器和服务器机器的IP地址、子网掩码、网关。复习网络配置等命令，以检查机器是否正确配置了网卡地址等。
2. 搭建实验拓扑：正确配置路由器的2个路由端口。复习路由器的配置命令，复习如何查看路由器的运行配置，以检查是否正确配置了路由器接口的IP地址、子网掩码等。
3. 安装Web和FTP服务器：在服务器机器上，正确安装Web与FTP服务器并启动它们。FTP服务器至少创建一个用户名和密码。
4. 在路由器上设置基于时间的ACL ：实现员工机在工作时间（9：00-18：00）仅可以访问FTP服务器，不可以访问Web服务器；在非工作时间仅可以访问Web服务器，不可以访问FTP服务器。

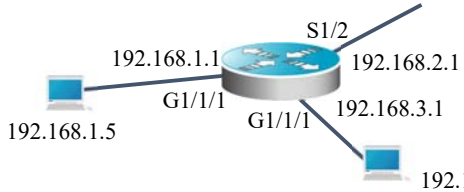
访问控制列表实验




```
1-RSR20-1#configure terminal
Enter configuration commands, one per line.   End with CNTL/Z.
1-RSR20-1(config)#inter
1-RSR20-1(config)#interface Giga
1-RSR20-1(config)#interface GigabitEthernet 0/0
1-RSR20-1(config-if-GigabitEthernet 0/0)#ip address 192.168.1.100 255.255.255.0
1-RSR20-1(config-if-GigabitEthernet 0/0)#
```

直连路由

直连路由是由链路层协议发现的，一般指去往路由器的接口地址所在网段的路径，该路径信息不需要网络管理员维护，也不需要路由器通过某种算法进行计算获得，只要该接口处于活动状态，路由器就会把通向该网段的路由信息填写到路由表中



	目标网段	出口
C	192.168.1.0	gigabitethernet 1/1/1
C	192.168.2.0	Serial 1/2
C	192.168.3.0	gigabitethernet 1/1/1

查看路由器端口状态的命令

- show ip interface brief
- R1

```
14-RSR20-1#show ip interface brief
Interface                  IP-Address(Pri)   IP-Address(Sec)   Status          Protocol
Serial 2/0                 no address        no address        up              down
SIC-3G-WCDMA 3/0           no address        no address        up              down
GigabitEthernet 0/0        no address        no address        down            down
GigabitEthernet 0/1        no address        no address        down            down
VLAN 1                     no address        no address        up              down
```

- R2

```
14-RSR20-2#sh ip int br
Interface                  IP-Address(Pri)   IP-Address(Sec)   Status          Protocol
Serial 2/0                 no address        no address        up              down
Serial 3/0                 no address        no address        down            down
GigabitEthernet 0/0        no address        no address        down            down
GigabitEthernet 0/1        no address        no address        down            down
VLAN 1                     no address        no address        up              down
```

*图中列出的以太网接口是千兆的GigabitEthernet ,第二个串口是“S 3/0” ,两个路由器之间的“S 2/0”已经连接起来了，所以会看到s2/0的status是 “up”

访问控制列表实验

- **若用实验室PC**
  - 实验用IP地址
  需配置在实验网卡上

- **若用个人笔记本电脑**
  - 到实验室助教处按规定借用USB转网卡转接头