访问控制列表（ACL）

主要内容

- 使用标准访问控制列表和扩展访问控制列表控制网络流量的方法
- 标准访问控制列表和扩展访问控制列表以及在路由接口应用ACL的实例。

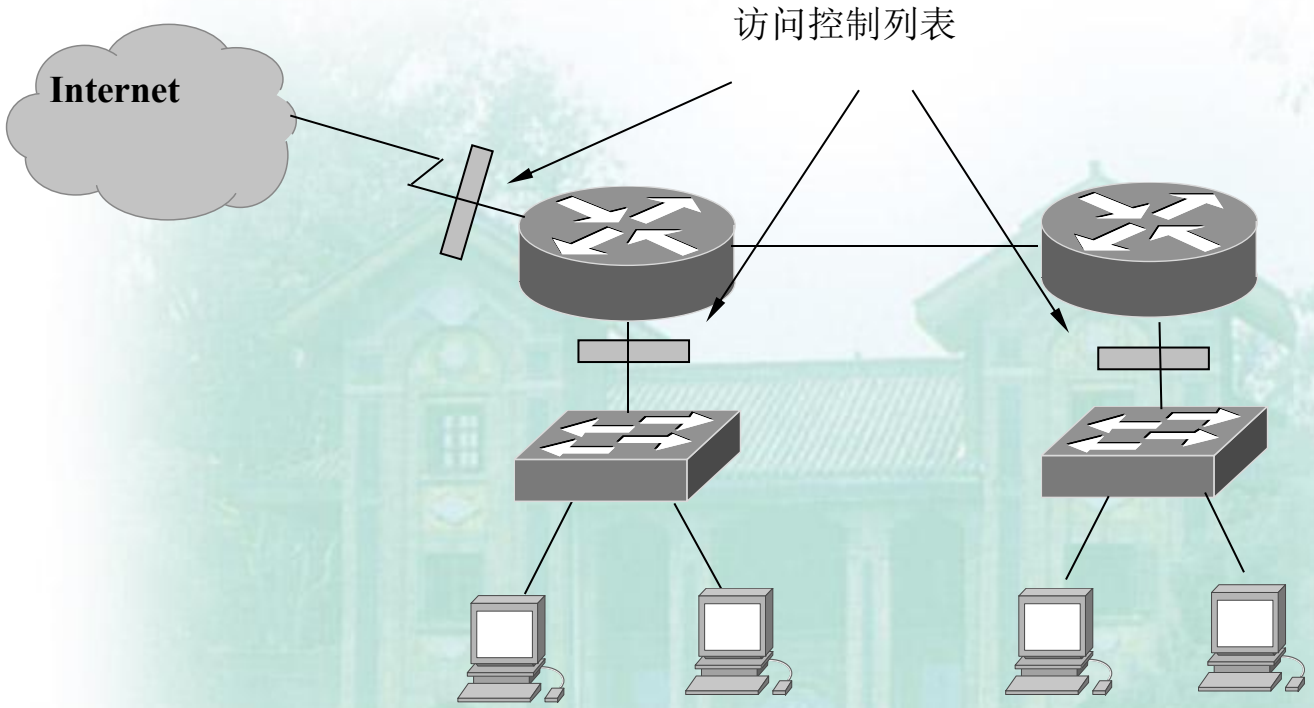
访问控制列表概述

概念

访问控制列表简称 ACL(Access Control Lists ），它使用包过滤技术，在路由器上读取第3层或第4层包头中的信息，如源地址、目的地址、源端口、目的端口以及上层协议等，根据预先定义的规则决定哪些数据包可以接收、哪些数据包需要拒绝，从而达到访问控制的目的。配置路由器的访问控制列表是网络管理员一件经常性的工作。

访问控制列表概述

组成



网络中使用ACL

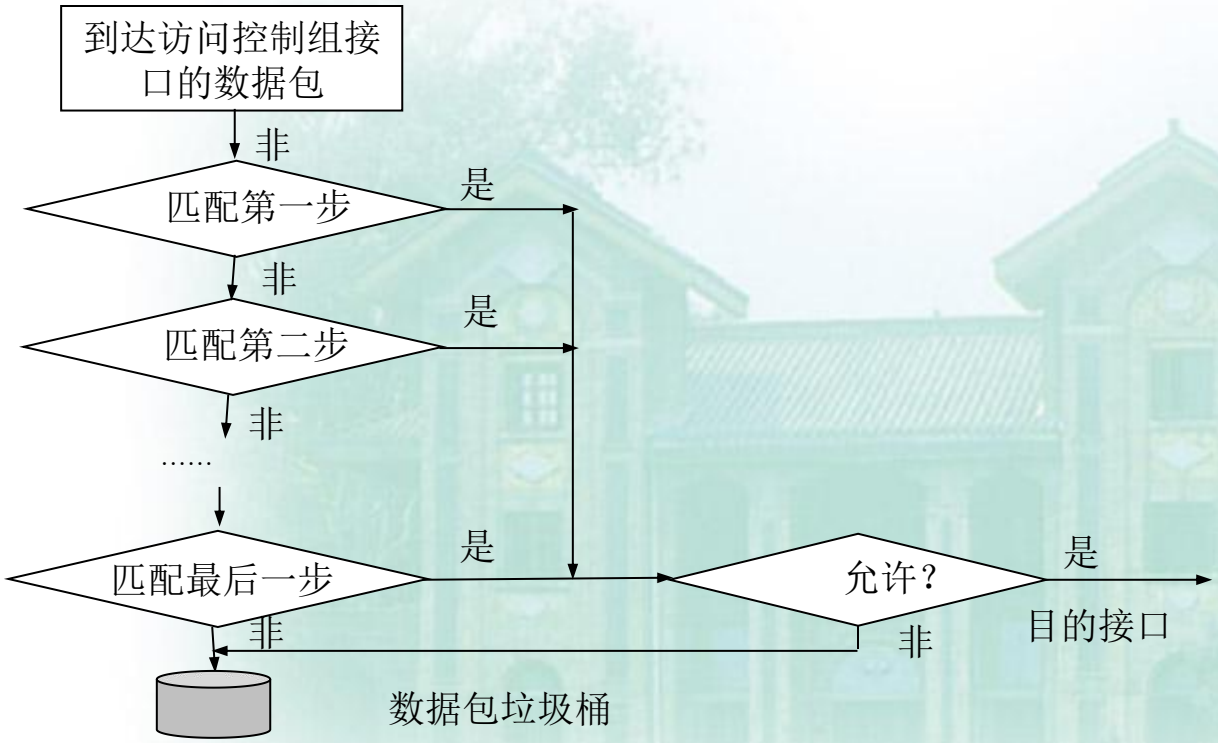
ACL的工作原理

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可桥接。然后路由器检查是否在入站接口上应用了ACL。
- 如果有ACL，就将该数据包与ACL中的条件语句相比较。
- 如果数据包被允许通过，就继续检查路由器选择表条目以决定转发到的目的接口。
- ACL不过滤由路由器本身发出的数据包，只过滤经过路由器的数据包。
- 下一步，路由器检查目的接口是否应用了ACL。如果没有应用，数据包就被直接送到目的接口输出。

ACL的工作原理

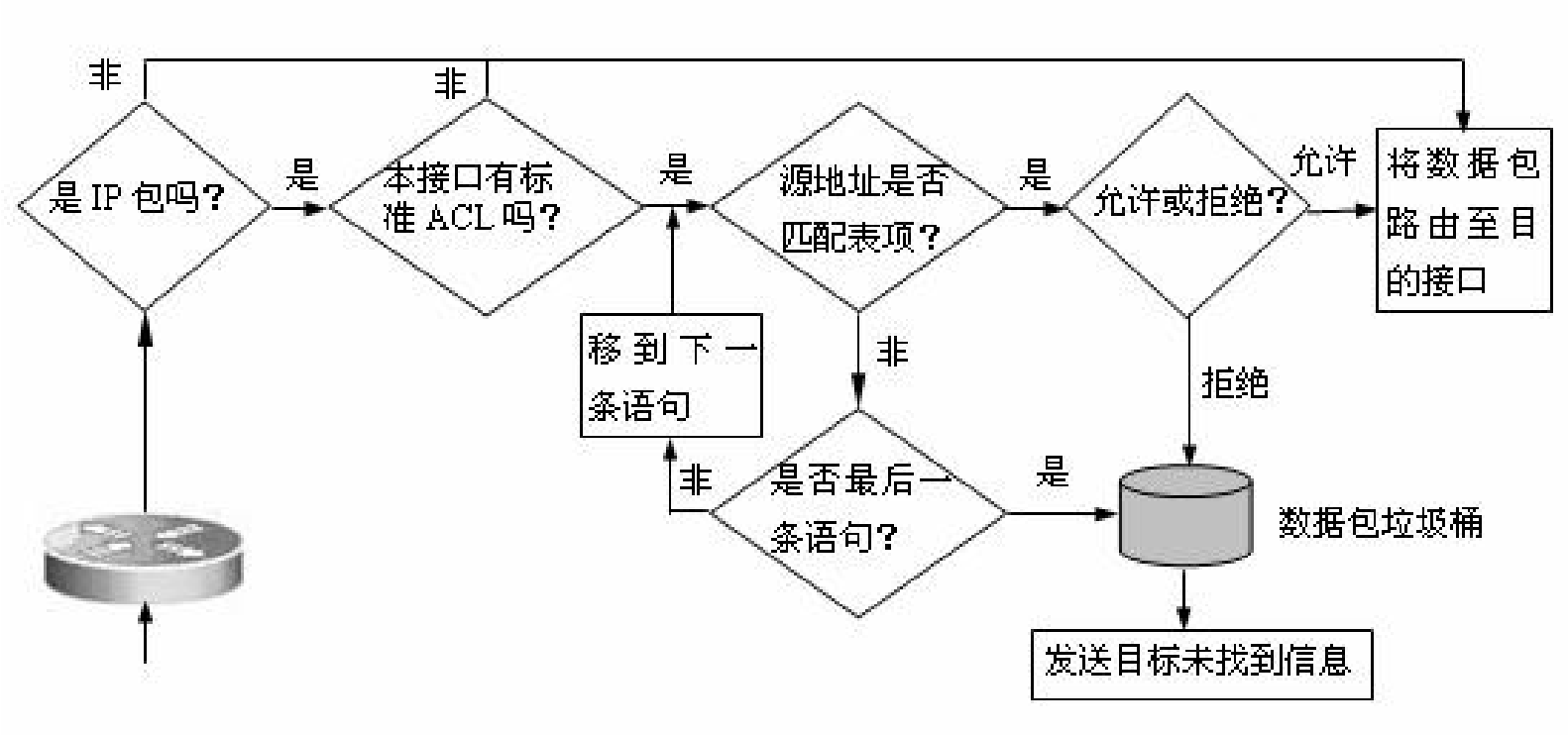
ACL匹配性检查



配置访问控制列表

- 最广泛使用的访问控制列表是IP访问控制列表
- IP访问控制列表工作于TCP/IP协议组。
- 按照访问控制列表检查IP数据包参数的不同，可以将其分成
  - 标准ACL
  - 扩展ACL

标准ACL的工作过程



标准ACL的工作过程

配置标准ACL

在路由器上RTB上配置：

- 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

配置标准ACL

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	如果满足测试条件，则拒绝从该入口来的通信流量
Permit	如果满足测试条件，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，用来记录经过ACL入口的数据包的情况

配置标准ACL

- 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
- 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：

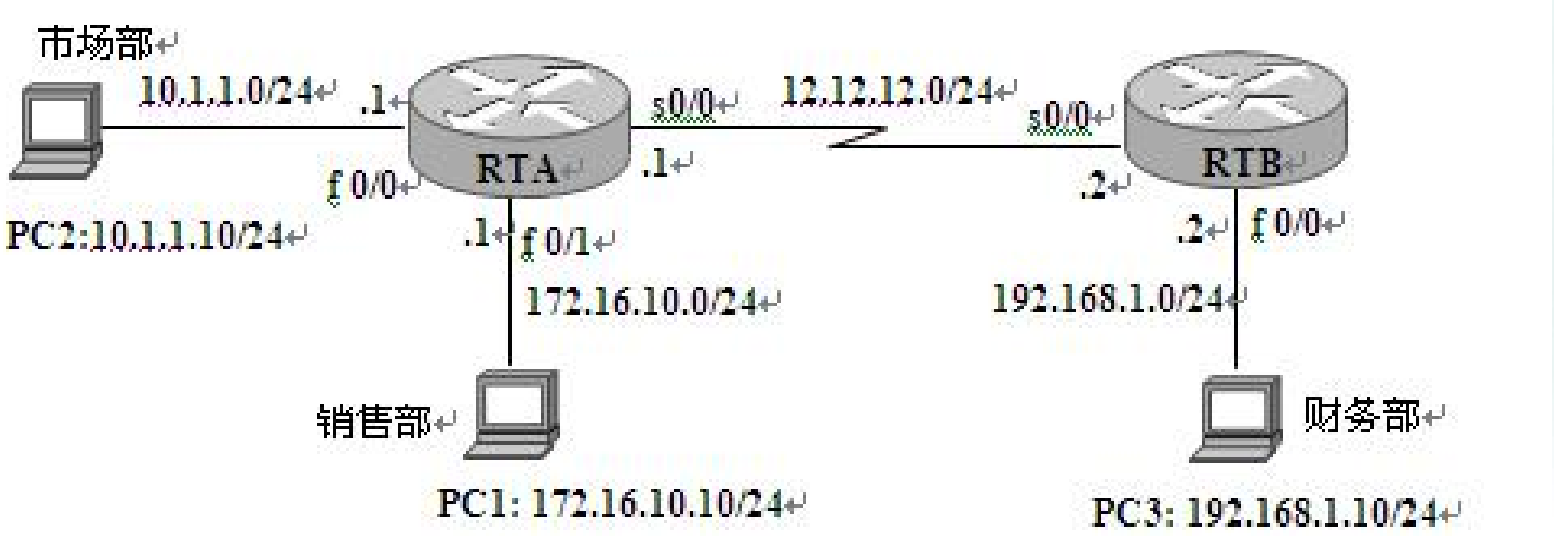
- Router (config) # access-list 10 permit host 172. 16. 30.22
- 另外，可以通过在access-list命令前加no的形式，来删除一个已经建立的标准ACL，使用语法格式如下：
- Router (config) # **no access-list** *access-list-number*

例如：

- Router (config) # no access-list 10

标准ACL应用实例

- 如图所示，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，保证网络正常通信。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。



标准ACL应用实例

配置标准ACL

- 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**

标准ACL应用实例

- 验证标准ACL
- 配置完IP访问控制列表后，如果想知道是否正确，可以使用
- show access-lists、show ip interface

  等命令进行验证。

验证标准ACL

①show access-lists命令

该命令用来查看所有访问控制列表的内容。

- 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)

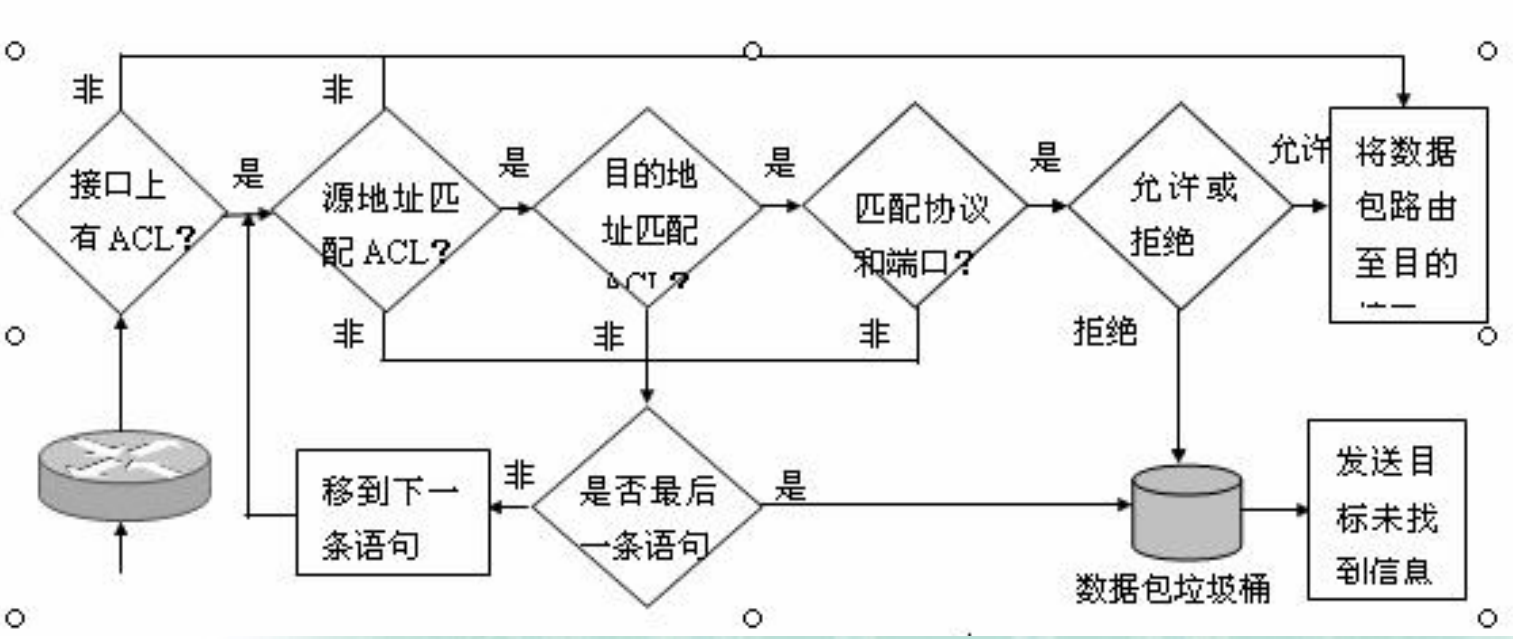
验证标准ACL

②show ip interface命令

该命令用于查看ACL作用在IP接口上的信息，并指出ACL是否正确设置。

```
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
```

扩展访问控制列表



扩展ACL的工作过程

配置扩展ACL

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

配置扩展ACL

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

扩展ACL应用实例

下面以一个实例来说明扩展ACL的配置和验证过程。

如下图所示，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，保证网络正常通信。

要求在RTA上配置扩展ACL，实现以下4个功能：

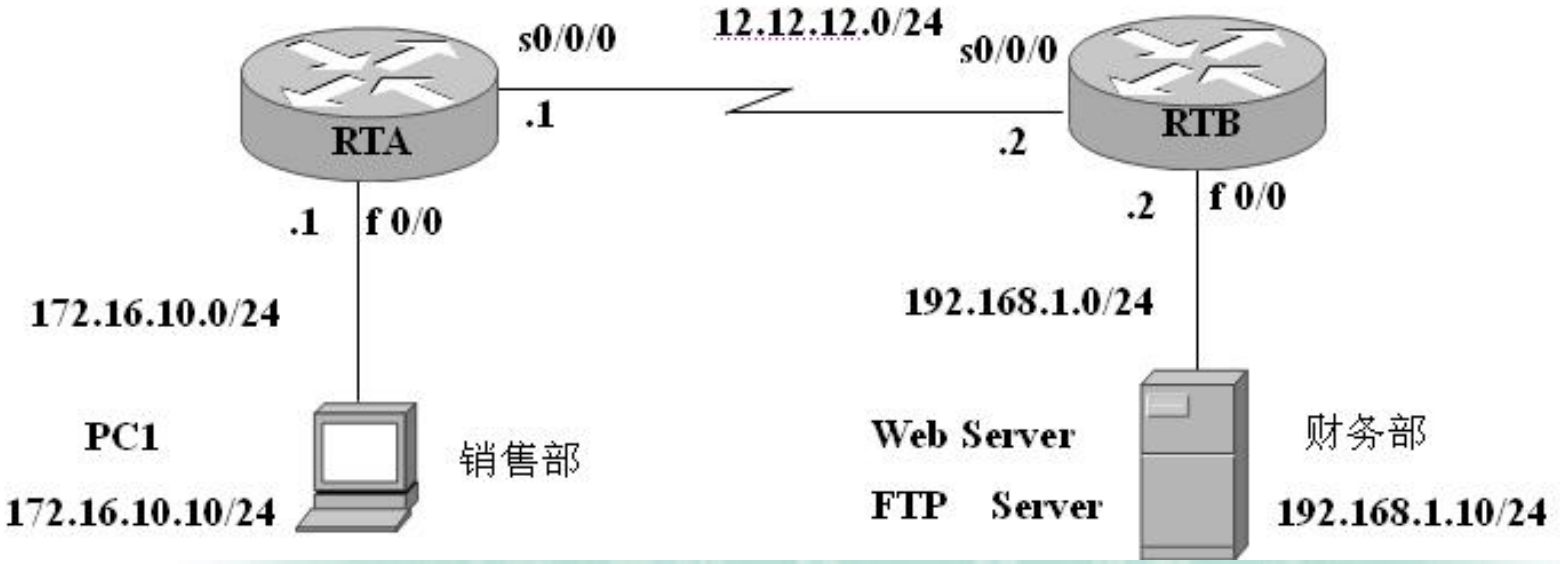
（1）允许销售部网络172.16.10.0的主机访问WWW Server 192.168.1.10；

（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应用实例



扩展ACL应用实例

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同样使用show access-list和show ip interface命令进行，其使用方法与标准ACL相同。