第7章　访问控制列表ACL

- ACL概述
- ACL的工作过程
- ACL分类
- ACL配置
- 翻转掩码
- 标准ACL的配置
- 扩展ACL的配置
- 命名（Named）ACL的配置
- 使用ACL控制虚拟终端（VTY）的访问

本章要求

- 1、了解ACL的概念、用途、工作过程和分类
- 2、掌握翻转掩码的概念
- 3、理解和掌握标准ACL、扩展ACL、命名ACL的配置过程
- 4、理解和掌握使用ACL控制虚拟终端访问的配置过程

ACL概述

- 访问控制列表（Access Control List，ACL）
  - 应用在路由器接口的指令列表
  - 指定哪些数据报可以接收、哪一些需要拒绝
- ACL用途

（1）限制网络流量、提高网络性能；

（2）提供对通信流量的控制手段；

（3）提供网络访问的基本安全手段；

（4）在路由器（交换机）接口处，决定哪种类型的通信流量被转发、哪种被阻塞。

ACL的工作过程

- ACL的操作过程
  - 入站访问控制操作过程
  - 出站访问控制操作过程
- ACL的逻辑测试过程

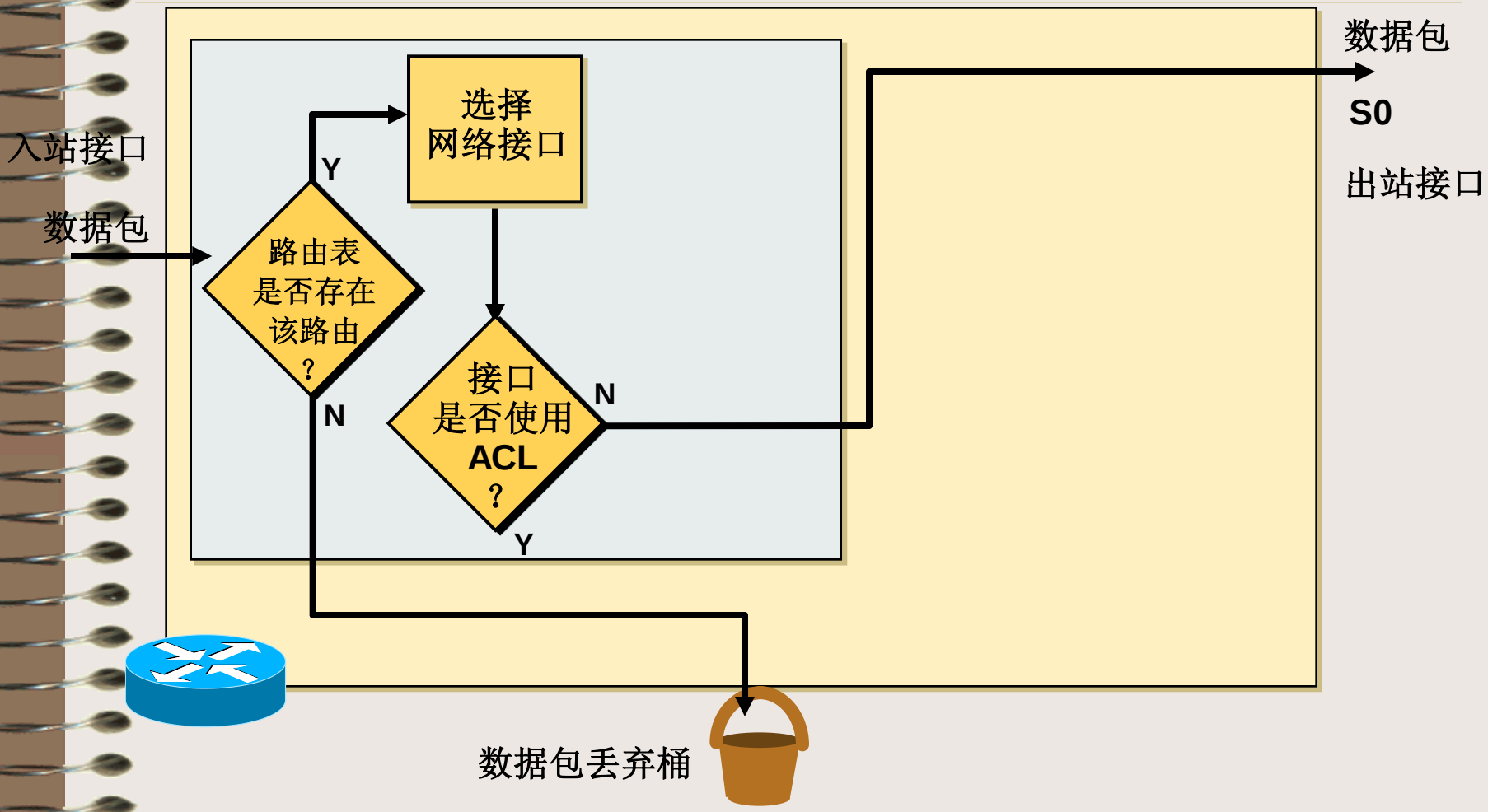
入站访问控制操作过程

- 相对网络接口来说，从网络上流入该接口的数据包，为入站数据流。
- 对入站数据流的过滤控制称为入站访问控制。
- 如果一个入站数据包被访问控制列表禁止（deny），那么该数据包被直接丢弃（discard）。
- 只有那些被ACL允许（permit）的入站数据包才进行路由查找与转发处理。
- 入站访问控制节省了那些不必要的路由查找转发的开销。

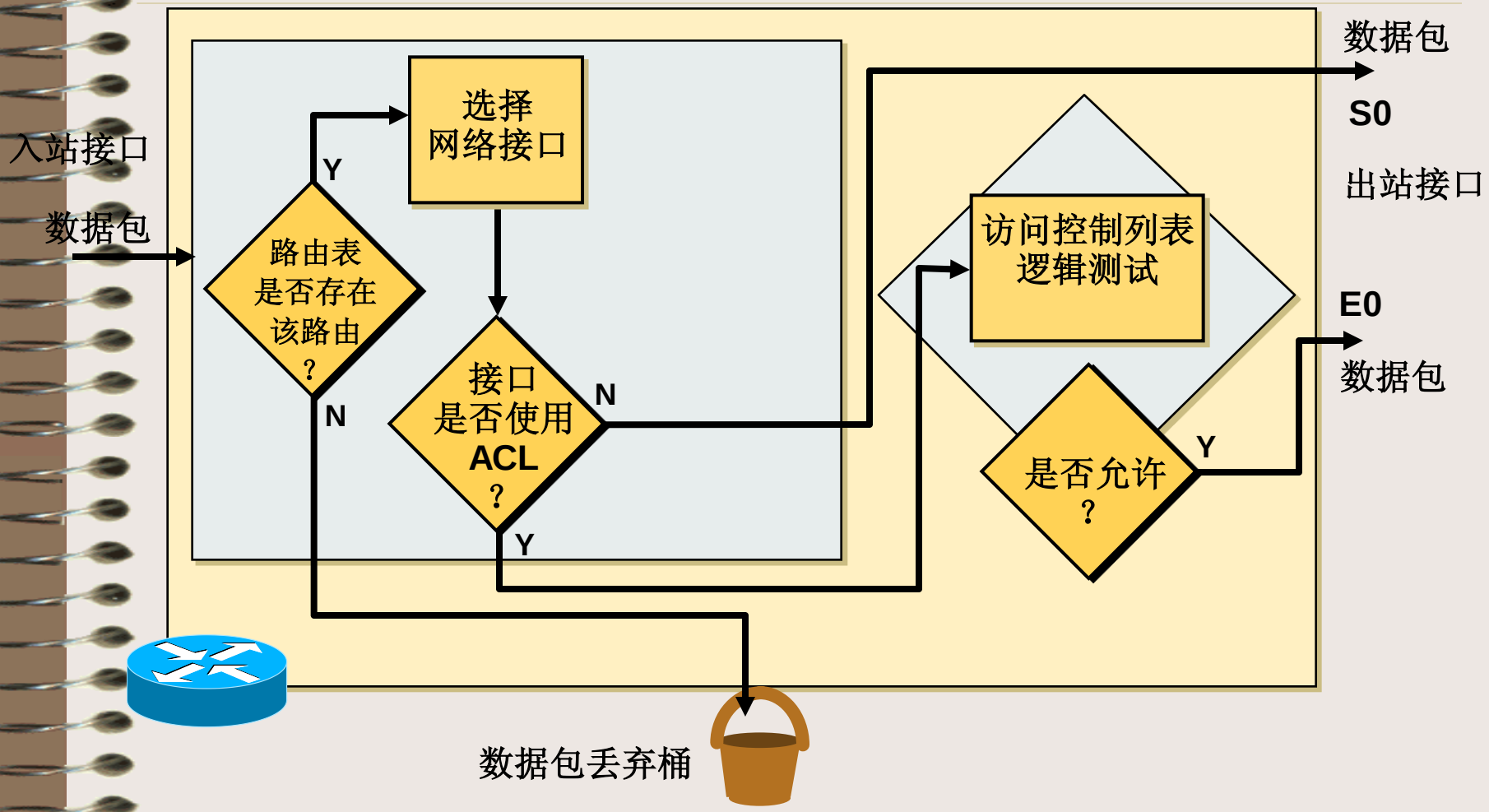
出站访问控制操作过程

- 从网络接口流出的网络数据包，称为出站数据流。
- 出站访问控制是对出站数据流的过滤控制。
- 那些被允许的入站数据流需要进行路由转发处理。
- 在转发之前，交由出站访问控制进行过滤控制操作。

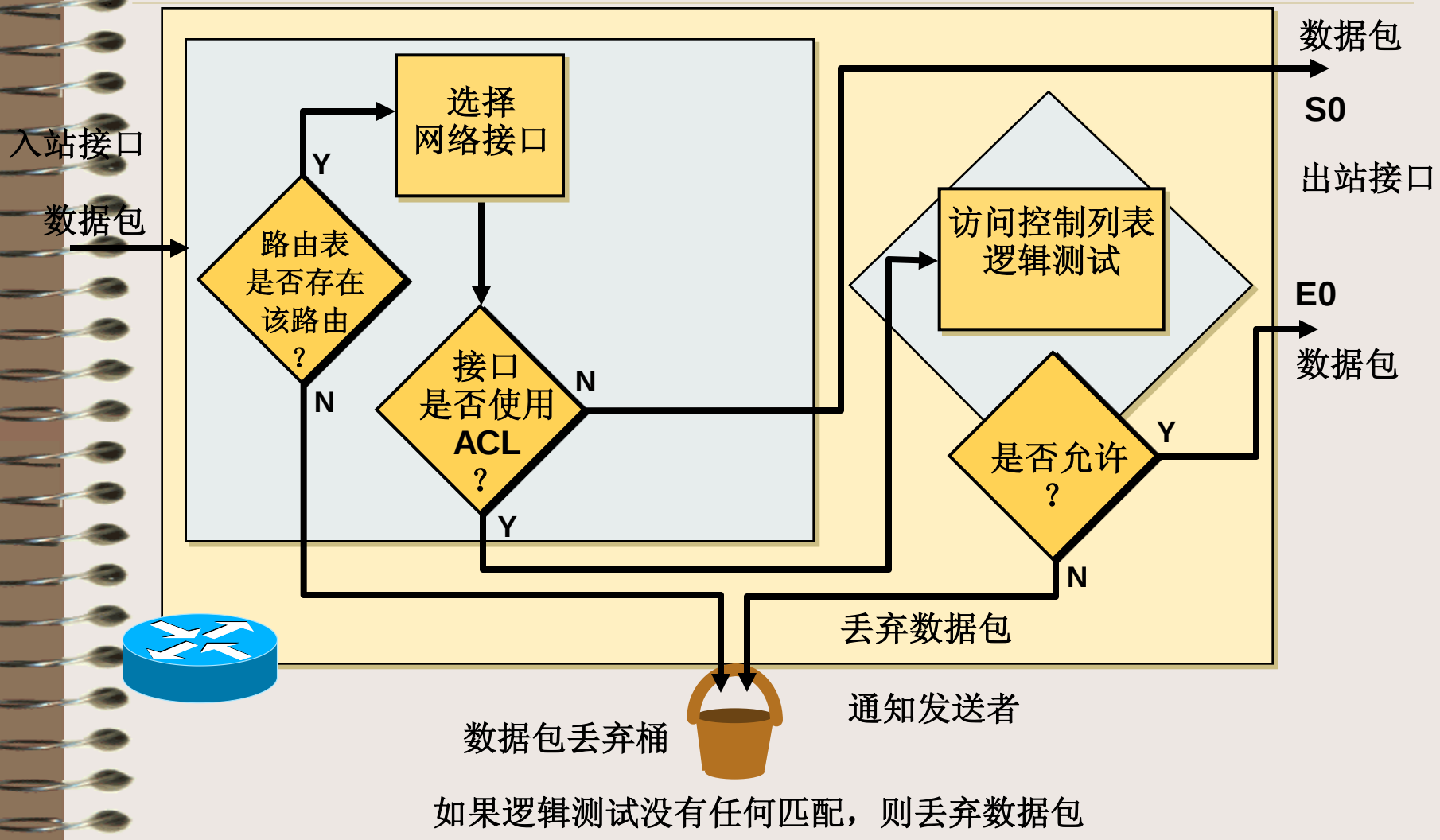
出站访问控制操作过程（续）



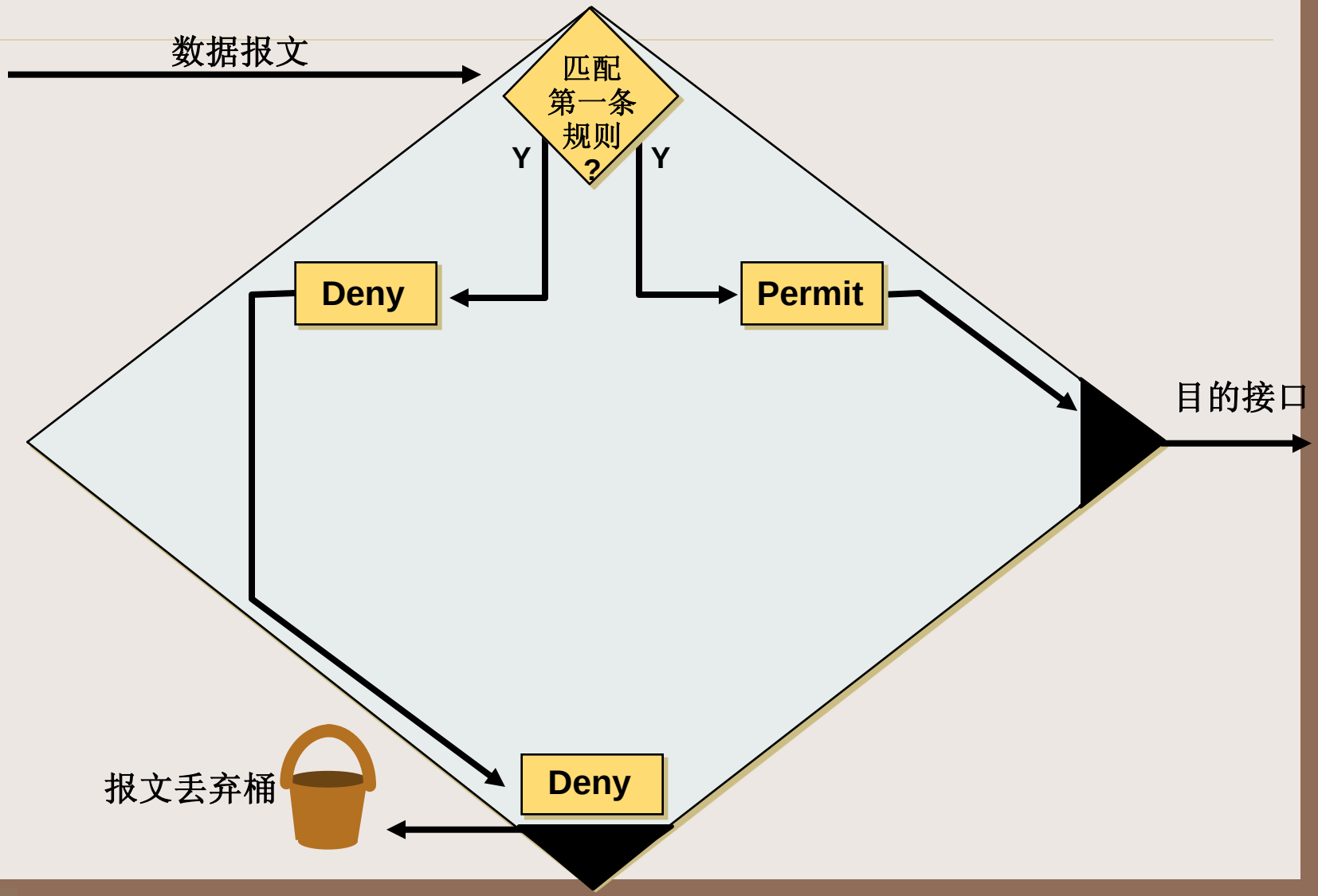
出站访问控制操作过程（续）



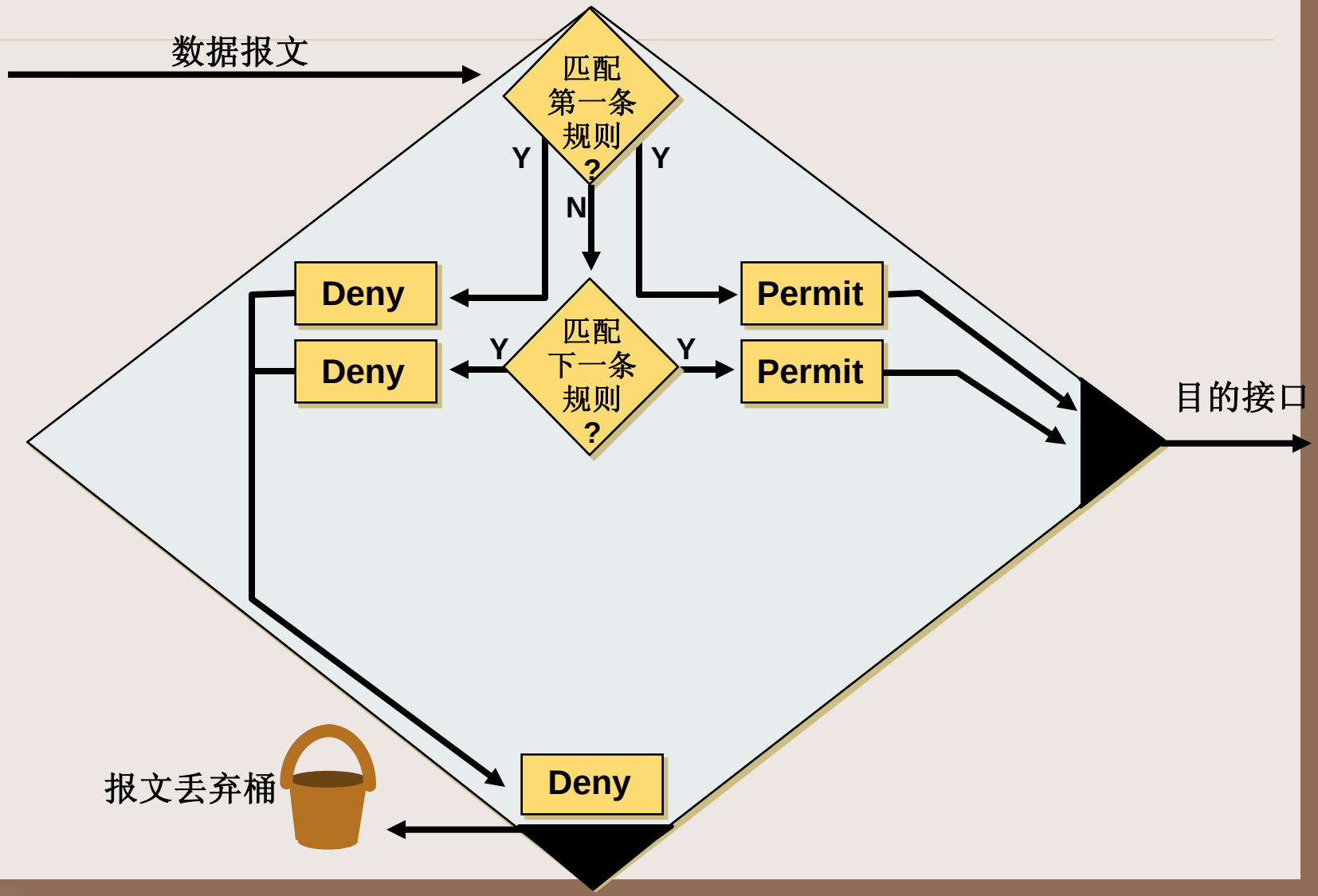
出站访问控制操作过程（续）



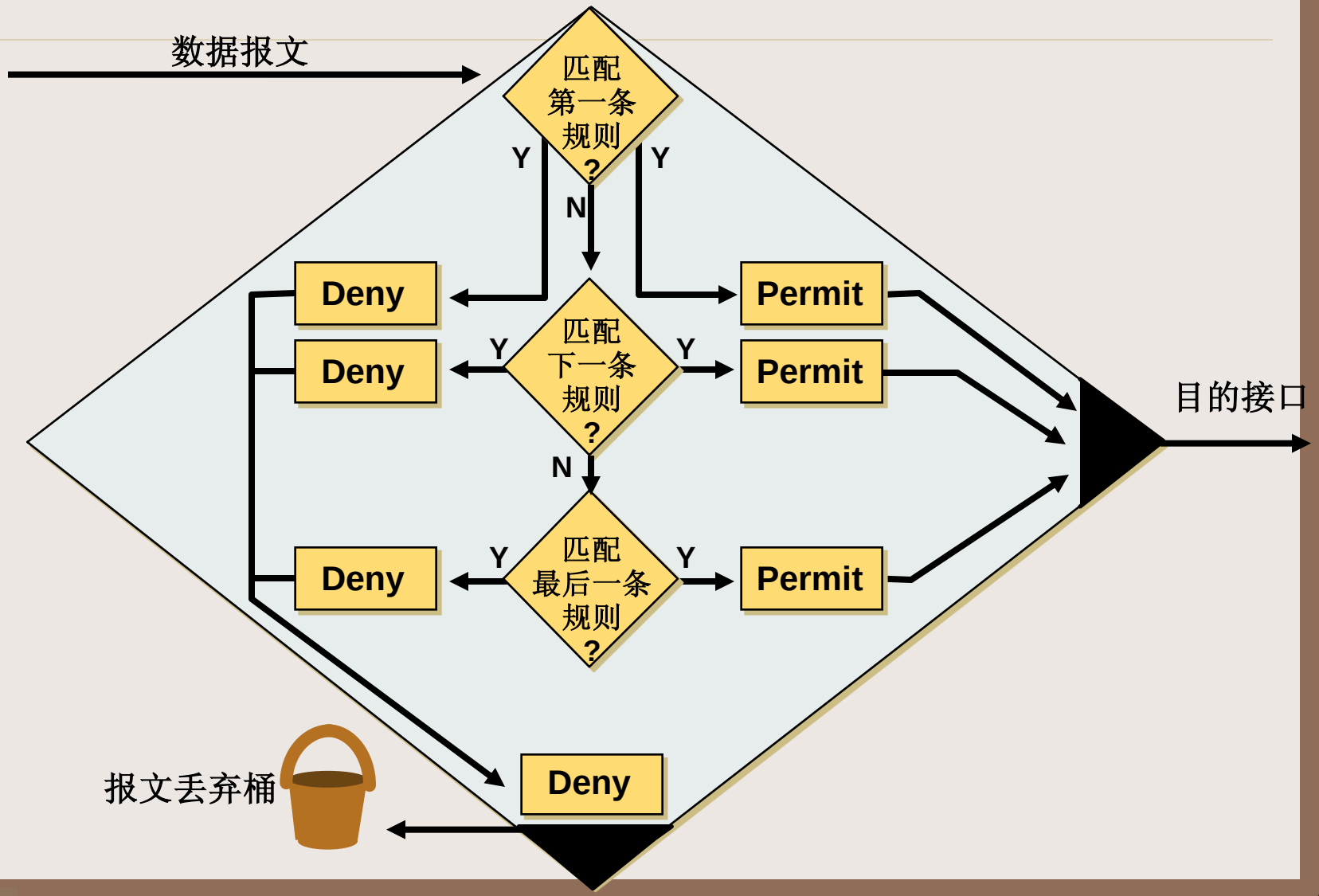
ACL的逻辑测试过程



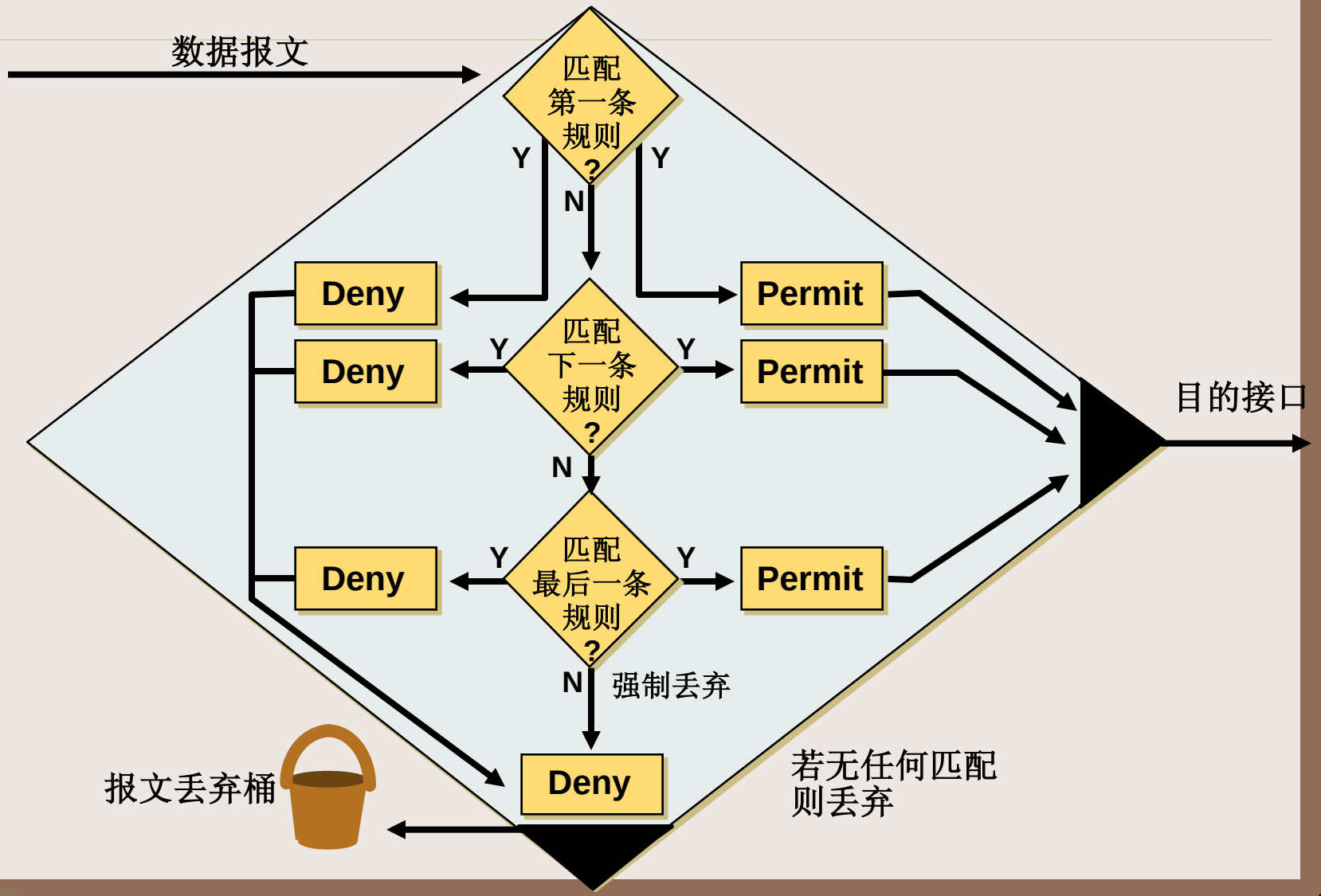
ACL的逻辑测试过程


数据报文
匹配
第一条
规则
?
Y
N
Y
Deny
Permit
匹配
下一条
规则
?
Y
Y
Deny
Permit
目的接口
报文丢弃桶
Deny

ACL的逻辑测试过程


数据报文
匹配第一条规则?
Y
N
Y
Deny
Permit
匹配下一条规则?
Y
Y
Deny
Permit
N
匹配最后一条规则?
Y
Y
Deny
Permit
目的接口
Deny
报文丢弃桶

ACL的逻辑测试过程

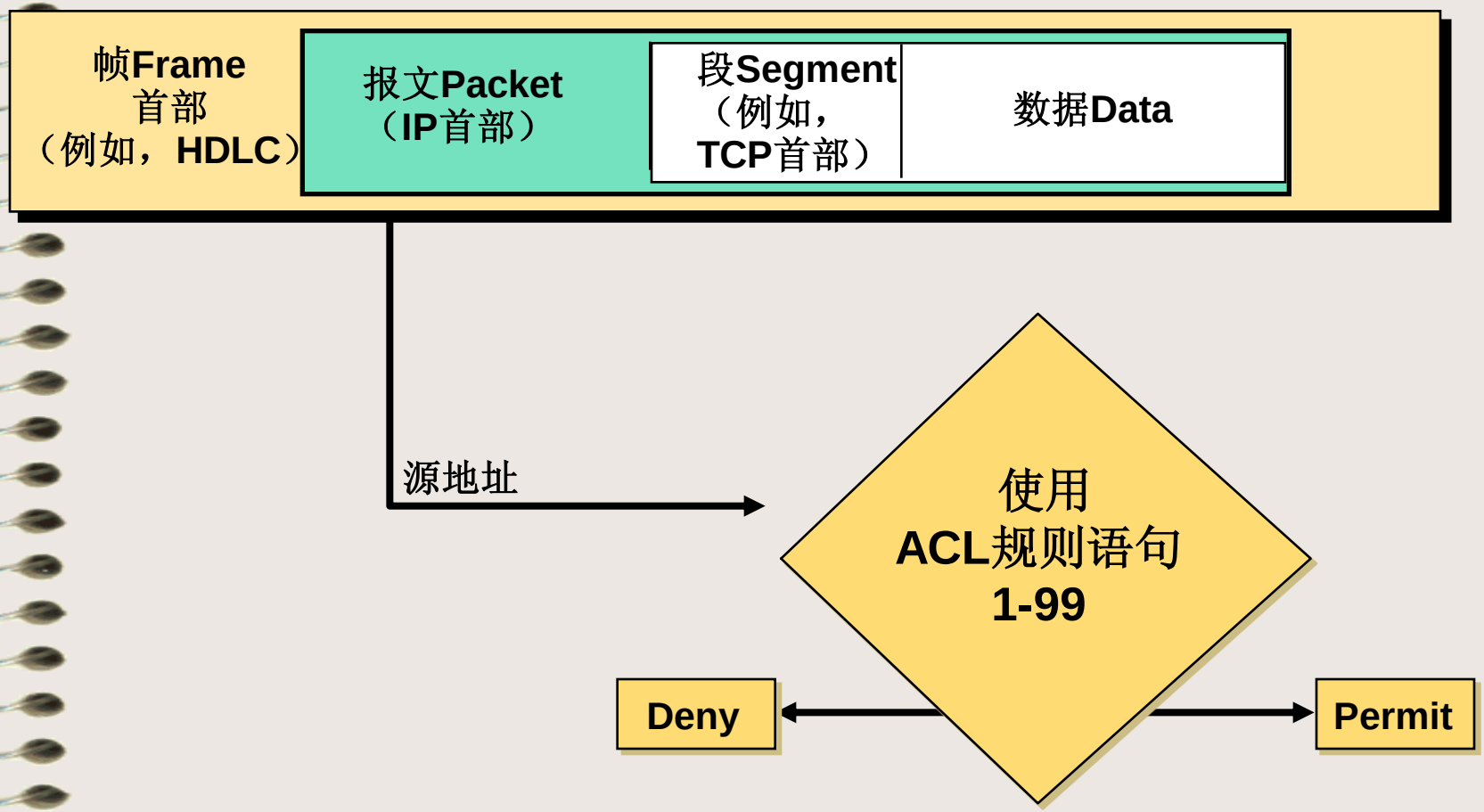

数据报文
匹配第一条规则?
Y
N
Y
Deny
Permit
匹配下一条规则?
Y
Y
Deny
Permit
N
匹配最后一条规则?
Y
Y
Deny
Permit
N
强制丢弃
Deny
报文丢弃桶
若无任何匹配则丢弃
目的接口

ACL分类

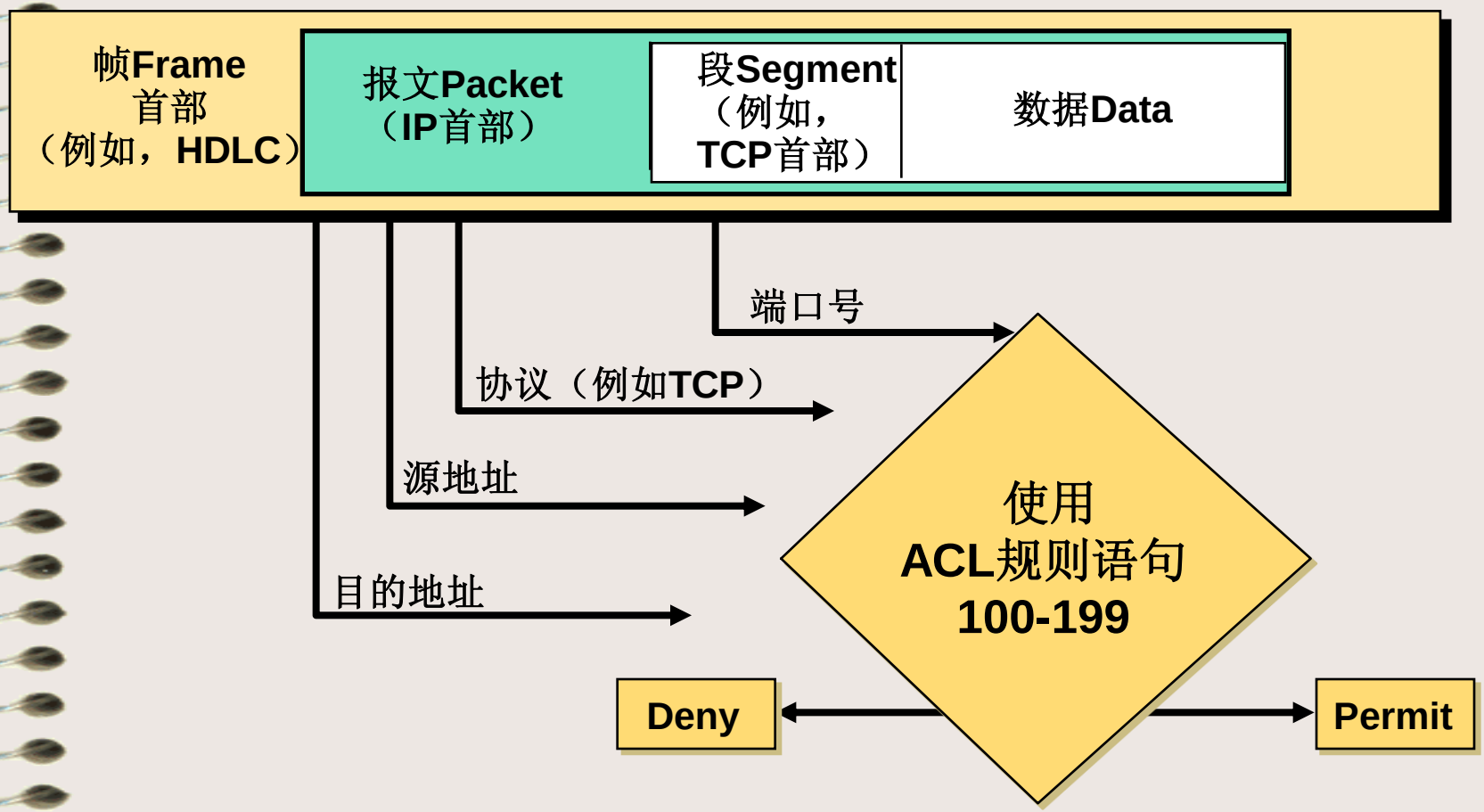
ACL类型		范围/标识
IP	Standard Extended Named	1-99 100-199, 1300-1999, 2000-2699 Name (Cisco IOS 11.2 and later)
IPX	Standard Extended SAP filters Named	800-899 900-999 1000-1099 Name (Cisco IOS 11.2. F and later)

- 标准IP ACL（1到99）根据IP报文的源地址测试
- 扩展IP ACL（100到199）可以测试IP报文的源、目的地址、协议、端口号

标准ACL


帧Frame
首部
（例如，HDLC）
报文Packet
（IP首部）
段Segment
（例如，
TCP首部）
数据Data
源地址
使用
ACL规则语句
1-99
Deny
Permit

扩展ACL


帧Frame
首部
（例如，HDLC）
报文Packet
（IP首部）
段Segment
（例如，
TCP首部）
数据Data
端口号
协议（例如TCP）
源地址
目的地址
使用
ACL规则语句
100-199
Deny
Permit

ACL配置

第一步：创建ACL

Router(config)#

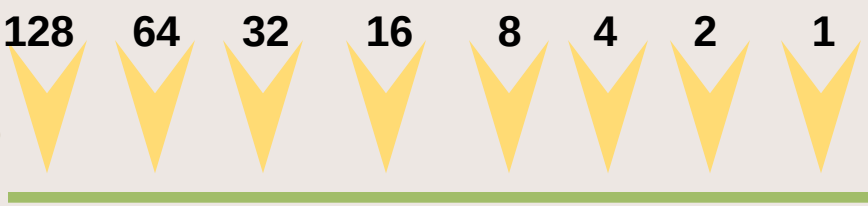
access-list *access-list-number* { permit | deny } { test conditions }

第二步：将ACL绑定到指定接口

Router(config-if)#

{ *protocol* } access-group *access-list-number {in | out}*

翻转掩码



									示例
0	0	0	0	0	0	0	0	=	check all address bits (match all)
0	0	1	1	1	1	1	1	=	ignore last 6 address bits
0	0	0	0	1	1	1	1	=	ignore last 4 address bits
1	1	1	1	1	1	0	0	=	check last 2 address bits
1	1	1	1	1	1	1	1	=	do not check address (ignore bits in octet)

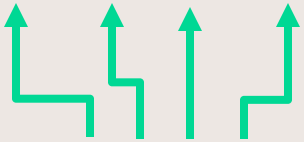
- 0代表检查对应地址位的值
- 1代表忽略对应地址位的值

host关键字

测试条件：检查所有的地址位（match all）

一个IP host关键字的示例如下：

172.30.16.29



反转掩码：　0.0.0.0

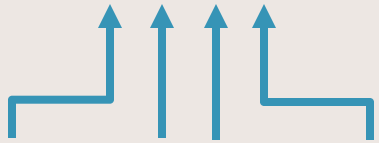
- 例如：172.30.16.29 0.0.0.0 表示检查所有的地址位
- 可以使用关键字host将上语句简写为：*host 172.30.16.29*

any关键字

测试条件：忽略所有的地址位（match any）

任何IP地址

0.0.0.0



反转掩码：255.255.255.255

- 接受任何地址： 0.0.0.0 255.255.255.255
- 可以使用关键字any将上语句简写为：*any*

通配符掩码和IP子网的对应

Check for IP subnets 172.30.16.0/24 to 172.30.31.0/24

Address and wildcard mask:

172.30.16.0 0.0.15.255

Network .host

172.30.16.0

				0	**0**	**0**	**1**	**0**	**0**	**0**	**0**
Wildcard mask:				0	0	0	0	1	1	1	1
				|<---- match ---->|<----- don't care ----->|							
0	**0**	**0**	**1**	**0**	**0**	**0**	**0**			**=**	**16**
0	**0**	**0**	**1**	**0**	**0**	**0**	**1**			**=**	**17**
0	**0**	**0**	**1**	**0**	**0**	**1**	**0**			**=**	**18**
						:					
0	**0**	**0**	**1**	**1**	**1**	**1**	**1**			**=**	**31**

标准ACL的配置

Router(config)#

access-list *access-list-number* {permit|deny} *source* [*mask*]

- 为访问控制列表增加一条测试语句
- 标准IP ACL的参数*access-list-number* 取值范围从1到99
- 缺省反转掩码 = 0.0.0.0
- “no access-list *access-list-number*” 命令删除指定号码的ACL

标准ACL的配置

Router(config)#

access-list *access-list-number* {permit|deny} *source* [*mask*]

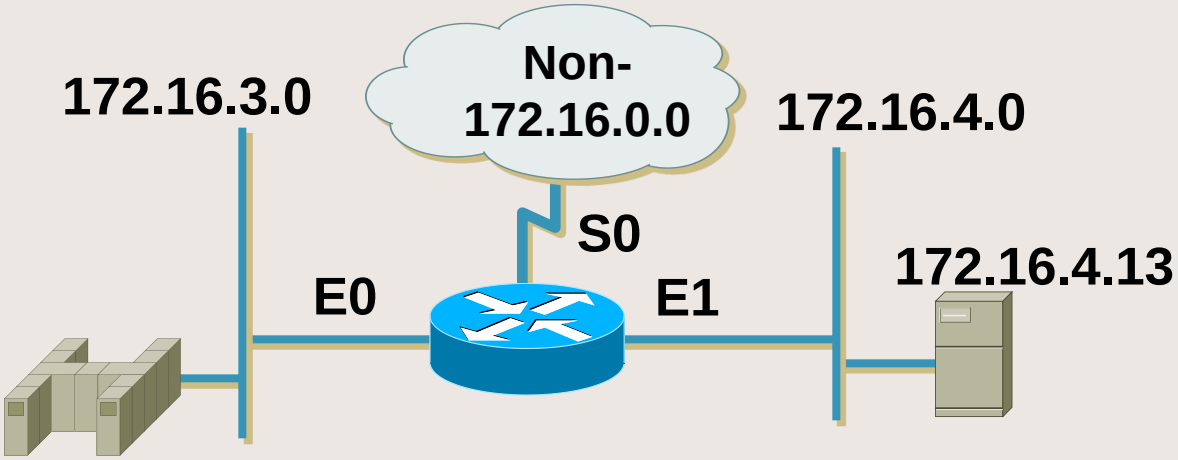
- 为访问控制列表增加一条测试语句
- 标准IP ACL的参数*access-list-number* 取值范围从1到99
- 缺省反转掩码 = 0.0.0.0
- “no access-list *access-list-number*” 命令删除指定号码的ACL

Router(config-if)#

ip access-group *access-list-number* { in | out }

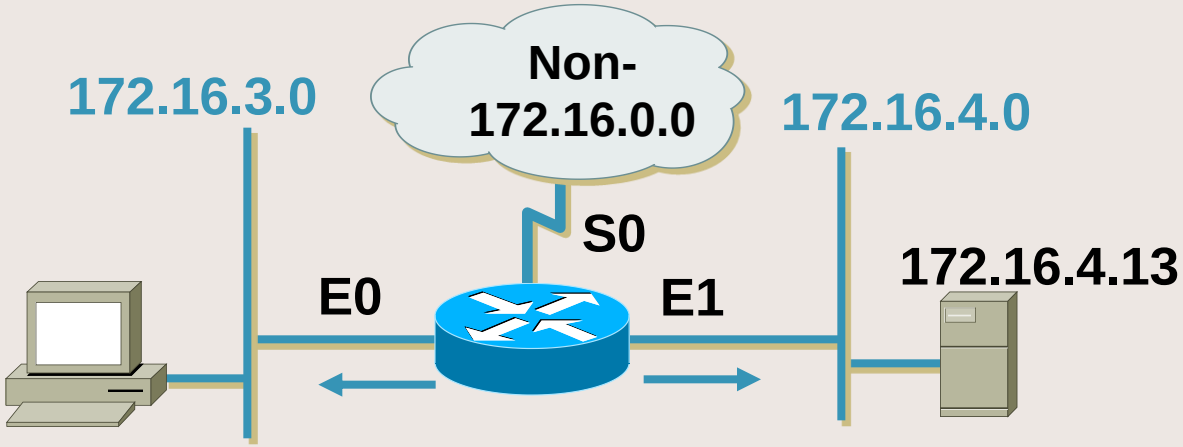
- 在特定接口上启用ACL
- 设置测试为入站（in）控制还是出站（out）控制
- 缺省为出站（out）控制
- “no ip access-group *access-list-number*” 命令在特定接口禁用ACL

标准ACL例1



access-list 1 permit 172.16.0.0 0.0.255.255
(implicit deny all - not visible in the list)
(access-list 1 deny 0.0.0.0 255.255.255.255)

标准ACL例1

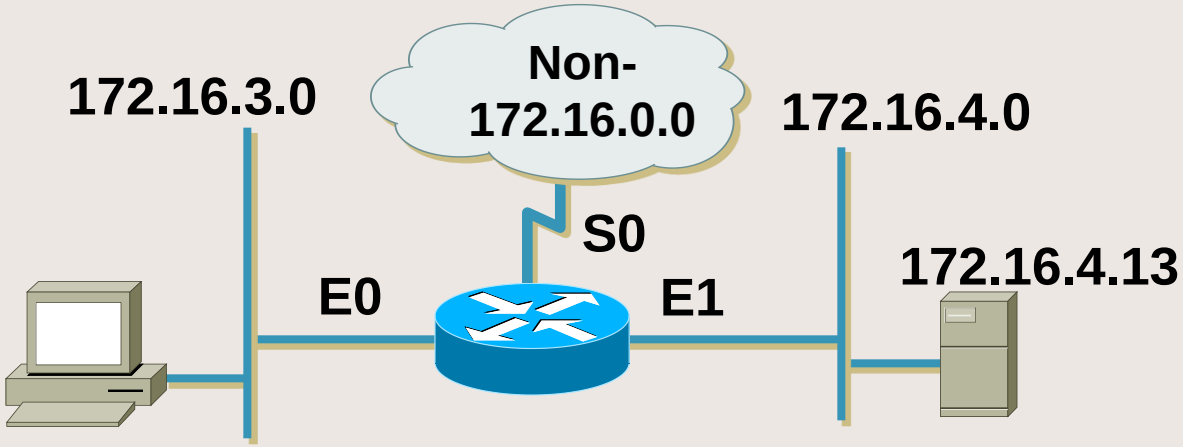


access-list 1 permit 172.16.0.0 0.0.255.255
(implicit deny all - not visible in the list)
(access-list 1 deny 0.0.0.0 255.255.255.255)

interface ethernet 0
ip access-group 1 out
interface ethernet 1
ip access-group 1 out

只允许本机所在网络访问

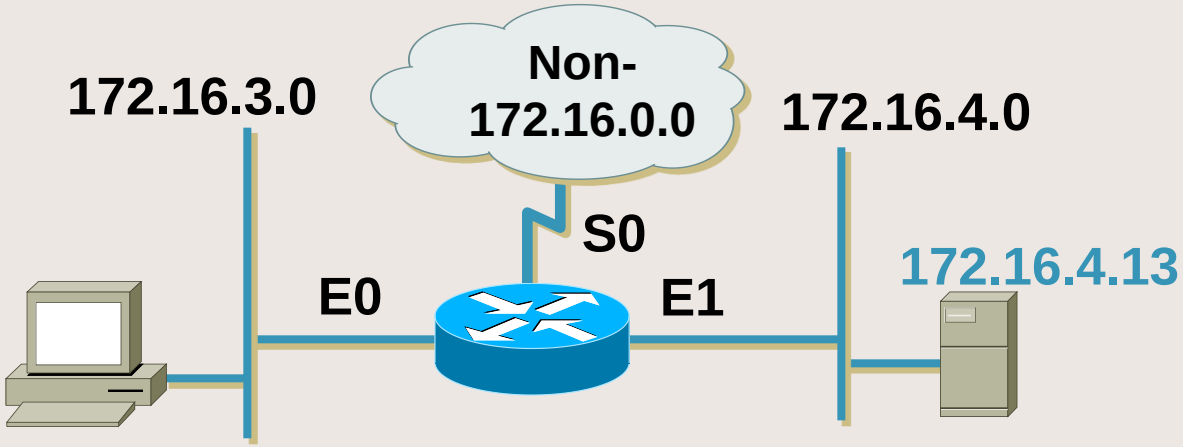
标准ACL例2




```
access-list 1 deny 172.16.4.13 0.0.0.0
```

拒绝特定主机的访问

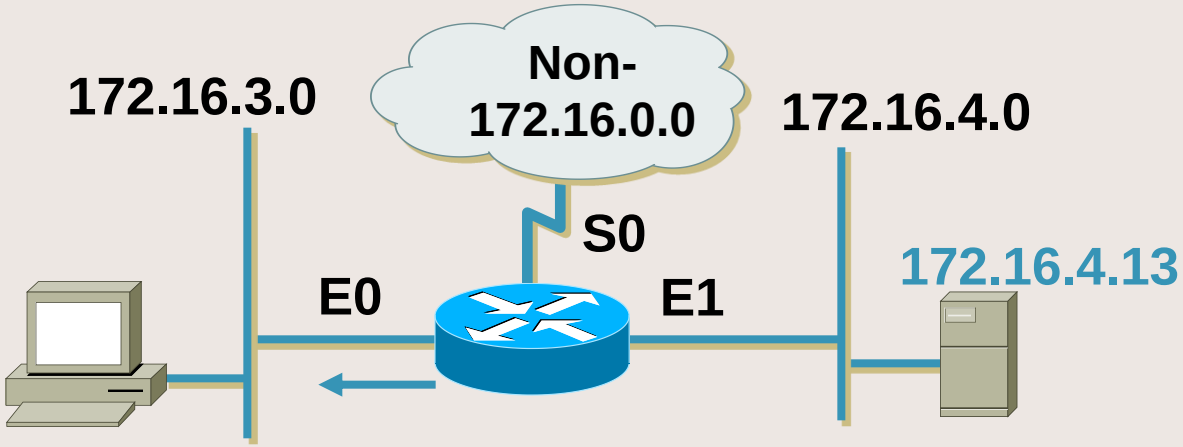
标准ACL例2



access-list 1 deny 172.16.4.13 0.0.0.0
access-list 1 permit 0.0.0.0 255.255.255.255
(implicit deny all)
(access-list 1 deny 0.0.0.0 255.255.255.255)

拒绝特定主机的访问

标准ACL例2

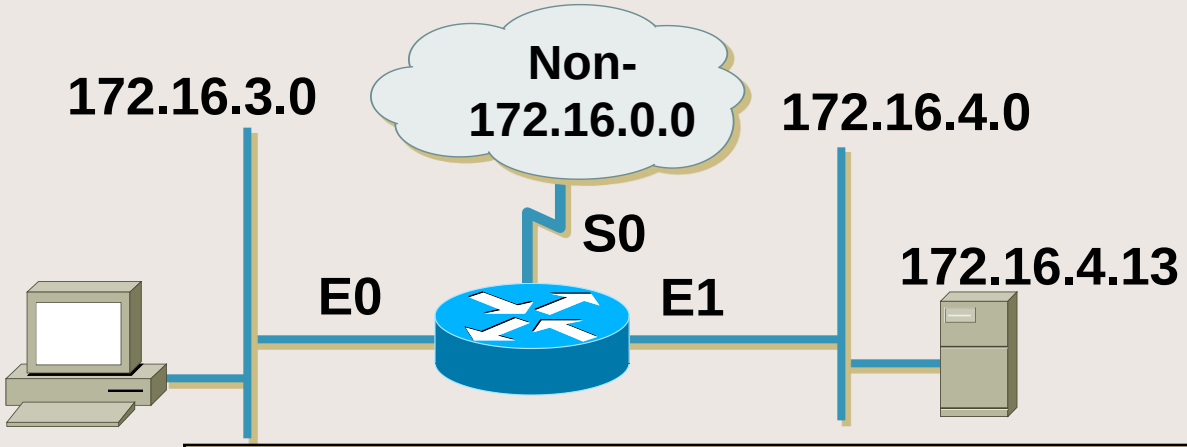



```
access-list 1 deny 172.16.4.13 0.0.0.0
access-list 1 permit 0.0.0.0  255.255.255.255
(implicit deny all)
(access-list 1 deny 0.0.0.0   255.255.255.255)

interface ethernet 0
ip access-group 1 out
```

拒绝特定主机的访问

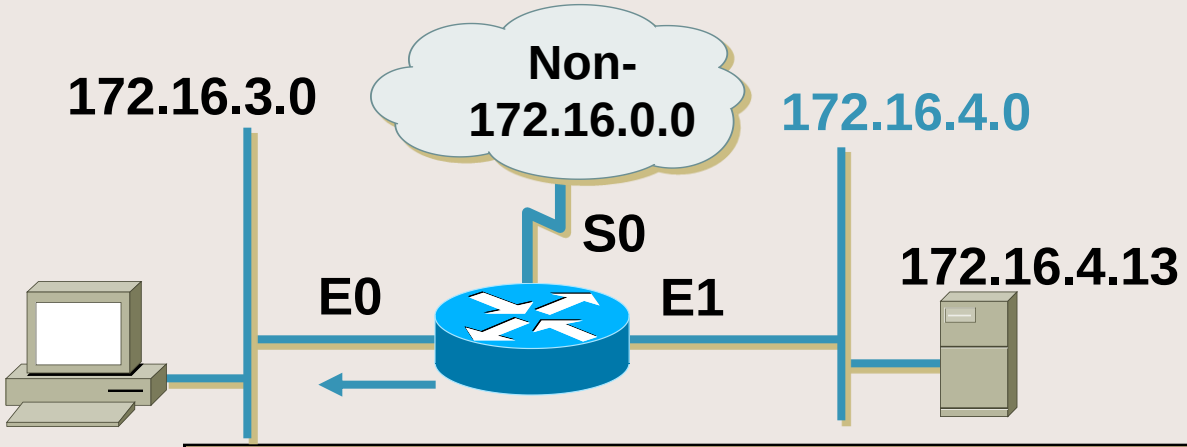
标准ACL例2



access-list 1 deny 172.16.4.0 0.0.0.255
access-list 1 permit any
(implicit deny all)
(access-list 1 deny 0.0.0.0 255.255.255.255)

拒绝特定子网的访问

标准ACL例2




```
access-list 1 deny 172.16.4.0  0.0.0.255
access-list 1 permit any
(implicit deny all)
(access-list 1 deny 0.0.0.0   255.255.255.255)

interface ethernet 0
ip access-group 1 out
```

拒绝特定子网的访问

扩展ACL的配置

Router(config)#

access-list ***access-list-number*** **{ permit | deny }** ***protocol source source-wildcard [operator port] destination destination-wildcard*** **[** ***operator port*** **] [established] [log]**

为扩展IP ACL增加一条测试语句
Eq-等于 lt-小于 gt-大于 neq-不等于
Establisted 用与TCP入站访问控制列表，意义在于允许TCP报文在建立了一个确定的连接后，后继报文可以通过
Log 向控制台发送一条规则匹配的日志信息

扩展ACL的配置

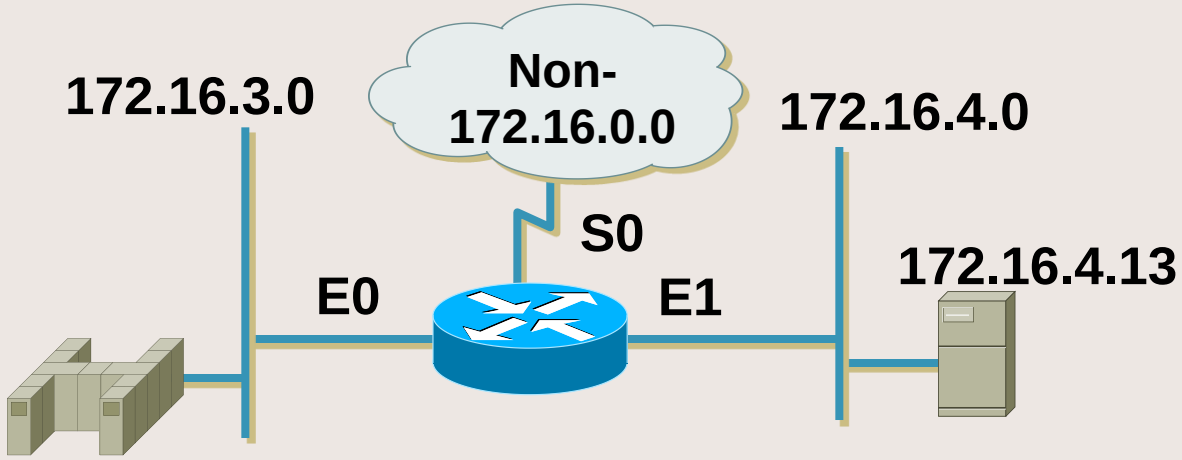
Router(config)# access-list *access-list-number*
{ permit | deny } *protocol source source-wildcard [operator port]*
***destination destination-wildcard* [*operator port*] [established] [log]**

为扩展IP ACL增加一条测试语句

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

在特定接口上启用扩展ACL

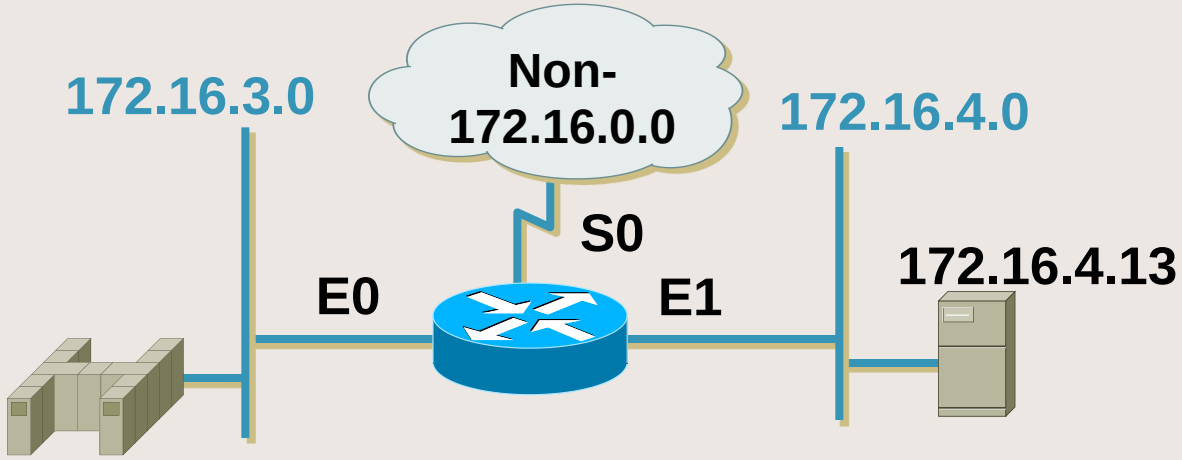
扩展ACL例1




```
access-list 101 deny tcp 172.16.4.0 0.0.0.255 172.16.3.0 0.0.0.255 eq 21
access-list 101 deny tcp 172.16.4.0 0.0.0.255 172.16.3.0 0.0.0.255 eq 20
```

- 禁止子网172.16.3.0中任何主机访问172.16.4.13上的ftp服务
- 允许其他任何服务

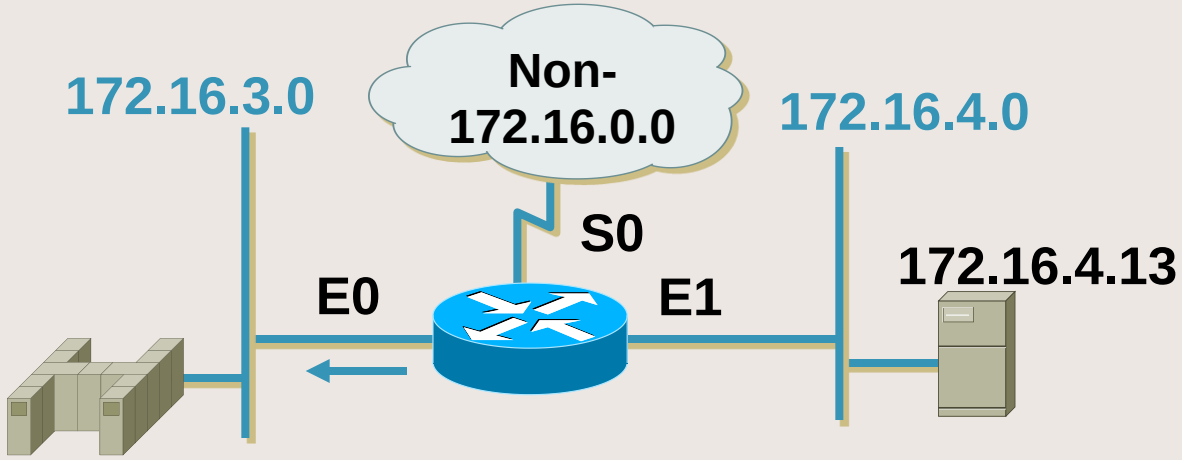
扩展ACL例1



access-list 101 deny tcp 172.16.4.0 0.0.0.255 172.16.3.0 0.0.0.255 eq 21
access-list 101 deny tcp 172.16.4.0 0.0.0.255 172.16.3.0 0.0.0.255 eq 20
access-list 101 permit ip any any
(implicit deny all)
(access-list 101 deny ip 0.0.0.0 255.255.255.255 0.0.0.0 255.255.255.255)

- 禁止子网**172.16.3.0**中任何主机访问**172.16.4.13**上的**ftp**服务
- 允许其他任何服务

扩展ACL例1

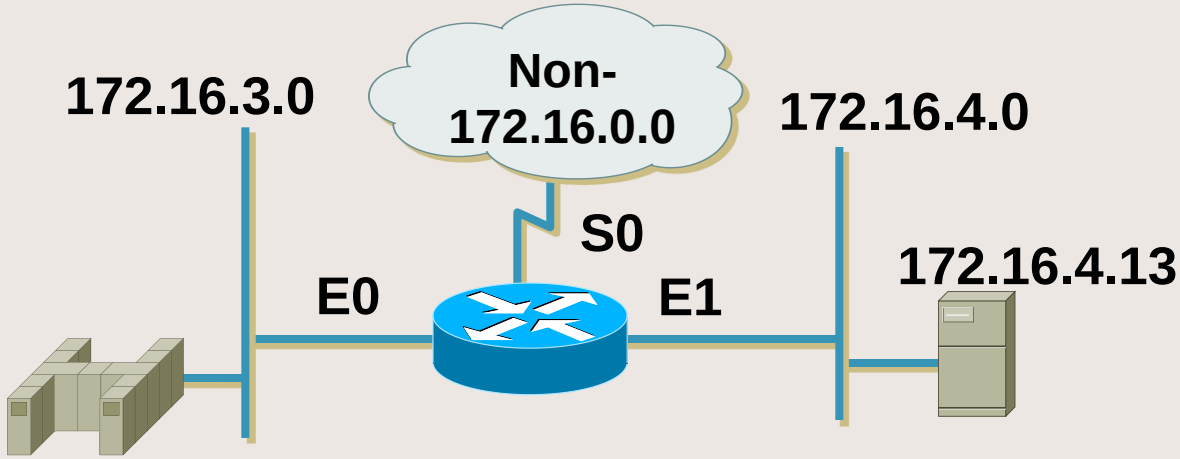



```
access-list 101 deny tcp 172.16.4.0 0.0.0.255 172.16.3.0 0.0.0.255 eq 21
access-list 101 deny tcp 172.16.4.0 0.0.0.255 172.16.3.0 0.0.0.255 eq 20
access-list 101 permit ip any any
(implicit deny all)
(access-list 101 deny ip 0.0.0.0 255.255.255.255 0.0.0.0 255.255.255.255)

interface ethernet 0
ip access-group 101 out
```

- 禁止子网172.16.3.0中任何主机访问172.16.4.13上的ftp服务
- 允许其他任何服务

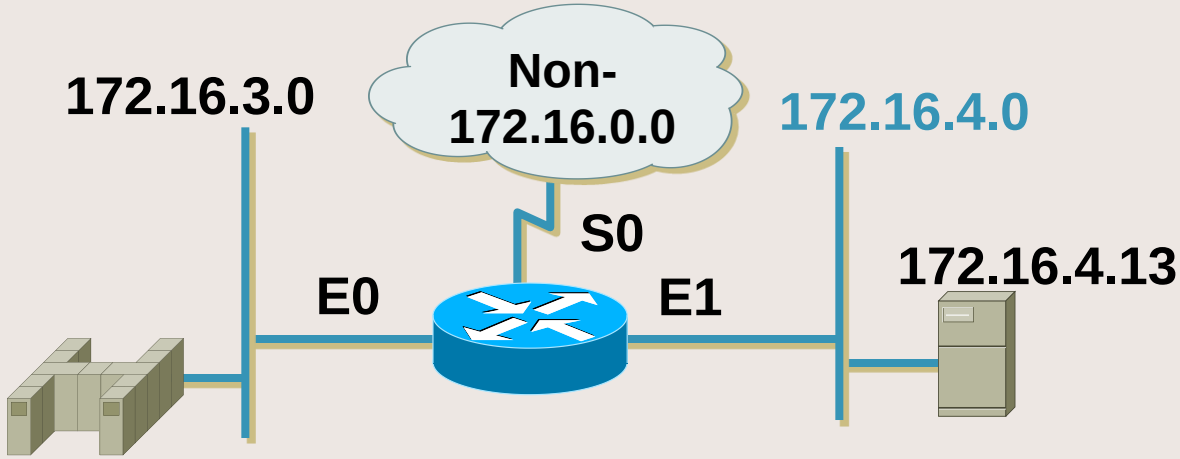
扩展ACL例2




```
access-list 101 deny tcp 172.16.4.0  0.0.0.255  any eq 23
```

- 禁止172.16.4.0网段的主机远程登录（telnet）到172.16.3.0网段的任何机器
- 允许其他任何数据通过

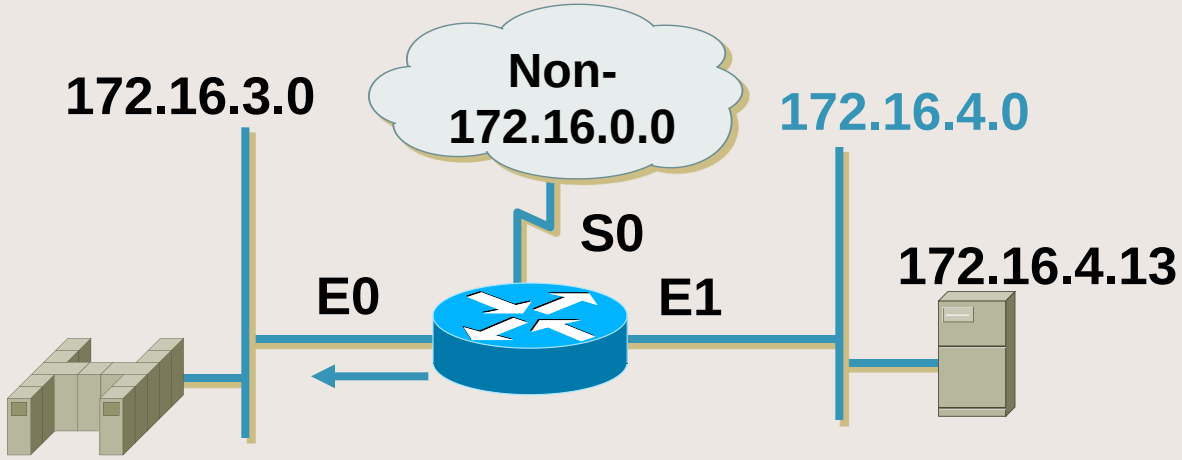
扩展ACL例2




```
access-list 101 deny tcp 172.16.4.0  0.0.0.255  any eq 23
access-list 101 permit ip any any
(implicit deny all)
```

- 禁止172.16.4.0网段的主机远程登录（telnet）到172.16.3.0网段的任何机器
- 允许其他任何数据通过

扩展ACL例2




```
access-list 101 deny tcp 172.16.4.0  0.0.0.255  any eq 23
access-list 101 permit ip any any
(implicit deny all)

interface ethernet 0
ip access-group 101 out
```

- 禁止172.16.4.0网段的主机远程登录（telnet）到172.16.3.0网段的任何机器
- 允许其他任何数据通过

命名（Named）ACL的配置

- **Cisco IOS Release 11.2以后的新增特性**

```
Router(config)#
 ip access-list { standard | extended } name
```

- 字符串名称必须唯一

命名（Named）ACL的配置

- Cisco IOS Release 11.2以后的新增特性

```
Router(config)#
 ip access-list { standard | extended } name
```

- 字符串名称必须唯一

```
Router(config {std- | ext-}nacl)#
 { permit | deny } { ip access list test conditions }
 { permit | deny } { ip access list test conditions }
 no { permit | deny } { ip access list test conditions }
```

- 配置permit和deny语句的时候不需在前面指定ACL号码
- “no”命令删除指定的命名ACL测试语句

命名（Named）ACL的配置

- Cisco IOS Release 11.2以后的新增特性

```
Router(config)# ip access-list { standard | extended } name
```

- 字符串名称必须唯一

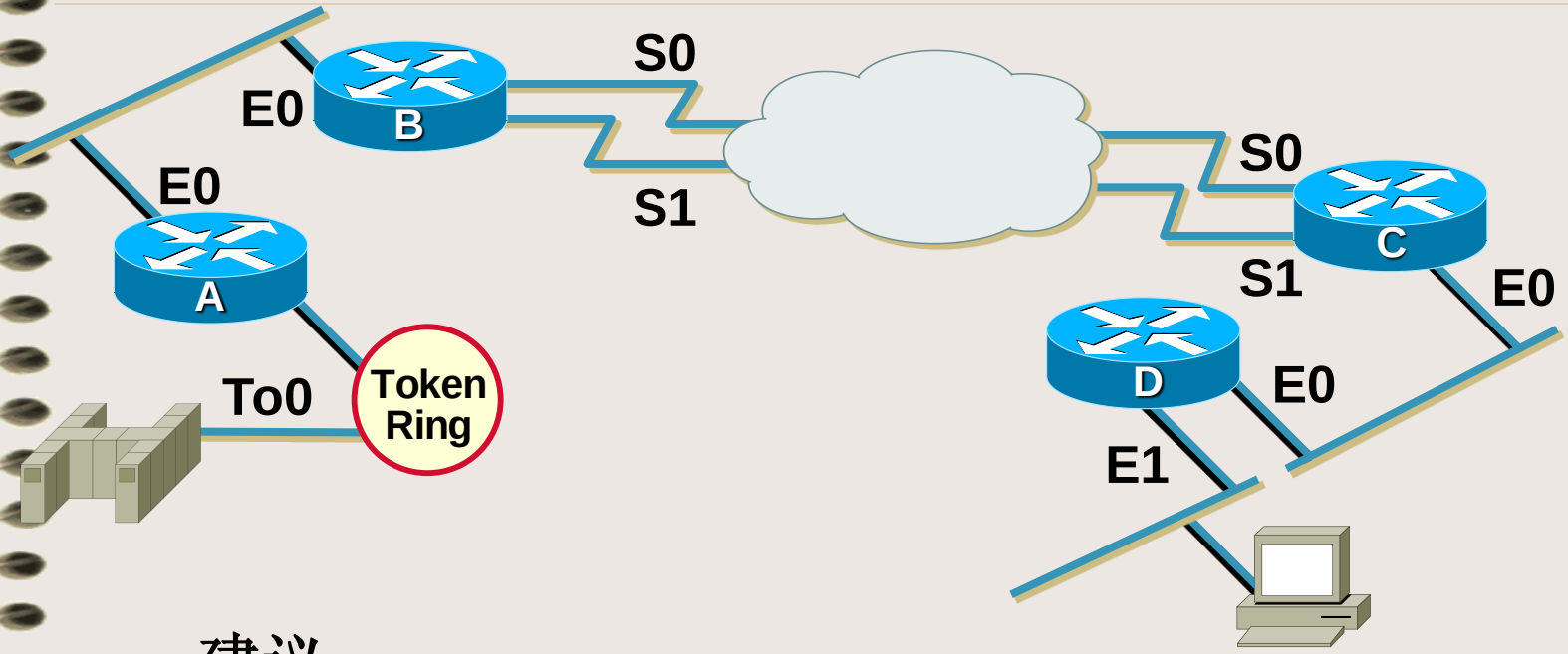
```
Router(config {std- | ext-}nacl)# { permit | deny }
{ ip access list test conditions }
{ permit | deny } { ip access list test conditions }
no { permit | deny } { ip access list test conditions }
```

- 配置permit和deny语句的时候不需在前面指定ACL号码
- “no”命令删除指定的命名ACL测试语句

```
Router(config-if)# ip access-group name { in | out }
```

- 在特定接口上启用命名ACL

设置ACL的位置



建议：

- 在靠近源地址的网络接口上设置扩展ACL
- 在靠近目的地址的网络接口上设置标准ACL

查看特定接口启用的ACL配置

```
wg_ro_a#show ip int e0
Ethernet0 is up, line protocol is up
  Internet address is 10.1.1.11/24
  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
  Proxy ARP is enabled
  Security level is default
  Split horizon is enabled
  ICMP redirects are always sent
  ICMP unreachables are always sent
  ICMP mask replies are never sent
  IP fast switching is enabled
  IP fast switching on the same interface is disabled
  IP Feature Fast switching turbo vector
  IP multicast fast switching is enabled
  IP multicast distributed fast switching is disabled
  <text ommitted>
```

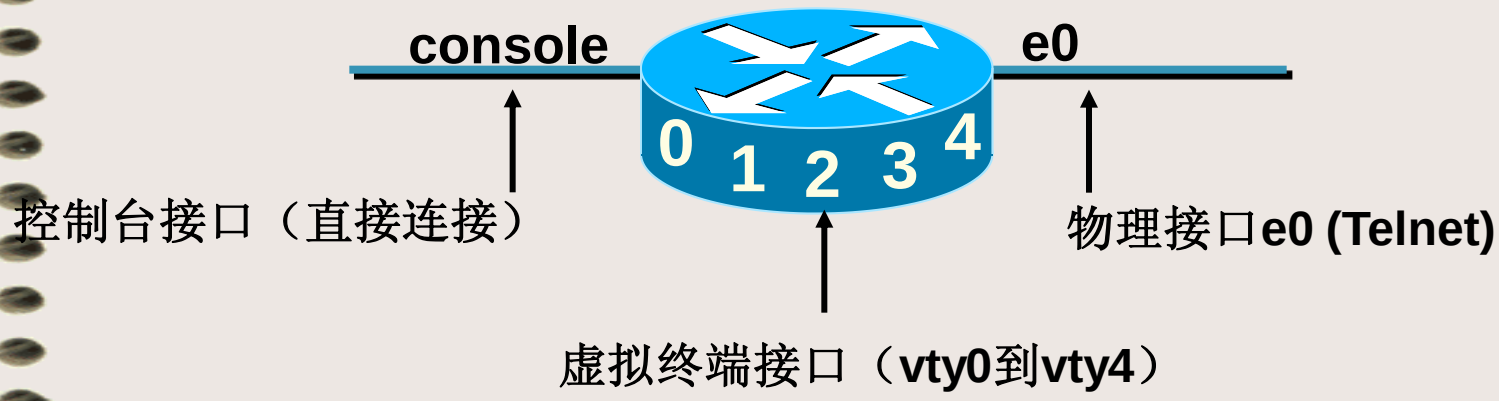
查看ACL测试语句

wg_ro_a#show {protocol} access-list {*access-list number*}

wg_ro_a#show access-lists {*access-list number*}

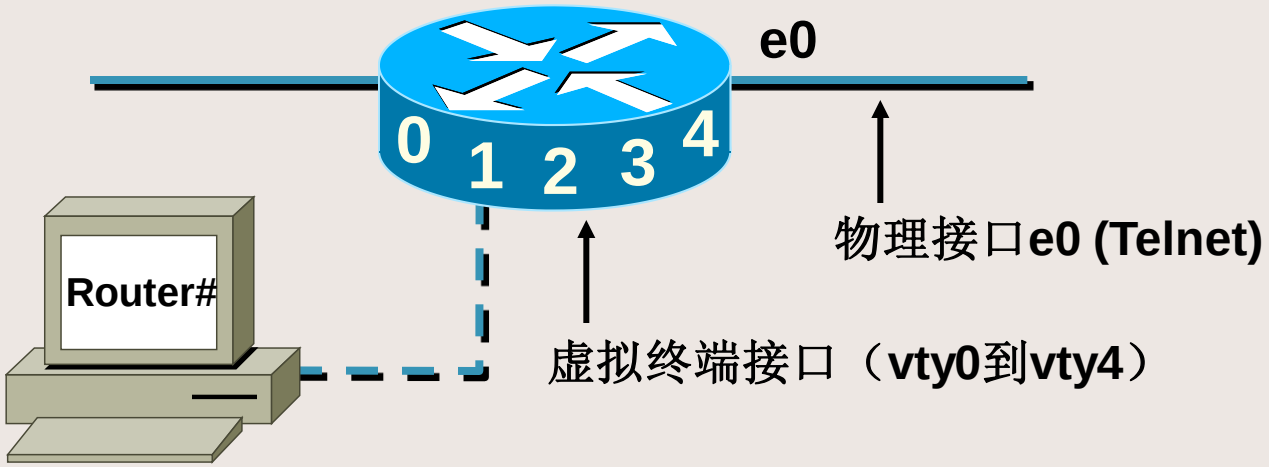
```
wg_ro_a#show access-lists
Standard IP access list 1
    permit 10.2.2.1
    permit 10.3.3.1
    permit 10.4.4.1
    permit 10.5.5.1
Extended IP access list 101
    permit tcp host 10.22.22.1 any eq telnet
    permit tcp host 10.33.33.1 any eq ftp
    permit tcp host 10.44.44.1 any eq ftp-data
```

使用ACL控制VTY的访问



- 5个虚拟终端接口（vty0到vty4）
- 对访问路由器vty的地址进行控制
- 对路由器发起的向外vty访问进行控制

如何控制VTY访问



（1）建立一个针对IP地址过滤的标准ACL；

（2）在IOS的子线路配置模式下，使用access-class命令对所有的vty绑定上述ACL。

对所有的vty端口设置同样的约束

虚拟终端Line配置命令

Router(config)#

line vty{*vty#* | *vty-range*}

进入line配置模式

Router(config-line)#

access-class *access-list-number* {in|out}

指定ACL控制入站/出站的vty访问连接

VTY访问控制示例

控制入站访问

```
access-list 12 permit 192.89.55.0 0.0.0.255
!
line vty 0 4
 access-class 12 in
```

只允许网络192.89.55.0的主机连接路由器的vty端口

访问列表配置指南(再记一次)

- 访问列表的编号指明了使用何种协议的访问列表
- 每个端口、每个方向、每条协议只能对应于一条访问列表
- 访问列表的内容决定了数据的控制顺序
- 具有严格限制条件的语句应放在访问列表所有语句的最上面
- 在访问列表的最后有一条隐含声明：deny any—每一条正确的访问列表都至少应该有一条允许语句
- 先创建访问列表，然后应用到端口上
- 访问列表不能过滤由路由器自己产生的数据

访问列表配置准则

- 访问列表中限制语句的位置是至关重要的
- 将限制条件严格的语句放在访问列表的最上面
- 使用 no access-list *number* 命令删除完整的访问列表
- 隐含声明 deny all

  在设置的访问列表中要有一句 permit any