计算机网络安全技术

- 课程代号：*40240572*
- 课程对象：本科生
- 授课教师：尹　霞
- 开课单位：计算机系网络所

访问控制的基本概念

课后作业补充知识

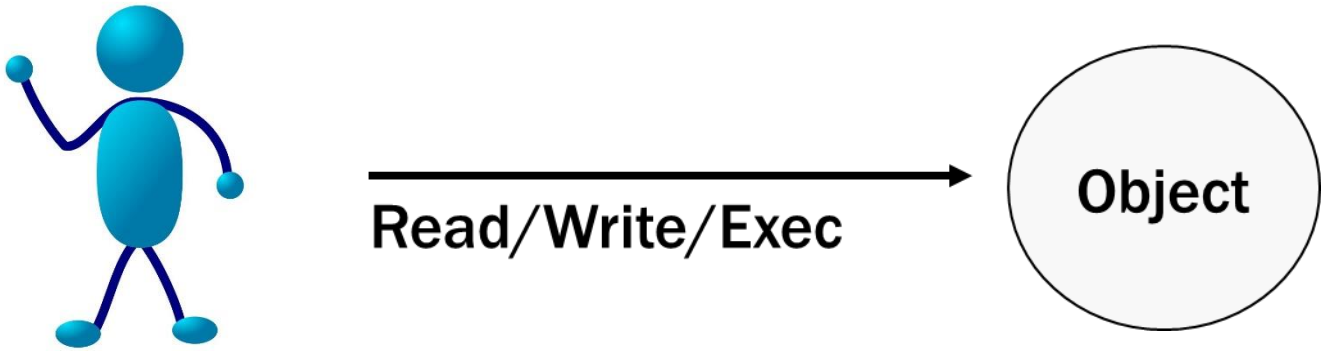
不在期末考试范围

访问控制的基本概念

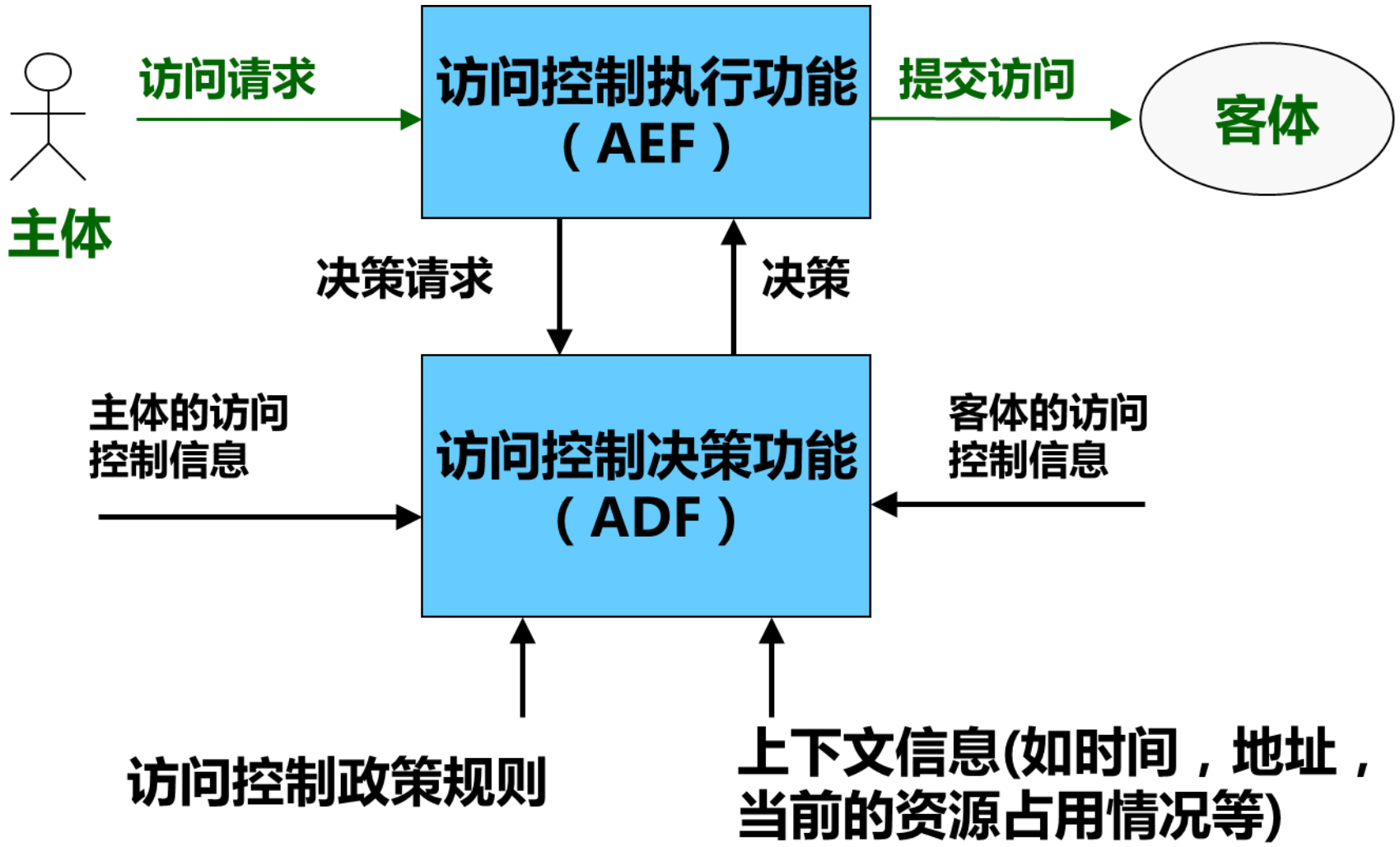
- 主体(Subject)
  - 主体是一个主动的实体，它提出对资源访问请求
  - 如用户，程序，进程等
- 客体(Object)
  - 含有被访问资源的被动实体
  - 如网络、计算机、数据库、文件、目录、程序、 外设等
- 访问(Access)
  - 对资源的使用，读、写、修改、删除等操作
  - 例如访问存储器、访问文件/目录/外设、访问数据库/网站等

访问控制的基本概念

- 访问可以被描述为一个三元组 (s, a, o)
  - 主体、发起者：**Subject、Initiator**
  - 客体、目标：**Object、Target**
  - 访问操作：**Access**



访问控制模型


访问请求
访问控制执行功能
（AEF）
提交访问
客体
主体
决策请求
决策
主体的访问
控制信息
访问控制决策功能
（ADF）
客体的访问
控制信息
访问控制政策规则
上下文信息(如时间，地址，
当前的资源占用情况等)

访问控制的基本概念

- 访问控制信息(ACI)的表示
  - 主体访问控制属性
  - 客体访问控制属性
  - 访问控制政策规则

- 授权(Authorization)
  - 怎样把访问控制属性信息分配给主体或客体
  - 如何浏览、修改、回收访问控制权限

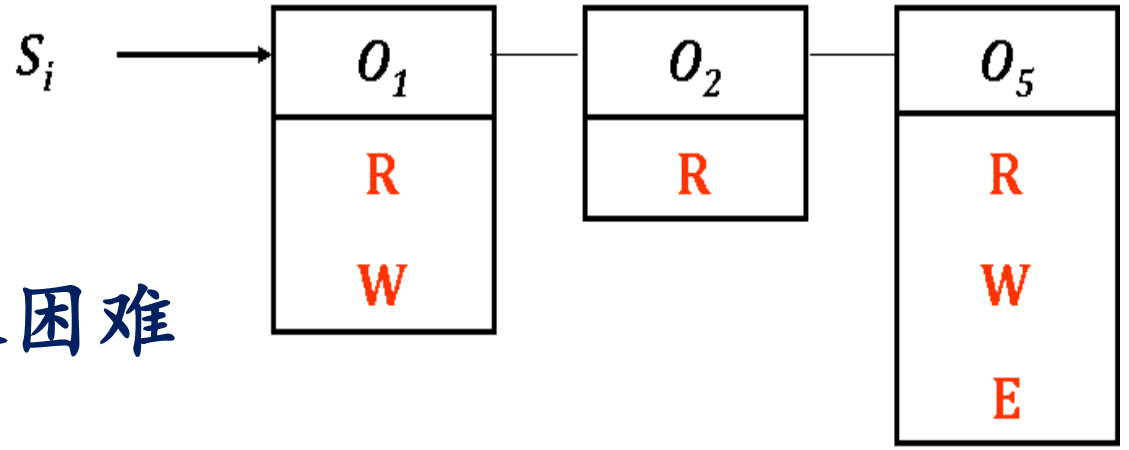
访问控制矩阵

- 按列看是客体的访问控制列表
  - **access control list**
- 按行看是主体的访问能力表
  - **capability list**

	Objects		
Subjects	O_1	O_2	O_3
S_1	Read/write		
S_2		Write	
S_3	Execute		Read

能力表(Capability List)

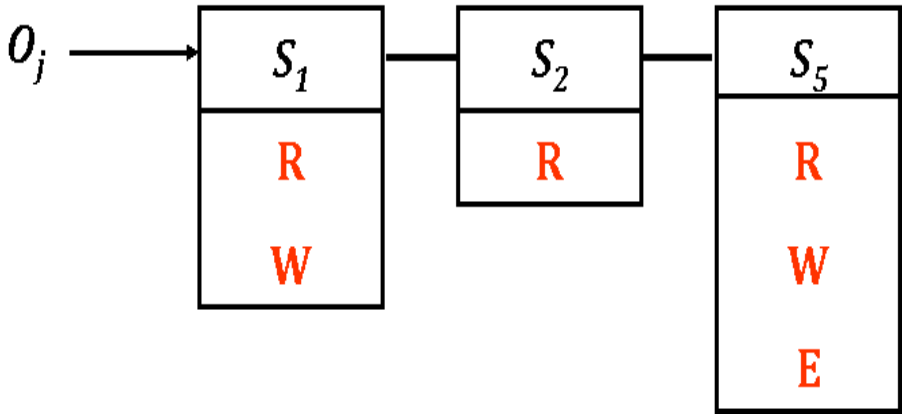
- 能力表与主体关联，规定主体所能访问的客体和权限
  - 从能力表得到一个主体所有的访问权限很容易
  - 从能力表浏览一个客体所允许的访问控制权限很困难



- 表示形式：用户Profile
  - 由于客体相当多，分类复杂，不便于授权管理（通过授权证书、属性证书等）

访问控制表(Access Control List)

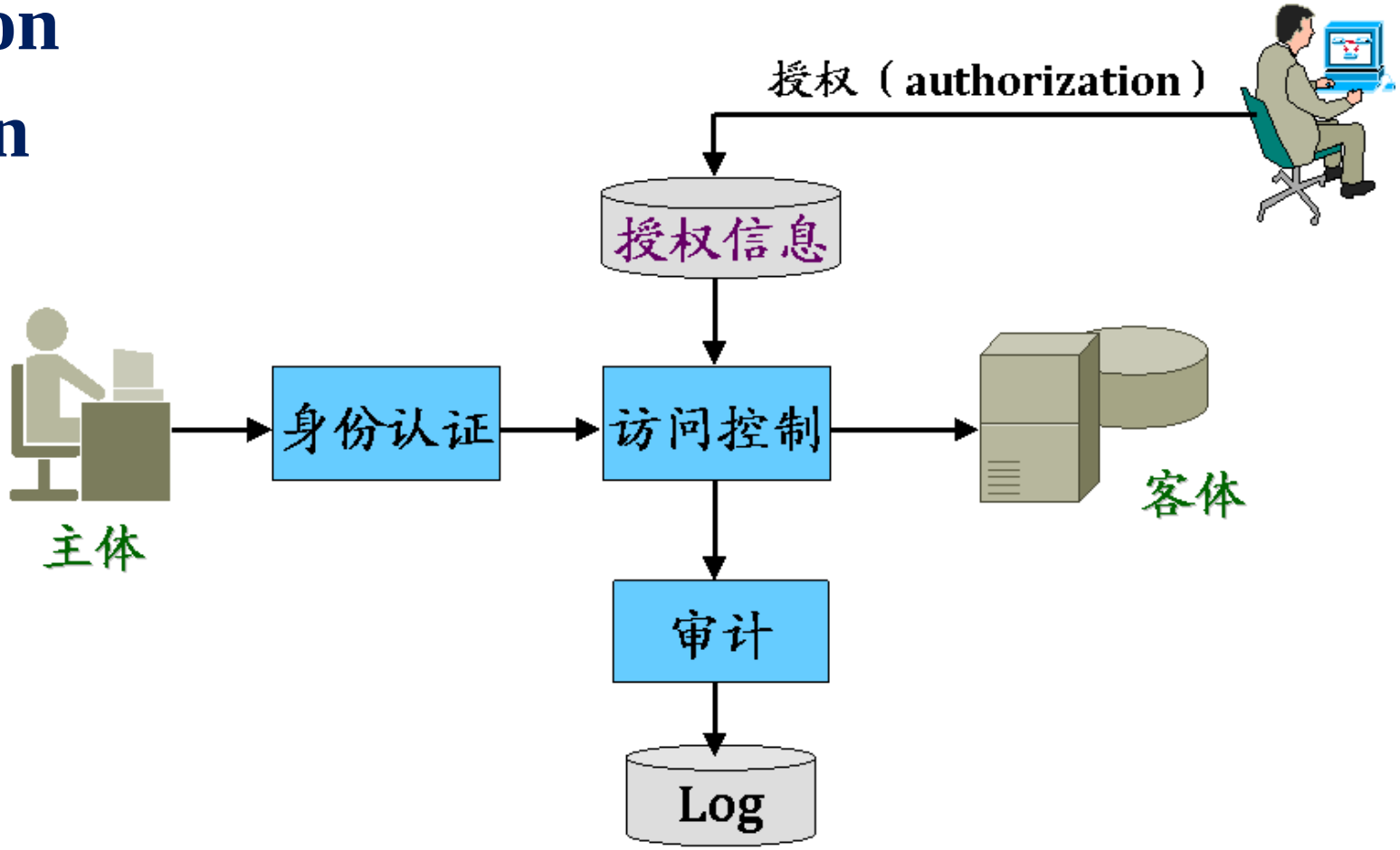
- 访问控制表与客体关联，规定能够访问它的主体和权限
  - 得到一个客体所有的访问权限很容易
  - 浏览一个主体的所有访问权限很困难



- 由于主体数量一般比客体少得多而且容易分组，授权管理相对简单

访问控制与其他安全机制的关系

- 认证、授权、审计（AAA）
  - **Authentication**
  - **Authorization**
  - **Audit**



访问控制与其他安全机制的关系

- 身份认证
  - 是访问控制的前提，保证主体身份的真实性
- 保密性
  - 限制用户对数据的访问，可以实现数据保密服务
- 完整性
  - 限制用户对数据的修改，实现数据完整性保护
- 可用性
  - 限制用户对资源的使用量，保证系统的可用性
- 安全管理相关的活动
  - 访问控制功能通常和审计、入侵检测联系在一起

访问控制列表ACL

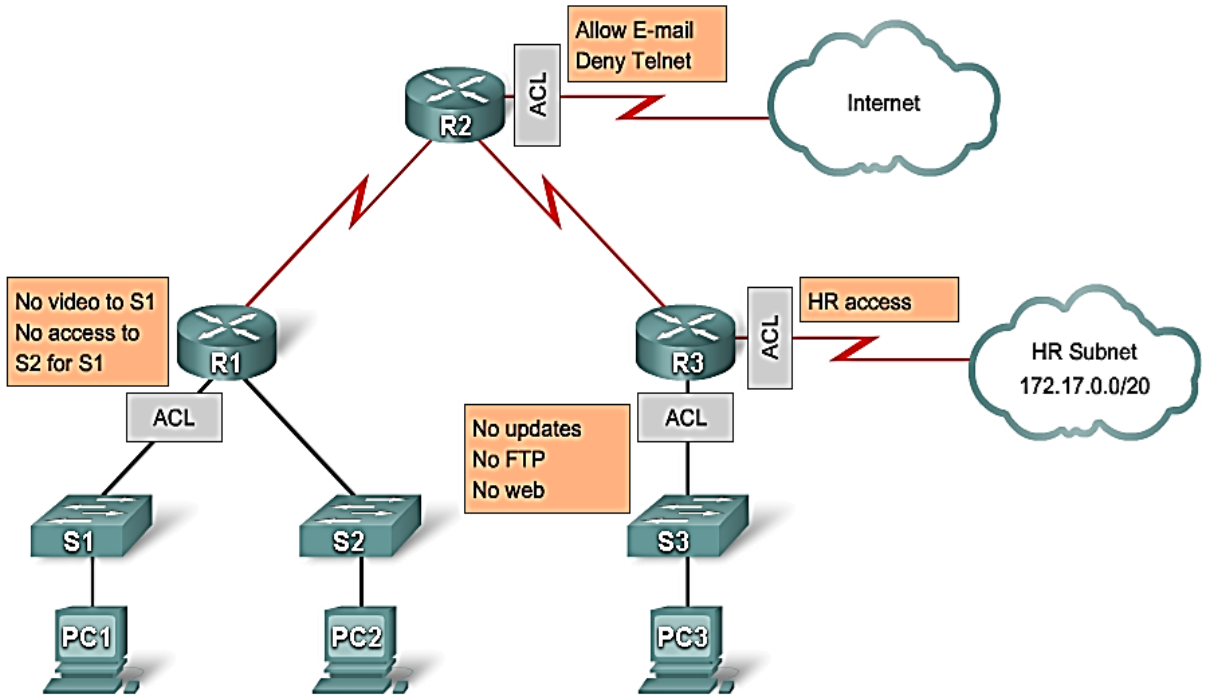
课后作业补充知识

不在期末考试范围

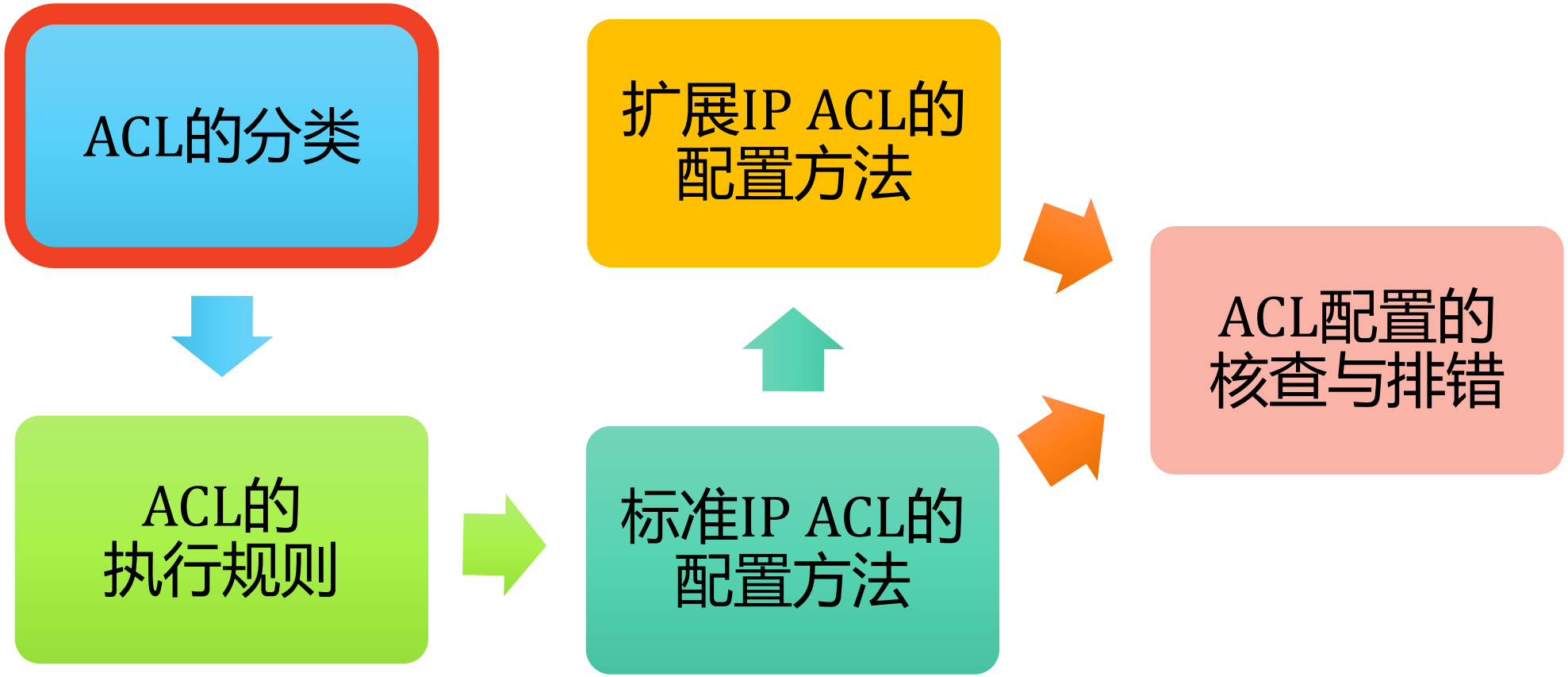
什么是访问控制列表ACL?

- ACL(Access Control List)是一组预先定义好的规则，被置于路由器的接口，根据进出数据包头中的信息，控制该数据包能否穿越路由器

- 路由器中的访问控制列表ACL是包过滤技术的具体实现，ACL可执行下列任务：
  - 限制网络流量
  - 提供基本的安全访问控制，禁止某些特征的数据包访问
  - 控制路由更新内容
  - 区分特定的数据流类型



访问控制列表ACL



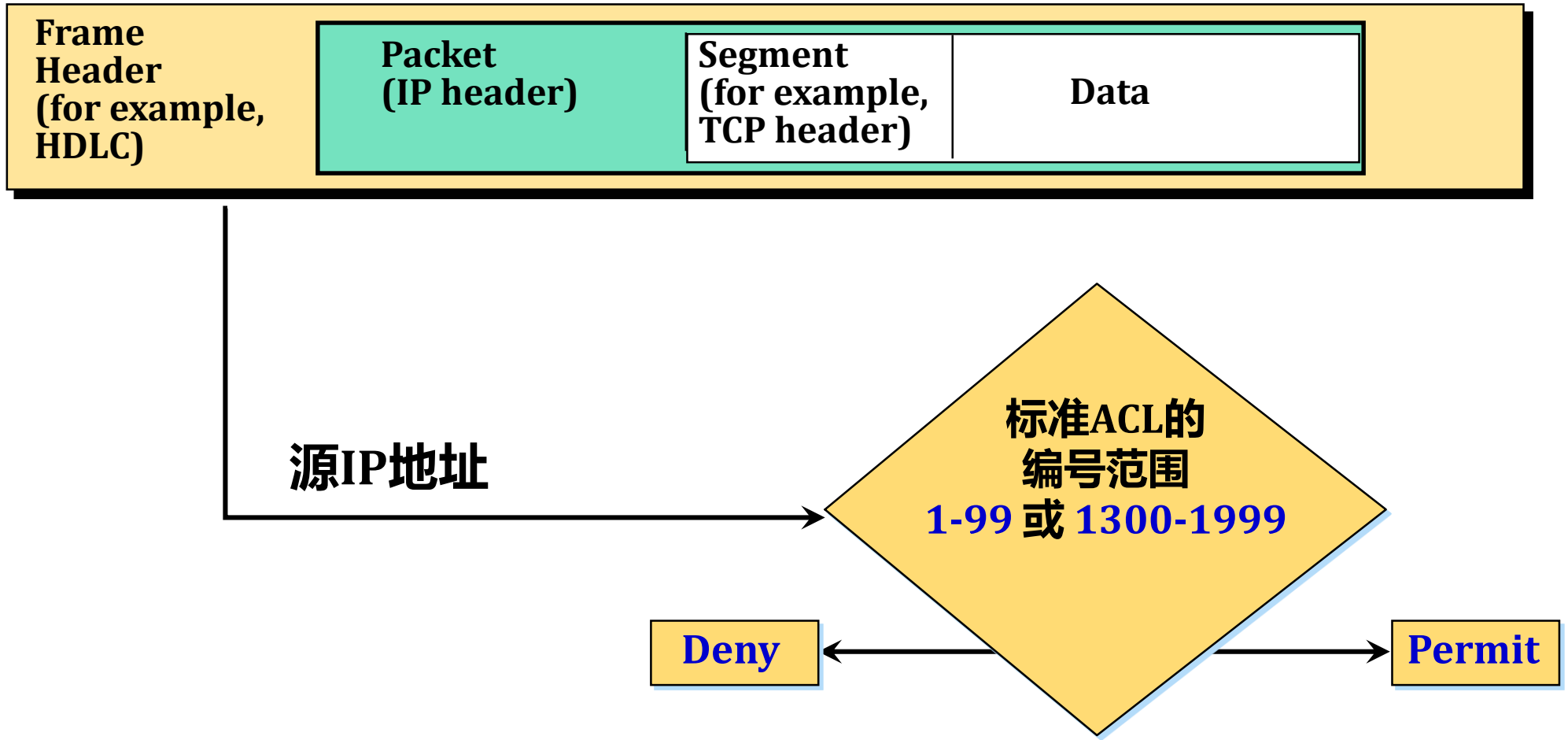
ACL的分类

- 标准IP ACL
  - 编号范围1-99以及1300-1999，限制条件为IP数据包头中的源IP地址
- 扩展IP ACL
  - 编号范围100-199以及2000-2699
  - 限制条件为IP数据包头中的源、目的IP地址、协议类型和源、目的端口号
- 其余编号范围的ACL是针对其它网络协议的

Access List Type		Number Range/Identifier
IP	Standard	1-99 , 1300-1999
	Extended	100-199 , 2000-2699
	Named	Name (Cisco IOS 11.2 and late)
IPX	Standard	800-899
	Extended	900-999
	SAP filters	1000-1099
	Named	Name (IOS 11.2. F and later)

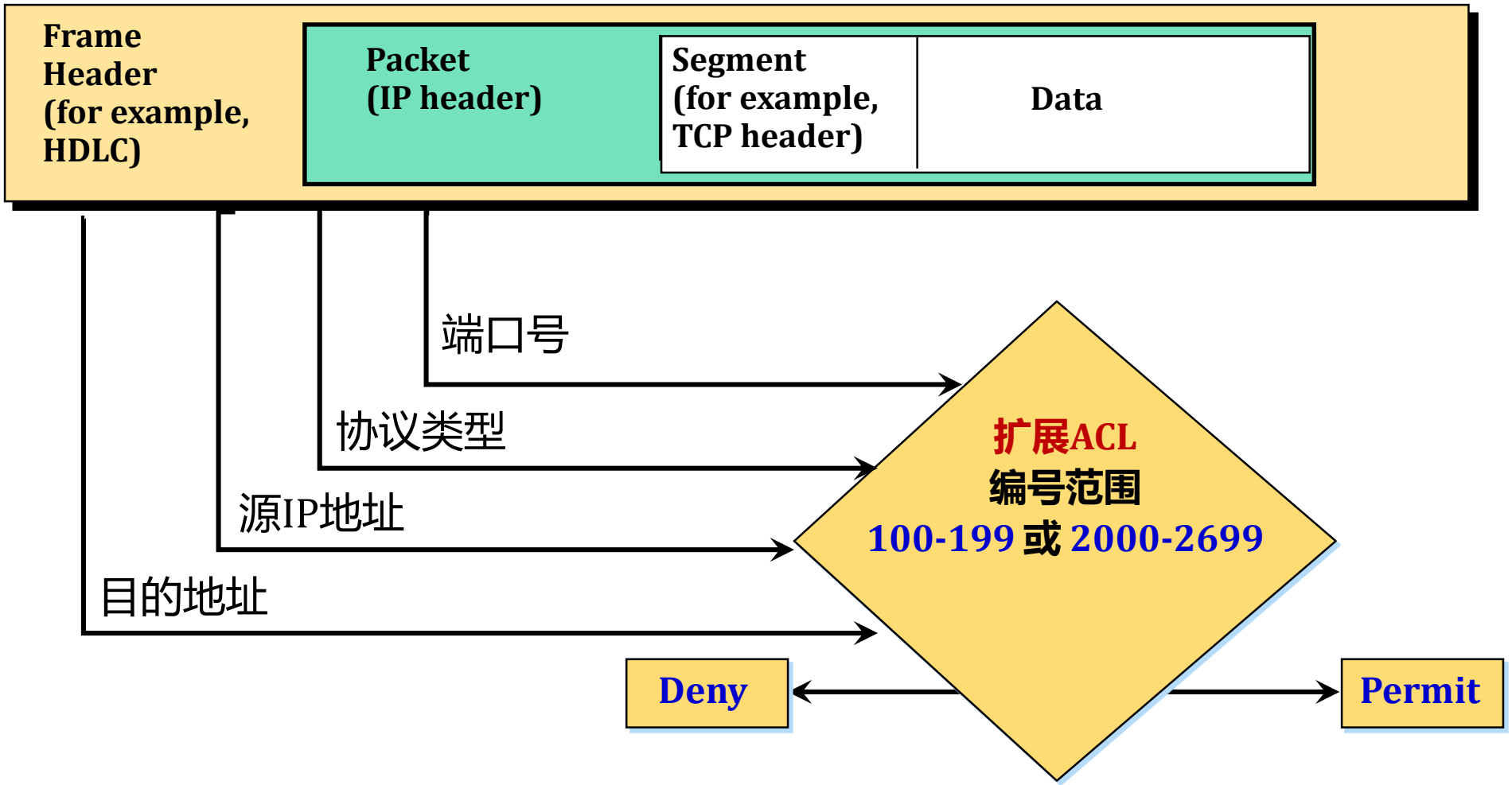
标准ACL的检查内容

TCP/IP数据包的结构图

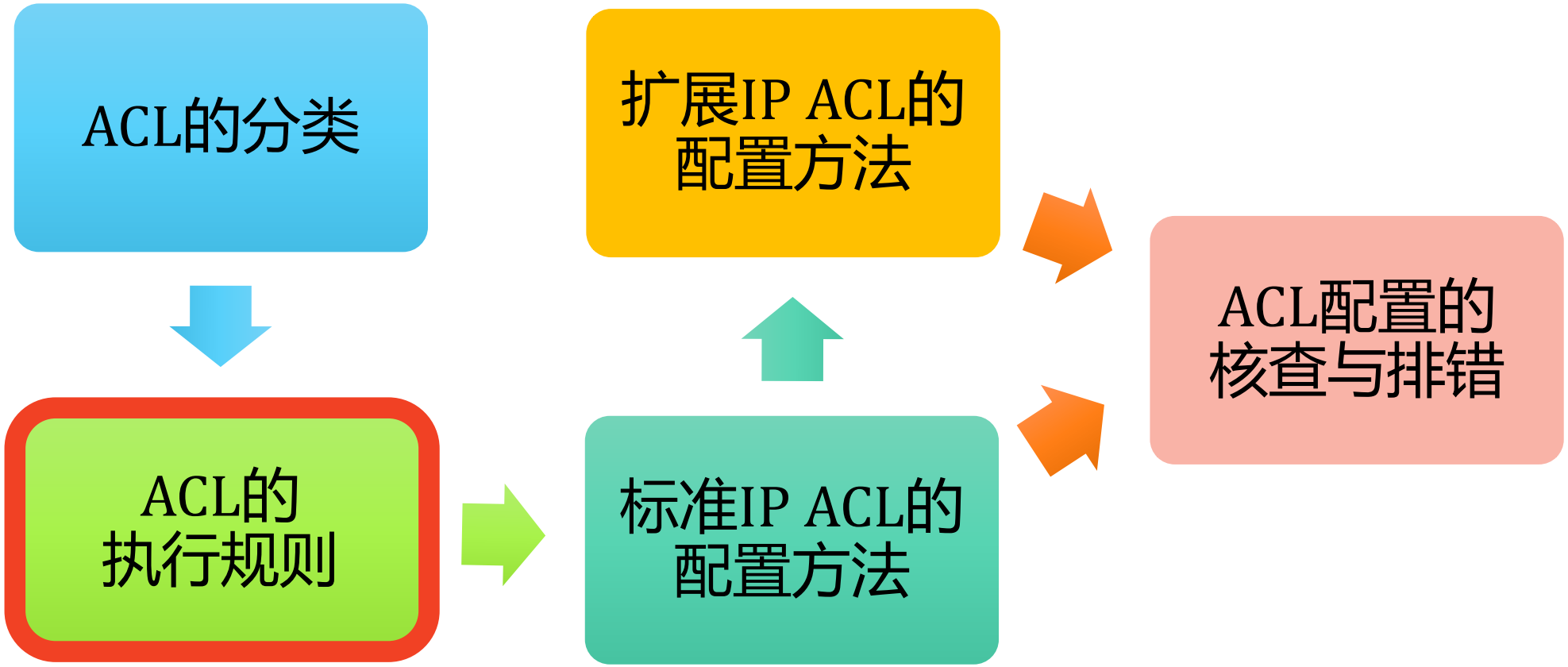


扩展ACL的检查内容

TCP/IP数据包的结构图

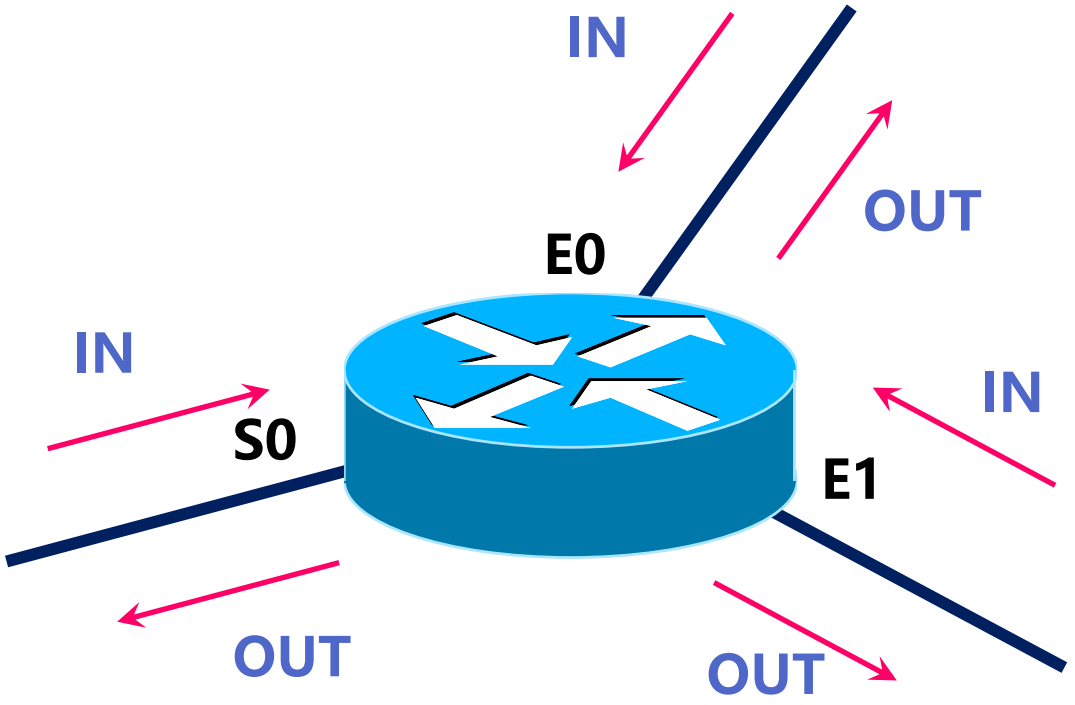


访问控制列表ACL



ACL的作用方向

- 设置规则：对于每个协议，每个路由器的每个接口的每个方向上只能设置一条ACL



ACL的配置规则

- 路由器总是自顶向下顺序检查所有规则
  - 未定义访问控制列表等于permit all
  - 最经常发生的规则放在列表的前面
  - 新增加的行将放在末尾
  - 设置了ACL后，最后一条永远是隐含拒绝一切deny all
- 配置规则时要从具体到一般，例如：
  - deny 192.168.2.0/24
  - permit 192.168.2.1
  - permit any

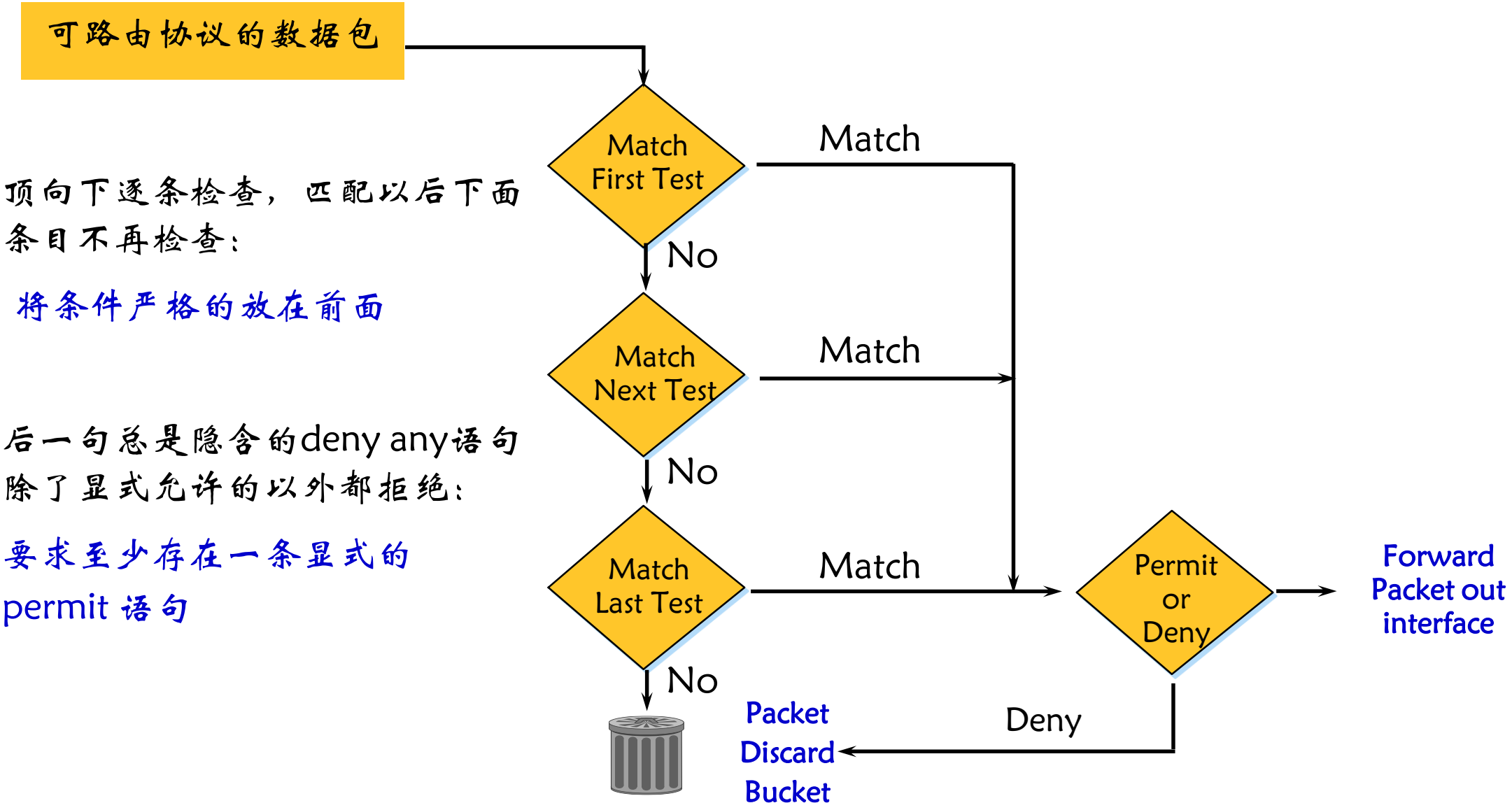
ACL的检查顺序

- 自顶向下逐条检查，匹配以后下面的条目不再检查：

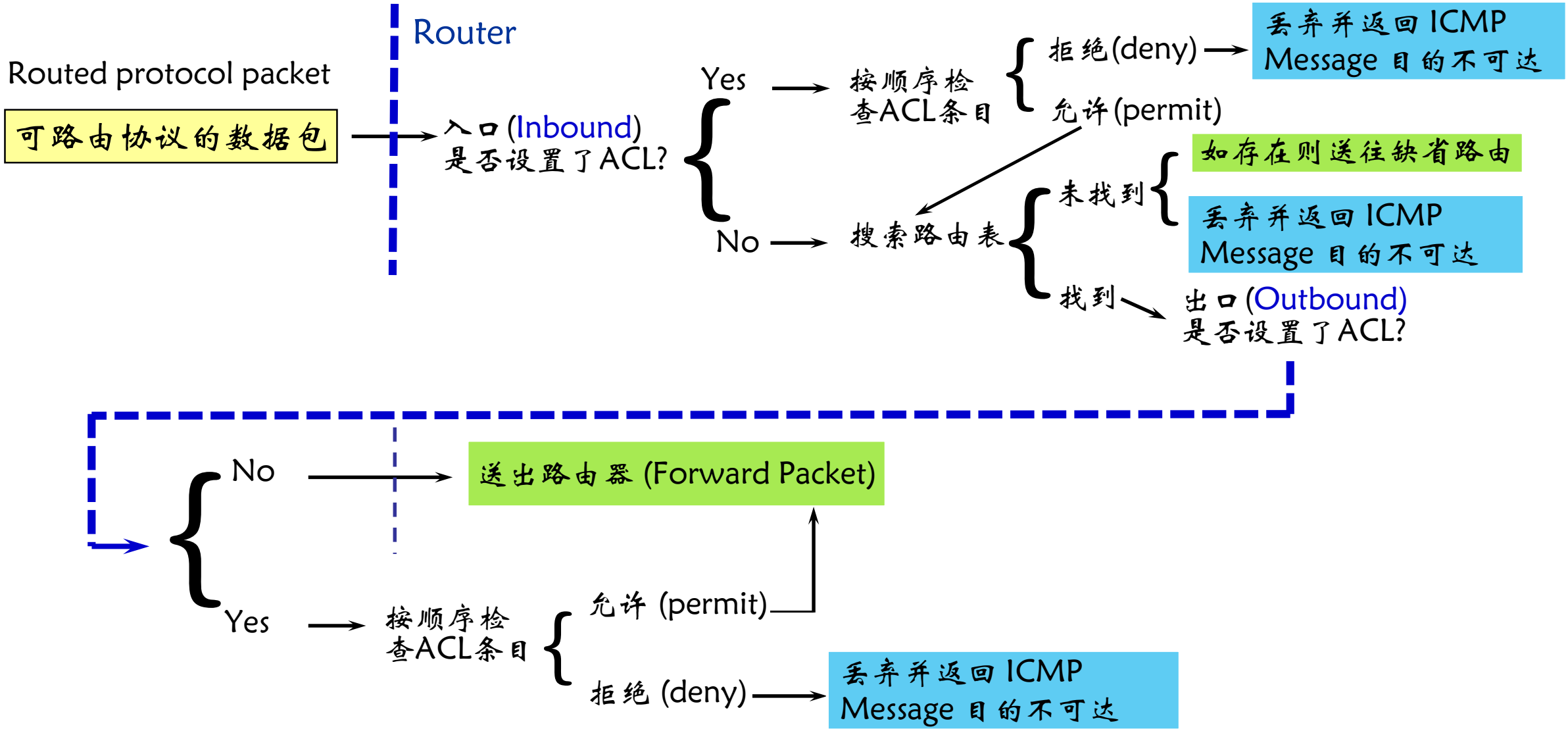
  将条件严格的放在前面

- 最后一句总是隐含的deny any语句，除了显式允许的以外都拒绝：

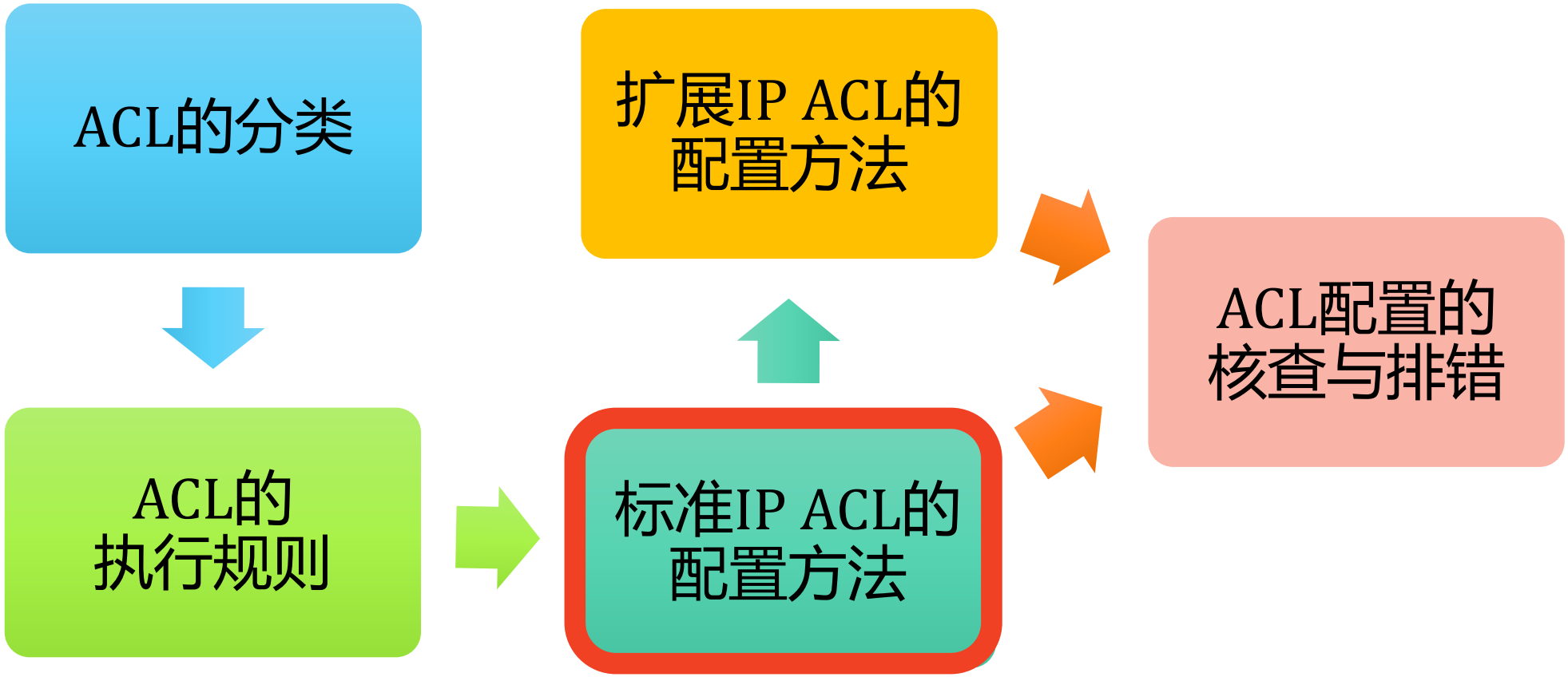
  要求至少存在一条显式的permit 语句



ACL与路由的相互关系



访问控制列表ACL



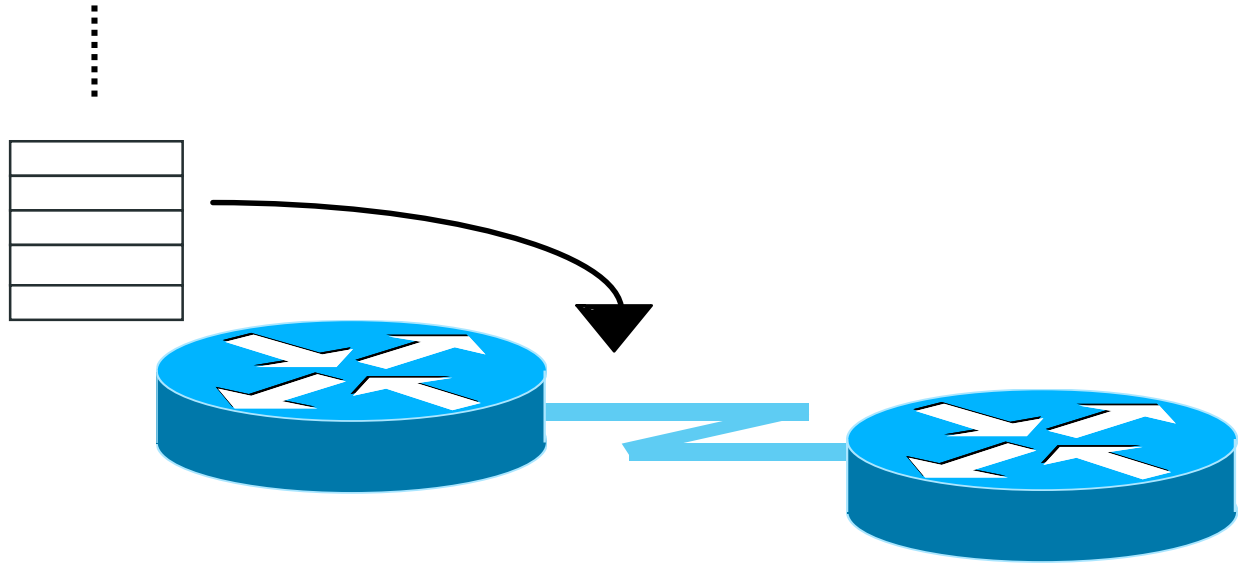
ACL的配置步骤

- 配置ACL的两个步骤:

  1. 定制ACL的规则

  2. 将规则应用到接口

access-list 1 deny	172.30.16.5 0.0.0.0
access-list 1 permit	172.30.16.0 0.0.0.255
access-list 1 deny	192.168.3.1 0.0.0.0
access-list 1 permit	192.168.1.0 0.0.0.255
access-list 1 deny	any



标准IP ACL的配置命令

- 定义标准ACL(编号范围 1- 99 和 1300 - 1999)

Router (config) #

```
access-list access-list-number { permit | deny }
  { source [ source-wildcard ] | any } [log]
```

- 将ACL应用到特定接口

Router (config-if) #

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

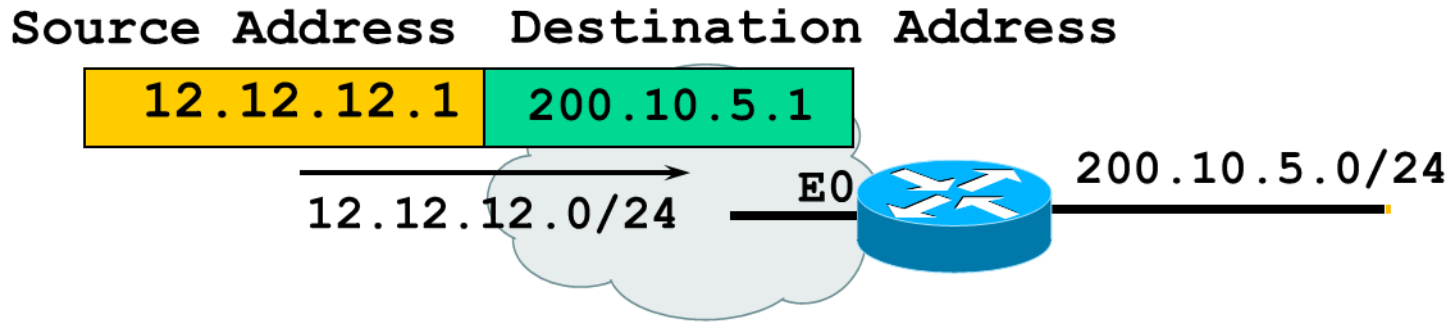
  - Log (可选参数) 将匹配该条目的数据包数量信息发送到控制台，间隔5分钟发送一次

ACL通配符掩码的规则

- 通配符掩码位是0表示必须匹配前面地址对应的比特
- 通配符掩码位是1表示不必匹配前面地址对应的比特

Address	Wildcard	Matches
0.0.0.0	255.255.255.255	any address
131.108.0.0	0.0.255.255	network 131.108.0.0
131.104.7.11	0.0.0.0	host 131.104.7.11
255.255.255.255	0.0.0.0	local broadcast
131.111.8.0	0.0.7.255	subnet 131.111.8.0/21

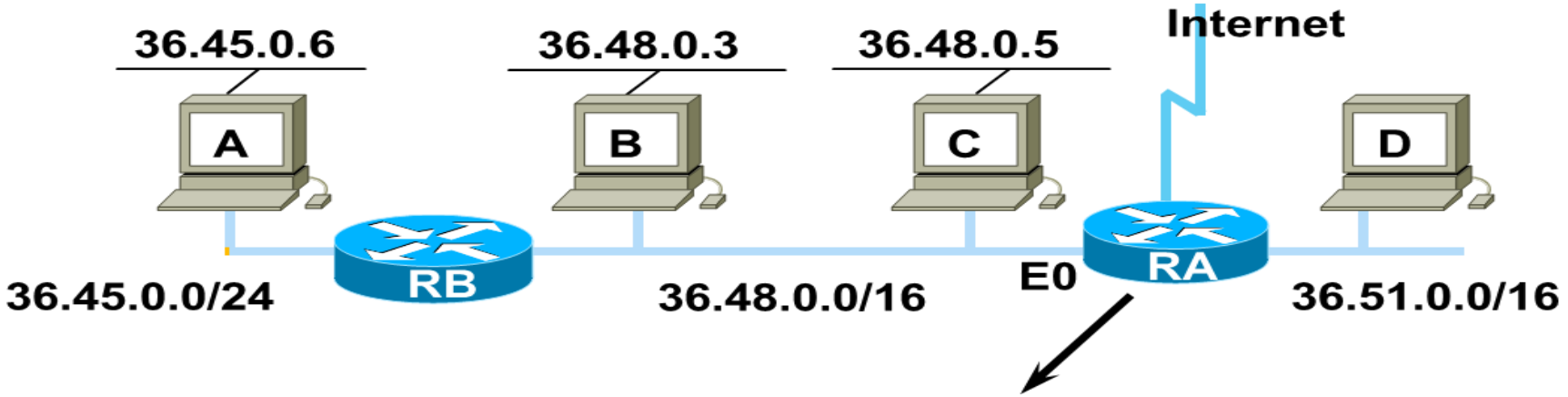
ACL的工作过程




```
access-list 3 permit 12.0.0.0   0.255.255.255
interface Ethernet 0
  ip access-group 3 in
```

IP address	12.0.0.0	00001100	00000000	00000000	00000000
wildcard mask	0.255.255.255	00000000	11111111	11111111	11111111
	12.any.any.any	00001100	any	any	any
Example	16.12.12.1	00010000	00001100	00001100	00000001
	0.255.255.255	00000000	11111111	11111111	11111111

标准IP ACL配置示例




```
RA(config)# access-list 1 deny 36.48.0.3 0.0.0.0
RA(config)# access-list 1 permit 36.48.0.0 0.0.255.255
! (Note: all other access implicitly denied)
RA(config)# interface ethernet 0
RA(config-if)# ip access-group 1 in
```

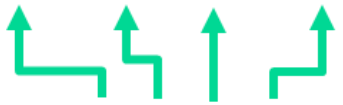
```
RA(config)# access-list 1 permit 36.48.0.0 0.0.255.255
RA(config)# access-list 1 deny 36.48.0.3 0.0.0.0
RA(config)# interface ethernet 0
RA(config-if)# ip access-group 1 in
```

→ 被前面的语句所包含，因此无效

特殊的通配符掩码表示方法

- 匹配所有的比特位 (match all)

172.30.16.29



Wildcard Mask: 0.0.0.0（检查所有比特）

标准语法：

access-list 1 permit 172.30.16.29 0.0.0.0

可使用关键字 host 表示为：

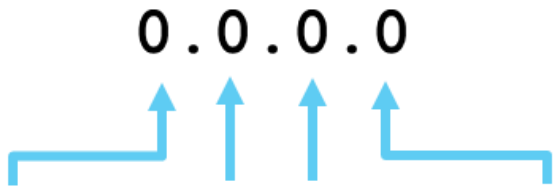
access-list 1 permit host 172.30.16.29

如果不写通配符掩码隐含为 0.0.0.0 ，例如：

access-list 1 permit 172.30.16.29

特殊的通配符掩码表示方法

- 忽略所有的比特位 (ignore all)



Wildcard Mask: 255.255.255.255 (忽略所有比特)

标准语法：

```
access-list 1 permit   0.0.0.0 255.255.255.255
```

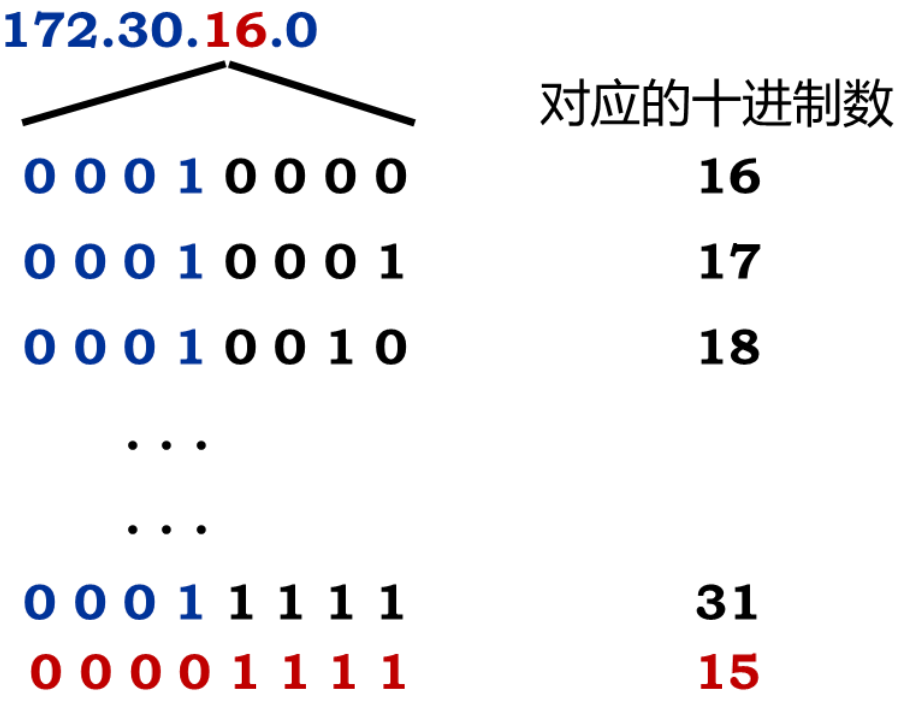
可使用关键字 any 表示为：

```
access-list 1 permit   any
```

案例1：复杂通配符掩码的计算方法

- 问题：如果IP子网的变化范围172.30.16.0/24 至172.30.31.0/24，要求用一条语句表示

- 第3个字节前4个比特是相同部分，必须完全匹配，通配符为0；
- 后面4个比特是全排列，为任意组合，因此通配符为1。
- 通配符以十进制形式表示为：0.0.15.255



最终配置结果：

```
access-list 1 permit 172.30.16.0  0.0.15.255
```

案例2：复杂通配符掩码的计算方法

- 问题：如果IP子网的变化范围改为 172.30.16.0/24 至 172.30.30.0/24，该如何配置？

```
access-list 1 deny 172.30.31.0  0.0.0.255
access-list 1 permit 172.30.16.0  0.0.15.255
```

案例3：复杂通配符掩码的计算方法

- 问题：如果IP子网允许通过的地址范围 200.10.5.10 ~ 15，该如何配置？

分析最后一个字节的变化范围

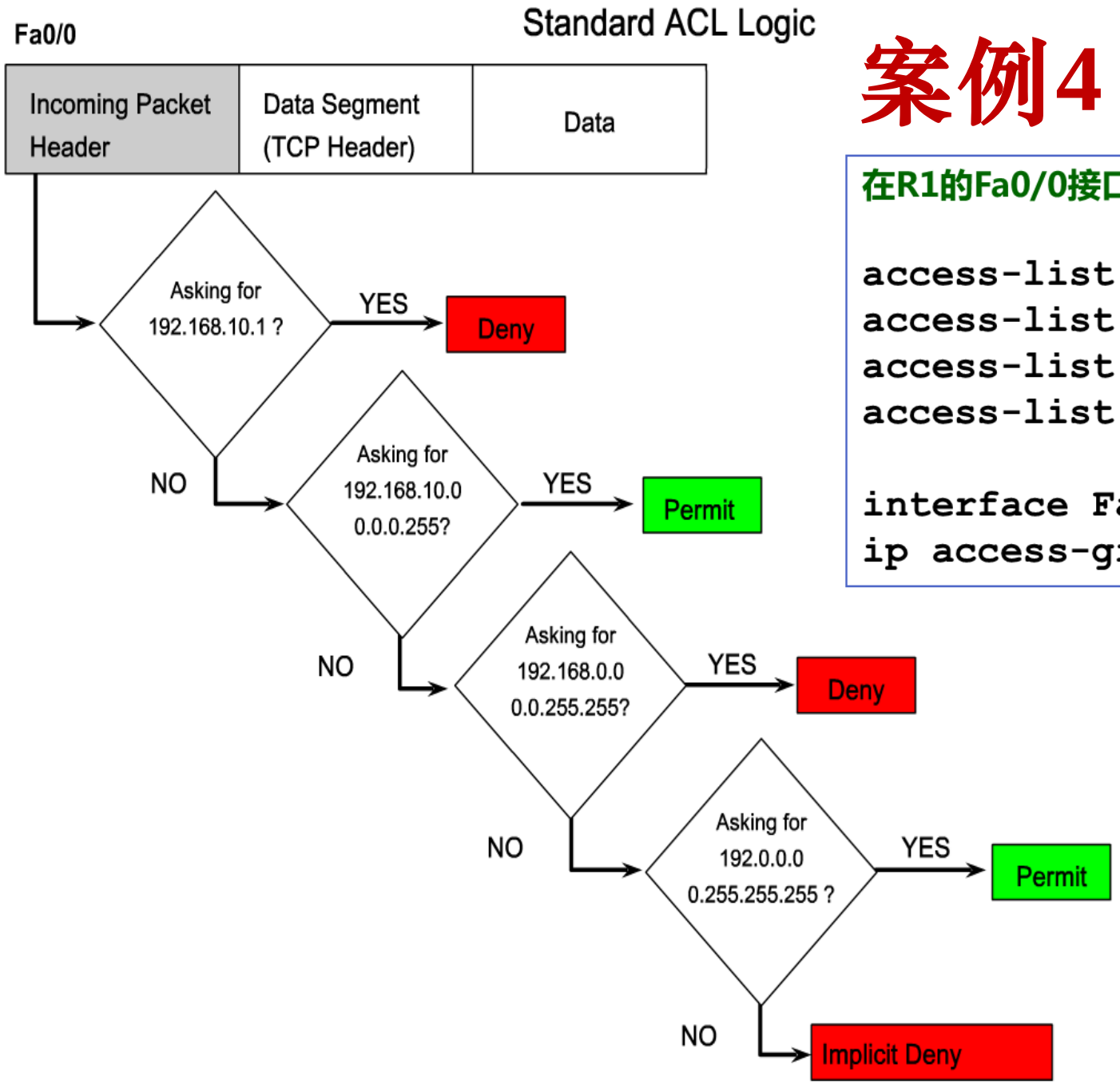
00001010	10
00001011	11
00001100	12
00001101	13
00001110	14
00001111	15

	00001010	(10)
	00001011	(11)
通配符掩码	00000001	(1)
	00001100	(12)
	00001101	(13)
	00001110	(14)
	00001111	(15)
通配符掩码	00000011	(3)

最终配置结果：

```
access-list 3 permit 200.10.5.10  0.0.0.1
access-list 3 permit 200.10.5.12  0.0.0.3
```

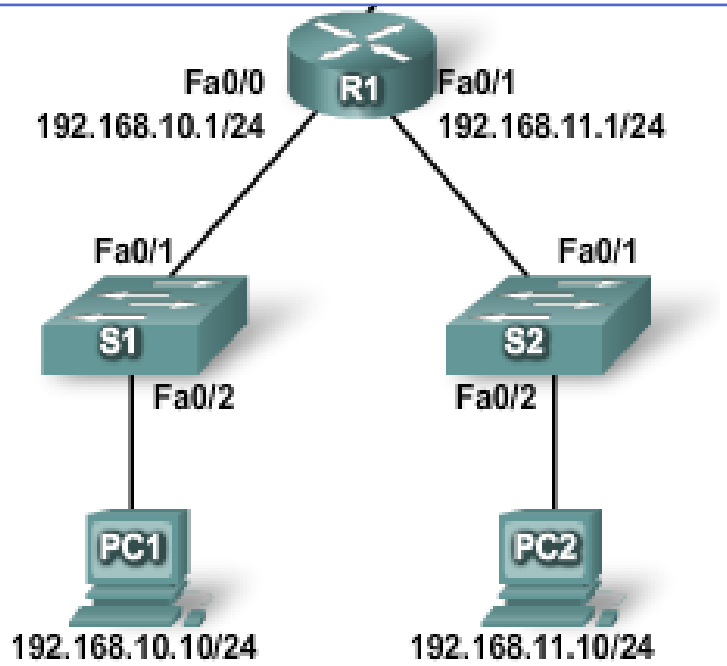
案例4：标准IP ACL配置



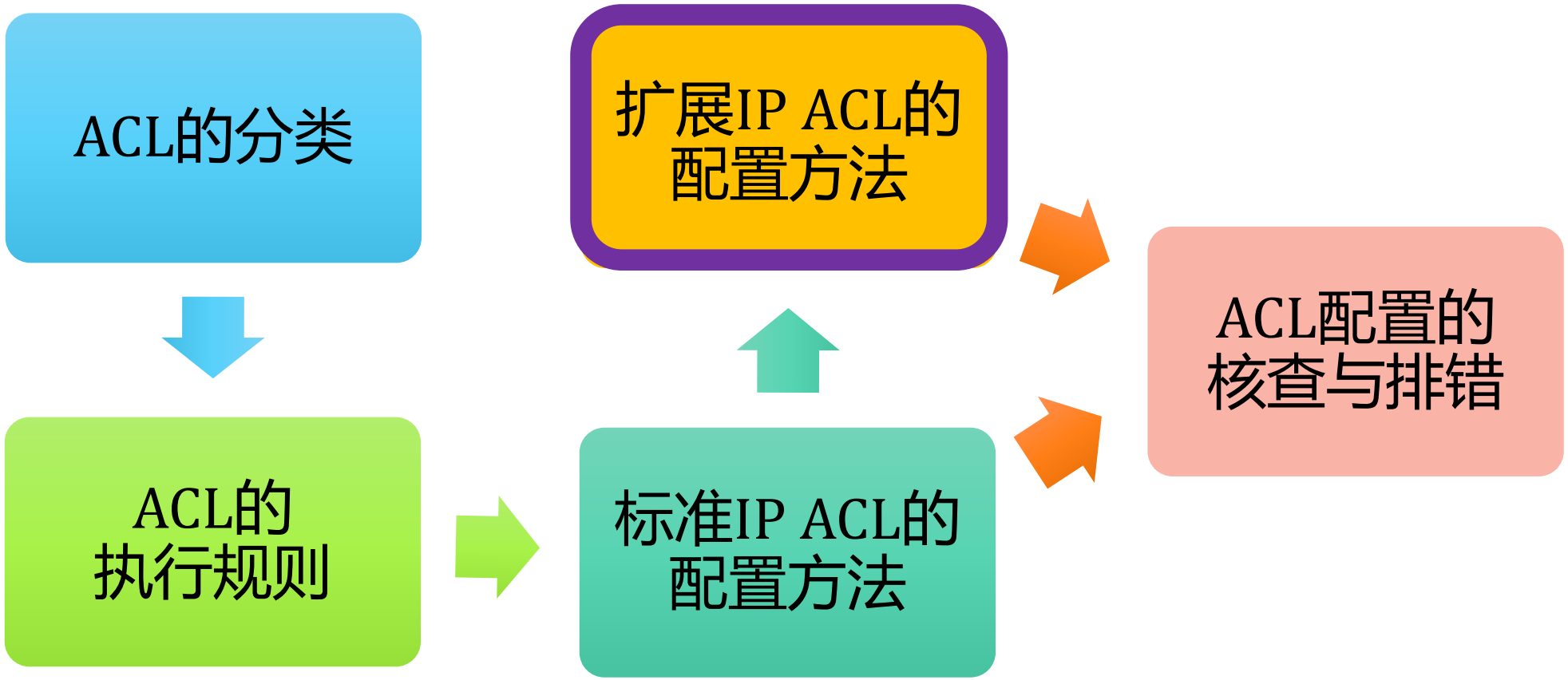
在R1的Fa0/0接口的入方向设置下列标准IP ACL:

```
access-list 7 deny 192.168.10.10
access-list 7 permit 192.168.10.0 0.0.0.255
access-list 7 deny 192.168.0.0 0.0.255.255
access-list 7 permit 192.0.0.0 0.255.255.255

interface Fa0/0
ip access-group 7 in
```

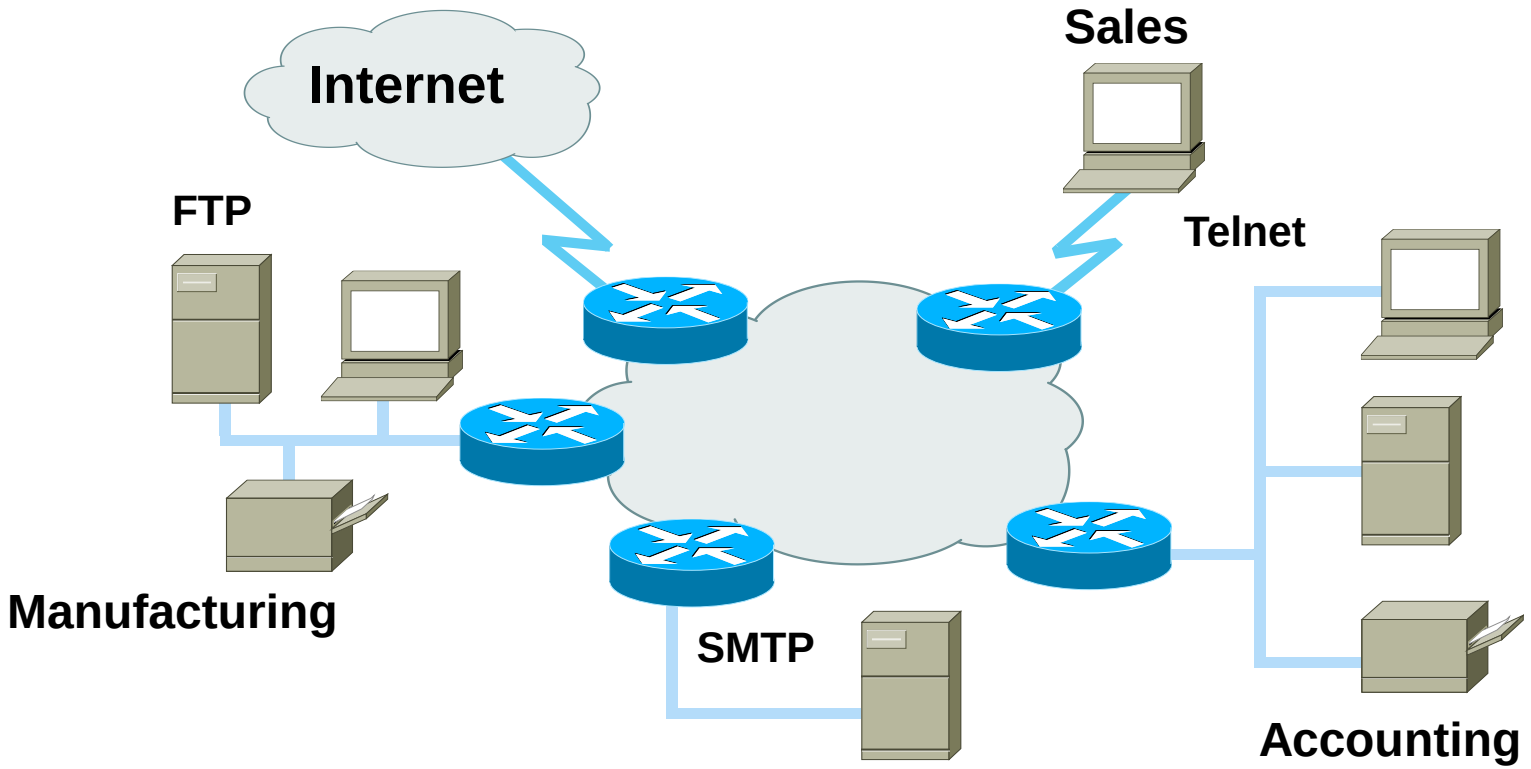


访问控制列表ACL



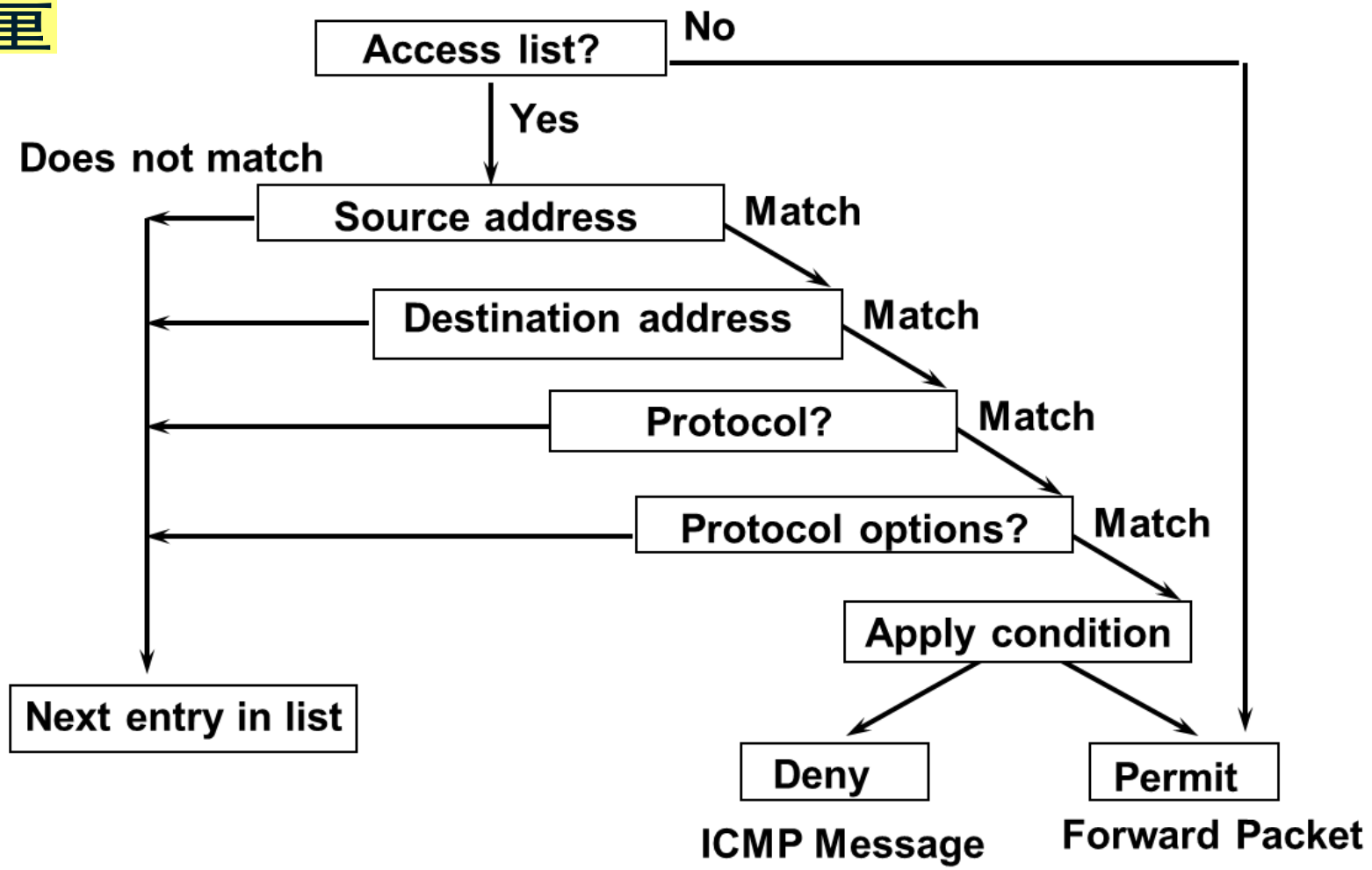
标准IP ACL的局限性

- 标准IP ACL只能根据包头中源IP地址控制流量



扩展IP ACL的优势

- 扩展IP ACL可以根据数据源地址、目的地址、上层应用程序控制流量



扩展IP ACL的配置命令

- 定义扩展IP ACL(编号范围 100- 199 和 2000 - 2699)

Router (config) #

```
access-list  access-list-number { permit | deny}
      {protocol | protocol-keyword}
     {source source-wildcard | any}
     { destination destination-wildcard | any }
      [ protocol-specific options ]
```

Protocol 字段关键字：ip, icmp, tcp, 和 udp 等。
Protocol-specific选项字段根据协议不同而变化。

- 将ACL应用到特定接口

Router (config-if) #

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

Protocol字段为TCP的语法

Router (config) #

```
access-list access-list-number { permit | deny } tcp
    { source source-wildcard | any }
    [ operator source-port  | source-port  ]
    { destination destination-wildcard | any }
    [ operator destination-port  | destination-port  ]
    [ established ]
```

Operator (**可选**) **其内容为:** lt, gt, eq, neq **或** range .

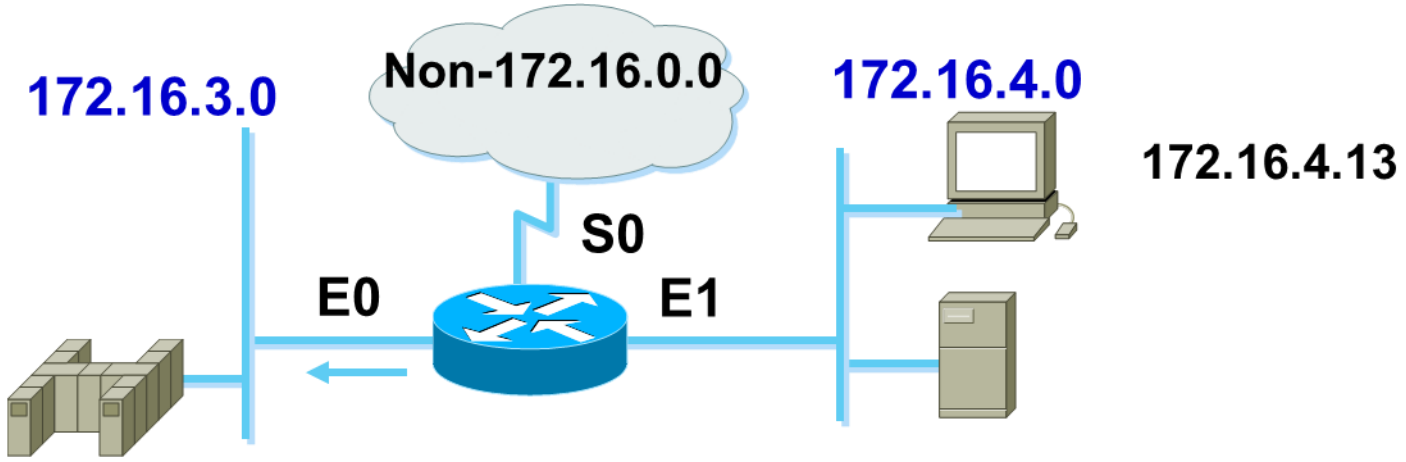
TCP端口号对应的协议

1	tcpmux TCP 端口服务多路复用
5	rje 远程作业入口
7	echo Echo 服务
9	discard 用于连接测试的空服务
11	systat 用于列举连接了的端口的系统状态
13	daytime 给请求主机发送日期和时间
17	qotd 给连接了的主机发送每日格言
18	msp 消息发送协议
19	chargen 字符生成服务；发送无止境的字符流
20	ftp-data FTP 数据端口
21	ftp 文件传输协议（FTP）端口
22	ssh 安全 Shell（SSH）服务
23	telnet Telnet 服务
25	smtp 简单邮件传输协议（SMTP）
37	time 时间协议
39	rlp 资源定位协议
42	nameserver 互联网名称服务
43	nicname WHOIS 目录服务
49	tacacs 用于终端访问控制器访问控制系统
50	re-mail-ck 远程邮件检查协议
53	domain 域名服务（如 BIND）
63	whois++ WHOIS++，被扩展了的 WHOIS 服务
67	bootps 引导协议（BOOTP）服务； 还被动态主机配置协议（DHCP）服务使用
68	bootpc Bootstrap（BOOTP）客户； 还被动态主机配置协议（DHCP）客户使用
69	tftp 小文件传输协议（TFTP）
70	gopher Gopher 互联网文档搜寻和检索
71	netrjs-1 远程作业服务
72	netrjs-2 远程作业服务
73	netrjs-3 远程作业服务
73	netrjs-4 远程作业服务
79	finger 用于用户联系信息的 Finger 服务
80	http 超文本传输协议（HTTP）
88	kerberos Kerberos 网络验证系统
95	supdup Telnet 协议扩展

端口号参见RFC 1700文档

案例：协议字段为TCP的扩展IP ACL

- 问题：禁止来自子网172.16.4.0/24的流量访问目的子网172.16.3.0/24中FTP服务，其它流量允许通过。




```
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
```

Protocol字段为UDP的语法

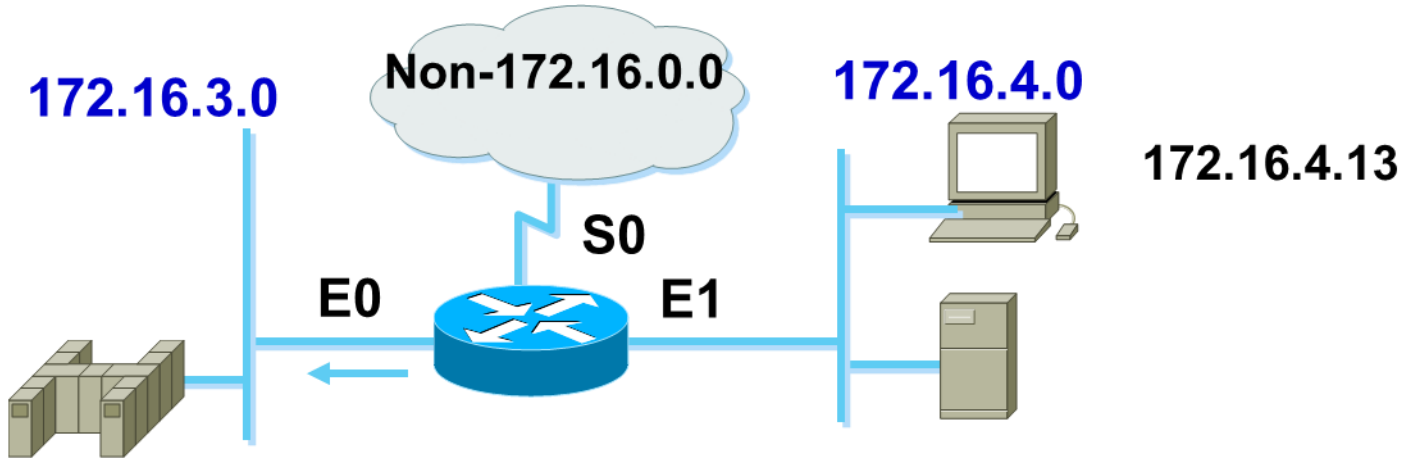
Router (config) #

```
access-list access-list-number { permit | deny } udp
    { source source-wildcard | any }
    [ operator source-port  | source-port  ]
    { destination destination-wildcard | any }
    [ operator destination-port  | destination-port  ]
```

Operator (可选) 其内容为: lt, gt, eq, neq 或 range .

案例：协议字段为UDP的扩展IP ACL

- 问题：禁止来自子网172.16.4.0/24的流量访问172.16.3.0/24子网中的TFTP服务，其它流量允许通过。




```
access-list 101 deny udp 172.16.4.0 0.0.0.255 any eq 69
access-list 101 permit ip any any
(implicit deny all)

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

Protocol字段为ICMP的语法

Router (config) #

```
access-list access-list-number { permit | deny } icmp
    { source source-wildcard | any }
    { destination destination-wildcard | any }
    [ icmp-type [ icmp-code ] | icmp-message ]
```

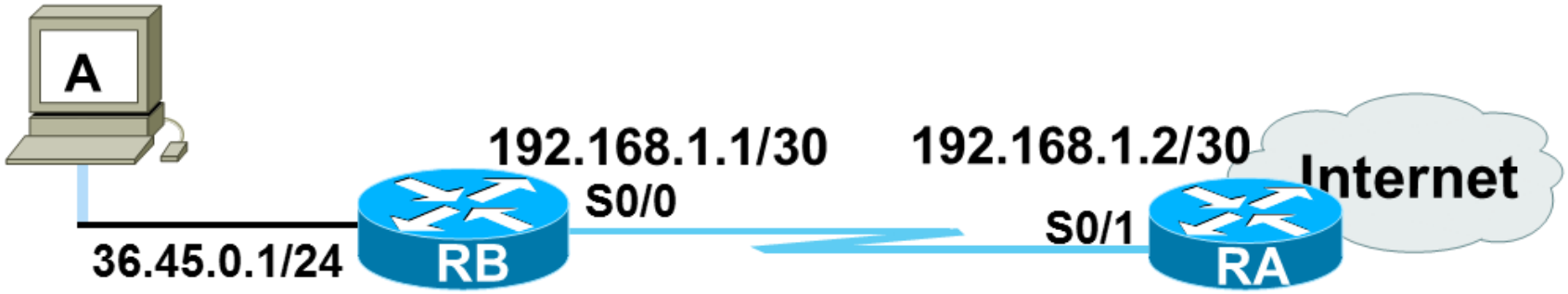
*icmp-type*参见下一页内容

- 部分ICMP 消息类型名称
- 完整的ICMP信息参见RFC 792文档

administratively-prohibited	information reply	port unreachable
alternate-address	mask-reply	reassembly-timeout
conversion-error	mask-request	redirect
dod-host-prohibited	mobile-redirect	router-advertisement
dod-net-prohibited	net-redirect	router-solicitation
echo	net-tos-redirect	source-quench
echo-reply	net-tos-unreachable	source-route-failed
general-parameter-problem	net-unreachable	time-exceeded

案例：协议字段为ICMP的扩展IP ACL

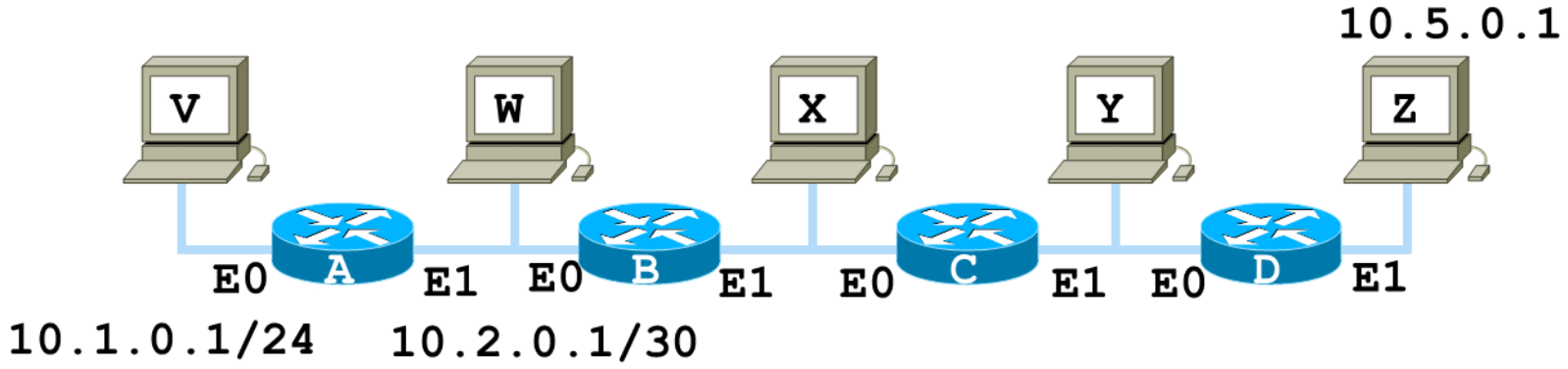
- 问题：要求在RB上能PING通RA的S0/1接口地址，但不允许来自RA及互联网上的流量PING RB的任何接口地址，其它流量允许通过，应该如何配置？




```
RB(config)# access-list 100 deny icmp any host 192.168.1.1
RB(config)# access-list 100 deny icmp any host 36.45.0.1
RB(config)# access-list 100 permit ip any any
RB(config)# interface S0/0
RB(config-if)# ip access-group 100 in
```

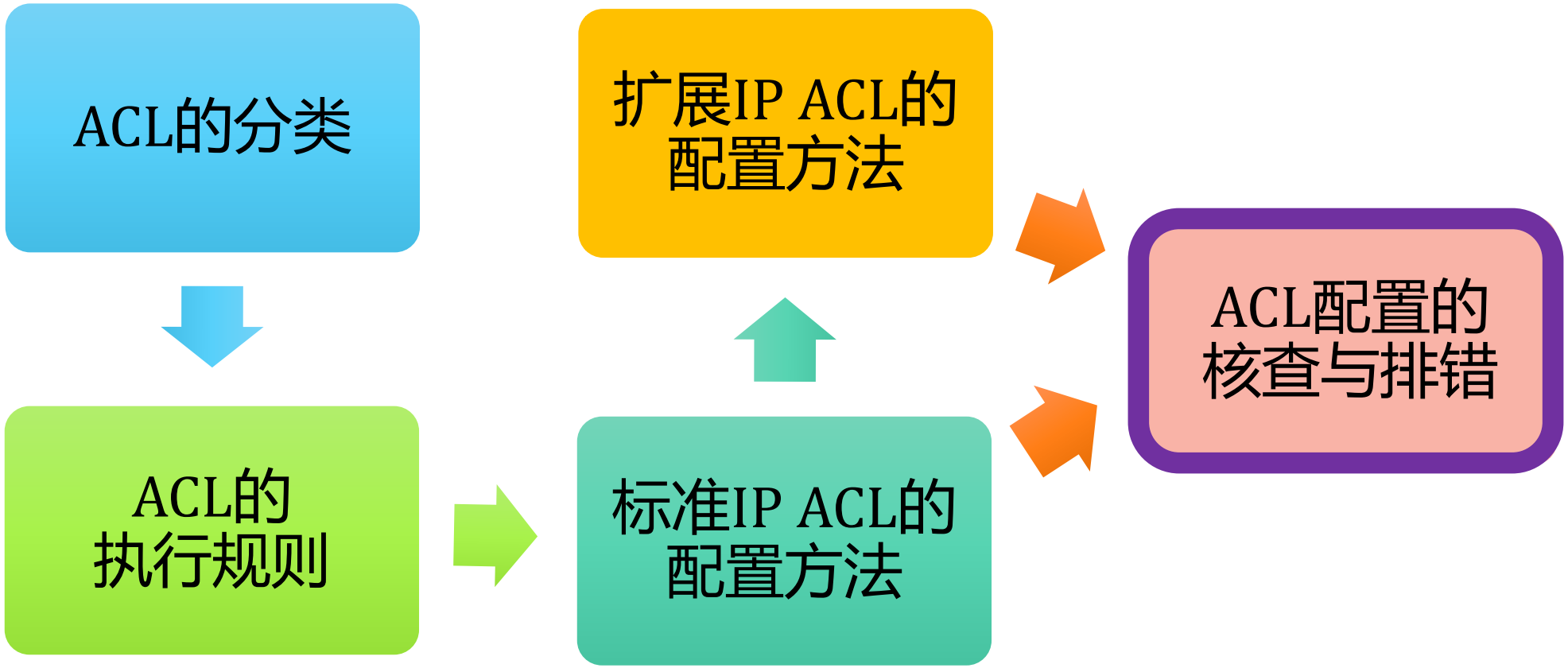
案例：ACL

- 问题：在路由器A右侧的网络中，只允许主机 Z Telnet 路由器A，其它类型流量不能Telnet路由器A，要求使用扩展IP ACL，如何设置？




```
RA(config)# access-list 100 permit tcp host 10.5.0.1 host 10.2.0.1 eq 23
RA(config)# access-list 100 permit tcp host 10.5.0.1 host 10.1.0.1 eq 23
RA(config)# access-list 100 deny tcp any host 10.2.0.1 eq 23
RA(config)# access-list 100 deny tcp any host 10.1.0.1 eq 23
RA(config)# access-list 100 permit ip any any
RA(config)# interface Ethernet1
RA(config-if)# ip access-group 100 in
```

访问控制列表ACL



检查接口上是否设置了ACL

```
Router# show ip interface 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>
```

显示访问控制列表的命令

- 显示所有协议的访问控制列表

Router #

```
show access-lists [ access-list-number ]
```

- 显示IP协议的访问控制列表

Router #

```
show ip access-lists [ access-list-number ]
```

- 案例

```
Router# show ip access-lists
Extended IP access list 101
    deny udp any any eq ntp
    permit tcp any any
    permit udp any any eq tftp
    permit icmp any any
    permit udp any any eq dns
Router#
```

ACL的配置规则总结

- 对于每个协议，在每个路由器接口的每个方向上只能设置一条ACL，后写入的覆盖先前的
- 自顶向下逐条检查，匹配后其余条目不再检查：将条件严格的放在前面
- 最后一句是隐含的deny any语句，至少需要存在一条显式的permit语句；未定义的ACL (空ACL)相当于permit any
- 新增加的语句总是置于最后一行
- 访问控制列表不能限制起源于本路由器的流量


Thanks a lot !

Activity is the only road to knowledge!

Computer Network Security @ 2023Fall