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

访问控制技术

- 访问控制的基本概念
- 防火墙的基本概念
- 防火墙的配置结构
- 访问控制列表ACL
- 虚拟局域网VLAN

1911–2021
清華大學 110周年校庆
110th ANNIVERSARY
TSINGHUA UNIVERSITY

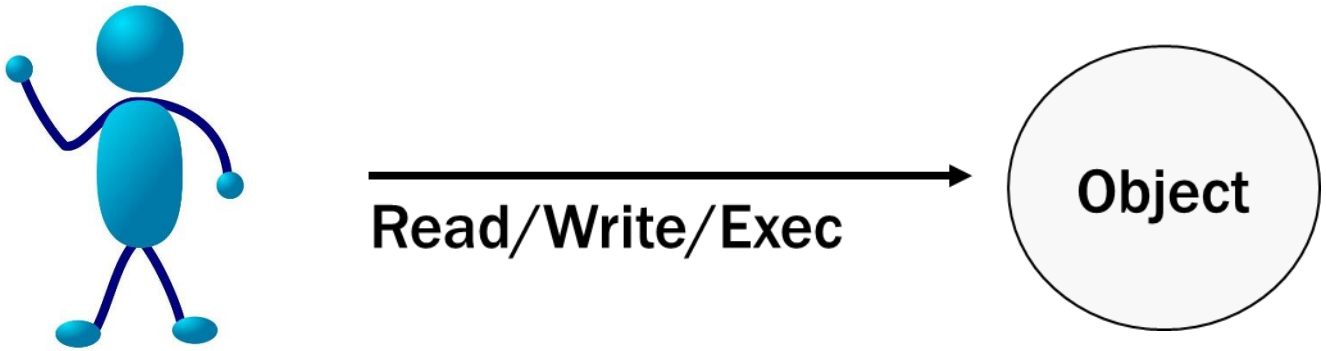
访问控制的基本概念

访问控制的基本概念

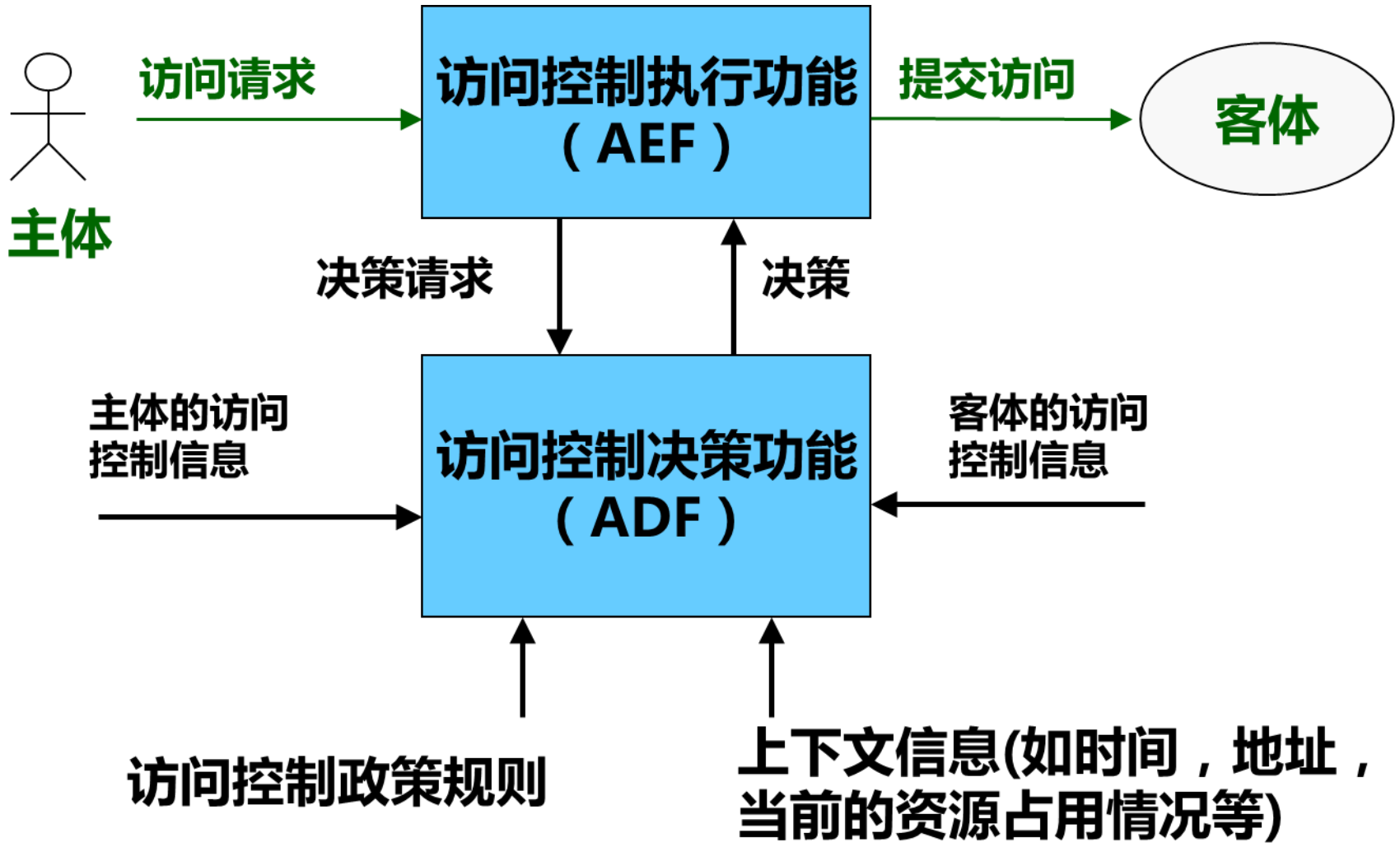
- 主体(Subject)
  - 主体是一个主动的实体，它提出对资源访问请求
  - 如用户，程序，进程等
- 客体(Object)
  - 含有被访问资源的被动实体
  - 如网络、计算机、数据库、文件、目录、程序、 外设等
- 访问(Access)
  - 对资源的使用，读、写、修改、删除等操作
  - 例如访问存储器、访问文件/目录/外设、访问数据库/网站等

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

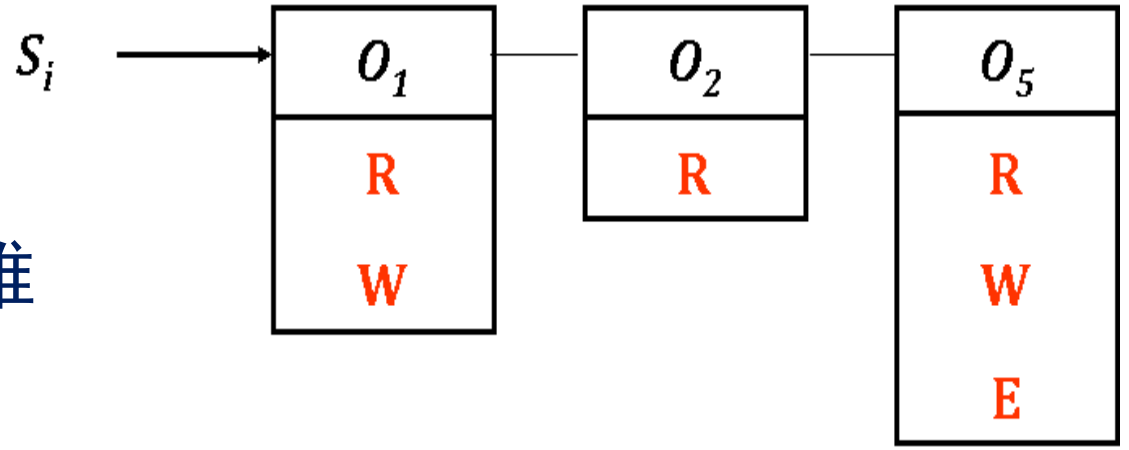
访问控制矩阵

- 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)

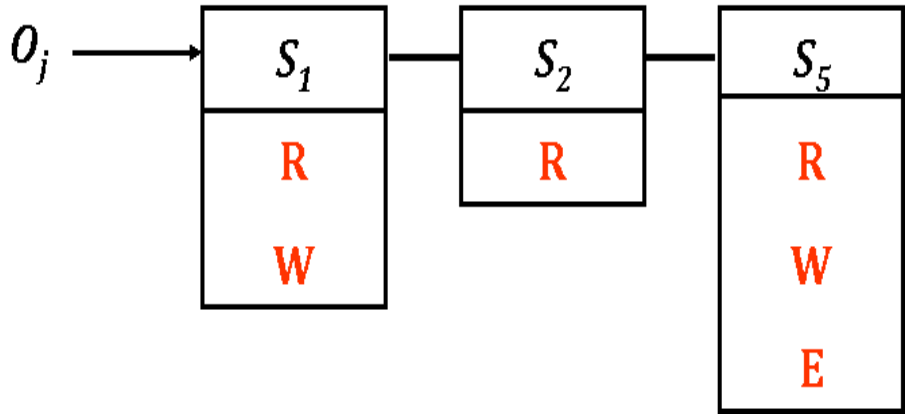
- 能力表与主体关联，规定主体所能访问的客体和权限
  - 从能力表得到一个主体所有的访问权限很容易
  - 从能力表浏览一个客体所允许的访问控制权限很困难



- 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)

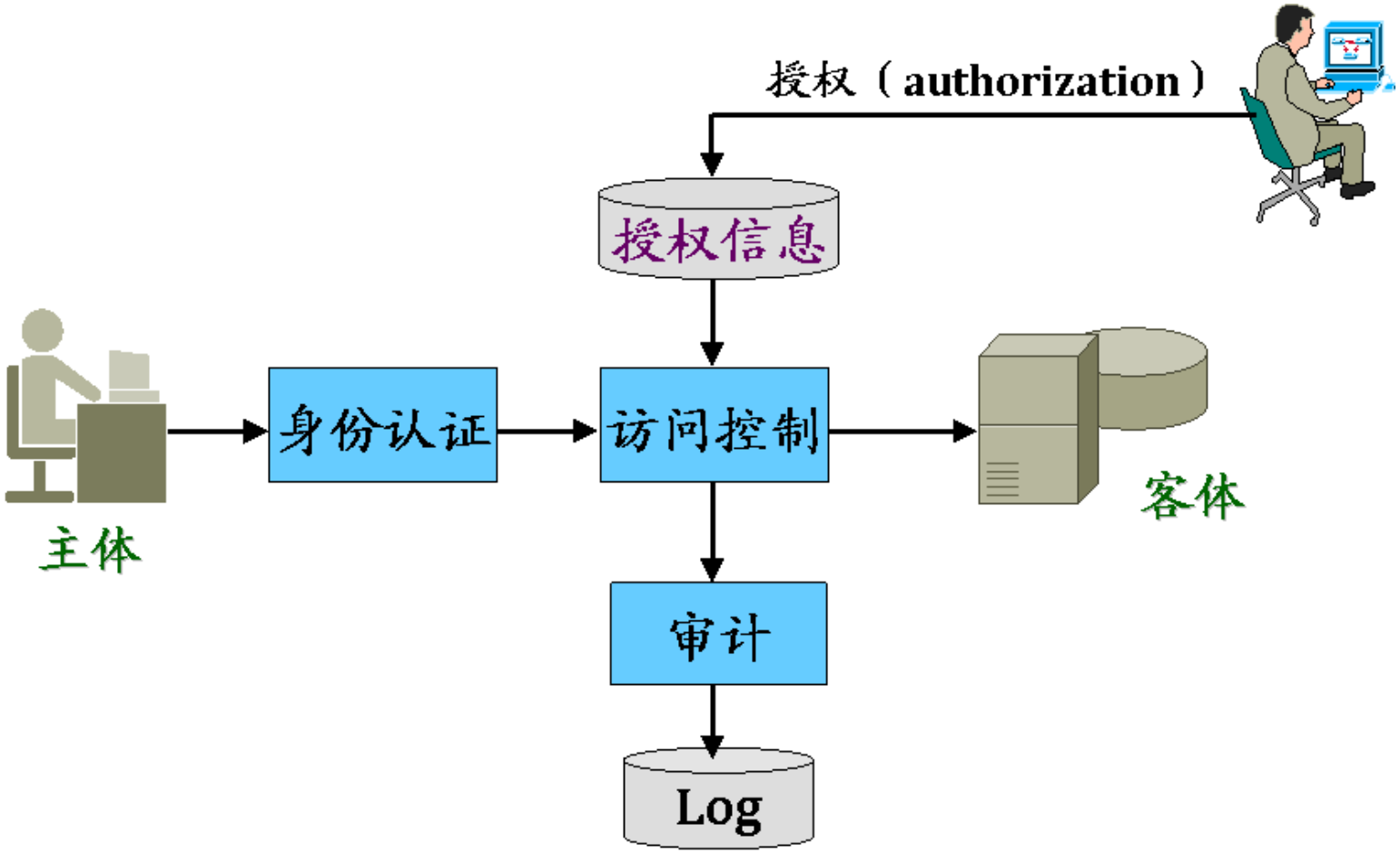
- 访问控制表与客体关联，规定能够访问它的主体和权限
  - 得到一个客体所有的访问权限很容易
  - 浏览一个主体的所有访问权限很困难



- 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（读取操作），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

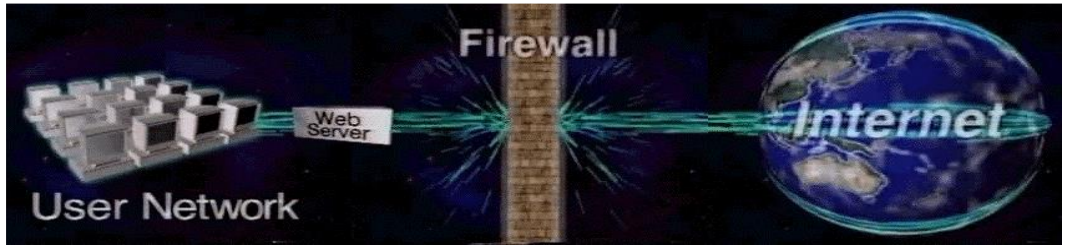
1911–2021
清華大學 110周年校庆
110th ANNIVERSARY
TSINGHUA UNIVERSITY

防火墙的基本概念

防火墙的基本概念

- 防火墙是在被保护网络和其他网络之间实施访问控制政策的一组设备，由软、硬件设备组成、在内网和外网之间、专用网与公共网之间的界面上构造的保护屏障

- 为什么需要防火墙？
  - 企业的业务对互联网需求
  - 企业网和Internet的连接的风险
  - 企业内部网不同安全需求的网段之间的隔离

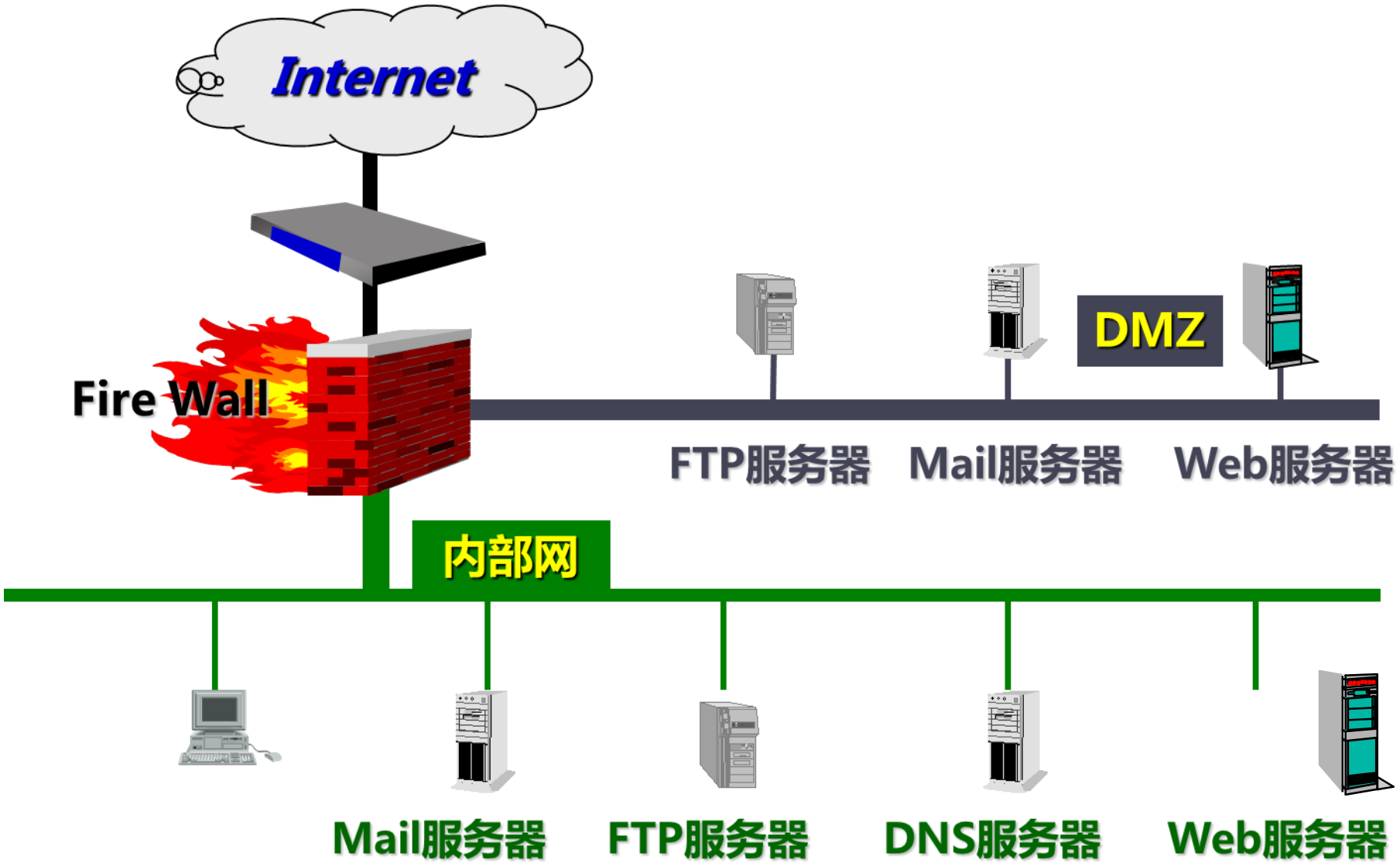


- 防火墙的作用
  - 隐藏内部网络结构及资源
  - 保护不安全的网络服务
  - 执行网络间的访问控制策略
  - 统一集中的安全管理
  - 记录并统计网络使用情况
  - 监视和预警

防火墙的设计目标

- 所有的通信，无论是从内部到外部还是从外部到内部的，都必须经过防火墙
- 只有授权的通信才能通过防火墙，这些授权将在本地安全策略中规定
- 不同类型的防火墙将实现不同的安全策略
- 防火墙本身对于渗透必须是免疫，这意味着必须使用运行安全操作系统可信系统

防火墙的定义


Internet
Fire Wall
DMZ
FTP服务器
Mail服务器
Web服务器
内部网
Mail服务器
FTP服务器
DNS服务器
Web服务器

防火墙的各种分类

从结构上划分

- 单一主机防火墙
- 路由器集成式防火墙
- 分布式防火墙

从性能上划分

- 百兆级防火墙
- 千兆级防火墙
- 万兆级防火墙

从应用部署位置上划分

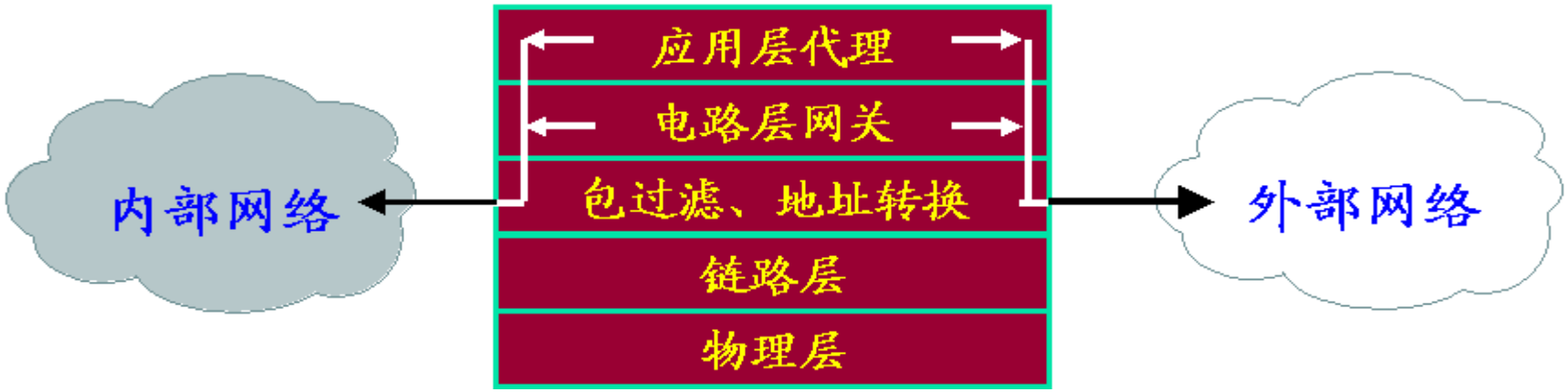
- 个人防火墙：
  - 安装于单台主机，通常为软件防火墙，价格便宜，性能差
- 边界防火墙
  - 传统防火墙，内外网络实施隔离，保护边界内部网络；硬件实现，价格较贵，性能较好
- 芯片级防火墙
  - 使用专有的ASIC(专用集成电路)芯片处理能力强，性能高，价格也最贵

防火墙的常用技术

- 防火墙常用来控制访问和加强站点安全策略的四项技术：
  - 服务控制(Service Control)
    - 基于服务端口号，基于服务器的IP地址等
  - 方向控制(Direction Control)
    - 比如，内部发起的可以通过，但反之不允许
  - 用户控制(Service Control)
    - 基于用户的身份进行控制，特别是允许外部用户访问内部网络，如VPN
  - 行为控制(Service Control)
    - 基于用户的行为进行控制，如Spam Email filter

防火墙的技术分类

- 防火墙技术上划分为四类
  - 网络层：包过滤技术(Packet filtering/screening)
  - 网络层：地址转换(NAT)
  - 传输层：电路层网关(Circuit Gateway)
  - 应用层：应用层代理(Proxy)

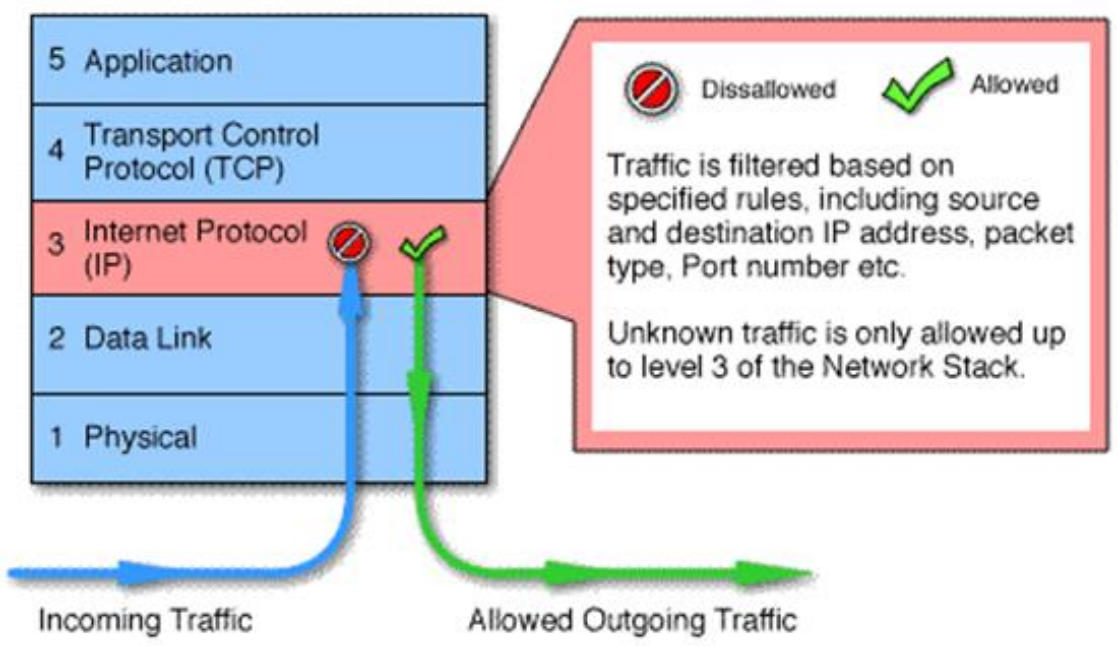


网络层：包过滤技术

- 包过滤技术工作在网络层
- 包过滤路由器依据一套规则对收到的IP包进行处理，决定是转发还是丢弃
- 包过滤技术是一种通用、廉价和有效的安全手段，经历了静态和动态两代
  - 第一代：静态包过滤类型防火墙
  - 第二代：动态包过滤类型防火墙
    - **Checkpoint和Cisco的PIX防火墙为包过滤技术防火墙的代表产品**

网络层：包过滤类型防火墙

- 包过滤类型防火墙几乎是与路由器同时产生的，它是根据定义好的过滤规则审查每个数据包，以便确定其是否与某一条包过滤规则匹配
- 过滤规则基于数据报头信息，对经过的每一个包进行检查：
  - IP 源地址、目标地址
  - ICMP的消息类型
  - TCP/UDP 源端口号、目标端口号
  - 协议 (TCP, UDP,ICMP, BGP等)



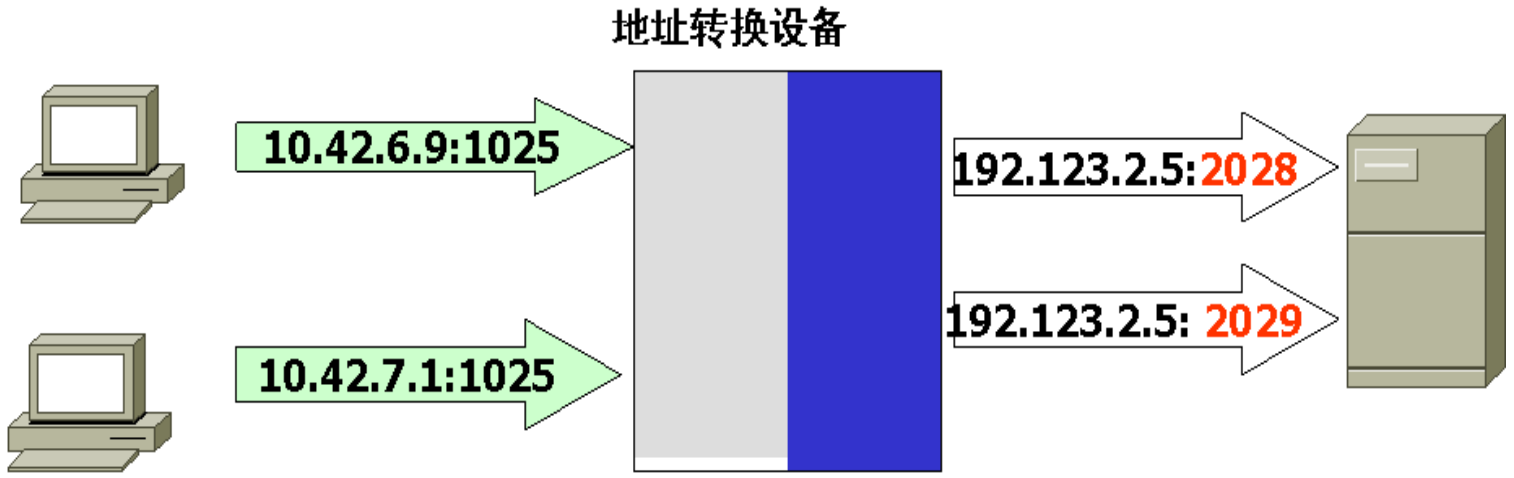
- 常见包过滤设备/软件：路由器中的访问控制表ACL

网络层：包过滤技术的优缺点

- 优点
  - 对应用透明
  - 可以保护所有的服务
  - 相对于高层防火墙，具有较好的网络性能
  - 保持Internet 端到端的特性
  - 无状态，防火墙负载较轻
- 缺点
  - 没有认证功能
  - 无法实施细粒度的访问控制
    不能防范IP地址欺骗
  - 不能防范IP分片攻击

网络层：地址转换NAT

- 类似路由器，工作在网络层；除了转发外，完成地址转换，可以隐蔽内部网络，节省地址空间；但是不能提供额外的安全性



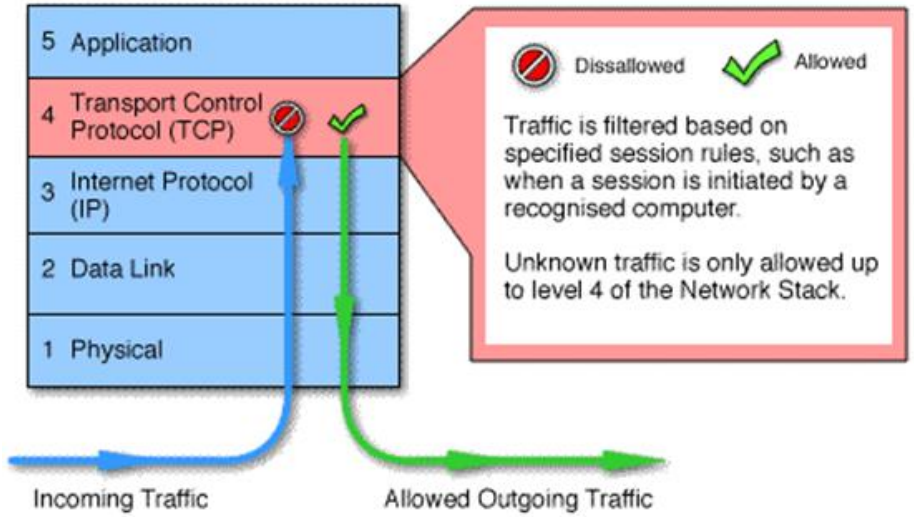
- 转换方式
  - 静态地址转换
  - 动态地址转换
  - 静态地址转换＋端口映射（Port Mapping）
  - 动态地址转换＋端口映射

网络层：地址转换NAT

- 优点
  - 节省IP地址资源
  - 隐蔽内部的网络
- 缺点
  - 地址转换破坏了IP包的完整性，破坏了Internet端到端的特性
  - 动态地址转换必须保留状态，破坏了网络无状态的特性
  - 网络日志变得困难
  - 端口映射使得包过滤变得困难

传输层：电路层网关

- 电路层网关（Circuit Gateway）工作在传输层/会话层
  - 在客户和服务器之间建立了两个连接
  - 对于收到的某个IP包，检查它是否属于某一个连接
  - 不检查内容，不实现应用协议
- 常见设备/软件
  - 商业防火墙硬件/软件
  - 免费软件：Socksd
- 相关标准
  - **rfc1928.txt**

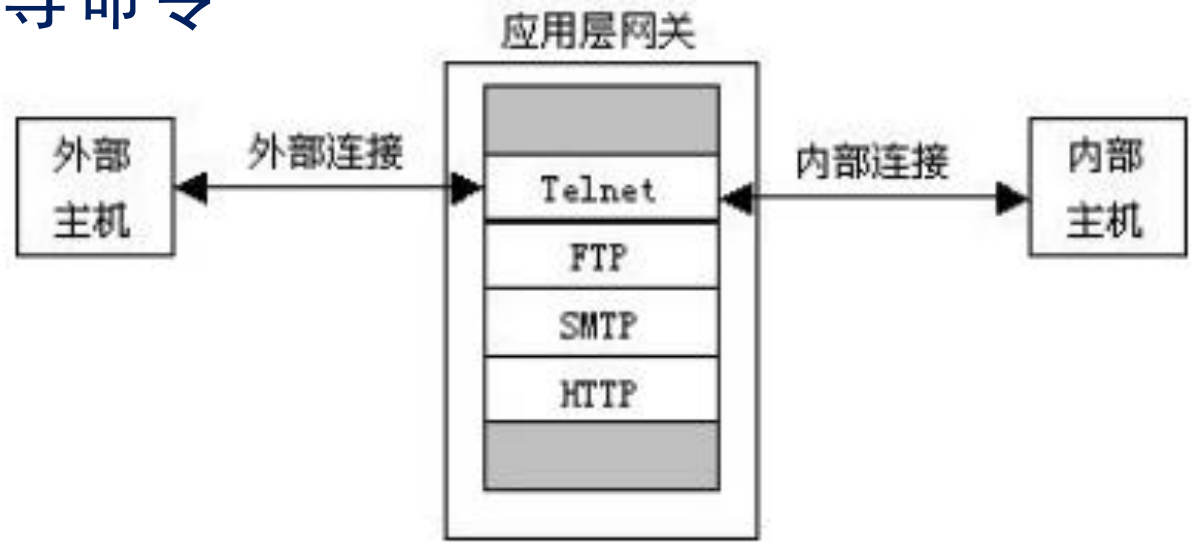


传输层：电路层网关

- 优点
  - 支持所有TCP应用，隐藏内部网络
  - 保持状态，可以检测、防范SYN Flood类型的攻击
- 缺点
  - 不支持UDP的应用
  - 对应用不透明，应用软件必须经过socksified才能使用防火墙
  - 保持状态，可能造成网络中断
  - 性能的开销较大
  - 防火墙本身易受DOS攻击

应用层：应用层代理Proxy

- 应用代理型防火墙工作应用层，其特点是完全“阻隔”了网络流量，对每种应用编制特定的程序，对其实现监视和控制
  - 可以支持身份认证功能
  - 除了基于地址、协议、端口的控制以外，还可以支持应用层命令的过滤，例如FTP的get, put等命令



应用层：应用层代理Proxy

- 优点
  - 功能强大，可以提供用户认证，可以进行细粒度的访问控制
  - 对于Web应用，可以提供内容缓存功能(cache)

- 缺点
  - 协议相关，需要对每一种应用协议编写Proxy程序
  - 必须修改应用程序
  - 通常用软件实现，影响网络性能

防火墙可以做什么

- 防火墙提供了单一阻塞点
  - 可以过滤掉一些潜在的攻击，防止了各种形式的IP欺骗和路由攻击
  - 可以进行用户身份认证、消息认证、数据加密
- 防火墙提供了一个安全事件监控点
  - 可以实施安全检查和警报
  - 可以关闭不使用的端口，禁止特定端口的特定流量，封锁木马等病毒
  - 可以禁止来自特殊站点的访问，防止来自不明入侵者的所有流量
- 防火墙是一个便利的平台
  - 可以方便地提供一些与网络安全无关的功能，
    例如地址转换器、网络管理等
  - 可以作为IPSec的平台，利用隧道模式实现虚拟专用网络

防火墙不可以做什么

- 防火墙需要用户定义访问控制规则，没有缺省配置
- 防火墙不能防止内部恶意的攻击者
- 防火墙无法控制没有经过它的连接
- 防火墙不能很好地防止病毒和信息扩散
- 防火墙不能替代内部网络系统的安全管理
- 防火墙无法防范全新的威胁和攻击

1911–2021
清華大學 110周年校庆
110th ANNIVERSARY
TSINGHUA UNIVERSITY

防火墙的配置结构

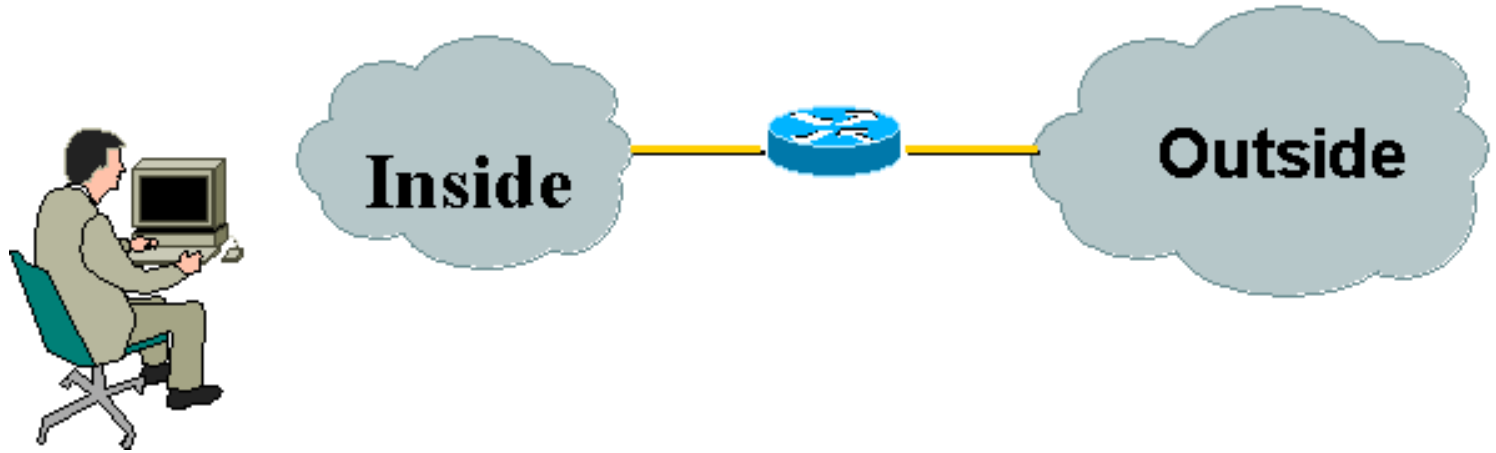
单盒、屏蔽主机、屏蔽子网

防火墙的配置结构

- 单盒结构(Single-Box Architecture)
- 屏蔽主机结构(Screened Host Architecture)
- 屏蔽子网结构(Screened Subnet Architecture)

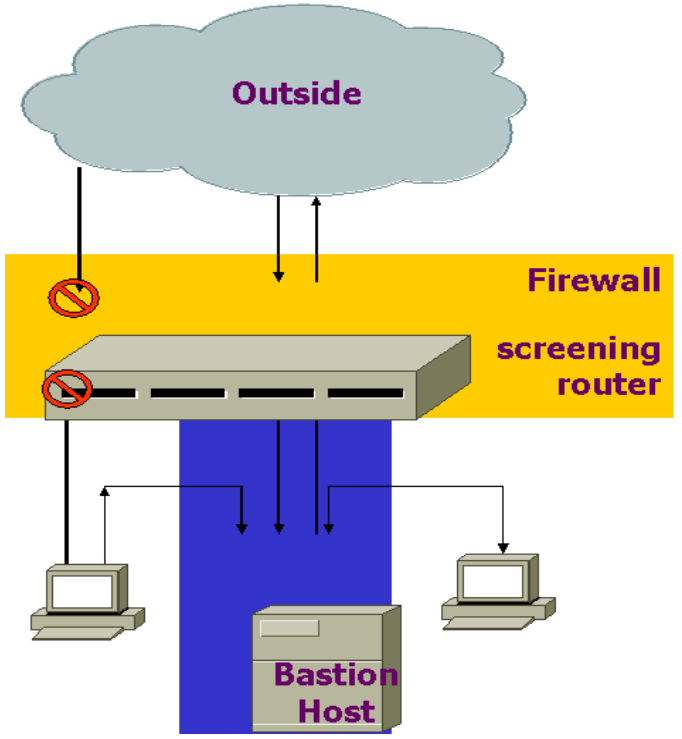
单盒结构

- 屏蔽路由器：简单的包过滤功能
  - 优点：投资小，配置简单，没有增加单一故障点
  - 缺点：在访问控制列表ACL较多时，影响路由器的性能
- 适用于如下环境
  - 网络内部的主机安全性比较好，规则简单
  - 对性能、可靠性要求比较高

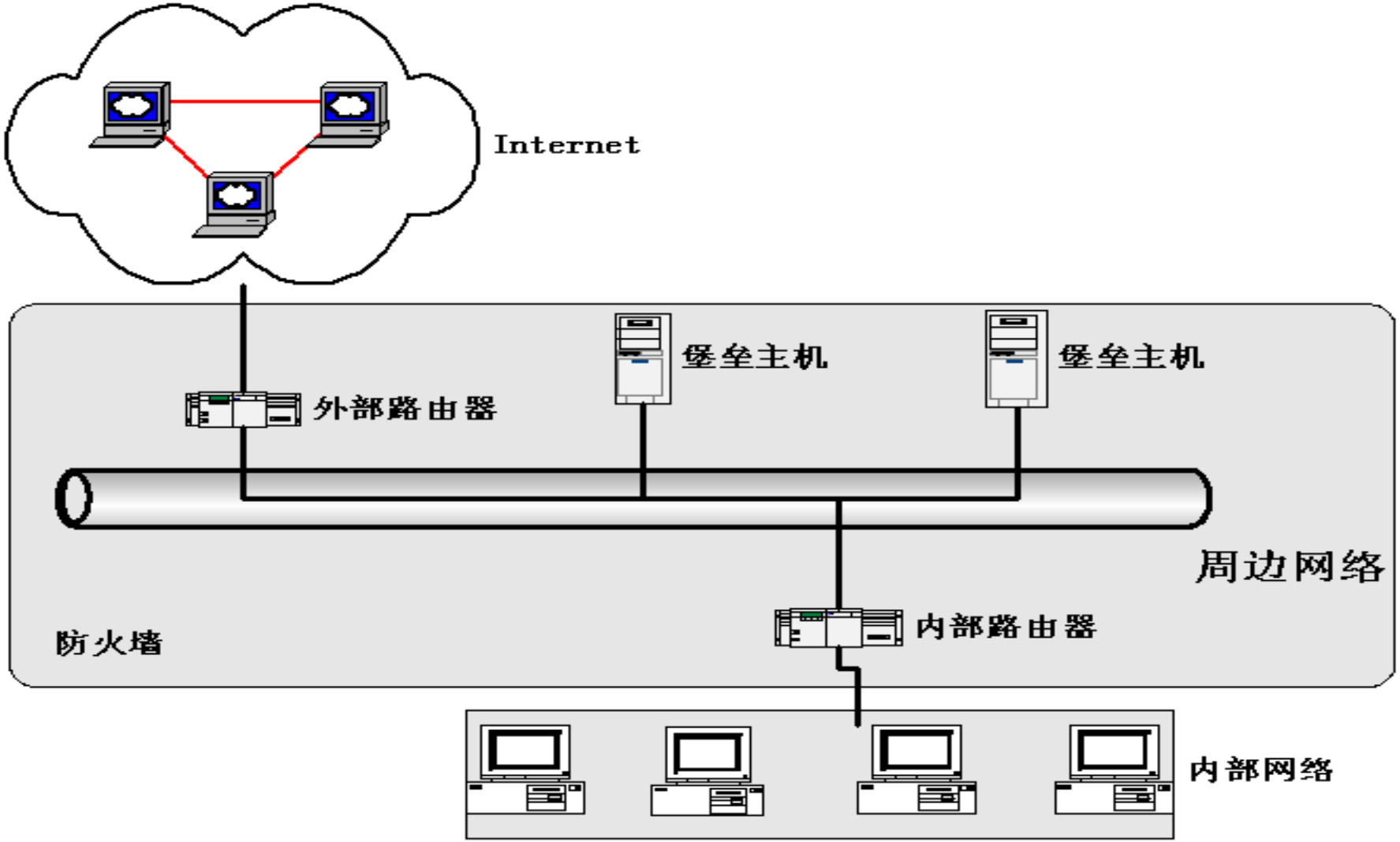


屏蔽主机结构

- 屏蔽主机模式由包过滤路由器和堡垒主机组成：
  - 堡垒主机：一种配置了安全防范措施的联网计算机，为网络通信提供了一个阻塞点
  - 堡垒主机在网络内部，通过防火墙的过滤使得这个主机是唯一可从外部到达的主机
  - 过滤路由器是否配置正确是这种防火墙安全的关键
- 适用于
  - 只对外提供较少的服务，外部连接比较少
  - 内部主机安全性配置较好



屏蔽子网结构

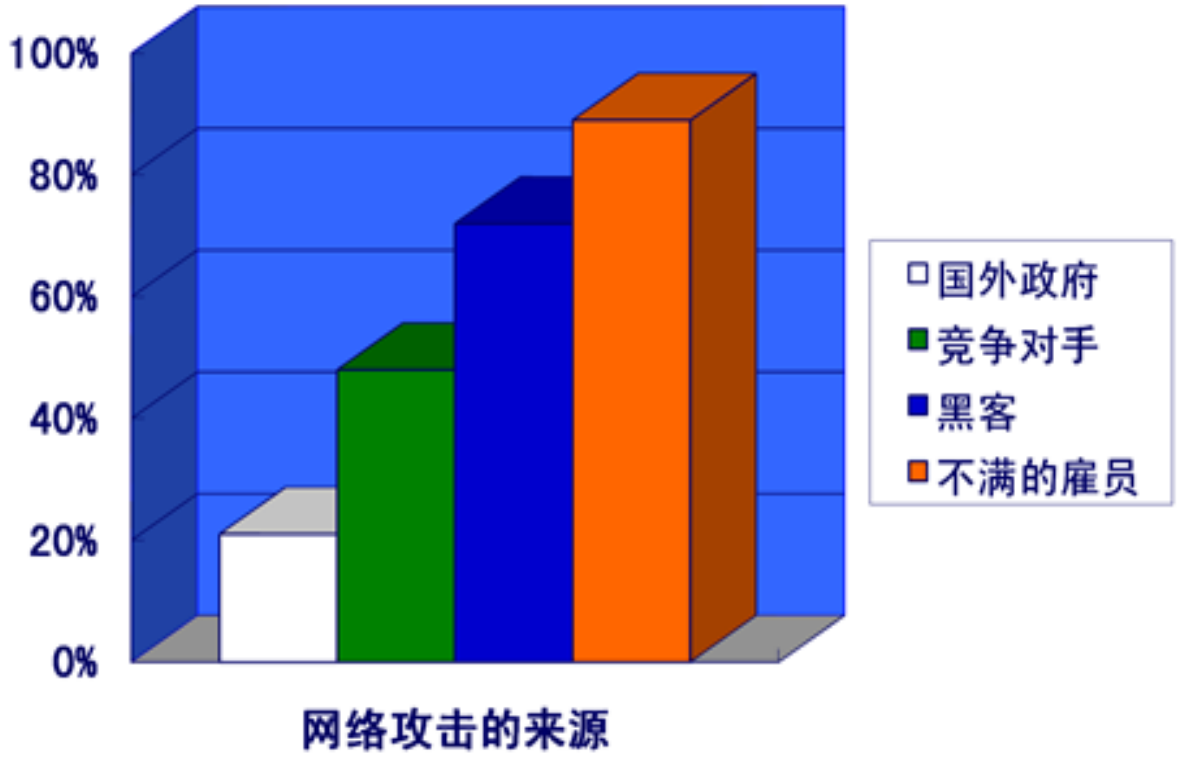


屏蔽子网结构

- DMZ(Demilitarized zone), 不设防区
  - 通常放置DNS/Web/Email/FTP/Proxy Server等
- 外部路由器
  - 只允许互联网对DMZ的访问
  - 拒绝所有目的地址为内部网络地址的包
  - 拒绝所有不以内部网络地址为源地址的包进入互联网
- 内部路由器
  - 保护内部网络，防止来自Internet或DMZ的访问
  - 内部网络一般不对外部提供服务，所以拒绝外部发起的一切连接，只允许内部对外的访问

关于防火墙的争论

- 防火墙破坏了Internet端到端的特性，阻碍了新应用的发展
- 防火墙有先天性不足：没有解决网络内部的安全问题，防外不防内
- 防火墙给人一种误解，降低了人们对主机安全的意识



1911–2021
清華大學 110周年校庆
110th ANNIVERSARY
TSINGHUA UNIVERSITY

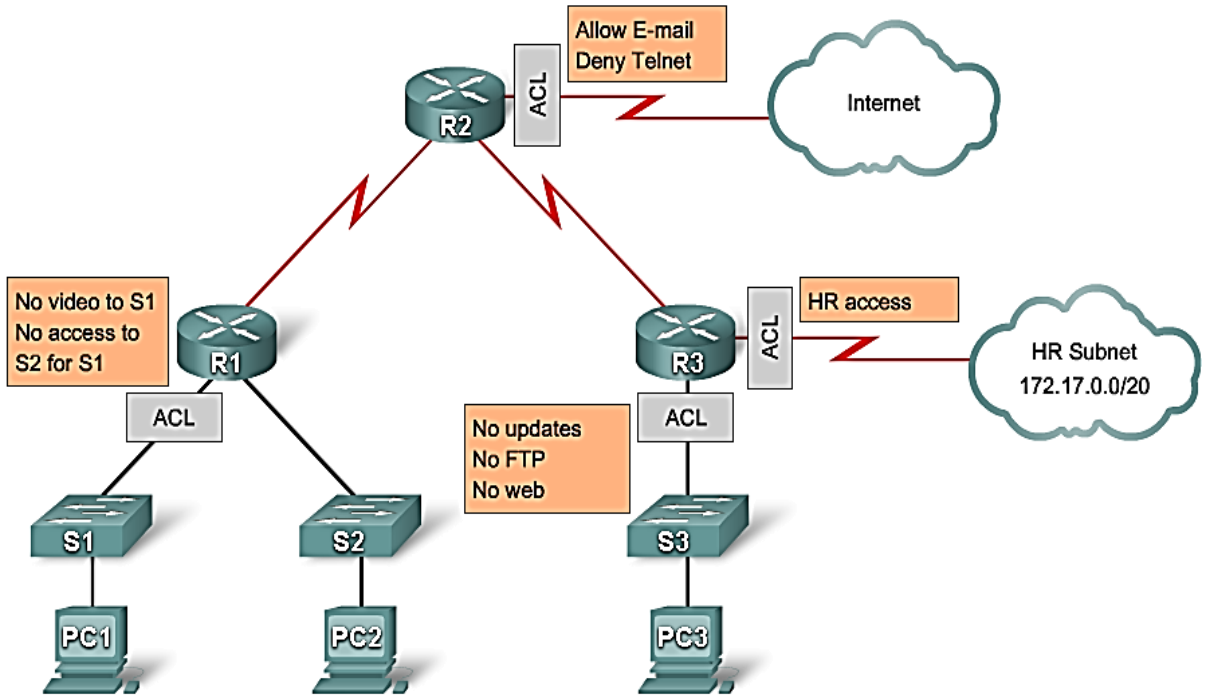
访问控制列表ACL

以Cisco路由器的配置命令为例

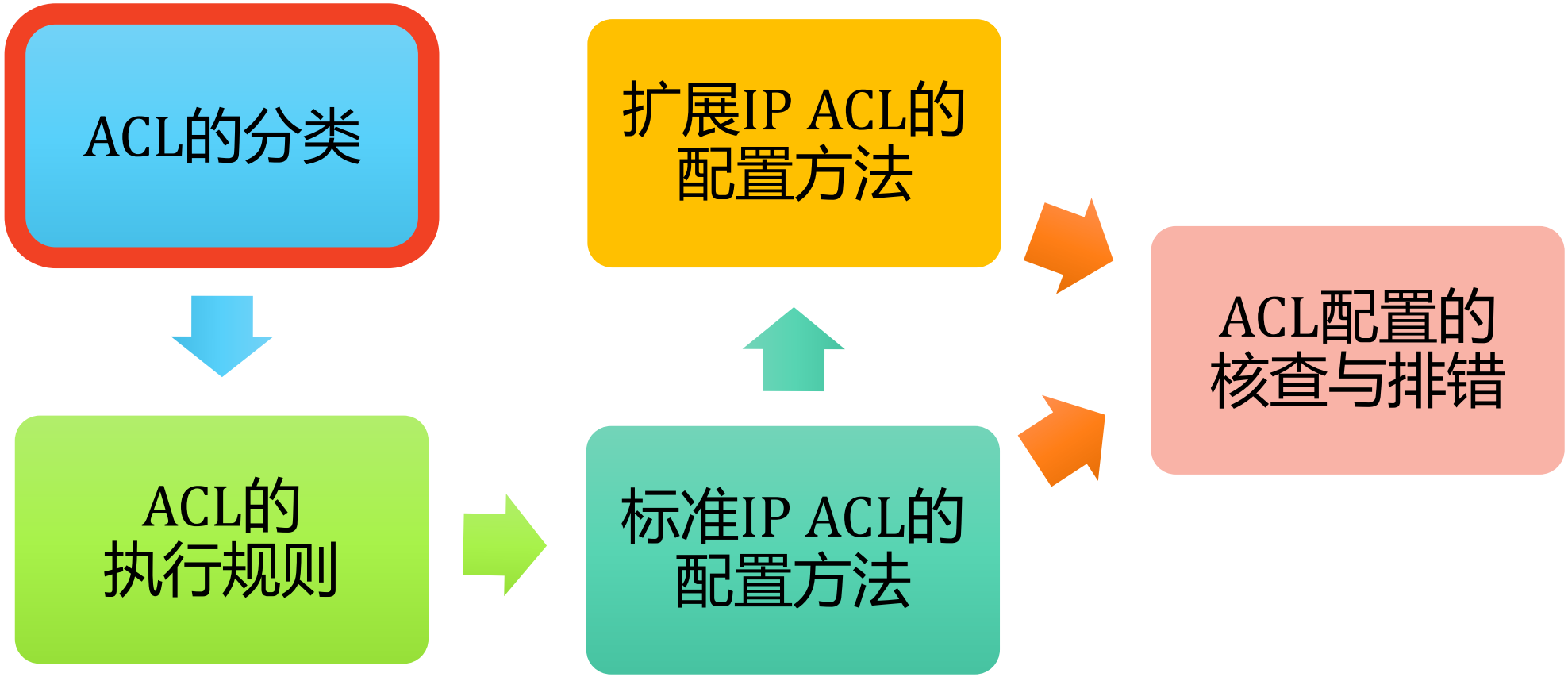
什么是访问控制列表ACL?

- 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



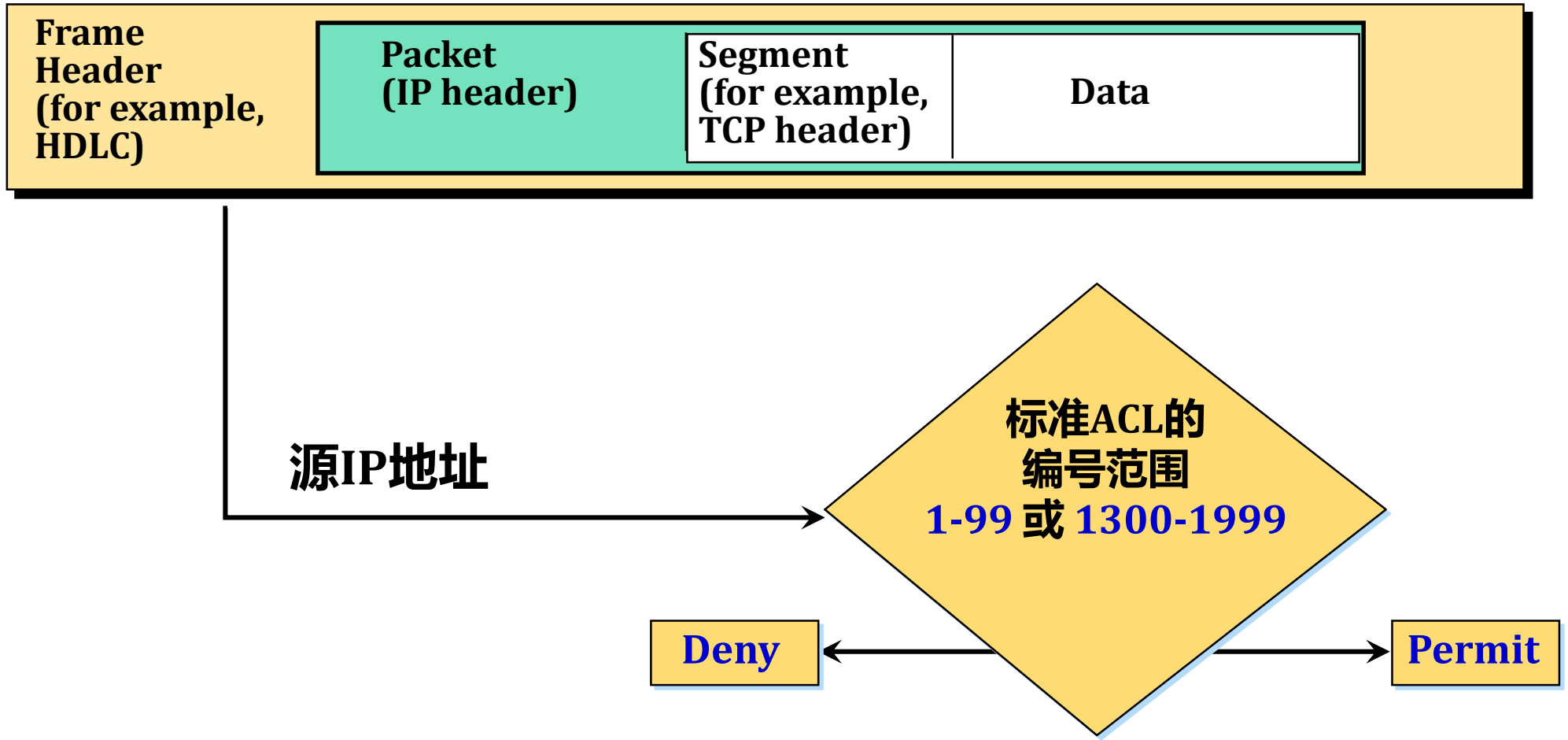
ACL的分类

- 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)

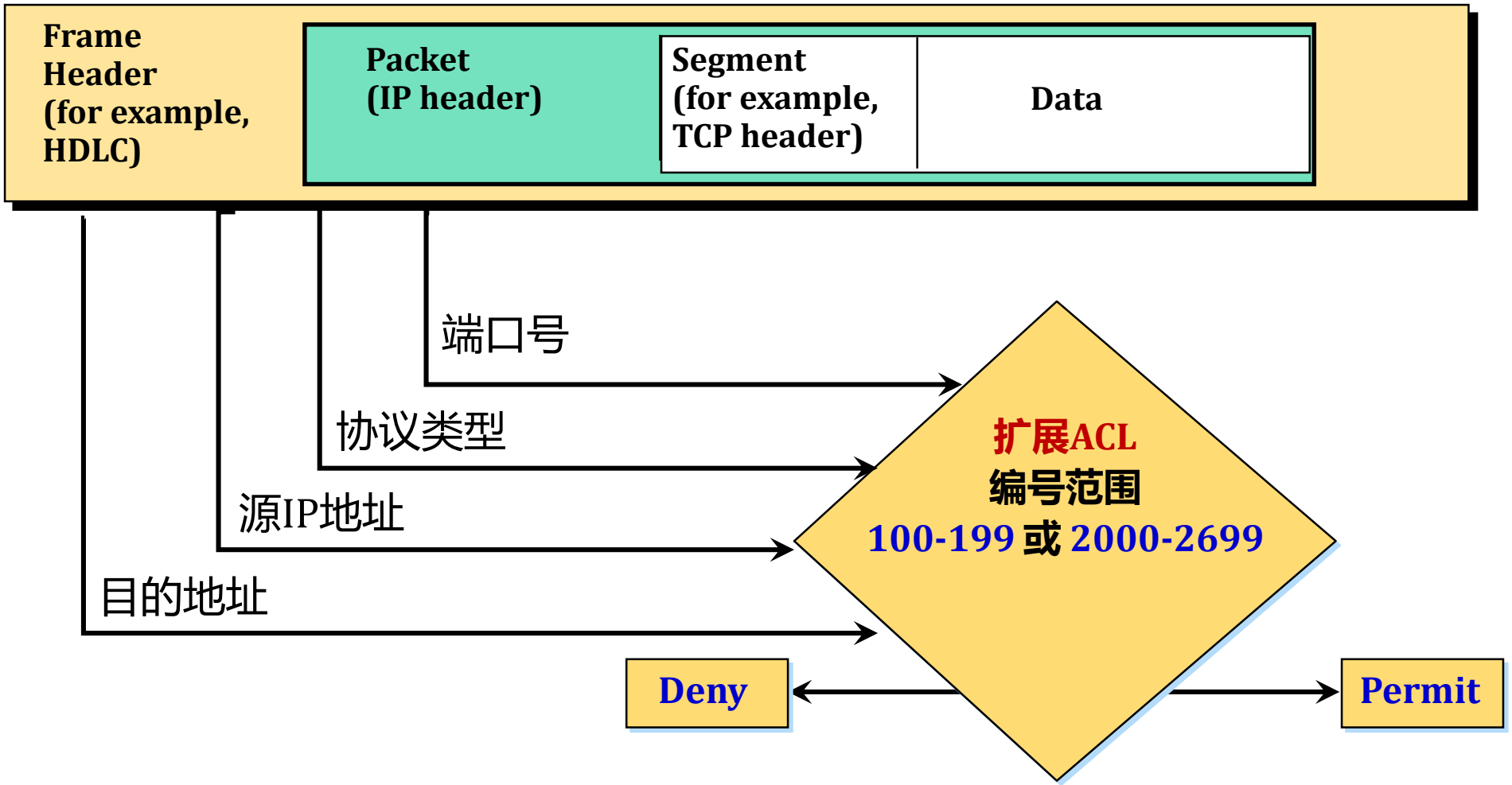
标准ACL的检查内容

TCP/IP数据包的结构图

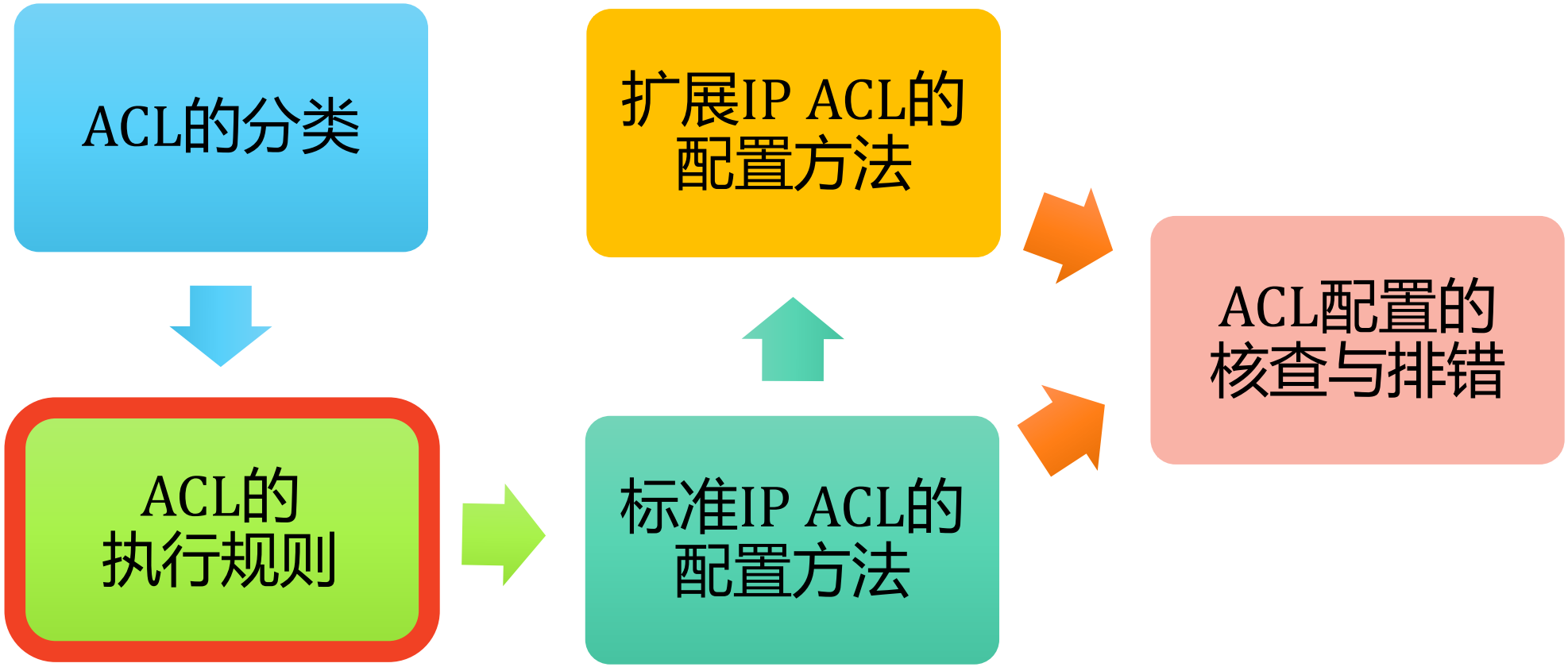


扩展ACL的检查内容

TCP/IP数据包的结构图

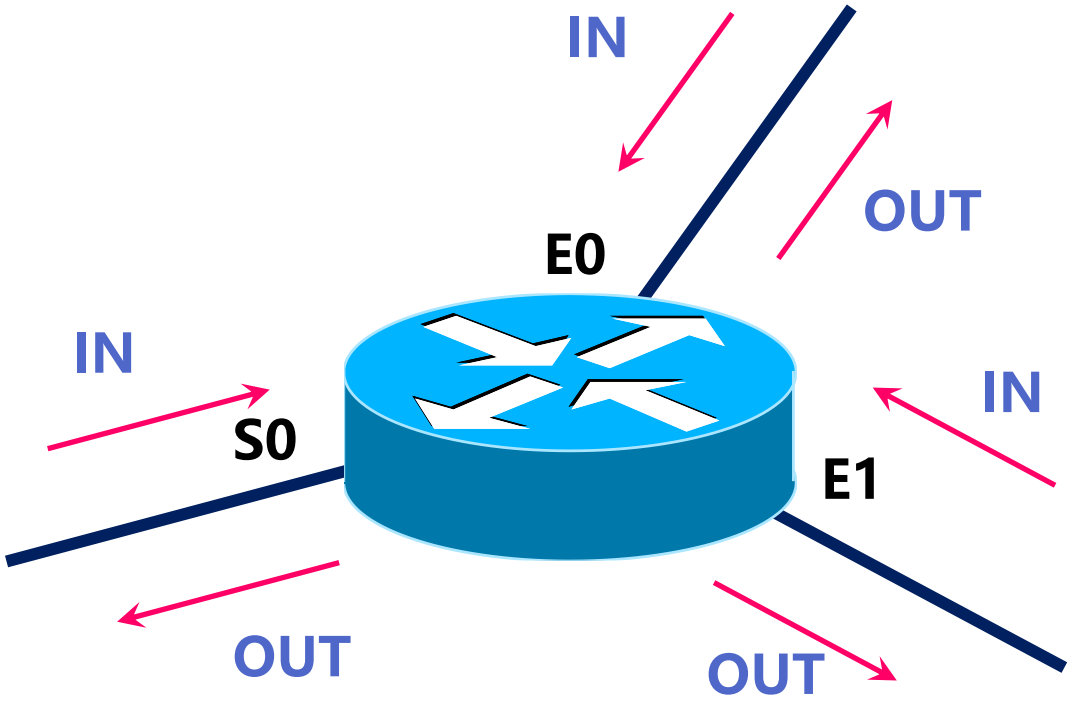


访问控制列表ACL



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

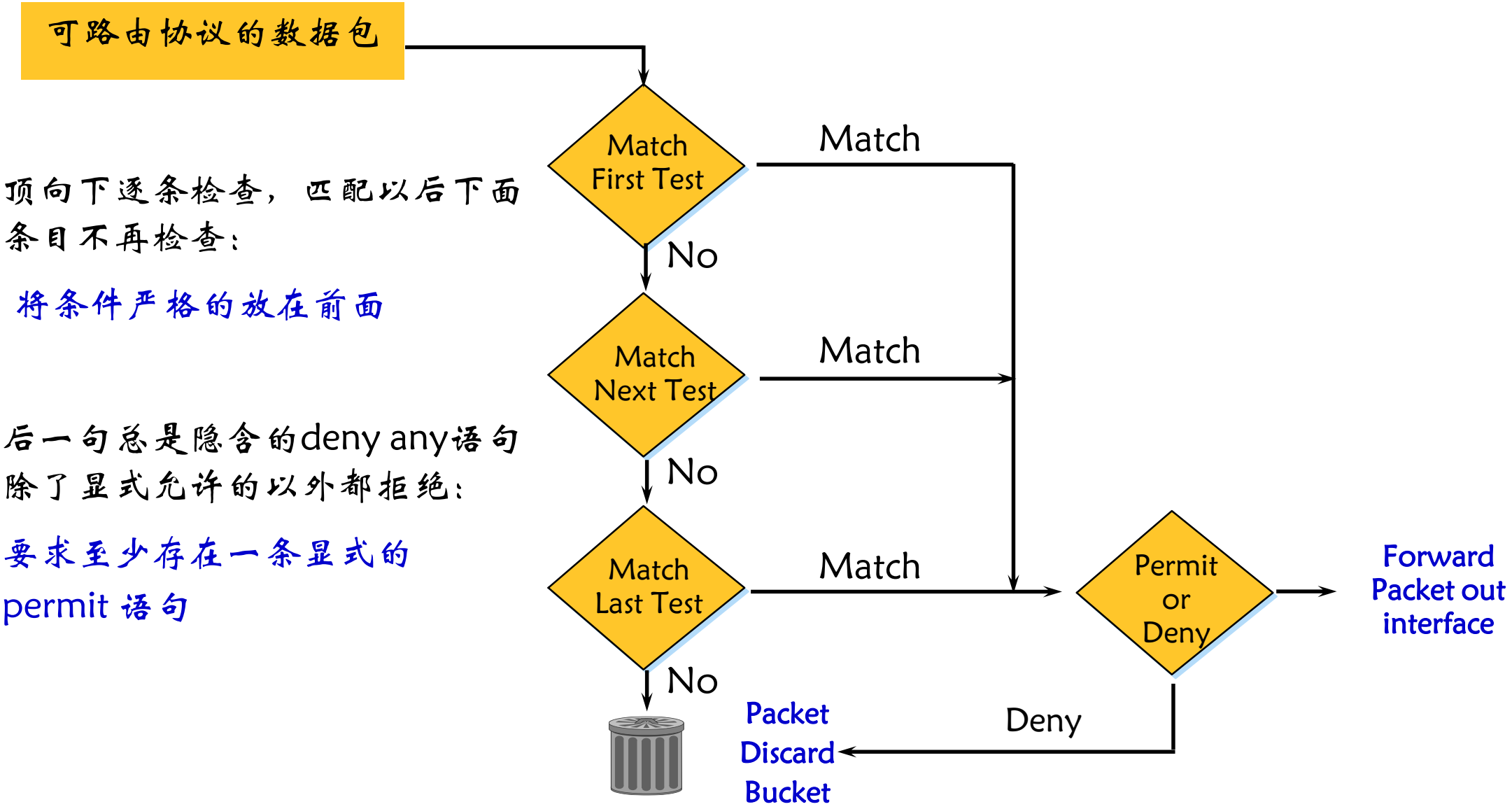
ACL的检查顺序

- 自顶向下逐条检查，匹配以后下面的条目不再检查：

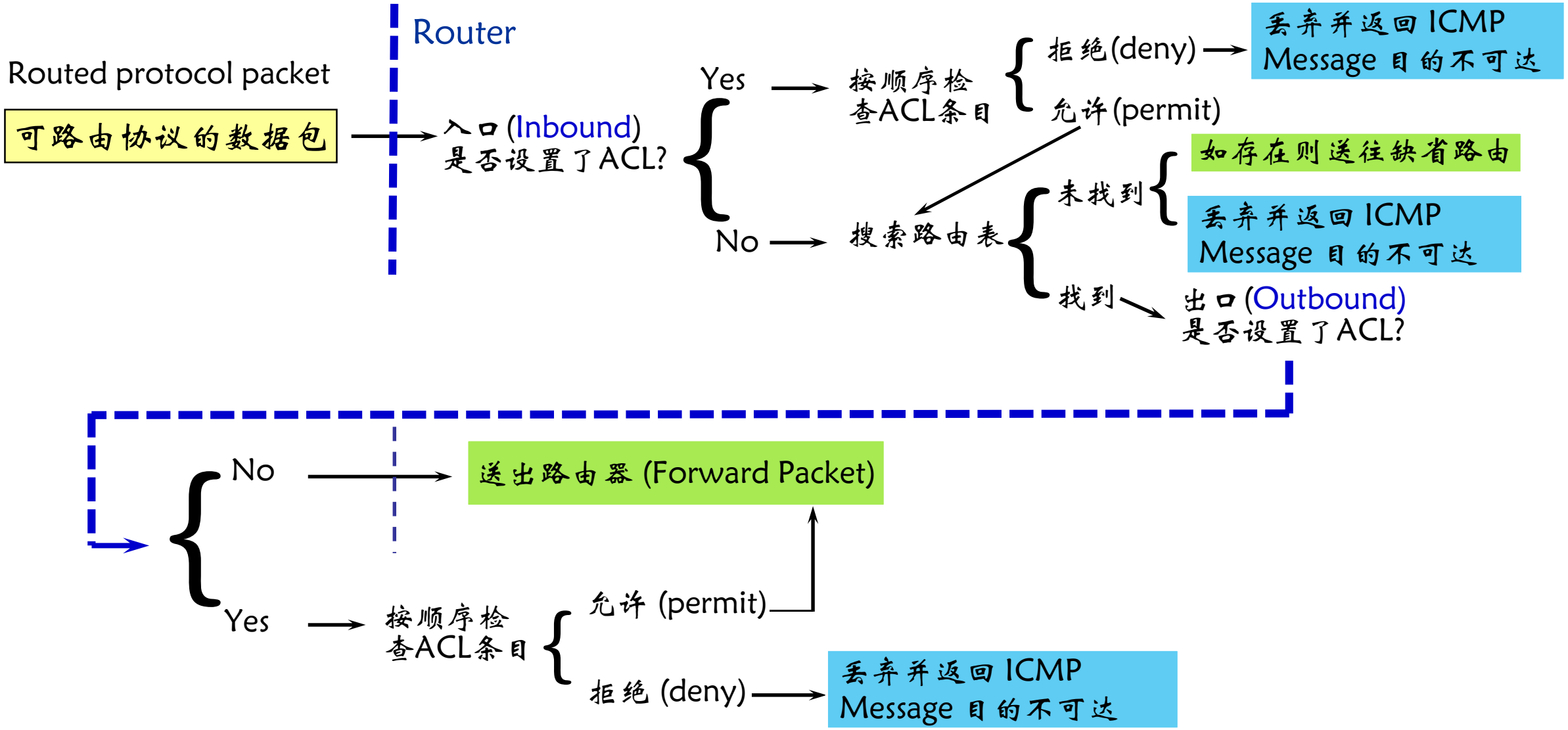
  将条件严格的放在前面

- 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：

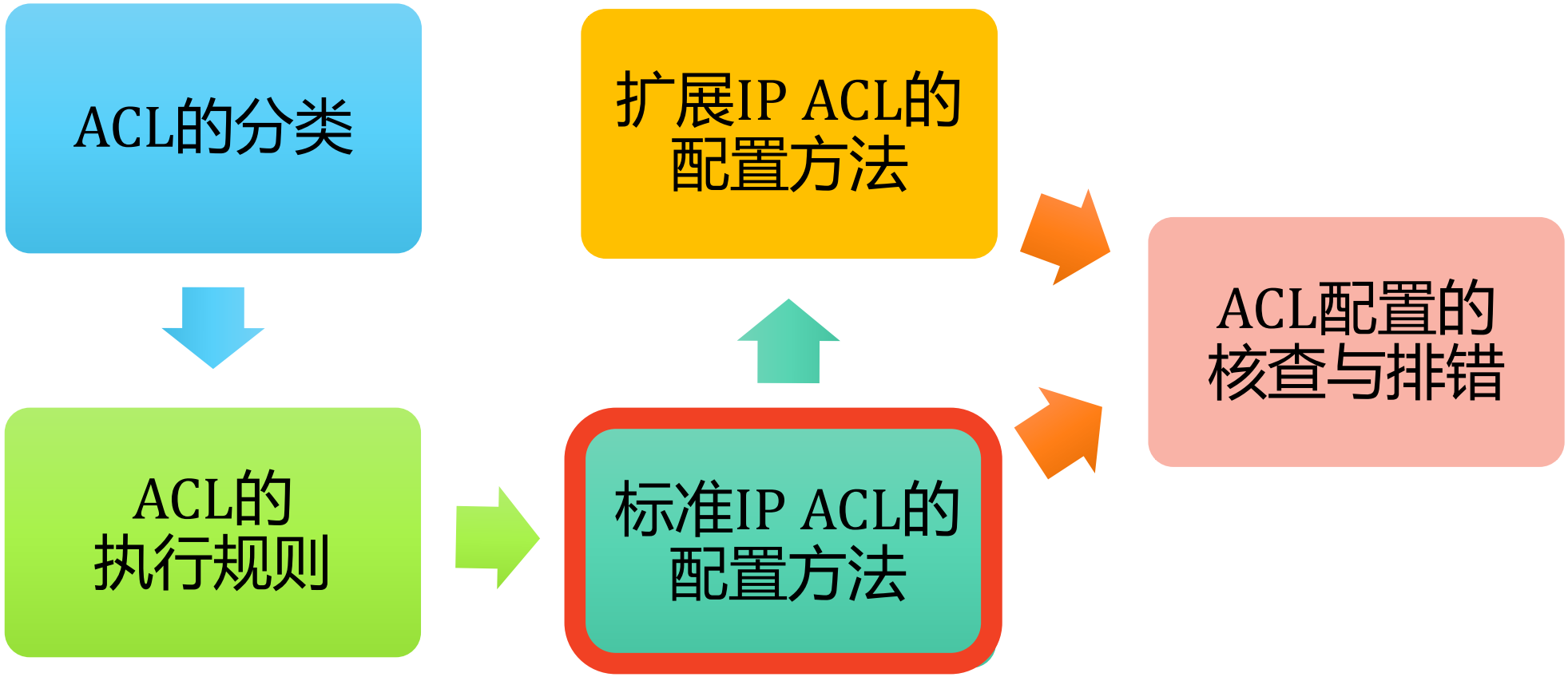
  要求至少存在一条显式的permit 语句



ACL与路由的相互关系



访问控制列表ACL



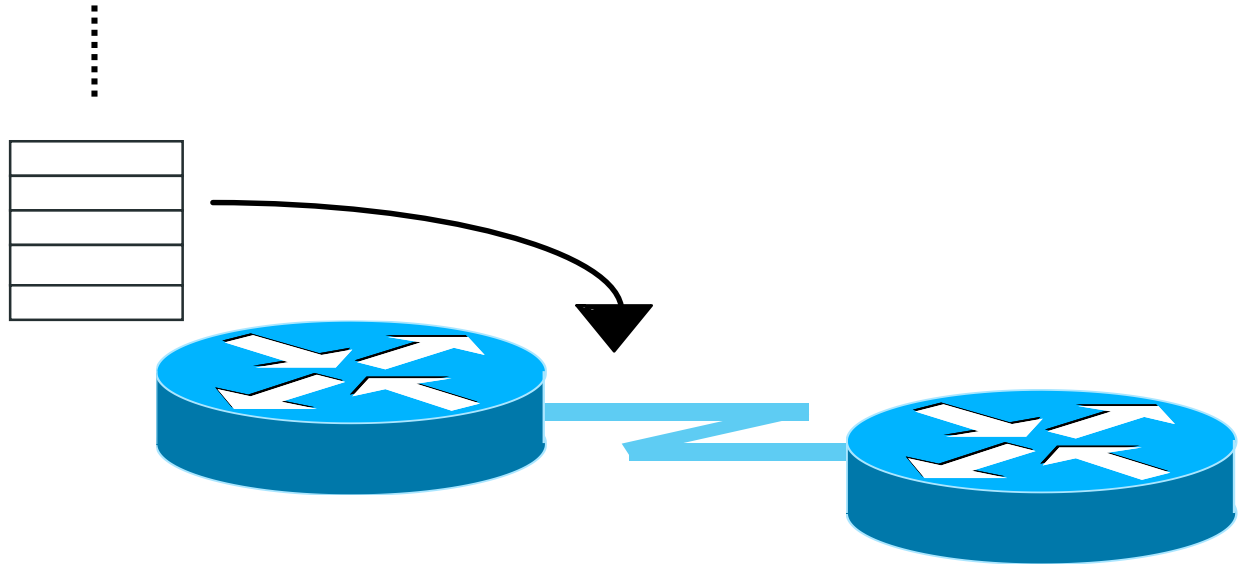
ACL的配置步骤

- 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 }
```

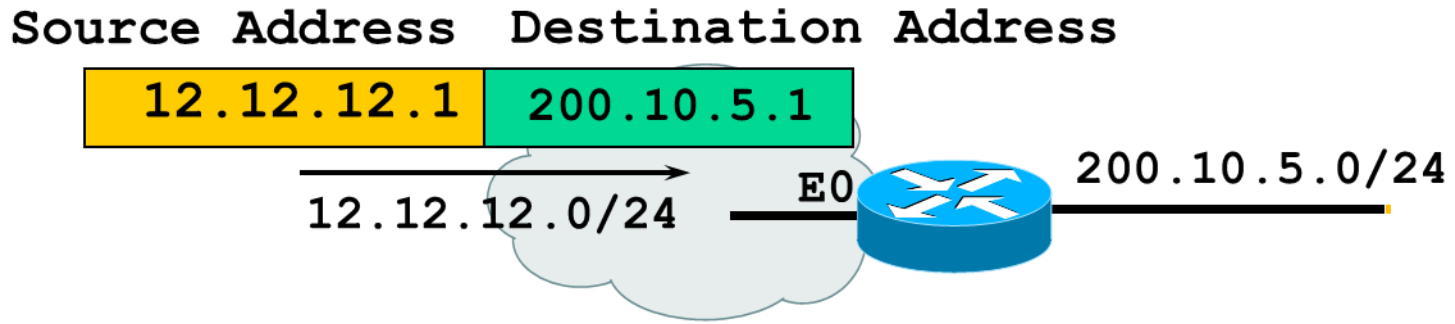
  - Log (可选参数) 将匹配该条目的数据包数量信息发送到控制台，间隔5分钟发送一次

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

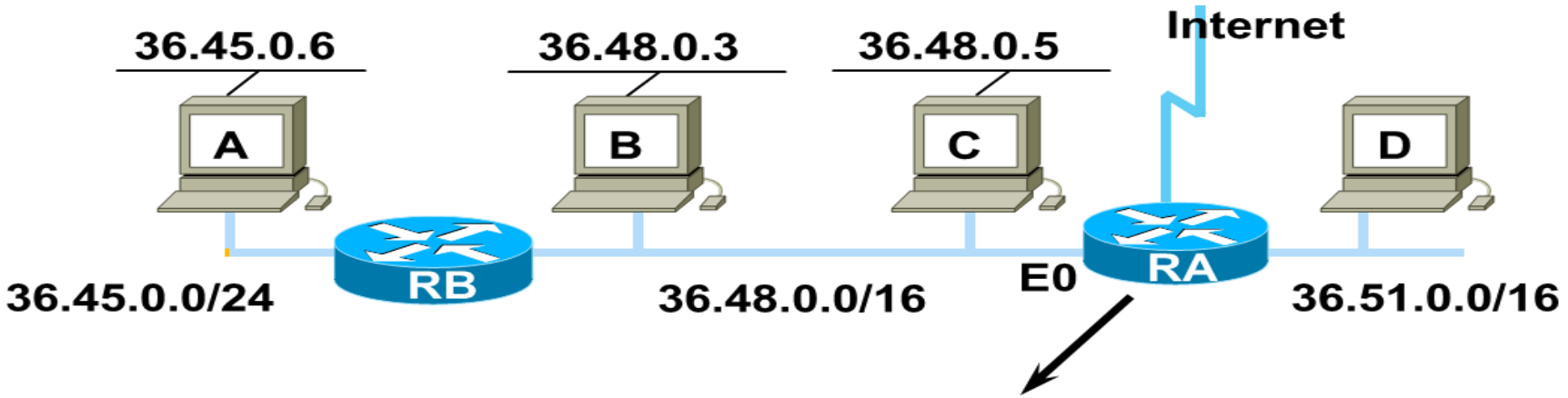
ACL的工作过程




```
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
```

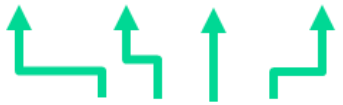
```
RA(config)# access-list 1 permit 36.48.0.0 0.0.255.255
RA(config)# access-list 1 deny 36.48.0.3 0.0.0.0
RA(config)# interface ethernet 0
RA(config-if)# ip access-group 1 in
```

→ 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：

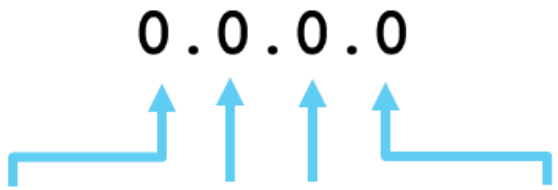
```
access-list 1 permit  host  172.30.16.29
```

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
```

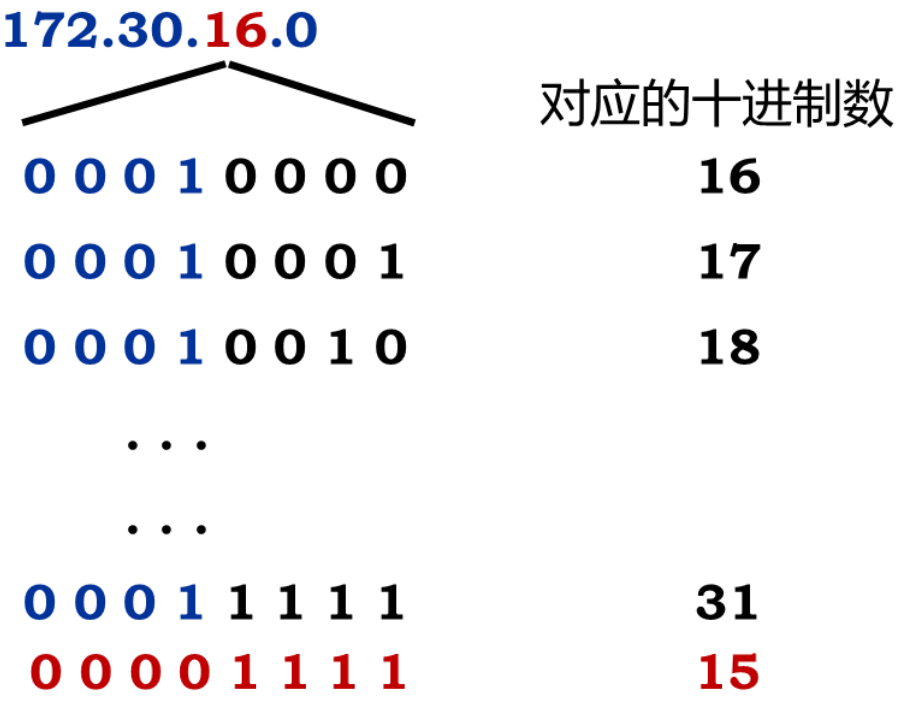
可使用关键字 any 表示为：

```
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

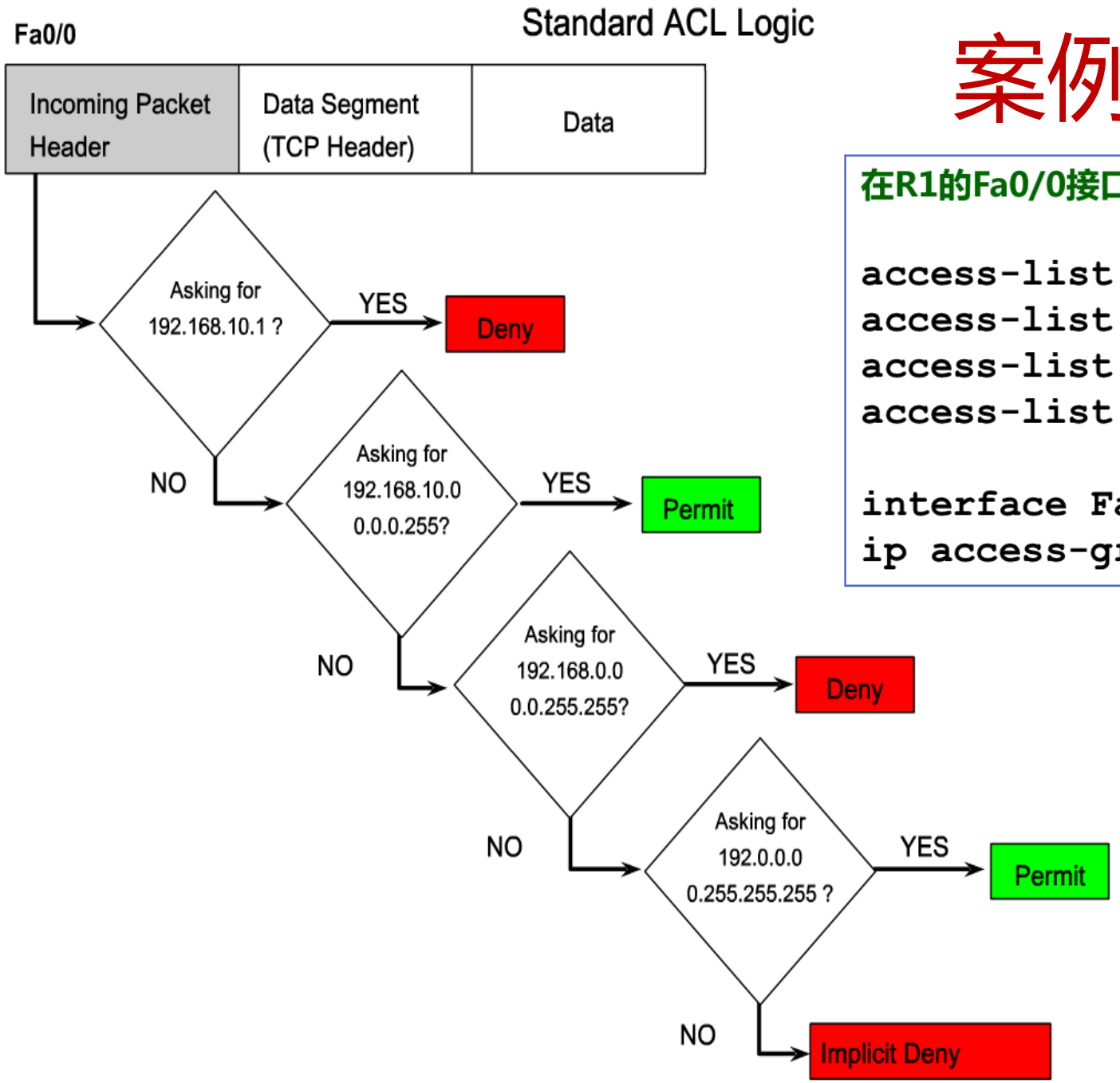
00001010	10
00001011	11
00001100	12
00001101	13
00001110	14
00001111	15

	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
```

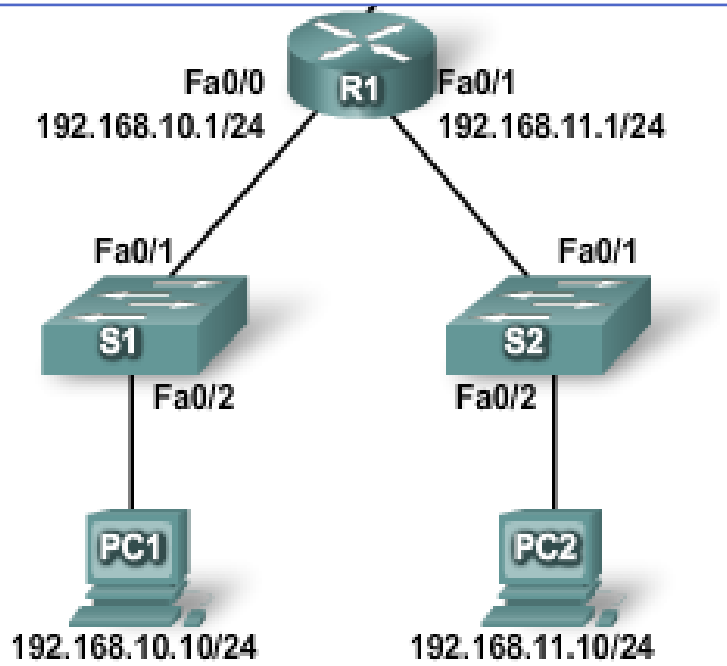
案例4：标准IP ACL配置



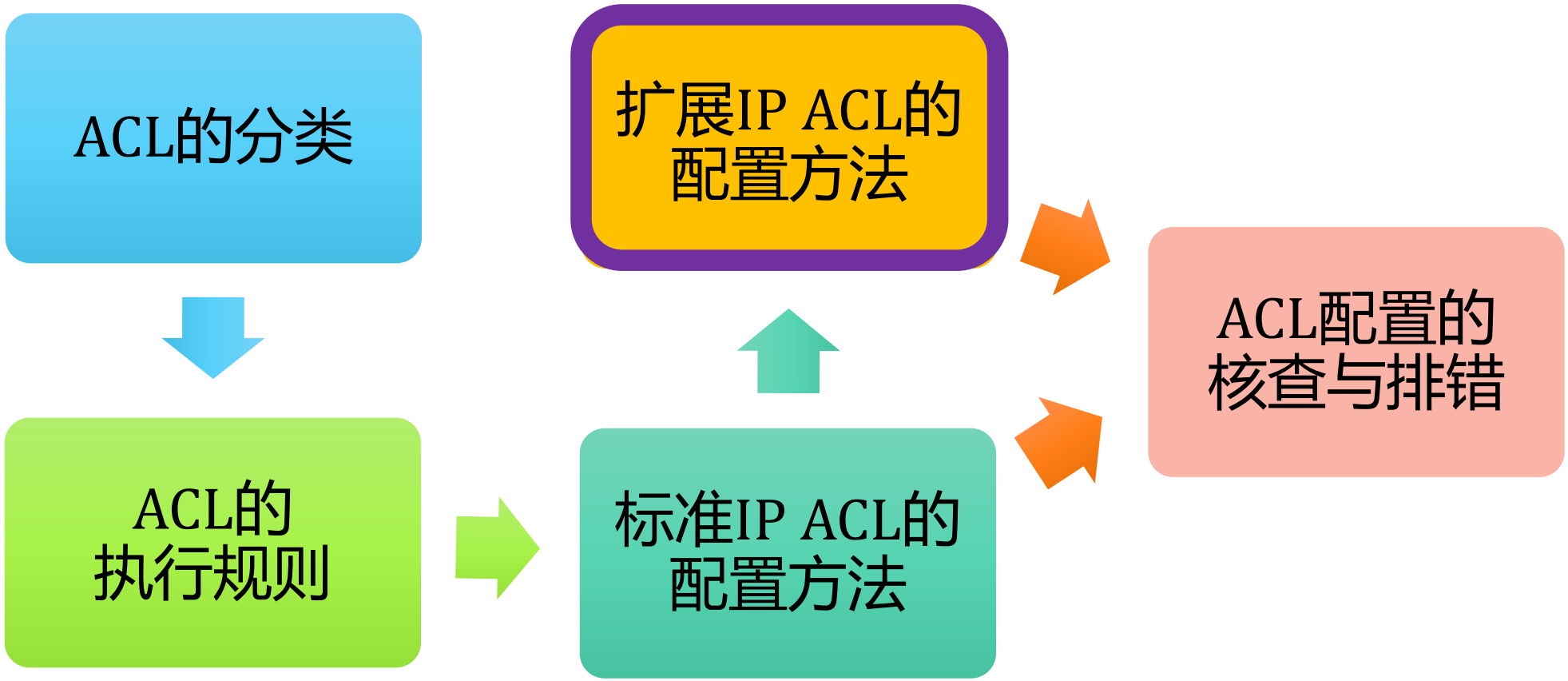
在R1的Fa0/0接口的入方向设置下列标准IP ACL:

```
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
```

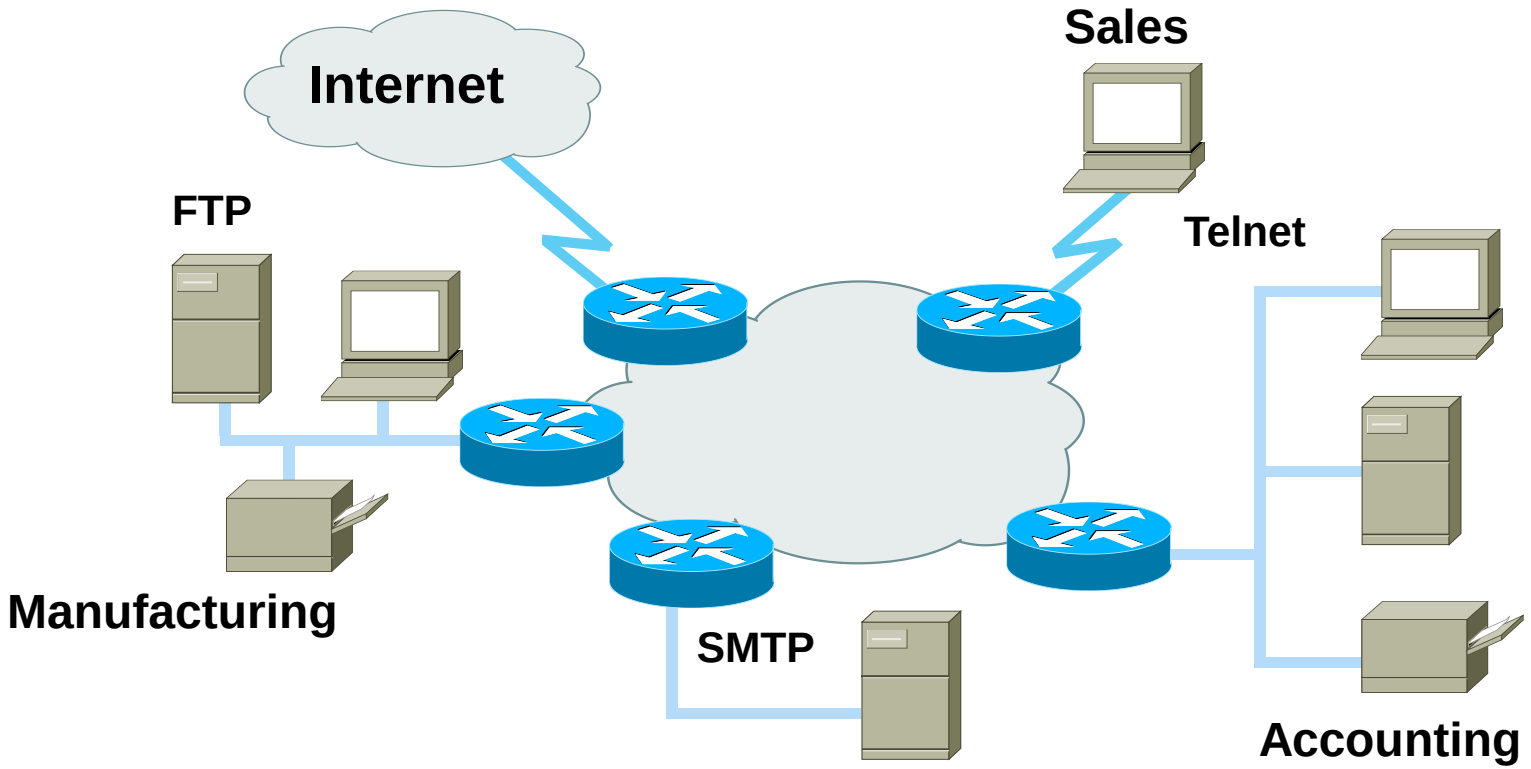


访问控制列表ACL



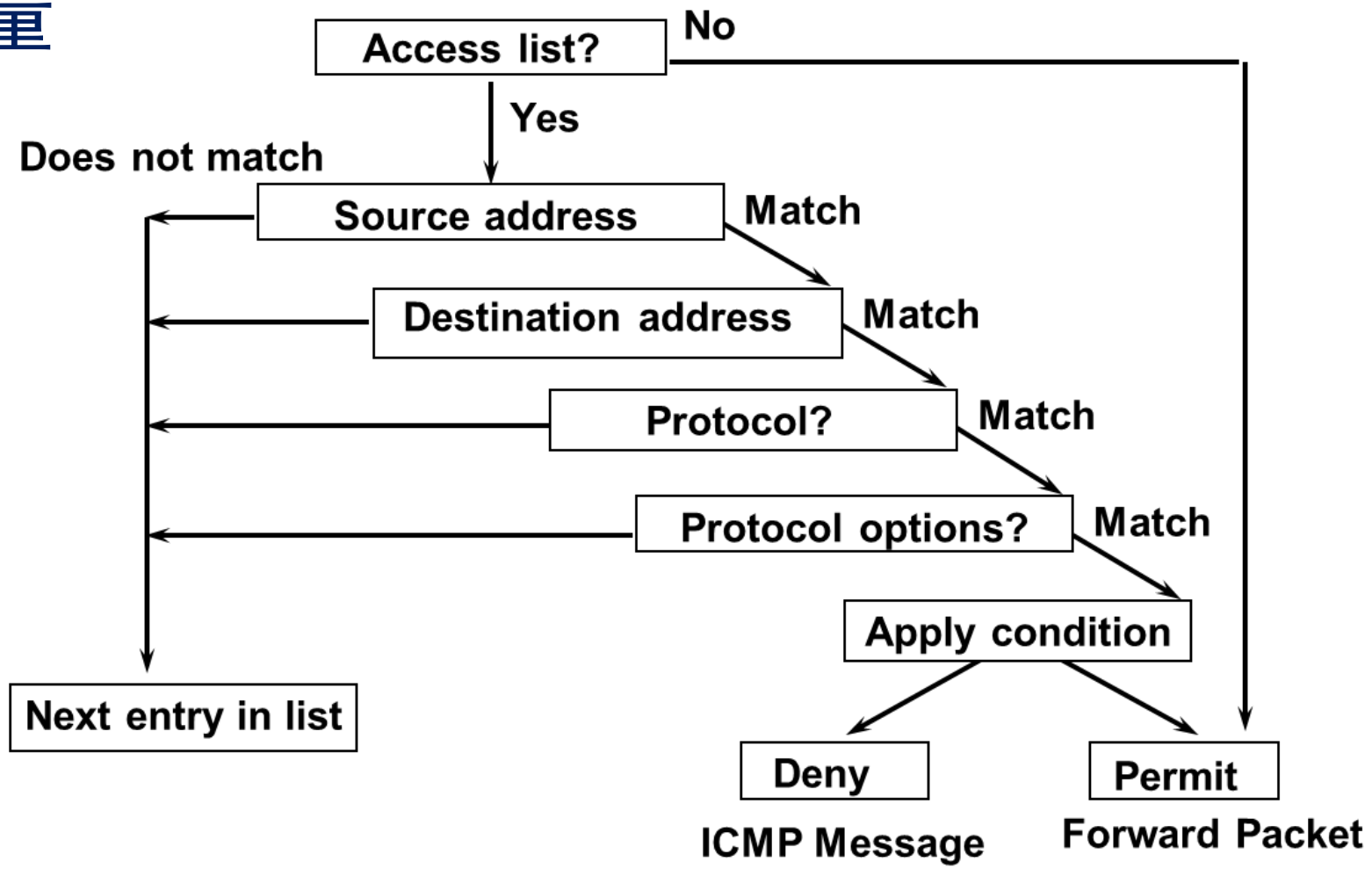
标准IP ACL的局限性

- 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 .

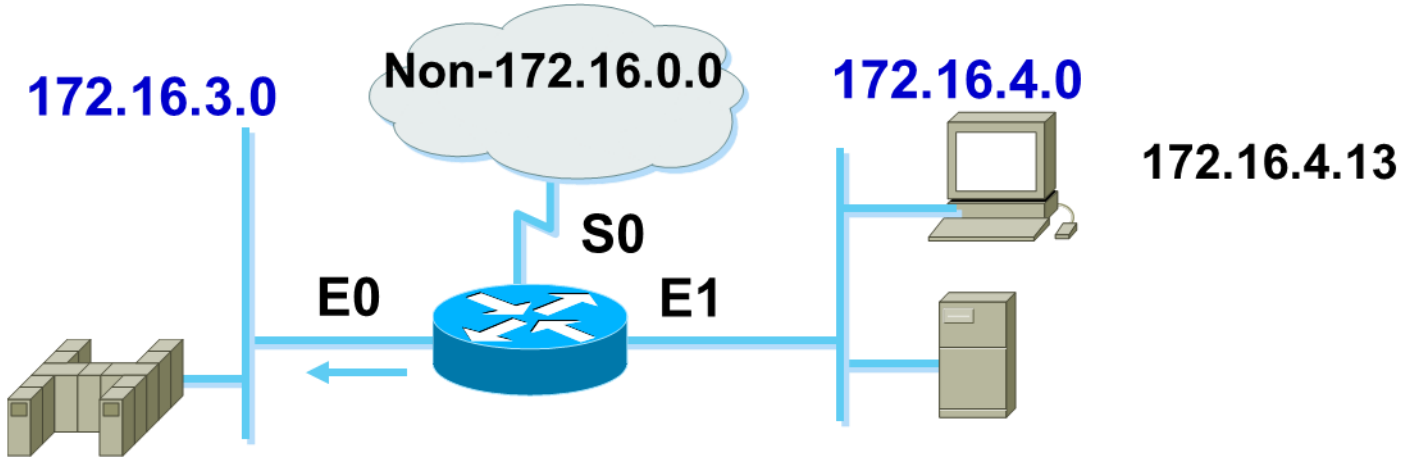
TCP端口号对应的协议

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

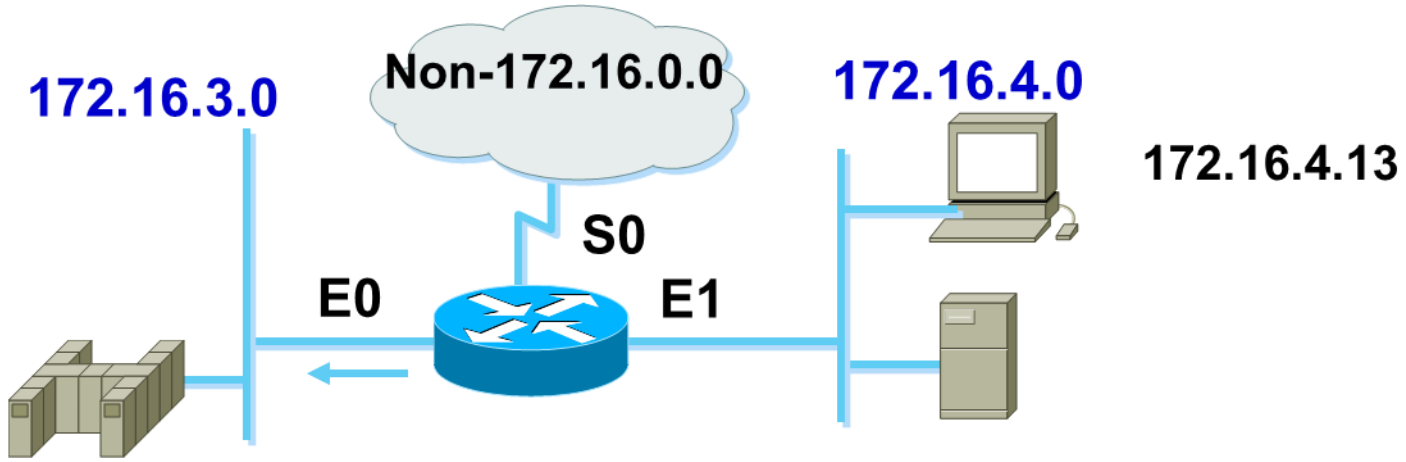
Router (config) #

```
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 ]
```

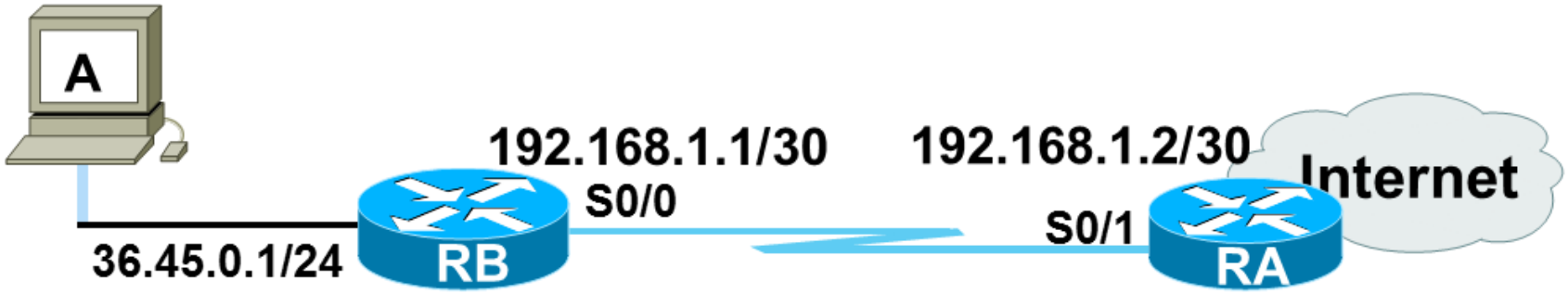
*icmp-type*参见下一页内容

- 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？



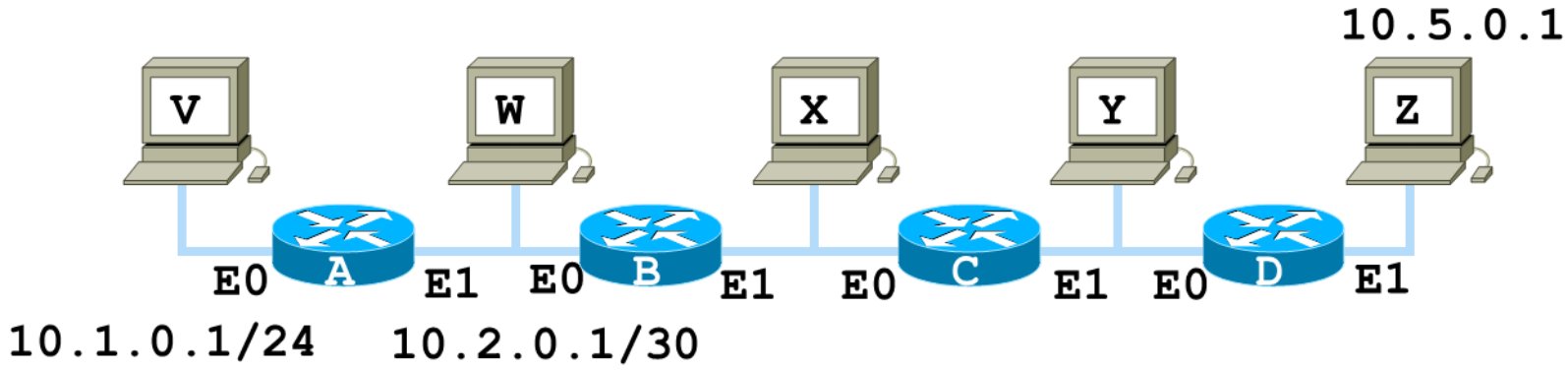

```
RB(config)# access-list 100 deny icmp any host 192.168.1.1
RB(config)# access-list 100 deny icmp any host 36.45.0.1
RB(config)# access-list 100 permit ip any any
RB(config)# interface S0/0
RB(config-if)# ip access-group 100 in
```

命名式ACL

- Cisco IOS 版本号11.2 及其后续版本支持命名式ACL 。
- 命名式ACL的名字必须唯一且区分大小写。
- 命名式ACL的名字可以是纯字母或字母与数字的组合，也可以是纯数字形式(即编号式ACL属于命名式ACL的子集)
- 编号式ACL不能单独删除一行语句，而命名式ACL能够单独删除一行。

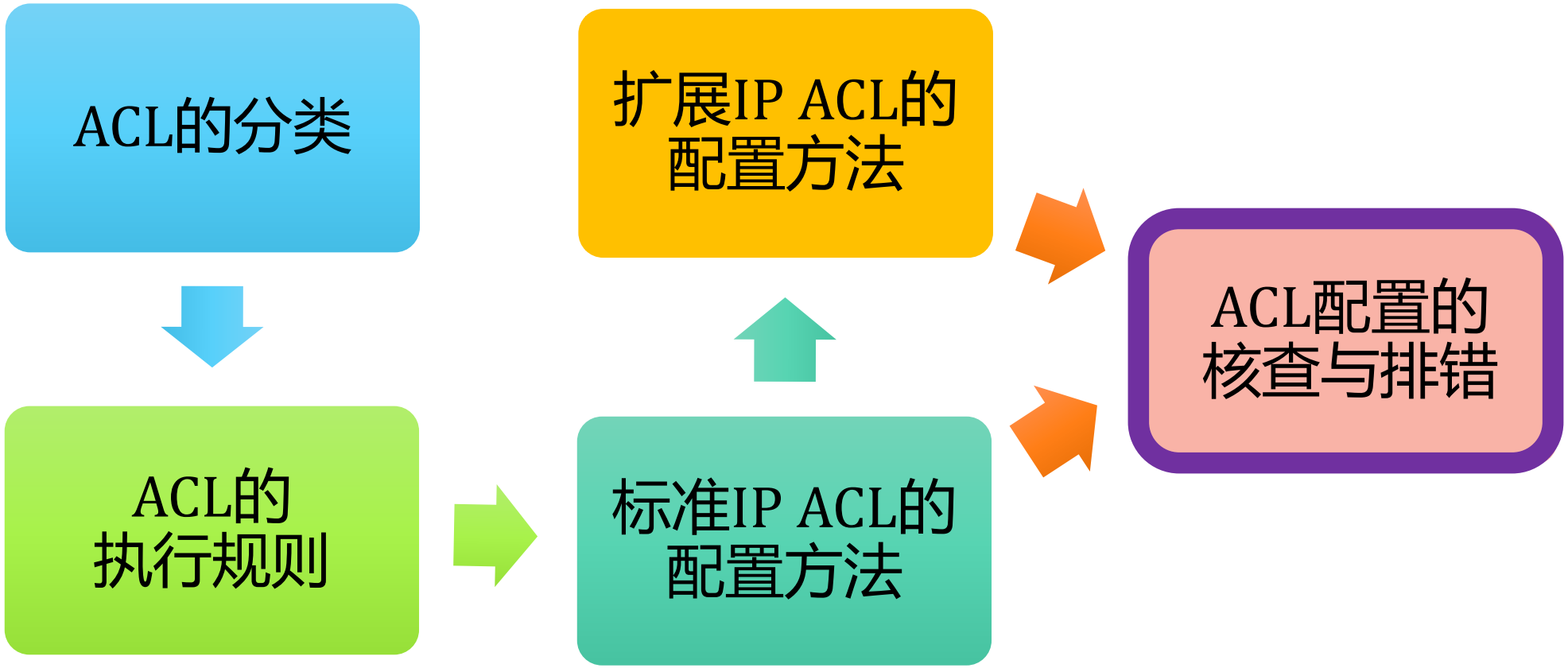
案例：ACL

- 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

1911–2021
清華大學 110周年校庆
110th ANNIVERSARY
TSINGHUA UNIVERSITY

虚拟局域网VLAN

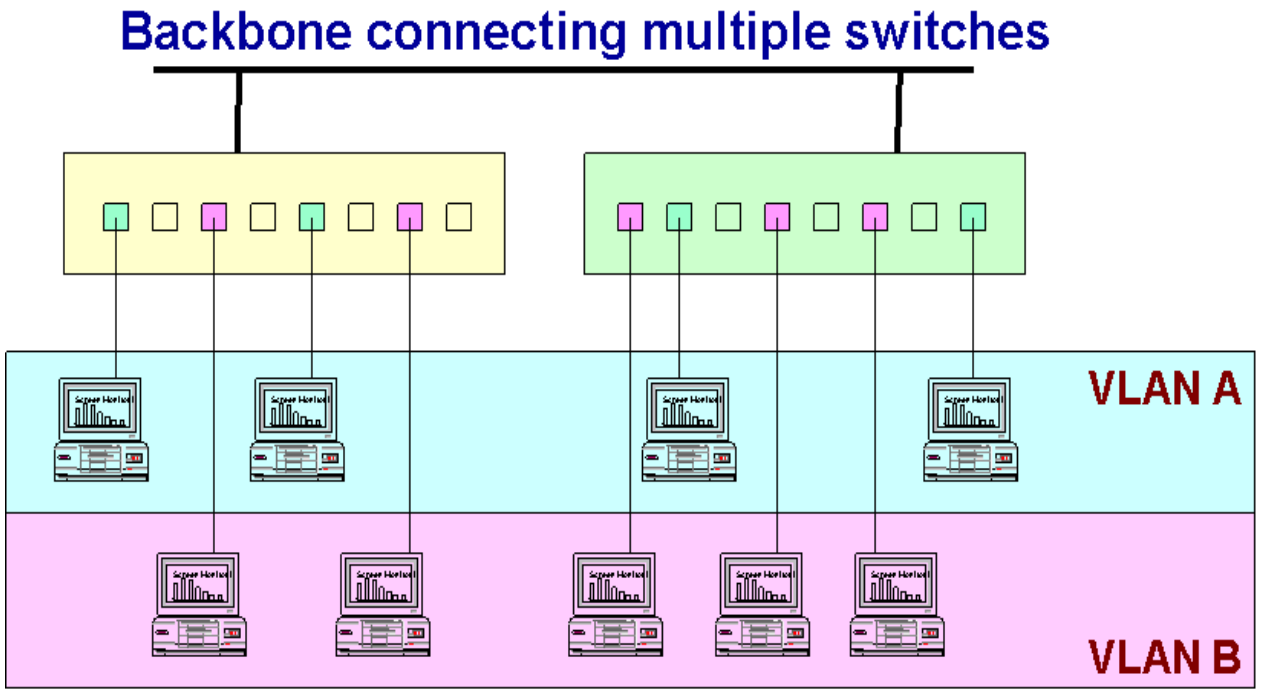
虚拟局域网的定义

- 虚拟局域网VLAN （ Virtual Local Area Network ）是一组逻辑上的设备和用户，这些设备和用户并不受物理位置的限制，可以根据功能、部门及应用等因素将它们组织起来，相互之间的通信就好像它们在同一个网段中一样；可以基于物理端口或者MAC地址划分VLAN
- 虚拟局域网的优势
  - 限制和防止网络上的广播风暴
  - 增强局域网的安全性，降低泄密风险，含有敏感数据的用户组可与网络的其余部分隔离

物理层VLAN： based on switch ports

- 将交换机端口分组，形成物理层VLAN(Port Based)
  - 优点：配置简单
  - 缺点：不允许一个端口同时属于多个VLAN；当终端计算机位置变化时，必须由管理员重新配置VLAN接口

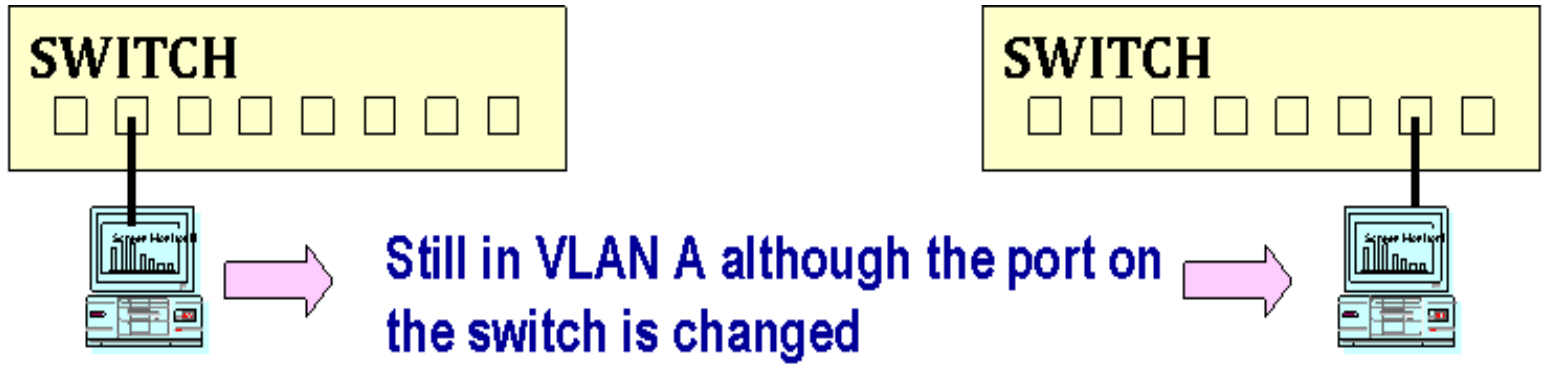
Port	VLAN
1	1
2	1
3	2
4	1



数据链路层VLAN：based on the MAC address

- 根据MAC Address分组，数据链路层VLAN(MAC Based)，也称“user-based VLAN”
  - 优点：用户物理移动时，不需要重新配置，依然属于原来的VLAN
  - 缺点：在初始时所有的用户，必须在至少一个VLAN上初始化

MAC Address	VLAN
1212354145121	1
2389234873743	2
3045834758445	2
5483573475843	1



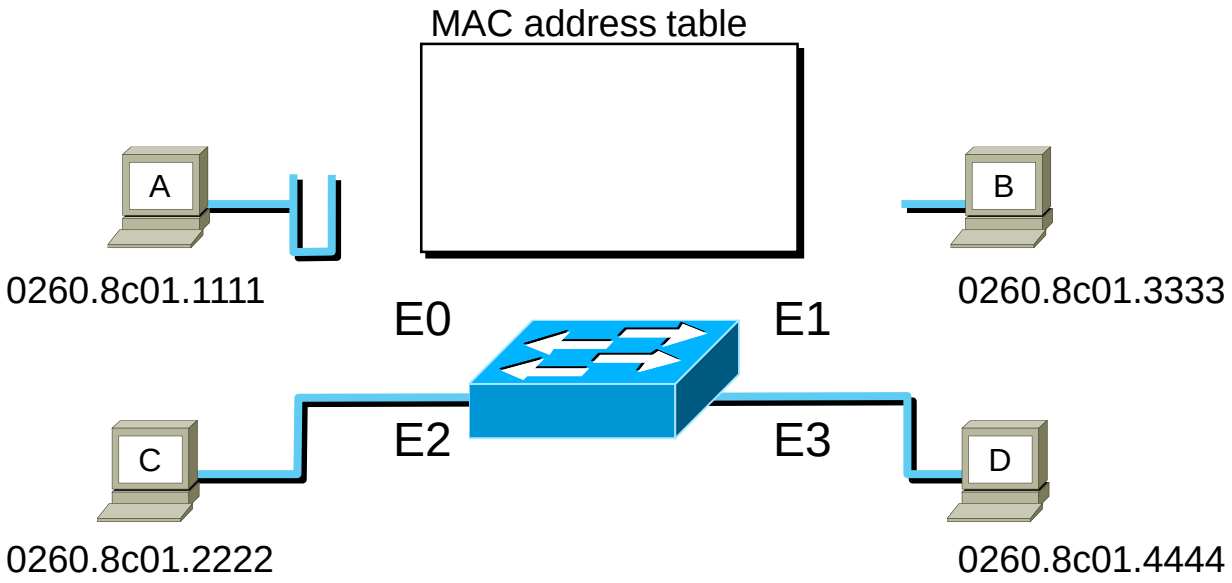
VLAN：Advantages and Disadvantages

- VLAN的优点：
  - 易于维护，容易解决人员位置的变动
  - 有效地控制广播流量，提高性能
  - 增强网络安全性

- VLAN的缺点：
  - 互操作性问题：标准滞后，实现上的不一致
  - 不同厂商实现方式不同，除非选择单一厂家的产品
  - 增加了管理的复杂性

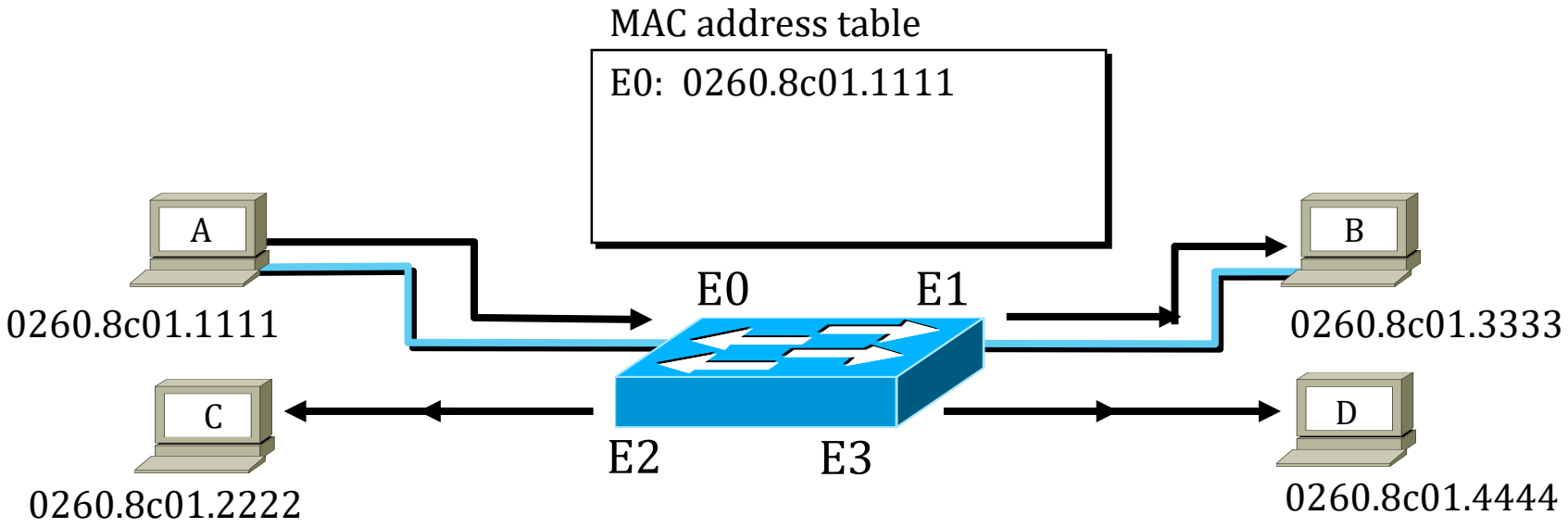
How Switches Learn Hosts Locations

- Initial MAC address table is empty



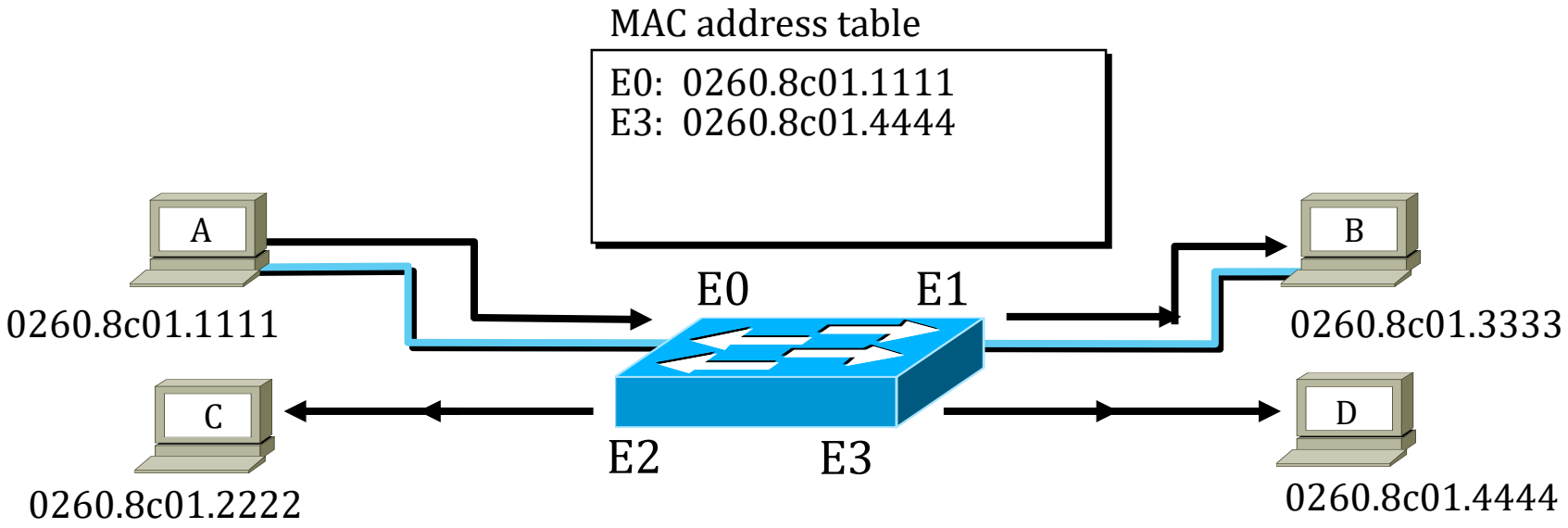
How Switches Learn Hosts Locations

- Station A sends a frame to Station C
- Switch caches station A MAC address to port E0 by learning the source address of data frames
- The frame from station A to station C is flooded out to all ports except port E0 (unknown unicasts are flooded)



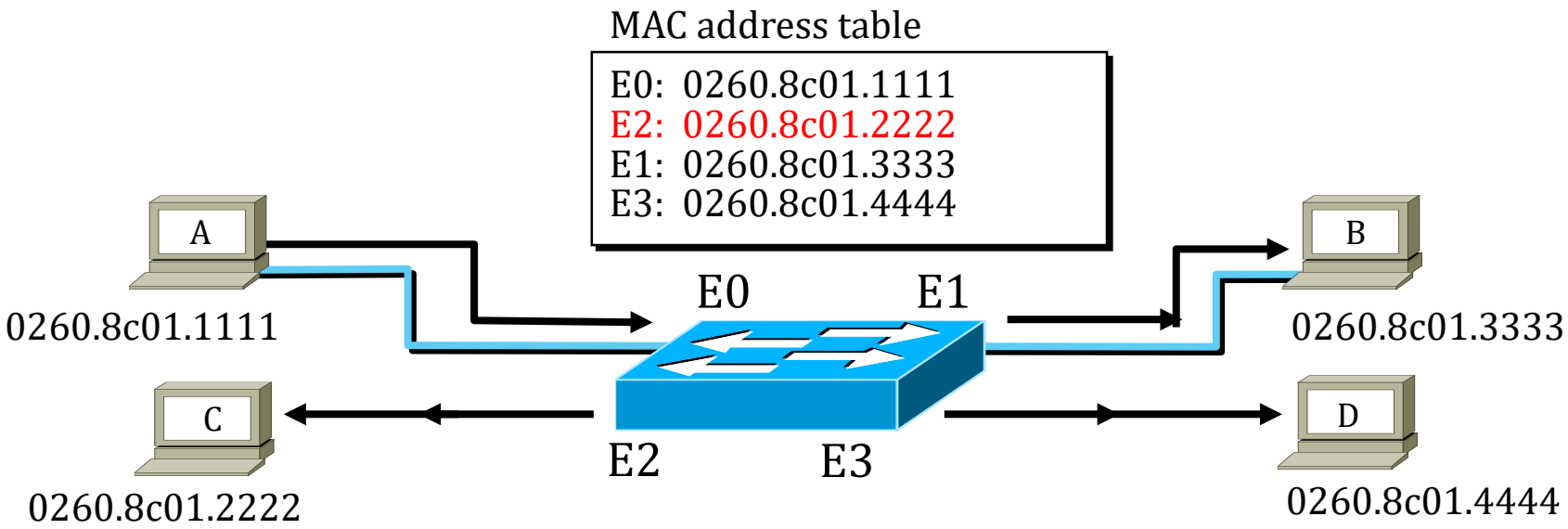
How Switches Learn Hosts Locations

- Station D sends a frame to station C
- Switch caches station D MAC address to port E3 by learning the source address of data frames
- The frame from station D to station C is flooded out to all ports except port E3 (unknown unicasts are flooded)



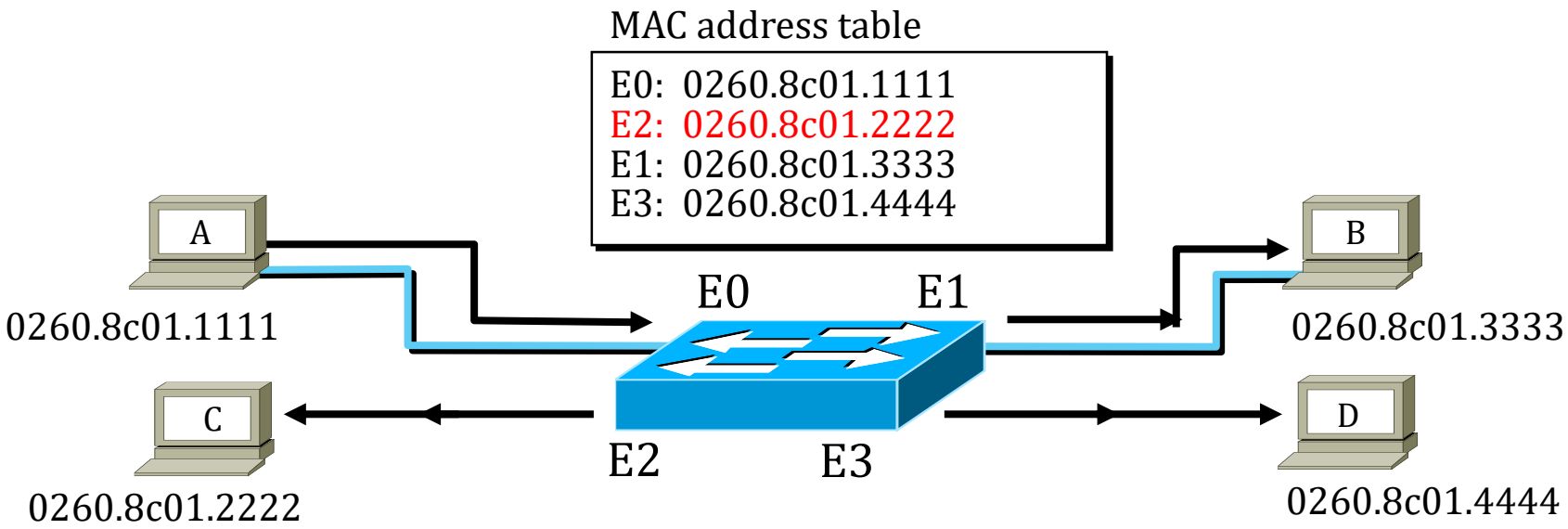
How Switches Filter Frames

- Station A sends a frame to station C
- Destination is known, frame is not flooded



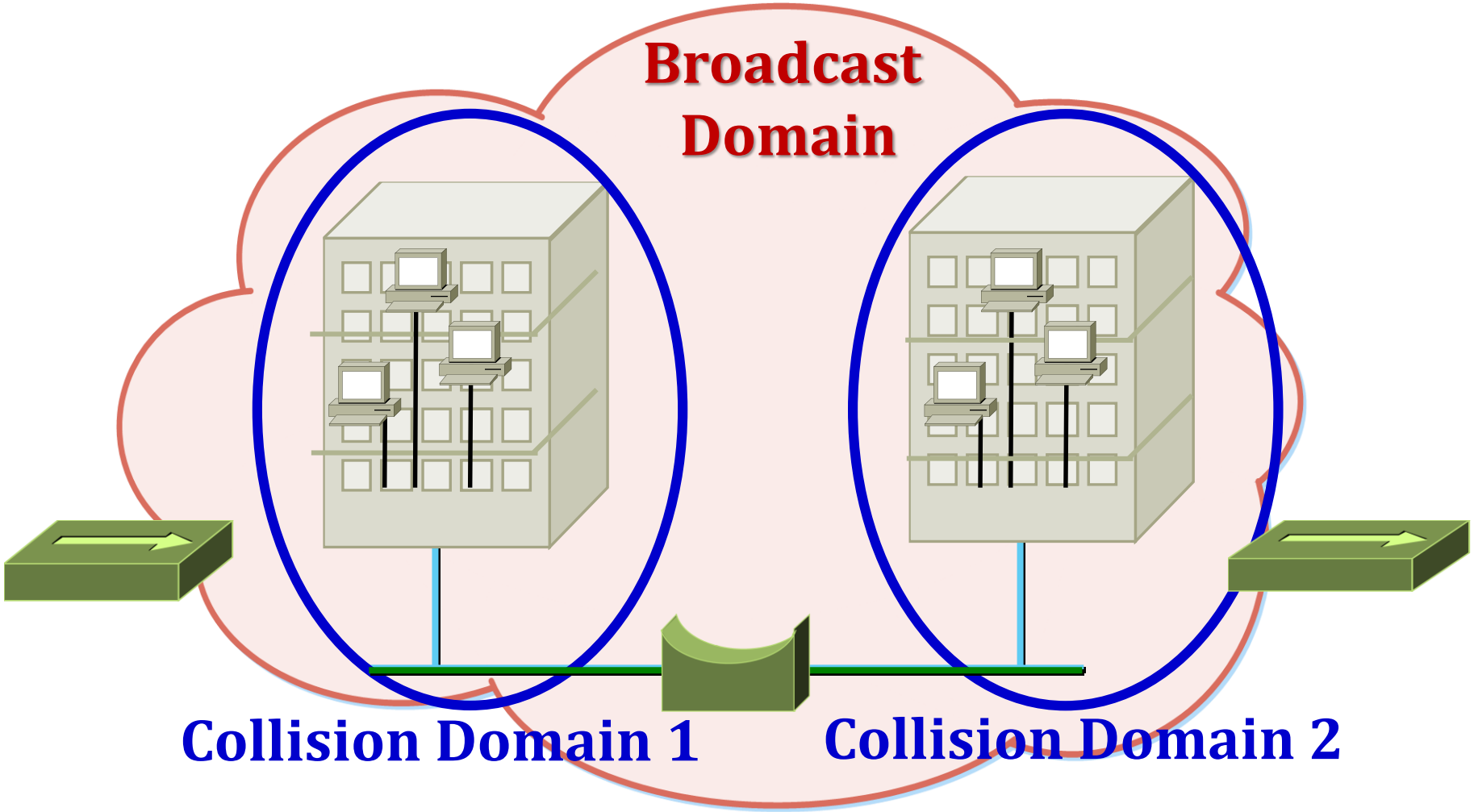
Broadcast and Multicast Frames

- Station D sends a broadcast or multicast frame
- Broadcast and multicast frames are flooded to all ports other than the originating port



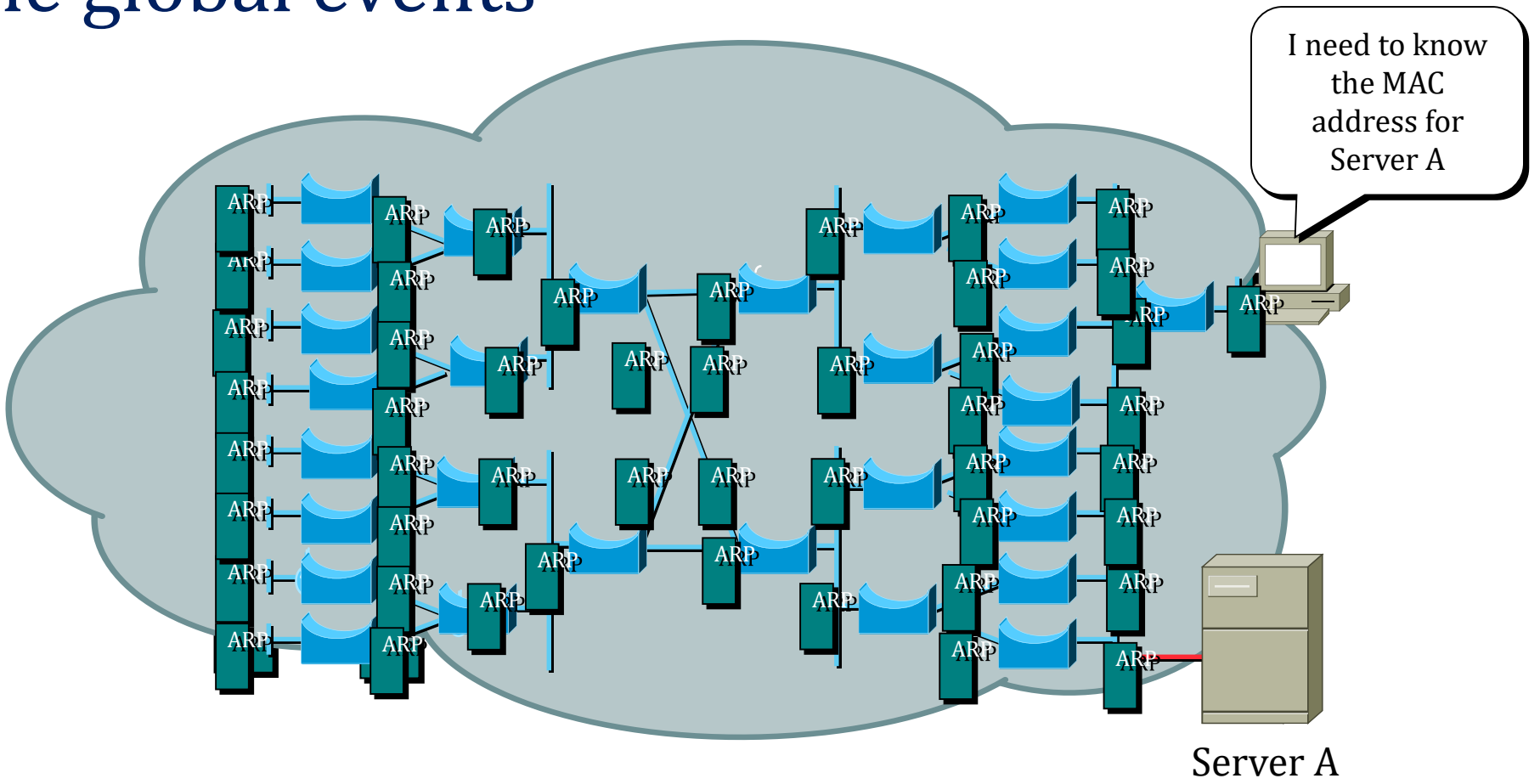
collision domains & broadcasts domains

- Bridges terminate collision domains



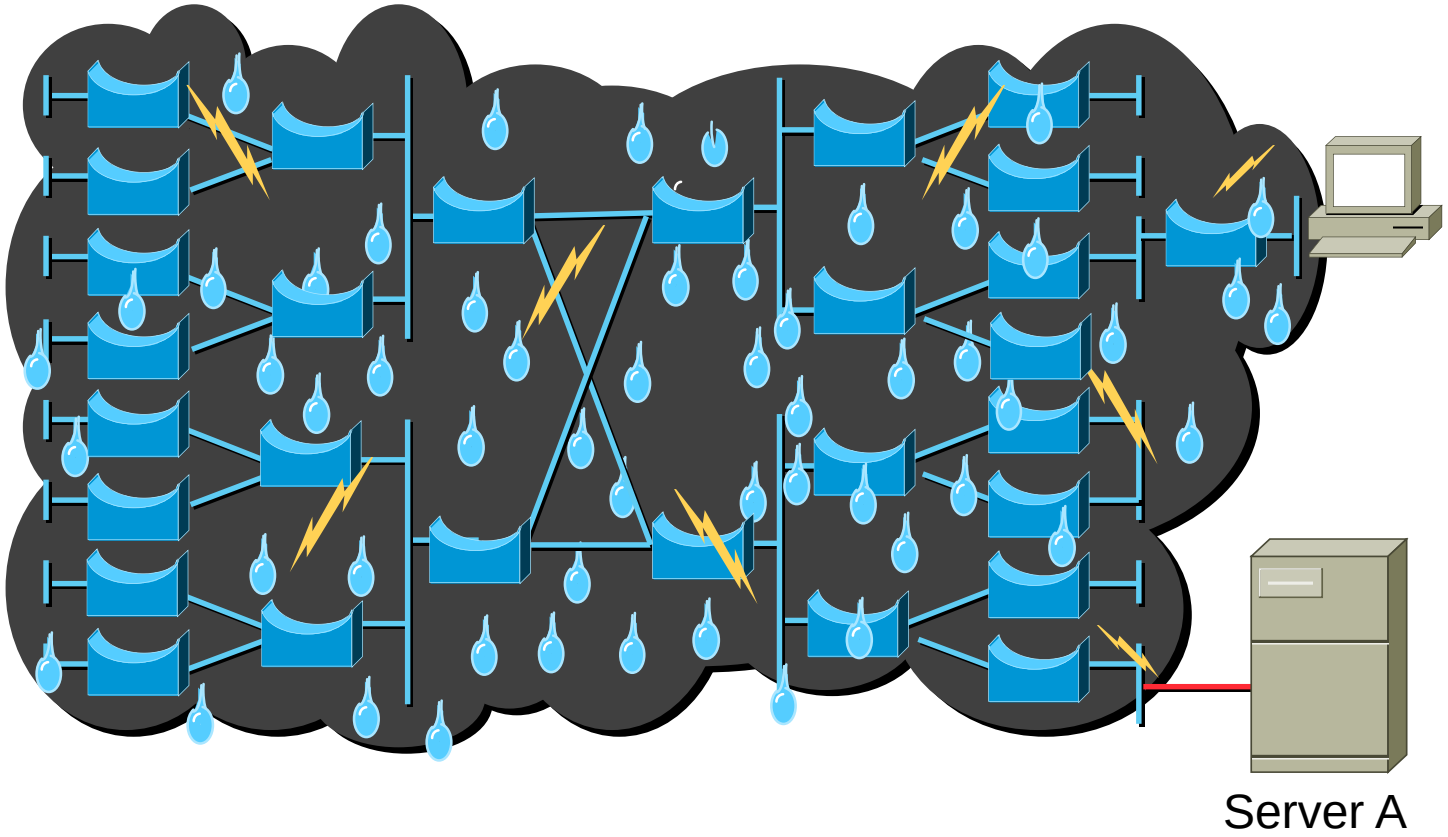
broadcast storms & network performance

- Multicast, broadcast, and unknown destination events become global events



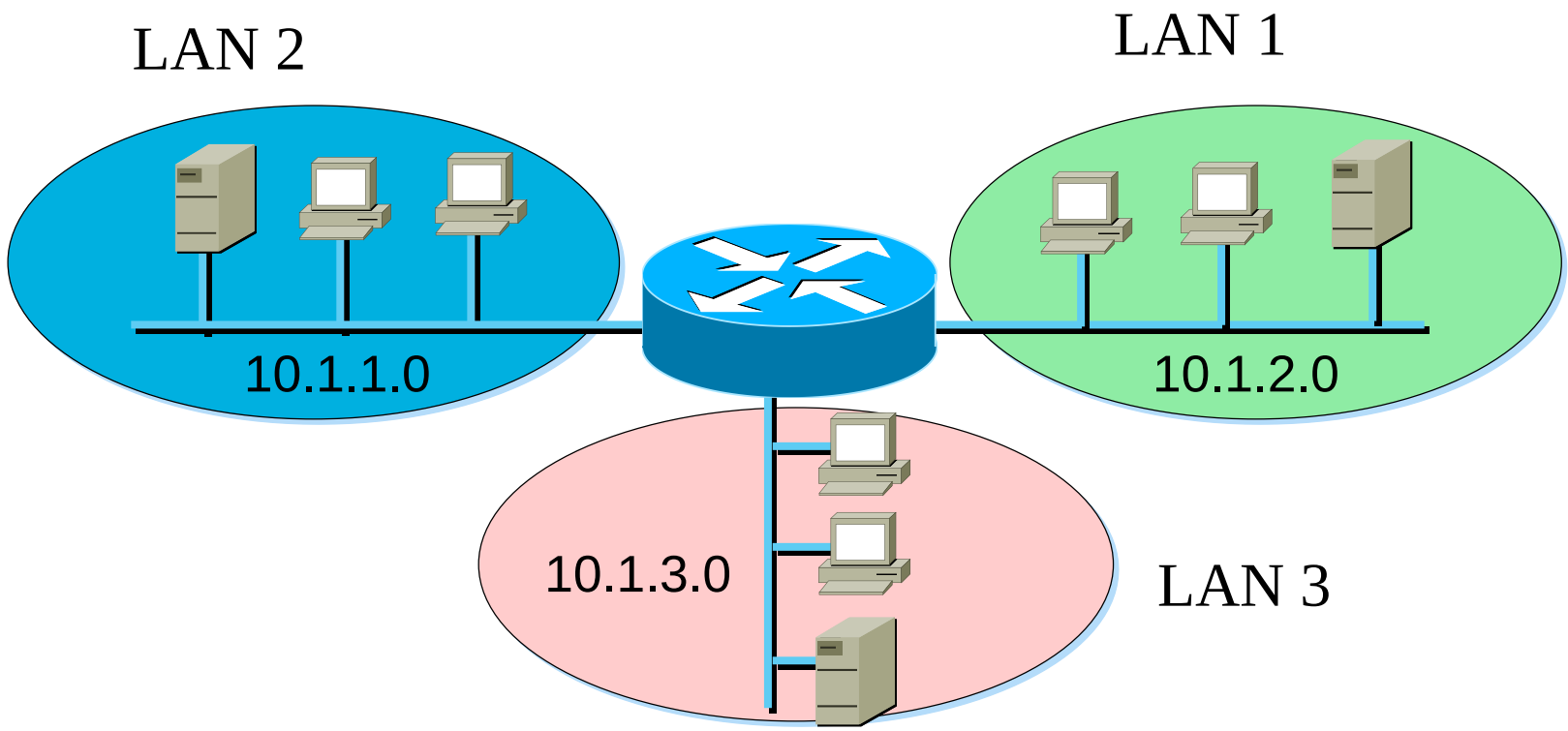
broadcast storm

- Broadcasts can consume all available bandwidth
- Each device must decode the broadcast frame

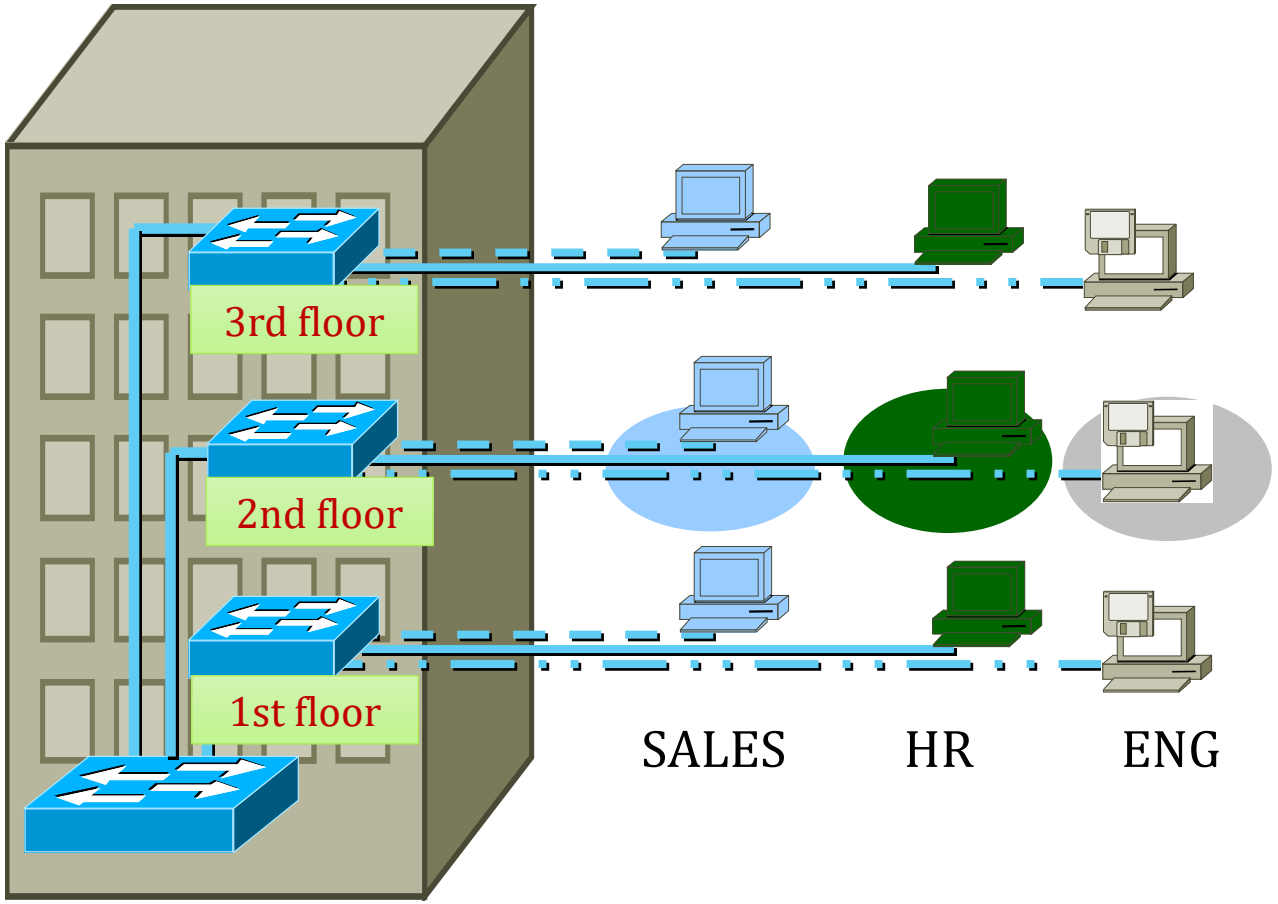


Broadcasts terminate at the router interface

- LAN broadcasts terminate at the router interface



Broadcasts terminate by VLAN

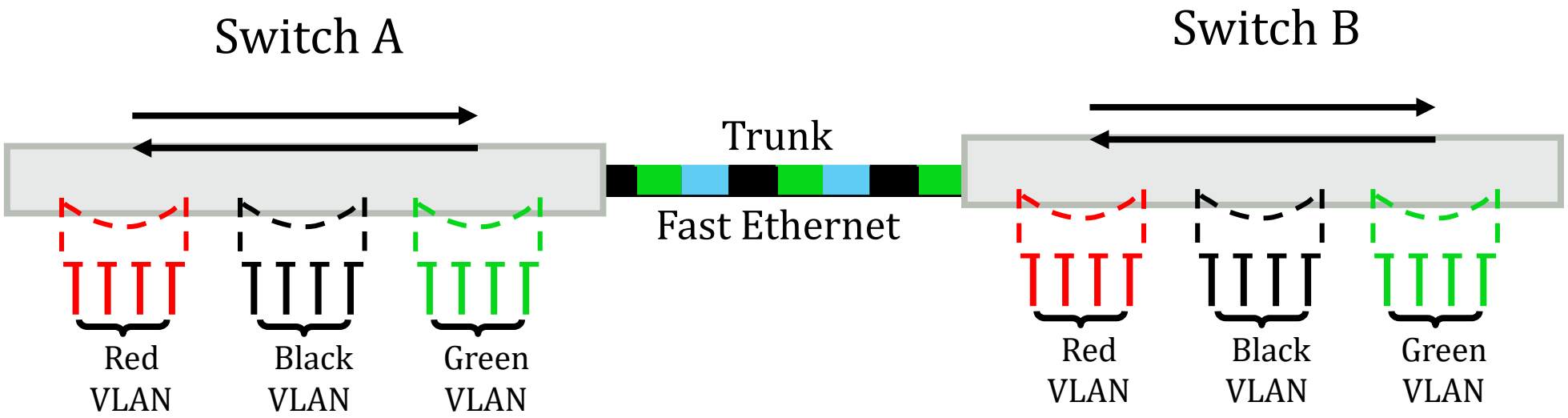


- Segmentation
- Flexibility
- Security

A VLAN = A broadcast domain = Logical network (subnet)

VLAN Operations

- Each logical VLAN is like a separate physical bridge
- VLANs can span across multiple switches
- Trunks carries traffic for multiple VLANs



计算机网络安全技术

Activity is the only road to knowledge

Computer Network Security @ 2020Fall