

● 广播信道数据链路层协议——CSMA/CD (载波监听多址接入 / 碰撞检测) 协议

- 进行**半双工通信**
- **争用期**——局域网的端到端往返时延 2τ
- 截断二进制指数**退避算法**
- **强化碰撞**——发送人为干扰信号

先听后发
边发边听
冲突停止
延时重发

● 扩展局域网

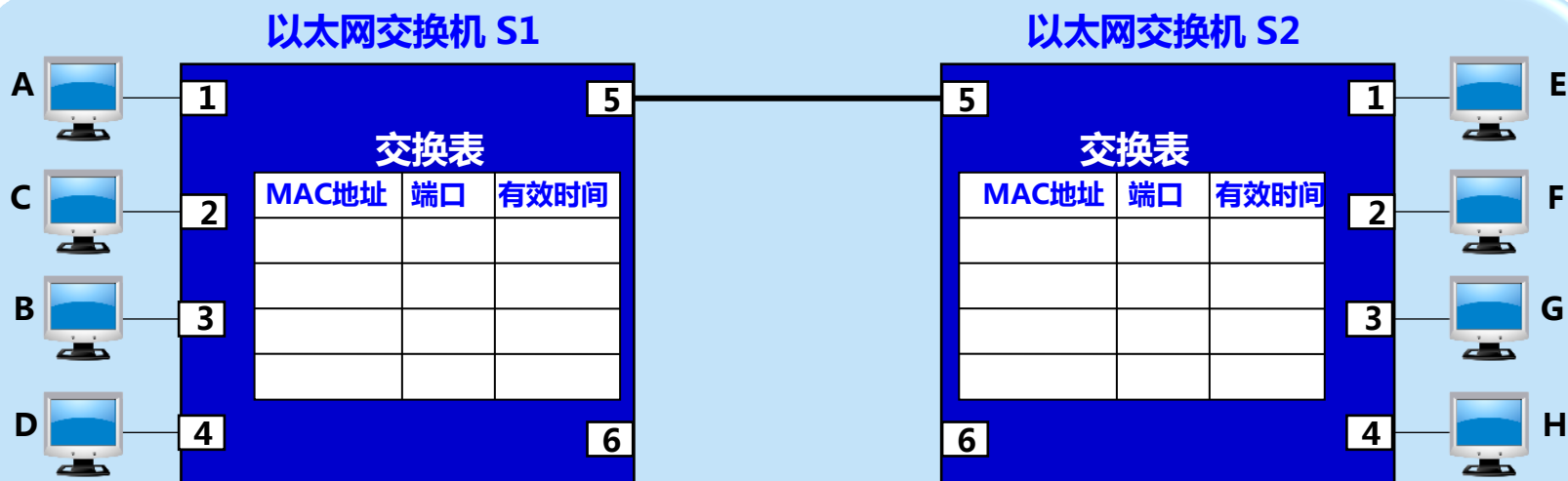
- 在物理层扩展 转发器(中继器) → **集线器**
- 在数据链路层扩展 网桥 → **交换机**

碰撞域
广播域

- 地址自学习
- 转发/过滤

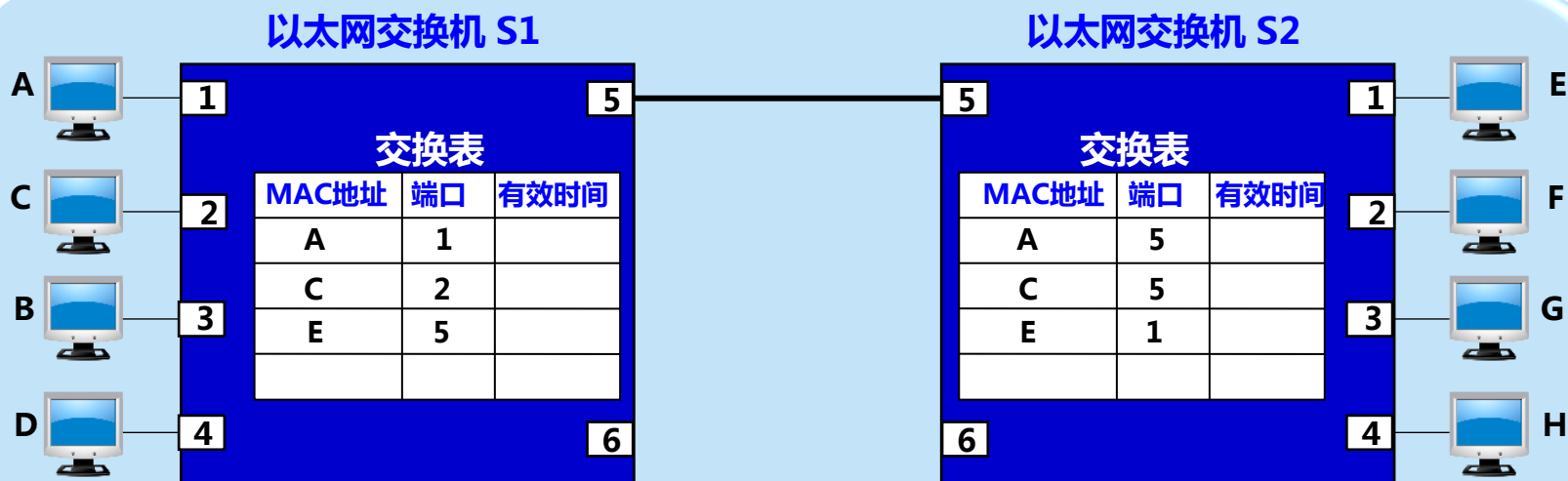
在数据链路层扩展局域网—以太网交换机

例



在数据链路层扩展局域网—以太网交换机

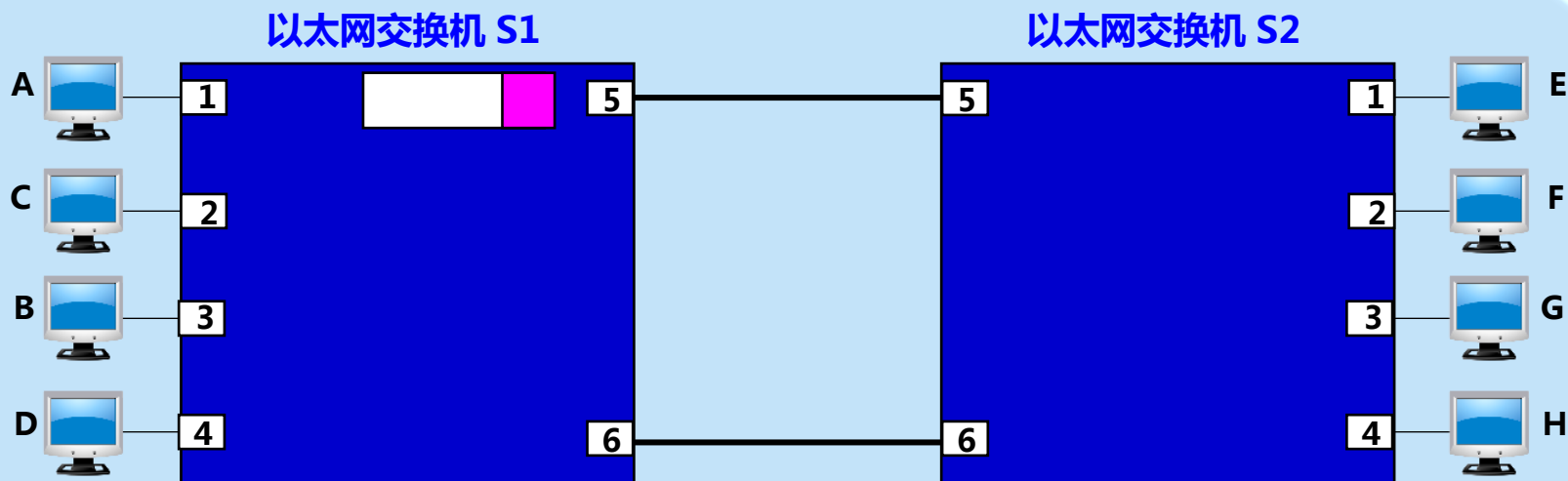
例



在数据链路层扩展局域网—以太网交换机

环路问题

- 为了提高网络可靠性，交换网络中通常会使用一些冗余链路。
- 冗余链路会带来环路风险，导致广播风暴和MAC地址不稳定等问题。

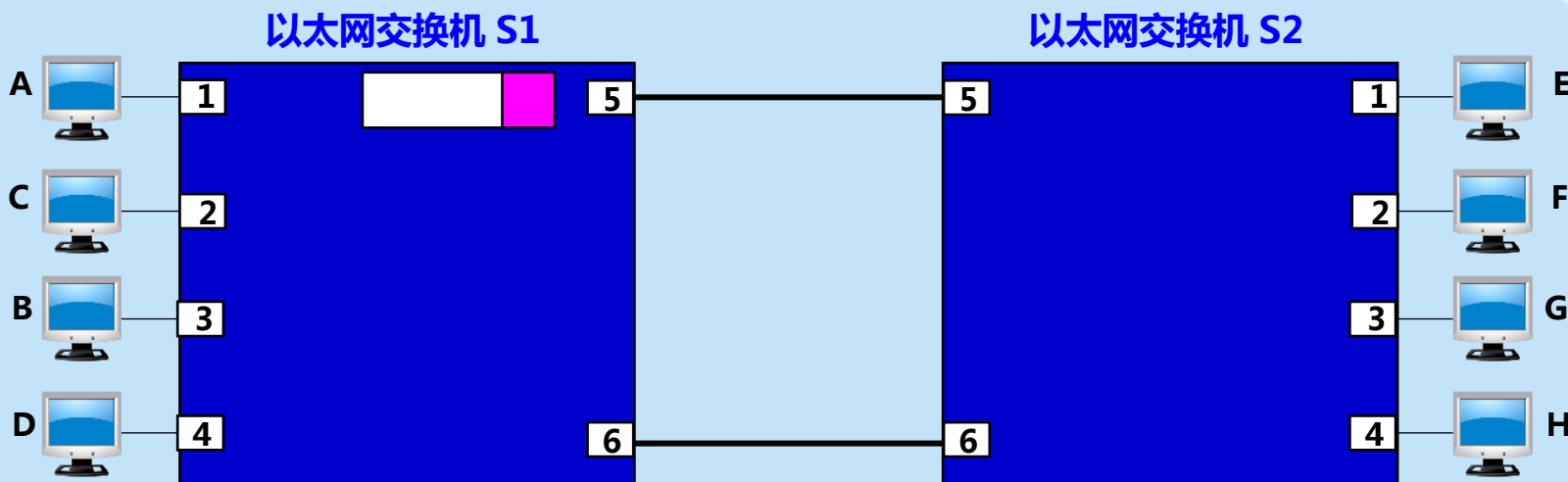


假定开始时，交换机 S1 和 S2 的交换表都是空的。
假定：主机 A 向主机 E 发送一帧。

在数据链路层扩展局域网—以太网交换机

环路问题

- 为了提高网络可靠性，交换网络中通常会使用一些冗余链路。
- 冗余链路会带来环路风险，导致广播风暴和MAC地址不稳定等问题。

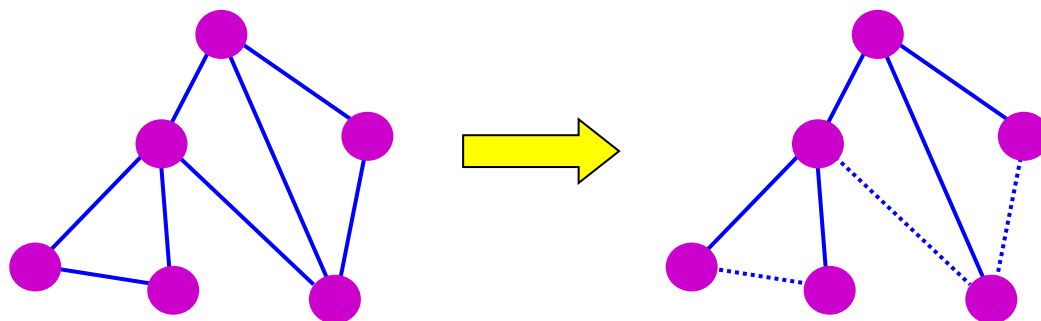


假定开始时，交换机 S1 和 S2 的交换表都是空的。
结果：交换机不断转发该广播帧，就会造成**广播风暴**。

在数据链路层扩展局域网——以太网交换机

环路问题

- IEEE 802.1D 标准制定了一个**生成树协议 (STP, Spanning Tree Protocol)**。
- 其**要点**是：**不改变**网络的**实际拓扑**，但在**逻辑上**则切断了某些链路，使得从一台主机到所有其他主机的路径是**无环路的树状结构**，从而消除了兜圈子现象。



在物理层扩展局域网

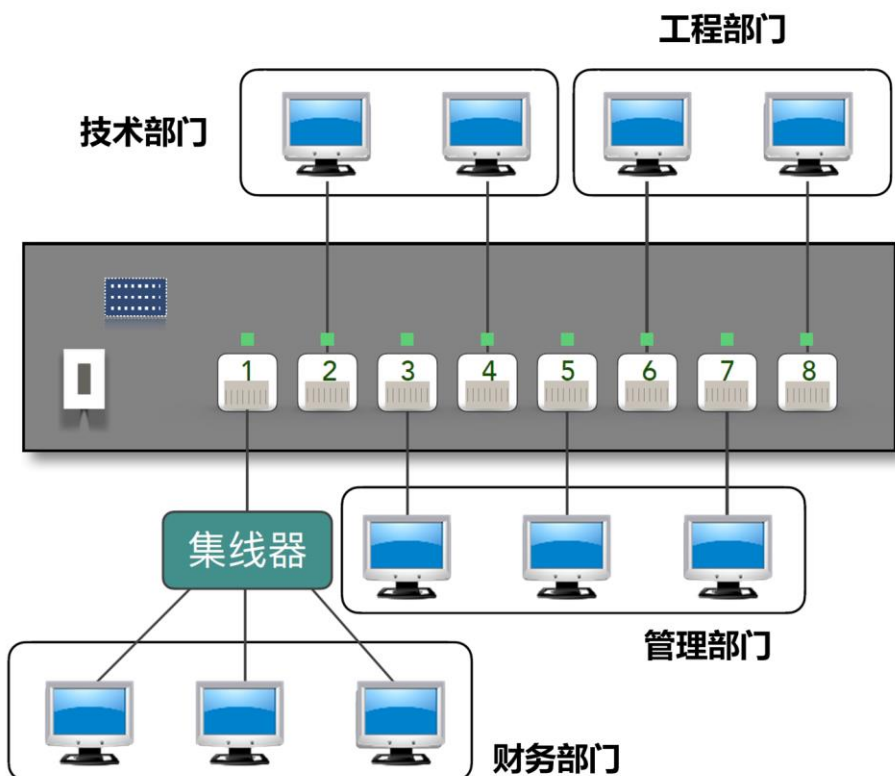
- 使用集线器组网
- 所有计算机都处于同一个碰撞域和同一个广播域
- 不支持不同速率的网络扩展

在数据链路层扩展局域网

- 使用交换机组网
- 交换机的每个端口是一个碰撞域，所有的端口属于同一个广播域
- 采用**存储转发**方式的交换机可以支持**不同速率**的设备进行连接

注：采用**直通方式**的交换机只要收到一帧最前面的目的MAC地址就立即执行转发操作，而不进行帧的缓冲，因此收发端口的**速率应完全相同**。

虚拟局域网 (VLAN)



- 广播域不能太大。
- 实际工作中，各部门功能单一，**部门内部可以相互访问**，但是部门之间不能相互访问（安全性）。
- **需要一种技术**将各部门从单一的广播域中隔离出来，以增强网络安全性。



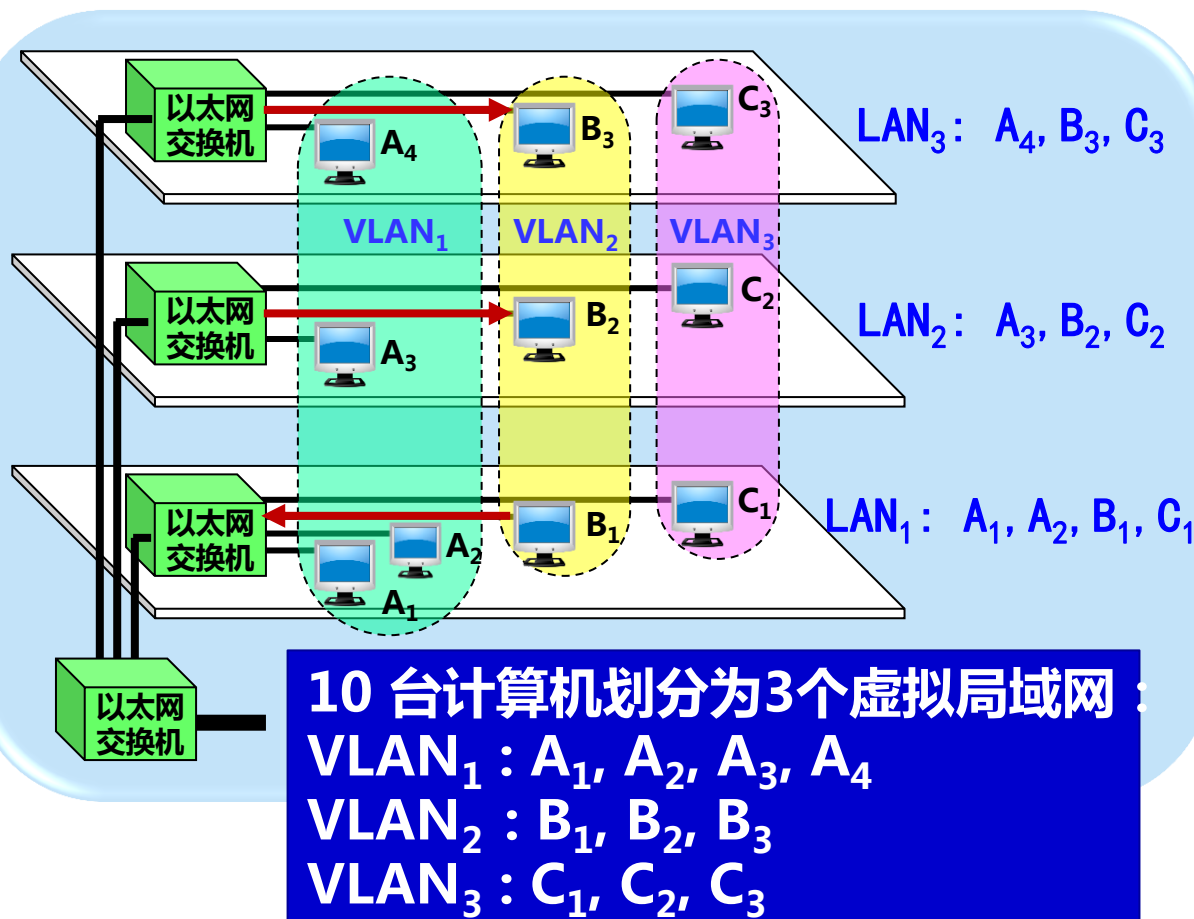
虚拟局域网技术

虚拟局域网（VLAN）

- 虚拟局域网（VLAN）其实只是局域网给用户提供的**一种服务**，而**并不是一种新型局域网**。功能和操作上与传统局域网基本相同，“**虚拟**”主要体现在**组网方式**上。
- VLAN是由一些**局域网网段构成的与物理位置无关的逻辑组**。
 - 这些网段具有某些**共同的需求**；
 - 每个VLAN的帧都有一个明确的标识符，用来指明发送帧的用户属于哪一个VLAN。
- 由于VLAN是**用户和网络资源的逻辑组合**，因此可按照需要将有关设备和资源非常方便地重新组合，使用户从不同的服务器或数据库中存取所需的资源。
- **划分VLAN的主要作用是隔离广播域**，增强网络的安全性和管理。

虚拟局域网 (VLAN)

VLAN = 广播域 + 逻辑网段



- VLAN 限制了接收广播信息的工作站数，使得网络不会因传播过多的广播信息（即“广播风暴”）而降低性能。
- 虚拟工作组的划分和管理由虚拟管理软件来实现，不需要改变原来的网络物理连接，增加了组网的灵活性。

虚拟局域网（VLAN）—— 优点和应用

- 虚拟局域网（VLAN）技术的主要优点
 - 控制广播风暴，提高了带宽利用率和网络功能性
 - 防止机密信息泄露，增强了局域网安全性
 - 网络连接更加灵活，节约了成本
 - 简化了网络管理
- 虚拟局域网（VLAN）技术的主要应用场合
 - 校园网
 - 大中型企业网
 - 行政机关网



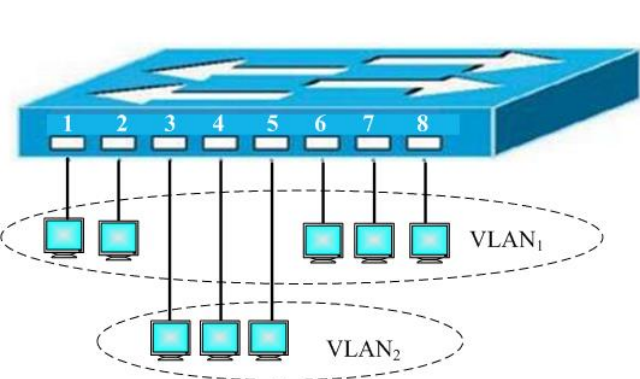
虚拟局域网（VLAN）——划分方法

- 基于交换机端口
- 基于MAC地址
- 基于协议类型
- 基于IP子网地址
- 基于高层应用或服务

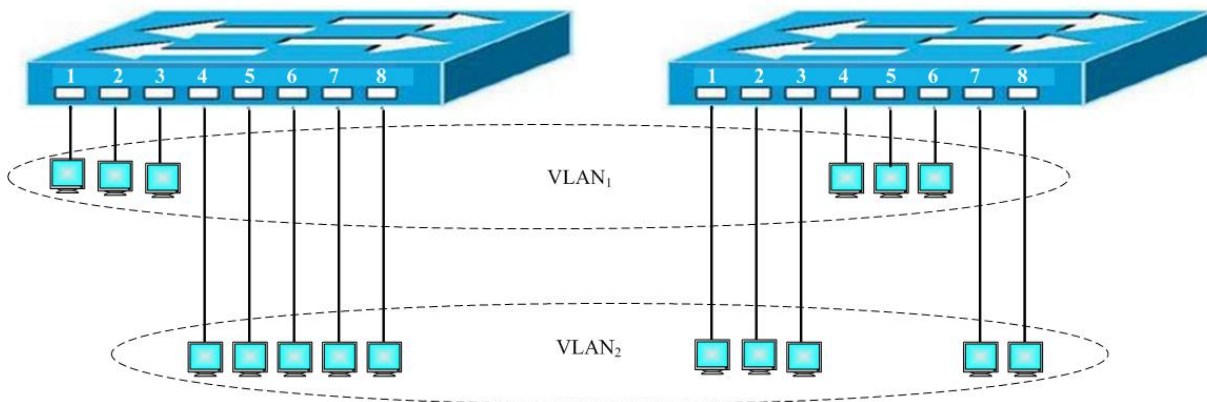
虚拟局域网（VLAN）——划分方法

● 基于交换机端口

- 属于在第一层划分VLAN的方法。
- **优点**：定义成员简单。
- **缺点**：不允许成员移动，成员移动需重新配置VLAN。



(a) 单交换机端口定义的VLAN



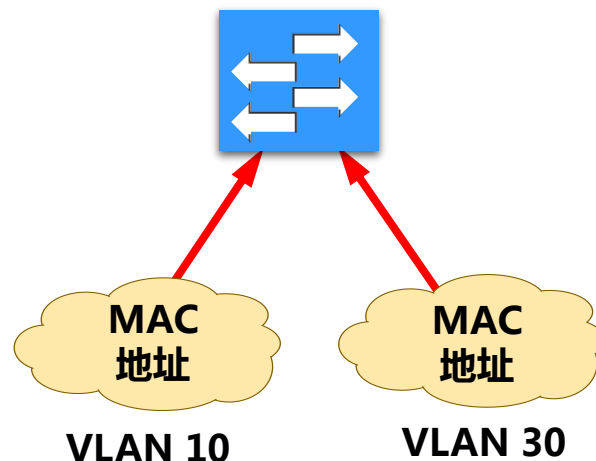
(b) 多交换机端口定义的VLAN

虚拟局域网（VLAN）——划分方法

● 基于MAC地址

- 属于在第二层划分VLAN的方法。
- 根据用户计算机的MAC地址划分VLAN。
- **优点**：允许用户移动，提高了终端用户接入的灵活性。
- **缺点**：需要输入和管理大量的MAC地址。如果用户的MAC地址改变了，则需要管理员重新配置VLAN。

MAC 地址	VLAN
00-15-F5-CC-C8-14	10
C0-AB-D5-00-18-F4	10
C0-C5-18-DE-BC-E6	30

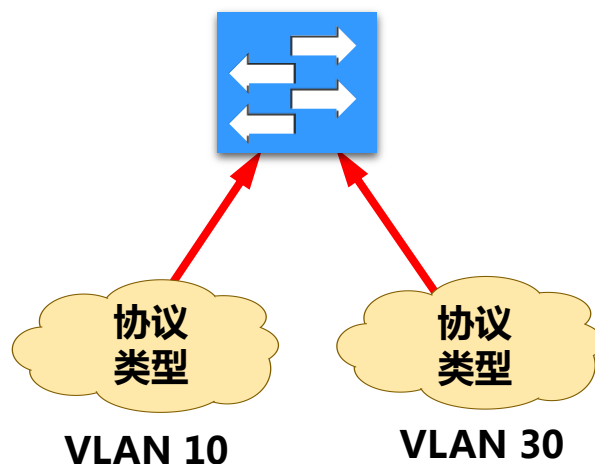


虚拟局域网（VLAN）——划分方法

● 基于协议类型

- 属于在第二层划分VLAN的方法。
- 根据以太网帧的第三个字段“类型”字段确定该类型的协议属于哪一个VLAN。
- **优点**：允许用户移动；不需要额外的帧标签来识别VLAN，可以减少网络流量。
- **缺点**：检查每一帧的“类型”字段，需要消耗处理时间，效率较低。

“类型”	VLAN
IP	10
IPX	30
.....	...

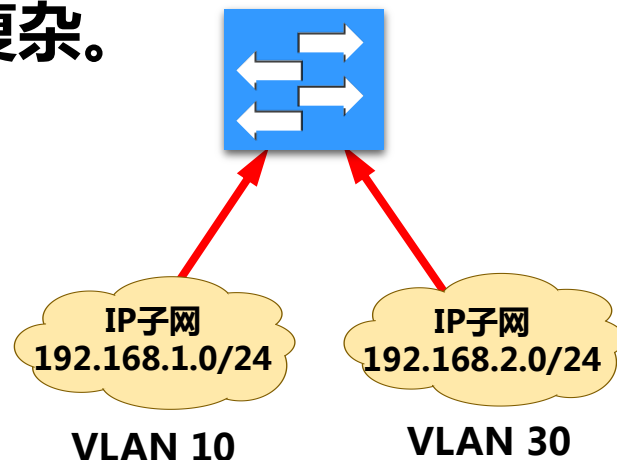


虚拟局域网（VLAN）——划分方法

● 基于IP子网地址

- 属于在第三层划分VLAN的方法。
- 根据以太网帧的第三个字段“类型”字段和IP分组首部中的源IP地址字段确定该IP分组属于哪一个VLAN。
- 优点：将指定网段或IP地址发出的报文在指定的VLAN中传输，减轻了网络管理者的任务量，且有利于管理。
- 缺点：网络中的用户分布需要有规律，且多个用户在同一网段中；效率低，配置复杂。

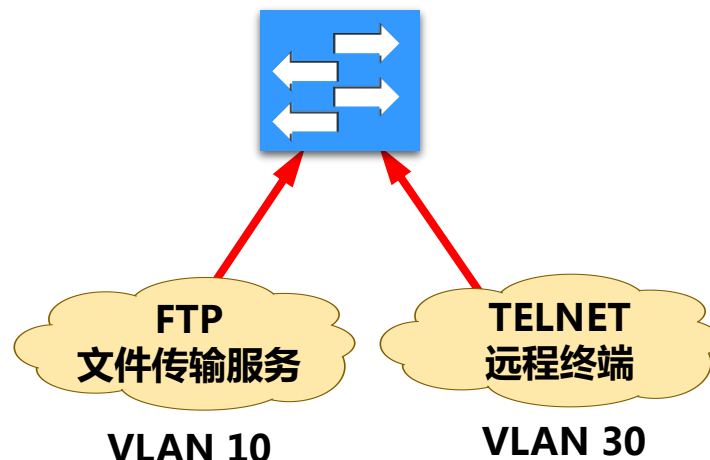
IP 子网	VLAN
192.168.1.0/24	10
192.168.2.0/24	30
.....	...



虚拟局域网（VLAN）——划分方法

- 基于高层应用或服务
 - 根据高层应用或服务、或者它们的组合划分VLAN。
 - **优点**：灵活。
 - **缺点**：复杂。

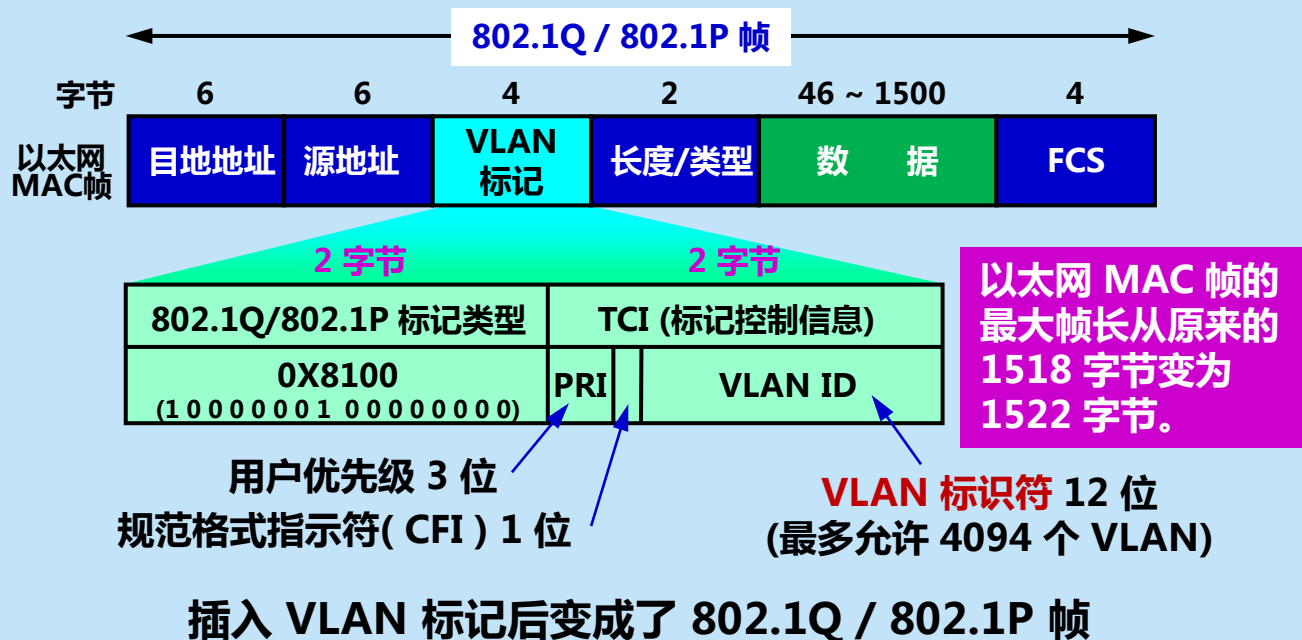
应用	VLAN
FTP	10
TELNET	30
.....	...



虚拟局域网（VLAN）——使用的以太网帧格式

- IEEE 批准了 802.3ac 标准，该标准定义了以太网帧格式的扩展，以支持虚拟局域网。
- 虚拟局域网协议允许在以太网的帧格式中插入一个4字节的标识符，称为 VLAN 标记 (tag)，用来指明该帧属于哪一个虚拟局域网。
- 插入VLAN标记的帧称为 IEEE 802.1Q/802.1P 帧或带标记的以太网帧。

虚拟局域网 (VLAN) — 使用的以太网帧格式



- 用户优先级：3位，共有8个，0最低，7最高。
- 规范格式指示符 (CFI)：1位，CFI=0表示MAC地址是规范格式，CFI=1表示MAC地址是非规范格式。
- VLAN标识符 (VID)：12位，VID = 0用于识别帧优先级，4095作为预留给值，故 VLAN 配置的最大可能值为4094。

虚拟局域网（VLAN）— 交换机端口的类型

- **Access端口**

- 一个Access 端口只属于一个VLAN
- Access端口发送不带标签的报文
- 缺省所有端口都包含在VLAN1中，且都是Access端口
- 一般与计算机或服务器连接

- **Trunk端口**

- 一个Trunk 端口可以属于多个VLAN
- Trunk 端口通过发送带标签的报文来区别某一数据包属于哪一VLAN
- 标签遵守IEEE802.1Q/IEEE802.1P协议标准
- 一般用于交换机之间的连接

- **Hybrid端口**

- 与Trunk类型端口类似，但可以允许多个VLAN发送时不打标签
- 可以用于交换机之间连接，也可以用于计算机之间的连接。

- 快速以太网
- 千兆以太网
- 万兆以太网

了解相关以太网规范和物理层标准
(参见教材P89-90)

两类地址

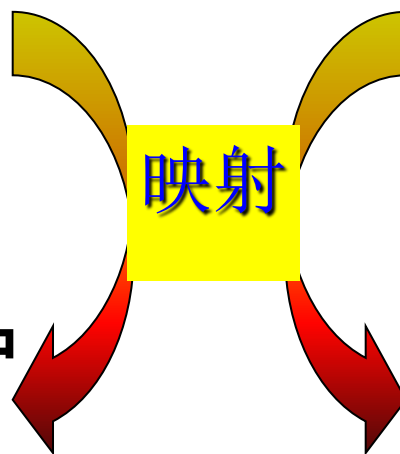
- IP数据报交付到主机或路由器需要**两类地址**

- **互联网：IP地址**

- ✓ 全网统一编址
- ✓ 具有全局唯一性
- ✓ 通常用软件实现
- ✓ 用在网络层的分组中

- **物理网：物理地址**

- ✓ 由所属的物理网络来定义
- ✓ 具有本地唯一性，不一定具有全局唯一性
- ✓ 通常写在硬件（网卡）上
- ✓ 包含在数据链路层使用的帧中



两类地址

在网络链路上传输的帧最终是按硬件地址找到目的主机的，那么为什么不直接使用硬件地址进行通信，而是要使用IP地址并调用ARP来寻找相应的硬件地址呢？

两类地址

- 由于全世界存在着各式各样的网络，它们使用不同的硬件地址。要使这些异构网络能够互相通信就必须进行非常复杂的硬件地址转换工作，因此几乎是不可能的事。
- **IP 编址把这个复杂问题解决了。**通过在物理网络上覆盖一层IP软件来实现对物理地址差异性的屏蔽，为上层用户提供“统一”的地址形式，而且不对物理地址做任何修改。
- 连接到互联网上的主机只需各自拥有一个唯一的 IP 地址，它们之间的通信就能像连接在同一个网络上那样简单方便。

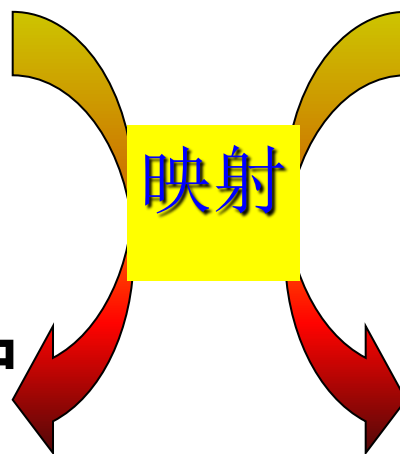
两级地址

● IP数据报交付到主机或路由器需要**两级地址**➤ **互联网：IP地址**

- ✓ 全网统一编址
- ✓ 具有全局唯一性
- ✓ 通常用软件实现
- ✓ 用在网络层的分组中

➤ **物理网：物理地址**

- ✓ 由所属的物理网络来定义
- ✓ 具有本地唯一性，不一定具有全局唯一性
- ✓ 通常写在硬件（网卡）上
- ✓ 包含在数据链路层使用的帧中



Network

IP地址和硬件地址
是否具有绑定关系？

Data Link

Physical

地址解析方法

● IP地址 → 物理地址

Static Table	
IP address	Physical address
.....
.....

- ◆ 使用协议按需获得
 - ☞ ARP (IP地址映射为物理地址)
- ◆ 需使用单播和广播物理地址

Dynamic Table	
IP address	Physical address
.....
.....

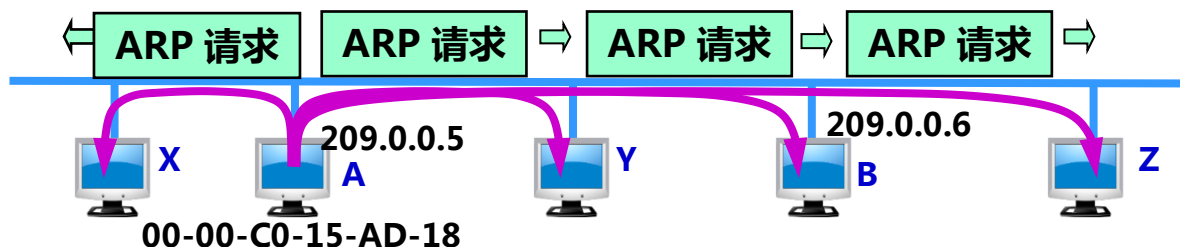
- ◆ 映射表是固定设置的,存储在网络的每个设备上
- ◆ 应用
 - ☞ 固定不变的网络
 - ☞ 面向连接的网络, 如 X.25、FR、ATM
- ◆ 局限
 - ☞ 更换网卡
 - ☞ 计算机移动

ARP 的工作原理

● IP地址 → 物理地址

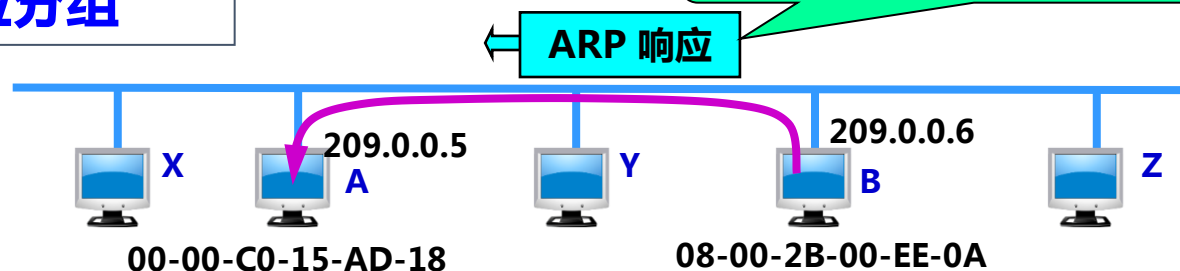
主机 A 广播发送
ARP 请求分组

我是 209.0.0.5，硬件地址是 00-00-C0-15-AD-18
我想知道主机 209.0.0.6 的硬件地址

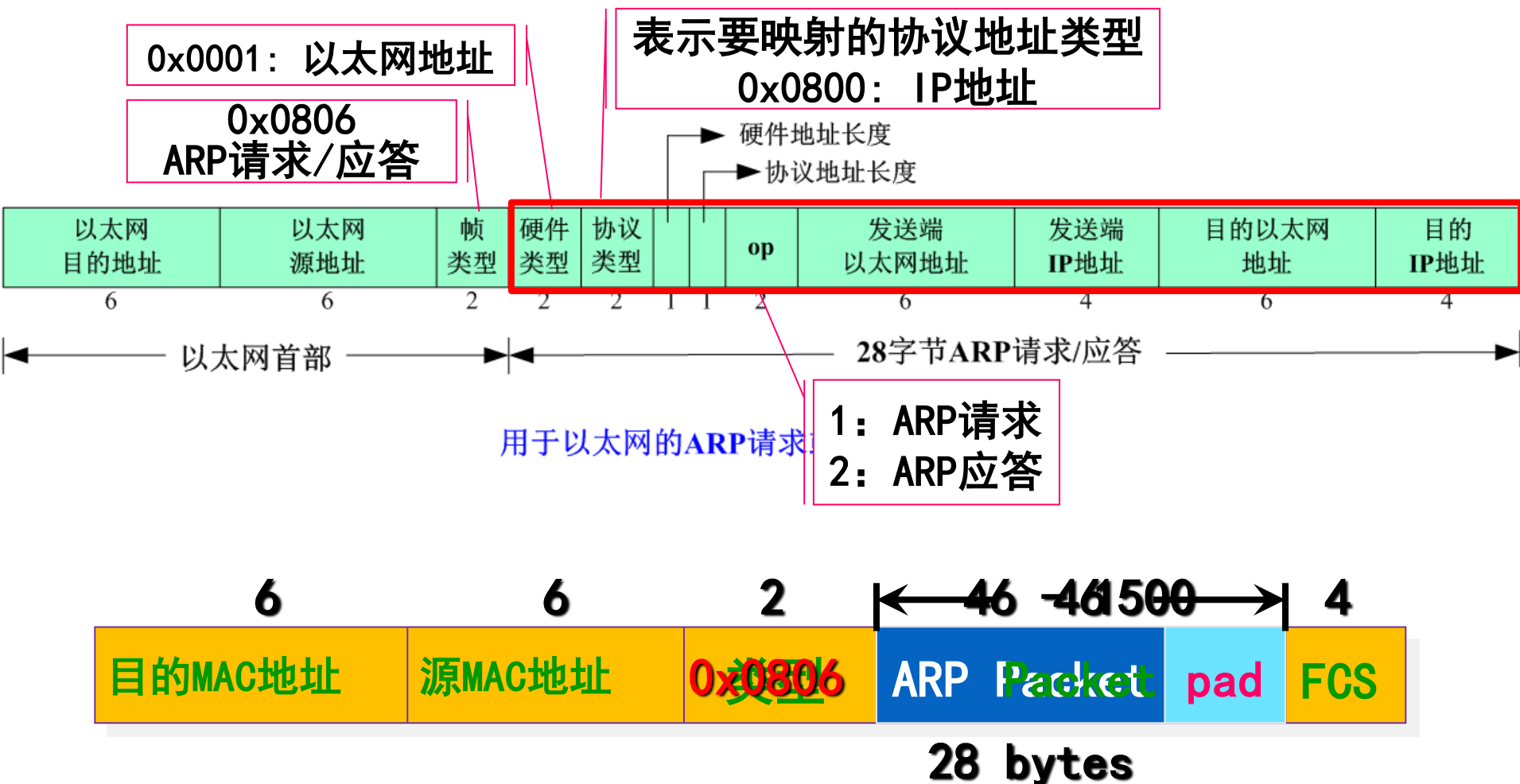


主机 B 向 A 单播发送
ARP 响应分组

我是 209.0.0.6
硬件地址是 08-00-2B-00-EE-0A



ARP 的分组格式



ARP高速缓存技术

- 不管网络层使用什么协议，在实际网络的数据链路上传送帧时，最终还是必须使用物理地址。
- 每一个主机都设有一个 **ARP 高速缓存区**(ARP cache)，用来**存放最近使用的 IP 地址到物理地址之间的映射记录**。
- 为了保证主机中 ARP 表的正确性和有效性，ARP 表要经常更新。给表中的每个表项分配了一个计时器，一旦某个表项超时，主机就会自动将其删除。
- 采用 ARP 高速缓存技术可以**提高网络运行的效率**。

< IP address ; MAC address ; TTL >

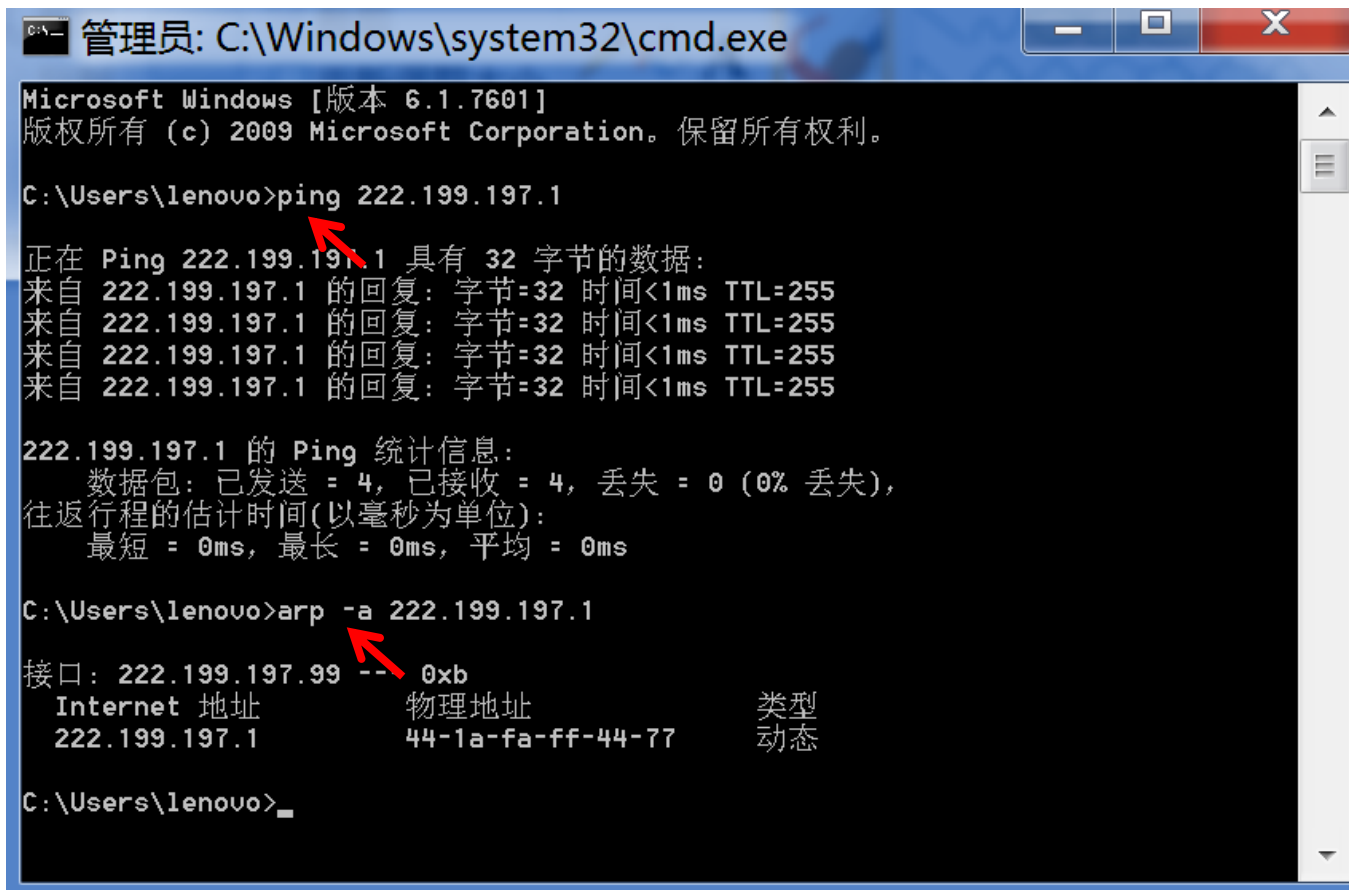
TTL (Time To Live) : 地址映射有效时间。

ARP 命令

- ARP 表中的内容可以查看，也可以添加和修改。

arp命令	
参 数	说 明
-a/g	arp -a 或 arp -g 显示ARP高速缓存中的所有内容
-d	arp -d inet_addr 删除ARP高速缓存中的某一项内容
-s	arp -s inet_addr eth_addr 用于静态绑定IP和MAC

ARP 命令



```
管理员: C:\Windows\system32\cmd.exe
Microsoft Windows [版本 6.1.7601]
版权所有 (c) 2009 Microsoft Corporation。保留所有权利。

C:\Users\lenovo>ping 222.199.197.1

正在 Ping 222.199.197.1 具有 32 字节的数据:
来自 222.199.197.1 的回复: 字节=32 时间<1ms TTL=255
来自 222.199.197.1 的回复: 字节=32 时间<1ms TTL=255
来自 222.199.197.1 的回复: 字节=32 时间<1ms TTL=255
来自 222.199.197.1 的回复: 字节=32 时间<1ms TTL=255

222.199.197.1 的 Ping 统计信息:
    数据包: 已发送 = 4, 已接收 = 4, 丢失 = 0 (0% 丢失),
    往返行程的估计时间(以毫秒为单位):
        最短 = 0ms, 最长 = 0ms, 平均 = 0ms

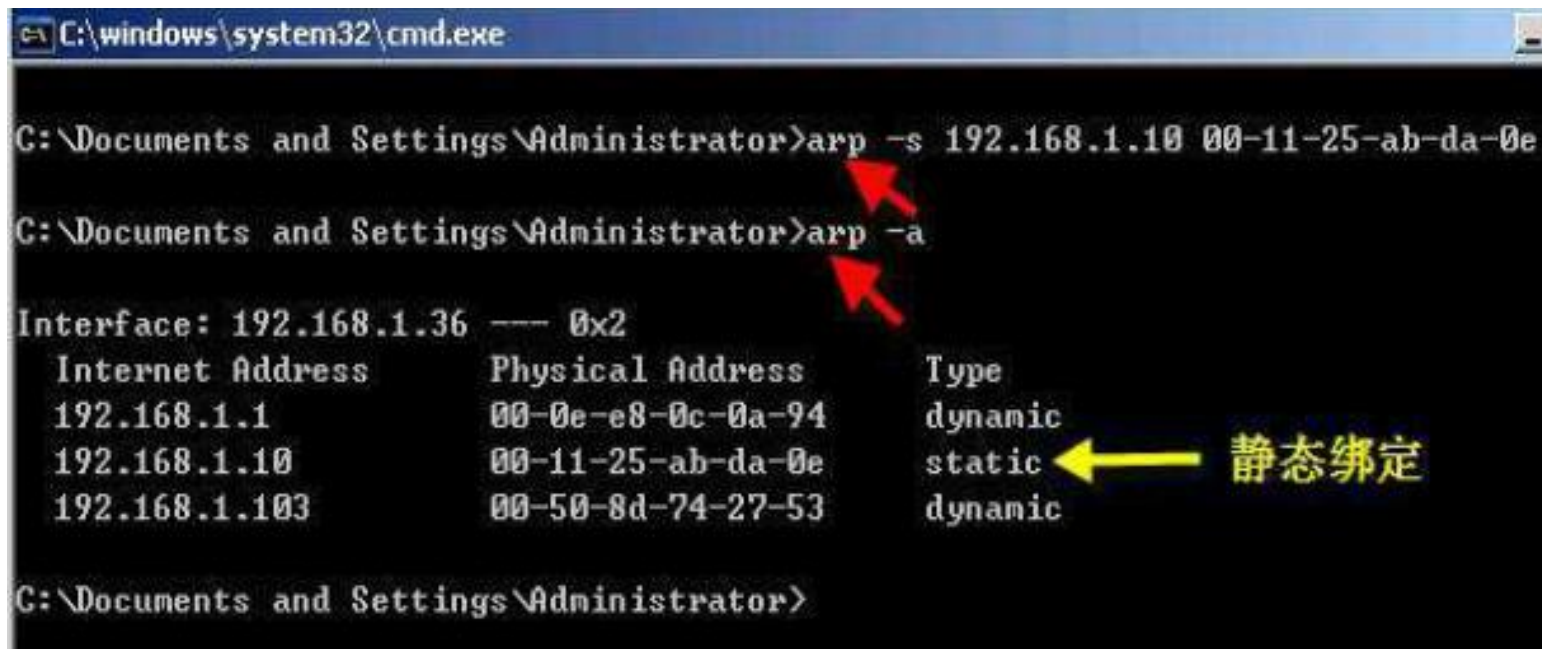
C:\Users\lenovo>arp -a 222.199.197.1

接口: 222.199.197.99 -- 0xb
    Internet 地址          物理地址          类型
    222.199.197.1          44-1a-fa-ff-44-77 动态

C:\Users\lenovo>
```

arp -a和**ping**命令结合可以查看某台主机的MAC地址

ARP 命令



```
C:\windows\system32\cmd.exe

C:\Documents and Settings\Administrator>arp -s 192.168.1.10 00-11-25-ab-da-0e

C:\Documents and Settings\Administrator>arp -a

Interface: 192.168.1.36 --- 0x2
    Internet Address      Physical Address      Type
    192.168.1.1           00-0e-e8-0c-0a-94     dynamic
    192.168.1.10          00-11-25-ab-da-0e     static
    192.168.1.103         00-50-8d-74-27-53     dynamic

C:\Documents and Settings\Administrator>
```

静态绑定

点对点的链路使用ARP吗？



点对点链路**不使用**ARP协议，因为在设置这些链路时，网络设备已获得了链路两端的IP地址，不需要ARP协议来实现IP地址和不同网络硬件地址的动态映射。

特殊的ARP

- 代理ARP

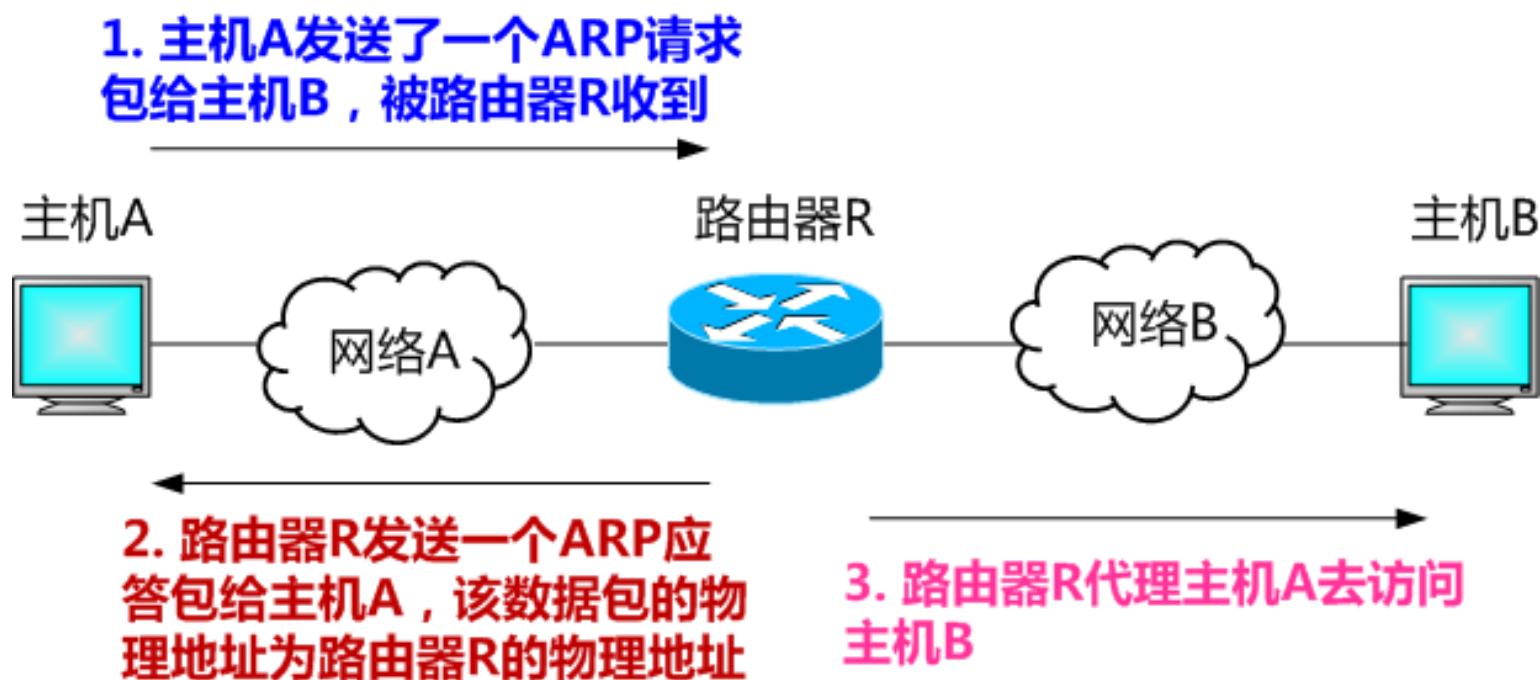
- 当出现跨网段的 ARP 请求时，路由器将自己的物理地址返回给发送 ARP 请求的主机，实现物理地址的代理，从而使主机能够通信。

- 免费ARP

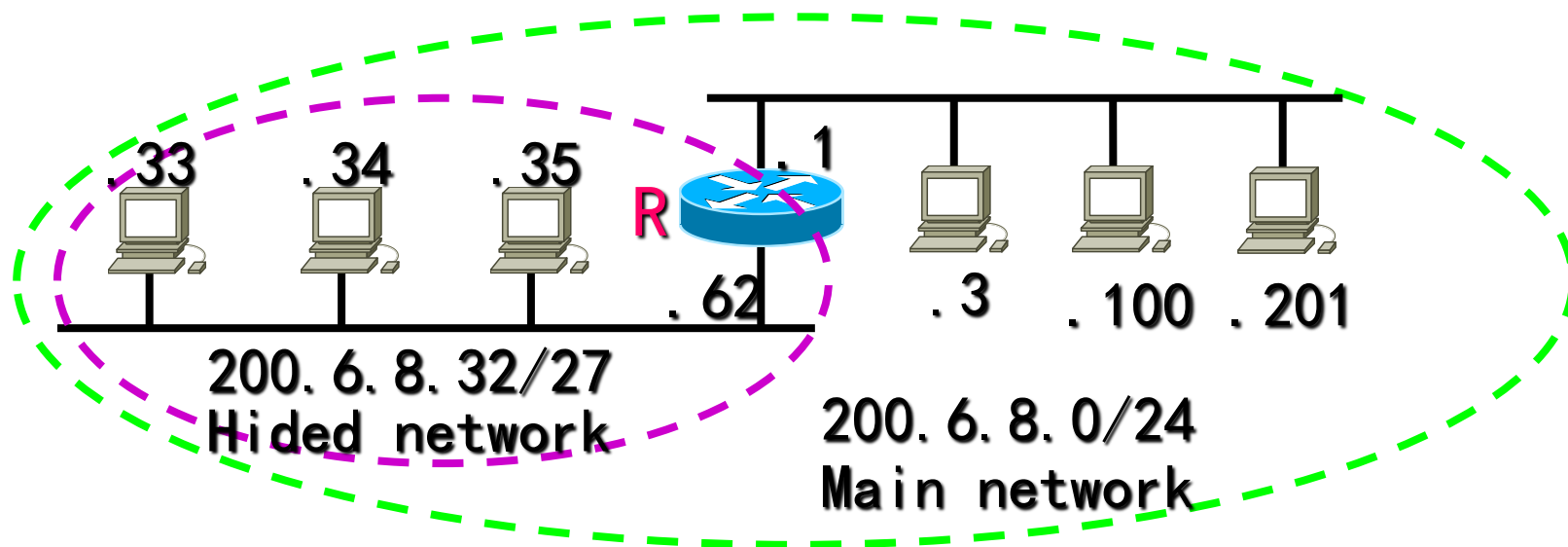
- 主机发送 ARP 广播来查找自己的IP地址，一般发生在系统引导时，用来获取网络接口的MAC地址。

特殊的ARP — 代理ARP

● 工作原理

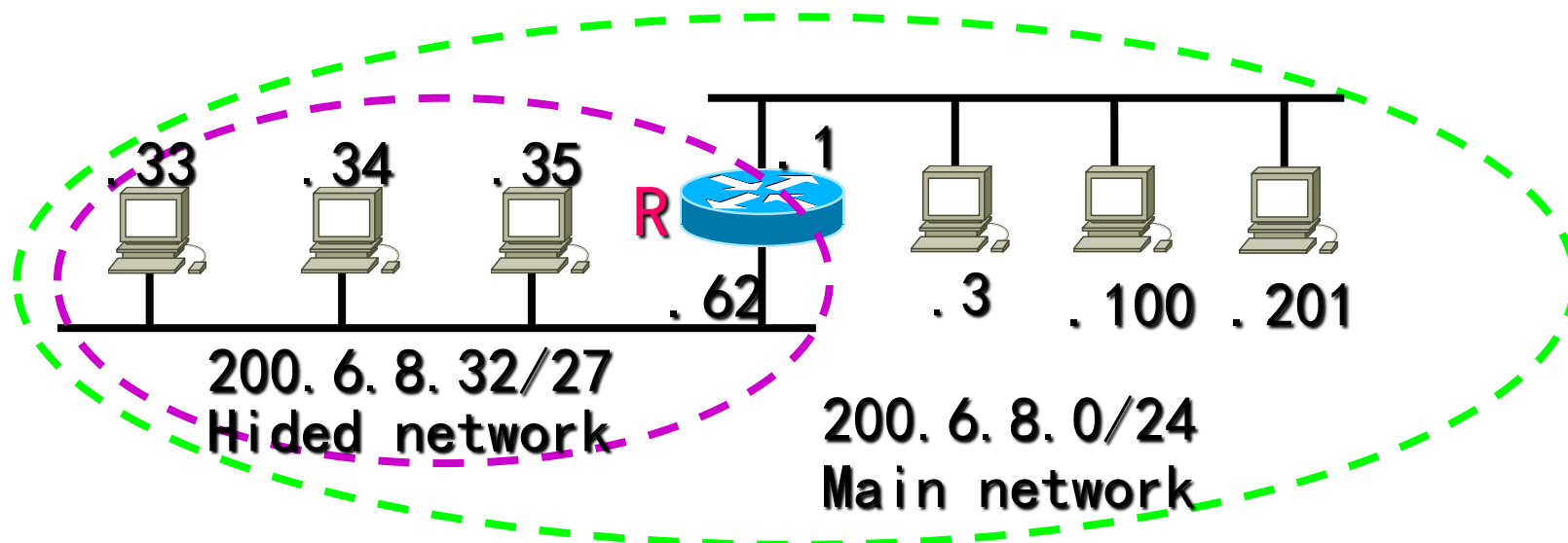


特殊的ARP — 代理ARP



- .35向.3发送IP分组 → IP分组发送成功
 - .35广播请求.62的ARP分组 → ARP成功
- .3向.35发送IP分组 → IP分组发送失败
 - .3广播请求.35的ARP分组, R不转发广播 → ARP失败

特殊的ARP — 代理ARP



特点：

- 针对具体的网络接口实现
 - 如：R在.62接口上可不启用代理ARP
- 多个IP地址与一个MAC地址的映射关系
 - 如：.3中，.33、.34、.35都映射于R的.1接口的MAC地址
- 保留网络外部特性，隐藏了内部网络的结构