



江苏师范大学  
JIANGSU NORMAL UNIVERSITY

电气工程及自动化学院  
SCHOOL OF ELECTRICAL ENGINEERING & AUTOMATION

# 计算机网络技术

授课教师：李灿

联系方式：57862787

[lic@jsnu.edu.cn](mailto:lic@jsnu.edu.cn)

课程网站：[sslic.cn/cnet](http://sslic.cn/cnet)

教研室：12#-407A（轨道交通系）



# 第5章 网络互连与因特网基础



# 本章内容

---

- 网络互连的基本概念
- 因特网接入技术
- 因特网的链路层与网络层
- 因特网的传输层协议

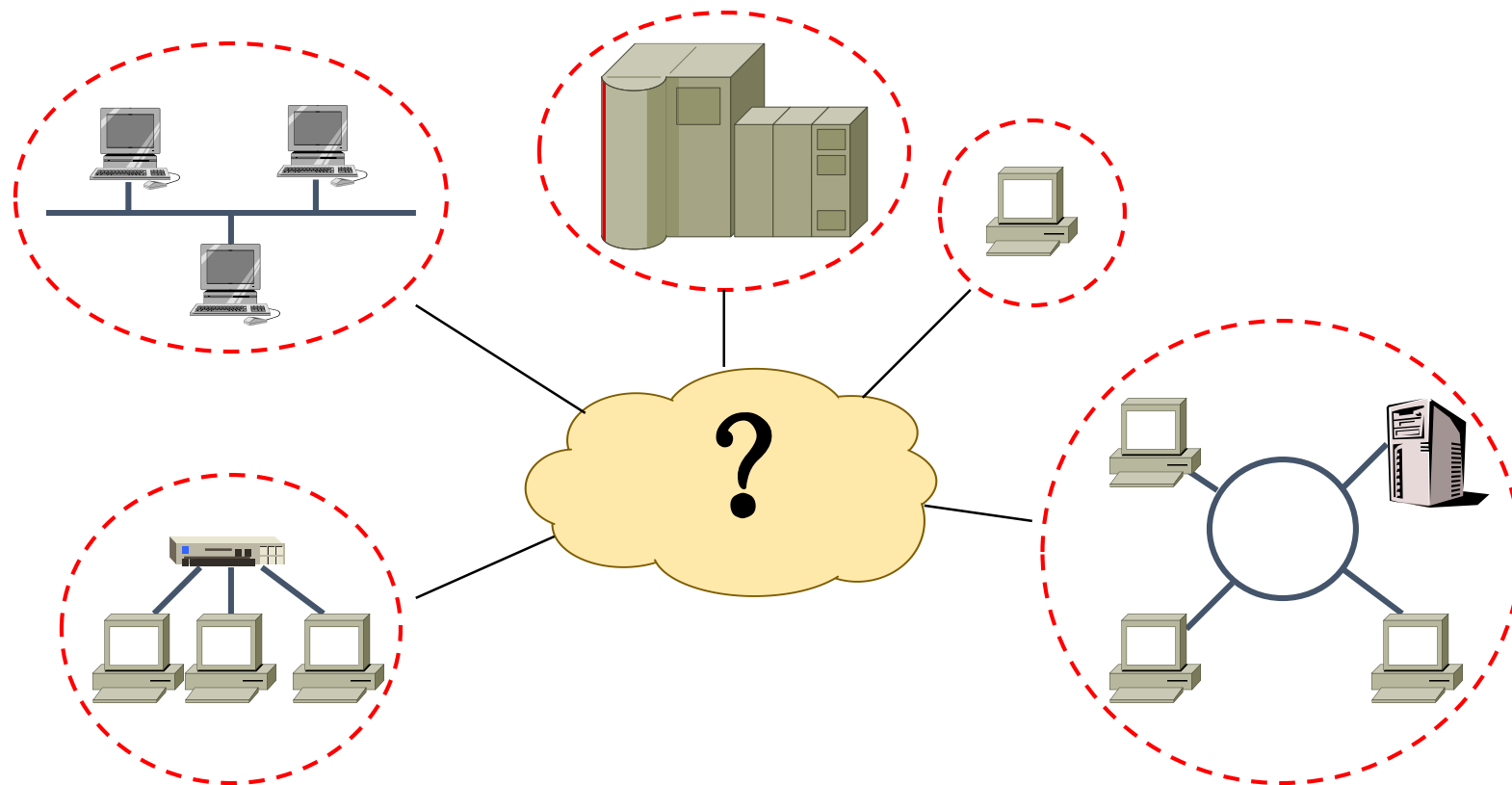


# 因特网概述

1. 因特网也叫**国际互联网**；
2. 因特网使用的协议是**TCP/IP协议（1983年）**；
3. 组成因特网的计算机网络包括**局域网**、**城域网**以及大规模的**广域网**；各种类型的计算机通过有线和无线连接在一起，构成因特网。
4. 通过相互连接，**主干网络**之间以高速通信线路互联，承担了网络上大部分的通信任务。
5. 由于因特网最早是从美国发展起来的，所以这些线路**主要在美国**交织，并扩展到世界各地。
6. 每个主干网络间都有许多交汇的节点，这些节点将下一级较小的网络和主机连接到主干网络上，这些较小的网络则为该服务区域的公司和个人用户提供连接服务。

# 5.1 网络互连的基本概念

- 网络互连的动力：更大范围的资源共享
- 网络互连：**HOST-LAN、LAN—LAN/WAN**
- 因特网协议：**TCP/IP**





# 网络互连的目的

1. 将不同/相同的网络用互连设备连接形成范围更大的网络
2. 为增加网络性能以及安全和管理方面的考虑将原来一个很大的网络划分为几个网段或逻辑上的子网
3. 实现异种网之间的服务和资源共享

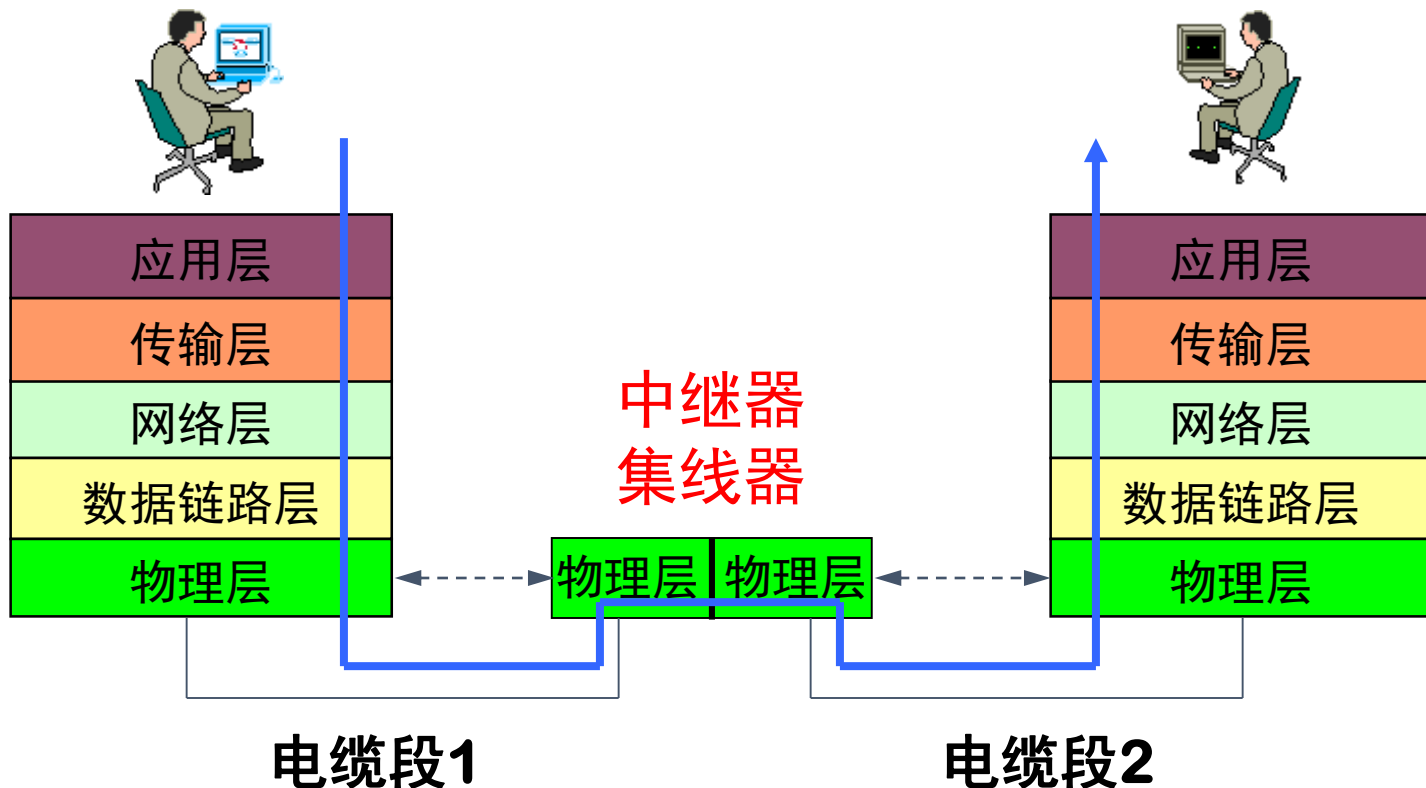


# 网络互连的层次

- 从网络体系结构的观点，网络互连可在四个层次上实现：
  - 物理层
  - 数据链路层
  - 网络层
  - 传输层和应用层

## ■ 物理层：中继器/集线器

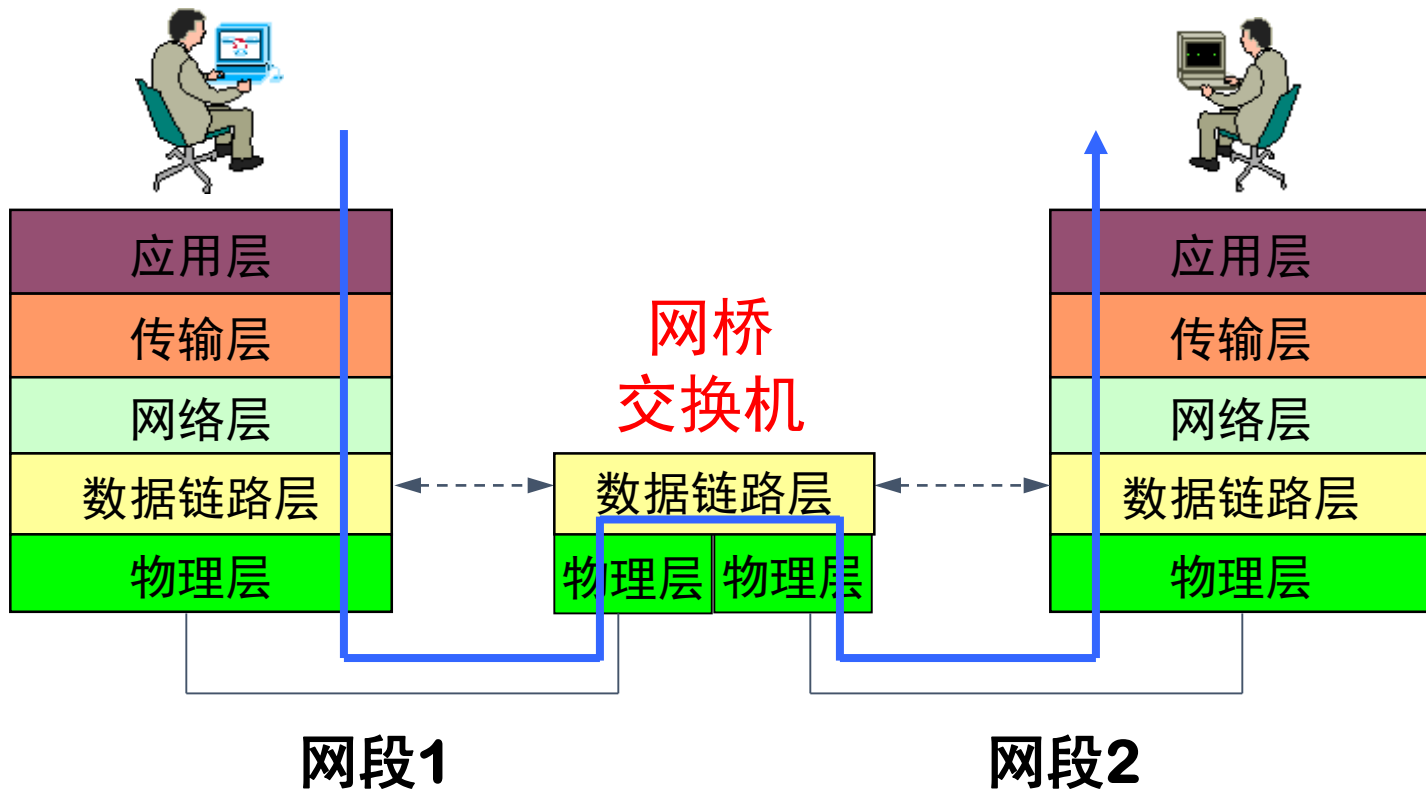
- 在电缆段之间复制位信号
- 没有地址概念，无寻址功能，本质上不能算网络互连





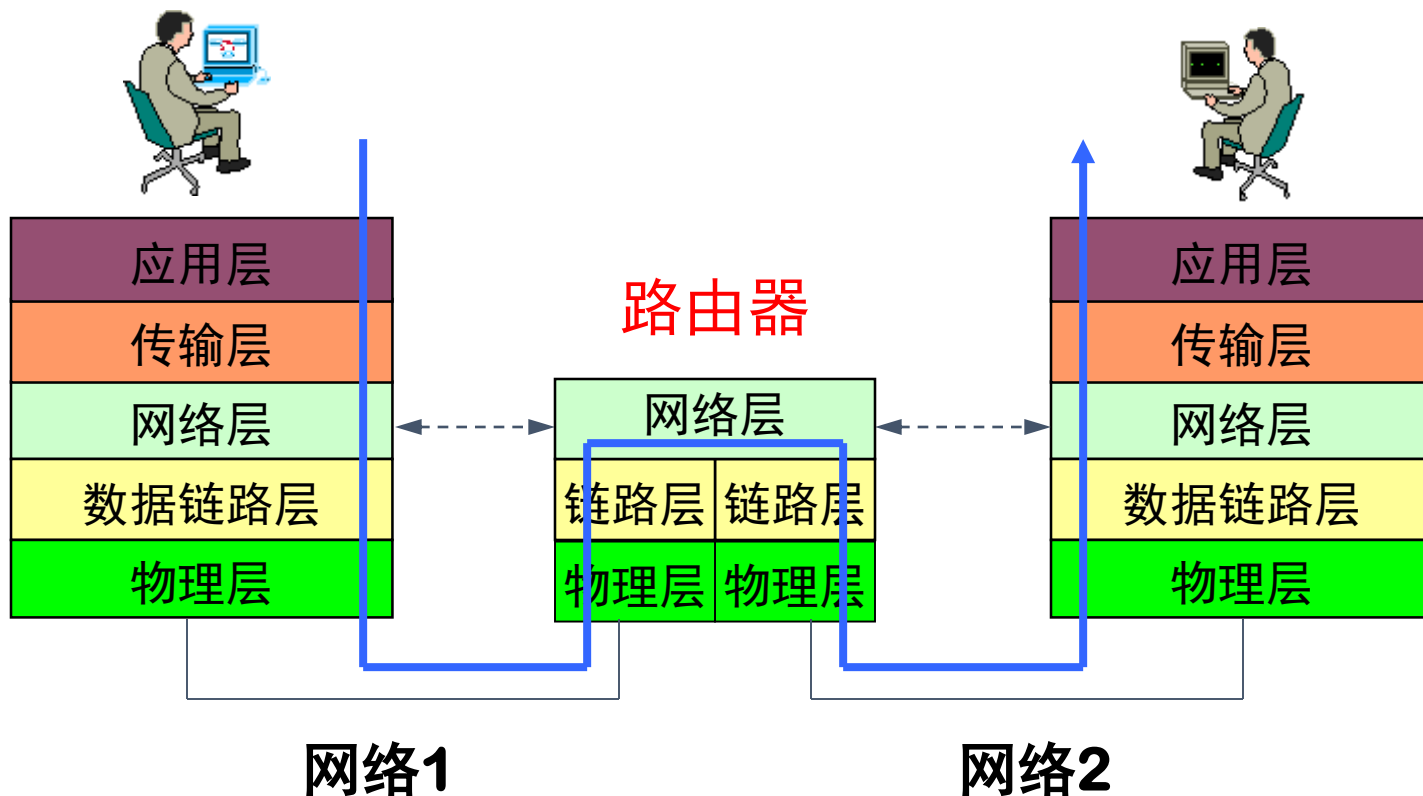
## ■ 数据链路层：网桥/交换机

- 在局域网之间复制数据帧
- 根据数据帧中的信息（MAC地址）进行转发



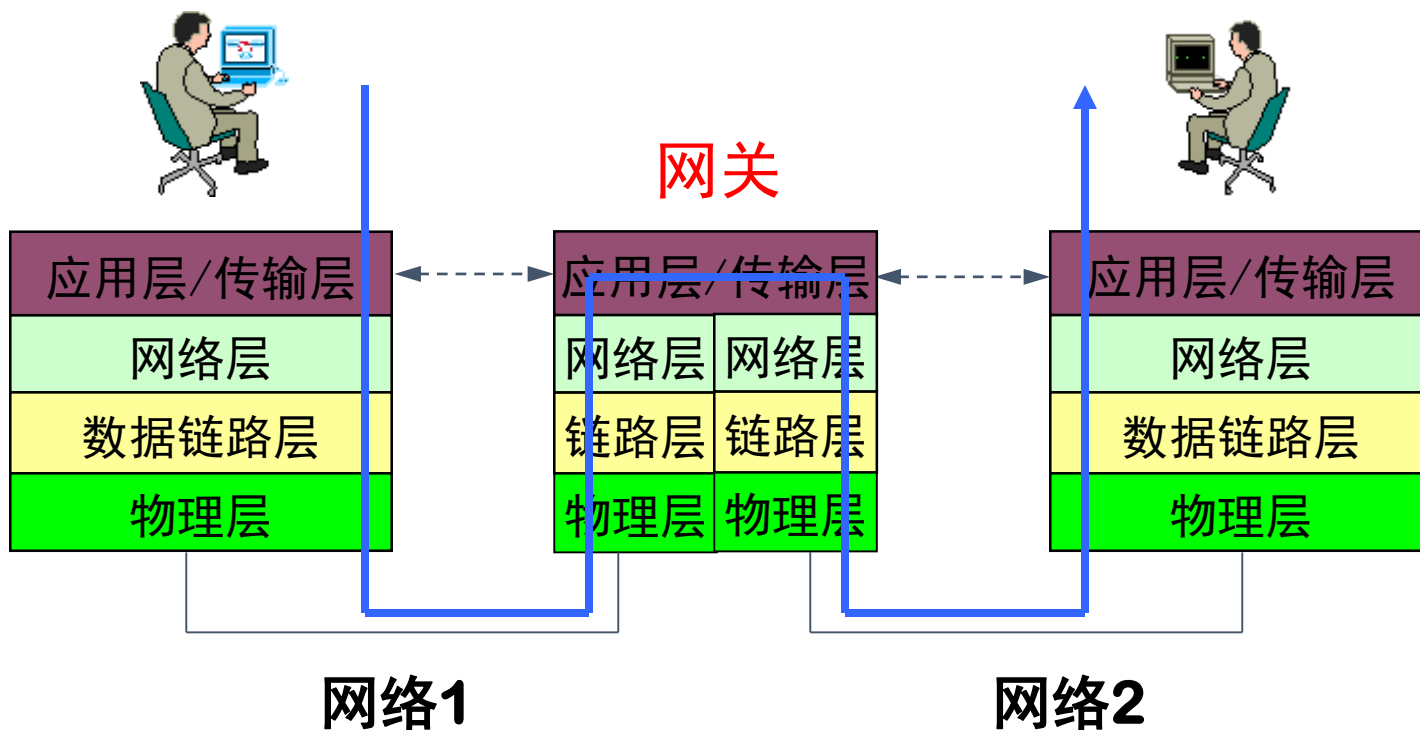
## ■ 网络层：路由器

- 在**网络**之间转发**报文分组**
- 根据分组中的逻辑地址（**IP地址**）进行转发



## ■ 传输层及应用层：网关

- 连接不同体系结构的网络
- 根据端口或其他特定标识寻址





# 不同类型网络互连

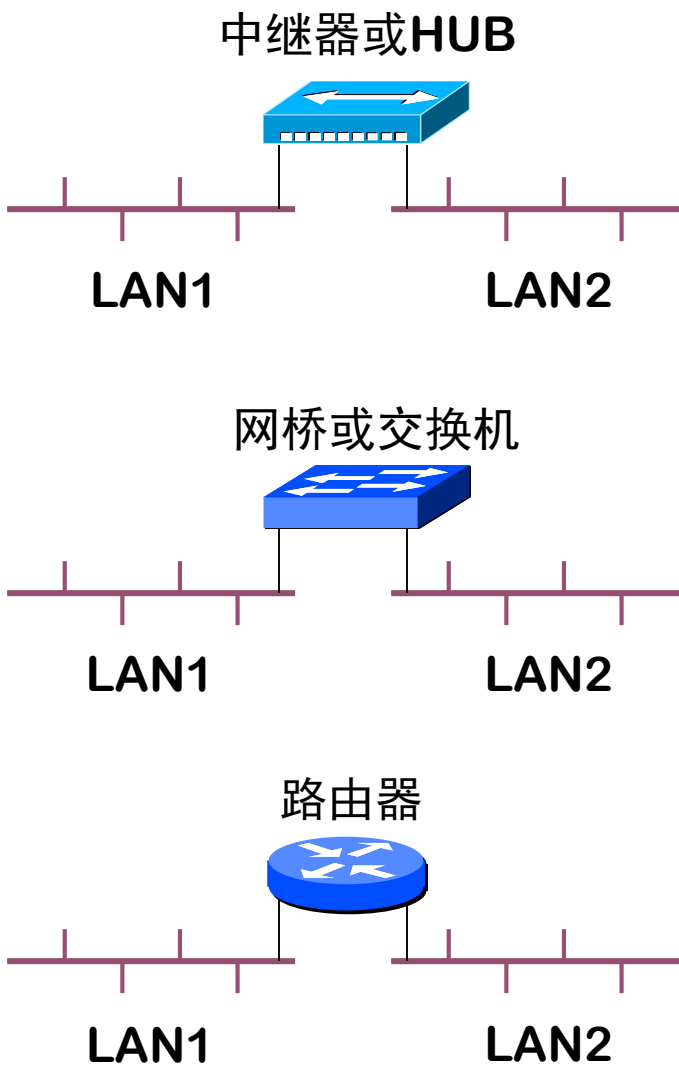
## ■ LAN——LAN互连

- 特点：范围有限、主干（**Backbone**）采用局域网技术  
如：**FDDI、Ethernet、Token Ring**
- 互连层次：**物理层**或者**数据链路层**
- 互连设备：中继器、集线器、网桥、交换机、**路由器**

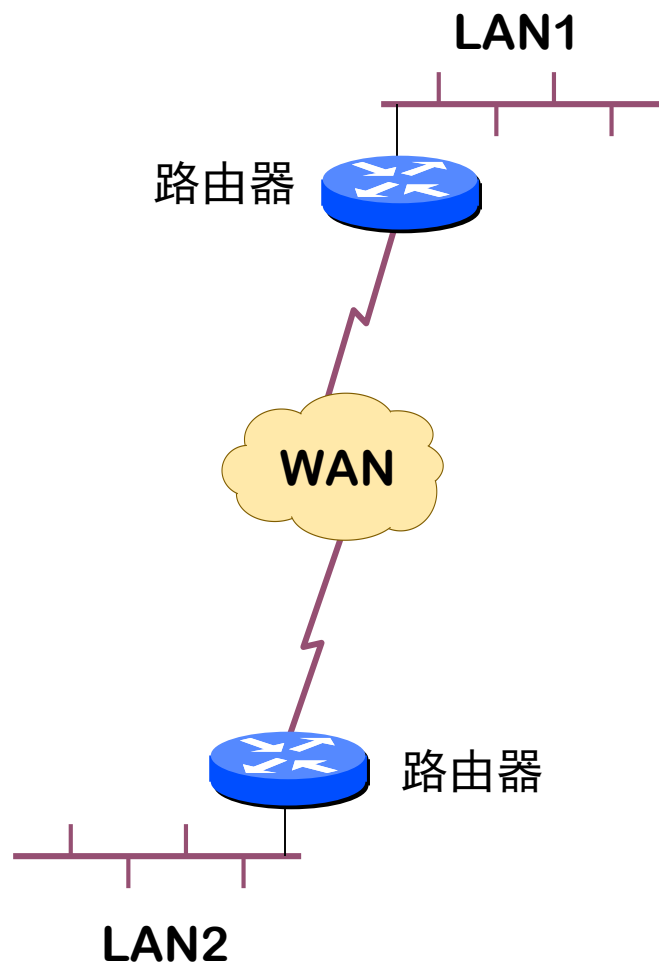
## ■ LAN——WAN互连

- 特点：范围大、主干采用广域网技术
- 互连层次：**网络层**或**更高层**
- 互连设备：路由器、网关（有时可采用远程网桥）

本地



远程





## 5.2 因特网的接入

- **因特网的接入**：如何把用户的计算机连接到因特网的接入点——因特网的边缘路由器
- 按用户类型划分：
  - 住宅接入
  - 机构接入
  - 移动接入



## 5.2.1 住宅接入网络

---

- 基于电话线接入
  - 电话拨号
  - ISDN
  - ADSL
- 基于闭路电视网接入
  - Cable Modem



## 5.2.1 住宅接入网络

### ■ 模拟调制解调器通过电话交换网拨号上网

- 用户计算机通过电话拨号与因特网服务提供商建立连接，在用户本地环路上传输的是模拟信号
- 拨号接入的速率最高不超过56kb/s

### ■ ISDN：一线通

- 在用户本地电话线环路上采用数字信号传输技术，能够在一条电话线上同时提供话音服务和数据通信服务，其接入速率一般可达到128Kb/s，ISDN只是一种过渡的技术





## 5.2.1 住宅接入网络

- 模拟调制解调器通过电话网拨号上网
- ISDN
- **ADSL**（非对称用户线路）
  - 在用户本地电话线环路上采用数字信号传输技术，能够在一条电话线上同时提供话音服务和数据通信服务，其下行传输速率可达到**8Mb/s**，上行传输速率也能达到将近**1Mb/s**
  - **上下行速率不对称**的特点非常适用于上网目的以因特网浏览为主的用户



## 5.2.1 住宅接入网络：线缆调制解调器

### ■ HFC: Hybrid Fiber Coax (光纤同轴电缆混合网络)

- 各住宅小区通过光纤与电信网连接，在小区内部则使用同轴电缆接到各住户
- HFC需要一种特殊的称为**线缆调制解调器**的设备来**支持网络接入**
- HFC通常由**光纤干线**、**同轴电缆支线**和**用户配线网络**三部分组成，从有线电视台出来的节目信号先变成光信号在干线上传输；到用户区域后把光信号转换成电信号，经分配器分配后通过同轴电缆送到用户

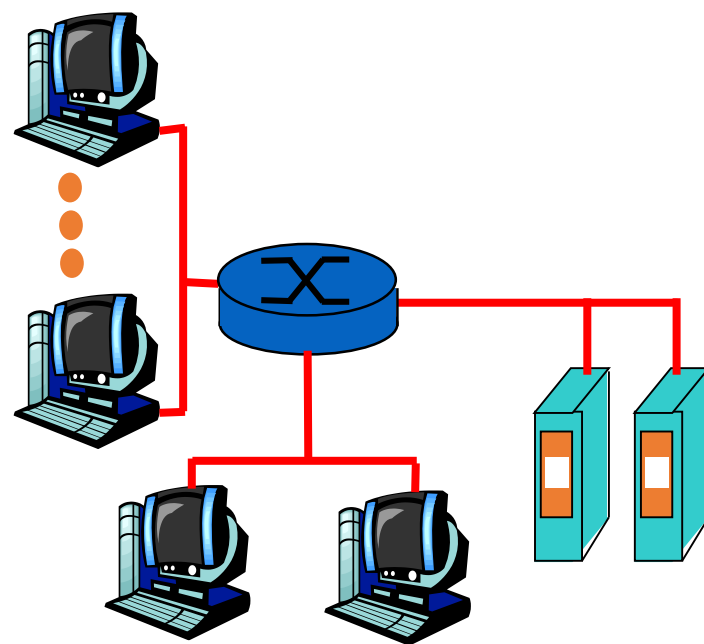


## 5.2.1 住宅接入网络：线缆调制解调器

- **HFC: Hybrid Fiber Coax**（光纤同轴电缆混合网络）
- **非对称**：下行可达**10Mb/s**，上行近**1Mb/s**
- **HFC**将家庭用户连接到 **ISP**（因特网服务提供商）的路由器
  - 若干个家庭用户**共享**上下行访问**带宽**
  - 关注点：拥塞，规模控制问题
  - 应用：在国内的个别地区试点
- **光纤接入**：住宅光猫连接光纤，通过双绞线接入用户设备

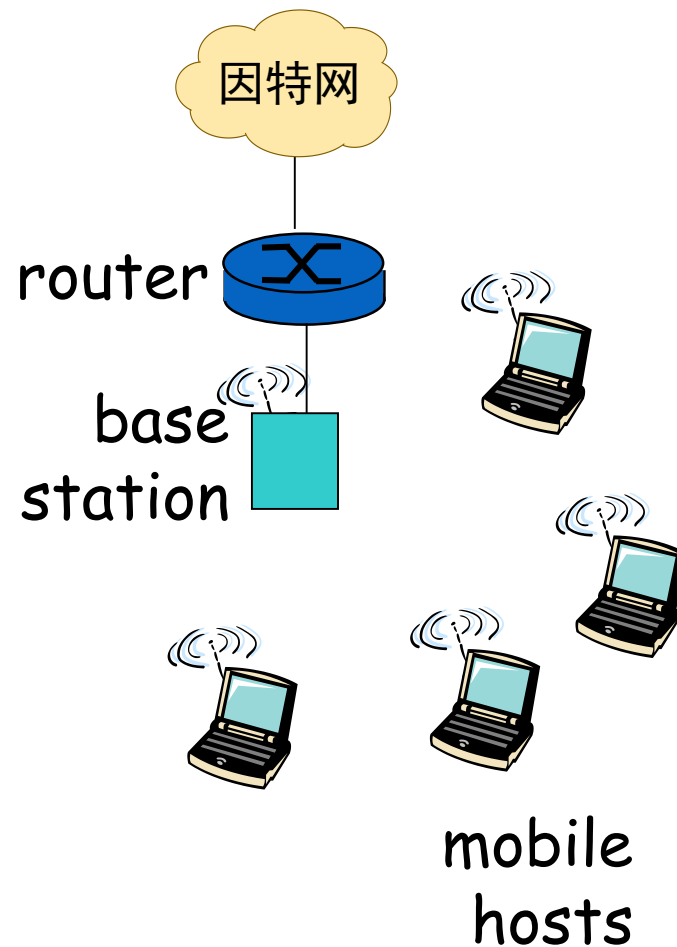
## 5.2.2 机构接入网络：局域网

- 公司/大学通过**局域网 (LAN)** 接入因特网的边缘接路由器
  - **局域网多是以太网**，需再配置一台路由器，才能与因特网的边缘路由器相连
  - 共享或专线电缆将计算机连接到路由器
  - 100Mb/s, 1Gb/s 以太网
- **应用**：企事业单位，住宅小区普遍使用的**LAN**



## 5.2.3 移动接入网络

- 使用无线电波连接移动式端系统和基站，再从基站接入边缘路由器
- 真正的无线互联网
- CDPD（蜂窝数字式分组数据交换网络）  
通过蜂窝式网络无线访问ISP路由器  
一个与蜂窝电话网络重叠的虚拟网络
- 使用CDPD只需在便携机上连接一个专用的无线调制解调器，即使坐在时速100公里的车厢内，也不影响上网
- 优势：可以利用现有的模拟传输的基础设施，投资小





## 5.3 因特网的链路层和网络层

### ■ 链路层协议

- **PPP**、**HDLC**、局域网相关协议（第6章）

### ■ 网络层协议

- **IP**：互联网络协议
- **ICMP**：因特网控制报文协议
- 路由协议
- **IGMP**：组播协议
- **ARP**、**RARP**



## 5.3.1 点对点协议：PPP

- 主要应用：拨号上网
- 一方发，一方收；一条链路：比广播信道简单得多
  - 不存在寻址问题（不必进行MAC寻址）；
  - 不会发生访问链路的冲突（无需介质访问控制）
  - 支持：电话拨号链路，ISDN 线路、X.25、DDN（数字数据网）等



# \*PPP 设计要求 [RFC 1557]

- **分组的成帧:** 将网络层的分组封装到数据链路层的帧中
  - 同时可以承载任意网络协议的网络层数据 (不仅仅是 IP)
  - 提供向上分用的能力
- **透明:** 在数据字段中, 必须能携带任意组合的位流, 不得限制网络层分组中位流的组合方式
- **差错检测 (但无需校正)**
- **网络层地址协商:**  
使得客户端的网络层可以学习/配置对方提供的网络地址
- **支持多种网络层协议**
- .....



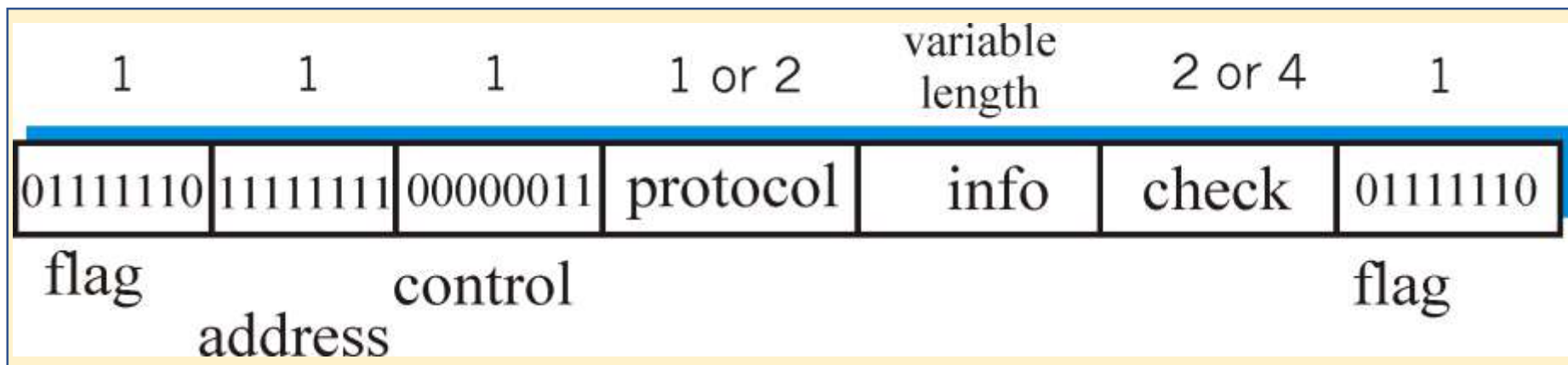


# PPP 组成

---

1. 串行通信线路上的**组帧方式**
2. **链路控制协议LCP**  
用于建立、配置、测试和拆除数据链路
3. **一组网络控制协议NCPs**  
用以支持不同的网络层协议

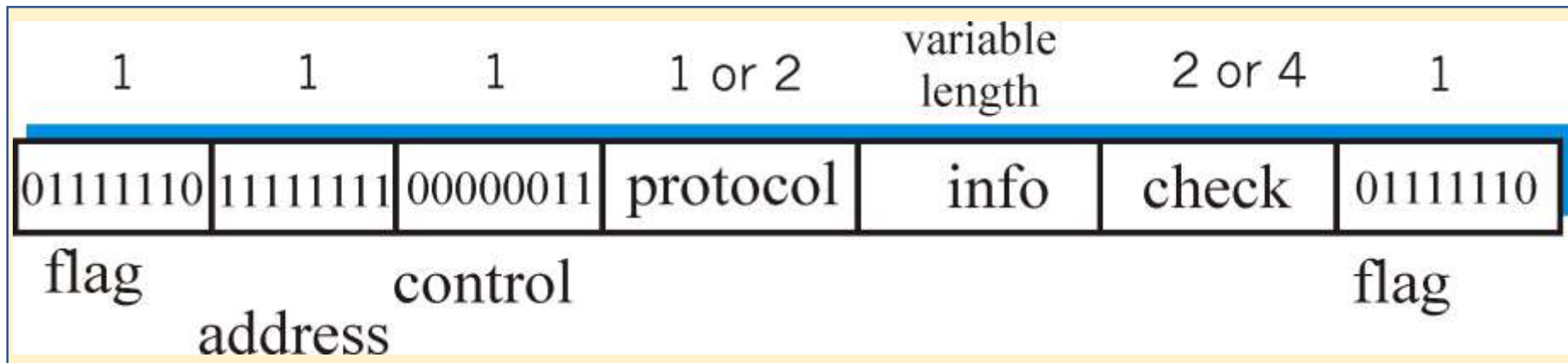
# PPP 数据帧（类似HDLC）



- **Flag**: 帧定界符(**7EH**)
- **Address**: 固定为**FFH**, 所有站必须接收
- **Control**: 缺省为**03H**, 表示为无编号帧
- **Protocol**: **数据类型**, 即帧中携带的数据属于哪一个上层协议 (LCP, IP, IPCP,...)

例: 取**C021H**表示链路控制数据, 取**0021H**表示IP分组, 取**8021H**表示网络控制数据

# PPP 数据帧（类似HDLC）



- **Flag**: 帧定界符(**7EH**)
- **Address**: 固定为**FFH**, 所有站必须接收
- **Control**: 缺省为**03H**, 表示为无编号帧
- **Protocol**: **数据类型**, 即帧中携带的数据属于哪一个上层协议
- **Info**: 所携带的上层数据
- **Check**: **CRC**校验和, 用于进行错误检测

**PPP**: 单点通信  
**HDLC**: 多点寻址



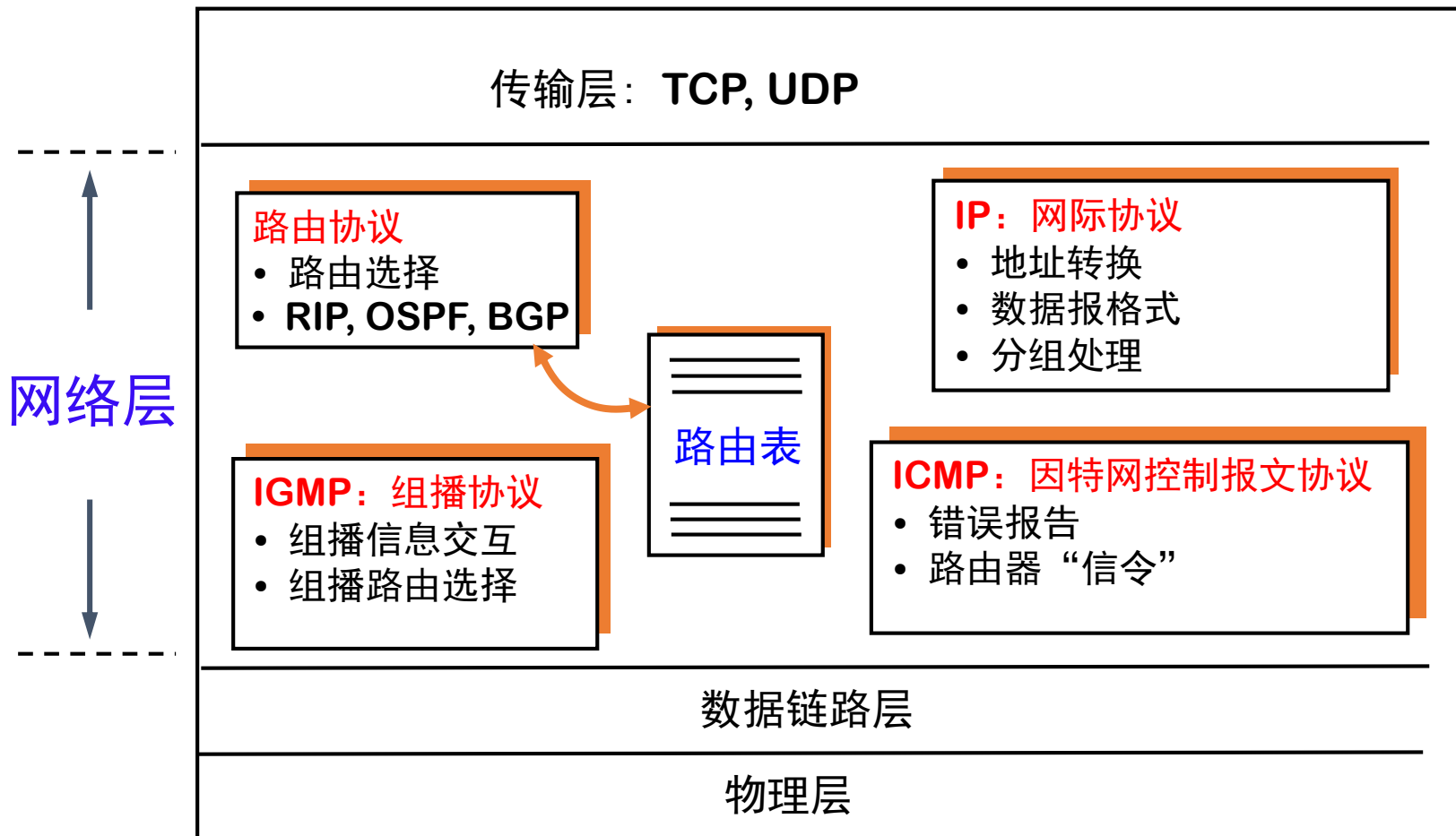
## 5.3.2 网络层与IP

---

- 因特网的网络层：
  - 仅提供无连接的数据报服务
  - 属于“尽力而为”的服务

## 5.3.2 网络层与IP

### ■ 因特网的网络层功能：





# 网络层协议组成

## 1. 网络互联协议IP

决定网络层的**编址机制**、数据报的格式（网络层的**PDU**）、各节点根据数据报的字段所应采取的动作

- IP协议有两个版本，**IPv4** 和**IPv6**

## 2. 路由选择协议

决定数据报在发送过程中**由信源到信宿所经过的路由器**

## 3. 网络控制信息协议ICMP

为用户提供网络中的**各种运行信息**

## 4. 组播协议IGMP

由于数据报的发送前不需要建立连接和接收方的响应，因此可以支持因特网上的**多点同时传送**



# 1. IP

- **IP: Internet Protocol**（网络之间互连的协议）
- **IP**规定了计算机在因特网上进行通信时应当遵守的规则  
任何厂家生产的计算机系统，只要遵守**IP**协议就可以与因特网互连互通
- **IP**提供**数据报**投递服务（主机到主机）
- **IP**的数据报投递服务是非连接、不可靠的
  - 非连接
    - 数据报之间没有相互的依赖关系
    - 不能保证报文的有序投递
  - 不可靠
    - 数据报的投递没有任何品质保证（**QoS**），数据报可能被正确投递，可能被丢弃
- **IP**地址具有**唯一性**，根据用户性质的不同，可以分为**5**类



# 1. IP： 相关概念

- 主机是**通过链路**与网络相连
- **主机与链路之间的边界**称为“**接口**”
- **路由器**的任务是在“**进线**”上**接收数据**，在“**出线**”上进行**转发**，至少要连接两条以上链路
- **路由器与链路之间的边界**也称为“**接口**”；路由器上有**多个接口**
- **每个接口都需要一个IP地址**
- 从技术上说，**IP地址只是与接口有关**
- **因特网上主机与网络的每个接口都必须有一个唯一的IP地址**，如果一台主机或路由器同因特网有多个接口，可以拥有多个**IP地址**，每个接口对应一个**IP地址**





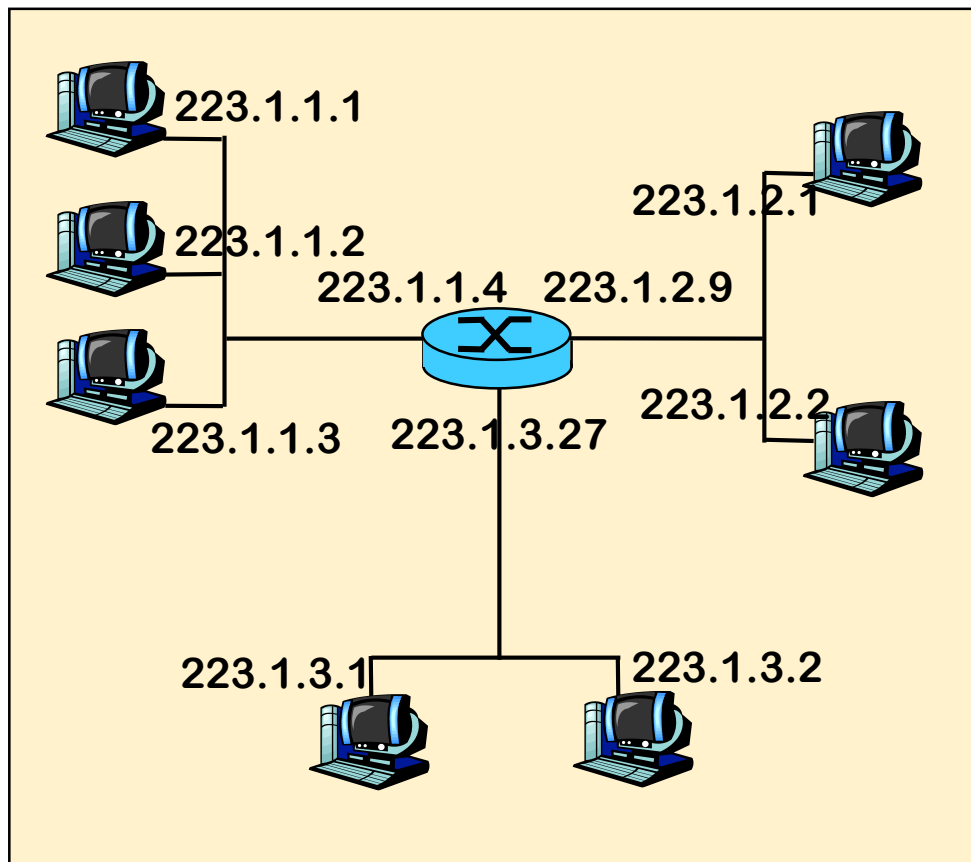
## 2. IP地址 (IPv4地址)

### ■ IP地址:

- **32bit**的逻辑地址, 用来在因特网中标识主机或路由器的网络接口

### ■ IP地址书写方法

- **32bit**划分为4个字节
- 写成**点分**的4个十进制数  
每个数范围**0~255**
- **点分十进制表示法**



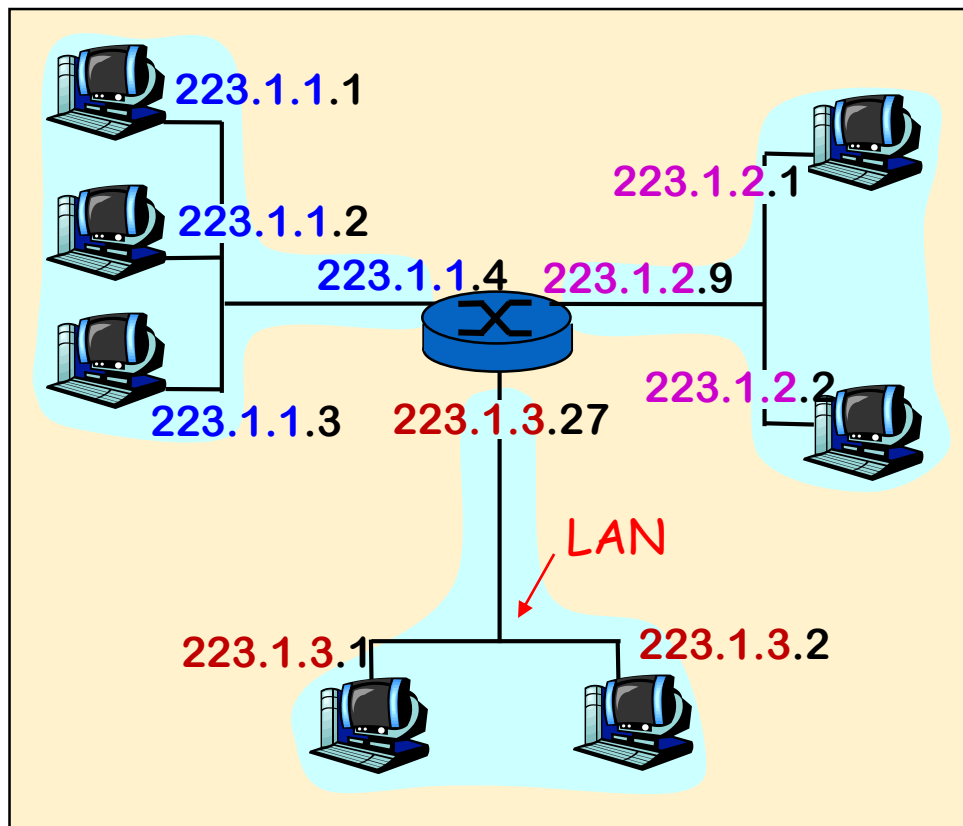
$$223.1.1.1 = \underbrace{11011111}_{223} \underbrace{00000001}_{1} \underbrace{00000001}_{1} \underbrace{00000001}_{1}$$

## 2. IP地址（IPv4地址）

### ■ IP地址包括两部分

- 网络地址（网络号）
- 主机地址（主机号）

- 具有相同网络地址的设备接口或  
不经过路由器就可以物理上相互  
通达的设备属于同一个网络



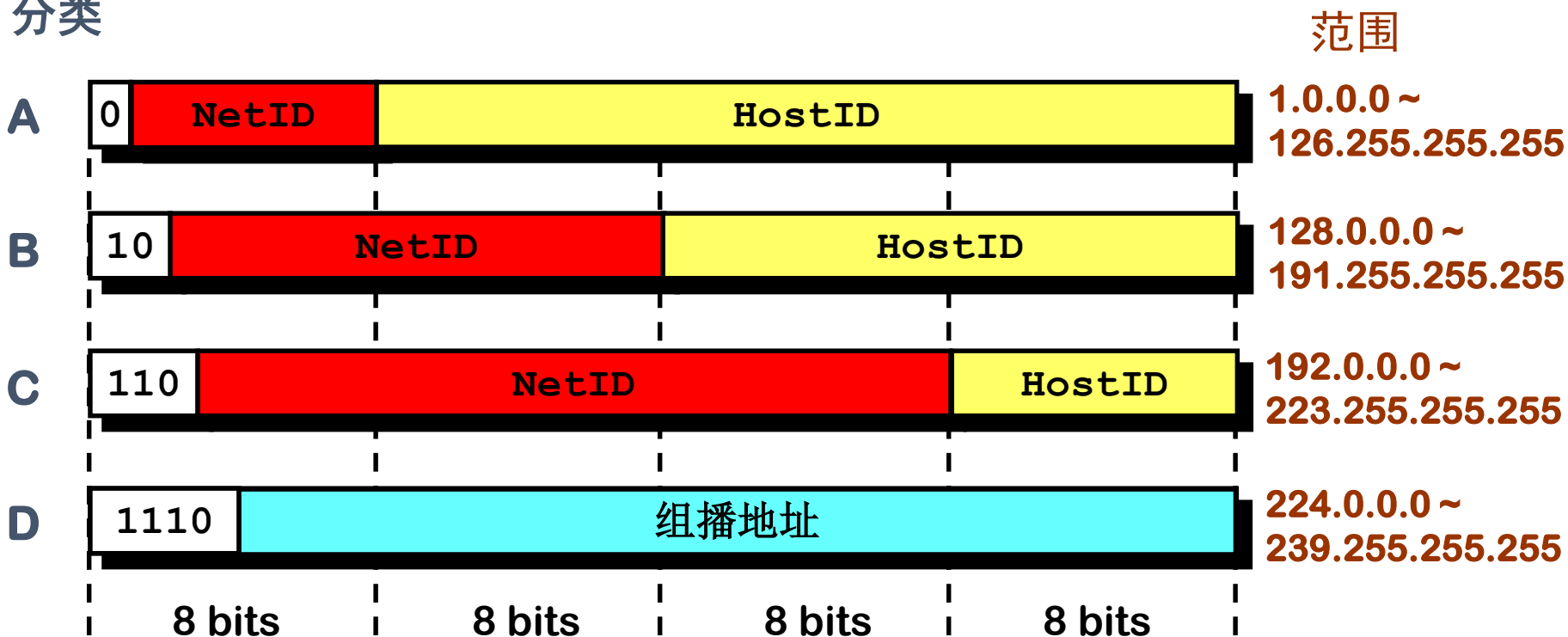
由3个IP网络组成的互联网  
(对于以223开头的IP地址,  
前24位为网络地址)



## 2. IP地址（IPv4地址）

- 为讨论“网络”的说法，重新审视IP地址：
  - 分类编址
  - IP地址分为A、B、C、D、E共5类。常用的是B和C两类

分类



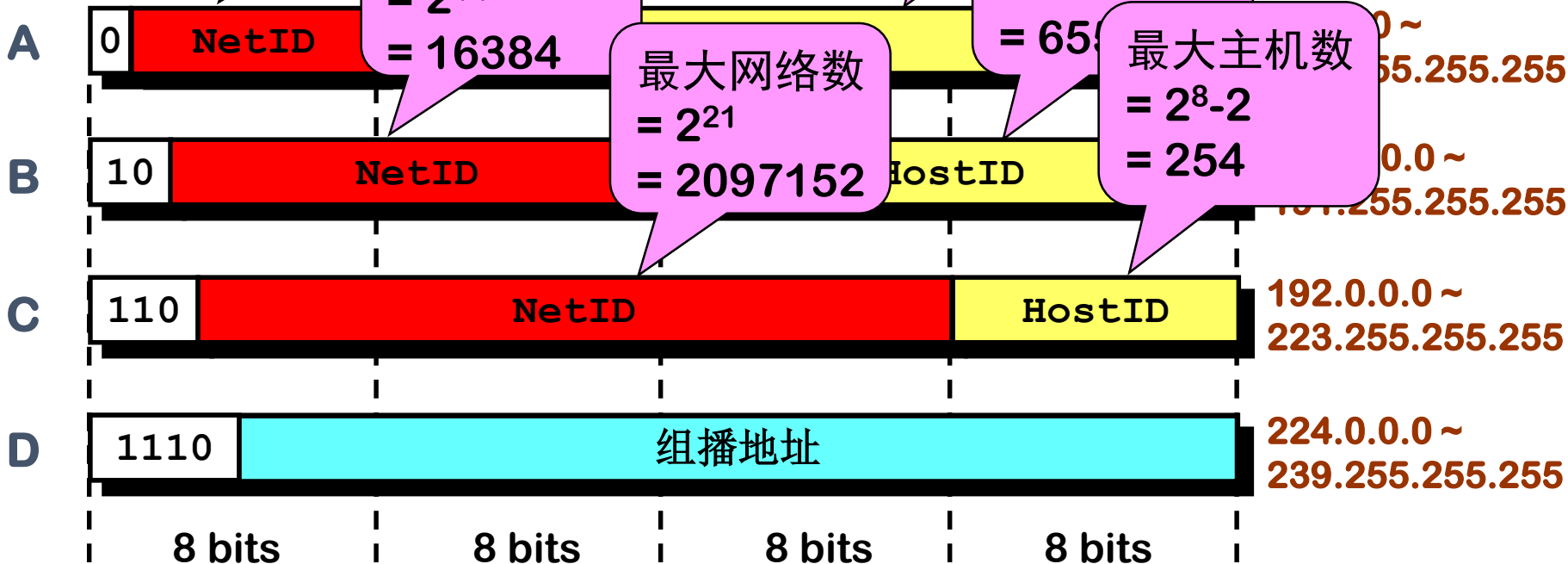
## 2. IP地址 (IPv4地址)

■ 为讨论“网络”的说法，重新审视IP地址：

• 分类编址

• IP地址分类 C、D、E共5类。常

分类





### 3. IP地址分类：A类



#### ■ A类IP地址

- A类IP地址由1字节网络地址和3字节主机地址组成，网络地址的最高位必须是“0”
- A类IP地址中网络的标识长度为7位，主机标识的长度为24位，A类网络地址数量较少，每个网络地址可以用于主机数达1600多万台的大型网络
- A类IP地址地址范围1.0.0.1-126.255.255.254（二进制表示为：00000001 00000000 00000000 00000001 - 01111110 11111111 11111111 11111110）注：全0与全1地址有特殊用途
- A类IP地址的子网掩码为255.0.0.0，每个网络支持的最大主机数为256的3次方-2=16777214台



### 3. IP地址分类： B类



#### ■ B类IP地址

- B类IP地址由2字节的网络地址和2字节主机地址组成，网络地址的最高位必须是“10”
- B类IP地址中网络标识长度为14位，主机标识的长度为16位，B类网络地址适用于中等规模的网络，每个网络所能容纳的计算机数为6万多台
- B类IP地址地址范围128.1.0.1-191.254.255.254（二进制表示为：10000000 00000001 00000000 00000001 - 10111111 11111110 11111111 11111110）
- B类IP地址的子网掩码为255.255.0.0，每个网络支持的最大主机数为256的2次方-2=65534台



### 3. IP地址分类：C类



#### ■ C类IP地址

- C类IP地址由3字节的网络地址和1字节主机地址组成，网络地址的最高位必须是“110”
- C类IP地址中网络的标识长度为21位，主机标识的长度为8位，C类网络地址数量较多，适用于小规模的网络，每个网络最多只能包含254台计算机
- C类IP地址范围 192.0.1.1-223.255.254.254（二进制表示为：11000000 00000000 00000001 00000001 - 11011111 11111111 11111110 11111110）
- C类IP地址的子网掩码为255.255.255.0，每个网络支持的最大主机数为 $256-2=254$ 台



### 3. IP地址分类：其他

- 其他几种特殊类型的IP地址，由TCP/IP协议规定：
  - IP地址中的第一个字节以“1110”开始的地址都叫多点广播地址  
即第一个字节大于223小于240的IP地址是多点广播地址——D类
  - IP地址中的每一个字节都为0的地址（0.0.0.0）对应于当前主机
  - IP地址中的每一个字节都为1的IP地址（255. 255. 255. 255）对应当前子网的广播地址
  - IP地址中以“11110”的地址都留着将来作为特殊用途使用——E类
  - IP地址中不能以十进制“127”作为开头，该类地址中数字127.0.0.1到127.1.1.1用于回路测试  
例：127.0.0.1代表本机IP地址，可以测试本机中配置的Web服务器localhost





## 4. 划分子网

### ■ 为什么要划分子网？

- **IP分类不合理，地址空间利用率低**

- 美国的某些机构拥有的地址空间甚至比其他一些国家的全部地址空间还大

- **每个网络都指定一个网络地址将使路由表太大**

- 增加了路由器成本
- 查找路由耗时增加
- 路由器之间交换的路由信息增加

- **两级IP地址不够灵活**

- 不能充分利用已申请到的地址资源扩充新的网络

### ■ 如何在现有的地址范围中建立多个网络？



# 4. 划分子网

## ■ 划分子网 (Subnetting)

• 又称子网寻址或子网路由选择

• 方法:

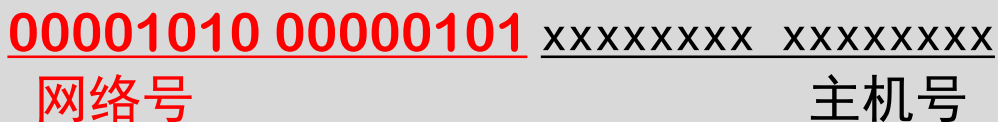
• 从IP地址的主机编号部分“借用”若干位作为子网编号

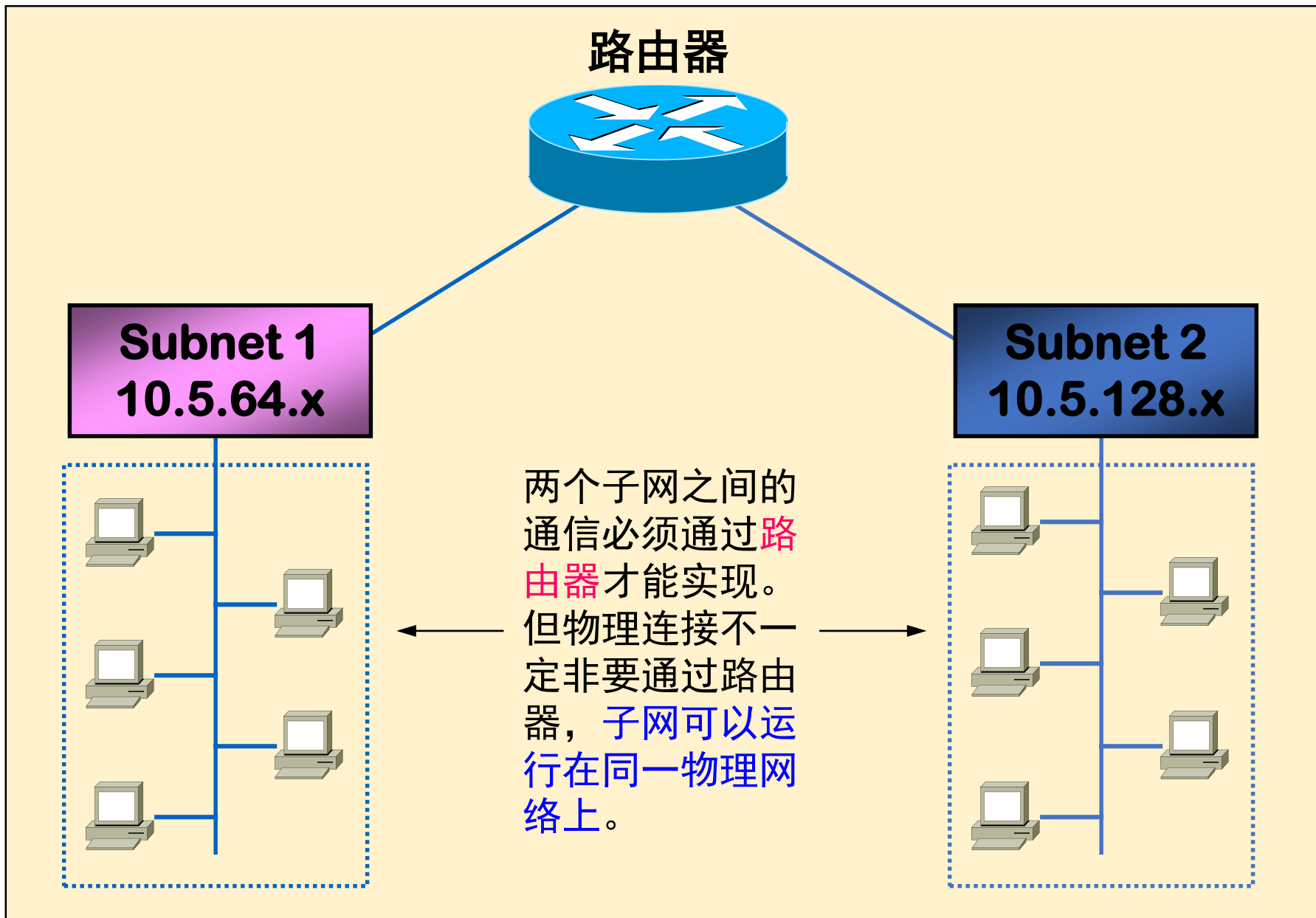
• 主机编号部分相应缩短

• 例如:

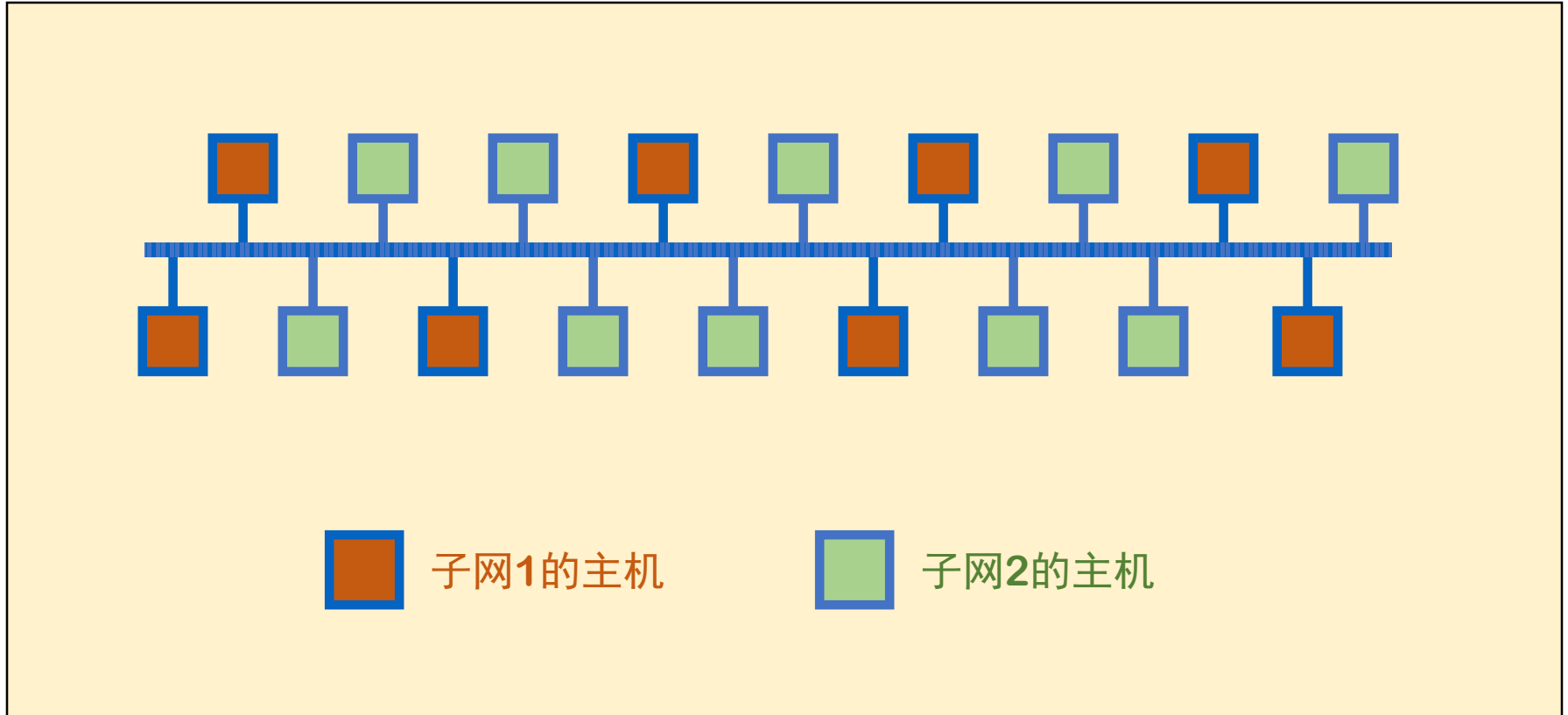
• 原来的网络: 10.5.0.0

• 借用2位划分子网后: 10.5.64.0和10.5.128.0





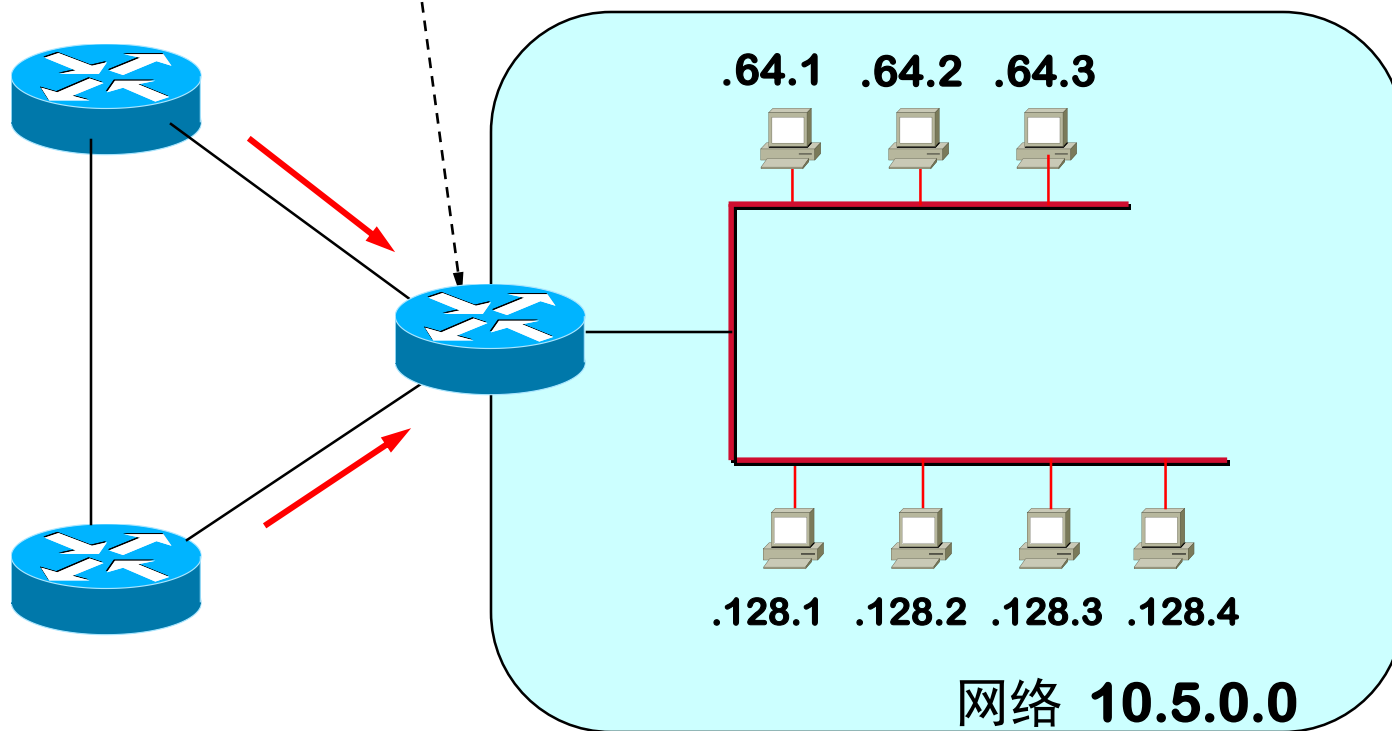
# 在一个物理网络上运行多个子网





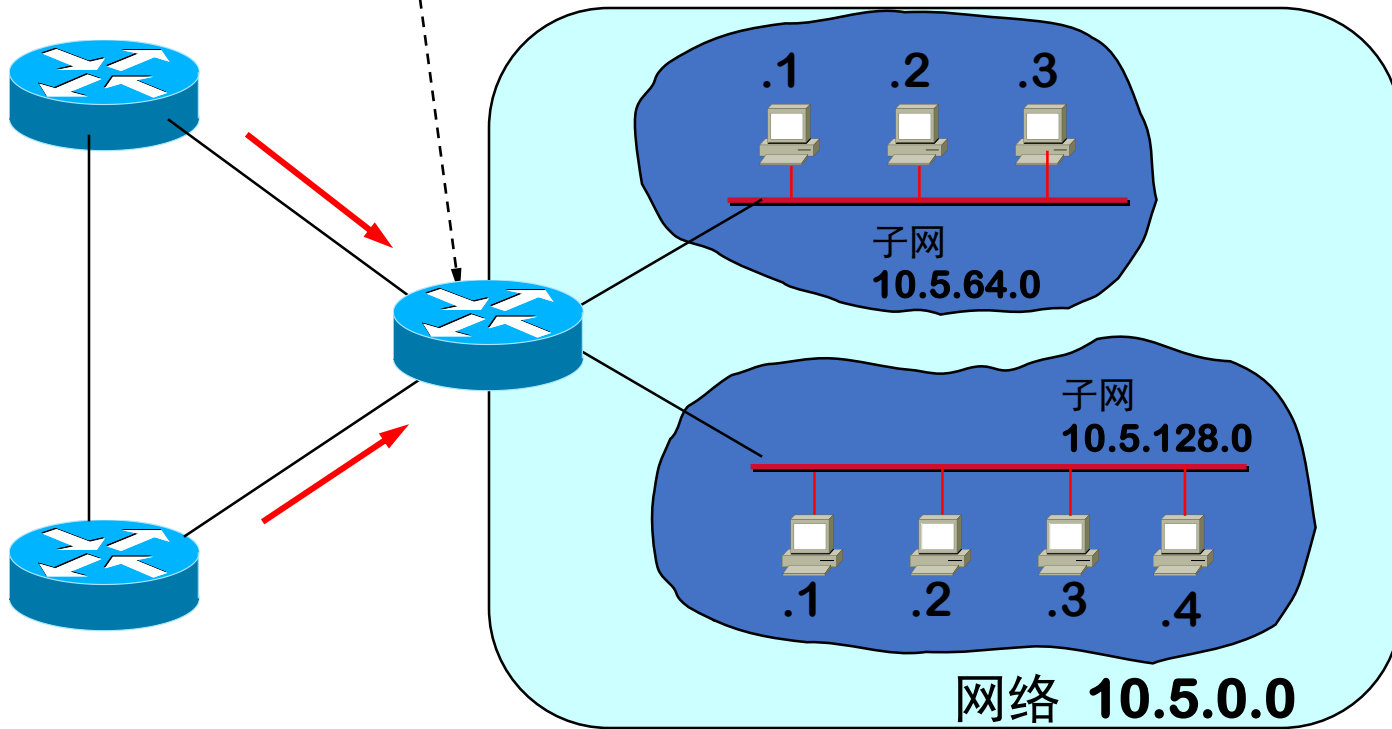
## ■ 划分子网后，网络**对外**仍是一个网络

所有目的地址为  
**10.5.x.x** 的分组  
均到达此路由器



## ■ 划分子网后，网络**对外**仍是一个网络

所有目的地址为  
10.5.x.x 的分组  
均到达此路由器





## 5. 子网掩码

### ■ 子网掩码（subnet mask）

- 又叫网络掩码、地址掩码、子网络遮罩
- 指明一个IP地址的哪些位标识的是主机所在的子网，以及哪些位标识的是主机的位掩码
- 将某个IP地址划分成网络地址和主机地址两部分
- 子网掩码不能单独存在，必须结合IP地址一起使用



## 5. 子网掩码

### ■ 子网掩码的作用

- 使网络内的计算机了解子网划分的结构
- 使边缘路由器了解子网划分的结构

### ■ 子网掩码的格式

- 子网掩码也是32bit长二进制数，由一串连续1后跟一串连续0组成

### ■ 前面的1与网络号和子网号对应，后面的0与主机号对应

例：10.5.0.0

- 子网结构为：00001010 00000101 SS XXXXXXXX XXXXXXXX
- 子网掩码为：11111111 11111111 11 XXXXXXXX XXXXXXXX  
写成十进制数为：255.255.192.0





## 5. 子网掩码

- 不划分子网时，各类IP地址默认的子网掩码为：

- A类：255.0.0.0
- B类：255.255.0.0
- C类：255.255.255.0

- 已知IP地址和子网掩码，如何计算子网地址？

- 用子网掩码和IP地址“按位相与”（AND操作），结果就是子网地址
- 例：IP地址10.5.100.1，子网掩码255.255.192.0，则子网地址为：

	00001010	00000101	01100000	00000001
AND)	11111111	11111111	11000000	00000000
	00001010	00000101	01000000	00000000
				(=10.5.64.0)

推论：若两个IP地址具有完全相同的子网地址，则它们在同一子网中



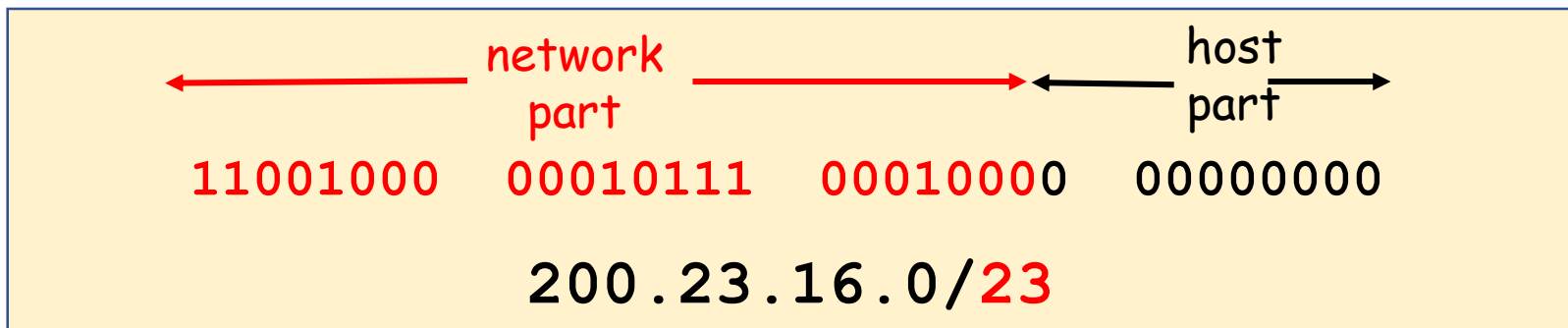
## 6. CIDR（无类域间路由）

### ■ 分类编址：

- 地址空间的利用率低，地址空间面临耗尽
- **例：**一个B类网址可以容纳65K台主机，但可能被一个只有2K台主机的企业占据

### ■ CIDR: Classless Inter-Domain Routing

- 地址的网络部分长度任意，不再分为固定的几种类型
- 地址格式: **a.b.c.d/x**，x为地址中网络部分的位数  
即子网掩码的位数





## 7. IP地址分配（P155）

- 用户IP地址 ← ISP ← InterNIC（国际互联网络信息中心）  
固定分配——静态IP地址

- IP地址资源有限，IP地址随用随申请，用完即归，不独占

- 动态主机配置协议：Dynamic Host Configuration Protocol, DHCP

- 可以提供即插即用接入机制
- 允许计算机加入到某一网络并自动获取IP地址而无须人工分配和配置
- 大量使用于拨号上网、ADSL上网和局域网应用
- DHCP对运行客户端和服务端的计算机都适用
- DHCP使用客户端/服务器方式运作
- DHCP也很适合于经常移动处所的计算机

- 查看网络属性



## 7. IP地址分配：DHCP

- 网络中需设置一台**DHCP服务器**
- 网络管理员在**DHCP服务器**中预先定义一个**IP地址池**
- **分配过程：**
  - 需要**申请IP地址**的主机在网络中广播 “**DHCP discover**” 报文
  - 网络中的**DHCP服务器**用 “**DHCP offer**” 报文**响应**
  - 主机发送**IP地址请求**：“**DHCP request**” 报文
  - **DHCP服务器**从地址池中**取出一个未被分配的IP地址**发送**给请求者**：“**DHCP ack**” 报文
- 互联网上的**IP地址**统一由**IANA**（Internet Assigned Numbers Authority，互联网网络号分配机构）的组织来管理

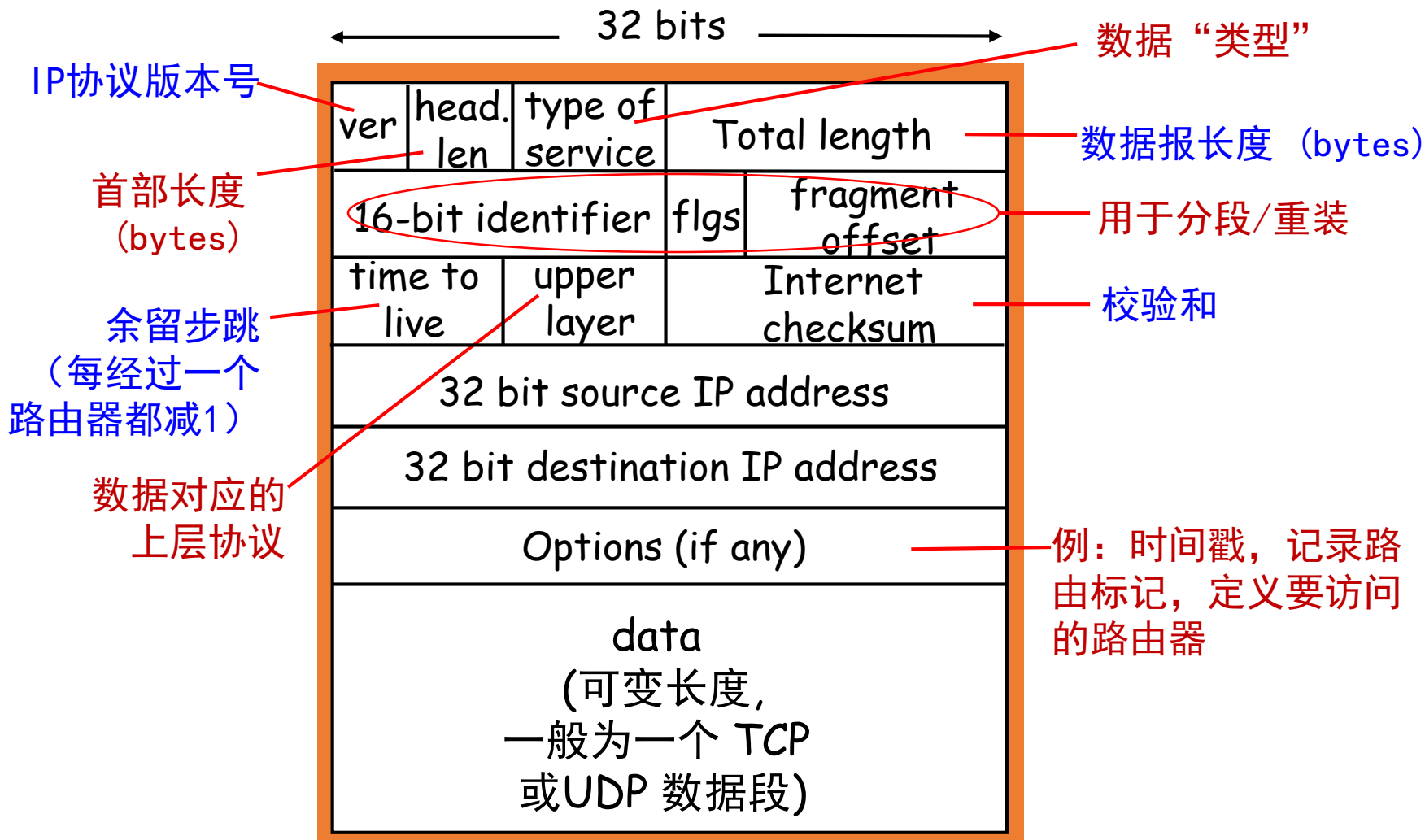


## 8. IP数据报格式（P141）

---

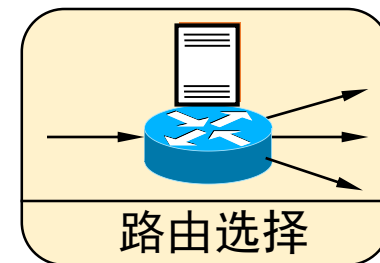
- IP数据报由**数据报头**和**数据域**两部分数据组成
- 报头由长度为**20字节**的**固定部分**和**可变长度**的**选项部分**组成

# 8. IP数据报格式



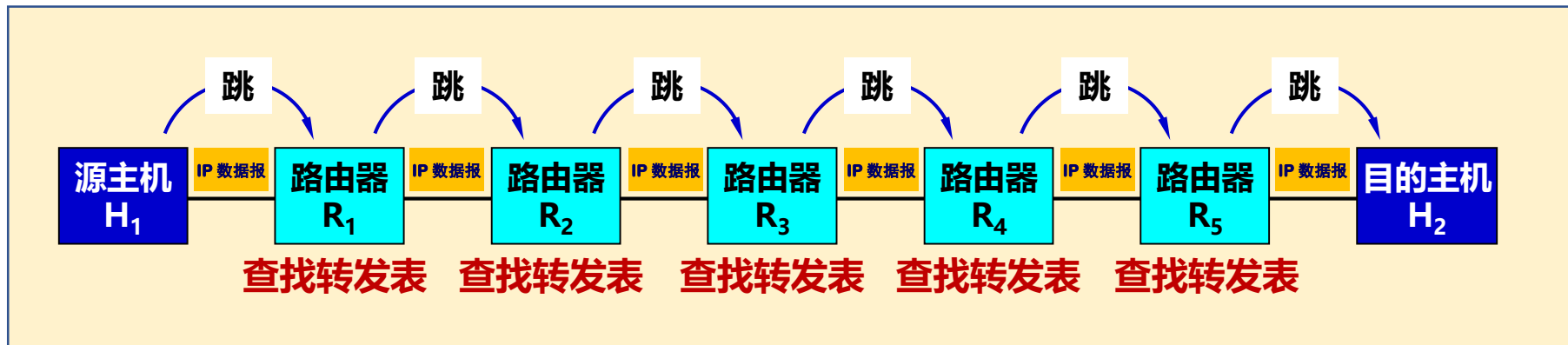
## 9. IP 路由选择

- 为分组选择一条从源主机到目的主机的最佳路径
  - 可选路径不止一条路径
  - 可能要跨越多个网络
- 网络中实现路由选择功能的设备是**路由器**  
对每一个接收到的分组，路由器必须确定从哪条路径将其转发出去
- 路由器根据其内部保存的一张**路由表**转发分组  
路由表中存放了到达其他网络的路由信息：
  - 目的IP地址
  - 下一个路由器地址（Next Hop）
  - 标志域
  - 网络接口等



# 9. IP 路由选择

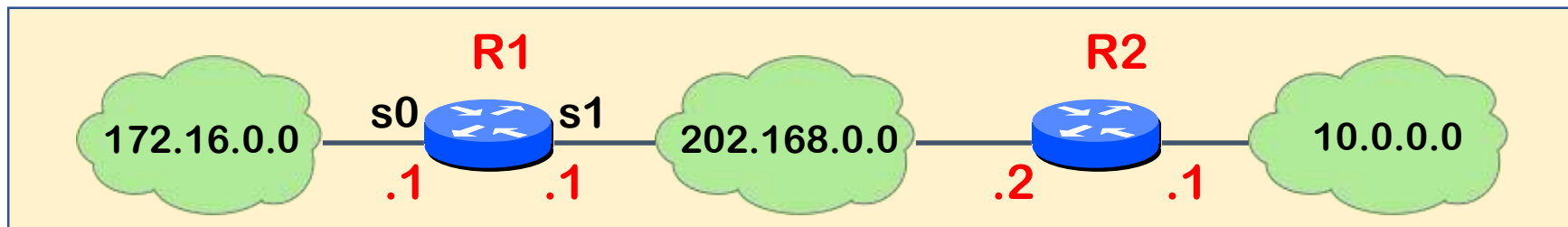
- 基于分组首部中的目的地址传送和转发（逐跳转发）





## 9. IP 路由选择

- 转发表中最主要的路由是（目的网络地址，下一跳地址）而不是（目的地址本身）——这样可压缩转发表大小！
- 查找转发表的过程就是逐行寻找前缀匹配

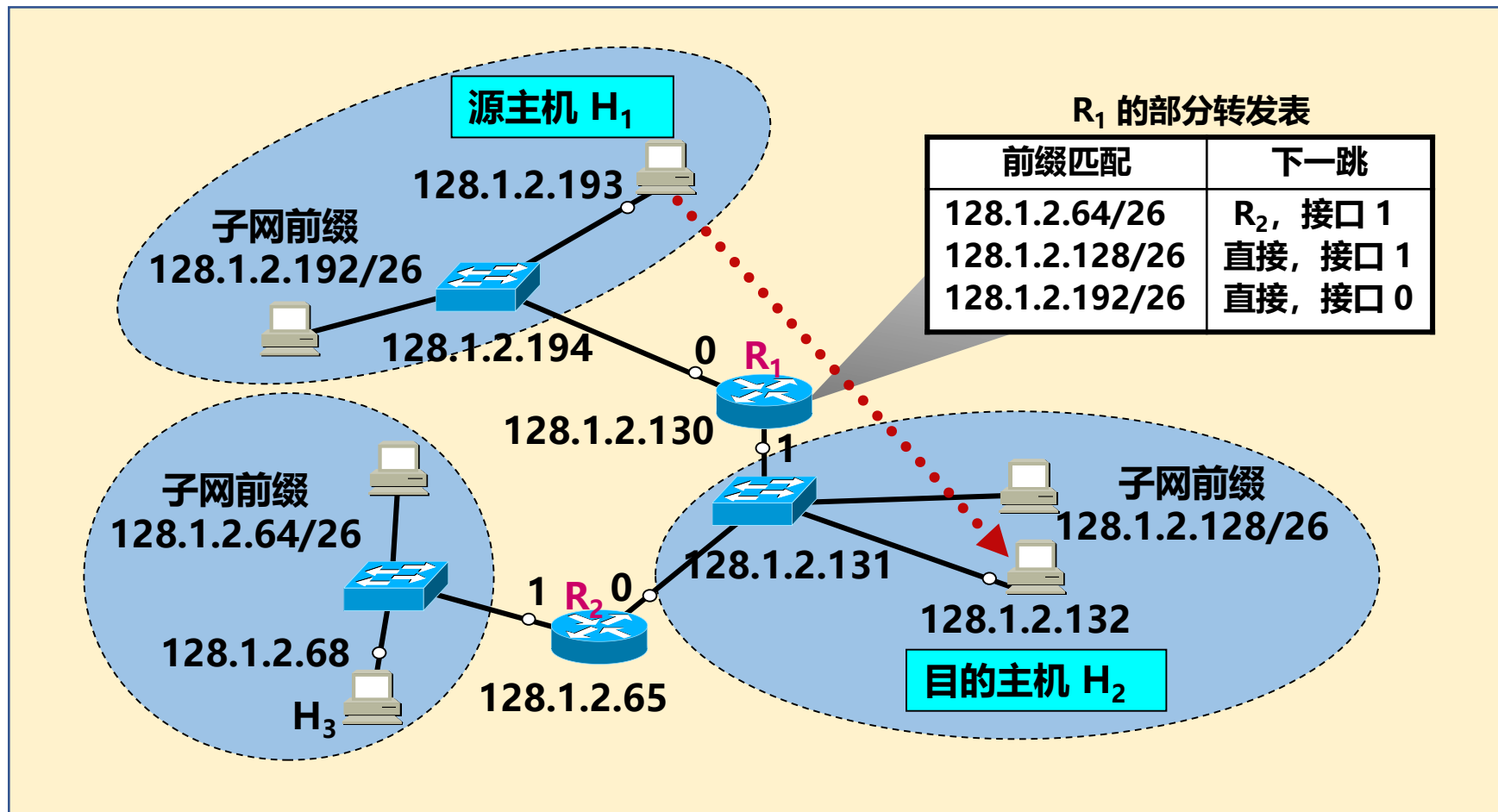


### R1的路由表

目的网络	下一跳路由器地址
172.16.0.0	直接交付（从s0）
202.168.0.0	直接交付（从s1）
10.0.0.0	202.168.0.2
Default	202.168.0.2

# 9. IP 路由选择

- **例：**主机 H1 发送出的、目的地址是 128.1.2.132 的分组是如何转发的？





## 5.3.3 因特网的IP路由技术

### ■ 路由选择

选择一条从信源网络到信宿网络的最佳路径，并在该路径上转发数据包  
实际上是查找输出接口

### ■ 路由选择是实现高效通信的基础，原则：

- 减小路由表中的路径数量（在因特网的骨干链路中尤其重要）
- 尽量选择廉价路径

### ■ 与目的主机连接只有两种类型

- 点到点链路
- 广播型网络（LAN）



# 1. 路由协议和算法：动态路由实现

- 静态路由：由网络管理员设置并随时更新
- 动态路由：路由器运行过程中根据网络情况动态维护
  - 全局路由协议
  - 局部路由协议



# 1. 路由协议和算法：全局路由协议

- 依据完整的网络全局拓扑信息计算到达各个网络的最佳路径
- 本协议需要了解每条网络链路的状态，故也称其为链路状态路由协议（Link State Routing Protocol, L-S）
- 路由计算在所有路由器中完成，运行L-S协议的每个路由器都要向所有路由器发送与自己相邻的路由器的链路状态信息，内容包括：
  - 路由器所连接的网段链路
  - 该链路的物理状态：连通性、开销、速度、距离、时延等信息
- 通过互相通告链路状态，每个路由器最终都可以建立一个关于整个网络拓扑结构的数据库，再使用Dijkstra算法计算出到达各网络的最佳路径
- 典型的L-S是OSPF  
Open Shortest Path First—开放式最短路径优先



# 1. 路由协议和算法：局部路由协议

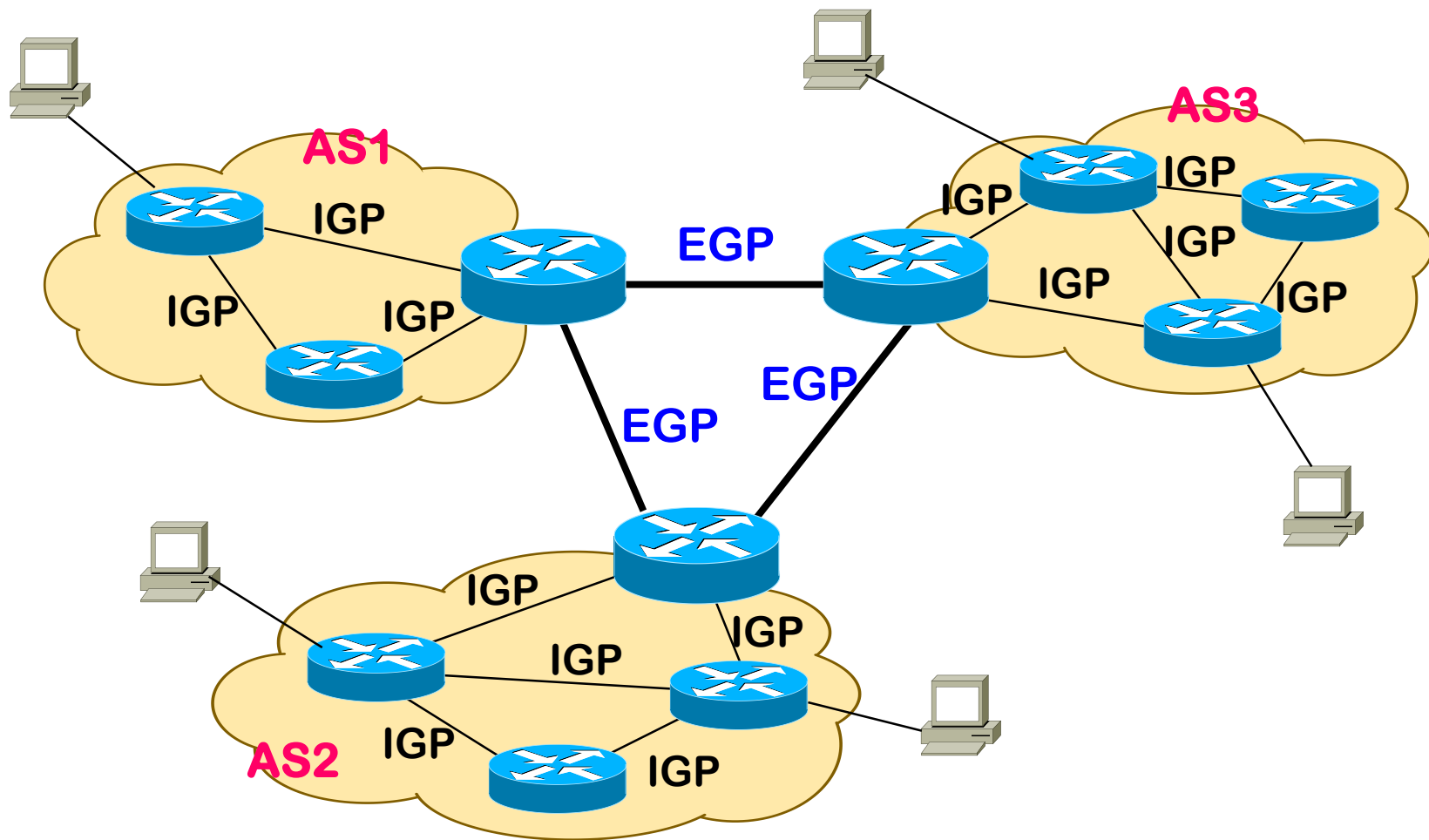
- 通过一系列重复的、分布的方式来计算最佳路径
- 每个路由器开始只知道与其直接相连的链路的信息
- 通过与相邻路由器的通信和一系列反复的计算，路由器可以逐渐获得到达某些网络的最佳路径信息
- 实践中称其为距离矢量路由协议 Distance Vector Routing Protocol, D-V
- D-V计算网络中链路的距离矢量，然后根据计算结果构造路由表。每一个路由器工作时会定期向相邻路由器发送消息，消息的内容就是自己的整个路由表，其中包括：
  - 到达信宿网络的下一步IP地址
  - 到达信宿网络所经过的距离
- 运行D-V的路由器会根据相邻路由器发送过来的信息，更新自己的路由表
- 典型的D-V是RIP（Routing Information Protocol），常被OSPF替代



## 2. 因特网路由协议：IP路由协议的层次

- 因特网被划分为许多**自治系统**（**Autonomous System, AS**）  
每个**AS**都是一个**互联网络**
- **AS**是由一组路由器组成的集合，处于相同的管理和技术手段控制之下，并运行相同的路由协议
- **AS**的特点：
  - 有权自主决定在本系统内采用何种路由选择协议
  - 一个**AS**内的所有网络都属于一个组织或机构管辖并在本**AS**内是连通的
- 因特网把路由协议分为两大类：
  - 运行在**AS**内部的-----**内部网关协议（IGP）**：如**RIP**、**OSPF**等
  - 运行在**AS**之间的-----**外部网关协议（EGP）**：如**BGP**（边界网关协议）

# AS、IGP和EGP







## 3. BGP (Border Gateway Protocol, P147)

- 自治系统之间动态交换路由信息的路由协议  
常应用于互联网的网关之间
- 路由表包含：
  - 已知路由器的列表
  - 路由器能够达到的地址
  - 到达每个路由器的路径的跳数
- 最新版本：**BGP-4**



## 4. 地址转换

---

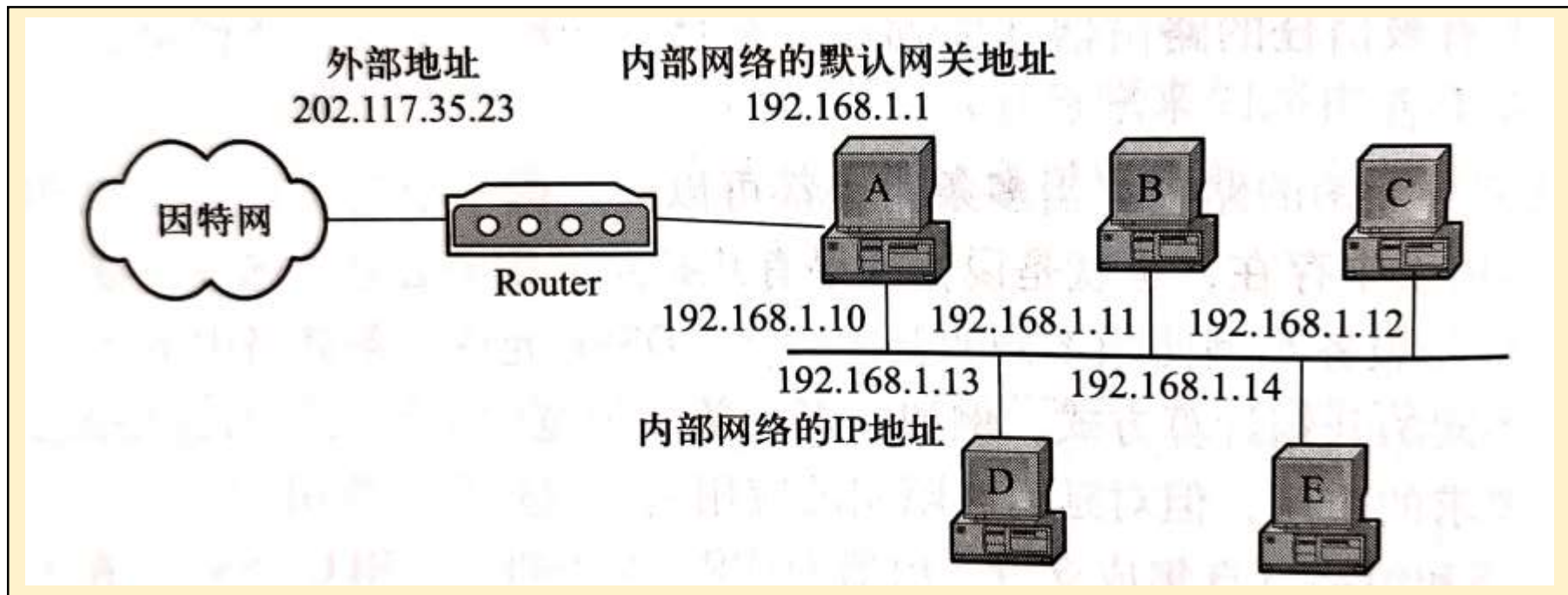
### ■ 原因：

接入因特网的任何计算机都必须有一个合法的全球唯一的IP地址，但由于IP资源稀缺，申请到的IP地址无法满足每台计算机分配一个全球唯一IP地址的需求

### ■ 解决：

为了使内网的多台计算机使用少量的全球唯一IP地址就实现因特网的访问，需要使用一种称为网络地址转换NAT或端口地址转换PAT的技术

## 4. 地址转换：NAT/PAT



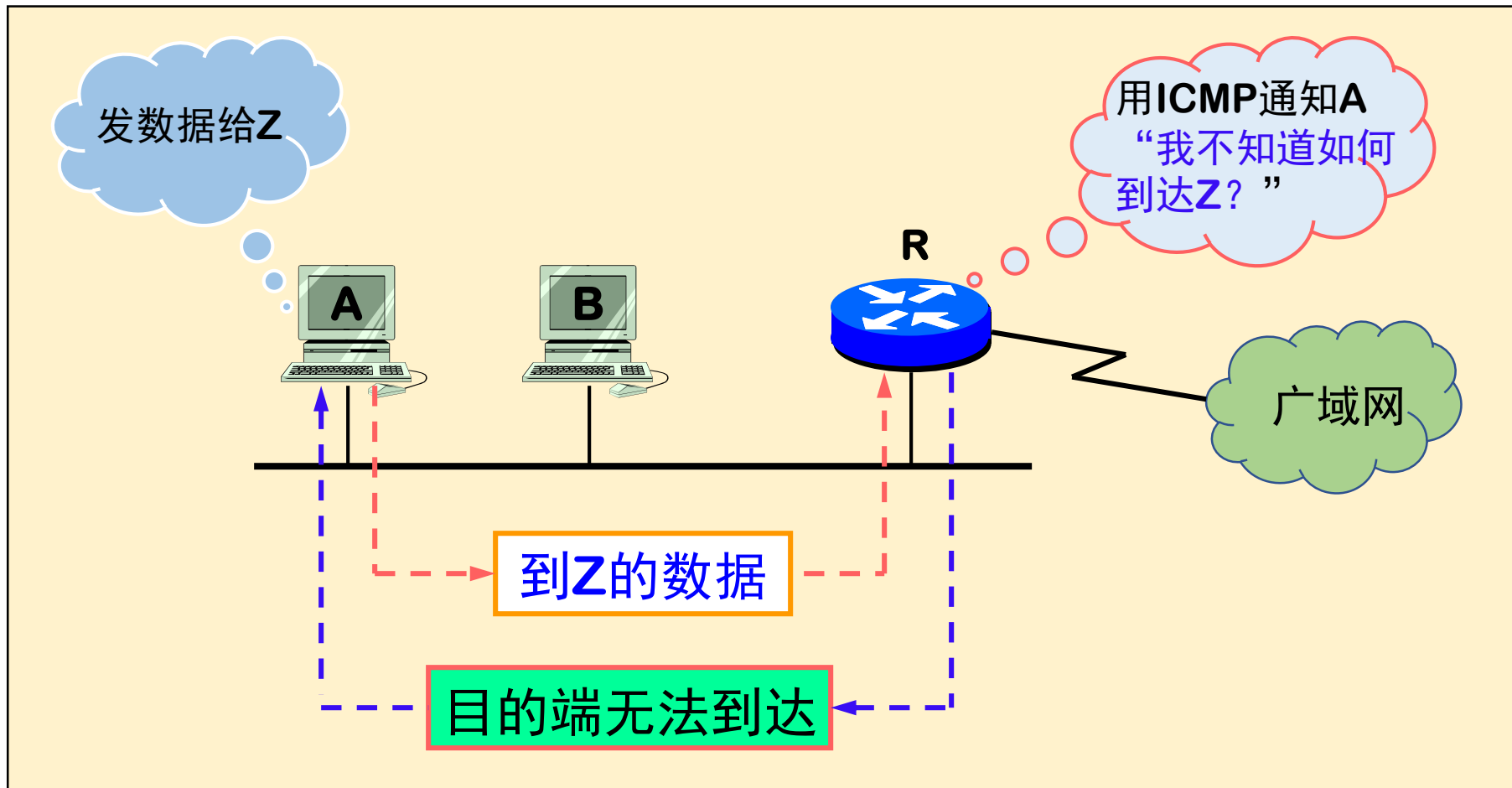
- 完美地解决了IP地址不足的问题
- 有效地避免来自网络外部的攻击，隐藏并保护网络内部的计算机
- 内部地址必须是因特网保留的IP地址  
例：10.0.0.10/8， 192.168.1.0/24
- **NAT**：外部IP地址池；**PAT**：仅1个外部IP地址；配合使用；端口映射



## 5.3.4 ICMP

- 因特网控制报文协议——Internet Control Message Protocol
- TCP/IP协议簇的子协议，属于网络层  
主要用于在主机与路由器之间传递控制信息：
  - 报告错误
  - 交换受限控制
  - 状态信息
- 当遇到IP数据无法访问目标、IP路由器无法按当前的传输速率转发数据包等情况时，会自动发送ICMP消息：
  - 询问消息
  - 错误消息
- 典型的网络命令：Ping, Tracert

□ 最常用的是“目的地无法到达”和“回声”消息



路由器R用ICMP消息通知目的地“不可达”



## 5.3.5 ARP和RARP

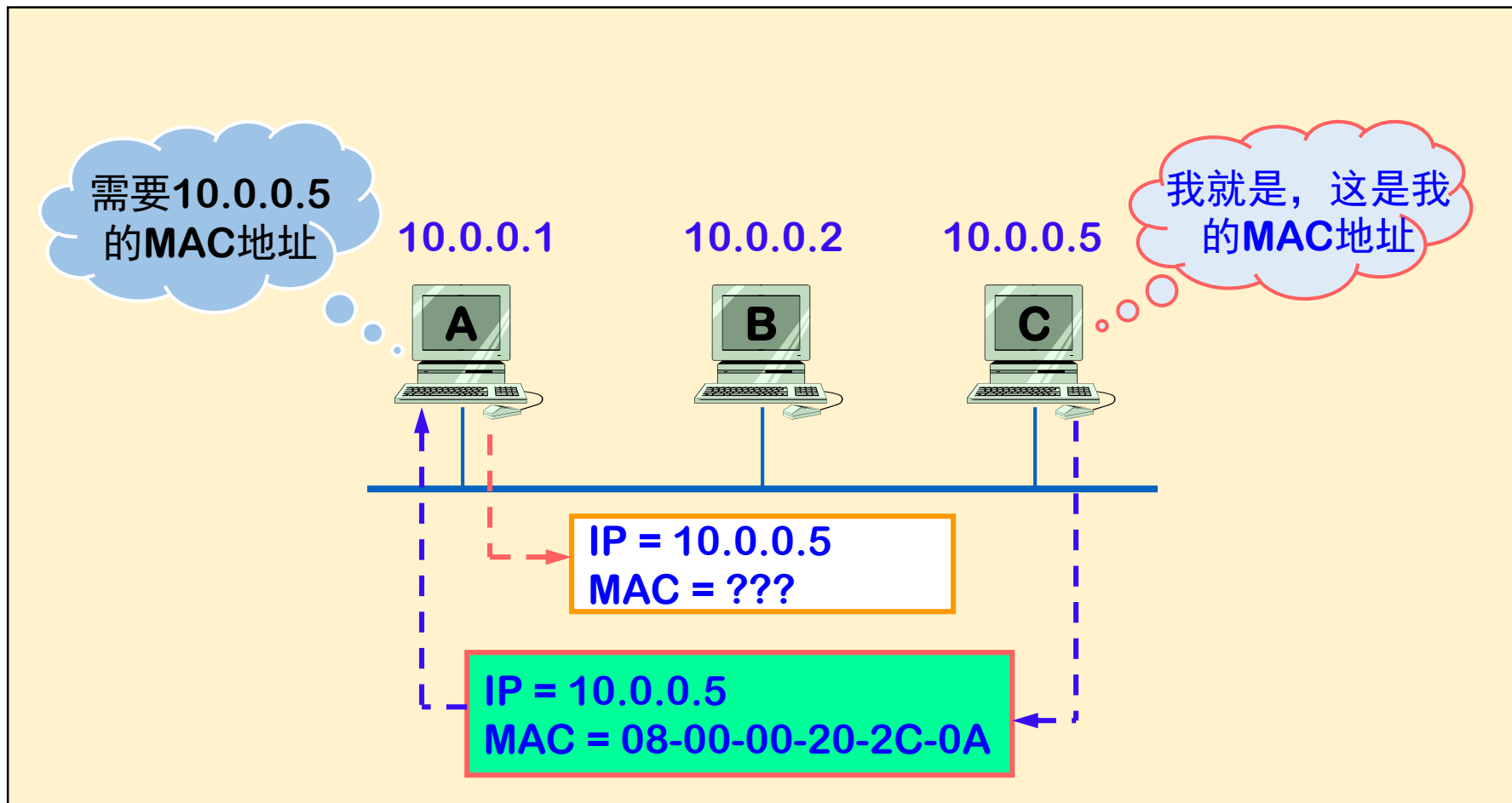
- **局域网**中，IP数据报必须交付给数据链路层被**封装成某种类型的帧**才能在网络中的站点之间**传输**
- 帧中包括了**源站点**和**目的站点**的**物理地址**以及其他一些**控制信息**
- 在局域网的**数据链路层**上使用了与IP地址不同的编址方案：**48位**的**物理地址**，即**MAC地址**
- 必须有某种方法在**IP地址**与**物理地址**之间进行**映射**  
实现这种地址映射的协议就是**ARP**（Address Resolution Protocol）
- 反之，需要**RARP**（Reverse ARP）



# 1. ARP

- ARP将一个已知的IP地址映射到MAC地址
- 映射方法：
  - 已知IP地址
  - 检查本地ARP高速缓存表
  - 若找到IP地址对应的表项，则取出表项中的MAC地址
  - 若IP地址不包含在表中，就向网上发广播来寻找；具有该IP地址的目的站用其MAC地址作为响应
- ARP只能用于具有广播能力的网络

## 例：A想知道10.0.0.5的MAC地址



□ 本机MAC地址查询：`getmac`, `ipconfig /all`





# 1. ARP

## ■ ARP工作过程：

- 需发送IP数据报的**主机**调用该主机上**ARP**实体**发送ARP请求数据报**，其中的**目标IP地址**域包含了接收机器的**IP地址**，**该请求数据报被封装在一个广播帧中**，**局域网**上**所有机器都必须接收该帧**；所有接收到**ARP**请求的**ARP**实体，从请求中**取出目标IP地址同本机地址进行比较**。
  - 如果**地址不同**就将请求**丢弃**，如果**地址相同**，则**发回一个ARP应答数据报**，给出本机的**IP地址和MAC地址**，**ARP应答数据报同样被封装在一个广播帧中**。
- ## ■ 为了提高效率，每个站点中都有一个**ARP缓冲区**
- **存储**接收到的**ARP**应答中的**IP地址-MAC地址**



## ※为什么需要地址解析协议？

■ 或者说，为何要进行地址映射？

■ Answer:

- 在因特网中，数据分组传输使用的是IP地址（逻辑地址）；而在局域网中，传输数据时需要使用物理地址（MAC地址）。
- 许多因特网的主机位于局域网中，当数据分组到达局域网时，需要把IP地址转换成MAC地址，然后把分组封装在局域网链路层的帧中，才能发送到该主机。

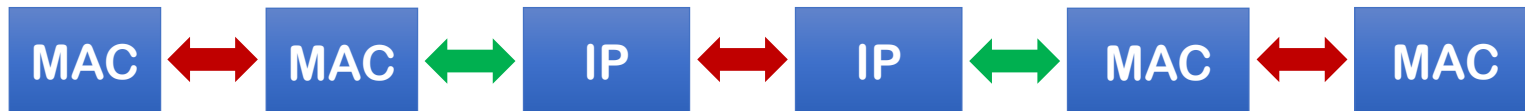
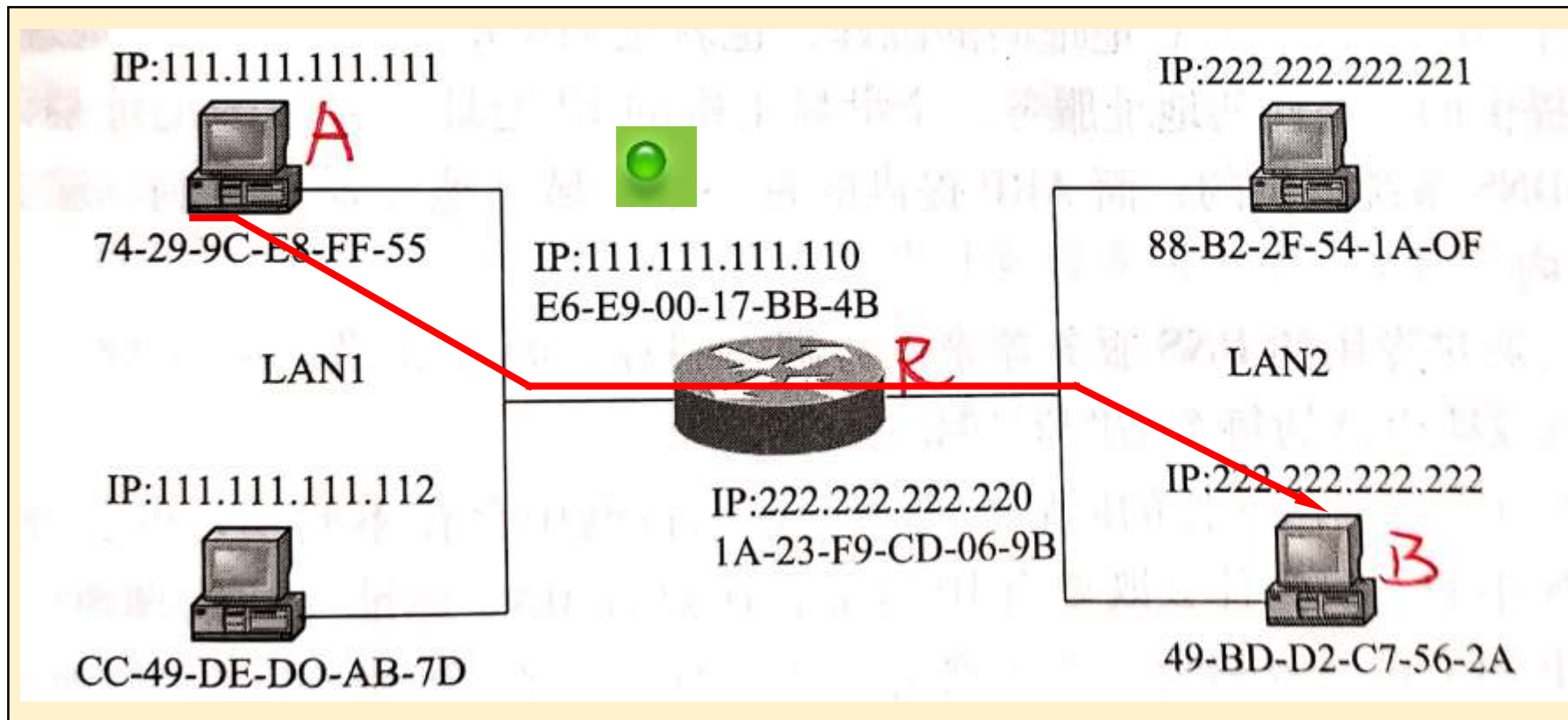


## \*2. RARP

- 作用：把MAC地址映射为IP地址
- 用于无盘工作站环境：  
把硬盘和主机分离，无盘工作站只执行操作不执行存储
  - 无盘工作站没有硬盘，配置的IP地址无法保存
- RARP的基本思想：
  - 网络中配置一台RARP服务器
  - RARP服务器中有一张预先配置好的MAC地址与IP地址的映射表
- 地址映射过程：
  - 无盘工作站启动时，从硬件配置中读出MAC地址，并将其封装在RARP请求报文中，广播到网上
  - RARP服务器收到请求报文后，在映射表中检查有无对应表项。若找到，将对应的IP地址装入响应报文中发回给请求者
- RARP也只能用于具有广播能力的网络

## 5.3.6 ARP与IP的交互

例：由R对A到B的数据包进行路由的过程





## 上例解释（自行阅读）

- 实际上，发送主机在发送分组之前，就已知道目的主机不在本地**LAN**上（只要比较目的主机和发送主机的**IP**地址中的网络地址部分便可知）所以必须将**分组发送给路由器，由路由器进行转发**
  - 路由器的**IP**地址（**Windows**中称为默认网关）在发送主机中已经预先设置（在本例中为**111.111.111.110**）
- 现在的问题是：发送主机如何得到**路由器接口的MAC地址**呢？当然是**使用ARP协议**！
- 一旦发送主机获得了**路由器接口的MAC地址**，就可以生成一个数据帧，发送给路由器
- **LAN1**上的路由器接口收到了发给它的数据帧后，将封装在其中的分组提交给网络层。这样，分组就成功地从主机发送到了路由器上！



## 上例解释（自行阅读）

- 接下来，路由器还必须将分组发送到目的地。
- 路由器首先需要**选择适当的接口来转发**，这项工作路由器可以通过查询路由表来完成。
  - 路由表告诉路由器：“**需要通过222.222.222.220接口转发该分组**”。于是，路由器把分组送到该接口。
  - 最后，接口将分组传送给其适配器，组成**新的数据帧**，并广播到**LAN2**中。
- 这时，数据帧的目的**MAC**地址才是真正的最终目的主机的**MAC**地址。
  - 路由器又是如何知道最终目的主机的**MAC**地址呢？还是使用**ARP**协议！
  - 路由器通过数据报中的目的**IP**地址和**ARP**协议来得到目的主机的**MAC**地址。



## \*5.3.9 IPv6

### ■ 初始的动机

IPv4的32-bit地址空间，2011年2月3日全球互联网IP地址相关管理组织宣布：现有的互联网IP地址已于当天分配完毕，**IP地址总库已经枯竭！**

### ■ IP地址的分配存在严重不公的问题

如北美占有约30亿个，亚洲只有不到4亿个，而拥有近N亿网民的中国，IPv4地址数量仅为2.5亿个，远远不能满足人们的需求

### ■ IPv6的地址多达 $2^{128}$ （340万亿亿亿亿）

地球上每平方米可分配0.668亿亿亿个IP地址

可以使地球表面每粒沙子都有一个IP地址



# IPv6地址表示

- 128位长，8组，每组为4个十六进制数：

2001:0db8:85a3:08d3:1319:8a2e:0370:7344

其他合法：

2001:0DB8:0000:0000:0000:0000:1428:57ab

2001:0DB8:0000:0000:0000::1428:57ab

2001:0DB8:0:0:0:0:1428:57ab

2001:0DB8:0::0:1428:57ab

2001:0DB8::1428:57ab

2001:DB8::1428:57ab

非法：

2001::25de::cade





## 5.4 因特网传输层协议

- 提供运行在不同主机中进程间的逻辑通信
- 传输协议仅运行在端系统中
- 传输 vs. 网络层服务：
  - 网络层: 在端系统间进行通信
  - 传输层: 在进程间进行通信
  - 传输层依赖于网络层的服务，反过来又加强了网络层的服务



# 传输层协议：回顾

- 面向连接的协议，可靠的，按序点对点递交：**TCP**
  - 拥塞控制
  - 流量控制
  - 连接建立
- 无连接的协议，不可靠的（“尽力而为”），无序的点对点或广播递交：**UDP**



## 5.4.1 UDP

- **User Datagram Protocol, 用户数据报协议**
  - OSI /RM一种**无连接**的**传输层**协议
  - 提供面向事务的简单**不可靠**信息**传送服务**
- **UDP基本上是IP与上层协议的接口**  
适用端口分别运行在同一台设备上的多个应用程序
- **主要作用：**
  - 将**网络数据流量**压缩成**数据包**的形式
  - 典型的数据包是一个**二进制数据**的**传输单位**
  - 数据包前**8字节**包含**报头信息**，剩余字节则包含**具体的传输数据**



## 5.4.1 UDP：特性

1. **无连接协议**，传输数据之前源端和终端**不建立连接**，想传送时就简单地**抓取**来自应用程序的**数据**，并**尽可能快地**把它**扔到网络上**。在发送端，**UDP**传送数据的速度仅受应用程序生成数据的速度、计算机能力和传输带宽的限制；在接收端，**UDP**把每个消息段放在队列中，应用程序每次从队列中读一个消息段。
2. 传输数据**不建立连接**，不需要维护连接状态，如收发状态等。因此**一台服务机**可**同时向多个客户机**传输相同的消息。
3. **UDP**信息包的标题很短，只有**8**个字节，相对于**TCP**的**20**个字节信息包的**额外开销很小**。
4. **吞吐量不受拥挤控制算法的调节**，只受应用软件生成数据的速率、传输带宽、源端和终端主机性能的限制。
5. **UDP**使用**尽最大努力交付**，即**不保证可靠交付**，因此主机**不需要维持复杂的链接状态表**（这里面有许多参数）。
6. **UDP**是**面向报文的**。发送方的**UDP**对应用程序交下来的报文（称为**UDP段**），在添加首部后就向下交付给**IP**层。既不拆分，也不合并，而是保留这些报文的边界，因此，应用程序需要选择合适的报文大小。



## 5.4.1 UDP：应用

- 既然**UDP**是一种不可靠的网络协议，那么还有什么使用价值或必要呢？其实不然，在有些情况下**UDP**协议可能会变得非常有用。因为**UDP**具有**TCP**所望尘莫及的**速度优势**。
- **UDP**协议在主流应用中发挥着作用。包括视频会议系统在内的许多应用都证明了**UDP**协议的存在价值。因为相对于可靠性来说，这些应用更加注重实际性能，所以为了获得更好的使用效果（例如，更高的画面帧刷新速率）往往可以牺牲一定的可靠性（例如，会面质量）。
- 这就是**UDP**和**TCP**两种协议的**权衡之处**。根据不同的环境和特点，两种传输协议都将在今后的网络世界中发挥更加重要的作用。



## 5.4.2 TCP

- **Transmission Control Protocol**，传输控制协议
  - 面向连接的、可靠的、基于字节流的传输层通信协议
- **TCP层位于IP层之上，应用层之下的传输层**

不同主机的应用层之间经常需要可靠的、像管道一样的连接  
但是IP层不提供这样的流机制，而是提供不可靠的分组交换
- **可靠性问题由TCP来解决！**



## 5.4.2 TCP

### ■ 主要作用：

- **全双工**：TCP建立连接之后，通信双方都同时可以进行数据的传输
- **可靠性保证**：采用超时重传和捎带确认机制
- **流量控制**：采用滑动窗口协议，对于窗口内未经确认的分组需要重传
- **拥塞控制**：采用广受好评的TCP拥塞控制算法（也称AIMD算法）

该算法包括三个主要部分：

- ① 加性增、乘性减
- ② 慢启动
- ③ 对超时事件做出反应



## 5.4.2 TCP：特性

1. 面向连接的传输
2. 端到端的通信
3. 高可靠性，确保传输数据的正确性，不出现丢失或乱序
4. 全双工方式传输
5. 采用字节流方式，即以字节为单位传输字节序列
6. 紧急数据传送功能





## 5.4.2 TCP：可靠性保障

### ■ TCP协议是如何确保数据传输高可靠性？

- 为了保证可靠性，发送段中每个字节都有递增的序列号。序号和确认号用来确保传输的可靠性。
- 此外，对每个TCP段都设立一个定时器，TCP协议用于控制报文是否需要重传的依据是设立重发定时器。在发送一个报文的同时启动一个重发定时器，如果在定时器超时前收到确认就关闭该定时器，如果定时器超时前没有收到确认，则重传该TCP段。



# ※TCP协议和UDP协议的区别※

TCP	UDP
面向连接	面向非连接
传输速度慢	传输速度快
保证数据顺序	不保证数据顺序
保证数据正确性	可能丢包
系统资源要求多	系统资源要求少



# 本章小结

- 网络互连的基本概念、体系结构和接入
- 因特网的链路层与网络层
  - 点对点协议
  - 网络层与IP协议
  - IP路由
  - **ARP和RARP**
  - **ARP与IP的交互**
  - **IP地址的分配（DHCP）**
  - **ICMP协议**
- 因特网的传输层
  - 无连接的传输：**UDP**
  - 面向连接的传输：**TCP**



# 作业

---

■ 第168页：

4, 11, 13