

专业测试保障卓越品质

The high quality derived from the professional testing

测试

# 计算机网络

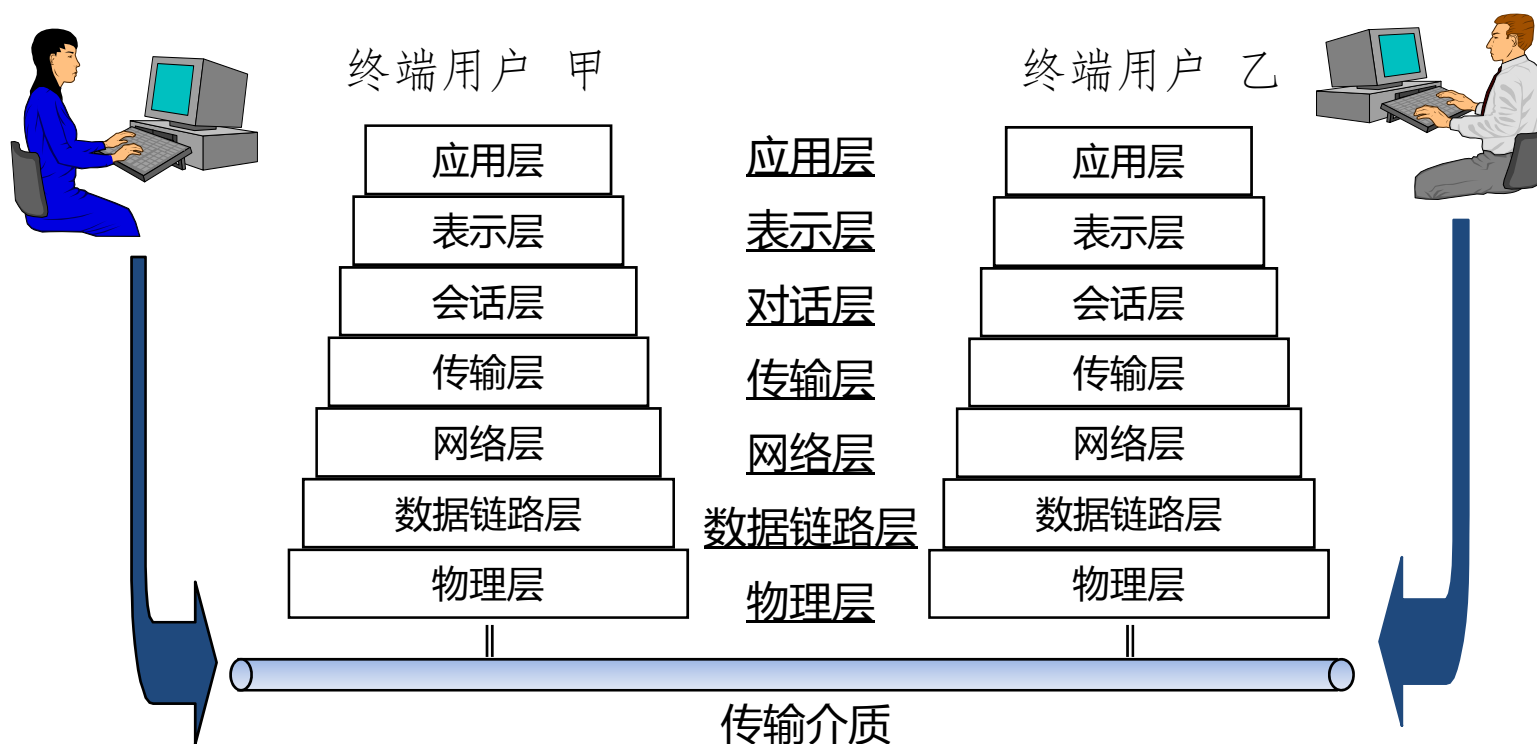
- 简单连接 ( 1960' s-1970' s )
  - 终端连接到主机
- 网络化连接 ( 1970' s-1980' s )
  - 局域网的连接
- 网络间互联 ( 1980' s-1990' s )
  - 互联网

- 按地域（覆盖范围）分类
  - 局域网（LAN-Local Area Network）
  - 城域网（MAN-Metropolitan Area Network）
  - 广域网（WAN-Wide Area Network）
- 按网络结构分类
  - 对等网络（Peer to Peer）
  - 客户机/服务器（Client/Server）
- 按应用技术分类
  - 局域网：Ethernet、Token Ring、FDDI
  - 广域网：PSTN、ISDN、xDSL、DDN、FR、X.25、ATM

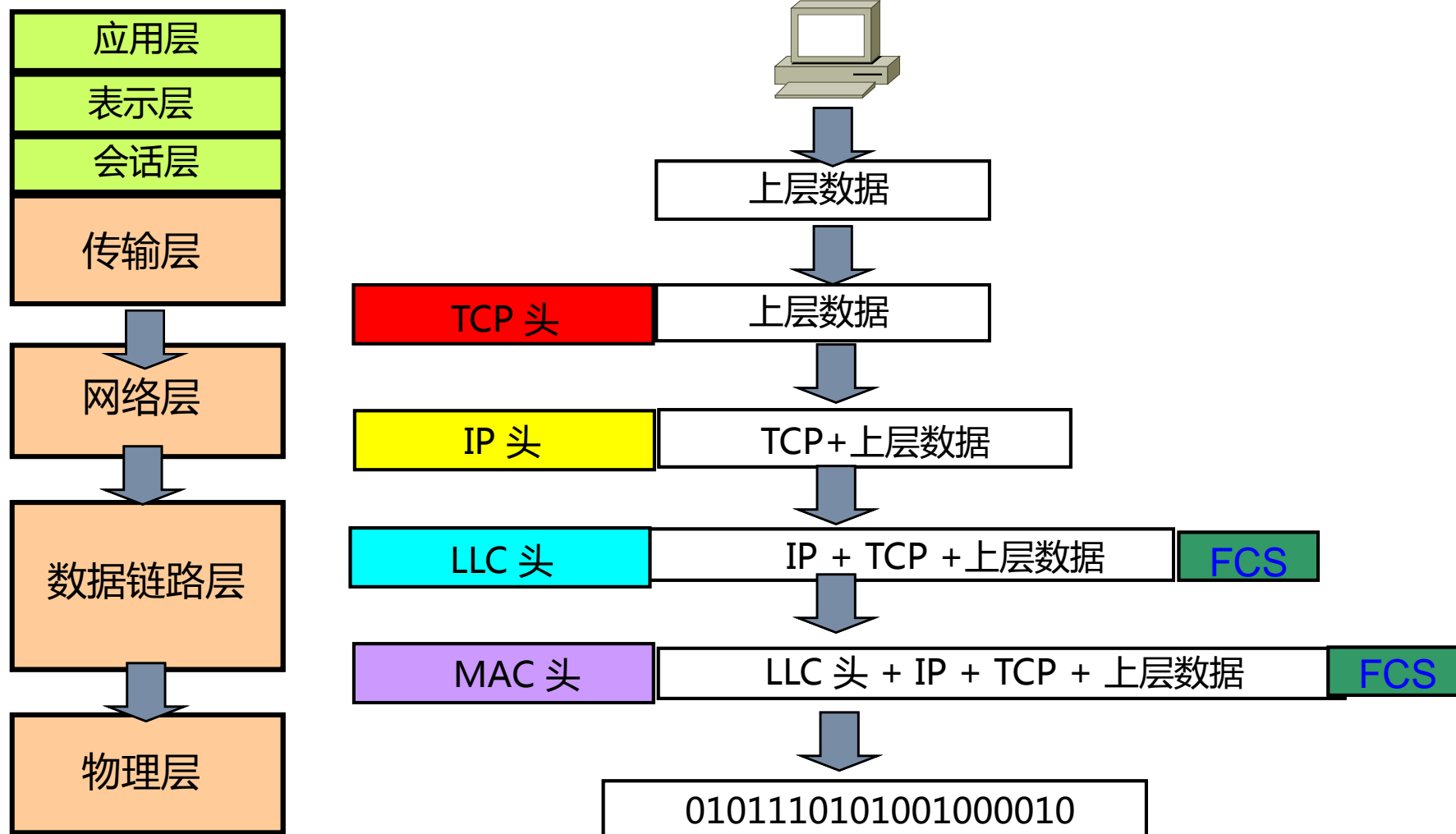
- ISO（国际标准化组织）
- IEEE（电子电气工程师协会）
- ANSI（美国国家标准局）
- EIA/TIA（电子工业协会）
- ITU（国际电信联盟）
- IAB（互联网行动委员会）

- ISO（国际标准化组织）制定了OSI（Open System Interconnect），意为开放式系统互联
- OSI/RM（Open System Interconnection Reference Model）基本参考模型：
  - 应用层（Application）——最高层（第7层）
  - 表示层（Presentation）
  - 会话层（Session）
  - 传输层（Transport）
  - 网络层（Network）
  - 数据链路层（Data Link）
  - 物理层（Physical）——最底层（第1层）

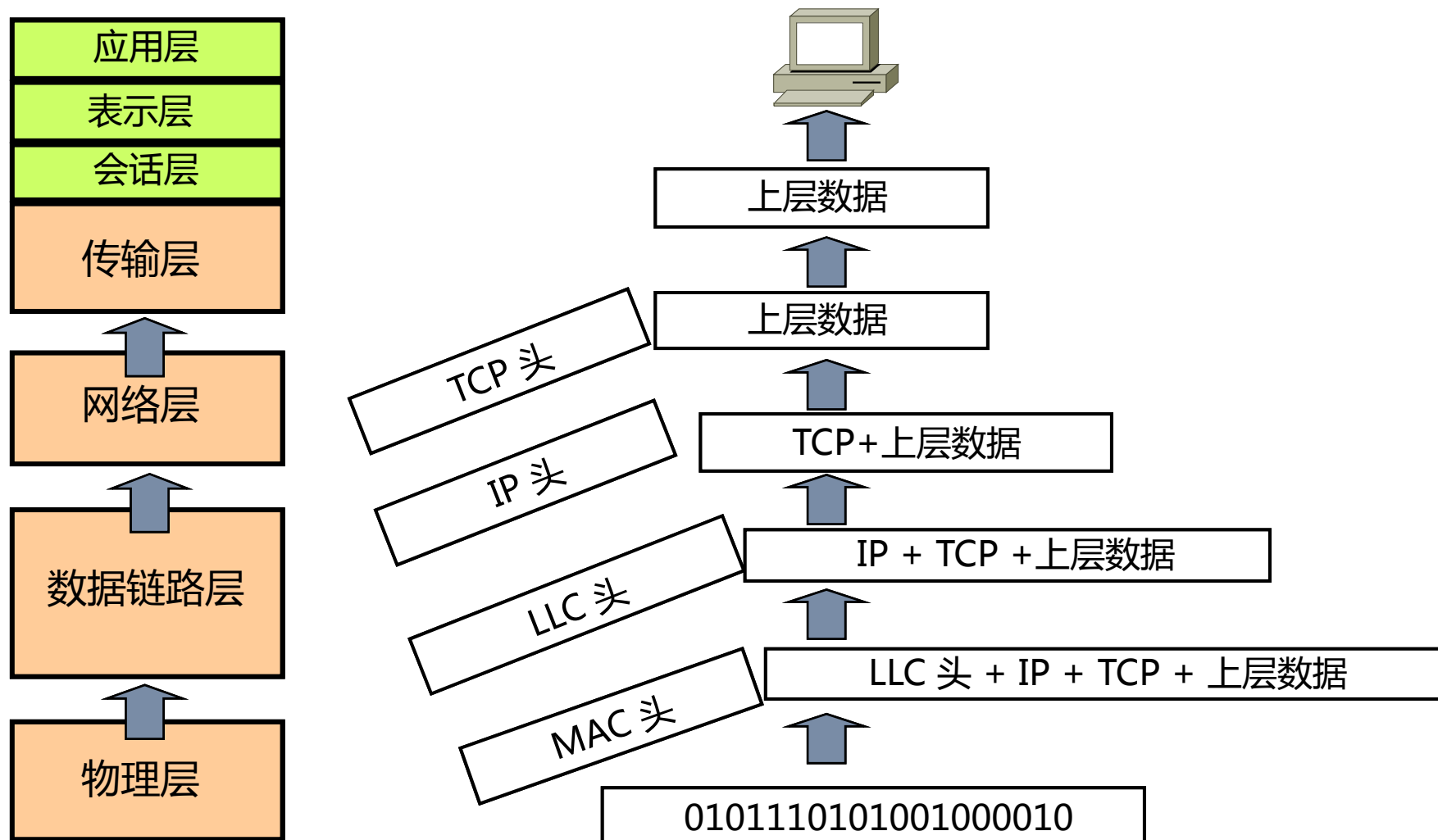
- 任何两个终端用户（End User）之间的通信都需要经过这七层转换（各层会对数据进行封装）：



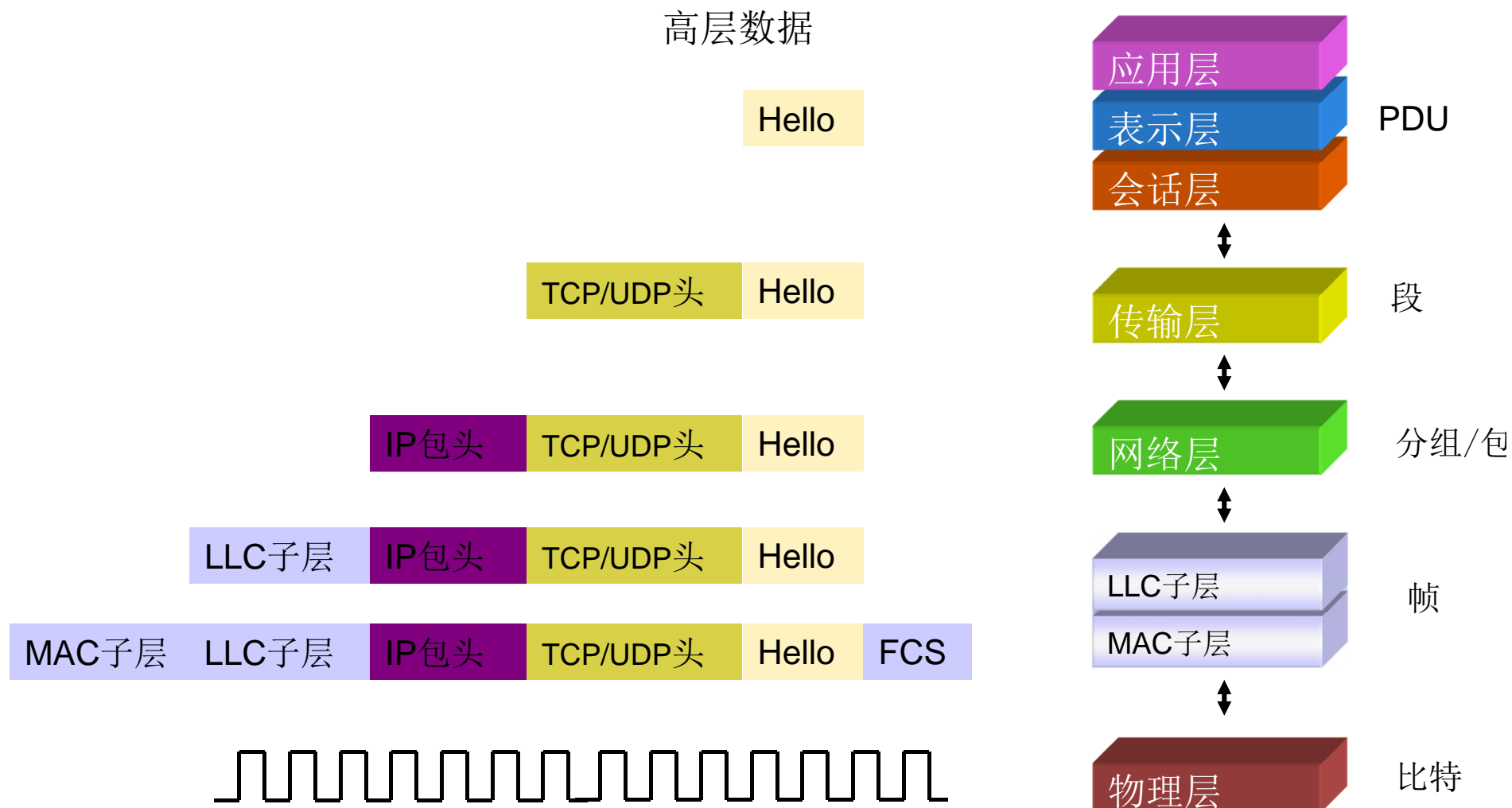
- 封装（encapsulate/encapsulation）
  - 数据要通过网络进行传输，要从高层一层一层的向下传送，如果一个主机要传送数据到别的主机，先把数据装到一个特殊协议报头中，这个过程就是封装。
- 封装
  - 切片
  - 加控制信息
- 解封装：上述的逆向过程



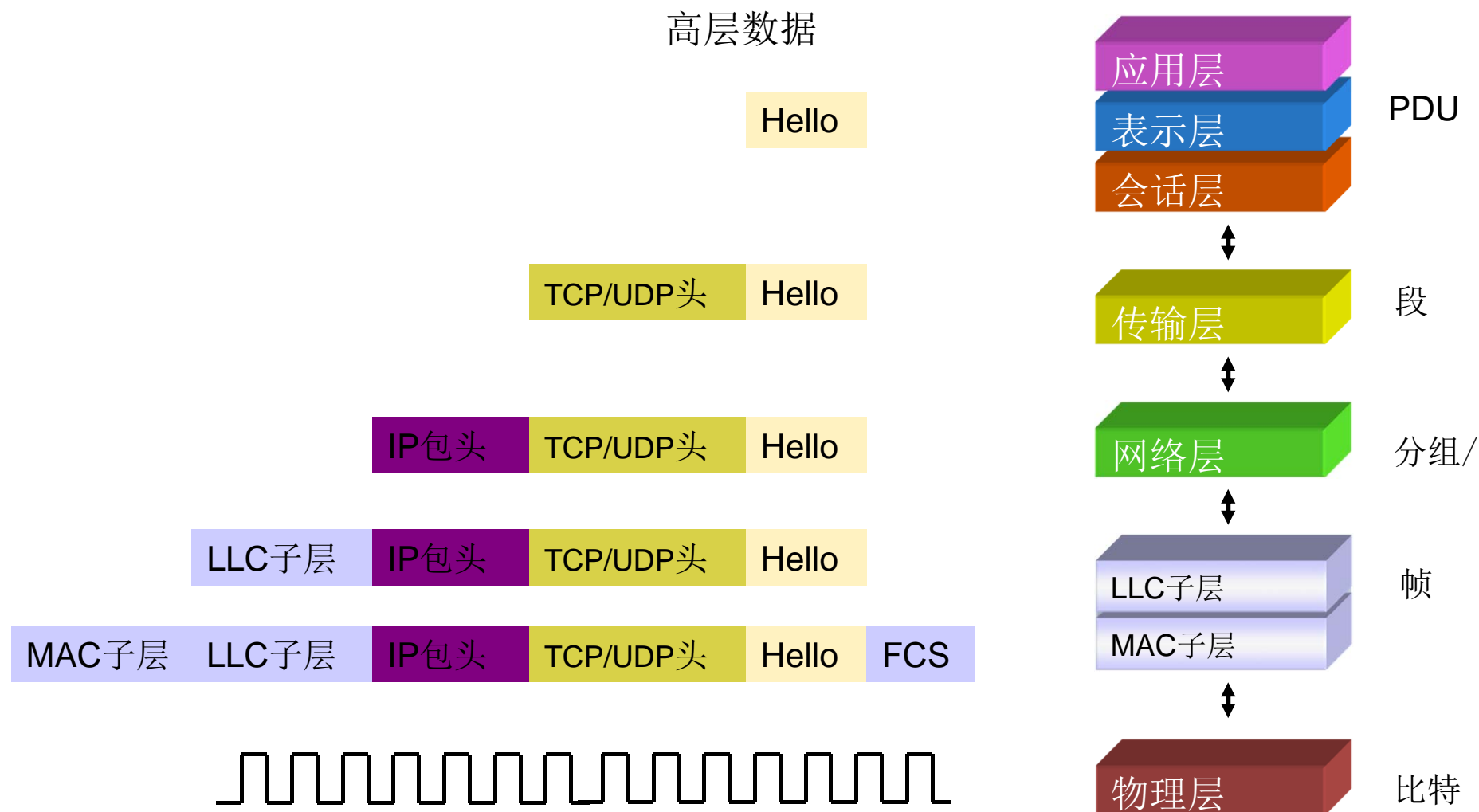




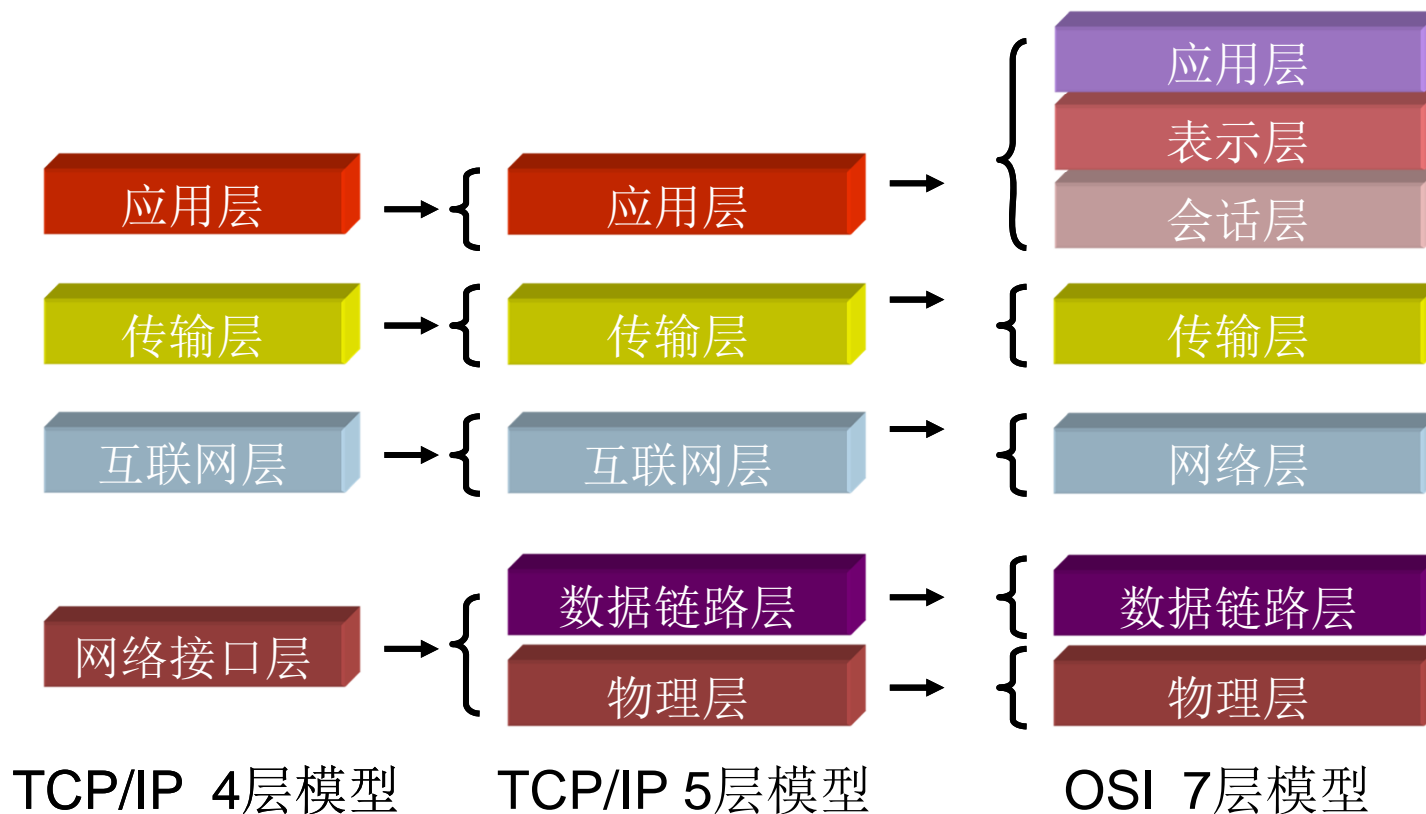
# 数据的封装与解封装过程实例



# 数据的封装与解封装过程实例



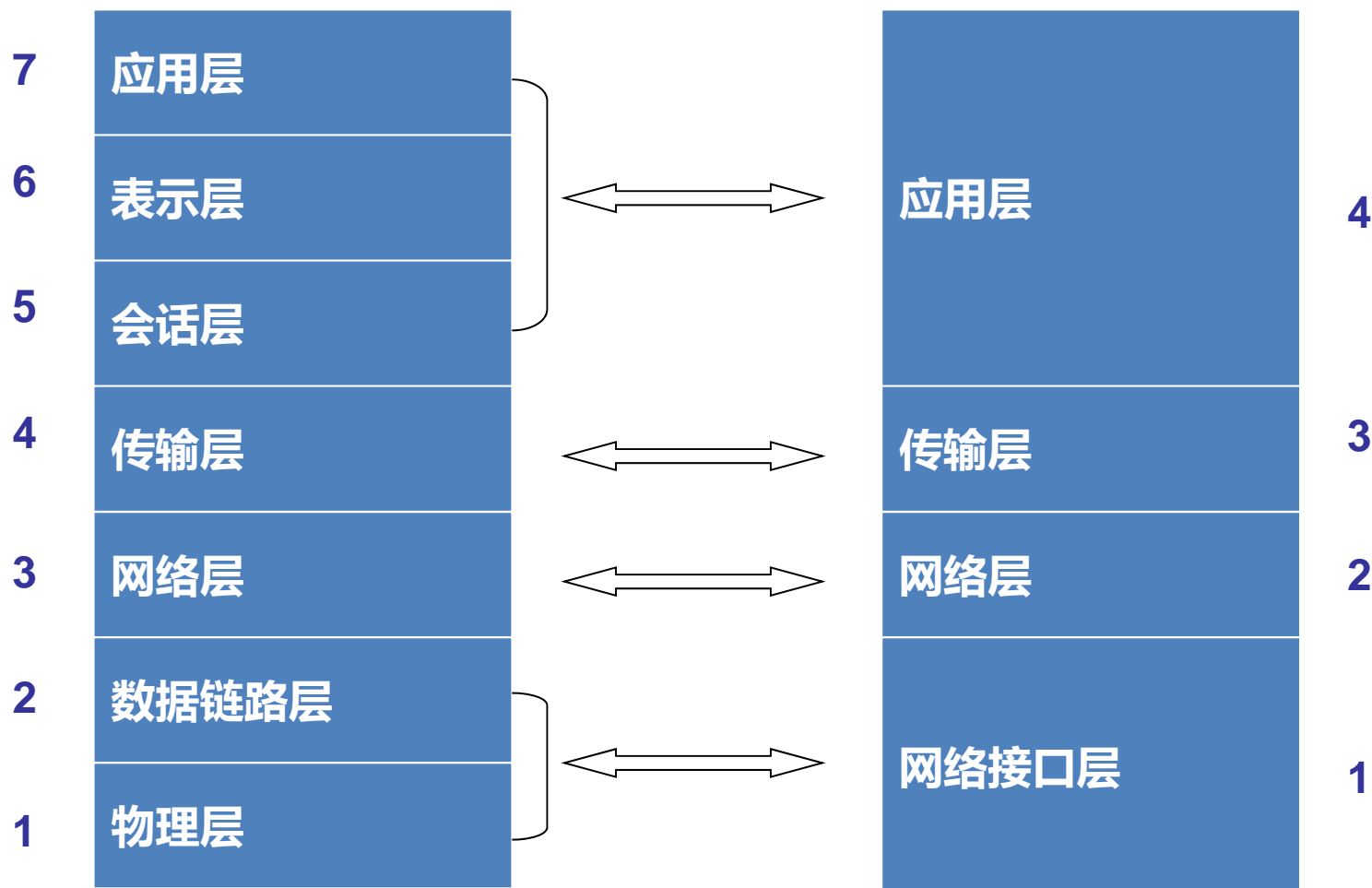
# TCP/IP协议参考模型



# TCP/IP模型的层次结构

OSI参考模型

TCP/IP模型

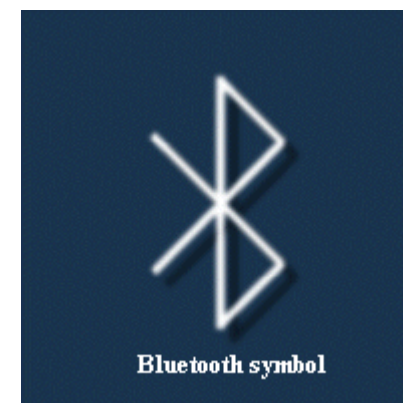


# OSI模型参考表格

具体7层	数据格式	功能与连接方式	典型设备
应用层 Application		网络服务与使用者应用程序间的一个接口	网关
表示层 Presentation		数据表示、数据安全、数据压缩	
会话层 Session		建立、管理和终止会话	
传输层 Transport	数据组织成数据段 Segment	用一个寻址机制来标识一个特定的应用程序（端口号）	防火墙
网络层 Network	分割和重新组合数据包Packet	基于网络层地址（IP地址）进行不同网络系统间的路径选择	路由器
数据链路层 Data Link	将比特信息封装成数据帧Frame	在物理层上建立、撤销、标识逻辑链接和链路复用 以及差错校验等功能。通过使用接收系统的硬件地址或物理地址来寻址	网桥和交换机
物理层 Physical	传输比特（bit）流	建立、维护和取消物理连接	中继器和集线器

- 局域网的标准
  - 由 IEEE802 委员会负责起草
  - 后来也成为ANSI、ISO的标准
- IEEE 802
  - IEEE802标准定义了 ISO/OSI 的**物理层**和**数据链路层**。
  - IEEE 802规范定义了网卡如何访问传输介质（如光缆、双绞线、无线等），以及如何在传输介质上传输数据的方法，还定义了传输信息的网络设备之间连接建立、维护和拆除的途径。
  - 遵循IEEE 802标准的产品包括网卡、桥接器、集线器、交换器、路由器以及其他一些用来建立局域网的组件。

- IEEE802.1A——局域网体系结构
- IEEE802.1B——寻址、网络互连与网络管理
- IEEE802.2——逻辑链路控制(LLC)
- IEEE802.3——CSMA/CD访问控制方法与物理层规范
- IEEE802.3i——10Base-T访问控制方法与物理层规范
- IEEE802.3u——100Base-T访问控制方法与物理层规范
- IEEE802.3ab——1000Base-T访问控制方法与物理层规范
- IEEE 802.3x——是全双工以太网数据链路层的流控方法。当客户终端向服务器发出请求后,自身系统或网络产生拥塞时,它会向服务器发出PAUSE帧,以延缓服务器向客户终端的数据传输。
- IEEE802.3z——1000Base-SX和1000Base-LX访问控制方法与物理层规范
- IEEE802.4——Token-Bus访问控制方法与物理层规范
- IEEE802.5——Token-Ring访问控制方法
- IEEE802.6——城域网访问控制方法与物理层规范
- IEEE802.7——宽带局域网访问控制方法与物理层规范
- IEEE802.8——FDDI访问控制方法与物理层规范
- IEEE802.9——综合数据话音网络
- IEEE802.10——网络安全与保密
- IEEE802.11——无线局域网访问控制方法与物理层规范
- IEEE802.12——100VG-AnyLAN访问控制方法与物理层规范
- IEEE 802.14——协调混合光纤同轴(HFC)网络的前端和用户站点间数据通信的协议。
- IEEE 802.15——无线个人网技术标准,其代表技术是bluetooth和zigbee。
- IEEE 802.16——宽带无线 MAN 标准 - WiMAX
- IEEE 802.17——弹性分组环 ( RRR ) 工作组
- IEEE 802.18——宽带无线局域网技术咨询组 ( Radio Regulatory )
- IEEE 802.19——多重虚拟局域网共存技术咨询组
- IEEE 802.20——移动宽带无线接入 ( MBWA ) 工作组





- 以太网

- 以太网(Ethernet) 最早是一个私有技术，由Xerox(施乐)公司创建。而后由Xerox、Intel和DEC公司联合开发。
- 是当今现有局域网采用的最通用的通信协议标准。
- 以太网使用 CSMA/CD 技术，并以10M/S的速率运行在多种类型的电缆上。
- IEEE 802.3 是以太网的标准，所以以太网也叫“802.3 局域网”。
- 以太网的编码方式是曼彻斯特编码。

专业测试保障卓越品质

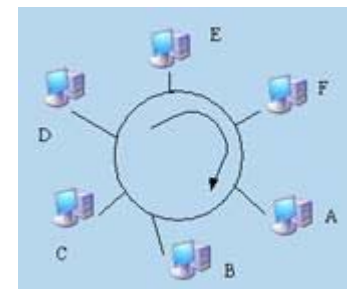
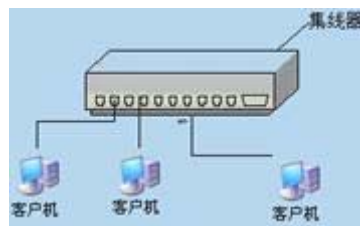
The high quality derived from the professional testing

测试

物理层

- 目的
  - 保证原始数据比特流的无误传输。
- 任务
  - 确定与物理媒体相关的电气特性、机械特性、功能特性及规程特性。
    - 机械特性：连接器形式与插针分配
    - 电气特性：接口电气信号特性
    - 功能特性：数据传送、控制、定时、接地
    - 规程特性：接口电路所使用的规程

- 拓扑结构 ( Topological Structure ) 是指用传输介质互连各种设备的物理布局。
  - 总线拓扑
  - 星形拓扑
  - 环形拓扑



- 带宽

- 带宽的单位：bps（比特率），即 bits / sec
- 注意：带宽的单位和文件的单位不同。
  - 带宽的大小，指的是每秒能吞吐多少个“位”（0/1）
  - 文件的大小，指的是1字节=8位（8个0/1）
- 网络距离与带宽
  - 距离与带宽成反比，距离越远，带宽越低
  - 例如，局域网的带宽比广域网大
- 网络的延迟
  - 数据从一端到另一端所花费的时间。
  - Ping命令就可以查看延时

- 网络适配器（即网卡）
  - 功能：完成物理层和数据链路层的功能，实现并行数据和串行信号之间的转换、数据帧的装配与拆装、介质访问控制和数据缓冲等。
- 网卡的种类
  - 按传输速率分10Mbps、100Mbps、10/100Mbps和1000Mbps网卡
  - 按传输数据信号的位数分8位、16位和32位网卡
  - 按接口分AUI接口网卡、BNC接口网卡、RJ-45接口网卡、ST、SC插头网卡和无线网卡等
  - 按总线插槽接口分ISA、EISA、VESA、PCI、PCMCIA和USB
  - 按实现技术分有线网卡和无线网卡
- NIC地址
  - 24位厂商地址 + 厂商编号的24位地址

- 传输介质
  - 双绞线（电信号传输）
    - UTP（非屏蔽双绞线，最常用）
      - 5类线（5）
      - 超5类线（5E）
      - 6类线（6）
    - STP（屏蔽双绞线，很少使用）
  - 同轴电缆（电信号传输）
  - 光纤（光信号传输）
  - 无线
- 连接器
  - 最常见的RJ45（水晶头）

- 物理层是TCP/IP模型的最底层
- 物理层为数据传输提供可靠环境



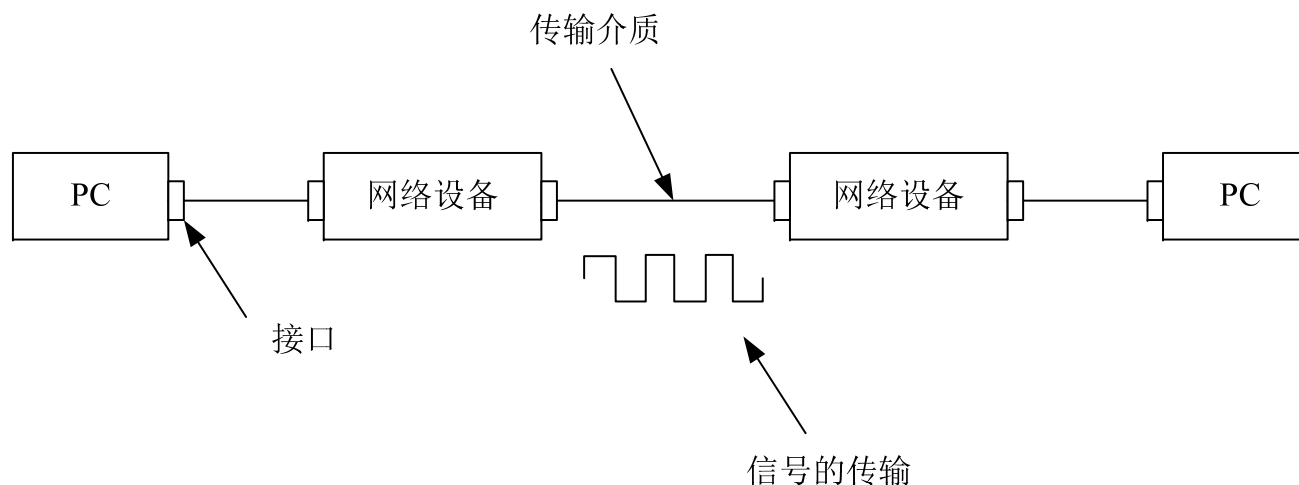
物理层是网络的基础，正如同公路是汽车通行的基础一样



- 物理层是TCP/IP模型的最底层，为数据通信的介质提供规范和定义
  - 直接面向实际承担数据传输的物理介质
  - 传输单位为比特
  - 主要负责在通信线路上比特流如何传输

# 物理层的功能

- 一：为数据端设备提供传送数据的线路
- 二：在线路上传输数据

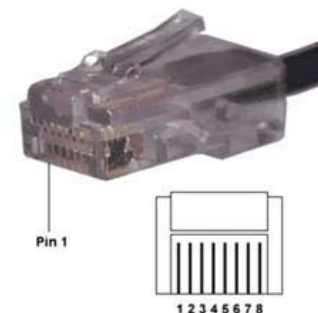


# 物理层关心的是什么

机械特性	通信设备间硬件连接接口的机械特点
电气特性	规定了在物理连接上导线的电气连接及有关的电路的特性
功能特性	指明物理接口各条信号线的用途
规程特性	指明利用接口传输的全过程及各项用于传输的事件发生的合法顺序

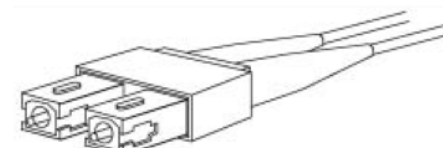
# 以太网接口

- RJ—45



- 光纤接口

- FC 圆形带螺纹光纤接头
- ST 卡接式圆形光纤接头
- SC 方型光纤接头
- LC 窄体方形光纤接头
- MT-RJ 收发一体的方型光纤接头



# 物理层的传输介质

- 有线介质
  - 双绞线
  - 光纤
- 无线介质
  - 无线电
  - 微波
  - 激光
  - 红外线

# 双绞线

- 双绞线TP是目前使用最广，价格相对便宜的一种传输介质
- 由两根绝缘铜导线相互缠绕组成，以减少对邻近线对的电气干扰
- 由若干对双绞线构成的电缆被称为双绞线电缆
- 非屏蔽双绞线UTP和屏蔽双绞线STP

# 双绞线的标准

- EIA/TIA-568——“商用建筑物电信布线标准”



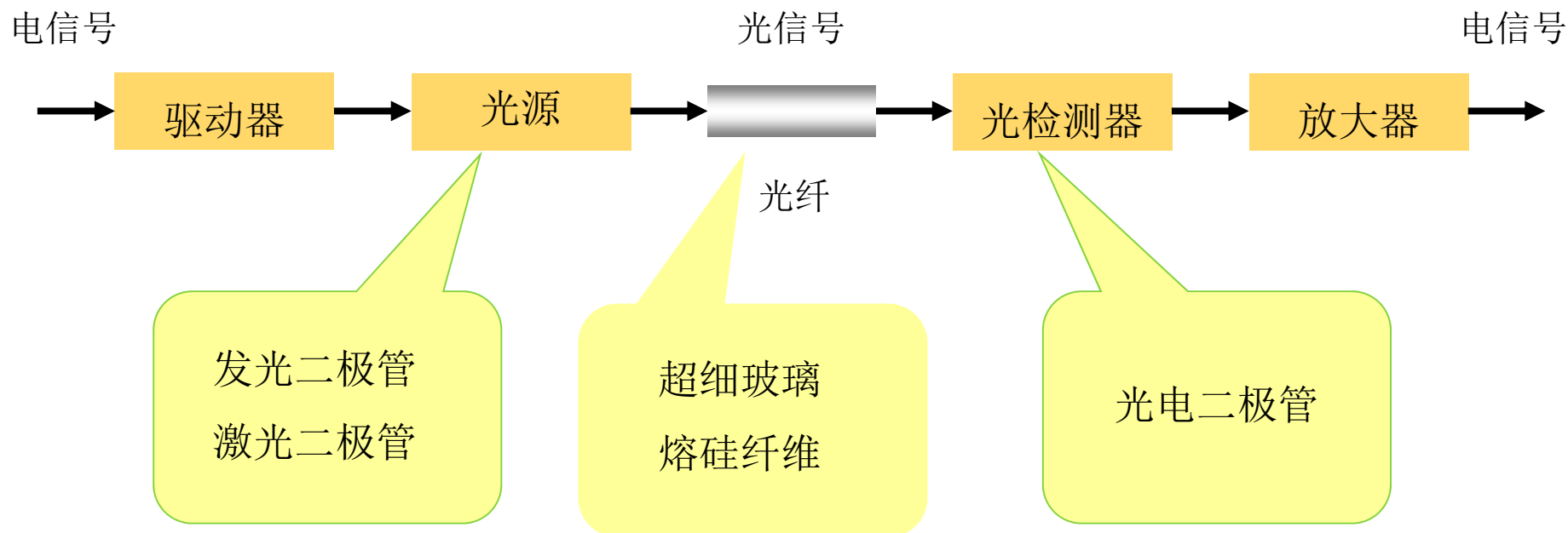
Cat 5e UTP



Cat 5e STP

# 光传输系统

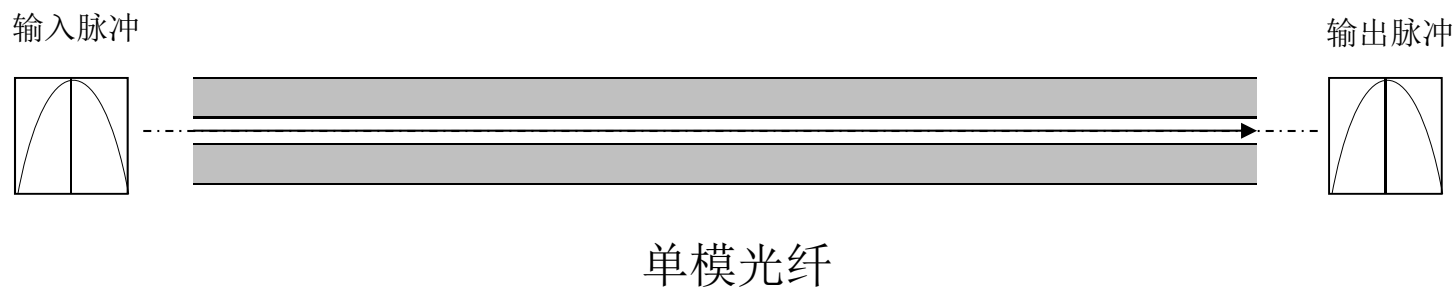
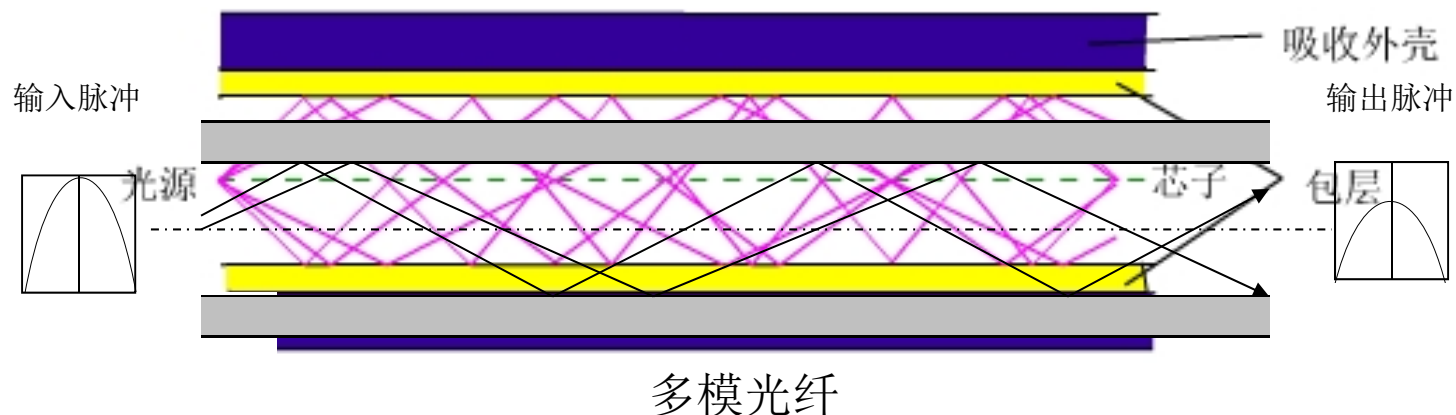
- 光传输系统由三个部分组成：光纤传输介质、光源和检测器





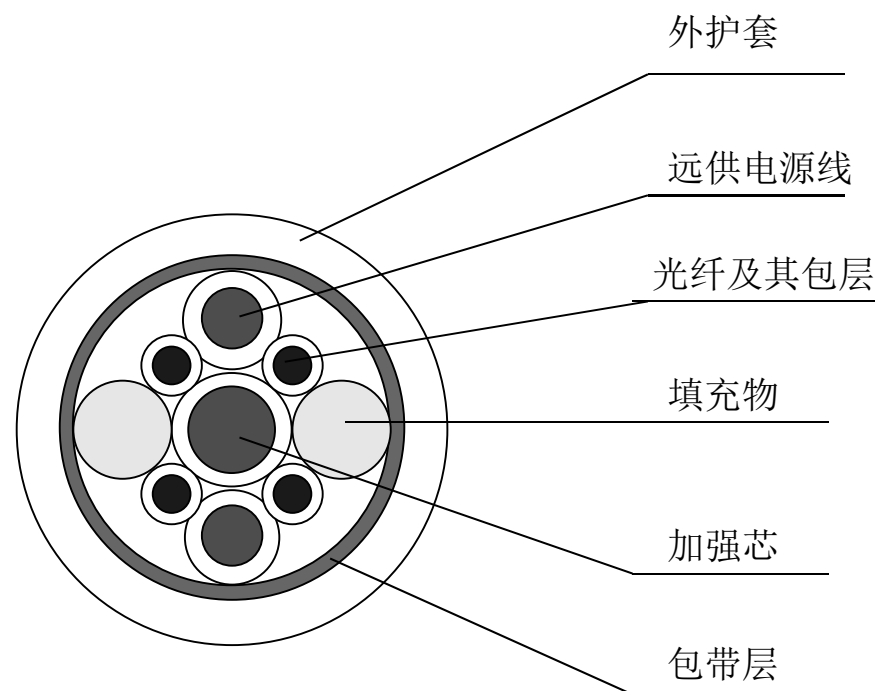
# 光信号在光纤中的传输

- 光脉冲在光纤中的传输是利用了光的全反射原理
- 光纤分为多模光纤和单模光纤



# 光缆的结构和传播特性

- 光缆的结构
- 光缆的传播特性
  - 损耗
  - 色散

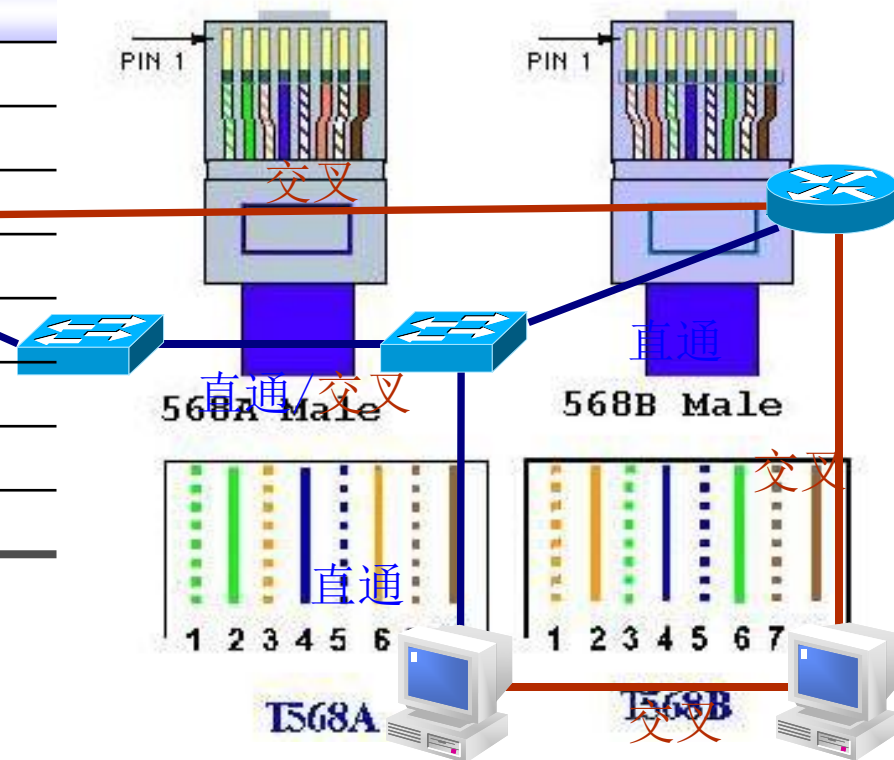


# 线缆的连接2-1

- EIA/TIA 568A和568B

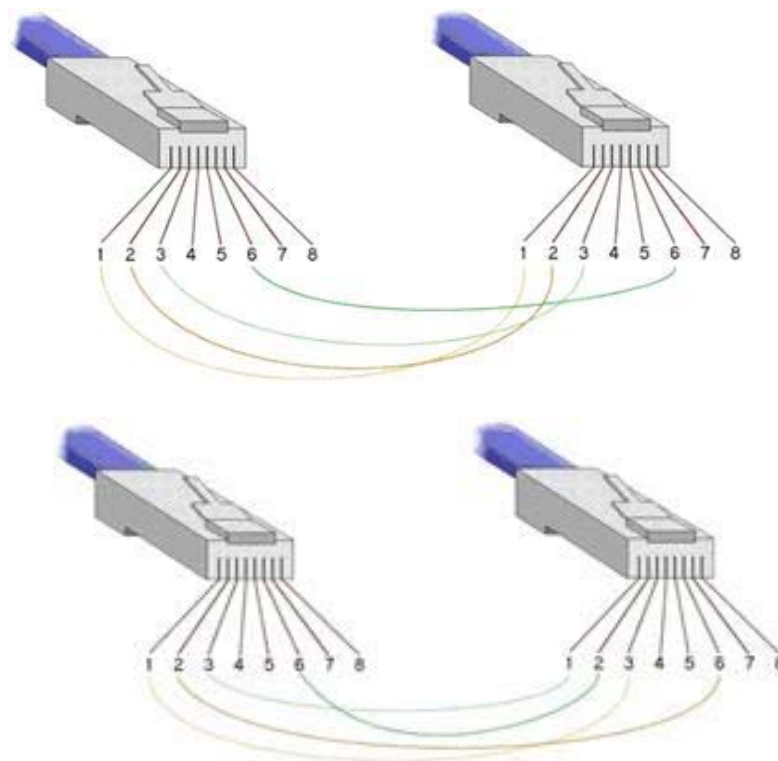
管脚号	用途	颜色
1	发送 +	白色和绿色
2	发送 -	绿色
3	接收 +	白色和橘黄色
4	不被使用	蓝色
5	不被使用	白色和蓝色
6	接收 -	橘黄色
7	不被使用	白色和棕色
8	不被使用	棕色

T568A标准中RJ-45连接器的  
管脚号和颜色编码



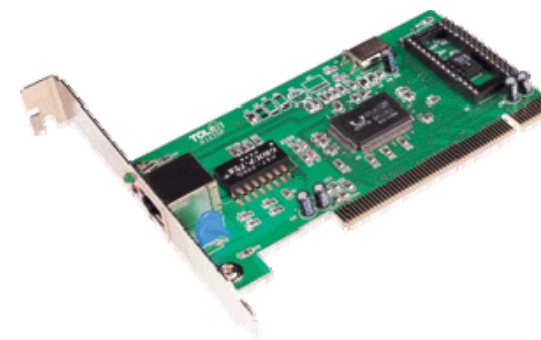
## 线缆的连接2-2

- 标准网线的线序
- 交叉网线的线序
- 制作过程



# 物理层的设备3-1

- 网络接口卡
  - 连接计算机和网络硬件
  - 按照提供的线缆接口类型可分为RJ-45接口网卡、光纤网卡等
  - 便携式电脑可使用PCMCIA网络接口卡

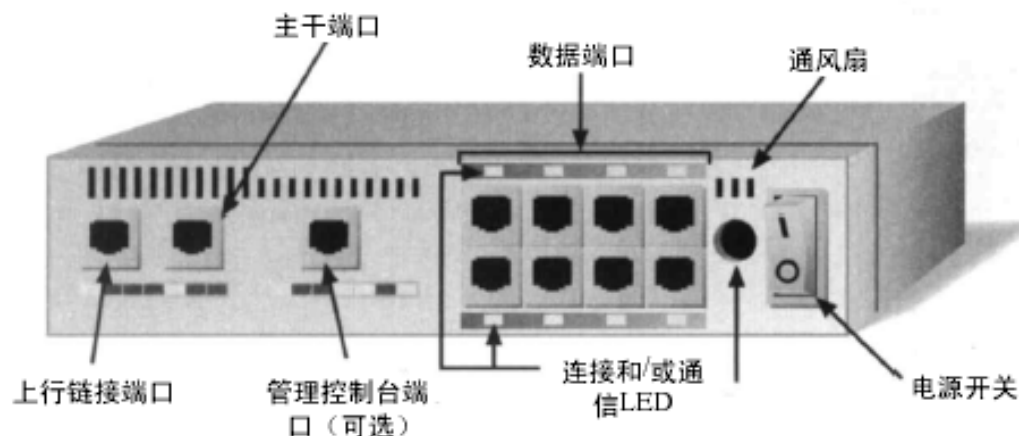


# 物理层的设备3-2

- 中继器
  - 能放大信号
  - 延长网络传输距离
  - 只包含有一个输入端口和一个输出端口，所以只能接收和转发数据流
  - 成本低

# 物理层的设备3-3

- 集线器
  - 最初只是一个多端口的中继器
  - 可用于星形拓扑结构
  - 能够支持各种不同的传输介质和数据传输速率
  - 有些集线器具有内部处理能力，例如，可以接受远程管理、过滤数据或提供网络诊断信息
  - 被交换机所取代



# 常见线缆

- 10Base5--粗缆 最大传输距离500米
- 10Base2--细缆 最大传输距离185米
- 10BaseT—双绞线 最大传输距离100米
- 10BaseF—光纤 传输距离1000米以上
- 100Mbps快速以太网
- 100Mbps快速以太网



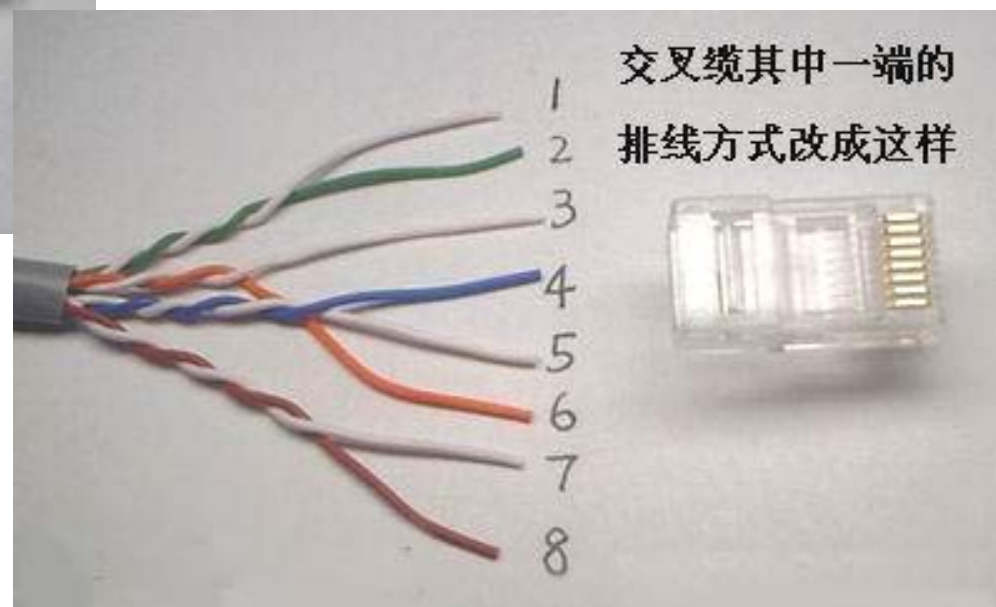
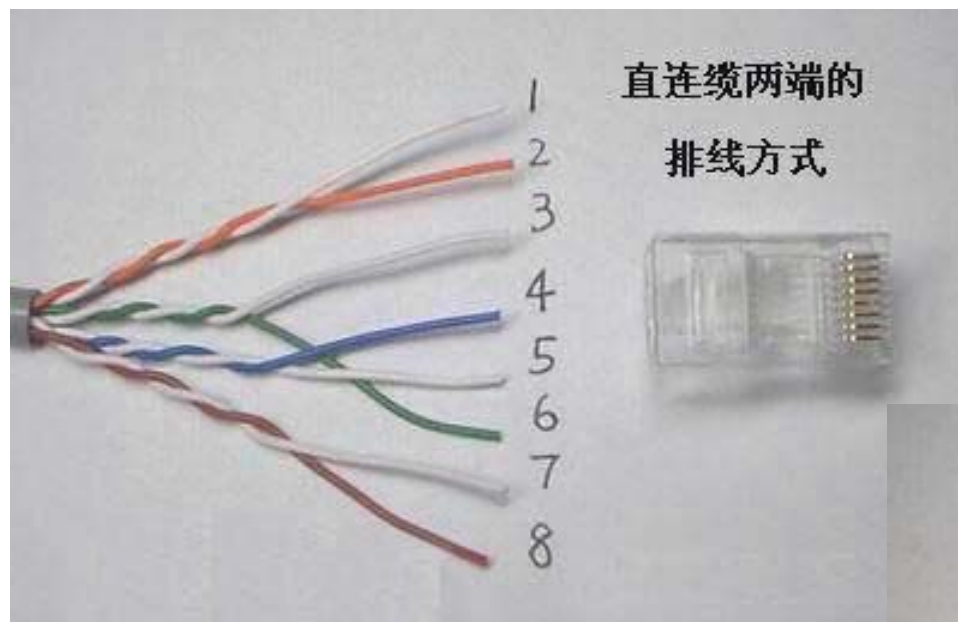


非屏蔽双绞线(UTP)



屏蔽双绞线(STP)

# 物理层-直连线 and 交叉线



# 物理层-典型光纤线路



- 无线技术的分类
  - GSM、GPRS、CDMA、3G
  - 蓝牙、红外、RFID
  - WiFi – IEEE 802.11 abgn



- 无线网络标准

- IEEE 802.11是IEEE最初制定的一个无线局域网标准。由于802.11在速率和传输距离上都不能满足人们的需要，IEEE小组又相继推出了802.11b和802.11a两个新标准。

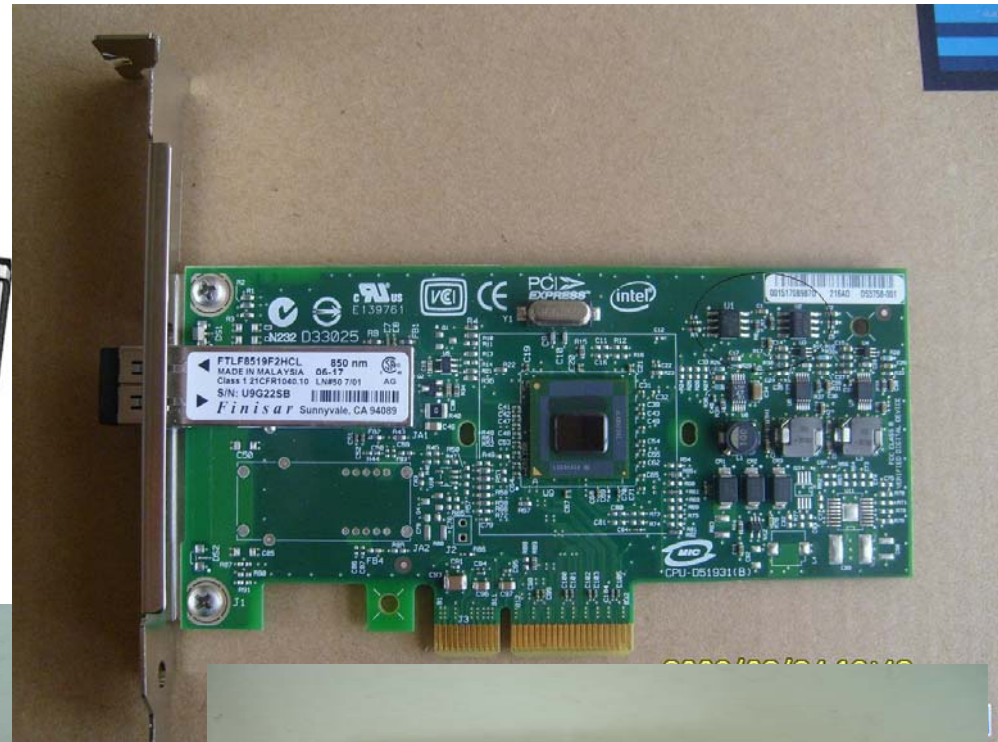
- IEEE 802.11家族

- 802.11 (原始标准) —— 2M bps, 2.4G Hz
- 802.11a (物理层补充) —— 54M bps, 5G Hz
- **802.11b** (也被称为**WLAN/Wi-Fi**) —— 11M bps, 2.4G Hz
  - 迅驰技术 (Centrino) 就是基于这个标准
- **802.11g** (兼容802.11b) —— 54M bps, 2.4G Hz
  - 目前最成熟的技术，家用的无线宽带路由器多是采用这个标准
- 802.11n —— 300M bps

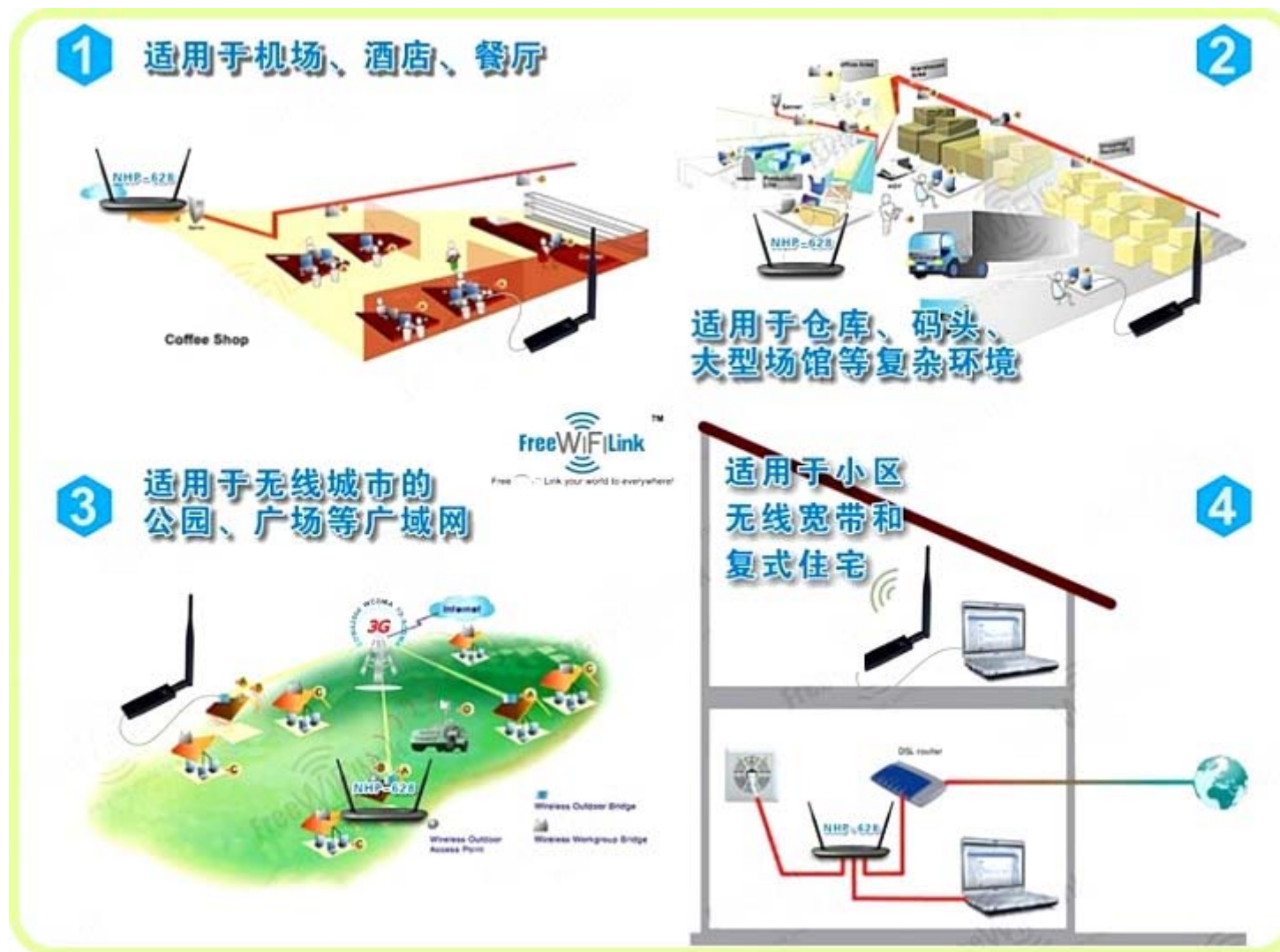




# 物理层-无线网卡

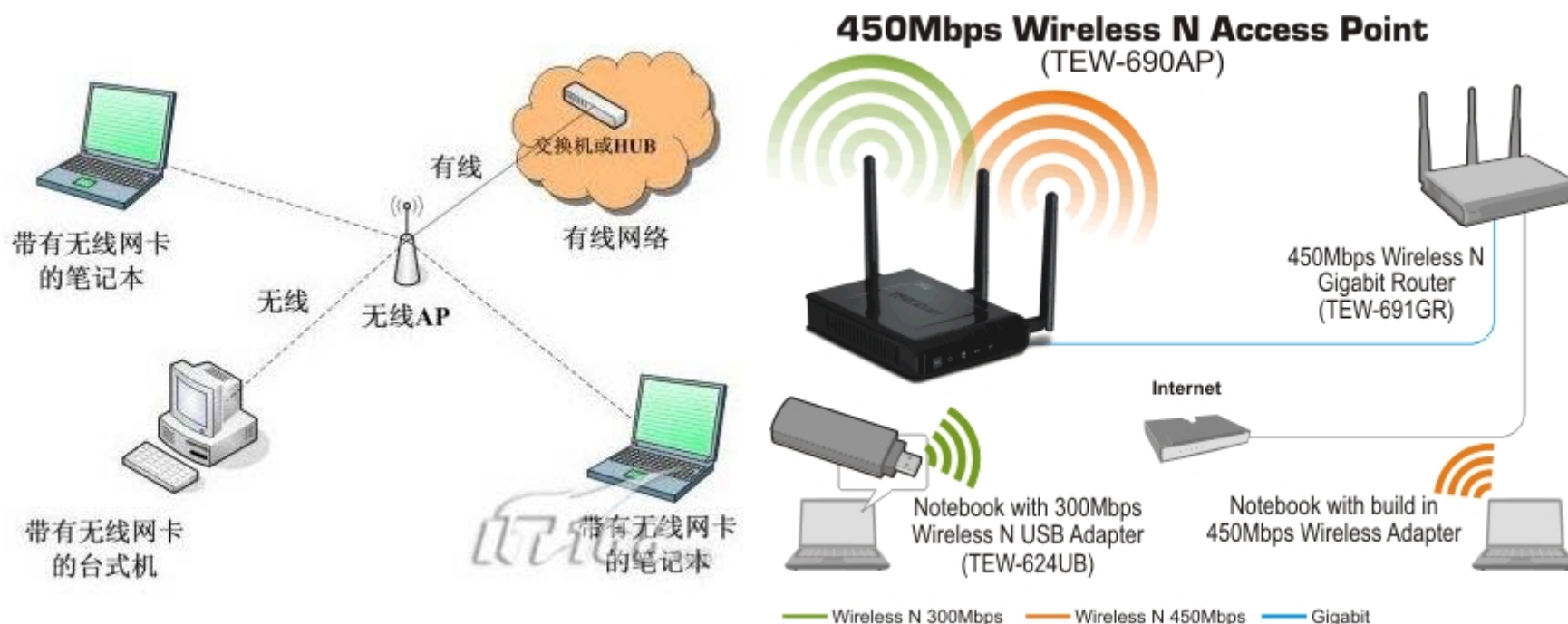


# 物理层-无线网卡之适用场合



- 无线AP

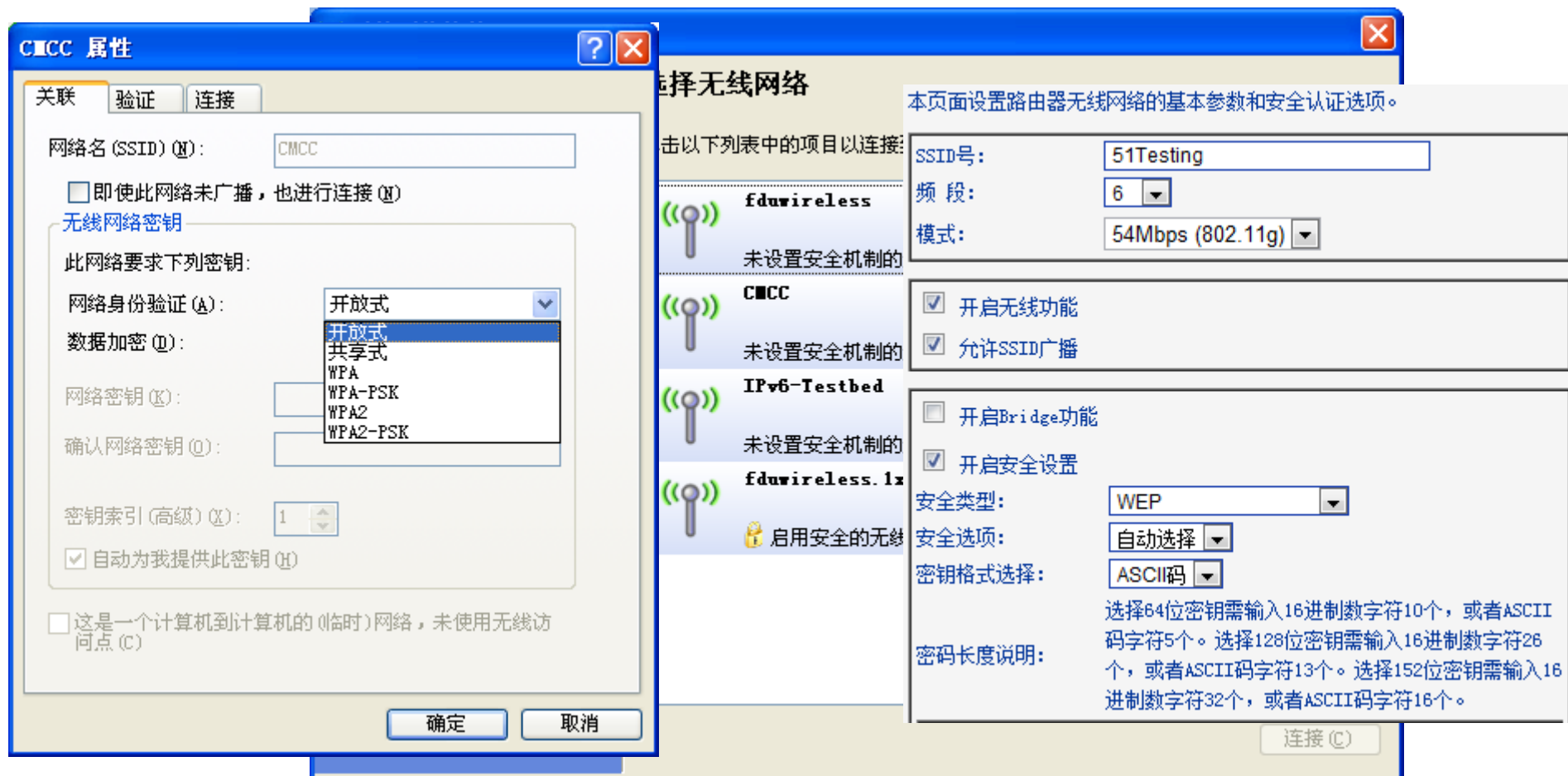
- 无线AP ( Access Point ) 即无线接入点，它是用于无线网络的无线交换机（相当于有线网络的集线器/交换机），也是无线网络的核心。





- **SSID**(Service Set Identifier)
  - SSID即“**无线网络名**”，是一个1~32个字符组成的ASCII字符串，它会输入到客户端和AP中。IEEE标准要求广播SSID，这有利于方便的架设无线网络，但同时也降低了安全程度。
  - 第一代WLAN安全主要依靠唯一的SSID和MAC地址来进行认证。
  - 通过嗅探器可以非常容易地从WLAN数据中捕获有效的SSID。
- **WEP**(Wired Equivalent Privacy)
  - 全称**有线等效协议**。是为了保证802.11b协议数据传输的安全性而推出的安全协议，该协议可以通过对传输的数据进行加密（静态密钥），以保证无线局域网中数据传输的安全性。
  - 采用**RC4**对称加密算法来加密从AP或无线网卡发送出去的数据包。
- **WPA/WPA2**(Wi-Fi Protected Access)
  - 全称**网络安全存取**。由于WEP的不安全性，在802.11i协议完善前，采用WPA为用户提供一个临时性的解决方案。WEP是共享一个密码，而WPA实现“一户一密”。WPA的核心就是TKIP和IEEE802.1X。
  - WPA2采用**AES**算法，比WEP更难以入侵。WPA2是WiFi联盟验证过的IEEE 802.11i标准的认证形式，实现了802.11i的强制性元素。

# 物理层-无线网络安全加密技术(2)



- 计算机数据的传输方法：
  - 模拟传输
    - 模拟信号转成数字信号，需要调制。模拟传输的调制方法：
      - 调幅 ( AM )
      - 调频 ( FM )
      - 调相 ( PM )
  - 数字传输
    - 数字传输的调制方法：
      - 脉码调制 ( PCM )
        - » T1 ( 北美采用的标准 )
        - » E1 ( 欧洲和中国采用的标准 )

专业测试保障卓越品质

The high quality derived from the professional testing

测试

## 数据链路层

- 目的
  - 保证数据在物理链路上实现**可靠**的传输
- 任务
  - 解决信道共享及维护数据帧的完整性
- 数据链路层由两个子层组成
  - LLC ( 逻辑链路控制层 , Logic Link Control )
  - MAC ( 介质访问控制层 , Media Access Control )
    - 解决数据如何在底层传输的问题

- 目的
  - 完成发送方占用信道的问题
- 任务
  - 将上层传下来的数据封装成帧进行发送（接收时进行相反的过程，将帧拆卸）
  - 实现和维护MAC协议
  - 比特差错检测
- 占用信道的方法
  - 争用（Contention）——以太网采用的方法
  - 令牌（Token passing）——令牌环网采用的方法
  - 轮询（Polling）
- MAC寻址
  - MAC地址：硬件厂商提供的唯一物理地址。用以在网络上区分各个设备。

- 目的
  - 保证帧传送的完整性和无误性
- 任务
  - 建立和释放LLC层的逻辑连接
  - 提供与高层（网络层）接口
  - 差错控制
  - 流量控制（Flow Control）

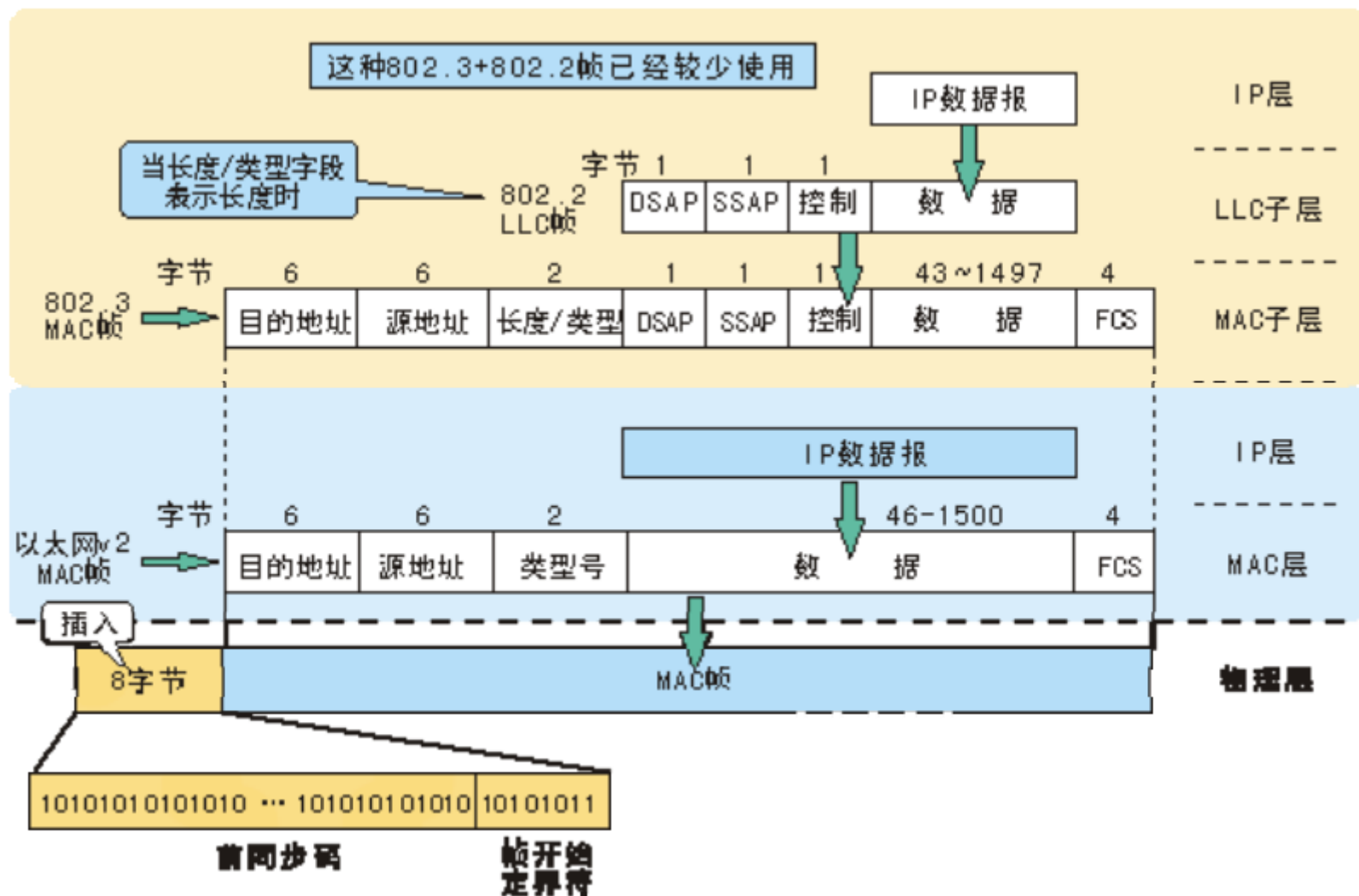
- 什么是CSMA/CD ?
  - 全称是 Carrier Sense Multiple Access with Collision Detection，即“带冲突检测的载波侦听多路访问”，是一种“争用”型的MAC协议。
- 目的
  - 提供寻址和介质存取的控制方式，使得不同设备或网络上的节点可以在多点的网络上通信而不相互冲突。
- 工作原理
  - 先听后发，边发边听，冲突停发，随机延迟后重发。
- 优点
  - 原理比较简单，技术上易实现，网络中各工作站处于平等地位，不需集中控制，不提供优先级控制。
- 缺点
  - 在网络负载增大时，冲突增加，发送时间延长，发送效率下降。



- 网桥(Bridge)
  - 一种在数据链路层实现中继，常用于连接两个或更多个局域网的网络互连设备。
  - 根据MAC地址对帧进行转发
    - 网桥从一个局域网接收MAC帧，拆封、校验之后，按另一个局域网的格式重新组装，发往它的物理层。
  - 可以隔离碰撞（冲突）。
  - 可以看作一个“低层的路由器”。
    - 网桥将多个网段在数据链路层连接起来。路由器则在网络层。
- 桥接(Bridging)
  - 基于公共的数据链路层协议将两个通信网络互连，并基于链路地址(MAC地址)选择要传递的数据的过程。
  - 一般的交换机，网桥就有桥接作用。

- 历史上的以太网有五种帧结构
  - Ethernet V1
  - Ethernet V2(ARPA)
    - 目前以太网事实上的标准
    - 在 RFC 894 中定义
  - RAW 802.3
  - 802.3/802.2 LLC
  - 802.3/802.2 SNAP

# 以太网的帧结构——Ethernet II



专业测试保障卓越品质

The high quality derived from the professional testing

测试

网络层

- 网络层的主要作用：
  - 建立网络连接，提供网络地址，提供寻址
  - 数据的分段和重组
  - 实现网络数据单元（包）的传送
  - 路由选择
  - 拥塞控制
  - 差错控制
  - 消除通信子网的质量差异
  - 确定网络层服务质量参数，如网络吞吐量、网络延迟等

- 数据交换方式
  - 电路交换
  - 存储转发交换（也叫报文交换）
  - 包交换（也叫分组交换）
    - 数据报方式
    - 虚电路方式

- 网络层提供的服务
  - 面向连接的服务
    - 主要是虚电路服务（电话型服务）
    - 典型服务是X.25协议
  - 面向无连接的服务
    - 主要是数据报服务（电报型服务）
    - 典型服务是IP协议

- 路由选择
  - 源节点和目的节点之间一般有多条传输路径供选择，网络中每个中间节点在收到一个数据包后，都要确定向下一个节点传送的路径，这就是路由选择。完成路由选择的设备叫路由器。
- 路由算法有以下几种：
  - 静态路由选择策略
    - 扩散法
    - 固定路由选择
    - 随机路由选择
  - 动态路由选择策略
    - 独立路由选择
    - 集中路由选择
    - 分布路由选择



## 网络层的功能

- 定义了基于IP协议的逻辑地址
- 选择数据通过网络的最佳路径

# 网络层-IP协议之IPv4数据报（1）

- IPv4数据报是一个可变长的包（最小为20字节，最大65536字节）。它由头部和数据两部分组成，头部的长度是20-60字节。

版本号 4位	头部长度 4位	服务类型8位	数据报总长度16位	
标识16位			标志3位	段偏移量13位
生存期8位		协议类型8位	头部校验和16位	
源IP地址32位				
目标IP地址32位				
可选项32位				
数据				

20  
字  
节

# 网络层-IP协议之IPv4数据报（2）

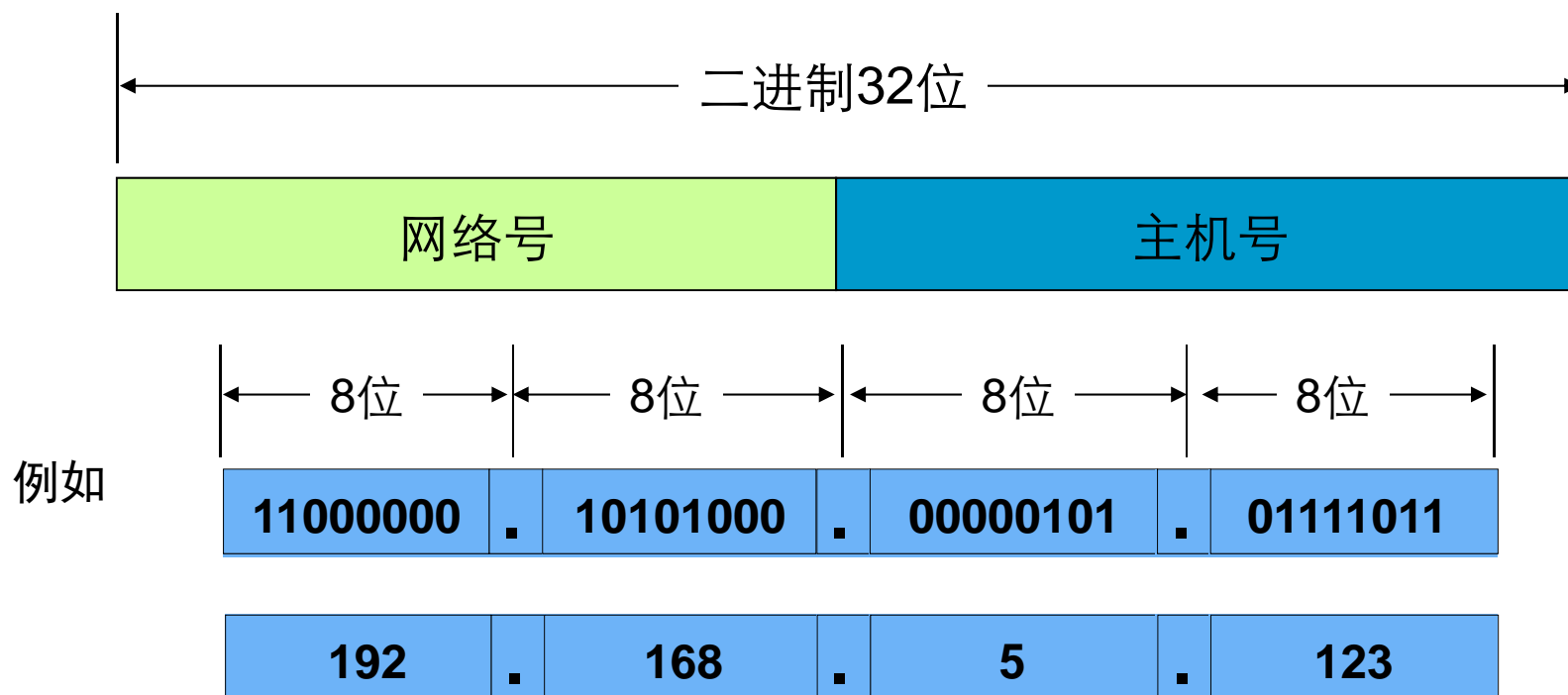


IP数据报发送顺序：先发报头，再发数据。

- 版本与协议类型
  - 版本：数据报对应的IP协议版本号（目前使用的IP协议版本号为4）
  - 协议类型：数据报数据区数据的高级协议类型（如TCP/UDP）
- 长度
  - 报头长度：报头区的长度（以32bit为单位）
  - 总长度：整个IP数据报的长度（以8bit为单位）
- 服务类型
  - 转发过程中对该数据报的处理方式
- 生存周期（TTL）
  - IP数据报在互联网中的存活时间（避免死循环）
- 头部校验和
  - 保证IP数据报报头的完整性
- 地址
  - 源IP地址：数据报的发送者
  - 目的IP地址：数据报的接收者

- IP地址

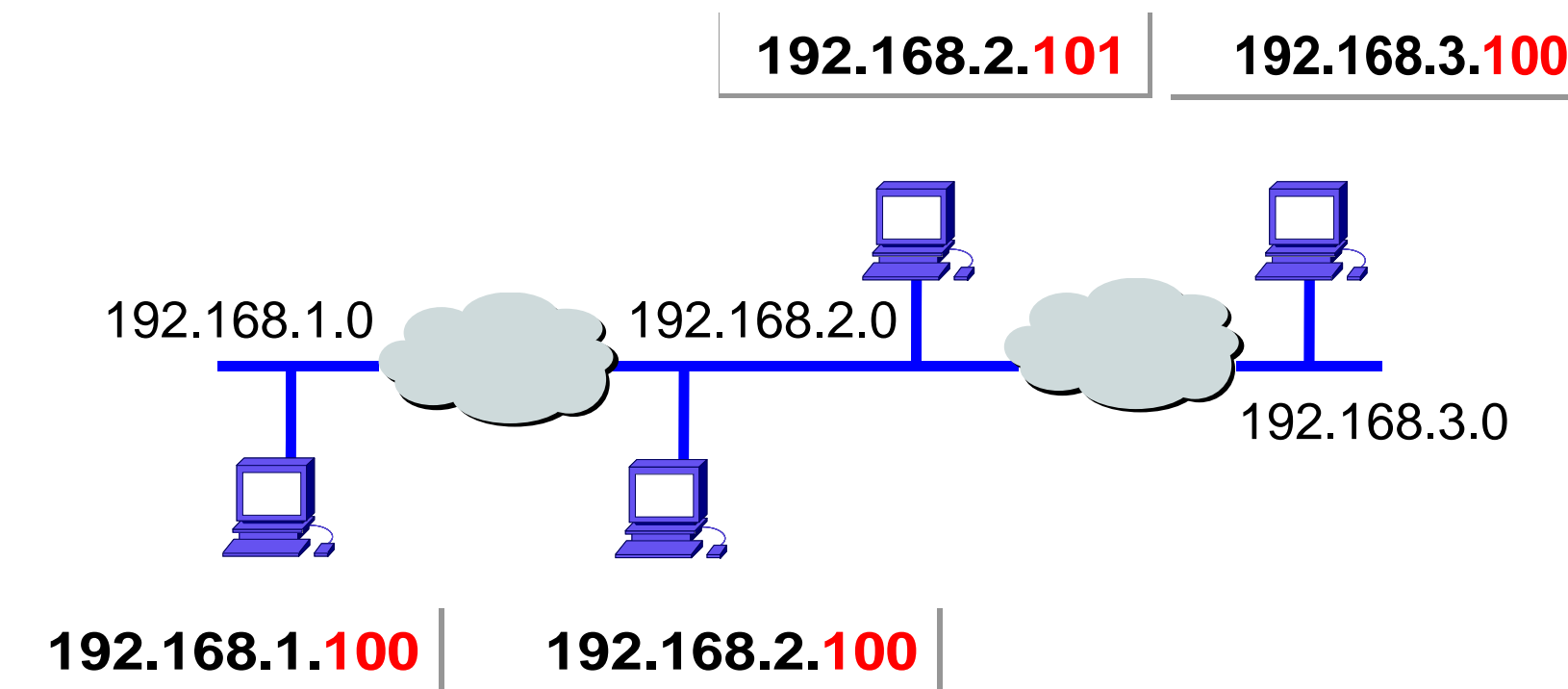
- IPv4地址由32位二进制数字组成，每8位为一段，共分为4段，段间用“.”分隔。为了易于阅读，IP地址的每一段表示为其对应的十进制数字，称为“点分十进制”表示形式。
- IPv4地址由类型、网络号和主机号三个部分组成。路由寻址时，首先根据地质的网络号到达网络，然后利用主机号到达主机。
- IPv4地址分为五类，不同的类型适用于不同规模的网络。



公有IP地址是唯一的，因为公有IP地址是全局的和标准的，所以没有任何两台连到公共网络的主机拥有相同的IP地址。所有连接Internet的主机都遵循此规则。公有IP地址是从Internet服务供应商（ISP）或地址注册处获得。

另外，在IP地址资源中，还保留了一部分被称为私有地址(private address)的地址资源供内部实现IP网络时使用。REC1918留出3块IP地址空间（1个A类地址段，16个B类地址段，256个C类地址段）作为私有的内部使用的地址，即10.0.0.0-10.255.255.255、172.16.0.0-172.31.255.255和192.168.0.0-192.168.255.255。根据规定，所有以私有地址为目标地址的IP数据包都不能被路由至外面的因特网上，这些以私有地址作为逻辑标识的主机若要访问外面的因特网，必须采用网络地址翻译(Network address translation，简称NAT)或应用代理(proxy)方式。

- 用来标识一个节点的网络地址

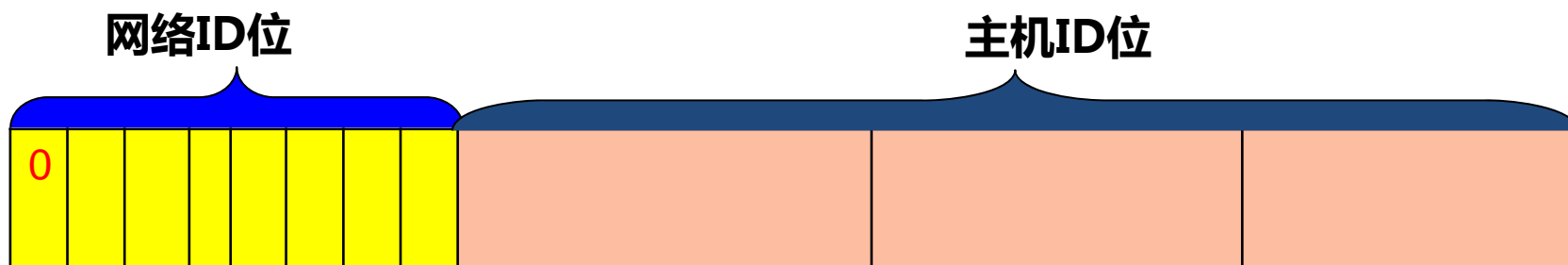


- 根据IP网络的大小，IP地址分为A类、B类、C类、D类和E类地址。A类地址表示大型的网络，支持大量的IP地址；B类地址表示中型的网络；C类表示小型的网络。为了区分这些地址，利用第一个八位组规则（first octet rule）。

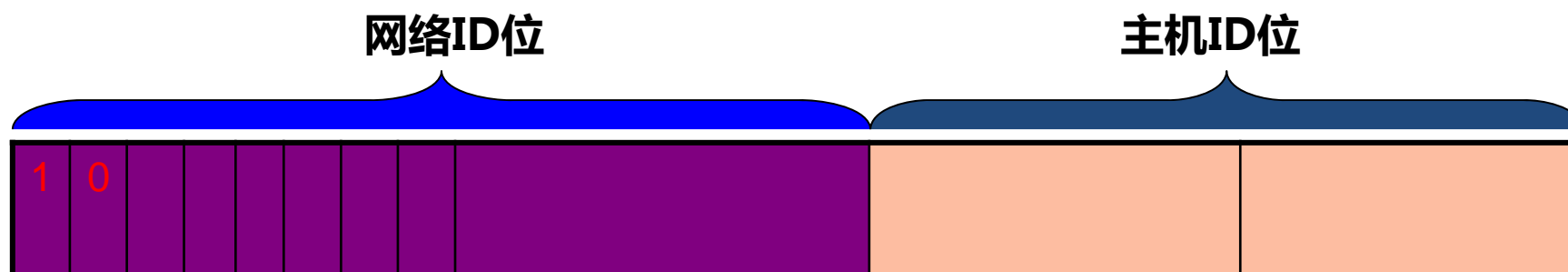
Classes	First octet rule	Maximum and Minimum(二进制)	十进制
A类	0	00000000-01111111	1~126
B类	10	10000000-10111111	128~191
C类	110	11000000-11011111	192~223
D类	1110	11100000-11101111	224~239（组播）
E类	11110	11110000-11111111	240~255（保留）



- IPv4 A类地址
  - A 类网络 ID 的前缀长度只有 8 位。
  - A 类网络 ID 的网络数量限制为1~ 126 个。
  - 主机 ID 24 位可用来标识多达 16,777,214 个主机。

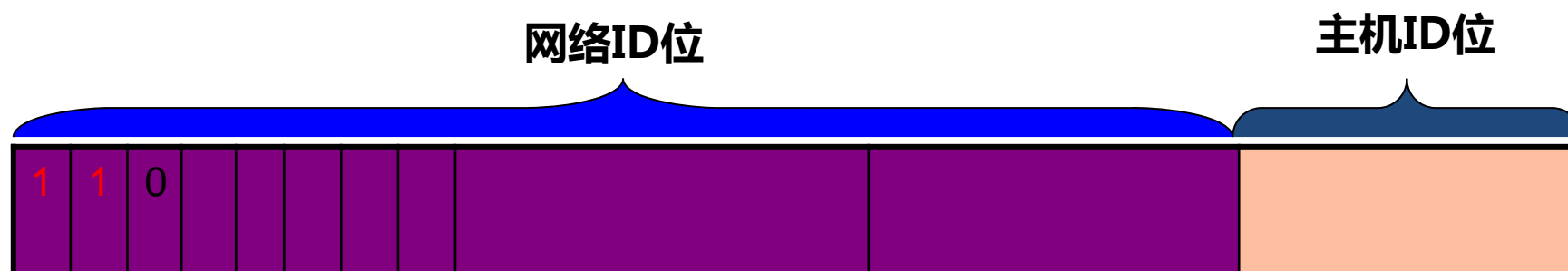


- IPv4 B类地址
  - 用 14 位表示 B 类网络 ID，用 16 位表示主机 ID。
  - 可以将 B 类地址分配给 16,384 个网络，（128~191）每个网络可以有 65,534 个主机。



- IPv4 C类地址

- C类地址的三个高序位总是设置为 110，前 24 位中剩余21位指定特定的网络，后 8 位指定了特定的主机。
- C类地址可以分配给 2,097,152 个网络，（ 192~223 ）每个网络可以有 254 个主机。



# 网络层-IP协议之特殊的IP地址

网络号	主机号	地址类型和用途
Any	全0	网络地址，代表特定网段
Any	全1	网段广播地址，代表特定网段的所有节点
127	Any	环回地址，常用于环回测试
全0		代表所有网络，常用于指定默认路由
全1		全网广播地址，代表所有节点

- 子网掩码的作用：
  - 区分IP地址中的网络号和主机地址。
  - 将一个网络再划分为若干个子网。
- 子网掩码的表示方法和IP地址一样，有十进制和二进制两种表示方法，对A类、B类、C类地址的掩码为：

Class	二进制表示	十进制表示
A类	11111111000000000000000000000000	255.0.0.0
B类	11111111111111110000000000000000	255.255.0.0
C类	11111111111111111111111100000000	255.255.255.0

- 网络地址的确定方法：
  - 将二进制的掩码和IP地址的二进制位进行“逻辑与（AND）”的操作，得出的结果就是网络地址；剩余的位就是主机地址。
  - 如果两台计算机的网络地址相同，则表示两台计算机属于同一网络。

- 静态IP地址
  - 由网络管理员手工配置。
  - 分IP公有地址和IP私有地址两类。
- 引导程序协议（BOOTP）
- 动态IP地址
  - 动态IP由DHCP服务器动态分配。DHCP服务器将地址池中的某个地址临时分配给主机，主机使用结束后再由DHCP服务器收回，供其他主机使用。
- 自动专用IP地址

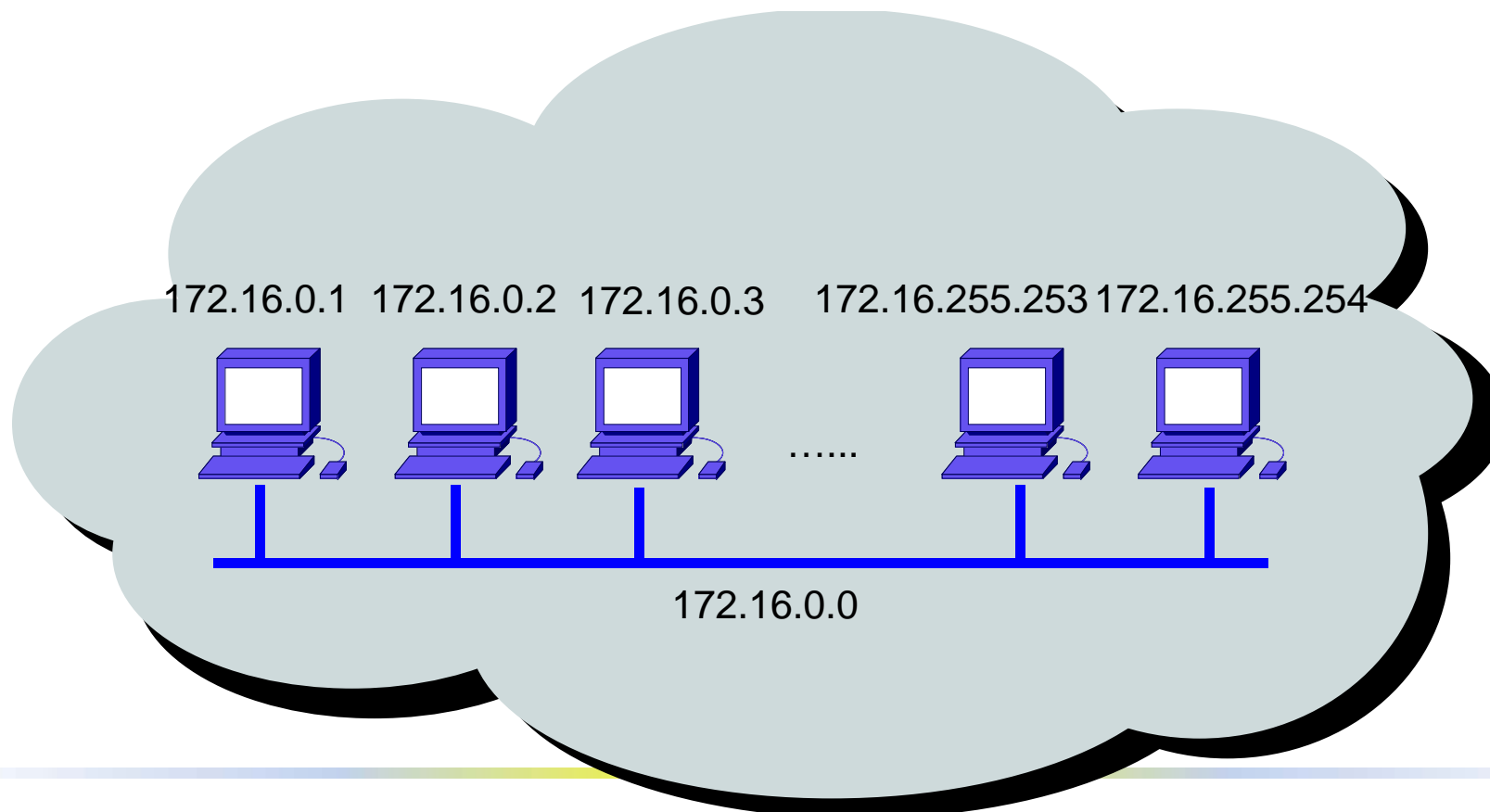
- 子网划分的作用
  - 可以连接不同的网络
  - 重新组合网络的通信量
  - 减轻网络地址数不够的负担
- 子网划分的方法
  - 可以从IP地址的主机号前面部分“借”位，并把它们指定为子网号。
  - 子网数的计算公式： $2^n$ （ $n \geq 2$ ,  $n$ 是子网号位数）
- 子网划分的步骤
  - 根据子网数目确定取子网号的位数。
    - 子网号必须是2位以上，主机号部分不能少于2位。
    - 子网号不能全为0，也不能全为1
  - 确定每个子网支持的最大主机数
  - 划分子网后的子网掩码
  - 为每个子网确定地址段

- 划分子网的作用
  - 通过将子网掩码变长，将大的网络划分成多个小的网络



# 未划分子网的IP地址

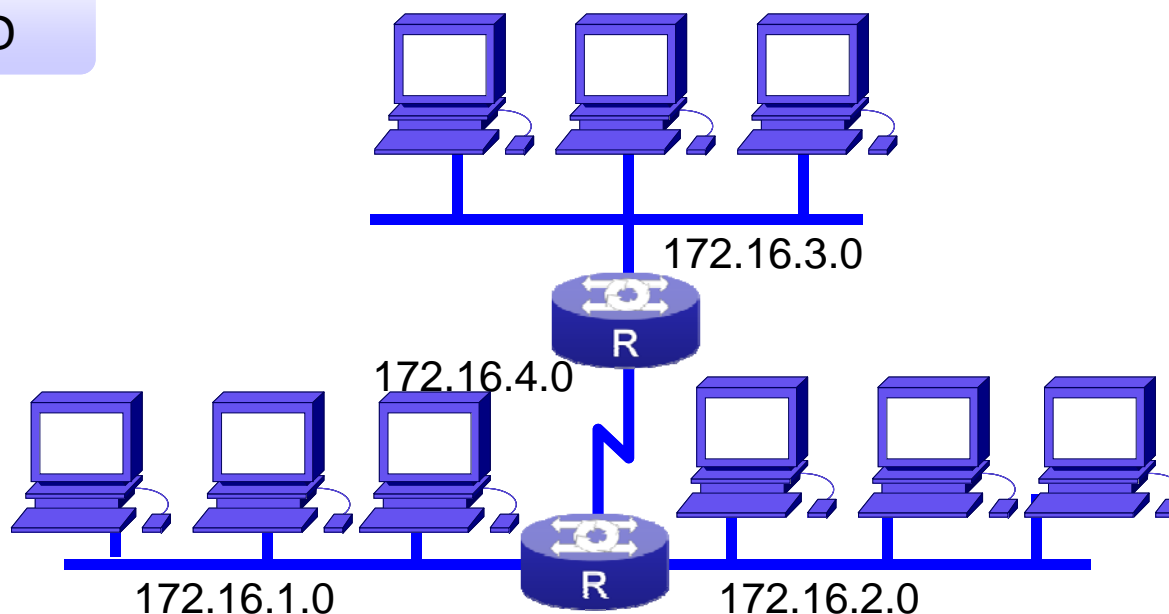
- 网络172.16.0.0，掩码255.255.0.0



# 划分子网后的IP地址

- 掩码变成255.255.255.0，  
网络划分为172.16.1.0、172.16.2.0、.....172.16.254.0

网络ID



## 不规则划分子网掩码（VLSM）

现在有一个C类IP地址: 192.168.5.0，想划分  
**20** 个子网，并且每子网里有**5** 台主机。

应该使用的子网掩码的长度是多少呢？

## 不规则划分子网掩码（VLSM）

- $2^n \geq$  需要划分的网络数量
- $2^m - 2 \geq$  每个网络中的主机数量
- $m+n=$  为划分子网前子网掩码的主机位

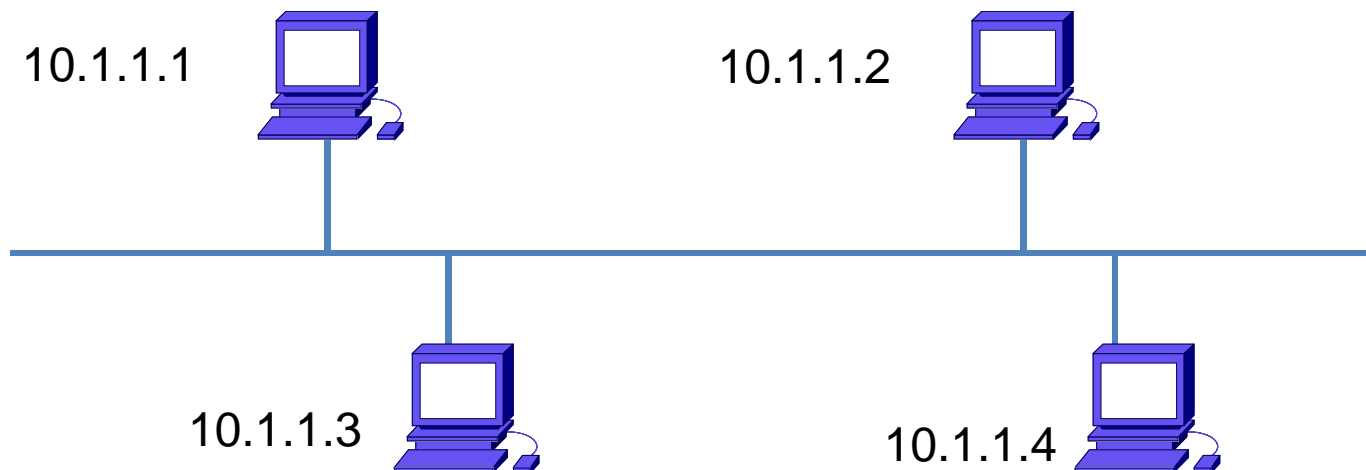
当 $n=5$ 时，  $2^n = 32 \geq 20$

$m=3$ ，  $2^m - 2 = 6 \geq 5$

因此，掩码为29位， 255.255.255.248

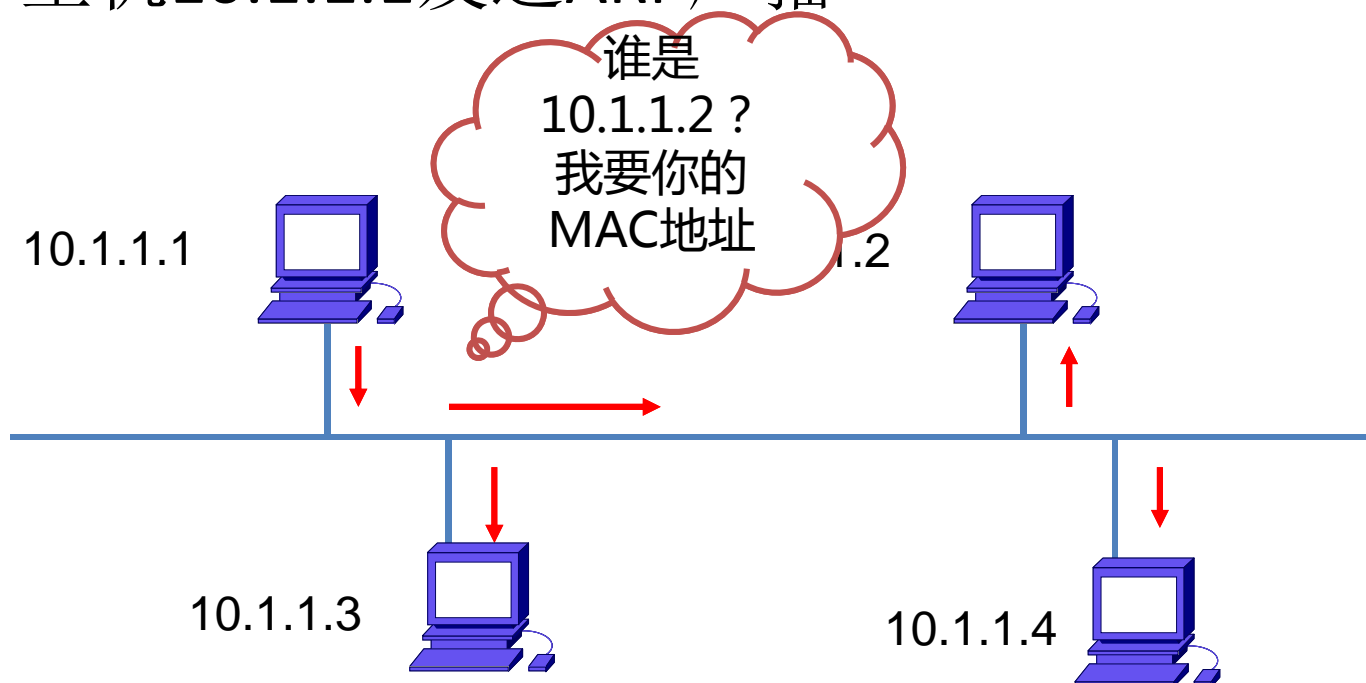
## ARP协议4—1

- IP地址解析为MAC地址
  - 主机10.1.1.1想发送数据给主机10.1.1.2，检查缓存，发现没有10.1.1.2的MAC地址



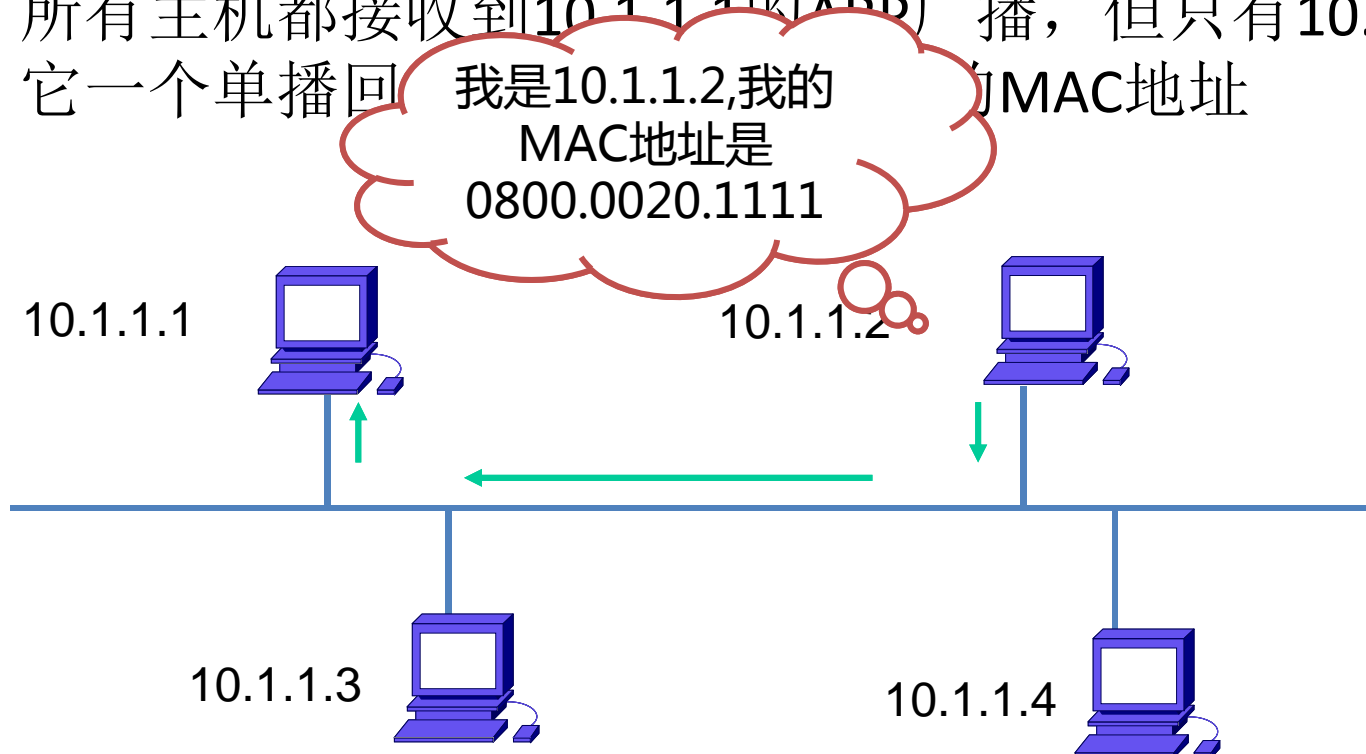
## ARP协议4—2

- IP地址解析为MAC地址
  - 主机10.1.1.1发送ARP广播



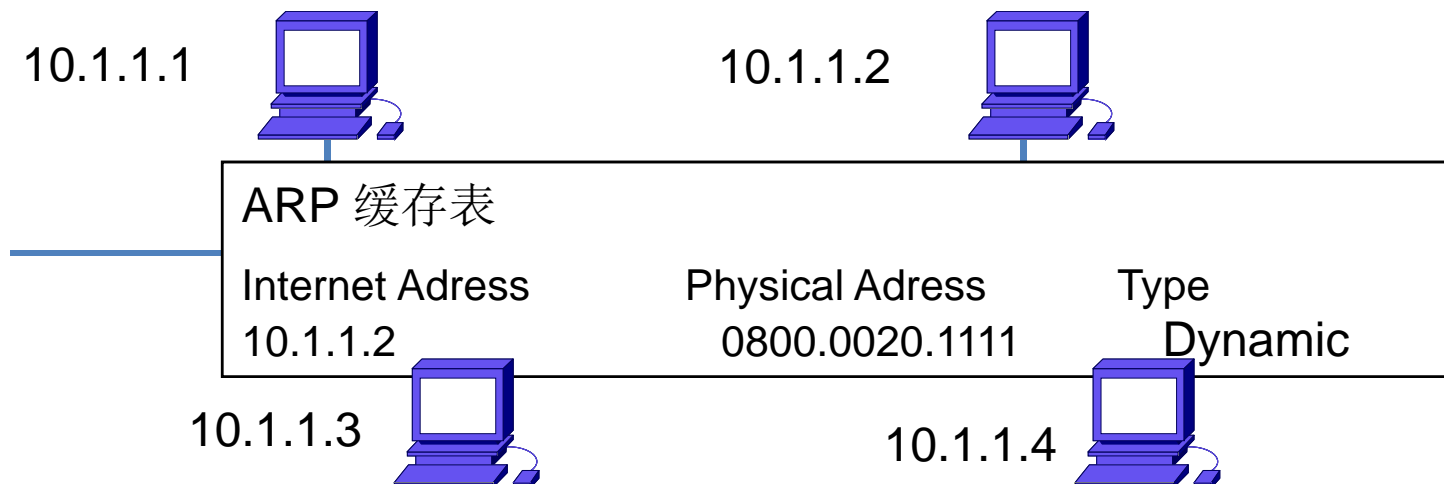
## ARP协议4—3

- IP地址解析为MAC地址
  - 所有主机都接收到10.1.1.1的ARP广播，但只有10.1.1.2给它一个单播回



## ARP协议4—4

- IP地址解析为MAC地址
  - 主机10.1.1.1将10.1.1.2的MAC地址保存到缓存中，发送数据





# 主机地址查询过程

```
C:\>arp -a  
No ARP Entries Found
```

```
C:\>ping 10.1.145.2
```

```
Pinging 10.1.145.2 with 32 bytes of data:
```

```
Reply from 10.1.145.2: bytes=32 time<10ms TTL=255  
Reply from 10.1.145.2: bytes=32 time<10ms TTL=255  
Reply from 10.1.145.2: bytes=32 time<10ms TTL=255  
Reply from 10.1.145.2: bytes=32 time<10ms TTL=255
```

```
Ping statistics for 10.1.145.2:
```

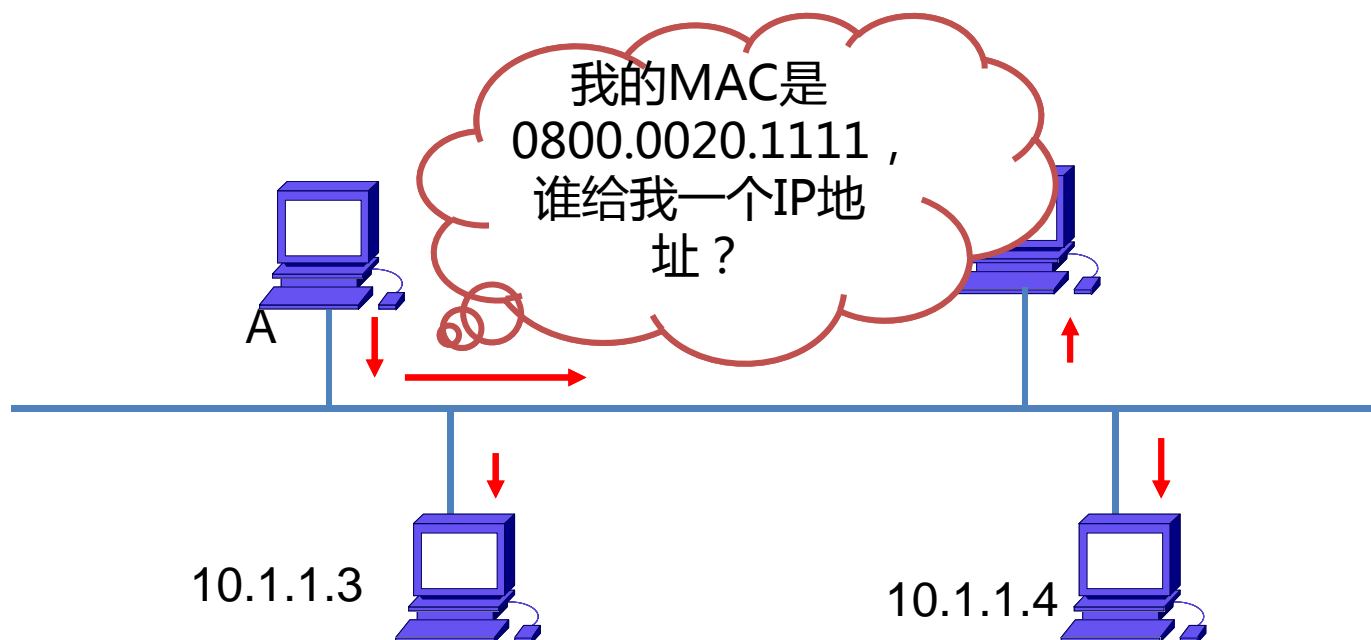
```
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),  
Approximate round trip times in milli-seconds:  
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

```
C:\>arp -a
```

```
Interface: 10.1.145.30 on Interface 0x10000003  
    Internet Address      Physical Address      Type  
    10.1.145.2            00-00-0c-07-ac-91    dynamic
```

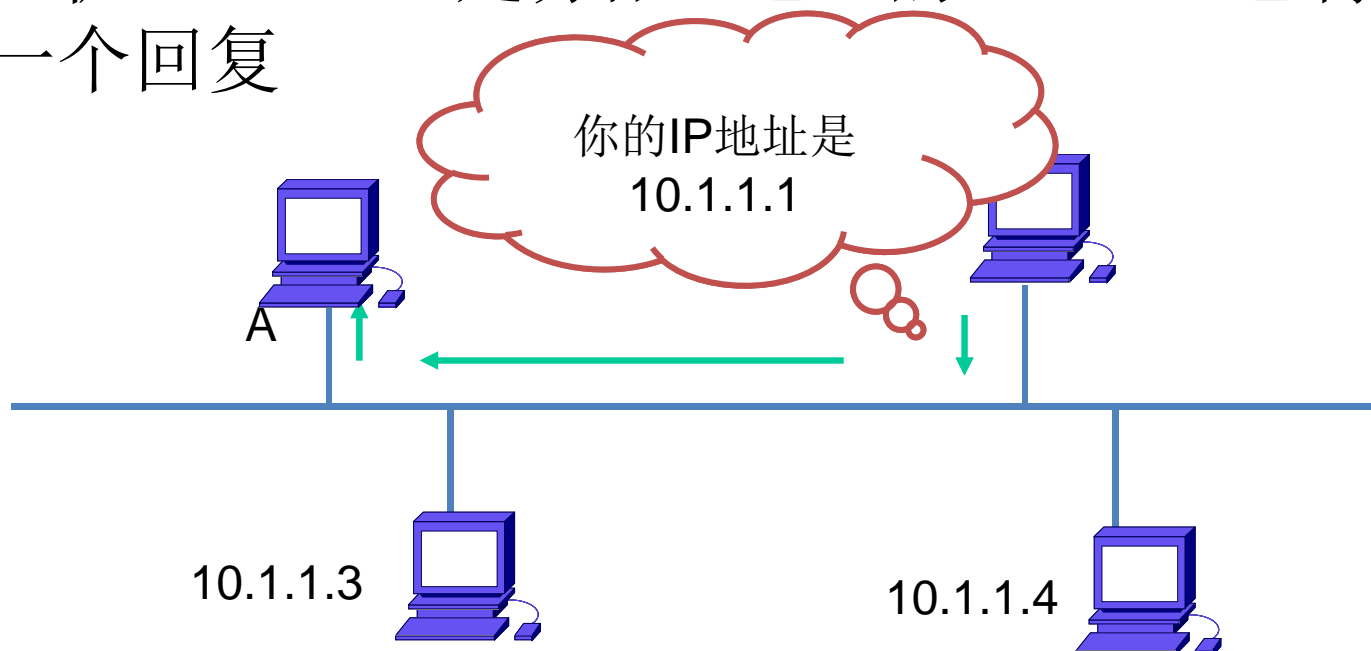
## RARP协议2—1

- MAC地址解析为IP地址
  - 主机A需要一个IP地址，发送RARP广播



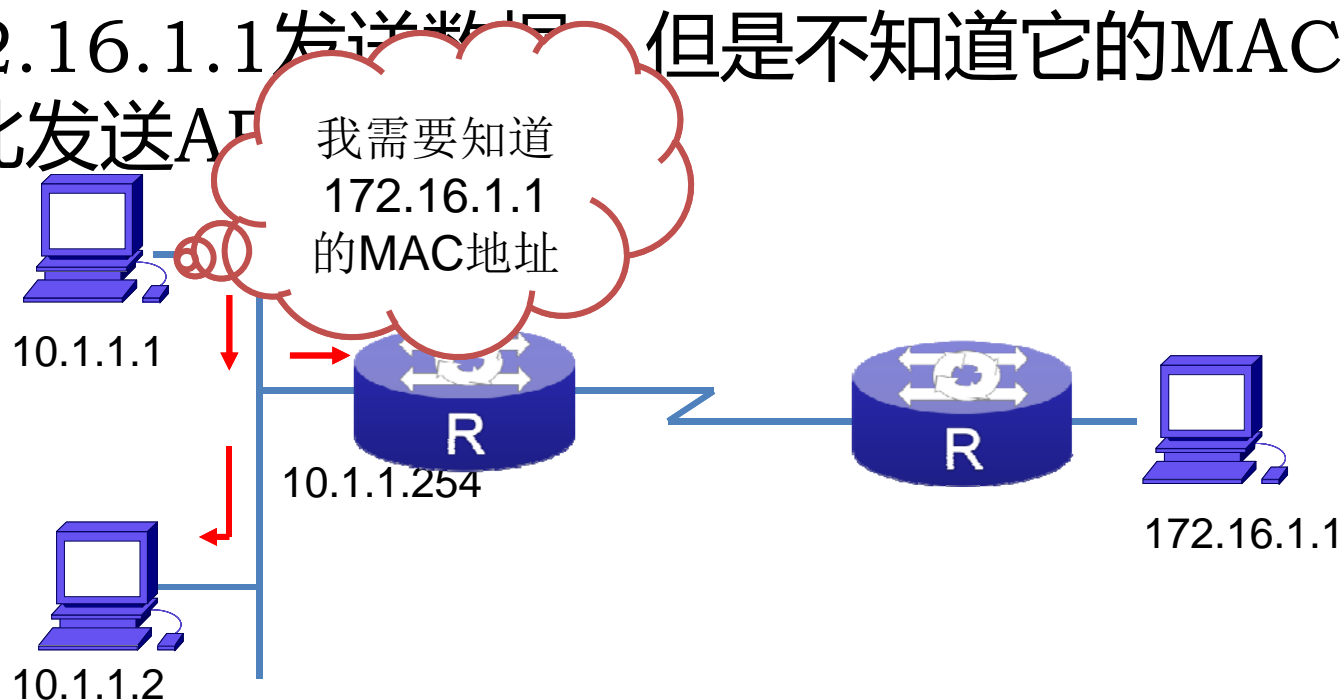
## RARP协议2—2

- MAC地址解析为IP地址
  - 主机10.1.1.254是分配IP地址的Server，它将给A一个回复



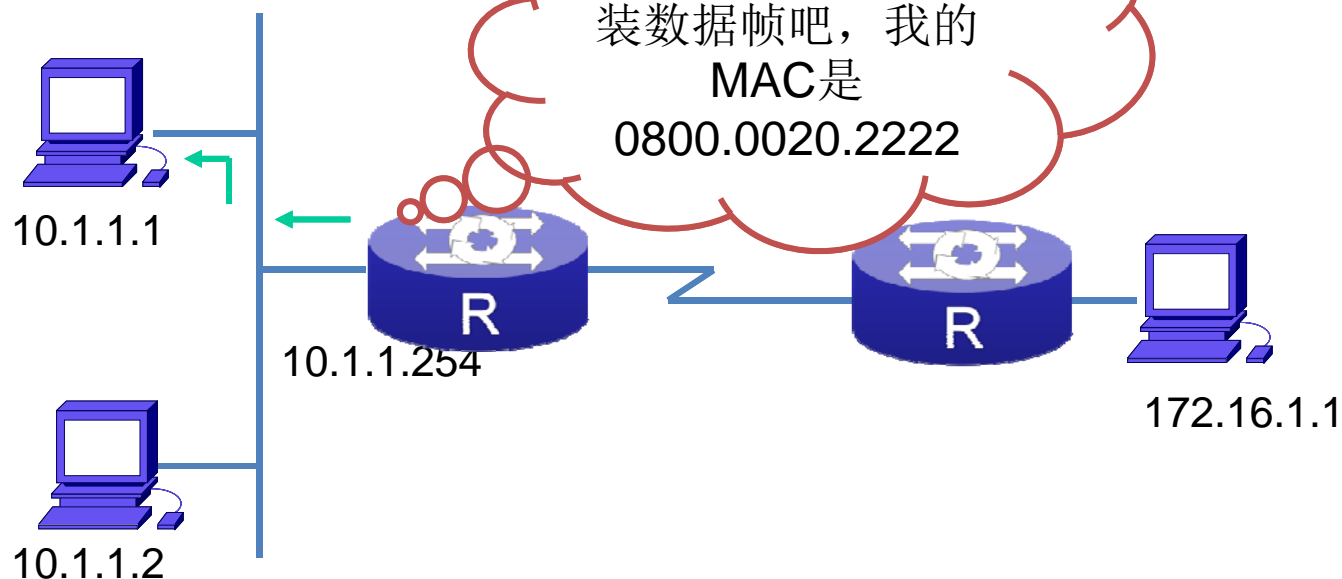
## 代理ARP工作原理2—1

- IP地址解析为网关的接口MAC地址
  - 主机10.1.1.1需要给不在同一网段的主机172.16.1.1发送数据，但是不知道它的MAC地址，因此发送ARP



## 代理ARP工作原理2—2

- IP地址解析为网关的接口MAC地址
  - 网关10.1.1.254给10.1.1.1一个单播回复，将自己的接口MAC地址告诉10.1.1.1

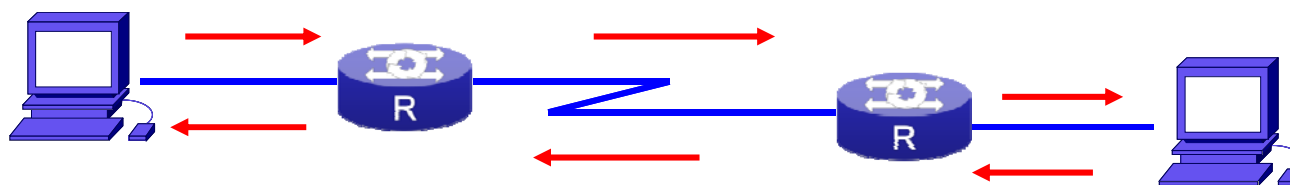


## ICMP协议

- ICMP消息通过IP数据报传送，被用来发送错误和控制信息。
- ICMP定义了很多信息类型，例如：
  - 目的地不可达
  - TTL 超时
  - 信息请求
  - 信息应答
  - 地址请求
  - 地址应答

## ICMP协议的应用2—1

- ICMP检测双向通路的连通性
- Ping命令使用ICMP协议
  - Ping [-t] [-a] [-l 字节数] Ip\_Adress/Target\_name

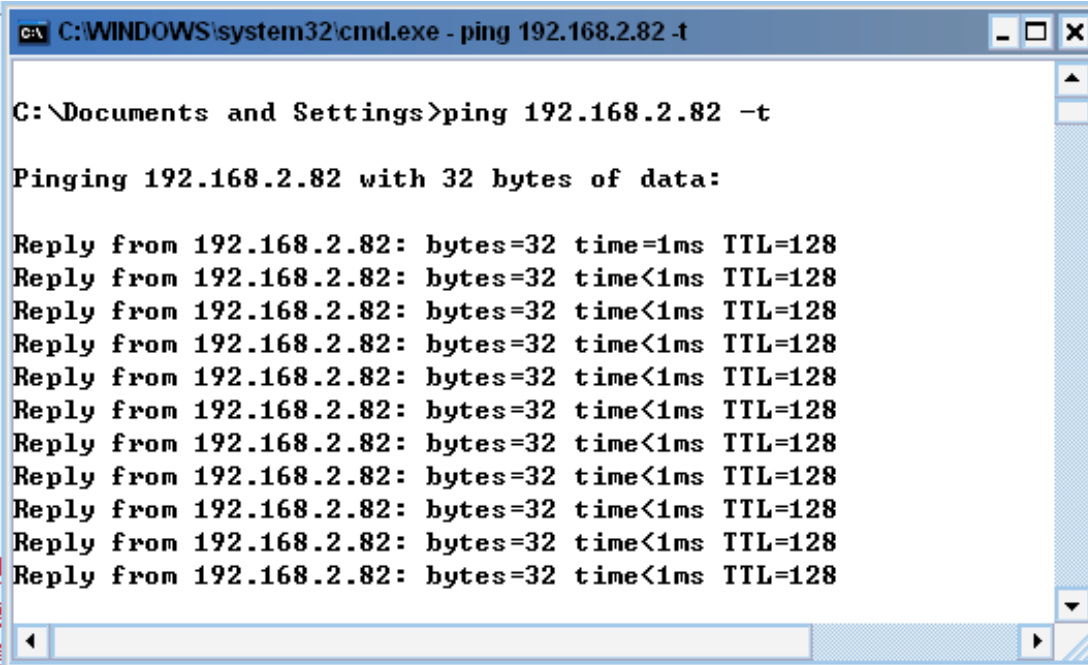


- 在一台计算机上向远程主机发起ping连接时，可能收到的返回信息有：
  - 连接建立成功
    - Reply from 192.168.1.1:bytes=32 time<1ms TTL=128
  - 目标主机不可达
    - Destination host unreachable.
  - 请求时间超时
    - Request timed out.
  - 未知主机名
    - Unknown host abc.



## Ping命令的参数3—1

- -t : 一直ping, 直到手动关闭 (Ctrl+C) 为止



```
C:\WINDOWS\system32\cmd.exe - ping 192.168.2.82 -t

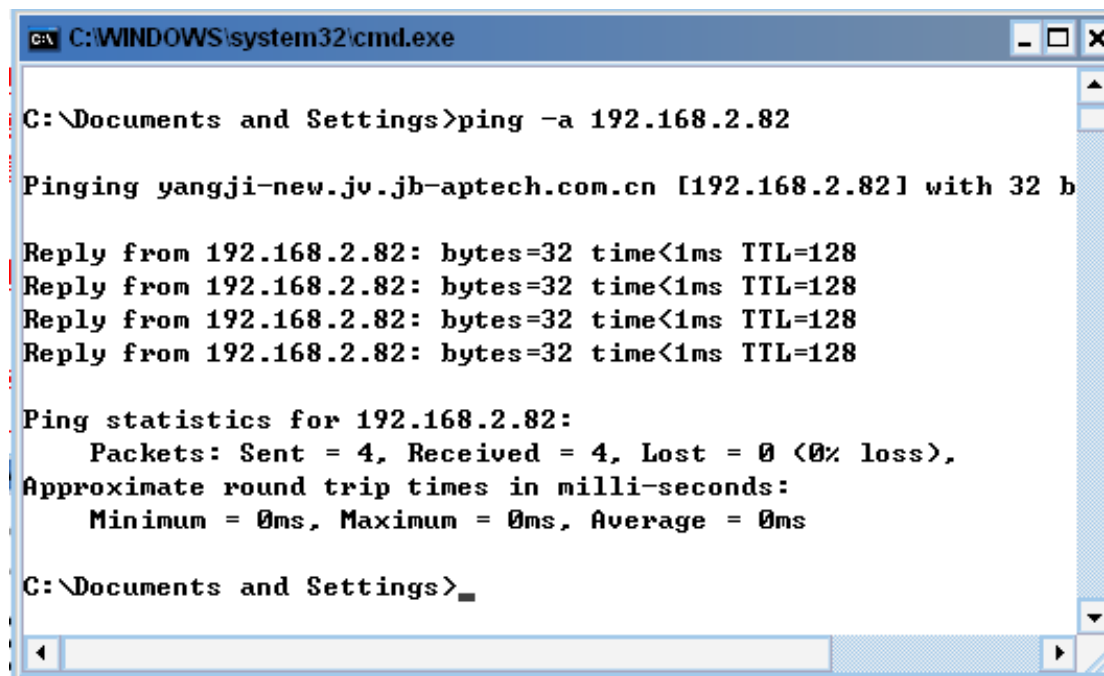
C:\Documents and Settings>ping 192.168.2.82 -t

Pinging 192.168.2.82 with 32 bytes of data:

Reply from 192.168.2.82: bytes=32 time=1ms TTL=128
Reply from 192.168.2.82: bytes=32 time<1ms TTL=128
Reply from 192.168.2.82: bytes=32 time<1ms TTL=128
Reply from 192.168.2.82: bytes=32 time<1ms TTL=128
Reply from 192.168.2.82: bytes=32 time<1ms TTL=128
Reply from 192.168.2.82: bytes=32 time<1ms TTL=128
Reply from 192.168.2.82: bytes=32 time<1ms TTL=128
Reply from 192.168.2.82: bytes=32 time<1ms TTL=128
Reply from 192.168.2.82: bytes=32 time<1ms TTL=128
Reply from 192.168.2.82: bytes=32 time<1ms TTL=128
Reply from 192.168.2.82: bytes=32 time<1ms TTL=128
Reply from 192.168.2.82: bytes=32 time<1ms TTL=128
```

## Ping命令的参数3—2

- -a : 显示对方的主机名



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

C:\Documents and Settings>ping -a 192.168.2.82

Pinging yangji-new.jv.jb-aptech.com.cn [192.168.2.82] with 32 b

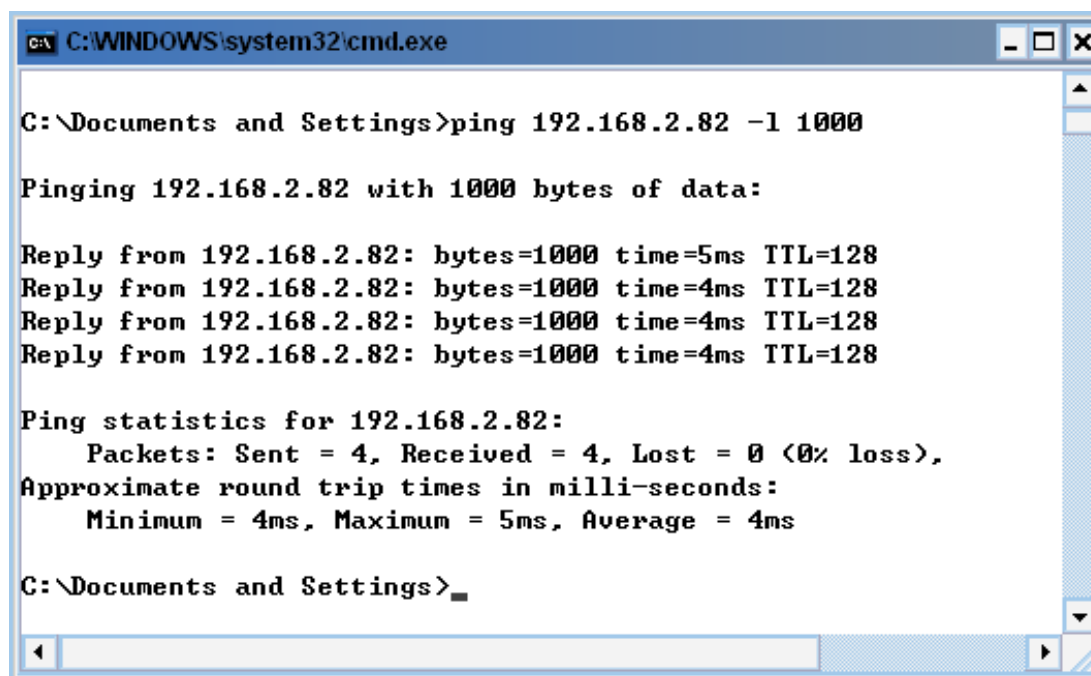
Reply from 192.168.2.82: bytes=32 time<1ms TTL=128
Reply from 192.168.2.82: bytes=32 time<1ms TTL=128
Reply from 192.168.2.82: bytes=32 time<1ms TTL=128
Reply from 192.168.2.82: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.2.82:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Documents and Settings>
```

## Ping命令的参数3—3

- -l 字节数: 发送指定大小的ping包



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

C:\Documents and Settings>ping 192.168.2.82 -l 1000

Pinging 192.168.2.82 with 1000 bytes of data:

Reply from 192.168.2.82: bytes=1000 time=5ms TTL=128
Reply from 192.168.2.82: bytes=1000 time=4ms TTL=128
Reply from 192.168.2.82: bytes=1000 time=4ms TTL=128
Reply from 192.168.2.82: bytes=1000 time=4ms TTL=128

Ping statistics for 192.168.2.82:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 4ms, Maximum = 5ms, Average = 4ms

C:\Documents and Settings>
```

- 中继器（集线器）
  - 中继器也叫转发器，属于物理层互联设备，可以将传送过来的二进制信号进行复制、整形、再生和转发（不做放大）。主要用于局域网传输距离的延伸，增加节点数，以及连接不同类型的网络（比如令牌环和以太网）。
  - 中继器物理上是星型拓扑，逻辑上是总线拓扑。
  - HUB是一个多端口的中继器。
- 网桥（交换机）
  - 网桥作用于物理层和数据链路层，用于网络中节点的物理地址过滤、网络分段以及跨网段数据帧的转发。它既可以延伸局域网的距离，扩充节点数，还可以将符合过重的网络划分为较小的网络，缩小冲突域。
  - 网桥起到隔离网段作用。但不能隔离广播，也不能控制广播风暴。
  - 交换机相当于很多个网桥的集合。
- 路由器
  - 路由器转发数据包时通过第三层（IP地址），以决定一个数据包如何重新包装及送到哪里。当它接收到数据包时，负责寻址，选择转发到下个节点的最佳路径。
  - 路由器丢弃所有的广播帧，所以可以抑制广播风暴。
- 网关
  - 网关也称网间协议转换器，具有高层协议的转换功能。网关通常是安装在路由器内部的软件，可以工作在 OSI 的所有七层中。安装了防火墙软件的计算机就是一种网关。

- 二层交换的作用及瓶颈
  - 交换机可以通过检查帧头的目标地址，将数据帧只转发到目标主机。
  - 在第二层采用交换技术提高了吞吐率，但大型扁平式的交换网络会有广播风暴、扩展树环路、网络间安全以及低效率的寻址问题。
- 三层交换机
  - 交换机和路由器相比，转发能力更强。但路由器又有交换机所没有的路由功能。因此，各个网络设备厂商推出了一个综合路由器和交换机功能的产品，即三层交换机，也称交换路由器或路由交换机。
  - 三层交换具有多伸缩性、流量管理和高性能等优点。
- 三层交换技术
  - 逐包转发交换
  - IP交换技术
  - **标记交换 ( MPLS )**
  - 基于路由的IP汇聚交换 ( ARIS )

专业测试保障卓越品质

The high quality derived from the professional testing

测试

传输层

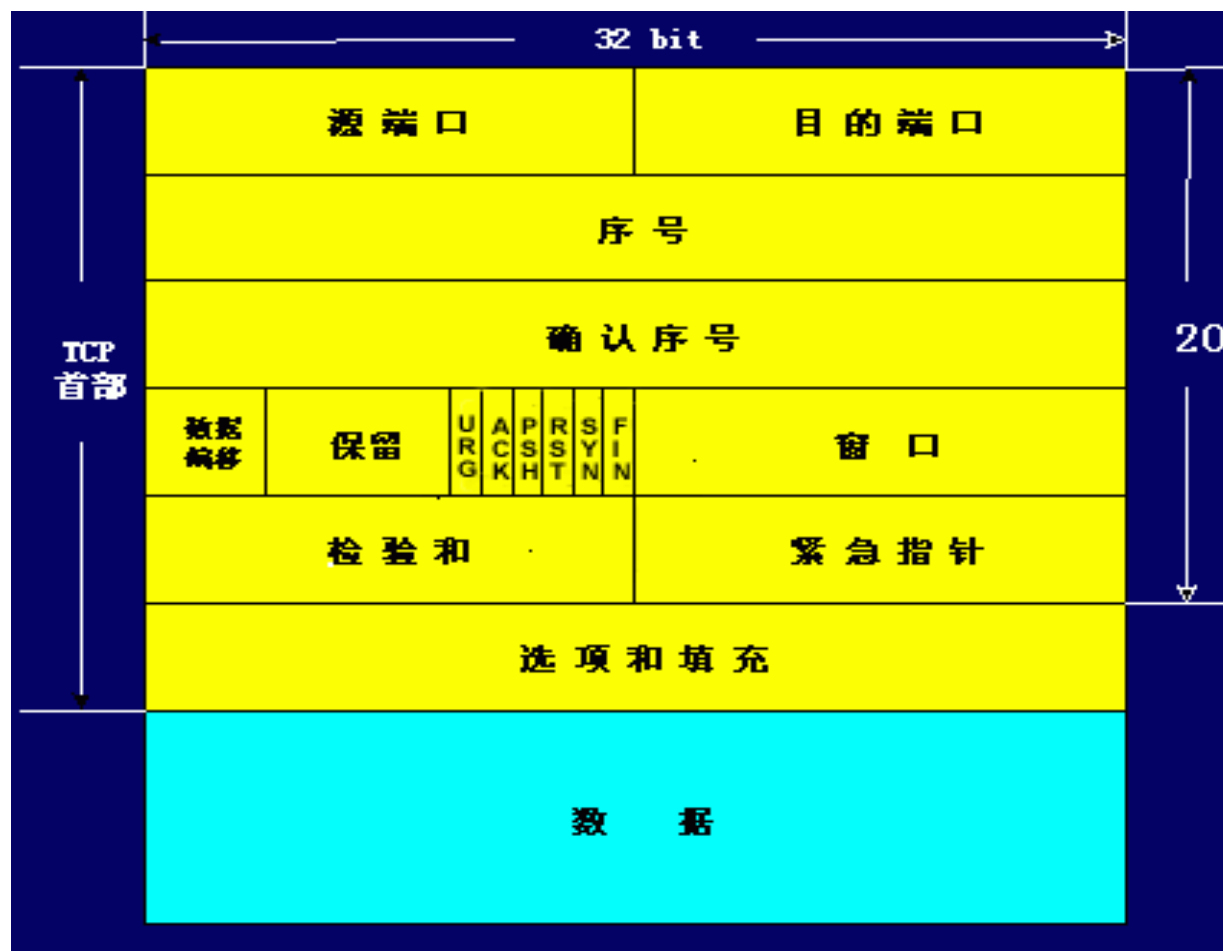
- 传输层提供的服务类似于数据链路层。区别是数据链路层控制局域网中单条链路上“**点到点**”传输的情形，而“**端到端**”是指从源端到目的端，中间可以一个或多个交换节点。
- 传输层的功能有下面几个：
  - 端到端的传递
  - 寻址（端口）
  - 可靠传递
  - 流量控制
  - 复用
  - 分段和重组

- 端到端的传递
  - 面向连接
    - 在源端和目的端之间建立一条虚电路
    - 面向连接有建立连接、数据传输和连接终止三个阶段
    - 典型协议：TCP（传输控制协议）
  - 面向无连接
    - 不提供顺序和流量控制
    - 典型协议：UDP（用户数据报协议）



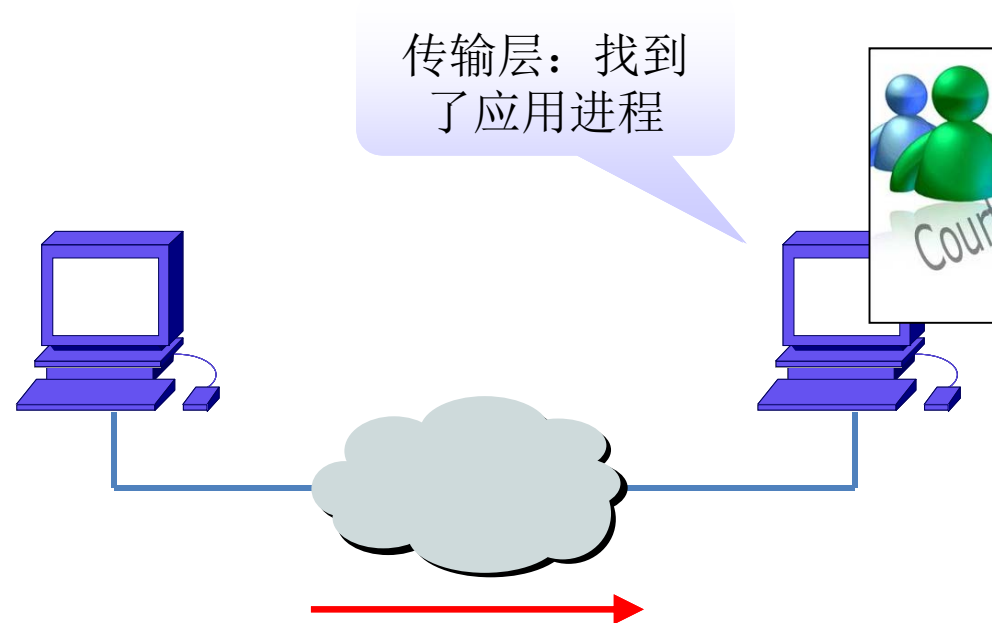
- IP是一个不可靠的面向无连接的协议，它不能确保数据报的正确传递。当需要可靠的端到端的传输服务时，可以使用TCP。而当需要提供较高数据传输速率时，可以使用UDP。
- TCP提供的服务
  - 面向连接
  - 点对点通信
  - 传输可靠性
  - 全双工通信
  - 流接口
  - 可靠的连接建立
  - 完美的连接终止

- TCP段的格式



- 端口号 ( Port )
  - 对于TCP或UDP的应用程序，都有标识该应用程序的端口号，即端口号用于区分各种应用。端口号的长度是16位，可提供65536（2的16次方）个不同的端口号。
  - 端口号1-255是公共端口，256-1024是用于Unix服务。
  - 端口号的另一种分配方法叫本地分配，使用1024以上的端口号。本地分配方式不受网络规模限制，但通信双方要预先知道。
- 套接字 ( Socket )
  - 计算机的IP地址加上TCP软件使用的端口号构成了套接字。套接字指向某一确定的程序的地址，通信时可根据套接字使一个进程和另一个进程对话。

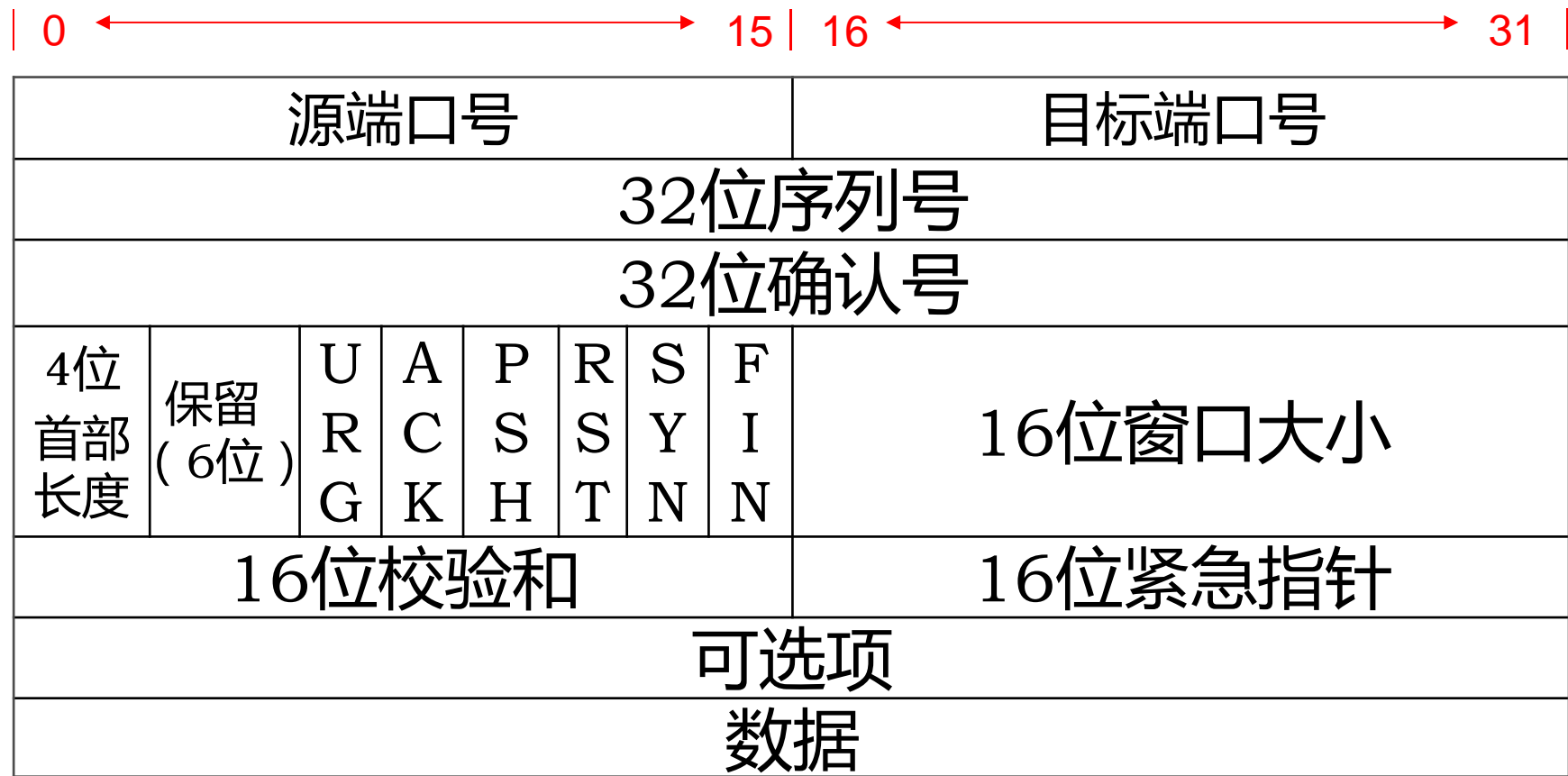
- IP层提供点到点的连接
- 传输层提供端到端的连接



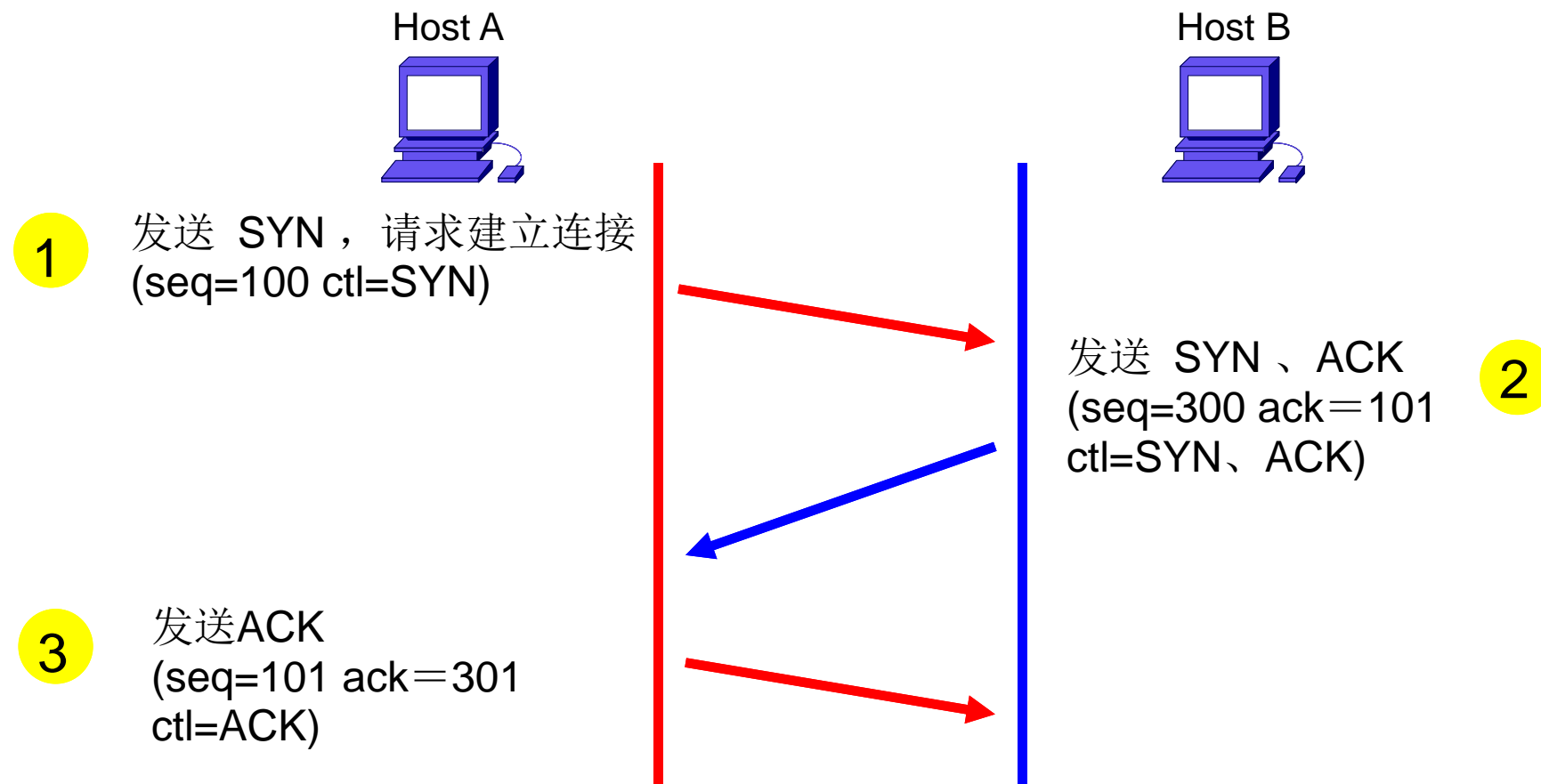
# 传输层的协议

- TCP（Transmission Control Protocol）
  - 传输控制协议
  - 可靠的、面向连接的协议
  - 传输效率低
- UDP（User Datagram Protocol）
  - 用户数据报协议
  - 不可靠的、无连接的服务
  - 传输效率高

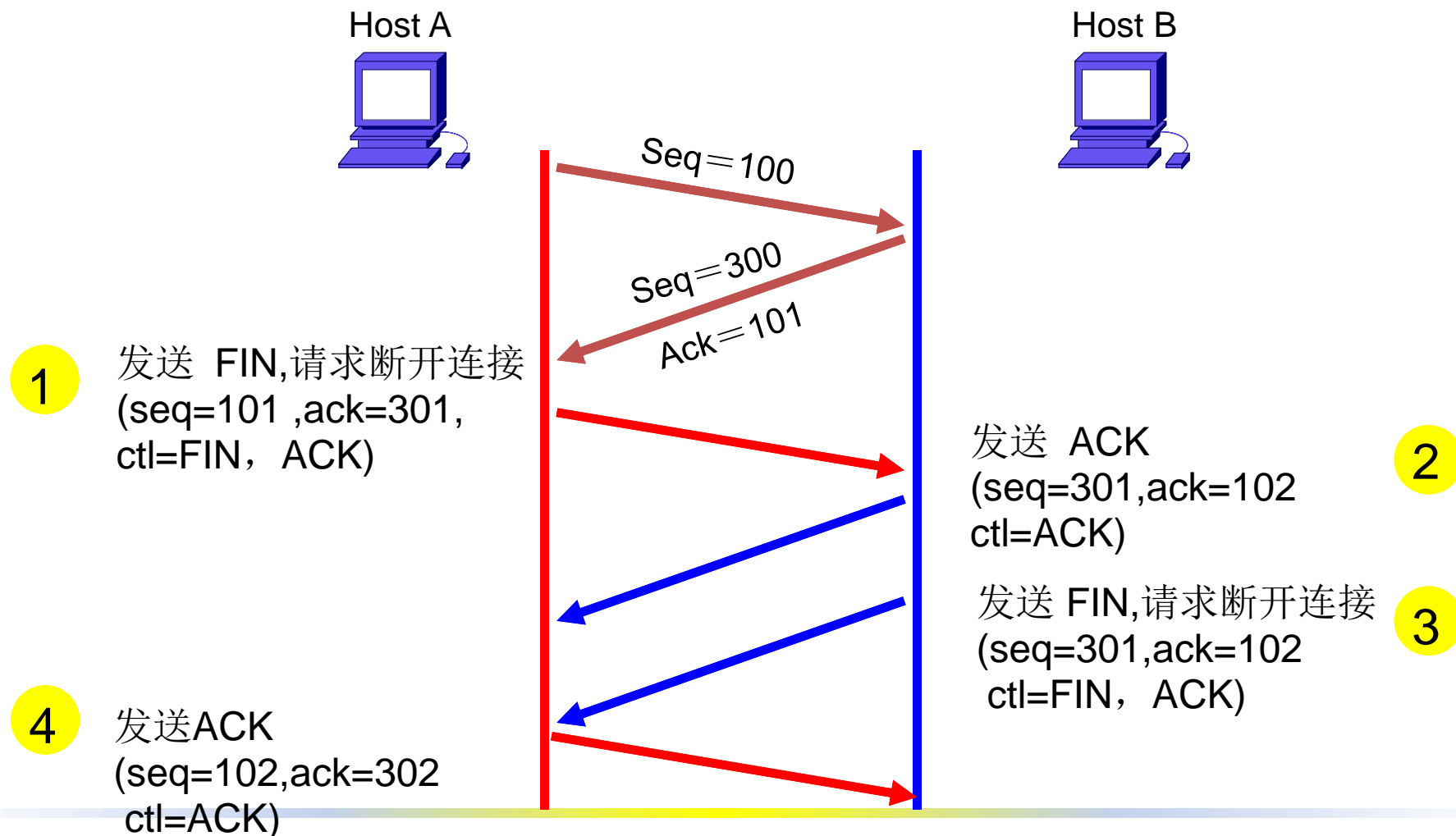
# TCP的封装格式



# TCP的连接—三次握手

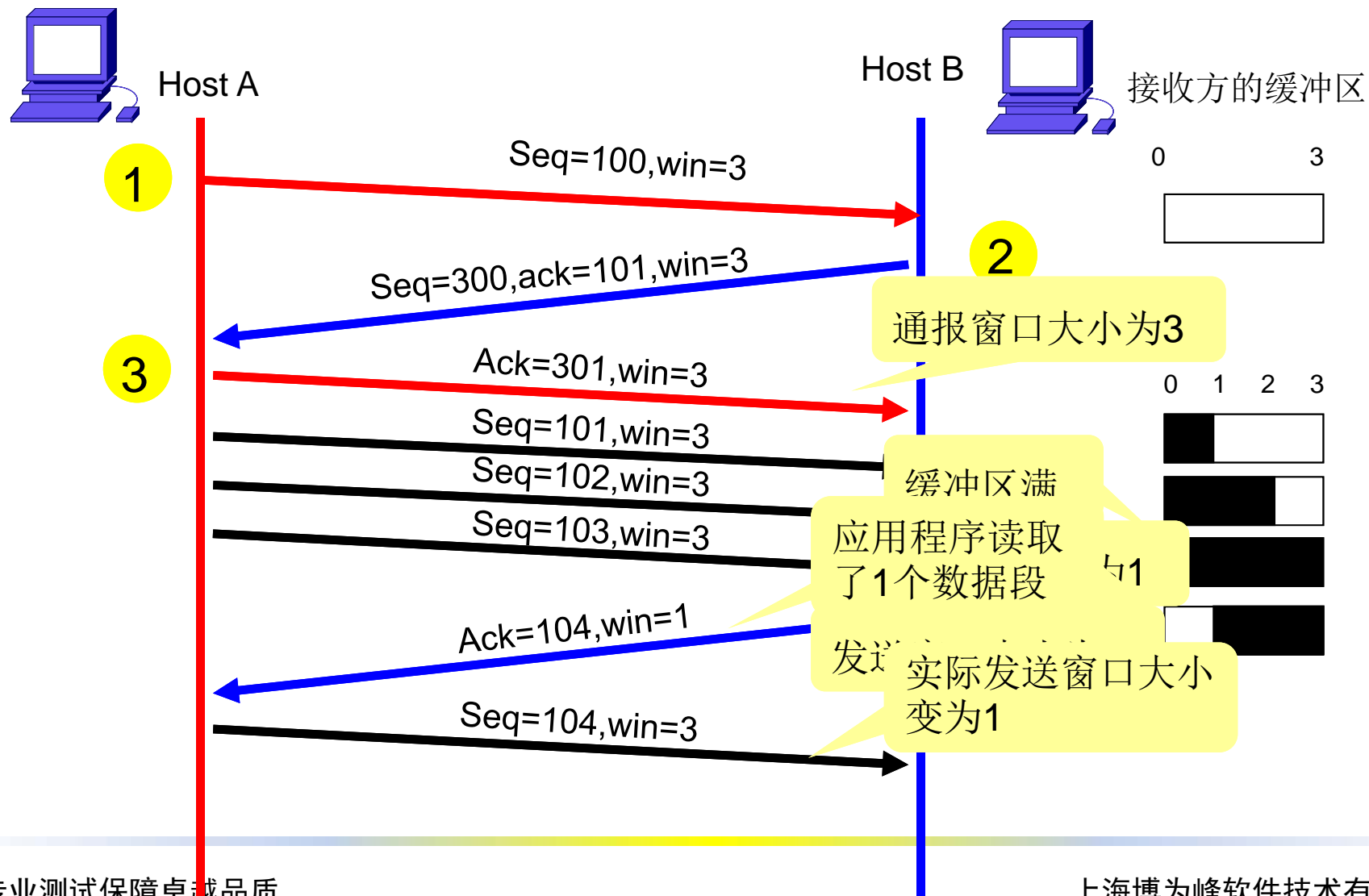


# TCP的四次断开

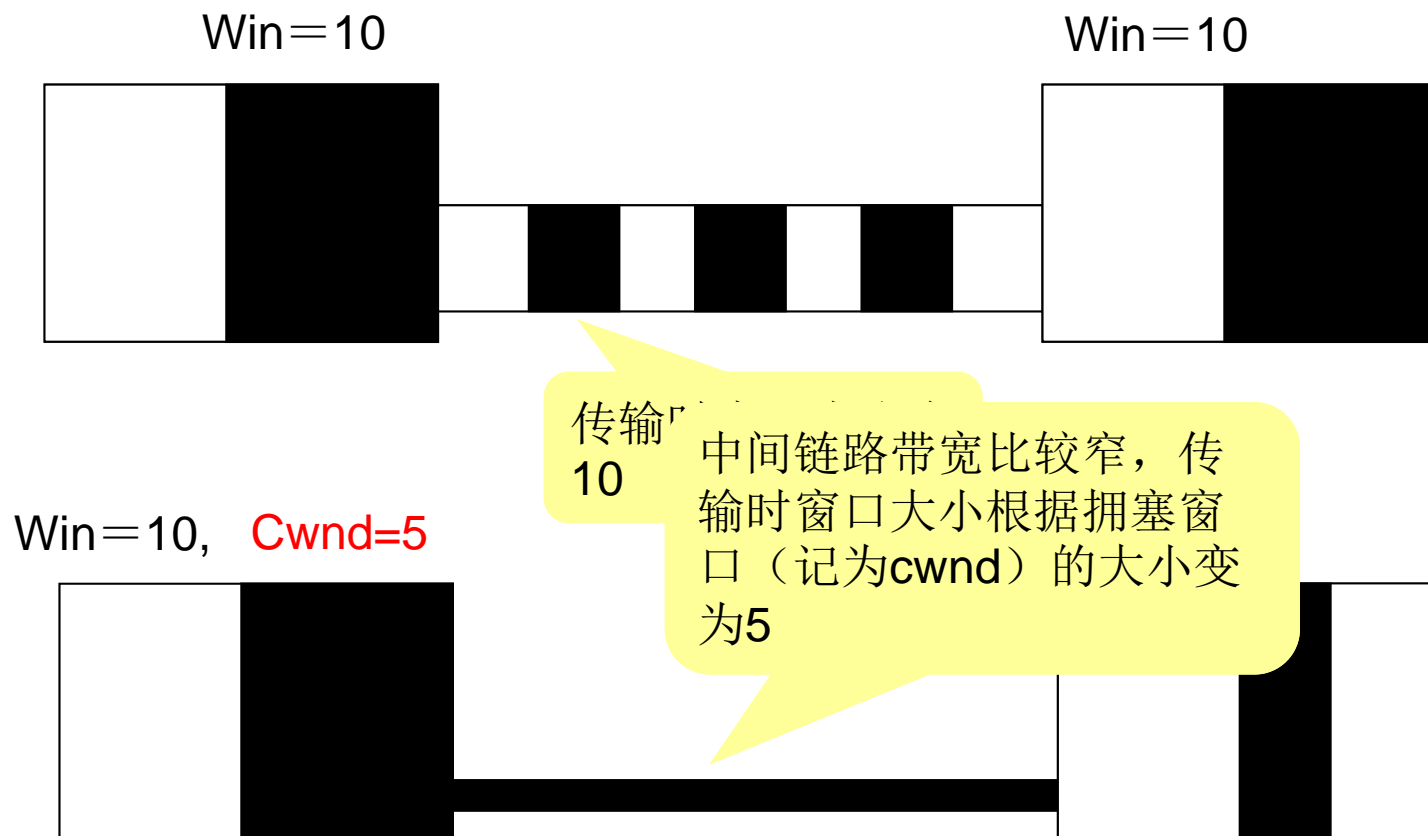




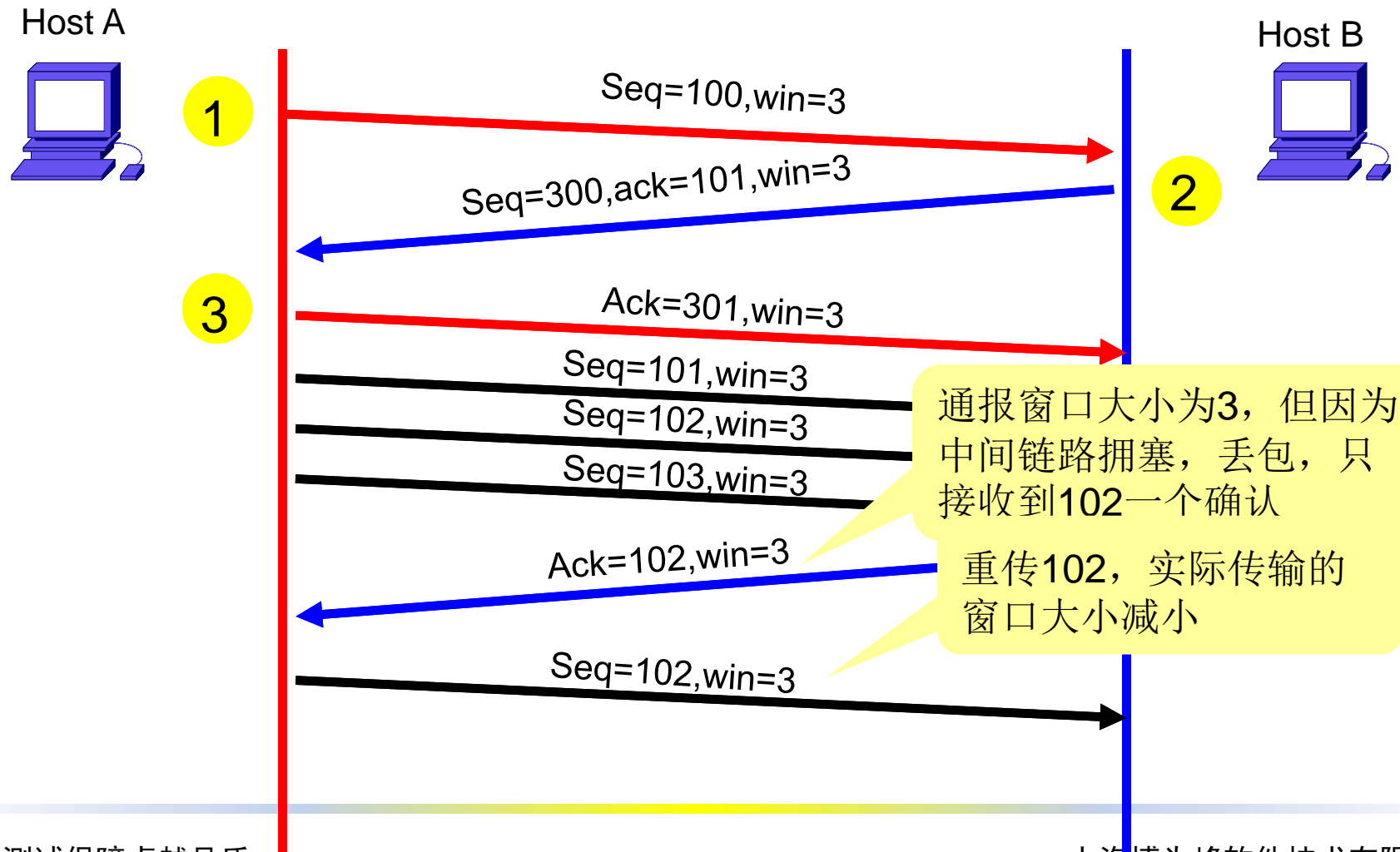
# TCP的流控机制—滑动窗口



## TCP的流控机制—拥塞控制2—1



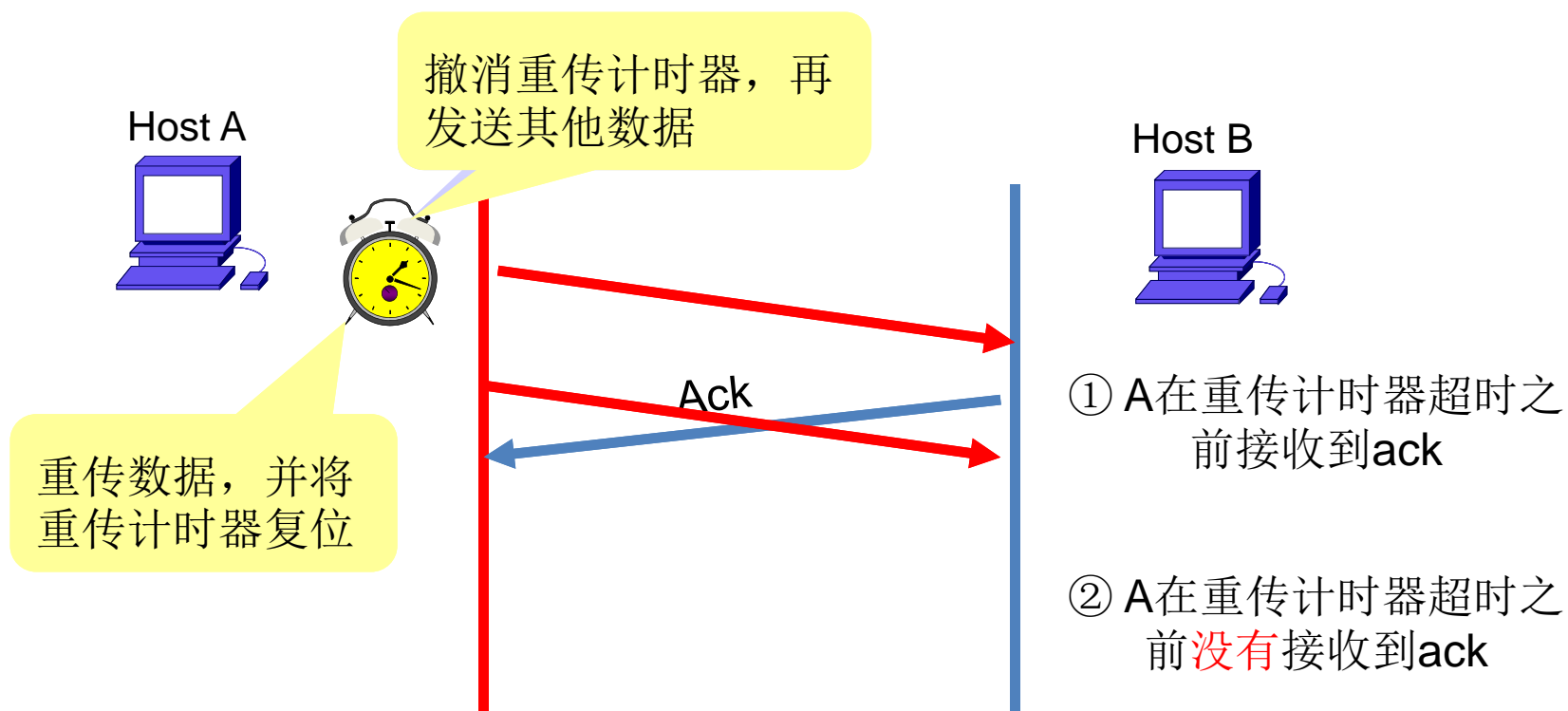
## TCP的流控机制—拥塞控制2—2



# TCP的差错控制

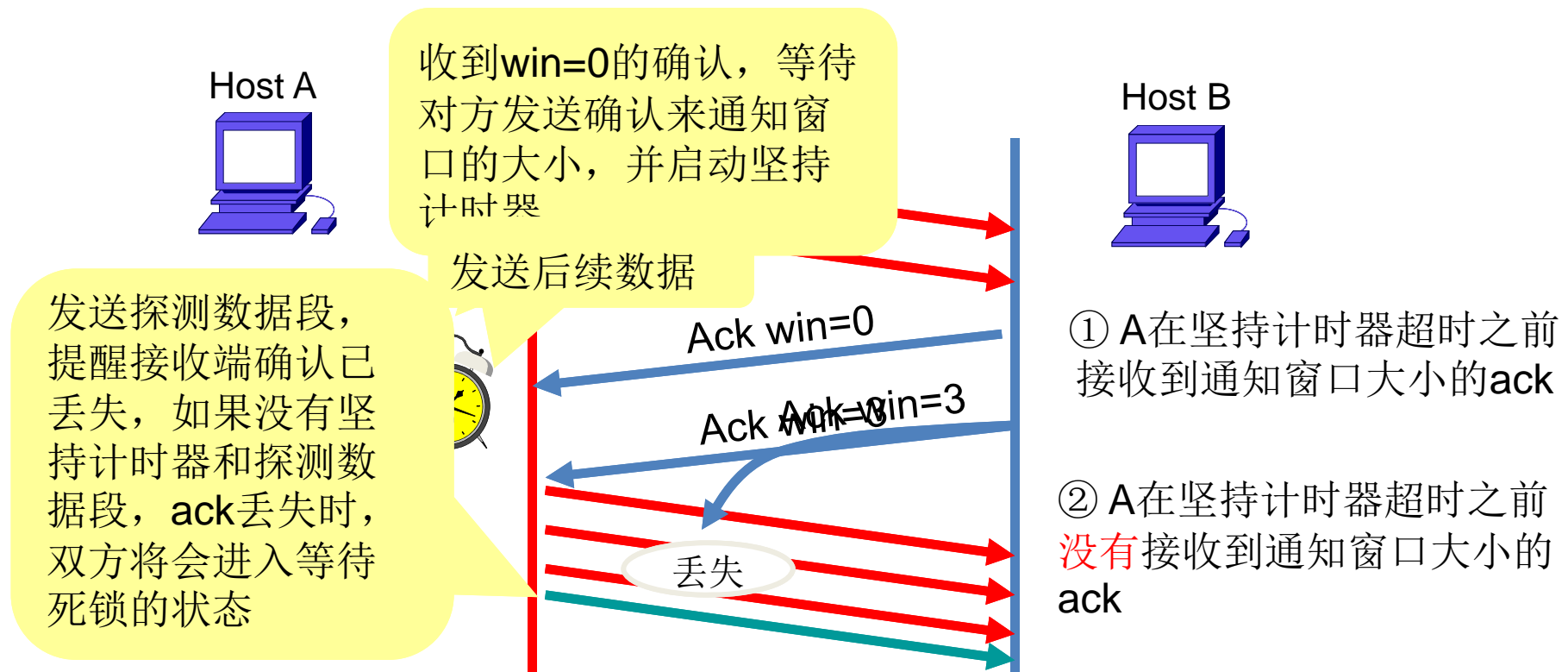
- TCP差错控制的3种方式
  - 校验和
  - 确认
    - 受损伤的数据段
    - 丢失的数据段
    - 重复的数据段
    - 失序的数据段
    - 确认的丢失
  - 超时

- 重传计时器—为了控制丢失的数据段



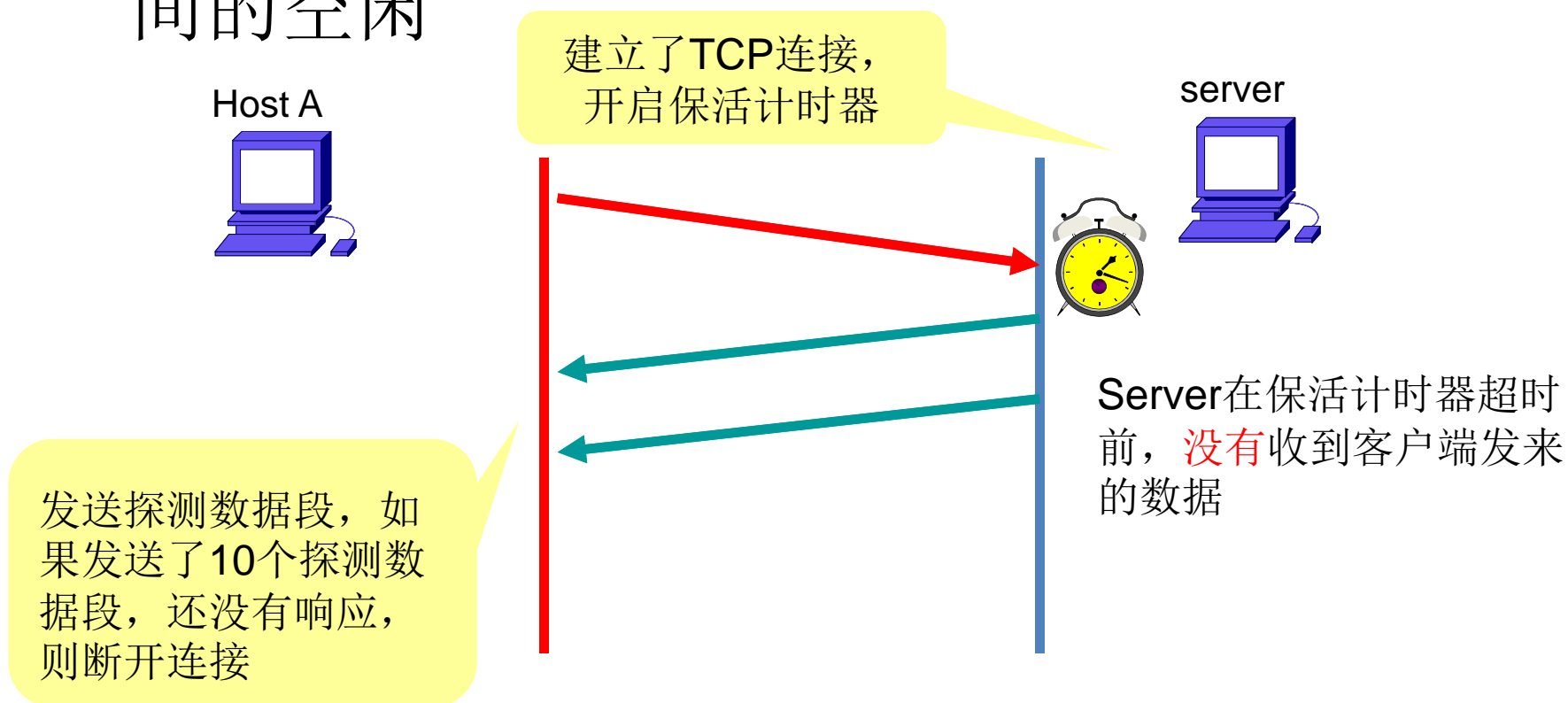
## TCP的计时器4—2

- 坚持计时器—为了防止零窗口死锁



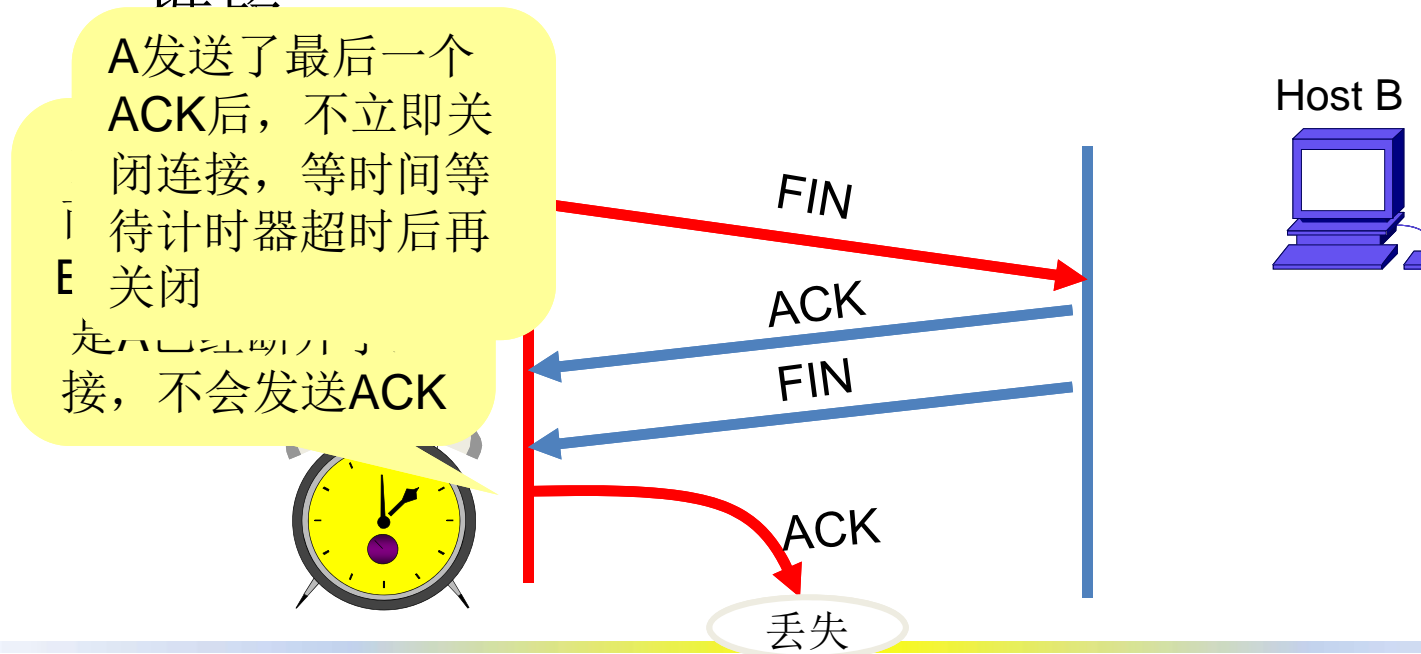
## TCP的计时器4—3

- 保活计时器—防止两个TCP之间的连接长时间的空闲



## TCP的计时器4—4

- 时间等待计时器—连接终止期间使用的
  - 在发送了最后一个ACK后，不立即关闭连接，而是等待一段时间，保证能接收到重复的FIN数据包

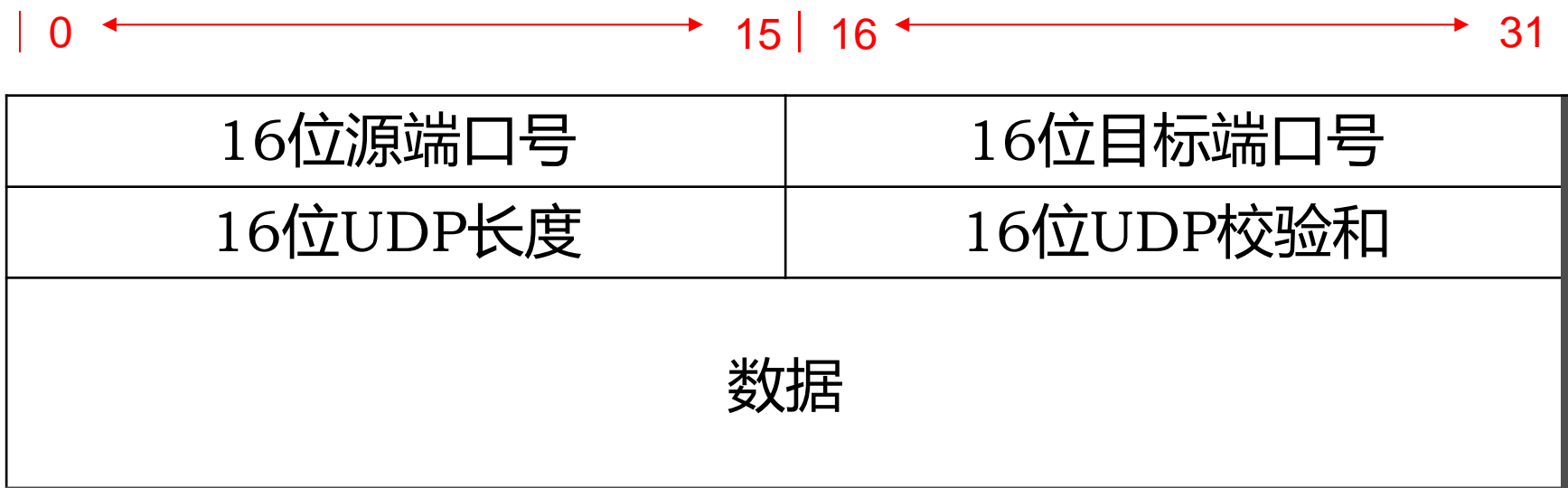




# TCP的应用

端口	协议	说明
21	FTP	文件传输协议，用于上传、下载
23	Telnet	用于远程登录，通过连接目标计算机的这一端口，得到验证后可以远程控制管理目标计算机
25	SMTP	简单邮件传输协议，用于发送邮件
53	DNS	域名服务，当用户输入网站的名称后，由DNS负责将它解析成IP地址，这个过程中用到的端口号是53
80	HTTP	超文本传输协议，通过HTTP实现网络上超文本的传输

# UDP的封装格式

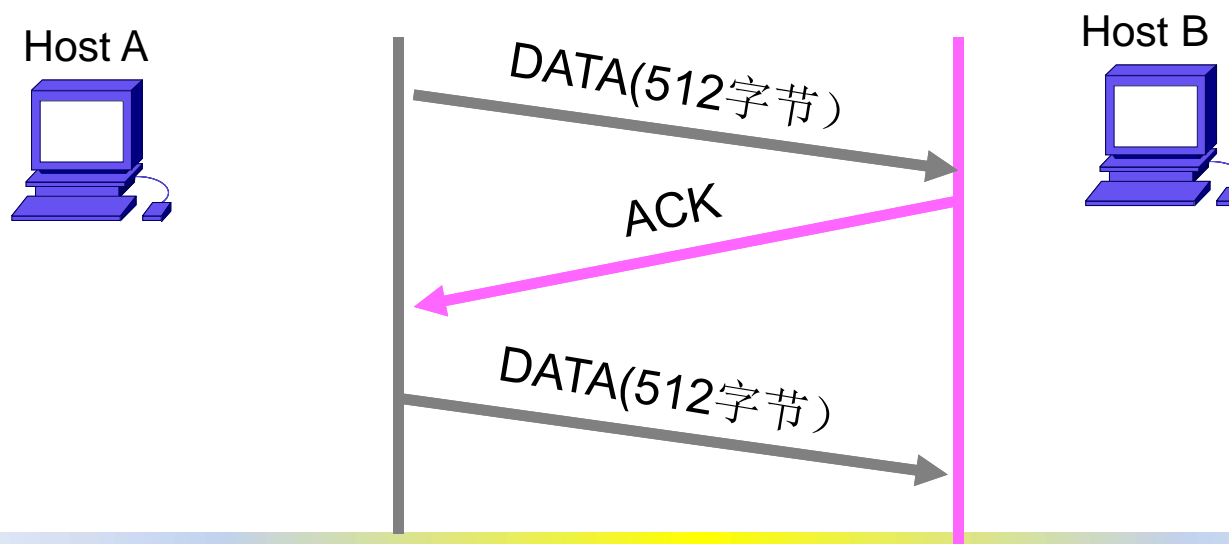


# UDP的使用

端口	协议	说明
69	TFTP	简单文件传输协议
53	DNS	域名服务
123	NTP	网络时间协议
111	RPC	远程过程调用

## UDP的流控和差错控制

- UDP没有流控机制
- UDP只有校验和来提供差错控制
  - 需要上层协议来提供差错控制：例如TFTP协议



专业测试保障卓越品质

The high quality derived from the professional testing

测试

会话层

- 会话层提供的服务：
  - 数据交换
  - 隔离服务
  - 与会话管理有关的服务
  - 会话层与传输层的交互
  - 同步点

专业测试保障卓越品质

The high quality derived from the professional testing

测试

表示层

- 表示层提供的服务：
  - 翻译
  - 数据加密
  - 认证
  - 数据压缩



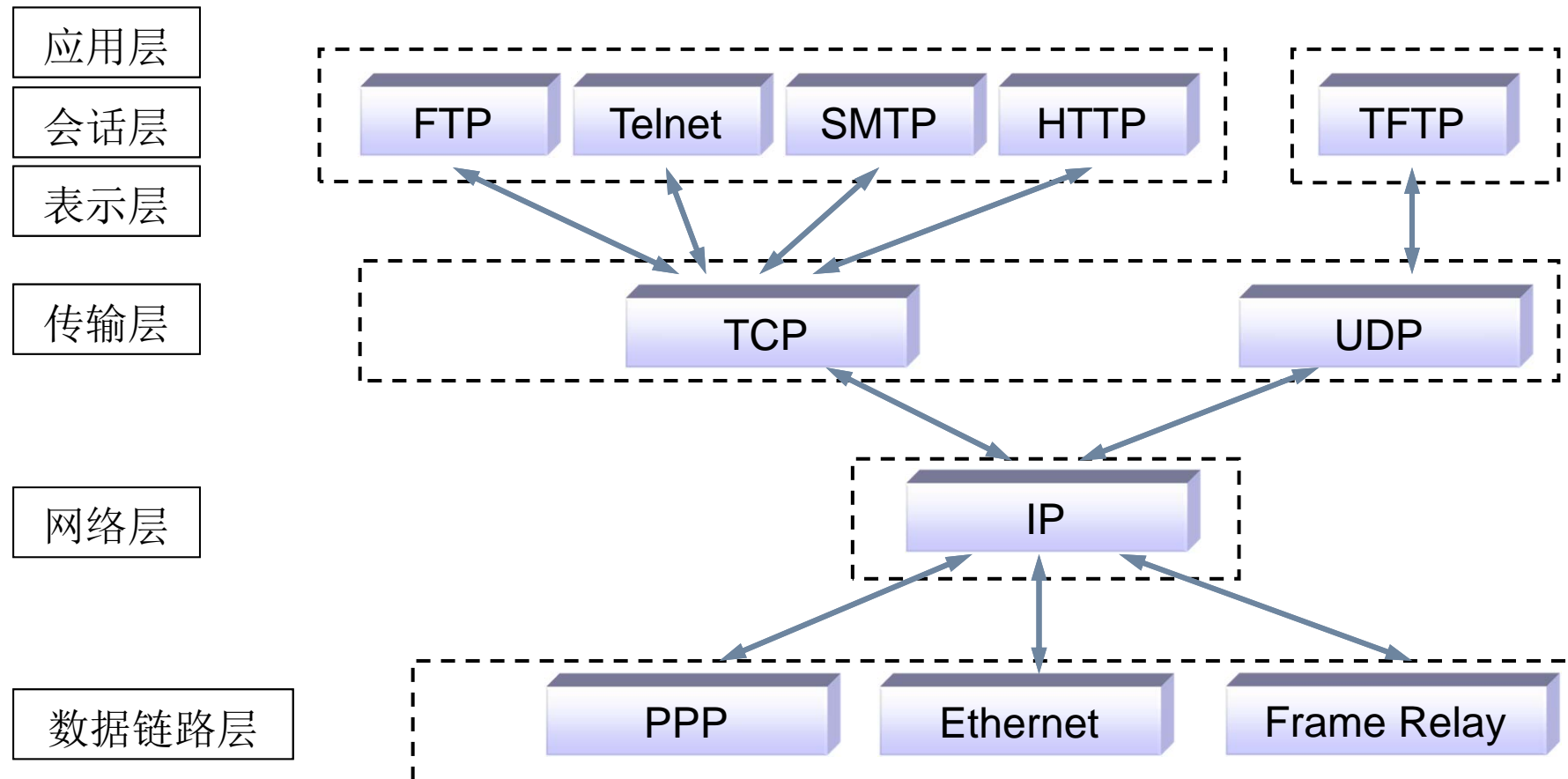
专业测试保障卓越品质

The high quality derived from the professional testing

测试

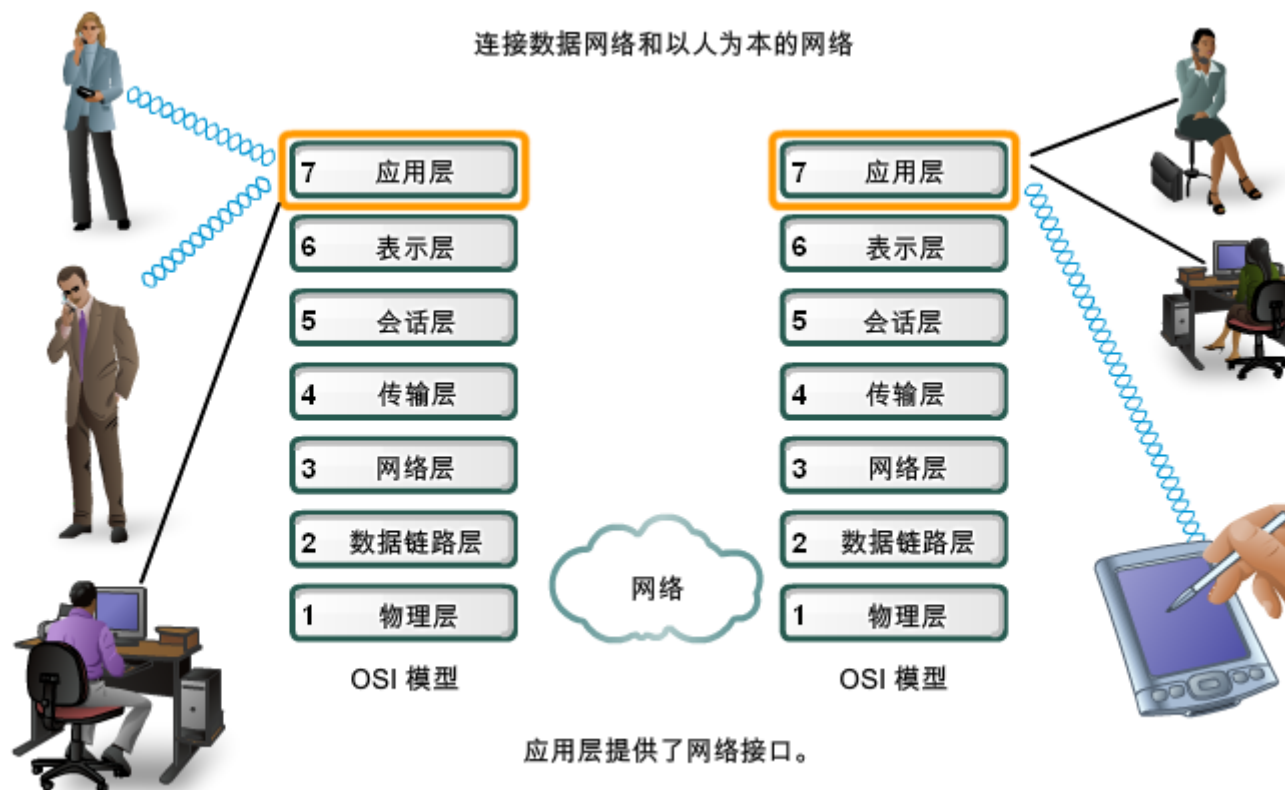
应用层

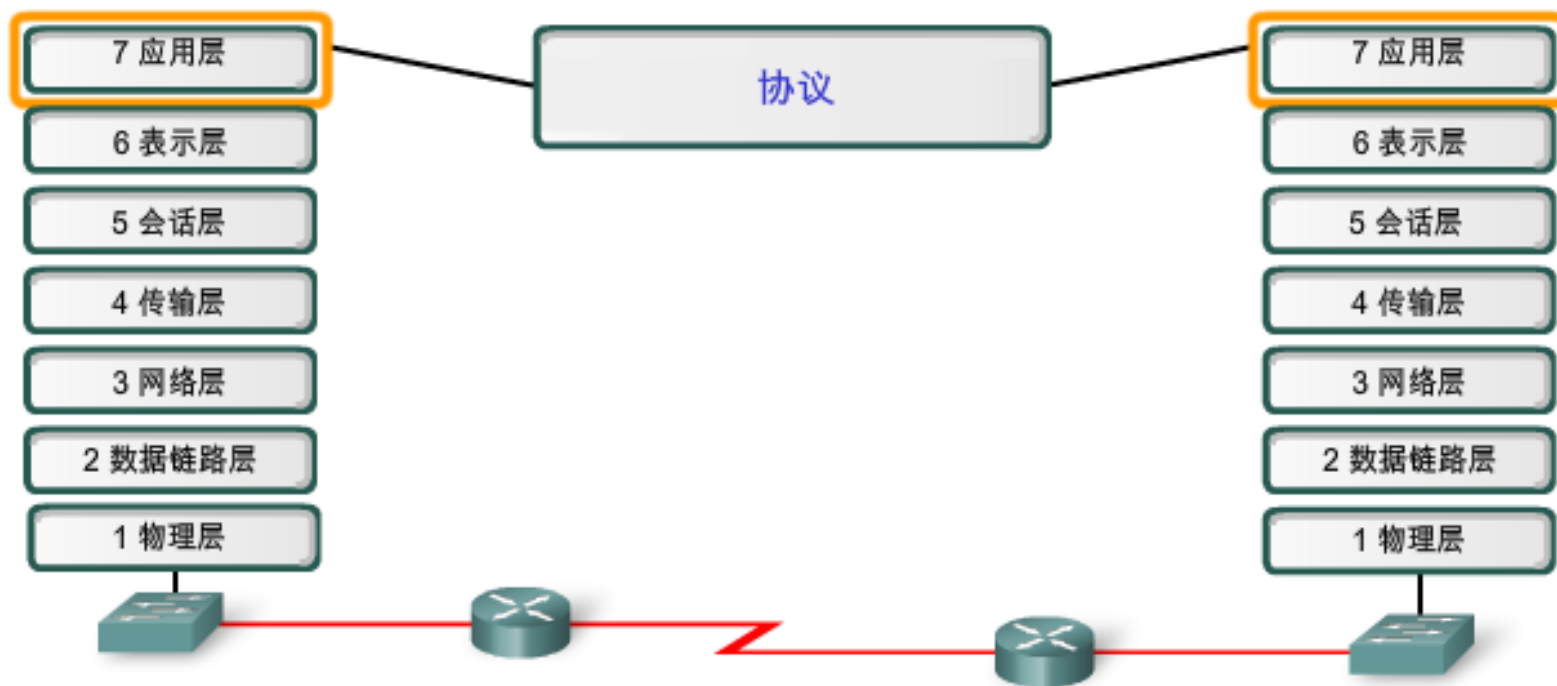
# TCP/IP协议栈



应用层服务启动数据传输过程。



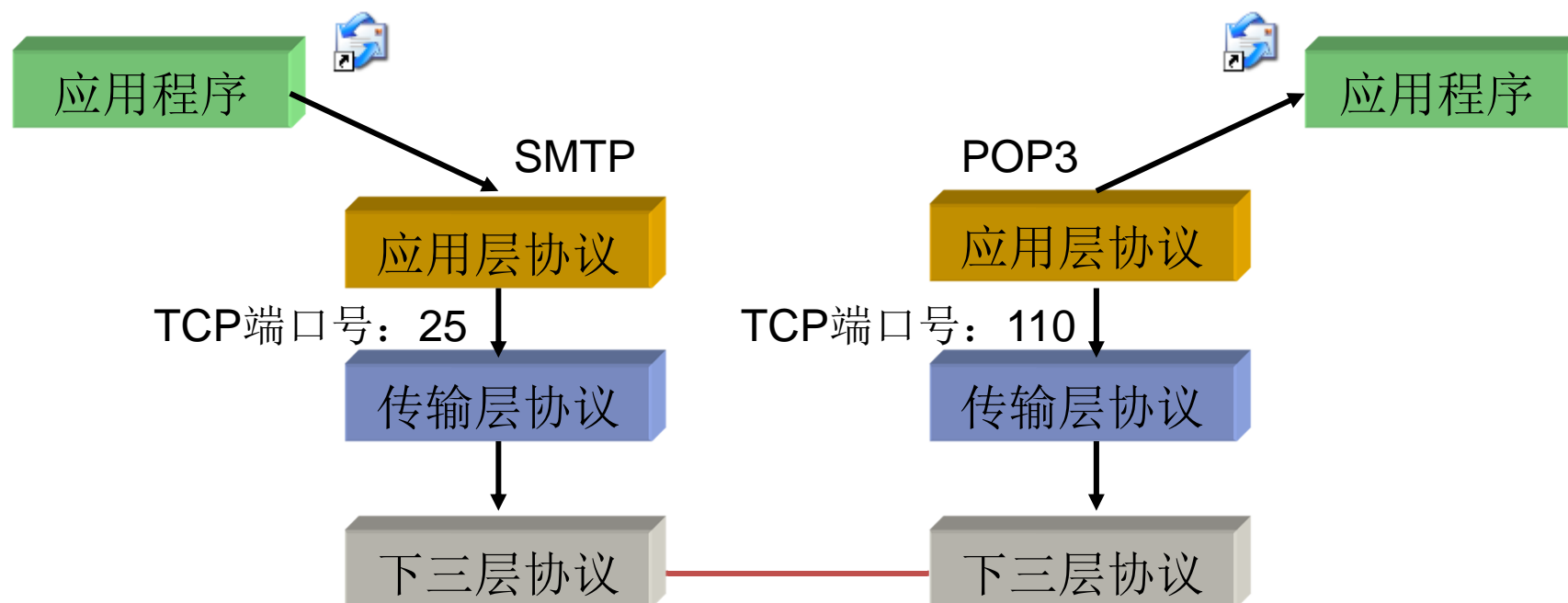




- TCP协议：
  - HTTP 80 超文本传输协议 ( www服务 )
  - HTTPS 443 安全的HTTP协议
  - FTP 21 文件传输协议
  - SMTP 25 简单邮件传输协议(发送邮件)
  - POP3 110 第三版邮局协议(接收邮件)
  - TELNET 23 远程登录协议
- UDP协议:
  - TFTP 69 简化的文件传输协议
  - DNS 53 域名解析协议
  - DHCP 67 动态主机配置协议
  - NTP 123 网络时间协议
  - SNMP 161 简单网络管理协议

## 应用层的功能

- 和应用程序协同工作，利用基础网络交换应用程序专用的数据



# 常用的应用层协议

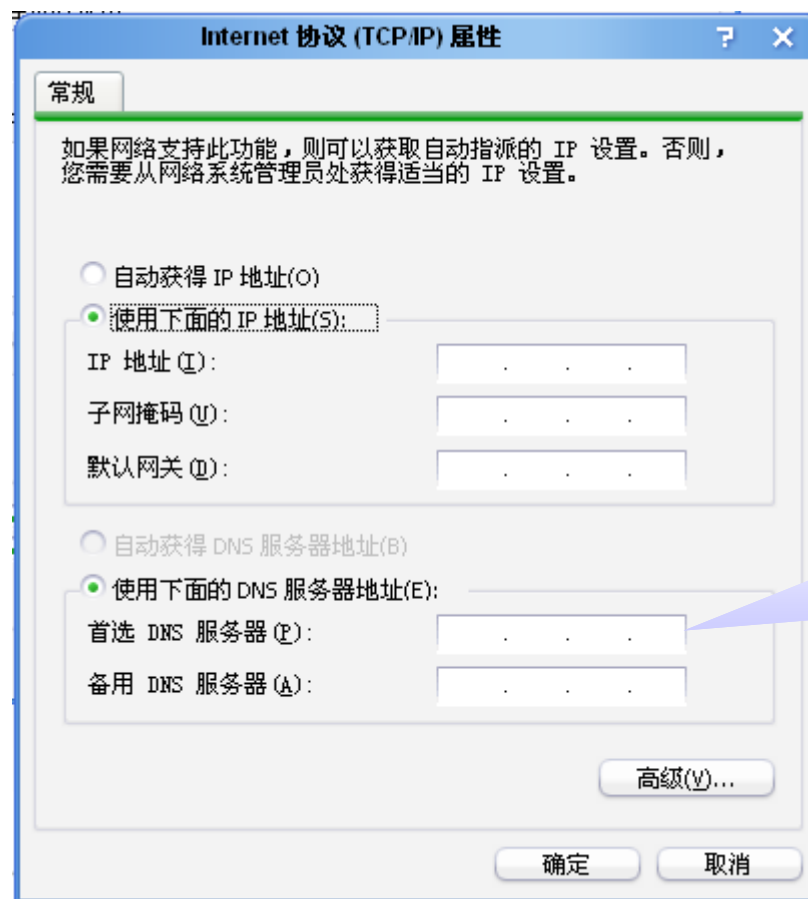
- DNS
- SMTP与POP3
- Telnet
- FTP
- HTTP



# DNS的功能

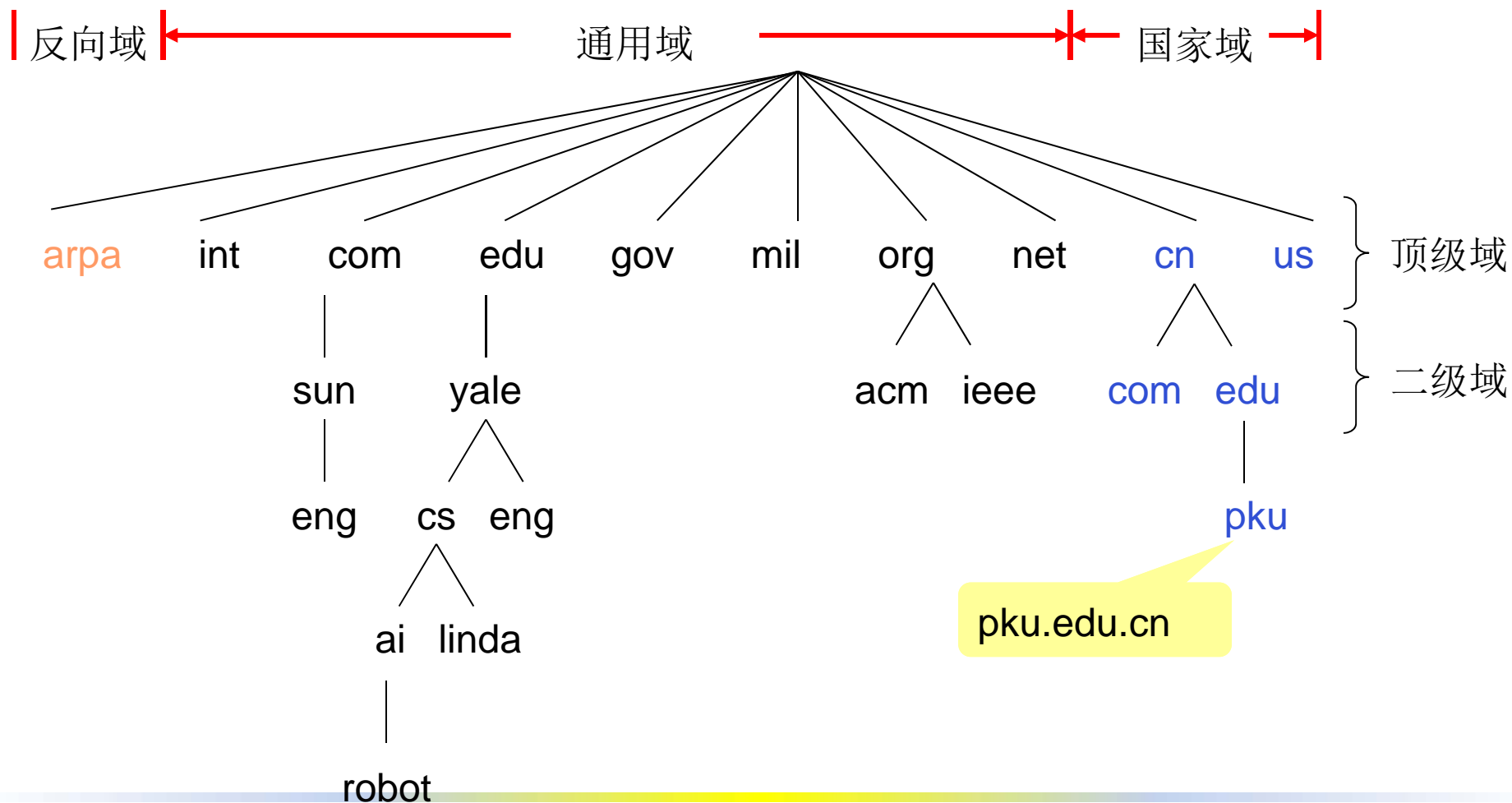
- DNS
  - Domain Name System 域名系统
  - 用来完成域名与IP地址之间的映射
  - 端口号为TCP或UDP的53

# DNS客户端的配置



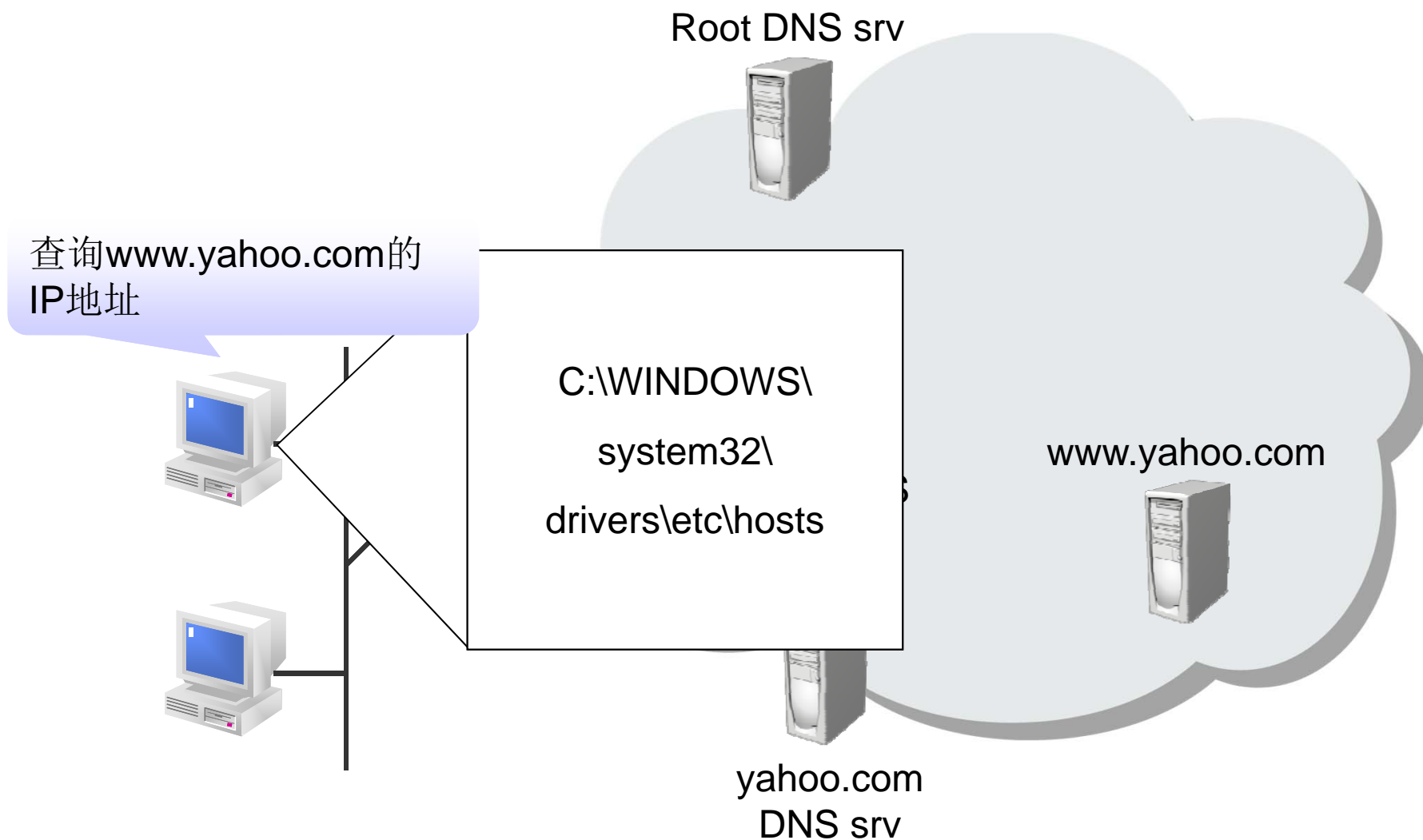
主机去查找的  
DNS服务器

# DNS名字空间



域	描述
Com	商业机构
Edu	教育机构
Gov	政府
Int	国际组织
Mil	美国军事网点
Net	网络
Org	其它组织机构

# DNS工作原理



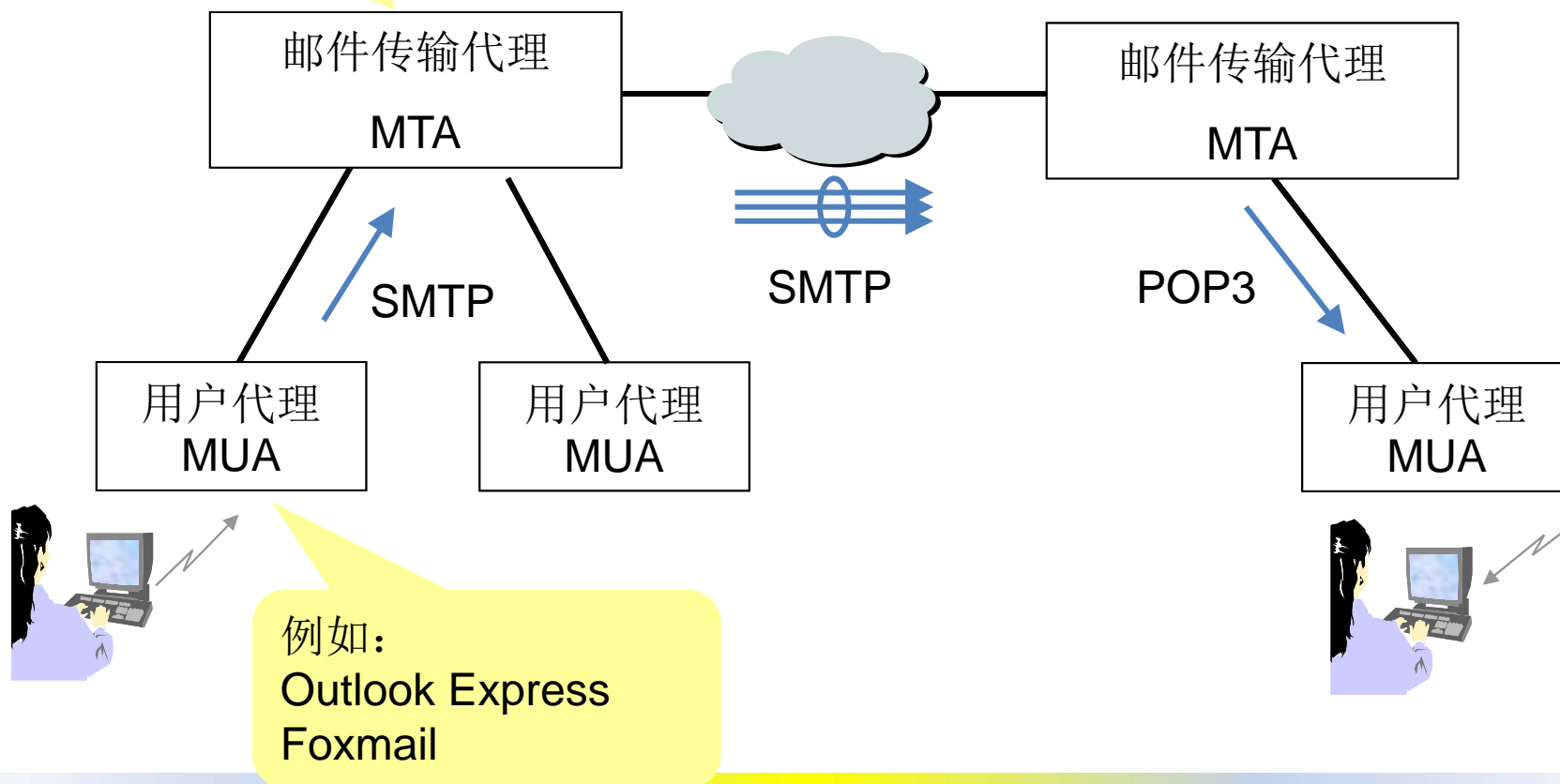


# SMTP与POP3

- SMTP
  - Simple Mail Transfer Protocol—简单邮件传输协议
  - 用于发送和接收邮件
  - 端口号25
- POP3
  - Post Office Protocol v3—邮局协议版本3
  - 用于客户端接收邮件
  - 端口号110

## 电子邮件的传输过程

例如：  
Exchange  
Sendmail





# Telnet

- Telnet
  - Terminal Network
  - 用于文本方式远程管理计算机或路由器等网络设备
  - 端口号为TCP的23

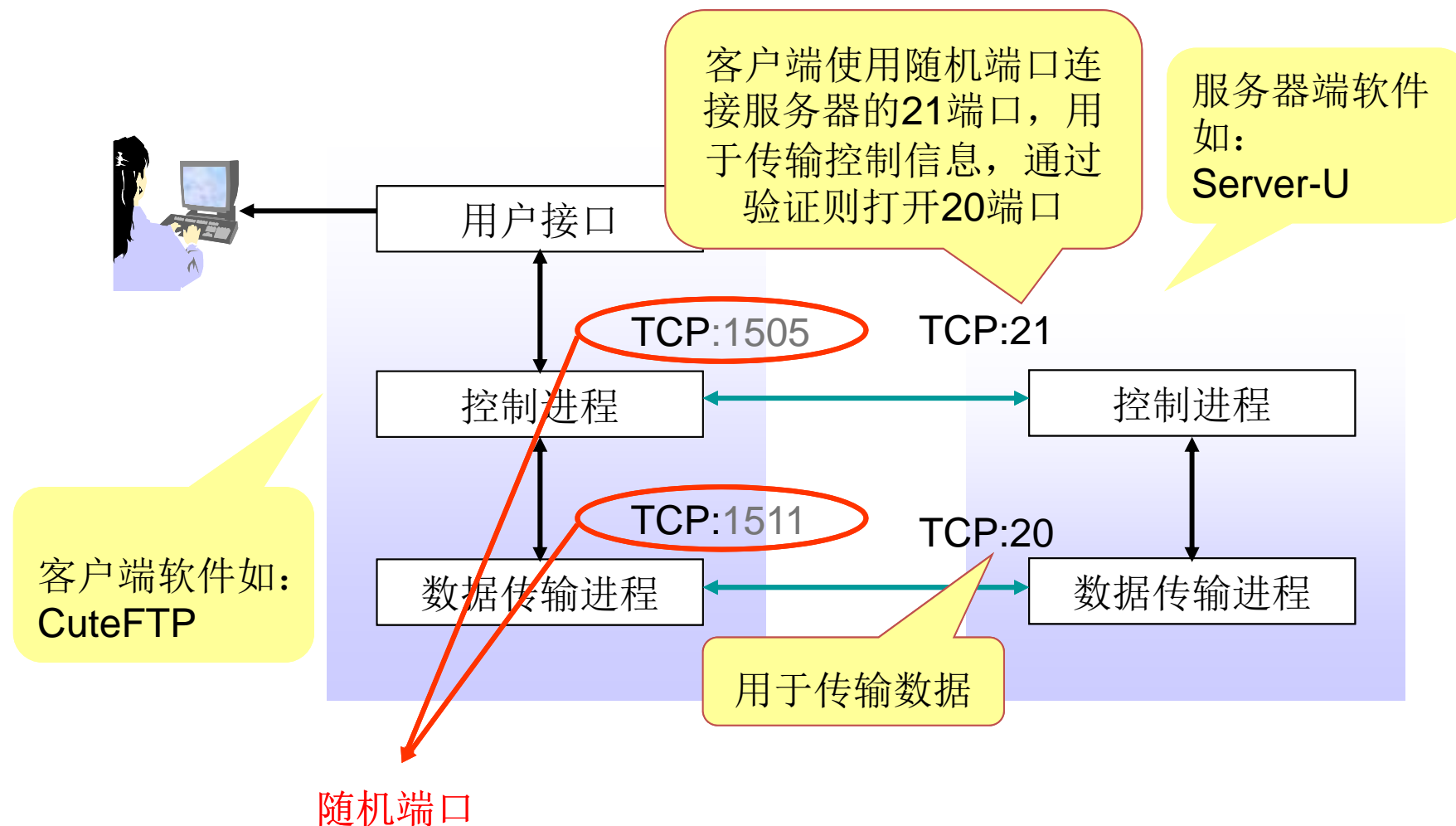
## Telnet的操作

- 在主机上操作  
开始—运行—cmd  
telnet 10.1.1.1

# FTP

- FTP
  - File Transfer Protocol-文件传输协议
  - 用于传输文件
  - 端口号为TCP的21和20

# FTP的工作原理

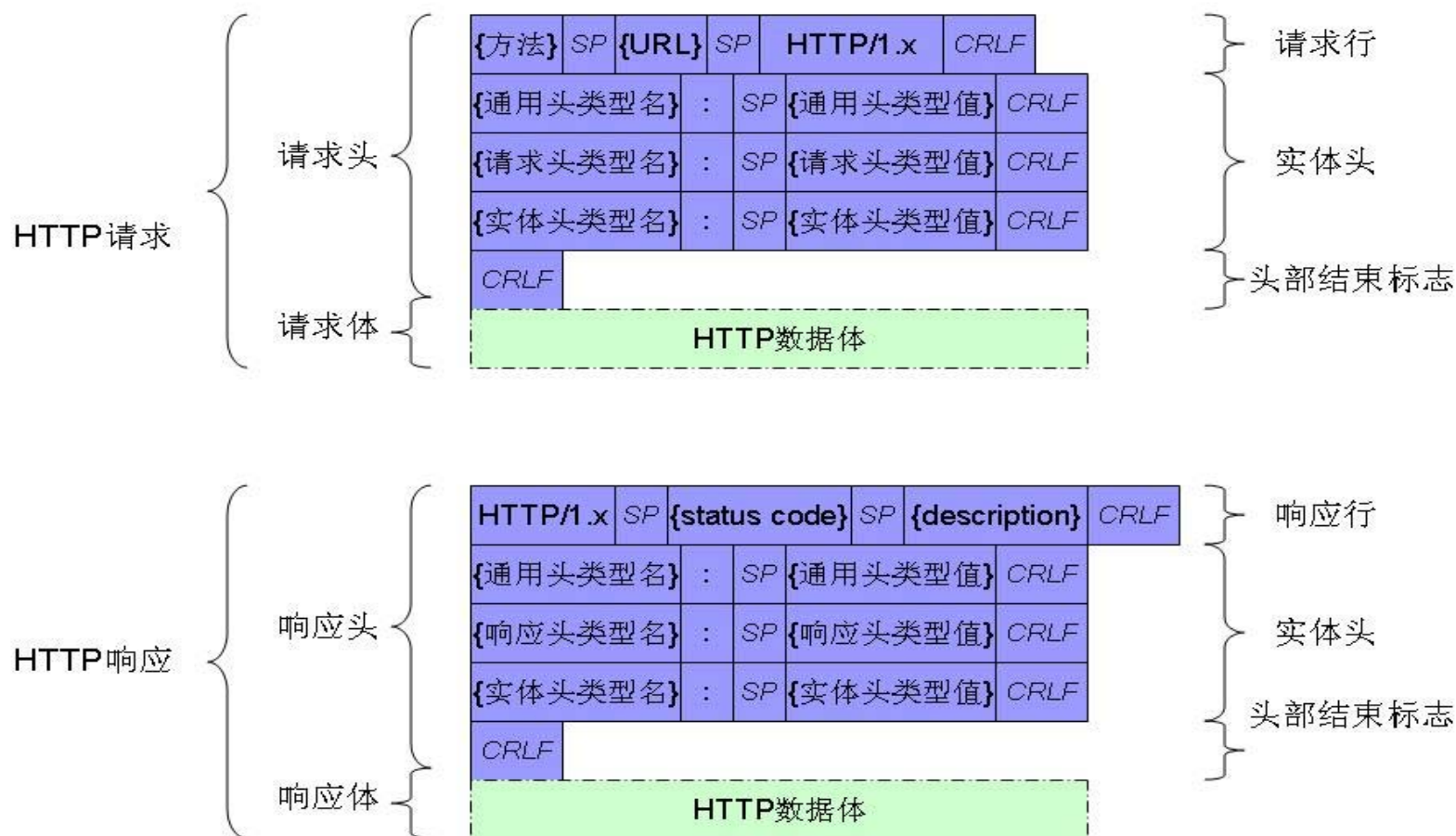


# HTTP

OSI中的层	功能	TCP/IP协议族
应用层	文件传输，电子邮件，文件服务，虚拟终端	DHCP · DNS · FTP · Gopher · HTTP · IMAP4 · IRC · NNTP · XMPP · POP3 · SIP · SMTP · SNMP · SSH · TELNET · RPC · RTCP · RTP · RTSP · SDP · SOAP · GTP · STUN · NTP · SSDP
表示层	数据格式化，代码转换，数据加密	没有协议
会话层	解除或建立与别的接点的联系	没有协议
传输层	提供 <u>端对端</u> 的接口	TCP · UDP · TLS · DCCP · SCTP · RSVP · PPTP
网络层	为 <u>数据包</u> 选择路由	IP (IPv4 · IPv6) · ICMP · ICMPv6 · IGMP · IS-IS · IPsec · BGP · RIP · OSPF · ARP · RARP
数据链路层	传输有地址的帧以及错误检测功能	Wi-Fi(IEEE 802.11) · WiMAX(IEEE 802.16) · ATM · DTM · 令牌环 · 以太网路 · FDDI · 帧中继 · GPRS · EVDO · HSPA · HDLC · PPP · L2TP · ISDN · STP
物理层	以二进制数据形式在物理媒体上传输数据	以太网路 · 调制解调器 · 电力线通信(PLC) · SONET/SDH · G.709 · 光导纤维 · 同轴电缆 · 双绞线

# HTTP协议结构

## HTTP协议——协议结构



# HTTP 协议举例

## HTTP协议——举例

浏览器请求

{  
GET /test.html HTTP/1.1  
Host: www.test.com

服务器响应

{  
HTTP/1.1 200 OK  
Content-Length: 38  
Content-Type: text/html  
Last-Modified: Fri, 20 Oct 2006 02:58:20 GMT  
Accept-Ranges: bytes  
ETag: "52bbd199f3f3c61:441"  
Server: Microsoft-IIS/6.0  
X-Powered-By: ASP.NET  
Date: Wed, 08 Nov 2006 06:28:59 GMT  
  
<HTML><BODY>hello world!</BODY></HTML>

