Computer Network

The Architecture of Computer Network

计算机网络概述

计算机网络概念

- 计算机网络由若干节点和连接这些节点的链路组成
- **互连网（internet）**：由多个计算机网络互连而成的计算机网络
- **互联网（Internet）**：专用名词，指当前全球最大的、开放的、由众多网络和路由器互连而成的特定计算机网络

计算机网络的组成

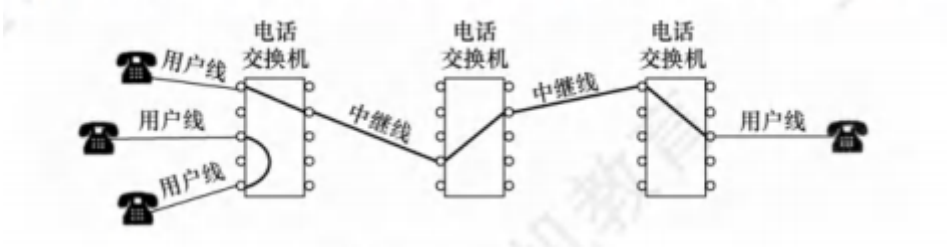
- 从**组成部分**看：计算机网络由**硬件、软件、协议**三大部分组成
- 从**工作方式**看：计算机网络由**边缘部分、核心部分**组成
- 从**功能组成**看：计算机网络由**通信子网、资源子网**组成

计算机网络的功能

- 数据通信
- 资源共享
- 分布式处理
- 提高可靠性
- 负载均衡

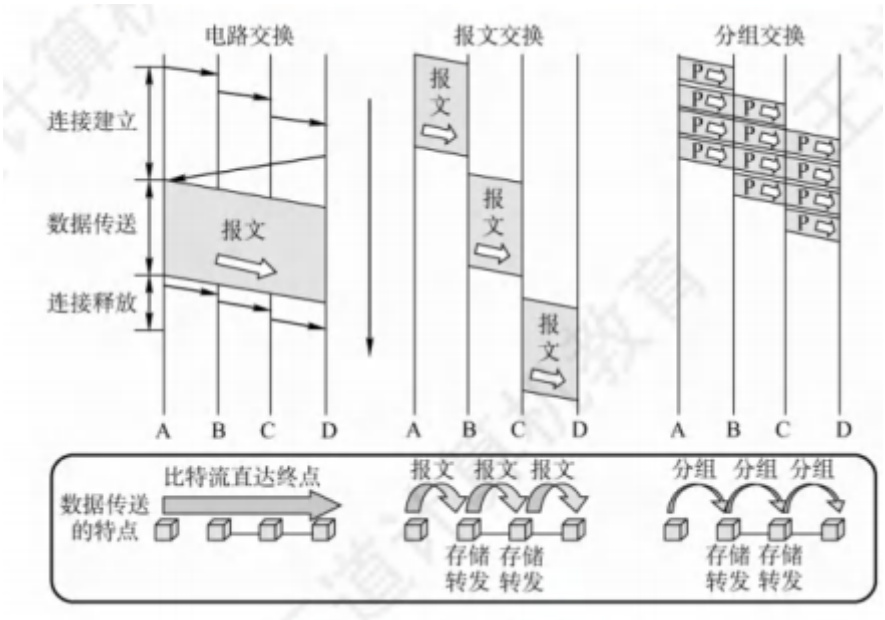
分组的转发

1. 电路交换
    - 电路交换分为三步：连接建立、数据传输和连接释放
    - 在进行数据传输前，两个结点之间必须先建立一条专用（双方独占）的物理通信路径
    - 在数据传输过程中， 这一物理通信路径始终被用户独占，直到通信结束后才被释放



- 优点：通信时延小、有序传输、没有冲突、适用范围广、实时性强、控制简单
- 缺点：建立连接时间长、线路利用率低、灵活性差、难以规格化、难以实现差错控制

2. 报文交换
   - 报文交换采用存储转发技术，整个报文先传送到相邻的结点，全部存储后查找转发表，转发到下 一个结点，如此重复，直至到达目的结点
   - 每个报文都可单独选择到达目的结点的路径
   - 优点：无需建立连接、动态分配线路、线路可靠性高、线路利用率高、提供多目标服务
   - 缺点：转发时延高、缓存开销大、错误处理低效
3. 分组交换
   - 比起报文交换直接将完整的报文转发给目的地，分组交换会将报文切分成多个更小的分组，这样处理后对于单个分组来说转发时延非常小，减小了出错概率和重发数据量



计算机网络的分类

1. 按分布范围分类
   - 广域网：几十到几千千米
   - 城域网：几到几十千米
   - 局域网：几十到几千米

    - 个人区域网：指在个人工作的地方将消费电子设备用无线技术连接起来的网络
2. 按传输技术分类
    - 广播式网络
    - 点对点网络
3. 按拓扑结构分类
    - 总线型
    - 星形
    - 环形
    - 网状
4. 按使用者分类
    - 公用网
    - 专用网
5. 按传输介质分类
    - 有线：双绞线、同轴电缆、光纤等
    - 无线：蓝牙、微波、无线电等

计算机网路的性能指标

- 速率
- 带宽
- 吞吐量
- 时延：发送时延（传输时延，指将分组推向链路所需的时间）、传播时延（电磁波在信道传播一定距离所需的时间）、处理时延、排队时延
- 往返时延（RTT）
- 信道利用率：**有数据通过时间 /（有 + 无）数据通过时间**

计算机网络体系结构参考模型

计算机网络分层模型

- SDU：服务数据单元，即为完成用户所要求的功能而传送的数据
- PCI：协议控制信息
- PDU：协议数据单元：对等层之间传送的数据单位
- **n-SDU + n-PCI = n-PDU = (n - 1)-SDU**

OSI 参考模型

1. 物理层：在物理介质上为数据端设备透明地传输原始比特流
2. 数据链路层：将网络层叫来的 IP 分组封装成帧，并可靠地传输到相邻节点的网络层。主要作用是加强物理层传输原始比特流的功能，将物理层提供的可能出错的物理连接改造为逻辑上无差错的数据链路，使之对网络层表现为一条无差错的链路
3. 网络层：将网络层的协议数据单元从源节点传输到目的节点，为分组交换网上的不同主机提供通信服务
4. 传输层：为端到端连接提供可靠的传输服务，为端到端连接提供流量控制、差错控制、服务质量、数据传输等管理服务
5. 会话层：允许不同主机上的各个进程之间进行会话
6. 表示层：协调不同信息表现形式，转换为标准编码
7. 应用层：用户与网络的接口

TCP/IP 模型

1. 物理层
2. 数据链路层
3. 网络层
4. 传输层
5. 应用层

Physical Layer

通信基础

基本概念

1. 数据、信号、码元
   - 数据：传输信息的实体
   - 信号：数据的电器或电磁表现
   - 码元：通信中数字信号的计量单位。在一个单位时间传输的的信号成为 k 进制码元。如果使用二进制编码，就只有 0 和 1 两种状态，属于数字脉冲信号的广义上的概念。
2. 信源、信道、信宿
   - 信源：产生和发送数据的源头
   - 信宿：接受数据的终点

    - 信道：信号的传输介质
3. 速率、波特、带宽
    - 速率：数据传输速率，单位是波特
    - 波特：1 波特表示通信系统每秒传输 1 个码元
    - 带宽：表示网络的通信线路所能传输数据的能力，即最高数据率

信道的极限容量

1. 奈奎斯特定理
    - **码元传输的速率最大不能超过信道频率带宽的 2 倍**
    - 设 W 为信道的频率带宽，V 为每个码元的离散电平数目，**理想低通信道下的极限数据传输速率 = 2WlogV**
2. 香农定理
    - 实际的信道会有噪声，所以奈奎斯特定理没有太大的实用性
    - 当带宽受限且有高斯噪声干扰时，**极限数据传输速率 = Wlog(1 + S/N)**
    - 其中， **S/N** 为信噪比

编码与调制

- **曼彻斯特编码**：每个码元的中间都发生电平跳变，其中向上跳变表示 0，向下跳变表示 1
- **差分曼彻斯特编码**：拥有更强的抗干扰能力。中间仍然跳变，但是时钟的下一时刻到来时，不跳变表示 1，否则为 0

传输介质

i. 双绞线：最常用的传输介质，通信距离一般为几千米到数十千米

ii. 同轴电缆：具有良好的抗干扰特性，可以用于传输较高速率的数据

iii. 光纤：利用光的全反射特性，进行通信，带宽极大。其中单模光纤适合长距离传输，多模光纤适合短距离传输

iv. 无线传输介质：主要有无线电波、微波等

物理层设备

i. 中继器

- 主要功能：整形、放大、转发信号，以消除信号经过一长段电缆后产生的失真和衰减，是信号的波形和强度达到所需的要求，进而扩大网络传输的距离

ii. 集线器（Hub）

- 实际上是一个多端口的中继器，当 Hub 工作时，一个端口接收到信号后，因为信号在从端口到 Hub 的传输过程中已有衰减，所以 Hub 便对该信号进行整形放大，直至再生到发送时的状态，并转发到其他所有处于工作状态的端口
- 只能在半双工的状态下进行工作

Data Link Layer

数据链路层的功能

数据链路层涉及三个基本问题：封装成帧、透明传输、差错检测

数据链路层所处的地位

- 链路：指从一个节点到相邻节点的一段物理线路
- 数据链路：将实现协议的硬件和软件加到链路上就构成了数据链路
- 帧：数据链路层对等实体之间进行逻辑通信的协议数据单元

为网络层提供服务

1. 无确认的无连接服务：源主机发送帧时不需要建立链路连接，目的主机收到帧时不需要发回确认。数据传输的可靠性由高层负责
2. 有确认的无连接服务：目的主机收到帧时需要进行确认
3. 有确认的面向连接服务：帧传输过程分为三个阶段：建立链路、传输帧、释放链路

链路管理

- 数据链路层连接的建立、维持和释放过程称为链路管理，它主要用于面向连接的服务
- 链路两端的结点要进行通信，必须首先确认对方已处于就绪状态，并交换一些必要的信息以对帧序号初始化
- 在传输过程中要能维持连接，而在传输完毕后要释放该连接

封装成帧和透明传输

- **封装成帧**：在一段数据的前后分别添加首部和尾部构成帧
- **透明传输**：指不论所传的数据是怎样的比特组合，都能够按原样无差错地在这个数据链路上传输

流量控制

- 限制发送方的发送速率，是指不超过接收方的接受能力

差错检测

- 帧在传输过程中发生的错误主要可分为帧错和位错
- **帧错**：帧丢失、重复或失序
- **位错**：帧中某些位出现差错

组帧

字符计数法

- 用一个计数字段记录该帧所含的字节数
- 但是如果这个字段发生了错误将会导致灾难性后果

字节填充法

- 使用特定字节来定界一帧的开始与结束
- 为了保持原文本的表达能力，允许转义字符的功能

零比特填充法

- 允许数据帧包含任意个数的比特，但是会用 01111110 来标志一帧的开始与结束
- 当然，为了避免冲突，在数据中每 5 个连续的 1 就会紧接着一个 0 进行填充，可以利用硬件进行解码
- 性能优于字节填充法

违规编码法

- 利用曼彻斯特编码表示所传输的数据，这样连续的 0 或 1 都是违规的编码
- 实际上也常用零比特编码以及违规编码法进行组帧

差错控制

检错编码

1. 奇偶校验码
2. 循环冗余码
    - 令 r = 除数位数 - 1
    - 在数据后添加 r 个 0 后除以 G(x) 得到余数
    - 将余数连接到原始数据之后即为最后的检错编码

纠错编码

- 海明码

流量控制与可靠传输机制

流量控制与滑动窗口机制

1. **停止-等待流量控制**
    - 最简单的流量控制方法
    - 发送方每次只允许发送一个帧
    - 接收方每次接受一个帧都要反馈一个应答信号，表示可以接受下一帧
    - 发送方收到应答信号后，才能发送下一帧
    - 传输效率很低
2. **滑动窗口流量控制**
    - 发送方和接收方都有自己的缓存——分别为**发送窗口**和**接收窗口**
    - 发送方每收到一个按序确认的确认帧，就将发送窗口向前滑动一个位置
    - 接收方每收到一个序号落入接收窗口的数据帧，即将该帧接收；不属于对应范围的帧一律丢弃
    - 从概念上看：
        - 停止-等待协议相当于发送窗口 = 1， 接收窗口 = 1
        - 后退 N 帧协议相当于发送窗口 > 1，接收窗口 = 1
        - 选择重传协议相当于发送窗口 > 1，接收窗口 > 1
        - 受 n 比特对帧编号的限制，后两种协议还需要满足 **发送窗口 + 接收窗口 ≤ 2^n**
        - 保证有序接受帧的条件为：**接收窗口的= 1**

可靠传输机制

采用确认和超时重传机制的可靠传输协议称为**自动重传请求（ARQ）**

1. **停止——等待协议（S-W）**
    - 数据帧丢失、发生位错、发送方收不到确认帧都会导致重传
2. **后退 N 帧协议（GBN）**
    - **累计确认**：允许接收方不需要每收到一个正确的数据帧就立即发回一个确认帧，可在连续收到多个正确的数据帧后对最后一个数据帧发回确认信息
    - 若采用 n 比特对帧编号，**发送窗口 ≤ 2^n - 1**

- 发送方发送 N 个数据帧后，若发现这 N 个帧的前一个数据帧在计时器超时的时候仍未收到其确认帧，则该帧被判为出错或丢失，此时发送方后就要重传这 N 个帧

3. **选择重传协议（SR）**
   - 发送方仅重传出错的帧，接收方不使用累计确认
   - 一旦接收方检测到某个数据帧出错，即将发送方发送一个否定帧 NAK，要求发送方立即重传对应的数据帧
   - SR 协议的发送窗口和接收窗口应满足：**发送窗口 + 接收窗口 ⩽ 2^n，接收窗口 ⩽ 2^(n -1)**

介质访问控制

信道划分介质访问控制

1. **频分复用**

   将信道的总频带划分为多个子频带，每个子频带作为一个子信道，每对用户使用一个子信道进行通信

2. **时分复用**

   将信道的传输时间划分为一段段等长的时间片，称为 **TDM 帧**，每个用户在每个 TDM 帧中占用固定序号的时隙

3. **波分复用**

   相当于光的频分复用，不同的波长作为不同的信道

4. **码分复用（CDM）**
   - 既共享信道的频率，也共享信道的时间
   - 不同站点的码片向量互相正交，在传达接收方时可以利用码片进行解码

随机访问介质访问控制

1. 纯 ALOHA 协议
   - 当总线型网络中的任何站点需要发送数据时，可以不进行任何检测就发送数据
   - 若在一段时间内未收到确认，则认为传输过程中发生了冲突，需要等待一段时间后在发送数据，直至发送成功
2. 时隙 ALOHA 协议
   - 将时间划分为一段段等长的时隙，规定站点只能在每个实习开始时才能发送帧
3. CSMA 协议（载波监听多路访问）

   a. 1-坚持 CSMA
      - 当站点要发送数据时监听信道

- 若信道空闲则立即发送（以 1 的概率发送）
- 若信道忙则继续监听直至信道空闲（坚持监听）

b. 非坚持 CSMA
- 当站点要发送数据时监听信道
- 若信道空闲则立即发送（以 1 的概率发送）
- 若信道忙则放弃监听，等待随机时间后继续监听（非坚持）

c. p-坚持 CSMA
- 当站点要发送数据时监听信道
- 若信道空闲则以 p 的概率发送
- 若信道忙则继续监听直至信道空闲（坚持监听）

4. CSMA/CD 协议（载波监听多路访问 / 冲突检测）
   - 使用于总线型半双工网路，由于全双工网络具有两条信道，所以不需要冲突检测
   - 在发送过程中，边发送边监听，如果监听到产生冲突则等待随机事件后重发
   - 随机时间的确定：0 - 2^k - 1 中的离散时间当中选一个
5. CSMA/CA 协议（载波监听多路访问 / 冲突避免）
   - 适用于无线局域网
   - 为了避免冲突，所有站发送数据后必须等待一段时间才能发送下一帧，称为帧间间隔（IFS）
   - SIFS：短 IFS，用来分隔属于一次对话的各帧
   - PIFS：点协调 IFS，在 PCF 操作中使用
   - DIFS：分布式协调 IFS，用于异步帧竞争访问的时延
   - CSMA / CA 算法的流程：
     i. 若站点最初有数据要发送（而非发送不成功再进行重传），且检测到信道空闲，那么在等待时间 DIFS 后，就发送整个数据帧
     ii. 否则，站点执行 CSMA/CA 退避算法，选取一个随机退避值。一旦检测到信道忙，退避计时器就保持不变。只要信道空闲，退避计时器就进行倒计时
     iii. 当退避计时器减至 0 时（这时信道只可能是空闲的），站点就发送整个帧并等待确认
     iv. 发送站若收到确认，就知道已发送的帧被目的站正确接收。这时要发送第二帧，就要从步骤 2 开始，执行 CSMA/CA 退避算法，随机选定一段退避时间

v. 若发送站在规定时间（由重传计时器控制）内未收到确认帧 ACK，就必须重传该帧，再次 使用 CSMA/CA 协议争用该信道，直到收到确认，或经过若干次重传失败后放弃发送

轮询访问：令牌传递协议

- 一个令牌沿着唤醒总线在各站之间依次传递，令牌是一个特殊的控制帧，确保同一时刻只有一个站独占信道
- 非常适合高负载的广播信道

局域网

局域网的基本概念和体系结构

- 局域网的三个要素：拓扑结构、传输介质、介质访问控制方式，其中最重要的是介质访问控制方式
- 常见局域网拓扑主要有：星形结构、环形结构、总线形结构、星形和总线形的复合结构
- 比较特殊的局域网拓扑实现有：
  - 局域网：逻辑总线形、物理星形
  - 令牌环：逻辑环形、物理星形
  - FDDI：逻辑环形、物理双环

以太网与 IEEE 802.3

- 信息以广播方式发送，使用 CSMA/CD 方式对总线进行访问控制
- 采用无连接的工作方式，发送的数据都是用曼彻斯特编码的信号
- 以太网的 MAC 帧格式：

以太网 MAC 帧格式有两种标准：DIX Ethernet V2 标准（即以太网 V2 标准）和 IEEE 802.3 标准。这里只介绍最常用的以太网 V2 的 MAC 帧格式，如图 3.25 所示。

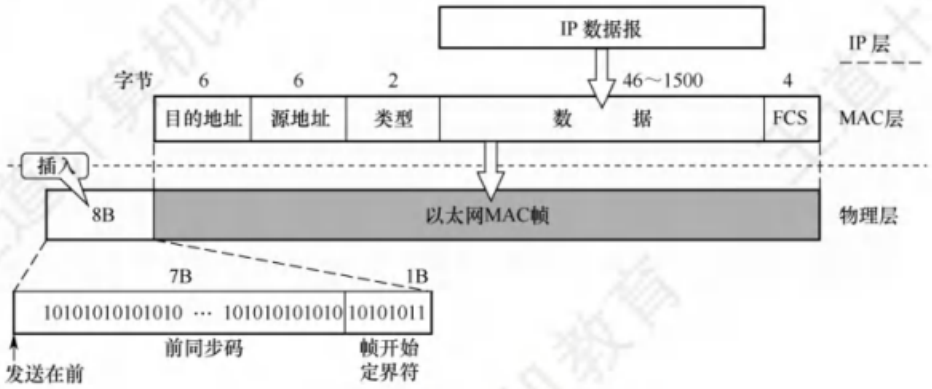


图 3.25　以太网 V2 标准的 MAC 帧格式

命题追踪 ▶▶ 以太网帧首部的内容、首部和尾部的长度（2010、2011）

在帧前面插入的 8 字节前导码分为两个字段：第一个字段是 7 字节的前同步码，用来实现 MAC 帧的比特同步；第二个字段是 1 字节的帧开始定界符，表示后面的信息就是 MAC 帧。

注　意

以太网帧不需要帧结束定界符，因为当以太网传送帧时，各帧之间必须有一定的间隙。因此，接收方只要找到帧开始定界符，其后面连续到达的比特流就都属于同一个帧。实际上，以太网采用了违规编码法的思想，因为以太网使用曼彻斯特编码，所以每个码元中间都有一次电压的跳变。发送方发完一个帧后，发送方网络接口上的电压不再变化，这样接收方就能很容易地找到帧的结束位置，这个位置往前数 4 字节就是 FCS 字段，于是就能确定数据字段的结束位置。

命题追踪 ▶▶ 以太网帧中目的地址和源地址的含义（2018）

目的地址：6 字节，帧在局域网上的目的适配器的 MAC 地址。

源地址：6 字节，传输帧到局域网上的源适配器的 MAC 地址。

类型：2 字节，指出数据字段中的数据应交给哪个上层协议处理，如网络层的 IP 协议。

命题追踪 ▶▶ 分析 IP 首部并判断其以太帧是否需要填充（2012）

数据：46～1500 字节，承载上层的协议数据单元（如 IP 数据报）。以太网的最大传输单元是 1500 字节，若 IP 数据报超过 1500 字节，则必须将该 IP 数据报分片。此外，由于 CSMA/CD 算法的限制，以太网帧必须满足最小长度是 64 字节，当数据字段的长度小于 46 字节时，MAC 子层就在数据字段的后面加一个整数字节的填充字段，以确保帧长不小于 64 字节。

IEEE 802.11 无线局域网

- 无线局域网的组成：主要分为**有固定基础设施的无线局域网**和**无固定基础设施的无线局域网**
- 802.11 局域网的 MAC 帧格式：

2．802.11 局域网的 MAC 帧

802.11 帧共有三种类型，即数据帧、控制帧和管理帧。数据帧的格式如图 3.28 所示。

802.11 数据帧由以下三部分组成：

1）MAC 首部，共 30 字节。帧的复杂性都在 MAC 首部。

2）帧主体，即帧的数据部分，不超过 2312 字节。它比以太网的最大长度长很多。

3）帧检验序列 FCS 是 MAC 尾部，共 4 字节。

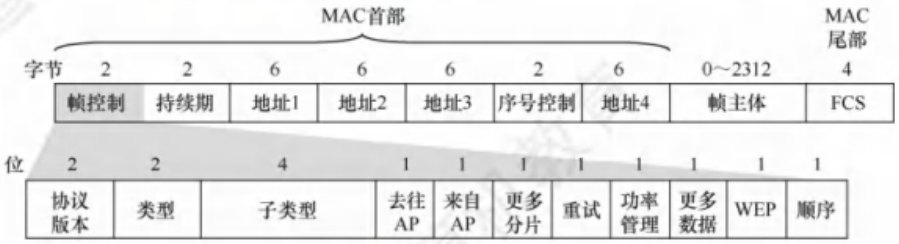


图 3.28　802.11 局域网的数据帧

命题追踪 ▶ 802.11 数据帧前三个地址的含义（2017、2022）

802.11 帧的 MAC 首部中最重要的是 4 个地址字段（都是 MAC 地址）。这里仅讨论前三个地址（地址 4 用于自组网络）。这三个地址的内容取决于帧控制字段中的“去往 AP”和“来自 AP”这两个字段的数值。表 3.4 中给出了 802.11 帧的地址字段最常用的两种情况。

表 3.4　802.11 帧的地址字段最常用的两种情况

去往 AP	来自 AP	地　址　1	地　址　2	地　址　3	地　址　4
0	1	接收地址 = 目的地址	发送地址 = AP 地址	源地址	——
1	0	接收地址 = AP 地址	发送地址 = 源地址	目的地址	——

地址 1 是直接接收数据帧的结点地址，地址 2 是实际发送数据帧的结点地址。

1）现在假定从一个 BSS 中的 A 站向 B 站发送数据帧。在 A 站发往 AP 的数据帧的帧控制字段中，“去往 AP=1”而“来自 AP=0”；地址 1 是 AP 的 MAC 地址，地址 2 是 A 站的 MAC 地址，地址 3 是 B 站的 MAC 地址。注意，“接收地址”与“目的地址”并不等同。

2）AP 接收到数据帧后，转发给 B 站，此时在数据帧的帧控制字段中，“去往 AP=0”而“来自 AP=1”；地址 1 是 B 站的 MAC 地址，地址 2 是 AP 的 MAC 地址，地址 3 是 A 站的 MAC 地址。注意，“发送地址”与“源地址”也不等同。

对这三个地址的理解方法如下：地址 1 和地址 2 分别是无线通信中信道两端的接收地址和发送地址。当主机发往 AP 时，接收地址不是实际的目的地址，因此用地址 3 来存放实际的目的地址；当 AP 发往主机时，发送地址不是实际的源地址，因此用地址 3 来存放实际的源地址。

广域网

PPP 协议（数据链路层协议）

- 点对点协议（Point-to-Point Protocol, PPP）是现在最流行的点对点链路控制协议
- 主要有两种应用：
  a. 用户通常都要连接到某个ISP才能接入互联网，PPP协议就是用户计算机与ISP通信时所用的数据链路层协议
  b. 广泛用于广域网路由器之间的专用线路

数据链路层设备

i. **网桥**

- 使用集线器在物理层扩展以太网会形成更大的冲突域（集线器不能解决数据冲突问题）

- 为了避免这个问题，可以使用网桥在数据链路层扩展以太网，原来的每个以太网成为一个网段
- 使用网桥进行扩展时，不会将原本独立的两个冲突域合并成一个更大的冲突域，这是因为网桥具有识别帧和转发帧的能力，根据帧首部中的目的 MAC 地址和网桥的帧转发表来转发或丢弃所受到的帧，起到过滤通信量的功能

ii. **以太网交换机**

- 也叫二层交换机。顾名思义，是因为数据链路层位于计算机网络工作模型的第二层
- 它相当于多接口的网桥，将网络分成小的冲突域，提供更大带宽
- 如果使用集线器，由于共享式的工作环境，平均带宽会被分流。但以太网交换机是全双工的，用户通信时独占带宽，因此传输效率大大提高

Network Layer

网络层的功能

异构网络互连

- 网络互连指将两个以上的计算机网络通过一定的方法用终极系统相互连接起来
- 中继系统主要有：
  - 物理层中继系统：转发器、集线器
  - 数据链路层中继系统：网桥、交换机
  - 网络层中继系统：路由器
  - 网络层以上中继系统：网关
- **虚拟互连网络**即逻辑互连网络，指互连起来的各种物理网络的异构性客观存在，但通过 IP 协议就可使性能各异的网络在网络层上看起来像是一个统一的网络

路由与转发

1. 路由选择：根据路由协议构造路由表并动态更新，以决定分组到达目的地节点的最优路径
2. 分组转发：指路由器根据转发表将分组从合适的端口转发出去

网络层提供的两种服务

1. 面向连接的虚电路服务
   - 当两台计算机通信时，先建立网络层的链接即逻辑上的虚电路
   - 连接一旦建立就固定了虚电路对应的物理路径

- 这条电路不是专用的，可能同时有若干条虚电路交叉
- 对网络故障的适应性较差，一个节点的故障会影响整条虚电路的工作

2. 无连接的数据报服务
   - 发送分组前不需要先建立连接
   - 高层协议将报文分成若干数据段，中间节点存储分组并寻找最佳路由，随后尽快转发
   - 对网络故障的适应性较强，故障节点不影响其他分组的转发

SDN（软件定义网络）

1. 控制平面
   - 对数据平面上的路由器进行集中式控制，方便软件控制网络
   - 远程控制器掌握各主机和中各网络的状态，为每个分组计算出最佳路由，通过 Openflow 协议将转发表下发给路由器，这样一来，路由器的工作就变得很单纯
2. 数据平面
   - 本地的路由器根据被分发的路由表进行分组转发

拥塞控制

1. 开环控制：在设计网络时实现将有关发生拥塞的因素考虑周到，力求网络工作时不发生拥塞，是一种静态的预防方法
2. 闭环控制：事先不考虑有关发生拥塞的各种因素，采用监测网络系统去监视，及时检测哪里发生了拥塞，然后将拥塞信息传到合适的地方

IPv4

IPv4 分组

1. IPv4 分组的格式
   - 一个 IP 分组由首部和数据部分组成，首部的前一部分长度固定，一共 20B
   - 图解首部组成：

- 首部部分字段的含义：
  - 首部长度：4位，以 4B 为单位，最大可以表示 60B，但是首部一般都只有 20B
  - 总长度：16位，以 1B 为单位。虽然最大可以表示 65535B，但一般不能超过 MTU 值
  - 标识：16位，每产生一个数据报就加 1
  - 标志：3位，最低位为 MF，MF = 1 表示后面还有分片，反之没有；中间位为 DF，DF = 0 表示允许分片，否则不允许；最高位无意义
  - 片偏移：13位，以 8B 为单位。指出分片在原始数据报中的位置

IPv4 与 NAT

1. IPv4地址
   - IP 地址由网络号和主机号组成，地址类型如图：

   - 主机号全 0 表示本网络本身；全 1 表示本网络的广播地址；32 位全为 0 表示本网络的本主机；32 位全 1 表示整个 TCP/IP 网络的广播地址
   - 地址管理机构只分配网络号，主机号由对应网络单位自行分配
   - 由转发器或桥接器连接的局域网仍然是同一网络，属于同一广播域
2. NAT（网络地址转换）
   - 通过将专用网络地址转换为公用地址，从而对外隐藏内部管理的 IP 地址
   - NAT 路由器收到分组后会为该 IP 分组生成端口号，并将对应的源地址改为全局 IP

- 分组到达目的全局 IP 后也会被对方的 NAT 路由器转换成目的私有地址

子网与路由聚合

1. 划分子网
   - 将 IP 地址继续分为三级，分别为网络号、子网号、主机号
   - 划分子网属于一个单位内部的业务，单位对外仍然表现为没有划分子网的网络
   - 划分子网的方法是从网络的主机号使用若干位作为子网号，从而减降低下属二级单位的路由表复杂度
2. 子网掩码和默认网关
   - 主机或路由器只需将 IP 地址与其对应的子网掩码按位与就能得到其子网的网络地址
   - 默认网关是子网与外部网络连接的设备，即连接本机或子网的路由器接口的 IP 地址。一般来讲，发送的分组如果用子网掩码判断出目的主机在子网中，则直接发送；否则将数据发送到默认网关，又该路由器将其转发到其他网络
3. 无分类域间路由选择（CIDR）
   - 消除传统 A、B、C 类网络地址即划分子网的概念，将网络表示为 **IP 地址 / 网络前缀所占的位置**，这被称为斜线记法
4. 路由聚合
   - 一个 CIDR 块有很多地址，在路由表中可以利用 CIDR 地址块查找目的网络，即合并前缀相同的 CIDR 地址块，降低路由表复杂度
5. 子网的划分，不太高效的做法是平均分配，比较搞笑的做法应该是按照组织大小倒序排序后不断在子网号高位补 **10**

网络层转发分组的过程

- 按下所述流程，如果中途有一步未能完成则继续进行下一步，最后总能利用默认路由实现分组转发
- **提取 IP → 查找特定主机路由 → 查找最长匹配子网掩码的路由 → 默认路由**

地址解析协议（ARP）

1. IP 地址与硬件地址
   - 硬件地址是 MAC 地址，只有将 IP 地址封装成链路层帧后，MAC 才会出现在 MAC 帧的首部
2. 地址解析协议（**ARP**，网络层协议）
   - ARP 协议用于完成从 IP 到 MAC 地址的映射

    - 每台主机都有 ARP 缓存，用来存放本局域网上各主机和路由器的 IP 地址到 MAC 地址的映射表，即 ARP 表
    - 工作原理：若要向目的 IP 发送分组，先从 ARP 表查找有无此 IP，如有可直接将硬件地址写入 MAC 帧；否则向全 1 MAC 广播地址发送 ARP 请求分组，局域网内所有主机都会收到此 ARP 请求，目的主机发现后就会发送响应分组，最后也能从 ARP 表查找到对应物理地址
3. 动态主机配置协议（**DHCP**，基于 UDP 的应用层协议）
    - 作用是给主机动态分配 IP 地址
    - 过程：**DHCP 发现（客户）→ DHCP 提供（服务）→ DHCP 请求（客户）→ DHCP 确认（服务）**
4. 网际控制报文协议（**ICMP**，网络层协议）
    - 作用是尽量保证 IP 数据报的有效转发和提高交付成功的机会
    - ICMP 报文有两种：**ICMP 差错报告报文** 以及 **ICMP 询问报文**
    - **ICMP 差错报告报文** 用于向源主机报告差错和异常情况，主要包括：
        - 终点不可达：路由器或主机不能交付数据报
        - 源点抑制：路由器或主机因为拥塞而丢弃数据报
        - 时间超过：路由器收到 TTL = 0 的数据报
        - 参数问题：路由器或目的主机收到的数据报的首部中有的字段不正确
        - 路由重定向：路由器把改变路由报文发送给主机，主机下次会把报文发送给其他路由器
    - **ICMP 询问报文** 主要包括：
        - 回送请求和回答报文：如 PING
        - 时间戳请求和回答报文：如 TRACEROUTE
        - 地址掩码请求和回答报文
        - 路由器询问和通告报文

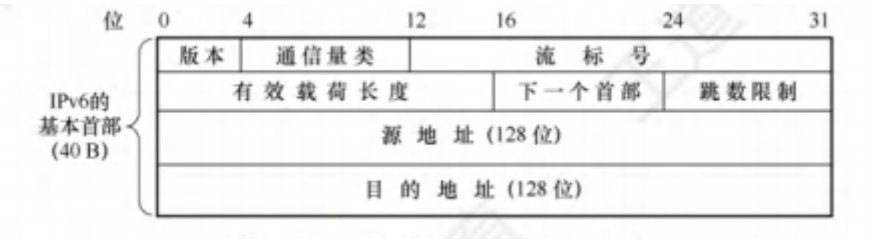
IPv6

IPv6 的特点

- 更大的地址空间
- 灵活的首部格式：具有可选的扩展首部
- 即插即用：使用 IPv6 不需要 DHCP
- 增强了安全性

IPv6 数据报的基本首部

- 基本首部字段数减少到只有 8 个：



IPv6 地址

- IPv6 数据报的目的地址有以下三种基本类型：
  - 单播：传统的点对点通信
  - 多播：一点对多点的通信
  - 任播：IPv6 增加的类型。其终点是一组计算机，但是数据报之交付其中的一台计算机，通常是距离最近的一台

从 IPv4 到 IPv6 过渡的方案

1. 双协议栈：在一台设备上同时兼容 IPv4 和 IPv6 的协议栈
2. 隧道技术：IPv6 要进入 IPv4 网络时，将 IPv6 封装成 IPv4 数据报的数据部分，等到离开 IPv4 网络时再拆分

路由算法与路由协议

路由算法

1. 静态路由与动态路由
   - 静态路由算法：由网络管理员手工配置每一条路由
   - 动态路由算法：根据网络流量负载和拓扑结构的变化来动态调整自身的路由表
2. **距离-向量路由算法**
   - 利用 **Bellman-Ford 算法** 计算单源最短路径
   - 距离-向量报文包括自身到其他所有目的节点的距离信息，如果网络很大，很可能产生十分大的更新报文，影响网络的工作效率
   - 最常见的距离-向量路由算法是 **RIP 算法**，采用跳数作为距离的度量
3. **链路状态路由算法**
   - 利用 **Dijkstra 算法** 计算单源最短路径
   - 链路状态路由算法要求每个节点都具有全网拓扑结构图
   - 节点主动测试所有相邻节点的状态，并定期将链路状态传播给所有其他节点

- 节点每收到一个链路状态报文，就利用报文和 Dijkstra 算法 更新自己的网络状态拓扑图
- 节点的链路状态只涉及相邻节点的连通状态，该算法适用于大型或路由信息变化聚敛的互联网环境
- 每个节点都使用同样的链路状态独立地计算路径，而不依赖中间节点的计算，链路状态报文不加改变地传播，采用该算法易于查找故障

分层次的路由选择协议

1. 内部网关协议（IGP）
   - 即在一个自治系统内部使用的路由选择协议
   - 目前这类协议使用得最多，如 RIP 和 OSPF
2. 外部网关协议（EGP）
   - 若源主机和目的主机处在不同的自治系统中（两个自治系统可能使用不同的 IGP），则当数据报传到一个自治系统的边界时，就需要使用一种协议将路由选择信息传递到另一个自治系统中，这样的协议就是外部网关协议
   - 目前使用最多的外部网关协议是 BGP-4
   - 自治系统之间的路由选择也称域间路由选择，自治系统内部的路由选择也称域内路由选择

路由信息协议（RIP，基于 UDP 的应用层协议）

1. RIP 的规定
   - 网络中的每个路由器都要维护从它自身到其他每个目的网络的距离记录
   - 使用跳数衡量到达目的网络的距离
   - RIP 认为好的路由就是通过的路由器数目少
   - RIP 允许一条路径最多只能包含 15 个路由器，16 表示不可达
   - 路由表的一个条目有三个字段：**<目的网络 N，距离 d，下一条路由器地址 X>**
2. RIP 的特点
   - 仅和相邻的路由器交换自身的路由表
   - 按固定的时间间隔交换路由信息；当网络拓扑变化时，路由器也及时向相邻路由器通告拓扑变化后的路由信息
3. RIP 的距离向量算法
   a. 对地址为 X 的相邻路由器发来的 RIP 报文，先修改此报文中的所有项目，把下一跳字段中的地址都改为 X，并把所有距离字段的值加 1
   b. 对修改后的 RIP 报文中的每个项目：

i. 如果原来路由表中没有目的网络，直接将该项目添加到路由表中

ii. 如果原来的路由表中有目的网络 N，且吓一跳路由器的地址是 X，用收到的项目更新原路由表中的项目

iii. 如果原来的路由表中有目的网络 N，但下一跳地址不是 X，只有新条目的距离更小时才更新原条目

c. 180 秒后还收不到相邻路由器的更新路由表，直接将此路由器记为不可达

4. 优点
   - 实现简单、开销小、收敛快
   - 好消息传播得快
5. 缺点
   - 限制网络的规模，最大的距离为 15
   - 路由器之间交换的是完整的路由表，网络规模越大，开销就会越大
   - 网络出现故障时，有可能会经过多次交换才会收敛，甚至会出现毒性传播，即坏消息传播得慢

开放最短路径优先协议（OSPF，网络层协议）

1. OSPF 的基本特点
   - OSPF 向本自治系统中的所有路由器发送链路状态，使用洪泛法，而 RIP 只向相邻路由器发送自身的路由表
   - 仅当链路状态发生变化时，才会用洪泛法向所有路由器发送信息，更新过程收敛很快
2. 基本工作原理
   a. 因为各路由器之间频繁地交换链路状态信息，所以所有路由器最终都能建立一个链路状态数据库，即全网的拓扑结构图

   b. 每个路由器利用链路状态数据库中的数据，使用 **Dijkstra 算法** 计算自己到达各目的网络的最优路径，构造出自己的路由表

   c. 当链路状态发生变化时，每个路由器重新计算到达各目的网络的最优路径，构造出新的路由表

边界网关协议（BGP，基于 TCP 的应用层协议）

- 作用是帮助不同自治系统 AS 的路由器之间交换路由信息
- 采用 **路径-向量路由选择协议**，注意这是前面没有提到的概念
- 每个 AS 的管理员选择一个本自治系统的 **BGP 发言人**
- 一个 BGP 发言人与其他 AS 中的发言人交换路由信息，建立 TCP 连接

- BGP 所交换的网络可达性的信息，就是要到达某个网络要经过的一系列自治系统

协　议	RIP	OSPF	BGP	
类型	内部	内部	外部	
路由算法	距离-向量	链路状态	路径向量	
传递协议	UDP	IP	TCP	
路径选择	跳数最少	代价最低	较好，非最佳	
交换结点	和本结点相邻的路由器	网络中的所有路由器	和本结点相邻的路由器	
交换内容	当前本路由器知道的全部信息，即自己的路由表	与本路由器相邻的所有路由器的链路状态	首次	整个路由表
			非首次	有变化的部分

协　议	RIP	OSPF	BGP	
类型	内部	内部	外部	
路由算法	距离-向量	链路状态	路径向量	
传递协议	UDP	IP	TCP	
路径选择	跳数最少	代价最低	较好，非最佳	
交换结点	和本结点相邻的路由器	网络中的所有路由器	和本结点相邻的路由器	
交换内容	当前本路由器知道的全部信息，即自己的路由表	与本路由器相邻的所有路由器的链路状态	首次	整个路由表
			非首次	有变化的部分

协　议	RIP	OSPF	BGP	
类型	内部	内部	外部	
路由算法	距离-向量	链路状态	路径向量	
传递协议	UDP	IP	TCP	
路径选择	跳数最少	代价最低	较好，非最佳	
交换结点	和本结点相邻的路由器	网络中的所有路由器	和本结点相邻的路由器	
交换内容	当前本路由器知道的全部信息，即自己的路由表	与本路由器相邻的所有路由器的链路状态	首次	整个路由表
			非首次	有变化的部分

网路层设备

冲突域和广播域

1. 冲突域：连接到同一物理介质上的所有结点的集合，只有物理层设备不能分割冲突域
2. 广播域：指接受同样广播消息的节点集合，只有网络层以上的设备可以分割广播域

路由器的组成和功能

- 路由器的任务是连接不同的网络并完成分组转发，在多个逻辑网络（多个广播域）互连时必须使用路由器，路由器可以隔离广播域
- 当源主机和目的主机不在同一个网络上时，需要由路由器按照转发表指出的路由将分组转发给下一个路由器（间接交付）
- 路由选择：也成为控制部分，核心构件是路由选择处理机，任务是根据所选定的路由选择协议构造出路由表并定期更新维护

- 分组转发：由**交换结构、输入端口、输出端口**构成。其中交换结构也称交换组织，作用是根据转发表对分组进行处理

路由表与分组转发

- **路由表**：由选择算法得出，主要用途是路由选择，每一个条目由 **<目的 IP，子网掩码，下一跳 IP，接口>** 组成
- **转发表**：由路由表得出。每一个条目由 **<目的站，下一跳>** 组成

Transport Layer

传输层提供的服务

传输层的功能

1. 应用进程之间的逻辑通信：从传输层来看，通信的真正端点不是主机而是主机当中的进程
2. 复用和分用：复用是指发送方不同的应用进程都可以使用同一个传输层协议传送数据；分用使之接收方的传输层在剥去报文的首部后能够把这些数据正确交付到目的应用进程
3. 差错检测：传输层要对收到的报文进行差错检测。对于 TCP 协议：报文出错则要求发送方重发；对于 UDP 协议，报文出错则直接丢弃
4. 面向连接和无连接的传输协议：TCP 面向连接，UDP 无连接

传输层的寻址与端口

1. 端口的作用：让应用层的各种进程将其数据通过端口向下交付给传输层，让传输层直到应当将其报文段中的数据向上通过端口交付给应用层相应的进程
2. 端口号
    - 服务器端使用的端口号：熟知端口号为 0-1023；登记端口号为 1024-49151
    - 客户端使用的端口号：49152-65535
3. 套接字：**<IP 地址，端口号>**

无连接服务与面向连接服务

- TCP 提供面向连接的可靠服务，主要适用于可靠性更重要的场合：HTTP、SMTP、FTP、TELNET
- UDP 提供无连接的不可靠服务，执行速度快、实时性好：DNS、TFTP、RIP、DHCP、SNMP、IGMP

UDP 协议

UDP 数据报

1. UDP 概述
    - 仅在 IP 层之上提供了两个最基本的功能：**复用分用、差错检测**
    - 无需建立连接，无连接时延
    - 无连接状态
    - 首部开销小
    - 没有拥塞控制
    - 支持一对一、一对多、多对一、多对多的交互通信
2. UDP 首部格式：8B
    - 源端口：16 位
    - 目的端口：16 位
    - 长度：16 位
    - 检验和：16 位
3. UDP 检验和
    - 计算检验和首先要为数据报构造伪首部以及对检验和字段暂时用全 0 代替
    - 此后将临时数据报每 16 位相加，结果求反码得到检验和字段

TCP 协议

TCP 协议的特点

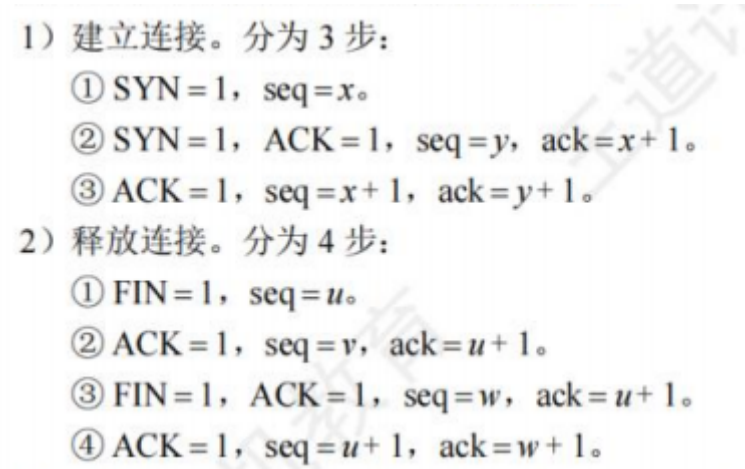
- 面向连接
- TCP 连接只能一对一
- TCP 提供可靠交付的服务
- TCP 提供全双工通信
- 面向字节流

TCP 报文段（（20 + 4N（可选））B）

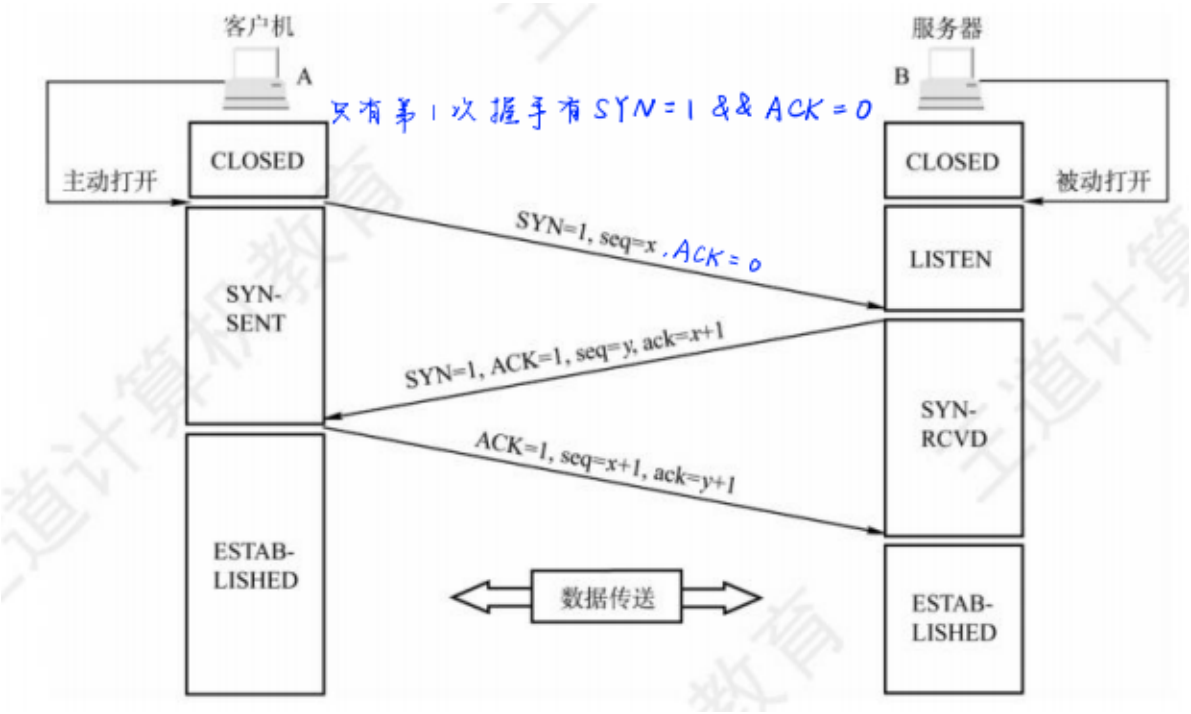
- 源端口：16 位
- 目的端口：16 位
- 序号：32 位。对所传输的每一个字节编号

- 确认号：32 位。对所期望收到下一个报文段的第一个字节的序号
- 数据偏移（首部长度）：4 位。指 TCP 报文段的数据起始处距离 TCP 报文段的起始处有多远。按照 4B 为单位，首部最大长度就是 60B
- 保留：6 位
- 紧急位 URG：报文推送的优先级
- 确认位 ACK：仅当 ACK = 1 时才有效，在建立 TCP 连接后都应置为 1
- 推送位 PSH：进程进行交互式通信时可以置为 1
- 复位位 RST：RST = 1 时表示 TCP 连接中出现严重差错，必须释放连接并重新建立
- 同步位 SYN：SYN = 1 表示报文用于建立连接
- 终止位 FIN：FIN = 1 表示报文段发送方已经发送完毕并要求释放连接
- 窗口：16 位
- 检验和：16 位。计算方法与 UDP 检验和一样
- 紧急指针：16 位。仅当 URG = 1 时有意义
- 选项：长度可变，最大 40B
- 填充：为了使整个首部长度是 4B 的整数倍

TCP 连接管理


1）建立连接。分为 3 步：
① SYN = 1，seq = x。
② SYN = 1，ACK = 1，seq = y，ack = x + 1。
③ ACK = 1，seq = x + 1，ack = y + 1。
2）释放连接。分为 4 步：
① FIN = 1，seq = u。
② ACK = 1，seq = v，ack = u + 1。
③ FIN = 1，ACK = 1，seq = w，ack = u + 1。
④ ACK = 1，seq = u + 1，ack = w + 1。

1. TCP 连接的建立（三次握手）
    a. 客户机 TCP 向服务器 TCP 发送连接请求报文段，其中 SYN = 1，初始序列号 seq = x
    b. 服务器 TCP 收到连接请求报文段后同意连接并发回确认，位该 TCP 连接分配缓存和变量。其中 SYN = ACK = 1；确认号 ack = x + 1，自身的初始序列号 seq = y
    c. 客户机收到确认报文段后，还要向服务器给出确认，为该 TCP 连接分配缓存和变量。其中 ACK = 1，确认号 ack = y + 1，序列号 seq = x + 1



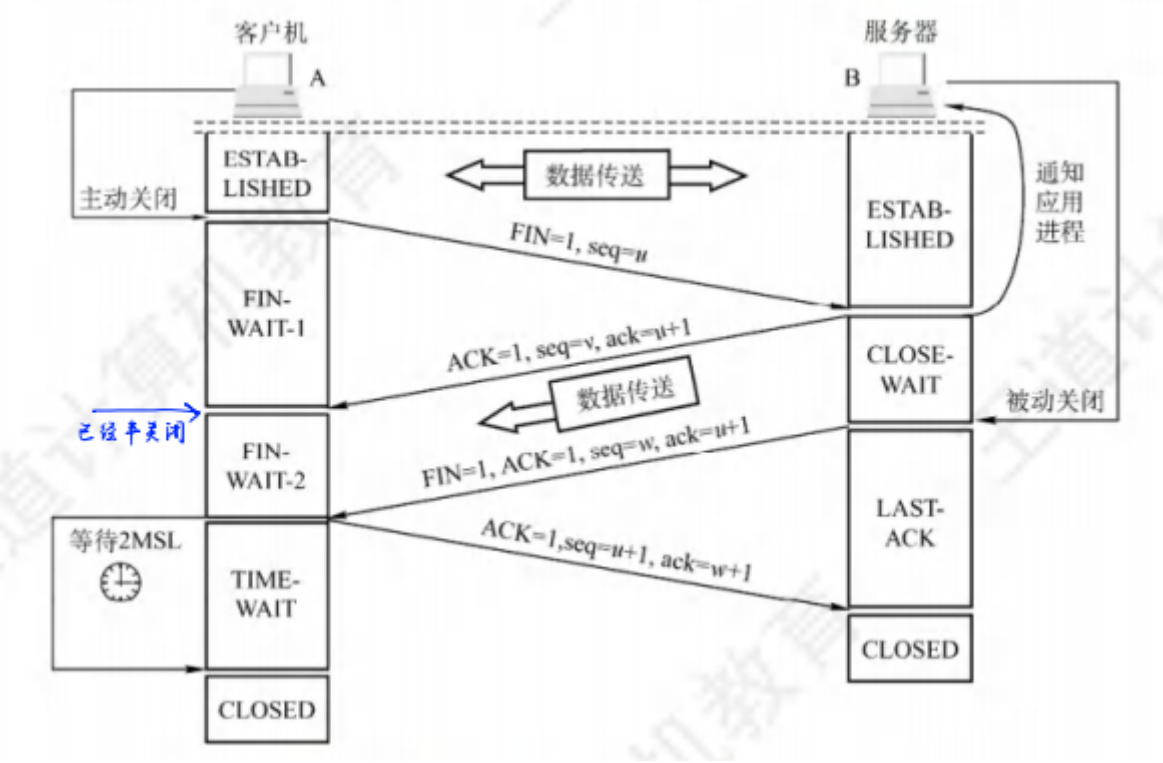
2. TCP 连接的释放（四次挥手）

   a. 客户机打算释放连接时，向 TCP 发送连接释放报文段，并停止发送数据，主动关闭 TCP 连接，该报文段的终止位 FIN = 1，序列号 seq = u

   b. 服务器收到连接释放报文段后发出确认，确认号 ack = u + 1，序列号 seq = v。此时 TCP 已处于**半关闭状态**

   c. 若服务器已经没有要向客户机发送的数据，通知 TCP 释放连接，此时 FIN = 1，设序列号 seq = w，重复上次已发送的确认号 ack = u + 1

   d. 客户机收到连接释放报文段后，必须发出确认，此时报文段的确认位 ACK = 1，确认号 ack = w + 1，序列号 seq = u + 1，服务器收到该确认报文段后进入连接关闭状态。客户机等待一段时间后也进入关闭状态



TCP 可靠传输

1. 序号：前面将 TCP 报文字段信息时已经提到序号是基于字节流进行排序的，它指出了 TCP 报文所传输的每一个字节是原始信息中的第几个字节，如此一来数据的保序就有了依据
2. 确认：TCP 默认使用累计确认，只确认数据流中第一个至丢失字节位置的字节
3. 重传
    - 两种时间会导致 TCP 的重传
    - 超时：采用自适应算法，动态调整 RTT，超时重传时间会略大于 RTT
    - 冗余 ACK：当发送方收到对同一个报文段的 3 个冗余 ACK 时就认为跟在这个被确认报文段之后的报文段已经丢失，进行重发

TCP 流量控制

- 流量控制的功能是让发送方的发送速率不要太快，以便让接收方来得及接收
- 这是一种**端到端的视角**：只关注两端的缓冲窗口，保证发送、接收速率与窗口大小之间的平衡
- 注意，流量控制不涉及传输细节的控制，所谓端到端的视角指的是流量控制不关注发送的过程：即无所谓信道的拥塞与否

TCP 拥塞控制

1. 拥塞控制是指防止过多的数据注入网络，保证网络中的路由器或链路不致过载
2. 慢开始和拥塞避免

a. 慢开始算法：先发送少量数据探测，若没有发生拥塞则适当增大拥塞窗口。具体说明为发送方先令发送窗口 cwnd = 1，随后指数增长直至达到 ssthresh 阈值后恢复线性增长

b. 拥塞避免算法：在 cwnd > ssthresh 后使用拥塞避免算法。只要发送方判断网络出现拥塞，则令 **ssthresh = cwnd / 2，cwnd = 1**

3. 快重传和快恢复

a. 快重传：发送方一旦连续收到 3 个冗余 ACK 则立即重传相应的报文段

b. 快恢复：在拥塞避免状态发生拥塞时，令 **cwnd = ssthresh = cwnd / 2**

Application Layer

网络应用模型

客户/服务器模型

- 有一个总是打开的主机成为服务器
- 客户机发出服务请求并等待接收结果
- 服务器收到请求后分析请求并进行必要处理
- 网络中各计算机的地位不平等
- 客户机相互之间不直接通信
- 可扩展性不佳，服务器支持的客户机数量有限

P2P 模型

- 各计算机没有固定的客户和服务器划分，任意一对计算机成为对等方，直接相互通信
- 可扩展性好
- 网络健壮性强，单个节点失效不影响其他节点
- 但是主机在获取服务的同时还要给其他节点提供服务，会占用较多的内存

域名系统（DNS）

层次域名空间

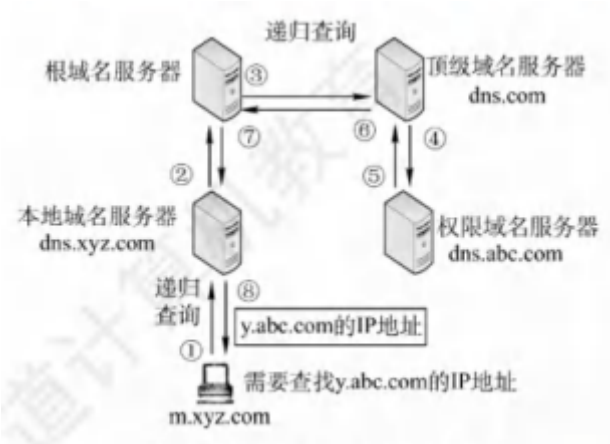
- 任何一个连接到因特网的主机或路由器都有一个唯一的层次结构名称，即域名
- 例如 www.baidu.com 中，www 为三级域名，baidu 为二级域名，com 为顶级域名，这些标号是不区分大小写的

域名服务器

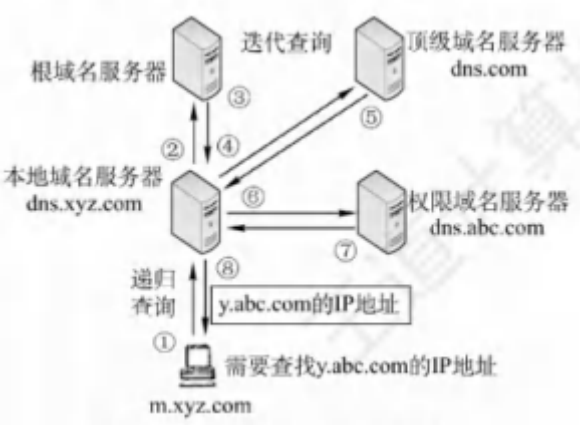
1. 根域名服务器
    - 最高层次的域名服务器，所有的根域名服务器都知道所有的顶级域名服务器和 IP 地址，是最重要的域名服务器
2. 顶级域名服务器
    - 负责管理在该顶级域名服务器注册的所有二级域名
3. 权限域名服务器
    - 每台主机都必须在权限域名服务器处登记
    - 一台主机最好至少有两个权限域名服务器
    - 许多域名服务器都同时充当本地域名服务器和权限域名服务器
4. 本地域名服务器
    - 当一台主机发出 DNS 查询请求时，查询星球保温就发送给该主机的本地域名服务器

域名解析过程

- **递归查询**
    - 主机向本地域名服务器的查询都是用递归查询
    - 递归查询是指若主机所询问的本地域名服务器所不知道被查询域名的 IP 地址，则本地域名服务器就以 DNS 客户的身份向根域名服务器继续发出查询请求报文



- **迭代查询**
    - 本地域名服务器向其他域名服务器采用递归查询或迭代查询
    - 迭代查询是指本地域名服务器只需向根域名服务器查询一次，后面几次查询都是递归在其他几个域名服务器之间进行的



文件传输协议（FTP）

1. 工作原理
   - 采用客户/服务器的工作方式，使用 TCP 可靠的传输服务
   - FTP 服务器进程由两大部分组成：主进程负责接受新的请求；若干从属进程负责处理单个请求
   - 工作流程：
     i. 打开数熟知端口 21
     ii. 等待客户进程发送连接请求
     iii. 启动从属进程处理客户进程发来的请求，从属进程对客户进程的请求处理完毕后即终止
     iv. 回到等待状态，继续接受其他客户进程的请求
2. 控制连接与数据连接
   - FTP 工作时使用两个并行的 TCP 连接：控制连接和数据连接
   - 控制连接监听 21 号端口，控制连接不用来传送文件，只传输控制信息
   - 数据连接有主动模式 PORT 和被动模式 PASV
   - PORT 模式下客户端连接到服务器的 21 号端口后客户端随机开放一个端口与服务器的 20 号端口连接
   - PASV 模式下服务器只会在本地随机开放一个端口并告知客户端可以对该端口进行数据传输

电子邮件

1. 电子邮件系统的组成结构
   - 用户代理：用户与电子邮件系统的接口
   - 邮件服务器：发送和接收邮件

- 电子邮件使用的协议：用于用户代理像邮件服务器发送邮件或在邮件服务器之间发送邮件

2. 电子邮件格式与 MIME
   - 电子邮件分为 **信封** 和 **内容** 两大部分，邮件内容又分为 **首部** 和 **主题** 两部分
   - 邮件内容的首部：
     - From：必填
     - To：必填
     - Subject：主题可选
   - 邮件内容主体为发送者想发送的内容
   - MIME（多用途因特网邮件扩展）：当发送端发送的邮件中包含有非 ASCII 数据时就用 MIME 进行转换

SMTP 和 POP3

1. SMTP（简单邮件传输协议）
   a. 连接建立：发件人的邮件发送到发送方邮件服务器的邮件缓存中后，SMTP 客户就每隔一定时间对邮件缓存扫描一次。如发现有邮件，就与接收方邮件服务器的 SMTP 服务器建立 TCP 连接，SMTP 服务器使用的熟知端口号为 25。SMTP 不使用中间的邮件服务器。TCP 连接总是在发送方和接收方这两个邮件服务器之间直接建立，而不管它们相隔多远，不管在传送过程中要经过多少个路由器。当接收方邮件服务器因 故障暂时不能建立连接时，发送方的邮件服务器只能等待一段时间后再次尝试连接
   b. 邮件传送：连接建立后，就可开始传送邮件
   c. 连接释放：邮件发送完毕后，SMTP 客户应发送 QUIT 命令。SMTP 服务器返回的信息是 221 (服务关闭),表示 SMTP 同意释放 TCP 连接。邮件传送的全部过程就此结束

2. POP3（邮局协议）
   - 有 **下载并保留** 和 **下载并删除** 两种工作方式
   - 下载并保留：用户从邮件服务器上读取邮件后邮件依然保存在邮件服务器上，用户可再次从服务器上读取该邮件
   - 下载并删除：邮件一旦被读取，就被从邮件服务器上删除

万维网（WWW）

1. 万维网的概念与组成结构
   - 万维网是一个分布式、联机式的信息存储空间。在这个空间中：，有用的事物称为资源，并由一个全域 **统一资源定位符（URL）** 标识。这些资源通过 **超文本传输协议（HTTP）** 传送给使用者，而后者通过单击链接来获取资源

- 其内核由三个标准构成：
  - 统一资源定位符（URL）
  - 超文本传输协议（HTTP）
  - 超文本标记语言（HTML）

2. 超文本传输协议（HTTP）
   - 基于 TCP 协议的应用层协议
   - HTTP 本身是无连接的，这意味着通信的双方在交换 HTTP 报文之前是不需要建立 HTTP 连接的
   - HTTP 无状态，同一客户在第二次访问同一个服务器上的页面时，服务器的响应与第一次被访问时的相同
   - 对于**非持续连接**：网页的元素对象的传输都需要单独建立一个 TCP 连接
   - 对于**持续连接**：指万维网服务器在发送响应后仍然保持这条连接，使同一个客户和该服务器可以继续在这条 TCP 连接上传送后续的 HTTP 请求报文和响应报文
3. HTTP 报文结构
   a. 请求报文
      - 方法
      - URL
      - 版本
      - Host
      - Connectioon
      - User-Agent
      - Accept-Language
      - 主体

   b. 响应报文
      - 版本
      - 状态码
      - Host
      - Connectioon
      - User-Agent
      - Accept-Language
      - 主体

4. 常见应用层协议小结

应用程序	FTP 数据连接	FTP 控制连接	TELNET	SMTP	DNS	TFTP	HTTP	POP3	SNMP
使用协议	TCP	TCP	TCP	TCP	UDP	UDP	TCP	TCP	UDP
熟知端口号	20	21	23	25	53	69	80	110	161

Jueming Liang

Sun-Yat-Sen University