中国科学技术大学

计算机网络复习

2021 年 9 月 23 日

学　　院:	信息科学技术学院
专　　业:	人工智能
课　　程:	计算机网络-2020 秋
授课老师:	洪佩琳老师

目录

0 期末考试事宜

- 考试时间：2021 年 1 月 21 日（周四）
- 考试地点：3C202
- 考试成绩占比分布：平时 20%（小测验作为平时作业计入），实验 20%，考试 60%
- 考前答疑时间：1 月 20 日（周三下午）

1 概述

1.1 Internet 的发展史

- 计算机网络

  通过同一种技术（通信线路和网络设备按某些协议/通信技术和通信协议）相互连接起来的（具有通信功能的）一组自主计算机的集合。

- 因特网

  - 起源：美国阿帕网（Advanced Research Projects Agency Network，ARPAnet ）
  - 协议：TCP/IP
  - 端系统：计算机（广义）

1.2 中国 Internet 的发展史

- 1989.9 建设中关村地区教育与科研示范网络(NCFC, The National Computing and Networking Facility of China）——中国科技网 CSTNet 前身
- 1994.5 NCFC 代表中国正式加入 Internet，向 InterNIC 注册 CN 域名
- 1994.9 中国公用计算机互联网（Chinanet）建设正式启动，96 年 1 月正式开通
- 1994.10 中国教育科研网（Cernet，China Education and Research Network) 开始启动
- 1996.9 中国金桥网（ChinaGBN) 正式开通
- 1997 Chinanet 与 CSTNet、Cernet、ChinaGBN 互连互通

1.3 IPv6 发展史

- IPv6 又叫下一代互联网协议，也缩写为 IPng（the Next Generation Internet Protocol)。
- 1996 年 3 月国际 IPv6 主干网（6bone) 建成
- 我国正式启动 “中国下一代互联网示范工程 CNGI”。建设目标是在 2003 年到 2005 年的时间内，采用 IPv6 技术，完成 CNGI 主干网

1.4 Internet 的应用

- 移动互联网

  特点：永远在线，基本实名（手机号码)，手机摄像头和 GPS 定位。

1.5 互联网与物联网

- 物联网特点

  - 物品、动物的相关属性信息来源于信息传感设备
  - 联网实体载有智能芯片，具有一定计算能力

  - 用于信息交换的互联网接入技术和传输技术：WLAN、3G、BlueTooth、ZigBee、UWB等，以及互联网
  - 高度分布和集中处理

- 物联网应用

  广泛应用于智能交通、环境保护、政府工作、公共安全、平安家居、个人健康等诸多领域

- 物联网体系结构
  - 感知层

    主要是识别物体，采集信息
  - 网络层

    网络层将感知层获取的信息进行传递和处理
  - 应用层

    与行业需求结合，实现行业智能化

1.6 网络的标准和标准化组织 ★

1.6.1 标准化的必要性及类型

- 事实标准：没有正式规划，由一些大厂商产品形成的标准。
- 法规标准：由一些权威标准化组织制定的标准。

1.6.2 国际标准界最有影响的组织

- 国际电信联盟 ITU（如 H.323，G.723.1 等）(http://www.itu.int)
- 国际标准化组织 ISO (http://www.iso.org)
- 电气电子工程师协会 IEEE（如 IEEE 802）(http://www.ieee.org)

1.6.3 Internet 的标准化组织

- Internet 工程任务组 IETF（如请求评注 RFC）(http://www.ietf.org)
- Internet 研究任务组 IRTF

1.6.4 其他组织

- 各种论坛 Forum（如 ATM Forum，http://www.atmforum.com）
- 美国国家标准协会 ANSI
- 地区标准化组织（如欧洲、日本的一些标准）

2 网络的体系结构与参考模型

2.1 网络的构成

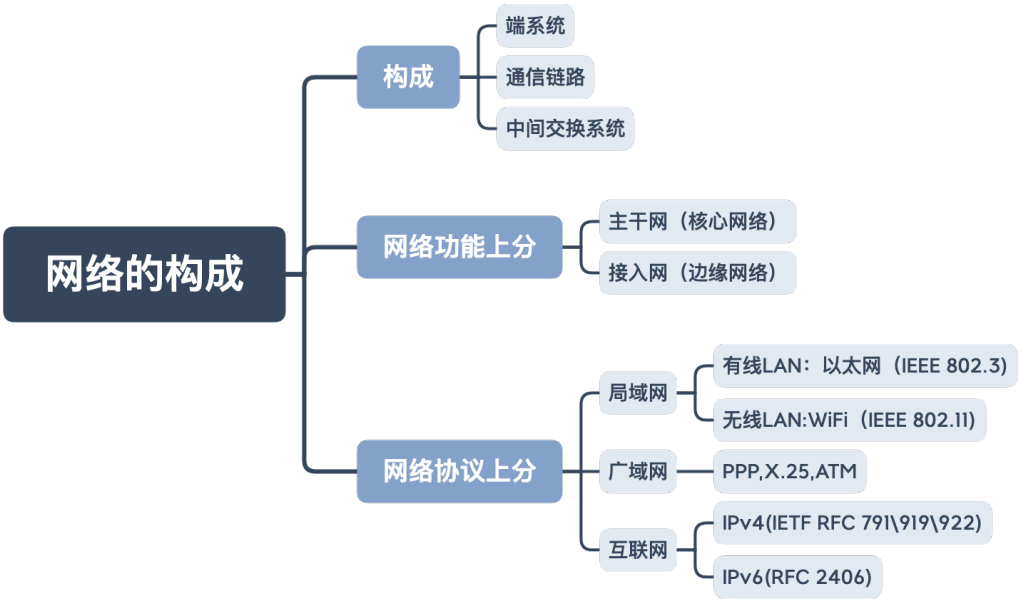


图 2.1: 网络的构成

2.2 网络的体系结构

- 网络的总体设计——层和协议的集合
  - 协议体系 (protocol architecture)
    - 网络协议：是指通信双方（或多方）关于如何进行通信的一种约定
    - 协议分层：为了降低设计的复杂度，增加网络的可扩展性，具有概念化、结构化的优点，有利于新业务的导入
  - 分层的原则
    - 将相似的功能集中在同一层内，必要时可将层的功能再分成子块，层数不宜过多，以避免层间接口的开销变大
    - 当功能差别较大时应分层处理
    - 各层只对相邻的上下层定义接口
  - 协议栈（protocol stack)：一个特定的系统所使用的一组协议（每一层一个或几个协议）
  - 参考模型的核心
    - 服务（service）
    - 接口（interface）
    - 协议（protocol）

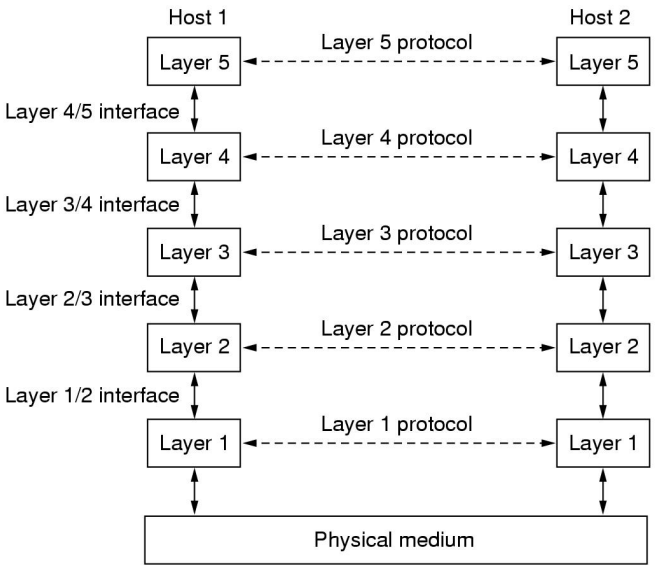


图 2.2: 层和协议的集合

相邻上下层之间都有接口，接口定义下层向上层提供的服务。

不同主机中对应的层称为对等实体（peer entity)。

第 n 层的通信规则和功能由该层的协议描述。

– 数据单元的名称与关系

  * 业务接入点 service access point
  * 数据单元的名称
    · SDU：业务数据单元
    · PDU：协议数据单元
    · PCI：协议控制信息
  * 数据单元的关系
    · N 层的 PDU=N 层 PCI+N 层 SDU
    · N 层的 SDU=N+1 层的 PDU

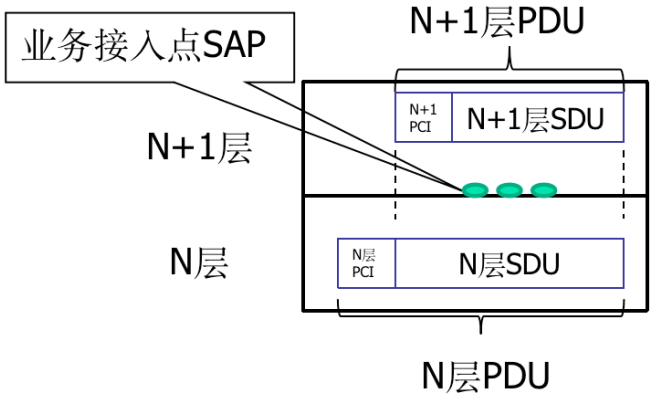


图 2.3: 数据单元的关系

- 服务
  - 面向连接的服务
    - 首先要在信源与信宿之间建立连接，然后在此连接上通信，最后拆除连接。
    - 特点：占用一定的资源，可靠，按序传送。(不同的层占用的资源不同，传输层服务会占用主机的资源，网络层或链路层会占用转发节点的资源)
  - 非连接服务
    - 传送数据前不需要建立连接，即有即送。
    - 将每个数据单元打包，在包头添加地址信息。
    - 特点：每个数据包独自寻路（重复劳动），同一数据流的包可能经由不同的路径到达目的地，到达的顺序也可能颠倒。(这是网络层或链路层服务的特点 ★)

2.3 OSI 模型 ★

- 基本术语

  国际标准化组织（International Standard Organization)

  开放系统互连（Open System Interconnection)

- ISO-OSI 模型

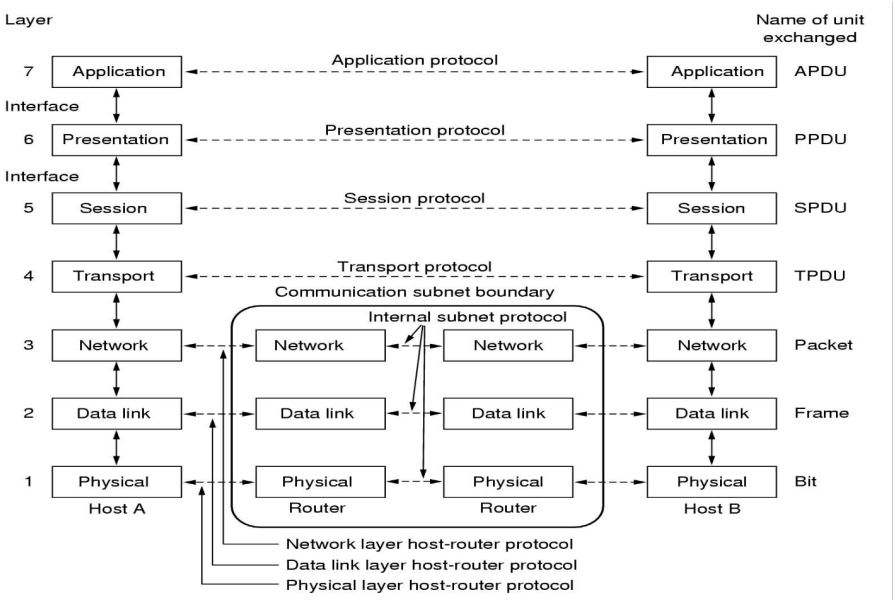


图 2.4: OSI 参考模型

- 应用层：

  处理应用进程之间所发送和接收的数据中包含的信息内容。

- 表示层：

  在两个应用层之间的传输过程中负责数据的表示语法

- 会话层：

  负责建立（或清除）在两个通信的表示层之间的通信通道，包括交互管理、同步，异常报告。

– 传输层：

为会话层提供与下面网络无关的可靠消息传送机制

– 网络层：（PDU：分组）

路由、转发，拥塞控制

– 数据链路层：（PDU：帧）

成帧，差错控制、流量控制，物理寻址，媒体访问控制

– 物理层：（PDU：Bit）

缆线，信号的编码，网络接插件的电、机械接口

2.4 TCP/IP 模型 ★

- TCP/IP 模型与 OSI 模型比较

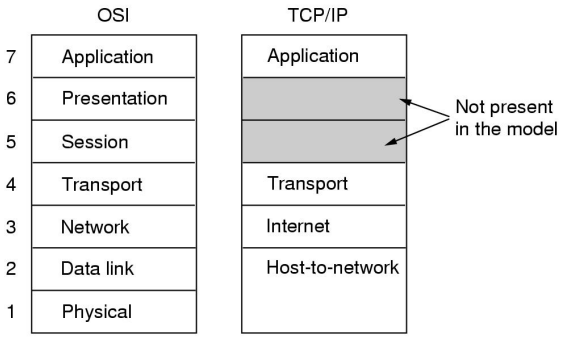


图 2.5: TCP/IP 模型与 OSI 模型比较

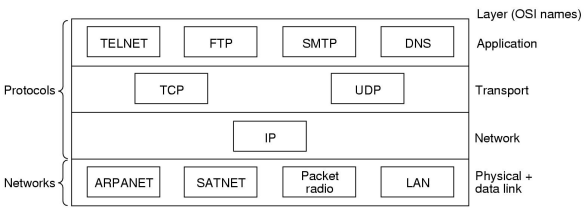


图 2.6: TCP/IP 模型

– 主机至网络层（或网络接口层），在 TCP/IP 模型中很少提及。

– 互联网层：提供非连接的分组交换功能。

– 传输层：提供可靠的面向连接的传输层协议 TCP 和不可靠的非连接传输层协议 UDP。

– 应用层：向用户提供应用服务。如 FTP，TELNET 等

- 数据的封装与拆封

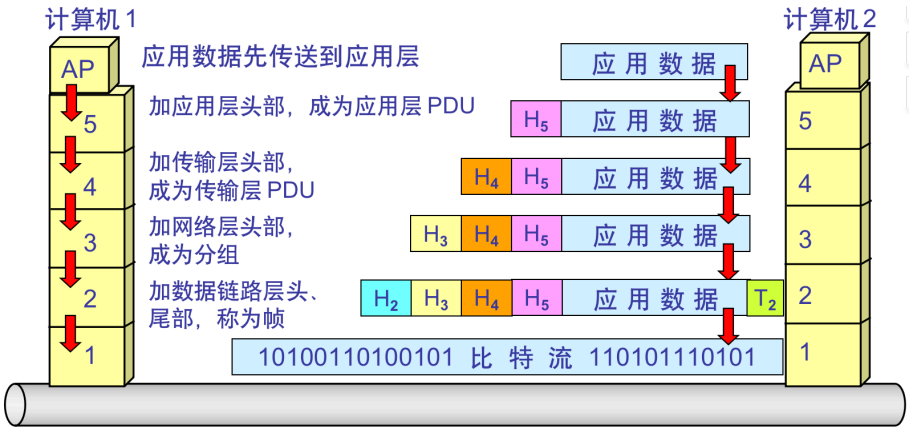


图 2.7: 数据的封装与拆封

2.5 OSI 与 TCP/IP 模型比较 ★

- 相同点：
  - 都是基于独立的协议栈概念
  - 两者都有功能相似的应用层、传输层、网络层
- 不同点：
  - 在 OSI 模型中，严格地定义了服务、接口、协议；在 TCP/IP 模型中，并没有严格区分服务、接口与协议
  - OSI 模型支持非连接和面向连接的网络层通信，但在传输层只支持面向连接的通信；TCP/IP 模型只支持非连接的网络层通信，但在传输层有支持非连接和面向连接的两种协议可供用户选择
  - TCP/IP 模型中不区分、甚至不提起物理层和数据链路层

2.6 网络的分类

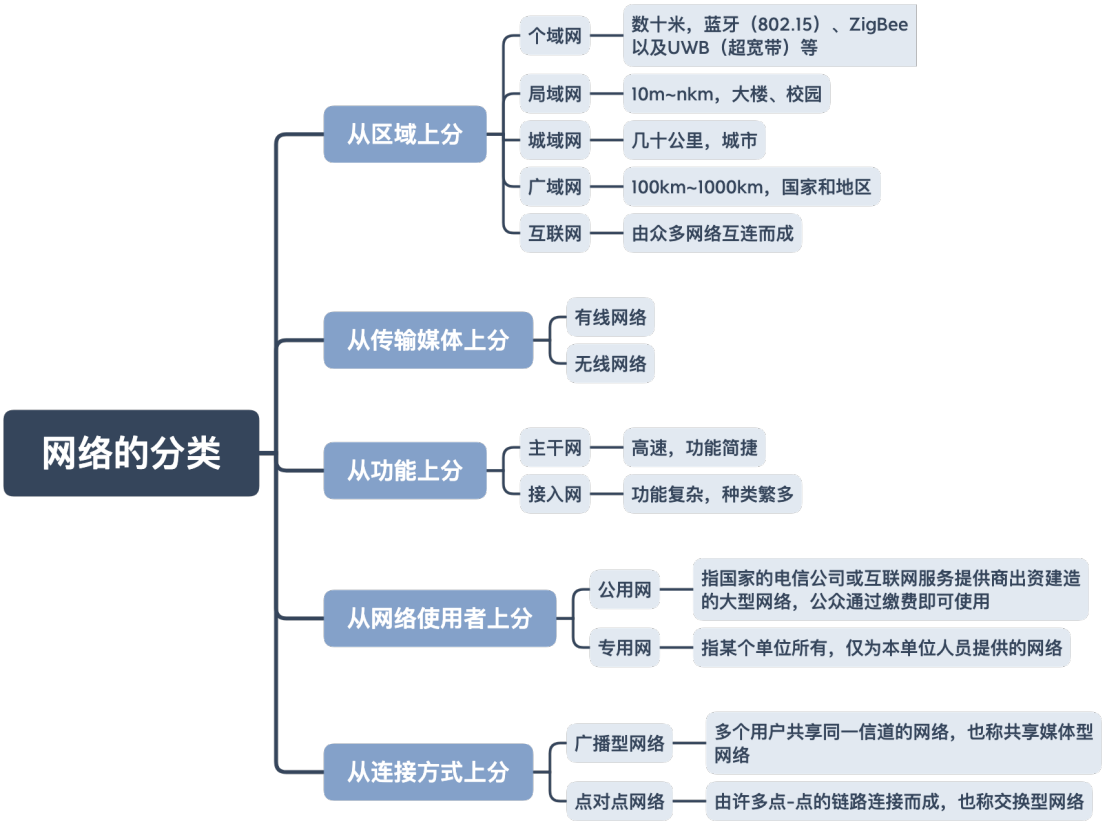


图 2.8: 网络的分类

2.7 小结

- 重点掌握 OSI 七层模型和 TCP/IP 模型，熟悉网络体系结构（层、服务、协议等基本概念）
- 思考题（部分课后习题）
  - 1. 在无连接通信和面向连接的通信两者之间，最主要的区别是什么?
  - 2.OSI 的哪一层处理以下问题：(a) 把传输的位流分成帧，(b) 在通过子网的时候决定使用哪条路由路径。

3 物理层

3.1 数据通信的理论基础 ★

- Fourier 级数

  任何正常的周期为 T 的函数 g(t) 都可以展开成 Fourier 级数:

$$g(t) = \frac{1}{2}c + \sum_{n=1}^{\infty} a_n \sin(2\pi n f t) + \sum_{n=1}^{\infty} b_n \cos(2\pi n f t)$$

- 传输速率与信道的带宽成正比（限制信道的带宽就是限制传输速率）

  – 带宽与传输速率

  1. 模拟信道的带宽以赫兹（Hz）为单位。
  2. 数字信道的带宽（传输速率）以每秒多少比特为单位（bps），有时候也以字节/秒（B/s）
  3. 假定比特率为：a 比特/秒; 则周期 T=8/a 秒;f=1/T=a/8 Hz

a	8/a	1/T	$n=f_{截}/f_1=8f_{截}/a$
bps	T(ms)	*f* 1	# harmonics
300	26.67	37.5	80
600	13.33	75.0	40
1200	6.67	150.0	20
2400	3.33	300.0	10
4800	1.67	600.0	5
9600	0.83	1200.0	2
19200	0.42	2400.0	1
38400	0.21	4800.0	0

- 信号在信道传输中的其他干扰因素

  信号的衰减、噪声、干扰等

  误比特率 = 错误比特数/传输总比特数，若误比特率 p，**帧长** n **比特，误帧率** $1-(1-p)^n$.
  设 p=10^{-4},n=1518B, **误帧率** 0.7，p=10^{-5}, **误帧率** 0.11，p=10^{-10}, **误帧率** 0.0000012.

- **信道的最大传输速率**

  – Nyquist **定理（有限带宽的无噪声信道）**

  如果一个任意的信号通过带宽为 B **的低通滤波器，那么每秒采样** 2B **次就能完整地重现通过该滤波器的信号。**

  最大数据传输率 =$2Blog_2V$（b/s）

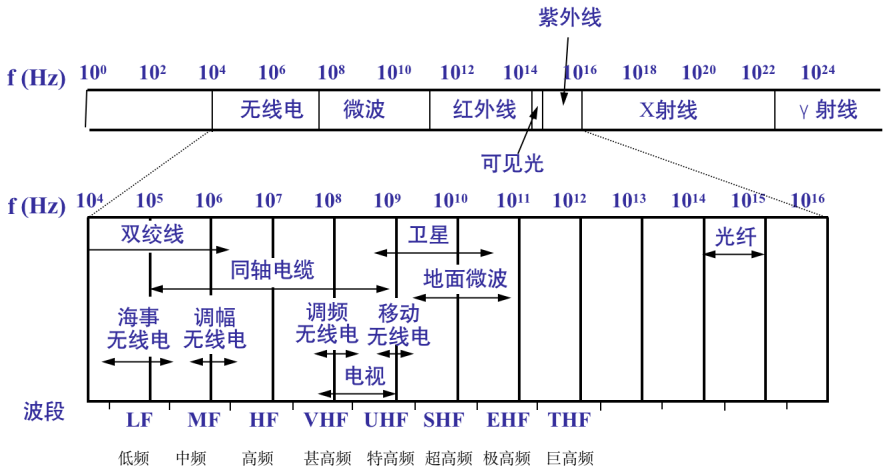
  – Shannon **定理**

  对任何带宽为 B Hz，**信噪比为** S/N **的信道，最大数据传输速率** =B log_2（1+S/N）b/s）
  信道的带宽或信道中的信噪比越大，则信息的极限传输速率就越高
  通常信噪比表示形式 $10log_{10}S/N$，**以分贝（**dB**）为单位，**20 **分贝的信噪比** S/N=100

3.2 传输介质

分为导向型和非导向型传输介质，导向型传输介质为：双绞线、同轴电缆、电力线、光纤；非导向型传输介质：无线传输。

- 电磁波的频谱



- 双绞线 TP(Twisted Pair)

  由两条相互绝缘的铜线组成，其典型粗细约 1mm，两条象螺纹一样绞在一起。

  - Shielded Twisted Pair(STP) 屏蔽双绞线
  - Unshielded Twisted Pair(UTP) 无屏蔽双绞线

  双绞线的传输距离一般为 100M，既可传输模拟信号，也可传输数字信号。

- 同轴电缆

  基带同轴电缆（Baseband Coax）：阻抗匹配为 50Ω，用于数字传输，1 公里电缆可达 1 2Gbps 的传输速率。又分为：

  - 粗缆（Thick）：如 10Base-5，单段长度不超过 500 米，最长 5 段达 2.5 公里。
  - 细缆（Thin）：如 10Base-2，单段长度不超过 185 米，最长 5 段达 925 米。

  宽带同轴电缆（Broadband Coax）：阻抗匹配为 75Ω，用于电视信号的模拟传输（CATV），带宽可达 800MHz 以上，采用 FDM 技术。传输数字信号时，要使用 Cable MODEM 这样的特殊设备，现在综合有线电视网络已成为 MAN 的一种形式。

- 电力线

  PLC（power line communication），用电力线作为信号的传输媒介，通过载波方式来传输模拟或数字信号的技术。

  自 20 世纪 50 年代起，电力线通信技术开始应用于中压和低压电网上，主要面向电力行业的运用，包括电力线自动抄表、电网负载控制和供电管理等。特点：

  - 用户数目最多，不用去重新铺设专用线路

  - 负载阻抗呈现随机性的特点，造成电力线载波通信的收、发信机的输出阻抗与输入阻抗很难和线路的阻抗相匹配，信号在传输过程中衰减很严重。电力线网络的拓扑具有时变性。

- 光纤

  光纤由传导光波的高纯石英玻璃纤维和保护层（jacket）构成，其中纤芯（core）的折射率大于包裹着它的包层（cladding）折射率，这样光信号就被保持在纤芯中不会散播出去。

  经常将多根光纤封装在坚固的外壳（sheath）中，形成所谓的多芯光缆。

  - 光发射系统：光源、传输介质、检测器
  - 有两种光源可用于信号源：LED（发光二极管）和 ILD（注入型激光二极管）。以光信号的有和无来表示二进制的“1”和“0”。
  - 接收端由光电二极管构成的光检测器将光信号转换成电信号。
  - 光纤的连接：机械式、熔结。
  - 光纤的类型：多模光纤、单模光纤

- 无线传输

  无线传输所使用的频段很广。低频 LF、中频 MF 波段电波沿地表传播，高频 HF 和甚高频 VHF 波段的地表电波会被地球吸收，但可通过地球上空的电离层反射实现长距离传播。微波在空间主要是直线传播。

  - 微波传输

    在 300MHz 以上，微波通过抛物状天线把能量集中于一小束，具有极高的信噪比，沿直线实现可视距传输。

    在地面因地表弯曲，需中继站接续微波信号，100 米高的塔可接续约 80 公里。

    天气和频率的影响可造成多路减弱。

    开放的波段：2.4 GHz 2.484 GHz，**即工业/科学/医学波段**。
  - 红外线与毫米波

    有方向性，便宜，穿透能力差，传输距离短。
  - 光通信

    激光通信，波束窄，需要对准，受天气（风和温度）干扰大
  - 低轨卫星

    铱星:66 颗，卫星高度 750km，采用圆形极地轨道，上下行链路运行在 L 波段（1.6GHz）

3.3 数字调制与多路复用

- 数字调制

  调制是对信号源进行处理，使其变为适合传输形式的过程。即把基带信号变为一个相对基带频率而言频率非常高的通带信号。通带信号叫做已调信号，而基带信号叫做调制信号。

  数字调制就是把要发送的数字信号转换到适合于传输的通带模拟信号的过程。

  由于基带（baseband）信号在长距离的传输信道上会受到衰减、畸变及噪音等的影响，因此在发送端必须转换成一种适合于在信道上传输的信道信号，这个转换过程就叫调制（modulation）。在接收端的相反转换过程称为解调（demodulation）

调制解调器（MODEM）就是调制器（MOdulator）和解调器（DEModulator）的组合

基带传输

- 不归零码（NRZ）: 数字信号的最直接表示是用正负电压分别表示二进制的 0、1 值
- 曼彻斯特编码: 每一比特的中央有一变迁，可用做时钟，由高到低为 “1”，由低到高为 “0”，相当于时钟信号与比特流的异或
- 不归零逆转: 信号有跳变表示 1，无跳变表示 0

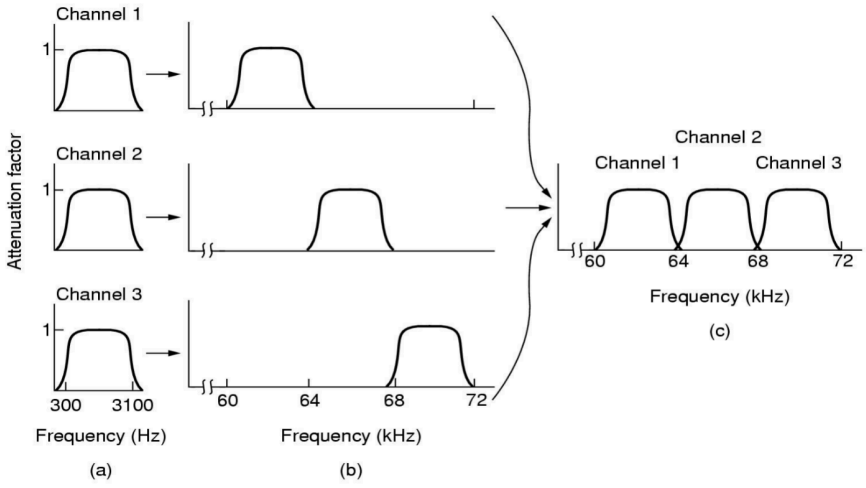
通带传输

- 幅度调制，AM；幅移键控，ASK
  载波的振幅随基带数字信号而变化
- 频率调制，FM；频移键控，FSK
  载波的频率随基带数字信号而变化
- 相位调制，PM；相移键控，PSK
  为了提高传输速率，采用更为复杂的调制技术, 如载波的初始相位随基带数字信号而变化，有 BPSK、QPSK，QAM

- 多路复用

  多路复用是指多个用户共享一条信道的一种机制。多路复用有频分多路复用（FDMA），时分多路复用（TDMA），码分多路复用（CDMA）几种

  - 频分复用



    数字传输中不同速率信号的变化：在时间轴上信号的宽度随带宽的增大而变窄

  - 时分复用

    基于时隙, 可能会造成线路资源的浪费;

    统计时分复用 STDM;

    一次群速度 T1: 1.544 Mbps；E1: 2.048Mbps

    二次群速率 T2: 6.312 Mbps；E2: 8.848Mbps

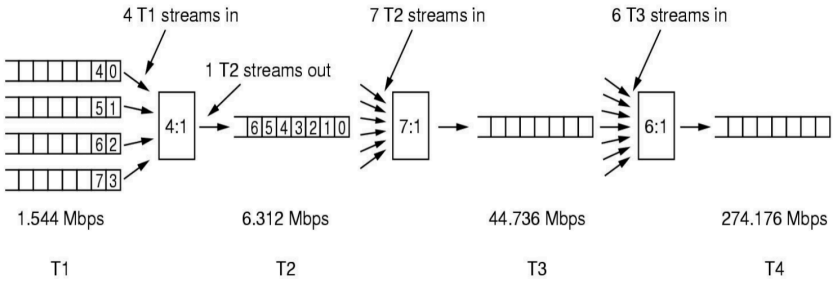


图 3.1: T 系列的群路复用

三次群速率 T3: 44.736Mbps；E3: 34.304Mbps

四次群速率 T4: 274.176Mbps；E4: 139.264Mbps

数字传输网的传输技术体制

* 数字传输网上传输的信号一般都是经过 TDM 以后形成的数字信号的群路信号
* 两类速率等级信号

  PDH（Plesiochronous Digital Hierarchy，准同步数字系列）:

  复接成群路信号的各支路信号的时钟频率有一定的偏差，复接时通过在各支路信号中插入一定数量的脉冲来实现各支路的同步。主要有北美的 T 系列和欧洲的 E 系列这两个互不兼容的标准。

  SDH（Synchronous Digital Hierarchy，同步数字系列）:

  1985 年美国贝尔通信研究所提出，称之为 SONET（Synchronous Optical NETwork，同步光网络），1986 年成为美国数字体系的新标准。CCITT 于 1988 年接受 SONET 概念，并与 ANSI 达成协议，将 SONET 修改后重新命名为 SDH

  SDH 拥有全世界统一的网络节点接口（NNI），是真正的数字传输体制上的国际标准。SDH 有一套开放的标准化光接口，因而使现有 PDH 中的两大标准得以兼容，可以很方便地在光路上实现互通，使信号传输、复用和交换过程得到简化，大大降低了联网成本。

  SONET/SDH **的速率及复用**

  SONET 的基本帧:

  是每 125 µs 内传输 810 个字节（用 90 列 × 9 行描述），因此数据速率 = 8 bit × 810 Byte × 8000 Hz = 51.84 Mbps，这是 SONET 最基本的信道，称作同步传输信号 STS-1

  3 条 STS-1 支流被合成为 1 条 3 × 51.84 Mbps = 155.52 Mbps 的 STS-3 流。对应于 STS-n 的光纤线路被称作 OC-n

  SDH 的基本帧:

  从 OC-3 155.52Mbps 开始，称作同步传输模块 STM-1

  OC-n 表示由 n 条单独的 OC-1 线路组成。

SDH等级		SONET等级	标准速率 (Mbps)
		OC-1/STS-1 （480 CH）	51.8400
155 M	STM-1 （1920 CH）	OC-3/STS-3 （1440 CH）	155.520
	STM-3	OC-9/STS-9	466.560
622 M	STM-4 （7696 CH）	OC-12/STS-12 （8046 CH）	622.080
	STM-6	OC-18/STS-18	933.120
	STM-8	OC-24/STS-24	1244.160
	STM-12	OC-36/STS-36	1866.240
2.5 G	STM-16 （30720 CH）	OC-48/STS-48 （32356 CH）	2488.320
10 G	STM-64 （122880 CH）	OC-192/STS-192 （129024 CH）	9953.280

图 3.2: SONET/SDH 的速率等级

* 波分复用

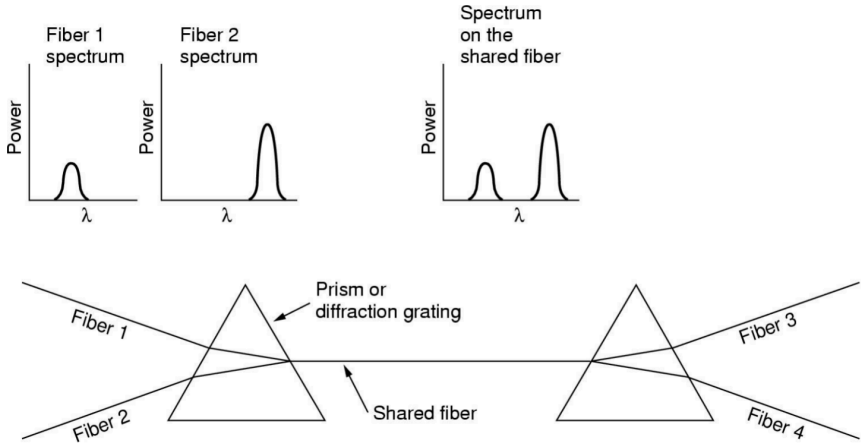


图 3.3: 波分复用

* 码分复用
  - 码分复用是扩频通信的一种形式，常用的名词是码分多址 CDMA (Code Division Multiple Access)
  - 每一个比特时间划分为 m 个短的间隔，称为码片
  - 各用户使用经过特殊挑选的彼此正交的码型，因此不会造成干扰
  - 例如，采用双极符号把码片序列写成-1,+1 的序列组合，设 m=8，A 站分配得到的码片序列为
    (-1 -1 -1 +1 +1 -1 +1+1)，若 A 站发送的是该序列，则表示发出的是“1”比特，若发送的是
    (+1 +1 +1 -1 -1 +1 -1 -1)，则表示发送的是“0”
  - 码片序列的正交关系
    令向量 S 表示站 S 的码片向量，令 T 表示其他任何站的码片向量。
    两个不同站的码片序列正交，就是向量 S 和 T 的规格化内积 (inner product) 都

是 0。

$$\mathbf{S} \bullet \mathbf{T} \equiv \frac{1}{m} \sum_{i=1}^{m} S_i T_i = 0$$

$$\mathbf{S} \bullet \mathbf{S} \equiv \frac{1}{m} \sum_{i=1}^{m} S_i S_i = 1$$

· CDMA 的工作原理

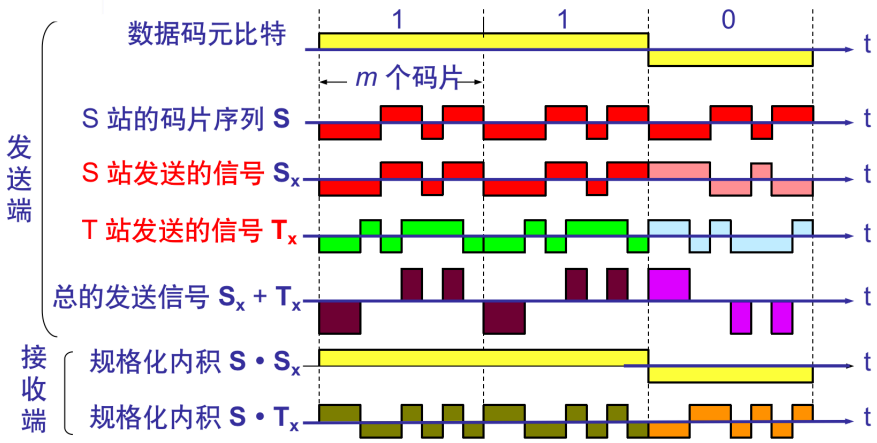


图 3.4: CDMA 的工作原理

3.4 交换技术 ★

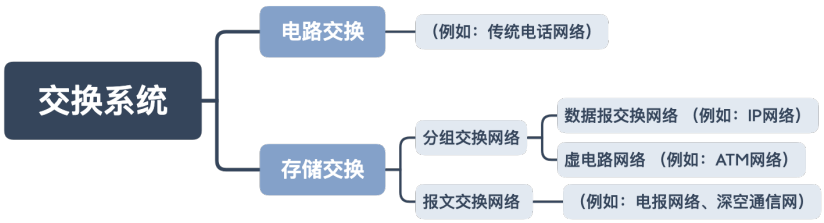


图 3.5: 交换系统的构成

- 电路交换

  在通信对端之间建立物理连接，通信期间一直维持着，通信双方专用，直到通信结束

  数据传输的唯一延时是电磁波的传播时间

  电路交换的优点是传输可靠，迅速，不丢失而又保序

- 存储交换

  – 报文交换

  数据传输以报文的整体为单位，即端点系统一次性发送数据块，长度不限且可变

  – 分组交换 ★

  将报文划分成若干个可以存放在内存中的分组来进行传送

* 数据报交换：无连接的分组交换
* 虚电路交换：面向连接的分组交换

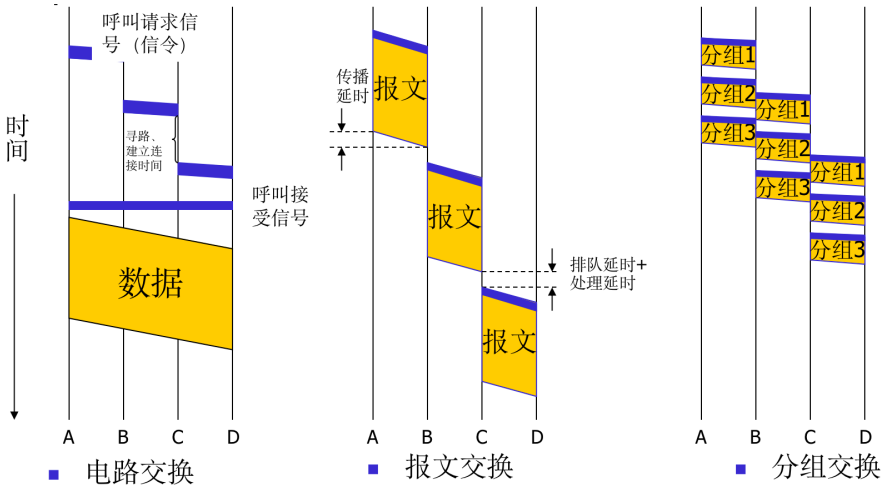


图 3.6: 三种交换技术的时序图

- 分组交换中的延时分析 ★
  - 传播延时

    取决于物理媒体传播速度和两点间距离
  - 传输延时

    节点发送（或接受）整个分组所需时间，用 L 比特表示分组长度，用 Rb/s 表示链路速率，则 L/R 为传输延时
  - 处理延时

    检查分组头部，寻路，差错校验等，与 CPU 速度和处理算法有关
  - 排队延时

    在节点上等待处理所需时间，与网络拥塞状况有关

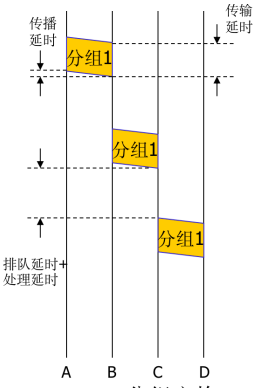


图 3.7: 分组交换

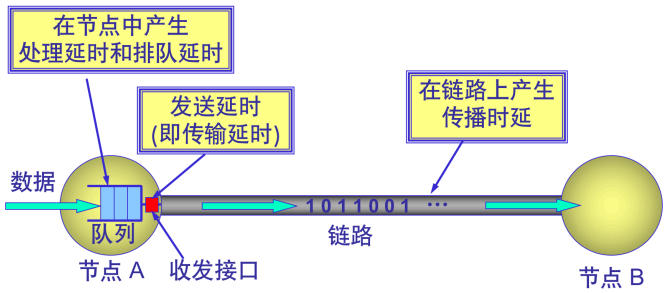


图 3.8: 分组交换的延时分析

  - 分组交换的总延时

    一个分组在路径上的总延时:

D= 总 d_{prop}+ 转发节点数 * $(d_{trans} + d_{pro} + d_{queue})$ +d_{trans}

n 个分组在路径上的总延时:

D= 总 d_{prop}+ 转发节点数 * $(d_{trans} + d_{pro} + d_{queue})$ +n*d_{trans}

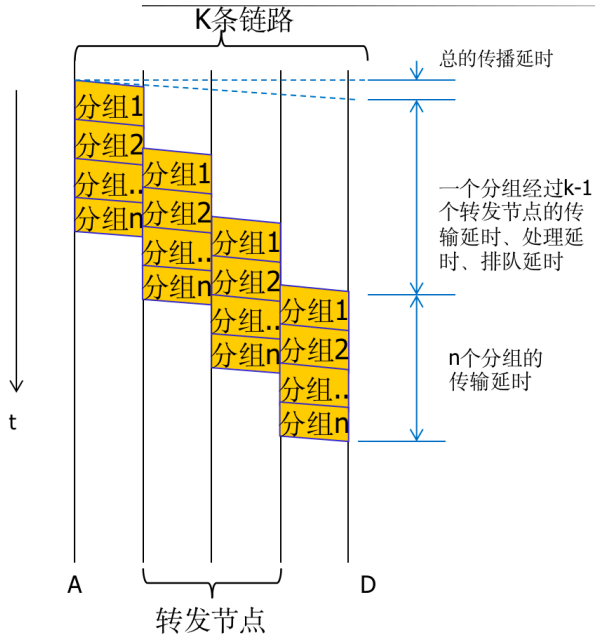


图 3.9: 分组交换的总延时

– 电路交换与分组交换的比较 ★

电路交换与分组交换的比较

	电路交换	分组交换
带宽	预先静态地保留所要带宽	根据需要动态地获得和释放带宽
带宽的浪费	已分配给线路上未用的带宽只能浪费掉	未用的带宽可以被别的传输所利用
数据传输	对数据传输是完全透明的	利用分组所携带的参数进行路由转发
传输延时	连续的通过物理线路传输	存储转发，会增加传输延时
保序	不会发生乱序现象	可能不按原顺序
计费方式	按时间、距离计费	按传输的字节或连接时间计费

图 3.10: 电路交换与分组交换的比较

4 数据链路层

4.1 数据链路层的基本概念与功能 ★

- 数据链路层的基本概念

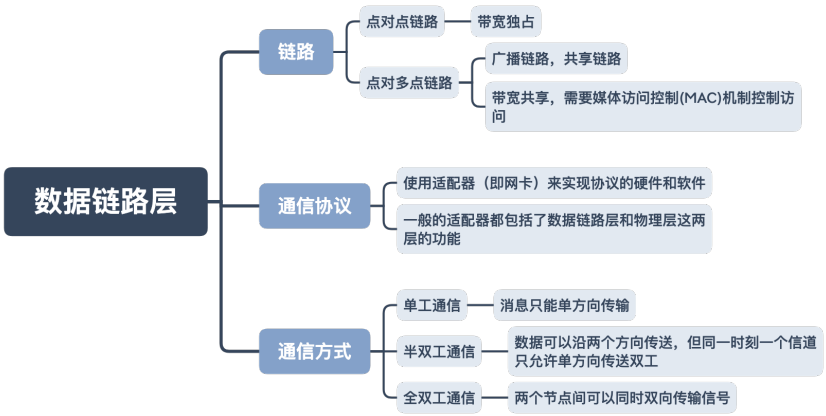


图 4.1: 数据链路层的基本概念

帧：在两个对等的数据链路层之间画出一个数字管道，这条数字管道上传输的数据单位就是帧

- 数据链路层的功能
  - 向网络层提供良好的服务接口
    - 无确认、无连接的服务
    - 有确认、无连接的服务
    - 面向连接的服务
  - 将物理层的比特流编成帧
    - 成帧 (framing)
      识别或表示一个帧的起始和结尾
    - 字符计数
      每一个帧的头上描述帧的长度
      缺点：帧头出错不光影响本数据帧，还影响后续的帧
    - 字符填充的标志字节法
      字符填充的标志字节法
    - 位标志
      用特殊的位序列表示帧的起始和结尾;
      ★ 为了避免起始、结尾标志与帧中的数据混淆，发送端的数据链路层在检测到数据比特流中有连续 5 个 1 出现时，就在其后加一个 0，接收端的数据链路层在将 5 个 1 后面的 0 取走还原
    - 物理层编码
      在物理层用 1.5 或 2 个物理位表示一个数据位来表示帧的起始与结尾

- 差错控制

  在有确认的服务中，接收方需要对收到的数据帧进行确认，通常以返回特别控制帧来告诉发送方收到的数据有没有出错

  对于端到端的确认还可以通过返回的数据帧中的某些位来捎带地进行确认

  如果发送的数据丢失，可以通过在发送端引入计数器，进行超时重发。为了避免相同的帧收到多次，需要对帧进行编号

- 流量控制

  当发送端的发送速度大于接收端的接收速度，或发送端所在的网络传输速率大于接收端所在的网络传输速率时，就需要流量控制

  窗口机制:

  在任意时刻，发送方发出 n 帧，其中有 l 帧已得到确认。而同一时刻，接收方收到并应答了 m 帧，显然 l<=m <=n，等待确认的帧的数目不允许超过 W，即 n-l <=W，该 W 就是窗口

4.2 差错检测与校正 ★

- 纠错码
  - 定义

    一帧由 m 个数据位（即报文）和 r 个冗余位（即校验位）组成，设总长度为 n（n=m+r），此长度为 n 的单元常称为 n 位码字
  - 海明距离

    两个码字对应位上不相同位的数目，例如，10001001 与 10110001 它们的海明距离为 3
  - n 位码字的集合，只有 2m 个码字是有效的
  - 码字集合的海明距离

    码字集合中任意两个有效码字间的最小海明距离，便是该集合的海明距离
  - 编码的检错和纠错能力

    取决于编码后码字的海明距离的大小

    为了检测出 d 个比特的错，需要使用距离为 d+1 的编码

    为了纠正 d 个比特的错，必须用距离为 2d+1 的编码
  - 纠正单比特错的校验位下界

    m 个信息位和 r 个校验位,n=m+r

    纠正单比特误码的校验位下界:2^r>=n+1
  - 海明编码

    编号为 2 的幂的位是校验位（如第 1，2，4，8…），其余为信息位

    校验位:

    1:（3，5，7，9，11）

    2:（3，6，7，10，11）

    4:（5，6，7）

    8:（9，10，11）

    能纠正单比特错: 在接收方，如果校验位 1 不满足偶校验，而其他校验位都满足，则第 1 位出错

- 检错码

  在多数通信中采用检错编码，但在单工信道中需要纠错编码

  - 改进的奇偶校验

    对数据位组成一个 L 位宽，K 位高的长方形距阵来发送，然后对每一列单独计算奇偶位，并附在最后一行作为冗余位

    差错检测能力分析：

    1. 该方法可以检测所有长度为 L 的突发性错误。
    2. 当出现错误长度大于 L 时，假设 L 列中任意一列检测出错的概率为 1/2，那么，整个数据块的错判率（实际出错却判为正确的概率）为 $(1/2)^L$
    3. 该方法用在 ICMP 报头检验中

  - 多项式编码（循环冗余码 CRC）★

    给定一个 m 比特的帧或报文，发送方生成 r 比特的序列（也称为帧检验序列 FCS，Frame Check Series），形成（m+r）的码字，该码字能被某个事先确定的数整除。接收方用相同的数去除收到的帧，如果无余数，则认为数据帧无差错

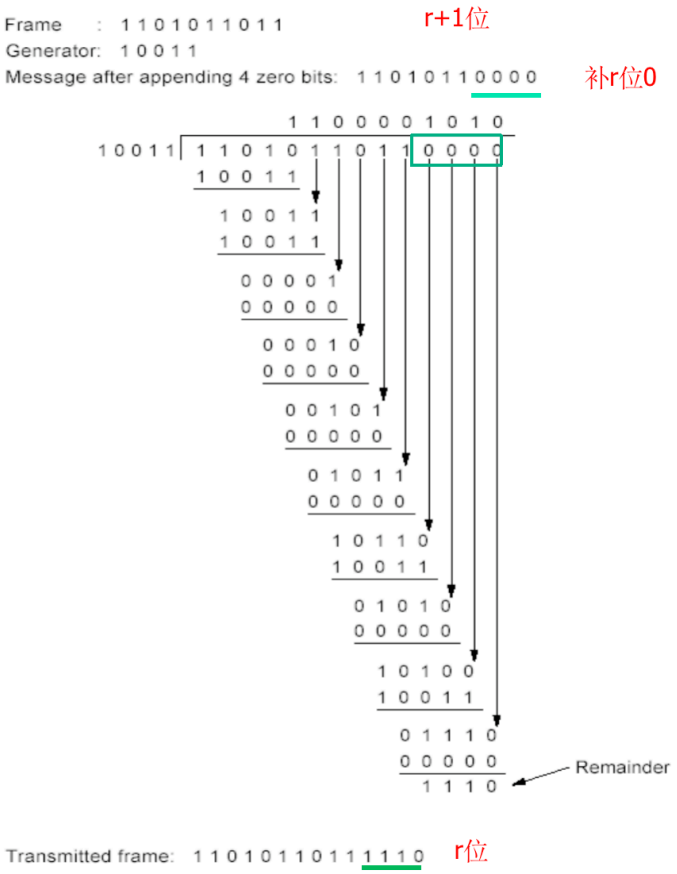


图 4.2: CRC 校验确定余数

★CRC 的检测能力分析

1. 能检验出所有长度小于等于 r 的错误（即检测率 100%）
2. 如果突发长度为 r+1，当且仅当差错与 G（X）相同时才被整除。根据突发错误长度的

定义，其第 1 位和最后 1 位必须是 1，因此与 G（X）完全相同的概率为 $(1/2)^{(r-1)}$。(检测率 $1-(1/2)^{(r-1)}$)

3. 对于长度大于 r+1 的差错，其错判率为 $1/2^r$。(检测率 $1-1/2^r$)

4.3 基本数据链路协议

- 一种无限制的单工协议
  - 完全理想的条件
    - 数据单向传输，收发双方的网络层一直处于就绪状态，
    - 处理时间可忽略不计，接收缓冲空间无限大（无需任何流量控制）
    - 信道不会损坏或丢失帧（无需任何差错控制）
  - 发送端无限循环地重复三个动作
    - 从网络层取分组。
    - 构造帧。
    - 发出帧。
  - 接收端也是无限循环地重复三个动作
    - 等待事件（唯一的未损坏帧的到达）发生。
    - 帧到达后，从硬件缓冲中取出新到的帧。
    - 将帧的数据部分传给网络层。
  - 只需成帧处理，无需做其它任何处理
- 无错信道的停-等协议
  - 条件基本同协议 1，

    修改：接收端需要一定的接收处理时间，接收缓冲只能存放一个帧。
  - 为了防止发送快于接收而造成数据丢失，发送端发送一帧后必须停止发送，等待接收端发回的反馈确认；
  - 接收端在收到一个帧并发送网络层后，需向发送端发一反馈确认短帧，表示可发新帧。
  - 由于需要反馈，且帧的发送和反馈是严格交替进行的，所以相当于采用半双工信道。
- 有噪音信道所涉及的问题
  - 考虑实际有噪信道，帧既可能损坏（接收端可通过校验检查出错误），也可能完全丢失。
  - 由于帧会丢失，发送端可能收不到反馈的确认帧，因此发送端必须引入超时机制（time out），即增加一个定时计数器，在一定时间后对没有确认的帧进行重发，也称作 ARQ (Automatic Retransmit reQuest)。

    时间值应选择稍大于两倍端到端的信号传播时间和接收端的接收处理时间之和。
  - 由于帧会丢失（假如确认帧丢失），为避免接收端收取重复的数据帧，必须通过为帧编制序号来解决重复帧的问题。

    帧的序号位数应尽量的短从而少占用帧头的空间,在简单停-等协议中只需 1 个比特位(“0” → “1”，“1” → “0”）即可

- 有噪音信道的停-等协议
  - ACKn 表示“第 n –1 号帧已经收到，现在期望接收第 n 号帧”
  - 发送端帧序号 N(S) 表示当前所发帧的序号，接收端维护的帧序号 N(R) 表示接收端当前所期待接收的帧序号。
  - 发送端从网络层取得第一个分组组帧，将 N(S)=0 的序号放入帧头中作为第一个帧发送，并启动定时计数器，等待响应帧。
  - 接收端收到一个帧后，对其序号和 N(R) 进行比较：

    若相等则对其接收，校验正确后送交网络层，将 N(R) 加 1（模 2 运算）并放入确认帧中反馈回发送端；若校验出错，则丢弃错帧，保持 N(R) 不变并放入确认帧中反馈回发送端。

    若不等，则将其作为重复帧丢弃；N（R）值不变，反馈确认帧。
  - 发送端若在规定的时间内没有收到接收端的反馈确认帧（超时），就认为数据帧丢失，在保持 N(S) 不变的情况下重新发送缓冲器中的（旧）帧；
  - 发送端若接收到确认帧后，比较确认帧中的序号和 N(S)：

    若不等，则将确认帧中的序号赋予 N(S)，从网络层获取新的分组并组成新帧（N(S) 作为序号放入帧头中）交由物理层发送出去。

    若相等，则保持 N(S) 不变，重新发送缓冲器中的（旧）帧。

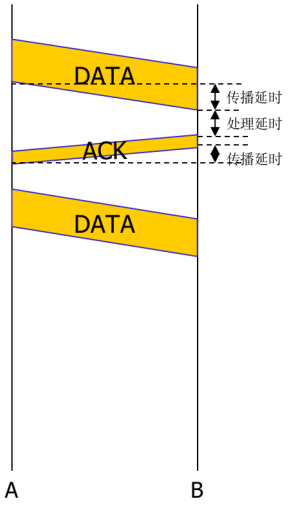


图 4.3: 无错停等

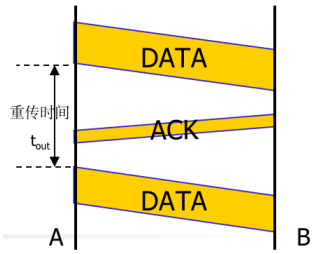


图 4.4: 有噪重传

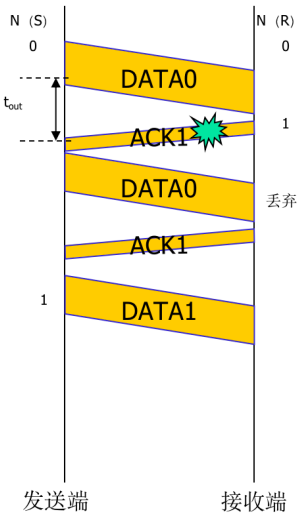


图 4.5: 有噪停等

- 停-等协议对信道利用率的影响
  - 在时延大的信道（如卫星通信）中，停-等协议的效率是很低的。
  - 考虑卫星通信，典型的传播时间约为 270ms。假设一个帧的发送时间为 20ms，则从发送站开始发送算起，经 20ms+ 270ms=290ms，数据帧才能到达目的站。假设不考虑目的站的处理时间，且认为确认帧非常短，其发送时间可忽略不计，则又需 270ms 确认帧才能被发送站收到。因此信道的利用率为：20ms/(290ms+270ms)=1/28，非常低。
  - 为了提高传输效率，可以设想让发送站连续不断地发送数据帧，当发完第 28 个帧数据后，恰好第 1 帧的确认帧到达，根据确认可紧接着发第 29 帧或重发第 1 帧。以后，每过 20ms（发一个帧）就有一个确认帧到达，这样信道的利用率就大大地提高了。

- 允许发送站连续发送多个帧而不需等待确认的做法称作管道化（pipelining），属于一种窗口（windows）机制。

- **延迟 * 带宽乘积**
  - 单向延迟 × 带宽——带宽延迟乘积：BD（单位：比特/字节/帧）

    第一个比特到达接收端之前，发送者能发送的比特数，是一个有用的链路性能参数，表示该管道的容量。
  - 往返延迟 × 带宽：2BD
    * 假设发送窗口为 W，它是发送端在接收到接收端给出的确认之前能够发送的帧（或字节，比特）数。
    * 若要链路利用率 100%，则 W=2BD+1（**单位：帧，注意，这里的** BD **单位要换成帧**），
    * 链路利用率 ≤W/(1+2BD)，注意，这里的 +1 是因为必须接收完整帧后确认帧才会被发出，所以 W 和 BD 的单位也应该是帧。该值是上限，因为没有考虑处理时间。

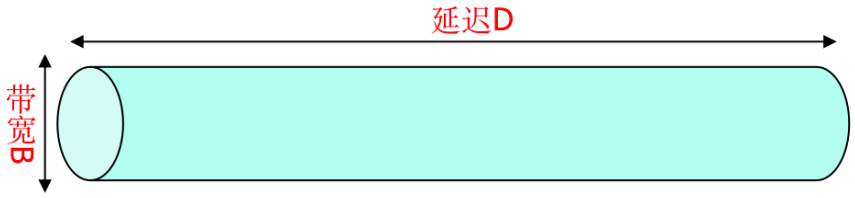


图 4.6: 延迟 * 带宽

4.4 滑动窗口协议 ★

- 滑动窗口协议是一种非常可靠、适用于各种条件的通用流量控制协议，特别是在效率、复杂性及对缓冲区的需求等方面可作灵活调配。
- 发送端和接收端分别设定发送窗口和接收窗口。
- 发送窗口用来对发送端进行流量控制。
- 主要的滑动窗口协议有回退 N 协议（go-back-n，出错全部重发）和选择重发协议，停-等协议是窗口大小为 1 的滑动窗。
- 帧序号用 n 位编码，范围为 0-2^n-1

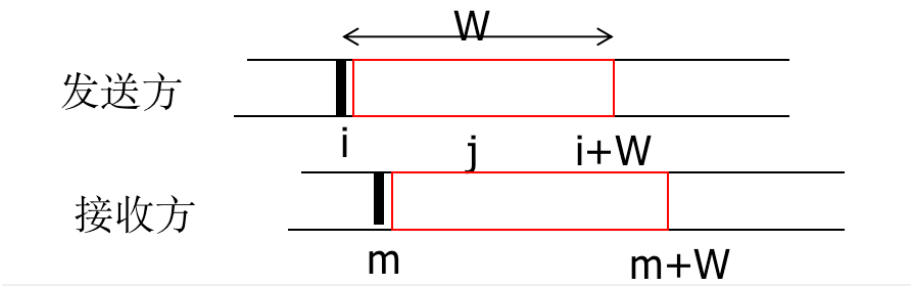


图 4.7: 发送方和接收方

- 发送窗口
  - 发送窗口就是发送端允许不等确认而连续发送的帧的序号表。
  - 允许连续发送的帧的数量称为发送窗口尺寸，表示为 W_T。发送端必须有 W_T 个输出缓冲区来存放 W_T 个数据帧的副本以备数据帧的重发。
  - 当发送端收到发送窗口下沿帧的肯定确认时，将发送窗口整体向前滑动一个序号，并从输出缓冲区中将相应的数据帧副本删除。

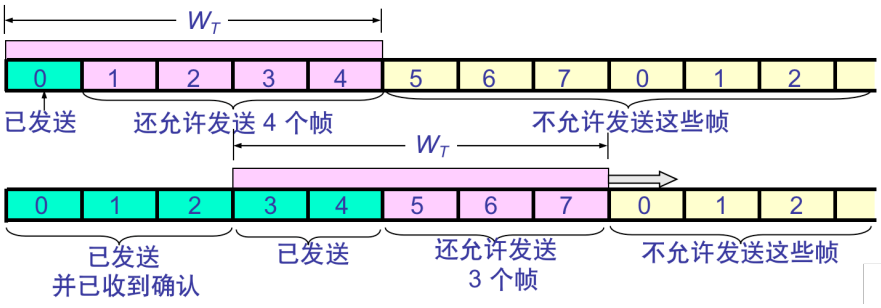


图 4.8: 发送方

- 接收窗口
  - 接收窗口是接收端允许接收的帧的序号表。
  - 允许接收的帧的数量称为接收窗口尺寸 W_R。同样接收端也必须设置相应数量的缓冲区来支持接收窗口。
  - 对接收端收到的帧的序号落在接收窗口外的帧被直接丢弃。只有落在接收窗口内的帧才会被接收端进行校验处理，若校验正确：

    当接收的帧不是接收窗口下沿帧时，必须暂存在输入缓冲区。

    当接收到接收窗口下沿帧时，会将其连同后面连续的若干个检验过的正确帧按顺序交给网络层，在发回确认帧的同时将接收窗口向前滑动相应的数量。

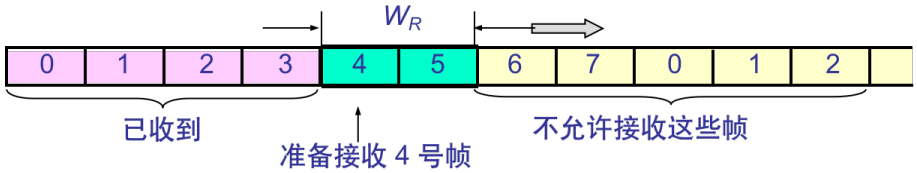


图 4.9: 接收方

- 数据的捎带确认
  - 在实际通信中，通常收发双方都相互发送数据。
  - 为了提高效率，可以将确认信息放在数据帧中作为一个控制字段连同数据一起发送给对方，这种方式称为捎带应答（piggybacking）。
  - 当一方收到对方的数据帧后：

    若正好也有数据需发给对方，则立即可使用捎带应答。

若暂时没有数据需发给对方或数据还未准备好，则等待一定的时间，如果在该时间内准备好了数据，则可以使用捎带应答。如果未准备好，为了防止对方等待时间过长而超时重发，必须立即发送一个单独的确认帧。

– 使用捎带应答就不用对每一个帧都作确认，可以用对下一帧的期待来代替对该帧之前的所有帧的确认 (累计确认)。

- 回退 N 协议和选择重发协议

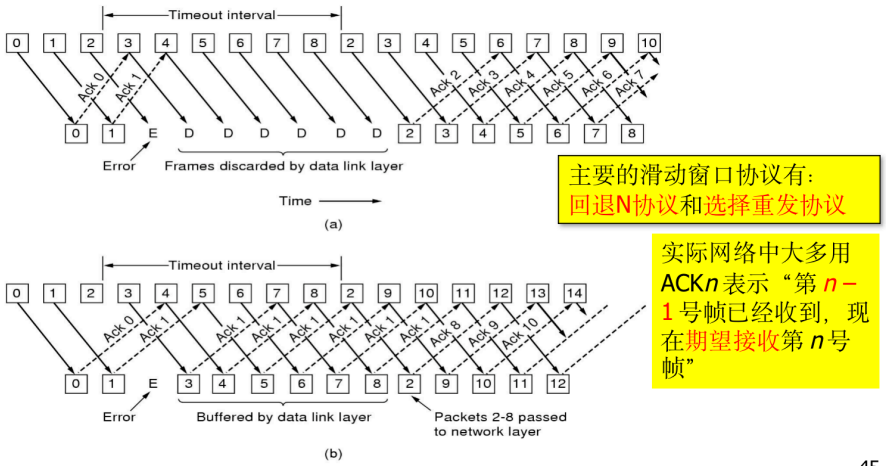


图 4.10: 回退 N 协议和选择重发协议

– 回退 N 协议（go-back-n）

  * 回退 N 协议 (也叫出错全部重发协议) 中，发送窗口的尺寸是大于 1，而接收窗口的尺寸则等于 1。
  * 由于接收窗口的尺寸为 1，接收端只能按顺序接受数据帧，一旦某个帧出错或丢失，只能丢弃该帧及其所有的后续帧（因为发送窗口的尺寸是大于 1 的）。发送端超时后需重发出错或丢失的帧及其后续所有的帧。
  * 发送端需要为每个待确认的帧都各自设置一个定时计数器。
  * 发送窗口的尺寸不能超过 2^n-1(这里的 n 为序号的编码位数)，否则会造成接收端无法分辨新、旧数据帧。

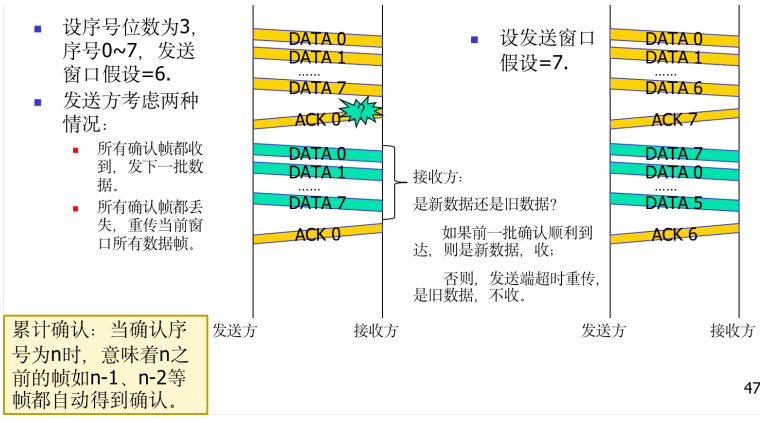


图 4.11: 发送窗口尺寸超过 2^n-1 造成帧的混淆

* 出错全部重发协议只要求发送端保持一定数量的缓存来保存没有确认的数据帧，对接收端没有缓存的要求。但在误码率高的情况下，会大大降低信道的利用率。

– 选择重发协议（selective repeat）

* 选择重发协议中，发送和接收窗口的尺寸都大于 1。
* 由于接收窗口的尺寸大于 1，接收端可存储坏帧之后的其它数据帧（落在接收窗口），接收端对错帧发否定确认帧，因此发送端只需重发出错的帧，而不需重发其后的所有后续帧。
* 接收端正确收到重发的帧后，可对其后连续的已接收的正确帧作一次总体确认（最大序号的确认），并交送网络层。大大提高了信道的利用率。
* 接收窗口的尺寸不能超过 2^n-1（即序号范围的 1/2），否则可能造成帧的重叠。

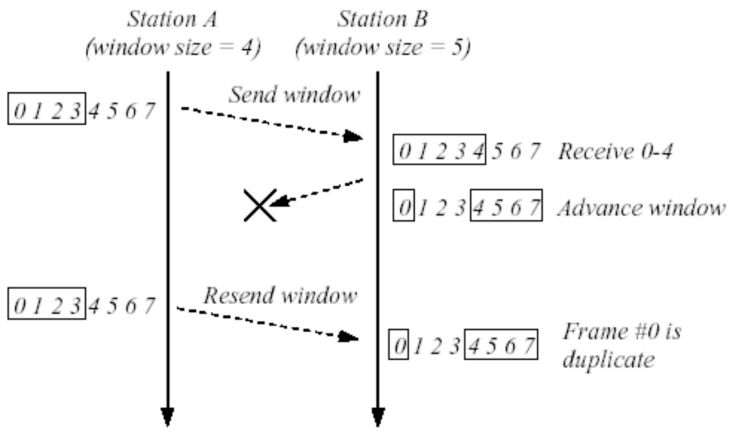


图 4.12: 接收窗口尺寸超过 2^n-1 造成帧的混淆

* 发送窗口的尺寸一般和接收窗口的尺寸相同（两者相加小于等于 2^n），发送端为每一个输出缓存区设置一个定时计数器，定时器一旦超时，相应输出缓存区中的帧就被重发。

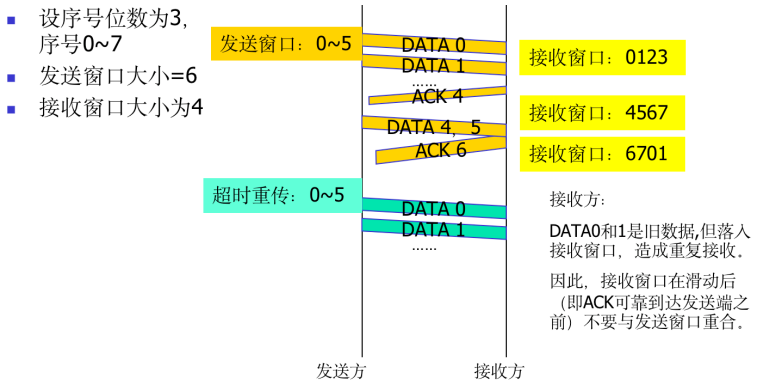


图 4.13: 发送窗口 + 接收窗口尺寸小于等于 2^n

4.5 面向位的协议 HDLC

- 高级数据链路控制（High-Level Data Link Control）是由国际标准化组织制定的面向位的有序链路层协议。

- 是为非平衡的链路级操作而研制的，采用主从结构，链路上一个主站控制多个从站，主站向从站发命令，从站向主站返回响应。
- HDLC 中只有一个地址域，即从站的地址，在命令帧中，它是目的地址，在响应帧中，它是源地址。
- HDLC 的帧格式

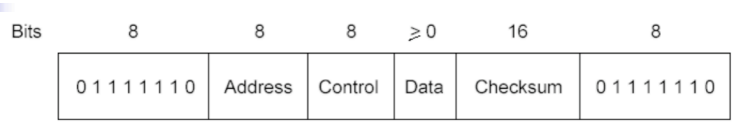


图 4.14: HDLC 的帧格式

  - 帧标志序列：01111110，作为起始和结束标志，在数据位有 5 个连续的 1 出现时，就插入 1 个 0（位填充）
  - 地址段：在命令帧中表示目的地址，在响应帧中表示源地址，全 1 为广播地址，全 0 为测试地址
  - 控制字段

    用来表示帧的种类，执行信息传送，监控功能：

    信息帧（I：Information）：用来实现信息的传送，含有信息字段

    监控帧（S：Supervision）：帧中不包含信息字段，具有监控链路的作用，并能对收到的帧进行确认。

    无编号帧（U：Unnumbered）：对数据链路进行附加控制。

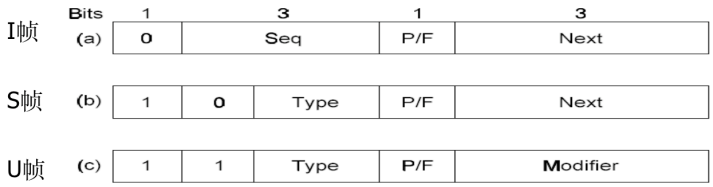


图 4.15: HDLC 的控制字段

Seq：发送端发送序列编号，这里是 3 比特，采用模 8 循环编号。

Next：表示发送端准备接收的序列号，也采用模 8 循环编号。

Type：表示监控功能的类型。Modifier：附加的修改功能。

P/F：在命令帧中作为询问比特，在响应帧中作为终止比特。

4.6 面向字节的数据链路层协议-PPP

SONET 上的数据链路层封装：

图 4.16: SONET 上的数据链路层封装

PPP 由以下 3 部分组成：

1. 串形链路上的数据报封装方法
2. 链路控制协议（LCP：Link Control Protocol），用来建立、配置、测试数据链路连接
3. 对不同的网络层协议定义了网络控制协议族

PPP 的帧格式:

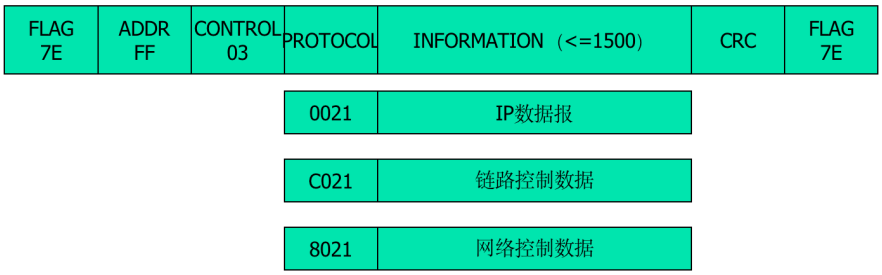


图 4.17: PPP 的帧格式

- PPP 有以下优点：
  - 可在一条串形线上支持多种网络层协议
  - 有 CRC 检错
  - 用网络控制协议动态协商每一端的 IP 地址
  - 链路控制协议协商多种数据链路选项。
- PPP 协议有同步传输和异步传输两种方式，在 SONET 同步传输网上，使用位填充方式，而在异步传输时，是一种面向字节的协议，采用字节填充。

5 局域网——以太网和 WIFI

5.1 传统 LAN 的基本概念 ★

- LAN 的模型
  - 局域网（LAN）是在一个小区域范围内对各种数据通信设备提供了互连的信息网。
  - 决定局域网特性的主要技术：
    - 用以传输数据的传输媒体
    - 用以连接各种设备的拓扑结构
    - 用以共享资源的媒体访问控制方法
- 局域网的数据链路层
  - 逻辑链路控制子层（LLC）（基本上不在采用）
    - 必须能支持链路的多路访问特性
    - 可利用 MAC 子层来摆脱与底层有关的某些操作，如拓扑结构、媒体、媒体访问控制访问
  - 媒体访问控制子层（MAC）
    - 成帧
    - CRC 校验
    - 根据网络的拓扑结构，不同的局域网采用不同的媒体访问控制方法
- 传统的 LAN 大多是共享媒体的 LAN（即采用广播信道），不需要路由选择功能，因此只具备 OSI 的第 1、2 层功能。在数据链路层，重点要解决媒体访问控制功能。

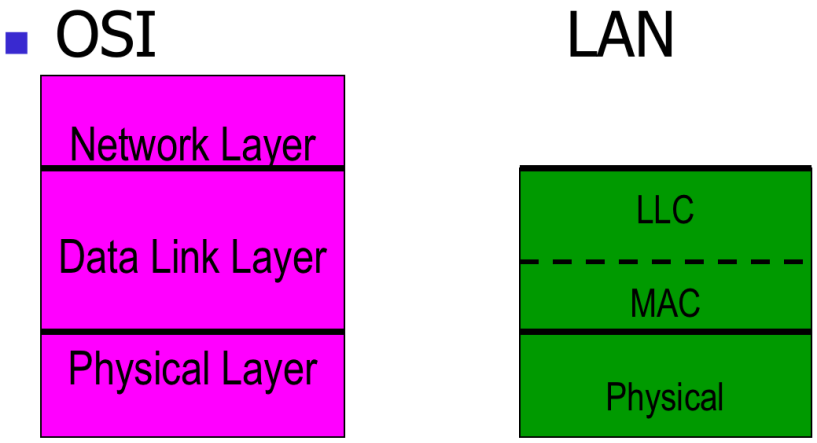


图 5.1: OSI 和 LAN

- LAN 的传输媒体

  双绞线、同轴电缆、光纤、无线电波、红外
- 局域网的拓扑结构

  星型（Star）、环型（Ring）、总线型（Bus）、树型（Tree）

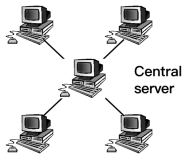


图 5.2: 星型

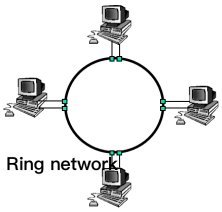


图 5.3: 环型

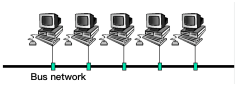


图 5.4: 总线型

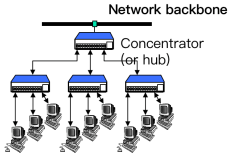


图 5.5: 树型

5.2 多路访问协议

- 对于广播信道，需要解决信道分配问题，信道的分配方案有：
  - 静态分配：如传统的 FDM 或 TDM，如果有 N 个用户，把带宽或时间分成 N 份，每个用户静态地占用一个。缺点是不能有效地处理突发数据，有的用户无通信量时白白浪费资源。
  - 动态分配：异步时分多路复用。分为两种：
    - 随机访问（争用，contention）：只要有数据，就可直接发送，发生冲突后再采取措施解决冲突。适用于负载轻的网络，负载重时效率低。
    - 控制访问：发送站点必须先获得发送的权利，再发送数据，不会发生冲突。在负载重的网络中可获得很高的信道利用率。主要有轮询（round-robin）和预约（reservation）两种方式。
- 动态信道分配的假设
  - 单信道：所有用户都共享同一个信道，在该信道上发送数据、接收数据。
  - 时间连续或分槽：
    时间连续：任意时刻都可发送。
    分槽：只在某个时槽的起始点可以发送。
  - 发送端能否检测冲突：如果多个用户同时发送数据，多路信号在时间上叠加使接收端无法正常解码，称为冲突。
    对有线信道，节点硬件可设计成边发送边检测冲突，而无线信道很难做到。
  - 载波侦听或不侦听：
    有载波侦听：发送前先侦听信道，可知道当前时刻信道是否“忙”
    无载波侦听
- 争用协议一：ALOHA 协议
  - 20 世纪 70 年代，美国夏威夷大学的 ALOHA 网通过无线广播信道将分散在各个岛屿上的远程终端连接到本部的主机上，是最早采用争用协议的网络。
  - 有两个版本：
    - 纯 ALOHA 协议（Pure ALOHA）：每个站点只要有数据就可发送；通过监听来自集线器的广播，发现是否发生冲突；若冲突，则等待一段随机时间，再重新发送。
    - 时隙 ALOHA 协议（Slotted ALOHA）：将信道时间分为离散的时间片，每个时间片可以用来发送一个帧。一个站点有数据发送时，必须等到下个时间片的开始才能发送。与纯 ALOHA 相比信道的利用率提高一倍。

- 争用协议二：CSMA 协议
  - 载波侦听多路访问（Carrier Sense Multiple Access）协议中，各站点不是随意发送数据帧，而是先要监听一下信道，根据信道的状态来调整自己的动作，只有发现信道空闲后再可发送数据。即“讲前先听”
  - 常见的四种 CSMA 协议：
    * 1-坚持式 CSMA（1-persistent CSMA）
      当一个站点要发送数据时，首先监听信道，若信道忙，就坚持监听，一旦发现信道空闲，就立即发送数据（发送数据的概率为 1）。若发生冲突，就等待一随机长时间，再重新开始监听信道。
      两种发生冲突的可能：信号传输的延迟造成的冲突、多个站点在监听到信道空闲时，同时发送。
      此协议的性能高于 ALOHA 协议。
    * 非坚持式 CSMA（non-persistent）
      当一个站点要发送数据时，先监听信道，若信道忙，就随机等待一段时间后再开始监听信道（非坚持）；一旦发现信道空闲，就立即发送数据。
      此协议的信道利用率高于 1-坚持式 CSMA 协议。
      网络的延迟增大。
    * p-坚持式 CSMA（p-persistent CSMA）用于时隙信道。当一个站点要发送数据时，先监听信道，若信道忙则等到下个时间片再监听信道；若信道空闲，则以概率 p 发送数据，概率 q=1-p. 推迟到下个时间片再重复上述过程，直到数据被发送。
      概率 p 的目的就是试图降低 1-坚持式协议中多个站点同时发送而造成冲突的概率。
      采用坚持监听是试图克服非坚持式协议中造成的时间延迟。
      p 的选择直接关系到协议的性能。
    * 带有冲突检测的 CSMA（CSMA with Collision Detection）CSMA/CD
      · CS 协议的“讲前先听”对 ALOHA 系统进行了有效的改进，但在发送过程中若发生冲突，仍要将剩余的无效数据发送完，既浪费了时间又浪费了带宽。
      · CD 协议的“边讲边听”可对 CSMA 作进一步的改进。发送过程中，仍然监听信道，通过检测回复信号的能量或脉冲宽度并将之与发送的信号作比较，就可判断是否发生冲突。一旦发生冲突，立即取消发送，等待一随机时间后再重新尝试发送。
    * 无线局域网（Wireless LAN）使用 CSMA 时存在的问题
      WLAN 基本使用 CSMA 协议，但由于各个站点发出的信号范围有限（不像有线网络中一个站点发出的信号可到达所有的站点），因此会造成：
      · 隐藏站点问题（hidden station problem）：图 (a) 中，A 向 B 发送时，由于 C 听不到误以为可发送数据，造成 B 接收失败。
      · 暴露站点问题（exposed station problem）：图 (b) 中，B 向 A 发送时，C 听到信道忙误认为它不能向 D 发送数据，实际上并不影响 A 和 D 两站的接收
    * CSMA/CA
      · CSMA/CA（避免冲突的 CSMA 协议）是 WLAN 采用的介质访问控制协议，其相应的国际标准为 IEEE 802.11。

图 5.6: 隐藏站点和暴露站点问题

- 发送方先发送短帧 RTS（Request to Send ），接收方响应一个短帧 CTS（Clear to Send ），使接收方周围的站点不会在即将到来的数据帧期间发送数据而导致冲突（避免冲突）。
- 当多个站点同时发短帧时仍会发生冲突，在预定时间内没有收到 CTS 的发送方采用二进制指数退避算法，在等待一随机时间后再次重试。

* CSMA/CA 的分析
  - A 首先向 B 发送一包含后继数据帧长度的 RTS 短帧。B 回复一个也包含数据帧长度（从 RTS 中得到）的 CTS 短帧。A 一旦收到 CTS，就开始发送数据。
  - 侦听到 RTS 的其它站点均保持足够长的沉默时间使 A 可无冲突地收到 CTS。侦听到 CTS 的站点也在后续的一定时间内（从 CTS 中可知）保持沉默。
    C 位于 A 范围内，B 范围外：能听到 RTS，听不到 CTS，也需保持静默。
    D 和 E 都位于 B 范围内：听到 CTS 后，关闭所有的发送，直到 A 到 B 的帧被认为发送完毕。

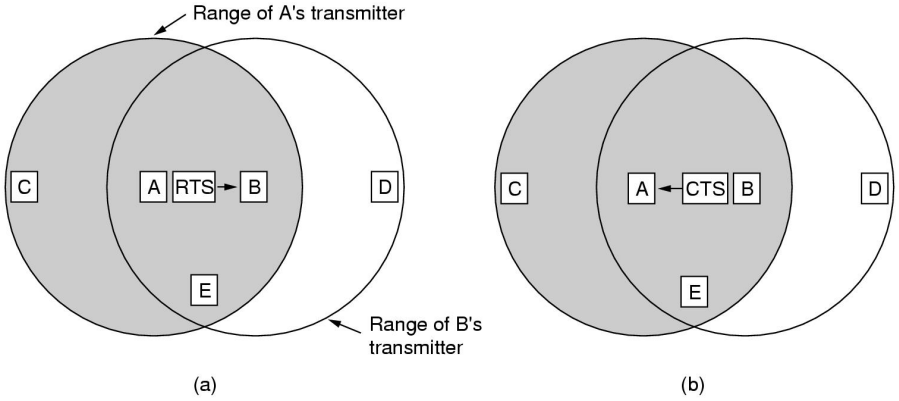


图 5.7: CSMA/CA 的分析

5.3 以太网的 MAC 协议 ★

5.3.1 IEEE 802.3 CSMA/CD

决定传统局域网的响应时间、吞吐量和效率的因素

- 传输媒体
- 拓扑结构
- 媒体访问控制方法

- 简单
- 有效的通道利用率
- 公平合理

- CSMA/CD 技术——是一种随机争用媒体访问控制方法

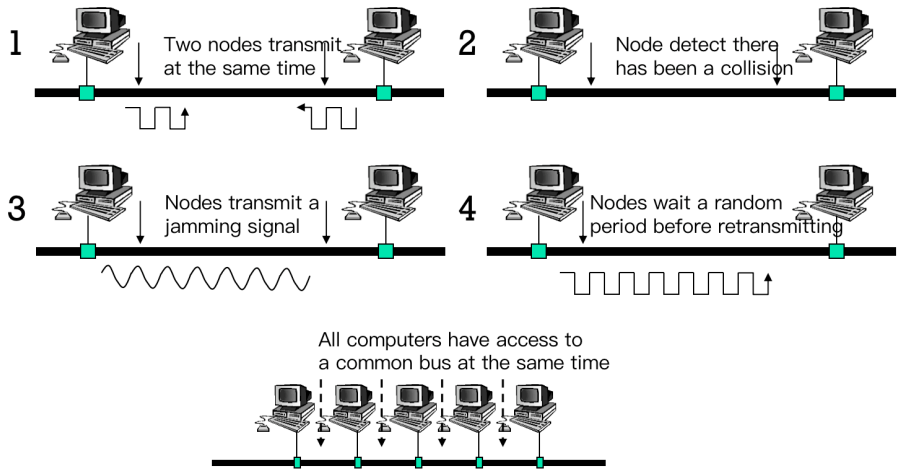


图 5.8: CSMA/CD 技术

- CSMA/CD 流程图

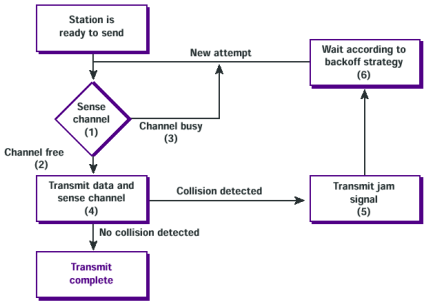


图 5.9: CSMA/CD 流程图

- 碰撞检测——碰撞域：不同站点同时发送数据可能产生碰撞的最大网段

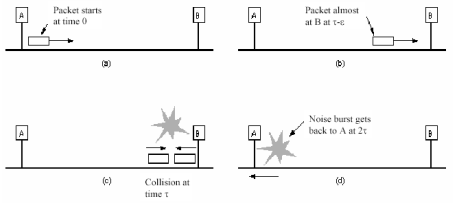


图 5.10: 碰撞检测

- 退避时间
  - 从发送数据帧到能检测出是否碰撞的最大所需时间 2 称为间隙时间。

- 退避时间 =r 间隙时间，r 是随机整数，在（0，2^k -1 ）区间内均匀取值，k=Min（尝试次数，10）。
- 对于 10BASE-5 局域网，规定网段的最大长度 500 米，允许最多 4 个中继器延长，最长 2500 米，间隙时间为 51.2 微秒。
- 对 10Mbps 的以太网，能检测出碰撞的最小帧长为 10Mbps*51.2 微秒 =512bit=64 字节。
- 802.3 帧格式

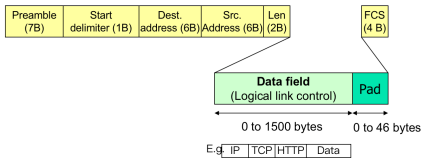


图 5.11: 802.3 帧格式

- 以太网 MAC 地址

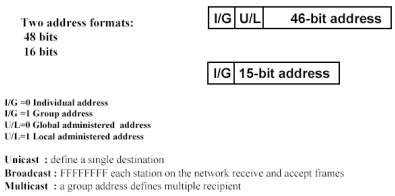


图 5.12: 以太网 MAC 地址

- Baseband IEEE 802.3

Name	Cable	Max. segment	Nodes/seg.	Advantages
10Base5	Thick coax	500 m	100	Good for backbones
10Base2	Thin coax	200 m	30	Cheapest system
10Base-T	Twisted pair	100 m	1024	Easy maintenance
10Base-F	Fiber optics	2000 m	1024	Best between buildings

图 5.13: Baseband IEEE 802.3

- IEEE 802.3 与 Ethernet 帧格式的比较

5.3.2 Fast Ethernet

- IEEE 802.3u 工作组规范 (1995,6)
- 特点：

  采用 CSMA/CD 媒体访问控制方式和 802.3 帧格式

  100BASE-TX 采用两对 5 类双绞线

  100BASE-T4 采用四对 3 类双绞线

  网络最大长度 250m（10M 以太网是 2500m，$51.2x10 - 6x10x10^6$=512bits）

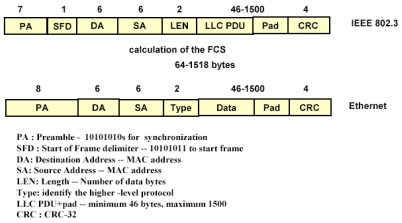


图 5.14: IEEE 802.3 与 Ethernet 帧格式的比较

Name	Cable	Length
100Base-T4	Twisted pair	100 m
100Base-TX	Twisted pair	100 m
100Base-F	Fiber optics	2000 m

图 5.15: Fast Ethernet 的物理规范

5.3.3 Gigabit Ethernet

- IEEE 802.3z(1998) 和 802.3ab 工作组规范
- 问题:

  在采用 CSMA/CD 的 MAC 子层中，碰撞检测时间与网络的最大距离成正比，在 10BASE-5 中，最大距离为 2500m，间隙时间为 51.2 微秒，最小帧长为 512 比特。在 100BASE-T 中，最大距离为 250m，帧格式不变，即间隙时间为 5.12 微秒。按此规律，千兆比以太网的最大距离为 25m，这显然不行。

- 解决方案

  载波扩展：最小帧长为 512 字节、网络最大距离 200m

  帧突发功能：允许在一定时间内连续发送多个 MAC 帧，最大突发长度为 8192 字节。

  全双工

Name	Cable	Max. range
1000BASE-SX	Fiber	220-550 mtr
1000BASE-LX	Fiber	550-5000 mtr
1000BASE-LH	Fiber	49-100 km
1000BASE-CX	Copper	25 mtr
1000BASE-T	Twisted pair	100 mtr

图 5.16: Gigabit Ethernet 的物理规范

5.4 无线 LAN★

- 扩频
  - 通道交叠
  - 通道不交叠
- IEEE 802 .11 基本概念及术语
  - 802.11 WLAN 的基本组件:

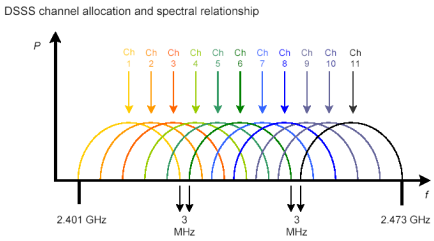


图 5.17: DSSS 通道交叠

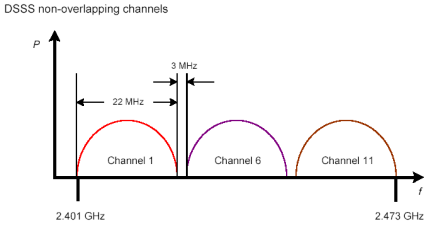


图 5.18: DSSS 通道不交叠

  * 接入点 AP(Access Point): 转发该 WLAN 上的所有帧，具备无线至有线的桥接功能。
  * 工作站（Station): 具备 WLAN 接口，能接入 WLAN 的主机。
  * 分布式系统（DS，Distribution system): 是 802.11 的逻辑组件，负责连接多个 AP，或将 AP 连接至骨干网（如目前的以太网）
- 基本服务集（BSS, basic service set)
  * 独立基本服务集（IBSS, independent BSS), 工作站之间相互可以直接通信（不需要通过 AP 转发)。
  * 基础结构型基本服务集 (infrastructure BSS), 接入点 AP 负责转发工作站之间的通信，但工作站必须先与接入点建立关联。每一个 BSS 都有一个 6 字节的识别符 BSSID，相当于 AP 的 MAC 地址。
- 扩展服务集（ESS, extended service set): 将几个 BSS 连接为 ESS。

5.5 网桥 ★

5.6 交换式局域网

6 网络层

7 互联网——Internet

8 传输层

9　应用层

10 网络安全

11 总复习部分

11.1 复习 1——基本术语缩写及其中英文全称

- 网络的标准化组织

  ITU：国际电信联盟（International Telecommunication Union）
  IETF：因特网工程任务组（The Internet Engineering Task Force）
  IEEE：电气电子工程师协会（Institute of Electrical and Electronics Engineers）
  ISO：国际标准化组织（International Organization for Standardization）
  RFC：请求评注（Request For Comments）

- 网络的体系结构

  OSI: 开放系统互连（Open System Interconnection）
  TCP/IP：传输控制协议/网际协议 (Transmission Control Protocol/Internet Protocol)
  PDU：协议数据单元（protocol data unit）
  SDU：业务数据单元（service data unit）

- 网络的分类和传输介质

  LAN：局域网（Local Area Network）
  MAN：城域网（Metropolitan Area Network)
  WAN：广域网（Wide Area Network)
  UTP：无屏蔽双绞线（Unshielded Twisted Pair）
  STP：屏蔽双绞线（Shielded Twisted Pair）

- 复用技术和传输技术

  FDM：频分多路复用（Frequency-division multiplexing）
  TDM：时分多路复用（Time-division multiplexing）
  WDM/DWDM：波分复用/密集型光波复用（Wavelength Division Multiplexing/Dense Wavelength Division Multiplexing）
  CDM/CDMA：码分多路复用/码分多址（code division multiplexing / $\cdots$ Access）
  SONET/SDH：同步光网络/同步数字系列（Synchronous Optical NETwork/Synchronous Digital Hierarchy）

- 数据链路层控制协议

  FCS：帧检验序列（Frame Check Series）
  CRC：循环冗余校验（Cyclic Redundancy Check）
  HDLC：高级数据链路控制（High-Level Data Link Control）
  PPP：点对点协议（Point to Point Protocol）
  LLC：逻辑链路控制（Logical Link Control）
  MAC：媒体访问控制（Media Access Control）

- 多路访问协议

  CSMA/CD：载波侦听多路访问/冲突检测（Carrier Sense Multiple Access with Collision Detection）
  CSMA/CA：载波侦听多路访问 / 冲突避免（Carrier Sense Multiple Access with Collision

Avoid）
RTS/CTS：请求发送/允许发送协议（Request To Send/Clear To Send）

- 无线局域网（IEEE 802.11）

  WLAN：无线局域网（Wireless LAN）
  AP：接入点（Access Point）
  BSS：基本服务集（basic service set）
  ESS：扩展服务集（extended service set）
  BSSID：基本服务集标识符（Basic Service Set Identifier）

- 802.11 MAC 子层

  PCF：点协调功能（Point Coordination Function）
  DCF：分布式协调功能（Distributed Coordination Function）
  SIFS：发送控制帧或下一个分片的间隔（28μs）（Short inter frame space）
  PIFS：PCF 帧发送间隔（50μs）（PCF inter frame space）
  DIFS：DCF 帧发送间隔（128μs）（DCF inter frame space）

- Internet 基本协议

  ARP：地址解析协议（Address Resolution Protocol）
  RARP：反向地址转换协议（Reverse Address Resolution Protocol）
  IPv4/IPv6：互联网通信协议第四/六版（Internet Protocol version 4/ $\cdots$ 6）
  DHCP：动态主机配置协议（Dynamic Host Configuration Protocol）
  ICMP：Internet 控制报文协议（Internet Control Message Protocol）
  IGMP：Internet 组管理协议（Internet Group Management Protocol）

- Internet 路由协议

  RIP：路由信息协议（Routing Information Protocol）
  OSPF：开放最短路径优先（Open Shortest Path First）
  BGP：边界网关协议（Border gateway Protocol）
  AS：自治系统（Autonomous System）
  IGP：内部网关协议（Interior Router Protocols）
  IGRP：距离矢量路由算法（Interior Gateway Routing Protocol）
  EGP：外部网关协议（Exterior Gateway Protocol）

- IP 寻址

  CIDR：无类别域间路由（Classless Inter domain Routing）
  NAT：网络地址转换（Network Address Translation）
  NAPT：网络地址端口转换（Network Address Port Translation）

- Internet 中的传输层协议

  TCP：传输控制协议（Transmission Control Protocol）
  UDP：用户数据报协议（User Datagram Protocol）
  RTT：往返时间（Round-Trip Time）
  RTO：重传计时器（Retransmission TimeOut）
  MSS：最大数据段长度（Maximum Segment Size）

- 域名系统、文件服务和电子邮件

  DNS：域名系统（Domain Name System）
  FTP：文件传输协议（File Transfer Protocol）
  SMTP：简单邮件传输协议（Simple Mail Transfer Protocol）
  POP：邮局协议（Post Office Protocol）
  IMAP：因特网消息访问协议（Internet Message Access Protocol）以前称作交互邮件访问协议（Interactive Mail Access Protocol）
  MIME：多用途 Internet 邮件扩展（Multipurpose Internet Mail Extensions）

- WWW（HTTP）

  WWW：万维网（World Wide Web）
  HTTP：超文本传输协议（HyperText Transfer Protocol）
  HTML：超文本标记语言（HyperText Markup Language）
  URL：统一资源定位符（Uniform Resource Locator）

- 网络安全

  DES：数据加密标准（Data Encryption Standard）
  PKI：公钥基础设施（Public Key Infrastructure）
  CA：证书签证机关（Certification Authority）
  IPSec：互联网安全协议（Internet Protocol Security）
  AH：认证头标（Authentication Header）
  ESP：封装安全载荷（Encapsulate Security Payload）

11.2 复习 2——基本概念

- 体系结构，层，协议，接口，服务
- OSI 参考模型，各层基本功能
  - 应用层：

    处理应用进程之间所发送和接收的数据中包含的信息内容。如 FTP、HTTP
  - 传输层：

    为应用层提供与下面网络无关的可靠消息传送机制，如 TCP，连接，定时器，流控，拥塞控制
  - 网络层：

    路由（路由算法、路由协议）、转发，拥塞控制，IP,ICMP
  - 数据链路层：

    成帧，差错控制、流量控制，物理寻址，媒体访问控制 (CSMA/CD,CSMA/CA)，局域网：以太网，WiFi
  - 物理层：

    缆线，信号的编码，网络接插件的电、机械接口

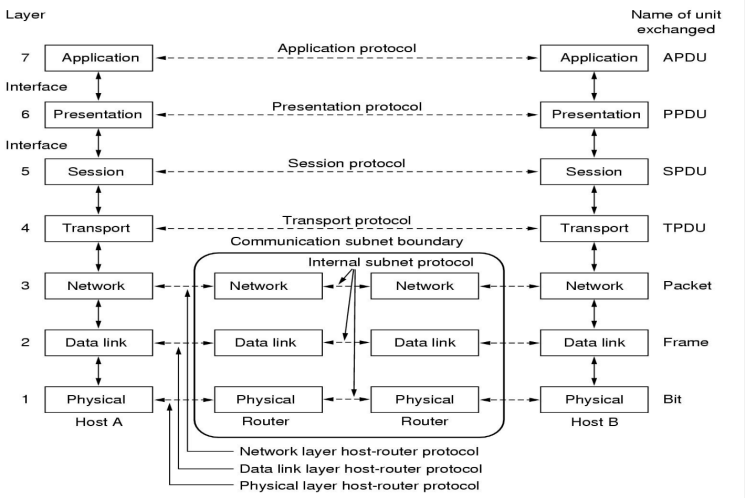


图 11.1: OSI 参考模型

- TCP/IP 参考模型，与 OSI 模型的相同与区别
  - TCP/IP 模型

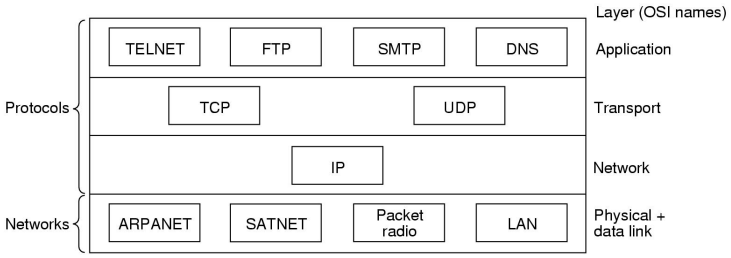


图 11.2: TCP/IP 模型

  - OSI 与 TCP/IP 模型的比较
    - 相同点：

      1. 都是基于独立的协议栈概念。
      2. 两者都有功能相似的应用层、传输层、网络层。

    - 不同点：

      1. 在 OSI 模型中，严格地定义了服务、接口、协议；在 TCP/IP 模型中，并没有严格区分服务、接口与协议。

      2.OSI 模型支持非连接和面向连接的网络层通信，但在传输层只支持面向连接的通信；TCP/IP 模型只支持非连接的网络层通信，但在传输层有支持非连接和面向连接的两种协议可供用户选择。

      3.TCP/IP 模型中不区分、甚至不提起物理层和数据链路层。

- 上下层数据单元的关系，特定层数据单元的名称
- 面向连接服务与无连接服务的区别
  - 面向连接的服务
    - 首先要在信源与信宿之间建立连接，然后在此连接上通信，最后拆除连接。

    * 特点：占用一定的存储资源（有状态），可靠，按序传送
  - 非连接服务
    * 传送数据不需要建立连接，即有即送。
    * 将每个数据单元打包，在包头添加地址信息。
    * 特点：每个数据包独自寻路（重复劳动），同一数据流的包可能经由不同的路径到达目的地，到达的顺序也可能颠倒。

11.3 复习 3——物理层

- 奈奎斯特定理与香农定理
  - 奈奎斯特定理，无噪信道，信号分 V 个离散等级，最大数据传输率 $=2Blog_2V(b/s)$
  - 香农定理：有噪信道，信噪比 S/N，最大数据传输率 $=Blog_2(1+S/N)(b/s)$
- 网络常用的传输介质
  - 有线：双绞线，同轴电缆，（电力线），光纤
  - 无线：电磁波，光
- 交换技术
  - 电路交换

    电路交换与分组交换的比较:
    * 电路交换预先静态地保留所要带宽;而分组交换却是根据需要动态地获得和释放带宽。
    * 在电路交换中，已分配给线路上未用的带宽只能浪费掉；而分组交换中，未用的带宽可以被别的传输所利用。
    * 电路交换对数据传输是完全透明的，而分组交换则要利用分组所携带的参数进行路由转发。
    * 分组交换是存储转发的，会增加传输延时；电路交换则是连续的通过物理线路传输。
    * 分组交换中，分组到达目的地可能不按原顺序；在电路交换中，不会发生乱序现象。
    * 分组交换可以按传输的字节或连接时间计费；电路交换按时间、距离计费。
  - 存储交换：分组交换，报文交换
  - 延时分析：传播延时，传输延时，处理延时，排队延时。
    * 分组交换中的延时分析
      · 传播延时（propagation delay）
      数据某比特从 A 节点到 B 节点传播所需的时间，取决于物理媒体传播速度（$2-3*10^8$m/s ）和 AB 两点间距离。
      · 传输延时 (transmission delay)
      节点发送（或接受）整个分组所需时间，用 L 比特表示分组长度，用 Rb/s 表示链路速率，则 L/R 为传输延时。
      · 处理延时 (processing delay)
      检查分组头部，寻路，差错校验等，与 CPU 速度和处理算法有关。

· 排队延时 (queue delay)
在节点上等待处理所需时间，与网络拥塞状况有关

* 分组交换的总延时
  · 一个分组在路径上的总延时
  D= 总 d_{prop}+ 转发节点数 *（d_{trans}+d_{pro}+d_{queue}）+d_{trans}
  · n 个分组在路径上的总延时
  D= 总 d_{prop}+ 转发节点数 *（d_{trans}+d_{pro}+d_{queue}）+n*d_{trans}

11.4 复习 4——数据链路层及局域网

- 向网络层提供的服务
  面向连接（如，帧中继），无连接有确认（如，802.11），无连接无确认（如，802.3）
- 成帧
- 差错检测：纠错码，检错码，超时重传
  – 海明编码，纠正单比特错的校验位下界 2^r>=n+1
  – CRC 编码及检测能力分析
    * 书上 166 例题，G(X)=X^4+X+1, 计算 1101011111 的检验和

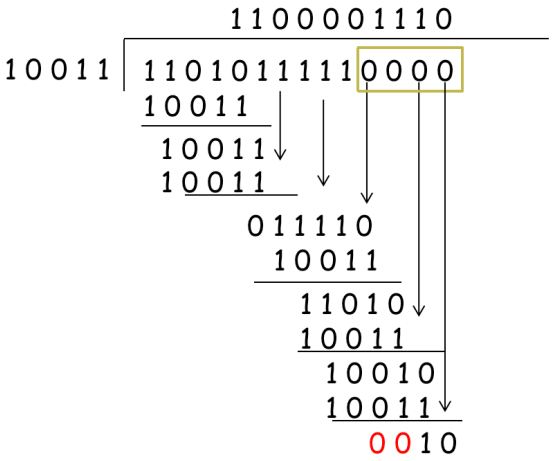


图 11.3: CRC 检验和

余数可以是 10，但帧检验序列一定是 r 位，和补 0 的个数一致，比除数少一位

* CRC 的错判率
  · 能检验出所有长度小于等于 r 的错误
  · 如果突发长度为 r+1，当且仅当差错与 G（X）相同时才被整除。根据突发错误长度的定义，其第 1 位和最后 1 位必须是 1，因此与 G（X）完全相同的概率为 $(1/2)^{r-1}$。
  · 对于长度大于 r+1 的差错，其错判率为 $(1/2)^r$。

- 流量控制：滑动窗口

  - 滑动窗口协议是通用的流量控制协议，特别是在效率、复杂性及对缓冲区的需求等方面可作灵活调配。
  - 发送端和接收端分别设定发送窗口和接收窗口, 大小分别为 Wt 和 Wr。
  - 帧序号用 n 位编码，序号范围为 0 2^n-1
  - 主要的滑动窗口协议有回退 N 协议和选择重发协议
    * 对于回退 N 协议，即 Wt<=2^n-1，Wr=1
    * 对于选择重发协议，Wt +Wr <=2^n, Wr <=2^{n-1}

- 基本链路层协议：停-等协议
  - 带宽延迟乘积：BD，比特
  - 链路利用率 W/(1 帧 +2BD), 注意单位一致

- 传统局域网的基本概念
  - 拓扑结构

- 媒体访问控制方法
  - 应用场景，常见方法
  - 动态信道分配：CSMA/CD, CSMA/CA

- 以太网/802.3
  - 碰撞检测，碰撞域，最小帧长的计算，最小帧长/最大帧长限制的原因

- WiFi/802.11
  - 支持的两种操作模式：PCF/DCF，DCF 与 CSMA/CA，地址，帧间间隔的用处。

- 局域网互联设备-网桥/交换机
  - 根据目的 MAC 地址转发数据帧
  - 根据源 MAC 地址，采用逆向学习生成地址查找表
  - 能隔离碰撞域，不能隔离广播域
  - 网桥连接不同局域网时存在的问题

11.5 复习 5——网络层和 IP

- 向传输层提供的服务
  - 面向连接-虚电路
  - 无连接-数据报:IPv4，IPv6 协议，ICMP 协议

问题	数据报	虚电路
连接建立	不需要	需要
路由与转发	每个分组都包含源/目的地址，独立路由，路由器根据分组的目的地址进行路由转发	建立连接时需要路由，一旦建立逻辑通道，后续分组都根据分组头的逻辑通道号转发
路由器状态	不保留分组路有过的状态信息	路由器需要保留每个连接的状态信息，以便后续分组的转发
分组路径与到达顺序	同一流的分组可能沿不同的路径到达目的端，有可能乱序	同一流的分组沿建立好的虚电路到达按序目的端
路由器故障影响	通过相邻节点的路由表更新，能迂回故障节点	故障路由器上的所有连接都将中断
服务质量	较难提供	易于在建立连接时在路径上的各个节点预留资源
拥塞控制	较难提供	在建立连接时，可根据网络的资源选择路径，避免网络拥塞

表 11.1: 虚电路与数据报的比较

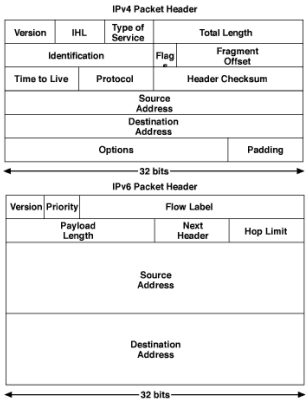


图 11.4: IPv4 与 IPv6 比较

V6: 6 fields +2 addr

V4: 10 fields + 2 addr + options

Deleted:

- Header length
- type of service
- identification, flags, fragment offset
- Header Checksum

Added:

- Traffic class
- Flow label

Renamed:

- length -> Payload length
- Protocol -> Next header
- time to live -> Hop limit

Redefined:

-Option mechanism

    * ICMP（互连网控制报文协议）
        · 分组由于各种原因无法投递而遭丢弃时，就用 ICMP 发送差错报告。ICMP 定义了两类报文：差错报文和信息报文
        · 差错报文
        源抑制：抑制发送过多分组的主机。
        超时：分组的 TTL 为 0。
        信宿不可达：报告子网、主机不能定位的信宿。
        重定向：路由重定向。
        参数问题：分组头参数出错。
        · 信息报文
        回音请求/响应（Echo request/reply）
        地址掩码请求/响应（Address mask request/reply）
        路由器发现（Router discovery）
        · 主要应用
        Ping，采用 ICMP 的回音请求报文，来测试目的主机的可达。
        Traceroute，通过发送递增的 TTL 值的回音请求报文，测试目的主机沿途经过的路由器地址。

- 路由算法
    - 自适应/非自适应（动态/静态路由）
    - 距离矢量与链路状态（给定邻居的路由表能迭代出最新路由表，或给定简单的拓扑与权重，能算出最短路径）DV: RIP,BGP ； LS: OSPF。IGP: RIP,OSPF；EGP: BGP。
        * 距离矢量
            · 节点向相邻节点告诉它所知道的所有节点的路由信息
            · 节点根据相邻节点的路由信息更新自己的路由表
            · 分布式计算
            · 可扩展性差
        * 链路状态
            · 节点向所有节点告诉其相邻节点的状态信息
            · 每个节点都有一个全局的拓扑结构
            · 根据此拓扑结构计算路由表
            · 可扩展性好，可靠
    - 层次化路由

- 拥塞控制
    - 拥塞控制与流量控制的区别
        * 拥塞控制
            · 网络负载的不均衡，例如，某个路由器的多个输入端口向同一个输出端口传输分组
            · 是全局问题，涉及的节点包括主机、路由器

· 拥塞发生在网络内，但对于无连接的网络很难在网络层单独控制拥塞，因此网络层和传输层共同承担拥塞控制

* 流量控制
  · 接收端或所在网络的接收速度小于发送端的发送速度
  · 只涉及收发两端，是局部问题

– 漏桶算法、令牌桶算法

* 令牌桶算法令牌桶容量 B bytes，令牌产生速率为 R bytes/s，计算机最大数据速率 M bytes/s，则计算机可以以 M 速率传输 S 秒。
  B+ R S=MS S=B/（M- R）=11ms
  例：ATM 网络中每个信元 53 个字节，每隔 53 s 产生一个新令牌，每个信元获取令牌后即可传输。令牌桶内已有 2000 个令牌。请问计算机用 10Mbps 的全速可以传输多长时间?
  解：R=53*8/53=8Mbps, B=2000*53*8=0.848Mb, S=0.848/(10-8)=0.424s

- 网络互连
  – 从物理层到应用层都有有哪些经典的互连设备，它们的转发机制?
  – 哪些设备能隔离碰撞域、广播域（路由器，能隔离碰撞域和广播域）
  – IP 地址的分类与无类别域间寻路，地址分配、聚类
  – 路由器对 IP 分组头的处理
- IP 地址与 MAC 地址的区别

MAC	IP
物理地址	逻辑地址
(数据链路层地址)	(网络层地址)
局部意义	全局意义
随机获得	上级分配
48 位	32 位
(如 08:00:39:00:2f:c3)	(如 202.38.75.11)

表 11.2: IP 地址与 MAC 地址的区别

- 地址解析（ARP,RARP)
- IPv4 地址分类:A(0),B(10),C(110),D(1110),E(1111)
- CIDR: 如：128.14.32.0/20 表示网络前缀 20 位，主机位 12 位，地址块共有 212 个地址，也可表示成 128.14.32/20。

  例如：已知有一块地址从 194.24.0.0 开始，可用的 IP 地址有 8192（213），有大学对地址需求如表 11.3 所示，请分配地址，并画出网络拓扑和路由表项。

  地址需求：1024=210，主机地址 10 比特长，网络前缀 22 比特；2048, 主机地址 11 比特，网络前缀 21 比特；4096, 主机地址 12 比特，网络前缀 20 比特.

  地址分配成块，不重复，具体标识接口时排除特殊地址，如主机地址为全 0，全 1。

	地址个数	范围	掩码	聚类地址
剑桥大学	2048	194.24.0.0-194.24.7.255	255.255.248.0	194.24.0.0/21
爱丁堡大学	1024	194.24.8.0-194.24.11.255	255.255.252.0	194.24.8.0/22
（可分配）	1024	194.24.12.0-194.24.15.255	255.255.252.0	194.24.12.0/22
牛津大学	4096	194.24.16.0-194.24.31.255	255.255.240.0	194.24.16.0/20

表 11.3: 地址需求

考虑路由表 1，要转发的 IP 分组，目的地址为 194.24.17.4，17=（00010001）

前 20-前 23 位：194.24.16.0

与第三项匹配

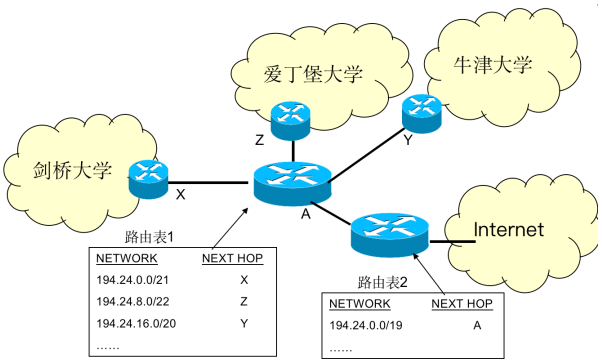


图 11.5: 拓扑图

- NAT：内外地址转换，实现内网私有地址与全局 IP 地址的转换。
- IPv6 地址: 十六进制冒号分割法, 如 1025:1ab6:0:0:0:87:a76f:1234，或 1025:1ab6::87:a76f:1234，::FFFF:129.144.52.38

11.6 复习 6——传输层

- Internet 中定义了两个不同的传输层协议
  - 用户数据报协议（UDP：User Datagram Protocol），提供无连接的服务，高效，适合于实时传输
  - 传输控制协议（TCP：Transmission Control Protocol），提供可靠的，面向连接的服务
    - 特点：连接，可靠，字节流、全双工，流控，拥塞控制
    - 连接建立、连接释放
    - 连接管理：六类定时器，重点关注重传定时的 RTT，RTO 设置与计算
- Internet 拥塞控制算法的实例
  - 假设最初拥塞窗口为 64kB，最大段长为 1kB，发生超时，将阈值设为其 1/2，即 32kB，并将拥塞窗口恢复为最大段长度，执行慢启动算法

– 直至拥塞窗口达到阈值，此后拥塞窗口按线性增加（每次只增加一个最大段长度），直至最终达到接收窗口大小或发生超时

– 若超时再将临界值设为当前拥塞窗口的 1/2，重复上述过程

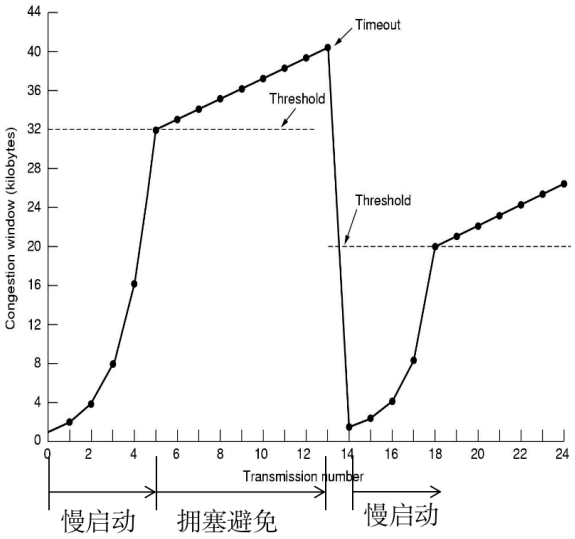


图 11.6: Internet 拥塞控制算法

- TCP　Reno 算法

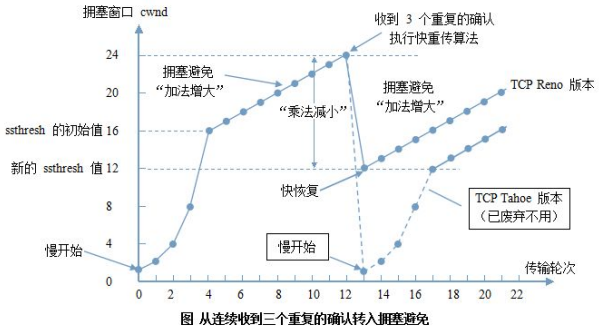


图 11.7: TCP Reno 算法

– TCP 的传输速率

设 TCP 的发送窗口为 w，往返时间为 RTT，则 TCP 瞬时最大发送速率为 w/RTT. 由于 w 是变化的，设丢包或收到三个重复 ACK 时的窗口为 W，且 W 不变，则 w 在 W/2 到 W 之间变化，忽略慢启动阶段，则一条连接的平均吞吐量 =0.75*W/RTT。

- RTT 与 RTO

– 1988 年 Jacobson 提出了另一个公式

* RTT：往返时间的估计值; M：往返时间的测量值
* α ，β ：平滑因子，典型 α =7/8，β=3/4; D：偏差变量
* RTTnew $\leftarrow$ αRTT+(1-α)M

    - Dnew ← βD+(1- β)|RTT-M|
    - RTT ← RTTnew
    - D ← Dnew
    - 重传时间 RTO ← RTT +4D
  - Karn 算法：对已经重传的数据段无需修改 RTT、D，而是在每次传输失败时将超时时间 RTO 加倍，直到该数据段被成功传输。

- 重传时间 RTO 计算实例
  - 设前个时刻 RTT 的估计值为 80ms，偏差变量 D 为 16ms，此时测得从发送数据段到收到确认所花费的时间为 160ms，那么根据 Jacobson 算法，计算得到的超时间隔为多少？假设所有平滑参数的值取为 7/8。
    - RTTn=7/8 *80+160/8=90(ms)
    - Dn=7/8 *16+1/8 *80=24
    - RTO=90+4 *24=186

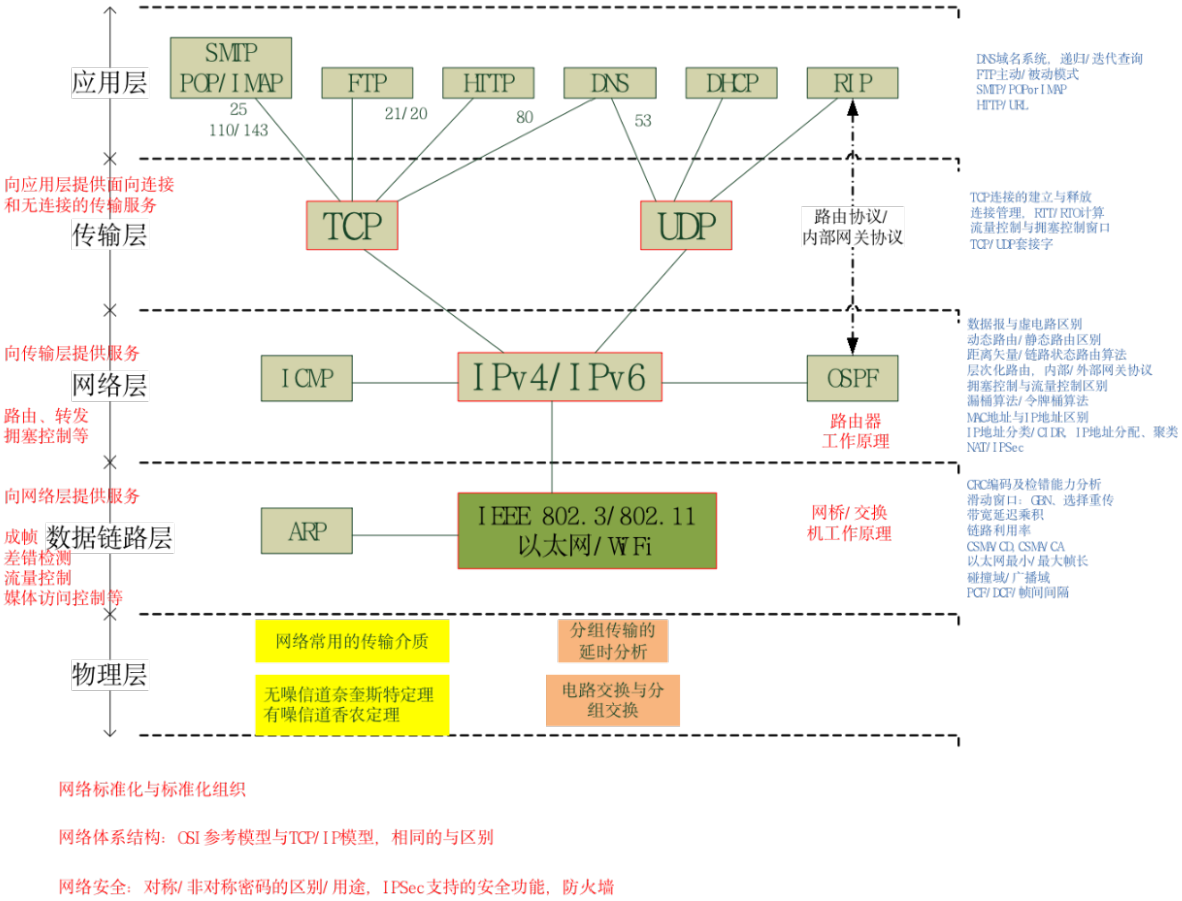
11.7 复习 7——应用层

- DNS
  - 组成：解析器，域名空间，资源记录，名字服务器
  - 传输层可采用 TCP 或 UDP 协议，端口号均为 53 号
  - 域名查询方法：递归查询，迭代查询
- FTP
  - 控制连接，TCP21 端口；数据连接，TCP20 号端口
  - 数据连接有主动模式与被动模式
- SMTP，POP3/IMAP
  - 分别为 TCP25 号端口和 110 端口
  - 组成：用户代理、邮件服务器，简单邮件传输协议，（邮件访问协议）
- WWW
  - 特点：超文本，超链接，超媒体
  - HTTP 协议，TCP80 端口
  - HTML 语言描述
  - URL 定位资源，由协议、主机域名、路径及文件名三部分组成

11.8 复习 8——网络安全

- 网络攻击类型：主动攻击和被动攻击，有哪些?
- 网络安全提供的安全服务

  - 认证，访问控制
  - 数据机密性，数据完整性
  - 不可否认性
- 密码体制
  - 对称密码，特点：加密密钥和解密密钥相同，加密速度快
  - 数据机密性，数据完整性
  - 非对称密码（公私钥密码），特点：加密密钥和解密密钥不相同，加密速度慢，可用于数字签名和密钥分发
- IPSEC
  - AH 头标：数据完整性保护，抗重播攻击
  - ESP 头标：提供数据机密性、完整性保护，抗重播攻击
- 防火墙
  - 包过滤防火墙
  - 状态检测防火墙
  - 代理型防火墙



网络标准化与标准化组织

网络体系结构：OSI 参考模型与TCP/IP模型，相同的与区别

网络安全：对称/非对称密码的区别/用途，IPSec支持的安全功能，防火墙