

【背诵】协议工程（分为以下四个部分）

- a. 协议说明: 提供给用户的服务+协议实体的内部操作
- b. 协议验证: 用于设计阶段, 进行可达性分析等
- c. 协议实现
- d. 协议测试: 一致性测试、互操作性测试、性能测试

形式化描述技术FDT/形式化方法fM（应用于协议工程研究中）

- 有啥模型

- 有限状态机FSM（扩展：EFSM）
- 形式化语言模型LOTOS/Estelle/SDL
- Petri网（扩展：时间/随机/高级Petri网）
- 进程代数（扩展：随机进程代数）
- 模型描述能力的增强会在某种程度上增加模型分析的难度

CRC检错能力分析（这里只记结论，推导太数学，可以看ppt）

- 若发的是T(x), 接收的是错误的T'(x)+E(x), 则当(E(x)/G(x))=0时不能发现错误
- 对于具有r个校验位的多项式:
 - 一定能查出1比特错
 - G(x)连x+1的倍数能查出奇数个比特错

- 能检查出所有长度≤r的突发差错
- 有1/(2^r(r-1))的概率查不出来+r+1突发差错
- 有1/(2^{r+1})的概率查不出长度大于r+1的突发差错或多个较短的突发差错

HDLc: 1976年ISO提出

- 面向比特, 采用滑动窗口技术, 校验和用CRC
- 3种站, 2种构型, 3种操作模式
- 帧类型: 信息帧/监控帧/无序号帧
- 构造协议: 选择站构型→操作模式→帧种类→12种任选功能→ok

X.25 LAPB（X.25的链路层协议, X.25在ch2中提到过）

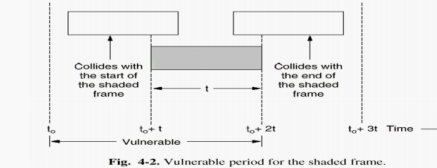
- LAP、LAPB是HDLc的子集, 帧格式与HDLc完全相同
- 检错纠错: CRC必用, 超时、序号、校验指示可选

PPP协议（Point-to-Point Protocol）

- SLIP的改进, 包括链路控制协议LCP和网络控制协议NCP
- 面向字符, 采用字符填充技术
- 以帧为单位发送, 而非原始IP包

纯ALOHA: 直接发, 发了再监听, 冲突后等待随机时间重发

- 冲突危险区: 前后各有一个帧时(2个帧时)



- 信道效率: 服从泊松分布, S=G·e^{-2G}, 最高18.4%

分槽ALOHA: 信道分为离散的时间槽, 长度为一个帧时, 只有当槽开始时可发

- 冲突危险区: 纯ALOHA的一半, 只有一个帧时(上面那张图只有前面那个冲突帧在分槽ALOHA中会和阴影帧一个时槽, 后面那个冲突帧会在下一个时槽发, 不会冲突)

- 信道效率, 依然是泊松分布, 冲突危险区减半所以S=G·e^{-G}, 最高36.8%

协议名称	监听-信道空闲	监听-信道忙	发送-冲突
ALOHA	我不听直接发	我不听直接发	等待随机时间
1-坚持型CSMA	直接发 (p=1)	坚持监听直到空闲	同1
非坚持型CSMA	直接发 (p=1)	等待随机时间再听	同1
P-坚持型CSMA	以概率p发	坚持监听直到空闲	同1

名称	工作原理	轻负载效率 (1个站发)	重负载效率 (都要发)	公平性
基本位图协议	N个站, 每个站对应竞争周期一个时槽, 若有帧发送则在对应时槽中发送比特1, N个时槽后大家都知道哪个站要发送, 此后按站序号发送 (全都发出)	d/(d+N)	N*d/(N+N*d) =d/(d+1)	序号大服务好
二进制下数法	地址用等长二进制串表示, 若有帧发送到广播位串, 广播后做“或”操作, 遇到更大的序号 (即本站地址这一位是0而“或”操作结果是1) 则放弃发送请求, 最后留下位串最大的	d/(d+log ₂ N) (从高到低依次广播+“或”操作每一位)	d/(d+log ₂ N) (和轻负载相同)	序号大服务好
令牌环协议	之后会详细讲 (IEEE802.5)	类似基本位图 (d/(d+N))	类似基本位图 (d/(d+1))	公平!

【概念】二进制指数后退算法

- 将冲突发生后的时间划分为长度为51.2微秒的时槽
- 发生第k次冲突后:
 - 若k<10, 各个站点随机从0~2^{k-1}-1中选择一个数, 等待这么多个时槽后, 再开始重传
 - 若10≤k≤16, 随机从0~2¹⁶⁻¹-1中选择一个数, 等待这么多个时槽后重传
 - 若i>16 (也可能≥, ppt上说的是“16次冲突后”, 有点歧义), 认为发送失败, 放弃努力报告上层

【快速以太网】802.3u: 10Mbps→100Mbps (Fast Ethernet) 10BaseX的含义: 10Mbps, 基带传输 (baseband), 4对双绞线 (twisted pair) X*100m的传输距离

- 100Base-T4使用4对双绞线, 8B6T编码, 三进制信号
- 共享式hub: 一个冲突域
- 交换式hub: 输入帧缓存, 一个端口构成一个冲突域

【千兆以太网】802.3z: 100Mbps→1Gbps 增加了extension域

- 使用扩展的802.3MAC子层接口, 通过GMII (Gigabit Media Independent Interface) 与物理层相连
- 采用8B/10B、4B/5B等编码
- 一个冲突域内只允许一个中继器

【万兆以太网】802.3ae: 1Gbps→10Gbps (10GE)

- 帧格式和前面的完全相同
- 只使用光纤
- 只工作在全双工方式, 不适用CSMA/CD, 传输距离大大提高

IEEE 802.3的mac子层采用CSMA/CD

距离向量路由算法 (Distance Vector Routing, 以下简称DV, 例题见P24)

- 最初用于ARPANET, 被RIP协议采用
- 【步骤】每个路由器向邻居发送自己到所有路由器的距离表, 本路由到X的距离利用邻居路由器X、自己到X的距离m更新, 为D_i = min (X_i + m_X)
- 注意: 本路由器中的老路由表在计算中不被使用, 更新是取所有邻居的最小值
- 【缺点】无穷计算问题, 选择路由时没有考虑链路带宽, 路由收敛速度慢, 路由报文开销大 (不是增量更新, 每次用全部的重算一遍), 不适合大规模网络 (例如采用它的RIP协议最大支持15跳)
- 改进- 水平分裂算法 (A告诉我的消息我不告诉A) 以避免无穷计算, 虽然广泛使用, 但有时候会失败

链路状态路由算法 (Link State Routing, 以下简称LS, 例题见P32)

- 使用的协议: OSPF, IS-IS; 步骤如下:
 - 启动时, 通过HELLO两次握手发现邻居节点; 简化拓扑, n个路由器连在一个LAN时, 引入人工节点DR (代表路由器), 原本C条路由之间的连线被简化成了DR与路由器们的n条
 - 测量每个邻居节点的延迟或开销 (用ECHO分组的往返时间/2, 或者根据带宽)
 - 将学习到的邻居信息封装成分组 (链路状态声明LSA), 内容是sender ID, seq, age、邻居结点list (邻居-延迟) ——【注意】分组定期创建, 或发生重大事件时创建
 - 把分组发送到全网路由器, 采用洪泛方式
 - 控制洪泛中产生的重复包, 分组含序号seq, 同一个路由器尽量使自己发出的不同分组序号不同; 其他路由接收到时可以判断是新分组/重复分组/过时分组, 只处理新分组
- 问题: 序号循环使用 路由器重启后序号重置 / 出错
- 改进: 用32位序号 增加age域, 计数超过Max丢弃
- 其他改进:
 - 1. 分组到达后延迟一段时间, 多接收一些分组, 把来源相同的进行比较, 丢弃重复的, 保留新的 (抑制抖动);
 - 2. 对分组进行应答, 发送ack
- 根据Dijkstra算法计算最短路径, 把邻居的信息汇总成图

健壮性: 如果路由器不能正常工作会发生什么?

- LS
 - 结点会广播错误的链路开销 (到邻居的开销)
 - 每个结点只计算自己的路由表
- DV
 - 结点会广播错误的路径开销 (到全网的开销)
 - 每个结点的路由表被别的结点使用, 错误会传播到全网

例如, 一个人把自己的路由表插入校園网并宣称自己到其他路由距离最短, 于是所有路由都转发给他了, 但他的路由不转发——变成一个路由黑洞

路由信息的复杂性

- LS
 - 路由信息向全网发送 把自己对邻居的认识 (准确) 发送给全网
 - N个节点, E个链路的情况下, 发送O(NE)个报文
- DV
 - 仅在邻居节点之间交换 把自己对全网的认识 (不一定准确) 发送给邻居
- 注意
 - LS发送的是链路信息, DV发送的是到所有结点的向量信息
 - LS信息定期创建 (30分钟) 或发生重大事件时创建, DV定期创建 (30秒钟)
 - LS发布增量信息, DV发布全部信息

收敛 (Convergence) 速度

- LS 收敛比较快
 - 使用最短路径优先算法, 算法复杂度为O(nlogn)
 - n个结点 (不分包括源结点), 需要n*(n+1)/2 次比较
 - 使用更有效的实现方法, 算法复杂度可以达到O(nlogn)
 - 可能存在路由振荡 (oscillations)
- DV Bellman-Ford算法
 - 收敛时间不确定
 - 可能会出现路由循环
 - count-to-infinity问题

【DV有但LS没有的优点】 (因此DV现在还在使用) DV的开销计算尺度是一致的 (可以把带宽、延迟等因素加权计算出统一的), 但LS可能各个路由算各自的, 互连时难以度量。因此在不同国家/运营商之间 (往往不便透露路由策略) 网络互连使用DV (距离向量) 算法。

拥塞: 网络上分组过多, 性能下降

拥塞产生的原因:

- 设备问题 —— 网络设备处理器性能低
- I/O问题 —— 高速端口输入, 低速端口输出; 多个输入对应一个输出
- 拥塞控制 vs. 流控制的差别:
 - 拥塞控制是全局问题, 解决通信子网和数据流问题 (涉及主机、路由器等)
 - 流控制是局部的点到点传输问题, 一般基于反馈控制, 解决快发慢收问题 (例如滑动窗口)

IP协议 (Internet Protocol)

IP头: 20个字节的固定部分 + 0-40个字节的变长部分。Version, IHL (注意单位是32-bit word, 即4 bytes), Type of Service, Total length, Identification, DF, MF (若分片, 除最后一个片段外都要置More Fragments位), Fragment offset (除最后一个片段外的所有片段的长度必须是8字节的倍数), TTL (最大值为255), Protocol, Header Checksum, Source address, Destination address, Options

IP地址: 网络号 + 主机号

有类地址 (A类0, B类10, C类110, D类1110, E类11110)

ABC的主机号都按字节对齐, D没有网络号 + 主机号, 表示多播, E是保留

【注意】全0表示本网络 / 本主机, 全1表示广播地址, 因此进行IP地址分配时要保留这两个, 不用于分配

子网: 子网掩码高len位全1, 与IP地址做AND得到网络地址。

开环控制

- 通过好的设计来解决问题, 避免拥塞发生
- 拥塞控制时, 不考虑网络当前状态

闭环控制

- 基于反馈机制
- 工作过程
 - 监控系统: 发现何时何地发生拥塞
 - 把发生拥塞的消息传给能采取动作的站点
 - 调整系统操作, 解决问题

CMIP协议 (Internet Control Message Protocol)

主要用来报告错误和测试, ICMP报文封装在IP分组中

ARP协议 (Address Resolution Protocol)

解决网络层地址 (IP地址) 与数据链路层地址 (MAC地址) 的映射问题

- 若目的主机在同一子网内, 用目的IP地址在ARP表中查找, 否则用缺省网关的IP地址在ARP表中查找
- 若未找到, 则发送广播分组, 目的主机收到后给出应答, ARP表增加一项
- (每个主机启动时会广播自己的IP-MAC地址, ARP表项中的动态ARP有生存期)

ARP攻击: 攻击者发出伪造的ARP响应, 更改目标主机ARP缓存中的IP-MAC项, 造成网络中断/中间人攻击; 存在于局域网

RIP协议 (Routing Information Protocol)

属于内部网关协议 (IGP), 封装在UDP分组中, 采用距离向量算法 (DV)

故障处理:

- 180s未收到邻居路由声明, 则认为其失效, 链路失效信息迅速传播到全网
- 使用毒性反转 (从A学到的消息还告诉A, 但是计算开环会发现是不可达的)

OSPF协议 (Open Shortest Path First)

属于外部网关协议 (EGP), 封装在TCP分组中, 采用链路状态算法 (类似距离向量, 每个BGP网关向邻居网关所有通往目的地的链路: 网关W收到了邻居网关X的路径。Path(W, Z) = u, Path(X, Z))

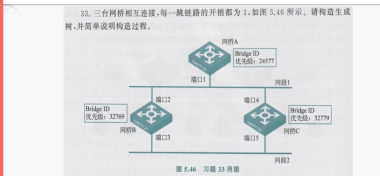
BGP协议 (Border Gateway Protocol)

属于外部网关协议 (EGP), 封装在TCP分组中, 采用距离向量算法 (类似距离向量, 每个BGP网关向邻居网关所有通往目的地的链路: 网关W收到了邻居网关X的路径。Path(W, Z) = u, Path(X, Z))

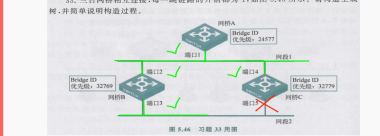
BGP消息: Open, Update, KeepAlive, Notification

为什么域间和域内的路由有所不同?

- 策略
 - 域间路由跨越不同管理域, 要控制流量如何路由
 - 域内路由属于同一管理域, 不需要定义策略
- 规模
 - 分層路由降低了路由表的大小, 减小了路由更新的流量
- 性能
 - 域内路由: 着重于性能 所以走最短路径
 - 域间路由: 策略更为重要 最短路径不一定最优, 可能考虑非路由因素 (不同运营商电信/联通等)



- 选择根网桥: 选择网桥ID最小的网桥作为根网桥, 即网桥A
- 非根桥选择根端口: 非根桥选择到根开销最小的端口为根端口, 开销相同则选择端口ID最小的
 - 网桥B选择端口2作为根端口
 - 网桥C选择端口4作为根端口
- 网段确定指定端口: 网段选择到根开销最小的端口为指定端口, 开销相同则选择网桥ID最小的, 若还相同 (同一个网桥) 则选择端口ID最小的
 - 网段1选择网桥A的端口1作为指定端口
 - 网段2选择网桥B的端口3作为指定端口



设备	端口	类型	状态
网桥 A (根)	端口 1	指定端口	转发
网桥 B	端口 2	根端口	转发
网桥 B	端口 3	指定端口	转发
网桥 C	端口 4	根端口	转发
网桥 C	端口 5	非指定端口或根端口	阻塞

【背诵】网桥技术

- 交换机的LAN是连接 网桥: 帧级别的处理
- 网桥的定义: 工作在数据链路层的一种网络互连设备, 在互连的LAN之间实现帧的存储和转发
- 使用场景
 - 连接相隔距离过长的两个LAN
 - 将负载很重的大LAN分隔成使用网桥互连的几个LAN以减轻负担 (隔离冲突域), 同时防止出故障的站点阻塞全网
 - 中继器不能隔离冲突域, 网桥/交换机可以隔离冲突域
 - 互连不同类型的LAN (不同类型协议之间的翻译)
 - 有助于安全保密
- 工作原理: 连接不同LAN的网桥具有多个MAC子层和多个物理层
- 互联网需要解决的问题
 - 3种不同的LAN (802.3/4/5) 互联共有9种组合, 每种组合需要做10种操作中的几种

共同需要的操作

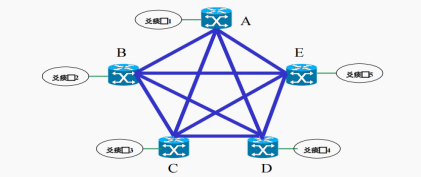
- 不同LAN帧格式——转换 (可能需要重新计算校验和)
- 不同的LAN速率——缓存
- 不同的最大帧长度——丢弃无法转发的帧
- 高层协议的计时器设置

SNMP（简单网络管理模式，Simple Network Management Protocol）

封装在 UDP 分组中。
五大管理功能：性能管理、故障管理、配置管理、记账管理、安全管理
SNMP网管模型的四个组成部分：agent、manager、information (MIB)、protocol (SNMP)
被管理节点：运行SNMP代理程序（agent），维护本地数据库（记录状态历史）
管理工作站：运行专门的网络管理软件（manager），使用管理协议与被管理节点上的SNMP代理通信，维护管理数据库
管理信息：每个站点使用多个对象描述自己的状态，所有的对象组成MIB（管理信息库）
管理协议（SNMP）：定义了网络管理工作站和SNMP代理之间的通信过程 & 协议数据单元（PDU=SDU+PCI）
管理工作站用来查询、修改被管理节点的状态
被管理节点用来向管理工作站产生“陷阱”（trap）报告
管理信息结构SMI：变量被定义为对象（object），相关对象们被集合成组（group），组被汇集成模块（module）。
管理信息库MIB：包含10个组，manager向agent查询的就是保存在MIB中的对象的值。
【注意】被管理节点是server，管理工作站是client

DNS：域名解析过程：应用->区域域名服务器-(若找不到)->根域名服务器-(若找不到)->authoritative域名服务器
根域名服务器
可能不知道 authoritative域名服务器，但知道中间的域名服务器，而中间域名服务器知道如何与authoritative域名服务器联系
因此出现了两种请求模式 ——
Recursive query（递归式）：问一个人就是把任务完全交给它
【优点】向用户提供较好的服务
【缺点】根域名服务器的负担重
Iterated query（反复式）：可以从别人那里得到额外信息。别人：“我不知道，但可以问它”
【优点】负担较小
【缺点】提供的服务不太好（需要自己查，而不是甩了锅就完事）

如图所示，5台路由由器组成全相连的网络，每台路由由器有5个接口，分别连接其它4台路由由器和1个局域网，每个局域网最多连接20台计算机，每台计算机分配1个IP地址。如果只有一个IPv4地址块202.112.10.0/24可供分配，请给出一种合理的地址分配方案，分别给出每个局域网的地址空间和路由器每个端口的地址以及它们的掩码。



- 5台路由由器之间有10条链路，每个链路连接的两个端口构成一个子网，需要4个IP地址。
- 202.112.10.（0，4，8，12，16，20，24，28，32，36）255.255.255.252
- 每个局域网网分配32个地址
- 202.112.10.（64，96，128，160，192），255.255.255.224

A发生的事件		初始	S ₂₀	R ₀₁	R ₁₂	S ₃₂	S _{2n} timeout	R _{NAK4}
							S ₂₂	
A方发送窗口	下界	0	0	1	2	2	2	4
	上界	2	3	3	3	4	4	4

A发生的事件		初始	R ₂₀	S ₀₃	S _{NA}
A方接收窗口	下界	2	3	3	
	上界	6	7	7	

【背诵】网络传输技术——SONET/SDH
o 80年代提出
o TDM（时分复用）技术，同步系统，由主时钟控制
o SONET路径：路径（path）>线路（line）>段（section）
o 复用基于字节

- OC-3c的c表示级联，非复用

计算机网络体系结构（续）

服务分类：面向连接的服务和无连接服务

面向连接的服务

- 当使用服务传送数据时，首先建立连接，然后使用该连接传送数据。使用后，关闭连接
- 特点：顺序性好

无连接服务

- 直接使用服务传送数据，每个包独立进行路由选择
- 特点：顺序性差

注意：连接并不意味着可靠，可靠要通过确认、重传等机制来保证

分层原则：
－ 优点：模块化，易于拓展；各层可独立演进，增强系统灵活性；便于异构互联
－ 缺点：协议间协同优化困难
端到端原则：
－ 优点：简化网络核心，降低网络复杂度和成本；提高系统灵活性，有利于新应用快速部署；保证可扩展性
－ 缺点：对实时性和可靠性要求高的应用支持不足；在网内进行一些细粒度的修改更加困难；端系统负担加重，弱终端体验可能变差

端到端原则：网络核心功能（如可靠传输、流量控制、数据加密等）优先在端系统（应用层 / 传输层）实现，中间网络节点（路由器、交换机等）仅提供“尽力而为”的转发服务；下层（如数据链路层、网络层）仅在必要时（如高误码率场景）补充实现，目的是优化性能而非替代端系统的核心功能。

多路复用技术

由于一条传输线路的能力远远超过传输一个用户信号所需的能量，为了提高线路利用率，经常让多个信号同时共用一条物理线路

常用的有四种方法

- 时分复用 TDM（Time Division Multiplexing）
 - T1载波，分成 24 个信道
- 频分复用 FDM（Frequency Division Multiplexing）
- 波分复用 WDM（Wavelength Division Multiplexing）
- 码分复用 CDM（Code Division Multiplexing）

A发生的事件		初始	S ₂₀	R ₀₁	R ₁₂	S ₃₂	<div>S_{2n}timeout</div> <div>S₂₂</div>	R _{A0K4}	S ₄₂	S ₅₂	S ₆₂	R ₂₅	<div>R_{NAK5}</div> <div>S₅₃</div>	R _{ACK7}
A方发送窗口	下界	0	0	1	2	2	2	4	4	4	4	5	5	7
	上界	2	3	3	3	4	4	4	5	6	7	7	7	7

A发生的事件		初始	R ₂₀	S ₀₃	<div>S₄₁</div> <div>S_{NAK3}</div>	R ₅₁	<div>ACKtimeout</div> <div>S_{ACK5}</div>		R ₅₁
A方接收窗口	下界	2	3	3	3	5	5	5	6
	上界	6	7	7	7	1	1	1	2

a. 电路交换（电话网、ISDN等）
原理：直接利用可切换的物理通信线路，连接通信双方
3个阶段：建立电路 传输数据 拆除电路
特点：发数据前必须建立点到点物理通路，建通路时间长，但数据传送延迟短
时分复用：时间分为帧，帧分为时槽（时槽在帧内的相对位置决定所属会话）
收发双方需要同步，非永久会话需要动态绑定时槽到一个会话
b. 报文交换——存储转发方式
原理：信息以报文（逻辑上完整的信息段）为单位进行存储转发
特点：线路利用率高；要求中间结点缓冲大；延迟时间长
c. 分组交换（包交换）——存储转发方式（可以认为是报文交换的改进）
原理
存储转发的单位——分组（比报文小，可定长可变长）

源节点把报文分成分组，信息以分组的单位（在中间节点）存储转发 目的节点把分组合成报文
统计复用，按需分配信道资源，不需要等待时槽；用附加的分组头区分数据
特点
每个分组独立进行路由选择
网络结点设备中不预先分配资源，（统计复用）线路利用率率高
是相比电路交换最大的优势，有效利用带宽+处理突发性的数据
易于重传，可靠性高
易于开始新的传输，让紧急信息优先通过
开销增加
问题：需要处理拥塞？需要复杂的路由器，难以保证端到端服务质量（延迟、带宽）
分类
数据报分组交换（IP网络等）
每个分组均带有网络地址（源、目的），可走不同的路径
虚电路分组交换（ATM网络等，ATM见chap2）？
电路交换和分组交换的结合
数据以分组形式传输，来自同一流的分组合通过同一预先建立的路径（虚电路）
传输，分组头不需要包含完整的地址信息（建立时会发带有全称网络地址的呼叫分组）
保证分组的顺序，但来自不同虚电路的分组合可能交错
路由器需要维护虚电路的状态信息
3个阶段：建立 传输 拆除

【背诵】物理层的四个特性

o 机械特性：主要定义物理连接的边界点（按插装量）

o 电气特性：规定传输二进制数位时，线路上传输的信号电压高低、阻抗匹配、传输速率和距离限制

o 功能特性：主要定义各条物理线路的功能（分为数据控制/定时/地）

o 规程特性：主要定义各条物理线路的工作规程/时序关系

【背诵】计算机网络的发展历史、互联网的发展历史

- 1940年代：计算机诞生，ENIAC
- 1960~1964：分组交换网络，Paul Baran（【其他】里有细节）
- 1969：ARPANET
- 1970年代：各类网络技术（X.25分组交换网，SNA、DNA等专用网络体系结构）以太网、teInet
- 1979：TCP/IP成熟
- 1980年代：ISO/OSI、LAN大发展、Internet初具规模
 - FTP、NFS、Email、USENET
- 1990年代：Internet商业化、Web技术（www之类的）
 - 中国局域网：Novell，TCP/IP
 - Internet在中国开始大规模发展
 - 1995年：CERNET（中国教育和科研计算机网）
- 2000年以后：网络应用、移动互联网、IPv6 **QQ**
 - 2006年：CNGI-CERNET2（Pv6相关）

模拟信号发送（模拟信号）

o 模拟数据(声音)

o 数字数据(二进制脉冲)

数字信号发送（数字信号）

o 模拟数据

o 数字数据(二进制脉冲)

数字信号发送的优点：价格便宜，对噪声不敏感；

数字信号发送的缺点：易受衰减，频率越高，衰减越厉害

1983年 ISO 的 OSI 模型正式成为国际标准

o 物理层 (Physical Layer)：在物理线路上传输原始的二进制数据位 (Bit)

o 数据链路层 (Data Link Layer)：在有差错的物理线路上提供无差错的数据传输 (Frame)

o 网络层 (Network Layer)：控制通信子网提供源点到目的点的数据传送 (Packet)

o 传送层 (Transport Layer)：为用户提供端到端的数据传送服务

o 会话层 (Session Layer)：为用户提供会话控制服务 (安全认证)

o 令牌管理和同步，例如，在数据流中插入检查点 (checkpoint)

o 表示层 (Presentation Layer)：为用户提供数据转换和表示服务

o 应用层 (Application Layer)

以 TCP/IP 协议为核心的 Internet 网络体系结构

- TCP/IP 参考模型把物理层和数据链路层合起来称为：Host-to-Network
 - 物理层：在物理线路上传输原始的 二进制数据位
 - 数据链路层：在有差错的物理线路上提供无差错的数据传输
- Internet层（网络层）：控制通信子网提供源点到目的点的 IP 包传送，实现异构网络互联
- 传送层：提供端到端的数据传送服务，TCP 和 UDP
- 应用层：提供各种 Internet 管理和应用服务功能

协议：同等层次中，通信双方信息交换必须遵守的规则（语法+语义+定时关系）

系）（目的主机第n层收到的=源主机第n层发出的）
服务：同一实体上下层间交换信息时必须遵守的规则

- 分类：面向连接的服务/无连接服务
- 连接并不意味着可靠，可靠要通过确认、重传等机制来保证
- 服务原语（由一组接口原语描述）：请求、响应、指示、确认

接口：定义了下层向上层提供的原语操作和服务

计算机网络的组成（两级结构）：资源子网+通信子网

- 资源子网（服务器，计算机）
- 通信子网（信道，路由器、交换机等网络互连设备）
 - 点到点通信（交换式通信）
 - 典型拓扑结构：star/ring/tree/complete/intersecting rings/irregular
 - 关键技术：**路由选择**
 - 广播通信
 - 典型拓扑结构：bus/ring
 - 关键技术：**通道分配**
 - 静态·分时切片，简单·利用率低
 - 动态使用，集中式/分布式仲裁，复杂·利用率高

【背诵】计算机网络的发展历史、互联网的发展历史

- 1940年代：计算机诞生，ENIAC
- 1960~1964：分组交换网络，Paul Baran（【其他】里有细节）
- 1969：ARPANET
- 1970年代：各类网络技术（X.25分组交换网，SNA、DNA等专用网络体系结构）以太网、teInet
- 1979：TCP/IP成熟
- 1980年代：ISO/OSI、LAN大发展、Internet初具规模
 - FTP、NFS、Email、USENET
- 1990年代：Internet商业化、Web技术（www之类的）
 - 中国局域网：Novell，TCP/IP
 - Internet在中国开始大规模发展
 - 1995年：CERNET（中国教育和科研计算机网）
- 2000年以后：网络应用、移动互联网、IPv6 **QQ**
 - 2006年：CNGI-CERNET2（Pv6相关）