数据链路层

两台主机所经过的网络可以是多种不同类型的，中间伴随着封装、解封装的一系列形态。不同的链路层可能采用不同的数据链路层协议，传送的是帧。
包含有如下信道类型：

1. 点对点信道：采用一对一的点对点通信
2. 广播信道：采用一对多的广播通信，使用专用的共享信道协议来协调这些主机的数据发送

数据链路层的功能：封装成帧，透明传输，差错控制，流量控制

- **封装成帧**：在一段数据的前后添加首部SOH和尾部EOH构成一个帧，进行了帧定界。具体定界方法：
  - 字符计数法：在帧头部使用一个计数字段表明帧内字数，数值包含首部和尾部。（对帧的正确性影响最大）
  - 字符填充的首尾定界符：使用特殊字符来界定帧的开始DLE_STX与结束DLE_ETX
  - 比特填充的首尾标志：采用特定比特模式01111110来标志一帧的开始和结束
  - 违规编码法：例如曼彻斯特编码的比特1对应*高低*电平，比特零对应*低高*电平，而*高高*和*低低*电平在数据比特中是违规的
- **透明传输**：
  - 若在要传输的二进制代码恰好出现SOH和EOT一样的，会找到错误的帧边界。可采用字节填充或字符填充（转义字符）
  - 传输过程中可能会产生比特差错
- **差错控制**：传输错误的比特占总数的比例称为误码率BER。于是传送的帧广泛使用循环冗余检验CRC的检验技术（一般只检验，不纠错）
  - 在发送端把数据分组，设每组k个比特，每组M后再添加n位冗余码用于差错检测，并一起发出去
  - CRC会对每一个接收到的帧都会校验，但无法检测到帧丢失、重复
  - eg. 与串位101101对应的多项式为`x^5 + x^3 + x^2 + x^0`

额流量控制★★★

流量控制是让接收方来控制发送方发送数据的速度，便于接收方能够及时接收和处理数据，以免造成数据溢出和丢失。
发收双方AB分别维持一个发送窗口和接收窗口，**发送窗口**在没有收到确认的情况下可以连续把窗口内的数据全部发送出去，**接收窗口**只允许接收落入窗口内的数据。
停止-等待机制：每发送一帧都要等待接收方发来应答信号后才能发送下一帧。
滑动窗口机制：接收窗口向前时并且接收方发送了确认帧，控制发送窗口向前移动。

按窗口大小分类

按照窗口大小，流量控制可以分为三种：发送窗口1，接收窗口1（停止等待）；发送窗口N，接收窗口1（GBN）；发送窗口N，接收窗口M（SR）。
`N≥M>1`

停止等待协议

发收窗口数量都为1。发送端给接收端发送数据，等待接收端确认回复ACK，并停止发送新数据包，等待期间开启计时器。发送方发送数据后要对数据标号，第一次发送的数据标号为0，出错重传数据为1。

网络利用率（经常计算最大利用率）：
利用率 = 发送数据时间/总时间，
设发送数据时间t1，传播时间t2，确认帧的发送时间t3，传播时延t2，那么利用率h = t1/(t1+t2+t3+t2)。
有两种情况：① 等长确认帧/捎带：t1=t2；② 确认帧忽略不计：t3=0。

后退N帧滑动窗口协议GBN

发送窗口N，接收窗口1。发送N帧数据给接收端，接收端确认回复ACK，等待期间停止发送新的数据包并开启计时器。
连续发送，累计确认，哪里出错从哪儿传。当网络质量很好时，停止等待协议的性能很好。

网络利用率：
设发送窗口w，发送时间t1，传播时延t2，确认帧发送时间t3，传播时间t2，利用率h = w×t1/(t1+t2+t3+t2)≤1

选择重传滑动窗口协议SR

发送窗口N，接受窗口M（N≥M）。*连续发送，选择确认，哪里出错传哪里*。
对窗口编号确需确认的位数是n，满足2^n ≥ 发送窗口+接收窗口。

网络利用率：w×t1/(t1+t2+t3+t2)≤1

数据链路层流量控制

发送缓存和接收缓存；接收窗口大小为1时可保证帧的有序接收；窗口大小在传输过程中是固定的；只有窗口向前滑动并且接收方发送确认帧后，发送方才有可能向前滑动。

窗口大小的讨论：停止等待（发送1接收1），GBN（发送2^n-1 接收1），SR（发送2^(n-1) 接收2^(n-1)）

利用率的讨论：w×t1/(t1+t2+t3+t2)≤1，2×t2=RTT。
① 停止等待 w=1，GBN w=2^n-1，SR w=2^(n-1)；
② h ≤ 1
③ 捎带或等长确认，t1 = t3；
④ 确认帧时间很小或忽略不计时，t3 = 0

带宽讨论：① 最大带宽（实际带宽）；② 理论带宽（题目中给定）。
实际带宽 ≤ 1 = 理论带宽；
h = w×L/(t1+t2+t3+t2)，发送方窗口大小w，帧长L。等长确认时t1=t3，帧时间很小时t3忽略不计

介质访问控制★★★

总线型介质访问：分时和共享，使用一对多的广播通信方式，因此必须用专用的共享信道协议来协调这些主机的数据发送。
介质访问控制分为：信道划分介质访问控制，随机访问介质访问控制（争用型介质访问控制），轮训访问介质访问控制。

信道划分介质访问控制

带宽访问时，可以在一条介质上同时携带多个传输信号来提高传输系统的利用率，也就是多路复用。具体分为：频分、时分、波分、码分 多路复用。

复用允许用户使用一个共享信道进行通信，降低成本，提高率用率。

- **频分复用FDMA**：用户分到一定频带后在通信过程中始终占用该频带。所有用户在同样时间占用不同的频率带宽资源
- **时分复用TDMA**：将时间切位各个时间片，让用户分时使用
- **波分复用WDMA**：光的分频复用，所以只适用于光纤。使用同一根光纤同事传世多个光载波信号
- **码分复用CDMA**：把每个比特时间分为m个短间隔，称为码片，每个站被指派一个唯一的m比特码片序列：发送比特1，则发送自己的m比特码片；发送比特0，则发送该码片序列的二进制反码
    - 让站的码片和各个分组进行向量内积（规格化内积）：内积结果正值，该站发送数据1；内积结果负值，该站发送数据0；内积结果0，该站不发送数据

随机访问介质控制

当若干计算机使用一条信道发送数据，需要去共享信道。随机接入就意味着所有用户都可以根据自己的意愿随机地发送信息，这样会容易产生冲突而导致冲突用户发送数据失败。

- **ALOHA协议**：网络中任何节点需要发送数据时，可以不进行任何检测就发送。若在一段时间内没有收到确认，则认为传输过程发生冲突。发生冲突后等待一段时间重发，直到发送成功。成功率18.4%
- **CSMA协议**：由ALOHA协议改进。发送数据前侦听其它设备是否在发送数据。侦听策略分为：
    - 坚持型：信道空闲时持续发送数据，忙时持续监听
    - 非坚持型：信道空闲时理解发送数据，忙时等待随机时间再监听
    - p-坚持型：信道空闲时以概率p发送数据、以概率1-p不发送数据，忙时等待随机时间再监听
- **CSMA/CD协议**：应用于有线网。当多个站点同时在总线发送数据，总线电压变化值增大，当检测到信号电压摆动超过一定门限值，就会认为总线上至少两个站在同时发送数据（碰撞）。
    - 工作过程分为：先听后发，边听边发，冲突停发，随机重发
    - 当某个站监听到总线空闲时，可能总线并非真的空闲。最先发送数据帧的站，最多在发送数据帧后至多2τ(两倍的端到端往返时延) 就可以知道发送的数据帧是否遭受到碰撞
- **CSMA/CA协议**：应用于无线网。发送数据前检查信道状态，等信道空闲时再等待一段时间后检测信道是否空闲。若空闲则直接发送数据，否则随机等待一段时间后重发。有三种信道空闲检测方式：
    - 能量检测：对信道能量进行检测，大于一定值时认为信道被占用
    - 载波检测：对接收信号与本地伪随机码PN码进行运算比较，超出一定值则表示信道被占用
    - 能量和载波混合检测：先向目标端发送请求传送报文RTS，等待收到目标端响应报文CTS，发送端才开始发送数据。若没有收到确认帧则会重传，经过若干次重传仍然失败后则会放弃重传

轮询访问介质访问控制

主要用在令牌环局域网。典型协议是令牌传递协议。
令牌环局域网把多个设备安排为一个物理或逻辑连接环，令牌在这个环上依次传递。若有设备需要发送数据，则在等待令牌传递到该设备后，由令牌承载数据发送到接收端。

局域网的数据链路层★

构建局域网后，局域网内的主机在同一网络。局域网覆盖地理范围小、只在相对独立的局部范围内，专门铺设的传输介质进行联网、传输效率高，通信延迟时间短、可靠性高，支持多种传输介质。
主要技术要素：网络拓扑结构，传输介质，介质访问控制方法。

局域网的标准：以太网

DIX EthernetV2是第一个局域网产品规约，IEEE802.3是第一个IEEE标准。二者只有很小的差别，可以将802.3局域网简称为以太网。
IEEE802将局域网分为 逻辑链路控制LLC子层、媒体介入控制MAC子层。
与接入到传输媒体有关的内容都在MAC子层，LLC子层与传输媒体无关。任何协议的局域网对LLC子层都是透明的。

以太网提供无连接的不可靠服务，尽最大努力交付。发送的数据采用曼彻斯特编码。
以太网资源的争用采用CSMA/CD协议。10Mbit/s的一台用以51.2μs为争用期，期内可发送512bit(64字节)，若前64字节均无冲突，则后续数据就不会发生冲突。

最短有效帧长 = 争用期×发送速度 = 2×(介质长度/传播速度) × 发送速度，
以太网规定最短有效帧为64字节，则小于64字节的帧都是由于冲突而一场终止的无效帧。

以太网的MAC层

以太网上的计算机都连接在一根总线上，易于实现广播通信。
对于一对一通信，则将接收站的硬件地址写入帧首部的目的地址字段，当数据帧中的目的地址与适配器的硬件地址一致，才能收到该数据帧。

局域网中**硬件地址/物理地址/MAC地址**，802标准所说的地址严格意义上是每个站的名字或标识符。
MAC地址由48位构成，前3字节是组织唯一标识符，后3字节是扩展唯一标识符。
MAC地址类型：单播帧(一对一)，广播帧(一对全体)，多播帧(一对多)。后二者只用于目的地址。

网络接口板/通信适配器/网络接口卡NIC/网卡。所配备重要功能：进行串并行转换，对数据进行缓存，在计算机的操作系统安装设备驱动程序，实现以太网协议。
适配器每从网络上收到一个MAC帧就先用硬件检查MAC帧中的MAC地址：若是发往本站的帧则收下，否则丢弃。

以太网的帧格式

以太网重用的MAC帧有：DIX EthernetV2，IEEE的802.3标准。最常用V2。 |目的地址6 |源地址6 |类型2 |数据46~1500 |FCS4 |

无效的MAC帧：数据字段的长度与字段的值不一致；帧的长度不是整数个字节；收到的FCS查出有误；数据字段长度不在46~1500字节之间（有效的MAC帧长度为64~1518字节）。
检查出无效的MAC帧丢弃，以太网不负责重传丢弃帧。

FCS的存在目的是校验，当传输媒体误码率为1×10^(-8)时，MAC子层可使未检测到的差错小于1×10(-14)。

在MAC帧前面插入由硬件生成的8个字节，前7字节是前同步码（迅速实现MAC帧的比特同步），后1字节是帧开始定界符。

广域网的数据链路层

广域网的目的是为了远距离传输而存在，大多数依赖于海底光缆。
范围涵盖很大的物理区域，覆盖从几十公里到几千公里，能链接多个城市或国家或洲以提供远距离通信。
使用协议：PPP、HDLC，由节点交换机组成，层次为下三层。

PPP协议

应满足的要求：简单，封装成帧，透明性，多种网络层协议，差错检测，检测连接状态，最大传送单元，网络层地址协商，数据压缩协商。

不需要的功能：纠错，流量控制，序号，多点线路，半双工或单工链路。

三个组成部分：一个将IP数据报凤凰岛串行链路的方法；链路控制协议LCP（创建链路完成链路的启动、测试、任选参数的协商和最终链路的断开）；网络控制协议NCP（调用链路层创建阶段选定的网络控制层协议）。

帧格式：

```
|F(7E) |A(FF) |C(03) |协议 |信息部分（IP数据报，不超过1500字节） |FCS |F(7E) |
|1 |1 |1 |2 |信息部分（IP数据报，不超过1500字节） |2 |1 |
```

PPP协议以`0x7E`开头

当PPP在异步传输时，就用一种特殊的字符填充法；当PPP在同步传输链路时，协议规定采用硬件来完成比特填充。

字符填充：
将信息字段中出现的`0x7E`替换为二字节序列`(0x7D),(0x5E)`，`0x7D`替换为二字节序列`(0x7D,0x5D)`。

透明传输问题：
在发送端发现5个连续的1会立刻填入一个0，在接收端则发现连续5个1则会将其后面一个0删除。

PPP协议的特点：不使用序号和确认机制；面向字节，所有PPP帧长度都是整数字节；只支持全双工链路；只支持全双工链路；面向连接的不可靠的协议；具有身份验证功能。

PPP协议的运行分为四个阶段

建立链路LCP，验证PAP、CHAP，网络控制协商NCP，终止PPP链路LCP

- *建立链路LCP*：PPP首先用LCP在链路两端建立连接，并且在两端动态协商一些参数，例如认证方式、是否支持压缩和MLP等
  - 若要完成建立、配置、测试、终止数据链路连接工作就需要通信两端互相交换LCP报文，基本上有三类：链路配置报文，链路维护报文，链路终止报文
  - LCP协议在建立两端链路链接还会经历的四种状态：初始化状态Initial 或 准启动状态Starting，请求发送Request-Sent，确认发送Ack-Sent，打开Open
  - LCP协商一些配置选项，发生LCP的配置请求帧：配置确认帧，配置否认帧，配置拒绝帧
- *验证PAP、CHAP*：验证协议有很多，包括 口令验证协议PAP、挑战握手身份验证协议CHAP、微软挑战握手身份验证协议2版本MS-CHAPv2，可扩展的身份验证协议EAP。其中PAP和CHAP用的最多
- *网络控制协商NCP*：负责建立并配置IP、IPX、AppleTalk等网络层协议，以及建立并中毒那多种第三层协议会话。NCP是PPP协议的另一个子层，主要作用是在通信亮度那协商网络层的参数（IP地址、DNS等）。PPP协议支持多协议栈，所以在不同协议栈中的NCP名称不一样（在IP协议栈中称为IPCP、在IPX协议栈中称为IPXCP）
- *终止PPP链路LCP*：LCP对链路直接终止

数据链路层设备★

碰撞域/冲突域指网络中一个站点发出的帧会与其他站点发出的帧产生碰撞或冲突的那部分。
广播域指网络中的任一设备发出的广播通信都能被网络中所有其它设备所接收。
在数据链路层使用**网桥**来扩展局域网。网桥工作在数据链路层，根据MAC帧目的地址对收到的帧进行转发。收到一个帧后会先检查此帧的目的MAC地址，再确定将该帧转发到对应接口。

网桥的优缺点： **优点**：过滤通信量，扩大了物理范围，提高了可靠性，可互联不同物理层、MAC子层、速率的局域网。
缺点：存储转发增加了时延，MAC子层没有流量控制功能，不同MAC子网的网段桥接在一起的时延更大，不适用于用户数高于几百个的大通信量局域网（容易广播风暴）。

透明网桥

目前使用最多的事透明网桥，“透明”指网络上的站点不知道所发送的帧将经过几个网桥，网桥对各站是不可见的。

透明网桥具有自学习算法来处理收到的帧和建立转发表。每收到一个帧后，将纪录其*源地址*和*进入网桥的接口*、*帧进入网桥的时间*，作为转发表中的一个项目。
收到帧后进行自学习，查找转发表与收到的源地址匹配。若无，则再转发表中增加项目[源地址，进入的接口，时间]。
转发帧时，匹配转发表：若无，则通过所有其它接口进行转发；若有，则按转发表给出的接口进行转发；若转发表给出的接口就是该帧进入网桥的接口，则应该丢弃。

广播时可能会存在回路问题，造成大规模网络资源浪费。于是引入一个生成树协议STP，不改变网络实际拓扑，但在逻辑上切断某些链路，使得一台主机到其它主机的路径都是无环路的树状结构。

原路由网桥

易安装但网络资源利用不充分。在发送帧时将详细路由信息放在帧首部。源站以广播形式向目的站发送一恶搞发现帧，每个发现帧都记录所经过的路由。
发现帧达到目的站时就会沿各自的路由返回源站，源站在得知这些路由后，从所有可能路由中选择一个最佳路由。凡从该源站向目的站发送帧的首部，都必须携带源站所确定的这一路由信息。

交换式网桥/以太网交换机/第二层交换机

通常有十多个接口（本质是一个多接口的网桥，可见交换机工作在数据链路层）。
每个接口以全双工的方式直接与主机相连，交换机能同时联通许多对接口让每一个相互通信的主机能进行无碰撞传输数据（如同独占通信媒体）。

工作方式

- **直通式交换**：检查前六个字节后转发，认为小于六个字节的数据报是碎片而不进行转发（转发延迟=发送6字节的发送延迟）。快速但缺乏安全性，无法支持不同速率的端口交换
- **存储转发式**：先把数据收下来，检查无误后再查找转发表发送（有误则丢弃）。可靠性高，但延迟较大

设备带宽的讨论

集线器和中继器处于同一冲突域，共享带宽。
网桥和交换机以全双工工作方式，独占带宽（对于N个接口的交换机而言，总带宽为N×单用户带宽）。但对于普通10Mb/s的共享式以太网，每个用户只有10Mb/s÷用户数。

虚拟局域网VLAN

在一个物理LAN内划分出多个虚拟LAN，每个VLAN是一个广播域，这就缩小了广播域范围，各个VLAN之间不能直接通信。

VLAN中的交换机端口可以分为：访问链接AccessLink；汇聚链接TrunkLink。
设置VLAN的顺序是：生成VLAN，设定访问链接（决定各端口属于哪个VLAN）。

设定访问链接的手法，分为两种：静态VLAN（事先固定），动态VLAN（根据所连计算机而动态改变设定）。

动态VLAN分为：基于MAC地址的VLAN，基于子网的VLAN，基于用户的VLAN

补充

- 数据链路层的功能：为网络层提供服务，帧定界、同步、透明传输，流量控制和差错控制
- 连续ARQ：GBN、SR。若窗口值以n比特编码，发送窗口最大值为2^n-1
- 有序接收：停止等待、GBN
- 发送窗口大小为a，则最少需要$n \geq \log_2(a+1)$位序列号来保证协议不出错
- 若GBN协议发送了0~7帧，收到了0、2、3号帧的确认，则发送方需要重复4
- A、B、C通过CDMA共享链路，A的码片序列是(1,1,1,1)，C从链路上收到的序列为(2,0,2,0,0,-2,0,-2,0,2,0,2)，计算C收到A发送的数据：
    - C收到的序列可排序为[[2,0,2,0],[0,-2,0,-2],[0,2,0,2]]，逐行乘以A的码片序列后，可得到(4,-4,4)，所以C收到A的数据为101
- CSMA/CD协议中的“争议期”：信号在最远两个断电之间往返传输的时间
- 以太网中发生介质访问冲突，则按照二进制指数回退算法决定下一次重发时间，因为该算法考虑到了网络负载对冲突的影响
- 采用二进制指数回退算法处理冲突时，首次重传的帧是再次发生冲突概率最低的
- 二进制回退算法中，设k为碰撞次数：$k \leq 10$，$k=k$；$10 \leq k \leq 16$，$k=10$；$k \geq 16$，报错
- 以太网的MAC协议提供无连接的不可靠服务