1. 计算机网络和因特网
2. 什么是因特网：两种描述方法：

* 具体的构成：构特网的基本硬件和软件。
* 提供的服务：分布式应用提供服务的网络基础设施。

2. 协议：控制网络中信息接收和发送的一组软件（定义了通信实体之间发送、接收报文的格式和传输顺序，以及收到报文所采取的动作。 不同的协议完成不同的通信任务）。

3. 物理媒体：将网络中不同端系统互相连接起来的物理线路。是进行数据传输的物理通路，通过传播电磁波或光脉冲来发送比特流。分为两大类：分为两大类：*导引型媒体*：电波沿着固体媒体传播。如双绞线、同轴电缆或光缆等。*非导引型媒体*：电波在空气或外层空间中传播。如无线电等。

①双绞线电缆：多对双绞线捆扎成一根电缆，并在外面覆盖上防护层；

*屏蔽双绞线STP*：抗电磁干扰能力强，贵，安装复杂。

*非屏蔽双绞线UTP*：分为若干类。常用于LAN。

②同轴电缆：套在一起的两个同心铜导体。内导体传递数据 。外导体用作地线及屏蔽干扰。特点：抗干扰能力强、数据率高。

③光纤：一种细而柔软的、能够引导光脉冲的媒体，每个脉冲表示一个比特（0或1）。

光缆：多个光纤集中在一起。特点：速率高、抗电磁干扰好、距离传输远。 用于长途电话网络，因特网的主干。成本高、不适于短途传输（如LAN）。

④陆地无线电信道：利用无线电波在自由空间传播实现通信。

⑤卫星无线电信道：通过一颗通信卫星连接两个或多个位于地球的微波发射方/接收方。

4. 网络交换方式：分组交换和电路交换

分组交换：源端系统将应用层报文划分为较小的数据块（未来的发展趋势）。

电路交换：通信双方必须先建立一个*专用的连接（电路）*，一直维持，直到通信结束。

分组和电路比较：电路交换效率不高：预先分配传输链路，空闲时，浪费链路时间。分组交换不适合实时服务：端到端时延不确定；分组交换带宽共享好，简单，有效，成本更低。分组交换按需分配链路，利用率高。

5. 分组交换网络中的延迟及计算

分组传输过程：从源主机出发，通过一系列路由器传输，最后到目的主机。

产生四种时延：节点处理时延、排队时延、传输时延和传播时延等。

节点总时延：各时延累加。节点总时延=处理时延+排队时延+传输时延+传播时延

处理时延：查比特差错，定输出链路。通常是微秒级或者更低。

排队时延：分组等待在链路上传输的排队时间。

传输时延：将分组的所有比特推（传）向链路所需要的时间。通常是微秒级或者更低。

传输时延= *L / R*（R= 链路的传输速率 (bps)，*L* = 分组长度 (比特)）

传播时延：一个比特从链路的起点到下一节点（路由器）传播所需要的时间。毫秒级。 以链路的传播速率传播。传播速率*s*：信号在线路上单位时间内传送的距离。速率范围2×108m*/*s ～ 3×108m*/*s。传播时延= *d* / *s* （*d* ：两个节点之间的距离）

6. TCP/IP的分层模型，各层PDU的名称和功能

应用层：提供各种网络应用。传输应用报文。

运输层：在应用程序客户机和服务器之间提供传输应用层报文服务( 进程到进程间的数据传输 )。传输报文段 。

网络层：主机和主机之间传输网络层分组。

链路层： 在邻近单元之间传输分组。

物理层：在节点之间传输比特流。

1. 应用层
2. 安全TCP套接字层(SSL)

套接字：同一台主机内应用层与运输层之间的接口。

TCP协议能保证交付所有的数据，但并不保证这些数据传输的速率以及期待的传输时延。

TCP协议不适合实时应用

①面向连接的服务（分为三阶段）

建立连接（握手过程）：客户机程序和服务器程序之间互相交换控制信息，在两个进程的套接字之间建立一个TCP连接。

传输报文： 连接是全双工的，即连接双方的进程可以在此连接上同时进行报文收发。

拆除连接：应用程序报文发送结束。

②可靠的传输服务：通信进程可以无差错、按适当顺序交付发送的数据。 没有数据丢失和重复。

③拥塞控制：当发送方和接收方之间的网络出现拥塞时，会抑制发送进程速率。对整个网络有益。

2. Web应用和HTTP协议

①基本术语：

Web页(文档)：由若干对象（即文件）组成

URL：Uniform Resource Locator。统一资源定位符。标识万维网WWW上的各种文档，全网范围唯一。

浏览器（客户机）：是Web应用的用户代理，用于显示所请求的Web页，提供导航功能和配置属性。实现了HTTP协议的客户机端。

Web服务器：用于存贮Web对象（由URL寻址）。 实现HTTP协议的服务器端。

②HTTP的特性：无状态，即HTTP是无状态协议，服务器不保存关于客户机的任何信息。

③HTTP连接：

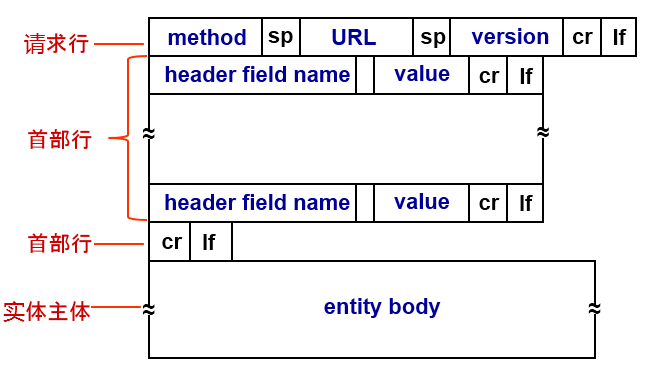
a.非持续连接 HTTP：每个TCP连接在服务器返回对象后关闭。每个TCP连接只传输一个请求报文和一个响应报文。浏览器可同时打开多个连接：并行的TCP连接：并行数大于1，默认打开5～10个；串行的TCP连接：最大并行数为1。

非持续连接缺点：服务器负担重，每一个请求对象建立和维护一个新的连接；每一个对象的传输时延长，包含两个RTT时延，一个用于TCP建立，一个用于请求和接收对象

b.持续连接HTTP：每一个对象的传输时延长：包含两个RTT时延，一个用于TCP建立，一个用于请求和接收对象。相同客户机与服务器之间的后续请求和响应报文通过相同的连接进行传送或同一服务器上的多个Web页也可以通过一个持久TCP连接传送给同一个客户机。连接经一定时间间隔(超时间隔)未被使用，服务器就关闭该连接。

持续连接的两种方式：非流水线方式，客户机只能在前一个响应接收到之后才能发出新的请求；流水线方式客户机可一个接一个连续产生请求（只要有引用就产生），即在前一个请求接收到响应之前可以产生新的请求，服务器一个接一个连续发送相应对象。

④请求和响应报文的首部行格式：



④COOKIE技术

*Cookie*：允许Web站点跟踪、识别用户；服务器可以限制用户访问，或把内容与用户身份关联，包括四个部分：a.在HTTP响应报文中有一个cookie 首部行；b.在HTTP请求报文中有一个cookie 首部行；c.用户主机中保留有一个 cookie 文件并由浏览器管理；d.Web站点的后端数据库保存cookie。

⑤Web缓存

Web缓存器(Web cache)：也叫代理服务器；能够代表起始服务器来满足HTTP请求的网络实体；Web缓存器既可以是服务器也可以是客户机。

3. 文件传输协议FTP ：两种连接

控制连接：用于在两主机间传输控制信息（如用户标识、口令等）；是持久的。

数据连接：用于准确传输文件；是非持久的。

4. 电子邮件：组成及其使用的协议

组成：用户代理、邮件服务器、简单邮件传输协议SMTP

协议：发送方：用户代理用SMTP将邮件推入其邮件服务器 🡪 邮件服务器再用SMTP将邮件转发到接收方的邮件服务器；接收方：通过其用户代理使用一个邮件访问协议（不是SMTP），从其邮件服务器上取回邮件。协议种类：POP3(第三版的邮局协议)、IMAP(因特网邮件访问协议)、HTTP。

5. DNS的功能和查询流程（DNS: 因特网的目录服务）PS:这一段ppt很乱，不好整理

功能：报文在网络中传输，使用IP地址；*域名系统DNS (Domain Name System)*，进行主机名到IP地址的转换；

迭代查询；

递归查询；

缓存与记录更新：一旦任何名字服务器学习到了名字映射，它就缓存该映射；

DNS记录:DNS分布式数据库的所有DNS服务器共同存储着资源记录，提供了主机名到IP地址的映射

第三章 传输层

1. UDP协议特性及其实现（UDP:用户数据报协议）

特性：UDP 是无连接的，即发送数据之前不需要建立连接；

UDP 使用尽最大努力交付，即不保证可靠交付，同时也不使用拥塞控制；

UDP 没有拥塞控制，很适合多媒体通信的要求；

UDP 支持一对一、一对多、多对一和多对多的交互通信：DNS、SNMP；

UDP上的可靠传输： 在应用层增加可靠性；应用层错误回复。

UDP 的首部开销小，只有 8 个字节；

UDP 是面向报文的；

应用层交给 UDP 多长的报文，UDP 就照样发送，即一次发送一个报文；

接收方 UDP 对 IP 层交上来的 UDP 用户数据报，在去除首部后就原封不动地交付上层的应用进程，一次交付一个完整的报文；

应用程序必须选择合适大小的报文。

2. 校验和的实现思想 UDP 校验和：对传输的数据进行差错检测。

发送方:将数据段看成16bit的整数序列；校验和: 数据段内容相加 (1的补码和)；发送者将校验和值放入UDP的校验和域

接收方:计算接收到数据段的校验和；检查计算的校验和是否等于校验和域中的值:NO – 检测到错误；YES – 没有检测到错误。

3. TCP协议特性及其实现 TCP：面向连接传输

TCP报文，固定报头为20字节，典型字段

连接管理：初始化 TCP 变量:序号、缓冲区和流控信息；*客户机：*连接的发起方；*服务器：*接受客户请求

可靠传输：

rdt1.0: 经可靠信道的可靠传输：底层信道非常可靠：无比特差错；无分组丢失。发送方、接收方的单独FSM:发送方将数据发向底层信道；接收方从底层信道读取数据。

rdt2.0: 具有比特差错的信道：底层信道模型使分组中的比特可能受损，利用校验和来检测比特差错。（rdt2.0有重大缺陷）

rdt2.1: 发送方处理受损的ACK/NAK；

rdt2.2: 一种无NAK的协议：rdt2.2假设：报文在传输过程中可能出错、ACK传输可能出错、ACK可能丢失。与rdt2.1一样的功能，仅使用ACK代替NAK，接收方对最后正确接收的分组发送ACK。接收方必须明确地包括被确认分组的序号。发送方收到冗余的ACK将导致和 NAK 相同的动作：*重传当前分组*。接收端必须给出ACK号；发送端必须检查收到的ACK号。

rdt3.0: 具有差错和丢包的信道：下面的信道也能丢失分组（数据或ACK）；方法:

发送方等待ACK一段“合理的”时间。rdt3.0 能够工作，但性能不太好

流水线协议：流水线: 发送方允许发送多个、“传输中的”，还没有应答的报文段。增加利用率。

流量控制：接收方控制发送方，发送方不能发送太多、太快的数据让接收方缓冲区溢出，即：发送方不能淹没接收方。

拥塞控制：抑止发送方速率来防止过分占用网络资源；

拥塞：非正式地: “太多的源发送太多太快的数据，使网络来不及处理”表现在：丢包，长延时。

控制拥塞的两类方法：

端到端的拥塞控制:不能从网络得到明确的反馈；从端系统根据观察到的时延和丢失现象推断出拥塞；这是TCP所采用的方法。

网络辅助的拥塞控制:路由器为端系统提供反馈；一个bit指示一条链路出现拥塞；指示发送方按照一定速率发送。

第四章 网络层

1. 路由器工作原理，基于目的网络的路由，不提供源地址认证。

路由器的两个关键功能：运行选路算法/协议(RIP, OSPF, BGP)网络层转发功能：将分组从路由器的输入链路传送到适当的输出链路

路由器结构：输入端口、交换结构、输出端口、选路处理器

1. 网际协议IP

因特网网络层的三个主要组件：IP协议、选路组件：决定数据报从源到目的地所流经的路径、ICMP（互联网控制报文协议）：报告数据报中的差错和对某些网络层信息请求进行响应。

IP报文：IP 数据报格式：由首部和数据两部分组成。首部：固定长度，共 20 字节，所有 IP 数据报必须具有。首部固定部分后面是一些可选字段，长度可变。

生存时间(8 位)记为 TTL (Time To Live)数据报在网络中可通过的路由器数的最大值。数据报每经过一台路由器，TTL值减1。若TTL=0，则该数据报必须丢弃。

协议号是将网络层与运输层绑定到一起的黏合剂；端口号是将运输层和应用层绑定到一起的黏合剂。（选择或判断会考吧）

IP编址：编址方法：分类的 IP 地址、子网的划分、构成超网

分类的 IP 地址：每一类地址都由两个固定长度的字段组成，其中一个字段是网络号 net-id，它标志主机（或路由器）所连接到的网络，而另一个字段则是主机号 host-id，它标志该主机（或路由器）。两级的 IP 地址可以记为：IP 地址 ::= { <网络号>, <主机号>}。

IP 地址的一些重要特点：a. IP地址是一种分等级的地址结构；b. 实际上 IP 地址是标志一个主机（或路由器）和一条链路的接口；c. 用转发器或网桥连接起来的若干个局域网仍为一个网络，因此这些局域网都具有同样的网络号 net-id；d. 所有分配到网络号 net-id 的网络，范围很小的局域网，还是可能覆盖很大地理范围的广域网，都是平等的。

子网的划分：划分子网纯属一个单位内部的事情。单位对外仍然表现为没有划分子网的网络；记法为：IP地址 ::= {<网络号>, <子网号>, <主机号>}。

无分类编址CIDR划分子网：1987 年，RFC 1009 就指明了在一个划分子网的网络中可同时使用几个不同的子网掩码。使用变长子网掩码 VLSM可进一步提高 IP 地址资源的利用率。在 VLSM 的基础上又进一步研究出无分类编址方法，它的正式名字是无分类域间路由选择 CIDR。无分类的两级编址的记法是：IP地址 ::= {<网络前缀>, <主机号>}。

NAT：网络地址转换

实现: NAT 路由器必须:*出数据报:* 每个外出的数据报用(NAT IP地址, 新port #) *代替* (源IP地址, port #)远程的客户机/路由器的响应，将用(NAT IP地址, new port #)作为目的地址 ；记住(在NAT转换表中)每个 (源IP地址, port #)到(NAT IP地址, 新port #) 转换对；入数据报: 对每个入数据报的地址字段用存储在NAT表中的(源IP地址, port #)替代对应的 (NAT IP地址, 新port #) 。

IPv6协议

初始动机:32-bit地址空间很快将会被完全分配完

附加的动机:首部格式帮助速率处理/转发；首部变化以促进QoS

IPv6 数据报格式:

固定长度 40 字节首部

不允许分片

IPv6地址表示

冒号十六进制表示法 105.220.136.100.255.255.255.255.0.0.18.128.140.10.255.255

冒号十六进制表示为：69DC:8864:FFFF:FFFF:0:1280:8C0A:FFFF

零压缩表示法 FF0C:0:0:0:0:0:B1

零压缩表示为： FF0C::B1

IPv6首部：*优先级 :* 标识特殊流的分组优先权；*流标签:* 标识在相同“流”中的数据报(流的概念没有很好定义)；*下一个首部:* 标识数据的上层协议。

1. 选路算法 选路目的：决定从源到目的地通过网络的“好的路径”(路由器序列)

//详细的看看课本或者ppt，有可能考大题。

链路状态选路算法：Dijkstra最低费用路径算法（最短通路算法）：以源节点为起点，每次找出一个到源节点的费用最低的节点，直到把所有的目的节点都找到为止

距离向量算法：距离向量选路DV算法

是一种迭代的、异步的和分布式的算法。分布式：每个节点都从其直接相连邻居接收信息，进行计算，再将计算结果分发给邻居。迭代：计算过程一直持续到邻居之间无更多信息交换为止。自我终结：算法能自行停止。异步：不要求所有节点相互之间步伐一致地操作。

层次选路：按区域或自治系统的形式组织路由器。将一个大的系统划分成若干小系统（自治系统），自治系统之间再互连。

AS内部选路协议：*RIP选路信息协议：*基于距离向量的路由协议。*OSPF开放最短路径优先：*采用Dijkstra最短费用路径算法，是一种链路状态协议

AS间选路协议：*BGP边界网关协议：*基于距离向量的路由协议。相邻BGP路由器相互交换路径信息。

1. 因特网中的选路

内部网关协议：RIP( 选路信息协议)、OSPF(开放最短路优先)、IGRP

外部网关协议：BGP(边界网关协议)、BGP4

第五章 数据链路层和局域网

1. 链路层提供的服务

成帧：把网络层数据报封装成链路层帧，再传送到链路上。

首部包括若干字段：如编号、物理地址等。

不同的链路层协议，帧格式可能不同

链路访问：由媒体访问控制MAC协议定义帧在链路上传输的规则。

点对点链路：一个发送方和一个接收方，MAC协议比较简单(或不存在)，即任何时候只要链路空闲，发送方都能够发送帧。

广播链路：多个节点共享一个链路（多路访问），使用MAC协议协调多个节点的帧传输。

差错检测：帧在传输时有可能出现*比特差错* (1->0、0->1)

差错检测用来检测是否存在一个或多个差错。

*发送节点：*在帧中设置差错检测比特；

*接收节点：*对收到的帧进行差错检测。

通过硬件实现。

1. 差错检测技术

奇偶校验（最基本的方法）、二位奇偶校验能够纠正1位错误

发送方：在要发送的信息*D*（*d*位）后面附加一个奇偶校验位，使“1”的个数是奇数（*奇校验*）或偶数（*偶校验*），一起传输发送（*d+*1位）。

接收方：检测收到的信息（*d+*1位）中“1”的个数。

*偶校验：*发现奇数个“1”，至少有一个比特发生差错（奇数个比特差错）。

*奇校验：*发现偶数个 “1”，至少有一个比特发生差错。

CRC计算：*DR* 能被 *G* 模 2 运算整除：即

*D*×2*r* XOR *R = nG*

等价的等式两边都用 *R* 异或，得到

*D*×2*r* *= nG* XOR *R*

即用 *G* 来除*D*×2*r*，余数值刚好为 *R*。

*R的计算：*将数据 *D* 后面添加 *r* 个0，除以给定的生成多项式 *G*，所得余数即为*R*（*r位*）。



CRC特点：能检测小于 *r*+1 位的突发差错、任何奇数个差错 。

1. 链路类型：点对点和共享

*两种网络链路：点对点链路*：链路两端各一个节点。一个发送和一个接收。

*广播链路：* 多个节点连接到一个共享的广播信道。

1. 共享介质使用多址访问技术 目的：协调多个节点在共享广播信道上的传输。

信道划分：主要有TDM、FDM、CDMA三种。设信道支持 *N* 个节点，传输速率是 *R* b/s。

a.时分多路复用 (TDM)：将时间划分为*时间帧*，每个时间帧再划分为*N个时隙*（长度保证发送一个分组），分别分配给*N*个节点。每个节点只在固定分配的时隙中传输。特点：避免冲突、公平：每个节点专用速率*R/N* b/s；节点速率有限：*R/N* b/s；效率不高：节点必须等待它的传输时隙。

b.频分多路复用 (FDM)：将总信道带宽*R* b/s划分为*N*个较小信道（频段，带宽为*R/N*），分别分配给*N*个节点。特点：与TDM类似：避免冲突、公平：*N*个节点公平划分带宽；节点带宽有限、效率不高：节点带宽为*R/N。*

随机访问：发送节点以信道全部速率（*R* b/s）发送；发生冲突时，冲突的每个节点分别等待一个随机时间，再重发，直到帧(分组)发送成功。

轮流协议：多路访问协议理想特性：只有一个节点活动时，吞吐量 *R* b/ s；有 *M* 个节点活动时，吞吐量 *R/M* b/ s。

a.轮询协议：指定一个主节点，以循环的方式轮询每个节点。并告诉节点能够传输的最大帧数。特点：消除冲突和空时隙，效率高；有轮询时延，活动节点不能立即传输帧，等待被轮询；如果主节点失效，整个信道都不能用。

b.令牌传递协议：没有主节点。设置一个令牌(token，小的专用帧)；

令牌以固定顺序循环传递，给节点传输机会；节点收到令牌；有帧要发送，传输，传完后将令牌转发到下一节点；否则，直接将令牌转发到下一节点。特点：令牌传递是分散的，效率高；一个节点的失效会使整个信道崩溃；一个节点忘记释放令牌，必须恢复令牌到环中。

5. 链路层编址

MAC地址（LAN地址、物理地址）：是节点“网卡”本身所带的地址（惟一）；

MAC地址长度通常为6 字节，共 248 个；6字节地址用16进制表示，每个字节表示为一对16进制数；“网卡”的MAC地址是永久的（生产时固化在其ROM里）。

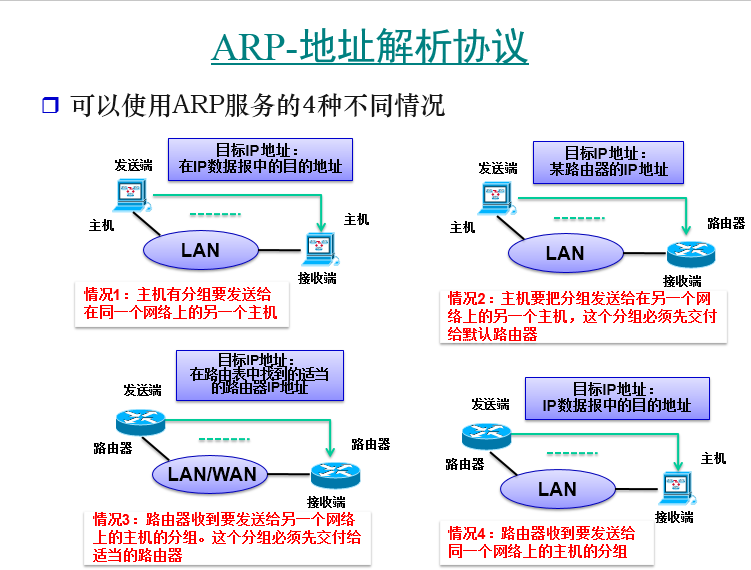
MAC地址分配： 由专门机构IEEE管理物理地址空间。负责分配六个字节中的前三个字节（高24位，地址块）

MAC 地址是平面结构：带有同一网卡的节点，在任何网络中都有同样的MAC地址。

IP地址具有层次结构*：*当节点移动到不同网络时，节点的IP地址发生改变。

MAC地址识别：*发送适配器：*将目的MAC地址封装到帧中，并发送。所有其他适配器都会收到这个帧；*接收适配器：*检查帧的目的MAC地址是否与自己MAC地址相匹配：匹配：接收该帧，取出数据报，并传递给上层。需要中断“父节点”；不匹配：丢弃该帧

ARP协议DHCP协议

ARP（Address Resolution Protocol）地址解析协议，负责完成逻辑地址向物理地址的动态映射，将32位逻辑地址（IP地址）转化为48位物理地址（MAC地址）。

6.以太网技术

连接方式：星型拓扑结构

以太网技术定义链路层和物理层的实现方式

10Base-2：以太网卡、T型连接器、细同轴电缆线段、两个“端接器”（吸收信号）组网费用低。

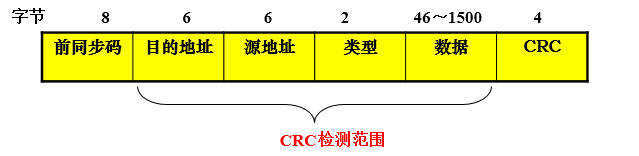
10Base-T和100Base-T：两种技术相似，只是速率不同帧格式。特点：使用星形拓扑；使用星形拓扑；每个接口通过RJ-45连接器用两对双绞线与节点的适配器点对点连接（发送/接收；适配器和集线器之间连接最长100 *m；任意两个节点之间最长200 m。*

吉比特以太网和10Gb/s以太网

吉比特以太网：1000Mb/s；标准以太网帧格式，与10BaseT和100BaseT技术兼容；允许点对点链路和共享的广播信道；采用星形拓扑，其中心是一个集线器或交换机；可作为主干互联多个以太网LAN；使用光纤或5类UTP电缆；

10吉比特以太网：将以太网技术扩展到了点对点广域网(WAN)链路。

以太网的帧结构



*发送方：*发送适配器将IP数据报封装成以太网帧，并传递到物理层；*接收方：*接收适配器从物理层收到该帧，取出IP数据报，并传递给网络层。

以太网提供无连接、不可靠的服务：

无连接服务：通信时，发送方适配器不需要先和接收方适配器“握手”。

不可靠的服务：接收到的帧可能包含比特差错。

共享式以太网采用CSMA/CD介质访问控制技术

物理层采用曼彻斯特编码

曼彻斯特编码：每位信号的中间都有一个跳变，两个作用：表示数据，根据跳变方向判断数据“1”或“0”；做同步时钟：接收方根据跳变来同步接收。

连接设备使用集线器和交换机。

交换机的工作原理

1. 交换机转发和过滤：过滤(filtering)：交换机判断一个帧是应该转发到某个接口还是丢弃；转发(forward)：交换机决定一个帧应该被指向哪个接口，并引导到该接口；过滤和转发通过交换机表(switch table)完成。
2. 过滤和转发的原理：交换机从接口*x*收到一个帧；根据目的MAC地址查表；找到对应项：确定转发接口*y，*判断目的节点与源节点是否在同一个网段：同段（x = y）：丢弃此帧（过滤）；不同段（x ≠ y）*：*将该帧放到接口*y*的输出缓冲区（*转发*）保证同一个网段中通信的帧，不被交换机转发到另一个网段去。未找到：向所有(除接收接口外)其它接口转发，进入自学习。

**Ps：根据计网复习ppt和平常上课ppt整理出来的，如果有遗漏或者错误请谅解。**

**不喜勿喷。**