**OSI**:物理层:传输比特流。数据链路层:提供无差错的数据传输帧.网络层:控制通信子网提供源点到目的点的数据传送（将数据报封装成包或者分组）运输层:为用户提供端到端的数据传送服务（TCP:报文段UDP:用户数据报）会话层:为用户提供会话控制服务（SPDU协议数据单元）表示层:为用户提供数据转换和表示服务（PPDU）应用层:提供多种应用协议满足用户需求（APDU）**TCP/IP四层协议**:网络接口层:对应七层中的数据链路层和物理层Internet层:控制通信子网提供源点到目的点的 IP 包传送.运输层:提供端到端的数据传送服务(TCP 和 UDP协议)应用层:提供各种 Internet 管理和应用服务功能**.网络层代表性协议**:IP协议.ICMP网际控制报文协议.路由协议.ARP协议.IGMP网际组管协议.传输层代表性协议:TCP传输控制协议.用户数据报协议UDP.应用层代表性协议:HTTP.SMTP.DNS.**下层**向上层提供服务,并对其屏蔽实现这些服务的细节,服务是水平的,协议是垂直的.**数据帧结构**-目的MAC6|源MAC6|类型2|数据|校验4.中继器集线器工作在物理层.**网桥**交换机工作在数据链路层.集线器不能隔离冲突域和广播域而且扩大冲突域.交换机能够隔离冲突域.**ARP协议**:解析出IP协议对应的硬件地址.目的MAC|源MAC|C2|D2|E2|06|04|0001|发送者MAC6|4|接受者MAC6|4|4|.**以太网最短帧长**:64bit. 目的:为了确保帧的第一位未被冲突而正确到达终点，必须保证可能的冲突信号返回时尚未发送结束，因为如在2 τ 内发送完毕，则无法检测冲突 .如何设计最短帧长: 在极限条件下，一个局域网中两个收发器间（允许接4个中继器）的最大距离为2500 m，往返5000 m，同轴电缆的时延特性为4.33 μs/km（相当于电磁波以77%的光速在电缆上传播），即如遇冲突，端到端并返回的时延为21.65 μs。然而，这是理想的时延，考虑到中继器的额外时延，最坏的情况下取估计时延为45 μs，再加上强化冲突需发送48 bit，接收方要接收到48 bit后才确认冲突，即再增加4.8 μs，共49.8 μs，所以通常以太网取51.2 μs为争用期的时间长度（传输512 bit，即64字节的时间），即帧的长度至少为64个字节.**CSMA/CD(**带冲突检测的载波侦听多路访问 )工作原理: 在一帧传输完成后的时间t0，想要发送的站点都可以尝试发送如两个或多个站点同时发送则发生冲突判断出冲突后，立即停止发送，并强化冲突，延时一个随机时隙数后，再重复以上过程.子网掩码与IP地址逐位相与得到网络地址.**默认网关**:进入路由器的接口ip地址.**子网掩码:**使路由器很方便的从数据报中的目的IP地址中提取出所要找的子网的网络地址.子网掩码中的1对应原来的网络号+子网号,0对应主机号.**ICMP协议**:ICMP报文作为IP层数据报的数据,类型:差错报文,控制报文,请求应答报文.作用: 提供了一种把通信服务中的差错向源站点报告的机制.IP协议提供的是尽力而为的通信服务数据报的丢失、重复、延迟、乱序在所难免 .**ICMP协议应用**: 测试报文的可达性、路由跟踪命令tracert、得到路径中最小的MTU.**ping**工作原理: 使用ping命令（即调用ping过程）时，将向目的站点发送一个ICMP回应请求报文（包括一些任选的数据），如目的站点接收到该报文，必须向源站点发回一个ICMP回应应答报文，源站点收到应答报文（且其中的任选数据与所发送的相同），则认为目的站点是可达的，否则为不可达.**tracert**命令工作原理: tracert过程是通过ICMP数据报超时报文来得到一张途经路由器列表的 .源主机向目的主机发一个IP报文，并置hop为1，到达第一个路由器时，hop减1，为0，则该路由器回发一个ICMP数据报超时报文，源主机取出路由器的IP地址即为途经的第一个路由端口地址.接着源主机再向目的主机发第二个IP报文，并置hop为2，然后再发第三个、第四个IP数据报，… …直至到达目的主机.**TCP三次握手**: 第一次握手：建立连接时,客户端发送syn包(syn=j)到服务器,并进入SYN\_SEND状态,等待服务器确认；第二次握手：服务器收到syn包,必须确认客户的SYN（ack=j+1）,同时自己也发送一个SYN包（syn=k）,即SYN+ACK包,此时服务器进入SYN\_RECV状态；第三次握手：客户端收到服务器的SYN＋ACK包,向服务器发送确认包ACK(ack=k+1),此包发送完毕,客户端和服务器进入ESTABLISHED状态,完成三次握手。**非正常的连接建立过程**(出现延迟的重复TPDU时三次握手的工作过程 ):来自一个已经释放连接的主机1的延迟重复的连接请求，该TPDU在主机1毫不知晓的情况下到达主机2。主机2通过向主机1发送一个接受连接请求的TPDU来响应该TPDU，并声明自己的序号为y(seq=y,ACK=x)，主机1收到这个确认后感到莫名其妙并当即拒绝，主机2收到了主机1 的拒绝才意识到自己受到了延时的重复TPDU的欺骗并放弃该连接。据此，延时的重复请求将不会产生不良后果 . **非正常的连接建立过程**(子网中同时有作废的CR和ACC的情况 ): 主机2收到了一个延时的CR并做了确认应答。在这里，关键是要认识到主机2已经声明使用y作为从主机2到主机1进行数据传输的初始序号，因此主机2十分清楚在正常情况下，主机1的数据传输应捎带对y确认的TPDU。于是，当第二个延时的TPDU到达主机2时，主机2根据它确认的是序号z而不是y知道这也是一个过时的重复TPDU。因此也不会无故建立无人要求的连接 . **非对称释放**:一方中止连接，则连接即告中断缺陷：可能导致数据丢失.对称释放:A提出中止请求，B同意即中止 问题：B如何知道A 收到了它的确认?**四次释放**: 1）关闭客户端到服务器的连接：首先客户端A发送一个FIN，用来关闭客户到服务器的数据传送，然后等待服务器的确认。其中终止标志位FIN=1，序列号seq=u。 2） 服务器收到这个FIN，它发回一个ACK，确认号ack为收到的序号加1。3） 关闭服务器到客户端的连接：也是发送一个FIN给客户端。 4） 客户段收到FIN后，并发回一个ACK报文确认，并将确认序号seq设置为收到序号加1。首先进行关闭的一方将执行主动关闭，而另一方执行被动关闭。**TCP协议和UDP协议区别**: 两者在如何实现信息的可靠传递方面有所不同。TCP面向连接包含了可靠性保证机制，而UDP不提供数据传送的保证机制不可靠的、无连接的。TCP在实际执行的过程中会占用大量的系统开销，严重地影响到传输速度。而UDP不考虑可靠性，将安全和排序等功能移交给上层应用来完成，极大地减少了时间，使速度得到了保证。**www上网过程**: 客户端的工作过程举例：假如有用户要访问http://www.ietf.org/rfc.html，则浏览器的工作过程如下：(1) 浏览器确定URL。(2) 浏览器向DNS询问web服务器www.ietf.org的IP 地址。(3) DNS的应答是209.173.57.180。(4) 浏览器和IP 地址为209.173.57.180的80 端口建立一条TCP 连接。(5) 浏览器执行HTTP 协议，发送GET /rfc.html 命令，请求读取该文件。(6) www.ietf.org 服务器返回/rfc.html文件到客户端。(7) 释放TCP 连接。(8) 浏览器显示/rfc.html页面。服务器端的工作过程(1) 接受来自客户(浏览器)的TCP连接：(2) 获取所需文件的名字。(3) 获取文件(从磁盘上)。(4) 将文件返回给客户。(5) 释放该TCP连接.**域名解析DNS概念**: 功能:将主机名映射为IP地址.递归查询:问上级,上级做(根任务重).迭代查询:问上级,上级将地址告诉你,你来做.**三层交换机工作原理**: (1)源主机在发起通信之前，将自己的IP地址与目的主机的IP地址进行比较，如果源主机判断目的主机与自己位于不同网段时，它需要通过网关来递交报文的，所以它首先需要通过一个ARP请求报文获取网关的MAC地址(在源主机不知道网关MAC地址的情形下)，即源主机先发送ARP请求帧以获取网关IP地址对应的MAC地址。(2)网关在收到源主机发来的ARP请求报文后以一个ARP应答报文进行回应，在应答报文中的“源MAC地址”就包含了网关的MAC地址。(3)在得到网关的ARP应答后，源主机再用网关MAC地址作为报文的“目的MAC地址”，以源主机的IP地址作为报文的“源IP地址”，以目的主机的IP地址作为“目的IP地址”，先把发送给目的主机的数据发给网关。(4)网关在收到源主机发送给目的主机的数据后，由于查看得知源主机和目的主机的IP地址不在同一网段，于是把数据报上传到三层交换引擎(ASIC芯片)，在里面查看有无目的主机的三层转发表。(5)如果在三层硬件转发表中没有找到目的主机的对应表项，则向CPU请求查看软件路由表，如果有目的主机所在网段的路由表项，则还需要得到目的主机的MAC地址，因为数据包在链路层是要经过帧封装的。于是三层交换机CPU向目的主机所在网段发送一个ARP广播请求包，以获得目的主机MAC地址。(6)交换机获得目的主机MAC地址后，向ARP表中添加对应的表项，并转发由源主机到达目的主机的灵气包。同时三层交换机三层引擎会结合路由表生成目的主机的三层硬件转发表。以后到达目的主机的数据包就可以直接利用三层硬件转发表中的转发表项进行数据交换，不用再查看CPU中的路由表了。**统一资源定位符URL**:<协议>://<主机>:<端口>/<路径>.使用什么协议获取该万维网文档,万维网文档在哪个主机上,协议具体地址.**ARP地址解析协**议: 如果A主机要对B主机进行数据传输的话:A主机先会查看自己的ARP高速缓存中是否有B主机的MAC地址记录。如果A主机的高速缓存中有B主机的记录，则直接通过这个MAC地址进行数据的传输。如果A主机的高速缓存中没有B主机的记录，则会向局域网的所有主机广播一个ARP请求，寻找B主机的MAC地址。当B主机收到A主机广播的ARP请求后，就会直接给A主机回复一个ARP数据包。当A主机收到B主机发送过来的请求后，将B的MAC地址写入高速缓存中，然后通过该MAC地址，A主机向B主机进行数据的传输.如果A主机和B主机不在同一个局域网的话，但是A主机要向B主机传输数据的话:A主机先通过广播一个ARP请求，找到本网络中的一个路由器的MAC地址，然后将数据包直接给路由器。当路由收到数据包后，如果B主机在同网络中的话，这时通过ARP找到B主机，然后把数据包给B主机。如果B主机不和A主机发送数据的路由器在同一网络内的话，则路由器会通过ARP协议找到下一跳的路由器，然后把数据包发送到该路由上，以此类推。**普通以太网**/IEEE 802.3：采用同轴电缆作为网络介质，传输速率达到10Mb/s.100Mb/s以太网：又称为快速以太网，采用双绞线作为网络介质，传输速率达到100Mb/s.1000Mb/s以太网：又称为千兆以太网，采用光缆或双绞线作为网络介质，传输速率达到1000Mb/s.**交换机工作原理**:交换机主要功能为转发数据帧.交换机学习过程:观察每个端口上的所有流量.记录每一帧的源MAC地址和端口关系.将学习内容添加到过滤表.交换机切入转发方式:最后校验,快速,无用功.存储转发:最先校验,减小无用功,有效工作.VLAN标记加在源MAC地址和类型之间.生成树作用. （1）**切入（直通）转发**，交换机在得到数据包的目的IP地址后就转发，这种方式的优点是转发速度较快，但不对转发的包进行完整性判断，会导致一些数据包碎片在网上传输。（2）**存储转发**，是交换机将一个数据包全部接收下来再转发出去，这种方式的好处就是可以判断一个数据包的完整性和正确性，隔离被破坏的数据包在网上继续流动。但因为是将数据包接收下来再传输，交换的速度比较慢。**滑动窗口原理**：发送的信息帧都有一个序号，从0到某个最大值，0 ~ 2n - 1，一般用n个二进制位表示；发送端始终保持一个已发送但尚未确认的帧的序号表，称为发送窗口。发送窗口的上界表示要发送的下一个帧的序号，下界表示未得到确认的帧的最小编号。发送窗口大小 = 上界 - 下界，大小可变；发送端每发送一个帧，序号取上界值，上界加1；每接收到一个正确响应帧，下界加1；接收端有一个接收窗口，大小固定，但不一定与发送窗口相同。接收窗口的上界表示允许接收的序号最大的帧，下界表示希望接收的帧；接收窗口容纳允许接收的信息帧，落在窗口外的帧均被丢弃。序号等于下界的帧被正确接收，并产生一个响应帧，上界/下界都加1接收窗口大小不变。2三个常见窗口协议：一位滑动窗口协议（1,1）、后退n帧的滑动窗口协议（7,1）、选择性重发滑动窗口协议（4,4）