**1.什么是网络？**从终端系统的角度来看，网络提供一项服务：移动信息。根据他们提供的服务来区分网络类型；服务从延迟、带宽、损失率、端部系统数、服务接口等。以基础设施为中心的视图：电子和光子作为通讯媒介；链接：光纤铜卫星；协议：TCP/IP,ATM,MPLS;功能：路由错误控制拥塞控制。

**2局域网**是一种将小区域内的各种通信设备互连在一起的通信网络。 特点： 高数据传输率、短距离、低出错。拓扑结构 ：星型结构、环型结构、总线型结构 、树型结构 。 传输介质 ：双绞线、基带同轴电缆、光纤、无线 。

2.1**信道分配**。解决信道争用的协议称为介质访问控制协议 MAC（数据链路层协议）

**(1)分配方法**：**a静态分配**：频分多路复用 FDM（波分复用WDM)--原理：将频带平均分配给每个要参与通信的用户；优点：适合于用户较少，数目基本固定，各用户的通信量都较大的情况.缺点：无法灵活地适应站点数及其通信量的变化. 时分多路复用 TDM--原理每个用户拥有固定的信道传送时槽.优点:适合于用户较少,数目基本固定,各用户的通信量都较大的情况;缺点：无法灵活地适应站点数及其通信量的变化.**b动态分配**:信道分配模型的五个基本假设: 站点模型,单信道假设, 冲突假设,连续时间和时间分槽(何时发送),载波监听和非载波监听(能否发送).

**(2)多路访问协议--**控制多个用户共用一条信道的协议 **A.ALOHA:**纯ALOHA--基本思想:用户有数据要发送时,可以直接发至信道; 然后监听信道看是否产生冲突,若产生冲突,则等待一段随机的时间重发.信道效率:S = Ge-2G,18.4%.、分槽ALOHA，（冲突危险区)--基本思想:把信道时间分成离散的时间槽,槽长为一个帧所需的发送时间.每个站点只能在时槽开始时才允许发送.其他过程与纯ALOHA协议相同.信道效率:S = Ge-G,36.8%. **B.载波监听多路访问协议CSMA**--站点在为发送帧而访问传输信道之前，首先监听信道有无载波， 若有载波，说明已有用户在使用信道，则不发送帧以避免冲突,多个用户共用一条线路. **a**.1-**坚持型CSMA:原理**--若站点有数据发送,先监听信道;若站点发现信道空闲,则发送;若信道忙,则继续监听直至发现信道空闲,然后完成发送; 若产生冲突,等待一随机时间,然后重新开始发送过程.**b非坚持型CSMA: 原理--**若站点有数据发送，先监听信道;若站点发现信道空闲,则发送;若信道忙,等待一随机时间,然后重新开始发送过程;若产生冲突,等待一随机时间,然后重新开始发送过程。信道效率比1-坚持CSMA高，传输延迟比坚持CSMA**.c. p-坚持型CSMA( 适用于分槽信道 ):原理--**若站点有数据发送，先监听信道;若站点发现信道空闲,则以概率p发送数据,以概率 q =1- p 延迟至下一个时槽发送.若下一个时槽仍空闲,重复此过程,直至数据发出或时槽被其他站点所占用;若信道忙,则等待下一个时槽,重新开始发送; 若产生冲突,等待一随机时间,然后重新开始发送**C.带冲突检测的载波监听多路访问协议 CSMA/CD 原理--**站点使用CSMA协议进行数据发送;在发送期间如果检测到冲突,立即终止发送,并发出一 个瞬间干扰信号,使所有的站点都知道发生了冲突;在发出干扰信号后,等待一段随机时间,再重复上述过程. **工作状态--**传输周期、竞争周期、空闲周期

**D无冲突协议:1.基本位图协议:原理--**共享信道上有N个站,竞争周期分为N个时槽,如果 一个站有帧发送,则在对应的时槽内发送比特1;N个时槽之后,每个站都知道哪个站要发送帧,这时按站序号发送轻负载下,效率为 d / (N + d);重负载下,效率为 d / (d + 1).**令牌传递**.**二进制下数法**:所有站的地址用等长二进制位串表示,若要占用信道,则广播该位串;不同站发的地址中的位做“ 或”操作,一旦某站了解到比本站地址高位更高的位置被置为“1”,便放弃发送请求.效率:d / (d + log2N). **E 有限竞争协议**--占用信道的策略:a竞争方法:如,CSMA;轻负载下,发送延迟小;重负载下,信道效率低b无冲突方法:如基本位图法;轻负载下,发送延迟大;重负载下,信道效率高.c有限竞争方法: 结合以上两种方法,轻负载下使用竞争,重负载下使用无冲突方法; 基本思路:将站分组,组内竞争**F适应树搜索协议--原理：**站点组织成二叉树;一次成功传输之后,第0槽全部站可竞争信道,只有一个站要使用信道则发送;有冲突则在第1槽内半数站（2以下站）参与竞争.如其中之一获得信道，本帧后的时槽留给3以下的站;如发生冲突,继续折半搜索. 当系统负载很重时,从根结点开始竞争发生冲突的概率非常大.为提高效率,可以从中间结点开始竞争.**G无线局域网协议--特点:**基于蜂窝（cell）的通信;每个蜂窝内只有一个信道（与蜂窝电话不同);一个站点发送的信号,只能被它周围一定范围内的站点 接收到;短距离传输。**与有线局域网不同,**隐藏站点问题/暴露站点问题.**传统的CSMA协议不适合于无线局域网,需要特殊的 MAC子层协议-- MACA：**基本过程:A向B发送RTS,帧，A周围的站点在一定时间内不发送数据,以保证CTS帧返回给A;B向A回答CTS（Clear To Send）帧,B周围的站点在一定 时间内不发送数据,以保证A发送完数据;A开始发送,若发生冲突,采用二进制指数后退算法等待随机时间,再重新开始。**MACAW对MACA协议做了改进:**对每个成功传输的数据帧，都要产生确认帧;增加了（发送站点的）载波监听,发生冲突后,针对每个数据流（相同源和目的地址）执行后退算法,而不是针对每个站点发生拥塞时,站点间交互信息

**2.2三种局域网的比较(1) 802.3:**优点.使用最为广泛;算法简单;站点可以在网络运行中安装;使用无源电缆;轻负载时,延迟为0.缺点:使用模拟器件,每个站点在发送的同时要检测冲突;最短帧长64字节，对于短数据来讲开销太大;无优先级,发送是非确定性,不适合于实时工作; 电缆最长2500米（使用中继器)速率提高时,帧传输时间减少,竞争时间不变（2τ）,效率降低;重负载时,冲突严重(**2)802.4** 优点:发送具有确定性,支持优先级,可处理短帧;使用宽带电缆,支持多信道;重负载时,吞吐量和效率较高. 缺点:使用大量的模拟装置; 协议复杂; 轻负载时,延迟大; 很难用光纤实现**(3)802.5:**优点使用点到点连接,完全数字化;使用线路中心,自动检测和消除电缆故障; 支持优先级,允许短帧,但受令牌持有时间限制,不允许任意长的帧;重负载时,吞吐量和效率较高. 缺点中央监控;轻负载,延迟大.

**3.网桥技术--**网桥（bridge）是工作在数据链路层的一种网络互连设备，它在互连的LAN之间实现帧的存储和转发。作用：互连不同类型的LAN;隔离负载,防止出故障的站点损害全网;有助于安全保密.**(1)透明网桥/生成树网桥:工作原理--**网桥工作在混杂方式,接收所有的帧;网桥接收到一帧后，通过查询地址/端口对应表来确定是丢弃还是转发;网桥刚启动时,地址/端口对应表为空，采用洪泛（ flooding）方法转发帧;在转发过程中采用逆向学习算法 收集MAC地址。网桥通过分析帧的源MAC地址得到MAC 地址与端口的对应关系，并写入地址/端口对应表;网桥软件对地址/端口对应表进行不断的更新，并定时检查,删除在一段时间内没有更新的地址/端口项; 帧的路由过程:目的LAN与源LAN相同，则丢弃帧;目的LAN与源LAN不同,则转发帧;目的LAN未知,则洪泛帧,并逆向学习.**(2) 源路由网桥**:原理-帧的发送者知道目的主机是否在自己的LAN内;如果不在,在发出的帧头内构造一个准确的路由序列,包含要经过的网桥、LAN的编号,并将发出的帧的源地址的最高位置1;每个LAN有一个12位的编号，每个网桥有一个4位的编号网桥只接收源地址的最高位为1的帧，判定是转发还是丢弃;源路由的产生：每个站点通过广播“发现帧”（ discovery frame）来获得到各个站点的最佳路由.若目的地址未知，源站发送“发现帧”，每个网桥 收到后广播，目的站收到后发应答帧，该帧经过网桥时被加上网桥的标识，源站收到后就知道了到目的站的最佳路由。

3.1**网桥**:是工作在数据链路层的一种网络互连设备,它在互连的LAN之间实现帧的存储和转发.**连接 802.X和 802.Y的网桥**:互连时需要解决的相同问题:不同LAN帧格式的转换;不同的LAN速率不同,网桥要有缓存能力;高层协议的计时器设置;不同的LAN支持的最大帧长度不同，分别为1500,8191, 5000.解决办法:丢弃无法转发的帧. **透明网桥/生成树网桥**: 网桥工作在混杂方式,接收所有的帧;网桥接收到一帧后,通过查询地址/端口对应表来确定是丢弃还是转发;网桥刚启动时,地址/端口对应表为空,采用洪泛方法转发帧;在转发过程中采用逆向学习算法 收集MAC地址.网桥通过分析帧的源MAC地址得到MAC 地址与端口的对应关系,并写入地址/端口对应表;网桥软件对地址/端口对应表进行不断的更新,并定时检查,删除在一段时间内没有更新的地址/端口项. **解决多个网桥产生回路的问题**:让网桥之间互相通信,用一棵连接每个LAN的生成树覆盖实际的拓扑结构.**构造生成树**:每个桥广播自己的桥编号,号最小的桥称为生成树的根;每个网桥计算自己到根的最短路径,构造出生成树,使得每个LAN和桥到根的路径最短;当某个LAN或网桥发生故障时,要重新计算生成树;生成树构造完后,算法继续执行以便自动发现拓扑结构变化,更新生成树. **源路由网桥**: 帧的发送者知道目的主机是否在自己的LAN内;如果不在,在发出的帧头内构造一个准确的路由序列,包含要经过的网桥、LAN的编.并将发出的帧的源地址的最高位置1; 每个LAN有一个12位的编号,每个网桥有一个4位的编号;网桥只接收源地址的最高位为1的帧,判定是转发还是丢弃;**源路由的产生**:每个站点通过广播“发现帧”来获得到各个站点的最佳路由.若目的地址未知,源站发送“发现帧”,每个网桥收到后广播,目的站收到后发应答帧,该帧经过网桥时被加上网桥的标识,源站收到后就知道了到目的站的最佳路由.**高速局域网技术:** 光纤分布式数据接口FDDI; DPT; 快速以太网: 将比特时间从100ns缩短为10ns; 千兆以太: 802.3z;

**4.网络层协议（1）网络层**一个网络连接的两个传送实体间交换网络服务数据单元提供功能和规程的方法，它使传送实体独立于路由选择和交换的方式；处理端到端传输的最低层;解决的关键问题是了解通信子网的拓扑结构，选择路由；**为传输层提供服务**a面向连接服务b无连接服务;**实现方式比较**a虚电路:路由器需要维护虚电路的状态信息;在建立连接时花费时间;很容易保证服务质量QoS适用于实时操作，但比较脆弱b数据报:每个数据报都携带完整的目的/源地址，浪费带宽;每次路由时过程复杂;不太容易保证服务质量，但是对于通信线路的故障，适应性很强。**（2）链路状态算法（LS）和距离向量算法（DV）的比较a路由信息的复杂性--**LS路由信息向全网发送n个节点E个链接**O(nE**)消息互发 **DV**仅在邻居间交换b**收敛速度LS**使用最短路径优先算法，算法复杂度为O(n\*2)n个结点（不包括源结点），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：收敛时间不同可能是路由循环，数到无穷的问题**c健壮性**LS节点可以发布不正确的链接成本，每个节点只计算自己的表；DV：可以修正错误的路径成本，每个节点的表被其他错误通过网络传播**（3）拥塞控制与流量控制的差别：**拥塞控制需要确保通信子网能够承载用户提交的通信量，是一个全局性问题，涉及主机、路由器等很多因素；流量控制与点到点的通信量有关，主要解决快速发送方与慢速接收方的问题，是局部问题，一般都是基于反馈进行控制的.**(4)漏桶算法与令牌桶算法的区别：**流量整形策略不同：漏桶算法不允许空闲主机积累发送权，以便以后发送大的突发数据；令牌桶算法允许，最大为桶的大小。漏桶中存放的是数据包，桶满了丢弃数据包；令牌桶中存放的是令牌，桶满了丢弃令牌，不丢弃数据包**.(5)网络互连设备**a中继器:物理层设备，在电缆段之间拷贝比特;对弱信号进行放大或再生,以便延长传输距离b网桥:数据链路层设备，在局域网之间存储转发帧;网桥可以改变帧格式c多协议路由器:网络层设备，在网络之间存储转发包;必要时，做网络层协议转换d传输网关:传输层设备，在传输层转发字节流e应用网关:应用层设备，在应用层实现互连；half-gateway（半网关）**（6）级联虚电路与无连接网络互连的比较：**级联虚电路优点路由器预留缓冲区等资源，保证服务质量;包按序号传输;短包头。缺点路由器需要大量内存，存储虚电路信息;一旦发生拥塞，没有其它路由;健壮性差;如果网络中有一个不可靠的数据报子网，级连虚电路很难实现。无连接网络互连优点无连接网络互连;缺点长包头;包不能保证按序号到达;不能保证服务质量。**(7)隧道技术**源和目的主机所在网络类型相同，连接它们的是一个不同类型的网络，这种情况下可以采用隧道技术**.(8)互联网路由两级路由算法-**内部网关协议（IGP）RIP，OSPF外部网关协议（EGP）BGP、自治系统AS**（8）网络之间互连的纽带是IP（Internet Protocol）协议。4.1Internet控制协议(1)Internet控制报文协议ICMP：**主要用来报告出错和测试；报文类型响应请求,报文不可达、源抑制和超时报文,时间戳;ICMP报文封装在IP包中.(2)**地址解析协议**ARP-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;工作过程建立一个ARP表，表中存放(IP地址,MAC地址)对,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,则发送广播包,目的主机收到后给出应答,ARP表增加一项;每个主机启动时,广播它的（IP地址，MAC地址）映射；ARP表中的表项有生存期,超时则删除.反向地址解析协议RARP解决MAC地址与IP地址的映射问题;主要用于无盘工作站启动;缺点：由于路由器不转发广播帧，RARP服务器必须与无盘工作站在同一子网内一种替代协议BOOTP(使用UDP)(3)RIP-跳数最大15跳,每30秒交换一次.**a内部网关协议**IGP:自治系统AS内使用的路由算法，RIP、OSPF--开放,公开发表、负载平衡、支持隧道技术;**b外部网关协议**EGP:自治系统AS之间使用的路由算法，BGP-[1]外部网关路由协议[2]边界网关协议通过TCP连接传送路由信息;采用路径向量算法，路由信息中记录路径的轨迹;消息类型：OPEN、UPDATE、KEEPALIVE、NOTIFICATION**(3)无类域间路由CIDR--**将剩余的C类地址分成大小可变的地址空间**4.3(1)与IPv4相比IPv6的主要变化:地址变长,由32位变成128位;IP头简化,由13个域减少为7个域,提高路由器处理速度由于IPv6包头定长,取消IHL域；Protocol域取消,用Next header域表示；取消与分段有关的域，IPv6采用不同的分段方法：所有主机和路由器必须支持576字节的包,当主机发送一个大包时,路由器不做分段,而是给主机发一个错误信息，由主机做分段；取消Checksum域.更好的支持选项功能;安全性提高;更注重服务类型。跳数限制8 位;IPv6把原来IPv4首部中选项的功能都放在扩展首部中,并将扩展首部留给路径两端的源站和目的站的主机来处理.数据报途中经过的路由器都不处理这些扩展首部;目的地址基本类型地址--单播多播任播（2）两种向 IPv6 过渡的策略：**使用双协议栈-装有两个协议栈,IPv4和IPv6,使用隧道技术-把IPv6 数据报封装成为IPv4 数据报,整个的 IPv6据报变成IPv4数据报的数据部分。**4.4路由器（1）基本结构**：**网络接口**完成网络报文的接收和.转发引擎负责决定报文的转发路径;**内部交换**为多个网络接口以及路由引擎模块之间的报文数据传送提供高速的数据通路;**路由引擎**由运行高层协议（特别是路由协议）的内部处理模块组成;**路由表**包含了能够完成网络报文正确转发的所有路由信息，它在整个路由器系统中起着承上启下的作用**(2)两种不同的报文处理路径:数据路径:**处理目的地址不是本路由器而需要转发的报文,它的实现好坏直接影响着路由器的整体性能.**控制路径:**处理目的地址是本路由器的高层协议报文,特别是各种路由协议报文.虽然控制路径不是路由器的关键路径,但是它负责完成路由信息的交互,从而保证了数据路径上的报文沿着最优的路径转发.**45IP多播（1）特点**多播使用组地址、永久组地址、动态的组成员、使用硬件进行多播**（2）两种协议a网际组管理协议IGMP**:管理本地；阶段一当某个主机加入新的多播组时,该主机应向多播组的多播地址发送IGMP报文,声明自己要成为该组的成员;本地的多播路由器收到IGMP报文后,将组成员关系转发给因特网上的其他多播路由器阶段二本地多播路由器要周期性地探询本地局域网上的主机，以便知道这些主机是否还继续是组的成员.只要对某个组有一个主机响应，那么多播路由器就认为这个组是活跃的.但一个组在经过几次的探询后仍然没有一个主机响应，则不再将该组的成员关系转发给其多播路由器.b多播路由选择协议：动态性DVMRP、CBT 、PIM-SM 、 PIM-DM **4.5转发多播数据报使用的方法(1)洪泛与剪除:反向路径广播RPB**路由器收到多播数据报时,先检查是否从源点经最短路径传送来的.若是,就向所有其他方向转发刚才收到的多播数据报（但进入的方向除外),,否则就丢弃而不转发.如果存在相同最短路径,选择这几条最短路径中的相邻路由器的IP地址最小**(2)隧道技术(3)基于核心的发现技术:**对每一个多播组 G 指定一个核心路由器,给出它的 IP 单播地址.**4.6多协议标记交换MPLS**(1)特点支持面向连接的服务质量;支持流量工程,平衡网络负载;有效地支持虚拟专用网 VPN**(2)基本工作原理**:IP分组的转发在传统的IP网络中,分组每到达一个路由器后,都必须提取出其目的地址,按目的地址查找路由表,并按照“最长前缀匹配”的原则找到下一跳的IP 地址.当网络很大时，查找含有大量项目的路由表要花费很多的时间.在出现突发性的通信量时,往往还会使缓存溢出，这就会引起分组丢失,传输时延增大和服务质量下降。在 MPLS 域的入口处，对打上标记的 IP 数据报用硬件进行转发**（3）基本工作过程:**MPLS 域中的各 LSR 使用专门的标记分配协议LDP交换报文，并找出标记交换路径LSP。各LSR根据这些路径构造出分组转发表。分组进入到MPLS域时,MPLS 入口结点把分组打上标记，并按照转发表将分组转发给下一个LSR.给IP数据报打标记的过程叫作分类;一个标记仅仅在两个标记交换路由器LSR 之间才有意义.分组每经过一个 LSR，LSR 就要做两件事：一是转发，二是更换新的标记；当分组离开 MPLS 域时，MPLS 出口结点把分组的标记去除。再以后就按照一般分组的转发方法进行转发**(4)转发等价类FEC**就是路由器按照同样方式对待的分组的集合.FEC 和标记是一一对应的关系;用于负载平衡**(5)封装技术:**在把IP数据报封装成以太网帧之前,先要插入一个MPLS首部

4.5**路由算法分类:**非自适应算法,静态路由算法.自适应算法,动态路由算法**.最优化原则:** 路由算法的目的是找出并使用汇集树.**汇集树:**从所有的源结点到一个给定的目的结点的最优路由的集合形成了一个以目的结点为根的树,称为汇集树;**静态路由算法:**Dijkstra算法;洪泛算法;选择性洪泛算法(将进来的每个包仅发送到与正确方向接近的线**);**基于流量的路由算法(既考虑拓扑结构,又兼顾网络负荷;前提:每对结点间平均数据流是相对稳定和可预测的;根据网络带宽和平均流量,可得出平均包延迟,因此路由选择问题归结为找产生网络最小延迟的路由选择算法.提前离线计算**.); 动态路由算法:**距离向量路由算法**(**算法的缺陷：对好消息反应迅速，对坏消息反应迟钝**);**水平分裂算法(工作过程与距离向量算法相同,区别在于到X的距离不向真正通向X的邻居结点报告,使得坏消息传播的也快);链路状态路由算法(主要问题:选择路由时,没有考虑线路带宽;路由收敛速度慢);**链路状态算法（LS）和距离向量算法（DV）的比较:**路由信息的复杂性(LS向全网发送;DV仅与邻居路由交换信息.);收敛速度(LS使用最短路径优先算法，算法复杂度为O(n\*\*2);n个结点（不包括源结点），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;DV可能有路由循环**;**计数无穷大问题;收敛时间变化.);健壮性(LS节点可以公布不正确的链接成本;每一个节点计算只需一个表.DV节点可以公布不正确的路径开销;通过其他节点获得节点表;通过网络传播错误);**分层路由(**分而治之的思想:根据需要,将路由器分成区域、聚类、区和组…可以减少路由表项.); **拥塞控制算法:拥塞(**网络上有太多的包时,性能会下降,这种情况称为拥塞.**)拥塞产生的原因:**多个输入对应一个输出;慢速处理器;低带宽线路.**拥塞控制与流量控制的差别:**拥塞控制:需要确保通信子网能够承载用户提交的通信量,是一个全局性问题,涉及主机、路由器等很多因素;流量控制:与点到点的通信量有,主要解决快速发送方与慢速接收方的问题,是局部问题,一般都是基于反馈进行控制的.**拥塞控制方法分为两类:**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). **衡量网络是否拥塞的参数**:缺乏缓冲区造成的丢包率;平均队列长度;超时重传的包的数目;平均包延迟;包延迟变化.**反馈方法**:向负载发生源发送一个告警包;包结构中保留一个位或域用来表示发生拥塞,一旦发生拥塞,路由器将所有的输出包置位,向邻居告警;主机或路由器主动地、周期性地发送探报,查询是否发生拥塞. **拥塞控制算法:开环控制**:基本思想(造成拥塞的主要原因是网络流量通常是突发性的;强迫包以一种可预测的速率发送;在ATM网中广泛使用.)**漏桶算法**(将用户发出的不平滑的数据包流转变成网络中平滑的数据包流；可用于固定包长的协议,如ATM;也可用于可变包长的协议,如IP,使用字节计数;无论负载突发性如何,漏桶算法强迫输出按平均速率进行,不灵活).令牌桶算法(漏桶算法不够灵活,因此加入令牌机制;基本思想：漏桶存放令牌,每ΔT秒产生一个令牌,令牌累积到超过漏桶上界时就不再增加.包传输之前必须获得一个令牌,传输之后删除该令牌);**漏桶算法与令牌桶算法的区别**:流量整形策略不同:漏桶算法不允许空闲主机积累发送权,以便以后发送大的突发数据;令牌桶算法允许,最大为桶的大小.漏桶中存放的是数据包,桶满了丢弃数据包;令牌桶中存放的是令牌,桶满了丢弃令牌,不丢弃数据包.**流说明:**一个数据流的发送方、接收方和通信子网三方认可的、描述发送数据流的模式和希望得到的服务质量的数据结构,称为流说明. **虚电路子网中的拥塞控制**:许可控制(基本思想:一旦发生拥塞,在问题解决之前,不允许建立新的虚电路);另一种方法是发生拥塞后可以建立新的虚电路,但要绕开发生拥塞的地区;资源预留(建立虚电路时，主机与子网达成协议,子网根据协议在虚电路上为此连接预留资源).**抑制包**:路由器监控输出线路及其它资源的利用情况,超过某个阈值,则此资源进入警戒状态;每个新包到来,检查它的输出线路是否处于警戒状态;若是,则向源主机发送抑制包,包中指出发生拥塞的目的地址.同时将原包打上标记(为了以后不再产生抑制包),正常转发;源主机收到抑制包后,按一定比例减少发向特定目的地的流量,并在固定时间间隔内忽略指示同一目的地的抑制包.然后开始监听,若此线路仍然拥塞,则主机在固定时间内减轻负载、忽略抑制包;若在监听周期内没有收到抑制包,则增加负载;通常采用的流量增减策略是:减少时,按一定比例减少,保证快速解除拥塞;增加时,以常量增加,防止很快导致拥塞.**加权公平队列**:公平队列算法(路由器的每个输出线路有多个队列;路由器循环扫描各个队列,发送队头的包;所有主机具有相同优先级;一些ATM交换机、路由器使用这种算法;一种改进:对于变长包,由逐包轮讯改为逐字节轮讯);加权公平队列算法(给不同主机以不同的优先级;优先级高的主机在一个轮讯周期内获得更多的时间片).**逐跳抑制包**:抑制包对它经过的每个路由器都起作用;能够迅速缓解发生拥塞处的拥塞;上游路由器要求有更多的缓冲区;**负载丢弃:**上述算法都不能消除拥塞时,路由器只得将包丢弃;针对不同服务,可采取不同丢弃策略**(**文件传输,优先丢弃新包,wine策略;多媒体服务,优先丢弃旧包,milk策略). **网络互连设备**:中继器;网桥;多协议路由器;传输网关;应用网关.**级联虚电路**:建立连接(当目的主机不在子网内时,则在子网内找一个离目的网络最近的路由器,与之建立一条虚电路;该路由器与外部网关建立虚电路;该网关与下一个子网中的一个路由器建立虚电路;重复上述操作,直到到达目的主机.);传输数据(相同连接的包沿同一虚电路按序号传输;网关根据需要转换包格式和虚电路号.);拆除连接.**无连接网络互连**:每个包单独路由,提高网络利用率,但不能保证包按顺序到达;根据需要,连接不同子网的多协议路由器做协议转换,包括包格式转换和地址转换等.**隧道技术**;**互联网路由:**两级路由算法**:**内部网关协议IGP(RIP,OSPF)外部网关协议EGP(BGP);自治系统AS.**分段**;**标记段**:树型标记法:偏移量法(定义一个基本段长度，使得基本段能够通过所有网络).

**5.传输层（1）传输控制协议TCP：**面向连接的、可靠的、端到端的、基于字节流的传输协议；TCP不支持多播（multicast）和广播；TCP连接是基于字节流的，而非消息流，消息的边界在端到端的传输中不能得到保留；**TCP拥塞控制两种情况a快网络小缓存接收者:**处理措施--在连接建立时声明最大可接受段长度；利用可变滑动窗口协议防止出现拥塞**b慢网络大缓存接收者--**处理措施:发送方维护两个窗口：可变发送窗口和拥塞窗口，按两个窗口的最小值发送；拥塞窗口依照慢启动算法和拥塞避免算法变化。**导致网络拥塞:**网络能力和接收能力**（2）用户数据协议UDP：**无连接的端到端传输协议;无连接建立，没有拥塞控制;**特点:**RFC768,没有装饰,最基本的互联网传输协议,最大可能交付,UCP段可能丢失

**6.QoS服务控制技术(1)**具备服务质量保证和服务质量控制两个方面的能力**(2)关键技术包括**：质量保证--采用适度轻载、区分服务(DiffServ)和流量工程(TE)相结合实现;质量控制、QoS管理、QoS服务标识和防盗。**(3)会话发起协议SIP--**以因特网为基础，把IP电话视为因特网上的新应用a**两种构件**是用户代理包括用户代理客户(呼叫)用户代理服务器(被呼叫)和网络服务器--代理服务器和重定向服务器

**7.SDN-将数据与控制相分离.(1)特点：架构角度：**控制平面与数据平面分离,逻辑集中管理**业务角度：**通过控制器管理，使低层网络被抽象出来网络资源被抽象成服务，实现了应用程序与网络设备的操作系统进行解耦和;应用看到的是网络服务**运营角度：**网络可以通过编程的方式来访问,从而实现应用程序对网络的直接影响,一些新型的接口,可以实现传统网络管理不能做到的网络优化。**特点1：**控制-转发分离:传统网络设备的CP与DP 不分离；设备之间通过控制协议交互转发信息；SDN 的思路是将网络设备的控制平面集中上收到Controller;网络设备上只保留转发平面（转发表项）；通过Controller实现网络统一部署和网络自动化**特点2**网络的抽象:通过Controller实现了对基础网络设施的抽象；应用程序看到的是Controller提供的网络服务。**特点3：**可编程接口（核心思想）传统的网元都具备管理接口，可以通过网关协议（SNMP、NETCONF）或CLI实现简单的编程；SDN可编程接口不是传统的网络管理，而是一种在应用与网元之间双向的、紧密联系的通信通道，可以实现传统网络不具备的网络快速优化能力

(2)主要好处是可编程带来的网络自动化**（3）Openflow模型：安全信道：**Controller通过安全信道向OpenFlow Switch下发命令和接收信息;**组表 Group Table：**用一个Group使OpenFlow可以支持额外的转发行为（如select）**流表 Flow Table：**OpenFlow交换机的基本表项**(4)架构:数据平面、控制平面和应用平面.**数据平面与控制平面之间利用 SDN 控制数据平面接口(control-data-plane interface,简称 CDPI)进行通信,CDPI 具有统一的通信标准,目前主要采用 OpenFlow 协议.控制平面与应用平面之间由 SDN 北向接口(northbound interface,简称 NBI)负责通信,NBI 允许用户按实际需求定制开发.

**8.可信网络**(1)含义:应当对其网络和用户的行为及其结果是可预期与可管理的，能够做到行为状态可监测、行为结果可评估、异常行为可管理.从用户的角度，需要保障服务的安全性和可生存性；从设计的角度，需要提供网络的可管理性(2) 研究的内容:网络信息传输的可信;服务提供者的可信;终端用户的可信.网络行为的信任评估包括身份信任和行为信任，而行为信任是建立内容信任的基础之上，内容信任内涵着服务能力、信任推荐、防护能力、行为记录等等。

**9.普适服务(1)概念:**普适服务和计算是新出现的计算范例，其基础架构和服务可以在任何时间、任何地点、通过任何格式无缝接入或获取(普适服务是一个新生的、快速发展的研究领域，致力于简化用户与海量的电子服务和技术之间的交互)(2)特征:普适性、移动性、个人化、自适应性、主动性、透明性、质量保证、安全性、多样性、易用性

**10普适计算（不可见的工具）（1）要求：**普适性、透明性、动态性、自适应性、永恒性、永恒性**（2）特点:**实现了物理世界与信息空间的融合**(3)范围a交互技术:**物理空间和信息空间之间无需人的干预交互(即其中任一个空间状态的改变可以引起另一个空间的状态的相应改变;语气识别(在语音识别上扩展)肢体语言识别(如手势、面部表情等)地理位置识别等)b**上下文感知**:能够感知在当前的情景中与交互的任务有关的上下文，并据此做出决策和自动地提供相应的服务c自适应技术:软件自适应、硬件自适应(可重构技术)、服务自适应；服务自适应和上下文感知计算类似区别在于前者主要是从服务的手段和质量来解决用户需求和可用资源矛盾的问题c软件系统:集中在中间件和系统软件

**11A、云计算与网格计算:**技术本质上来说“云”计算与网格并没有根本上的区别基于互联网实现分布式计算资源的整合，以服务的形式输出给需要的人，按需提供服务的计算模式。 但是，网格要整合的是资源差异性比较大的节点（硬件、操作系统、应用资源都不同的计算机或平台），并且其分布式节点可以分布于全球各地（属于不同所有者），通过互联网连接成“一体”

**B普适计算与云计算：**概念不同：普适计算是学术概念云计算是商业概念；高度不同：普适计算是一种思想-融合；云计算是一种手段；研究的重心不同：普适计算强调终端与服务；云计算更关注集合与协同应该成为未来并存的计算模式

1. **IPV6**

**（1）IPv6的提出：**CIDR仅仅是一种临时补救措施，不能从根本上解决IP地址空间匮乏的问题；移动电话、家电上网等需要大量的IP地址；

IPv6与IPv4不兼容，但与其它Internet协议兼容，如TCP、UDP、OSPF、BGP、DNS等，但实际上还是需要开发另外一套协议栈。

**（2）IPv6的目标：**即使在不能有效分配地址空间的情况下，也能支持数十亿的主机；减少路由表的大小；简化协议，使得路由器能够更快的处理包；

提供比IPv4更好的安全性；更多的关注服务类型，特别是实时数据；支持Multicast；支持移动功能；协议具有很好的可扩展性；增强安全性；在一段时间内，允许IPv4与IPv6共存。

**（3）与IPv4相比，IPv6的主要变化：**地址变长，由32位变成128位；IP头简化，由13个域减少为7个域，提高路由器处理速度；由于IPv6包头定长，取消IHL域；Protocol域取消，用Next header域表示；取消与分段有关的域，IPv6采用不同的分段方法：所有主机和路由器必须支持576字节的包，当主机发送一个大包时，路由器不做分段，而是给主机发一个错误信息，由主机做分段；取消Checksum域。更好的支持选项功能；安全性提高；

更注重服务类型。

（4）IPv6 将首部长度变为固定的 40 字节，称为基本首部。把首部中不必要的功能取消了，使得 IPv6 首部的字段数减少到只有 8 个。通信量类(traffic class)—8 位。这是为了区分不同的 IPv6 数据报的类别或优先级。版本(version)—4 位。它指明了协议的版本,对IPv6 该字段总是6.流标号(flow label)—20 位。 “流”是互联网络上从特定源点到特定终点的一系列数据报， “流”所经过的路径上的路由器都保证指明的服务质量。所有属于同一个流的数据报都具有同样的流标号.有效载荷长度(payload length)—16 位。它指明 IPv6 数据报除基本首部以外的字节数（所有扩展首部都算在有效载荷之内），其最大值是 64 KB。下一个首部(next header)—8 位。它相当于 IPv4 的协议字段或可选字段。IPv6 把原来 IPv4 首部中选项的功能都放在扩展首部中，并将扩展首部留给路径两端的源站和目的站的主机来处理。数据报途中经过的路由器都不处理这些扩展首部（只有一个首部例外，即逐跳选项扩展首部）。

这样就大大提高了路由器的处理效率。六种扩展首部：逐跳选项、路由选择、分片、鉴别、封装安全有效载荷、目的站选项

1. I**Pv6 将实现 IPv6 的主机和路由器均称为结点**。一个结点就可能有多个与链路相连的接口。IPv6 地址是分配给结点上面的接口的。一个接口可以有多个单播地址。其中的任何一个地址都可以当作到达该结点的目的地址。即一个结点接口的单播地址可用来唯一地标志该结点。
2. **IPv6 地址分类**：**未指明地址**：这是 16 字节的全 0 地址，可缩写为两个冒号“::”.这个地址只能为还没有配置到一个标准的 IP 地址的主机当作源地址使用;这类地址仅此一个.**环回地址**:即 0:0:0:0:0:0:0:1（记为 ::1）。作用和IPv4的环回地址一样。这类地址也是仅此一个.**多播地址:**功能和 IPv4 的一样。这类地址占 IPv6 地址总数的 1/256。**本地链路单播地址** (Link-Local Unicast Address) 有些单位的网络使用 TCP/IP 协议，但并没有连接到互联网上。连接在这样的网络上的主机都可以使用这种本地地址进行通信，但不能和互联网上的其他主机通信。这类地址占 IPv6 地址总数的 1/1024。**全球单播地址:**IPv6 的这一类单播地址是使用得最多的一类。曾提出过多种方案来进一步划分这128位的单播地址。根据2006年发布的草案标准RFC 4291的建议,IPv6 单播地址的划分方法非常灵活。
3. 向 IPv6 过渡只能采用逐步演进的办法，同时，还必须使新安装的 IPv6 系统能够向后兼容：IPv6 系统必须能够接收和转发 IPv4 分组，并且能够为 IPv4 分组选择路由。两种向 IPv6 过渡的策略：**使用双协议栈--**是指在完全过渡到 IPv6 之前，使一部分主机（或路由器）装有两个协议栈，一个 IPv4 和一个 IPv6。双协议栈的主机（或路由器）记为 IPv6/IPv4，表明它同时具有两种 IP 地址：一个 IPv6 地址和一个 IPv4 地址。双协议栈主机在和 IPv6 主机通信时是采用 IPv6 地址，而和 IPv4 主机通信时就采用 IPv4 地址。根据 DNS 返回的地址类型可以确定使用 IPv4 地址还是 IPv6 地址**。使用隧道技术:在 IPv6 数据报要进入IPv4网络时，把 IPv6 数据报封装成为 IPv4 数据报，整个的 IPv6 数据报变成了 IPv4 数据报的数据部分。当 IPv4 数据报离开 IPv4 网络中的隧道时，再把数据部分（即原来的 IPv6 数据报）交给主机的 IPv6 协议栈**
4. **SDx:软件定义（Soft Defined）:**软件定义通过制定策略集管理、规模扩张获得更便宜、更有弹性的计费方式，可以最大限度利用资源获得扩展收益，通过最大化规模获得更高速。**优势：**软件比硬件容易开发，容易创新。硬件发展很快，性能越来越强大，为软件定义提供了很好的基础。管理异构的资源GPU，需要利用软件定义计算的方法。软件定义可以与开源软件结合，从而推动创新。软件定义网络（SDN）软件定义存储（SDS）软件定义数据中心（SDDC）软件定义基础设施（SDI）软件定义无线电 软件定义仪器 软件定义汽车（百度）
5. **NFV**，即网络功能虚拟化，Network Function Virtualization。通过使用x86等通用性硬件以及虚拟化技术，来承载很多功能的软件处理。从而降低网络昂贵的设备成本。可以通过软硬件解耦及功能抽象，使网络设备功能不再依赖于专用硬件，资源可以充分灵活共享，实现新业务的快速开发和部署，并基于实际业务需求进行自动部署、弹性伸缩、故障隔离和自愈等。**传统网络存在问题：**基于 IP 的核心体系架构难以修改，新的功能只能通过打补丁的方式在其他层面实施，这往往导致网络节点臃肿和可扩展性差；互联网正在渗透到更加广泛和深入的商业领域，需要更加可信的安全保证，而现有网络层中缺乏安全机制，互联网容易受到各种类型的攻击；应用模式从端到端模式转变为对海量内容的获取，传统 TCP/IP 端到端网络体系架构提出了挑战；互联网的“尽力而为”的思想，直接承载电信级业务仍存在部分技术问题；互联网的建设和运维规模逐年攀升，现有网络结构不具备虚拟化的特征，导致了大量的资源浪费。
6. **未来网络发展趋势分析:**应处理好革新式架构与演进式部署的关系;遵循简单开放的基本原则;应注重应用驱动的因素;应内嵌安全性等需求;具有天然服务分发能力;考虑引入利益相关者之间的博弈关系;考虑建设大规模网络创新实验平台