**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。**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 。**协议：**为进行网络中的数据交换而建立的规则、标准或约定。由以下三个要素组成：（1）语法：即数据与控制信息的结构或格式。（2）语义：即需要发出何种控制信息，完成何种动作以及做出何种响应。（3）同步：即事件实现顺序的详细说明。协议是控制两个对等实体进行通信的规则的集合。在协议的控制下，两个对等实体间的通信使得本层能够向上一层提供服务，而要实现本层协议，还需要使用下面一层提供服务。**协议和服务的概念的区分：**1、协议的实现保证了能够向上一层提供服务。本层的服务用户只能看见服务而无法看见下面的协议。下面的协议对上面的服务用户是透明的。2、协议是“水平的”，即协议是控制两个对等实体进行通信的规则。但服务是“垂直的”，即服务是由下层通过层间接口向上层提供的。上层使用所提供的服务必须与下层交换一些命令，这些命令在OSI中称为服务原语。**通信交换方式：**电路交换、报文交换、分组交换、混合交换。电路交换是直接利用可切换的物理通信线路进行信息交换；报文交换是信息以报文为单位进行存储转发；分组交换是信息以分组为单位进行存储转发，源结点把报文分为分组，在中间结点存储转发，目的结点把分组合成报文，分组交换包含虚电路和数据报，虚电路是由分组交换通信所提供的面向连接的通信服务。在两个节点或应用进程之间建立起一个逻辑上的连接或虚电路后，就可以在两个节点之间依次发送每一个分组，接收端收到分组的顺序必然与发送端的发送顺序一致，因此接收端无须负责在接收分组后重新进行排序，报文交换是每个分组均带有全称网络地址（源、目的），可走不相同的路径。**物理层：**是[计算机网络](https://baike.baidu.com/item/%E8%AE%A1%E7%AE%97%E6%9C%BA%E7%BD%91%E7%BB%9C)[OSI模型](https://baike.baidu.com/item/OSI%E6%A8%A1%E5%9E%8B)中最低的一层。物理层规定:为传输数据所需要的物理链路创建、维持、拆除，而提供具有机械的，电子的，功能的和规范的特性。**数据链路层：**数据链路层是[OSI参考模型](https://baike.baidu.com/item/OSI%E5%8F%82%E8%80%83%E6%A8%A1%E5%9E%8B)中的第二层，介乎于[物理层](https://baike.baidu.com/item/%E7%89%A9%E7%90%86%E5%B1%82/4329158)和[网络层](https://baike.baidu.com/item/%E7%BD%91%E7%BB%9C%E5%B1%82/4329439)之间。[数据链路](https://baike.baidu.com/item/%E6%95%B0%E6%8D%AE%E9%93%BE%E8%B7%AF)层在[物理层](https://baike.baidu.com/item/%E7%89%A9%E7%90%86%E5%B1%82/4329158)提供的服务的基础上向[网络层](https://baike.baidu.com/item/%E7%BD%91%E7%BB%9C%E5%B1%82/4329439)提供服务，其最基本的服务是将源自网络层来的数据可靠地传输到相邻节点的目标机网络层。**网络层：**网络层为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，网络层是处理端到端传输的，它提供面向连接的服务和无连接的服务。**传输层：**该层协议为网络端点主机上的进程之间提供了可靠、有效的报文传送服务。其功能紧密地依赖于网络层的虚拟电路或数据报服务。传输层定义了主机应用程序之间端到端的连通性。传输层也称为[运输层](https://baike.baidu.com/item/%E8%BF%90%E8%BE%93%E5%B1%82)，传输层只存在于端开放系统中，是介于低3层[通信子网](https://baike.baidu.com/item/%E9%80%9A%E4%BF%A1%E5%AD%90%E7%BD%91" \t "_blank)系统和高3层之间的一层，但是很重要的一层，因为它是源端到[目的](https://baike.baidu.com/item/%E7%9B%AE%E7%9A%84" \t "_blank)端对数据传送进行控制从低到高的最后一层。**会话层：**会话层是建立在传输层之上，利用传输层提供的服务，使应用建立和维持会话，并能使会话获得同步。会话层使用校验点可使通信会话在通信失效时从校验点继续恢复通信。这种能力对于传送大的文件极为重要。**表示层：**表示层向上对应用层服务，向下接受来自会话层的服务。表示层为在应用过程之间传送的信息提供表示方法的服务，它只关心信息发出的语法和语义。**应用层：**应用层是七层OSI模型的第七层。应用层直接和[应用程序接口](https://baike.baidu.com/item/%E5%BA%94%E7%94%A8%E7%A8%8B%E5%BA%8F%E6%8E%A5%E5%8F%A3" \t "_blank)并提供常见的[网络应用服务](https://baike.baidu.com/item/%E7%BD%91%E7%BB%9C%E5%BA%94%E7%94%A8%E6%9C%8D%E5%8A%A1)。应用层也向[表示层](https://baike.baidu.com/item/%E8%A1%A8%E7%A4%BA%E5%B1%82)发出请求。**介质访问控制子层（MAC）：**它定义了数据帧怎样在介质上进行传输。在共享同一个带宽的链路中，对连接介质的访问是“先来先服务”的。物理寻址在此处被定义，逻辑拓扑（信号通过物理拓扑的路径）也在此处被定义。线路控制、出错通知（不纠正）、帧的传递顺序和可选择的流量控制也在这一子层实现。**多路复用技术：**频分复用（FDM）、时分复用（TDM）、波分复用（WDM）、码分多路复用（CDMA）。**ALOHA协议：**分为纯ALOHA协议、时隙ALOHA协议。纯ALOHA协议：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; 时隙ALOHA协议：把频道在时间上分段，每个传输点只能在一个分段的开始处进行传送。用户每次必须等到下一个时间片才能开始发送数据，每次传送的数据必须少于或者等于一个频道的一个时间分段。**载波监听多路访问协议（CSMA）：**是一种[允许](https://baike.baidu.com/item/%E5%85%81%E8%AE%B8/3896772)多个设备在同一信道发送信号的[协议](https://baike.baidu.com/item/%E5%8D%8F%E8%AE%AE/670528)，其中的设备监听其它设备是否忙碌，只有在线路空闲时才发送。分为：1-坚持型CSMA、非坚持型CSMA、p-坚持型CSMA。**CSMA/CD：**载波监听多路访问/冲突检测，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，可以提高信道利用率。**CSMA/CA：**载波监听多路访问/冲突避免，是一种数据传输是避免各站点之间数据传输冲突的算法，其特点是发送包的同时不能检测到信道上有无冲突，只能尽量“避免”。用于无线局域网。 当[主机](https://baike.baidu.com/item/%E4%B8%BB%E6%9C%BA/455151" \t "_blank)需要发送一个数据帧时，首先检测信道，在持续检测到信道空闲达一个时间间隔之后，主机发送数据帧。接收主机正确接收到该数据帧，等待一个时间间隔后马上发出对该数据帧的确认。若源站在规定时间内没有收到确认帧，就必须重传此帧，直到收到确认为止，或者经过若干次重传失败后放弃发送。**无冲突协议：**基本位图协议，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，发送延迟大，重负载下，信道效率高。**有限竞争协议：**竞争方法和无冲突方法相结合，竞争方法例如CSMA，无冲突方法例如基本位图协议。**无线局域网特点：**基于蜂窝的通信；每个蜂窝内只有一个信道；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。**无线局域网与有线局域网的区别：**无线局域网具有隐藏站点问题，即由于站点距离竞争者太远，从而不能发现潜在介质竞争者的问题称为隐藏点问题。暴露站点问题，即由于非竞争者距离发送站点太近，从而导致介质非竞争者不能发生数据的问题称为暴露站点问题。**IEEE802协议：**802.1基本介绍和原语定义；802.2逻辑链路控制子层；802.3采用CSMA/CD技术的局域网；802.4采用令牌总线技术的局域网；802.5采用令牌环技术的局域网。**逻辑链路控制子层（LLC）**：逻辑链路控制子层LLC是LAN中位于MAC之上一个子层，它屏蔽了各种MAC的差别向其上层提供统一的数据链路服务。主要功能是处理两个站点之间帧的交换，实现端到端的无差错的帧传输和应答功能以及[流量控制](https://www.baidu.com/s?wd=%E6%B5%81%E9%87%8F%E6%8E%A7%E5%88%B6&tn=SE_PcZhidaonwhc_ngpagmjz&rsv_dl=gh_pc_zhidao" \t "_blank)功能。由于LAN的介质共享特点，因而也可以实现广播式通信。LLC提供无确认无连接服务和面向连接的服务。无确认无连接服务提供无需建立数据链路连接而网络层实体能交换链路服务数据单元的手段。数据传送方式可以是点到点、点到多点式，也可以是广播式。这是一种数据报服务。面向连接的服务，在这种服务下必须先建立链路连接，才能进行帧的传送。它提供了建立、维持、复位和终止数据链路层连接的手段。还提供了数据链路层的定序、流控和错误恢复，这是一种虚电路服务。**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。**交换机：**工作在数据链路层，主要功能包括物理编址、错误校验、帧序列以及数据流控制。**静态路由算法：**静态路由[算法](https://baike.baidu.com/item/%E7%AE%97%E6%B3%95)很难算得上是算法，只不过是开始路由前由[网管](https://baike.baidu.com/item/%E7%BD%91%E7%AE%A1)建立的表映射。这些映射自身并不改变，除非[网管](https://baike.baidu.com/item/%E7%BD%91%E7%AE%A1)去改动。使用[静态路由](https://baike.baidu.com/item/%E9%9D%99%E6%80%81%E8%B7%AF%E7%94%B1)的[算法](https://baike.baidu.com/item/%E7%AE%97%E6%B3%95)较容易设计，在[网络通信](https://baike.baidu.com/item/%E7%BD%91%E7%BB%9C%E9%80%9A%E4%BF%A1)可预测及简单的[网络](https://baike.baidu.com/item/%E7%BD%91%E7%BB%9C)中工作得很好。由于[静态路由](https://baike.baidu.com/item/%E9%9D%99%E6%80%81%E8%B7%AF%E7%94%B1)[系统](https://baike.baidu.com/item/%E7%B3%BB%E7%BB%9F)不能对网络改变做出反映，通常被认为不适用于的大型、易变的网络。例如：最短路径路由算法、Dijkstra算法、洪泛算法、基于流量的路由算法。

**动态路由算法：**通过分析收到的路由更新[信息](https://baike.baidu.com/item/%E4%BF%A1%E6%81%AF)来适应[网络](https://baike.baidu.com/item/%E7%BD%91%E7%BB%9C)环境的改变。如果[信息](https://baike.baidu.com/item/%E4%BF%A1%E6%81%AF)表示网络发生了变化，路由软件就重新计算路由并发出新的路由更新信息。这些信息渗入[网络](https://baike.baidu.com/item/%E7%BD%91%E7%BB%9C)，促使[路由器](https://baike.baidu.com/item/%E8%B7%AF%E7%94%B1%E5%99%A8)重新计算并对[路由表](https://baike.baidu.com/item/%E8%B7%AF%E7%94%B1%E8%A1%A8)做相应的改变。[动态路由算法](https://baike.baidu.com/item/%E5%8A%A8%E6%80%81%E8%B7%AF%E7%94%B1%E7%AE%97%E6%B3%95)可以在适当的地方以[静态路由](https://baike.baidu.com/item/%E9%9D%99%E6%80%81%E8%B7%AF%E7%94%B1)作为补充。例如：距离向量路由算法、链路状态算法。**路由算法应有的特性：**正确性、简单性、健壮性、稳定性、公平性、最优性。**分层路由：**IS-IS区域提供了一种在IS-IS域中伸缩路由的方法。正常的IS-IS区域和连接它们的骨干区域形成两级的路由层次。区域内的路由称作一级路由。域内独立的区域之间的路由称作[二级路由](https://baike.baidu.com/item/%E4%BA%8C%E7%BA%A7%E8%B7%AF%E7%94%B1/10985106" \t "_blank)。**拥塞控制：**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。其中，拥塞控制分为两类：开环控制和闭环控制。开环控制，通过好的设计来解决问题，以避免拥塞发生，拥塞控制时，不考虑网络当前状态；闭环控制，基于反馈机制，其工作流程是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。拥塞控制算法有漏桶算法、令牌桶算法、公平队列算法、加权公平队列算法。**流量控制：**流量控制与点对点的通信量有关，主要是解决快速发送方与慢速接收放的问题，是局部问题，一般都是基于反馈进行控制的。**控制报文协议（ICMP）：**主要用来报告出错和测试。**地址解析协议（ARP）：**解决网络层地址（ip地址）和数据链路层地址（mac地址）的映射问题。**反向地址解析协议（RARP）：**解决数据链路层地址（mac地址）和网络层地址（ip地址）的映射问题。**路由协议：**1、内部网关协议（IGP），自治系统内使用的路由算法，例如：RIP（路由信息协议是基于距离矢量算法的路由协议，利用跳数来作为计量标准。在带宽、配置和管理方面要求较低，主要适合于规模较小的网络中）、OSPF（[开放式最短路径优先](https://baike.baidu.com/item/%E5%BC%80%E6%94%BE%E5%BC%8F%E6%9C%80%E7%9F%AD%E8%B7%AF%E5%BE%84%E4%BC%98%E5%85%88/8966505)的简单说就是两个相邻的[路由器](https://baike.baidu.com/item/%E8%B7%AF%E7%94%B1%E5%99%A8/108294)通过发报文的形式成为邻居关系，邻居再相互发送链路状态信息形成邻接关系，之后各自根据最短路径算法算出路由，放在OSPF路由表，OSPF路由与其他路由比较后优的加入全局路由表）。2、外部网关协议（EGP）：自治系统之间使用的路由算法，例如BGP（边界网关协议系统的主要功能是和其他的边界网关协议系统交换网络可达信息。网络可达信息包括列出的[自治系统](https://baike.baidu.com/item/%E8%87%AA%E6%B2%BB%E7%B3%BB%E7%BB%9F/129715" \t "_blank)（AS）的信息）。**解决IPv4地址枯竭的方法：**1、子网划分，可以把基于类的[IP网络](https://www.baidu.com/s?wd=IP%E7%BD%91%E7%BB%9C&tn=SE_PcZhidaonwhc_ngpagmjz&rsv_dl=gh_pc_zhidao" \t "_blank)进一步分成更小的网络，每个子网由路由器界定并分配一个新的子网网络地址,子网地址是借用基于类的网络地址的主机部分创建的；2、无类域间路由（CIDR），无类别域间路由是一个用于给用户分配IP地址以及在互联网上有效地路由IP数据包的对IP地址进行归类的方法；3、网络地址转换（NAT），是一种将私有(保留)地址转化为合法IP地址的转换技术,它被广泛应用于各种类型Internet接入方式和各种类型的网络中。NAT不仅完美地解决了lP地址不足的问题，而且还能够有效地避免来自网络外部的攻击，隐藏并保护网络内部的计算机；4、IPv6，IPv6的地址长度为128位，是IPv4地址长度的4倍，IPv6包括单播、多播、任播。**向IPv6过渡的方法：**1、双协议栈，双协议栈技术就是指在一台设备上同时启用IPv4协议栈和IPv6协议栈。这样的话，这台设备既能和IPv4网络通信，又能和IPv6网络通信。如果这台设备是一个路由器，那么这台路由器的不同接口上，分别配置了IPv4地址和IPv6地址，并很可能分别连接了IPv4网络和IPv6网络。如果这台设备是一个计算机，那么它将同时拥有IPv4地址和IPv6地址，并具备同时处理这两个协议地址的功能；2、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。**TCP协议：**传输控制协议是一种面向连接的、可靠的、基于字节流的传输层通信协议，由IETF的RFC 793 定义。TCP旨在适应支持多网络应用的分层协议层次结构。 连接到不同但互连的计算机通信网络的主计算机中的成对进程之间依靠TCP提供可靠的通信服务。TCP假设它可以从较低级别的协议获得简单的，可能不可靠的数据报服务。 原则上，TCP应该能够在从硬线连接到分组交换或电路交换网络的各种通信系统之上操作。**TCP的主要特点：**（1）基于流的方式；（2）面向连接；（3）可靠通信方式；（4）在网络状况不佳的时候尽量降低系统由于重传带来的带宽开销；（5）通信连接维护是面向通信的两个端点的，而不考虑中间网段和节点。**为了满足TCP这些特点，TCP做了如下的规定：**①数据分片，在发送端对用户数据进行分片，在接收端进行重组，由TCP确定分片的大小并控制分片和重组；②到达确认：接收端接收到分片数据时，根据分片数据序号向发送端发送一个确认；③超时重发：发送方在发送分片时启动超时定时器，如果在定时器超时之后没有收到相应的确认，重发分片；④滑动窗口：TCP连接每一方的接收缓冲空间大小都固定，接收端只允许另一端发送接收端缓冲区所能接纳的数据，TCP在滑动窗口的基础上提供流量控制，防止较快主机致使较慢主机的缓冲区溢出；⑤失序处理：作为IP数据报来传输的TCP分片到达时可能会失序，TCP将对收到的数据进行重新排序，将收到的数据以正确的顺序交给应用层；⑥重复处理：作为IP数据报来传输的TCP分片会发生重复，TCP的接收端必须丢弃重复的数据；⑦数据校验：TCP将保持它首部和数据的检验和，这是一个端到端的检验和，目的是检测数据在传输过程中的任何变化。如果收到分片的检验和有差错，TCP将丢弃这个分片，并不确认收到此报文段导致对端超时并重发。**TCP的连接建立采用三次握手，过程如下：**1、客户端发送SYN（SEQ=x）报文给服务器端，进入SYN\_SEND状态；2、服务器端收到SYN报文，回应一个SYN （SEQ=y）ACK（ACK=x+1）报文，进入[SYN\_RECV](https://baike.baidu.com/item/SYN_RECV" \t "_blank)状态；3、客户端收到服务器端的SYN报文，回应一个ACK（ACK=y+1）报文，进入Established状态。**TCP的连接终止采用四次分手，过程如下：**1、某个应用进程首先调用close，称该端执行“主动关闭”（active close）。该端的TCP于是发送一个FIN分节，表示数据发送完毕；2、接收到这个FIN的对端执行 “被动关闭”（passive close），这个FIN由TCP确认；3、一段时间后，接收到这个文件结束符的应用进程将调用close关闭它的套接字。这导致它的TCP也发送一个FIN；4、接收这个最终FIN的原发送端TCP（即执行主动关闭的那一端）确认这个FIN。**UDP协议：**用户数据报协议，属于传输层的协议，无连接，不保证传输的可靠性。对于来自应用层的数据包，直接加上UDP报头然后传送给IP。UDP头部中有一个校验和字段，可用于差错的检测，但是UDP是不提供差错纠正的。**UDP适用场合：**在选择UDP作为传输协议时必须要谨慎。在[网络](https://baike.baidu.com/item/%E7%BD%91%E7%BB%9C" \t "_blank)质量令人十分不满意的环境下，UDP协议数据包丢失会比较严重。但是由于UDP的特性：它不属于连接型协议，因而具有资源消耗小，处理速度快的优点，所以通常音频、视频和普通数据在传送时使用UDP较多，因为它们即使偶尔丢失一两个数据包，也不会对接收结果产生太大影响。**TCP和UDP之间的区别：**TCP 是面向连接的传输控制协议，而UDP 提供了无连接的数据报服务；TCP 具有高可靠性，确保传输数据的正确性，不出现丢失或乱序；UDP 在传输数据前不建立连接，不对数据报进行检查与修改，无须等待对方的应答，所以会出现分组丢失、重复、乱序，应用程序需要负责传输可靠性方面的所有工作；UDP 具有较好的实时性，工作效率较 TCP 协议高；UDP 段结构比 TCP 的段结构简单，因此网络开销也小。TCP 协议可以保证接收端毫无差错地接收到发送端发出的字节流，为应用程序提供可靠的通信服务。对可靠性要求高的通信系统往往使用 TCP 传输数据。

**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。**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。**普适计算：**普适计算，又称普存计算、普及计算、遍布式计算、泛在计算，是一个强调和环境融为一体的计算概念，而[计算机](https://baike.baidu.com/item/%E8%AE%A1%E7%AE%97%E6%9C%BA/140338)本身则从人们的视线里消失。在普适计算的模式下，人们能够在任何时间、任何地点、以任何方式进行信息的获取与处理。**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” 。**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。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。

**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。**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。

1. ***计算机网络技术的历史和新进展***。高速计算机信息网络是信息社会的神经和血管，体系结构是网络的骨架和神经，协议是网络的心脏和血液。Internet的发展速度是历史上发展最快的一种技术，Internet 正在以超过摩尔定理的速度发展。**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。***局域网与介质访问子层****。***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 。

**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）。信道分配方法：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)。

**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。

**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。

1. ***网络层协议与路由选择* 。（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。**

**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。

**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。

**路由器基本结构**:网络接口;转发引擎;内部交换;路由引擎;路由表.**路由器提供报文处理路径**:数据路径(处理目的地址不是本路由器而需要转发的报文)；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).**路由器必须完成两个基本功能**:路由查找;内部交换过程。

**网际组管理协议IGMP**(为了使路由器知道多播组成员的信息):IGMP使用IP数据报传递其报文(即IGMP报文加上IP首部构成IP数据报),但它也向IP提供服务.在主机和多播路由器之间的所有通信都是使用IP多播。**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。**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。***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**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。***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。**(2)主要好处是**可编程带来的网络自动化

***六、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。

**七、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。

**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。

**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” **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**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**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。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

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。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:.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.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。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**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 IPv6 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。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。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**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）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。**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**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). **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.(2)主要好处是可编程带来的网络自动化.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.普适服务: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.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).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;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.软件系统:集中在中间件和系统软件.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”.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;**局域网**：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 ）多路访问协议：控制多个用户共用一条信道的协议。（1）ALOHA（纯ALOHA、分槽ALOHA）；（2）载波监听多路访问协议CSMA若站点有数据发送,先监听信道;若站点发现信道空闲,a.坚持型CSMA: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; b.非坚持型CSMA:则发送;若信道忙,等待一随机时间,然后重新开始发送过程;c. p-坚持型CSMA(适用于分槽信道):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。d.CSMA/CD（边发送边监听）：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。（3）无冲突协议、有限竞争协议 占用信道的策略：竞争方法：如CSMA（轻负载下，发送延迟小；重负载下，信道效率低）；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）；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）（4）无线局域网协议：通信基于蜂窝;每个蜂窝内只有一个信道;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（特点）**LAN（局域网）参考模型：**（1）LLC（提供确认机制和流量控制）提供三种服务:不可靠的数据报服务,已确认的数据报服务,可靠的面向连接的服务；（2）MAC（媒体访问管理;数据封装）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。连接k个不同LAN的网桥具有k个MAC子层和k个物理层。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。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。多个网桥（并行网桥）可能产生回路（解决：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）10Base-T：表示在双绞线上传送的数据率为10[Mb/s](https://www.baidu.com/s?wd=Mb/s&tn=SE_PcZhidaonwhc_ngpagmjz&rsv_dl=gh_pc_zhidao)[基带信号](https://www.baidu.com/s?wd=%E5%9F%BA%E5%B8%A6%E4%BF%A1%E5%8F%B7&tn=SE_PcZhidaonwhc_ngpagmjz&rsv_dl=gh_pc_zhidao)的以太网。“T”代表双绞线.[100BASE-T](https://www.baidu.com/s?wd=100BASE-T&tn=SE_PcZhidaonwhc_ngpagmjz&rsv_dl=gh_pc_zhidao)是在双绞线上传送100[Mb/s](https://www.baidu.com/s?wd=Mb/s&tn=SE_PcZhidaonwhc_ngpagmjz&rsv_dl=gh_pc_zhidao)[基带信号](https://www.baidu.com/s?wd=%E5%9F%BA%E5%B8%A6%E4%BF%A1%E5%8F%B7&tn=SE_PcZhidaonwhc_ngpagmjz&rsv_dl=gh_pc_zhidao)的[星型拓扑](https://www.baidu.com/s?wd=%E6%98%9F%E5%9E%8B%E6%8B%93%E6%89%91&tn=SE_PcZhidaonwhc_ngpagmjz&rsv_dl=gh_pc_zhidao)以太网，仍使用[IEEE802.3](https://www.baidu.com/s?wd=IEEE802.3&tn=SE_PcZhidaonwhc_ngpagmjz&rsv_dl=gh_pc_zhidao)的CSDA/CD（载波监听多点接入/[冲突检测](https://www.baidu.com/s?wd=%E5%86%B2%E7%AA%81%E6%A3%80%E6%B5%8B&tn=SE_PcZhidaonwhc_ngpagmjz&rsv_dl=gh_pc_zhidao)）协议。网络层为传输层提供的服务:面向连接服务;无连接服务;通信子网提供的服务.**ISO 定义**：网络层（处理端到端传输的最低层）为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。**路由算法（RIP、OSPF、IS-IS协议）分类：**（1）非自适应算法，静态路由算法：①最短路径路由算法（构建子网的拓扑图，图中的每个结点代表一个路由器，每条弧代表一条通信线路。为了选择两个路由器间的路由，算法在图中找出最短路径，如Dijkstra算法）；②洪泛算法（把收到的每一个包，向除了该包到来的线路外的所有输出线路发送）③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（off-line）计算）（2）自适应算法，动态路由算法：①距离向量路由算法：将自己对全网拓扑结构的认识告诉给邻居（无限计算问题：对好消息反应迅速，对坏消息反应迟钝）②水平分裂算法（坏消息也传播的快）：③链路状态路由算法：将自己对邻居的认识洪泛给全网。**链路状态算法（LS）和距离向量算法（DV）的比较:**①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.);②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.);③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);**最优化原则：**如果路由器 J 在路由器 I 到 K 的最优路由上，那么从 J 到 K 的最优路由会落在同一路由上。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，即汇集树；路由算法的目的是找出并使用汇集树。**移动用户的路由转发过程：**当一个包发给移动用户时，首先被转发到用户的家乡局域网；该包到达用户的家乡局域网后，被家乡代理接收，家乡代理查询移动用户的新位置和与其对应的外部代理的地址；家乡代理采用隧道技术，将收到的包作为净荷封装到一个新包中，发给外部代理；家乡代理告诉发送方，发给移动用户的后续包作为净荷封装成包直接发给外部代理；外部代理收到包后，将净荷作为数据链路帧发给移动用户；**拥塞：**网络上有太多的包时，性能会下降，这种情况称为拥塞。（多输入对应一输出、慢速处理器、低带宽线路）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。**拥塞控制算法：**（1）开环控制：通过好的设计来解决问题，避免拥塞发生；①漏桶算法（可用于ATM、IP协议）：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；②令牌桶算法：漏桶存放令牌，每隔T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；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.（2）闭环控制：基于反馈（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）机制。抑制包；加权公平队列：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；负载丢弃：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**网络互联设备**：中继器、网桥、多协议路由器、传输网关、应用网关 1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）工作过程：主机1发送一个包，目的IP地址 = 主机2-IP，将包封装到局域网帧中，帧目的地址 = 路由器1-MAC；局域网传输；路由器1剥掉局域网帧头、帧尾，将得到的IP包封装到广域网网络层包中，包目的地址 = 路由器2地址；广域网传输；路由器2剥掉广域网包头，将得到的IP包封装到局域网帧中，包目的IP地址 = 主机2-IP，帧目的地址 = 主机2-MAC地址；局域网传输；主机2接收。**两级路由算法**：内部网关协议（RIP，OSPF）、外部网关协议（BGP）、自治系统AS（内部网关协议IGP、外部网关协议EGP） 防火墙（两个路由器 + 一个应用网关）：为防止网络中的信息泄露出去或不好的信息渗透进来，在网络边缘设置防火墙；TCP和UDP的区别：（1）TCP面向连接;UDP是无连接的（2）TCP提供可靠的服务。即通过TCP连接传送的数据，无差错，不丢失，不重复，且按序到达;UDP尽最大努力交付但不保证可靠交付（3）TCP面向字节流，;UDP是面向报文的（4）UDP没有拥塞控制，因而发送速率快（5）每一条TCP连接只能是点到点的;UDP支持一对一，一对多，多对一和多对多的交互通信（6）TCP首部开销20字节;UDP的首部只有8个字节（7）TCP的逻辑通信信道是全双工的可靠信道，UDP则是不可靠信道.TCP拥塞控制：（1）慢启动算法：连接建立时拥塞窗口初始值为该连接允许的最大段长，阈值为64K；发出一个最大段长的TCP段，若正确确认，拥塞窗口变为两个最大段长；发出（ 拥塞窗口/最大段长）个最大长度的TCP段，若都得到确认，则拥塞窗口加倍；重复上一步，直至发生丢包超时事件，或拥塞窗口大于阈值（2）拥塞避免算法:若拥塞窗口大于阈值,从此时开始,拥塞窗口线形增长,一个RTT周期增加一个最大段长,直至发生丢包超时事件;当超时事件发生后,阈值设置为当前拥塞窗口大小的一半,拥塞窗口重新设置为一个最大段长;执行慢启动算法.**尽最大努力交付：**(1)不保证源主机发送出来的IP数据报一定无差错地交付到目的主机(2)不保证源主机发送出来的IP数据报都在某一规定的时间内交付到目的主机(3)不保证源主机发送出来的IP数据报一定按发送时的顺序交付到目的主机(4)不保证源主机发送出来的IP数据报不会重复交付到目的主机(5)不故意丢弃IP数据报。**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;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。(2)主要好处是可编程带来的网络自动化。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”。 **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。**计算机网络技术的历史和新进展。**高速计算机信息网络是信息社会的神经和血管，体系结构是网络的骨架和神经，协议是网络的心脏和血液。Internet的发展速度是历史上发展最快的一种技术，Internet 正在以超过摩尔定理的速度发展。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。局域网与介质访问子层。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 。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）。信道分配方法：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)。**网络层协议与路由选择 。**（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；（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）。**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。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。路由器基本结构:网络接口;转发引擎;内部交换;路由引擎;路由表.路由器提供报文处理路径:数据路径(处理目的地址不是本路由器而需要转发的报文)；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).路由器必须完成两个基本功能:路由查找;内部交换过程。网际组管理协议IGMP(为了使路由器知道多播组成员的信息):IGMP使用IP数据报传递其报文(即IGMP报文加上IP首部构成IP数据报),但它也向IP提供服务.在主机和多播路由器之间的所有通信都是使用IP多播。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。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**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。五、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。(2)主要好处是可编程带来的网络自动化六、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。

七、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。

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。

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” 3**.以太网协议、基本内容**（数据单元的格式，首部的内容）以太网V2的MAC帧较为简单，有五个字段组成。前两个字段分别为6字节长的目的地址和源地址字段。第三个字段是2字节的类型字段，用来标志上一层使用的是什么协议，以便把收到的MAC帧的数据上交给上一层的这个协议（0800表示IP协议、0806表示ARP请求、0835表示ARP应答）。第四个字段是数据字段，其长度在46到1500字节之间（46字节是这样得出的：最小长度64字节减去18字节的首部和尾部就得出数据字段的最小长度）。最后一个字段是4字节的帧检验序列FCS（使用CRC检验）。（2）基本原理： 以太网采用带冲突检测的载波帧听多路访问（CSMA/CD）机制。以太网中节点都可以看到在网络中发送的所有信息，因此，我们说以太网是一种广播网络。以太网的工作过程如下：当以太网中的一台主机要传输数据时，它将按如下步骤进行：①监听信道上是否有信号在传输。如果有的话，表明信道处于忙状态，就继续监听，直到信道空闲为止。 ②若没有监听到任何信号，就传输数据。③传输的时候继续监听，如发现冲突则执行退避算法，随机等待一段时间后，重新执行步骤1（当冲突发生时，涉及冲突的计算机会发送会返回到监听信道状态。注意：每台计算机一次只允许发送一个包，一个拥塞序列，以警告所有的节点）。**"三网融合"有几个含义?**融合后的下一代互联网络将会发生哪些本质上的改变?两个：广义的上是指电信网、计算机网和[有线电视网](https://baike.baidu.com/item/%E6%9C%89%E7%BA%BF%E7%94%B5%E8%A7%86%E7%BD%91/3515951)三大网络的物理合一。指高层业务应用的融合，其表现为技术上趋向一致，网络层上可以实现互联互通，形成无缝覆盖，业务层上互相渗透和交叉，应用层上趋向使用统一的[IP协议](https://baike.baidu.com/item/IP%E5%8D%8F%E8%AE%AE/131947)，为提供多样化、多媒体化、个性化服务的同一目标逐渐交汇在一起，通过不同的安全协议，最终形成一套网络中兼容多种业务的运维模式。

改变：1.信息服务将由单一业务转向文字、话音、数据、图像、视频等多媒体综合业务。2.有利于极大地减少基础建设投入，并简化网络管理，降低维护成本。3.将使网络从各自独立的专业网络向综合性网络转变，网络性能得以提升，资源利用水平进一步提高。4.三网融合是业务的整合，它不仅继承了原有的话音、数据和视频业务，而且通过网络的整合，衍生出了更加丰富的增值业务类型，如图文电视、VOIP、[视频邮件](https://baike.baidu.com/item/%E8%A7%86%E9%A2%91%E9%82%AE%E4%BB%B6)和网络游戏等，极大地拓展了业务提供的范围。5.三网融合打破了电信运营商和广电运营商在视频传输领域长期的恶性竞争状态，各大运营商将在一口锅里抢饭吃，看电视、上网、打电话资费可能打包下调。

6.物联网是在互联网基础之上发展起来的，与互联网在基础设施上有一- 定程度的重合，但它不是互联网概念、技术和应用的简单扩展，那么物联网与互联网之间是怎样的关系?  
（一）物联网联系的主体是物，而互联网连接的主体是人。从涵盖范围上来讲，物联网覆盖的范围要比互联网大得多

（二）物联网并不是单一的对物进行连接，物联网是连接了人之后，才延继而申到对“物”的连接；而互联网是可以直接对“人”进行连接的。

（三）从涵盖范围上来讲，物联网覆盖的范围要比互联网大得多。

（四）物联网的诞生重要是为了帮助人类更好地管理“物”，对物体等进行实时监控管理；而互联网的主要目标服务对象是人，用于互相交换信息。

（五）与互联网相比，物联网的实现相对要困难了许多；因为互联网服务过程是人直接参与的时候占了大部分。

（六）人可以对互联网中出现的问题，及时发现与解决；但是物联网却脱离了人的直接参与，物体出现的问题，也全部交由人工智能进行分析管理，而人工智能远远达不到人的头脑那么灵活，所以一些特殊性问题就难以得到及时的发现和解决。

（七）物联网比互联网更加的复杂，在未来，物联网的应用可能会远远超过互联网，比互联网的作用更大，更强。人类可以很轻松地对物体进行控制与管理。

**论述P2P物联网的架构特点及其在实际应用中的优势和挑战**答案：一、P2P物联网的定义和架构特点**:**P2P物联网是指在物联网中采用点对点通信模式的网络架构。其主要特点包括：去中心化：P2P物联网不依赖中央服务器，设备之间可以直接通信，数据传输和处理分布在网络中的各个节点。对等通信：每个设备既是数据的提供者，也是数据的消费者，能够直接交换数据和资源。自组织网络：P2P网络能够自动发现和连接设备，形成自组织、自愈合的网络结构，适应动态变化的环境。二、P2P物联网的优势:高可靠性：由于没有单点故障，网络中一个节点的故障不会影响整体运行，适合关键应用。低延迟：设备间直接通信，减少数据传输延迟，提高响应速度。可扩展性：易于增加新设备，网络架构无需重大改动，支持大规模扩展。自治性：网络具备自组织和自愈合能力，适应复杂多变的环境。三、P2P物联网的挑战安全性：缺乏中央服务器，安全管理复杂，需确保数据机密性和完整性，防止恶意攻击。节点管理：设备既是客户端又是服务器，资源的共享和管理需合理机制。设备异构性：不同设备可能使用不同协议和接口，实现互联互通困难。移动性管理：设备经常移动，保持连接稳定性。能耗管理：电池供电设备需优化能耗，延长使用寿命。四、实际应用案例智能家居：设备通过P2P网络直接通信，实现快速响应和良好用户体验。传感器网络：提高数据采集效率和可靠性，适用于环境监测等领域。工业互联网：结合区块链技术，增强安全性和信任度，提高生产效率。五、总结P2P物联网在架构特点、优势和挑战方面具有独特性，其应用前景广阔。然而，仍需解决安全性、节点管理、设备异构性等挑战，以实现更广泛的应用。通过深入探讨这些方面，可以更好地理解P2P物联网的技术细节和实际应用。**云物联网的架构、优势与挑战**一、架构设备层：包含各种物联网设备，如传感器和智能设备，负责数据的收集和传输。连接层：负责设备与云平台之间的数据传输，可能使用多种通信协议。云平台层：提供数据存储、处理和分析服务，常见的有AWS、Azure等平台。应用层：为用户提供各种功能和服务，基于处理后的数据进行决策和操作。二、优势**:**可扩展性：云计算平台能够轻松扩展资源，以应对大量设备和数据。数据处理与分析：云平台具备强大的计算能力，支持实时数据分析，助力决策。成本效益：企业无需自建服务器，按需付费，降低运营成本。三、挑战安全与隐私：数据传输和存储的安全性至关重要，需防范黑客攻击和数据泄露。延迟：某些应用需要实时响应，云处理可能引入延迟，影响用户体验。互联网依赖：网络中断可能导致设备无法正常工作。数据管理：大规模数据的存储和检索需要高效策略。互操作性：不同厂商设备和协议的兼容性问题。四、实际应用智慧城市：通过 IoT 设备收集数据，优化交通、环境等城市运营。工业物联网：工厂设备连接云平台，实现预测性维护，提升生产效率。healthcare：远程监测患者健康数据，及时发现异常。五、未来趋势边缘计算与云 IoT 的结合，数据在设备端或边缘节点处理，减少延迟和带宽压力，可能是未来发展方向。结论**:**云 IoT 具有广阔的前景，但也面临技术和安全上的挑战。理解这些方面对于实际应用至关重要。