**第二章：局域网与介质访问子层 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. **信道分配方法**:静态分配(FDM、TDM、WDM);动态分配: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(确定何时发送)、载波监听和非载波监听(确定能否发送)). **(动态分配)多路访问协议:纯ALOHA协议**: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协议**: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%.**1-坚持型CSMA**: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.**非坚持型CSMA**: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 1-坚持CSMA大.**p-坚持型CSMA(**适用于分槽信道**)**: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. **带冲突检测的载波监听多路访问协议 CSMA/CD**: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. **无冲突协议:基本位图协议(**在实际发送信息前先广播发送请求的协议称为预留协议**)：**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). **有限竞争协议（**轻负载下使用竞争，重负载下使用无冲突方法**）**:**适应树搜索协议**: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. **无线局域网具有**: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.**无线局域网**:信号只能被发送站点周围一定范围内的站点接收,MAC子层协议需要尽量保证接收站点周围一定范围内只有一个发送站点.冲突被接收站点发现,某一时刻,信道上可以有多可有效数据帧.**MACA**: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. **802系列标准**:802.1 基本介绍和接口原语定义;802.2 逻辑链路控制（LLC）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.**引入LLC子层的原因**:MAC子层只提供尽力而为的数据报服务,不提供确认机制和流量控制(滑动窗口),有些情况下,这种服务足够,如支持IP协议;当需要确认和流控的时候,这种服务就不能满足,需要LLC.**LLC提供三种服务选项**:不可靠的数据报服务,可靠的面向连接的服务,已确认的数据报服务.LLC子层提供确认机制和流量控制.**MAC**:媒体访问管理;数据封装（发送和接收）.**分成两个子层的原因**:管理多点访问信道的逻辑不同于传统的数据链路控制;对于同一个LLC,可以提供多个MAC选择.**802.3的信号编码:**曼切斯特编码.**交换式802.3 LAN实现方法**:一个卡内是一个802.3LAN,构成自己的冲突域,卡间并行;使用端口缓存,无冲突发生.**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;轻负载时,延迟大. **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;

**第五章：网络层协议与路由选择 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.**网络层的地位**:位于数据链路层和传输层之间,使用数据链路层提供的服务,为传输层提供服务;通信子网的最高层;处理端到端传输的最低层.**网络层的两种实现方式----数据报和虚电路**:都属于分组交换,采用存储转发机制.数据报:每个分组被单独路由,分组带有全网唯一的地址.虚电路**:**先在源端和目的端之间建立一条虚电路,所有分组沿虚电路按次序存储转发,最后拆除虚电路.在虚电路中,每个分组无须进行路径选择. **路由算法应具有的特性:**正确性;简单性;健壮性;稳定性;公平性;最优性.**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). **网络层协议**: IP协议(格式、地址、子网划分);**控制协议:**因特网控制报文协议ICMP(主要用来报告出错和测试);地址解析协议ARP(解决IP地址与MAC地址的映射问题);反向地址解析协议RARP(解决MAC地址与IP地址的映射问题);**分层路由**:三种路由:区域内;区域间;自治系统间.**边界网关协议BGP**: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.**BGP息**:OPEN;UPDATA;KEEPALIVE;NOTIFICATION.**无类域间路由CIDR**:基本思想:将剩余的C类地址分成大小可变的地址空间.**最长匹配原则**:路由查找时,若多个路由表项匹配成功,选择掩码长(1比特数多)的路由表项.CIDR思想可用于所有IP地址,没有A、B、C类之分.**IPv6数据报由两大部分组成**:基本首部(固定的40字节:版本(4位)、通信量类(8位)、流标号(20位)、有效载荷长度(16位)、下一个首部(8位)、跳数限制(8位)、源地址(128位)、目的地址(128位));有效载荷(有效载荷也称为净负荷。有效载荷允许有零个或多个扩展首部,再后面是数据部分).**IPv6地址表示**:16字节地址表示成用冒号(:)隔开的8组,每组4个16进制位.打头的“0”可以省略,0123可以写成123;一组或多组16个“0”可以被一对冒号替代,但是一对冒号只能出现一次.**IPv6地址分类:**未指明地址(全0地址：：);环回地址(::1);多播地址;本地链路单播地址(占IPv6地址总数的1/1024.**两种向IPv6过渡的策略**:双协议栈;隧道技术(在IPv6数据报要进入IPv4网络时, IPv6数据报封装成为IPv4数据报,个的IPv6数据报变成了IPv4数据报的数据部分. IPv4数据报离开IPv4网络中的隧道时,把数据部分(原来的IPv6数据报)给主机的IPv6协议栈). **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**: 洪泛与剪除.路由器转发多播数据报使用洪泛的方法(这就是广播)为了避免兜圈子,采用了叫做**反向路径广播 RPB**策略.**RPB基本思想**: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.如果存在几条同样长度的最短路径),那么只能选择一条最短路径,选择的准则就是看这几条最短路径中的相邻路由器谁的IP地址最小.**隧道技术**:将多播数据包封装在单播IP数据报中.**多协议标记交换MPLS**: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.)**MPLS基本原理**:在 MPLS 域的入口处,给每一个IP数据报打上固定长度“标记”,然后对打上标记的IP数据报用硬件进行转发.采用硬件技术对打上标记的IP数据报进行转发就称为标记交换.“交换”也表示在转发时不再上升到第三层查找转发表,而是根据标记在第二层(链路层)用硬件进行转发.**标记交换路由器LSR** 同时具有标记交换和路由选择这两种功能,标记交换功能是为了快速转发.**“转发等价类”**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. **MPLS首部的格式:**标记值(20位)**;**实验(3位);栈S(1位);生存时间TTL(8位).

**第六章：传输层 传输层提供两种服务：**面向连接的传输服务:连接建立,数据传输,连接释放;无连接的传输服务.**传输服务**:传输服务原语.**传输协议**:寻址(方法:定义传输服务访问点TSAP(Transport Service Access Point),将应用进程与这些TSAP相连.在Internet中,TSAP为(IP address, local port).**Internet传输协议:**TCP协议(TCP协议需要解决的主要问题:滑动窗口;可变滑动窗口;慢启动). **TCP 协议**:按字节分配序号,每个字节有一个32位的序号;传输实体之间使用**段**(TPDU)交换数据;每个段包含一个20字节的头(选项部分另加)和0个或多个数据字节.段的大小必须首先满足65535字节的IP包数据净荷长度限制,还要满足底层网络传输介质的最大传输单元(MTU)的限制,比如以太网的MTU为1500字节;TCP实体使用滑动窗口协议,确认序号等于接收方希望接收的下一个序号.**TCP格式**:源端口和目的端口(各16位);序号和确认号(以字节为单位编号,各32位);TCP头的长度(4位,长度单位为32位字,包含可选项域);6位的保留域;6位的标识位:置1表示有效.**URG**:和紧急指针配合使用,发送紧急数据;**ACK**:确认号是否有效;**PSH**:指示发送方和接收方将数据不做缓存,立刻发送或接收;**RST**:由于不可恢复的错误重置连接;**SYN**:用于连接建立指示;**FIN**:用于连接释放指示.窗口大小(16位);校验和(16位);可选项域.**TCP连接管理**:**三次握手**:建立连接(服务器方执行LISTEN和ACCEPT原语,被动监听;客户方执行connect原语,产生一个SYN为1和ACK为0的TCP段,表示连接请求;服务器方的传输实体接收到这个TCP段后,首先检查是否有服务进程在所请求的端口上监听,若没有,回答RST置位的TCP段;若有服务进程在所请求的端口上监听,该服务进程可以决定是否接受该请求.在接受后,发出一个SYN置1和ACK置1的TCP段表示连接确认,并请求与对方的连接;发起方收到确认后,发出一个SYN置0和ACK置1的TCP段表示给对方的连接确认;);单向的连接释放(释放连接时,发出FIN位置1的TCP段并启动定时器,在收到确认后关闭连接.若无确认并且超时,也关闭连接.).**加权平均往返时间:新的 RTTS = (1 − α) × (旧的RTTS) + α × (新的RTT样本).**0 ≤ α < 1.。若 α 很接近于零,表示RTT值更新较慢.若选择α接近于1,则表示RTT值更新较快.α为0.125;**超时重传时间 RTO**: **RTO = RTTS + 4 × RTTD**;RTTD 是RTT的偏差的加权平均值;第一次的RTTD为RTT的一半,**新的RTTD = (1 − β) × (旧的RTTD) + β × ⏐RTTS − 新的 RTT 样本⏐**; β为0.25.**Karn算法:**在计算平均往返时间 RTT 时,只要报文段重传了,就不采用其往返时间样本.**改进**: **新的RTO = γ × (旧的RTO);** **γ**为2.**TCP传输策略**:窗口管理机制(窗口大小为0时,正常情况下,发送方不能再发TCP段,但有两个例外:紧急数据可以发送;为防止死锁,发送方可以发送1字节的TCP段,以便让接收方重新声明确认号和窗口大小).**如何改进传输层的性能**:1:发送方缓存应用程序的数据,等到形成一个比较大的段再发出;2:在没有可能进行”捎带”的情况下,接收方延迟发送确认段;3:使用Nagle算法(当应用程序每次向传输实体发出一个字节时,传输实体发出第一个字节并缓存所有其后的字节直至收到对第一个字节的确认;然后将已缓存的所有字节组段发出并对再收到的字节缓存,直至收到下一个确认);4:使用Clark算法解决**傻窗口症状(**当应用程序一次从传输层实体读出一个字节时,传输层实体会产生一个一字节的窗口更新段,使得发送方只能发送一个字节;)解决办法:限制收方只有在具备一半的空缓存或最大段长的空缓存时,才产生一个窗口更新段.**TCP拥塞控制**:两种情况(快网络小缓存接收者;慢网络大缓存接收者).**处理第一种拥塞的措施**: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.**第二种拥塞的措施**: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.**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.**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.

**第七讲** **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;