第一学时：计算机网络体系结构

【知识点】

（一） 计算机网络概述

计算机网络的概念、组成与功能：

计算机网络：就是利用通信设备和线路将地理位置不同的、功能独立的多个计算机系统互连起来，以功能完善的网络软件（即网络通信协议、信息交换方式、网络操作系统等）实现网络中资源共享和信息传递的系统。

计算机网络：资源子网＋通信子网

资源子网：主机 Host＋终端 Terminal

通信子网：通信链路组成

网络节点：分组交换设备 PSE、分组装 / 卸设备 PAD、集中器 C、网络控制中心 NCC、网间连接器 G。统称为接口住处处理机 IMP。

阐述协议的定义、协议三要素：

为进行计算机网络中的数据交换而建立的规则、标准或约定的集合。协议总是指某一层协议，准确地说，它是对同等实体之间的通信制定的有关通信规则约定的集合。网络协议的三个要素：

1)语义（Semantics)。涉及用于协调与差错处理的控制信息。

2)语法（Syntax)。涉及数据及控制信息的格式、编码及信号电平等。

3)定时（Timing)。涉及速度匹配和排序等。

计算机网络的分类：

1.按网络的分布范围分类:广域网 WAN、局域网 LAN、城域网 MAN

2.按网络的交换方式分类:电路交换、报文交换、分组交换

3.按网络的拓扑结构分类:星形、总线、环形、树形、网形

4.按网络的传输媒体分类:双绞线、同轴电缆、光纤、无线

5.按网络的信道分类:窄带、宽带

6.按网络的用途分类:教育、科研、商业、企业

计算机网络与互联网的发展历史，计算机网络的标准化工作及相关组织如 IETF，RFC 等。

网络发展三阶段：面向终端的网络；计算机－计算机网络；开放式标准化网络。

1.面向终端的计算机网络

以单个计算机为中心的远程联机系统，构成面向终端的计算机网络。用一台中央主机连接大量的地理上处于分散位置的终端。如 50 年代初美国的 SAGE 系统。

为减轻中心计算机的负载,在通信线路和计算机之间设置了一个前端处理机 FEP 或通信控制器 CCU 专门负责与终端之间的通信控制,使数据处理和通信控制分工。在终端机较集中的地区，采用了集中管理器(集中器或多路复用器)用低速线路把附近群集的终端连起来,通过 MODEM 及高速线路与远程中心计算机的前端机相连。这样的远程联机系统既提高了线路的利用率，又节约了远程线路的投资。

2.计算机－计算机网络

60 年代中期，出现了多台计算机互连的系统，开创了“计算机－计算机”通信时代，并存多处理中心，实现资源共享。美国的 ARPA 网，IBM 的 SNA 网，DEC 的 DNA 网都是成功的典例。这个时期的网络产品是相对独立的，未有统一标准。

3.开放式标准化网络

由于相对独立的网络产品难以实现互连，国际标准化组织 ISO(Internation Standards

Organization)于 1984 年颁布了一个称为“开放系统互连基本参考模型”的国际标准 ISO 7498，简称 OSI/RM。即著名的 OSI 七层模型。从此，网络产品有了统一标准，促进了企业的竞争，大大加速了计算机网络的发展。

（二） 计算机网络体系结构与参考模型

计算机网络分层结构：

所谓网络的体系结构(Architecture)就是计算机网络各层次及其协议的集合。层次结构一般以垂直分层模型来表示。

层次结构的要点：

1) 除了在物理媒体上进行的是实通信之外，其余各对等实体间进行的都是虚通信。

2)对等层的虚通信必须遵循该层的协议。

3)n 层的虚通信是通过 n/n-1 层间接口处 n-1 层提供的服务以及 n-1 层的通信（通常也是虚通信）来实现的。

层次结构划分的原则：

1)每层的功能应是明确的，并且是相互独立的。当某一层的具体实现方法更新时，只要保持上、下层的接口不变，便不会对邻居产生影响。

2)层间接口必须清晰，跨越接口的信息量应尽可能少。

3)层数应适中。若层数太少，则造成每一层的协议太复杂；若层数太多，则体系结构过于复杂，使描述和实现各层功能变得困难。

网络的体系结构的特点是：

1) 以功能作为划分层次的基础。

2)第 n 层的实体在实现自身定义的功能时，只能使用第 n-1 层提供的服务。

3)第 n 层在向第 n+1 层提供的服务时，此服务不仅包含第 n 层本身的功能，还包含由下层服务提供的功能。

4)仅在相邻层间有接口，且所提供服务的具体实现细节对上一层完全屏蔽。

ISO/OSI 参考模型

开放系统互连(Open System Interconnection)基本参考模型是由国际标准化组织(ISO)制定的标准化开放式计算机网络层次结构模型，又称 ISO's OSI 参考模型。“开放”这个词表示能使任何两个遵守参考模型和有关标准的系统进行互连。

OSI 包括了体系结构、服务定义和协议规范三级抽象。OSI 的体系结构定义了一个七层模型，用以进行进程间的通信，并作为一个框架来协调各层标准的制定；OSI 的服务定义描述了各层所提供的服务，以及层与层之间的抽象接口和交互用的服务原语；OSI 各层的协议规范，精确地定义了应当发送何种控制信息及何种过程来解释该控制信息。

需要强调的是，OSI 参考模型并非具体实现的描述，它只是一个为制定标准机而提供的概念性框架。在 OSI 中，只有各种协议是可以实现的，网络中的设备只有与 OSI 和有关协议相一致时才能互连。

TCP/IP 模型 ，重点是相关的术语（SDU、PDU、IDU 及 SAP），比较 TCP/IP 网络体系结构与 OSI/RM 的异同点，OSI/RM 的信息流动过程。

【教学重点和难点】ISO/OSI 参考模型和 TCP/IP 模型

【典型习题讲解】TCP/IP 模型

第二学时：物理层

【知识点】

（一） 通信基础

信道、信号、宽带、码元、波特、速率等基本概念：

1)数据传输速率--每秒传输二进制信息的位数，单位为位/秒，记作 bps 或 b/s。

计算公式：S=1/T*log2N(bps)

式中 T 为一个数字脉冲信号的宽度(全宽码)或重复周期(归零码)单位为秒；

N 为一个码元所取的离散值个数。通常 N=2K，K 为二进制信息的位数，K=log2N。

N=2 时，S=1/T，表示数据传输速率等于码元脉冲的重复频率。

2)信号传输速率--单位时间内通过信道传输的码元数，单位为波特，记作 Baud。

计算公式：B=1/T (Baud)

式中 T 为信号码元的宽度，单位为秒．信号传输速率,也称码元速率、调制速率或波特率。

可见：S=B*log2N (bps) 或 B=S/log2N (Baud)

3)信道容量表示一个信道的最大数据传输速率，单位：位/秒(bps)

信道容量与数据传输速率的区别是，前者表示信道的最大数据传输速率，是信道传输数据能力的极限，而后者是实际的数据传输速率。像公路上的最大限速与汽车实际速度的关系一样。

4)离散的信道容量

奈奎斯特(Nyquist)无噪声下的码元速率极限值 B 与信道带宽 H 的关系：

B=2*H (Baud)

奈奎斯特公式--无噪信道传输能力公式：

C=2*H*log2N (bps)

式中 H 为信道的带宽，即信道传输上、下限频率的差值，单位为 Hz；N 为一个码元所取的离散值个数。

5)连续的信道容量

香农公式--带噪信道容量公式：C=H*log2(1+S/N) (bps)

式中 S 为信号功率，N 为噪声功率，S/N 为信噪比，通常把信噪比表示成 10lg(S/N)分贝(dB)。

阐述数据传输的几种方式（四种），多元调制、PCM（脉冲编码调制）、抽样定理及其计算 ，曼彻斯特编码和差分曼彻斯特编码 。

多路复用技术及其分类（FDM 和 TDM、WDM）：

多路复用技术就是把许多个单个信号在一个信道上同时传输的技术。频分多路复用 FDM 和时分多路复用 TDM 是两种最常用的多路复用技术。

1.频分多路复用 FDM 技术原理

在物理信道的可用带宽超过单个原始信号所需带宽情况下，可将该物理信道的总带宽分割成若干个与传输单个信号带宽相同(或略宽)的子信道，每个子信道传输一路信号，这就是步分多路复用。

多路原始信号在步分复用前，先要通过频谱搬移技术将各路信号的频谱搬移到物理信道频谱的不同段上，使各信号的带宽不相互重叠，然后用不同的频率调制每一个信号，每个信号要一个样以它的载波频率为中心的一定带宽的通道。为了防止互相干扰，使用保护带来隔离每一个通道。

2.时分多路复用 TDM 技术原理

若媒体能达到的位传输速率超过传输数据所需的数据传输速率，可采用时分多路复用 TDM 技术，即将一条物理信道按时间分成若干个时间片轮流地分配给多个信号使用。每一时间片由复用的一个信号占用，这样，利用每个信号在时间上的交叉，就可以在一条物理信道上传输多个数字信号。

时分多路复用 TDM 不仅局限于传输数字信号，也可同时交叉传输模拟信号。

数据通信系统的一般结构（DTE、DCE 和信道）。

数据通信方式及串行通信的分类（单工、半双工、全双工）：

1.并行通信方式

并行通信传输中有多个数据位，同时在两个设备之间传输。发送设备将这些数据位通过对应的数据线传送给接收设备，还可附加一位数据校验位。接收设备可同时接收到这些数据，不需要做任何变换就可直接使用。并行方式主要用于近距离通信。计算机内的总线结构就是并行通信的例子。这种方法的优点是传输速度快，处理简单。

2.串行通信方式

串行数据传输时，数据是一位一位地在通信线上传输的，先由具有几位总线的计算机内的发送设备，将几位并行数据经并--串转换硬件转换成串行方式，再逐位经传输线到达接收站的设备中，并在接收端将数据从串行方式重新转换成并行方式，以供接收方使用。串行数据传输的速度要比并行传输慢得多，但对于覆盖面极其广阔的公用电话系统来说具有更大的现实意义。

3.串行通信的方向性结构

串行数据通信的方向性结构有三种，即单工、半双工和全双工。

单工数据传输只支持数据在一个方向上传输；

半双工数据传输允许数据在两个方向上传输，但是，在某一时刻，只允许数据在一个方向上传输，它实际上是一种切换方向的单工通信；

全双工数据通信允许数据同时在两个方向上传输，因此，全双工通信是两个单工通信方式的结合，它要求发送设备和接收设备都有独立的接收和发送能力。

数据传输的同步技术，信源与信宿 ，编码与调制.

数据交换技术分类及特点，主要是电路交换、报文交换与分组交换的区别和联系:

数据经编码后在通信线路上进行传输，按数据传送技术划分，交换网络又可分为电路交换网、报文交换网和分组交换网。

电路交换的工作原理

1.电路交换的三个过程

1)电路建立：在传输任何数据之前，要先经过呼叫过程建立一条端到端的电路。

2)数据传输：电路建立以后，数据就可以从一端发送到另一端在整个数据传输过程中，所建立的电路必须始终保持连接状态。

3)电路拆除：数据传输结束后，由某一方发出拆除请求，然后逐节拆除到对方节点。

2.电路交换技术的优缺点及其特点

1)优点：数据传输可靠、迅速，数据不会丢失且保持原来的序列。

2)缺点：在某些情况下，电路空闲时的信道容易被浪费：在短时间数据传输时电路建立和拆除所用的时间得不偿失。因此，它适用于系统间要求高质量的大量数据传输的情况。

3)特点：在数据传送开始之前必须先设置一条专用的通路。在线路释放之前，该通路由一对用户完全占用。对于猝发式的通信，电路交换效率不高。

报文交换的工作原理

问题的提出：当端点间交换的数据具有随机性和突发性时，采用电路交换方法的缺点

是信道容量和有效时间的浪费。采用报文交换则不存在这种问题。

1.报文交换原理

报文交换方式的数据传输单位是报文，报文就是站点一次性要发送的数据块，其长度不限且可变。当一个站要发送报文时，它将一个目的地址附加到报文上，网络节点根据报文上的目的地址信息，把报文发送到下一个节点，一直逐个节点地转送到目的节点。

每个节点在收到整个报文并检查无误后，就暂存这个报文，然后利用路由信息找出下一个节点的地址，再把整个报文传送给下一个节点。因此，端与端之间无需先通过呼叫建立连接。

一个报文在每个节点的延迟时间，等于接收报文所需的时间加上向下一个节点转发所需的排队延迟时间之和。

2.报文交换的特点

1)报文从源点传送到目的地采用"存储--转发"方式，在传送报文时，一个时刻仅占用一段通道。

2)在交换节点中需要缓冲存储，报文需要排队，故报文交换不能满足实时通信的要求。

3.报文交换的优点

1)电路利用率高。由于许多报文可以分时共享两个节点之间的通道，所以对于同样的通信量来说，对电路的传输能力要求较低。

2)在电路交换网络上，当通信量变得很大很大时，就不能接受新的呼叫。而在报文交换网络上，通信量大时仍然可以接收报文，不过传送延迟会增加。

3)报文交换系统可以把一个报文发送到多个目的地，而电路交换网络很难做到这一点。

4)报文交换网络可以进行速度和代码的转换。

4.报文交换的缺点

1)不能满足实时或交互式的通信要求，报文经过网络的延迟时间长且不定。

2)有时节点收到过多的数据而无空间存储或不能及时转发时，就不得不丢弃报文，而且发出的报文不按顺序到达目的地。

分组交换的工作原理

分组交换是报文交换的一种改进，它将报文分成若干个分组，每个分组的长度有一个上限，有限长度的分组使得每个节点所需的存储能力降低了，分组可以存储到内存中，提高了交换速度。它适用于交互式通信，如终端与主机通信。分组交换有虚电路分组交换和数据报分组交换两种。它是计算机网络中使用最广泛的一种交换技术。

1.虚电路分组交换原理与特点

在虚电路分组交换中，为了进行数据传输，网络的源节点和目的节点之间要先建一条逻辑通路。每个分组除了包含数据之外还包含一个虚电路标识符。在预先建好的路径上的每个节点都知道把这些分组引导到哪里去，不再需要路由选择判定。最后，由某一个站用清除请求分组来结束这次连接。它之所以是“虚”的，是因为这条电路不是专用的。

虚电路分组交换的主要特点是：在数据传送之前必须通过虚呼叫设置一条虚电路。但并不像电路交换那样有一条专用通路，分组在每个节点上仍然需要缓冲，并在线路上进行排队等待输出。

2.数据报分组交换原理与特点

在数据报分组交换中，每个分组的传送是被单独处理的。每个分组称为一个数据报，每个数据报自身携带足够的地址信息。一个节点收到一个数据报后，根据数据报中的地址信息和节点所储存的路由信息，找出一个合适的出路，把数据报原样地发送到下一节点。由于各数据报所走的路径不一定相同，因此不能保证各个数据报按顺序到达目的地，有的数据报甚至会中途丢失。整个过程中，没有虚电路建立，但要为每个数据报做路由选择。

（二） 传输介质　双绞线、同轴电缆、光纤与无线传输介质 ， 物理层接口的特性：

传输媒体是通信网络中发送方和接收方之间的物理通路，计算机网络中采用的传输媒体分有线和无线两大类。

传输媒体的特性对网络数据通信的质量有很大影响，这些特征是：

⑴物理特性：说明传输媒体的特性。

⑵传输特性：包括是使用模拟信号发送还是使用数字信号发送、调制技术、传输容量及传输频率范围。

⑶连通性：采用点到点连接还是多点连接。

⑷地理范围：在不用中间设备并将失真限制在允许范围内的情况下，整个网络所允许的最大距离。

⑸抗干扰性：防止噪音、电磁干扰对传输数据影响的能力。

⑹相对价格：包括元件、安装和维护等价格。

1.有线传输媒体

1)双绞线(TP)--由螺旋状扭在一起的两根绝缘导线组成。双绞线一般分为非屏蔽双绞线(UTP)和屏蔽双绞线(STP)。计算机网络中最常用的是第三类和第五类非屏蔽双绞线。

⑴物理特性：铜质线芯，传导性能良好。

⑵传输特性：可用于传输模拟信号和数字信号，对于模拟信号，约 5--6 公里需要一个放大器；对于数字信号，约 2--3 公里需要一个中继器。双绞线的带宽达 268kHz。

对于模拟信号，可用频分多路复用技术把它分成 24 路来传输音频模拟信号，根据目前的 Modem 技术，若使用移相键控法 PSK，每路可达 9600bps 以上，这样，在一条 24 路的双绞线上，总传输率可达 230kbps。

对于数字信号，使用 T1 线路总传输率可达 1.544Mbps。达到更高传输率也是可能的，但与距离有关。

对于局域网(10BASE-T 和 100BASE-T 总线)，传输速率可达 10Mbps-100Mbps。常用的 3 类双绞线和 5 类双绞线电缆均由 4 对双绞线组成，3 类双绞线传输速率可达 10Mbps，5 类双绞线传输速率可达 100Mbps。但与距离有关。

⑶连通性：可用于点到点连接或多点连接。

⑷地理范围：对于局域网，速率 100Kbps,可传输 1 公里；速率 10Mbps--100Mbps,可传输 100 米。

⑸抗干扰性：低频(10kHz 以下)抗干扰性能强于同轴电缆，高频(10-100kHz)抗干扰性能弱于同轴电缆。

⑹相对价格：比同轴电缆和光纤便宜得多。

2)同轴电缆--由绕同一轴线的两个导体所组成，被广泛用于局域网中。为保持同轴电缆的正确电气特性，电缆必须接地，同时两头要有端接器来削弱信号反射作用。

⑴物理特性：单根同轴电缆直径约为 1.02-2.54cm，可在较宽频范围工作。

⑵传输特性：基带同轴电缆仅用于数字传输，阻抗为 50Ω，并使用曼彻斯特编码，数据传输速率最高可达 10Mbps。宽带同轴电缆可用于模拟信号和数字信号传输，阻抗为 75Ω，对于模拟信号，带宽可达 300-450MHz。在 CATV 电缆上，每个电视通道分配 6MHz 带宽，而广播通道的带宽要窄得多，因此，在同轴电缆上使用频分多路复用技术可以支持大量的视、音频通道。基带 50

⑶连通性：可用于点到点连接或多点连接。

⑷地理范围：基带同轴电缆的最大距离限制在几公里；宽带电缆的最大距离可以达几十公里。

⑸抗干扰性：能力比双绞线强。

⑹相对价格：比同轴电缆贵，比光纤便宜。

3)光纤--由能传导光波的石英玻璃纤维外加保护层构成的。光纤具有宽带、数据传输率高、抗干扰能力强、传输距离远等优点。按使用的波长区的不同分为单模和多模光纤通信方式。

⑴物理特性：在计算机网络中均采用两根光纤(一来一去)组成传输系统。按波长范围可分为三种：0.85um 波长(0.8-0.9um)、1.3um 波长(1.25-1.35um)和 1.55um 波长区(1.53-1.58um)。不同的波长范围光纤损耗特性也不同，其中 0.85um 波长区为多模光纤通信方式，1.55um 波长区为单模光纤通信方式，1.3um 波长区有多模和单模两种方式。

⑵传输特性：光纤通过内部的全反射来传输一束经过编码的光信号，内部的全反射可以在任何折射指数高于包层媒体折射指数的透明媒体中进行。实际上光纤作为频率范围从 10^{14}-10^{15}Hz 的波导管，这一范围覆盖了可见光谱和部分红外光谱。光纤的数据传输率可达 Gbps 级，传输距离达数十公里。目前，一条光纤线路上只能传输一个载波，随着技术进一步发展，会出现实用的多路复用光纤。

⑶连通性：采用点到点连接还是多点连接。

⑷地理范围：可以在 6-8 公里的距离内不用中继器传输，因此光纤适合于在几个建筑物之间通过点到点的链路连接局域网。

⑸抗干扰性：不受噪声或电磁影响，适宜在长距离内保持高数据传输率，而且能够提供良好的安全性。

⑹)相对价格：目前价格比同轴电缆和双绞线都贵。

2.无线传输媒体

1)微波通信：载波频率为 2GHZ 至 40GHZ。频率高，可同时传送大量信息；由于微波是沿直线传播的，故在地面的传播距离有限。

2)卫星通信：是利用地球同步卫星作为中继来转发微波信号的一种特殊微波通信形式。卫星通信可以克服地面微波通信距离的限制，三个同步卫星可以覆盖地球上全部通信区域。

3)红外通信和激光通信：和微波通信一样，有很强的方向性，都是沿直线传播的。但红外通信和激光通信要把传输的信号分别转换为红外光信号和激光信号后才能直接在空间沿直线传播。

微波、红外线和激光都需要在发送方和接收方之间有一条视线通路，故它们统称为视线媒体。

（三） 物理层设备　中继器 ，集线器，重点比较其功能和性能的区别。

【教学重点和难点】带宽，速率的概念，电路交换、报文交换与分组交换的区别，中继和集线的区别

【典型习题讲解】带宽，速率的计算

第三学时： 数据链路层

【知识点】

（一） 数据链路层的功能 链路管理，帧定界，流量控制，差错控制，将数据和控制信息区分开，透明传输，寻址等主要功能。

（二） 组帧

（三） 差错控制　检错编码和纠错编码的基本原理的算法解析

用以使发送方确认接收方是否正确收到了由它发送的数据信息的方法称为反馈差错控制。通常采用反馈检测和自动重发请求(ARQ)两种基本方法来实现。

1.反馈检测法

反馈检测法也称回送校检法或“回声”法，主要用于面向字符的异步传输中，如终端与远程计算机间的通信。这是一种无须使用任何特殊代码的差错检测法。双方进行数据传输时，接收方将接收到的数据（可以是一个字符，也可以是一帧）重新发回发送方，由发送方检查是否与原始数据完全相符。若不相符，则发送方发送一个控制字符（如 DEL）通知接收方删去出错的数据，并重新发送该数据；若相符，则发送下一个数据。

反馈检测法原理简单，实现容易，也有较高的可靠性。但每个数据均被传输两次，信道利用率很低。这种差错控制方法一般用于面向字符的异步传输中，因为这种场合下信道效率并不是主要矛盾。

2.自动重发请求法(ARQ 法)

实用的差错控制方法，既要传达室输可靠性高，又要信道利用率高。为此可使发送方将要发送的数据帧附加一定的冗余检错码一并发送，接收方则根据检错码对数据帧进行差错检测，若发现错误，就返回请求重发的应答，发送方收到请求重发的应答后，便重新传送该数据帧。这种差错控制方法就称为自动重发请求法(Automatic Repeat reQuest)，简称 ARQ 法。

ARQ 法仅需返回少量控制信息，便可有效地确认所发数据帧是否正确被接收。ARQ 法有几种实现方案，空闲重发请求(Idle RQ)和连续重发请求(Continuous RQ)是其中最基本的两种方案。

(1)空闲重发请求(Idle RQ)。空闲重发请求方案也称停等(Stop and Wait)法，该方案规定发送方每发送一帧后就要停下来等待接收方的确认返回，仅当接收方确认正确接收后再继续发送下一帧 。空闲重发请求方案的实现过程如下：

①发送方每次仅将当前信息帧作为待确认帧保留在缓冲存储器中；

②当发送方开始发送信息帧时，随即启动计时器；

③当接收方收到无差错信息帧后，即向发送方返回一个确认帧；

④当接收方检测到一个含有差错的信息帧时，便舍弃该帧；

⑤若发送方在规定时间内收到确认帧，即将计时器清零，继而开始下一帧的发送；

⑥若发送方在规定时间内未收到确认帧，(即计时器超时)，则应重发存于缓冲器中的待确认信息帧。

从以上过程可以看出，空闲 RQ 方案的收、发送方仅需设置一个帧的缓冲存储空间，便可有效地实现数据重发并确保接收方接收的数据不会重份。空闲 RQ 方案最主要的优点就是所需的缓冲存储空间最小，因此在链路端使用简单终端的环境中被广泛采用。

(2)连续重发请求(Continuous RQ)。连续重发请求方案是指发送方可以连续发送一系列信息帧，即不用等前一帧被确认便可发送下一帧。这就需要在发送方设置一个较大的缓冲存储空间(称作重发表)，用以存放若干待确认的信息帧。当发送方到对某信息帧的确认帧后便可从重发表中将该信息帧删除。所以，连续 RQ 方案的链路传输效率大大提高，但相应地需要更大的缓冲存储空间。连续 RQ 方案的实现过程如下：

①发送方连续发送信息帧而不必等待确认帧的返回；

②发送方在重发表中保存所发送的每个帧的备份；

③重发表按先进先出(FIFO)队列规则操作；

④接收方对每一个正确收到的信息帧返回一个确认帧；

⑤每一个确认帧包含一个惟一的序号，随相应的确认帧返回；

⑥接收方保存一个接收次序表，它包含最后正确收到的信息帧的序号；

⑦当发送方收到相应信息帧的确认后，从重发表中删除该信息帧的备份；

⑧当发送方检测出失序的确认帧(即第 N 号信息帧和第 N+2 号信息帧的确认帧已返回，而 N+1 号的确认帧未返回)后，便重发未被确认的信息帧。

上面连续 RQ 过程是假定在不发生传输差错的情况下描述的，如果差错出现，如何进一步处理还可以有两种策略，即 GO-DACK-N 策略和选择重发策略。

GO-DACK-N 策略的基本原理是，当接收方检测出失序的信息帧后，要求发送方重发最后一个正确接收的信息帧之后的所有未被确认的帧；或者当发送方发送了 N 个帧后，若发现该 N 帧的前一个帧在计时器超时后仍未返回其确认信息，则该帧被判为出错或丢失，此时发送方就不得不重新发送出错帧及其后的 N 帧。这就是 GO-DACK-N(退回 N)法名称的由来。因为，对接收方来说，由于这一帧出错，就不能以正常的序号向它的高层递交数据，对其后发送来的 N 帧也可能都不能接收而丢弃。GO-DACK-N 可能将已正确传送到目的方的帧再重传一遍，这显然是一种浪费。另一种效率更高的策略是当接收方发现某帧出错后，其后继续送来的正确的帧虽然不能立即递交给接收方的高层，但接收方仍可收下来，存放在一个缓冲区中，同时要求发送方重新传送出错的那一帧。一旦收到重新传来的帧后，就可以原已存于缓冲区中的其余帧一并按正确的顺序递交高层。这种方法称为选择重发(SELECTICE REPEAT)。

（四） 流量控制与可靠传输机制 . 流量控制、可靠传输与滑轮窗口机制的基本原理和方法，重点解析单帧滑动窗口与停止-等待协议，.多帧滑动窗口与后退 N 帧协议（GBN），多帧滑动窗口与选择重传协议（SR）并进行实例化描述。

流量控制涉及链路上字符或帧的发送速率的控制, 以使接收方在接收前的足够的缓冲存储空间来接收每一个字符或帧。例如,在面向字符的终端——计算机链路中，若远程计算机为许多台终端服务，它就有可能因不能在高峰时按预定速率传输全部字符而暂时过载。同样，在面向帧的自动重发请求系统中，当待确认帧数量增加时，有可能超出缓冲器存储空间，也会造成过载。下面介绍两种常用的流量控制方案：XON/XOFF 方案和窗口机制。

1.XON/XOFF 方案

增加缓冲存储空间在某种程度上可以缓解收、发双方在传输速率上的差异，但这是一种被动、消极的方法。因为，一方面系统不允许开设过大的缓冲空间，另一方面对于速率显著失配并且又传送大量数据的场合，仍会出现缓冲空间不够的现象。XON/XOFF 方案方案则是一种相比之下更主动、更积极的流量控制方法。

XON/XOFF 方案中使用一对控制字符来实现流量控制，其中 XON 采用 ASCII 字符集中的控制字符 DC1，XOFF 采用 ASCII 字符集中的控制字符 DC3。当通信路上的接收方发生过载时，便向发送方发送一个 XOFF 字符，发送方接收 XOFF 字符后便暂停发送数据；等接收方处理完缓冲器中的数据，过载恢复后，再向发送方发送一个 XON 字符，以通知发送方恢复数据发送。在一次数据传输过程中，XOFF、XON 的周期可重复多次，但这些操作对用户来说是透明的。

许多异步数据通信软件包均支持 XON/XOFF 协议。这种方案也可用于计算机向打印机或其它终端设备发送字符，在这种情况下，打印机或终端设备中的控制部件用以控制字符流量。

2.窗口机制

为了提高信道的有效利用率，如前所述采用了不等待确认帧返回就连续发送若干帧的方案。由于允许连续发送多个未被确认的帧 ，帧号就需采用多位二进制才能加以区分。因为凡被发出去蛤尚未被确认的帧都可能出错或丢失而要求重发，因而这些帧都要保留下来。这就要求发送方有较大的发送缓冲区保留可能要求重发的未被确认的帧。

但是缓冲区容量总是有限的，如果接收方不能以发送方的发送速率处理接收到的帧，

则还是可能用完缓冲容量而暂时过载。为此，可引入类似于空闲 RQ 控制方案的调整措施，其本质是在收到一确定帧之前，对发送方可发送的帧的数目加以限制。这是由发送方调整保留在重发表中的待确认帧的数目来实现的。如果接收方来不及时对心到的帧进行处理，则便停发确认信息，此时发送方的重发送方的重发表就会增长，当达到重发表限度时，发送方就不再发送新帧，直至再次收到确认信息为止。

不了实现此方案，发送方存放待确认帧的重发表中，应设置待确认帧数目的最大限度，这一限度被称为链路的发送窗口。显然，如果窗口设置为 1，即发送方缓冲能力仅为一个帧，则传输控制方案就回到了空闲 RQ 方案，此时传输效率很低。故窗口限度应选为使接收方尽量能处理或接受收到的所有帧。当然选择时还必须考虑诸如帧的最大长度、可使用的缓冲存空间以及传输速率等因素。

重发表是一个连续序号的列表，对应发送方已发送但尚未确认的那些帧。这些帧的序号有一个最大值，这个最大值即发送窗口的限度。所谓发送窗口就是指示发送方已发送但尚未确认的帧序号队列的界，其上、下界分别称为发送窗口的上、下沿，上、下沿的部距称为窗口尺寸。接收方类似地也有接收窗口，它批示允许接收和帧的序号。

发送方每次发送一帧后，待确认帧的数目便增 1，每收到一个确认信息后，待确认帧的数目便减 1。当重发表长度计数值，即待确认帧的数目等于发送窗口尺寸时，便停止发送新的帧。

一般帧号只取有限位二进制数，到一定时间后就又反复循环。若帧号配 3 位二进制数，则帧号在 0~7 间循环。如果发送窗口尺寸取值为 2。则发送如图 3.15 所示。图中发送方阴影部分表示打开的发送窗口，接收方阴影部分则表示打开的接收窗口。当传送过程进行时，打开的窗口位置一直在滑动，所以也称为滑动窗口(Slidding Window)，或简称为滑窗。

一般来说，凡是在一定范围内到达的帧，即使它们不按顺序，接收方也要接收下来。若把这个范围看成是接收窗口的话，由接收窗口的大小也应该是大于 1 的。而 Go-back-N 正是接收窗口等于 1 的一个特例，选择重发也可以看做是一种滑动窗口协议，只不过其发送窗口和接收窗口都大于 1。若从滑动窗口的观点来统一看待空闲 RQ、Go-back-N 及选择重发三种协议，它们的差别仅在于各自窗口尺寸的大小不同而已：

空闲 RQ：　　发送窗口=1，接收窗口=1；

Go-back-N：　发窗口>1，接收窗口>1;

选择重发：　发送窗口>1,接收窗口>1。

若帧序号采用 3 位二进制编码，由最大序号为 Smax=2^3-1=7。对于有序接收方式，发送窗口最大尺寸选为 Smax；对于无序接收方式，发送窗口最大尺寸至多是序号范围的一半。发送方管理超时控制的计时器数应等于缓冲器数，而不是序号空间的大小。

（五）介质访问控制 . 讲授信道划分，频分多路复用、时分多路复用、波分多路复用、码分多路复用的概念和基本原理。重点随机访问介质访问控制. 主要是 ALOHA 随机争用协议（ 纯 ALOHA 技术 和 时隙 ALOHA 技术），CSMA 随机访问技术（先听后说），以及非坚持型算法，1-坚持型算法和 p-坚持型算法。CSMA/CD 随机访问技术，主要是 CSMA/CD—带有碰撞（冲突）检测的载波监听多路访问控制方法及其主要特点：先听后说，边听边说（二进制指数避让算法）。

具有冲突检测的载波监听多路访问 CSMA/CD

具有冲突检测的载波监听多路访问 CSMA/CD 采用随机访问和竞争技术，这种技术只用于总线拓扑结构网络。CSMA/CD 结构将所有的设备都直接连到同一条物理信道上,该信道负责任何两个设备之间的全部数据传送，因此称信道是以“多路访问”方式进行操作的。站点以帧的形式发送数据，帧的头部含有目的和源点的地址。帧在信道上以广播方式传输，

所有连接在信道上的设备随时都能检测到该帧。当目的地站点检测到目的地址为本站地址的帧时，就接收帧中所携带的数据，并按规定的链路协议给源站点返回一个响应。

采用这种操作方法时，在信道上可能有两个或更多的设备在同一瞬间都会发送帧，从而在信道上千万帧的重叠而出现并有差错，这种现象称为冲突。为减少这种冲突，源站点在发送帧之前，首先要监听信道上是否有其它站点发送的载波信号(即进行“载波监听”)，若监听到信道上有载波信号则推迟发送，直到信道恢复到安静(空闲)为止。另外，还要采用边发送边监听的技术(即“冲突检测”)，若监听到干扰信号，就表示检测到冲突，于是就要立即停止发送。为了确保冲突的其它站点知道发生了冲突，首先在短时间里持续发送一串阻塞(Jam)码,卷入冲突的站点则等待一随机时间，然后准备重发受到冲突影响的帧。这种技术对发生冲突的传输能迅速发现并立即停止发送,因此能明显减少冲突次数和冲突时间。

轮询访问介质访问控制：令牌传递协议。

控制令牌是另一种传输媒体访问控制方法。它是按照所有站点共同理解和遵守的规则，从一个站点到另一个站点传递控制令牌，一个站点只有当它占有令牌时，才能发送数据端帧，发完帧后，即把令牌传递下一个站点。其操作次序如下：

⑴首先建立一个逻辑环，将所有站点同物理媒体相连，然后产生一个控制令牌。

⑵控制令牌由一个站点沿着逻辑环顺序向下一个站点传递。

⑶等待发送帧的站点接收到控制令牌后，把要发送的帧利用物理媒体发送出去，然后再将控制令牌沿逻辑环传递给下一站点。

控制令牌方法除了用于环形网拓扑结构(即令牌环)之外,也可以用于总线网拓扑结构(即令牌总线)。

【教学重点和难点】流量控制与可靠传输机制，介质访问控制
【典型习题讲解】滑动窗口，CSMA/CD 协议；CSMA/CA 协议

第四学时： 数据链路层（续）

（一） 局域网 ．局域网的基本概念与体系结构 ，分析 LAN 特性的三个主要技术：传输介质、拓扑结构、介质访问控制方法（MAC）其中 MAC 最重要。 以太网与 IEEE 802.3，包括总线网、以太网（Ethernet），以太网及其标准（10BASE、100BASE 和 1000BASE），以太网中继规则（5-4-3-2-1 规则）。

IEEE 在 1980 年 2 月成立了局域网标准化委员会（简称 IEEE 802 委员会），专门从事局域网的协议制订，形成了一簇的标准，称为 IEEE 802 标准。该标准已被国际标准化组织 ISO 采纳，作为局域网的国际标准系列，称为 ISO 8802 标准。要这些标准中，根据局域网的多种类型，规定了各自的拓朴结构、媒体访问控制方法、帧和格式和听任等内容。

IEEE 802.1 是局域网的体系结构、网络管理和网际互连协议。IEEE 802.2 集中了数据链路层中与媒体无亲的 LLC 协议。涉及与媒体访问有关的协议，则根据具体网络的媒体访问控制访问分别处理，其中主要的 MAC 协议有：IEEE 802.3 载波监听多路访问/冲突检测 CSMA/CD 访问方法和物理层协议、IEEE 802.4 令牌总线（Token Bus)访问方法和物理层的协议、IEEE 802.5 令牌环（Token Ring)访问方法和物理层协议，IEEE 802.6 关于城域网的分布式他列总线 DQDB（Distributed Queue Dual Bus)的标准等。

IEEE 802 标准定义了 LLC 子层和 MAC 子层的帧格式。数据传输过程中，LLC 子层将高层递交的报文分组作为 LLC 的信息字段，再加上 LLC 子层目的服务访问点（DSAP)、源服务访问点（SSAP）及相应的控制信息以构成 LLC 帧。

LLC 的链路只有异步平衡方式（ABM），而不用政党响应方式（NRM）和异步响应（ARM）。也即节点均为组合站，它们既可作为主站发送命令，也可作为从站响应命令。IEEE 802.2 标准定义的 LLC 帧格式与 HDLC 的帧格式有点类似，其控制字段的格式和功能完全效仿 HDLC 的平衡方式制定。LLC 帧也分为信息帧、监控帧和无编号帧三类。信息帧主要用于信息数据传输，监控帧主要用于流量控制，无编号帧用于 LLC 子层传输控制信号以对逻辑链路进行建立与释放。LLC 帧的类型取决于控制字段的第 1 、2 位，信息帧和监控帧的控制字段均为 2 字长，无编号帧的控制字段为 1 字节。监控帧控制字段中的第 5 ～ 8 位为保留位，一般设置为 0 。控制字段中的其它位含义与 HDLC 控制字段中的含义相同。

交换以太网特点、三种转发机制及 VLAN（虚拟局域网）概念。令牌环网的基本原理，IEEE802.5--令牌环网（Token Ring）令牌环介质访问控制方法工作原理及其特点，IEEE802.4--令牌总线网（Token-Bus）令牌总线介质访问控制方法工作原理及其特点，总结令牌总线的特点，即物理上是总线结构，逻辑上是令牌环。

（二） 广域网　广域网的基本概念 ，. PPP 协议 ， HDLC 协议 包括 HDLC 链路结构，HDLC 的帧格式，零比特插入删除技术（位填充删除技术），HDLC 的帧类型（信息帧（I 帧）、监控帧（S 帧）、无编号帧（U 帧））。

HDLC 是通用的数据链路控制协议，在开始建立数据链路时，允许选用特定的操作方式。所谓操作方式，通俗地讲就是某站点是以主站点方式操作还是以从站方式操作，或者是二者兼备。链路上用于控制目的的站称为主站，其它的受主站控制的站称为从站。主站对数据流进行组织，并且对链路上的差错实施恢复。由主站发往从站的帧称为命令帧，而从从站返回主站的帧称为响应帧。连有多个站点的链路通常使用轮询技术，轮询其它站的站称为主站，而在点-点链路中每个站均可为主站。主站需要比从站有更多的逻辑功能，所以当终端与主机相连时，主机一般总是主站。在一个站连接多个链路的情况下，该站对于一些链路而言可能是主站，而对于一些链路而言又可能是从站。有些站可兼备主站和从站的功能，这种站称为组合站，用于组合站之间信息传输的协议是对称的，即在链路上主、从站具有同样的传输控制功能，这又称作平衡操作。相对的，那种操作时有主站、从站之分的，且各自功能不同的操作，称为非平衡操作。

HDLC 中常有的操作方式有以下三种：

①正常响应方式 NRM(Norma Responses Model) 。这是一非平衡数据链路方式，有时也称非平衡正常响应方式。该操作方式适用于面向终端的点—点或一点与多点的链路。在这种操作方式中，传输过程由主站启动，从站只有收到主站某个命令帧后，才能作出响应向主站传输信息。响应信息可以由一个或多个帧组成，若信息由多个帧组成，则应指出哪一个是最后一帧 。主站负责整个链路，且具有轮询、选择从站及向从站发送命令的权利，同时也负责对超时、重发及各类恢复操作的控制。

②异步响应方式 ARM Asynchronous Responses Mode)这也是一种非平衡数据链路操作方式，与 NRM 不同的是，ARM 下的传输过程由从站启动。从站主的动发送给主站的一个或一组帧中可包含有信息，也可以是仅以控制为目的而发的帧。在这种操作方式，与 NRM 不同的是，ARM 下的传输过程由从站启动。从站主的动发送给主站的一个或一组帧中可包含有信息，也可以是仅以控制为目的而发的帧。在这种操作方式下，由从站来控制超时和重发。该方式对采用轮询方式的多站链路来说是必不可少的。

③异步平衡方式 ABM(Asynchronous Balanced Mode).这是一种允许任何节点来启动传输的操作方式。为了提高链路传输效率，节点之间在两个方向上都需要有较高的信息传输量。在这种操作方式下，任何时候任何站点都能启动传输操作，每个站点既可作为主站又可作为从站，即每个站都是组合站。各站都有相同的一组协议，任何站点都可以发送或接

收命令，也可以给出应答，并且各站对差错恢复过程都负有相同的责任。
ATM 网络基本原理。

ATM 采用异步时分复用方式工作，来自不同信息源的信元汇集到一起，在一个缓冲器内排队，队列中的信元著个输出到传输线路，在传输线路上形成首尾相接的信元流。信元的信头中写有信息的标志(如 A 和 B)，说明该信元去往的地址，网络根据信头中的标志来转移信元。

信息源随机地产生信息，因为信元到达队列也是随机的。高速的业务信元来得十分频繁、集中，低速的业务信元来得很稀疏。这些信元都按先来后到在队列中排队，然后按输出次序复用到传输线上。具有同样标志的信元在传输线上并不对应某个固定的时间间隙，也不是按周期出现的，也即信息和它在时域的位置之间没有关系，信息只是按信头中的标志来区分的。这种复用方式称为异步时分复用(Asynchronous Time Division Multiolex)，又称统计复用(Statistic Multiptx)。而在同步时分复用方式(如 PCM 复用方式)中，信息以它在一帧中的时间位置(时隙)来区分，一个时隙对应着一条信道，不需要另外的信息头来标识信息的身份。

异步时分复用方式使 ATM 具有很大的灵活性，任何业务也都可按实际需要来占用资源。对于特定的业务，传送速率可随信息到达的速率而变化，因此网络资源得到了最大限度的利用。ATM 网络可以适用于任何业务，不论其特性如何(速率高低、突发性大小、质量和实时性要求等)，网络都按同时的模式来处理，真正做到了完全的业务综合。

若某个时刻队列中没有等待发送的信元，此时线路上就出现未分配信元(信头中含有标志 φ)；反之，若某个时刻传输线路上找不到可以传送新元的机会(信云啊都已排满)，而队列已经充满缓冲区，此时为了尽量减少对业务质量的影响，将优先级别低的信元丢弃。缓冲区的容量必须根据信息流量来计算，以使信元丢弃率在 10-9 以下。

为了提高处理速度和降低延迟，ATM 以面向连接器的方式工作。网络的处理工作十分简单：通信开始时建立虚电路，以后用户将虚电路标志写入信头(即地址信息)，网络根据虚电路标志将信元送往目的地。

经过 ATM 网络中的节点提供信元的交换。其实，ATM 网络的节点完成的只是虚电路的交换，因为同一虚电路上的所有信元都选择同样的路由，经过同样的通路到达目的地。在接收段，这些信元到达的次序总是和发送次序相同。

ATM 交换节点的工作比 X.25 分组交换网中的节点要简单得多。ATM 节点只做信头的 CRC 检验，对于信息的传输差错根本不过问。ATM 节点不做差错控制(信头中根本你没有信元的编号)，也不参与流量控制，这些工作都留给终端去做。ATM 节点的主要工作就是读信头，并根据信头的内容快速的将信元送往要去的地方，这件工作在很大的程度上依靠硬件来完成，所以 ATM 交换的速度非常快，可以和光纤的传输速度相匹配。

（三） 数据链路层设备

网桥，网桥的概念：

网桥是一种存储转发设备，用来连接类型相似的局域网。从互连网络的结构看，网桥属于 DCE 级的端到端的连接；从协议层次看，网桥属于链路层范畴，存该层对数据帧进行存储转发。它既不同于只作单纯信号增强的转接器，也不同于进行网络层转换的网间连接器。但网桥仍然是一种网络连接的方法，因为局域网本身没有网络层，只有在主机站点上才有网络层或提供网络层服务的功能。

网桥接收帧并送到数据链路层进行差错校验，然后送到物理层再经物理传输媒体送到另一个子网。在转发帧以前，网桥对帧的内容和格式不做修改或仅做很少的修改。 网桥应该有足够的缓冲空间，以便能满足高峰负荷时的要求。另外，必须具备寻址和路由选择的；

逻辑功能。

透明网桥与生成树算法；源选径网桥与源选径算法。局域网交换机及其工作原理。

【教学重点和难点】IEEE 802.x 系列协议，网桥选径算法
【典型习题讲解】HDLC 协议，网桥选径算法

第五学时： 网络层

（一） 网络层的功能 异构网络互联原则，路由与转发的区别和工作原理，拥塞控制的一半处理方式。

（二） 路由算法 静态路由与动态路由的划分原则，距离-向量路由算法 ，链路状态路由算法 ，层次路由路由选择算法及其分类，Dijstra 算法（求最短路由），OSPF 部分详细讲解，. D-V 法和 L-S 法(距离矢量法和链路状态法)，介绍计算路由的方法，并写出路由表、画出路由树。

（三） IPv4 IPv4 分组原则，是一种分等级的地址结构。IPv4 地址与 NAT，地址转换的必要性和原理。子网划分与子网掩码的基本思路和具体实践中的注意事项。CIDR 的概念和作用，即消除了传统的 A 类、B 类和 C 类地址以及划分子网的概念，有效地分配 IPv4 的地址空间。

从概念上说，IP 地址的层次结构具有两个重要特性：

- 每台主机分配了一个唯一的地址。
- 网络标识号的分配必须全球统一，但主机标识号可由本地分配，不需全球一致。

IP 地址有不同的版本：IPv4、IPv6。现以当前因特网使用的 IPv4(第 4 版本)为例说明 IP 编址，因特网(IP 网)为每台主机分配一个唯一的 4 字节(32 比特)IP 地址。为了便于管理，把这 32 位地址按分级地址空间的树形表示法分为两个部分：网络号和主机号(net-id，host-id)。主机号为全 0 的网络地址定义为网络号，它标识因特网上的唯一网络。

4 字节的 IP 地址，采用"点分十进制"的方法来表示，例如，202.119.224.93。每一个十进制数表示 4 个字节中的一个，排列次序从左到右。由于每个字节为 8 比特，所以每个十进制数只允许在 0~255 范围内。根据因特网上的网络规模，IP 地址可分为 A 类、B 类、C 类、D 类和 E 类。

(1) A 类网：网络号为 1 字节，定义最高比特为 0 为 A 类网识别符，余下 7 比特为网络号，主机号则可有 24 比特编址。可见 A 类网支持大型网络，可用网络号为 126 个，每个 A 类网可含 2^{24}=16777216 个主机号。比如，IP 地址为 15.1.2.25，是 A 类网，其网络号为 15，主机号为 1.2.25。

(2) B 类网：网络号为 2 字节，定义最高二比特为 10 为 B 类网识别符，余下 14 比特为网络号，主机号则可有 16 比特编址。B 类网是中型网络，可用网络号为 16382 个，每个 B 类网可含 2^{16}=65536 个主机号。

(3) C 类网：网络号为 3 字节，定义最高三比特为 110 为 C 类网识别符，余下 21 比特为网络号，主机号仅有 8 比特编址。C 类网是小型网络，可用网络号为 2097150 个，每个 C 类网可含 2^{8}=256 个主机号，可用主机号为 254 个。

(4) D 类网：不分网络号和主机号，定义最高四比特为 1110 为 D 类网址识别符，表示一个多播地址，即多目的地传输，可用来识别一组主机。

如何识别任一 IP 地址的属性？只须从点分法的最左一个十进制数，就可判断其归属。

例如，1~126 属 A 类网址，128~191 属 B 类网址，192~223 属 C 类网址，224~239 属 D 类网址。除了以上四类网址外，还有 E 类地址，暂未使用。

对于因特网 IP 地址中有特定的专用地址，不作分配：

(1) 主机地址全为"0"

不论哪类网络，主机地址全为"0"表示指向本网，常用在路由表中。例如，18.0.0.0 表示其网络号为 18。

(2) 主机地址全为"1"

主机地址全为"1"表示广播地址，向特定的所在网上所有主机发送数据报。例如，IP 地址为 202.119.224.225，是要求指向 202.119.224 网上的所有主机转发数据报。

(3) 4 字节 32 比特全为"1"

若 IP 地址 4 字节 32 比特全为"1"，表示仅在本网内进行广播发送。

(4) 网络号 127

TCP/IP 协议规定网络号 127 不可用于任何网络。其中有一个特别地址：127.0.0.1 称之为回送地址(loopback)，它将信息通过自身的接口发送后返回，可用来测试端口状态。ARP 协议是解决同一个局域网上的主机或路由器的 IP 地址和硬件地址的映射问题。DHCP 协议透过 "租约" 的概念，有效且动态的分配客户端的 TCP/IP 设定，包括 IP 地址，子网掩码，网关，DNS 等。ICMP 协议 允许主机或路由器报告差错情况和提供有关异常情况的报告，阐明 ICMP 不是高层协议，而是 IP 层的协议，是为 IP 层数据报的数据，加上数据报的首部，组成 IP 数据报发送出去，典型应用如 ping, tracert 等。

（四） IPv6

IPv6 的主要特点，IPv6 地址的特点和优点，包括扩展的地址层次结构，首部格式，选项，允许协议继续扩充，支持即插即用（即自动配置），支持资源的预分配。

IPv6 数据包有一个 IPv6 报头、多个扩展报头和一个上层协议数据单元组成。

IPv6 报头 （IPv6 Header）

每一个 IPv6 数据包都必须包含报头，其长度固定为 40 字节。IPv6 基本报头也称之为固定报头。固定报头包含 8 个字段，总长度为 40 个字节。这 8 个字段分别为：版本、流量类型、流标签、有效载荷长度、下一个包头、跳限制、源 IPv6 地址、目的 IPv6 地址。

扩展报头 （Extension Header）

IPv6 扩展报头是可能跟在基本 IPv6 报头后面的可选报头。IPv6 数据包中可以包含一个或多个扩展报头，当然也可以没有扩展报头，这些扩展报头可以具有不同的长度。IPv6 报头和扩展报头代替了 IPv4 报头及其选项。新的扩展报头格式增强了 IPv6 的功能，使其具有极大的扩展性。与 IPv4 报头中的选项不同，IPv6 扩展报头没有最大长度的限制，因此可以容纳 IPv6 通信所需要的所有扩展数据。IPv6 扩展报头是可能跟在基本 IPv6 报头后面的可选报头。为什么在 IPv6 中要设计扩展报头这种字段呢？我们知道在 IPv4 的报头中包含了所有的选项，因此每个中间路由器都必须检查这些选项是否存在，如果存在，就必须处理它们。这种设计方法会降低路由器转发 IPv4 数据包的效率。为了解决这种矛盾，在 IPv6 中，相关选项被移到了扩展报头中。中间路由器就不需要处理每一个可能出现的选项（在 IPv6 中，每一个中间路由器必需处理唯一的扩展报头是逐跳选项扩展报头），这种处理方式提高了路由器处理数据包的速度，也提高了其转发性能。下面是一些扩展报头：

逐跳选项报头（Hop-by-Hop Options header）

目标选项报头（Destination Options header）

路由报头（Routing header）

分段报头（Fragment header）

认证报头（Authentication header）

封装安全有效载荷报头（Encapsulating Security Payload header）

在典型的数据包中，并不是每一个数据包都包括所有的扩展报头。在中间路由器或目标需要一些特殊处理时，发送主机才会添加相应扩展报头(具体扩展报头内容下面会详细讲解)。如果数据包中没有扩展报头，也就是说数据包只包括基本的报头和上层协议单元，基本报头的下一个报头（Next Header）字段值指明上层协议类型。

上层协议数据单元 （Upper Layer Protocol Data Unit）

上层协议数据单元一般由上层协议包头和他的有效载荷构成，有效载荷可以是一个 ICMPv6 报文、一个 TCP 报文或一个 UDP 报文。

【教学重点和难点】路由算法，子网划分

【典型习题讲解】子网划分

第六学时： 网络层（续）

（一） 路由协议 自治系统（AS），Internet 路由选择协议分类（IGP 和 EGP）， 两种常用内部网关协议包括 RIP（基于 D-V 法）和 OSPF（基于 L-S 法），BGP 路由协议。

在动态路由中，管理员不再需要与静态配置那样对路由器上的路由表进行手工维护，而是在每台路由器上运行一个路由表的管理程序。这个路由表的管理程序会根据路由器上的接口的配置（如 IP 地址的配置）及所连接的链路的状态，生成路由表中的路由表项。这个路由表的管理程序也就是动态路由协议。采用动态路由协议管理路由表在大规模的网络中是十分有效的。

RIP（Routing Information Protocol）路由协议就是一种动态路由协议，它采用距离矢量算法，距离矢量算法就是相邻的路由器之间互相交换整个路由表，并进行矢量的叠加，最后达到知道整个网络路由。它通过 UDP 报文交换路由信息，每隔 30 秒向外发送一次更新报文。如果路由器经过 180 秒没有收到来自对端的路由更新报文，则将所有来自此路由器的路由信息标记为不可达，若在其后 120 秒内仍未收到更新报文，就将这些路由从路由表中删除。

RIP 使用跳数（Hop Count）来衡量到达目的地的距离，路由器到与它直接相连网络的跳数为 0，通过一个路由器可达的网络的跳数为 1，其余依此类推。为限制收敛时间，RIP 规定 metric 取值 0～15 之间的整数，大于或等于 16 的跳数被定义为无穷大，即目的网络或主机不可达。

每个运行 RIP 的路由器管理一个路由数据库，该路由数据库包含了到网络所有可达目的地的一个路由项，这个路由项包含下列信息：

目的地址：主机或网络的地址。

下一跳地址：为到达目的地，本路由器要经过的下一个路由器地址。

接口：转发报文的接口。

Metric 值：本路由器到达目的地的开销，可取值 0～16 之间的整数。

定时器：该路由项最后一次被修改的时间。

路由标记：区分该路由为内部路由协议路由还是外部路由协议路由的标记。

RIP 启动和运行的整个过程可描述如下：

某路由器刚启动 RIP 时，以广播形式向其相邻路由器发送请求报文，相邻路由器收到请求报文后，响应该请求，并回送包含本地路由信息的响应报文。

路由器收到响应报文后，修改本地路由表，同时向相邻路由器发送触发修改报文，广

播路由修改信息。相邻路由器收到触发修改报文后，又向其各自的相邻路由器发送触发修改报文。在多次的触发修改广播后，各路由器都能得到并保持最新的路由信息。

并且，RIP 每隔 30 秒向其相邻路由器广播本地路由表，相邻路由器在收到报文后，对本地路由进行维护，选择一条最佳路由，再向其各自相邻网络广播修改信息，使更新的路由最终能达到全局有效。同时，RIP 采用超时机制对过时的路由进行超时处理，以保证路由的实时性和有效性。

距离矢量协议无论是实现还是管理都比较简单，但是它的收敛速度慢，支持站点的数量有限，路由表更新信息将占用较大的网络带宽，并且会产生路由环路，为避免路由环路，RIP 应用水平分割（Split Horizon）、毒性逆转（Poison Reverse）技术，并采用触发更新（Triggered Update）机制。RIP 协议有 RIP-1 和 RIP-2 两个版本，RIP-2 支持明文认证和 MD5 密文认证，并支持变长子网掩码等。

距离矢量协议也称为 Bellman-Ford 协议,网络中路由器向相邻的路由器发送它们的全部路由信息。路由器根据从相邻路由器接收到的信息来更新自己的路由表。然后，将信息传递到它的相邻路由器。这样逐级的传递下去以达到全网同步。也就是说距离矢量路由表中的某些路由项有可能建立在第 2 手信息的基础之上的，每个路由器都不了解整个网络拓扑，它们只知道与自己直接相连的网络情况，并根据从邻居得到的路由信息更新自己的路由表，进行矢量行叠加后转发给其它的邻居。

距离矢量路由协议启动时会首先初始化路由表，路由器在路由表中生成其直连路由并传播出去，直连路由是指与其直接相连的网络的情况。然后，路由器会定期地把路由表传送给相邻的路由器，让其它路由器知道自己的网络情况。

每个路由器收到一条 RIP 选路信息后的计算过程如下。路由表每行至少包括三个字段：

（目的网络，跳数，下一跳路由器）

例如，（D，2，R）表示，到目的网络 D 的报文要送到相邻的路由器 R，跳数为 2 跳。

当收到相邻路由器 R 发来的一个跳数为 M，目的站为 D 的更新消息时，本机将其与现有的路由表比较：

如果：

1.本机中没有到 D 的路由存在，则生成路由表项（目的网络，跳数，下一跳路由器）：(D,M+1,R);

2.否则，如果存在（D, * ,R），则更新为 (D,M+1,R);

3.否则，如果存在到 D 的路由跳数大于 M＋1,则更新为（D，M+1,R）;

4.否则，不更新。

在经过了若干个更新周期后，路由信息会被传递到每台路由器上，达到平衡。

OSPF 工作原理分析

OSPF 是一种分层次的路由协议，其层次中最大的实体是 AS（自治系统），即遵循共同路由策略管理下的一部分网络实体。在每个 AS 中，将网络划分为不同的区域。每个区域都有自己特定的标识号。对于主干（backbone）区域，负责在区域之间分发链路状态信息。这种分层次的网络结构是根据 OSPF 的实际提出来的。当网络中自治系统非常大时，网络拓扑数据库的内容就更多，所以如果不分层次的话，一方面容易造成数据库溢出，另一方面当网络中某一链路状态发生变化时，会引起整个网络中每个节点都重新计算一遍自己的路由表，既浪费资源与时间，又会影响路由协议的性能（如聚合速度、稳定性、灵活性等）。因此，需要把自治系统划分为多个域，每个域内部维持本域一张唯一的拓扑结构图，且各域根据自己的拓扑图各自计算路由，域边界路由器把各个域的内部路由总结后在域间扩散。这样，当网络中的某条链路状态发生变化时，此链路所在的域中的每个路由器重新计算本域路由表，而其它域中路由器只需修改其路由表中的相应条目而无须重新计算整个路由表，

节省了计算路由表的时间。

OSPF 由两个互相关联的主要部分组成：“呼叫”协议和“可靠泛洪”机制。呼叫协议检测邻居并维护邻接关系，可靠泛洪算法可以确保统一域中的所有的 OSPF 路由器始终具有一致的链路状态数据库，而该数据库构成了对域的网络拓扑和链路状态的映射。链路状态数据库中每个条目称为 LSA（链路状态通告），共有 5 种不同类型的 LSA，路由器间交换信息时就是交换这些 LSA.每个路由器都维护一个用于跟踪网络链路状态的数据库，然后各路由器的路由选择就是基于链路状态，通过 Dijkastra 算法建立起来最短路径树，用该树跟踪系统中的每个目标的最短路径。最后再通过计算域间路由、自治系统外部路由确定完整的路由表。与此同时，OSPF 动态监视网络状态，一旦发生变化则迅速扩散达到对网络拓扑的快速聚合，从而确定出新的网络路由表。

OSPF 的设计实现要涉及到指定路由器、备份指定路由器的选举、协议包的接收、发送、泛洪机制、路由表计算等一系列问题。

Dijkstra 算法的描述如下：

（1）初始化集合 E，使之只包含源节点 S，并初始化集合 R，使之包含所有其它节点。初始化路径列 O,使其包含一段从 S 起始的路径。这些路径的长度值等于相应链路的量度值，并以递增顺序排列列表 O.

（2）若列表 O 为空，或者 O 中第 1 个路径长度为无穷大，则将 R 中所有剩余节点标注为不可达，并终止算法。

（3）首先寻找列表 O 中的最短路径 P，从 O 中删除 P.设 V 为 P 的最终节点。若 V 已在集合 E 中，继续执行步骤 2.否则，P 为通往 V 的最短路径。将 V 从 R 移至 E.

（4）建立一个与 P 相连并从 V 开始的所有链路构成的侯选路径集合。这些路径的长度是 P 的长度加上与 P 相连的长度。将这些新的链路插入有序表 O 中，并放置在其长度所对应的等级上。继续执行步骤 2.

Dijkstra 算法举例：

下面我们以路由器 A 为例，来说明最短路径树的建立过程：

（1）路由器 A 找到了路由器 B、C，将它们列入候选列表{B：1；C：2}.

（2）从候选列表中找出最小代价项 B，将 B 加入最短路径树并从候选列表中删除。接着从 B 开始寻找，找到了 D，将其放入候选列表{C：2；D：2}.

（3）从列表中找出 C，再由 C 又找到了 D.但此时 D 的代价为 4，所以不再加入候选列表。最后将 D 加入到最短路径树。此时候选列表为空，完成了最短路径树的计算。

OSPF 路由表的计算与实现

有关路由表的计算是 OSPF 的核心内容，它是动态生成路由器内核路由表的基础。在路由表条目中，应包括有目标地址、目标地址类型、链路的代价、链路的存活时间、链路的类型以及下一跳等内容。关于整个计算的过程，主要由以下五个步骤来完成：

（1）保存当前路由表，当前存在的路由表为无效的，必须从头开始重新建立路由表；

（2）域内路由的计算，通过 Dijkstra 算法建立最短路径树，从而计算域内路由；

（3）域间路由的计算，通过检查 Summary-LSA 来计算域间路由，若该路由器连到多个域，则只检查主干域的 Summary-LSA；

（4）查看 Summary-LSA：在连到一个或多个传输域的域边界路由器中，通过检查该域内的 Summary-LSA 来检查是否有比第（2）（3）步更好的路径；

（5）AS 外部路由的计算，通过查看 AS-External-LSA 来计算目的地在 AS 外的路由。

通过以上步骤，OSPF 生成了路由表。但这里的路由表还不同于路由器中实现路由转发功能时用到的内核路由表，它只是 OSPF 本身的内部路由表。因此，完成上述工作后，往往还要通过路由增强功能与内核路由表交互，从而实现多种路由协议的学习。

（二） IP 组播 组播的概念，地址 ，路由算法，组播协议主要包括组管理协议（IGMP)和组播路由协议。组播路由协议可分为三类：密集模式协议（如 DVMRP，PIM-DM)、稀疏模式协议（如 PIM-SM，CBT）和链路状态协议（MOSPF)。主要介绍 PIM-DM 和 PIM-SM 协议。组播树的建立，加入和退出组播的过程。

（三） 移动 IP 移动 IP 的概念 ，通信过程

（四） 网络层设备 路由器的组成和功能 ，路由表与路由转发

【教学重点和难点】RIP，OSPF 路由协议，组播和移动 IP 的概念
【典型习题讲解】OSPF 路由协议

第七学时： 传输层

（一） 传输层提供的服务 传输层的作用，是通信子网与资源子网的桥梁，设置目的是在源、目主机的进程间提供可靠的端对端通信，分析传输层与数据链路层的异同点，网络服务质量类型（三类：A 型、B 型和 C 型)。传输层的功能，寻址与端口，无连接服务与面向连接服务。

（二） UDP 协议 UDP 数据报，校验，主要特点为，发送数据之前不需要建立连接，UDP 的主机不需要维持复杂的连接状态表，UDP 用户数据报只有 8 个字节的首部开销，网络出现的拥塞不会使源主机的发送速率降低。对实时应用很重要。

用户数据报协议是对 IP 协议组的扩充，它增加了一种机制，发送方使用这种机制可以区分一台计算机上的多个接收者。每个 UDP 报文除了包含某用户进程发送数据外，还有报文目的端口的编号和报文源端口的编号，从而使 UDP 的这种扩充，使得在两个用户进程之间的递送数据报成为可能。

UDP 是依靠 IP 协议来传送报文的，因而它的服务和 IP 一样是不可靠的。这种服务不用确认、不对报文排序、也不进行流量控制，UDP 报文右能会出现丢失、重复、失序等现象。

（三） TCP 协议 TCP 段 ，连接管理，即 TCP 连接建立与释放（三次握手)，可靠传输 ，流量控制与拥塞控制，包括可变发送窗口协议等。TCP 采用大小可变的滑动窗口进行流量控制。窗口大小的单位是字节，在 TCP 报文段首部的窗口字段写入的数值就是当前给对方设置的发送窗口数值的上限。发送窗口在连接建立时由双方商定。但在通信的过程中，接收端可根据自己的资源情况，随时动态地调整对方的发送窗口上限值(可增大或减小)。

TCP 提供的是一种可靠的数据流服务。当传送受差错干扰的数据，或基础网络故障，或网络负荷太重而使网际基本传输系统(无连接报文递交系统)不能正常工作时，就需要通过其它协议来保证通信的可靠。TCP 就是这样的协议，它对应于 OSI 模型的运输层，它在 IP 协议的基础上，提供端到端的面向连接的可靠传输。

TCP 采用“带重传的肯定确认”技术来实现传输的可靠性。简单的“带重传的肯定确认”是指与发送方通信的接收者，每接收一次数据，就送回一个确认报文，发送者对每个发出去的报文都留一份记录，等到收到确认之后再发出下一报文分组。发送者发出一个报文分组时，启动一个计时器，若计时器计数完毕，确认还未到达，则发送者重新送该报文分组。

简单的确认重传严重浪费带宽，TCP 还采用一种称之为“滑动窗口”的流量控制机制来提高网络的吞吐量，窗口的范围决定了发送方发送的但未被接收方确认的数据报的数量。每当接收方正确收到一则报文时，窗口便向前滑动，这种机制使网络中未被确认的数据报数量增加，提高了网络的吞吐量。

TCP 通信建立在面向连接的基础上，实现了一种“虚电路”的概念。双方通信之前，先建立一条连接，然后双方就可以在其上发送数据流。这种数据交换方式能提高效率，但事先建立连接和事后拆除连接需要开销。TCP 连接的建立采用三次握手的过程，整个过程由发送方请求连接、接收方再发送一则关于确认的确认三个过程组成。

TCP 的拥塞控制和流量控制是一个比较复杂的问题，它包括发送端发送报文的大小和报文的时机，接收端发送确认和窗口大小的策略。同时还要兼顾不同网络的具体情况，算法要具有一定的自适应性，在保证可靠传输的同时，尽量提高传输效率。

这里主要对目前公认的比较行之有效的一些拥塞控制和流量控制算法进行介绍和验证。主要有：TCP 的滑动窗口机制、TCP 的糊涂窗口综合症和 Nagle 算法分析、网络拥塞的处理、TCP 的超时与重传、TCP 的窗口探查技术、TCP 的快重传和快恢复。

TCP 的滑动窗口机制

为了提高报文段的传输速率，TCP 采用大小可变的滑动窗口进行流量控制。窗口大小的单位是字节。发送窗口在连接建立时由双方商定，但在通信过程中，接收端可根据自己的接收缓存的大小，随时动态地调整发送端的发送窗口的上限值。这就是接收端窗口 rwnd（receiver window），这个值被放在接收端发送的 TCP 报文段首部的窗口字段中。

同时，发送端根据其对当前网络拥塞程度的估计而确定的窗口值，叫做拥塞窗口 cwnd（congestion window）。其大小与网络的带宽和时延密切相关。

发送端设置的当前能够发送数据量的大小叫做发送窗口，发送窗口的上限值由下面公式确定：

发送窗口的上限值＝Min[cwnd,rwnd]

rwnd 由接收端根据其接收缓存确定，发送端确定 cwnd 比较复杂，详细情况在慢启动和拥塞避免一节中叙述。

发送窗口的左边沿对应已发送数据中被确认的最高序号＋1，其右边沿对应左边沿的序号加上发送窗口的大小。在数据传输的过程中，这个发送窗口不时地向右移动构成了滑动窗口。窗口的两个边沿的相对运动增加或减少了窗口的大小。我们使用三个术语来描述窗口左右边沿的运动：

（1）当窗口左边沿向右边沿靠近时，我们称之为窗口合拢。这种现象发生在数据被发送和确认时。如果窗口的左边沿与右边沿重合，则称其为一个零窗口，此时发送方不能发送任何数据。

（2）当窗口右边沿向右移动时将允许发送更多的数据，我们称之为窗口张开。这种现象发生在另一端的接收进程读取已经确认的数据并释放了 TCP 的接收缓存时。

（3）当右边沿向左移动时，我们称之为窗口收缩。这种情况一般不会发生，但是 TCP 必须能够在某一端产生这种情况时进行处理。

TCP 的糊涂窗口综合症和 Nagle 算法

TCP 的流量控制方案是基于窗口的，有可能会出现一种被称为“糊涂窗口综合症”的状况。其中一种情况是，如果接受方处理较慢，并且每次从其接收缓存取走很少量数据就通告这个很小的窗口，而不是等到有较大的窗口时才通告；发送方得到这个很小的接收窗口后，立即按照这个窗口大小组成一个 TCP 报文段发送出去，而不是等待其它的数据以便发送一个大的报文段。如此往复，会导致网络的传输效率降低。

对于糊涂窗口综合症的现象，发送和接收双方均可以采取措施加以避免。

发送端比较有效的方法是采用 Nagle 算法。该算法主要是：在连接建立开始发送数据时，立即按序发送缓存中的数据（必须小于或等于 MSS），在已经传输的数据还未被确认的情况下，后续数据的发送由数据是否足以填满发送缓存的一半或一个最大报文段长度决定。

接收端采用推迟确认技术，对收到的报文段进行确认和通告窗口的前提条件是：接收缓存的可用空间至少得到总空间的一半或者达到最大报文长度之后。如果条件不满足，则推迟发送确认和窗口通告。

总之，避免糊涂窗口综合症的总的原则是：接收端避免通告小窗口，发送端尽量将数据组成较大的报文段发送出去。

TCP 的慢启动和拥塞避免

为了保证网络平稳高效的运行，防止网络流量的剧烈起伏震荡。1999 年公布的因特网建议标准[RFC2581]提出了慢启动（slow-start）和拥塞避免算法（congestion avoidance）。

慢启动算法的原理是：在主机开始发送数据时，采用试探的方式，由小到大逐渐增大发送端的拥塞窗口数值。通常是在一开始 cwnd 应设置为不超过 2×MSS（最大报文段）个字节，在每收到一个对新的报文段的确认后，拥塞窗口至多增加 1 个 MSS 的数值。使分组注入到网络的速率比较合理。

拥塞避免算法是使发送端的拥塞窗口 cwnd 每经过一个 RTT 就增加一个 MSS 的大小（而不管在时间 RTT 内收到了几个 ACK）。

慢启动与拥塞避免算法相比较，拥塞窗口增加的方式分别是指数方式和线性方式。慢启动算法使发送端在发送数据的开始阶段逐步增加注入网络的分组数，但随着拥塞窗口按指数方式快速增长，势必会引起网络拥塞。需要在网络拥塞之前，将拥塞窗口的增长速率降下来，也就是将慢启动算法切换到拥塞避免算法。因此，需要设置一个慢启动门限变量 ssthresh，利用 ssthresh 得到慢启动和拥塞避免的综合算法：

当 cwnd<ssthresh 时，使用慢启动算法；

当 cwnd>ssthresh 时，使用拥塞避免算法；

当 cwnd=ssthresh 时，既可以使用慢启动算法，也可以使用拥塞避免算法。

网络拥塞的处理

网络拥塞是指发送端没有按时收到确认报文或者收到了重复的确认报文。

在任何时候，只要发送端发现网络拥塞，根据没有得到确认的已发送数据量 FlightSize，给出如下公式设置慢启动门限值：ssthresh≤max（FlightSize/2，2×MSS）。

以及设置拥塞窗口：cwnd＝1。

然后，重新执行上一节所述的慢启动和拥塞避免的综合算法。

这样，能够迅速地减少主机发送到网络中的分组数，使得发生拥塞的主机或者路由器有时间把队列中的积压分组处理完毕。

TCP 的超时与重传

超时与重传机制是 TCP 中最主要和最复杂的技术之一。发送端在每发送一个报文段，TCP 为其保留一个复本、设定一个定时器并等待确认信息。如果定时器超时，而发送的报文段中的数据仍未得到确认，则重传这一报文段。因此可见，定时器重传数据的确定是关键。

针对网络环境的复杂性，TCP 采用了一种自适应算法，提出超时重传时间应略大于平均往返时延 RTT，而 RTT 是根据各个报文段的往返时延样本的加权平均得出的。如何比较精确的估计 RTT 的值，Karn 算法是目前公认的效果较好的算法。

Karn 算法提出在计算平均往返时延 RTT 时，不计算发生过报文段重传的往返时延样本；同时报文段每重传一次，相应增大重传时间：

新的重传时间＝γ×（旧的重传时间）

其中，系数γ的典型值是 2。并且，当不再发生报文段重传时，才根据报文段的往返时

延更新 RTT 和重传时间的数值。

这样得出的平均往返时延 RTT 和重传时间就比较准确，并且实践证明，该方法比较合理和有效。

TCP 的窗口探查技术

当接收端的接收缓存已满，不能继续接收数据，需要向发送端发送一个窗口为 0 的通告报文。发送端接收到这个报文后，停止发送数据，等待新的窗口通告。如果接收端通过确认报文通告窗口，TCP 协议并不对这个确认报文进行确认，如果这个确认丢失了，则双方就有可能因为等待对方而使连接中止：接受方等待接收数据（因为它已经向发送方通告了一个非 0 的窗口），而发送方在等待允许它继续发送数据的窗口更新。为防止这种死锁情况的发生，发送方使用一个坚持定时器（persist timer）来周期性地向接受方查询，以便发现窗口是否已增大。这些从发送方发出的报文段称为窗口探查（window probe），窗口探查是包含一个字节的数据的报文段。

TCP 的快重传和快恢复

为了避免 TCP 因等待重传定时器超时而空闲较长时间，又提出了两个新的拥塞控制算法：快重传和快恢复。

快重传算法是指当发送端连续收到三个重复的 ACK 报文时，即可认为某一报文段丢失并且网络仍能够进行正常报文传输。因此，不必等待那个报文的定时器超时，而直接重传那个认为是丢失的报文段。即在某些情况下更早地重传被估计为丢失的报文段。

快恢复算法是慢启动算法的一个补充，它与快重传算法配合使用。具体步骤如下：

（1） 当发送端收到连续 n（n≥3）个重复的 ACK，设置慢启动门限值：

$$ssthresh \leq \max(FlightSize/2, 2\times MSS)$$

同时，将 cwnd 设置为 ssthress+n×MSS。

（2） 如果发送窗口值还容许发送报文段，就按拥塞避免算法继续发送报文段。

（3） 若收到了确认新的报文段的 ACK，就将 cwnd 缩小到 ssthress。

在采用快恢复算法时，慢启动算法只在 TCP 连接建立时才使用

【教学重点和难点】无连接服务与面向连接服务，流量控制与拥塞控制
【典型习题讲解】UDP 和 TCP 的区别，TCP 流量控制

第八学时： 应用层

【知识点】

（一） 网络应用模型 包括客户/服务器模型 和 . P2P 模型

（二） DNS 系统 层次域名空间，域名服务器 ，域名解析过程，采用层次结构的命名树作为主机的名字，并使用分布式的域名系统 DNS。名字到域名的解析是由若干个域名服务器程序完成的。域名服务器程序在专设的结点上运行，即域名服务器。

DNS 查询分为两类：递归查询和迭代查询。进行递归查询时，DNS 客户机向 DNS 服务器发送请求，即使 DNS 服务器没有所请求的信息，则会联系其他 DNS 服务器来提供答案或返回查询失败信息。进行迭代查询时，DNS 允许 DNS 服务器根据自己的高速缓存提供最佳答案，如果不能答复，则一般会返回一个指针，指向有下级域名空间授权的 DNS 服务器，DNS 客户机根据指针所指向的 DNS 服务器查询。

（三） FTP FTP 协议的工作原理， 控制连接与数据连接，FTP 使用客户服务器方式。一

个 FTP 服务器进程可同时为多个客户进程提供服务。FTP 的服务器进程由两大部分组成：一个主进程，负责接受新的请求；另外有若干个从属进程，负责处理单个请求。

FTP 协议是文件传输协议（File Transfer Protocol）的简称，它采用两个 TCP 连接来传输一个文件，它们是控制连接和数据连接。

1) 控制连接以通常的客户服务器方式建立。服务器以被动方式打开用于 FTP 的端口（21），等待客户的连接。客户则以主动方式打开 TCP 端口 21，来建立连接。控制连接始终等待客户与服务器之间的通信。该连接将命令从客户传给服务器，并传回服务器的应答。由于命令通常是由用户键入的，所以 IP 对控制连接的服务主要责任就是“最大限度地减小迟延”。

2) 每当一个文件在客户与服务器之间传输时，就创建一个数据连接。由于该连接用于数据传输目的，所以 IP 对数据连接的服务特点就是“最大限度提高吞吐量”。

（四） 电子邮件 电子邮件系统的组成结构，电子邮件格式与 MIME ，SMTP 协议与 POP3 协议，SMTP 包括连接建立，主要在在发送主机的 SMTP 客户和接收主机的 SMTP 服务器之间建立的。邮件传送过程以及连接释放，也就是邮件发送完毕后，SMTP 应释放 TCP 连接。

电子邮件的发送和接收过程为：

（1）发信人调用用户代理来编辑要发送的邮件，用户代理用 SMTP 将邮件传送给发送端邮件服务器。

（2）发送端邮件服务器将邮件放入邮件缓存队列中，等待发送。

（3）运行在发送端邮件服务器的 SMTP 客户进程，发现在邮件缓存中有待发送的邮件，就向运行在接收端邮件服务器的 SMTP 服务器进程发起 TCP 连接建立。当 TCP 连接建立后，SMTP 客户进程开始向远程的 SMTP 服务器发送邮件。如果有多个邮件在邮件缓存中，则 SMTP 客户一一将它们发送到远程的 SMTP 服务器。当所有的待发邮件发完了，SMTP 就关闭所建立的 TCP 连接。

（4）运行在接收端邮件服务器中的 SMTP 服务器进程收到邮件后，将邮件放入收信人的用户邮箱中，等待收信人在他方便时进行读取。收信人在打算收信时，调用用户代理，使用 POP 协议将自己的邮件从接受端邮件服务器的用户邮箱中取回（如果邮箱中有来信的话）。

SMTP 不使用中间邮件服务器。由于 SMTP 只能传送可打印的 7 位 ASCII 码邮件，因此在 1993 年又提出了通用因特网邮件扩充 MIME（Multipurpose Internet Mail Extensions）。MIME 并没有改动 SMTP 或取代它。MIME 的意图是继续使用目前的[RFC 822]格式，但增加了邮件主体的结构，并定义了传送非 ASCII 码的编码规则。

（五） WWW WWW 的概念与组成结构，即 WWW 以客户服务器方式工作。浏览器就是在用户计算机上的 WWW 客户程序。WWW 文档所驻留的计算机则运行服务器程序，也称为 WWW 服务器。客户程序向服务器程序发出请求，服务器程序向客户程序送回客户所要的 WWW 文档。在一个客户程序主窗口上显示出的万 WWW 文档称为页面(page)。HTTP 协议是一个应用层协议，它使用 TCP 连接进行可靠的传送。HTTP 是面向事务的(transaction-oriented)应用层协议，它是万维网上能够可靠地交换文件（包括文本、声音、图像等各种多媒体文件）的重要基础。

【教学重点和难点】DNS 过程，SMTP 协议与 POP3 协议, HTTP 协议

【典型习题讲解】客户/服务器模型和 DNS 过程