

第一章 计算机网络概述

[选择] 计算机网络是计算机技术和通信技术相结合的产物。这种结合开始于 **20 世纪 50 年代**。

[选择] 计算机网络中 PSE(分组交换设备)属于网络系统的 **通信子网**。

[选择] 通信子网主要由网络节点和通信链路组成。网络节点也成为转接节点或中间节点，下面属于转接节点的是 **集中器**。

[选择] 中心节点是控制中心，任意两个节点间的通信最多只需两步，但这种网络系统，网络可靠性低，网络共享能力差，并且一旦中心节点出现故障则导致全网瘫痪。这种网络拓扑结构是 **星形结构**。

[选择] 现代计算机网络系统的基础是 **分组交换技术**。

[选择] 主机 HOST 属于计算机网络系统中的 **资源子网**。

[选择] 计算机网络是由通信子网和资源子网组成，下列设备中属于通信子网的是 **集中器**。

[选择] 现代计算机网络最为重要的功能是 **资源共享**。

[选择] 星形、总线形、环形和网形结构式按照 **网络拓扑结构** 分类。

[选择] 下列网络拓扑结构中，通信子网不能采用点一点线路的是 **总线形**。

[选择] 下列对于星形拓扑结构的描述中，不正确的是 **不容易进行故障和诊断**。

[选择] 下列叙述中，哪一个不是总线型拓扑结构的优点 **故障诊断和隔离容易**。

[选择] 按覆盖的地理范围进行分类，计算机网络可以分为三类是 **局域网、广域网与城域网**。

[填空] 在网络节点中，FEP 是负责与终端 T 之间的通信控制的设备。

[填空] 在计算机网络的四个发展阶段中，第一阶段的计算机网络是 **面向终端** 的计算机。

[填空] 面向终端的计算机网络发展阶段，在终端较集中的地区是通过 **低速** 线路将其连至集中器或多路复用器，然后通过 **高速通信** 线路、调制解调器与远程中心计算机相连。

[填空] 计算机网络的雏形是 **终端—通信线路—计算机系统**。

[填空] 当前，三大网络是指 **电信业务网、广播电视网、及 计算机网**。

[填空] 电信业一般认为传输速率达到 **2Gbps** 的骨干网乘坐宽带网。

[填空] 接入网技术可根据使用的传输介质的不同分为 **光纤接入、铜线接入、光纤同轴电缆混合接入** 和 **无线接入** 等。

[填空] WAP 是指 **无线应用协议**。

[填空] 计算机网络的功能主要表现在三方面，它们是 **硬件资源共享、软件资源共享和 用户间信息交换**。

[填空] 计算机网络按交换方式分为电路交换网、**报文交换** 和 **分组交换**。

[填空] 覆盖一个国家或几个洲的计算机网络称为 **广域网 WAN**；在同一建筑或覆盖几公里内范围的网成为 **局域网 LAN**；而分布范围介于两者之间的是 **城域网 MAN**。

[填空] 点对点式网与广播式网络的重要区别是路由选择机制和 **分组存储转发**。

[简答] 简述计算机网络发展的四个阶段及其特点。

计算机网络发展的四个阶段是：**面向终端的计算机网络、计算机—计算机网络、开放式标准化网络、因特网广泛应用与高速网络技术的发展。**

面向终端的计算机网络阶段：以单个计算机为中心的远程联机系统。**中心计算机**进行信息的集中处理，其余各终端设备都没有自主处理能力。

计算机—计算机网络阶段：计算机与计算机之间的直接通信，并呈现出多处理中心的特点。

开放式标准化网络阶段：不同体系结构的产品能容易互连。

因特网的广泛应用与高速网络技术的发展阶段：用户可以利用 **Internet** 实现全球范围的电子邮件、WWW 信息查询与浏览、电子新闻、文件传输、语音与图像通信服务功能。随着 **Internet** 飞速发展与广泛应用的同时，高速网络技术发展表现在宽带综合业务数字网 **B-ISDN**、异步传输模式 **ATM**、高速局域网、交换局域网与虚拟网络。

[简答] 计算机网络的定义是什么？

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、信息交换方式和网络操作系统等) 实现网络中资源共享和信息传递的系统。

[简答] 简述计算机网络的功能。

计算机网络的功能主要表现在硬件资源共享、软件资源共享和用户间信息交换三个方面。

(1) 硬件资源共享。可以在全网范围内提供对处理资源、存储资源、输入输出资源等昂贵设备的共享，使用户节省投资，也便于集中管理和均衡分担负荷。

(2) 软件资源共享。允许互联网上的用户远程访问各类大型数据库，可以得到网络文件传送服务、远程管理服务和远程文件访问服务，从而避免软件研制上的重复劳动以及数据资源的重复存贮，也便于集中管理。

(3) 用户间信息交换。计算机网络为分布在各地的用户提供了强有力的通信手段。用户可以通过计算机网络传送电子邮件、发布新闻消息和进行电子商务活动。

[简答] 简述总线形星形环形网络拓扑的优缺点。

总线形拓扑结构具有以下优点：

- (1) 所需电缆数量较少。
- (2) 结构简单，无源工作有较高可靠性。
- (3) 易于扩充。

总线拓扑结构的缺点：

- (1) 总线传输距离有限，通信范围受到限制。
- (2) 故障诊断和隔离比较困难。
- (3) 分布式协议不能保证信息的及时传送，不具实时功能，站点必须有介质访问控制功能，从而增加了站点的硬件和软件开销。

星形拓扑结构的优点：

- (1) 控制简单。
- (2) 故障诊断和隔离容易。
- (3) 方便服务。

星形拓扑结构的缺点是：

- (1) 需要耗费大量的电缆，安装、维护的工作量也骤增。
- (2) 中央节点负担重，形成“瓶颈”，一旦发生故障，则全网受影响。
- (3) 各站点的分布处理能力较低。

环形拓扑结构的优点：

- (1) 电缆长度短，只需要将各节点逐次相连。
- (2) 可使用光纤。光纤的传输速率很高，十分适合于环形拓扑的单方面传输。
- (3) 所有站点都能公平访问网络的其他部分，网络性能稳定。

环形拓扑结构的缺点：

- (1) 节点故障会引起全网故障，是因为数据传输需要通过环上的每一个节点，如某一节点故障，则引起全网故障。
- (2) 节点的加入和撤出过程复杂。
- (3) 介质访问控制协议采用令牌传递的方式，在负载很轻时信道利用率相对较低。

网络拓扑结构的优点是不受瓶颈问题和失效问题的影响，可靠性高。缺点是结构复杂、协议复杂，成本较高。

[应用] 远程联机系统中为什么需要调制解调器？

因为在远程联机系统中的计算机与远程终端的通信当时只能利用公用电话系统，而利用电话线传输计算机与远程终端发出的信号，就必须经过数据转换。由于计算机和远程终端发出的信号都是数字信号，而公用电话系统的传输系统只能传输模拟信号。利用调制解调器就是为实现两种信号的转换。

调制解调器的作用是：在通信前，先把从计算机或远程终端发出的数字信号转换成可以在电话线上传

送的模拟信号，通信后再将被转换的信号进行复原。

第2章 计算机网络体系结构

[选择]在组成网络协议的三要素中，数据与控制信息的机构与格式是指 语法 。

[选择]在 OSI 参考模型中，实现数据格式转换功能应在 表示层 。

[选择]OSI 模型的最底层是 物理层 。

[选择]IP 协议位于 TCP/IP 模型的 互连层 。

[选择]网络协议三要素中的定时是 速度匹配和排序 。

[选择]下面关于网络分层体系结构描述正确的是 不同层的实体之间可以通过相应的协议进行通信 。

[选择]通信子网不包括 传输层 。

[选择]在 OSI 七层模型中，实现网络的安全和保密、数据压缩等功能的协议层是 表示层 。

[选择]OSI 七层模型中，实现端到端的透明数据传输服务的系一层是 传输层 。

[选择]完成路由选择功能是在 OSI 参考模型的 网络层 。

[选择]两端用户传输文件，是由下列 OSI 参考模型中的哪一层处理 应用层 。

[选择]TCP/IP 层次模型中，下列哪一层是 TCP/IP 的实现基础 主机—网络层 。

[填空]网络分层结构中， n 层是 n+1 层的服务提供者，同时是 n-1 层的用户。

[填空]计算机网络系统需要解决许多复杂的问题，所采用的解决方法是 分层 。

[填空]网络协议的三个要素是 语义、语法 和定时。

[填空]网络体系结构是网络各层及其 协议 的集合。

[填空]网络层次模型中对等实体间进行的都是需通信，而且遵循该层的 协议 。

[填空]继世界上第一个网络体系结构提出后，许多公司纷纷提出各自的网络体系结构，这些网络体系结构共同之处是都采用了 分层技术 。

[填空]OSI 参考模型将网络划分为 七层 。

[填空]层次结构模型中，数据经过发送方从上到下逐层传递的过程中，每层都要加上适当的控制信息，这样的控制信息称为 报头 。

[填空]层次结构模型中，数据在发送方各层从上到下逐层传递，到达最底层数据成为由 0 和 1 组成的 比特流，然后再转换为 电信号 在物理介质上传输到接收方。

[填空]通信服务类型有两类，分别是： 面向连接服务 、 无连接服务 。

[填空]面向连接服务的数据传输过程要经过 3 个过程，它们是 建立接连 、 维护连接 和 释放连接 。

[填空]网络数据传输可靠性一般通过 确认 和 重传 机制保证。

[填空]TCP/IP 协议簇中， TCP 提供 传输层 服务； IP 提供 网络层 服务。

[填空]TCP/IP 体系结构的传输层包含两个独立的协议 TCP 和 IP 。

[简答]协议与服务有何区别？又有何关系？

服务是由下层向上层通过层间接口提供的，上层的实体通过服务原语来使用其下层所提供的服务。上层是服务的用户，下层是服务的提供者。

协议是定义同层对等实体之间进行数据交换的规则、标准或约定，利用协议来实现它们的服务定义。

本层的服务用户只能看见服务，而无法看见下面的协议，下层的协议对上层的服务用户是透明的，因此，只要不改变本层提供给服务用户的服务，高层实体可以任意地改变它们的协议。

服务式垂直的，协议是水平的。

[简答]计算机网络采用分层结构的理由是什么？它的好处是什么？层次结构的划分要遵循的主要原则是什么？

及三级网络系统是一个十分复杂的系统。将一个复杂系统分解为若干个容易处理的子系统，然后“分而治之”逐个加以解决，这种结构化设计方法是工程设计中常用的手段。分层式系统分解的最好方法之一。

分层结构的优点在于：

(1)每一层实现一种相对独立的功能。每一层不必知道下面一层是如何实现的，只要知道下层通过层间接口提供的服务是什么及本层向上层提供什么样的服务。

(2)系统经分层后，每一层次的功能相对简单且易于实现和维护。

(3)若某一层需要作改动或被代替时，只要层间接口不发生变化，则其他层次都不会受其影响，因此有很大的灵活性。

(4)易于交流、理解和标准化。

分层的原则：

(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，便不会对邻层产生影响。

(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，则多种功能混杂在一层中，造成每一层的协议太复杂；若层数太多，则体系接口过于复杂，使描述和实现各层功能变得困难。

[简答]简述面向连接服务和无连接服务的特点。

面向连接服务的主要特点有：

(1)数据传输过程前必须经过建立连接、维护连接和释放连接三个过程。

(2)在数据传输过程中，个分组不需要携带目的节点的地址。

(3)面向连接服务可确保数据传送的次序和传输的可靠性，但需通信开始前的连接开销，协议复杂，通信效率不高。

无连接服务的特点是：每个分组都要携带完整的目的节点的地址，各分组在通信子网中是独立传送的。不需要建立连接、维护连接和释放连接三个过程，节省连接开销和许多保证机制，通信协议相对简单，效率较高；不同分组可能选择不同路径到达目的节点，先发送不一定先到达，可能会出现乱序、重复与丢失的现象，稳定性不好。

[简答]TCP/IP 协议的主要特点是什么？其主要缺点是什么？

TCP/IP 协议的主要特点：

(1)开放的协议标准，可以免费试用，并且独立于特定的计算机硬件与操纵系统；

(2)独立于特定的网络硬件，可以运行在局域网、广域网，更适用于互联网中；

(3)统一的网络地址分配方案，使得整个 TCP/IP 设备在网中都具有惟一的地址；

(4)标准化的高层协议，可以提供多种可靠的用户服务。

TCP/IP 模型的主要缺点有：首先，该模型没有清楚的区分哪些是模范、哪些是实现；其次，TCP/IP 模型的主机—网络层定义了网络层与数据链路层的接口，并不是常规意义上的一层，接口和层的区别是非常重要的，TCP/IP 模型没有将它们区分开来。

[应用]为什么网络体系结构需要标准化？

计算机网络系统是非常复杂的系统，计算机之间互相通信涉及到许多复杂的技术问题，为实现计算机网络通信，实现网络资源共享，计算机网络采用的是对解决复杂问题的十分有效的分层解决问题的方法。

但由于网络系统体系结构各不相同，对各种体系接口来说，同一体系结构的网络产品互联是很容易实现的，而不同体系结构的产品却很难实现互连。由于社会的发展迫切要求不同体系结构的产品都能够很容易地得到互连，人们迫切希望建立一系列的国际标准，以得到一个“开放”的系统，所以网络体系结构需要标准化。

[应用]试比较 OSI/RM 和 TCP/IP 模型的异同点。

相同：都以协议栈的概念为基础，协议栈中的协议彼此相互独立；都采用了层次结构的概念，各层的功能也大体相似。

不同：层的数量不同；OSI 模型有七层，而 TCP/IP 只有四层，它们都有网络层（或者简称互连网层）、传输层和应用层，但其他的层并不相同；OSI 模型的网络层同时支持无连接和面向连接的通信，但是传输

层上只支持面向连接的通信； TCP/IP 模型的网络只提供无连接的服务，但在传输层上同时支持两种通信模式。

第3章 物理层

[选择] RS-232C 接口标准属于 物理层。

[选择] OSI 模型中提供透明位流传输的是 物理层。

[选择] 双绞线交合的目的是 减少干扰。

[选择] 以下描述不正确的是 基带同轴电缆主要用于模拟传输系统。

[选择] 曼彻斯特的编码采用 自同步法 实现同步。

[选择] 报文交换方式是数据交换方式之一，则以下描述正确的是 这种方式对同等通信容量而言，效率比电路交换方式高。

[选择] 数据通信系统中，调制解调器属于 数据电路终接设备 DCE。

[选择] 物理层协议有四个方面的特性。其中，通信介质的电气连接及有关电路特性方面的内容属于 电气特性。

[选择] 电话通信中最常用的传输介质是 双绞线。

[选择] 电缆中使用屏蔽层的目的是为了减少 辐射电磁干扰。

[选择] 下列传输介质中， 光纤 的带宽最宽，数据传输率高，抗干扰能力最强。

[选择] 通信子网的组成主要包括 网络节点和通信链路。

[选择] 数据传输速率公式： $R = \frac{1}{T} \bullet \log_2 N$ 中，T 的含义是 单位脉冲信号宽度。

[选择] 如果一个码元可以表示 8 种离散状态，则数据传输速率是其调制速率的 3 倍。

[选择] 信号传输率为 1200Baud，每个码元可取 4 种离散状态，该信号的数据传输率是 2400bps。

[选择] 并行传输与串行传输相比 速度快、费用高。

[选择] 采用全双工通信方式，数据传输的方向形结构为 可以在两个方向上同时传输。

[选择] 外同步法中，接收端的同步信号是由 发送端送来的。

[选择] 异步时分多路复用 TDM 技术中的时间片分配策略是 动态分配随时可变。

[选择] 就同步方式而言，异步传输属 群同步。

[选择] 采用脉码调制方法对模拟信号进行编码，每次采样使用 256 个量化级进行量化，若数据传输速率为 64Kbps，那么每秒钟采样的次数是 8000 次。

[选择] 目前，国际性的标准约定调制解调器的产品速率是 56Kbps。

[选择] 电话网采用的是 电路交换技术。

[选择] 数据报交换过程中 不必建立虚电路，但要为每个数据报作路由选择。

[选择] 在数据传送中，报文内容不按顺序到达目的节点的是数据报方式。

[选择] 下面有关交换技术的说法中，正确的是 在数据报分组交换中，不保证分组的按序到达，而且目的地需要重新组装报文。

[填空] 调制解调器最主要的功能是 数字数据和模拟信号转换。

[填空] 物理层的传输单位是 比特流。

[填空] 在数据通信系统中，DTE 指的是数据终端设备，是对属于用户所有的联网设备或工作站的统称。DCE 指的是 数据电路终接设备，是为用户提供入网连接点的网络设备的统称。

[填空] DTE 与 DCE 接口的各根导线的电气连接方式有三种，分别是：非平衡方式、采用差动接收器的非平衡方式 和 平衡方式。

[填空] 在物理层的四个特性中，功能特性 规定了接口信号的来源、作用以及其它信号之间的关系。

[填空] 目前由 ITU 建议在物理层使用的规程有 V 系列标准和 X 系列标准；这些标准一般都称作 建议。

[填空] X.21 的设计目标是要减少信号线的数目，其机械特性采用 15 芯 标准连接器。X.21 接口适用于由 数字

线路 访问公共数据网的地区。

[填空]常用的三种有线传输介质是双绞线、 同轴电缆 和 光纤。

[填空]光纤通过内部的 全反射 来传输一束经过编码的光信号。

[填空]人们将小区制移动通信系统叫做 蜂窝移动通信系统。

[填空]在蜂窝移动通信系统中，多址接入方法主要有 3 种，码分多址接入、时分多址接入 和 频分多址接入。

[填空]数据传输速率是指 每秒能传输的二进制信息位数，单位为位 /秒。

[填空]调制速率的单位是 波特。

[填空]若一个码元对应一位二进制信息，则此 时调制速率 和 数据传输速率 是相等的。

[填空]数据通信系统中，信道容量 表征信道的最大数据传输速率。

[填空]香农公式 $C = H \cdot \log_2(1 + \frac{S}{N})$ 中，S 表示 信号功率，N 为 噪声功率，S/N 为 信噪比。

[填空]误码率的定义为 二进制数据位传输时出错的概率。

[填空]就通信方式而言通常情况下，并行通信 用于近距离通信，串行通信 用于远距离通信。

[填空]串行通信的方向形结构有三种，单工 半双工 和 全双工。

[填空]为了获得更大的数字信号传输距离，可以使用 中继器 克服数字传输的衰减。

[填空]最常用的两种多路复用技术是 频分多路复用 FDM 和 时分多路复用 TDM。

[填空]数字通信系统具有两个显著的优点：抗干扰性强 和 保密性好。

[填空]在模拟信道上传输数字信号，必须使用 调制解调器。

[填空]传输线路存在三个主要问题：衰减、延迟畸变 和 噪声。

[填空]三种调制形式是 调幅、调频 和 相位调制。

[填空]ADSL 称为 非对称数字用户线路。

[填空]分组交换的具体过程有 虚电路分组交换 和 数据报分组交换 两种。

[简答]物理层的接口有哪几个方面的特性？各包含些什么内容？

物理层的接口特性包括机械特性、电气特性、功能特性、规程特性。其中：

机械特性对插头和插座的几何尺寸、插针或插孔芯数及其排列方式、锁定装置型式等作了详细规定。

电气特性规定了导线的电气连接及有关电路的特性；接口线的信号电平、发送器的输出阻抗、接收器的输入阻抗等电气参数。

功能特性规定了接口信号的来源、作用及与其他信号之间的关系。

规程特性规定了使用交换电路进行数据交换的控制步骤。

[简答]比较双绞线、同轴电缆与光线的特点。

双绞线可用于模拟和数字传输。其价格便宜，适用于低通信容量局域网。双绞线有屏蔽和屏蔽的两种。

同轴电缆分 50 基带电缆和 75 宽带电缆两类。基带电缆又分细同轴电缆和粗同轴电缆。基带电缆仅仅用于数字传输，数据率可达 10Mnps。宽带电缆是 CATV 系统中使用的标准、它即可使用频分多路复用的模拟信号发送，也可传输数字信号。同轴电缆的价格比双绞线贵一些，但其抗干扰性能比双绞线强。当需要连接较多设备而且通信容量相当大时可以选择同轴电缆。

光纤是非常理想的传输介质，与同轴电缆和双绞线相比，它频带宽、速率高、体积小、重量轻、衰减小、能电磁隔离误码率低等优点。适用于长距离传输。但光线成本高且安装较困难。

[简答]什么是频分多路复用 FDM？

在物理信道的可用宽带超过单个原始信号所需带宽的情况下，可将该物理信号的总宽带分割成若干个与传输单个信号带宽相同的子信道，每个子信道传输一种信号，这就是频分多路复用。

[简答]什么是曼彻斯特编码和差分曼彻斯特编码？各有什么特点？

曼彻斯特编码每一位的中间有一跳变，位中间的跳变即作为时钟信号，又作为数据信号；从高到低的跳变表示“1”，从低到高的跳变表示“0”。

差分曼彻斯特编码每位中间的跳变仅提供时钟定时，而用每位开始有无跳变表示“0”或“1”，有跳变

表示“0”，无跳变表示“1”。

[计算] 设 A、B 两站位于长 1m 的基带总线局域网的两端，数据传输速率为 10Mbps，信号传播速率为 200m/μs，若 A 向 B 发送 800bit 的数据帧，B 接收完毕该帧所需的时间是多少，经过多长时间两站发现冲突？

解：接受结束所需的时间： $1 \times 10^3 \text{m} \div 200 \text{m}/\mu\text{s} + 800 \text{bit} \div 10 \text{bit}/\mu\text{s} = 85 \mu\text{s}$

[计算] 若信道带宽为 4KHz，用 16 种状态编码，在不考虑信道噪声情况下的最大速率。

解：本题应用奈奎斯特公式计算：

$$\text{最大数据传输速率} = 2 \times H \times \log_2 N = 2 \times 4 \text{K} \times \log_2 16 = 32 \text{Kbps}$$

[计算] 设电话线路的带宽为 3KHz，信噪比为 30dB，求该信道的最大数据传输速率 (b/s)

解：表征有噪声干扰的信道上数据最大的传输速率应用香农公式计算。

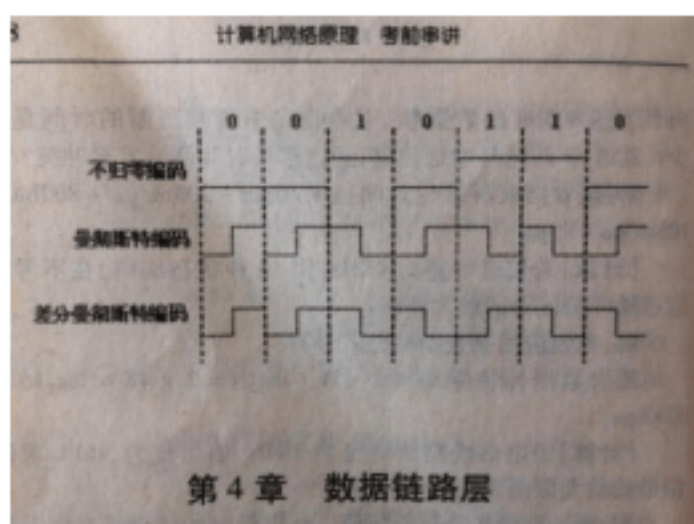
香农公式：
$$C = H \times \log_2 \left(1 + \frac{S}{N} \right)$$
，其中 H 为信道带宽，S 为信号功率，N 为噪声功率，S/N 为信

噪比，C 表示信道最大的数据传输速率。

所以， $C = 3 \text{K} \times \log_2 (1 + 10^{30/10}) = 3 \text{K} \times \log_2 (1 + 1000) \approx 30 \text{Kbps}$

[应用] 控制字符 SYN 的 ASCII 码编码为 0010110，请画出 SYN 的 NRZ、曼彻斯特编码和差分曼彻斯特编码的信号波形。

信号波形如下图所示：



第 4 章 数据链路层

[简答] 数据链路层为什么要引入计时超时机制和帧编号？

为了避免由于数据帧或反馈信息帧丢失而导致发送方永收不到接收方发来的反馈信息，进而使传输过程停止引入计时器超时机制。

为了避免同一帧数据被重复发送多次而引入帧编号的方法，即赋予每帧一个序号，从而使接收方能从该序号来区分是新发送的帧还是已经接收但又重新发送来的帧。

[简答] 请说明什么是流量控制。

流量控制是对发送方数据流量的控制，使其发送效率不致超过接收方所能承受的能力。它并不是数据链路层特有的功能，许多高层协议中也提供流量控制功能。只不过流量控制的对象不同而已。对于数据链路层，控制的是相邻两节点之间的数据链路上的流量；对于传输层，控制的是从源到最终目的之间端对端的流量。

[简答] 简述传输错误的成因及其解决方法。

传输中的差错都是由噪声引起的。噪声有随机热噪声和冲击噪声。随机热噪声：信道物理固有的、持续存在的；冲击噪声：外界特定的短暂原因造成的。其中冲击噪声是产生差错的主要原因。

解决方法：进行差错控制，首要任务就是如何进行差错检测。差错控制可通过以下两种方法解决。即：

(1) 自动请求重发 ARQ。

(2) 前向纠错 FEC。

[简答]比较停等式 ARQ，回退 N 和选择重传协议的区别。

停等式 ARQ，发送窗口和接收窗口大小均为 1，发送方没法送一帧之后就必须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。该方法所需的缓冲存储空间最小，缺点是信道效率很低。

回退 N，发送窗口大于 1，接受窗口等于 1.允许发送方可以连续发送信息帧，但是，一旦某帧发生错误，必须重新发送该帧及其后的 n 帧。这种方式提高了信道的利用率，但允许已发送有待于确认的帧越多，可能要退回来重发的帧也越多。

[简答]试比较 BSC 和 HDLC 协议的特点。

BSC 是最早出现的面向字符的同步协议，其特点是利用已定义好的一种标准字符编码的一个子集来执行通信控制功能。由于 BSC 协议与特定的字符编码集关系过于密切，故兼容性较差。为满足数据透明性而采用的字符填充法，实现起来比较麻烦，且也依赖于所采用的字符编码集。BSC 是一个半双工协议，它的链路传输效率很低。

HDLC 是面向比特的数据链路控制协议的典型代表，该协议不依赖于任何一种字符编码集；数据报文可透明传输，用于实现透明传输的“0 比特插入法”易于硬件实现；全双工通信，有较高的数据链路传输效率；所有帧采用 CRC 检验，对信息帧进行顺序编号，可防止漏收或重发，传输可靠性高；传输控制功能与处理功能分离，具有较大灵活性。

[简答]试比较 SLIP 与 PPP 协议的主要区别。

SLIP 提供在串行通信线路上封装 IP 分组的简单方法，用以使远程用户通过电话线和 MODEM 能方便地介入 TCP/IP 网络。SLIP 是一种简单的组帧方式。其缺点是：SLIP 不支持在连接过程中的动态 IP 地址分配，通信双方必须事先告诉对方 IP 地址；SLIP 帧无协议类型字段，只能支持 IP 协议；SLIP 帧中无校验字段，因此链路层上无法检测出传输差错，必须由上层实体或具有纠错能力的 MODEM 来解决传输差错问题。

PPP 是点到点协议，具有处理错误检测、支持多个协议、允许在连接时刻协商 IP 地址、允许身份认证等功能。

[计算]设要发送的二进制数据为 10110011，若采用 CRC 校验方法，生成多项式为 x^4+x^3+1 ，试求出实际发送的二进制数字序列。

解：

$$\begin{array}{r} 11010100 \\ 11001 \overline{) 101100110000} \\ \underline{11001} \\ 11110 \\ \underline{11001} \\ 11111 \\ \underline{11001} \\ 11000 \\ \underline{11001} \\ 0100 \end{array}$$

要发送的二进制数字序列为：101100110100

[计算]采用生成多项式 $x^6+x^4+x^2+1$ 发送的报文到达接收方为 101011000110，所接收的报文是否正确？试说明理由。

解：多项式 $x^6+x^4+x^2+1$ 对应的位串是 1010101，用它来除接收到的报文，若能整除则所接收报文正确，否则收到的报文不正确。进行如下的二进制除法：

$$\begin{array}{r} 1010101 \overline{) 101011000110} \\ \underline{1010101} \\ 11000110 \\ \underline{1010101} \\ 1100110 \\ \underline{1100110} \\ 000000 \end{array}$$

不能够整除，所以收到的报文是错误的。

[计算]用 BSC 规程传输一批汉字（双字节），若已知采用不带报头的分块传输，且最大报文块长为 129 字节，共传输了 5 帧，其中最后一块报文长为 101 字节。问每个报文最多能传多少汉字？该批数据共有多少汉字？

(假设采用单字节的块校验字符。)

解：BSC 规程，不带报头的分块传输的帧格式为：

SYN	SYN	STX	报文	ETB/ETX	BCC
-----	-----	-----	----	---------	-----

故 4 帧每帧最多能传的汉字数为：

$$(129-3(\text{SYN}+\text{SYN}+\text{STX})-2(\text{ETB}+\text{BCC}))/2=62(\text{个})$$

该批数据共有的汉字数为：

$$62*4+(101-3(\text{SYN}+\text{SYN}+\text{STX})-2(\text{ETX}+\text{BCC}))/2=296(\text{个})$$

[应用]在数据通信过程中出现差错时不可避免的，必须进行差错控制。那么什么是差错控制？其核心是什么？在数据通信过程中是如何进行差错控制的？

差错时直接手段收到的数据与发送端实际发出的数据出现不一致。产生差错主要是因为通信线路上噪声干扰的结果。差错控制是指在数据通信过程中能发现或纠正差错，把差错限制在尽可能小的允许范围内的技术和方法。

差错控制的核心是差错控制编码，即对传输的数据信息加上与其满足一定关系的冗余码，构成一个码字后再发送。接收端收到该码字后，检查信息位和附加的冗余位之间的关系，以检查传输过程是否有差错。利用差错控制编码来进行差错控制的方法基本有两类：自动请求重发 ARQ、前向纠错 FEC。

[应用]假设 HDLC 帧的地址字段为 10010101，控制字段为 00001011，信息字段为 10101011，生成多项式 $G(x)=x^{16}+x^{12}+x^5+1$ ，试求出帧校验序列。

HDLC 帧校验序列字段是对两个标志字段之间的整个帧的内容进行校验。因此帧校验序列的计算过程应该是：

CRC 生成多项式 $G(X)$ 对应的位串是 10001000000100001，也即除数为 10001000000100001，被除数为 1001010100001011101010110000000000000000。进行二进制除法，求得的余数即为帧校验序列。

第 5 章 网络层

[选择]提供虚电路服务的通信子网内部的实际操作可以是 虚电路方式，也可以是数据报方式。

[选择]在虚电路建立过程中，每个节点的虚电路表中要记录两个逻辑信道号，它们是 前一个节点所选取的逻辑信道号和本节点所选取的逻辑信道号。

[选择]一个网络节点从某条线路收到一个分组后，再向除该条线路外的所有线路发送收到的分组，这种路由算法称 泛射路由选择。

[选择]路由选择算法可以分为静态路由选择算法和动态路由选择算法，距离矢量路由算法是动态路由选择算法。

[选择]下列能够实现即插即用的设备是 网桥。

[选择]关于网际互联，以下描述中不正确的是 对于异构网络来说，不能实现网络互连。

[选择]以下关于网桥的说法中，不正确的是网 桥能够实现局域网和广域网的互连。

[选择]IP 协议提供的是 无连接的数据报服务。

[选择]IP 数据报分段的重组通常在上层进行 目的主机。

[选择]从协议层次看，网络层体现了 网络应用环境中资源子网访问通信子网的方式。

[选择]虚电路是 逻辑通路，非专用的。

[选择]采用虚电路操作支持虚电路服务方式的是 SNA。

[选择]使用生成树 (Spanning Tree)来解决 广播路由选择。

[选择]当进行拥塞控制时，进行资源预留法用于 虚电路的分组交换网。

[选择]当路由器因为来不及处理分组而被淹没时，采用的拥塞控制方法成为 负载丢失。

[选择]两个网络互连时，它们之间的差异可以表现在 OSI 七层模型中的 任一层上 。

[选择]实现网路物理层的链接，对网段上的衰减的信号进行放大整形或再生的中继设备是 转发器 。

[选择]在 OSI 参考模型中，路由器工作在 网络层 。

[选择]在 TCP/IP 协议簇中，IP 层的数据单元称为 数据报 。

[选择]以下陈述正确的是 到达目的主机的 IP 数据报顺序与发送的顺序可能不一致 。

[选择]IP 协议是无连接的，其信息传输方式 数据报方式 。

[选择]以下关于地址转换协议 ARP 的描述中，正确的是 ARP 是采用广播方式发送的 。

[选择]在 TCP/IP 协议簇中，用来将物理地址转换成 IP 地址的协议是 RARP 。

[选择]IPv6 的地址长度是 128 位。

[填空]节点的路由选择要依靠网络当前的状态信息来决定的策略称为 动态路由选择策略 ，这种策略能较好地适应 网络流量 、 拓扑结构 的变化，有利于网络性能的改善。

[填空]网络层是在 数据链路 层提供的数据帧的传送功能上，进一步管理网络中的数据通信，向 传输 层提供最基本的 端到端 数据传送服务。

[填空]网络层的目的是实现两个系统之间的数据透明传送，具体功能包括 路由选择 、 拥塞控制 和网际互连等。

[填空]在分组交换方式中，通信子网内部有 虚电路 和数据报 两种方式。

[填空]所谓占用某条逻辑信道，实际上是指占用了该段物理信道上节点分配的 分组缓冲器 。

[填空]通信子网中节点间的物理信道在逻辑上均可看作是由多条逻辑信道组成，不同的逻辑信道在节点内部通过 逻辑信道号 加以区分，各条逻辑信道 异步地 分时复用同一条物理信道。

[填空]当虚电路拆除时，节点的虚电路表空间和逻辑信道号必须 回收 。

[填空]在数据报操作方式中，一个节点接收到一个数据报后，根据数据报中的 地址信息 和节点所存储出的路由信息 ，找出一个合适的出路把数据报发送到下一节点。

[填空]通信子网中一个网络节点收到一个分组后，要确定向下一节点传送的路径，这就是 路由选择 。

[填空]最优化原则 和汇集树 为路由选择算法提供了一种衡量标准。

[填空]三种静态路由选择算法是 最短路由选择算法 、 扩散法 和基于流量的路由选择算法。

[填空]最为常见的两个动态路由选择算法是 距离矢量路由算法 和 链路状态路由算法 。

[填空]在实际的网络总被广泛应用的路由算法是 链路状态路由算法 。

[填空]那些离开了原始站点还想继续连接网络的主机称为 移动主机 。

[填空]拥塞控制解决的方案有 开环的 和闭环的 两类。

[填空]完成开环控制的手段中共同之处是，他们在作出决定的时候 不考虑网络的当前状态 。

[填空]闭环方案建立在 反馈环路 的概念基础上。

[填空]解决拥塞问题，当系统资源已达到了极限，不能增加的时候，唯一办法就是 降低系统的负载 。

[填空]决定一个流所要求的服务质量的 4 个特征是 可靠性 、 延迟 、 抖动、 带宽 。

[填空]有一种服务质量方法，这种方法不需要提前建立流，它主要由每台路由器在局部范围内实现，而不牵涉到整条路径， 这种方法叫 做基于类 的服务质量。 IETF 对这种方法的体系进行了标准化， 称为 区分服务 。

[填空]实现 Qos 保证的关键技术是 MPLS 。

[填空]ATM 交换机是面向连接的 异步传输模式 ，传输的是 53 字节的信元。

[填空]网桥的作用是通过 过滤 和转发 功能实现的。

[填空]透明网桥维护一个基于 MAC 地址的过滤数据库。

[填空]当网桥初始化时，过滤数据库为空，为了能够了解到所有目的地的位置，透明网桥有一个 自动学习 机制，采用逆向学习法，从收到帧的源地址确定端口连接的 LAN 位置。

[填空]在 Internet 中广泛使用的网络互连协议有 路由信息协议 RIP 和开放最短路径优先协议 OSPF 。

[填空]每个 RIP 路由器每隔 30 秒广播一个路由信息。

[填空]目前最主要的内部网关协议是 开放最短路径优先协议 。

[填空]路由器的主要功能有 建立并维护路由表和分组转发功能。

[填空]网关也称 协议转换器，用于高层协议的转换。

[填空]IP 向上层提供统一的 IP 数据报 和统一的 IP 地址，使得各种物理帧及物理地址的差异性对上层协议不复存在。

[填空]因为不同物理网络的 最大传输单元 MTU 不同，所以 IP 数据报有分段与重组操作。

[填空]在 IP 报头中控制分段和重组的 IP 头域有三个：标识域、标志域、分段偏移域。

[填空]为了使互联网能报告差错，或提供有关意外情况的信息，在 IP 层有 互联网控制报文协议 ICMP。

[填空]因特网支持两类组地址：永久组地址 和 临时组地址。

[简答]简述网络层的主要功能。

网络层在数据链路层提供的两个相邻结点之间的数据帧的传送功能上，进一步管理网路中的数据通信，将数据设法从源端经过若干个中间节点传送到目的端，从而向传输层提供最基本的端到端的数据传送服务。网络层的目的是实现两个端系统之间的数据透明传送，具体功能包括路由选择、拥塞控制和网际互连等。

[简答]什么是拥塞？造成拥塞的原因是什么？

拥塞现象是指到达通信子网中某一部分的分组数量过多，使得该部分网路来不及处理，以致引起这部分乃至整个网络性能下降的现象，严重时甚至会导致网络通信业务等陷入停顿即出现死锁现象。

造成拥塞的原因：多条流入线路有分组到达，并需要统一输出线路，此时，如果路由器没有足够的内存来存放所有这些分组，那么有的分组就会丢失。路由器的慢速处理器的缘故，以至于难以完成必要的处理工作，如缓冲区排队、更新路由表等。

[简答]流量控制与拥塞控制有何关系与区别？

流量控制与拥塞控制有何关系与区别如下：

流量控制：接收端向发送端发出信号，请求发送端降低发送速率。拥塞控制：接收端也向发送端发出信号，告之发送端，网络已出现麻烦，必须放慢发送速率。

流量控制：主要控制收发端之间的通信量；拥塞控制：是全局性控制，涉及所有主机路由器以及其他降低网络性能的有关因素。

[简答]网际互联的意义是什么？作为中间系统，转发器、网桥、路由器和网关有何区别？

网际互联的目的是一个网络上的用户能访问其他网络上的资源，使网上的用户互相通信和交换信息。这不仅有利于资源共享，也可以从整体上提高网络的可靠性。

(1)转发器 (repeater)：一种工作在物理层的设备。它对网段上的衰减信号进行放大整形或再生，用来扩展网段距离。

(2)网桥 (bridge)：一种工作在数据链路层的设备。在不同或相同的局域网之间存储和转发帧。

(3)路由器 (router)：一种工作在网络层的设备。在不用的网络之间存储和转发分组。路由器从一条输入线路上接收分组，然后再向另一条输出线路转发，这两条线路可能属于不同的网络，采用的协议也可能不同。

(4)网关 (gateway)：网关提供传输层及传输层以上各层间的协议转换。

[计算]考虑下面虚电路服务实现涉及到的设计问题。如果虚电路用在子网的内部，每个数据报文必须有一个 3 字节的报头，每个路由器必须留有 8 字节的空间来标识虚电路。如果内部使用数据包，则要使用一个 15 字节的分组头。假定每站段传输宽带的费用为每字节 0.1 元人民币；路由器存储器的价格为每字节 0.1 元人民币，并且按照两年的使用时间来计算（每周工作 40 小时）。平均会话期为 1000 秒，传输 200 个分组；分组平均需传送 4 个站段。请问：子网内部采用虚电路还是采用数据报便宜一些？便宜多少？

解：每个分组经过 4 段链路意味着路上包括 5 个路由器。

虚电路实现方案：需要在 1000 秒内固定分配 $5 \times 8 = 40$ 字节的存储空间。

存储器使用的时间是 2 年，即 $2 \times 52 \times 40 \times 3600 = 1.5 \times 10^7$ 的 7 次方秒

每字节每秒的费用 $= 0.1 / (0.5 \times 10^7 \text{ 的 } 7 \text{ 次方}) = 6.7 \times 10^{-9}$ 次方 元

总费用，即 1000 秒 40 字节的费用 $= 1000 \times 40 \times 6.7 \times 10^{-9} \text{ 的 } -9 \text{ 次方} = 2.7 \times 10^{-4}$ 次方 元

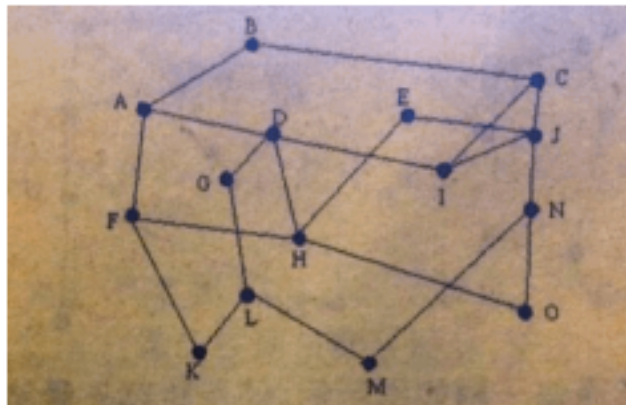
数据报实现方案：比上述虚电路实现方案需多传 $(15-3)*4*200=9600$ 字节

每字节每链路费用 $=0.1/10$ 的 6 次方 $=10$ 的 -7 次方

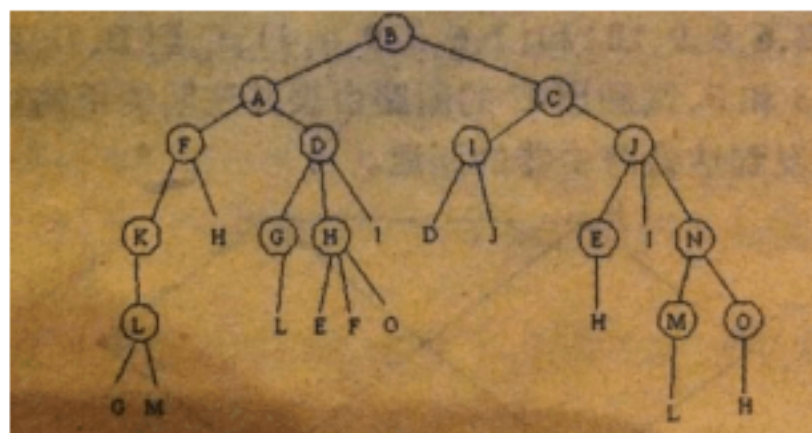
总费用，即 9600 字节每链路费用 $=9600*10$ 的 -7 次方 $=9.6*10$ 的 -4 次方 元

可见，本题中采用虚电路实现方案更为经济，在 1000 秒的时间内便宜 $6.9*10$ 的 -4 次方 元。

[应用] 如下图所示子图，采用： (1) 反向路径转发； (2) 汇集树。从 B 广播，分别可形成多少个分组。



解：由逆向路径转发算法构造的图，如下图



在第一跳的时候，B 发送分组给 A 和 C，这些分组中的每一个都是在通向 B 的首选路径上到来的。在图 (5-3) 中字母外面加一个圆圈就表示这样的分组。在第二跳的时候，共产生了 4 个分组，其中，在第一跳接收到分组的路由器各产生 2 个分组。在第三跳所产生的 10 个分组中，只有 5 个是在首选路径上到来的。其他都是重复分组。在经过第 5 跳和 28 个分组以后，广播过程终止了。

下面所示由逆向路径转发算法构造的路由器 B 的汇集树，如下图形成 14 个分组。



[应用] 某通信子网如图所示，使用距离矢量路由算法。假设到达路由器 C 的路由器 B、D、E 的矢量分别为 $(5,0,8,12,6,2)$ 、 $(16,12,6,0,9,10)$ 和 $(7,6,3,9,0,4)$ ；C 到 B、D、E 的延迟分别为 6、3 和 5，试画出 C 的新路由表并注明使用的输出线路及从 C 出发到达各路路由器的延迟。

第 6 章 传输层

[选择] 在 TCP/IP 协议簇中，面向连接的传输层协议是 TCP。

[选择] 关于 TCP 和 UDP 协议的描述，不正确的是 UDP 协议要求对方发出的每个数据包都要确认。

[选择] 下面哪个协议是无连接的传输层协议 UDP。

[选择] 数据链路层和传输层都具有的功能是 流量控制。

[选择] 传输层的作用是向源主机与目的主机进程之间提供 端到端 数据传输。

[选择] TCP 提供的服务是 面向连接的字节流通信。

[选择] 在 TCP 的段结构中，不包括的信息是 源 IP 地址和目的 IP 地址。

[选择] 在 TCP 的段结构中，以下哪个标志位是建立连接时要用到的 SYN。

[选择] 为了保证连接的可靠性，TCP 通常采用 三次握手法。

[选择] TCP 采用的流量控制协议是 可变大小的滑动窗口协议。

[填空] 传输层利用 网络层 提供的服务，向 应用层 提供服务。

[填空] TPDU 是 传输协议数据单元。

[填空] 传输服务是通过建立连接的两个传输实体之间的采用的 传输协议 来实现的。

[填空] 因特网传输地址由 IP 地址和主机端口号 组成。

[填空] 传输层是 OSI 七层模型中负责的 数据通信 最高层，又是面向 网络通信 的低三层和面向 信息处理 的高三层之间的中间层。

[填空] TCP 段结构中端口地址是 16 比特。

[填空] 端口号小于 256 为常用端口，服务器 一般都是通过常用端口号来识别的。

[填空] 大多数 TCP/IP 实现给临时端口分配 1024-5000 之间的端口号。

[填空] 超文本传送协议 HTTP 使用的端口号是 80。TCP 端口 21 表示 文件传输协议 FTP。SMTP 是 25。TELNET 是 23。

[填空] 因为是双工通信，TCP 连接释放采用 对称 释放方式。

[填空] TCP 协议用于控制数据段是否需要重传的依据是设立 重发定时器。

[填空] 因特网中，对拥塞控制的最有效的方法是 降低数据传输速率。

[填空] 造成拥塞出现，是由 网络容量 和 接受容量 两个方面的问题引起的，需要分别处理。

[填空] 拥塞窗口大小的确定使用 慢速启动法。UDP 提供了无连接的数据报服务，在传输数据前无须建立连接。

[填空] UDP 端口 53 表示 域名解析服务 DNS。

[简答] 传输协议要素有哪些。

寻址。当一个应用程序希望与另一个应用程序传输数据时，必须招明是与哪附上应用程序相连。寻址的方法一般采用定义传输地址。因特网传输地址由 IP 地址和主机端口号 组成。

建立连接。在实际的网络应用中，采用三次握手的算法，并增加某些条件以保证建立起可靠的连接，

增加的条件是：所发送的报文都要有递增的序列号；对每个报文设立一个计时器，设定一个最大时延，对那些超过最大时延仍没有收到确认信息的报文就认为已经丢失，需要重传。

释放连接。也采用三次握手的算法。

[简答] TCP与 UDP对于端口号的使用有什么规定 ？

TCP 与 UDP段结构中端口地址都是 16 比特，可以有在 0-65535 范围内的端口号。对于这 65536 个端口号有以下的使用规定：

端口号小于 256 的定义为常用端口，服务器一般都是通过常用端口号来识别的。任何 TCP/IP 实现所提供的服务是用 1-1023 之间的端口号，是 IANA来管理的；

客户端只需保证该端口号在本机上是惟一的就可以了。客户端端口号因存在时间很短暂又称为临时端口号；

大多数 TCP/IP 实现给临时端口号分配 1024-5000 之间的端口号。大于 5000 的端口号是为其他服务器预留的。

[简答] 简述 TCP所提供服务的的主要特点 。

- (1) 面向连接的传输；
- (2) 端到端的通信；
- (3) 高可靠性，确保数据的正确性，不出现丢失或乱序；
- (4) 全双工方式传输；
- (5) 采用字节流的方式，即以字节为单位传输字节序列；
- (6) 紧急数据传送功能。

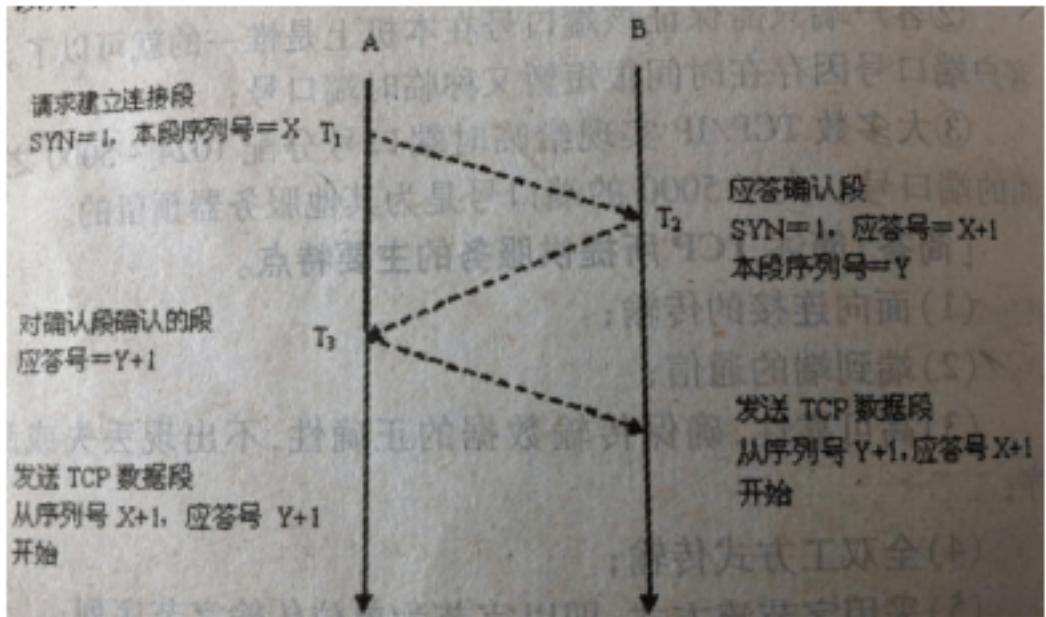
[简答] UDP提供什么样的服务，它的应用场合是什么样的？

UDP 提供的报务是不可靠的，无连接的服务。UDP适用于无须应答并且通常一次只传送少量数据的情况。

由于 UDP协议在传输的过程中无须建立逻辑连接，对数据包也不进行检查，因此 UDP协议具有较好的实时性，效率高。在有些情况下，包括视频电话会议系统在内的众多的客户 / 服务器模式的网络应用都 UDP 协议。

[应用] 画图说明 TCP采用三次握手协议建立连接的过程。并说明 TCP协议时如何确保数据传输高可靠性的。

三次握手协议建立连接的过程是 ；第一方向别一方发送连接请求段，另一方回应对连接请求的确认段，第一方再发送对对方确认段的确认。这个过程可以用下图表示：



图中，SYN为请求建立连接的标志，三次握手的过程如下：

在 T_1 时刻，A向 B发送请求建立连接段序列号为 X。

在 T_2 时刻，B发送应答 A 的 X序号的请求建立连接的段，该应答段的序列号为 Y。

在 T_3 时刻，A发送对 B的应答段的应答，应答号为 Y+1，表明应答号为 Y的段已接收。

至此，连接建立成功。

为了保证可靠性，发送的报文都有递增的序列号。序号和确认号用来确保传输的可靠性。此外，对每个报文都设立一个计时器，设定一个最大时延。对那些超过最大时延仍没有收到确认信息的报文就认为已经丢

失，需要重传。

第7章 应用层

[选择] IP 地址 129.66.51.37，它的网络标识部分是 129.66。

[选择] 在 Internet 域名体系中，域名由若干分量组成，各分量之间用圆点分隔，各分量按照从右到左越来越小的方式分多屋排列。

[选择] 以下关于域名的描述中，不正确的是 com是一个国际顶级域名。

[选择] 下列不属于电子邮件协议的是 ICMP。

[选择] E-mail 件地址 chang@online.sh.cn 中没有包含的信息是 邮件客户机。

[选择] 接入 Internet 的每一台计算机都有一个唯一的地址标识，这个地址标识为 IP 地址。

[选择] IP 地址是一个 32 位的二进制数，它通常采用点分 十进制数表示。

[选择] 网络标识在一个 IP 地址中的作用是，它规定了主机所属的网络。

[选择] 以下 IP 地址中，属于 C 类地址的是 193.1.1.2。

[选择] IP 地址 205.140.36.88 的主机标识是 88。

[选择] 网址 "www.sina.com.cn" 中的 "cn" 表示 中国。

[选择] 用于表示教育机构的域名是 edu。

[选择] 域名和 IP 地址之间的关系是 一个 IP 地址对应多个域名。

[选择] 域名系统所要解决的问题是 实现域名和 IP 地址之间的转换。

[选择] 在电子邮件中所包含的信息 可以是文本，声因，图像和应用程序。

[选择] 一个 E-mail 地址为 chang@sina.com, 则该 E-mail 的账号是 chang。

[选择] 发送电子邮件时，如果接收方没有开机，那么邮件将 保存在邮件服务器上。

[选择] 接收 E-mail 所用的网络协议是 POP3。

[选择] www的作用是 信息浏览。

[选择] 客户端浏览器和 www服务器之间传输网页使用的协议是 HTTP。

[选择] 超文本的含义是指 带有超链接的文本。

[选择] URL 的作用 定位主机地址。

[选择] 地址 "http://www.g.cn" 中的 "http" 是指 协议。

[选择] 下列属于 B 类 IP 地址的是 128.2.2.10。

[选择] 在 Internet 的服务功能中，远程登录所使用的命令是 telnet。

[填空] 应用层协议是 网络 和 用户 之间的接口。即网络用户是通过不同的应用协议来使用网络的。

[填空] IP 协议是根据实现信息传递的 IP 地址。

[填空] IP 地址是 4 字节二进制数据组成。

[填空] IP 地址的两个组成部分是 网络标识 和 主机标识。

[填空] 利用子网掩码可以 判断两台主机是否在同一子网中。

[填空] 为了用户使用和记忆都很方便，Internet 引进了字符形式的 IP 地址，称为 域名。

[填空] 域名系统 DNS是一个 分布式数据库 系统，由域名空间，域名服务器 和 地址转换请求程序 三部分组成。

[填空] 域名由若干个分量组成，级别最低的域名写在最 左边，级别最高的顶级域名写在最 右边。

[填空] 二级域名 gov 代表政府部门； org 代表 非盈利组织。

[填空] 域名服务器的三种不同类型是：本地域名服务器，根域名服务器 和 授权域名服务器。

[填空] 用户 E-mail 地址的格式为：用户名 @主机域名。

[填空] SMTP协议的端口号是 25；通过 用户代理 程序和 邮件传输代理 程序实现邮件的传输。

[填空] 电子邮件客户端程序查看邮件服务器中自己的邮箱使用 POP或 IMAP 协议。

[填空] www是指通过 HTTP 协议链接起来的无数 Web服务器中的网页资源。

[填空] www采用的是 客户机 / 服务器 的工作模式。

[填空]www服务器上的信息通常以 超文本 的方式进行组织。

[填空]HTTP的含义是 超文本传输协议 ；它是 应用 层协议，用于浏览器访问 Web服务器上的超文本信息。

[填空]在 HTTP中通过 统一资源定位器 URL来标识被操作的资源。

[简答]目前在 Internet 上有哪些使用比较广泛的应用 。

目前在因特网上使用最广泛的应用层协议：超文本传输协议，文件传输协议，远程登录协议 Telnet ，电子邮件协议 SMTP和 POP3, 域名系统 DNS

[简答]什么是域名 ？其结构是什么 ？什么是域名系统 DNS？

32 位的二进制数的 IP 地址以用户来说不方便使用和记忆。为此，Internet 引进了字符形式的 IP 地址，即域名。它用来惟一标识因特网上的主机或路由器。它只是一个逻辑概念，并不反映出计算机所在的物理地点。

域名由若干个分量组成，各分量之间用 "." 分隔

N级域名， 二级域名 . 顶级域名

每一级的域名都由英文字母和数字组成 （长度不超过 63 个字符，并且不区分大小写 ），级别最低的域名写在最左边，而级别最高的顶级域名则写在最右边。

Internet 上的域名由域名系统 DNS统一管理。DNS是一个分布式数据库，由域名空间，域名服务器，和地址转换请求程序三部分组成。DNS负责域名和 IP 地址之间的转换。

[简答]说明域名解析的过程 。

当应用进程需要将一个主机域名映射为 IP 地址时，就调用域名解析函数，解析函数将待转换的域名放在 DNS请求中，以 UDP报文方式发给本地域名服务器。本地的域名服务查到域名后，将对应的 IP 地址放在应答报文中返回。同时域名服务器还必须具有连向其他域名服务器的信息以支持不能解析时的转发。若域名服务器不能回答该请求，则此域名服务器就暂时成为 DNS中的另一个客户，向根域名服务器发出请求解析，根域名服务器一定能找到下面的所有二级域名的域名服务器，这样以此类推，一直向下解析，直到查询到所请求的域名。

[简答]说明 POP协议与 IMAP协议各自的特点，两者有何区别 ？

电子邮件系统使用邮局协议，众邮件服务器中自己的邮箱中取出邮件。POP 协议是一种离线式工作协议。POP3是目前最常用的电子邮件服务协议。POP3遵循存储转发机制，用户可按需要在客户端与邮件服务器之间建立连接，将邮件服务器上的邮件取到客户机上，同时删除服务器上已取出的邮件，并断开连接。用户就可以在客户机上阅读收取的邮件了。

与 POP3协议类似，IMAP 也提供面向用户的邮件收取服务。常用的版本是 IMAP4。IMAP4改进了 POP3的不足，用户可以通过浏览信件头来决定是否收取，删除和检索邮件折特定部分，还可以在服务器上创建或更改文件夹或邮箱，它除了支持 POP3协议的脱机操作模式外，还支持联机操作和断连接操作。它为用户提供了有选择的从邮件服务器接收邮件的功能，基于服务器的信息处理功能和共享信箱功能。IMAP4 的脱机模式不同于 POP3, 它不会自动删除在邮件器上已收取的邮件。其联机模式和断连接模式也是将邮件服务作为 " 远程文件服务器 " 进行访问更加灵活方便。

[简答]WWW的工作流程是怎样的

WWW 采用客户机 / 服务器的工作模式，具体如下：

(1) 用户使用浏览器或其他程序建立客户机与服务器连接，并发送浏览请求。

(2)Web 服务器接收到请求后，返回信息到客户机。

(3) 通信完成，关闭连接。

[简答]简述 HTTP的含义及其作用

HTTP 是超文本传输协议，是客户端浏览器或其他程序与 Web服务器之间的应用层通信协议。在 Internet 上的 Web服务器上存放的都是超文本信息，客户机需要通过 HTTP协议传输所要访问的超文本信息。HTTP 包含命令和传输信息，不仅可用于 Web访问，也可以用于其他因特网 / 内联网应用系统之间的通信，从而实现各类应用资源超媒体访问的集成。

[简答] 统一资源定位器 URL 的作用是什么 ?URL 的完整格式是什么样的 ?

统一资源定位器是为了能够使客户端程序查询不同的信息资源时有统一访问方法而定义的一种地址标识方法。在 Internet 上所有资源都有一个独一无二的 URL 地址。URL 的完整格式为 : 协议 :// 主机名或 IP 地址 : 端口号 / 路径名 / 文件名。

[简答] 什么是匿名 FTP

所谓匿名服务器指的是不需要专门的用户名和口令就可以进入的系统。用户连接匿名 FTP 服务器时, 都可以用 "anony-mous" 作为用户名, 以自己的 E-mail 地址作为口令登录。登录成功后, 用户可从匿名服务器上下载文件。匿名服务器的标准目录为 pub, 用户通常可以访问该目录下的所有子目录中的文件。考虑到安全问题, 大多数匿名服务器不允许用户上传文件。

[应用] 假设在 Internet 上有一台 WWW 服务器, 其域名为 www.gohelper.edu.cn, 服务端口为默认。在大学校园有一台主机为 123.11.33.90, 子网掩码 255.255.255.234 默认路由配置为 123.11.33.1, DNS 配置为 123.11.11.1。现在请分析并写出从此主机访问 WWW 服务器的某网页的过程。

- (1) 将该主机的 IP:123.11.33.90 和默认路由器 IP:123.11.33.1 分别与子网掩码 255.255.255.234 进行"与"操作, 得到子网号都为 001, 所以主机与默认路由器在同一子网中。但是主机与 DNS 并不在同一个子网中。主机上访问 URL:www.gohelper.edu.cn/test.html 时, 首先构造一个域名请求报文, 送到路由器上;
- (2) 路由器 123.11.33.1 收到封装有该报文的 IP 分组后, 将根据路由信息将该分组转发出去, 直到 DNS 服务器 123.11.11.1 ;
- (3) DNS 服务器 123.11.11.1 收到封装有该报文的 IP 分组后, 将首先查询所管辖的域名信息, 由于 DNS 服务器能解析域名, 就将 www.gohelper.edu.cn 转换成 IP 地址, 并将响应报文发送给路由器 123.11.33.1 。
- (4) 路由器 123.11.33.1 将报文发送给主机 123.11.33.90 。
- (5) 主机与 WWW 服务器 IP 在端口 80 建立 TCP 连接。
- (6) 当 TCP 连接建立后, 主机发送获取 /test.html 的 HTTP 请求。
- (7) WWW 服务器接收到 HTTP 请求, 构建好 Web 页面, 将信息返回主机 123.11.33.90 。
- (8) 主机将收到的信息进行解释和显示。

第 8 章 局域网技术

[选择] CSMA 技术中, 如信道空闲, 则立即发送; 若信道忙则放弃监听、随机等待一段时间, 再开始监听信道, 该算法规则称为 非坚持性算法。

[选择] 有关 CSMA/CD 的叙述中, 错误的是 CSMA/CD 是一种无冲突协议。

[选择] 以太网采用的介质访问控制协议是 1-坚持 CSMA/CD。

[选择] 令牌总线的介质访问控制方法和物理层技术规范由 IEEE802.4 描述。

[选择] 100BASE-F 种的 " 100 " 的含义是 数据传输速率为每秒 100Mbit。

[选择] 信道动态分配策略本质上属于 异步时分多路复用。

[选择] 在非坚持 CSMA 协议中, 当监听到信道忙时, 该节点会是 随机等待一段时间再开始监听。

[选择] 局域网中, MAC 指的是 介质访问控制子层。

[选择] 令牌环局域网的标准是 IEEE802.3。

[选择] IEEE802.9 标准定义了 语音数据综合局域网技术。

[选择] 以太网标准是 IEEE802.3。

[选择] 以太网采用的发送策略是 站点采用带冲突检测的 CSMA 协议进行发送。

[选择] CSMA/CD 适用的网络拓扑结构是 总线形。

[选择] 10BASE2 试用的传输介质是 细缆。

[选择] 当 IEEE802.3MAC 帧种的目地址字段为全 " 1 " 时, 表示 广播地址。

[选择] Ethernet 局域网是基带系统, 它采用 曼彻斯特编码。

[选择] IEEE802.3MAC 帧起始定界符字段 SFD, 其比特模式为 10101011。

[选择]光纤分布数据接口 FDDI MAC 帧和 IEEE802.5 的帧十分相似，不同的是 FDDI 帧含有前导码，FDDI 的令牌帧没有优先位和预约位。

[选择]FDDI 方法和 IEEE802.5 一样都采用令牌传送协议，但是 FDDI 协议发送站发完帧后，可立即发送新令牌，802.5 发送出去的帧的前沿回到发送站时，才发送新的令牌帧。

[选择]10BASE-T 和 100BASE-T 相比，以下说法不正确的是 两者的冲突检测时间是相同的。

[选择]以太网的 MAC 地址长度为 48 位。

[选择]从传输技术上，计算机网络分为 广播网和点到点网。

[选择]决定局域网特性的主要技术有三个，他们是 传输介质、网络拓扑结构和介质访问控制协议。

[选择]局域网都以 广播 信道作为通信基础；广域网大都采用 点到点 信道。

[填空]介质访问就是指 网络节点使用信道进行通信。

[填空]局域网中，在数据链路层专门设计了一个 介质访问控制 MAC 子层，用来实现广播网中的信道分配，解决信道争用的问题。

[填空]信道动态分配策略包括 随机访问和控制访问。

[填空]随机访问又称争用；控制访问有两种方法：轮转和预约。

[填空]目前介质访问控制协议可划分为 3 类：争用协议、无冲突协议和有限争用协议。

[填空]CSMA 是指 载波监听多路访问协议。

[填空]CSMA/CD 的中文含义是 带有冲突检测的载波监听多路访问协议。

[填空]OSI/RM 的数据链路层，在局域网参考模型中被分成 介质访问控制 MAC 和逻辑链路控制 LLC 两个子层。

[填空]IEEE802.4 是 令牌总线 访问方法和物理层协议。

[填空]IEEE802 标准中包括了局域网中最常用的三种介质访问控制方法，包括：CSMA/CD 总线、Token Bus 令牌总线、Token Ring 令牌环。

[填空]10BASE2 使用的编码技术是曼彻斯特码。最大段长 185 米，每段节点数 30。

[填空]IEEE802.3 采用的介质访问控制方法是 1-坚持 CDMA/CD(或 CSMA/CD)。

[填空]10BASE-T 使用的传输介质是 双绞线；物理上是 星型 拓扑结构，逻辑上是 总线 拓扑结构。

[填空]IEEE802.3 标准提供了 MAC 子层的功能说明，内容主要有 数据封装和介质访问管理 两个方面。前者包括成帧、编址 和差错检测；后者包括 介质分配 和竞争处理。

[填空]控制令牌访问技术可用于 令牌总线 和 令牌环 两种拓扑结构网络。

[填空]令牌环的介质访问控制功能包括：帧发送、令牌发送、帧接收和优先权操作。

[填空]DDI 是指 光纤分布数据接口；以光纤作为传输介质的高性能的 令牌环网。

[填空]FDDI 标准中，采用 ANSI 设计的一种称为 4B/5B 的代码进行数据编码。这种编码技术中，每次对 4 位数据 进行编码，每四位数据编码成 5 位符号。

[填空]在一般环网中，只有一个主时钟的集中式时钟方案，但在绕环运行时，时钟信号会偏移。为了消除这种时钟偏移现象，采用一种称为 弹性缓冲器 来消除这种偏移。

[填空]快速以太网的数据传输速率是 100Mbps。代表是 100BASE-T。

[填空]100BASE-TX 和 100BASE-FX 使用的数据编码都是 4B/5BNRZI。

[填空]目前，常用的无线接入技术主要有 IEEE802.11 无线局域网技术、红外 Ir 端口技术和蓝牙技术。

[填空]无线网络标准是 IEEE802.11。

[填空]无线局域网采用 载波监听多路访问/冲突防止协议 CSMA/CA 实现介质资源共享。

[填空]WAP 是指 无线应用协议。

[填空]WAP 移动终端上的浏览器所识别的描述语言是 无线标记语言 WML 和 无线标记语言脚本 WMLScript。

[填空]Ad Hoc 网络又称 移动自组网 或 多跳网络。它是 移动通信 和计算机网络相结合的网络。

[填空]Client/Server 工作模式以 数据库管理系统 为后援，将 数据库操作 与 应用程序 分离开来，分别由服务器

端数据库和客户端工作站来执行。

[简答]简述局域网的特点。

覆盖范围小、传输速率高、通信延迟小、误码率低。

[简答]信道的静态分配策略是什么样的？它有何特点？

静态分配策略：是预先将频带或时隙固定地分配给各个网络节点，各节点都有自己专用的频带或时隙，彼此之间不会产生干扰。静态分配策略包括频分多路复用和同步时分多路复用。

静态分配策略的特点：适用于网络节点数目少而固定，且每个节点都有大量数据要发送的场合。此时采用静态分配策略不仅控制协议简单，而且信道利用率较高。

[简答]信道的动态分配策略有什么特点？

动态分配策略本质上属于异步时分多路复用，包括随机访问和控制访问。各站点当有数据要发送时，才占用信道进行数据传输。动态分配策略种的随机访问，各个节点有数据就发送，发生碰撞之后再采取措施解决。适用于负载较轻的网络，网络延迟较短。控制访问是使发送节点首先获得信道的使用权，然后再发送数据，因而不会出现碰撞和冲突。当网络负载较重时，可以获得很高的信道利用率。

[简答]简述 1-坚持 CSMA、非坚持 CSMA 和 p-坚持 CSMA 算法的特点。

1-坚持 CSMA(1-persistent CSMA) 的基本思想是：当一个节点要发送数据时，首先监听信道；如果信道空闲就立即发送数据；如果信道忙则等待，同时继续监听直至信道空闲；如果发生生冲突，则随机等待一段时间后，再重新开始监听信道。

非坚持 CSMA 的基本思想是：当一个节点要发送数据时，首先监听信道；如果信道空闲就立即发送数据；如果信道忙则放弃监听，随机等待一段时间，再开始监听信道。非坚持 CSMA 会减少发送数据导致冲突的概率，但会使得数据在网络中的平均延时时间增加。

p-坚持 CSMA(P-persistent CSMA) 用于时分信道 (Slotted Channel)，其基本思想是当一个节点要发送数据时，首先监听信道；如果信道忙则坚持监听到下一个时隙；如果信道空闲，便以概率 p 发送数据，以概率 $1-p$ 推迟到下一个时隙；如果下一个时隙信道仍然空闲，则仍以概率 p 发送数据，以概率 $1-p$ 推迟到下一个时隙；这样一直持续下去，直到数据被发送出去，或因其他节点发送而检测到信道忙为止，若是后者，则等待一段随机的时间后重新开始监听。P-坚持 CSMA 的性能依赖于概率 p 的选取。

[简答]简答 CSMA/CD 工作原理。

CSMA/CD 是带有冲突检测的 CSM，其基本思想是当一个节点要发送数据时，首先监听信道；如果信道空闲就立即发送数据，并继续监听；如果在数据发送过程中监听到了冲突，则立刻停止数据发送，等待一段随机的时间后，重新开始尝试发送数据。

[简答]IEEE802.3 协议的以太网 (Ethernet) 采用什么样的媒体访问控制方法？

以太网采用带有冲突检测的载波监听多路访问 (CSMA/CD) 技术，并用二进制指数退避和 1-坚持算法。

[简答]简述令牌环的操作过程。

网络空闲时，只有一个令牌在环路上绕行。令牌是一个特殊的比特模式，其中包含一位“令牌数据帧”标志位，标志位为“0”表示该令牌为可用的空令牌，标志位为“1”，表示有站点正占用令牌在发送数据帧。

当一个站点要发送数据时，必须等待并获得一个令牌，将令牌的标志位置为“1”，随后便可发送数据。

环路中的每个站点便转发数据，边检查数据帧中的目的地址，若为本站点的地址，边读取其中所携带的数据。

数据帧绕环一周返回时，发送站点将其从环路上撤销。同时根据返回的有关信息确定所传数据有无出错。若有错则重发存于缓冲区中的待确认帧，否则释放缓冲区中的待确认帧。

发送站点完成数据发送后，重新产生一个令牌传至下一个站点，以使其他站点获得发送数据的许可权。

[简答]FDDI 网主要特性是什么？

FDDI 网的主要特性是： 光纤分布数据接口 FDDI 是以光纤作为传输介质的高性能令牌环网； 它的逻辑拓扑结构是一个环，物理拓扑结构可以是环形、带树形的环或是带星形的环； FDDI 使用基于 IEEE802.5 令牌环标准的令牌传递协议； 使用 IEEE802.2 标准定义的 LLC 协议，与 IEEE802 局域网兼容； 数据传输速率达 100Mb/s，采用 4B/5B 编码，信道介质的信号传输速率达到 125Mbaud； 使用分布式时钟方案，信道分配采用定时令牌循环时间。

[简答]简述局域网操作系统的基本服务功能 。

文件服务。局域网操作系统中最重要、最基本的网络服务功能。

打印服务。

数据库服务。

通信服务。

信息服务。

分布式服务。

[简答]简述移动主机登录到外地代理的过程 。

- (1) 外地代理定期广播一个分组，宣布自己的存在及其地址。一个新来的主机可以等到这个消息。
- (2) 移动主机登录到外地代理，并给出其原来所在的地址，当前数据链路层的地址，以及一些安全性信息。
- (3) 外地代理与移动主机的主代理联系，核实移动主机是否真的在那。
- (4) 主代理检查安全性信息，如果核实通过，则通知外地代理继续。
- (5) 当外地代理从主代理处得到确认信息后， 在它的表中加入一个表项， 并通知移动主机， 登陆成功。

[计算]1 万个站点正在竞争使用一时分 ALOHA 信道，信道时隙为 125 μ s，信道时隙为 125 μ s。如果每个站点平均每小时发出 18 次请求，试计算总的信道载荷 G。

解：网络负载 G 是指单位帧时内系统发送的数据帧的平均数量。 每个终端每 200(=3600/18)秒发送 1 次帧，总共有 10000 个终端，因此，总负载是 200 秒发 10000 次帧，平均每秒 50 次帧。每秒 8000 个时隙，所以平均每个时隙发送次数是 $G=50 \div 8000=1/160$ 。

[计算]场 1km、数据率为 10Mb/s 的基带总线 LAN，信号传播速度为 200m/ μ s，试计算：(1)1000b 的帧从发送开始到接收结束的最大时间是多少？ (2)若两相距最远的站点在同一时刻发送数据，则经过多长时间两站发现冲突？

解：(1)首先 1000b 的帧进入信道的时间为： $1000\text{bit}/10\text{Mbps}=100 \mu\text{s}$ ；进入信道后的信号传播时间为： $1000\text{m}/200(\text{m}/\mu\text{s})=5 \mu\text{s}$ ；1000b 的帧从信道接收的时间为： $1000\text{bit}/10\text{Mbps}=100 \mu\text{s}$ ；所以 1000b 的帧从发送开始到接收结束的最大时间为： $100 \mu\text{s}+5 \mu\text{s}+100 \mu\text{s}=205 \mu\text{s}$

(2)发现冲突的时间为最大传播时间的 2 倍，冲突发现前的最大传播时间为 $500\text{m}/200(\text{m}/\mu\text{s})=2.5 \mu\text{s}$ ，所以两站发现冲突的时间为： $2 \times 2.5 \mu\text{s}=5 \mu\text{s}$

[计算]一个 1Km 长的、10Mbps 的 CSMA/CD 局域网 (不是 IEEE802.3)，其信号传播速度为 200m/ μ s，数据帧长度为 256 位，其中包括 32 位首部、校验和以及其他开销。传输成功后的第一个时隙被留给接收方，用来使接收方捕获信道并发送一个 32 位的确认帧。假定不考虑冲突，试计算该局域网的有效数据传递速率 (不包括开销)。

解：发送数据帧 256 位所需时间 $=256\text{bit}/10\text{Mbps}=25.6 \mu\text{s}$

数据帧在信道上的传播时间 $=1000\text{m}/(200\text{m}/\mu\text{s})=5 \mu\text{s}$

共用时间 $=25.6 \mu\text{s}+5 \mu\text{s}=30.6 \mu\text{s}$

回发确认帧 32 位所需时间 $=32\text{bit}/10\text{Mbps}=3.2 \mu\text{s}$

确认帧在信道上的传播时间 $=1000\text{m}/(200\text{m}/\mu\text{s})=5 \mu\text{s}$

共用时间 $=3.2 \mu\text{s}+5 \mu\text{s}=8.2 \mu\text{s}$

故数据有效传输速率为： $(256-32)\text{b}/(30.6+8.2) \mu\text{s}=5.77\text{Mbps}$

[计算]如果环路上有 100 个站点，任意两站间的平均距离位 10m，数据传输速率为 10Mbps，信号传播速率

为 $200\text{m}/\mu\text{s}$ ，若每个站引入 1 位延迟，试计算：(1)两站点间链路的位长度为多少位？(2)整个环路的有效位长度为多少位？

解：(1)两站点间信号的传播时延为： $100 \times 10\text{m} \div 200\text{m}/\mu\text{s} = 0.05\mu\text{s}$ ，所以根据环的比特长度 = 信号传播时延 \times 数据传输速率 + 延迟位数，计算得出两站点间链路长度为： $0.05\mu\text{s} \times 10\text{Mbps} + 100 = 150\text{bit}$

(2)100 个站点的传播时延为： $100 \times 10\text{m} \div 200\text{m}/\mu\text{s} = 5\mu\text{s}$ ，所以根据环的比特长度 = 信号传播时延 \times 数据传输速率 + 延迟位数，计算得出整个环路的有效位长度为： $5\mu\text{s} \times 10\text{Mbps} + 100 = 150\text{bit}$ 。

[计算]长 1km，数据传输速率为 16Mbps 的 802.5 令牌环，信号传播速度为 $200\text{m}/\mu\text{s}$ ，环路上每个站点引入一位延迟。该环的比特长度为 220bit，请问环路上有多少个站点？

解：根据环的比特长度 = 信号传播时延 \times 数据传输速率 + 每站延迟位数 \times 站点数

得出：站点数 = (环的比特长度 - (线路长度 / 信号传播速率) \times 数据传播速率) / 每站延迟位数

$= (220 - (1\text{Km} / 200\text{m}/\mu\text{s}) \times 16\text{Mbps}) / 1$

$= (220 - 5\mu\text{s} \times 10\text{Mbps}) / 1$

$= 140$

所以此环上有 140 个站点。

[计算]已知 FDDI 环上共有 50 个站点，令牌绕环运行一周的传播时延为 20ms，令牌持有时间为 10ms。则该 FDDI 环可取得的最大效率是多少？

解：已知：50 个站点，令牌绕环运行一周的传播时延为 20ms

所以，令牌在两相邻站点间的传播时间是 $20/50 = 0.4\text{ms}$

又有一个站点对令牌持有时间为 10ms

所以，该 FDDI 环可取得的最大效率就是：

$10/(10 + 0.4) \times 100\% = 96\%$

[应用]考虑建立一个 CSMA/CD 网，电缆长 1Km，不用重发器，传输速率为 1Gb/s。电缆中的信号速率是 200000Km/s。请问：最小帧长度是多少？

对于 1km 的电缆，单程传播时间为 $1\text{km} \div 200000\text{km/s} = 5\mu\text{s}$ ，来回路程传播时间为 $2 \times 5\mu\text{s} = 10\mu\text{s}$ 。以 1Gbps 速率工作， $10\mu\text{s}$ 可以发送的比特数为：

$10\mu\text{s} \times 1\text{Gbps} = 1000\text{bit} = 1250$ 字节。所以，最短帧是 1250 字节。

[应用]试比较 10Mb/s 以太网、100Mb/s 以太网和 1Gb/s 以太网的异同点。10Mb/s 以太网升级到 100Mb/s 和 1Gb/s 时，需要解决哪些技术问题？

10Mb/s 以太网、100Mb/s 以太网和 1Gb/s 以太网。

相同点是：相同的帧结构；相同的介质访问控制方法——CSMA/CD；相同的组网方法。

不同点是：数据传输速率不同；采用的传输介质不同；底层编码方式及物理层协议也有所差异。

10Mb/s 以太网升级到 100Mb/s 和 1Gb/s 时，需要解决技术问题有：一是要定义新的物理层标准；而是为了保持最短帧长 64 字节，要提出解决冲突检测的方法；三是在发送短帧时，如何提高效率。

第 9 章 实用网络技术

[选择]帧中继的帧格式类似于 HDLC 的帧格式，帧中继帧格式中没有 控制字段 C 字段。

[选择]下了关于虚电路的叙述中，正确的是 永久虚电路由公共传输网络提供者设置，一经设置便长期存在。

[选择]帧中继的基础是 分组交换技术。

[选择]帧中继网主要采用的传输介质是 光纤。

[选择]ATM 中的信元长度是 固定长度。

[选择]“截获”是一种网络安全攻击形式，所攻击的目标是信息的 保密性。

[选择]那种网络安全攻击以数据的保密性为攻击目标 截获。

[选择]对于网络安全攻击，下面描述中正确的是 对于主动攻击通常可以采取有效的监测和恢复手段进行保护。

[选择]关于加密技术下列说法中，正确的是 传统的加密技术加密密钥和解密密钥相同，而且密钥必须保密，这种方法称为秘密密钥加密。

[选择]将获得信息再次发送以在非授权情况下进行传输，这属于 修改。

[选择]常用的秘密密钥加密算法是 DES。

[选择]DES 中密钥的长度是 56 位。

[选择]防止发送方否认的方式是 数字签名。

[选择]常用的公开密钥加密算法是 RSA。

[填空]X.25、帧中继及 ATM 等都是采用 分组交换 技术的广域网。

[填空]分组交换网络提供 虚电路 和 数据报 两种服务。

[填空]X.25 所规定的虚电路服务属于 面向连接 的 OSI 服务方式。

[填空]X.25 分组及分组格式规定每个分组由 分组头 和 数据信息 两部分组成。

[填空]X.25 协议的数据分组中，P(S)称为 分组发送顺序号；P(R)称为 分组接收顺序号。

[填空]帧中继的帧结构与 HDLC 帧格式不同之处是没有 控制字段。

[填空]ATM 是指 异步传输模式。

[填空]ATM 的信元具有固定的长度，即 53 个字节。其中信头是 5 个字节，信息段是 48 个字节。

[填空]ATM 以分组交换技术为基础，采用 异步时分 的复用工作方式。

[填空]第三层交换技术是综合了第二层 交换 和第三层 路由 的优点，在第三层提供交换能力。

[填空]目前已提出的 LS 交换解决方案有 基于核心模型 和 基于边缘多层混合交换模型。

[填空]Fast IP 技术的主要技术基础是 下一跳解析协议 NHRP。

[填空]Net Flow 技术是基于 核心模型 的 L3 交换方案，目的是提高 路由器 的性能。

[填空]建立虚拟局域网的交换技术包括 端口交换、帧交换 和 信元交换。

[填空]一般情况下，VLAN 之间互连和数据传输仍要借助于路由手段来实现，而对于无法进行路由选择的协议则借助于 交换功能 来实现。

[填空]VPN 是指 虚拟专用网。

[填空]虚拟专用网指的是依靠 Internet 服务提供商 ISP 和网络服务提供商 NSP，在公用网络中建立专用的数据通信网络的技术。

[填空]VPN 的安全技术有 隧道技术、加解密技术 和 密钥管理技术 使用者与设备身份认证技术。

[填空]最常用使用者与设备身份认证技术是 使用者名称与密码 或卡片式认证等。

[填空]目前最有影响的网络管理协议有两个：简单网络管理协议 SNMP 和 公共管理信息服务和公共管理信息协议 CMIS/CMIP。

[填空]网络安全是为了在数据传输期间保护数据并且保证数据的传输是可信的，它强调的是网络中信息或数据的 完整性、可用性 以及 保密性。

[填空]网络安全攻击可分为 主动攻击 和被动攻击。其中 被动攻击 的主要目的是窃听和监视信息的传输并存储；主动攻击 主要是修改数据流或创建一些虚假数据流。

[填空]对于被动攻击通常采取预防手段；对于主动攻击通常采取 监测和恢复 手段。

[填空]网络安全机制有 加密机制、认证机制、数字签名机制 和检测机制。

[填空]对称数据加密技术是指加密和解密过程采用 同一把密钥。

[填空]三重 DES，即 TDEA 使用了三个密钥，并执行了三次 DES 算法，这个函数的执行顺序是 加密-解密-加密。TDEA 的有效密钥长度为 168bit。

[填空]应用广泛的数字签名方法主要有三种：RSA 签名、DSS 签名、Hash 签名。

[填空]Hash 签名是最主要的数字签名方法，也称为数字摘要法或 数字指纹法。

[简答]帧中继的常见应用有哪些？

帧中继即可作为公用网络的接口，也可作为专用网络的接口。常见应用如下：

(1) 局域网的互连。帧中继具有支持不同数据速率的能力，非常适合与处理局域网-局域网的突发数

据流量。基于帧中继的局域网互连，只要局域网内每个用户只网络间有一条带宽足够的线路，则既不用增加物理线路也不占用物理端口，就可以增加端-端线路，而不对用户性能产生影响。

(2) 语音传输。帧中继不仅适用于对时延不敏感的局域网的应用，还可以进行对时延要求较高的低档语音的应用。

(3) 文件传输。适合大流量文件的传输。

[简答]简述 **ATM** 信元的结构，并说明信元头部各字段的作用和意义。

ATM 网络中传输分组称为信元 (Cell)。信元实际上就是分组，具有固定的长度，即总是 53 字节。其中 5 个字节是信头 (Header)，48 个字节是信息段。信头包含各种控制信息，主要是表示信元去向的逻辑地址，另外还有一些维护信息、优先级及信头的纠错码。信息段中包含来自各种不同业务的用户数据，这些数据透明的穿越网络。信元的格式与业务类型无关。

[简答]什么是第三层交换？第三层交换有哪些解决方案？

第三层交换技术是一种新兴的网络互联技术，它综合第二层交换和第三层路由的优点，在第三层提供交换能力。

第三层交换的解决方案分为两类：一类是基于核心模型；另一类基于边缘多层混合交换模型。

[简答]什么是虚拟局域网？建立虚拟局域网的交换技术有哪些？

虚拟局域网 (Virtual LAN, VLAN) 是通过路由和交换设备在网络的物理拓扑基础上建立的逻辑网络。一个 VLAN 可以看作是一组网络节点的集合，这些节点不必位于同一个物理网络中，但可以不受地理位置的限制而像在同一个局域网中那样进行数据通信。

建立虚拟局域网的交换技术包括端口交换 (Port Switch)、帧交换 (Frame Switch) 和信元交换 (Cell Switch) 3 种方式。

端口交换也成为配置交换，现在使用一个或几个通过背板连接的端口交换机，通过软硬件的控制和管理，把交换机上的端口划分成为若干个共享式的互相独立的 VLAN。

帧交换，局域网交换机在每一个端口上提供一个独立的共享介质端口，在此端口上可以共享集线器也可以接单独的一个网络节点。在一个端口上接收到的帧被正确地转发到输出端口上，在寻路和转发是帧不会被破坏的。对于广播帧，可以转发到交换机的所有端口。

信元交换在 ATM 交换机上实现，一个或者多个互联的 ATM 交换机组成的核心系统。ATM 交换机端口上接收到信元后，正确转发到输出端口。

[简答]简述常用的虚拟局域网的划分方法有哪些。各有什么特点？

划分 VLAN 的常用方法有按交换机端口号、按 MAC 地址或者按第三层协议来划分。

按交换机端口号划分 VLAN，通常将交换设备端口进行分组来划分 VLAN。

按 MAC 地址划分 VLAN，是由网管人员指定属于同一个 VLAN 的各网络节点的 MAC 地址。

按第三层协议划分 VLAN，决定成员身份是主要考虑协议类型或网络层地址进行划分。

[简答]什么是虚拟专用网 **VPN**？有什么特点？

VPN 指的是依靠 ISP 和 NSP，在公用网络中建立专用的数据通信网络的技术。

VPN 的特点有：

(1) 安全保障。VPN 通过建立一个隧道，利用加密技术对传输数据进行加密，以保证数据的私有和安全性。

(2) 服务质量保证 (QoS)。VPN 可以针对不同要求提供不同等级的服务质量保证。

(3) 可扩充性和灵活性。VPN 支持通过 Internet 和 Extranet 的任何类型的数据流。

(4) 可管理性。VPN 可以从用户和运营商角度方便进行管理。

[简答]简述 **VPN** 主要采用的四项安全保证技术。

VPN 主要采用隧道技术 (Tunneling)、加解密技术 (Encryption & Decryption)、密钥管理技术 (Key Management) 和使用者与设备身份认证技术 (Authentication)。

[简答]说明网络安全攻击的几种形式。

主要有四种方式：中断、截获、修改和伪造。

中断是以可用性作为攻击目标，它毁坏系统资源，使网络不可用。

截获是以保密性为攻击目标，非授权用户通过某种手段获得对系统资源的访问。

修改是以完整性作为攻击目标，非授权用户不仅获得访问而且对数据进行修改。

伪造是以完整性作为攻击目标，非授权用户将伪造的数据插入到正常传输的数据中。

[应用]请说明帧中继与 X.25 协议的主要差别。

帧中继是继 X.25 后发展起来的数据通信方式。从原理上看，帧中继与 X.25 都同属于分组交换。与 X.25 协议的主要差别有：

- (1) 帧中继带宽较宽。
- (2) 帧中继的层次结构中只有物理层和链路层，舍去了 X.25 的分组层。
- (3) 帧中继采用 D 通道链路接入规程 LAPD(Link Access Procedure on the D-Channel)。X.25 采用 HDLC 的平衡链路接入规程 LAPB。
- (4) 帧中继可以不用网络层而只使用链路层来实现复用和转接。
- (5) 与 X.25 相比，帧中继在操作处理上做了大量的简化。不需要考虑传输差错问题，其中间节点只做帧的转发操作，不需要执行接收确认和请求重发等操作，差错控制和流量均交由高层端系统完成，大大缩短了节点的时延，提高了网内数据的传输速率。

[应用]加入数字签名和验证的文件传输过程是怎样的？如何防止有第三方冒充发送方法送出文件？

只有加入数字签名及验证才能真正实现在公开网络上的安全传输。加入数字签名和验证的文件传输过程如下：

首先发送方用哈希函数从原文得到数字签名，然后采用公开密钥体系用发送方的私有密钥对数字签名进行加密，并把加密后的数字签名附加在要发送的原文后面。

发送方选择一个秘密密钥对文件进行加密，并把加密后的文件通过网络传输到接收方。

发送方用接收方的公开密钥对秘密密钥进行加密，并通过网络把加密后的秘密密钥传输到接收方。

接收方使用自己的私有密钥对密钥信息进行解密，得到秘密密钥的明文。

接收方用秘密密钥对文件进行解密，得到经过加密的数字签名。

接收方用发送的公开密钥对数字签名进行解密，得到数字签名的明文。

接收方用得到的明文和哈希函数重新计算数字签名，并与解密后的数字签名进行对比。如果两个数字签名是相同的，则说明文件在传输过程中没有被破坏。

如果第三方冒充发送方发送了一个文件，因为接收方在对数字签名进行解密时使用的是发送方的公开密钥，只要第三方不知道发送方的私有密钥，则解密出来的数字签名和经过计算的数字签名必然是不相同的。这就提供了一个安全的确认发送方身份的方法。