目　录

第1章　概　述

1.1　复习笔记

一、计算机网络在信息时代中的作用

计算机网络的两个重要功能：

1．连通性

连通性是指计算机网络使上网用户之间都可以交换信息，好像互联网上的用户可以彼此直接连通。

2．共享

共享是指资源共享，如：信息共享、软件共享、硬件共享。

二、互联网概述

1网络的网络

（1）计算机网络的组成

计算机网络（简称网络）由若干结点和连接这些结点的链路组成。

（2）相关概念

①互联网（网络的网络）：网络之间通过路由器互连起来所构成的覆盖范围更大的网络；

②因特网（Internet）：世界上最大的，开放的，由众多网络相互连接而成的特定互联网；

③万维网（WWW）：环球信息网，是互联网所能提供的服务其中之一，是基于互联网运行的一项服务；

④主机：与网络相连的计算机。

2因特网发展的三个阶段

（1）从单个网络ARPANET向互联网发展；

（2）建成三级结构（主干网、地区网、校园或企业网）的互联网；

（3）逐渐形成多层次ISP（互联网服务提供商）结构的互联网。

3因特网的标准化工作及相关组织

（1）所有的因特网标准都是以RFC的形式在互联网上发表。制订互联网的正式标准要经过以下三个阶段：

①互联网草案——有效期6个月，还不算是RFC文档；

②建议标准——从这个阶段开始成为RFC文档；

③互联网标准——达到正式标准并分配编号。

（2）在国际上，有众多的标准化组织负责制定、实施相关网络标准，主要有以下几种：

①国际标准化组织（ISO）：制定的主要网络标准或规范，如OSI参考模型、HDLC等。

②国际电信联盟（ITU）：其前身为国际电话电报咨询委员会（CCITT），其下属机构ITU-T制定了大量有关远程通信的标准。

③国际电气电子工程师协会（IEEE）：世界上最大的专业技术团队，由计算机和工程学专业人士组成。其代表性研究成果是802标准。

三、互联网的组成

1互联网的组成

（1）如图1-1所示，按工作方式可将互联网分为如下两个部分：

①边缘部分：连接在互联网上的所有主机，用户直接使用来进行通信和资源共享；

②核心部分：由大量网络和连接这些网络的路由器组成，为边缘部分提供服务。

图1-1　因特网的边缘部分与核心部分

（2）按功能组成可分为通信子网和资源子网：

①通信子网：由各种传输介质、通信设备和相应的网络协议组成，为网络提供数据传输、交换和控制能力，实现联网的计算机间的数据通信，其中通信子网包括物理层、数据链路层、网络层。

②资源子网：由主机、终端以及各种软件资源、信息资源组成，负责全网的数据处理业务，面向网络用户提供各种网络资源与服务。

2端系统之间的通信方式

边缘部分的主机又称端系统，而计算机之间的通信是指“主机A中的某进程和主机B中的某进程进行通信”，在网络边缘的端系统之间的通信方式主要有以下两种：

（1）客户/服务器（C/S）方式

如图1-2所示，客户（Client）和服务器（Server）是通信中所涉及的两个应用进程，客户（如A）是服务请求方，在知道服务器程序地址的前提下，主动向服务器发起请求服务；服务器（如B）是服务提供方，处理客户发来的请求，且服务器可同时处理多个远地或本地客户的请求。有时还有另外一种浏览器/服务器（B/S）方式，这仍是C/S方式的一种特例。

图1-2　客户服务器工作方式

（2）对等连接（P2P）方式

如图1-3所示，对等连接方式实质上还是使用了C/S方式，但对等连接中的每一台主机既是客户又是服务器，该方式可以支持大量对等用户同时工作。

图1-3　对等连接工作方式

3三种数据交换方式

如图1-4所示，其中ABCD为四个终端设备，从通信资源的分配角度来看，交换是按照某种方式动态分配传输线路的资源，数据交换主要分为三种交换方式：

（1）电路交换

电路交换是建立连接（占用通信资源）→通话（一直占用通信资源）→释放连接（归还通信资源）的过程；像一个管道一样，使得整个报文的比特流连续地从源点到终点。

（2）报文交换

采用存储转发技术，将整个报文先传送到相邻结点，存储下来后再查找转发表，转发到下一个结点的交换方式，是分组交换的前身。

（3）分组交换

采用存储转发技术，将一个报文划分成几个分组后再进行传输，即对单个分组可进行存储与转发。

图1-4　三种交换的比较，P_1～P_4表示4个分组

四、计算机网络在我国的发展（略）

五、计算机网络的类别

1计算机网络的定义

简单来讲，计算机网络是一些相互连接的、以共享资源为目的的、自治的计算机的集合。

2计算机网络的分类

（1）按网络的作用范围可分为：

①广域网WAN；

②城域网MAN；

③局域网LAN；

④个人区域网PAN。

（2）按网络的使用者可分为：

①公用网；

②专用网。

（3）按拓扑结构可分为：

①星形网络；

②总线形网络；

③环形网络；

④网状形网络。

（4）用来把用户接入到互联网的网络可分为：

①本地接入网；

②居民接入网。

六、计算机网络的性能

1计算机网络的性能指标（见表1-1）

表1-1　计算机网络的性能指标

性能指标		解释
速率		连接在计算机网络上的主机在数字信道上传送数据的速率，单位是 bit/s（比特每秒）
带宽		带宽表示单位时间内网络中的某信道所能通过的“最高数据率”
吞吐量		表示单位时间内通过某个网络（或信道、接口）的实际数据量
时延	发送时延	发送时延＝数据帧长度（bit）/发送速率（bit/s）
	传播时延	传播时延＝信道长度（m）/电磁波在信道上的传播速率（m/s）
	处理时延	主机或路由器在收到分组时用于处理所花费的时间，例如差错检验或查找路由表等
	排队时延	分组在进入路由器输入队列中排队等待的时间，往往取决于网络当时的通信量
时延带宽积		时延带宽积＝传播时延×带宽
往返时间 RTT		往返时间 RTT 表示从发送方发送数据开始，到发送方收到来自接收方的确认总共经历的时间
利用率	信道利用率	信道被有效利用（有数据通过）的百分比
	网络利用率	网络利用率：全网络的信道利用率的加权平均值

【注意】信道或网络的利用率过高会产生非常大的时延。

2计算机网络的非性能特征

（1）费用

（2）质量

（3）标准化

（4）可靠性

（5）可扩展性和可升级性

（6）易于管理和维护

七、计算机网络体系结构

1实体、协议、服务、服务访问点

如图1-5表示计算机网络中相邻两层之间的关系。

图1-5　相邻两层之间的关系

（1）实体

任何可以发送或接收信息的硬件或软件进程。

（2）网络协议（简称协议）

协议是控制两个对等实体进行通信的规则的集合，它的三个要素为：

①语法：数据与控制信息的结构或格式；

②语义：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：事件实现顺序的详细说明。

（3）服务

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，本层协议的实现需要下一层提供的服务。

（4）服务访问点

同一系统中相邻两层的实体进行交互的地方即服务访问点SAP。

【注意】协议与服务的区别：

①协议的实现保证了能够向上一层提供服务；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；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。

2ISO/OSI参考模型和TCP/IP参考模型

计算机网络的各层及协议的集合就是网络的体系结构，通常包括两种常见模型：

（1）ISO提出的开放系统互联参考模型OSI/RM（简称OSI参考模型）；

（2）TCP/IP参考模型。

【注意】OSI与TCP/IP参考模型的对比（重点）：

相似之处：

①二者均采用分层的体系结构，且分层的功能也大体相似；

②二者均基于独立的协议栈的概念；

③二者均能实现异构网络的互联。

不同之处：

①OSI精确定义了服务、协议、接口的概念，而TCP/IP在这三个概念上没有明确区分；

②OSI未偏向某种特定的协议，通用性良好，而TCP/IP则是对已有协议的描述；

③OSI在网络层支持无连接和面向连接的服务，而TCP/IP却认为可靠性是端到端的问题，选择在传输层支持无连接和面向连接的服务。

3具有五层协议的体系结构

如图1-6所示为计算机网络的体系结构图，本书后面章节将按照五层协议的体系结构进行讲解。

图1-6　计算机网络体系结构图

（1）物理层

在物理媒体上为数据端设备透明地传送比特流，传输数据的单位是比特。

（2）数据链路层

将网络层交下来的IP数据报组装成帧（Frame）进行传输，还能进行差错控制、流量控制和传输管理。

（3）网络层

负责为分组交换网上的不同主机提供通信服务。

（4）运输层

负责向两个主机中进程之间的通信提供服务。主要两种协议：

①传输控制协议TCP：一种面向连接的、可靠的数据传输服务，其数据传输的单位是报文段；

②用户数据报协议UDP：一种无连接的、尽最大努力传输的服务，其数据传输的单位是用户数据报。

（5）应用层

应用层是体系结构中的最高层，直接为用户的应用进程提供服务。

如图1-7所示说明了应用进程的数据在各层之间的传递过程中所经历的变化。

图1-7　数据在各层之间的传递过程

【注意】需要记住OSI参考模型另外两层的作用：

①会话层：负责管理主机间的会话进程，包括建立、管理及终止进程的会话；

②表示层：处理两个通信系统间交换信息的方式，此外还具有数据压缩、加密和解密等功能。

4TCP/IP的体系结构

事实上，TCP/IP的层次结构已经成为应用广泛的国际标准，它分为应用层、运输层、网际层和网络接口层共四层，如图1-8所示为该结构的应用举例，需要注意的是，用路由器转发分组时，使用的最高层为网际层，并没有应用到上面两层。

图1-8　TCP/IP四层协议的应用举例

1.2　课后习题详解

1计算机网络向用户可以提供哪些服务？

答：计算机网络向用户提供的最主要服务有：数据通信、资源共享，此外还有分布式处理、提高可靠性、负载均衡等功能。

2试简述分组交换的要点。

答：分组交换是报文交换的一种改进，采用存储转发技术；它将较长的报文段划分成比较短的分组，经过路由器的存储转发，再到接收端合并接收；有高效、迅速、可靠等优点。

3试从多个方面比较电路交换、报文交换和分组交换的主要优缺点。

答：（1）电路交换

电路交换是建立连接（占用通信资源）→通话（一直占用通信资源）→释放连接（归还通信资源）的过程；像一个管道一样，使得整个报文的比特流连续地从源点到终点。

优点：数据不会丢失，且数据保持原来的序列，简单可靠；

缺点：建立连接后一直占用信道，使其利用率降低，且对通信终端物理上有要求，难以差错控制。

（2）报文交换

采用存储转发技术，将整个报文先传送到相邻结点，存储下来后再查找转发表，转发到下一个结点的交换方式，是分组交换的前身。

优点：采用存储转发技术，不存在建立连接的时延，用户随时可以发送报文；

缺点：报文交换时的排队时延长，且报文本身长度大，对用作转发的路由器暂存空间要求大。

（3）分组交换

采用存储转发技术，将一个报文划分成几个分组后再进行传输，即对单个分组即可进行存储与转发。

优点：动态分配带宽，逐段占用网络，路由结点交换灵活，网络时延降低，差错减少，可靠性提高；

缺点：存储转发时也存在排队时延。

4为什么说互联网是自印刷术以来人类在存储和交换信息领域中的最大变革？

答：21世纪的一些重要特征就是数字化、网络化和信息化，它是一个以网络为核心的信息时代。我们的日常生活、学习、工作都离不开互联网，可以说互联网是人类自印刷术发明以来在通信方面最大的变革。

5互联网基础结构的发展大致分为哪几个阶段？请指出这几个阶段最主要的特点。

答：因特网的发展大致分为3个阶段：

（1）从单个网络ARPANET向互联网发展，TCP/IP协议初步形成；

（2）建成三级结构（主干网、地区网、校园或企业网）的互联网；

（3）逐渐形成多层次ISP（互联网服务提供商）结构的互联网。

6简述互联网标准制定的几个阶段。

答：所有的因特网标准都是以RFC的形式在互联网上发表。制订互联网的正式标准要经过以下三个阶段：

（1）互联网草案——有效期6个月，还不算是RFC文档；

（2）建议标准——从这个阶段开始成为RFC文档；

（3）互联网标准——达到正式标准并分配编号。

7小写和大写开头的英文名字internet和Internet在意思上有何重要区别？

答：（1）internet（互联网或互连网）是一个通用名词，它泛指由多个计算机网络互连而成的网络。在这些网络之间的通信协议可以是任意的。

（2）Internet（因特网）则是一个专用名词，它指当前全球最大的、开放的、由众多网络相互连接而成的特定计算机网络，它采用TCP/IP协议族作为通信的规则，且其前身是美国的ARPANET。

（3）区别：后者实际上是前者的双向应用。

8计算机网络都有哪些类别？各种类别的网络都有哪些特点？

答：（1）从网络的作用范围进行分类

①局域网LAN：一般用微型计算机或工作站通过高速通信线路相连，覆盖范围小（通常是几十到几千米）；

②城域网MAN：大多采用以太网技术，覆盖范围一般是一个城市，约为5～50km；

③广域网WAN：提供长距离通信，覆盖范围一般为几十到几千公里，也称为远程网；

④个人区域网PAN：个人区域网就是在个人工作地方把属于个人使用的电子设备用无线技术连接起来的网络，其范围大约在10m左右。

（2）从网络的使用者进行分类

①公用网：电信公司出资建造的大型网络；

②专用网：某个部门为本单位的特殊业务的需要而建造的网络。

（3）用来把用户接入到因特网的网络

这种网络称为接入网AN，又称本地接入网或居民接入网。它既不属于因特网的核心部分，也不属于因特网的边缘部分。

（4）按拓扑结构分类：

①星形网络：每个终端或计算机均单独与中央设备相连的网络；

②总线形网络：用传输线将网络中的计算机连接起来；

③环形网络：网络中所有计算机连接形成一个环；

④网状形网络：网络中的每个结点至少有两条线路与其他结点相连。

9计算机网络中的主干网和本地接入网的主要区别是什么？

答：计算机网络中的主干网和本地接入网的主要区别是：

（1）主干网：分布式，提供高速传输、路由器最优化通信及远程覆盖等功能；它的设施共享，使用率高；

（2）本地接入网：集中式，所有的信息流必须经过中央处理设备，是用于把用户接入因特网的网络，分散独立，接入业务种类多，线路施工难度大，设备运行环境恶劣。

10试在下列条件下比较电路交换和分组交换。要传送的报文共x（bit）。从源点到终点共经过k段链路，每段链路的传播时延为d（s），数据率为b（bit/s）。在电路交换时电路的建立时间为s（s）。在分组交换时分组长度为p（bit），且各结点的排队等待时间可忽略不计。问在怎样的条件下，分组交换的时延比电路交换的要小？（提示：画一下草图观察k段链路共有几个结点。）

答：由题可知：

电路交换时延：kd＋x/b＋s；

分组交换时延：kd＋（x/p）×（p/b）＋（k－1）×（p/b）；

其中（k－1）×（p/b）表示k段传输中，有（k－1）次的储存转发延迟。

当s＞（k－1）×（p/b）时，分组交换的时延比电路交换的要小。

11在上题的分组交换网中，设报文长度和分组长度分别为x和（p＋h）（bit），其中p为分组的数据部分的长度，而h为每个分组所带的控制信息固定长度，与p的大小无关。通信的两端共经过k段链路。链路的数据率为b（bit/s），但传播时延和结点的排队时间均可忽略不计。若打算使总的时延最小，问分组的数据部分长度p应取为多大？（提示：参考图1-9的分组交换部分，观察总的时延由哪几部分组成。）

图1-9　11题图（分组交换示意图）

答：忽略排队时间和传播时延，分组交换总时延＝发送时延，共有x/p个分组，每个分组长度为p＋h，故分组交换时延D＝（x/p）×（（p＋h）/b）＋（（k－1）×（p＋h））/b，再求D对p的导数D′（p）＝（－xh）/bp^2＋（k－1）/b，令D′（p）＝0，解得p的取值应该为：

$$p=\sqrt{xh/(k-1)}$$

12因特网的两大组成部分（边缘部分与核心部分）的特点是什么？它们的工作方式各有什么特点？

答：（1）边缘部分由所有连接在互联网上的主机组成，用户直接进行数据通信和资源共享，工作方式一般有客户/服务器（C/S）方式和对等连接（P2P）方式。

（2）核心部分是由大量网络和连接这些网络的路由器组成，为边缘部分提供高速远程分组交换等服务，其工作方式主要有电路交换、分组交换和报文交换。

13客户/服务器方式与P2P对等通信方式的主要区别是什么？有没有相同的地方？

答：（1）客户/服务器方式与对等通信方式的主要区别如表1-2所示。

表1-2　客户/服务器方式与对等通信方式的区别

区别	客户/服务器方式	P2P
处理请求	一点（服务器）对多点（客户）	点对点（对等）
服务器	一直打开的某主机称为服务器	没有专门的服务器
服务请求方和提供方	客户是服务请求方，服务器是服务提供方	对等交换，不做区分
IP 地址	服务器有固定的 IP 地址	参与的主机 IP 可变

（2）相同点：对等通信方式（P2P）本质是客户/服务器方式，实际上是客户/服务器方式双向应用。

14计算机网络有哪些常用的性能指标？

答：计算机网络常用的性能指标包括：

（1）速率（又称数据率或比特率）

连接在计算机网络上的主机在数字信道上传送数据的速率，单位是bit/s（比特每秒）。

（2）带宽

计算机网络中，带宽表示单位时间内网络中的某信道所能通过的“最高数据率”，显然单位和速率单位相同。

（3）吞吐量

表示单位时间内通过某个网络（或信道、接口）的实际数据量。

（4）时延

数据（一个报文或分组，甚至比特）从网络（或链路）的一端传送到另一端所需的时间。主要有以下几种：

①发送时延（传输时延）：主机或路由器发送数据帧所需要的时间（从发送数据帧的第一个比特算起，到该帧的最后一个比特发送完毕的时间）；发送时延＝数据帧长度（bit）/发送速率（bit/s）。

②传播时延：电磁波在信道中传播一定的距离需要花费的时间；传播时延＝信道长度（m）/电磁波在信道上的传播速率（m/s）。

③处理时延：主机或路由器在收到分组时用于处理所花费的时间，例如差错检验或查找路由表等。

④排队时延：分组在进入路由器输入队列中排队等待的时间，往往取决于网络当时的通信量。

综上可知：总时延＝发送时延＋传播时延＋处理时延＋排队时延。

（5）时延带宽积

时延带宽积＝传播时延×带宽。

（6）往返时间RTT

往返时间RTT表示从发送方发送数据开始，到发送方收到来自接收方的确认（接收方收到数据后便立即发送确认）总共经历的时间。

（7）利用率

①信道利用率：信道被有效利用（有数据通过）的百分比；

②网络利用率：全网络的信道利用率的加权平均值。

15假定网络的利用率达到了90%。试估算一下现在的网络时延是它的最小值的多少倍？

答：设网络利用率为U，网络时延为D，网络时延最小值为D_0，且U＝90%，则D＝D_0/（1－U），解得D/D_0＝10；所以，现在的网络时延是它的最小值的10倍。

16计算机通信网有哪些非性能特征？非性能特征与性能指标有什么区别？

答：（1）计算机通信网的非性能特征包括：费用、质量、标准化、可靠性、可扩展和可升级性、易于管理和维护等方面；

（2）非性能特征与性能指标的区别：性能指标和非性能特征分别从定量和定性两个不同的角度来描述计算机通信网络的特征，对于计算机通信网来说两者都很重要。

17收发两端之间的传输距离为1000km，信号在媒体上的传播速率为2×10^8m/s。试计算以下两种情况的发送时延和传播时延：

（1）数据长度为10^7bit，数据发送速率为100kbit/s。

（2）数据长度为10^3bit，数据发送速率为1Gbit/s。

从以上计算结果可得出什么结论？

答：发送时延和传播时延的计算公式：

发送时延＝数据帧长度（bit）/发送速率（bit/s）；

传播时延＝信道长度（m）/电磁波在信道上的传播速率（m/s）；

根据题设条件，可知：

（1）发送时延＝10^7bit/（100×10^3bit/s）＝100s；

传播时延＝1000×10^3m/（2×10^8m/s）＝5ms；

（2）发送时延＝10^3bit/（1×10^9bit/s）＝1μs；

传播时延＝1000×10^3m/（2×10^8m/s）＝5ms；

结论：若数据长度大且发送速率低，则在总时延中，发送时延往往大于传播时延；若数据长度短且发送速率高，则传播时延有可能是总时延中的主要成分。

18假设信号在媒体上的传播速率为2.3×10^8m/s。媒体长度l分别为：

（1）10cm（网络接口卡）

（2）100m（局域网）

（3）100km（城域网）

（4）5000km（广域网）

试计算当数据率为1Mbit/s和10Gbit/s时在以上媒体中正在传播的比特数。

答：媒体中正在传播的比特数即为传播时延带宽积，时延带宽积＝传播时延×数据率；其中，传播时延＝信道长度（m）/电磁波在信道上的传播速率（m/s）；

（1）传播时延＝0.1/（2.3×10^8）≈4.35×10^{-10}；

数据率为1Mbit/s时：比特数＝$4.35\times10^{-10}\times1\times10^6$＝$4.35\times10^{-4}$（bit）；

数据率为10Gbit/s时：比特数＝$4.35\times10^{-10}\times10\times10^9$＝4.35（bit）；

（2）传播时延＝100/（2.3×10^8）＝4.35×10^{-7}；

数据率为1Mbit/s时：比特数＝$4.35\times10^{-7}\times1\times10^6$＝$4.35\times10^{-1}$（bit）；

数据率为10Gbit/s时：比特数＝$4.35\times10^{-7}\times10\times10^9$＝$4.35\times10^3$（bit）；

（3）传播时延＝10^5/（2.3×10^8）＝4.35×10^{-4}；

数据率为1Mbit/s时：比特数＝$4.35\times10^{-4}\times1\times10^6$＝$4.35\times10^2$（bit）；

数据率为10Gbit/s时：比特数＝$4.35\times10^{-4}\times10\times10^{9}=4.35\times10^{6}$（bit）；

（4）传播时延＝（5×10^{6}）/（2.3×10^{8}）＝2.17×10^{-2}；

数据率为1Mbit/s时：比特数＝$2.17\times10^{-2}\times1\times10^{6}=2.17\times10^{4}$（bit）；

数据率为10Gbit/s时：比特数＝$2.17\times10^{-2}\times10\times10^{9}=2.17\times10^{8}$（bit）。

19长度为100字节的应用层数据交给运输层传送，需加20字节的TCP首部。再交给网络层传送，需加上20字节的IP首部。最后交给数据链路层的以太网传送，再加上首部和尾部共18字节。试求数据的传输效率。数据的传输效率是指发送的应用层数据除以所发送的总数据（即应用数据加上各种首部和尾部的额外开销）。

若应用层数据长度为1000字节，数据的传输效率是多少？

答：数据长度为100字节的数据传输效率：100/（100＋20＋20＋18）＝63.3%；

数据长度为1000字节的数据传输效率：1000/（1000＋20＋20＋18）＝94.5%。

20网络体系结构为什么要采用分层次的结构？试举出一些与分层体系结构思想相似的日常生活。

答：（1）分层次的结构可以带来很多好处：

①各层之间独立地实现某种功能，能降低系统复杂度；

②层间影响小，灵活性好；

③结构上可分隔开，各层都可以采用最合适的技术来实现；

④上层单向使用下层提供的服务，易于调试和维护；

⑤能促进标准化工作。

（2）举例：日常工作中物流系统和邮政系统均能体现这种分层思想。

21协议与服务有何区别？有何关系？

答：（1）协议与服务的区别：

①协议是“水平”的，控制对等实体之间通信的规则，服务是“垂直”的，是由下层向上层通过层间接口提供的；

②只有那些能够被高一层实体看得见的功能才能称之为服务；

③协议的实现保证了能够向上一层提供服务，下面的协议对上面的服务用户是透明的。

（2）协议与服务的联系

①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；

②要实现本层协议，还需要使用下面一层所提供的服务；

③只要不改变提供给用户的服务，实体可以任意地改变它们的协议。

22网络协议的三个要素是什么，各有什么含义？

答：协议是控制两个对等实体进行通信的规则的集合，它的三个要素为：

（1）语法：数据与控制信息的结构或格式；

（2）语义：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：事件实现顺序的详细说明。

23为什么一个网络协议必须把各种不利的情况都考虑到？

答：因为网络中的情况是多变的，当发生特殊情况时，若没有考虑到该情况则会使得网络一直处于一种“理想”状态，不能正确地进行处理，例如：两个朋友约好下午3时在某公园门口“不见不散”，这就是一个很不科学的协议，因为如果其中任何一方临时有急事来不了而又无法通知对方时，则另一方按照协议就必须永远等待下去。因此，设计网络协议时，必须考虑到各种不利情况。

24试述具有五层协议的网络体系结构的要点，包括各层的主要功能。

答：（1）应用层：体系结构中的最高层，直接为用户的应用进程提供服务。

（2）运输层：负责向两个主机中进程之间的通信提供服务。主要两种协议：

①传输控制协议TCP：一种面向连接的、可靠的数据传输服务，其数据传输的单位是报文段；

②用户数据报协议UDP：一种无连接的、尽最大努力传输的服务，其数据传输的单位是用户数据报。

（3）网络层：负责为分组交换网上的不同主机提供通信服务。

（4）数据链路层：将网络层交下来的IP数据报组装成帧（Frame）进行传输，还能进行差错控制、流量控制和传输管理。

（5）物理层：在物理媒体上为数据端设备透明地传送比特流，传输数据的单位是比特。

25试举出日常生活中有关“透明”这个名词的例子。

答：透明表示某一个实际存在的事物看起来却好像不存在一样。比如电脑上的应用程序，用户只知道程序的功能，而不知道程序的具体实现，此时，程序实现对用户来讲是“透明”的。

26解释以下名词：协议栈、实体、对等层、协议数据单元、服务访问点、客户、服务器、客户-服务器方式。

答：（1）协议栈：计算机网络中为了完成通信而使用的多种协议按层次顺序组合在一起构成协议栈；

（2）实体：任何可发送或接收信息的硬件或软件进程；

（3）对等层：在网络体系结构中，通信双方实现同样功能的层；

（4）协议数据单元：OSI参考模型中在对等层次之间传送的数据单位；

（5）服务访问点（SAP）：在同一系统中相邻两层的实体进行交互的地方；

（6）客户：通信中的服务请求方；

（7）服务器：通信中的服务提供方；

（8）客户-服务器方式：一种通信方式，客户发起请求，服务器响应请求，并为客户提供相应服务。

27试解释everything over IP和IP over everything的含义。

答：（1）everything over IP：TCP/IP体系结构下，各种网络应用均建立在IP基础上；

（2）IP over everything：TCP/IP体系结构下，IP通过网络接口层可以应用在不同物理网络上。

28假设要在网络上传送1.5MB的文件。设分组长度为1KB，往返时间RTT＝80ms。传送数据之前还需要有建立TCP连接的时间，这时间是2×RTT＝160ms。试计算在以下几种情况下接收方收完该文件的最后一个比特所需的时间。

（1）数据发送速率为10Mbit/s，数据分组可以连续发送。

（2）数据发送速率为10Mbit/s，但每发送完一个分组要等待一个RTT时间才能再发送下一个分组。

（3）数据发送速率极快，可以不考虑发送数据所需的时间。但规定在每一个RTT往返时间内只能发送20个分组。

（4）数据发送速率极快，可以不考虑发送数据所需的时间。但在第一个RTT往返时间内只能发送一个分组，在第二个RTT内可以发送两个分组，在第三个RTT内可以发送四个分组（即$2^{3-1}=2^2=4$个分组）。（这种发送方式见教材第五章TCP的拥塞控制部分。）

答：（1）这些文件的发送时间＝$1.5\times2^{20}\times8$bit/（10×10^6bit/s）＝1.258s；

文件发送的同时也在信道中传播，而最后一个分组的传播时间需要0.5×RTT＝40ms；

则总共需要的时间＝2×RTT＋1.258＋0.5×RTT＝0.16＋1.258＋0.04＝1.458s。

（2）文件需要划分的个数＝1.5MB/1KB＝1536；

从第一个分组到达直到最后一个分组到达要经历1535×RTT＝1535×0.08＝122.8s；

则总共需要的时间＝1.458＋122.8＝124.258s。

（3）在每一个RTT往返时间内只能发送20个分组，文件一共分为了1536个分组，需要76个RTT，76个RTT可以发送76×20＝1520个分组，最后剩下16个分组一次发送完；而最后一次发送的分组到达接收方也需要0.5×RTT；

因此，总共需要的时间＝76.5×RTT＋2×RTT＝6.12＋0.16＝6.28s。

（4）在两个RTT后就开始传送数据，经过n个RTT后就发送了$1＋2＋4＋…＋2^n$个分组，若n＝10，便能发送完所有分组；这样，考虑到建立TCP连接的时间和最后的分组传送到终点需要的时间，现在总共需要的时间＝（2＋10＋0.5）×RTT＝12.5×0.08＝1s。

29有一点对点链路，长度为50km。若数据在此链路上的传播速度为2×10^8m/s，试问链路的带宽应为多少才能使传播时延和发送100字节的分组的发送时延一样大？如果发送的是512字节长的分组，结果又应如何？

答：该链路的传播时延＝（50×10^3）/（2×10^8）＝2.5×10^{-4}s；

当发送100Byte时，发送时时延要与传播时延一样，则带宽为100×8/（2.5×10^{-4}）＝3.2Mbit/s；

当发送512Byte时，发送时时延要与传播时延一样，则带宽为512×8/（2.5×10^{-4}）＝16.384Mbit/s。

30有一点对点链路，长度为20000km。数据的发送速率是1kbit/s，要发送的数据有100bit。数据在此链路上的传播速度为2×10^8m/s。假定我们可以看见在线路上传播的比特，试画出我们看到的线路上的比特（画两个图，一个在100bit刚刚发送时，另一个是再经过0.05s后）。

答：由题可知，数据的传播时延为：2×10^7/（2×10^8）＝0.1s，发送时延为：100/（1×10^3）＝0.1s，则发送时延＝传播时延，故数据在线路上传播时，其比特传输示意图如图1-10所示。

图1-10　数据传输图

31条件同上题。但数据的发送速率该为1Mbit/s。和上题的结果相比较，你可以得出什么结论？

答：当发送速率改为1Mbit/s时，发送时延＝100/（1×10^6）＝1×10^{-4}s，则发送时延＜＜传播时延，此时在开始发送到发送完毕经历的时间短，宏观上看相当于数据一旦发送，整个数据就一起在链路上传播，接收端一点点接收相应的比特数据，直到接收完所有数据。

32以1Gbit/s的速率发送数据。试问在以距离或时间为横坐标时，一个比特的宽度分别是多少？

答：（1）以距离为横坐标时，一个比特的宽度＝（1bit×2×10^8m/s）/（1×10^9bit/s）＝0.2m；

（2）以时间为横坐标，1Gbit/s速率发送数据时，每一个比特的持续时间为10^{-9}s。

33我们在互联网上传送数据经常是从某个源点传送到某个终点，而并非传送过去又再传送回来。那么为什么往返时间RTT是个很重要的性能指标呢？

答：互联网中的数据不总是单向传输的，很多时候需双向交互，这时需要知道往返时间RTT，它包括了中间结点的处理时延、排队时延等，是不可忽略的，因此，RTT也是一项重要的性能指标。

1.3　考研真题详解

1OSI参考模型的第5层（自下而上）完成的主要功能是（　　）。[2019年408统考]

A．差错控制

B．路由选择

C．会话管理

D．数据表示转换

【答案】C

【解析】OSI参考模型分层（自上而下）：应用层、表示层、会话层、传输层、网络层、数据链路层、物理层，所以OSI参考模型自下而上的第五层即自上而下的第三层为会话层，它负责通信主机间的会话的建立，管理和拆除，答案选C。

2TCP/IP参考模型的网络层提供的是（　　）。[2011年408统考]

A．无连接不可靠的数据报服务

B．无连接可靠的数据报服务

C．有连接不可靠的虚电路服务

D．有连接可靠的虚电路服务

【答案】A

【解析】首先，需要知道TCP/IP参考模型的网络层采用的是IP。这样就可以根据IP数据报的首部来判断网络层提供的是什么服务。

①无连接与有连接区分：该协议是否使用连接，只需看其首部有没有建立连接的字段。显然，IP数据报并没有像TCP报文一样（首部含有如SYN、FIN等建立连接的字段）。故IP提供的是无连接的服务。

②不可靠与可靠区分：如果是可靠的，在分组首部中必须含有序号以及校验数据部分的校验和字段，而IP分组中都没有（IP数据报首部中的校验和字段仅仅校验首部，并不校验数据）。故IP提供的是不可靠的服务。

③数据报与虚电路区分：IP分组中头部含有源IP地址和目的IP地址，并不是一个虚电路号，所以网络层采用的是数据报服务。

此外需要记住OSI在网络层支持无连接和面向连接的服务，而TCP/IP却认为可靠性是端到端的问题，它选择在传输层支持无连接和面向连接的服务。

3下列选项中，不属于网络体系结构所描述的内容是（　　）。[2010年408统考]

A．网络的层次

B．每一层使用的协议

C．协议的内部实现细节

D．每一层必须完成的功能

【答案】C

【解析】A项：网络的层次包括如ISO/OSI模型的七层结构，TCP/IP模型的四层结构；

B项：每一层使用的协议，如网络层的IP，传输层的TCP和UDP等；

D项：每一层必须完成的功能，如网络层提供路由选择、网络互联等功能，传输层提供不同主机不同进程之间的通信内容等功能；

以上3个概念在教材中都有详细说明，只有C项中协议的内部实现细节没有提及，因为内部实现细节由工作人员完成，对于用户和程序员来说是透明的，我们并不需要知道。

4在OSI参考模型中，自下而上第一个提供端到端服务的层次是（　　）。[2009年408统考]

A．数据链路层

B．传输层

C．会话层

D．应用层

【答案】B

【解析】概念区分：

①点到点：这里的“点”是指通信子网中的节点，可以是主机，也可以是路由器、交换机等设备。因为从源主机到目标主机中间可能经过多个路由器和交换机，所以每时每刻都是微观的，即只需关注当前节点到下个节点，而不是宏观的源节点到终节点。在OSI参考模型的七层结构中，下面三层包括物理层、数据链路层、网络层都属于点对点的服务。

②端到端：这里的“端”是指端口号，任何一个应用进程都会对应一个端口号，所以端到端的服务又被称为进程到进程的服务（有些教材也称为应用到应用的服务）。从宏观的角度看，端到端是由一段一段的点到点通信构成的。在OSI参考模型中的七层结构中，上面四层包括传输层、会话层、表示层、应用层都属于端到端的服务。综上，自下而上第一个提供端到端服务的层次是传输层，故B正确。

第2章　物理层

2.1　复习笔记

一、物理层的基本概念

物理层并非指具体的传输媒体，而是指屏蔽掉传输媒体和通信手段的差异来传输比特流。

可以将物理层的主要任务描述为确定与传输媒体的接口有关的一些特性，即：

1．机械特性；

2．电气特性；

3．功能特性；

4．过程特性。

二、数据通信的基础知识

1数据通信系统的模型

数据通信系统主要由源系统、传输系统和目的系统组成。

2有关通信的几个基本概念

（1）数据和信号

①数据：传送信息的实体；

②信号：数据的电气或电磁表现，分为连续变化的模拟信号（模拟数据）和离散变化的数字信号（数字数据）。

a．模拟信号：代表信息的参数的取值是连续的。

b．数字信号：代表信息的参数的取值是离散的。

c．码元：代表不同离散数值的基本波形称为码元。在二进制编码中，只有两种码元，一种是状态0，另一种是状态1。

（2）信道相关的概念

①信源：产生和发送数据的源头；

②信宿：接收数据的终点；

③信道：信号的传输媒介；

④三种基本通信方式

a．单向（单工）通信：只能有一个方向的通信而没有反方向的交互；

b．双向交替（半双工）通信：通信的双方都可以发送和接收信息，但不能同时发送和接收；

c．双向同时（全双工）通信：通信的双方可以同时发送和接收信息。

（3）速率和带宽的概念

①速率：单位时间内传输的数据量，可用码元（用一个固定时长的波形信号表示一个k进制数称作码元）传输速率或信息传输速率表示：

a．码元传输速率：单位时间内数字通信系统传输的码元个数，单位是波特（Baud）；

b．信息传输速率：单位时间内数字通信系统传输的二进制码元个数，单位是bit/s。

【注意】若一个码元携带nbit的信息量，则mBaud的码元传输速率对应m×nbit/s的信息传输速率。

②带宽：见第1章定义。

3编码与调制

（1）基带信号、编码、调制和带通信号的基本概念

①基带信号（基本频带信号）：来自信源的信号；

②编码：将数据变为数字信号的过程；

③调制：将数据变为模拟信号的过程。

a．基带调制：仅仅对基带信号的波形进行转换，使其能与信道特性相适应，转换后仍然是基带信号。

b．带通调制：把基带信号的频率范围搬移到较高的频段，并将数字信号转换成模拟信号，使其能更好地在模拟信道中传输。

④带通信号：经过载波调制后的信号。

（2）常用编码方式

数字信号常用编码方式，主要有以下四种（见表2-1和图2-1）：

表2-1　数字信号常用编码方式

不归零制（NRZ）	用正电平代表 1，负电平代表 0 来表示二进制数字，但电平不归零
归零制	用正电平代表 1，负电平代表 0 来表示二进制数字，但电平会归零
曼彻斯特编码	将一个码元分成两部分，码元周期中心向上跳变表示 0，向下跳变表示 1，也可相反定义
差分曼彻斯特编码	码元中心均有跳变，码元开始边界有跳变表示 0，没有跳变表示 1

图2-1　数字信号常用编码方式

（3）常用调制方式

如图2-2所示为最基本的三种调制方法，说明如下：

①调幅（AM）：载波的振幅随基带数字信号而变化；例如，0或1分别对应于无载波或有载波输出；

②调频（FM）：载波的频率随基带数字信号而变化；例如，0或1分别对应于频率f_1或f_2；

③调相（PM）：载波的初始相位随基带数字信号而变化；例如，0或1分别对应于相位0度或180度。

图2-2　三种最基本的调制方法

4与信道传输速率相关的两大定理

（1）奈奎斯特定理

在理想低通（无噪声、带宽有限）的信道中，设信道的带宽为W（Hz），则为防止码间串扰，其信道的极限码元传输率为2WBaud；设每个码元离散电平的数目为V，则信道的极限数据率为$2W\log_2 V$（bit/s）。

（2）香农定理

在带宽受限且有高斯白噪声干扰的信道中，设W为信道的带宽，S为信道所传输信号的平均功率，N为信道内部的高斯白噪声功率，则S/N为信噪比（当信噪比以分贝为单位时，信噪比＝$10\log_{10}$（S/N）（dB）），这种情况下信道的极限数据传输速率C＝$W\log_2$（1＋S/N），单位时bit/s。香农公式表明，信道的带宽或信道中的信噪比越大，信息的的极限传输速率就会越高。

三、物理层下面的传输媒体

传输媒体即传输介质或传输媒介，是数据传输系统中在发送器和接收器之间的物理通路。传输媒体可分为两大类：导引型传输媒体和非导引型传输媒体。

1导引型传输媒体

（1）双绞线

由两根采用一定规则并排绞合且相互绝缘的铜导线组成，绞合减少了相邻导线的电磁干扰；在局域网和传统电话网中普遍使用，价格便宜。双绞线有屏蔽双绞线（STP）和非屏蔽双绞线（UTP）。

（2）同轴电缆

由内导体铜质芯线、绝缘层、网状编织的屏蔽层和塑料外壳组成；广泛用于传输较高速率要求的数据。

（3）光缆

利用光导纤维传递光脉冲来进行通信；通信容量大、传输损耗小、中继距离长、抗雷电和电磁干扰性能好、无串音干扰、保密性好、体积小，重量轻，但价格昂贵，设备要求高。

2非导引型传输媒体

利用无线电波在自由空间的传播可较快地实现多种通信，进行无线传播的常见非导向传输媒体有：

（1）短波通信（高频通信）

依靠电离层的反射，一般应用短波无线电台时是低速传输。

（2）无线电微波通信

微波通信主要有两种方式：

①地面微波接力通信

地面微波接力通信的通信信道容量大、微波传输质量高、可传输电话、电报、图像、数据等信息，但它容易受恶劣天气影响，且通信的隐蔽性和保密性差，维护困难。

②卫星通信

卫星通信的通信距离远，克服了地面微波接力通信距离的限制，覆盖面积广，但它的传播时延大。

此外，还有红外通信、激光通信等非导向传输媒体，不一一赘述。

四、信道复用技术

数据在传输过程中，可以在发送端进行复用，使其传输过程共享一个信道，再在接收端进行分用。

1频分复用（FDM）

如图2-3（a）所示，用户在分配到一定的频带后，通信过程中自始至终都占用这个频带的一种技术。

图2-3　频分复用和时分复用

2时分复用（TDM）

如图2-3（b）所示，将时间划分为一段段等长的时分复用帧，每个用户占用固定的时分复用帧的一种技术。

3统计时分复用（STDM）

如图2-4所示，STDM是一种改进的时分复用，当终端有数据传输才分配到时间片，当一个帧的数据放满了，就发送出去，能明显提高信道利用率。

图2-4　统计时分复用的工作原理

4波分复用（WDM）

波分复用是一种光的频分复用，在发送端用合波器使光中传输多种不同的波长（频率），在接收端用分波器分解不同的光波，如图2-5所示。

图2-5　波分复用的工作原理

5码分复用（CDM）

码分多址（CDMA）是码分复用的一种方式，每一个用户可以在同样的时间使用同样的频带进行通信，各个用户使用经过特殊挑选的不同码型，故各用户之间不会有干扰。使用CDMA的每一个站被指派一个唯一的mbit码片序列，下面举例说明CDMA的工作原理：

设A站点的芯片序列为00011011，则A发送1即发送序列00011011，发送0即发送序列11100100，可以用一种特殊方式表示这种序列（即把0写作－1，1写作＋1来表示站点的码片向量），例如00011011的码片向量S＝（－1－1－1＋1＋1－1＋1＋1）；现有B站点，其码片向量设为T＝（－1－1＋1－1＋1＋1＋1－1）；此时，两个不同站点的码片向量是正交的，即S·T＝0；

现A站点向C站点发送1，B站点向C站点发送0，它们到了公共信道后将进行叠加（线性相加），则此时公共信道上的码片向量为S＋（－T）＝S－T，到达C站点后需进行数据分离，若要得到来自A站点的数据，则计算得S·（S－T）＝1（即A发送的数据为1），计算来自B站点的数据同理。

五、数字传输系统

1早期数字传输系统的缺点

（1）速率标准不统一；

（2）不是同步传输。

2同步光纤网SONET和同步数字系列SDH

SONET是一种数字传输标准，整个同步网络的各级时钟都来自一个非常精确的主时钟，它还为光纤传输系统定义了同步传输的线路速率等级结构；

SDH一般认为是SONET的同义词，但它的基本速率与SONET不同。

六、宽带接入技术

宽带接入技术是为了提高用户的上网速率。

1ADSL技术

非对称数字用户线ADSL技术是用数字技术对现有的模拟电话用户线进行改造，使它能承载宽带数字业务。基于ADSL的接入网由以下三个部分组成：

（1）数字用户线接入复用器DSLAM（包括了许多ADSL调制解调器）；

（2）用户线；

（3）用户家中的一些设施。

2光纤同轴混合网（HFC网）

HFC网是基于有线电视网的一种居民宽带接入网，它除了传送电视节目外，还提供电话、数据和其他宽带交互型业务；它将原来有线电视网主干中的同轴电缆换成了光纤，且每个家庭要接收数字电视信号时需要安装一个机顶盒。

3FTTx技术

（1）FTTx

FTTx是一种实现宽带居民接入网的方案，其中x可代表不同的光纤接入地点；网民所期待的是做到光纤到户FTTH，即将光纤一直铺设到用户家庭，但其价格高昂，且不是每个用户都有这么高的数据要求。

（2）无源光网络PON

为有效利用光纤资源及控制运营和管理成本，在光纤干线和用户之间可以使用不需要配备电源的无源光网络PON，目前最流行的无源光网络有以太网无源光网络EPON和吉比特无源光网络GPON。

2.2 课后习题详解

1物理层要解决哪些问题，物理层的主要特点是什么？

答：（1）物理层要解决的主要问题：

①尽可能屏蔽掉物理设备、传输媒体和通信手段的差异，使数据链路层感觉不到这些差异；

②解决物理连接的建立，维持和释放问题，并在连接各种计算机的硬件设备上传输数据比特流；

③在两个相邻系统之间唯一地标识数据电路。

（2）物理层的主要特点：

①物理层是为了描述传输媒体接口的机械、电气、功能和过程特性的；

②由于物理连接的方式和传输媒体的种类很多，具体的物理协议相当复杂。

2规程与协议有什么区别？

答：规程特指物理层的协议，故在物理层二者没有多大区别。而在其他层不用“规程”，而用“协议”。

3试给出数据通信系统的模型并说明其主要组成构件的作用。

答：如图2-6所示为数据通信系统的模型，其主要构件和作用说明如下：

（1）源系统：一般包括源点和发送器；源点设备（又称信源）产生要传输的数据，且通常生成的数据要通过发送器编码后才能在传输系统中进行传输；

（2）目的系统：包括接收器和终点；接收器接收传输系统传送过来的信号，并将其转换为能够被目的设备处理的信息；终点设备（又称信宿）从接收器获取传送来的信息；

（3）传输系统：在源系统和目的系统之间的传输系统，它可以是简单的传输线，也可以复杂的网络系统。

图2-6 数据通信系统的模型图

4试解释以下名词：数据，信号，模拟数据，模拟信号，基带信号，带通信号，数字数据，数字信号，码元，单工通信，半双工通信，全双工通信，串行传输，并行传输。

答：（1）数据：传送消息的实体；

（2）信号：数据的电气的或电磁表现；

（3）模拟数据：连续变化的数据；

（4）模拟信号：连续变化的信号；

（5）基带信号：来自信源的信号；

（6）带通信号：经过载波调制后的信号；

（7）数字数据：取值仅允许为有限几个离散数值的数据；

（8）数字信号：取值仅允许为有限几个离散数值的信号；

（9）码元：用一个固定时长的信号波形表示一位k进制数，这种代表不同离散数值的基本波形称为码元；

（10）单工通信：只能有一个方向的通信而没有反方向的交互；

（11）半双工通信：通信的双方都可以发送和接收信息，但不能同时发送和接收；

（12）全双工通信：通信的双方可以同时发送和接收信息；

（13）串行传输：逐个比特按照时间顺序传输；

（14）并行传输：多个比特在多个并行信道上同时传输。

5物理层的接口有哪几个方面的特性，各包含些什么内容？

答：物理层的主要任务可描述为确定与传输媒体接口的一些特性，即：

（1）机械特性：指明接口所用接线器的形状和尺寸、引脚数目和排列、固定和锁定装置等；

（2）电气特性：指明在接口电缆的各条线上出现的电压的范围；

（3）功能特性：指明某条线上出现的某一电平的电压表示何种意义；

（4）过程特性：指明对于不同功能的各种可能事件的出现顺序。

6数据在信道中的传输速率受哪些因素的限制？信噪比能否任意提高，香农公式在数据通信中的意义是什么，“比特/秒”和“码元/秒”有何区别？

答：（1）根据香农定理，极限信息传输速$C=W\log_2(1+S/N)$（bit/s），其中W为带宽，S/N为信噪比，可知，数据在信道中的传输速率受到信噪比和带宽的限制；

（2）信噪比S/N不能任意提高，因为受系统发射功率的限制，信号功率S不可能无穷大，且噪声总是存在的，它的功率N也不可能无穷小；

（3）香农公式的意义：只要信息传输速率低于信道的极限信息传输速率就一定可以找到某种办法来实现无差错的传输；

（4）“比特/秒”是信息的传输速率，“码元/秒”是码元的传输速率；它们的关系是：若一个码元携带nbit的信息量，则mBaud的码元传输速率对应m×nbit/s的信息传输速率。

7假定某信道受奈氏准则限制的最高码元速率为20000码元/秒。如果采用振幅调制，把码元的振幅划分为16个不同等级来传送，那么可以获得多高的数据率（bit/s）？

答：最高比特率C＝码元速率×$\log_2$V（bit/s）＝20000×$\log_2$16（bit/s）＝80000（bit/s）。

8假定要用3kHz带宽的电话信道传送64kb/s的数据（无差错传输），试问这个信道应具有多高的信噪比（分别用比值和分贝来表示），这个结果说明什么问题？

答：根据香农公式$C=W\log_2(1+S/N)$（bit/s），可得$S/N=2^{C/W}-1$，其中C＝64000bit/s，W＝3000Hz，则信噪比为：$S/N=2^{64000/3000}-1\approx2642245$；

用分贝表示为：$10\times\log_{10}(S/N)=10\times\log_{10}2642245=64.2$dB；

结果表明这是一个信噪比很高的信道，且用分贝表示信噪比更加直观简明。

9用香农公式计算一下，假定信道带宽为3100Hz，最大信息传输速率为35kbit/s，那么若想使最大信息传输速率增加60%，问信噪比S/N应增大到多少倍？如果在刚才计算出的基础上将信噪比S/N再增大到10倍，问最大信息速率能否再增加20%？

答：根据香农公式$C=W\log_2(1+S/N)$，可得$S/N=2^{C/W}-1$，其中W＝3100Hz，若使最大信息传输速率增加60%，那么$(S/N)_2=2^{C\times(1+0.6)/W}-1=(2^{C/W})^{1.6}-1=(S/N+1)^{1.6}-1$，而由原始的W＝3100Hz，C＝35kbit/s，易得S/N≈2504，所以$(S/N)_2=(S/N+1)^{1.6}-1\approx274215$，故$(S/N)_2/(S/N)\approx274215/2504\approx110$，信噪比S/N应增大到大约110倍。

如果在此基础上将信噪比S/N再增大到10倍，那么$(S/N)_3=274215\times10=2742150$，由香农公式$C=W\log_2(1+S/N)$，可得$C_3=3100\times\log_2(1+2742150)\approx66299$bit/s，而$C_2=1.6\times35000=56000$bit/s，所以最大信息速率增加为：$(C_3-C_2)/C_2=(66299-56000)/56000\times100\%\approx18.4\%$；所以最大信息速率只能再增加18.4%左右。

10常用的传输媒体有哪几种，各有何特点？

答：常见的传输媒体及其特点如下：

（1）双绞线：由采用一定规则并排绞合且相互绝缘的两根铜导线组成，绞合减少了相邻导线的电磁干扰；在局域网和传统电话网中普遍使用，价格便宜；

（2）同轴电缆：由内导体铜质芯线、绝缘层、网状编织的屏蔽层和塑料外壳组成；广泛用于传输较高速率要求的数据；

（3）光缆：利用光导纤维传递光脉冲来进行通信；通信容量大、传输损耗小、中继距离长、抗雷电和电磁干扰性能好、无串音干扰、保密性好、体积小，重量轻，但价格昂贵，设备要求高；

（4）短波通信（高频通信）：依靠电离层的反射，一般应用短波无线电台时是低速传输；

（5）无线电微波通信：微波通信主要有两种方式：

①地面微波接力通信：通信信道容量大、微波传输质量高、可传输电话、电报、图像、数据等信息，但它容易受恶劣天气影响，且通信的隐蔽性和保密性差，维护困难；

②卫星通信：通信距离远，克服了地面微波接力通信距离的限制，覆盖面积广，但它的传播时延大。

11假定有一种双绞线的衰减是0.7dB/km（在1kHz时），若容许有20dB的衰减，试问使用这种双绞线的链路的工作距离有多长，如果要使这种双绞线的工作距离增大到100公里，问应当使衰减降低到多少？

答：使用这种双绞线的链路的工作距离为：20dB/（0.7dB/km）＝28.57km；

如果要使这种双绞线的工作距离增大到100公里，则应当使衰减降到20dB/100km＝0.2dB/km。

12试计算工作在1200nm到1400nm之间以及工作在1400nm到1600nm之间的光波的频带宽度。假定光在光纤中的传播速率为2×10^8m/s。

答：由公式c＝fλ，可得f＝c/λ，则：

1200nm和1400nm波长之间的带宽：

$\Delta f=f_1-f_2=c/\lambda_1-c/\lambda_2=2\times10^8\times(1/1200-1/1400)\times10^9=2.38\times10^4$GHz＝23.8THz；

1400nm和1600nm波长之间的带宽：

$\Delta f=f_1-f_2=c/\lambda_1-c/\lambda_2=2\times10^8\times(1/1400-1/1600)\times10^9=1.786\times10^4$GHz＝17.86THz。

13为什么要使用信道复用技术，常用的信道复用技术有哪些？

答：使用信道复用技术是为了提高系统容量和系统效率；常用的信道复用技术有：

（1）频分复用（FDM）：用户在分配到一定的频带后，通信过程中自始至终都占用这个频带的一种技术；

（2）时分复用（TDM）：将时间划分为一段段等长的时分复用帧，每个用户占用固定的时分复用帧的一种技术；

（3）统计时分复用（STDM）：STDM是一种改进的时分复用，当终端有数据传输才分配到时间片，能明显提高信道利用率；

（4）波分复用（WDM）：是一种光的频分复用，在发送端用合波器使光中传输多种不同的波长（频率），在接收端用分波器分解不同的光波；

（5）码分复用（CDM）：是一种靠不同的编码来区分各路原始信号的复用方式，其中码分多址（CDMA）是码分复用的一种常用方式。

14试写出下列英文缩写的全文，并进行简单的解释。

FDM，TDM，STDM，WDM，DWDM，CDMA，SONET，SDH，STM-1，OC-48。

答：（1）FDM是频分复用，它是用户在分配到一定的频带后，通信过程中自始至终都占用这个频带的一种技术；

（2）TDM是时分复用，它是将时间划分为一段段等长的时分复用帧，每个用户占用固定的时分复用帧的一种技术；

（3）STDM是统计时分复用，它是一种改进的时分复用，当终端有数据传输才分配到时间片，能明显提高信道利用率；

（4）WDM是波分复用，它是一种光的频分复用，在发送端用合波器使光中传输多种不同的波长（频率），在接收端用分波器分解不同的光波；

（5）DWDM是密集波分复用，是使用可见光频谱的带宽特征在单个光纤上同时传输多种光波信号的技术；

（6）CDMA是码分多址，是码分复用的一种常用方式，采用扩频的码分多址技术用户可以在同一时间、同一频段上根据不同的编码获得业务信道，每一个用户可以在同样的时间使用同样的频带进行通信；

（7）SONET是同步光纤网，是光纤数字化传输的美国标准，它为光纤传输系统定义了同步传输的线路速率等级结构；

（8）SDH是同步数字系列，是以SONET为基础制定的国际标准，它简化了复用和分用技术，需要时可直接接入到低速支路，而不经过高速到低速的逐级分用，上下电路方便；

（9）STM-1是第一级同步传递模块，是SDH的基本速率，相当于SONET体系中的OC-3速率；

（10）OC-48是SONET体系中的速率表示，对应于SDH的STM-16速率，常用近似值为2.5Gb/s。

15码分多址CDMA为什么可以使所有用户在同样的时间使用同样的频带进行通信而不会互相干扰？这种复用方法有何优缺点？

答：（1）每一个用户使用了相互正交的不同的码型表示数据，不会发生干扰；

（2）优点：频谱利用率高，容量大；覆盖范围大，有很强的抗干扰能力，CDMA还可提高通信的语音质量和数据传输的可靠性，减少干扰对通信的影响，增大通信系统的容量，降低手机的平均发射功率等等。

（3）缺点：需要为各站分配不同互相正交的码片序列且地域受线路影响，安装时间长等。

16共有四个站进行码分多址CDMA通信。四个站的码片序列为：

A：（－1－1－1＋1＋1－1＋1＋1）；

B：（－1－1＋1－1＋1＋1＋1－1）；

C：（－1＋1－1＋1＋1＋1－1－1）；

D：（－1＋1－1－1－1－1＋1－1）。

现收到这样的码片序列：（－1＋1－3＋1－1－3＋1＋1）。

问哪个站发送数据了？发送数据的站发送的1还是0？

答：设接收到的码片序列为S，站A、B、C、D的码片序列分别为T_1、T_2、T_3、T_4。根据公式

$$S \cdot T \equiv \frac{1}{m}\sum_{i=1}^{m} S_i T_i$$

对站A计算可得：$S \cdot T_1$＝（1/8）（1－1＋3＋1－1＋3＋1＋1）＝1，所以站A发送的数据为1；

同理，计算B、C、D站：

$S \cdot T_2$＝－1，所以站B发送的数据为0；

$S \cdot T_3$＝0，所以站C未发送数据；

$S \cdot T_4$＝1，所以站D发送数据为1.

综上，发送数据的站有A、B、D站，分别发送的是1、0、1，C站没有发送数据。

17试比较ADSL，HFC以及FTTx接入技术的优缺点。

答：（1）ADSL技术：用数字技术对现有的模拟电话用户线进行改造，使它能够承载宽带业务；

优点：成本低，易实现；

缺点：带宽和质量差异性大。

（2）HFC网：是基于有线电视网的一种居民宽带接入网，它除了传送电视节目外，还提供电话、数据和其他宽带交互型业务；

优点：具有很宽的频带，并且能够利用已经有相当大的覆盖面的有线电视网；

缺点：需要大量的资金和时间布置。

（3）FTTx（光纤到x接入点技术）：是一种实现宽带居民接入网的方案，其中x可代表不同的光纤接入地点；

优点：带宽非常宽；

缺点：造价较高，技术复杂，费用高，有时候不能充分利用带宽资源造成浪费。

18为什么在ADSL技术中，在不到1MHz的带宽中却可以使传送速率高达每秒几个兆比特？

答：ADSL采用了DMT调制技术，使得每秒传送一个码元就相当于每秒传送多个比特。

19什么是EPON和GPON？

答：（1）EPON即以太网无源光网络，是在链路层使用以太网协议，利用PON的拓扑结构实现了以太网的接入；

（2）GPON即吉比特无源光网络，采用了通用封装方法GEM，可承载多业务，对各种业务类型都能够提供服务质量保证，是很有潜力的宽带光纤接入技术。

2.3　考研真题详解

1100Base-T快速以太网使用的导向传输介质是（　　）。[2019年408统考]

A．双绞线

B．单模光纤

C．多模光纤

D．同轴电缆

【答案】A

【解析】快速以太网标准100Base-T采用的传输介质是5类无屏蔽双绞线（UTP），答案选A。

2下列选项中，不属于物理层接口规范定义范畴的是（　　）。[2018年408统考]

A．接口形状

B．引脚功能

C．物理地址

D．信号电平

【答案】C

【解析】物理层提供透明的比特流传输，从不关心比特流里面携带的信息。物理层有四大特性，分别为机械特性，电气特性，功能特性，规程特性。AB项，属于机械特性；D项，属于电气特性；C项不是物理层考虑的范围；答案选C。

3下列选项中，不属于OSI体系结构中物理层功能的是（　　）。[北京邮电大学2018研]

A．比特0和1使用何种电子信号表示

B．1个比特持续多长时间

C．传输能否在两个方向上同时进行

D．避免快速发送方“淹没”慢速接收方

【答案】D

【解析】物理层的功能主要是提供透明的比特流传输，为上层数据链路层提供服务。提供二进制数据位流的编码方式，传输持续时间以及确定是双向传输、双向交替传输还是单向传输。而避免快速发送方“淹没”慢速接收方使数据链路层中流量控制需要考虑的问题，不属于物理层的功能。答案选D。

4在图2-7所表示的采用“存储-转发”方式分组的交换网络中所有的链路的数据传输速度为100Mbps，分组大小为1000B，其中分组头大小为20B。若主机H1向主机H2发送一个大小为980000B的文件，则在不考虑分组拆装时间和传播延迟的情况下，从H1发送到H2接受完为止，需要的时间至少是（　　）。[2010年408统考]

图2-7　第4题图

A．80ms

B．80.08ms

C．80.16ms

D．80.24ms

【答案】C

【解析】“存储-转发”的概念：当路由器收到一个分组，先暂时存储下来，再检查其首部，查找转发表，按照首部中的目的地址，找到合适的接口转发出去。因为分组的大小为1000B，其中分组头大小为20B，故每个分组的数据部分为980B，所以大小为

980000B的文件应该拆分为1000个分组进行传送，每一个分组1000B（加上了头部20B），所以一共需要传送1000000B的信息，而链路的数据传输速度为100Mbit/s，即12.5MB/s，所以主机H1传送完所有数据需要的时间是：1000000B/（12.5MB/s）＝80ms。

80ms时恰好最后一个分组从主机H1发出去，此时还没有被主机H2接收。由于题干已经说明所有链路的数据传输速度相同，所以应该走一条最短的路径，才能使得时间最少，从图中可以看出，直线走最短。此时最后一个分组需要经过再次存储-转发（不考虑传播时延），才能到达主机H2，每次存储转发的时间为1000B/（12.5MB/s）＝0.08ms，故两次存储转发需要0.16ms；

综上所述，总时间为：80ms＋0.16ms＝80.16ms。

5在无噪声情况下，若某通信链路的带宽为3kHz，采用4个相位，每个相位具有4种振幅的QAM调制技术，则该通信链路的最大数据传输速率是（　　）。[2009年408统考]

A．12Kbps

B．24Kbps

C．48Kbps

D．96Kbps

【答案】B

【解析】由奈奎斯特定理可得，该通信链路的最高码元传输速率为2×3kHz＝6（kBaud），又由题意可得每个码元有16个有效的离散值，即一个码元携带$n=\log_2 16=4$bit的信息量，因此该通信链路的最大数据传输速率是6×4Kbps＝24Kbps。

第3章　数据链路层

3.1　复习笔记

一、使用点对点信道的数据链路层

1数据链路层的功能

数据链路层的主要功能如下：

（1）为网络层提供服务；

（2）链路管理：数据链路层连接的建立、维持和释放；

（3）帧定界、帧同步和透明传输；

（4）流量控制与差错控制。

2数据链路和帧

（1）数据链路

链路（物理链路）就是一段从一个结点到相邻结点且中间无任何交换结点的物理线路；数据链路（逻辑链路）是把需要实现的通信协议的硬件和软件加到链路上的链路。

（2）帧

帧是数据链路层中的协议数据单元，数据链路层将网络层交下来的数据组成帧发送到网络上，并把接收到的帧中的数据上交给网络层。

3点对点信道的数据链路层的特点

如图3-1所示的三层模型，链路上的通信均可看做是结点（A）和结点（B）之间的通信，且只涉及网络层、数据链路层和物理层。这种点对点通信的主要步骤是：

（1）结点A的数据链路层把网络层交下来的IP数据报添加首部和尾部封装成帧；

（2）结点A把封装好的帧发送给结点B的数据链路层；

（3）若结点B的数据链路层收到的帧无差错，则从收到的帧中提取出IP数据报上交给网络层；否则丢弃。

图3-1　使用点对点信道的数据链路层

4封装成帧

如图3-2所示，将IP数据报作为帧的数据部分并加上首部和尾部可以封装成数据链路层的帧，它的首部和尾部具有帧定界的功能，同时，首部和尾部还包括一些必要的控制信息。

图3-2　用帧首部和帧尾部进行封装成帧

【注意】每一种链路层协议都规定了传输的帧的数据部分的上限，即最大传送单元MTU。

5透明传输

（1）进行透明传输的原因

当数据部分中出现类似于SOH或EOT这种控制字符一样的8比特组合，就会出现帧定界的错误，为了避免这种定界错误，需要进行透明传输。

（2）解决透明传输问题的具体方法

为解决透明传输问题，可以采用以下几种组帧方法：

①字符计数法：如图3-3，在帧的头部使用一个计数字段标明帧内的字符数；

图3-3　字符计数法

②字节（字符）填充法

如图3-4所示，在帧的数据部分发现类似于“SOH”和“EOT”等控制字符时，为避免其定界错误，可以在其前面加上一个转义字符“ESC”，若转义字符也出现在数据部分中，也在其前面加一个转义字符。

图3-4　字节填充法

③零比特填充法

比特填充法允许数据帧包含任意个数的比特，但在发送方的数据链路层的信息位中若出现5个连续的“1”，需要自动在后面添加一个“0”，在接收方进行逆操作，以避免误判帧的首尾标志（01111110）。例如传输数据101111110101时需要添“0”使其为：1011111010101。

6差错检测

（1）差错检测技术提出的原因

这里的差错指的是比特差错，即比特在传输过程中可能会产生差错：1可能会变成0，而0也可能变成1。

【注意】数据链路层只能保证无差错接收，而它由于不需要保证向网络层提供“可靠传输”服务，所以还存在帧丢失、帧重复或帧失序等错误。

（2）循环冗余检验

现举例说明循环冗余校验码的原理：

假设一组数据有k个比特，如M＝101011（k＝6），则循环冗余校验要求在M的后面添加n位冗余码构成k＋n位的帧发送出去，其中n位冗余码可按二进制的模2运算求得，相当于在M后添加n位0，并除以事先商定的长度为n＋1的除数P（假设这里P＝1101），记得到的商为Q，余数为R，此时R就作为冗余码（称为帧检验序列FCS）添加到M后面并发送出去。

如图3-5所示为计算M的冗余码过程，由该计算可得Q＝110110，FCS＝R＝110，则发送的数据为2^nM＋FCS，即101011110，共k＋n＝9位。

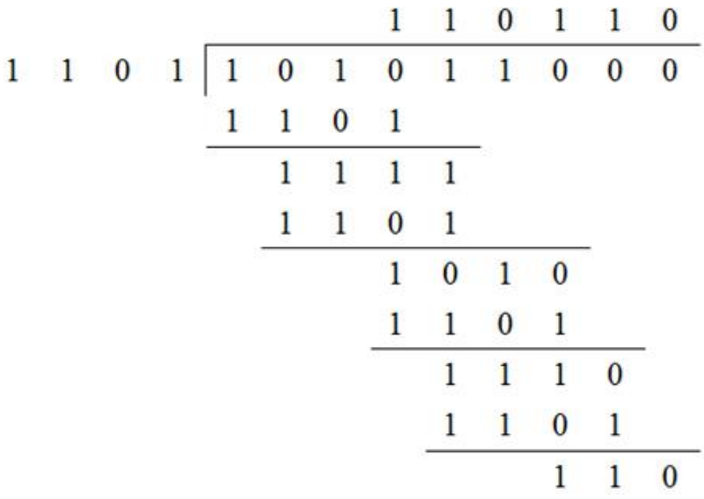

图3-5　冗余码计算举例

二、点对点协议PPP

1PPP协议概述

（1）定义

PPP协议是用户计算机和ISP进行通信时所使用的数据链路层协议，是使用串行线路通信的面向字节的协议。

（2）PPP协议的设计要求

①简单（首要需求）；

②需要使用特定的帧定界符封装成帧；

③需要保证透明传输；

④必须能够在同一条物理链路上同时支持多种网络层协议的运行；

⑤必须能够在多种类型的链路上运行；

⑥必须能够对接收端收到的帧进行差错检测，并丢弃有差错的帧；

⑦必须具有检测功能机制以检测链路是否处于正常工作状态；

⑧必须对每一种类型的点对点链路设置最大传送单元MTU的标准默认值；

⑨必须使通信的两个网络层的实体能够通过协商知道或配置彼此的网络层地址；

⑩必须提供一种方法来协商使用数据压缩算法。

（3）PPP协议的组成

①一个将IP数据报封装到串行链路的方法；

②链路控制协议LCP：用来建立、配置、测试和管理数据链路；

③网络控制协议NCP：PPP允许使用多种网络层协议，NCP为每一个网络层协议建立和配置逻辑连接。

2PPP协议的帧格式

（1）PPP帧的字段

如图3-6所示，PPP帧的主要字段组成如表3-1所示。

表3-1　PPP帧的主要字段组成

标志字段 F	规定用 0x7E（即帧定界符）表示一个帧的开始或结束
地址字段 A	规定为 0xFF（即 11111111）
控制字段 C	规定为 0x03（即 00000011）
协议字段	占 2 个字节，说明信息部分运载的是什么类型的分组，例入 0x0021 表示信息部分是 IP 数据报
信息部分	信息字段的长度是可变的，其范围是大于等于 0 小于等于 1500 字节
帧检验序列 FCS	占 2 个字节，检验区包括地址字段、控制字段、协议字段和信息字段

图3-6　PPP帧的格式

（2）字节填充和零比特填充

当信息字段出现和标志字段一样的比特组合时需要使用填充方法区分它们，前面已经介绍了常见的三种填充方法，而PPP协议中主要应用字节填充和零比特填充方法，需要注意的是这里我们把转义字符定义为0x7D。

3PPP协议的工作状态

如图3-7所示为PPP链路的建立、使用和撤销工作状态图。当链路在静止状态时检测到有载波信号，则建立物理连接，进入链路建立状态；然后LCP开始商定配置选项，成功则进行身份鉴别，失败则返回静止状态；身份鉴别成功或无须鉴别时，采用NCP配置网络层，成功则打开链路，失败则终止链路。

图3-7　PPP协议的状态图

三、使用广播信道的数据链路层

1局域网

（1）局域网的特点

①网络为一个单位所拥有，且地理范围和站点数目均有限；

②具有较高的数据率、较低的时延和较小的误码率；

③具有广播功能和组播功能；

④各个站点的关系是平等的。

（2）局域网的分类

按网络拓扑进行分类，主要分为星形结构、环形结构、总线形结构、星形和总线形结合的复合型结构四种。

（3）共享信道的划分

要使众多用户能够合理而方便的使用共享通信媒体资源，可进行如下划分：

①静态划分信道：例如前面的频分复用、时分复用和波分复用等，它不适合局域网使用；

②动态媒体接入控制（多点接入）：信道并非在用户通信时固定分配给用户；可分为随机接入和受控接入。

（4）以太网的两个标准

以太网采用无连接的工作方式，尽最大努力交付数据，提供不可靠服务，下面是以太网的两大标准：

①DIX Ethernet V2（世界上第一个局域网产品规约）

②IEEE的802.3标准

如图3-8所示，IEEE 802把局域网的数据链路层拆成逻辑链路控制LLC子层和媒体接入控制MAC子层：

a．MAC子层：与接入到传输媒体有关的内容放在MAC子层，它向上层屏蔽对物理层访问的各种差异，并提供对物理层的统一访问接口；

b．LLC子层：与传输媒体无关，向网络层提供无确认无连接、面向连接、带确认无连接、高速传送等连接服务。

图3-8　局域网数据链路层分层

（5）适配器

计算机与外界局域网的连接需要通过通信适配器，它装有处理器和存储器，能进行数据串行传输和并行传输的转换，且适配器在接收和发送各种帧时不使用计算机的CPU。

2CSMA/CD协议

（1）概述

在总线结构的局域网或半双工网络环境中，当有两个或者多个用户同时发送信息，可能会产生冲突，为解决这种冲突，可以采用载波侦听多路访问/碰撞检测（CSMA/CD）协议。

（2）CSMA/CD工作流程

CSMA/CD工作流程可概括为“先听后发、边听边发、冲突停发、随机重发”，具体的为：

①适配器将准备好的以太网帧放入缓存中，并开始侦听；

②若侦听到信道空闲，则开始传输该帧；若侦听到信道忙，则等待至空闲再传输；

③在传输过程中继续侦听其他适配器是否也有发送，若在整个传输过程中没有侦听到其他数据的发送，则传输成功，否则停止传输，并传输一个48bit的拥塞信号；

④终止传输后采用截断二进制指数退避算法等待一段随机时间后返回到第②步。

（3）传播时延对载波侦听的影响

如图3-9所示，设τ为单程的传播时延，可看出，最先发送数据帧的A站，在发送数据帧后至多经过时间2τ就可知道所发送的数据帧是否遭受了碰撞；称以太网端到端往返时间2τ为争用期（碰撞窗口）。

图3-9　传播时延对载波监听的影响

（4）截断二进制指数退避算法

用于解决碰撞所采用的截断二进制指数退避算法如下：

①确定基本退避时间，一般取争用期2τ；

②设重传次数为k，且k≤10，即重传次数k＝min[重传次数，10]；

③从离散的整数集合[0，1，…，（2^k－1）]中随机取出一个数r，重传的退避时间＝2rτ；

④当重传达16次仍不能成功时，则丢弃该帧，并向高层报告。

【注意】截断二进制指数退避算法使得重传的退避时间随重传次数的增大而增大，从而减少发送碰撞的概率。

3使用集线器的星形拓扑

（1）使用集线器的双绞线以太网

如图3-10所示，采用星形拓扑的以太网中心增设了一种叫集线器的可靠性非常高的设备。

图3-10　使用集线器的双绞线以太网

（2）集线器的特点

①使用集线器的以太网在逻辑上仍是一个总线网，各站共享逻辑上的总线，使用CSMA/CD协议；

②一个集线器有许多接口，像一个多接口的转发器；

③集线器工作在物理层，它的转发为简单转发，即收到什么就转发什么；

④集线器采用了专门的芯片，进行自适应串音回波抵消。

4以太网的信道利用率

如图3-11所示，要提高以太网的信道利用率，就必须减小τ与T_0之比。在以太网中定义了参数$\alpha=\tau/T_0$（以太网单程端到端时延τ与帧的发送时间T_0之比），且极限信道利用率$S_{max}=T_0/(\tau+T_0)=1/(1+\alpha)$。

图3-11　以太网的信道被占用的情况

5以太网的MAC层

（1）MAC层的硬件地址

在局域网中，硬件地址又称为物理地址或MAC地址；当适配器每从网上收到一个MAC帧，就用硬件检查其目的地址，看是否是发往本站的帧；所有的适配器必须识别以下三种帧中的①②：

①单播帧（一对一）：收到的帧的MAC地址与本站的硬件地址相同；

②广播帧（一对全体）：发送给本局域网上所有站点的帧（全1地址）；

③多播帧（一对多）：发送给本局域网上部分站点的帧。

（2）MAC帧的格式

①字段说明

如图3-12所示为以太网MAC帧的组成，现对各字段进行说明（见表3-2）：

表3-2　MAC帧的组成

字段	解释
目的地址和源地址	各占 6 字节，存储发往的地址和源地址
类型	占 2 个字节，标识上一层使用的协议
数据字段	长度为 46～1500 字节，小于 46 字节时在后面添加填充字段，以便成为 64 字节的有效帧
帧检验序列 FCS	占 4 字节，存储循环冗余校验的冗余码

图3-12　以太网V2的MAC帧格式

②无效的MAC帧

a．帧的长度不是整数个字节；

b．用收到的帧检验序列FCS查出有差错；

c．收到的帧的MAC客户数据字段的长度不在46～1500字节之间。

四、扩展的以太网

1在物理层扩展以太网

在物理层扩展以太网通常是对物理线路或物理设备进行拓展，使以太网的覆盖范围更广，常见有两种方式：

（1）使用光纤与光纤调制解调器扩展以太网；

（2）使用多个集线器扩展以太网。

2在数据链路层扩展以太网

（1）数据链路层扩展以太网的方法

在数据链路层扩展以太网主要是利用网桥（现在是以太网交换机），根据收到的以太网MAC帧的目的地址进行转发和过滤。

（2）以太网交换机

①以太网交换机的工作原理

以太网交换机的实质是多端口的网桥，它检测从端口收到的数据帧的源和目的MAC地址，并与系统内部的动态查找表比较，若地址不在该表中则加入该查找表，并将数据帧发送到相应的目的端口。

②以太网交换机的特点

a．采用全双工工作模式，每个端口都与单个主机相连；

b．它是一种即插即用设备，通过自学习建立动态查找表；

c．独占传输媒体的带宽，且每一对相互通信的主机能无碰撞地传输数据。

（3）以太网交换机的自学习功能

如图3-13所示，举例说明以太网交换机的自学习功能如下：

以太网交换机有四个端口1、2、3、4分别连接MAC地址为A、C、B、D的四台计算机，当A从端口1向B发送一帧，查找表此时为空，则记录MAC地址A与对应端口1；之后向除端口1外的所有端口进行广播，只有B能够正确接收，则记录MAC地址B与对应的端口3。

图3-13　以太网交换机的交换表

3虚拟局域网

虚拟局域网VLAN是由一些具有某些共同需求的局域网网段构成的与物理位置无关的逻辑组。

五、高速以太网

1常见以太网传输介质

如表3-3所示为常见以太网的传输介质及其适用情况，解释“参数”栏中各符号含义：10表示数据率（单位是Mbit/s），BASE表示介质上的信号为基带信号（即基带传输，采用曼彻斯特编码），数字5表示最大段长为500米，2表示200米（实际上是185米），T表示双绞线，FL表示光纤，需要记住这些参数的含义。

表3-3　传输介质及其适用情况

参数	10BASE5	10BASE2	10BASE-T	10BASE-FL
传输媒体	基带同轴电缆（粗缆）	基带同轴电缆（细缆）	非屏蔽双绞线	光纤对
编码	曼彻斯特编码	曼彻斯特编码	曼彻斯特编码	曼彻斯特编码
拓扑结构	总线形	总线形	星形	点对点
最大段长	500m	185m	100m	2000m
最多结点数目	100	30	2	2

2100BASE-T以太网

100BASE-T是在双绞线上传送100Mbit/s基带信号的星形拓扑以太网，它又称为快速以太网；在全双工或半双工方式下工作，半双工下使用CSMA/CD协议，全双工下不使用CSMA/CD协议以保证不发生冲突。

3吉比特以太网

吉比特以太网又叫千兆以太网，允许在1Gbit/s下用全双工和半双工两种方式工作，半双工下使用CSMA/CD协议，与10BASE-T和100BASE-T技术向后兼容。

410吉比特和100吉比特以太网

10GE的帧格式与10Mbit/s，100Mbit/s和1Gbit/s以太网的帧格式完全相同，并保留了802.3标准规定的以太网最小帧长和最大帧长，工作在全双工方式下，不使用CSMA/CD协议，并使用光纤作为传输媒体；

100GE工作在全双工方式下，不使用CSMA/CD协议，使用单模光纤传输时，可以达到40km的传输距离。

3.2　课后习题详解

1数据链路（即逻辑链路）与链路（即物理链路）有何区别？“电路接通了”与“数据链路接通了”的区别何在？

答：（1）链路（物理链路）就是一段从一个结点到相邻结点且中间无任何交换结点的物理线路；数据链路（逻辑链路）是把需要实现的通信协议的硬件和软件加到链路上的链路；

（2）“电路接通了”表示链路两端的结点交换机已经开机，物理连接已经能够传送比特流了。但是，数据传输并不可靠。在物理连接的基础上，再建立数据链路连接，才是“数据链路接通了”，此时数据链路连接才具有检测、确认和重传等功能。

2数据链路层中的链路控制包括哪些功能？试讨论数据链路层作为可靠的链路层有哪些优点和缺点。

答：（1）数据链路层中的链路控制功能主要包括：链路管理、帧定界、流量控制、差错控制、将数据和控制信息分开、透明传输、寻址等；

（2）优点：通过重传，帧编号和确认机制为上一层提供了可靠的数据传输服务；

（3）缺点：降低了通信效率，尤其是在通信环境本身优质的情况下。

3网络适配器的作用是什么？网络适配器工作在哪一层？

答：（1）网络适配器的作用：网络适配器装有处理器和存储器，能进行数据串行传输和并行传输的转换；当适配器收到正确的帧时，它将其交付给协议栈中的网络层，当计算机要发送IP数据报时，就由协议栈把IP数据报向下交给适配器，组装成帧后发送到局域网，当适配器收到有差错的帧时，就把这个帧丢弃而不必通知计算机。

（2）网络适配器工作在物理层和数据链路层。

4数据链路层的三个基本问题（封装成帧、透明传输和差错检测）为什么都必须加以解决？

答：（1）封装成帧：封装成帧能在数据的前后分别添加首部和尾部，且它是分组交换的必然要求；

（2）透明传输：为了避免数据中的符号和帧定界符混淆，需进行透明传输；

（3）差错检测：数据在传输过程中可能会产生差错，为了保证数据可靠性，需要进行差错检测。

5如果在数据链路层不进行封装成帧，会发生什么问题？

答：如果在数据链路层不进行帧定界，将无法区分分组与分组，也无法区分分组的控制信息和数据，从而导致帧数据错误，造成数据混乱、通信失败。

6PPP协议的主要特点是什么？为什么PPP不使用帧的编号？PPP适用于什么情况？为什么PPP协议不能使数据链路层实现可靠传输？

答：（1）PPP协议的主要特点：

①点对点协议，既支持异步链路，也支持同步链路，且只支持全双工链路；

②PPP是面向字节的；

③PPP的两端可以运行不同的网络层协议，但仍然可以使用同一个PPP进行通信。

（2）PPP不使用帧的编号的原因：

①PPP协议最基本的特点就是简单，不使用帧编号能使数据链路层的开销小一些；

②数据链路层的可靠传输并不能保证网络层的可靠，所以没有必要使用帧的编号保证其可靠性；

③PPP协议在帧格式中有帧检验序列FCS字段保证无差错接受。

（3）PPP协议适用于点对点线路的传输，负责用户计算机和ISP的通信。

（4）可靠的传输由传输层的TCP协议负责，数据链路层的PPP协议进行差错检测，只能保证无差错接收，无法实现可靠传输。

7要发送的数据为1101011011，采用CRC的生成多项式是P（X）＝X^4＋X＋1，试求应添加在数据后面的余数。

数据在传输过程中最后一个1变成了0，问接收端能否发现？

若数据在传输过程中最后两个1都变成了0，问接收端能否发现？

采用CRC检验后，数据链路层的传输是否就变成了可靠传输？

答：根据给出的生成多项式，可得除数为10011，用11010110110000除以10011得到冗余码（余数）为1110，把它添加在要发送的数据后面一起发送出去。

（1）数据在传输过程中若最后一个1变成了0，则应该用11010110101110除以10011，余数为011，不为0，接收端可以发现差错；

（2）数据在传输过程中若最后两个1都变成了0，则应该用11010110001110除以10011，余数为101，不为0，接收端可以发现差错；

（3）可靠的传输由传输层的TCP协议负责，数据链路层使用CRC进行差错检测，只能保证无差错接收，无法实现可靠传输。

8要发送的数据为101110，采用CRC的生成多项式是P（X）＝X^3＋1，试求应添加在数据后面的余数。

答：M＝101110，模2运算后为101110000，与除数P＝1001相除后得R＝011，所以应该添加在数据后面的余数为011。

9一个PPP帧的数据部分（用十六进制写出）是7D 5E FE 27 7D 5D 7D 5D 65 7D 5E。试问真正的数据是什么（用十六进制写出）？

答：PPP帧格式采用特殊的字符填充法。具体做法：将0x7E转变成为（0x7D，0x5E），将0x7D转变成为（0x7D，0x5D）。因此，反推出真正的数据是7E FE 27 7D 7D 65 7E。

10PPP协议使用同步传输技术传送比特串0110111111111100。试问经过零比特填充后变成怎样的比特串？若接收端接收到的PPP帧的数据部分是000111011111101111110110，问删除发送端加入的零比特后变成怎样的比特串？

答：零比特填充法是当进行扫描的时候，每遇到5个连续的1，即插入一个0；读取的时候，每扫描到5个连续的1，即删除后面接着的一个0。因此，经过填充的比特串为：011011111011111000（加上下划线的0是填充的），经过删除的比特串为：000111011111_11111_110（下划线表示删除了0）。

11试分别讨论以下各种情况在什么条件下是透明传输，在什么条件下不是透明传输。（提示：请弄清什么是“透明传输”，然后考虑能否满足其条件。）

（1）普通的电话通信。

（2）互联网提供的电子邮件服务。

答：（1）由于电话系统的带宽有限，而且还有失真，因此电话机两端的输入声波和输出声波是有差异的，从“传送声波”这个意义上讲，普通的电话通信并不是透明传输。但对“听懂说话的意思”来讲，基本上是透明传输，但有时个别语音会听错或者听不清，这时就不是透明传输。

（2）电子邮件有时是透明传输，但有时又不是。因为国外有些邮件服务器为了防止垃圾邮件，对来自某些域名的邮件一律阻拦，这就不是透明传输。

12PPP协议的工作状态有哪几种？当用户要使用PPP协议和ISP建立连接进行通信时，需要建立哪几种连接？每一种连接解决什么问题？

答：（1）PPP协议的工作状态有：链路静止状态，链路建立状态，鉴别状态，网络层协议状态，链路打开状态和链路终止状态。

（2）使用PPP协议和ISP需建立的连接：链路静止、链路建立、鉴别、网络层协议、链路打开。

（3）链路静止时，在用户PC和ISP的路由器之间并不存在物理层的连接。链路建立时，目的是建立链路层的LCP连接，此阶段双方进行协商。鉴别时，只允许传送LCP协议的分组、鉴别协议的分组以及监测链路质量的分组，若鉴别身份成功则进入网络层协议状态。网络层协议连接协商网络层协议，PPP链路两端的网络控制协议NCP根据网络层的不同协议互相交换网络层特定的网络控制分组。链路打开时，链路的两个PPP端点可以彼此向对方发送分组，直到某一方希望终止为止。

13局域网的主要特点是什么？为什么局域网采用广播通信方式而广域网不采用呢？

答：（1）局域网的主要特点是：

①网络为一个单位所拥有，且地理范围和站点数目均有限；

②具有较高的数据率、较低的时延和较小的误码率；

③具有广播功能和组播功能；

④各个站点的关系是平等的。

（2）局域网通常进行一对多的访问，随机使用信道，共享通信媒体，适合采用广播通信，广域网由更大的地理空间、更多的主机构成，若要将广播用于广域网，易产生广播风暴，甚至会导致网络无法运行。

14常用的局域网的网络拓扑有哪些种类？现在最流行的是哪种结构？为什么早期的以太网选择总线拓扑结构而不使用星形拓扑结构，但现在却改为使用星形拓扑结构？

答：（1）常用的局域网的网络拓扑分为：星形网，环形网，总线网和树形网；

（2）现在最流行的是星形网；

（3）早期的以太网选择总线拓扑结构而不使用星形拓扑结构，但现在却改为使用星形拓扑结构的原因是：当时很可靠的星形拓

扑结构较贵，人们都认为无源的总线结构更加可靠，事实上总线形结构存在诸多问题，技术日益成熟、成本逐渐降低的星形结构逐渐成为主流。

15什么叫做传统以太网？以太网有哪两个主要标准？

答：（1）传统以太网表示最早流行的10Mbit/s速率的以太网，采用半双工工作模式，及CSMA/CD的方式来传输数据。

（2）以太网的两个主要标准是：DIX Ethernet V2与IEEE 802.3标准。

16数据率为10Mbit/s的以太网在物理媒体上的码元传输速率是多少码元/秒？

答：以太网使用曼彻斯特编码，这意味着发送每一位数据都占用两个信号周期，所以码元传输速率是数据率的两倍。标准以太网的数据速率是10Mbit/s，则码元传输速率是20M码元/秒。

17为什么LLC子层的标准已制定出来了但现在却很少使用？

答：市场上的TCP/IP体系经常使用的局域网只剩下DIX Ethernet V2而不是IEEE 802.3标准中的局域网，因此，IEEE 802委员会制定的逻辑链路控制子层LLC的作用已经消失，现在已经很少使用。

18试说明10BASE-T中的“10”“BASE”和“T”所代表的意思。

答：“10”表示10Mbit/s的数据率；“BASE”表示连接线上的信号是基带信号；“T”代表双绞线。

19以太网使用的CSMA/CD协议是以争用方式接入到共享信道。这与传统的时分复用TDM相比优缺点如何？

答：CSMA/CD是一种动态的媒体随机接入共享信道方式，而传统的时分复用TDM是一种静态的划分信道，TDM按时隙固定分配信道，当用户没有数据要传送时，信道在该用户时隙就浪费了，就此而言CSMA/CD更加灵活；但因为CSMA/CD是用户共享信道，所以当同时有多个用户需要使用信道时会发生碰撞，降低信道利用率，而TDM中用户在分配的时隙中不会与别的用户发生冲突。事实上，当网络上负载较轻时，CSMA/CD协议很灵活；但网络负载很重时，TDM效率就很高。

20假定1km长的CSMA/CD网络的数据率为1Gbit/s。设信号在网络上的传播速率为200000km/s。求能够使用此协议的最短帧长。

答：当一个站在发送数据后，最迟要经过两倍的端到端的传播时延，才能检测到是否发生了碰撞。

对于1km电缆，单程端到端传播时延为：$\tau=1\div200000=5\times10^{-6}=5\mu s$，则端到端往返时延为：$2\tau=10\mu s$。

为了能按照CSMA/CD工作，数据帧的发送时延不能小于10μs，以1Gbit/s速率工作，10μs可发送的比特数为：$（10\times10^{-6}s）\times（1.0\times10^{9}bit/s）=10000bit$。

因此，能够使用此协议的最短帧长为10000bit或1250字节。

21什么叫做比特时间，使用这种时间单位有什么好处？100比特时间是多少微秒？

答：（1）1比特时间就是发送1比特所需的时间；

（2）这种时间单位与数据率密切相关；

（3）对10Mbit/s以太网，100比特时间是10微秒。

22假定在使用CSMA/CD协议的10Mbit/s以太网中某个站在发送数据时检测到碰撞，执行退避算法时选择了随机数r=100。试问这个站需要等待多长时间后才能再次发送数据？如果是100Mbit/s的以太网呢？

答：10Mbit/s以太网中争用期定为51.2us，重传应推后的时间为r倍的争用期。对于10Mbit/s的以太网来说，等待的时间为：100×51.2us=5.12ms。

同理，100Mbit/s的以太网中争用期定为5.12us，等待时间为：100×5.12us=512us。

23下列公式表示，以太网的极限信道利用率与连接在以太网上的站点数无关。能否由此推导出：以太网的利用率也与连接在以太网上的站点数无关？请说明你的理由。

$S_{max}=T_0/（\tau+T_0）=1/（1+\alpha）$

答：不能。以太网的极限信道利用率是假设以太网上的各站发送数据都不会产生碰撞。这是一种理想化的情况，而实际上的以太网有多个站同时工作时发送数据的时刻是随机的，就可能发生碰撞，站点数越多，产生碰撞的可能性越大，信道的利用率越低，所以以太网的利用率也与连接在以太网上的站点数有关。

24假定站点A和B在同一个10Mbit/s以太网网段上。这两个站点之间的传播时延为225比特时间。现假定A开始发送一帧，并且在A发送结束之前B也发送一帧。如果A发送的是以太网所容许的最短的帧，那么A在检测到和B发生碰撞之前能否把自己的数据发送完毕？换言之，如果A在发送完毕之前并没有检测到碰撞，那么能否肯定A所发送的帧不会和B所发送的帧发生碰撞？（提示：在计算时应当考虑到每一个以太网帧在发送到信道上时，在MAC帧前面还要增加若干字节的前同步码和帧定界符）

答：假设在时间t=0时，A开始传输一帧，由于MAC帧最小帧长为64字节，再加上前同步码和帧定界符共64+8=72字节，则A发送完毕需要72×8=576比特时间；又因为t=225比特时间时，A发送的第一个比特能到达B站点，此时B能够检测到A在发送数

据，故当t≤224比特时间，B发送了数据，A就一定能在发送完毕之前检测到碰撞，如果A在发送完毕之前并没有监测到碰撞，那么就能肯定A所发送的帧不会和B发送的帧发生碰撞。

25在上题中的站点A和B在t＝0时同时发送了数据帧。当t＝255比特时间，A和B同时检测到发生了碰撞，并且在t＝225＋48＝273比特时间完成了干扰信号的传输。A和B在CSMA/CD算法中选择不同的r值退避。假定A和B选择的随机数分别是r_A＝0和r_B＝1。试问A和B各在什么时间开始重传其数据帧？A重传的数据帧在什么时间到达B？A重传的数据会不会和B重传的数据再次发生碰撞？B会不会在预定的重传时间停止发送数据？

答：以太网的争用期为512比特时间，以太网还规定了帧间最小间隔96比特时间，若适配器检测到信道空闲，即在96比特时间内没有检测到信道上有信号，就发送这个帧。因此，有

t＝0时，A和B开始传输；

t＝225时，A和B检测到碰撞；

t＝273时，A和B结束干扰信号的传输；

t＝273＋225＝498时，B的最后一比特到达A，A检测到空闲信道；

t＝498＋96＝594时，A开始传输；

t＝273＋512＝785时，B再次检测信道；

t＝594＋225＝819时，A的信号到达B；

t＝785＋96＝881时，如果B没有监测到碰撞，B开始发送数据。

因为在B安排重传时间881比特时间前，A的重传信号在819比特时间到达了B，所以在A重传数据的时候B暂停传输，这样A和B就不会冲突。

B会在预定的重传时间停止发送数据。

26以太网上只有两个站，它们同时发送数据，产生了碰撞。于是按截断二进制指数退避算法进行重传。重传次数记为i，i＝1，2，3，…。试计算第1次重传失败的概率、第2次重传失败的概率、第3次重传失败的概率，以及一个站成功发送数据之前的平均重传次数I。

答：把重传的次数从1开始编号，第i次重传的含义是已经产生了i次碰撞，在第i次可选择的整数集合[0，1，…，2^i-1]中，仍然同时选择了同一个数值，这样的概率是$1/2^i$。因此：

（1）设第i次重传失败的概率为P_i，则可知$P_i=1/2^k$，k＝min[i，10]。

则$P_1=2^{-1}=0.5$；$P_2=2^{-2}=0.25$；$P_3=2^{-3}=0.125$。

（2）第i次成功发送出去的概率

$P[传送第i次成功]=P[第1次传送失败]\times P[第2次传送失败]\ldots P[第i-1次传送失败]\times P[第i次传送成功]=2^{-1}\times 2^{-2}\times\ldots\times 2^{-(i-1)}\times(1-2^{-i})$

所以平均重传次数$I=1\times(1-1/2)+2\times(1/2)\times(1-1/2^2)+\ldots=1+1/2+(1/2)\times(1/2^2)+\ldots\approx 1.64$。

27有10个站连接到以太网上。试计算以下三种情况下每一个站所能得到的带宽。

（1）10个站都连接到一个10Mbit/s以太网集线器；

（2）10个站都连接到一个100Mbit/s以太网集线器；

（3）10个站都连接到一个10Mbit/s以太网交换机。

答：所有连接在这个集线器上的站点共享信道；交换机的每个端口都有一条独占的带宽，因此：

（1）10个站共享10Mbit/s，每个站得到的带宽为1Mbit/s；

（2）10个站共享100Mbit/s，每个站得到的带宽为10Mbit/s；

（3）每一个站独占10Mbit/s。

2810Mbit/s以太网升级到100Mbit/s，1Gbit/s和10Gbit/s时，都需要解决哪些技术问题？为什么以太网能够在发展的过程中淘汰掉自己的竞争对手，并使自己的应用范围从局域网一直扩展到城域网和广域网？

答：（1）将10Mbit/s以太网升级到100Mbit/s，1Gbit/s和10Gbit/s，需要解决一下问题：

①为了兼容较低速率的以太网，帧格式应该保持不变；

②在采用半双工工作方式时，为了保证在速率提高的同时令参数α保持较小的值，需要减小最大电缆长度或增大帧的最小长度；

③由于速率不断提升，以太网的传输媒体逐渐由铜线向光纤过渡；

④从半双工向全双工方式过渡，高速以太网需要工作在全双工方式下。

（2）以太网应用范围的扩大是因为其本身有很多好处：

①它是一种成熟的技术；

②互操作性很好；

③在广域网中使用以太网价格便宜；

④统一的帧格式，无需进行格式转换，从而简化了操作和管理。

29以太网交换机有何特点？用它怎样组成虚拟局域网？

答：（1）以太网交换机的特点主要有：

①采用全双工工作模式，每个端口都与单个主机相连；

②它是一种即插即用设备，通过自学习建立动态查找表；

③独占传输媒体的带宽，且每一对相互通信的主机能无碰撞地传输数据。

（2）按照端口划分VLAN，即将交换机中的某些端口定义为一个单独的区域，从而形成一个VLAN。不同交换机上的若干个端口可以组成同一个VLAN，分配到同一个VLAN的各网段上的所有站点都在同一个广播域中，可以直接通信。

30在图3-14中，某学院的以太网交换机有三个接口分别和学院三个系的以太网相连，另外三个接口分别和电子邮件服务器、万维网服务器以及一个连接互联网的路由器相连。图中A，B和C都是100Mbit/s以太网交换机。假定所有链路的速率都是100Mbit/s，并且图中的9台主机中的任何一个都可以和任何一个服务器或主机通信。试计算这9台主机和两台服务器产生的总的吞吐量的最大值。为什么？

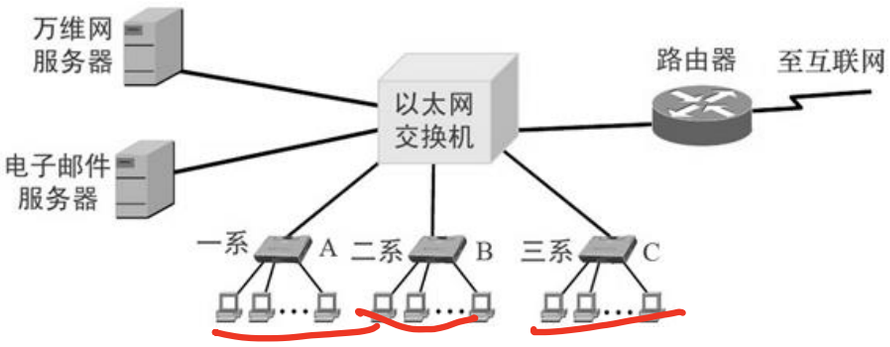

图3-14　30题图

答：因为三个系各有一台主机分别访问两个服务器和通过路由器上网，其他主机在系内通信，则9台主机的吞吐量为900Mbit/s，再加上两个服务器的吞吐量，总的吞吐量＝900＋200＝1100Mbit/s。

31假定在图3-14中的所有链路的速率仍然为100Mbit/s，但三个系的以太网交换机都换成为100Mbit/s的集线器。试计算这9台主机和两个服务器产生的总的吞吐量的最大值。为什么？

答：将三个系的以太网交换机换成集线器后，每个系组成一个碰撞域，其最大吞吐量为100Mbit/s，则总的吞吐量＝3×100＋200＝500Mbit/s。

32假定在图3-14中的所有链路的速率仍然为100Mbit/s，但所有的以太网交换机都换成100Mbit/s的集线器。试计算这9台主机和两个服务器产生的总的吞吐量的最大值。为什么？

答：将所有的以太网交换机都换成集线器后，整个系统处于同一个碰撞域，则总的吞吐量＝100Mbit/s。

33在图3-15中，以太网交换机有6个接口，分别接到5台主机和一个路由器。

图3-15　33题图

在下面表中的“动作”一栏中，表示先后发送了4个帧。假定在开始时，以太网交换机的交换表是空的。试把该表中的其他栏目都填写完。

动作	交换表的状态	向哪些接口转发帧	说明
A 发送帧给 D			
D 发送帧给 A			
E 发送帧给 A			
A 发送帧给 E			

答：填写后的结果如表3-4所示。

表3-4　33题结果表

动作	交换表的状态	向哪些接口转发帧	说明
A 发送帧给 D	写入(A,1)	除 1 外所有接口	表空时不知道转发给哪个接口
D 发送帧给 A	写入(D,4)	1	交换机已知 A 在接口 1
E 发送帧给 A	写入(E,5)	1	交换机已知 A 在接口 1
A 发送帧给 E	不变	5	交换机已知 E 在接口 5

34有两台主机A和B接在800m长的电缆线的两端，并在t＝0时各自向对方发送一个帧，长度为1500bit（包括首部和前同步码）。假定A和B之间有4个转发器，在转发帧时会产生20比特的时延。设传输速率为100Mbit/s，而CSMA/CD的退避时间是随机数r倍的争用期，争用期为512bit，在发生第一次碰撞后，在退避时A选择r＝0而B选择r＝1。忽略发生碰撞后的人为干扰信号和帧间最小间隔。

（1）设信号的传播速率是2×10^8m/s。试计算从A到B（包括4个转发器）的传播时延。

（2）在什么时间（以秒为单位）B完全收到了A发送的帧？

（3）现在假定只有A发送帧，帧长仍为1500bit，但4个转发器都用交换机来代替。交换机在进行存储转发时还要产生额外的20bit的处理时延。在什么时间（以秒为单位）B完全收到了A发送的帧？

答：（1）从A到B的传播时延＝800m/（2×10^8m/s）＋4×20bit/（100×10^6bit/s）＝4.8μs。

（2）发送1帧需要的时间是1500/（100×10^6bit/s）＝15μs，比从A到B传播一个比特所需的时间还要多；

在t＝0时，A和B同时发送帧；

在t＝4.8μs时，A和B都检测出碰撞；

在t＝9.6μs时，B终止发送的帧的最后一个比特到达A，A立即重传；

在t＝14.4μs时，A重传帧的第一个比特到达B；

A发送1500bit所需要的时间是1500/（100×10^6bit/s）＝15μs；

在t＝29.4μs时，A重传帧的最后一个比特到达B。

（3）整个传输链路被4个交换机分成5个网段。在主机和交换机之间或两个交换机之间的传播时延是：每一段电缆长度800/5＝160m除以电磁波的传播速率2×10^8m/s，算出为0.8μs。因此总的传播时延是5×0.8＝4μs；

主机A和4个交换机的发送时延一共是5×15＝75μs；

4个交换机的处理时延是4×0.2＝0.8μs；

因此，B收完A所发送的帧总共经历的时延＝4＋75＋0.8＝79.8μs。

3.3　考研真题详解

1假设一个采用CSMA/CD协议的100Mbps局域网，最小帧长是128B，则在一个冲突域内两个站点之间的单向传播延时最多是（　　）。[2019年408统考]

A．2.56μs

B．5.12μs

C．10.24μs

D．20.48μs

【答案】B

【解析】传播延迟的计算方法为最小帧长的字节形式换算为比特形式，然后除以带宽，即传播延迟＝128×8bit÷100Mbps＝10.24μs，题目为单向传播延时，所以为传播延时的一半，即5.12μs，答案选B。

2IEEE802.11无线局域网的MAC协议CSMA/CA进行信道预约的方法是（　　）。[2018年408统考]

A．发送确认帧

B．采用二进制指数退避

C．使用多个MAC地址

D．交换RTS和CTS帧

【答案】D

【解析】信道预约以避免冲突使用的是RTS/CTS机制，发送站点在向接收站点发送数据包之前，发送一个请求发送RTS帧，以申请对介质的占用，当接收站点收到RTS信号后，立即在一个短帧隙SIFS之后回应一个准许发送CTS帧，告知对方已准备好接收数据。双方在成功交换RTS/CTS信号对（即完成握手）后才开始真正的数据传递，保证了多个互不可见的发送站点同时向同一接收站点发送信号时，实际只能是收到接收站点回应CTS帧的那个站点能够进行发送，避免了冲突发生。即使有冲突发生，也只是在发送RTS帧时。答案选D。

3下列关于CSMA/CD协议的叙述中，错误的是（　　）。[2015年408统考]

A．边发送数据帧，边检测是否发生冲突

B．适用于无线网络，以实现无线链路共享

C．需要根据网络跨距和数据传输速率限定最小帧长

D．当信号传播延迟趋近0时，信道利用率趋近100%

【答案】B

【解析】CSMA/CD适用于有线网络，而CSMA/CA则广泛应用于无线局域网。CSMA/CD的基本原理：所有节点都共享网络传输信道，节点在发送数据之前，首先检测信道是否空闲，如果信道空闲则发送，否则就等待；在发送出信息后，再对冲突进行检测，当发现冲突时，则取消发送。

4以太网的MAC协议提供的是（　　）。[2012年408统考]

A．无连接不可靠服务

B．无连接可靠服务

C．有连接不可靠服务

D．有连接可靠服务

【答案】A

【解析】有连接与无连接的判断：很明显MAC帧首部格式中只有目的MAC地址、源MAC，所以是无连接的。

是否可靠的判断：如果是可靠的，首部中必须含有序号以及校验数据部分的校验和字段，而MAC协议中都是没有的，所以可以判断这种服务是不可靠的。

5在一个采用CSMA/CD协议的网络中，传输介质是一根完整的电缆，传输速率为1Gbps，电缆中的信号传播速度是200000km/s。若最小数据帧长度减少800比特，则最远的两个站点之间距离至少需要（　　）。[2009年408统考]

A．增加160m

B．增加80m

C．减少160m

D．减少80m

【答案】D

【解析】信号在电缆中的传播速度为2×10^8m/s，按照CSMA/CD的方式，电缆的传输速率为1Gbps＝10^9bps，这样最小帧的发送时间不能小于$800/10^9$，单程时间为$800/10^9/2$。知道了这个单程时间以及信号传播速度可以算出减少距离为：（$800/10^9/2$）$\times2\times10^8$＝80m。

第4章　网络层

4.1　复习笔记

一、网络层提供的两种服务

网络层提供了虚电路和数据报两种服务，如表4-1所示为它们主要区别。

表4-1　虚电路服务与数据报服务的对比

对比的方面	虚电路服务	数据报服务
思路	可靠通信应当由网络来保证	可靠通信应当由用户主机来保证
连接的建立	必须有	不需要
终点地址	仅在连接建立阶段使用，每个分组使用短的虚电路号	每个分组都有终点的完整地址
分组的转发	属于同一条虚电路的分组均按照同一路由进行转发	每个分组独立选择路由进行转发
当结点出故障时	所有通过出故障的结点的虚电路均不能工作	出故障的结点可能会丢失分组，一些路由可能会发生变化
分组的顺序	总是按发送顺序到达终点	到达终点时不一定按发送顺序
端到端的差错处理和流量控制	可以由网络负责，也可以由用户主机负责	由用户主机负责

二、网际协议IP

1IP协议概述

网络层实现的功能主要有：异构网络互联、路由与转发、拥塞控制；TCP/IP体系中网络层通常被称为网际层或IP层，网际协议IP是TCP/IP体系中最主要的协议之一，也是最重要的互联网标准协议之一；与IP协议配套使用的还有三个协议：

（1）地址解析协议ARP；

（2）网际控制报文协议ICMP；

（3）网际组管理协议IGMP。

2虚拟互连网络

（1）虚拟互连网络的概念

虚拟互连网络即逻辑互连网络，参与互连的网络都使用相同的网际协议IP，使得物理上异构的网络在逻辑上像是一个统一的网络。

（2）网络系统的中间设备

两个以上的计算机网络可以通过中间设备连接起来构成更大的网络系统，常见的有以下四种中间设备：

①物理层使用的中间设备：中继器、集线器；

②数据链路层使用的中间设备：网桥或交换机；

③网络层使用的中间设备：路由器；

④网络层以上使用的中间设备：网关。

3分类的IP地址

（1）IP地址及其表示方法

IP地址的编址方法经历了分类的IP地址、子网的划分、构成超网三个阶段；IP地址在整个互联网范围是唯一的一个32为标志符，通常用点分十进制表示，并由网络号和主机号两个部分组成；

（2）IP地址的分类

根据IP地址的网络号和主机号，可将其分为如图4-1所示的几类，并对一些有特殊用途的IP地址说明如下：

①用主机号全0表示本网络本身，例如203.84.74.0；

②用主机号全1表示本网络的广播地址，例如203.84.74.255；

③127.0.0.0为环路自检地址，代表任意主机本身；

④0.0.0.0表示本网络上的本主机；

⑤255.255.255.255表示整个TCP/IP网络的广播地址（受限广播地址）。

图4-1　IP地址中的网络号字段和主机号字段

根据以上分类，可知常用的三种类别的IP地址及其范围如下：

A类地址的网络号字段占一个字节，可指派的网络数为2^7-2，最大主机数是$2^{24}-2$；

B类地址的网络号字段占两个字节，可指派的网络数为$2^{14}-1$，最大主机数是$2^{16}-2$；

C类地址的网络号字段占三个字节，可指派的网络数为$2^{21}-1$，最大主机数是2^8-2。

【注意】

①同一个局域网上的主机或路由器的IP地址中的网络号是一样的；

②用网桥（它只在链路层工作）互连的网段仍然是一个局域网，只能有一个网络号；

③路由器总是具有两个或两个以上的IP地址。即路由器的每一个接口都有一个不同网络号的IP地址；

④当两个路由器直接相连时，在连线两端的接口处，可以分配也可以不分配IP地址。

4IP地址与硬件地址

IP地址与硬件地址的区别在于：

（1）物理地址是数据链路层和物理层使用的地址，而IP地址是网络层和以上各层使用的地址；

（2）IP地址放在IP数据报的首部，而硬件地址则放在MAC帧的首部；

（3）在IP层抽象的互联网上只能看到IP数据报，路由器转发并不改变源IP地址和目的IP地址，且路由器根据目的IP地址进行路由选择；

（4）在局域网的链路层，只能看见MAC帧。

5地址解析协议ARP

（1）ARP概述

ARP是一种工作在网络层的，并用来完成IP地址到MAC地址映射的协议。

（2）ARP工作原理

当主机A准备向本局域网上的主机B发送IP数据报时，有以下情况：

①当ARP高速缓存中有主机B的IP地址时，查出相应的硬件地址并写入MAC帧，并把该帧通过局域网发到对应硬件地址；

②当ARP高速缓存中没有主机B的IP地址时，通过目的MAC地址为FF-FF-FF-FF-FF-FF的帧封装并广播ARP请求分组，主机B收到广播后向A发送带有IP地址和硬件地址映射关系的响应分组，A收到响应后将此映射关系写入高速缓存并执行情况①中操作。

（3）ARP协议的四种典型情况

①发送方是主机，要把IP数据报发送到同一个网络上的另一个主机时，用ARP找目的主机的硬件地址；

②发送方是主机，要把IP数据报发送到另一个网络上的一个主机，用ARP找本网络的一个路由器地址，接下来由该路由器完成剩余操作；

③发送方是路由器，要把IP数据报转发到本网络上的主机，用ARP找目的主机的硬件地址；

④发送方是路由器，要把IP数据报转发到另一个网络上的另一个主机，用ARP找本网络的一个路由器地址，接下来由该路由器完成剩余操作。

6IP数据报的格式

（1）IP数据报的格式

如图4-2是IP数据报的格式，并对各字段说明如下（见表4-2）：

表4-2　IP数据报的字段

字段	解释
版本	占 4 位，指 IP 协议的版本，目前广泛使用 IPv4
首部长度	占 4 位，以 32 位为单位，常用长度为 20 字节，最大为 60 字节
区分服务	占 8 位，用来获得更好的服务，一般不使用
总长度	占 16 位，指首部和数据之和的长度，单位为字节
标识	占 16 位，是一个计数器，每产生一个数据报，计数器就加 1，并将此值赋给标识字段
标志	占 3 位，最低位 MF＝1 表示后面还有分片，MF＝0 表示最后一个分片；标志字段中间的一位 DF＝0 表示允许分片，否则不允许
片偏移	占 13 位，片偏移指出某片在原分组中的相对位置，以 8 个字节为偏移单位
生存时间 TTL	占 8 位，表明数据报在网络中可通过的路由器的最大值，标识分组在网络中的寿命
协议	占 8 位，指出数据报携带的数据使用何种协议
首部检验和	占 16 位，只检验数据报的首部，不包括数据部分
源地址	占 32 位，标识发送方的 IP 地址
目的地址	占 32 位，标识接收方的 IP 地址

图4-2　IP数据报的格式

【注意】IP数据报中三个关于长度的标记首部长度、总长度、片偏移分别对应的基本单位为4B、1B、8B。

（2）IP数据报的分片

由于IP数据报被封装在链路层的数据报中，链路层的最大传送单元MTU限制着IP数据报的长度，因此发送时需要分片，且分片在目的地的网络层重新组装。例如将总长度为3820字节的数据报（标识设为123）分成长度不超过1420字节的片，经计算可知与分片有关的字段值如表4-3所示，其分片后结果如图4-3所示。

表4-3　IP数据报首部中与分片有关的字段值

数据报	总长度	标识	MF	DF	片偏移
原始数据报	3820	123	0	0	0
分片 1	1420	123	1	0	0
分片 2	1420	123	1	0	175
分片 3	1020	123	0	0	350

图4-3　数据报分片举例

7IP层转发分组的流程

分组转发算法如下：

（1）从数据报的首部提取目的主机的IP地址D，得出目的网络地址为N；

（2）若N与此路由器直接相连，数据报直接交付给D，否则间接交付，执行（3）；

（3）若路由表中有目的地址为D的特定主机路由，则把数据报传送给路由表中所指明的下一跳路由，否则执行（4）；

（4）若路由表中有到达网络N的路由，则把数据报传送给路由表中所指明的下一跳路由，否则执行（5）；

（5）若路由表中有一个默认路由，则把数据报传送给路由表中所指明的默认路由，否则执行（6）；

（6）报告转发分组出错。

三、划分子网和构造超网

1子网划分与子网掩码

（1）子网划分

采用{<网络号>，<主机号>}形式的两级IP地址空间利用率低，且不够灵活，为解决这些不足提出了形如{<网络号>，<子网号>，<主机号>}的三级IP地址，其划分子网的思路如下：

①划分子网属于单位内部的事，对外仍表现为没有划分；

②从网络的主机号借用若干位作为子网号以组成三级IP地址，且主机号也相应减少同样的位数；

③从其他网络发送给本单位某个主机的IP数据报，仍根据IP数据报的目的网络号找到连接在本单位网络上的路由器，路由器在收到IP数据报后，再按目的网络号和子网号找到目的子网，把IP数据报交付给目的主机。

（2）子网掩码

子网掩码是一个与IP地址对应的长为32bit的二进制串，由一串连续的1和后面跟随的连续0组成；主要用于和IP地址按位“与”，从而得出IP地址相应的子网的网络地址。例如某主机的IP地址为136.34.50.56，子网掩码为255.255.255.0，则进行按位“与”后得到该主机所在子网的网络号为136.34.50.0。

2使用子网时分组的转发

经子网划分后，路由表主要包括目的网络地址、子网掩码、下一跳地址，此时路由器转发分组的算法如下：

（1）从收到的分组的首部提取目的IP址D；

（2）用各网络的子网掩码和D逐位相“与”，若结果与相应的网络地址匹配，进行直接交付，否则间接交付，执行（3）；

（3）若路由表中有目的地址为D的特定主机路由，则把分组传送给路由表中所指明的下一跳路由，否则执行（4）；

（4）对路由表中的每一行（目的网络地址，子网掩码，下一跳地址）中的子网掩码和D逐位相“与”并设其结果为N，若N与该行的目的网络地址匹配，则把分组传送给该行指明的下一跳路由器，否则执行（5）；

（5）若路由表中有一个默认路由，则把分组传送给路由表中所指明的默认路由器；否则执行（6）；

（6）报告转发分组出错。

3无分类编址CIDR（构造超网）

（1）网络前缀

无分类域间路由选择（CIDR）是在变长子网掩码基础上提出的消除A、B、C三类传统网络划分的方法；它主要的特点有两个：

①消除了传统的A类、B类和C类地址以及划分子网的概念，采用{<网络前缀>，<主机号>}中的“网络前缀”代替子网络的概念；CIDR还可使用“斜线记法”（CIDR记法）表示，即在IP地址后面加上斜线“/”，然后写上网络前缀所占的位数，例如128.14.35.7/20表示前20位是网络前缀；

②CIDR把网络前缀都相同的连续的IP地址组成一个“CIDR地址块”，这个过程称为路由聚合或构造超网；例如有网络1：206.1.0.0/17，网络2：206.1.128.0/17，这两个网络的二进制表示中前16位均是相同的，有时候需要将它们聚合成更大的地址块，如网络1和网络2可以聚合为206.1.0.0/16。

（2）最长前缀匹配

使用CIDR时，路由表由网络前缀和下一跳地址组成，查找路由表可能会出现不止一个的匹配结果，则此时应选择具有最长网络前缀的路由（因为网络前缀越长，其地址块就越小，路由就越具体）。

四、网际控制报文协议ICMP

1ICMP报文概述

ICMP协议是IP层协议，为提高IP数据报交付成功的机会，ICMP允许主机或路由器报告差错或异常情况，ICMP分为ICMP差错报告报文和ICMP询问报文两大类。

（1）ICMP差错报告报文

ICMP差错报告报文共有五种（见表4-4）：

表4-4　ICMP差错报告报文

报文种类	解释
终点不可达	路由器或主机不能交付数据报时发送
源点抑制	路由器或主机由于拥塞而丢弃数据报时发送
时间超过	路由器收到生存时间 TTL 为零的数据报时或当终点在预先规定的时间内不能收到一个数据报的全部数据报片时，除丢弃该数据报外，还要发送时间超过报文
参数问题	路由器或目的主机收到的数据报的首部中存在不正确的字段时，丢弃该数据报，并发送参数问题报文
改变路由（重定向）	路由器把改变路由报文发送给主机，让主机知道下次应将数据报发送给另外的路由

还有一些情况不应该发送ICMP报文，具体如下：

①对ICMP差错报告报文不再发送ICMP差错报告报文；

②对第一个分片的数据报片的所有后续数据报片都不发送ICMP差错报告报文；

③对具有多播地址的数据报都不发送ICMP差错报告报文；

④对具有特殊地址（如127.0.0.0或0.0.0.0）的数据报不发送ICMP差错报告报文。

（2）ICMP询问报文

常用的ICMP询问报文有（最常用的是前两种）：

①回送请求和回答报文；

②时间戳请求和回答报文；

③掩码地址请求和回答报文；

④路由器询问和通告报文。

2ICMP的应用举例

ICMP的应用常见有分组网间探测PING（测试两个主机之间的连通性）和traceroute（跟踪一个分组从源点到终点的路径）。

五、互联网的路由选择协议

1分层次的路由选择协议

互联网采用的路由选择协议主要是自适应的（即动态的）、分布式路由选择协议；互联网可以划分为许多较小的自治系统AS，目前，一个大的ISP就是一个自治系统，此时路由选择协议可分为：

（1）内部网关协议IGP：在一个自治系统内部使用的路由选择协议与在互联网中的其他自治系统选用什么路由选择协议无关，如RIP和OSPF协议；

（2）外部网关协议EGP：若源主机和目的主机处在不同的自治系统中，当数据报传到一个自治系统的边界时，就需要使用一种协议将路由选择信息传递到另一个自治系统中，目前使用最多的是BGP-4。

2内部网关协议RIP

（1）RIP协议的相关规定

RIP是一种分布式的基于距离向量的路由选择协议，它规定：

①网络中的每一个路由器都需记录从它自己到其他每一个目的网络的距离；

②距离即跳数，规定一个路由器到直接相连的网络的跳数为1，之后每经过一个路由器跳数加1；

③RIP协议将优先选择跳数较少的路径；

④RIP协议最多只允许一条路径包含15个路由器，当跳数为16时表示网路不可达；

⑤默认在任两个使用RIP协议的路由器之间每30s广播一次更新信息，动态维护路由表。

（2）RIP协议的特点

①仅和相邻路由器交换信息；

②路由器交换的信息是当前本路由器所知道的全部信息，即自己的路由表；

③按固定的时间间隔交换路由信息；

④好消息传播得快，坏消息传播得慢。

（3）距离向量算法

路由表组成为<目的网络N，距离d，下一跳路由器X>，对每一个相邻路由器发送过来的RIP报文，进行以下步骤：

①对地址为X的相邻路由器发来的RIP报文，先把报文中的所有“下一跳”字段的地址都改为X，并把所有的“距离”字段的值加1；

②对修改后的RIP报文中的每一个项目，进行以下步骤：

a．当原来的路由表中没有目的网络N时，把该项目添加到路由表中；

b．当原来的路由表中有目的网络N且下一跳地址是X时，用收到的项目替换原表中相应项目；

c．当原来的路由表中有目的网络N且下一跳地址不是X时，若收到的项目中d小于原表中的d，则用收到的项目更新路由表，否则不进行操作。

③若3分钟还没有收到相邻路由器的更新路由表，则把此相邻路由器记为不可达的路由器（置跳数为16）；

④返回。

（4）RIP协议的报文格式（略）

（5）RIP协议的优缺点

①优点：实现简单，开销较小，收敛过程较快；

②缺点：

a．RIP协议限制了网络的规模，它能使用的最大距离为15；

b．路由器之间需要交换整个路由表，使得网络规模扩大，开销增加；

c．网络故障时出现的收敛现象“坏消息传播得慢”，使更新过程的收敛时间过长。

【注意】RIP是应用层协议，使用UDP传送数据。

3内部网关协议OSPF

（1）OSPF和RIP的不同点（见表4-5）

表4-5　OSPF和RIP的不同点

OSPF	RIP
使用洪泛法向本自治系统中所有路由器发送信息	只向相邻路由器发送路由信息
发送的信息是与本路由器相邻的所有路由器的链路状态，是路由器所知道的部分信息	发送的是整个路由表信息
只有当链路状态发生变化时，才使用洪泛法发送信息	定期交换路由信息
网络层协议	应用层协议

（2）OSPF的基本特点

①OSPF最主要的特征就是使用分布式的链路状态协议，而不是像RIP那样的距离向量协议；

②OSPF允许管理员给每条路由指派不同的代价，更为灵活；

③所有在OSPF路由器之间交换的分组都具有鉴别功能，保证仅在可信赖的路由器之间交换链路状态信息；

④OSPF支持可变长度的子网划分和无分类的编址CIDR；

⑤每一个链路状态都带上一个32位的序号，序号越大状态就越新。

（3）OSPF的基本工作原理

路由器之间频繁交换链路状态信息，从而建立起一个链路状态数据库（实际上就是全网的拓扑结构），然后每个路由器根据这个拓扑结构使用Dijkstra最短路径算法计算自己到各目的网络的最短路径，以此构造路由表。

（4）OSPF的五种分组类型（见表4-6）

表4-6　OSPF的分组类型

分组类型	解释
问候分组	用来发现和维持邻站的可达性
数据库描述分组	向邻站给出自己的链路状态数据库中的所有链路状态项目的摘要信息
链路状态请求分组	向对方请求发送某些链路状态项目的详细信息
链路状态更新分组	用洪泛法对全网更新链路状态
链路状态确认分组	对链路更新分组的确认

4外部网关协议BGP

（1）BGP协议概述

外部网关协议BGP是不同自治系统的路由器之间交换路由信息的协议，是一种应用层协议；它力求寻找一条能够到达目的网络且比较好的路由，而不需要寻找一条最佳路由；BGP采用了路径向量路由选择协议。

（2）BGP协议工作原理

每个自治系统至少选择一个路由器作为“BGP发言人”，BGP发言人与其他自治系统的BGP发言人建立TCP连接，并在此连接上交换BGP报文以建立BGP会话，再利用BGP会话交换路由信息，当所有BGP发言人相互交流完路由信息后，各自找出到达各个自治系统的较好路由。

（3）BGP-4的四种报文（见表4-7）

表4-7　BGP-4的四种报文

报文	解释
OPEN（打开）报文	用来与相邻的另一个 BGP 发言人建立关系，使通信初始化
UPDATE（更新）报文	用来发送某一路由的信息，及列出要撤销的多条路由
KEEPALIVE（保活）报文	用来确认打开报文及周期性地证实邻站的连通性
NOTIFICATION（通知）报文	用来发送检测到的差错

【注意】三种路由协议的比较如表4-8所示。

表4-8　三种路由协议的比较

协议	RIP	OSPF	BGF
类型	IGP（内部）	IGP（内部）	EGP（外部）
路由算法	距离向量算法	链路状态算法	路径向量算法
传递信息的协议	UDP	IP	TCP
路径选择	选择跳数最少的	选择代价最低的	较好的即可
与之交换的结点	相邻路由器	网络中所有路由器	相邻路由器
交换的内容	路由表	链路状态	有变化的部分

5路由器的构成

（1）路由器的结构与功能

如图4-4所示，路由器主要由路由选择和分组转发两部分组成，路由选择部分即控制部分，分组转发部分由交换结构、一组输入端口和一组输出端口组成，路由器主要完成分组转发和路由计算功能。

图4-4　典型的路由器的结构

（2）路由表与路由转发

路由表用于路由选择，主要是根据路由选择算法得来的；而在路由转发时通常使用更为简单的转发表，它的表项和路由表有直接的关系，但通常仅包括分组发往的目的地址、分组的下一跳即可。

六、IPv6

1IPv6的特点

要根本解决IP地址耗尽的问题，需要使用IPv6，它的主要特点有：

（1）IPv6地址将从IPv4的32为增加到128位，使得具有更大的地址空间；

（2）扩展的地址层次结构；

（3）灵活的首部格式；

（4）改进的选项；

（5）允许协议继续扩充；

（6）支持即插即用；

（7）支持资源的预分配；

（8）IPv6首部是8B的整数倍，而IPv4是4B的整数倍；

（9）在传输路径中，IPv6不允许路由器对其分片；

（10）IPv6增加了安全性。

2IPv6地址

（1）IPv6的地址类型

IPv6数据报的目的地址一般是以下三种基本类型地址之一：

①单播：即传统的点对点通信；

②多播：即一点对多点的通信，分组被交付到一组计算机的每一个；

③任播：即目的站是一组计算机，但数据报交付时通常只交付距离最近的那一个。

（2）IPv6的地址表示

为使地址表示更加简单，IPv6采用冒号十六进制记法，例如68E6:8C64:FFFF:FFFF:0:1180:960A:FFFF，它允许把数字前面的0

省略，也允许对0进行压缩，如FF05:0:0:0:0:0:0:B3可压缩为FF05::B3。

3IPv4到IPv6过渡

由IPv4到IPv6过渡可以采用两种策略：

（1）双协议栈技术：在完全过渡到IPv6之前，使部分主机（或路由器）装有两个协议栈分别适用两类地址；

（2）隧道技术：将整个IPv6数据报封装到IPv4数据报的数据部分，使IPv6可以在IPv4网络的隧道中传输。

七、IP多播

1IP多播的基本概念

IP多播分为只在本局域网上进行硬件多播和在互联网的范围进行多播两种，多播地址的特点如下：

（1）多播地址只能用于目的地址，而不能用于源地址；

（2）多播数据报不产生ICMP差错报文；

（3）与单播相比，在一对多的通信中，多播可大大节约网络资源。

2IP多播的地址

IP多播使用D类地址格式，它的前四位为1110，能表示的范围为224.0.0.0～239.255.255.255，且多播数据报中首部的协议字段值为2，表示使用IGMP协议。

3网际组管理协议IGMP和多播路由选择协议

（1）网际组管理协议IGMP

IGMP协议让连接在本地局域网上的多播路由器知道本局域网上是否有主机参加或退出某个多播组，它可看做TCP/IP协议的一部分，其工作分为两个阶段：

①第一阶段：当某个主机加入新的多播组时，该主机应向多播组的多播地址发送一个IGMP报文，声明自己要成为该组的成员。本地的多播路由器收到IGMP报文后，将组成员关系转发给互联网上的其他多播路由器。

②第二阶段：组成员关系是动态的，本地多播路由器要周期性地探询本地局域网上的主机，以便知道这些主机是否还继续是组的成员。

（2）多播路由选择协议

①转发多播数据报时使用的方法

a．洪泛与剪除；

b．隧道技术；

c．基于核心的发现技术。

②常见的多播路由选择协议

a．距离向量多播路由选择协议DVMRP；

b．基于核心的转发树CBT；

c．开放最短通路优先的多播扩展MOSPF；

d．协议无关多播-稀疏方式PIM-SM；

e．协议无关多播-密集方式PIM-DM。

八、虚拟专用网VPN和网络地址转换NAT

1虚拟专用网VPN

由于IP地址紧缺，对一个机构而言，所能申请的IP地址一般小于本机构的主机数，此时可以选用一些只能在本机构使用的内部地址，并利用公用的互联网作为本机构各专用网之间的通信载体，这样的专用网称为虚拟专用网VPN。

2网络地址转换NAT

网络地址转换NAT是将专用网络地址转换为公用网络地址一种方法，它隐藏了内部管理的IP地址，使得整个专用网仅需要一个全球IP地址即可实现与互联网相连。

九、多协议标记交换MPLS（略）

4.2　课后习题详解

1网络层向上提供的服务有哪两种？试比较其优缺点。

答：（1）网络层向上提供的两种服务：面向连接的虚电路服务和无连接的数据报服务。

①虚电路服务：计算机进行通信前应先建立一条虚电路，然后双方沿着已建立的虚电路发送分组；

②数据报服务：计算机在发送分组时不需要先建立连接，每一个分组独立发送，与其前后的分组无关。

（2）两种服务的比较如表4-1所示（见笔记部分）。

则其优缺点比较可从以下几个方面说明：

①从占用通信子网资源方面：虚电路服务将占用结点交换机的存储空间，而数据报服务头部占用空间；

②从时间开销方面：虚电路服务有创建连接的时间开销；而数据报服务有选择路由的时间开销；

③从拥塞避免方面：虚电路服务基本上能避免拥塞，而数据报服务则很困难；

④从健壮性方面：数据报服务的健壮性更好。

总之，虚电路服务适用于具有交互作用的信息，不仅及时、传输较为可靠，而且网络开销小；数据报服务适用于传输单个分组构成的、不具交互作用的信息以及对传输要求不高的场合。

2网络互联有何实际意义，进行网络互联时，有哪些共同的问题需要解决？

答：（1）网络互联可扩大用户共享资源范围和通信区域，使处于不同地理位置的计算机能进行通信；

（2）网络互联时，存在不同的寻址方案、不同的最大分组长度、不同的网络接入机制、不同的超时控制、不同的差错恢复方法、不同的状态报告方法、不同的路由选择技术、不同的用户接入控制、不同的服务（面向连接服务和无连接服务）、不同的管理与控制方式等，这些问题都需要共同解决。

3作为中间设备，转发器、网桥、路由器和网关有何区别？

答：（1）工作的层次不同：转发器是物理层使用的中间设备，网桥是数据链路层的中间设备，路由器是网络层的中间设备，而网关负责网络层以上的数据中继；

（2）处理数据的方式不同：转发器不执行数据过滤功能，它和网桥都是用于扩大一个网络，此时范围虽然扩大了，但仍然是一个网络；而路由器用来在互联网中进行网络互联和路由选择，一般讨论的互联网都是指用路由器进行互联的互联网络；网关能用于将异构网连接在一起。

4试简单说明下列协议的作用：IP、ARP、RARP和ICMP。

答：（1）IP：网际协议，实现网络互连（性能各异的网络在用户面前像一个统一的网络）；

（2）ARP：地址解析协议，将IP地址转换成物理地址，解决同一个局域网上的主机或路由器上的IP地址和硬件地址的映射问题；

（3）RARP：逆向地址解析协议，将物理地址转换成IP地址；

（4）ICMP：网际控制报文协议，进行差错控制和传输控制，减少分组的丢失。

5IP地址分为几类？各如何表示？IP地址的主要特点是什么？

答：（1）IP地址被分为A、B、C、D、E五类，如图4-1所示（见笔记部分），其中A、B、C类为单播地址，D类地址用于多播，E类地址保留为以后用；其中A、B、C类表示分别如下：

①A类地址的网络号字段占一个字节，最前面的1位是0，可指派的网络数为2^7-2，最大主机数是$2^{24}-2$，范围为1.0.0.1～126.255.255.254；

②B类地址的网络号字段占两个字节，最前面的2位是10，可指派的网络数为$2^{14}-1$，最大主机数是$2^{16}-2$，范围为128.1.0.1～191.255.255.254；

③C类地址的网络号字段占三个字节，最前面的3位是110，可指派的网络数为$2^{21}-1$，最大主机数是2^8-2，范围为192.0.1.1～223.255.255.254。

（2）IP地址的主要特点

①IP地址由网络号和主机号两部分组成，是一种分等级的地址结构；

②IP地址是标志一个主机和一条链路的接口，当一个主机同时连接在多个网络上，该主机就有多个IP地址；

③由转发器或网桥连接起来的若干个局域网仍为一个网络，同一个局域网上的主机或路由器的IP地址中的网络号是一样的；

④所有分配到网络号的网络都是平等的；

⑤IP地址可用来指明一个网络的地址。

6试根据IP地址的规定，计算出表4-9中的各项数据。

表4-9　IP地址的指派范围

网络类别	最大可指派的网络数	第一个可指派的网络号	最后一个可指派的网络号	每个网络中的最大主机数
A	126（2^7-2）	1	126	16777214
B	16383（$2^{14}-1$）	128.1	191.255	65534
C	2097151（$2^{21}-1$）	192.0.1	223.255.255	254

答：（1）A类地址的网络号字段占1个字节，且第一位固定为0，可指派的网络号为126个（即2^7-2）。减2是因为网络号为00000000的IP地址是保留地址，网络号为01111111的IP地址用于测试本主机进程之间的通信。A类地址的主机号占3字节，因此每一个A类网络中的最大主机数为16777214个（即$2^{24}-2$）。减2是因为全0的主机号字段表示该IP地址是“本主机”所连接到的单个网络地址，而全1表示该网络上的所有主机。

（2）B类地址的网络号字段有2字节，且前两位固定为10。网络号字段的后14位无论如何取值，网络号字段都不可能是全0或全1，因此网络总数不用减2。但B类网络地址128.0.0.0是不指派的，可以指派的B类最小网络地址为128.1.0.0。因此B类地址可指派的网络数为16383个（即$2^{14}-1$），每一个网络上的最大主机数为65534个（即$2^{16}-2$），减2是因为要扣除全0和全1的主机号。

（3）C类地址的网络号字段有3字节，且前三位固定为110。C类网络地址192.0.0.0也是不指派的，可以指派的C类最小网络地址为192.0.1.0，因此C类地址可指派的网络总数为2097151个（即$2^{21}-1$），每一个C类地址的最大主机数为254个（即2^8-2）。

7试说明IP地址与硬件地址的区别。为什么要使用这两种不同的地址？

答：（1）IP地址与硬件地址的主要区别有：

①硬件地址（物理地址）由48bit构成，而IP地址（这里指IPv4）由32bit构成；

②硬件地址放在MAC帧首部，而IP地址放在IP数据报首部；

③在数据链路层及其以下使用硬件地址，而在网络层及网络层以上使用IP地址。

（2）使用这两种不同的地址的原因：硬件地址在一定程度上与硬件保持了一致，它能够保证与硬件的连接无误，而IP地址给予逻辑域的划分，不受硬件的限制，且IP层抽象的互联网屏蔽了下层的复杂实现细节，使我们能够使用统一的、抽象的IP地址进行通信；所以两者必不可少。

8IP地址方案与我国的电话号码体制的主要不同点是什么？

答：IP地址方案与我国的电话号码体制的主要不同点：

（1）交换方式不同：IP地址方案是基于存储转发交换的，而电话号码基于电路交换的。

（2）IP地址分为网络号和主机号，用来标示网络中的某一台主机，它可以是静态的也可以是动态的，与主机地理位置无关。而电话号码则是固定的用来标示某一个用户终端，透过一个具体的电话号码，可以知道相应的国家代码，地区代码，交换局代码，及用户代码。

9（1）子网掩码为255.255.255.0代表什么意思？

（2）一个网络的现在掩码为255.255.255.248，问该网络能够连接多少个主机？

（3）一个A类网络和一个B类网络的子网号subnet-id分别为16个1和8个的1，问这两个网络的子网掩码有何不同？

（4）一个B类地址的子网掩码是255.255.240.0。试问在其中每一个子网上的主机数最多是多少？

（5）一A类网络的子网掩码为255.255.0.255，它是否为有效的子网掩码？

（6）某个IP地址的十六进制表示是C2.2F.14.81，试将其转换为点分十进制的形式，这个地址是哪一类IP地址？

（7）C类网络使用子网掩码有无实际意义，为什么？

答：（1）可以代表C类地址对应的子网掩码默认值；也能表示A类和B类地址的掩码，即主机号由最后8位决定，路由器寻找网络由前24位决定；

（2）255.255.255.248的二进制序列为：11111111 11111111 11111111 11111000，根据掩码的定义，后三位是主机号，一共可以表示$2^3=8$个主机号，除掉全0和全1的两个，该网络能够接6个主机；

（3）子网掩码都是255.255.255.0，但是对应的子网的数目不同，前者为65534（$2^{16}-2$），后者为254（$2^{8}-2$）；

（4）子网掩码255.255.240.0对应的二进制序列为11111111 11111111 11110000 00000000，可知主机号有12位，所以每个子网的主机数最多为：$2^{12}-2=4094$；

（5）该子网掩码为有效的子网掩码，但不推荐这样使用；

（6）用点分十进制表示：194.47.20.129，为C类地址；

（7）有实际意义，对于小网络可进一步简化路由表，提高网络利用率。

10试辨认以下IP地址的网络类别：

（1）128.36.199.3

（2）21.12.240.17

（3）183.194.76.253

（4）192.12.69.248

（5）89.3.0.1

（6）200.3.6.2

答：A类地址以1～127开始，B类地址以128～191开始，C类地址以192～223开始，故（1）（3）为B类网，（2）（5）为A类网，（4）（6）为C类网。

11IP数据报中的首部检验和并不检验数据报中的数据，这样做的最大好处是什么？坏处是什么？

答：IP数据报中的首部检验和并不检验数据报中的数据的好处是：首部较数据部分更短，所以转发分组更快；坏处是：由于没有检验数据部分，也就难以及时发现数据部分出现的差错。

12当某个路由器发现一IP数据报的检验和有差错时，为什么采取丢弃的办法而不是要求源站重传此数据报？计算首部检验和为什么不采用CRC检验码？

答：（1）不要求源站重发是因为地址子段也有可能出错，且源站数据报发送完毕后没有缓存，重传没有意义；

（2）数据报每经过一个路由器，路由器就要计算一下校验和，而CRC检验码使用多项式除法，计算较复杂，为了进一步减小计算检验和的工作量，简化计算，减少路由器检验的时间，故不采用CRC检验码。

13设IP数据报使用固定首部，其各字段的具体数值如图4-5所示（除IP地址外，均为十进制表示）。试用二进制运算方法计算应当写入到首部检验和字段中的数值（用二进制表示）。

图4-5　IP数据报示意图

答：首先把检验和字段置零，并将IP数据报首部划分为16位字的序列。依次对这些16位字的序列进行二进制反码求和，计算过程如下：

```
 0  1  0  0  0  1  0  1  0  0  0  0  0  0  0  0
 0  0  0  0  0  0  0  0  0  0  0  1  1  1  0  0
 0  0  0  0  0  0  0  0  0  0  0  0  0  0  0  1
 0  0  0  0  0  0  0  0  0  0  0  0  0  0  0  0
 0  0  0  0  0  1  0  0  0  0  0  1  0  0  0  1
 0  0  0  0  0  0  0  0  0  0  0  0  0  0  0  0
 0  0  0  0  1  0  1  0  0  0  0  0  1  1  0  0
 0  0  0  0  1  1  1  0  0  0  0  0  0  1  0  1
 0  0  0  0  1  1  0  0  0  0  0  0  0  1  1  0
 0  0  0  0  0  1  1  1  0  0  0  0  1  0  0  1
-------------------------------------------------
 0  1  1  1  0  1  0  0  0  1  0  0  1  1  1  0
```

将求得的结果取反得检验和为：1000101110110001。

14重新计算上题，但使用十六进制运算方法（每16位二进制数字转换为4个十六进制数字，再按十六进制加法规则计算）。比较这两种方法。

答：首先把检验和字段置零，并将IP数据报首部划分为16位字的序列，其次将这些16位字的序列转换为十六进制数字，最后对这些十六进制数进行十六进制反码求和。计算过程如下：

```
4  5  0  0
0  0  1  C
0  0  0  1
0  0  0  0
0  4  1  1
0  0  0  0
0  A  0  C
0  E  0  5
0  C  0  6
0  7  0  9
-----------
7  4  4  E
```

将求得的结果取反得检验和为8BB1。二进制求和利用满2进1的运算规则，十六进制将四位二进制作为一个整体，满16进1，两者所得结果是相同的。

15什么是最大传送单元MTU？它和IP数据报首部中的哪个字段有关系？

答：在IP层下面的数据链路层所限定的帧的数据字段的最大长度，称为最大传送单元MTU；与IP数据报中“总长度”字段有关系，是IP数据报首部中的“总长度字段”的上限值。

16在互联网中将IP数据报分片传送的数据报在最后的目的主机进行组装。还可以有另一种做法，即数据报片通过一个网络就进行一次组装。试比较这两种方法的优劣。

答：（1）在最后的目的主机进行组装时，对于所传数据报来讲仅需要进行一次分段和一次组装，用于分段和组装的开销相对较小。但主机若在最终组装时发现分组丢失，则整个数据报要重新传输，时间开销很大；

（2）若每通过一次网络就进行一次组装，由于并非所有的数据报片都经过同样的路由器，则会导致有时进行组装时会出现缺片现象；又由于组装后可能还需要继续分成更小的数据报片，则会使分片与组装次数增多，造成的开销也更大；但若通过一个网络后组装时发现分段丢失，可以及时地重传数据报，时间开销较前者小，同时可靠性提高。

17一个3200位长的TCP报文传到IP层，加上160位的首部后成为数据报。下面的互联网由两个局域网通过路由器连接起来，但第二个局域网所能传送的最长数据帧中的数据部分只有1200位，因此数据报在路由器必须进行分片。试问第二个局域网向其上层要传送多少比特的数据（这里的“数据”当然指的是局域网看见的数据）？

答：IP数据报的长为：3200＋160＝3360（bit），第二个局域网分片应分为⌈3360/1200⌉＝3（片）；三片的首部共为：160×3＝480（bit）；则总共要传送的数据共3360＋480＝3840（bit）。

18（1）有人认为：“ARP协议向网络层提供了转换地址的服务，因此ARP应当属于数据链路层。”这种说法为什么是错误的？

（2）试解释为什么ARP高速缓存每存入一个项目就要设置10～20分钟的超时计时器。这个时间设置得太大或太小会出现什么问题？

（3）举出至少两种不需要发送ARP请求分组的情况（即不需要请求将某个目的IP地址解析为相应的硬件地址）。

答：（1）ARP不是向网络层提供服务，它本身就是网络层的一部分，它为IP协议提供了转换地址的服务。数据链路层使用硬件地址而不使用IP地址，无需ARP协议转换即可正常运行，因此ARP协议不在数据链路层。

（2）当网络中某个IP地址和硬件地址的映射发生变化时，ARP高速缓存中的相应项目就要改变。ARP为保存在高速缓存中的每一个映射地址项目都设置生存时间，凡超过生存时间的项目就从高速缓存中删除掉。设置这种地址映射项目的生存时间太长会使更换网卡的主机迟迟无法和网络上的其他主机通信，而时间太短则会使ARP请求和响应分组的通信太过频繁。

（3）在源主机的ARP高速缓存中已经有了该目的IP地址项目；源主机和目的主机使用点对点链路。

19主机A发送IP数据报给主机B，途中经过了5个路由器。试问在IP数据报的发送过程中总共使用了几次ARP？

答：IP数据报从主机A发送到主机B的过程中共使用了6次ARP。其中主机A使用1次ARP，每个路由器各使用1次ARP。

20设某路由器建立了如下路由表：

目的网络	子网掩码	下一跳
128.96.39.0	255.255.255.128	接口 m0
128.96.39.128	255.255.255.128	接口 m1
128.96.40.0	255.255.255.128	R2
192.4.153.0	255.255.255.192	R3
*（默认）	—	R4

现共收到5个分组，其目的站IP地址分别为：

（1）128.96.39.10

（2）128.96.40.12

（3）128.96.40.151

（4）192.4.153.17

（5）192.4.153.90

试分别计算其下一跳。

答：分组转发算法如下：

（1）从数据报的首部提取目的主机的IP地址D，得出目的网络地址为N；

（2）若N与此路由器直接相连，数据报直接交付给D，否则间接交付，执行（3）；

（3）若路由表中有目的地址为D的特定主机路由，则把数据报传送给路由表中所指明的下一跳路由，否则执行（4）；

（4）若路由表中有到达网络N的路由，则把数据报传送给路由表中所指明的下一跳路由，否则执行（5）；

（5）若路由表中有一个默认路由，则把数据报传送给路由表中所指明的默认路由，否则执行（6）；

（6）报告转发分组出错。

根据该算法，以求（5）为例说明解题过程：

路由器收到的分组的目的地址D_5＝192.4.153.90。

将题中子网掩码255.255.255.128与D5进行AND运算得192.4.153.0，显然与网络128.96.39.0、128.96.39.128、128.96.40.0均不匹配；

再将题中子网掩码255.255.255.192与D5进行AND运算得192.4.153.64，显然与网络192.4.153.0不匹配，则下一跳只能选择默认路由R_4。

得出答案是（1）接口m0；（2）R_2；（3）R_4；（4）R_3；（5）R_4。

21某单位分配到一个B类IP地址，其net-id为129.250.0.0。该单位有4000台机器，分布在16个不同的地点。如选用子网掩码为255.255.255.0，试给每一个地点分配一个子网号码，并算出每个地点主机号码的最小值和最大值。

答：4000/16＝250，平均每个地点250台机器。如选255.255.255.0为掩码，则每个网络所连主机数＝2^8－2＝254＞250，共有子网数2^8－2＝254＞16，能满足实际需求；其分配方法如表4-10所示。

表4-10　子网分配表

地点	子网号（二进制表示）	子网网络号	主机 IP 的地址范围
1	00000001	129.250.1.0	129.250.1.1～129.250.1.254
2	00000010	129.250.2.0	129.250.2.1～129.250.2.254
3	00000011	129.250.3.0	129.250.3.1～129.250.3.254
4	00000100	129.250.4.0	129.250.4.1～129.250.4.254
5	00000101	129.250.5.0	129.250.5.1～129.250.5.254
6	00000110	129.250.6.0	129.250.6.1～129.250.6.254
7	00000111	129.250.7.0	129.250.7.1～129.250.7.254
8	00001000	129.250.8.0	129.250.8.1～129.250.8.254
9	00001001	129.250.9.0	129.250.9.1～129.250.9.254
10	00001010	129.250.10.0	129.250.10.1～129.250.10.254
11	00001011	129.250.11.0	129.250.11.1～129.250.11.254
12	00001100	129.250.12.0	129.250.12.1～129.250.12.254
13	00001101	129.250.13.0	129.250.13.1～129.250.13.254
14	00001110	129.250.14.0	129.250.14.1～129.250.14.254
15	00001111	129.250.15.0	129.250.15.1～129.250.15.254
16	00010000	129.250.16.0	129.250.16.1～129.250.16.254

22一个数据报长度为4000字节（固定首部长度）。现在经过一个网络传送，但此网络能够传送的最大数据长度为1500字节。试问应当划分为几个短些的数据报片，各数据报片的数据字段长度、片偏移字段和MF标志应为何数值？

答：IP数据报固定首部长度为20字节，则数据报数据部分长度为4000－20＝3980字节，因为⌈3980/1480⌉＝3，故应该划分3个数据报片；其各字段的值如表4-11所示。

表4-11　分片后字段值表

数据报	总长度（字节）	数据长度（字节）	MF	片偏移
原始数据报	4000	3980	0	0
分片 1	1500	1480	1	0
分片 2	1500	1480	1	185
分片 3	1040	1020	0	370

23分两种情况（使用子网掩码和使用CIDR）写出互联网的IP层查找路由的算法。

答：（1）划分子网，使用子网掩码的情况：

①从数据报的首部提取目的主机的IP地址D，得出目的网络地址为N；

②若N与此路由器直接相连，数据报直接交付给D，否则间接交付，执行③；

③若路由表中有目的地址为D的特定主机路由，则把数据报传送给路由表中所指明的下一跳路由，否则执行④；

④若路由表中有到达网络N的路由，则把数据报传送给路由表中所指明的下一跳路由，否则执行⑤；

⑤若路由表中有一个默认路由，则把数据报传送给路由表中所指明的默认路由，否则执行⑥；

⑥报告转发分组出错。

（2）使用CIDR的情况

①从数据报的首部提取目的主机的IP地址D，得出目的网络地址为N。

②若N与此路由器直接相连，数据报直接交付给D，否则间接交付，执行③。

③若路由表中有目的地址为D的特定主机路由，则把数据报传送给路由表中所指明的下一跳路由，否则执行④。

④若路由表中有到达网络N的路由，则把数据报传送给路由表中所指明的下一跳路由，否则执行⑤。

⑤若路由表中有网络前缀一项，就表示使用了CIDR，这时应对路由表中的每一行，用掩码进行和目的站IP地址D相“与”的运算，设得出结果为M。选择M对应的目的站网络号中网络前缀最长的一行，数据报传递给路由表中所指明的下一站路由器；否则，执行⑥。

⑥若路由表中有一个默认路由，则将数据报传递给路由表中所指明的默认路由器；否则，执行⑦。

⑦报告路由选择出错。

24试找出可产生以下数目的A类子网的子网掩码（采用连续掩码）：

（1）2；

（2）6；

（3）30；

（4）62；

（5）122；

（6）250。

答：找出最小的2的m次幂，使其不小于子网数+2，则子网长度应为m，答案如下：

（1）255.192.0.0；

（2）255.224.0.0；

（3）255.248.0.0；

（4）255.252.0.0；

（5）255.254.0.0；

（6）255.255.0.0。

25以下有4个子网掩码，哪些是不推荐使用的？为什么？

（1）176.0.0.0；

（2）96.0.0.0；

（3）127.192.0.0；

（4）255.128.0.0。

答：子网掩码推荐使用一串1和跟随的一串0组成的序列；题中只有（4）是连续的1和连续的0的掩码，是推荐使用的，其余都不推荐使用。

26有如下的4个/24地址块，试进行最大可能的聚合。

212.56.132.0/24

212.56.133.0/24

212.56.134.0/24

212.56.135.0/24

答：题中只有第三个字节不相同，先将其地址转化为二进制表示，然后根据CIDR地址的定义进行聚合；分别转化成二进制表示如下：

132＝（10000100）$_2$；

133＝（10000101）$_2$；

134＝（10000110）$_2$；

135＝（10000111）$_2$；

所以共同的前缀有22位，即11010100 00111000 100001，则聚合的CIDR地址块为：212.56.132.0/22。

27有两个CIDR地址块208.128/11和208.130.28/22。是否有哪一个地址块包含了另一个地址？如果有，请指出，并说明理由。

答：先将地址转化为二进制表示，然后看前缀是否有重复的地方。208.128/11的前缀为：11010000 100；

208.130.28/22的前缀为：11010000 10000010 000111，它的前11位与208.128/11的前缀是一致的，所以208.128/11地址块包含了208.130.28/22这一地址块。

28已知路由器R_1的路由表如表4-12所示。

表4-12　路由器R_1的路由表

地址掩码	目的网络地址	下一跳地址	路由器接口
/26	140.5.12.64	180.15.2.5	m2
/24	130.5.8.0	190.16.6.2	m1
/16	110.71.0.0	—	m0
/16	180.15.0.0	—	m2
/16	190.16.0.0	—	m1
默认	默认	110.71.4.5	m0

试画出各网络和必要的路由器的连接拓扑，标注出必要的IP地址和接口。对不能确定的情况应当指明。

答：各网络和必要的路由器的连接拓扑如图4-6所示。

图4-6　28题答案

29一个自治系统有5个局域网，其连接图如图4-7所示。LAN_2至LAN_5上的主机数分别为：91，150，3和15。该自治系统分配到的IP地址块为30.138.118/23。试给出每一个局域网的地址块（包括前缀）。

图4-7　自制系统连接图

答：对LAN_3，主机数150，（2^7-2）＜150＋1＜（2^8-2），所以主机位为8bit，网络前缀为24，分配地址块30.138.118.0/24；

对LAN_2，主机数91，（2^6-2）＜91＋1＜（2^7-2），所以主机位为7bit，网络前缀为25，分配地址块30.138.119.0/25；

对LAN_5，主机数为15，（2^4-2）＜15＋1＜（2^5-2），所以主机位为5bit，网络前缀27，分配的地址块为30.138.119.192/27；

对LAN_1，主机数为3，（2^2-2）＜3＋1＜（2^3-2），所以主机位为3bit，网络前缀29，分配的地址块为30.138.119.232/29；

对LAN_4，主机数为3，（2^2-2）＜3＋1＜（2^3-2），所以主机位为3bit，网络前缀29，分配的地址块为30.138.119.240/29。

分配网络前缀时应先分配地址数较多的前缀。题目中没有说LAN_1上有几个主机，但至少需要分配三个地址给三个路由器用，所以本题可以有多种答案。

30一个大公司有一个总部和三个下属部门。公司分配到的网络前缀是192.77.33/24，公司的网络布局如图4-8所示，总部共有五个局域网，其中LAN_1～LAN_4都连接到路由器R_1上，R_1再通过LAN_5与路由器R_5相连。R_2和远地的三个部门的局域网LAN_6～LAN_8通过广域网相连。每一个局域网旁边标明的数字是局域网上的主机数。试给每一个局域网分配一个合适的网络前缀。

图4-8　公司系统连接图

答：本题求解思路类似于上题，根据每个局域网的主机数目计算即可，其中一种答案如表4-13所示。

表4-13　局域网分配表

LAN_1	192.77.33.0/26
LAN_3	192.77.33.64/27
LAN_6	192.77.33.96/27
LAN_7	192.77.33.128/27
LAN_8	192.77.33.160/27
LAN_2	192.77.33.192/28
LAN_4	192.77.33.208/28
LAN_5	192.77.33.224/29

31以下地址中的哪一个和86.32/12匹配？请说明理由。

（1）86.33.224.123；

（2）86.79.65.216；

（3）86.58.119.74；

（4）86.68.206.154。

答：题中地址块86.32/12的第二个字节的二进制表示为00100000，前缀12位，说明第二个字节的前四位在前缀中，给出的四个地址的第二字节的前四位分别为：0010，0100，0011和0100，因此只有（1）匹配。

32以下的地址前缀中的哪一个地址和2.52.90.140匹配？请说明理由。

（1）0/4；

（2）32/4；

（3）4/6；

（4）80/4。

答：将2.52.90.140和（1）（2）（3）（4）掩码相“与”的结果仍为2.52.90.140的匹配，故（1）与2.52.90.140匹配。

33下面前缀中的哪一个和地址152.7.77.159及152.31.47.252都匹配？请说明理由。

（1）152.40/13；

（2）153.40/9；

（3）152.64/12；

（4）152.0/11。

答：将152.7.77.159和152.31.47.252分别（1）（2）（3）（4）中的地址按位进行与运算，若仍得到152.7.77.159和152.31.47.252，则相匹配，可知前缀（4）和这两个地址都匹配。

34与下列掩码相对应的网络前缀各有多少位？

（1）192.0.0.0；

（2）240.0.0.0；

（3）255.224.0.0；

（4）255.255.255.252。

答：192的二进制表达式为11000000，故与（1）对应的网络前缀是2比特；同理与（2）对应的网络前缀是4比特；与（3）对应的网络前缀是11比特；与（4）对应的网络前缀是30比特。

35已知地址块中的一个地址是140.120.84.24/20。试求这个地址块中的最小地址和最大地址。地址掩码是什么？地址块中共有多少个地址？相当于多少个C类地址？

答：地址140.120.84.24/20是无分类编址，斜线后面的20是网络前缀的比特数，即IP地址的前20位是网络前缀，后12位为主机号；易知其子网掩码为255.255.240.0；计算最小地址的方法是将IP地址与地址掩码进行与操作，结果为140.120.80.0/20，计算最大地址的方法是将主机号的比特位全部置1，结果为140.120.95.255/20；地址块中共有2^{12}＝4096个地址，相当于16个C类地址。

36已知地址块中的一个地址是190.87.140.202/29，重新计算上题。

答：计算思路与上题同，不同的是此题子网掩码为255.255.255.248；则最小地址为190.87.140.200/29；最大地址为190.87.140.207/29；

地址块中共有2^3＝8个地址，相当于1/32个C类地址。

37某单位分配到一个地址块136.23.12.64/26。现在需要进一步划分为4个一样大的子网。试问：

（1）每个子网的网络前缀有多长？

（2）每一个子网中有多少个地址？

（3）每一个子网的地址块是什么？

（4）每一个子网可分配给主机使用的最小地址和最大地址是什么？

答：（1）在现在地址块的基础上再划分4个同规模的子网，需要两比特的二进制数来表示，故每个子网的网络前缀是26＋2＝28位；

（2）每个子网的地址中有4位留做主机号，因此共有2^4＝16个地址；

（3）子网的地址块由子网的最小地址和地址块的网络前缀位数表示：

第一个子网的地址块是136.23.12.64/28；

第二个子网的地址块是136.23.12.80/28；

第三个子网的地址块是136.23.12.96/28；

第四个子网的地址块是136.23.12.112/28。

（4）因为主机号是全0和全1的地址，一般并不使用，所以主机分配地址如下：

①第一个子网的地址块是136.23.12.64/28，可分配给主机使用的

最小地址：136.23.12.01000001＝136.23.12.65/28；

最大地址：136.23.12.01001110＝136.23.12.78/28。

②第二个子网的地址块是136.23.12.80/28，可分配给主机使用的

最小地址：136.23.12.01010001＝136.23.12.81/28；

最大地址：136.23.12.01011110＝136.23.12.94/28。

③第三个子网的地址块是136.23.12.96/28，可分配给主机使用的

最小地址：136.23.12.01100001＝136.23.12.97/28；

最大地址：136.23.12.01101110＝136.23.12.110/28。

④第四个子网的地址块是136.23.12.112/28，可分配给主机使用的

最小地址：136.23.12.01110001＝136.23.12.113/28；

最大地址：136.23.12.01111110＝136.23.12.126/28。

38IGP和EGP这两类协议的主要区别是什么？

答：IGP是在一个自制系统内部使用的路由选择协议，主要考虑在AS内部如何高效地工作，只关心本自治系统内如何传送数据报，与互联网中其他自治系统使用什么协议无关，对费用和代价考虑不多。EGP是在不同的AS边界传递路由选择信息的协议，不关心AS内部使用何种协议，但必须考虑其他方面的政策，需要多条路由，代价费用方面可能更重要。

39试简述RIP，OSPF和BGP路由选择协议的主要特点。

答：RIP、OSPF和BGP路由选择协议的主要特点，如表4-14所示。

表4-14　RIP、OSPF、BGP路由选择协议主要特点

主要特点	RIP	OSPF	BGP
网关协议	内部	内部	外部
路由表内容	目的网，下一站，距离	目的网，下一站，距离	目的网，完整路由
最优通路依据	跳数	费用	多种策略
算法	距离矢量	链路状态	距离矢量
传送方式	运输层 UDP	IP 数据报	建立 TCP 连接
其他	简单 效率低 跳数为 16，不可达 好消息传得快，坏消息传得慢	效率高 路由频繁交换信息， 难维持一致性	规模大，统一度量， 可达性

40RIP使用UDP，OSPF使用IP，而BGP使用TCP。这样做有何优点，为什么RIP周期性地和邻站交换路由信息而BGP却不这样做？

答：（1）RIP使用UDP，OSPF使用IP，而BGP使用TCP的优点：

①RIP只和邻站交换信息，UDP虽不保证可靠交付，但它满足RIP的要求的同时，开销更小；

②OSPF使用可靠的洪泛法，并直接使用IP，灵活性好并且开销更小；

③BGP需要交换整个路由表并更新信息，TCP提供可靠支付以减少带宽的消耗。

（2）RIP使用不保证可靠交付的UDP，必须不断的（周期性的）和邻站交换信息才能使路由信息及时得到更新；但BGP使用保证可靠交付的TCP，因此不需要这么做。

41假定网络中的路由器B的路由表有如下的项目（这三列分别表示“目的网络”“距离”和“下一跳路由器”）：

N_1	7	A
N_2	2	C
N_6	8	F
N_8	4	E
N_9	4	F

现在B收到从C发来的路由信息（这两列分别表示“目的网络”和“距离”）：

N_2	4
N_3	8
N_6	4
N_8	3
N_9	5

试求出路由器B更新后的路由表（详细说明每一个步骤）。

答：路由表组成为<目的网络N，距离d，下一跳路由器X>，对每一个相邻路由器发送过来的RIP报文，进行路由更新操作为：

（1）对地址为X的相邻路由器发来的RIP报文，先把报文中的所有“下一跳”字段的地址都改为X，并把所有的“距离”字段的值加1；如下所示：

N_2	5	C
N_3	9	C
N_6	5	C
N_8	4	C
N_9	6	C

（2）对修改后的RIP报文中的每一个项目，进行以下步骤：

①当原来的路由表中没有目的网络N时，把该项目添加到路由表中；

②当原来的路由表中有目的网络N且下一跳地址是X时，用收到的项目替换原表中相应项目；

③当原来的路由表中有目的网络N且下一跳地址不是X时，若收到的项目中d小于原表中的d，则用收到的项目更新路由表，否则不进行操作。则②操作如下所示：

N_1	7	A	不用更新
N_2	5	C	相同的下一跳，直接更新
N_3	9	C	新的项目，添加进来
N_6	5	C	不同的下一跳，距离更短，更新
N_8	4	E	不同的下一跳，距离一样，不更新
N_9	4	F	不同的下一跳，距离更大，不更新

42假定网络中的路由器A的路由表有如下的项目（格式同上题）：

N_1	4	B
N_2	2	C
N_3	1	F
N_4	5	G

现在A收到从C发来的路由信息（格式同上题）：

N_1	2
N_2	1
N_3	3
N_4	7

试求出路由器A更新后的路由表（详细说明每一个步骤）。

答：路由表组成为<目的网络N，距离d，下一跳路由器X>，对每一个相邻路由器发送过来的RIP报文，进行路由更新操作为：

（1）对地址为X的相邻路由器发来的RIP报文，先把报文中的所有“下一跳”字段的地址都改为X，并把所有的“距离”字段的值加1；如下所示：

N_1	3	C
N_2	2	C
N_3	4	C
N_4	8	C

（2）对修改后的RIP报文中的每一个项目，进行以下步骤：

①当原来的路由表中没有目的网络N时，把该项目添加到路由表中；

②当原来的路由表中有目的网络N且下一跳地址是X时，用收到的项目替换原表中相应项目；

③当原来的路由表中有目的网络N且下一跳地址不是X时，若收到的项目中d小于原表中的d，则用收到的项目更新路由表，否则不进行操作。则②操作如下所示：

N_1	3	C	不同的下一跳，距离更短，更新
N_2	2	C	相同的下一跳，直接更新
N_3	1	F	不同的下一跳，距离更大，不更新
N_4	5	G	不同的下一跳，距离更大，不更新

43IGMP协议的要点是什么？隧道技术在多播中是怎样使用的？

答：（1）IGMP协议的要点：

①IGMP是用来进行多播的，采用多播协议可以明显地减轻网络中各种资源的消耗，IP多播实际上只是硬件多播的一种抽象。

②IGMP只有两种分组，即询问分组和响应分组。IGMP使用IP数据报传递其报文，但它也向IP提供服务。

③IGMP属于整个网际协议IP的一个组成部分。

（2）隧道技术的实现：当多播数据报在传输过程中遇到不运行多播路由器的网络时，路由器就对多播数据报进行再次封装（即添加首部），通过了隧道以后，再由路由器剥去其首部，使它又恢复成原来的多播数据报，继续向多个目的站转发。

44什么是VPN？VPN有什么特点和优缺点？VPN有几种类型？

答：（1）由于IP地址紧缺，对一个机构而言，所能申请的IP地址一般小于本机构的主机数，此时可以选用一些只能在本机构使用的内部地址，并利用公用的互联网作为本机构各专用网之间的通信载体，这样的专用网称为虚拟专用网VPN。

（2）VPN的特点：

①VPN通过建立一个隧道，利用加密技术对传输数据进行加密，以保证数据的私有性和安全性；

②具有很好的扩充性和灵活性；

③VPN可以从用户和运营商角度方便进行管理；

④VPN可以为不同要求用户提供不同等级的服务质量保证。

（3）VPN的优点：

①连接方便灵活；

②使用VPN可降低成本；

③传输数据安全可靠；

④虚拟专用网使用户可以利用ISP的设施和服务且完全掌握着自己网络的控制权。

（4）VPN的缺点：VPN比普通网络更复杂，需购买专门的硬件和软件，费用比普通网络更高。

（5）①按VPN的协议分类：VPN的隧道协议主要有3种，PPTP、L2TP和IPSec，其中PPTP和L2TP协议工作在OSI模型的第二层，又称为二层隧道协议；IPSec是第三层隧道协议，是最常见的协议。L2TP和IPSec配合使用是目前性能最好、应用最广泛的一种。

②按VPN的应用分类：分别是内联网，外联网和远程接入VPN，其中内联网的各网点属于同一机构，而外联网的网点属于不同机构。

③按所用的设备类型进行分类：网络设备提供商针对不同客户的需求，开发出不同的VPN网络设备，主要为交换机、路由器和防火墙。

45什么是NAT？NAPT有哪些特点？NAT的优点和缺点有哪些？

答：（1）NAT即网络地址转换；它能够完成将专用网络地址转换成公用网络地址；

NAT的优点：

①通过NAT，专用网内部主机可使用专用地址与因特网上的主机通信；

②通过NAT，一个全球合法IP地址可被多台专用网内部主机分享使用，节省全球IP地址资源。

NAT的缺点：通信必须由专用网内的主机发起，专用网内部的主机不能充当服务器。

（2）NAPT即网络地址与端口号转换；其特点是：

①在路由器转发IP数据报时，NA,PT对IP地址和端口号都进行转换，对于出专用网的数据，把专用网内不同的源IP地址转换为同样的全球IP地址，把源主机端口号转换为不同的新的端口号；对于入专用网的应答，NAPT根据不同的目的端口号，从NAPT转换表中找到正确的目的主机；

②NAPT工作在网络层和传输层。

46试把下列IPv4地址从二进制记法转换为点分十进制记法。

（1）10000001 00001011 00001011 11101111

（2）11000001 10000011 00011011 11111111

（3）11100111 11011011 10001011 01101111

（4）11111001 10011011 11111011 00001111

答：（1）129.11.11.239；

（2）193.131.27.255；

（3）231.219.139.111；

（4）249.155.251.15。

47下列IPv4地址是否存在错误？如有，请指明。

（1）111.56.045.78

（2）221.34.7.8.20

（3）75.45.301.14

（4）11100010.23.14.67

答：（1）错误；点分十进制中不应该包括类似于045这样以0开头的数；

（2）错误；IPv4地址长度为4个字节，该地址超过了四个字节；

（3）错误；IPv4地址的每个字节的数小于等于255，题中301超过了255；

（4）错误；不允许将二进制记法与点分十进制记法混合使用。

48假设一段地址的首地址为146.102.29.0，末地址为146.102.32.255，求这个地址段的地址数。

答：以上两个地址的二进制表示分别为：

首地址：10010010 01100110 00011101 00000000；

末地址：10010010 01100110 00100000 11111111；

显然这两个地址为B类地址，且前两个字节的地址相等，第三个字节29到32有32－29＋1＝4个地址段，则这个地址段的地址数＝4×256＝1024。

49求下列每个地址的类别。

（1）00000001 00001011 00001011 11101111

（2）11000001 10000011 00011011 11111111

（3）10100111 11011011 10001011 01101111

（4）11110011 10011011 11111011 00001111

答：（1）A类；

（2）C类；

（3）B类；

（4）E类。

50求下列每个地址的类别

（1）227.12.14.87

（2）193.14.56.22

（3）14.23.120.8

（4）252.5.15.111

答：可将题中的点分十进制的第一个字节用二进制表示出来，再对比IPv4各类地址的特征可知：

（1）D类；

（2）C类；

（3）A类；

（4）E类。

51给出某地址块中的一个地址为73.22.17.25。求该地址块的地址数及其首地址和末地址。

答：73的二进制表示为：01001001，可知该地址是A类地址，故该地址块的地址数为2^{24}＝16777216，首地址是73.0.0.0，末地址是73.255.255.255。

52已知某网络有一个地址是167.199.170.82/27，问这个网络的网络掩码、网络前缀长度和网络后缀长度是多少？

答：由于167.199.170.82/27的网络号占27位，则子网掩码为255.255.255.224，网络前缀长度为27，网络后缀长度为32－27＝5。

53已知地址块中的一个地址是167.199.170.82/27，求这个地址块的地址数、首地址以及末地址各是多少？

答：由于167.199.170.82/27的网络号占27位，则该地址块的地址数＝2^5＝32，首地址为167.199.170.64，末地址为167.199.170.95。

54某单位分配到一个初始地址块为14.24.74.0/27的地址块。该单位需要用到三个子网，他们的三个子地址块的具体要求是：子网N_1需要120个地址，子网N_2需要60个地址，子网N_3需要10个地址。请给出地址块的分配方案。

答：根据每个子网需要的地址数可以进行如下分配：

N_1子网分配14.24.74.0/25～14.24.74.127/25范围的地址；

N_2子网分配14.24.74.128/26～14.24.74.191/26范围的地址；

N_3子网分配14.24.74.192/28～14.24.74.207/28范围的地址。

55如图4-9所示，网络145.13.0.0/16划分为四个子网N_1，N_2，N_3和N_4。这四个子网与路由器R连接的接口分别是m0，m1，m2和m3。路由器R的第五个接口m4连接到互联网。

图4-9　55题图

（1）试给出路由器R的路由表。

（2）路由器R收到一个分组，其目的地址是145.13.160.78。试给出这个分组是怎样被转发的。

答：（1）根据图4-9所示，可知路由器R的路由表如下所示：

目的网络地址	目的网络地址的子网掩码	下一跳
145.13.0.0	255.255.192.0	直接交付，接口 m0
145.13.64.0	255.255.192.0	直接交付，接口 m1
145.13.128.0	255.255.192.0	直接交付，接口 m2
145.13.192.0	255.255.192.0	直接交付，接口 m3
其他	—	默认路由器，接口 m4

（2）收到的分组目的地址为145.13.160.78，与255.255.192.0进行“与”操作得145.13.128.0，则该分组从路由器的接口m2转发。

56收到一个分组，其目的地址D＝11.1.2.5。要查找的路由表中有这样三项：

路由1　到达网络11.0.0.0/8

路由2　到达网络11.1.0.0/16

路由3　到达网络11.1.2.0/24

试问在转发这个分组时应当选择哪一个路由？

答：目的地址为D＝11.1.2.5，根据最长前缀匹配原则，可知路由3能与之匹配，则应选择路由3。

57同上题。假定路由1的目的网络11.0.0.0/8中有一台主机H，其IP地址是11.1.2.3。当我们发送一个分组给主机H时，根据最长前缀匹配准则，上面的这个路由表却把这个分组转发到路由3的目的网络11.1.2.0/24。是最长前缀匹配准则有时会出错吗？

答：最长前缀匹配准则本身是不存在问题的；

理由：主机H的IP地址分配错误才是问题产生的原因，网路11.0.0.0/8在分配网络主机号时，不允许使用11.1.0.0/16上的任何一台主机号，更不会允许分配11.1.2.0/24网络上的主机号，这样才能避免地址混乱。

58已知一CIDR地址块为200.56.168.0/21。

（1）试用二进制表示这个地址块。

（2）这个CIDR地址块包括有多少个C类地址块？

答：（1）该地址块的二进制表示为：11001000 00111000 10101000 00000000（下划线部分为网络号）；

（2）由于C类地址网络号占24位，则该地址块还包括$2^{(24-21)}$＝8个C类地址块。

59建议的IPv6协议没有首部检验和。这样做的优缺点是什么？

答：由于数据链路层已经将有差错的帧丢弃了，网络层没必要再进行检验，IPv6省去这个步骤使得对首部的处理更简单。

60在IPv4首部中有一个“协议字段”，但在IPv6的固定首部中却没有。这是为什么？

答：IPv6使用“下一个首部”字段代替IPv4的“协议”字段完成相关功能。

61当使用IPv6时，ARP协议是否需要改变？如果需要改变，那么应当进行概念性的改变还是技术性的改变？

答：IPv6已经没有ARP协议了；但IPv6中的ICMPv6包括了IPv4中的ARP的功能，也就是说，从概念上讲，ARP的功能在IPv6中仍然是不可缺少的，但在技术上却进行了很多改进。

62IPv6只允许在源点进行分片。这样做有什么好处？

答：好处是能够加快网络中IP数据报的转发速度（分片与重装是十分耗时的）。

63设每隔1微微秒就分配出100万个IPv6地址。试计算大概要用多少年才能将IPv6地址空间全部用光。可以和宇宙的年龄（大约有100亿年）进行比较。

答：IPv6地址空间大小为2^{128}（即3.4×10^{38}），由题可知1s可以分配10^{18}个地址，一年可分配$10^{18}\times60\times60\times24\times365=3.15\times10^{25}$，则可分配$3.4\times10^{38}/(3.15\times10^{25})=1.08\times10^{13}$年，大约是宇宙年龄的1000倍，显然即便地址空间不均匀分配也不会用完。

64试把以下的IPv6地址用零压缩方法写成简洁形式：

（1）0000:0000:0F53:6382:AB00:67DB:BB27:7332

（2）0000:0000:0000:0000:0000:0000:004D:ABCD

（3）0000:0000:0000:AF36:7328:0000:87AA:0398

（4）2819:00AF:0000:0000:0000:0035:0CB2:B271

答：（1）::F53:6382:AB00:67DB:BB27:7332；

（2）::4D:ABCD；

（3）::AF36:7328:0:87AA:398；

（4）2819:AF::35:CB2:B271。

65试把以下的零压缩的IPv6地址写成原来的形式：

（1）0::0

（1）0:AA::0

（3）0:1234::3

（4）123::1:2

答：（1）0000:0000:0000:0000:0000:0000:0000:0000；

（2）0000:00AA:0000:0000:0000:0000:0000:0000；

（3）0000:1234:0000:0000:0000:0000:0000:0003；

（4）0123:0000:0000:0000:0000:0000:0001:0002。

66从IPv4过渡到IPv6的方法有哪些？

答：由IPv4到IPv6过渡可以采用两种方法：

（1）双协议栈技术：在完全过渡到IPv6之前，使部分主机（或路由器）装有两个协议栈分别适用两类地址；

（2）隧道技术：将整个IPv6数据报封装到IPv4数据报的数据部分，使IPv6可以在IPv4网络的隧道中传输。

67多协议标记交换MPLS的工作原理是怎样的？它有哪些主要的功能？

答：（1）工作原理：在MPLS域的入口处，给每一个IP数据报一个固定长度的“标记”，然后用硬件转发它们，使得IP数据报转发过程加快；

（2）主要功能：属于一种面向连接的连网技术；通过给IP数据报打上标记，加快IP数据报的转发速度；具有转发等价类FEC的功能；通过对特殊路由器的管理，能解决网络中负载均衡和拥塞问题，当网络拥塞时，可实时建立新的转发路由分散流量以缓解网络拥塞。

4.3　考研真题详解

一、选择题

1若将101.200.16.0/20划分为5个子网，则可能的最小子网的可分配IP地址数是（　　）。[2019年408统考]

A．126

B．254

C．510

D．1022

【答案】B

【解析】①101.200.16.0/20可写为101.200.00010000.0/20，从第21位（包含21位）开始，取一位可以划分为两个子网，即101.200.00010000.0/21和101.200.00011000.0/21；

②将第二个子网再次划分，划分出新的第二个子网和第三个子网，即将101.200.00011000.0/21划分为101.200.00011000.0/22和101.200.00011100.0/22；

③将第三个子网再次划分，划分出新的第三个子网和第四个子网，即将101.200.00011100.0/22划分为101.200.00011100.0/23和101.200.00011110.0/23；

④将第四个子网再次划分，划分出新的第四个子网和第五个子网，即将101.200.00011110.0/23划分为101.200.00011110.0/24和101.200.00011111.0/24；

综上，可以得出，最小子网的前缀为24，子网大小为$2^8-2=254$，答案选B。

2以下不具有信道侦听功能的多路访问协议是（　　）。[西安电子科技大学2018研]

A．CSMA

B．CSMA/CA

C．CSMA/CD

D．ALOHA

【答案】D

【解析】ALOHA协议在任意时间都可以发送，如果遇到冲突，则随机等待一段时间再次发送。而CSMA协议是改进的ALOHA协议，先听后发，边发边听，具有信道侦听功能。答案选D。

3某路由表中有转发接口相同的4条路由表项，其目的网络地址分别为35.230.32.0/21、35.230.40.0/21、35.230.48.0/21和35.230.56.0/21，将该4条路由聚合后的目的网络地址为（　　）。[2018年408统考]

A．35.230.0.0/19

B．35.230.0.0/20

C．35.230.32.0/19

D．35.230.32.0/20

【答案】C

【解析】根据最长前缀匹配原则，四条路由表项可以分别表示为：

①35.230.00100000.0/21

②35.230.00101000.0/21

③35.230.00110000.0/21

④35.230.00111000.0/21

将以上四条路由表项进行“与”运算，得到35.230.00100000.0/19即35.230.32.0/19，答案选C。

4某路由器的路由表如下表所示：

目的网络	下一跳	接口
169.96.40.0/23	176.1.1.1	S1
169.96.40.0/25	176.2.2.2	S2
169.96.40.0/27	176.3.3.3	S3
0.0.0.0/0	176.4.4.4	S4

若路由器收到一个目的地址为169.96.40.5的IP分组，则转发该IP分组的接口是（　　）。[2015年408统考]

A．S1

B．S2

C．S3

D．S4

【答案】C

【解析】根据“最长前缀匹配原则”，169.96.40.5与169.96.40.0的二进制表示的前27位匹配，故选C。选项D为默认路由，只有当前面的所有目的网络都不能和分组的目的IP地址匹配时才使用。

5某主机的IP地址为180.80.77.55，子网掩码为255.255.252.0。若该主机向其所在子网发送广播分组，则目的地址可以是（　　）。[2012年408统考]

A．180.80.76.0

B．180.80.76.255

C．180.80.77.255

D．180.80.79.255

【答案】D

【解析】此题其实就是求该网络的广播地址。首先，由IP地址的第一字节180，可以判断主机的IP地址为B类地址。另外，从子网掩码255.255.252.0中可以判断该网络从主机位拿出6位作为子网号。所以，可以得出主机位为10位。接下来将77转换成二进制，即01001101。保持前6位不变，将后两位以及IP地址的最后一个字节都置为1，即0100111111111111，转换成十进制为79.255。故该网络的广播地址为：180.80.79.255。

6下列关于IP路由器功能的描述中，正确的是（　　）。[2012年408统考]

Ⅰ．运行路由协议，设置路由表

Ⅱ．监测到拥塞时，合理丢弃IP分组

Ⅲ．对收到的IP分组头进行差错校验，确保传输的IP分组不丢失

Ⅳ．根据收到的IP分组的目的IP地址，将其转发到合适的输出线路上

A．仅Ⅲ、Ⅳ

B．仅Ⅰ、Ⅱ、Ⅲ

C．仅Ⅰ、Ⅱ、Ⅳ

D．Ⅰ、Ⅱ、Ⅲ、Ⅳ

【答案】C

【解析】路由器的基本功能可以定义为：路由处理和分组转发。

Ⅰ：路由器上都会运行相应的路由协议，如RIP、OSPF协议等；另外，设置路由表也是路由器必须完成的，故Ⅰ正确。

Ⅱ：当监测到拥塞时，路由器会将IP分组丢弃，并向源点发送源点抑制报文，故Ⅱ正确。

Ⅲ：尽管路由器会对IP分组首部进行差错校验，但是不能确保传输的IP分组不丢失。当路由器收到的数据报的首部中有的字段值不正确时，就丢弃该数据报，并向源站发送参数问题报文，故Ⅲ错误。

Ⅳ：这是路由表最基本的路由功能，当路由器某个输入端口收到分组，路由器将按照分组要去的目的地（即目的网络），把该分组从路由器的某个合适的输出端口转发给下一跳路由器。下一跳路由器也按照这种方法处理分组，直到该分组到达终点为止，故Ⅳ正确。

7ARP的功能是（　　）。[2012年408统考]

A．根据IP地址查询MAC地址

B．根据MAC地址查询IP地址

C．根据域名查询IP地址

D．根据IP地址查询域名

【答案】A

【解析】ARP协议的主要功能是用于将IP地址解析到MAC地址。ARP请求分组是广播发送的，而ARP响应分组是普通的单播。ARP是一种用于将各种协议地址解析成物理地址的协议，因此报文格式中的两个长度字段分别指出后面各个地址字段的长度；硬件类型字段指出发送方物理网络类型（1代表以太网）；协议类型字段指明发送方所请求解析的协议地址类型（0x0800代表IP协议）；操作字段指明报文的类型，1为ARP请求，2为ARP响应。

8在子网192.168.4.0/30中，能接受目的地址为192.168.4.3的IP分组的最大主机数是（　　）。[2011年408统考]

A．0

B．1

C．2

D．4

【答案】C

【解析】在网络192.168.4.0/30中只有两位主机号，取值范围为：192.168.4.0～192.168.4.3；

可以发现192.168.4.3恰好是其广播地址（广播地址的概念就是主机号全为“1”）。既然是广播地址，所以只要是在此网络内的主机，全部都可以接收到广播地址所发出的IP分组。而此网络一共有两个主机（4－2＝2，要去掉全“0”和全“1”）。

二、综合题

某公司网络如图4-10所示。IP地址空间192.168.1.0／24被均分给销售部和技术部两个子网，并已分别为部分主机和路由器接口分配了IP地址，销售部子网的MTU＝1500B，技术部子网的MTU＝800B。

请回答下列问题。

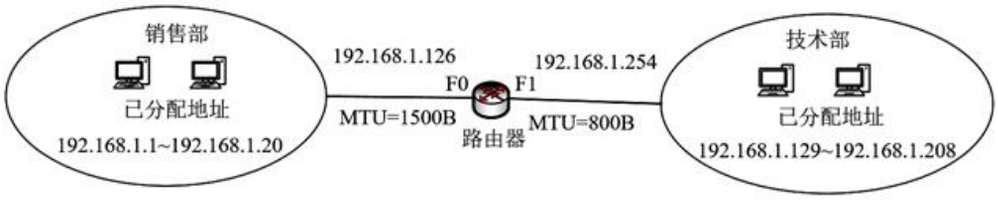

图4-10

（1）销售部子网的广播地址是什么？技术部子网的子网地址是什么？若每个主机仅分配一个IP地址，则技术部子网还可以连接多少才主机？

（2）假设主机192.168.1.1向主机192.168.1.208发送一个总长度为1500B的IP分组，IP分组的头部长度为20B，路由器在通过接口F1转发该IP分组时进行了分片。若分片时尽可能分为最大片，则一个最大IP分片封装数据的字节数是多少？至少需要分为几个分片？每个分片的片偏移量是多少？[2018年408统考]

答：

（1）分析：该IP地址空间需要分为两个子网，即网络号只有1位，主机号有7位，每个子网可用主机数为27根据图可知销售部的网络号为0，主机号全为1即为其广播地址。技术部的网络号为1，可用主机为27－2－（208－129）＋1＋1。

销售部子网的广播地址是192.168.1.127，技术部子网的子网地址是192.168.1.128；技术部子网还可以连接主机数：126－（（208－129）＋1＋1）＝45（台）。

（2）分析：由图可知，端口F1的最大传输单元为800B，其中IP分组的头部固定长度为20B，这里需要注意分片的数据长度必须为8B的整数倍，即最大IP分片封装数据的字节数需要向下取整，至少需要的分片数则要向上取整。第一次传时，片偏移为0。第二次传时，片偏移为776/8=97。

最大IP分片封装数据的字节数：⌊（800-20）/8⌋×8＝776，至少需要的分片数：⌈（1500－20）/776⌉＝2，2个分片的片偏移量分别是：0和97。

第5章　运输层

5.1　复习笔记

一、运输层协议概述

1运输层的功能

从通信和信息处理角度讲，传输层向应用层提供服务，是面向通信的最高层，也是面向用户功能的最底层，它的主要功能有：

（1）提供用户进程之间的逻辑通信（端到端通信）；

（2）提供复用与分用；

（3）对收到的报文进行差错检测；

（4）提供面向连接的TCP协议和无连接的UDP协议。

2运输层的端口

（1）端口的作用

①应用层的各个进程的数据可以通过端口向下交付给传输层；

②传输层的数据可以通过端口上交给应用层。

（2）端口号

应用进程可以通过端口号进行标识，可将端口号分为两类：

①服务端使用的端口号

服务端可以使用范围为0～1023的熟知端口号和范围为1024～49151的登记端口号两类。如表5-1所示为常用的熟知端口号（需要记住）。

表5-1　常用熟知端口号

应用程序	FTP	TELNET	SMTP	DNS	TFTP	HTTP	SNMP
端口号	21	23	25	53	69	80	161

②客户端使用的端口号

这类端口号仅在客户进程运行时才动态选择，范围为49152～65535，又叫临时端口号。

二、用户数据报协议UDP

1UDP概述

（1）UDP的概念

在IP的数据报服务之上增加了复用和分用功能以及差错检测功能，且UDP只做传输层协议能做的最少工作。

（2）UDP的主要特点

①UDP是无连接的，发送数据之前不需要建立连接，减少了开销和发送数据之前的时延；

②UDP是尽最大努力交付的，不保证可靠交付；

③UDP是面向报文的，发送方的UDP对应用程序交下来的报文，在添加首部后就向下交付给IP层；

④UDP没有拥塞控制，因此网络出现的拥塞不会使源主机的发送速率降低；

⑤UDP支持一对一、一对多、多对一和多对多的交互通信；

⑥UDP的首部开销小，只有8个字节，比TCP的20个字节的首部要短。

2UDP的首部格式

如图5-1所示，用户数据报UDP有数据字段和首部字段，首部字段只有8个字节，共四个字段（见表5-2）。

表5-2　UDP首部字段

字段	解释
源端口	源端口号，在需要对方回信时选用，不需要时可用全 0
目的端口	目的端口号，在终点交付报文时必须要使用
长度	UDP 用户数据报的长度，其最小值是 8（仅有首部）
检验和	检测 UDP 用户数据报在传输中是否有错，有错就丢弃

【注意】UDP检验采用的方式为：

①在发送方，将全“0”放入检验和字段，并添加伪首部，再将UDP数据报看成由许多16位的字符串连接起来，在通过二进制反码运算求和并将结果存入检验和字段；

②在接收方，将收到的UDP数据报及伪首部按二进制反码计算求和，若和为全“1”，则无差错，否则丢弃。

图5-1　UDP用户数据报的首部和伪首部

三、传输控制协议TCP概述

1TCP最主要的特点

（1）TCP是面向连接的运输层协议，在使用TCP协议之前，必须先建立TCP连接；

（2）每一条TCP连接只能有两个端点，每一条TCP连接只能是点对点的（一对一）；

（3）TCP提供可靠交付的服务，通过TCP连接传送的数据，无差错、不丢失、不重复、并且按序到达；

（4）TCP提供全双工通信；

（5）面向字节流，TCP中的“流”指的是流入到进程或从进程流出的字节序列。

2TCP的连接

TCP将连接作为最基本的抽象，且TCP连接的端点叫做套接字；可用套接字标识网络上某主机上的某应用（进程），套接字＝（主机IP地址，端口号）。

四、可靠传输的工作原理

1停止等待协议

（1）停止等待的概念

在全双工工作方式下，通信双方既是发送方又是接收方；“停止等待”即每发送完一个分组就等待对方的确认，确认后再发送下一个分组。

（2）停止等待协议的两种基本情况

①无差错情况：如图5-2（a）所示，A发送分组M_1，等待B确认M_1后再继续发送M_2；

图5-2　停止等待协议

②出现差错

分组可能在传输过程中出现差错，主要有以下情况：

a．超时重传：如图5-2（b）所示，B接收M_1时检测出差错后丢弃M_1，停止等待协议要求A每发完一个分组便设置一个超时计时器，当A超过一段时间仍未收到确认，就认为刚才发送的分组丢失，并进行超时重传；

b．确认丢失：如图5-3（a）所示，B接收到无差错的M_1时，向A发回确认，但在途中确认丢失，A仍然无法得到B的确认，此时A进行超时重传，且在重传的新的M_1到达B时，B将丢弃重复的M_1并发回重传确认；

c．确认迟到：如图5-3（b）所示，M_1传输并无差错，只是M_1的确认到达A时迟到了，此时A对重复的确认什么也不做，而B对丢弃重复的M_1。

图5-3　确认丢失和确认迟到

【注意】

①发送方发送完一个分组后，必须暂时保留已发送的分组的副本；

②分组和确认分组都必须进行编号；

③超时计时器设置的重传时间应当比数据在分组传输的平均往返时间更长一些；

④停止等待协议信道利用率低（信道利用率＝发送分组需要的时间/（发送分组需要的时间＋往返时间＋确认分组需要的时间））。

2连续ARQ协议

如图5-4（a）所示，发送方维持的发送窗口大小为5，位于发送窗口内的5个分组都可连续发送出去，而不需要等待对方的确认。连续ARQ协议规定发送方每收到一个确认，就把发送窗口向前滑动一个分组的位置，如图5-4（b）所示；接收方一般采用累积确认的方式，在收到几个分组后，对按序到达的最后一个分组发送确认。

图5-4　连续ARQ协议的工作原理

五、TCP报文段的首部格式

TCP传输的数据单元称为TCP报文段，首部的前20个字节是固定的，如图5-5所示，后面有4n字节是可选的，TCP首部的最小长度是20字节。其首部各字段说明如下（见表5-3）。

表5-3　TCP报文段首部字段

字段	解释
源端口和目的端口	各占 2 个字节，分别写入源端口号和目的端口号
序号	占 4 字节，指本报文段发送的数据的第一个字节的序号
确认号	占 4 字节，是期望收到对方下一个报文段的第一个数据字节的序号
数据偏移（即首部长度）	占 4 位，指出 TCP 报文段的数据起始处距离 TCP 报文段的起始处有多远
保留	占 6 位，保留为今后使用，但目前应置为 0
紧急位 URG	当 URG＝1 时，表明紧急指针字段有效
确认位 ACK	仅当 ACK＝1 时确认号字段才有效，TCP 连接建立后所有传送的报文段 ACK 均置为 1
推送位 PSH	当 PSH＝1 时，将报文段尽快交付给应用程序
复位位 RST	当 RST＝1 时，TCP 连接中出现严重差错，必须释放连接，再重新建立运输连接
同步位 SYN	在连接建立时用来同步序号，SYN＝1 表示该报文为连接请求或接收报文
终止位 FIN	当 FIN＝1 时，表示该报文段发送方数据发送完毕，请求释放连接
窗口	占 2 字节，指出当前允许对方发送的数据量
检验和	占 2 字节，检验和字段检验的范围包括首部和数据两部分
紧急指针	占 2 字节，它指出本报文段中紧急数据的字节数
选项	长度可变，最长可达 40 字节

图5-5　TCP报文段的首部格式

六、TCP可靠传输的实现

1以字节为单位的滑动窗口

在任意时刻，发送方维持一组允许发送的帧的序号，即发送窗口；接收方维持一组允许接收的帧的序号，称为接收窗口；TCP的滑动窗口是以字节为单位的，其工作原理如图5-6与图5-7所示，其中P_1、P_2、P_3是发送窗口的三个状态指针：

（1）构造发送窗口（发送方由接收方发回的确认报文构造自己的发送窗口）；

（2）发送方发送数据，接收方收到数据后发回确认；

（3）发送方每收到一个确认，发送窗口便向前滑动一个位置，当发送窗口内没有可以发送的数据时（窗口内的数据全部发送但未收到确认），发送方停止发送，直到收到接收方的确认使窗口移动后才能继续发送；

（4）接收方每收到一个数据，接收窗口前移一个位置，并发回确认，接收窗口外的数据一律丢弃。

图5-6　根据B给出的窗口值，A构造出自己的发送窗口

图5-7　A发送了11个字节的数据

2超时重传时间的选择

TCP的发送方在规定时间内未收到确认时需要进行重传，而超时重传时间的选择采用一种自适应算法：

（1）从第一次测量RTT样本开始，计算加权平均往返时间：新的RTT_S＝（1－α）×（旧的RTT_S）＋α×（新的RTT样本），其中0≤α＜1，RFC 6298推荐的α＝1/8＝0.125；

（2）计算RTT的偏差的加权平均值：新的RTT_D＝（1－β）×（旧的RTT_D）＋β×|RTT_S－新的RTT样本|，这里β是小于1的系数，推荐使用1/4＝0.25；

（3）超时计时器设置的超时重传时间RTO＝RTT_S＋4RTT_D。

3选择确认SACK

TCP的接收方在接收发送方发送的序号不连续的数据字节流时，若这些字节的序号都在接收窗口之内，那么接收方就先收下这些数据，但要把这些信息准确地告诉发送方，使发送方不要再重复发送这些已收到的数据；而这些准确信息便包括了每一个字节块的左边界和右边界，这时的确认除了保持原有的“确认号字段”不变外，还需要在TCP首部增加SACK选项。

七、TCP的流量控制

TCP的流量控制是使用滑动窗口实现的，记接收窗口为rwnd，发送方A发送数据给接收方B，B向A发送确认报文，这时确认报文首部中的窗口字段将rwnd通知给A，A再通过rwnd控制自己发送窗口的大小。例如图5-8所示。

图5-8　利用可变窗口进行流量控制举例

图5-8中的例子存在一种特殊情况，若B向A发送了零窗口的报文段后不久，B又向A发送了rwnd＝400的报文段，然而这个报文段在传送过程中丢失了，A一直等待收到B发送的非零窗口的通知，而B也一直等待A发送的数据，这就造成了死锁；为解决这个问题可以为每一个连接设置一个持续计时器。

八、TCP的拥塞控制

1拥塞控制和流量控制的区别

（1）拥塞控制是为了让网络能够承受现有的网络负荷，防止过多数据注入网络，是一个全局控制过程；

（2）流量控制是接收方控制发送方，是一种点对点的流量的控制。

2几种拥塞控制方法

（1）慢开始和拥塞避免

①慢开始算法

建立了TCP连接并开始发送报文段时，令拥塞窗口cwnd＝1（即一个最大报文长度MSS），并在每次收到一个对新的报文段的确认后，使cwnd＋1，这种使得每经过一个往返时延RTT后拥塞窗口cwnd加倍（即cwnd的大小呈指数增长）直到cwnd增大到慢开始门限ssthresh的过程叫慢开始算法。

②拥塞避免算法

发送端的拥塞窗口cwnd每经过一个往返时延RTT就增加一个MSS的大小（按线性增长），直到出现一次超时（网络拥塞），令慢开始门限ssthresh等于当前cwnd的一半，这种算法叫拥塞避免算法。

③网络拥塞的处理过程

例如在如图5-9所示的例子中，拥塞处理过程如下：

a．初始时，拥塞窗口cwnd＝1，慢开始门限的初始值ssthresh＝16个报文段；

b．在执行慢开始算法时，拥塞窗口cwnd的初始值为1，以后发送方每收到一个对新报文段的确认ACK，就把拥塞窗口值加1，然后开始下一轮的传输，这个过程呈指数增长，当拥塞窗口cwnd增长到慢开始门限值ssthresh时，就改为执行拥塞避免算法，此时拥塞窗口按线性规律增长。

c．假定拥塞窗口的数值增长到24时，网络出现超时（网络拥塞），更新ssthresh＝12（即变为超时时刻的拥塞窗口数值24的一半），拥塞窗口再重新设置为1，并继续执行a～c的过程。

图5-9　慢开始和拥塞避免算法的实现举例

（2）快重传和快恢复

①快重传

当发送端连续收到三个重复的ACK报文时，直接重传对方尚未收到的报文段，而不必等待超时计时器超时。

②快恢复

如图5-10所示，快恢复算法要求当发送方连续收到三个重复确认时，就执行“乘法减小”算法，把慢开始门限ssthresh减小为当前cwnd的一半，再令cwnd＝新的ssthresh，之后执行拥塞避免算法，使cwnd线性增长。

【注意】不管是拥塞控制还是流量控制都会影响发送窗口的大小，即发送窗口大小取两者的最小值。

图5-10　快恢复算法示例

九、TCP的运输连接管理

1TCP的连接建立

如图5-11所示，TCP连接的建立即三次握手的过程，其步骤如下：

（1）客户机向服务器发送一个连接请求报文，其中SYN＝1，且随机选择一个起始序号seq＝x；

（2）服务器收到连接请求报文后，若同意建立连接则发回确认并为该TCP连接分配TCP缓存和变量，确认报文中SYN＝1，ACK＝1，确认号字段ack＝x＋1，并产生服务器的随机起始序号seq＝y；

（3）客户机收到确认报文后，还需向服务器发送确认，且需要给该连接分配TCP缓存和变量，这个报文中ACK＝1，seq＝x＋1，ack＝y＋1。

图5-11　用三次握手建立TCP连接

2TCP的连接释放

如图5-12所示，TCP连接的释放即四次挥手的过程，其步骤如下：

（1）客户机想释放连接时，向服务器发送连接释放报文，并停止发送数据（主动关闭连接），该报文中FIN＝1，seq＝u（这里u是前面传送过的数据的最后一个字节的序号加1），注意此时服务器仍能向客户机发送数据。

（2）服务器收到连接释放请求后发送确认报文，其中ACK＝1，seq＝v，ack＝u＋1，此时客户机到服务器这个方向的连接释放成功。

（3）若服务器想释放连接，则向客户机发送连接释放报文，此时FIN＝1，ACK＝1，seq＝w，ack＝u＋1。

（4）客户机收到服务器的连接释放请求后，也需要发送确认报文，此时ACK＝1，seq＝u＋1，ack＝w＋1，之后TCP连接还需要时间等待计时器设置的时间2MSL后才能关闭连接。

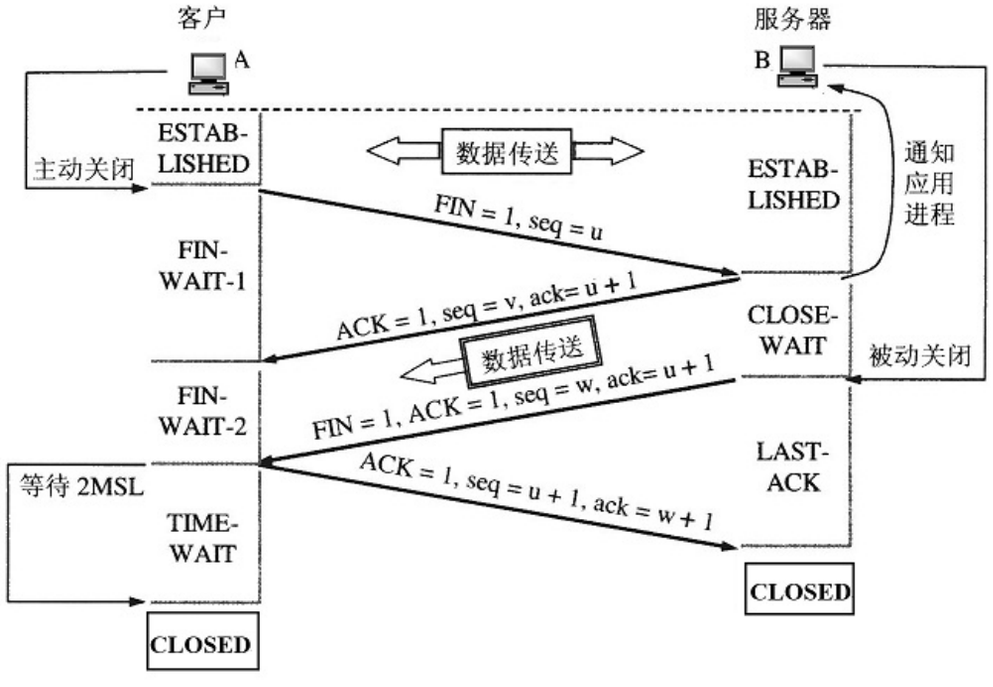

图5-12　TCP连接释放的过程

3TCP的有限状态机

如图5-13所示为TCP连接的各种状态之间的关系，即给出了TCP的有限状态机。图中每一个方框即TCP可能具有的状态。每个方框中的大写英文字符串是TCP连接状态名。状态之间的箭头表示可能发生的状态变迁。箭头旁边的字，表明引起这种变迁的原因，或表明发生状态变迁后又出现什么动作。粗实线箭头表示对客户进程的正常变迁。粗虚线箭头表示对服务器进程的正常变迁。另一种细线箭头表示异常变迁。

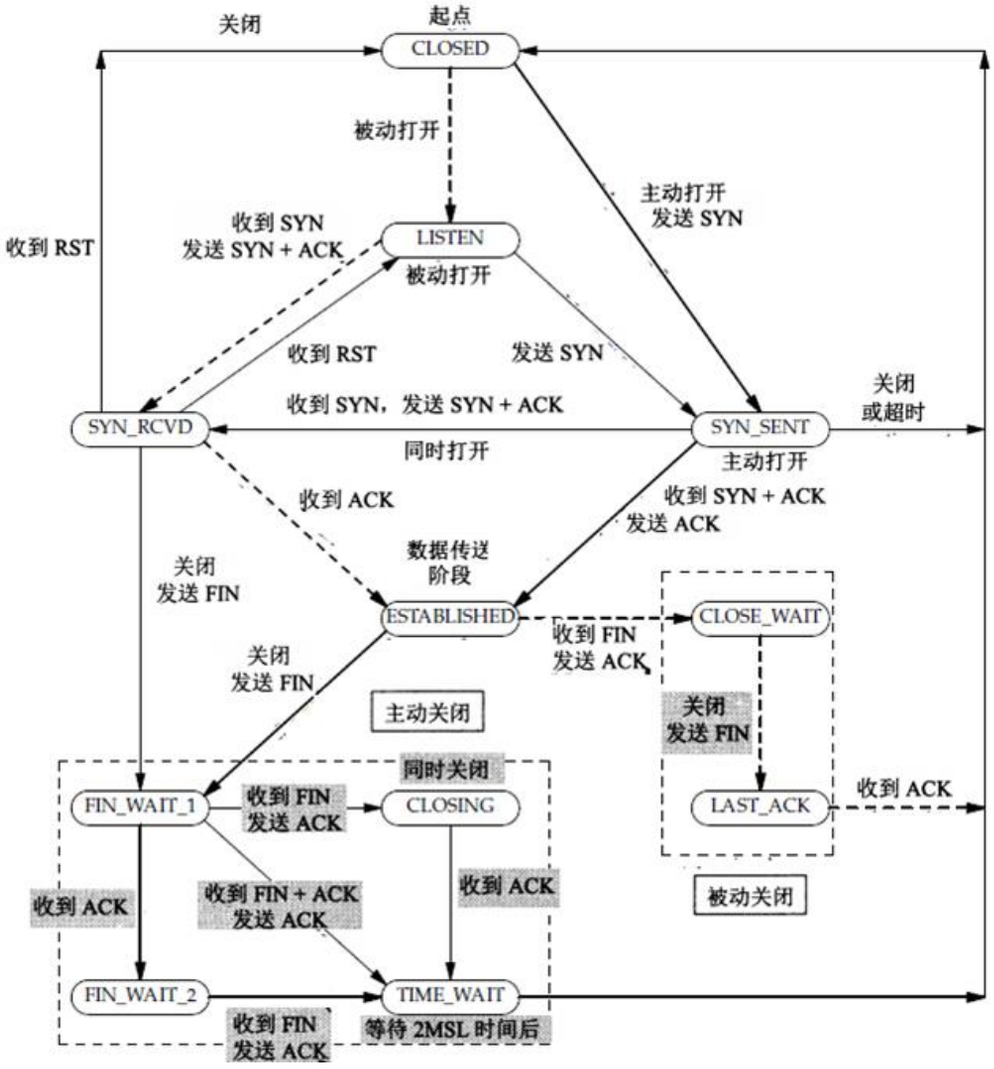

图5-13　TCP的有限状态机

5.2　课后习题详解

1试说明运输层在协议栈中的地位与作用。运输层的通信和网络层的通信有什么重要的区别？为什么运输层是必不可少的？

答：（1）运输层在协议栈中的地位与作用：

地位：运输层是整个网络体系结构中的关键层次之一，它处于通信子网和资源子网之间，是整个协议层次中最核心的一层；

作用：解决计算机程序到计算机进程之间的通信问题（“端”到“端”的通信），还有复用和分用、差错检测、可靠传输、拥塞控制以及流量控制等功能。

（2）运输层的通信和网络层的通信的区别：

①运输层为应用进程提供端到端的逻辑通信，网络层为主机之间提供逻辑通信；

②运输层对收到的报文（首部＋数据部分）进行差错检测，而在网络层只检验首部；

③运输层包括面向连接的TCP和无连接的UDP两种协议，而网络层无法同时实现这两种协议。

（3）各种应用进程之间通信需要“可靠或尽力而为”的两类服务质量，必须由运输层以复用和分用的形式加载到网络层。运输层还要对收到的报文进行差错检测。因此，运输层是必不可少的。

2网络层提供数据报或虚电路服务对上面的运输层有何影响？

答：网络层为主机之间提供逻辑通信，而运输层提供端到端的逻辑通信，故数据报或虚电路服务不影响其上面运输层的运行机制。

3当应用程序使用面向连接的TCP和无连接的IP时，这种传输是面向连接的还是无连接的？

答：从运输层来看是面向连接的，从网络层来看则是无连接的。

4试画图解释运输层的复用。画图说明许多个运输用户复用到一条运输连接上，而这条运输连接又复用到IP数据报上。

答：如图5-14所示表示运输层的复用机制。

图5-14　运输层的复用

5试举例说明有些应用程序愿意采用不可靠的UDP，而不愿意采用可靠的TCP。

答：UDP是无连接的，减少了开销和发送数据之前的时延，即便它是不可靠的服务，但为了实时性，例如视频会议、语音通话均会采用不可靠的UDP，若这些应用采用TCP，出错则会引起重传，不满足实际要求。

6接收端收到有差错的UDP用户数据报时应如何处理？

答：接收端通过UDP首部检验和来检测UDP用户数据报在传输中是否有错，若有差错则丢弃该数据报。

7如果应用程序愿意使用UDP完成可靠传输，这可能吗？请说明理由。

答：这是可能的，但需要对UDP的不可靠的传输进行适当的改进，以减少数据的丢失。应用进程本身可在不影响应用的实时性的前提下，增加一些提高可靠性的措施，如采用前向纠错或重传已丢失的报文。

8为什么说UDP是面向报文的，而TCP是面向字节流的？

答：（1）UDP是面向报文的原因：发送方UDP对应用程序交下来的报文，在添加首部后就向下交付给IP层，UDP对应用层交下来的报文，既不合并，也不拆分，而是保留这些报文的边界；接收方UDP对IP层交上来的UDP用户数据报，在去除首部后就原封不动地交付上层的应用进程，一次交付一个完整的报文。

（2）TCP是面向字节流的原因：TCP把应用程序交下来的数据看成是一连串的无结构的字节流，接收方应用程序收到的字节流必须和发送方应用程序发出的字节流完全一样。

9端口的作用是什么？为什么端口号要划分为三种？

答：（1）端口的作用是：

①应用层的各个进程的数据可以通过端口向下交付给传输层；

②传输层的数据可以通过端口上交给应用层。

（2）为了区分程序属于服务端还是客户机，需要将端口号分成两类，即服务端使用的端口号和客户机使用的端口号；而服务端中有些程序是需要被熟知的，有些登记使用即可，所以服务端使用的端口号分为熟知端口号和登记端口号，故划分成了三种。

10试说明运输层中伪首部的作用？

答：伪首部通常有TCP伪首部和UDP伪首部。伪首部并非TCP&UDP数据报中实际的有效成分。伪首部是一个虚拟的数据结构，其中的信息是从数据报所在IP分组头的分组头中提取的，既不向下传送也不向上递交，而是仅仅为计算校验和。这样的校验和，即校验了TCP&UDP用户数据的源端口号和目的端口号以及TCP&UDP用户数据报的数据部分，又检验了IP数据报的源IP地址和目的地址。伪报头保证了TCP&UDP数据单元到达正确的目的地址。

11某应用进程使用运输层的用户数据报UDP，但继续向下交给IP层后，又封装成IP数据报。既然都是数据报，是否可以跳过UDP而直接交给IP层？哪些功能UDP提供了但IP没有提供？

答：（1）不可以跳过UDP而直接交给IP层，因为IP数据报只能找到目的主机而无法找到目的进程，目的进程必须通过运输层的目的端口才能找到。

（2）UDP提供对应用进程的复用和分用功能，以及提供对数据部分的差错检验，而IP没有提供。

12一个应用程序用UDP，到了IP层将数据报再划分为4个数据报片发送出去。结果前两个数据报片丢失，后两个到达目的站。过了一段时间应用程序重传UDP，而IP层仍然划分为4个数据报片来传送。结果这次前两个到达目的站而后两个丢失。试问：在目的站能否将这两次传输的4个数据报片组装成为完整的数据报？假定目的站第一次收到的后两个数据报片仍然保存在目的站的缓存中。

答：在目的站不能将这两次传输的4个数据报片组装成为完整的数据报；

理由：两次传输的IP数据报的标识字段不同，所以不能组装成一个IP数据报。

13一个UDP用户数据报的数据字段为8192字节。在链路层要使用以太网来传送。试问应当划分为几个IP数据报片？说明每一个数据报片的数据字段长度和片偏移字段的值。

答：UDP用户数据报的数据字段为8192字节，添加首部后即为IP层的数据部分，所以IP层的数据部分长为8192＋8＝8200；在一个以太网上，UDP用户数据报的最大长度是1500字节，则应当划分成6个数据报片，数据字段的长度：前5个是1480字节，最后一个是800字节；各个片偏移字段的值分别是：0，185，370，555，740和925。

14一UDP用户数据报的首部的十六进制表示是：06 32 00 45 00 1C E2 17。试求源端口、目的端口、用户数据报的总长度、数据部分长度。这个用户数据报是从客户发送给服务器还是从服务器发送给客户？使用UDP的这个服务器程序是什么？

答：十六进制的06 32代表源端口，00 45代表目的端口，00 1C代表用户数据报的总长度，E2 17代表检验和字段。因此源端口1586，目的端口69，UDP用户数据报总长度28字节，数据部分长度20字节。

由于目的端口号＜1023，即目的端口是熟知端口，因此，该数据报是从客户发送给服务器的，熟知端口69对应的服务程序是TFTP。

15使用TCP对实时话音数据的传输有没有什么问题？使用UDP在传送数据文件时会有什么问题？

答：（1）TCP提供面向连接的可靠数据传输，虽然传输可靠，但重传数据会有时延，不适合实时传输；

（2）使用UDP传送数据文件时，如果出现了差错，UDP仅仅是少收了这个出错的报文段，并不通知发送方重传，这样就不能保证正确地传送数据。

16在停止等待协议中如果不使用编号是否可行？为什么？

答：在停止等待协议中如果不使用编号是不行的；编号是为了区分发送和接收的分组，若不进行编号，重复帧等都无法识别，不能正确传输。

17在停止等待协议中，如果收到重复的报文段时不予理睬（即悄悄地丢弃它，其他什么也不做）是否可行？试举出具体例子说明理由。

答：不行；如图5-15所示，当发生确认丢失的情形，由于原报文段M_1已经收到，此时如果重传的报文段被悄悄丢弃而不发送确认，则导致发送方A一直收不到M_1确认，重复地重传M_1。

图5-15　TCP收到重复的报文段

18假定在运输层使用停止等待协议。发送方在发送报文段M_0后在设定的时间内未收到确认，于是重传M_0，但M_0又迟迟不能达到接收方。不久，发送方收到了迟到的对M_0的确认，于是发送下一个报文段M_1，不久就收到了对M_1的确认。接着，发送方发送新的报文段M_0，但这个新的M_0在传送过程中丢失了。正巧，一开始就滞留在网络中的M_0现在到达接收方。接收方无法分辨M_0是旧的。于是收下M_0，并发送确认。显然，接收方后来收到的M_0是重复的，协议失败了。

试画出类似于图5-16所示的双方交换报文段的过程。

图5-16　停止等待协议

答：双方交换报文段的示意图，如图5-17所示。

图5-17　双方交换报文段的示意图

19试证明：当用n比特进行分组的编号时，若接收窗口等于1（即只能按顺序接收分组），则仅在发送窗口不超过2^n-1时，连续ARQ协议才能正确运行。窗口单位是分组。

证明：如图5-18所示，设发送窗口记为W_T，接收窗口记为W_R；

假定用3比特进行编号，设接收端窗口正好在7号分组处（有阴影的分组）。发送窗口W_T的位置不可能比②更靠前，也不可能比③更靠后，也不可能出现如①这种极端情况；

对于①和②的情况下，W_T内无重复序号，即$W_T \leq 2^n$；

对于③这种情况下，在W_T+W_R的范围内无重复序号，即$W_T+W_R \leq 2^n$，又由于$W_R=1$，因此$W_T \leq 2^n-1$；

综上所述，得证。

图5-18　连续ARQ协议示意图

20在连续ARQ协议中，若发送窗口等于7，则发送端在开始时可连续发送7个分组。因此，在每一分组发出后，都要置一个超时计时器。现在计算机里只有一个硬时钟。设这7个分组发出的时间分别为t_0，t_1，…，t_6，且t_{out}都一样大。试问如何实现这7个超时计时器（这叫软时钟法）？

答：如图5-19所示，可以用相对发送时间实现一个链表；因为计算机里只有一个硬时钟，则可以用相对发送时间实现的链表表示7个超时计时器，并将它们链接到硬时钟后面。

图5-19　链表实现

21假定使用连续ARQ协议，发送窗口大小是3，而序号范围是[0，15]，而传输媒体保证在接收方能够按序收到分组。在某一时刻，在接收方，下一个期望收到的序号是5。试问：

（1）在发送方的发送窗口中可能出现的序号组合有哪些？

（2）接收方已经发送出的、但在网络中（即还未到达发送方）的确认分组可能有哪些？说明这些确认分组是用来确认哪些序号的分组。

答：（1）因为下一个期望收到的序号是5，则表明序号4为止的分组都已经收到；若这些确认都已经到达发送方，则发送窗口的范围是[5，7]；若这些确认都已经丢失，即发送方并未收到这些确认，则发送窗口此时范围应该是[2，4]；故发送窗口可能的序号组合为[2，3，4]、[3，4，5]、[4，5，6]、[5，6，7]。

（2）如果接收方期望收到序号为5的分组，则说明它已经接收了序号4以前的分组并给出了确认。如果这些确认没有被发送方收到，则确认消息可能包括2、3、4。由于发送方已经发送了序号为2、3、4的分组，因此必然收到了序号1的确认。一旦接收方发出序号1的确认，则不会再发送小于1的确认，因此可能停留在网络中的确认号为2、3、4，用来确认序号为2、3、4的分组。

22主机A向主机B发送一个很长的文件，其长度为L字节。假定TCP使用的MSS为1460字节。

（1）在TCP的序号不重复使用的条件下，L的最大值是多少？

（2）假定使用上面计算出的文件长度，而运输层、网络层和数据链路层所用的首部开销共66字节，链路的数据率为10Mbit/s，试求这个文件所需的最短发送时间。

答：（1）TCP报文段首部中序号占4字节，序号范围是[0，$2^{32}-1$]，共2^{32}个序号。若TCP的序号不重复使用，则L最多可以分成2^{32}报文段，TCP建立时需要消耗一个序号，因此L最多只能分成$2^{32}-1$个报文段，L的最大值是$2^{32}-1 \approx 4$GB；

（2）4GB的文件可以分成4G/1460个数据报，加上运输层、网络层和数据链路层所有的首部开销，每个数据报的长度变为（1460＋66），此时总的文件长度为（4G/1460）×（1460＋66）≈4489123390字节；传输时间为（4489123390×8bit）/（10×10^6bit/s）≈3591.3s≈59.85分钟≈1小时。

23主机A向主机B连续发送了两个TCP报文段，其序号分别是70和100。试问：

（1）第一个报文段携带了多少字节的数据？

（2）主机B收到第一个报文段后发回的确认中的确认号应当是多少？

（3）如果B收到第二个报文段后发回的确认中的确认号是180，试问A发送的第二个报文段中的数据有多少字节？

（4）如果A发送的第一个报文段丢失了，但第二个报文段到达了B。B在第二个报文段到达后向A发送确认。试问这个确认号应为多少？

答：（1）第一个报文段的数据序号是70到99，共100－70＝30字节的数据；

（2）主机B收到第一个报文段后发回的确认中的确认号为：99＋1＝100；

（3）A发送的第二个报文段中的数据长度为：179－100＋1＝80（字节）；

（4）因为此时收到的报文段的最后一个序号为69，当在第二个报文段到达后，B向A发送确认，所以这个确认号应为70。

24一个TCP连接下面使用256kbit/s的链路，其端到端时延为128ms。经测试，发现吞吐量只有120kbit/s。试问发送窗口W是多少？（提示：可以有两种答案，取决于接收端发出确认的时机）。

答：已知往返时延＝128×2＝256ms，设发送窗口为W（bit），发送端连续地将窗口内数据发完需要的时间为T，分两种情况：

（1）如图5-20（a）所示，若接收端在接收完一批完整的发送窗口大小的数据后才返回确认，则有W/（（W/（256×10^{3}））＋256×10^{-3}）＝120×10^{3}；解得W≈7228字节；

（2）如图5-20（b）所示，若接收端每收到一个很小的报文段即发回确认，则有W/（256×10^{-3}）＝120×10^{3}；解得W＝3840字节。

图5-20　分情况讨论发送窗口大小

25为什么在TCP首部中要把TCP的端口号放入最开始的4个字节？

答：在ICMP的差错报文中要包含IP首部后面的8个字节的内容，而这里面有TCP首部中的源端口和目的端口。当TCP收到ICMP差错报文时需要用这两个窗口来确定是哪条连接出了差错。

26为什么在TCP首部中有一个首部长度字段，而UDP的首部中就没有这个字段？

答：TCP首部除固定长度部分以外，还有选项字段，即TCP首部长度是可变的，需要首部长度字段说明实际长度，而UDP首部长度是固定的，不需要额外加上一个首部长度字段。

27一个TCP报文段的数据部分最多为多少字节，为什么？如果用户要传送的数据的字节长度超过TCP报文段中的序号字段可能编出的最大序号，问还能否用TCP来传送？

答：（1）一个TCP报文段的数据部分最多为65495字节。因为此数据部分加上TCP首部的20字节，再加上IP首部的20字节，正好是IP数据报的最大长度65535字节。若IP首部包含了选择，则IP首部长度超过20字节，这时TCP报文段的数据部分的长度将小于65495字节。

（2）如果数据的字节长度超过TCP报文段中的序号字段可能编出的最大序号，则通过循环使用序号（即若当前序号增加到最大则下一个序号为0），仍能用TCP来传送。

28主机A向主机B发送TCP报文段，首部中的源端口是m而目的端口是n。当B向A发送回信时，其TCP报文段中的首部中的源端口和目的端口分别是什么？

答：源端口和目的端口分别是n和m（回信时端口号和发送来的相反）。在一台机器上，一个进程对应一个端口。端口的作用是唯一标识这个进程。源端口标识发起通信的那个进程，目的端口标识接受通信的那个进程。

29在使用TCP传送数据时，如果有一个确认报文段丢失了，也不一定会引起与该确认报文段对应的数据的重传。试说明理由。

答：当数据还未重传就收到了对更高序号的确认时，就不再需要重传该确认报文段对应的数据。因此，即使这个确认报文段丢失

了，只要及时收到了更高序号的确认，就不会引起与该确认报文段对应的数据的重传。

30设TCP使用的最大窗为65535字节，而传输信道不产生差错，带宽也不受限制。若报文段的平均往返时间为20ms，问所能得到的最大吞吐率是多少？

答：在发送时延可忽略的情况下，最大数据率＝最大窗口×8/平均往返时间＝26.214Mbit/s。

31通信信道带宽为1Gbit/s，端到端时延为10ms。TCP的发送窗口为65535字节。试问：可能达到的最大吞吐率是多少？信道的利用率是多少？

答：往返延迟时间RTT＝2×10ms＝20ms；

则发送时延＝L/C＝（65535×8）/（1×10^9）＝0.00052428s；

最大吞吐量＝L/（L/C＋RTT）＝（65535×8）/（0.02＋0.00052428）＝25.5Mb/s；

线路效率＝单位时间内最大吞吐量/线路速率＝25.5Mbit/s/1Gbit/s＝2.55%；

所以可能达到的最大吞吐率是25.5Mb/s，信道的利用率是2.55%。

32什么是Karn算法？在TCP的重传机制中，若不采用Karn算法，而是在收到确认时都认为是对重传报文段的确认，那么由此得出的往返时延样本和重传时间都会偏小。

试问：重传时间最后会减小到什么程度？

答：Karn算法在计算加权平均RTT_S时，只要报文段重传了，就不采用其往返时延样本，这样得出的加权平均RTT_S和RTO就较为准确；而不采用Karn算法时，若TCP发送了报文段后，没有收到确认，于是超时重传报文；但刚刚重传了报文后，马上收到了原报文的确认，这里却把原来的确认错当成了重传报文的确认，这样得出的往返时间会很小，甚至最后减小到接近于零。

33假定TCP在开始建立连接时，发送方设定超时重传时间RTO＝6秒。

（1）当发送方收到对方的连接确认报文段时，测量出RTT样本值为1.5秒。试计算现在的RTO值。

（2）当发送方发送数据报文段并收到确认时，测量出RTT样本值为2.5秒。试计算现在的RTO值。

答：（1）因为$RTO＝RTT_S＋4\times RTT_D$；其中RTT_D是RTT_S的偏差加权均值。

初次测量时，RTT_D（1）＝RTT（1）/2；

后续测量中，$RTT_D(i)＝(1－\beta)\times RTT_D(i－1)＋\beta\times|RTT_S－RTT(i)|$；

这里取β＝1/4，且由题可知RTT（1）＝1.5s，则：

RTT_S（1）＝RTT（1）＝1.5s；

RTT_D（1）＝RTT（1）/2＝0.75s；

$RTO(1)＝RTT_S(1)＋4\times RTT_D(1)＝1.5＋0.75\times4＝4.5s$。

（2）由题可知RTT（2）＝2.5s；RTT_s（1）＝1.5s；RTT_D（1）＝0.75s；

取α＝1/8，$RTT_s(2)＝(1－\alpha)\times RTT_s(1)＋\alpha\times RTT(2)＝(1-1/8)\times1.5＋1/8\times2.5＝1.625s$；

$RTT_D(2)＝(1－\beta)\times RTT_D(1)＋\beta\times|RTT_S(2)－RTT(2)|＝(1－1/4)\times0.75＋|1.625－2.5|/4\approx0.78s$；

$RTO(2)＝RTT_S(2)＋4\times RTT_D(2)＝1.625＋0.78\times4\approx4.75s$。

34已知第一次测得TCP的往返时间RTT是30ms。接着收到了三个确认报文段，用它们测量出的往返时间样本RTT分别是：26ms，32ms和24ms。设α＝0.1。试计算每一次的新的加权平均往返时间值RTT_S。讨论所得出的结果。

答：已知α＝0.1，旧的RTT＝30ms，M_1＝26ms，M_2＝32ms，M_3＝24ms，所以有：

$RTT_{S1}＝0.9\times30＋(1－0.9)\times26＝29.6$；

$RTT_{S2}＝0.9\times29.6＋(1－0.9)\times32＝29.84$；

$RTT_{S3}＝0.9\times29.84＋(1－0.9)\times24＝29.256$；

因此，新的估计往返时延值分别是29.6ms、29.84ms、29.256ms。

由计算结果可知RTT样本值变化较大时，加权往返时间RTT_S变化可能很小；事实上，它们跟α的大小有关，若α选取很接近于0，

表示新的RTT_S值与旧的RTT_S相比变化不大，RTT值更新较慢；若α选取接近1，则表示新的RTT_S受新的RTT样本影响较大，RTT更新较快。

35试计算一个包括5段链路的运输连接的单程端到端时延。5段链路中有2段是卫星链路，有3段是广域网链路。每条卫星链路又由上行链路和下行链路两部分组成。可以取这两部分的传播时延之和为250ms。每一个广域网的范围是1500km，其传播时延可按150000km/s来计算。各数据链路速率为48kbit/s，帧长为960bit。

答：5段链路的传播时延＝[250×2＋（1500/150000）×3×1000]ms＝530ms，5段链路的发送时延＝[960÷（48×1000）]×5×1000ms＝100ms，所以5段链路单程端到端时延＝530ms＋100ms＝630ms。

36重复35题，但假定其中的一个陆地上的广域网的传输时延为150ms。

答：传播时延＝250×2＋（1500/150000）×3×1000＝530ms，发送时延＝960/（48×1000）×4×1000＋150＝230ms，则总时延为530＋230＝760ms。

37在TCP的拥塞控制中，什么是慢开始、拥塞避免、快重传和快恢复算法？这里每一种算法各起什么作用？“乘法减小”和“加法增大”各用在什么情况下？

答：（1）慢开始算法及其作用

建立了TCP连接并开始发送报文段时，令拥塞窗口cwnd＝1（即一个最大报文长度MSS），并在每次收到一个对新的报文段的确认后，使cwnd＋1，这种使得每经过一个往返时延RTT后拥塞窗口cwnd加倍（即cwnd的大小呈指数增长）直到cwnd增大到慢开始门限ssthresh的过程叫慢开始算法；

作用：按指数增长调整拥塞窗口cwnd，使分组注入网络的速率更合理。

（2）拥塞避免算法

发送端的拥塞窗口cwnd每经过一个往返时延RTT就增加一个MSS的大小（按线性增长），直到出现一次超时（网络拥塞），令慢开始门限ssthresh等于当前cwnd的一半，这种算法叫拥塞避免算法；

作用：可使拥塞窗口cwnd按线性规律缓慢增长。

（3）快重传

当发送端连续收到三个重复的ACK报文时，直接重传对方尚未收到的报文段，而不必等待超时计时器超时；

作用：由于不用等待重传计时器到时，所以采用快重传后可以使整个网络的吞吐量提高。

（4）快恢复

快恢复算法要求当发送方连续收到三个重复确认时，就执行“乘法减小”算法，把慢开始门限ssthresh减半，再令cwnd＝新的ssthresh，之后执行拥塞避免算法，使cwnd线性增长。

作用：采用快恢复这样的拥塞控制方法使得TCP的性能有明显的改进。

（5）“乘法减小”和“加法增大”的适用情况：

①乘法减小是指不论在慢开始阶段还是拥塞避免阶段，只要出现一次超时（即出现一次网络拥塞），就把慢开始门限值ssthresh设置为当前的拥塞窗口值的一半，当网络频繁出现拥塞时，ssthresh值就下降得很快，以大大减少注入到网络中的分组数；

②加法增大是指执行拥塞避免算法后，在收到对所有报文段的确认后（即经过一个往返时间），就把拥塞窗口cwnd增加一个MSS大小，使拥塞窗口缓慢增大，以防止网络过早出现拥塞。

38设TCP的ssthresh的初始值为8（单位为报文段）。当拥塞窗口上升到12时网络发生了超时，TCP使用慢开始和拥塞避免。试分别求出第1次到第15次传输的各拥塞窗口大小。你能说明拥塞窗口每一次变化的原因吗？

答：拥塞窗口大小依次为1、2、4、8、9、10、11、12、1、2、4、6、7、8、9。如图5-21所示。

1、2、4、8执行的是慢开始算法，它们是按着指数规律递增，当拥塞窗口是8时，达到了ssthresh初始值，所以开始执行拥塞避免“加法增大”，当拥塞窗口达到12时，开始执行“乘法减小”，即采取慢开始的算法；当传输次数达到11次的时候，拥塞窗口达到了新的ssthresh值6，所以又开始执行“加法增大”。

图5-21　慢开始和拥塞避免情况

39TCP的拥塞窗口cwnd大小与传输轮次n的关系如表5-4所示。

表5-4　TCP的拥塞窗口与传输轮次的关系

cwnd	1	2	4	8	16	32	33	34	35	36	37	38	39
n	1	2	3	4	5	6	7	8	9	10	11	12	13
cwnd	40	41	42	21	22	23	24	25	26	1	2	4	8
n	14	15	16	17	18	19	20	21	22	23	24	25	26

（1）试画出如图5-22所示的拥塞窗口与传输轮次的关系曲线。

图5-22　慢开始和拥塞避免算法的实现举例

（2）指明TCP工作在慢开始阶段的时间间隔。

（3）指明TCP工作在拥塞避免阶段的时间间隔。

（4）在第16轮次和第22轮次之后发送方是通过收到三个重复的确认还是通过超时检测到丢失了报文段？

（5）在第1轮次、第18轮次和第24轮次发送时，门限ssthresh分别被设置为多大？

（6）在第几轮次发送出第70个报文段？

（7）假定在第26轮次之后收到了三个重复的确认，因而检测出了报文段的丢失，那么拥塞窗口cwnd和门限ssthresh应设置为多大？

答：（1）画出题干的拥塞窗口与传输轮次的关系曲线，结果如图5-23所示。

图5-23　拥塞窗口与传输轮次的关系曲线

（2）慢开始工作间隔：[1，6]和[23，36]。

（3）拥塞避免的时间间隔：[6，16]和[17，22]。

（4）第16轮次之后发送方通过快恢复方法来发送数据，因此断定为收到了三个重复的确认；第22轮次后发送方采用慢开始方法来发送数据，因此它是通过超时检测机制来确认报文段的丢失。

（5）在第1轮次发送时，阈值ssthresh被设置为32。在第18轮次发送时，阈值ssthresh被设置为发生拥塞时的一半，即21。在第24轮次发送时，阈值ssthresh是13。

（6）将各次传输轮次的发送数据相加可知，在第7轮次发送出第70个报文段。

（7）在第26轮次后收到三个重复的确认，因此检测出报文段的丢失，根据拥塞控制的算法应该采用快恢复算法，门限ssthresh减半，而拥塞窗口cwnd设置为慢开始门限ssthresh减半后的数值，因此均设置为4。

40TCP在进行流量控制时是以分组的丢失作为产生拥塞的标志，有没有不是因拥塞而引起的分组丢失的情况？如有，请举出三种情况。

答：有不是因拥塞而引起的分组丢失的情况，例如：

（1）IP数据报已经到达终点，终点的缓存没有足够的空间存放此数据报；

（2）当IP数据报在传输过程中需要进行分片，但其中的一个数据报片未能及时达到终点，而终点组装IP数据报已超时，因而只能丢弃该数据报；

（3）数据报在转发过程中经过一个局域网的网桥，但网桥在转发该数据报帧的时候，由于没有足够的差错空间而只好丢弃。

41用TCP传送512字节的数据。设窗口为100字节，而TCP报文段每次也是传送100字节的数据。再设发送端和接收端的起始序号分别选为100和200，试画出类似于图5-24的工作示意图。从连接建立阶段到连接释放都要画上。

图5-24　41题图

答：如图5-25所示为41题工作示意图。

图5-25　从连接建立到释放连接的全过程

42在图5-26中所示的连接释放过程中，在ESTABLISHED状态下，服务器进程能否先不发送ack＝u＋1的确认？（因为后面要发送的连接释放报文段中仍有ack＝u＋1这一信息）

图5-26　TCP连接释放的过程

答：如果B不再发送数据了，是可以把两个报文段合并成为一个，即发送FIN＋ACK报文段。但如果B还有数据要发送，而且要发送一段时间，就不能合成一个来发送，因为A迟迟收不到确认，就超时重传这个FIN报文段，浪费网络资源，故此时必须先发送ack＝x＋1的确认。

43在图5-27中，在什么情况下会发生从状态SYN-SENT到状态SYN-RCVD的变迁？

图5-27　TCP的有限状态机

答：当A和B都作为客户，即同时主动打开TCP连接。这时每一方的状态变迁都是：

CLOSED→SYN-SENT→SYN-RCVD→ESTABLISHED

44试以具体例子说明为什么一个运输连接可以有多种方式释放。可以设两个互相通信的用户分别连接在网络的两结点上。

答：假设两个互相通信的用户分别为A和B，并假设A和B之间已经建立连接，此时释放的方式可能有：

（1）主机A发出释放连接的请求；

（2）主机B发出释放连接的请求；

（3）由于网络以及其他未知原因，网络不提供传输服务，主机A与主机B之间的连接释放。

45解释为什么突然释放运输连接就可能会丢失用户数据，而使用TCP的连接释放方法就可保证不丢失数据。

答：当主机1和主机2之间连接建立后，主机1发送了一个TCP数据段并正确抵达主机2，接着主机1发送另一个TCP数据段，主机2在收到第二个TCP数据段之前发出了释放连接请求，如果就这样突然释放连接，主机1发送的第二个TCP报文段会丢失。而使用TCP的连接释放方法，主机2发出了释放连接的请求，只会释放主机2到主机1方向的连接，即主机2不再向主机1发送数据，但仍然可接收主机1发来的数据，所以可保证不丢失数据。

46试用具体例子说明为什么在运输连接建立时要使用三次握手。说明如不这样做可能会出现什么情况。

答：三次握手即对每次发送的数据量进行跟踪协商使数据段的发送和接收同步，TCP使用三次握手才能够正确地对连接进行管理，如果把三次握手改成仅需要两次握手，可能会发生死锁，如下面例子所述：

考虑计算机A和B之间的通信，假定A给B发送一个连接请求分组，B收到了这个分组，并发送了确认应答分组。按照两次握手的协定，B认为连接已经成功地建立了，可以开始发送数据分组。可是，A在B的应答分组在传输中被丢失的情况下，将不知道B是否已准备好，也不知道B发送数据使用的初始序列号，A甚至怀疑B是否收到自己的连接请求分组。在这种情况下，A认为连接还未建立成功，将忽略B发来的任何数据分组，只是一直在等待连接确认应答分组。而B在发出的分组超时后，重复发送同样的分组，这样就形成了死锁。

47一客户向服务器请求建立TCP连接。客户在TCP连接建立的三次握手中的最后一个报文段中捎带上一些数据，请求服务器发送一个长度为L字节的文件。假定：

（1）客户和服务器之间的数据传送速率是R字节/秒，客户与服务器之间的往返时间是RTT（固定值）。

（2）服务器发送的TCP报文段的长度都是M字节，而发送窗口大小是nM字节。

（3）所有传送的报文段都不会出现差错（无重传），客户收到服务器发来的报文段后就及时发送确认。

（4）所有的协议首部开销都可忽略，所有确认报文段和连接建立阶段的报文段的长度都可忽略（即忽略这些报文段的发送时间）。

试证明，从客户开始发起连接建立到接收服务器发送的整个文件所需的时间T是：

T＝2RTT＋L/R　当nM＞R（RTT）＋M

或T＝2RTT＋L/R＋（K－1）[M/R＋RTT－nM/R]　当nM＜R（RTT）＋M

其中，K＝⌈L/nM⌉，符号⌈x⌉表示若x不是整数，则把x的整数部分加1。

（提示：求证的第一个等式发生在发送窗口较大的情况，可以连续地把文件发送完。求证的第二个等式发生在发送窗口较小的情况，发送几个报文段后就必须停顿下来，等收到确认后再继续发送。建议先画出双方交互的时间图，然后再进行推导）。

答：

图5-28　TCP双方交互时间图

由题可知，从客户端发送TCP连接请求到客户端收到第一个报文段所需的时间的为2RTT。

（1）如图5-28（a）所示，当nM＞R（RTT）＋M时，由于发送窗口较大，可以连续把文件发送完，相当于连续的发送每一个报文段。服务器发送整个文件的时间为L/R，因此，T＝2RTT＋L/R。

（2）如图5-28（b）所示，当时nM＜R（RTT）＋M，由于发送窗口较小，发送完一个窗口的报文段后，因为还没有收到确认，必须停下等待确认。

文件的长度为L可以被分为的窗口数为K，若不能整除，最后一个窗口的长度为（L－（K－1）nM），前（K－1）个窗口每个窗口的发送时间等于一个往返时延和下一个窗口中第一个报文段的发送时间的和，即为RTT＋M/R；

最后一个窗口的发送时间为：[L－（K－1）nM]/R；总的发送时间为：T＝2RTT＋（K－1）（RTT＋M/R）＋[L－（K－1）nM]/R＝2RTT＋L/R＋（K－1）（RTT＋M/R－nM/R）；

综上所述，题中结论得证。

48网络允许的最大报文段长度为128字节，序号用8位表示，报文段在网络中的寿命为30秒。求发送报文段的一方所能达到的最高数据率。

答：具有相同编号的报文段不应该同时在网络中传输，必须保证当序列号循环回来重复使用的时候，具有相同序列号的报文段已经从网络中消失。若序号用8比特表示，报文段的寿命为30s，那么在30s的时间内发送方发送的报文段的数目不能多于255个。网络允许的最大报文段长度为128B，则每一条TCP连接所能达到的最高数据传输速率＝255×128×8bit/30s＝8704bit/s＝8.704kbit/s。

49下面是以十六进制格式存储的一个UDP首部：

CB84000D001C001C

试问：

（1）源端口号是什么？

（2）目的端口号是什么？

（3）这个用户数据报的总长度是多少？

（4）数据长度是多少？

（5）这个分组是从客户到服务器方向的，还是从服务器到客户方向的？

（6）客户进程是什么？

答：（1）源端口号是最前面的四位十六进制（$CB84_{16}$），即52100；

（2）目的端口号是第二个四位十六进制（$000D_{16}$），即13；

（3）该用户数据报的总长度是第三个四位十六进制（$001C_{16}$）定义的，即28字节；

（4）数据的长度是整个分组的长度减去首部的长度，也就是28－8＝20字节；

（5）目的端口号是13（熟知端口），所以是从客户到服务器的；

（6）客户进程是Daytime。

50把图5-29计算UDP检验和的例子自己具体演算一下，看是否能够得出书上的计算结果。

图5-29　50题图

答：可参考教材5.5.2自行演算，此处略。

51在以下几种情况下，UDP的检验和在发送时的数值分别是多少？

（1）发送方决定不使用检验和。

（2）发送方使用检验和，检验和的数值是全1。

（3）发送方使用检验和，检验和的数值是全0。

答：（1）置为全0；

（2）检验和的数值为全1，则求反得全0；

（3）检验和的数值为全0，则求反得全1。

52UDP和IP的不可靠程度是否相同？请加以解释。

答：UDP用户数据报的检验和既检验UDP用户数据报的首部又检验整个的UDP用户数据报的数据部分，而IP数据报的检验和仅仅检验IP数据报的首部。UDP用户数据报的检验和还增加了伪首部，即还检验了下面的IP数据报的源IP地址和目的IP地址。

53UDP用户数据报的最小长度是多少？用最小长度的UDP用户数据报构成的最短IP数据报的长度是多少？

答：UDP的最小长度是8字节，用最小长度的UDP用户数据报构成的最短IP数据报的长度是20＋8＝28字节。

54某客户使用UDP将数据发送给一服务器，数据共16字节。试计算在运输层的传输效率（有用字节与总字节之比）。

答：UPD用户数据报的总长度＝8＋16＝24字节，因此，在运输层的传输效率＝16/24＝0.667。

55重做54题，但在IP层计算传输效率。假定IP首部无选项。

答：IP数据报的总长度＝20＋24＝44字节，因此，在IP层的传输效率＝16/44＝0.364。

56重做题54，但在数据链路层计算传输效率。假定IP首部无选项，在数据链路层使用以太网。

答：以太网有14字节的首部，4字节的尾部（FCS字段），但其数据字段的最小长度是46字节，而我们的IP数据报仅有44字节，因此还必须加上2字节的填充，且发送以太网的帧之前还有8字节的前同步码。这样，以太网的总长度＝14＋4＋2＋44＋8＝72字节，因此，在数据链路层的传输效率＝16/72＝0.222。

57某客户有67000字节的分组。试说明怎样使用UDP数据报将这个分组进行传送。

答：客户有67000字节的分组，加上UDP首部后长度为67000＋8＝67008字节，即IP数据报的数据部分长度为67008字节，假设该分组需要在以太网上传输，则可以将其分成⌈67008/1480⌉＝46个分组，前45个分组长度均为1500字节，最后一个分组为428字节。

58TCP在时间为4:30:20（即4点30分20秒）发送了一个报文段。由于没有收到确认，因此在4:30:25重传了前面这个报文段，并在4:30:27收到了确认。若以前的RTT值是4秒，根据Karn算法，新的RTT值是多少？

答：根据Karn算法，只要是TCP报文段重传了，就不采用其往返时间样本。本题中收到的确认是在重传后收到的。因此RTT值没有变化，仍然是以前的数值（4s）。

59TCP连接使用1000字节的窗口值，而上一次的确认号是22001。现在收到了一个报文段，确认了字节22401。试用图来说明在这之前与之后的窗口情况。

答：窗口的变化如图5-30所示。

图5-30　窗口的变化图

60同上题。但接收方收到确认字节为22401的报文段时，其窗口字段变为1200字节。试用图来说明在这之前与之后的窗口情况。

答：窗口的变化如图5-31所示。

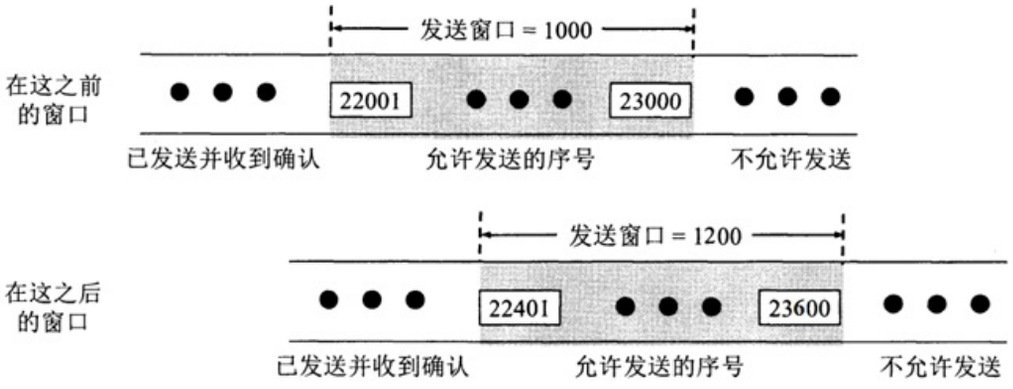

图5-31　窗口的变化图

61在本题中列出的8种情况下，画出发送窗口的变化，并标明可用窗口的位置。已知主机A要向主机B发送3KB的数据。在TCP连接建立后，A的发送窗口大小是2KB。A的初始序号是0。

（1）一开始A发送1KB的数据。

（2）接着A就一直发送数据，直到把发送窗口用完。

（3）发送方A收到对第1000号字节的确认报文段。

（4）发送方A再发送850B的数据。

（5）发送方A收到ack＝900的确认报文段。

（6）发送方A收到对第2047号字节的确认报文段。

（7）发送方A把剩下的数据全部都发送完。

（8）发送方A收到ack＝3072的确认报文段。

答：窗口变化如图5-32所示。

图5-32　窗口变化示意图

62TCP连接处于ESTABLISHED状态。以下的事件相继发生：

（1）收到一个FIN报文段。

（2）应用程序发送“关闭”报文。

在每一个事件之后，连接的状态是什么？在每一个事件之后发生的动作是什么？

答：（1）处于ESTABLISHED状态又能收到一个FIN报文段，说明它是TCP服务器端而不是客户端；当这个服务器端收到FIN时，服务器就向客户端发送ACK报文段，并进入到CLOSE-WAIT状态（这是被动关闭）；注意这时客户端不会再发送数据了，但服务器端如还有数据要发送给客户端，那么还是可以继续发送的。

（2）应用程序发送“关闭”报文给服务器，表明没有数据要发送了，这时服务器就应当发送FIN报文段给客户，然后转换到LAST-ACK状态，并等待来自客户端的最后的确认。

63TCP连接处于SYN-RCVD状态。以下的事件相继发生：

（1）应用程序发送“关闭”报文。

（2）收到FIN报文段。

在以上的每一个事件之后，连接的状态是什么？在每一个事件之后发生的动作是什么？

答：（1）处于SYN-RCVD状态而又能够收到应用程序发送的“关闭”报文，说明它是TCP的客户端而不是服务器端，这时，客户端就应当向服务器端发送FIN报文段，然后进入到FIN-WAIT-1状态。

（2）当客户收到服务器端发送的FIN报文段后，就向服务器发送ACK报文段，并进入到CLOSED状态。

64TCP连接处于FIN-WAIT-1状态。以下的事件相继发生：

收到ACK报文段。

收到FIN报文段。

发生了超时。

在以上的每一个事件之后，连接的状态是什么？在每一个事件之后发生的动作是什么？

答：（1）处于FIN-WAIT-1状态的只有TCP的客户，当收到ACK报文段后，TCP客户不发送任何报文段，只是从FIN-WAIT-1状态进入到FIN-WAIT-2状态。

（2）在收到FIN报文段后，TCP客户发送ACK报文段，并进入到TIME-WAIT状态。

（3）当发生了超时，也就是经过了2MSL时间后，TCP客户进入到CLOSED状态。

65假定主机A向B发送一个TCP报文段。在这个报文段中，序号是50，而数据一共有6字节长。试问，在这个报文段中的确认字段是否应当写入56？

答：A期望下次收到B发送的数据中的第一个字节的编号，而这个数值是A已经收到的数据的最后一个字节的编号加1，然而题目中并未给出这些条件；题目给出的是A向B发送的数据中第一个字节的编号是50，并且在这个报文段中共有6字节的数据，这些都和此报文段中的确认字段是什么毫无关系；因此，我们无法知道这个报文段中的确认字段应当写入的数值。

66主机A通过TCP连接向B发送一个很长的文件，因此这需要分成很多个报文段来发送。假定某一个TCP报文段的序号是x，那么下一个报文段的序号是否就是x＋1呢？

答：设某一个TCP报文段的序号是x，那么下一个报文段的序号应当是x＋n，其中n是这个报文段中的数据长度的字节数，则仅在此报文段中仅有1个字节的数据时，下一个报文段的序号才是x＋1。

67TCP的吞吐量应当是每秒发送的数据字节数，还是每秒发送的首部和数据之和的字节数？吞吐量应当是每秒发送的字节数，还是每秒发送的比特数？

答：（1）TCP的吞吐量本来并没有标准的定义，TCP的吞吐量可定义为每秒发送的数据字节数。

（2）计算机内部的数据传送是以每秒多少字节作为单位的，而在通信线路上的数据率则常用每秒多少比特作为单位。

68在TCP的连接建立的三报文握手过程中，为什么第三个报文段不需要对方的确认？这会不会出现问题？

答：第三个报文段之所以不需要确认，对于其原因进行讨论如下（模拟一个TCP连接建立和发送数据的过程来说明），其中（3）中可能导致连接建立出现问题。

（1）设A是客户端，假设三报文握手过程中的第三个报文段丢失了，但A并不知道，此时A以为对方收到了这个报文段，觉得TCP连接已经建立，于是就开始发送数据报文段给B。

（2）B由于并没有收到三报文握手中的最后一个报文段，它就不能进入TCP的连接已建立状态，此时B处于一种“半开连接”状态，即仅仅把TCP连接打开了一半，这时它已经初始化了连接变量和缓存，但不能接收数据；通常，B在经过一段时间后，如果还没有收到来自A的确认报文段，就终止这个半开连接状态，那么A就必须重新建立TCP连接；因此，在这种情况下，第三个报文段的丢失，就导致了TCP连接无法建立。

（3）假设A在这段时间内，紧接着就发送了数据，由于TCP具有累计确认的功能，在A发送的数据报文段中，自己的序号也没有改变，仍然是和丢失的确认真的序号一样（丢失的那个确认帧不消耗序号），并且确认位ACK＝1，确认号也是B的初始序号加1；当B收到这个报文段后，从TCP的首部就可以知道，A已确认了B刚才发送的SYN＋ACK报文段，于是就进入了连接已建立状态；接着，就接收A发送的数据，在这种情况下，A丢失的第二个报文段对TCP的连接建立就没有影响；

综上所述，A发送的第二个报文段仅仅是确认的报文段，是个可以省略的报文段，即使丢失了也无妨，只要下面紧接着就可以发送数据报文段即可。

69现在假定使用类似TCP的协议（即使用滑动窗口可靠传送字节流），数据传输速率是1Gbit/s，而网络的往返时间RTT＝140ms。假定报文段的最大生存时间是60秒。如果要尽可能快地传送数据，在我们的通信协议的首部中，发送窗口和序号字段至少各应当设为多大？

答：发送窗口至少应当能够容纳的比特数＝往返时间×数据率＝RTT×1Gbit/s＝140×10^{-3}s×10^9bit/s＝140×10^6bit＝17.5×10^6B；每一个字节的数据需要有一个编号，假定发送窗口一共有w位，那么总的号码数应当大于17.5×10^6B，即：$2^w\geq17.5\times10^6$B，则$w\geq\log_2$（17500000）＝24.06；可见只用24位的发送窗口小了一点，必须使用w＝25位的发送窗口才行。

TCP的窗口字段为16位，60秒钟以1Gbit/s的速率可以发送60s×10^9bit/s＝7.5×10^9B的数据，假定需要n位的序号字段，那么总的序号数应满足$2^n\geq7.5\times10^9$，解得$n\geq\log_2$（7.5×10^9）＝32.8；因此，取序号字段长度n＝33位即可保证在报文段的最大生产时间内没有重复的序号（注意TCP的序号字段为32位）。

【注意】1B＝8bit这个关系一定要熟记，计算中经常用到。

70假定用TCP协议在40Gbit/s的线路上传送数据。

（1）如果TCP充分利用了线路的带宽，那么需要多长的时间TCP会发生序号绕回？

（2）假定现在TCP的首部中采用了时间戳选项。时间戳占用了4字节，共32位。每隔一定的时间（这段时间叫做一个嘀嗒）时间戳的数值加1。假定设计的时间戳是每隔859微秒，时间戳的数值加1。试问要经过多少时间才发生时间戳数值的绕回？

答：（1）使用TCP协议在40Gbit/s的线路上传送数据，每秒可传送5×10^9字节的数据；TCP的序号字段有32位，则共有2^{32}个不同序号，可以发送的时间是2^{32}/（5×10^9）＝0.859s＝859ms；则需859ms才发生序号绕回；

（2）时间戳数据绕回的时间是：$2^{32}\times859\times10^{-6}s=3.69\times10^{6}s=42.7$天。

71在教材5.5节中指出：例如，若用2.5Gbit/s的速率发送报文段，则不到14秒钟序号就会重复。请计算验证这句话。

答：在2.5Gbit/s的线路每秒可传送0.3125×10^{9}字节的数据，TCP报文段的序号字段共可产生2^{32}个不同序号，发送的时间是$2^{32}/(0.3125\times10^{9})=13.74s<14s$，故说法正确。

72已知TCP的接收窗口大小是600（单位是字节，为简单起见以后就省略了单位），已经确认了的序号是300。试问，在不断地接收报文段和发送确认报文段的过程中，接收窗口也可能会发生变化（增大或缩小）。请用具体例子（指出接收方发送的确认报文段中的重要信息）来说明哪些情况是可能发生的，而哪些情况是不允许发生的。

答：如图5-33为接收窗口变化情况，其说明如下：

图5-33　接收窗口变化情况

如图中（1）所示，这是题目开始的情况，接收方发送的确认报文段中的接收窗口rwnd＝600；已确认的序号是300，接收方发送的确认报文段的ack＝301，表示期望收到开始的序号为301的数据，其中序号301到900都在接收窗口内。

如图中（2）所示，接收窗口增大总是不受限制的；只要接收端的TCP能够拿出更多的空间来接收发来的数据，就可以这样做；图中给出的例子是：已确认的序号是350，接收方发送的确认报文段为ack＝351，假定现在接收窗口从情况（1）的600增大到了700，即rwnd＝700，现在接收窗口的范围是从351到1050；当接收窗口增大时，接收窗口的前沿总是向前移动的。

如图中（3）所示，这种情况是接收窗口变小了，但接收窗口的前沿没有变化；例如，现在的已确认的序号是350，接收方发送的确认报文段的ack＝351，假定现在接收窗口从情况（1）的600减少到了550，即rwnd＝550，接收窗口的范围是从351到900。

如图中（4）所示，这种情况是接收窗口变小了，同时接收窗口的前沿也向前移动了；例如，现在已确认的序号是400，接收方发送的确认报文段的ack＝401，假定现在接收窗口从情况（1）的600减少到了550，即rwnd＝550，接收窗口的范围是从401到950。

如图中（5）所示，这种情况是接收窗口变小了，但接收窗口的前沿是后退的；例如，现在已确认的序号是400，接收方发送的确认报文段的ack＝401，假定现在接收窗口从情况（1）的600减小到了300，即rwnd＝300，接收窗口的范围是从401到700，注意这种情况是不允许出现的，也就是说，接收窗口的前沿是不允许后退的。在开始时，接收窗口的前沿的编号是900，不管是接收窗口是变大还是变小，这个窗口的前沿的编号可以不动，也可以前移，但是不允许后退。

73在上题中，如果接收方突然因某种原因不能够再接收数据了，可以立即向发送方发送把接收窗口置为零的报文段（即rwnd＝0）。这时会导致接收窗口的前沿后退。试问这种情况是否允许？

答：这种情况是允许的；当发送方收到这样的信息，并不是把发送窗口缩回到零，而是立即停止发送，什么时候可以再发送数据，就要等接收方重新开放接收窗口，即给出一个非零的接收窗口。

74流量控制和拥塞控制的最主要的区别是什么？发送窗口的大小取决于流量控制还是拥塞控制？

答：（1）区别：

①拥塞控制是为了让网络能够承受现有的网络负荷，防止过多数据注入网络，是一个全局控制过程；

②流量控制是接收方控制发送方，是一种点对点的流量的控制。

（2）不管是拥塞控制还是流量控制都会影响发送窗口的大小，即发送窗口大小取两者的最小值。

5.3　考研真题详解

一、选择题

1对于滑动窗口协议，如果分组序号采用3比特编号，发送窗口大小为5，则接收窗口最大是（　　）。[2019年408统考]

A．2

B．3

C．4

D．5

【答案】B

【解析】对于滑动窗口协议，如果分组序号采用n比特编号，则：发送窗口大小＋接收窗口大小≤2^n，由题意可知，分组序号采用3比特编号，发送窗口大小为5，所以接收窗口大小≤2^3-5，即最大为3，答案选B。

2某客户通过一个TCP连接向服务器发送数据的部分过程如图5-34所示。客户在t0时刻第一次收到确认序列号ack_seq=100的段，并发送序列号seq=100的段，但发生丢失。若TCP支持快速重传，则客户重新发送seq=100段的时刻是（　　）。[2019年408统考]

A．t1

B．t2

C．t3

D．t4

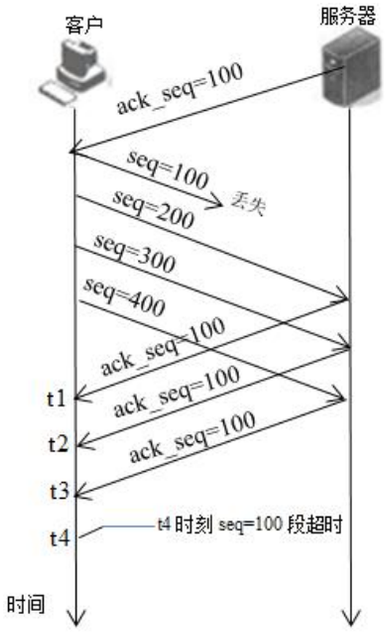

图5-34

【答案】C

【解析】当连续三次收到相同的序列号时，将会重新发送。

3UDP协议实现分用（demultiplexing）时所依据的头部字段是（　　）。[2018年408统考]

A．源端口号

B．目的端口号

C．长度

D．校验和

【答案】B

【解析】UDP进程依据UDP用户数据报头部中的目的端口号字段的值将UDP用户数据报交付给相应的应用进程。

4主机甲通过128kbps卫星链路，采用滑动窗口协议向主机乙发送数据，链路单向传播延迟为250ms，帧长为1000字节。不考虑确认帧的开销，为使链路利用率不小于80%，帧序号的比特数至少是（　　）。[2015年408统考]

A．3

B．4

C．7

D．8

【答案】B

【解析】以发送周期为切入点来思考这个问题。开始发送帧到收到第一个确认帧为止，用时：T＝第一个帧的传输时延＋第一个帧的传播时延＋确认帧的传输时延＋确认帧的传播时延。因为确认帧的开销不计，所以它的传输不计。但是传播时延要计的。所以T＝1000B/128kbps＋RTT＝0.5625s，那么在0.5625s内需要发送多少数据可以满足利用率80%呢？设为L字节，则：L128kbpsT≥0.8→L＝7200BL128kbpsT≥0.8→L＝7200B，就是说在一个发送周期内至少发7.2帧就可满足要求。因此，需要编号的比特数为n，有2n−1≥7.22n−1≥7.2成立，所以n至少为4。

5主机甲与主机乙之间已建立一个TCP连接，主机甲向主机乙发送了3个连续的TCP段，分别包含300B、400B和500B的有效载荷，第3个段的序号为900。若主机乙仅正确接收到第1个和第3个TCP段，则主机乙发送给主机甲的确认序号是（　　）。[2011年408统考]

A．300

B．500

C．1200

D．1400

【答案】B

【解析】首先应该计算出第二个段的第一个字节的序号。第三个段的第一个字节序号为900，由于第二个段有400B，所以第二个段的第一个字节的序号为900－400＝500。由于确认号就是期待接收下一个TCP段的第一个字节序号，所以主机乙发送给主机甲的确认序号是500。这一题相对比较简单，考生只要理解TCP发送确认号的原理就可以了。

6主机甲向主机乙发送一个（SYN＝1，SEQ＝11220）的TCP段，期望与主机乙建立TCP连接，若主机乙接受该连接请求，则主机乙向主机甲发送的正确的TCP段可能是（　　）。[2011年408统考]

A．（SYN＝0，ACK＝0，SEQ＝11221，ack＝11221）

B．（SYN＝1，ACK＝1，SEQ＝11220，ack＝11220）

C．（SYN＝1，ACK＝1，SEQ＝11221，ack＝11221）

D．（SYN＝0，ACK＝0，SEQ＝11220，ack＝11220）

【答案】C

【解析】首先，不管是连接还是释放，一般只要写出来，SYN、ACK、FIN的值一定是1，排除A项和D项。确认号是甲发送的序列号加1，ack的值应该为11221（即11220已经收到，期待接收11221），所以排除B项可得正确答案是C项。另外需要重点提醒的是，乙的SEQ值是主机随意给的，和甲的SEQ值没有任何关系，这里只是巧合。

7主机甲和主机乙之间建立一个TCP连接，TCP最大段长度为1000字节，若主机甲的当前拥塞窗口为4000字节，在主机甲向主机乙连续发送2个最大段后，成功收到主机乙发送的第一段的确认段，确认段中通告的接收窗口大小为2000字节，则此时主机甲还可以向主机乙发送的最大字节数是（　　）。[2010年408统考]

A．1000

B．2000

C．3000

D．4000

【答案】A

【解析】发送方的发送窗口的上限值应该取接收方窗口和拥塞窗口这两个值中较小的一个，于是此时发送方的发送窗口为MIN{4000，2000}＝2000字节，由于发送方还没有收到第二个最大段的确认，所以此时主机甲还可以向主机乙发送的最大字节数为2000－1000＝1000字节。

8一个TCP连接总是以1KB的最大段来发送TCP段，发送方有足够多的数据要发送。当拥塞窗口为16KB时发生了超时，如果接下来的4个RTT（往返时间）时间内的TCP段的传输都是成功的，那么当第4个RTT时间内发送的所有TCP段都得到肯定应答时，拥塞窗口的大小是（　　）。[2009年408统考]

A．7KB

B．8KB

C．9KB

D．16KB

【答案】C

【解析】当拥塞窗口为16KB时发生了超时，慢开始门限值减半后将变成8KB，发送窗口变为1KB。下面逐一列出各个RTT之后的拥塞窗口大小。

①开始重传：此时拥塞窗口为1KB；

②第一次RTT结束：执行慢开始算法，此时拥塞窗口为2KB；

③第二次RTT结束：执行慢开始算法，此时拥塞窗口为4KB；

④第三次RTT结束：执行慢开始算法，此时拥塞窗口为8KB；

⑤第四次RTT结束：由于第三次RTT结束的时候拥塞窗口的大小已经和慢开始门限值相等，所以此时应该结束使用慢开始算法，转而使用拥塞避免算法，故此时拥塞窗口为8KB＋1KB＝9KB。

9数据链路层采用后退N帧（GBN）协议，发送方已经发送了编号0～7的帧。当计时器超时时，若发送方只收到0、2、3号的确认，则发送方需要重发的帧数是（　　）。[2009年408统考]

A．2

B．3

C．4

D．5

【答案】C

【解析】根据后退N帧协议工作原理：发送方发送完一个数据帧后，不是停下来等待确认帧，而是可以连续再发送若干个数据帧。如果这时收到了接收方的确认帧，那么还可以接着发送数据帧。但一旦某个帧出错，接收方只能简单的丢弃该帧及其所有的后续帧。发送方超时后需重发该出错帧及其后续所有的帧。接收方只允许顺序接收，发送方收到3号帧的确认，因此，接受方正确接收了3号以及3号以前的帧，因此发送方需要重新发送的帧为4～7号这4个帧。

二、综合题

本地主机C通过TCP协议向远端服务器S发送数据，下图5-35和图5-36以十六进制格式列出了C发给S的某个IP包的前40字节内容。

45 00 02 28 14 08 40 00 40 06 48 9a c0 a8 00 67 d3 44 47 d6

52 b0 00 50 16 dc aa 14 81 87 c3 04 50 18 01 02 66 2c 00 00

（1）以点分十进制格式写出C和S的IP地址，以十进制写出TCP连接两端的端口号。

（2）这个IP包中的TTL字段值是多少？在IP包头部中设置TTL字段的目的是什么？

（3）不计IP和TCP包头，这个数据包运载了多少字节的应用层数据？以十六进制写出应用层首字节对应的SEQ序号。假设C不再继续发送数据，那么，S正确接收到这个IP包后回复包TCP包头中的ACK序号应该怎么填写？[北京邮电大学2018研]

图5-35

图5-36

答：（1）根据IP包头格式，可以将十六进制与二进制转换后划分成不同部分：version：0100；IHL：0101；Type of service：000000；Total length：0000 0010 0010 1000；Identification：0001 0100 0000 1000；DF：1；MF：0；Fragment offset：00000 0000 0000；Time to live：0100 0000；Protocol：0000 0110；Header checksum：0100 1000 1001 1110；Source address：1100 0000.1010 1000.0000 0000.0110 0111；Destination address：1101 0011.0100 0100.0100 0111.1101 0110；所以源IP地址为：192.168.0.103；目的IP地址为：211.68.71.214

根据TCP包头格式，可以得到Source port：（52 b0）$_{16}$＝21168；Destination port：（00 50）$_{16}$＝80。

（2）由上一小问可以看出TTL字段的二进制表示是0100 0000，所以字段值为64。设置TTL字段值的目的是可以避免数据报在网络中无休止的传递。当该字段为0时，报文将被删除，避免死循环的发生。

（3）由IP包头格式可得Total length=（1000101000）$_2$=552，即网络层中IP数据包总长度为552字节，则应用层数据有：552－20＝532，532－20＝512字节数据。ACK＝SEQ＋窗口大小＝16 dc ab 16。

第6章　应用层

6.1　复习笔记

一、域名系统DNS

1域名系统概述

域名系统DNS是互联网使用的命名系统，用来把便于人们使用的机器名字转换为IP地址；DNS系统采用客户/服务器模式，其协议运行在UDP上，使用53号端口。

2因特网的域名结构

例如域名www.baidu.com中标号www为三级域名，标号baidu为二级域名，标号com为顶级域名，类似于这种表示方法，互联网采用层次树状结构的命名方法命名域名，如图6-1所示为域名空间结构。

图6-1　互联网的域名空间

【注意】域名中的标号使用应注意以下几点：

①标号中的英文不区分大小写；

②每一个标号不超过63个字符，多标号组成的完整域名不超过255个字符；

③标号按级别从低（左）到高（右）书写。

3域名服务器

（1）域名服务器的概念与分类

①概念

互联网的域名系统通过设置相应权限的域名服务器来保存相应范围主机的域名到IP地址的映射。

②分类

互联网上的DNS域名服务器是按照层次安排的，如图6-2所示。

图6-2　树状结构的DNS域名服务器

根据域名服务器所起的作用，可以把域名服务器划分为以下四种不同的类型（见表6-1）：

表6-1　域名服务器种类

根域名服务器	最高层次的域名服务器，所有的根域名服务器都知道所有的顶级域名服务器的 IP 地址
顶级域名服务器	负责管理在本顶级域名服务器注册的所有二级域名
权限域名服务器	每一个主机都必须在权限域名服务器处登记，一个主机最好有两个权限域名服务器
本地域名服务器	当主机发出 DNS 查询请求时，该报文首先发给该主机的本地域名服务器

（2）域名解析过程

①两种域名解析方式

域名解析是将域名映射成IP地址或者把IP地址映射成域名的过程，如图6-3所示。

图6-3　两种域名解析方式

域名解析主要有以下两种方式：

a．递归查询方式

主机向本地域名服务器的查询一般采用递归查询方式，递归查询过程：如果主机所询问的本地域名服务器不知道被查询域名的IP地址，那么本地域名服务器就以DNS客户的身份，向其他根域名服务器继续发出查询请求报文（即替该主机继续查询），而不是让该主机自己进行下一步的查询；

b．迭代查询

本地域名服务器向根域名服务器的查询通常是采用迭代查询，迭代查询的特点是：当根域名服务器收到本地域名服务器发出的迭代查询请求报文时，要么给出所要查询的IP地址，要么告诉本地域名服务器下一步应当向哪一个域名服务器进行查询，然后让本地域名服务器进行后续的查询（而不是替本地域名服务器进行后续的查询）。

②域名解析示例

主机m.xyz.com发送邮件给主机y.abc.com，其查询主机y.abc.com的IP地址的步骤：

a．主机m.xyz.com向本地域名服务器dns.xyz.com发起递归查询；

b．本地域名服务器采用迭代查询，向一个根域名服务器发起查询；

c．根域名服务器告诉本地域名服务器，下一次应查询的顶级域名服务器dns.com的IP地址；

d．本地域名服务器向顶级域名服务器dns.com发起查询；

e．顶级域名服务器dns.com告诉本地域名服务器，下一次应查询的权限域名服务器dns.abc.com的IP地址；

f．本地域名服务器向权限域名服务器dns.abc.com发起查询；

g．权限域名服务器dns.abc.com告诉本地域名服务器，所查询的主机的IP地址；

h．本地域名服务器最后把查询结果告诉主机m.xyz.com。

二、文件传送协议

1FTP的工作原理

（1）FTP的功能

文件传送协议FTP只提供文件传送的一些基本的服务，使用可靠的TCP运输服务与客户/服务器的工作方式，其主要功能有：

①提供文件传输功能给不同的主机系统；

②提供对远程FTP服务器的文件管理功能；

③提供公用文件共享功能。

（2）FTP的工作步骤

FTP的服务器进程由主进程（负责接受新的请求）与若干个从属进程（负责处理单个请求）组成，其工作步骤如下：

①打开熟知端口21（控制端口），使客户进程能够连接上；

②等待客户进程发出连接请求；

③启动从属进程来处理客户进程发来的请求，从属进程对客户进程的请求处理完毕后即终止；

④回到等待状态，继续接受其他客户进程发来的请求。

【注意】主进程与从属进程的处理是并发地进行。

（3）FTP的两种连接

如图6-4所示，FTP的客户和服务器之间要建立两个并行的TCP连接：

①控制连接：在整个会话期间一直保持打开，FTP客户所发出的传送请求，通过控制连接发送给服务器端的控制进程，它不用来传送文件；

②数据连接：实际用于传输文件的连接。

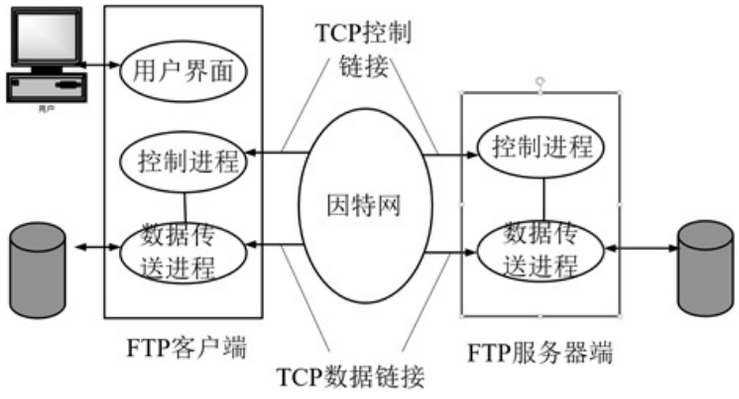

图6-4　FTP使用的两个TCP连接

2简单文件传送协议TFTP

简单文件传送协议TFTP是一个很小且易于实现的文件传送协议，可用于UDP环境，代码所占的内存较小。

三、远程终端协议TELNET

TELNET是一个简单的远程终端协议。用户用TELNET就可在其所在地通过TCP连接注册（登录）到远地的另一个主机上（使用主机名或IP地址）。

四、万维网WWW

万维网是一个资料空间，把海量信息分布到整个互联网上，每台主机的文档都独立进行管理，它采用客户/服务器方式工作；其内核部分主要由三个标准构成。

1统一资源定位符URL

URL负责标识万维网上的各种文档，且每个文档在整个万维网范围内具有唯一的标识符URL，它的一般形式为：<协议>://<主机>:<端口>/<路径>；其中，<协议>指出使用什么协议来获取该万维网文档，例如http；<主机>指出这个万维网文档是在哪一个主机上；<端口>和<路径>有时可省略。

2超文本传送协议HTTP

（1）HTTP的操作过程

如图6-5所示，万维网网点的服务器进程不断监听TCP的端口80以发现是否有浏览器（客户）向它发出连接建立请求，一旦监听到连接建立请求并建立了TCP连接之后，浏览器就向万维网服务器发出浏览某个页面的请求，服务器响应并返回所请求的页面；最后，TCP连接释放。其中浏览器和服务器之间的请求和响应，必须遵循超文本传送协议HTTP。

图6-5　万维网的工作过程

（2）HTTP的特点

①HTTP本身是无连接的，它使用面向连接的TCP作为运输层协议，保证数据的可靠传输；

②HTTP是无状态的，同一客户在第二次访问同一服务器的页面时，服务器的响应与第一次相同；

③HTTP既可以使用非持久连接（每一个网页元素对象的传输都需要单独建立一个TCP连接），又可以使用持久连接（HTTP/1.1支持，万维网服务器在发送响应后仍保持着这条连接）。

（3）HTTP的报文结构

①HTTP报文的分类

HTTP报文的每个字段都是一个ASCII码串，有下面两类：

a．请求报文：从客户向服务器发送的请求报文，如图6-6（a）所示；

b．响应报文：从服务器到客户的回答报文，如图6-6（b）所示。

图6-6　两种HTTP报文

②HTTP报文的结构

a．开始行：用于区分是请求报文还是响应报文；请求报文中的开始行叫做请求行，响应报文中的开始行叫做状态行；开始行的三个字段之间用空格分隔开，最后的“CR”和“LF”分别代表“回车”和“换行”；

b．首部行：用来说明浏览器、服务器或报文主体的一些信息；

c．实体主体：在请求报文中一般都不用这个字段，而在响应报文中也可能没有这个字段。

③HTTP报文示例

如下所示为一个完整的HTTP请求报文的示例：

Get /dir/index.htm HTTP/1.1　{请求行使用了相对URL}

Host:www.xyz.edu.com　{此行是首部行的开始。这行给出主机的域名}

Connection:close　{告诉服务器发送完请求报文的文档后就可释放连接}

User-Agent:Mozilla/5.0　{表明用户代理是使用火狐浏览器Firefox}

Accept-Language:cn　{表明用户希望优先得到中文版本的文档}

空行　{请求报文的最后还有一个空行}

【注意】如表6-2所示为HTTP请求报文中的几个常用方法。

表6-2　HTTP请求报文中的几个常用方法

方法	意义
OPTION	请求一些选项的信息
GET	请求读取由 URL 所标志的信息
HEAD	请求读取由 URL 所标志的信息的首部
POST	给服务器添加信息
PUT	在指明的 URL 下存储一个文档
DELETE	删除指明的 URL 所标志的资源
TRACE	用来进行环回测试的请求报文
CONNECT	用于代理服务器

3超文本标记语言HTML

超文本标记语言HTML是一种制作万维网页面的标准语言，它消除了不同计算机之间信息交流的障碍。

五、电子邮件

1电子邮件的组成

如图6-7所示，电子邮件主要由以下几个构件组成（见表6-3）：

表6-3　电子邮件的构件

构件	解释
用户代理	用户与电子邮件系统的接口，一般是运行在用户 PC 中的一个程序（具有邮件撰写、显示、处理和通信的功能）
邮件服务器	用于发送和接收邮件，并向发件人报告邮件发送结果
邮件发送协议和邮件读取协议	例如 SMTP 是邮件发送协议，POP3 是邮件读取协议

图6-7　电子邮件的最主要的组成构件

2电子邮件的信息格式

一个电子邮件分为信封和内容两大部分，邮件内容首部包括一些关键字，后面加上冒号；例如常见关键字：

“To:”：后面填入一个或多个收件人的电子邮件地址；

“Subject:”：后面填入邮件的主题；

“From:”：后面一般自动填写发件人信息。

3两种常见邮件协议

（1）简单邮件传送协议SMTP

SMTP是一种采用“推”的方式来进行邮件传输的协议，它的通信主要有以下三个阶段：

①连接建立：发件人的邮件送到发送方邮件服务器的邮件缓存后，SMTP客户每隔一定时间就对邮件缓存扫描一次，若发现有邮件，就使用SMTP的熟知端口号25与接收方邮件服务器的SMTP服务器建立TCP连接；

②邮件传送：邮件的传送从MAIL命令开始，MAIL命令后面有发件人的地址；

③连接释放：邮件发送完毕后，SMTP客户应发送QUIT命令。

（2）邮件读取协议POP3

邮局协议POP3是一种采用“拉”的方式进行邮件传输的协议，它使用客户/服务器的工作方式，在传输层使用TCP协议，端口号是110。

接收邮件的用户PC机中的用户代理必须运行POP客户程序，而在收件人所连接的ISP邮件服务器中则运行POP服务器程序。POP3协议的一个特点就是只要用户从POP服务器读取了邮件，POP服务器就把该邮件删除。

【注意】读取邮件的协议还有网际报文存取协议IMAP，它比POP3复杂得多。

4电子邮件的收发过程

电子邮件的收发过程如下：

（1）发信人使用用户代理编辑要发送的文件，用户代理使用SMTP协议将邮件发送到发送方邮件服务器；

（2）发送方邮件服务器将邮件放入邮件缓存队列并等待发送；

（3）SMTP客户进程定期扫描邮件缓存，若发现有邮件，就向接收方的SMTP服务器发送建立TCP连接；

（4）TCP连接建立后，SMTP将邮件从客户进程发往服务器，发完后关闭连接；

（5）接收方邮件服务器将收到的邮件放入收信人的用户邮箱中，等待收件人读取；

（6）收件人调用用户代理，使用POP3（或IMAP）协议从接收方邮件服务器中的用户邮箱中取出。

5通用互联网邮件扩充MIME

如图6-8所示，MIME并没有改动或取代SMTP，它继续使用目前的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。

图6-8　MIME和SMTP的关系

六、动态主机配置协议DHCP

1DHCP的概念

DHCP协议用于给主机动态分配IP地址，是基于UDP的应用层协议，工作在客户/服务器模式下。

2DHCP的工作过程

DHCP的工作过程如下：

（1）需要动态配置IP地址的主机（DHCP客户）在启动时广播“DHCP发现报文”，试图找到本网络的DHCP服务器；

（2）DHCP服务器收到“DHCP发现报文”后，在其数据库中查找该主机的配置信息，若找到，直接向网络中广播“DHCP提供报文”，该报文包括了IP地址和相关配置信息；若找不到，则从服务器的IP地址池中取出一个地址分配给主机，同样向网络中广播“DHCP提供报文”；

（3）DHCP客户机收到“DHCP提供报文”后，若接受DHCP服务器提供的相关参数，则通过广播“DHCP请求报文”向DHCP服务器请求提供IP地址；

（4）DHCP服务器广播“DHCP确认报文”，将IP地址分配给DHCP客户机。

七、简单网络管理协议SNMP

SNMP是用于在IP网络管理网络节点（服务器、工作站、路由器、交换机及集线器等）的一种标准协议，它是一种应用层协议；SNMP能够发现并解决网络问题并规划网络增长；SNMP的操作只有两种基本的管理功能：

1．“读”操作：用Get报文来检测各被管对象的状况；

2．“写”操作：用Set报文来改变各被管对象的状况。

SNMP的这些功能通过探询操作来实现，即SNMP管理进程定时向被管理设备周期性地发送探询信息。

八、应用进程跨越网络的通信（略）

九、P2P应用

P2P模型是相对于客户/服务器模型而言的，与C/S模型相比，其主要优点有：

1．各节点地位平等，消除了对某个服务器的完全依赖，提高了系统效率和资源利用率；

2．可扩展性好，没有传统服务器上关于带宽的过多限制；

3．单个结点的宕机不会影响整个网络，健壮性良好；

4．用户之间可以直接共享文档。

【注意】如表6-4所示为常见的应用层协议总结。

表6-4　常见应用层协议

应用程序	FTP 数据连接	FTP 控制连接	TELNET	SMTP	DNS	TFTP	HTTP	POP3	SNMP
使用协议	TCP	TCP	TCP	TCP	UDP	UDP	TCP	TCP	UDP
熟知端口	20	21	23	25	59	69	80	110	161

6.2　课后习题详解

1互联网的域名结构是怎样的？它与目前的电话网的号码结构有何异同之处？

答：（1）互联网的域名结构由标号序列组成，各标号之间用点隔开：三级域名.二级域名.顶级域名，例如域名www.baidu.com中标号www为三级域名，标号baidu为二级域名，标号com为顶级域名，各标号分别代表不同级别的域名。

（2）相同之处：都采用若干个分量表示，各个分量之间代表不同的级别。

不同之处：

①电话号码网中级别高的域名写在最左边，级别最低的域名写在最右边；而域名系统则相反；

②打电话时按号码拨打即可，但在互联网中，不能按域名直接通信，域名系统必须进行域名到IP地址的转换并得到了IP地址后，才能进行通信。

2域名系统的主要功能是什么？域名系统中的本地域名服务器、根域名服务器、顶级域名服务器以及权限域名服务器有何区别？

答：（1）域名系统的主要功能：将域名解析为主机能识别的IP地址。

（2）本地域名服务器、根域名服务器、顶级域名服务器以及权限域名服务器的区别：

①根域名服务器：最高层次的域名服务器，所有的根域名服务器都知道所有的顶级域名服务器的IP地址；

②顶级域名服务器：负责管理在本顶级域名服务器注册的所有二级域名；

③权限域名服务器：每一个主机都必须在权限域名服务器处登记，一个主机最好有两个权限域名服务器；

④本地域名服务器：当主机发出DNS查询请求时，该报文首先发给该主机的本地域名服务器。

3举例说明域名转换的过程。域名服务器中的高速缓存的作用是什么？

答：（1）主机m.xyz.com发送邮件给主机y.abc.com，其查询主机y.abc.com的IP地址（域名转换）的步骤：

①主机m.xyz.com向本地域名服务器dns.xyz.com发起递归查询；

②本地域名服务器采用迭代查询，向一个根域名服务器发起查询；

③根域名服务器告诉本地域名服务器，下一次应查询的顶级域名服务器dns.com的IP地址；

④本地域名服务器向顶级域名服务器dns.com发起查询；

⑤顶级域名服务器dns.com告诉本地域名服务器，下一次应查询的权限域名服务器dns.abc.com的IP地址；

⑥本地域名服务器向权限域名服务器dns.abc.com发起查询；

⑦权限域名服务器dns.abc.com告诉本地域名服务器，所查询的主机的IP地址；

⑧本地域名服务器最后把查询结果告诉主机m.xyz.com。

（2）高速缓存用来存放最近查询过的域名以及从何处获得域名映射信息的记录，域名服务器中的高速缓存的作用是：提高DNS查询效率，减轻域名服务器的负荷，并减少因特网上的DNS查询报文数量。

4设想有一天整个因特网的DNS系统都瘫痪了（这种情况不大会出现），试问还有可能给朋友发送电子邮件吗？

答：有可能。DNS是因特网上使用的命名系统，用来便于人们使用域名转换为IP地址，通常人们发送电子邮件时是通过邮箱服务器别名进行识别的。如果DNS系统瘫痪时，虽然无法通过邮箱服务器别名查找邮件地址，但可以通过IP地址直接进行通信，前提是你必须记住自己邮箱服务器的IP地址和朋友邮箱服务器的IP地址。

5文件传送协议FTP的主要工作过程是怎样的？为什么说FTP是带外传送控制信息？主进程和从属进程各起什么作用？

答：（1）FTP的主要工作过程如下：

①打开熟知端口21（控制端口），使客户进程能够连接上；

②等待客户进程发出连接请求；

③启动从属进程来处理客户进程发来的请求，从属进程对客户进程的请求处理完毕后即终止；

④回到等待状态，继续接受其他客户进程发来的请求。

（2）由于FTP使用了一个分离的控制连接，因此FTP的控制信息是带外传送的，使用两个独立的连接使得协议更加简单，也更容易实现。

（3）主进程负责接收新的请求；若干个从属进程负责处理单个请求。

6简单文件传送协议TFTP与FTP的主要区别是什么？各用在什么场合？

答：（1）简单文件传送协议TFTP是一个很小且易于实现的文件传送协议；它与TCP的主要区别是：

①两者均使用客户/服务器方式，但TFTP使用UDP连接，FTP使用TCP连接；

②TFTP较FTP更加简单，它只支持文件传输而不支持交互。

（2）FTP适用于客户与服务器任意多次双向传送单一文件或多个文件；而TFTP适用于文件传送功能简单，速度要求高，内存容量要求低的文件传送情景。

7远程登录TELNET的主要特点是什么？什么叫做虚拟终端NVT？

答：（1）TELNET是一个简单的远程终端协议。用户用TELNET就可在其所在地通过TCP连接注册（登录）到远地的另一个主机上（使用主机名或IP地址）；TELNET的主要特点包括：

①使用客户/服务器方式，在本地主机运行TELNET客户进程，而在远地主机上运行TELNET服务器进程；

②TELNET能够适应许多异构的计算机和操作系统的差异。

（2）网络虚拟终端NVT是为了适应计算机和操作系统的差异，TELNET定义的数据和命令通过互联网的方式。

8解释以下名词。各英文缩写词的原文是什么？

WWW，URL，HTTP，HTML，CGI，浏览器，超文本，超媒体，超链，页面，活动文档，搜索引擎。

答：（1）WWW：原文是World Wide Web，又称万维网，是一个大规模的、联机式的信息储藏所；

（2）URL：原文是Uniform Resource Locator，又称统一资源定位符，用来标志万维网上的各种文档，并使每一个文档在整个万维网的范围内具有唯一的标识符；

（3）HTTP：原文是Hyper Text Transfer Protocol，又称为超文本传输协议，主要是为了实现万维网上各种链接，使万维网客户程序与万维网服务器程序之间的交互遵守严格的协议；

（4）HTML：原文是Hyper Text Markup Language，又称为超文本标记语言，是一种制作万维网页面的标准语言，消除了不同计算机之间信息交流的障碍；

（5）CGI：原文是Common Gateway Interface，又称为通用网关接口，它定义了动态文档应当如何创建，输入数据应如何提供给应用程序，以及输出结果应当如何使用；

（6）浏览器：在用户主机上的万维网客户程序；

（7）超文本：是由多个信息源链接而成的一种文本信息；

（8）超媒体：超媒体与超文本的区别是文档内容不同，它不仅包含有文本信息，还包含有其他表示方式的信息，如图形、图像、声音、动画，或者活动视频图像；

（9）超链：指超文本中的一种链接；

（10）页面：指在一个客户程序主窗口上显示出来的万维网文档；

（11）活动文档：是一种提供屏幕连续更新的技术，即将所有的工作都转移给浏览器端；

（12）搜索引擎：在万维网中用来进行搜索的程序。

9假定一个超链从一个万维网文档链接到另一个万维网文档时，由于万维网文档上出现了差错而使得超链指向一个无效的计算机名字。这时浏览器将向用户报告什么？

答：当万维网文档上出现了差错而使得超链接指向一个无效的计算机名字时，浏览器会将向用户报告：404 Not Found。

10假定要从已知的URL获得一个万维网文档。若该万维网服务器的IP地址开始时并不知道。试问：除HTTP外，还需要什么应用层协议和运输层协议？

答：假定要从已知的URL获得一个万维网文档，若该万维网的IP地址开始时并不知道，则除HTTP外，应用层还需要DNS协议，而运输层需要UDP协议（DNS使用）和TCP协议（HTTP使用）。

11你所使用的浏览器的高速缓存有多大？请进行一个实验：访问几个万维网文档，然后将你的计算机与网络断开，然后再回到你刚才访问过的文档，你的浏览器的高速缓存能够存放多少个页面？

答：浏览器的高速缓存大小与用户所使用的机器有直接的关系，因不同机器而定，这里略。

12什么是动态文档？试举出万维网使用动态文档的一些例子。

答：（1）动态文档：指文档的内容是在浏览器访问万维网服务器时才由应用程序动态创建；

（2）举例：查看天气预报时，因为天气预报时实时的，所以一般在我们访问的时候才更新实时数据并创建。

13浏览器同时打开多个TCP连接进行浏览的优缺点如何？请说明理由。

答：（1）优点：可以同时下载好几个对象（文件或图片），加快了下载的速度；

（2）缺点：由于计算机连接到网络的线路的数据率是受限的，几个下载的数据率的总和不能超过连接到网络的线路的数据率；这时还要对大量的文件进行缓存，会占用较多的存储空间，并且，由于浏览器要耗费时间来把这些文件存储在磁盘上，有可能反而降低了浏览器的效率。

14当使用鼠标点击一个万维网文档时，若该文档除了有文本外，还有一个本地.gif图像和两个远地.gif图像。试问：需要使用哪个应用程序，以及需要建立几次UDP连接和几次TCP连接？

答：需要使用支持HTTP协议的应用程序；

若使用HTTP/1.0，则需要建立0次UDP连接和4次TCP连接（1个文本和3个图像各使用一个TCP连接）；

若使用HTTP/1.1，则需要建立0次UDP连接和1次TCP连接（1个文本和3个图像使用同一个TCP连接）。

15假定你在浏览器上点击一个URL，但这个URL的IP地址以前并没有缓存在本地主机上。因此需要用DNS自动查找和解析。假定要解析到所要找的URL的IP地址共经过n个DNS服务器，所经过的时间分别为RTT_1，RTT_2，…，RTT_n。假定从要找的网页上只需要读取一个很小的图片（即忽略这个小图片的传输时间）。从本地主机到这个网页的往返时间是RTT_W。试问从点击这个URL开始，一直到本地主机的屏幕上出现所读取的小图片，一共要经过多少时间？

答：从点击URL开始到本地主机屏幕上出现小图片，共分为两个过程：域名解析和图片传输。

域名解析在运输层采用的是UDP协议，所以迭代查询经过n个DNS服务器需要时间为：$RTT_1+RTT_2+\ldots+RTT_n$；

图片传输时，在运输层采用TCP协议传输，所需时间为$2RTT_W$；

因此，总共需要的时间为：$RTT_1+RTT_2+\ldots+RTT_n+2RTT_W$。

16在上题中，假定同一台服务器的HTML文件中又链接了三个非常小的对象。若忽略这些对象的发送时间，试计算客户点击读取这些对象所需的时间。

（1）没有并行TCP连接的非持续HTTP；

（2）使用并行TCP连接的非持续HTTP；

（3）流水线方式的持续HTTP。

答：域名解析需要的时间不变，为：$RTT_1+RTT_2+\ldots+RTT_n$。

（1）当采用没有并行TCP连接的非持续HTTP传输时，请求一个万维网文档的时间是$2RTT_W$，则所需时间$=RTT_1+RTT_2+\ldots+RTT_n+2RTT_W$（建立TCP连接和读取HTML文件用时）$+3\times$（$2RTT_W$）（读取三个对象的用时）$=RTT_1+RTT_2+\ldots+RTT_n+8RTT_W$。

（2）当采用并行的TCP连接的非持续HTTP传输时，能节省后续的（除第一个对象）的建立TCP请求的时间，即花费的时间为：$2RTT_W+(n-1)RTT_W=2RTT_W+(3-1)RTT_W=4RTT_W$，总的时间$=RTT_1+RTT_2+\ldots+RTT_n+4RTT_W$。

（3）当采用流水线方式HTTP时，总的时间$=RTT_1+RTT_2+\ldots+RTT_n+2RTT_W$（建立TCP连接和读取HTML文件的用时）$+RTT_W$（连续读取三个对象的用时）$=RTT_1+RTT_2+\ldots+RTT_n+3RTT_W$。

17在浏览器中应当有几个可选解释程序，试给出一些可选解释程序的名称。

答：在浏览器中的解释程序数目并无明确规定，其中HTML解释程序是必不可少的，而其他的解释程序则是可选的，例如，Java小应用程序解释程序是可选解释程序。

18一个万维网网点有1000万个页面，平均每个页面有10个超链。读取一个页面平均要100ms。问要检索整个网点所需要的最少时间。

答："平均每个页面有10个超链"为干扰条件，因为题中并未指出是否还要点击这10个超链，以及是否要在点击超链后再继续点击下去等条件，即本题是求读取这1000万个网页需要的时间；又因为读取一个页面平均要100ms，那么读取1000万个页面，就需要时间$T=10^7\times100\times10^{-3}=10^6s\approx11.6$天。

19搜索引擎可分为哪两种类型？各有什么特点？

答：（1）搜索引擎可以划分为两类：全文检索搜索引擎和分类目录搜索引擎。

（2）它们的特点分别是：

①全文检索搜索引擎：是一种纯技术型的检索工具，它通过搜索软件到互联网上的各网站收集信息，找到一个网站后可以从这个

网站再链接到另一个网站，然后按照一定的规则建立起一个很大的在线数据库供用户查询；用户输入关键词即可进行查询；这种方式可以检索出大量的信息，但查询结果不够准确。

②分类目录搜索引擎：它不采集网站的任何信息，而是利用各网站向搜索引擎提交网站信息时填写的关键词和网站描述等信息，经过人工审核编辑后，将符合网站登录条件的输入到分类目录的数据库中，供网上用户查询；这种方式查询的准确性较好，但所得到的内容比较有限。

20试述电子邮件的最主要的组成部件。用户代理UA的作用是什么？没有UA行不行？

答：（1）电子邮件的主要组成部件有三个：用户代理、邮件服务器、邮件发送协议和邮件读取协议。

（2）用户代理UA是用户与电子邮件系统的接口，在多数情况下，是指在用户PC机中运行的程序。用户代理向用户提供一个很友好的接口来发送和接收邮件，它的功能主要包括：

①撰写：给用户提供编辑信件的环境；

②显示：在计算机屏幕上显示信件；

③处理：包括发送邮件和接收邮件；

④通信：发信人在撰写完邮件后，利用邮件发送协议发送到用户所使用的邮件服务器。

（3）没有用户代理是不行的。如果没有用户代理UA，那么对于要使用电子邮件的用户就很不方便了。

21电子邮件的信封和内容在邮件的传送过程中起什么作用？和用户的关系如何？

答：（1）电子邮件由信封和内容两部分组成，其作用分别是：

①信封的作用：电子邮件的传输程序根据邮件信封上的信息来传送邮件，例如信封上的收件人信息尤为重要。

②内容的作用：电子邮件的内容在邮件传送过程中是不暴露出来的，它包含了用户想要传输的信息，且用户可以传送任意格式的内容，只需收件人能够读取这种格式的邮件即可。

（2）信封和内容与用户的关系：用户在写好首部后，邮件系统会自动将信封所需的信息提取出来并写在信封上，而内容需要用户撰写，传送过程中邮件系统不改变其内容，收件人用户接收邮件并读取后才能看到内容。

22电子邮件的地址格式是怎样的？请说明各部分的意思。

答：电子邮件系统规定电子邮件地址的格式为：

收信人邮箱名@邮箱所在主机的域名；

其中“@”表示“在”的意思；收信人邮箱名即用户名，是收信人自定义的字符串标识符，收信人邮箱名的字符串在邮箱所在计算机中必须是唯一的；邮箱所在地域名在整个互联网的范围内必须是唯一的。

23试简述SMTP通信的三个阶段的过程。

答：SMTP是一种采用“推”的方式来进行邮件传输的协议，它的通信主要有以下三个阶段：

（1）连接建立：发件人的邮件送到发送方邮件服务器的邮件缓存后，SMTP客户每隔一定时间就对邮件缓存扫描一次，若发现有邮件，就使用SMTP的熟知端口号25与接收方邮件服务器的SMTP服务器建立TCP连接；

（2）邮件传送：邮件的传送从MAIL命令开始，MAIL命令后面有发件人的地址；

（3）连接释放：邮件发送完毕后，SMTP客户应发送QUIT命令。

24试述邮局协议POP的工作过程。在电子邮件中，为什么必须使用POP和SMTP这两个协议？IMAP与POP有何区别？

答：（1）邮局协议POP的工作过程：

当收取邮件时，电子邮件软件首先根据用户名和密码调用DNS协议对POP服务器进行IP地址解析，然后邮件程序便开始使用TCP协议连接邮件服务器的110端口。当邮件程序成功地连上POP服务器后，将邮箱的账号和密码传给POP服务器，当完成认证后，邮件程序请求服务器返回邮箱的统计资料，比如邮件总数和邮件大小等；接着邮件程序根据这些信息决定接收哪一封邮件，接收后将邮件服务器中的该邮件置为删除状态，当使用QUIT时，邮件服务器便会将置为删除标志的邮件删除。

（2）使用POP和SMTP这两个协议的意义：

SMTP协议是用来发送电子邮件的，而POP协议是用户读取电子邮件的协议，这两个协议都必不可少。

（3）IMAP与POP的区别：

①IMAP是一个联机协议，用户可以在自己的PC机上操纵ISP邮件服务器的邮箱，就像在本地操纵一样。

②在用户发出删除邮件命令之前，IMAP服务器邮箱中的邮件一直保存着，而POP协议只要用户从POP服务器读取了邮件，POP服务器就把该邮件删除。

③当用户PC机上的IMAP客户程序打开IMAP服务器的邮箱时，用户就可看到邮件的首部，若用户需要打开某个邮件，则该邮件才传到用户的计算机上。而POP服务器只有在用户输入鉴别信息后，才允许读取邮件。

25MIME与SMTP的关系是怎样的？什么是quoted-printable编码和base64编码？

答：（1）MIME与SMTP的关系：SMTP存在着一些缺点和不足，所以提出了通用因特网邮件扩充协议MIME，MIME并没有改动或取代SMTP，它继续使用目前的RFC 822格式，但增加了邮件主题的结构，并定义了传送非ASCII码的编码规则，因此，MIME邮件可以在现有的电子邮件程序和协议下传送。

（2）quoted-printable编码：适用于当所传送的数据中只有少量的非ASCII码的情况，它对于所有可以打印的ASCII码，除非特殊字符等号外，都不改变。

（3）base64编码：适用于任意的二进制文件，它先将二进制代码划分为一个24bit长的单元，然后将每一个24bit单元划分为4个6bit组，每一个6bit组按照一定方法转换成ASCII码。

26一个二进制文件共3072字节长。若使用base64编码，并且每发送完80字节就插入一个回车符CR和一个换行符LF，问一共发了多少个字节？

答：使用base64编码转换后共需要传送的字节数为3072×8/6＝4096（字节），根据题意，每80个字节就插入两个字节（回车符和换行符），又4096＝51×80＋16，所以一共要插入的字节数为2×（51＋1）＝104（字节）；

因此，一共需要传输的字节数为4096＋104＝4200（字节）。

27试将数据11001100 10000001 00111000进行base64编码，并得出最后传送的ASCII数据。

答：将题中24位二进制代码11001100 10000001 00111000划分为4个6位组：110011 001000 000100 111000，对应的十进制分别为51、8、4、56，据此查找base64编码表可知最后传送的ASCII数据为zIE4。

28试将数据01001100 10011101 00111001进行quoted-printable编码，并得出最后传送的ASCII数据。这样的数据用quoted-printable编码后，其编码开销有多大？

答：（1）quoted-printable编码的规则是对于可打印的ASCII码，除特殊字符“＝”外，都不改变，“＝”和不可打印的ASCII码以及非ASCII码的数据的编码方法是：先将每个字节的二进制代码用两个十六进制数字表示，然后在前面再加上一个等号“＝”；本题中01001100 10011101 00111001的第一个和第三个字节是ASCII码，不变化，第二个字节10011101换成两个十六进制表示为：9D，在其前面加上等号变为：＝9D；将第一个和第三个字节转换成ASCII码后分别为L、9，则最后传送的ASCII数据为：L＝9D9。

（2）编码开销＝5－3＝2字节，而原来只有3字节的数据；编码开销百分比＝2/3×100%＝66.7%。

29电子邮件系统需要将人们的电子邮件地址编成目录以便于查找。要建立这种目录应将人名划分为几个标准部分（例如，姓、名）。若要形成一个国际标准，那么必须解决哪些问题？

答：在国际上形成这样一个标准非常困难。就人名的书写方法而言，英美等西方国家是名字在前，姓在后，但是中国等亚洲国家则是先写姓再写名字，而东欧、西亚还有非洲等国家除姓名之外很多还有中间名，称呼的种类也非常多，此外还有各式各样的头衔。

若要形成一个国际标准，那么必须解决的问题是：

将世界各地的人名按照统一的划分格式进行标准划分，比如一个人的名字按照“姓＋中间名＋名字”，以此才有可能形成国际标准。

30电子邮件系统使用TCP传送邮件。为什么有时我们会遇到邮件发送失败的情况？为什么有时对方会收不到我们发送的邮件？

答：虽然SMTP使用TCP连接试图使邮件的传送可靠，但它并不能保证不丢失邮件，例如对方的邮件服务器不工作，邮件就发送不出去，或者对方的邮件服务器出故障也会使邮件丢失。

31基于万维网的电子邮件系统有什么特点？在传送邮件时使用什么协议？

答：（1）基于万维网的电子邮件系统的特点：用户可以随时通过万维网浏览器进行邮件的收发，邮件系统中的用户代理就是普通的万维网浏览器，这为用户提供了极大的便利。

（2）基于万维网的电子邮件系统在传送邮件时使用HTTP协议和SMTP协议。

32DHCP协议用在什么情况下？当一台计算机第一次运行引导程序时，其ROM中有没有该主机的IP地址、子网掩码或某个域名服务器的IP地址？

答：（1）动态主机配置协议DHCP提供即插即用连网机制，允许一台计算机加入新的网络和获取IP地址不用手工参与，因此，DHCP对运行客户软件和服务器软件的计算机都适用。且DHCP服务器分配给DHCP客户的IP地址是临时的，因此还适用于经常移动位置的计算机。

（2）由于制造厂家并不知道IP地址等信息，因此当一台计算机第一次运行引导程序时，ROM中并没有该计算机的IP地址、子网掩码，或某个域名服务器的IP地址的任何一个。

33什么是网络管理？为什么说网络管理是当今网络领域中的热门课题？

答：（1）网络管理：指网络管理员通过网络管理程序对网络上的资源进行集中化管理的操作，主要包括故障管理、配置管理、计费管理、性能管理和安全管理；

（2）网络管理对一个网络系统的高效运行非常重要，随着网络使用的普及，网络性能维护、网络计费使用以及网络安全管理等方面逐渐成为人们研究的热点问题，因此，网络管理也就成为了当今网络领域中的热门课题。

34解释下列术语：网络元素、被管对象、管理进程、代理进程。

答：（1）网络元素：指被管设备，包括硬件设备和软件设备，有时也称作网元；

（2）被管对象：可以是被管设备中的某个硬件，也可以是某些硬件或软件配置参数的集合；

（3）管理进程：运行中的管理程序；

（4）代理进程：在每一个被管设备中，都要运行一个程序以便和管理站中的管理程序进行通信，这些运行着的程序叫做网络管理代理程序，或简称为代理；

35SNMP使用UDP传送报文，为什么不使用TCP？

答：使用无连接的UDP使得在网络上传送SNMP报文的开销较小，虽然UDP不保证可靠交付，但是SNMP使用周期性地发送探询报文段方法，来对网络资源进行实时监视，如果丢失了一个探寻报文，经过一段时间后会再发送一个，这样在一定程度保证了可靠性，比使用TCP更好。

36为什么SNMP的管理进程使用探询掌握全网状态属于正常情况，而代理进程使用陷阱向管理进程报告属于较少发生的异常情况？

答：SNMP的管理进程使用探询掌握全网状态，如果要想非常准确地掌握全网的状态，那么SNMP的探询频率就必须选择得非常高；且由于网络规模相差很大，网络中网元的数目有多有少。因此，SNMP标准不可能规定出探询的频率统一设为多少，这种由SNMP探询发现的网络中的问题，是属于网络管理中的正常情况。

SNMP还考虑到两次探询之间在网络中可能发生的问题，这些问题可以由陷阱向管理进程报告，这就属于较少发生的异常情况。

37SNMP使用哪几种操作？SNMP在Get报文中设置了请求标识符字段，为什么？

答：（1）SNMP有两种操作：

①“读”操作：用Get报文来检测各被管对象的状况；

②“写”操作：用Set报文来改变各被管对象的状况。

（2）在Get报文中设置有请求标识符字段，是因为管理进程可以同时向许多代理发出Get报文，这些报文都使用UDP传送，先发送的有可能后到达，设置了请求标识符可以使管理进程能够识别返回的响应报文对应于哪一个请求报文。

38什么是管理信息库MIB？为什么要使用MIB？

答：（1）管理信息库MIB是一个网络中所有可能的被管对象构成的虚拟的信息存储器。

（2）使用MIB的原因：只有在MIB中的对象才是SNMP能够管理的；MIB在被管理的实体中创建了命名对象，并规定了其类型。MIB的定义与具体的网络管理协议无关，这对于厂商和用户都有利，厂商可以在产品中包含SNMP代理软件，并保证在定义新的MIB项目后该软件仍能够遵守标准。管理程序就是使用MIB中这些信息的值对网络进行管理。

39什么是管理信息结构SMI？它的作用是什么？

答：（1）管理信息结构SMI是SNMP的重要组成部分，它定义了命名对象和定义对象类型的通用规则，以及对象和对象的值进行编码的规则。

（2）SMI的作用：

①规定被管对象应怎样命名；

②规定用来存储被管对象的数据类型有哪几种；

③规定在网络上传送的管理数据应如何编码。

40用ASN.1基本编码规则对以下4个数组（SEQUENCE-OF）进行编码。假定每一个数字占用4个字节。

2345，1236，122，1236。

答：SEQUENCE-OF类型的类别属于ASN.1定义的通用类（编码是00），格式属于结构化数据类型（编码是1），编号为10000。因此，SEQUENCE-OF的TLV编码的标记T字段的二进制编码是00110000，用十六进制写出是：0x30。

SEQUENCE-OF类型长度L字段，是4个INTERGER数字的ASN.1编码的长度，即24字节，24＝0x18。

现以对2345编码为例（INTEGER 2345）：

INTEGER类型的类别属于ASN.1定义的通用类（编码是00），格式属于简单数据类型（编码是0），编号为00010，因此，INTEGER 2345的TLV编码的标记T字段的二进制编码是00000010，用十六进制写出是：0x02；

INTEGER类型的数用4字节表示，因此长度字段L是单字节长度（1字节），其值的十六进制表示是0x04；

又因为2345的十六进制表示（使用4字节表示）为：0x00000929；

则INTEGER 2345的ASN.1编码是：020400000929，一共需要6字节。

其他数的编码和上述过程类似，则整个的编码为：

```
30 18
  02 04 00 00 09 29
  02 04 00 00 04 D4
  02 04 00 00 00 7A
  02 04 00 00 04 D4
```

41SNMP要发送一个GetRequest报文，以便向一个路由器获取ICMP的icmpInParmProbs的值。在icmp中变量icmpInParmProbs的标号是5，它是一个计数器，用来统计收到的类型为参数问题的ICMP差错报告报文的数目。试给出这个GetRequest报文的编码。

答：（1）变量icmpInParmProbs的对象标识符是1.3.6.1.2.1.5.5，加上后缀“.0”，则为1.3.6.1.2.1.5.5.0；

（2）GetRequest报文的编码为：

```
A0 1D
  02 04 00 01 06 14
  02 01 00
  02 01 00
  30 0F
    30 0D
    06 09 01 03 06 01 02 01 05 05 00
    05 00
```

42对象tcp的OBJECT IDENTIFIER是什么？

答：对象tcp的OBJECT IDENTIFIER是{1.3.6.1.2.1.6}。

43在ASN.1中，IP地址（IPAddress）的类别是应用类。若IPAddress＝131.21.14.2，试求其ASN.1编码。

答：若IPAddress＝131.21.14.2，则其ASN.1编码为：40 04 83 15 0E 02。

44什么是应用编程接口API？它是应用程序和谁的接口？

答：（1）应用编程接口API就是系统调用接口，它是应用进程的控制权和操作系统的控制权进行转换的一个接口。

（2）API是应用程序和操作系统之间的接口。

45试举出常用的几种系统调用的名称，说明它们的用途。

答：列举出下面的常用系统调用的名称和用途：

（1）bind（绑定）：用于指明套接字的本地地址；

（2）listen（收听）：用于把套接字设置为被动方式，以便随时接受客户的服务请求；

（3）accept（接受）：用于把远地客户进程发来的连接请求提取出来；

（4）connect：用于和远地服务器建立连接；

（5）send：用于在TCP连接上传送数据；

（6）recv：用于接收数据；

（7）close：用于释放连接和撤销套接字。

46图6-9表示了各应用协议在层次中的位置。

（1）简单讨论一下为什么有的应用层协议要使用TCP而有的却要使用UDP？

（2）为什么MIME画在SMTP之上？

（3）为什么路由选择协议RIP放在应用层？

图6-9　46题图

答：（1）应用层协议根据各自功能的需求，有的需要使用面向连接的TCP服务，提供可靠的数据传输服务，如FTP，HTTP等；而有的协议使用无连接的UDP服务，提供比较灵活的服务，如DHCP，SNMP等。

（2）MIME协议是扩展了的SMTP协议，是基于SMTP的，所以要放在SMTP上面。

（3）由于RIP协议是基于UDP协议而创建的，所以RIP协议应该放在UDP协议的上一层，即应用层。

47现在流行的P2P文件共享应用程序都有哪些特点？存在哪些值得注意的问题？

答：（1）P2P文件共享应用程序的特点如下：

①P2P工作方式下，不需要使用集中式的媒体服务器，解决了集中式媒体服务器可能出现的瓶颈问题，且各节点地位平等，消除了对某个服务器的完全依赖，提高了系统效率和资源利用率；

②P2P的可扩展性好，没有传统服务器上关于带宽的过多限制；

③P2P模式下，单个结点的宕机不会影响整个网络，健壮性良好。

（2）需要注意的问题：

①文件知识产权保护问题；

②P2P流量的有效管理问题；

③占用大量带宽资源的问题；

④指定流量收费标准的问题。

48使用客户-服务器方式进行文件分发。一台服务器把一个长度为F的大文件分发给N个对等方。假设文件传输的瓶颈是各计算机（包括服务器）的上传速率u。试计算文件分发到所有对等方的最短时间。

答：使用客户-服务器模式进行文件分发时，假设服务器不停地发数据，客户机不停地下载数据，则文件分发到所有对等方的最短时间为NF/u。

49重新考虑上题的文件分发任务，但采用P2P文件分发方式，并且每个对等方只能在接收完整个文件后才能向其他对等方转发。试计算文件分发到所有N个对等方的最短时间。

答：采用P2P方式时，文件成功发送到N个对等方所用的最短时间为$[\log_2（N+1）]F/u$。

50再重新考虑上题的文件分发任务，但可以把这个非常大的文件划分为一个个非常小的数据块进行分发，即一个对等方在下载完一个数据块后就能向其他对等方转发，并同时可下载其他数据块。不考虑分块增加的控制信息，试计算整个大文件分发到所有对等方的最短时间。

答：将大文件分成小的数据块再进行分发，这种情况下一个对等方在下载完一个数据块后就能向其他对等方转发，并同时可下载其他数据块，这时将其发送到所有对等方的最短时间为F/u。

6.3　考研真题详解

1下列关于FTP协议的叙述中，错误的是（　　）。[2017年408统考]

A．数据连接在每次数据传输完毕后就关闭

B．控制连接在整个会话期间保持打开状态

C．服务器与客户端的TCP20端口建立数据连接

D．客户端与服务器的TCP21端口建立控制连接

【答案】C

【解析】AB项，FTP协议使用控制连接和数据连接，控制连接存在于整个FTP会话过程中，数据连接在每次文件传输时才建立，传输结束就关闭。CD项，默认情况下FTP协议使用TCP20端口进行数据连接，TCP21端口进行控制连接。但是是否使用TCP20端口建立数据连接与传输模式有关，主动方式使用TCP20端口，被动方式由服务器和客户端自行协商决定，C错，D对。答案选C。

2使用手机中的浏览器访问北京邮电大学主页http://www.bupt.edu.cn过程中，手机中不会用到的协议为（　　）。[北京邮电大学2017研]

A．IP

B．TCP

C．DNS

D．OSPF

【答案】D

【解析】在访问的过程中，首先使用DNS（域名解析）协议将域名解析为IP地址，进行TCP三次握手连接访问。没有用到OSPF协议。答案选D。

3某浏览器发出的HTTP请求报文如下：

GET /index.html HTTP/1.1

Host：www.test.edu.cn

Connection：Close

Cookie：123456

下列叙述中，错误的是（　　）。[2015年408统考]

A．该浏览器请求浏览index.html

B．Index.html存放在www.test.edu.cn上

C．该浏览器请求使用持续连接

D．该浏览器曾经浏览过www.test.edu.cn

【答案】C

【解析】Connection的连接方式：Close表明为非持续连接方式，keep-alive表示持续连接方式。Cookie值是由服务器产生的，HTTP请求报文中有Cookie报头表示曾经访问过www.test.edu.cn服务器。

4若用户1与用户2之间发送和接收电子邮件的过程如图6-10所示，则图中①、②、③阶段分别使用的应用层协议可以是（　　）。[2012年408统考]

图6-10　发送和接收电子邮件的过程

A．SMTP、SMTP、SMTP

B．POP3、SMTP、POP3

C．POP3、SMTP、SMTP

D．SMTP、SMTP、POP3

【答案】D

【解析】电子邮件主要由3部分组成：用户代理、邮件服务器、邮件发送协议和邮件读取协议；

①邮件发送协议SMTP

SMTP是一种采用“推”的方式来进行邮件传输的协议，它的通信主要有以下三个阶段：

a．连接建立：发件人的邮件送到发送方邮件服务器的邮件缓存后，SMTP客户每隔一定时间就对邮件缓存扫描一次，若发现有邮件，就使用SMTP的熟知端口号25与接收方邮件服务器的SMTP服务器建立TCP连接；

b．邮件传送：邮件的传送从MAIL命令开始，MAIL命令后面有发件人的地址；

c．连接释放：邮件发送完毕后，SMTP客户应发送QUIT命令。

②邮件读取协议POP3

邮局协议POP3是一种采用“拉”的方式进行邮件传输的协议，它使用客户/服务器的工作方式，在传输层使用TCP协议，端口号是110。

接收邮件的用户PC机中的用户代理必须运行POP客户程序，而在收件人所连接的ISP邮件服务器中则运行POP服务器程序。POP3协议的一个特点就是只要用户从POP服务器读取了邮件，POP服务器就把该邮件删除。

所以本题中用户1使用SMTP向用户1的邮件服务器发送邮件，用户1的邮件服务器使用SMTP向用户2的邮件服务器发送邮件，用户2使用POP3协议从用户2的邮件服务器中接收邮件。

5如果本地域名服务无缓存，当采用递归方法解析另一网络某主机域名时，用户主机和本地域名服务器发送的域名请求条数分别为（　　）。[2010年408统考]

A．一条、一条

B．一条、多条

C．多条、一条

D．多条、多条

【答案】A

【解析】首先，如果主机所询问的本地域名服务器不知道被查询域名的IP地址，那么本地域名服务器就以DNS客户的身份向其他服务器继续发出查询请求报文，而不是让该主机自己进行下一步的查询，所以主机只需向本地域名服务器发送一条域名请求即可；其次，题目已经说明用递归方法解析另一个网络某主机域名，而递归方法解析一定要查到主机需要的IP地址才返回，所以本地域名服务器只需发送一条域名请求给根域名服务器即可，然后依次递归，最后再依次返回结果。

第7章　网络安全

7.1　复习笔记

一、网络安全问题概述

1计算机网络面临的安全性威胁

计算机网络上的通信面临两大类威胁，即被动攻击和主动攻击。

（1）被动攻击

这是指攻击者从网络上窃听他人的通信内容，通常把这类攻击称为截获。

（2）主动攻击

常见的主动攻击方式：

①篡改；

②恶意程序：计算机病毒、计算机蠕虫、特洛伊木马、逻辑炸弹、后门入侵、流氓软件等；

③拒绝服务。

2计算机网络安全的内容

计算机网络安全设定以下四大目标：

（1）保密性；

（2）端点鉴别；

（3）信息的完整性；

（4）运行的安全性。

3数据加密模型

一般的数据加密模型如图7-1所示。

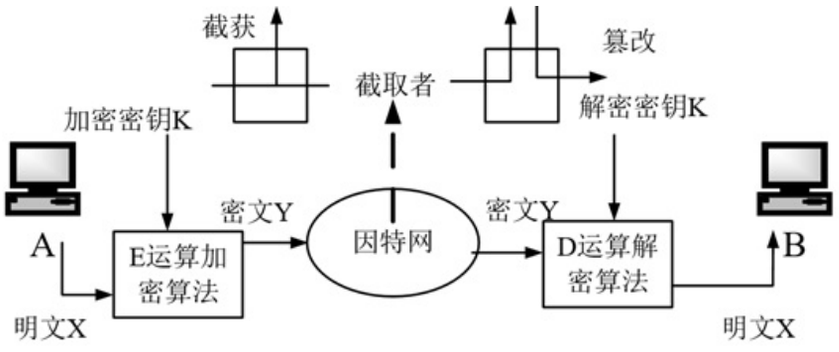

图7-1　一般的数据加密模型

用户A向B发送明文X，但通过加密算法E运算后，就得出密文Y。图中所示的加密和解密用的密钥K（key）是一串秘密的字符串（即比特串）。明文通过加密算法变成密文的一般表示方法：$Y=E_K(X)$。

二、两类密码体制

1对称密钥密码体制

对称密钥密码体制，即加密密钥与解密密钥是相同的密码体制；例如数据加密标准DES属于对称密钥密码体制，且DES的保密性仅取决于对密钥的保密，而算法是公开的。

2公钥密码体制

公钥密码体制使用不同的加密密钥与解密密钥；其中加密密钥P_K是向公众公开的，解密密钥S_K（私钥）则是需要保密的；加密算法E和解密算法D也都是公开的。

【注意】任何加密方法的安全性取决于密钥的长度，以及攻破密文所需的计算量，而不单取决于加密的体制。

三、数字签名

数字签名必须保证能够实现以下三点功能：

1．报文鉴别：接收者能够核实发送者对报文的签名；

2．保证报文的完整性：接收者确信所收到的数据和发送者发送的完全一样而没有被篡改过；

3．不可否认：发送者事后不能抵赖对报文的签名。

四、鉴别

鉴别可分为两种：一种是报文鉴别，另一种是实体鉴别。

1．报文鉴别

（1）密码散列函数

散列函数的两大特点：

①输入长度不固定，可以很长，但输出长度固定，并且很短，其中输出叫做散列值；

②不同的散列值对应不同的输入，但不同的输入却能得到相同的散列值。

（2）实用的密码散列函数MD5和SHA-1

①MD5：可对任意长的报文进行运算，然后得出128位的MD5报文摘要代码；

②安全散列算法SHA：和MD5相似，比MD5更安全，但码长为160位，计算起来比MD5更慢。

2．实体鉴别

实体鉴别和报文鉴别不同；报文鉴别是对每一个收到的报文都要鉴别报文的发送者，而实体鉴别则是在系统接入的全部持续时间内对和自己通信的对方实体只需验证一次。

五、密钥分配

密钥管理包括：密钥的产生、分配、注入、验证和使用，密钥分配应采用网内分配方式，即对密钥自动分配。

1．对称密钥的分配

目前常用的密钥分配方式是设立密钥分配中心KDC；KDC是大家都信任的机构，它给需要进行秘密通信的用户临时分配一个会话密钥。

2．公钥的分配

认证中心CA将公钥与其对应的实体（人或机器）进行绑定，每个实体都有CA发来的证书，里面有公钥及其拥有者的标识信息（人名或IP地址），此证书被CA进行了数字签名。

六、互联网使用的安全协议

1网络层安全协议

（1）IPsec协议族

IPsec协议族是能够在IP层提供互联网通信安全的协议族，IPsec协议族中的协议可划分为以下三个部分：

①IP安全数据报格式的两个协议：鉴别首部AH协议和封装安全有效载荷ESP协议；

②有关加密算法的三个协议；

③互联网密钥交换IKE协议。

（2）IP安全数据报的格式

如图7-2所示为IP安全数据报的格式。

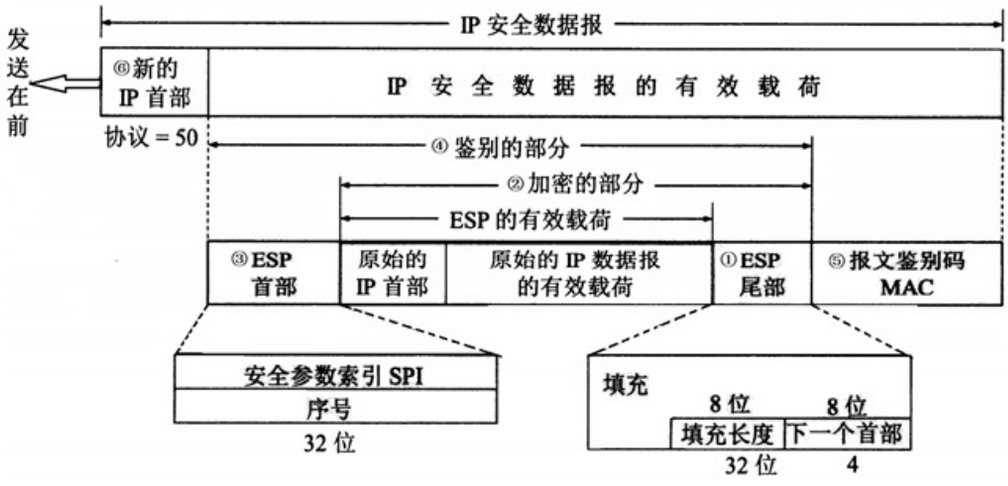

图7-2　IP安全数据报的格式

2运输层安全协议

运输层广泛使用下面两个安全协议：

（1）安全套接层SSL：作用在端系统应用层的HTTP和运输层之间，在TCP之上建立起一个安全通道，为通过TCP传输的应用层数据提供安全保障；

（2）运输层安全TLS：为所有基于TCP的网络应用提供安全数据传输服务。

3应用层安全协议

应用层安全协议很多，例如PGP协议；

PGP协议是一个完整的电子邮件安全软件包，包括加密、鉴别、电子签名和压缩等技术；它提供电子邮件的安全性、发送方鉴别和报文完整性。

七、系统安全：防火墙与入侵检测

1防火墙

防火墙是一种访问控制技术，它严格控制进出网络边界的分组，禁止任何不必要的通信以减少入侵的发生；防火墙也是一种特殊编程的路由器，安装在一个网点和网络的其余部分之间，目的是实施访问控制策略。一般把防火墙里面的网络称为“可信的网络”，外面的网络称为“不可信的网络”。

2入侵检测系统

入侵检测系统IDS是在入侵已经开始，但还没有造成危害或在造成更大危害前，及时检测到入侵，以便尽快阻止入侵，把危害降低到最小；入侵检测方法一般可分为基于特征的入侵检测和基于异常的入侵检测两种。

八、一些未来的发展方向（略）

7.2　课后习题详解

1计算机网络都面临哪几种威胁？主动攻击和被动攻击的区别是什么？对于计算机网络，其安全措施都有哪些？

答：（1）计算机网络上的通信面临两大类威胁，即被动攻击和主动攻击。

①被动攻击

这是指攻击者从网络上窃听他人的通信内容，通常把这类攻击称为截获。

②主动攻击

常见的主动攻击方式：

a．篡改；

b．恶意程序：计算机病毒、计算机蠕虫、特洛伊木马、逻辑炸弹、后门入侵、流氓软件等；

c．拒绝服务。

（2）主动攻击和被动攻击的区别：

主动攻击是指攻击者对某个连接中通过的PDU进行各种处理，如有选择地更改、删除、延迟这些PDU，甚至还可将合成的或伪造的PDU送入到一个连接中去。

被动攻击是攻击者只是观察和分析某一个协议数据单元PDU而不干扰信息流。即使这些数据对攻击者来说是不易理解的，他也可通过观察PDU的协议控制信息部分，了解正在通信的协议实体的地址和身份，研究PDU的长度和传输的频度，以便了解所交换数据的性质。

（3）对于计算机网络的安全措施有以下几种：

①为用户提供安全可靠的保密通信，即把在网络上传送的数据进行加密；

②设计出一种尽可能比较安全的计算机网络；

③对接入网络的权限加以控制，并规定每个用户的接入权限。

2试解释以下名词：

（1）重放攻击；

（2）拒绝服务；

（3）访问控制；

（4）流量分析；

（5）恶意程序。

答：（1）重放攻击：指攻击者对某个连接中通过的PDU进行各种处理，如有选择的更改、删除某些PDU；

（2）拒绝服务：指攻击者向互联网上的服务器不停地发送大量分组，使其无法为客户提供正常服务；

（3）访问控制：也称为存取控制或接入控制，对接入网络的权限加以控制，并规定每个用户的接入权限；

（4）流量分析：通过观察PDU的协议控制信息部分，了解正在通信的协议实体的地址和身份，研究PDU的长度和传输的频度，以便了解所交换的数据的某种性质；

（5）恶意程序：通常是指带有攻击意图的一段程序，例如病毒、特洛伊木马、逻辑炸弹等。

3为什么说计算机网络的安全不仅仅局限于保密性？试举例说明，仅具有保密性的计算机网络不一定是安全的。

答：（1）保密性就是把通信的内容进行加密，使得即使通信的内容被攻击者截获，也无法懂得所截获的内容的含义。但这仅仅是计算机网络上的通信面临的四种威胁之一。

（2）假定某个计算机网络仅具有保密性，那么在这种计算机网络上的通信还会面临其他三种威胁（中断，篡改和伪造）。因此，安全的计算机网络还必须具有安全的网络协议，以及使用可靠的访问控制方法。

4密码编码学、密码分析学和密码学都有哪些区别？

答：密码编码学是密码体制的设计学，而密码分析学则是在未知密钥的情况下从密文推演出明文或密钥的技术。密码编码学与密码分析学合起来即为密码学。

5“无条件安全的密码体制”和“在计算上是安全的密码体制”有什么区别？

答：两者的主要区别是：

（1）无条件安全的密码体制：指无论截获者获得了多少密文，在密文中都没有足够的信息来唯一地确定出对应的明文，则这一密码体制为无条件安全的，这在理论上是不可破的。

（2）在计算上是安全的密码体制：指密码不能在一定时间内被可以使用的计算资源破译，这在计算上（而不是在理论上）是不可破的。

6试破译下面的密文诗。加密采用替代密码。这种密码是把26个字母（从a到z）中的每一个用其他某个字母替代（注意，不是按序替代），密文中无标点符号。空格未加密。

kfd ktbd fzm eubd kfd pzyiom mztx ku kzyg ur bzha kfthcm ur mfudm zhx

mftnm zhx mdzythc pzq ur ezsszcdm zhx gthcm zhx pfa kfd mdz tm sutythc

fuk zhx pfdkfdi ntcm fzld pthcm sok pztk z stk kfd uamkdim eitdx sdruid

pd fzld uoi efzk rui mubd ur om zid uok ur sidzkf zhx zyy ur om zid rzk

hu foiia mztx kfd ezindhkdi kfda kfzhgdx ftb boef rui kfzk

答：the time has come the walrus said to talk of many things of ships and shoes and sealing wax of cabbages and kings and why the sea is boiling hot and whether pigs have wings but wait a bit the oysters cried before we have our chat for some of us are out of breath and all of us are fat no hurry said the carpenter they thanked him much for that

7对称密钥体制与公钥密码体制的特点各如何？各有何优缺点？

答：（1）对称密钥体制：

特点：加密密钥与解密密钥的密码体制是相同的，且收发双方必须共享密钥，对称密钥的密钥是保密的，没有密钥，解密就不可行，知道算法和若干密文不足以确定密钥。

优点：加解密速度快，安全强度高，使用的加密算法比较简便高效，密钥简短，破译极其困难，系统开销小，适合加密大量数据。

缺点：密钥的发送过程十分复杂，花费较高；当用户很多、分布很广时，密钥的分配存储就成了大问题；通信双方必须统一密钥，才能发送保密信息。

（2）公钥密码体制：

特点：加密密钥和解密密钥是不同的，且加密密钥是向公众公开的，而解密密钥是需要保密的，发送方拥有加密或者解密密钥，而接收方拥有另一个密钥。两个密钥之一也是保密的，无解密密钥，解密不可行，知道算法和其中一个密钥以及若干密文不能确定另一个密钥。

优点：密钥少，好管理，分配简单；不需要用密钥通道和复杂的协议来传送密钥；可实现数字签名和数字鉴别。

缺点：加密速度慢，开销较大。

8为什么密钥分配是一个非常重要但又十分复杂的问题？试举出一种密钥分配的方法。

答：（1）密钥分配是指如何将密钥分配给用户，密钥必须通过最安全的通路进行分配，若分配出现差错将造成泄漏等安全问题，显然是十分重要的；对称密钥加密术需要双方之间有一个共享密钥，如果有100万个人要互相通信，那么每个人都要掌握大约100万个不同的密钥，总共大约需要10亿个密钥，显然这是十分复杂的，所以一般我们需要使用恰当的密钥分配方法。

（2）以利用一个可信的第三方（密钥分配中心KDC）为例：

KDC是大家都信任的机构，其任务就是给需要进行秘密通信的用户临时分配一个会话密钥，假定用户A和B都是KDC的登记用户。A和B在KDC登记时，就已经在KDC的服务器上安装了各自和KDC进行通信的主密钥K_A和K_B。密钥分配分为三个步骤：

①用户A向密钥分配中心KDC发送明文，说明想和用户B通信。在明文中给出A和B在KDC登记的身份。

②KDC用随机数产生“一次一密”的会话密钥K_{AB}，供A和B的这次会话使用，然后向A发送回答报文。这个回答报文用A的密钥K_A加密。这个报文中包含有这次会话使用的密钥K_{AB}和请A转给B的一个票据，它包含A和B在KDC登记的身份，以及这次会话将要使用的密钥K_{AB}。这个票据由KDC用B的密钥K_B加密，因此A无法知道此票据的内容，因为A没有B的密钥K_B。当然A也不需要知道此票据的内容。

③当B收到A转来的票据并使用自己的密钥K_B解密后，就知道A要和他通信，同时也知道KDC为这次和A通信所分配的会话密钥K_{AB}。

此后，A和B就可使用会话密钥K_{AB}进行这次通信了。

9公钥密码体制下的加密和解密过程是怎样的？为什么公钥可以公开，如果不公开是否可以提高安全性？

答：（1）公钥密码体制的加密和解密过程如下：

假设发送者为A，接收者为B，B的加密密钥和解密密钥分别是PK_B和SK_B。

加密过程：发送者A用B的公钥PK_B通过E运算对明文X加密，得出密文

$$E = E_{PK_B}(X)$$

解密过程：接收者B用自己的私钥SK_B通过D运算进行解密，恢复出明文

$$D_{SK_B}(Y) = D_{SK_B}(E_{PK_B}(X)) = X$$

（2）因为公钥是用来对明文加密的而不是解密的，私钥是用来解密的，所以任何人都可以获得公钥，公钥是否公开对安全性没有影响。

10试述数字签名的原理。

答：数字签名的原理：

（1）被发送文件采用哈希算法对原始报文进行运算，得到一个固定长度的数字串，作为报文摘要，不同的报文得到的报文摘要各异，但是对相同的报文它的报文摘要却是唯一的；

（2）发送方生成报文的报文摘要，用自己的私钥对摘要进行加密形成发送方的数字签名；

（3）这个数字签名将作为报文的附件和报文一起发送给接收方；

（4）接收方首先从接收到的原始报文中用同样的算法计算出新的报文摘要，再用发送方的公钥对报文附件的数字签名进行解密，比较两个报文摘要，如果值相同，接收方就能确认该数字签名是发送方的。

11为什么需要进行报文鉴别？鉴别和保密、授权有什么不同？报文鉴别和实体鉴别有什么区别？

答：（1）使用报文鉴别是为了对付主动攻击中的篡改和伪造；

（2）鉴别是要验证通信的对方的确是自己所要通信的对象，而不是其他的冒充者；保密是指网络信息不被泄露给非授权的用户、实体或过程，即信息只为授权用户使用；授权涉及到的问题是所进行的过程是否被允许（如是否可以对某文件进行读或写）；

（3）报文鉴别是对每一个收到的报文都要鉴别报文的发送者，而实体鉴别是在系统接入的全部持续时间内对和自己通信的对方实体只需要验证一次，实体可以是一个人，也可以是一个进程（客户或服务器）。

12试分别举例说明以下情况：

（1）既需要保密，也需要鉴别；

（2）需要保密，但不需要鉴别；

（3）不需要保密，但需要鉴别。

答：（1）例如作战指挥下达命令时，既需要保密，也需要鉴别；

（2）在银行进行个人存款，需要保密，但不需要鉴别；

（3）在互联网上传送非保密文件，且该文件需要鉴别是否完整或是否被篡改。

13A和B共同持有一个只有他们二人知道的密钥（使用对称密码）。A收到了用这个密钥加密的一份报文。A能否出示此报文给第三方，使B不能否认发送了此报文？

答：不行；对称密钥密码体制，即加密密钥与解密密钥是相同的密码体制；例如数据加密标准DES属于对称密钥密码体制，且DES的保密性仅取决于对密钥的保密，而算法是公开的。该题中若A将密码出示给了第三方，那么A将无法证明B是该报文的唯一发送方。

14图7-3所示的具有保密性的签名与使用报文鉴别码相比较，哪一种方法更有利于进行鉴别？

图7-3　14题图

答：若要传送很长的报文，使用具有保密性的签名将花费很长时间进行D运算与E运算，效率很低，但若使用报文鉴别码则会高效很多。

15试述实现报文鉴别和实体鉴别的方法。

答：（1）报文鉴别

报文摘要MD是进行报文鉴别的简单方法，如图7-4所示，A把较长的报文X经过报文摘要算法运算后得出很短的报文摘要H。然后用自己的私钥对H进行D运算，即进行数字签名。得出已签名的报文摘要D（H）后，并将其追加在报文X后面发送给B。B收到报文后首先把已签名的D（H）和报文X分离。然后进行下面操作：

①用A的公钥对D（H）进行E运算，得出报文摘要H；

②对报文X进行报文摘要运算，看是否能够得出同样的报文摘要H。

若能得到一样的H，就能以极高的概率断定收到的报文是A产生的，否则就不是。

图7-4　用报文摘要鉴别报文

（2）实体鉴别

实体鉴别是在系统接入的全部持续时间内，对和自己通信的对方实体只验证一次，例如：

A向远端的B发送自己身份的报文A和口令的报文，并使用双方约定好的共享对称密钥K_{AB}进行加密，B在收到此报文后，使用共享对称密钥K_{AB}进行解密，从而鉴别A的身份。

16结合图7-5计算UDP的检验和的例子，说明这种检验和不能用来鉴别报文。

图7-5　16题图

答：用这种方法进行报文鉴别是不行的，因为采用UDP校验和的方式，很容易发生UDP中数据已更改，但检验和却不变的情况；这样来鉴别报文无法判定是否为一个伪造的报文。

17报文的保密性与完整性有何区别？什么是MD5？

答：（1）报文的保密性和完整性的区别：

①保密性是对未授权的访问进行掩蔽，即未授权的人不会知道其报文的内容，甚至让未授权的人不知道有这样一个报文的存在；

②完整性是不让未授权的人修改报文的内容。

（2）MD5是一种报文摘要算法，它可以对任意长的报文进行运算，然后得出128bit的MD5报文摘要代码。算法的大致过程如下：

①先将任意长的报文按模2^{64}计算其余数（64bit），追加在报文的后面。

②在报文和余数之间填充1～512bit，使得填充后的总长度是512的整数倍。填充的首位是1，后面都是0。

③将追加和填充后的报文分割为一个个512bit的数据块，每512bit的报文数据再分成4个128bit的数据块并依次送到不同的散列函数进行4轮计算。每一轮又都按32bit的小数据块进行复杂的运算，直到计算出MD5报文摘要代码（128bit）。

18什么是重放攻击？怎样防止重放攻击？

答：（1）重放攻击：入侵者C从网络上截获A发给B的报文，且C将这个加密报文直接发送给B，使B误认为C就是A，然后B就向C发送许多本来应当发送给A的报文；

（2）为了防止重放攻击，可以使用不重数。不重数就是一个不重复使用的大随机数，即“一次一数”。在鉴别过程中不重数可以使B能够把重复的鉴别请求和新的鉴别请求区分开。

19图7-6的鉴别过程也有可能被骗子利用。假定A发送报文和B联系，但不巧被骗子P截获了，于是P发送报文给A：“我是B”。接着，A就发送图7-6中的第一个报文“A，R_A”，这里R_A是不重数。本来，P必须也发给A另一个不重数，以及发回使用两人共同拥有的密钥K_{AB}加密的R_A，即K_{AB}（R_A）。但P根本不知道K_{AB}，只好就发送同样的R_A作为自己的不重数。A收到R_A后，发给P报文“K_{AB}（R_A）”，P仍然不知道密钥K_{AB}，也照样发回报文“K_{AB}（R_A）”。接着A就把一些报文发送给P了。虽然P不知道密钥K_{AB}，但可以慢慢设法攻破。试问A能否避免这样的错误？

图7-6　19题图

答：可以避免；若A和B对不同的会话使用不同的不重数集，此时P发回同样的R_A作为自己的不重数，A很容易判断出这不是自己人发来的报文。

20什么是“中间人攻击”？怎样防止这种攻击？

答：（1）中间人攻击（简称“MITM攻击”）：是一种“间接”的入侵攻击，通过各种技术手段将受入侵者控制的一台计算机（中间人）虚拟放置在网络连接中的两台通信计算机之间，入侵者把这台计算机模拟成一台或两台原始计算机，使“中间人”能够与原始计算机建立活动连接并允许其读取或篡改传递的信息，此时两个原始计算机用户却认为他们是在互相通信；

（2）防范手段：

①将一些机密信息进行加密后再传输，这样即使被“中间人”截取也难以破解；

②使用认证方式检测MITM的攻击。

21试讨论Kerberos协议的优缺点。

答：（1）Kerberos协议的优点：

①安全性高；

②透明性高；

③可扩展性好。

（2）Kerberos协议的缺点：

①身份鉴别采用对称加密机制，加密和解密时的密钥相同，交换密钥时的安全性不高；

②Kerberos服务器与用户共享的密钥是用户的口令字，服务器在响应时不验证用户的真实性，而是直接认为它是合法用户，若攻击者截获了响应报文，很容易实现密码攻击；

③AS和TGS是集中式管理，容易形成瓶颈，系统的性能和安全也严重依赖于AS和TGS的性能和安全；

④随用户数增加，密钥管理较复杂。

22互联网的网络层安全协议族IPsec都包含哪些主要协议？

答：在IPsec中最主要的两个协议就是鉴别首部AH协议和封装安全有效载荷ESP协议。其中AH提供源点鉴别和数据完整性，但它不能保密；而ESP比AH更复杂，它还提供保密性。

23用户A和B使用IPsec进行通信。A需要向B接连发送6个分组。是否需要在每发送一个分组之前，都先建立一次安全关联SA？

答：不需要；当建立起一次安全关联SA后，接下来发送的6个分组都使用建立的这一个安全关联。

24在图7-7中，公司总部和业务员之间先建立了TCP连接，然后使用IPsec进行通信。假定有一个TCP报文段丢失了。后来在重传该序号的报文段时，相应的IPsec安全数据报是否也要使用同样的IPsee序号呢？

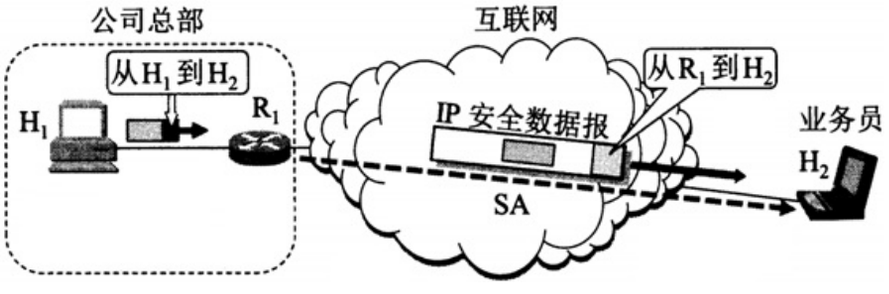

图7-7　24题图

答：不需要；IPsec每发送一个IPsec数据报都需要使用一个新的序号，且该序号是上一次使用的序号加1。

25试简述SSL的工作过程。

答：现举例说明SSL的工作过程，假定A有一个使用SSL的安全网页，B上网时用鼠标点击到这个安全网页的链接。接着，服务器和浏览器就进行握手协议，其主要过程如下：

（1）浏览器向服务器发送浏览器的SSL版本号和密码编码的参数选择。

（2）服务器向浏览器发送服务器的SSL版本号、密码编码的参数选择及服务器的证书。

（3）浏览器有一个可信的CA表，表中有每一个CA的公钥。当浏览器收到服务器发来的证书时，就检查此证书是否在自己的可

信的CA表中。若不在，则后面的加密和鉴别连接就不能进行下去；若在，浏览器就使用CA的公开密钥对证书解密，这样就得到了服务器的公开密钥。

（4）浏览器随机地产生一个对称会话密钥，并用服务器的公钥加密，然后将加密的会话密钥发送给服务器。

（5）浏览器向服务器发送一个报文，说明以后浏览器将使用此会话密钥进行加密。然后浏览器再向服务器发送一个单独的加密报文，表明浏览器端的握手过程已经完成。

（6）服务器也向浏览器发送一个报文，说明以后服务器将使用此会话密钥进行加密。然后服务器再向浏览器发送一个单独的加密报文，表明服务器端的握手过程已经完成。

（7）SSL的握手过程至此已经完成，下面就可开始SSL的会话过程。

26在图7-8中，假定在第一步，顾客发送报文给经销商时，误将报文发送到一个骗子处，而骗子就接着冒充经销商继续下面的步骤。试问在报文交互到第几个步骤时，顾客可以发现对方并不是真正的经销商？

图7-8　26题图

答：顾客在第④步用CA发布的公钥鉴别B的证书时，即可发现B是骗子。

27电子邮件的安全协议PGP主要都包含哪些措施？

答：PGP是一个完整的电子邮件安全软件包，包括加密、鉴别、电子签名和压缩等技术，它只是将现有的加密算法综合在一起而已；电子邮件的安全协议PGP主要包括鉴别、电子签名、加密、压缩和密钥管理等措施，且密钥管理是PGP系统的一个关键。

28试述防火墙的工作原理和所提供的功能。什么叫做网络级防火墙和应用级防火墙？

答：（1）防火墙是一种特殊编程的路由器，安装在一个网点和网络的其余部分之间，目的是实施访问控制策略。防火墙的工作原理：防火墙中的分组过滤路由器检查进出被保护网络的分组数据，按照系统管理员事先设置好的防火墙规则来与分组进行匹配，符合条件的分组就能通过，否则就丢弃。

（2）防火墙提供的功能有两个：

①阻止：阻止某种类型的流量通过防火墙；

②允许：允许某种类型的流量通过防火墙。

（3）网络级防火墙：主要是用来防止整个网络出现外来非法的入侵，属于这类的有分组过滤和授权服务器。前者检查所有流入本网络的信息，然后拒绝不符合事先制定好的一套准则的数据，而后者则是检查用户的登录是否合法。

（4）应用级防火墙：从应用程序来进行访问控制。通常使用应用网关或代理服务器来区分各种应用。

7.3 考研真题解

本章内容不是考试重点，所以基本上没有学校的考研试题涉及到本章内容。因此，读者可以简单了解，不必作为复习重点，本部分也就没有选用考研真题。

第8章　互联网上的音频/视频服务

8.1　复习笔记

一、概述

1多媒体信息的特点

多媒体信息（包括声音和图像信息）最主要的两个特点如下：

（1）多媒体信息的信息量往往很大；

（2）在传输多媒体数据时，对时延和时延抖动均有较高的要求。

2音频/视频服务的分类

目前互联网提供的音频/视频服务大体上可分为三种类型：

（1）流式存储音频/视频：能边下载边播放；

（2）流式实况音频/视频：发送方边录制音频/视频节目边发送，接收时也能够连续播放；

（3）交互式音频/视频：用户使用互联网和其他人进行实时交互式通信。

二、流式存储音频/视频

1具有元文件的万维网服务器

在万维网服务器中，除了真正的音频/视频文件外，还增加一个元文件以提高流式存储音频/视频的下载效率。

2媒体服务器

为了更好地提供播放流式音频/视频文件的服务，可以使用两个分开的服务器，即一个普通的万维网服务器和一个媒体播放器。

媒体服务器又称流式服务器，媒体服务器与普通的万维网服务器的最大区别就是：媒体服务器是专门为播放流式音频/视频文件而设计的。

3实时流式协议RTSP

实时流式协议RTSP又称为带外协议，它以客户/服务器方式工作，其本身并不传送数据，而仅仅是使媒体播放器能够控制多媒体流的传送。

图8-1表示使用RTSP的媒体服务器的工作过程。

图8-1　使用RTSP的媒体服务器的工作过程

三、交互式音频/视频

1IP电话概述

（1）IP电话的定义

狭义的IP电话就是指在IP网络上打电话，广义的IP电话则不仅仅是电话通信，而且还可以是IP网络上进行的交互式多媒体实时通信（包括话音、视像等），甚至还包括即时传信IM。

（2）IP电话网关

IP电话网关是公用电话网与IP网络的接口设备，它的作用是：

①在电话呼叫阶段和呼叫释放阶段进行电话信令的转换；

②在通话期间进行话音编码的转换。

（3）IP电话的通话质量

IP电话的通话质量主要由通话双方端到端的时延和时延抖动、话音分组的丢失率决定。

2IP电话所需要的几种应用协议

在IP电话的通信中，至少需要两种应用协议：

（1）信令协议：使我们在互联网上能找到被叫用户；

（2）话音分组的传送协议：使用于电话通信的话音数据能够以时延敏感属性在互联网中传送。

3实时运输协议RTP

实时运输协议RTP为实时应用提供端到端的的运输，但不提供任何服务质量的保证。

4实时运输控制协议RTCP

实时运输控制协议RTCP的主要功能是：服务质量的监视与反馈、媒体间的同步（如某一个RTP发送的声音和图像的配合），以及多播组中成员的标志。

5H.323

H.323是互联网的端系统之间进行实时声音和视频会议的标准；它不是一个单独的协议而是一组协议。

6会话发起协议SIP

由于H.323太过复杂而不便于发展基于IP的新业务，所以需要一套简单的标准；会话发起协议SIP也就成为了互联网的建议标准；SIP使用文本方式的客户/服务器协议，包含两种构件（用户代理和网络服务器）。

四、改进“尽最大努力交付”的服务

1使互联网提供服务质量

服务质量QoS是服务性能的总效果，它决定了一个用户对服务的满意程度；互联网应当设法增加一些机制（分组的分类、管制、调度以及呼叫接纳）来提供一定的服务质量。

2调度和管制机制

（1）调度机制

“调度”就是指排队的规则，常见有以下几种策略：

①先进先出FIFO；

②简单地按优先级排队；

③公平排队；

④加权公平排队WFQ。

（2）管制机制

对一个数据流，可根据以下三个方面进行管制：

①平均速率：一定时间间隔内通过的分组数；

②峰值速率：峰值速率限制了数据流在非常短的时间间隔内的流量；

③突发长度：非常短的时间间隔内连续注入到网络中的分组数。

3综合服务IntServ与资源预留协议RSVP

（1）综合服务IntServ

IntServ可对单个的应用会话提供服务质量的保证，它定义了两类服务：

①有保证的服务：保证一个分组在通过路由器时的排队时延有一个严格的上限；

②负载受控的服务：可以使应用程序得到比通常的“尽最大努力”更加可靠的服务。

IntServ共有以下四个组成部分：

①资源预留协议RSVP：它是IntServ的信令协议；

②接纳控制：决定是否同意对某一资源的请求；

③分类器：把进入路由器的分组进行分类，并根据分类的结果把不同类别的分组放入特定的队列；

④调度器：根据服务质量要求决定分组发送的前后顺序。

（2）资源预留协议RSVP

一个会话声明它所需的服务质量后，路由器能够确认是否有足够的资源来满足该会话的要求；而RSVP协议使得应用能将自己的QoS要求通过信令通知给网络，网络可以对此应用预留相应的资源，它在进行资源预留时采用了多播树的方式。

4区分服务DiffServ

由于综合服务IntServ和资源预留协议RSVP较为复杂，很难在大规模的网络中实现，为此提出区分服务的策略，区分服务DiffServ的要点如下：

（1）DiffServ力图不改变网络的基础结构，但在路由器中增加区分服务的功能；

（2）网络被划分为许多个DS域；

（3）边界路由器中的功能较多，可分为分类器和通信量调节器两大部分；

（4）DiffServ提供了一种聚合功能。

8.2　课后习题详解

1音频/视频数据和普通的文件数据都有哪些主要的区别？这些区别对音频/视频数据在互联网上传送所用的协议有哪些影响？既然现有的电信网能够传送音频/视频数据，并且能够保证质量，为什么还要用互联网来传送音频/视频数据呢？

答：（1）音频/视频数据和普通的文件数据的区别：

①多音频/视频数据信息的信息量往往很大；

②在传输音频/视频数据时，对时延和时延抖动均有较高的要求。

（2）这些区别导致了新的流式存储音频/视频和流式实况音频/视频等传送方式的出现。

（3）用互联网来传送音频/视频数据的原因：

①方便、灵活；

②向电信公司租用电话线路的价格太高，而互联网传输信息却很廉价。

2端到端时延与时延抖动有什么区别？产生时延抖动的原因是什么？为什么说在传送音频/视频数据时对时延和时延抖动都有较高的要求？

答：（1）端到端时延与时延抖动的区别：

端到端的时延是指信号按照固定长度打包经IP分组送入网络中进行传送，在发送端和接收端的时间差；而时延抖动是指时延的变化。

（2）产生时延抖动的原因：

在使用IP协议的互联网中，每个分组是独立地传送，因而这些分组到达接收端是非等时的，即每个分组的时延不同，因此产生了时延抖动。

（3）在传送音频/视频数据时对时延和时延抖动都有较高的要求的原因：

多媒体数据往往是实时数据。若时延非常小时，传送的实时音频/视频数据可以认为是实时的，但若时延太大，显然不是实时的了，且时延抖动会使重放失真增大，因此在传送音频/视频数据时对时延和时延抖动都有较高的要求，从而减少它们带来的影响。

3目前有哪几种方案改造互联网，使互联网能够适合于传送音频/视频数据？

答：为了使互联网能够适合于传送音频/视频数据，目前常采用的几种方案：

（1）大量使用光缆，使用具有大量高速缓存的高速路由器传送实时数据；

（2）将互联网改造为能够对端到端的带宽实现预留，从而根本改变因特网的协议栈——从无连接的网络变为面向连接的网络；

（3）付出较小的代价部分改动互联网的协议栈。

4实时数据和等时的数据是一样的意思吗？为什么说互联网是不等时的？实时数据都有哪些特点？试说明播放时延的作用。

答：（1）实时数据和等时数据不一样。实时数据是指在发送实时数据的同时，接收端边接收边播放。而等时数据是指发送时的时间间隔是恒定的。实时数据往往是等时数据，但等时的数据不一定是实时数据。

（2）传统的互联网是不等时的，因为在使用IP协议的互联网中，每一个分组是独立地选择路由和传送，因而这些分组在接收端变成为了不等时的。

（3）实时数据的特点：等时、连续、对时延和时延抖动有较高要求。

（4）播放时延的作用：由于分组以非恒定速率达到，因此早到达的分组在缓存中停留的时间较长，而晚到达的分组在缓存中停留的时间较短。从缓存中取出分组是按照固定的时钟节拍进行的，因此到达的非等时分组，就变为了等时的分组，这在很大程度上消除了时延的抖动。

5流式存储音频/视频、流式实况音频/视频和交互式音频/视频都有何区别？

答：（1）流式存储音频/视频：能边下载边播放；

（2）流式实况音频/视频：发送方边录制音频/视频节目边发送，接收时也能够连续播放；

（3）交互式音频/视频：用户使用互联网和其他人进行实时交互式通信。

6媒体播放器和媒体服务器的功能是什么？请用例子说明。媒体服务器为什么又称为流式服务器？

答：（1）媒体播放器是一个单独的用来播放音频/视频节目的程序，主要功能有播放音频/视频节目，管理用户界面、解压缩、消除时延抖动和处理传输带来的差错；例如Windows Media Player便是典型的媒体播放器。

（2）媒体服务器的功能：使用元文件的URL接入到媒体服务器，请求下载浏览器所请求的音频/视频文件，给出响应并把该音频/视频文件发送给媒体播放器。

（3）媒体服务器也称为流式服务器是因为它与万维网服务器不同，支持流式音频和视频的传送。例如在线看电影，影像文件不必下载到本地硬盘，也不必等到影像文件全部准备完毕，在等待几分钟或几秒钟后就可以观看电影。

7实时流式协议RTSP的功能是什么？为什么说它是个带外协议？

答：（1）实时流式协议RTSP是为了给流式过程增加更多的功能而设计的协议，它以客户/服务器方式工作，是一个应用层的多媒体播放控制协议，用来使用户在播放从互联网下载的实时数据时能够进行控制；

（2）RTSP本身并不传送数据，而仅仅是使媒体播放器能够控制多媒体流的传送，因此又称为带外协议。

8狭义的IP电话和广义的IP电话都有哪些区别？IP电话都有哪几种连接方式？

答：（1）狭义的IP电话就是指在IP网络上打电话；广义的IP电话则不仅仅是电话通信，而且还可以是IP网络上进行的交互式多媒体实时通信（包括话音、视像等），甚至还包括即时传信IM。

（2）IP电话的连接方式：

①两个PC机用户之间的通话；

②PC机到固定电话之间的通话；

③两个固定电话之间打IP电话。

9IP电话的通话质量与哪些因素有关？影响IP电话话音质量的主要因素有哪些？为什么IP电话的通话质量是不确定的？

答：（1）影响IP电话通话质量的因素：

①通话双方端到端的时延和时延抖动；

②话音分组的丢失率。

（2）影响IP电话话音质量的因素：语音编解码技术、分组丢失率、接收端缓存空间和播放时延的大小、路由器的转发分组速率等。

（3）IP电话的通话质量是不确定的，是因为影响IP电话通话质量的两个因素是不确定的，它主要取决于当时网络的通信量。若网络上的通信量非常大以致发生了网络拥塞，那么端到端时延和时延抖动以及分组丢失率都会很高，这就导致IP电话的通话质量下降。

10为什么RTP协议同时具有运输层和应用层的特点？

答：从开发者的角度看，RTP应当是应用层的一部分。在应用程序的发送端，开发者必须编写用RTP封装分组的程序代码，然后把RTP分组交给UDP套接字接口。在接收端，RTP分组通过UDP套接字接口进入应用层后，还要利用开发者编写的程序代码从RTP分组中把应用数据块提取出来。

RTP封装了多媒体应用的数据块，并且由于RTP向多媒体应用程序提供了服务（如时间戳和序号），可以将RTP看成是在UDP之上的一个运输层子层协议。

11RTP协议能否提供应用分组的可靠传输？请说明理由。

答：RTP协议不能提供应用分组的可靠传输；因为RTP是用UDP来传送的，UDP不能保证可靠传输，另外，RTP本身也不提供确保可靠传输的机制。

12在RTP分组的首部中为什么要使用序号、时间戳和标记？

答：（1）一次RTP会话开始时的初始序号是随机选择的，序号使接收端能够发现丢失的分组，同时也能将失序的RTP分组重新按序排好。

（2）时间戳反映了RTP分组中的数据的第一个字节的采样时刻，在一次会话开始时，时间戳的初始值也是随机选择的，即使是在没有信号发送时，时间戳的数值也要随时间而不断地增加。接收端使用时间戳可准确知道应当在什么时间还原哪一个数据块，从而消除时延的抖动。时间戳还可用来使视频应用中的声音和图像同步。

（3）标记M置1时表示这个RTP分组具有特殊意义。例如，在传送视频流时用来表示每一帧的开始。

13RTCP协议使用在什么场合？RTCP使用的五种分组各有何主要特点？

答：（1）RTCP协议主要应用在服务质量的监视和反馈、媒体间的同步，以及多播组中成员的标志等。

（2）RTCP的五种分组如下：

①结束分组BYE表示关闭一个数据流；

②特定应用分组APP使应用程序能够定义新的分组类型；

③接收端报告分组RR用来使接收端周期性地向所有的点用多播方式进行报告；

④发送端报告分组SR用来使发送端周期性地向所有接收端用多播方式进行报告；

⑤源点描述分组SDES给出会话中参加者的描述。

14IP电话的两个主要信令标准各有何特点？

答：IP电话的两个标准：ITU-T定义的H.323协议和IETF提出的会话发起协议SIP。

（1）H.323协议的特点：H.323是互联网的端系统之间进行实时声音和视像会议的标准；它以已有的电路交换电话网为基础，增加了IP电话的功能；它的信令沿用原有电话网的信令模式，与原有电话网的连接比较容易。H.323标准指明了四种构件，使用这些构件连网就可以进行点对点或一点对多点的多媒体通信。

（2）SIP协议的特点：由于H.323太过复杂而不便于发展基于IP的新业务，所以需要一套简单的标准；会话发起协议SIP也就成为了互联网的建议标准；SIP使用文本方式的客户/服务器协议，包含两种构件（用户代理和网络服务器）。SIP使用了HTTP的许多首部、编码规则、差错码以及一些鉴别机制，它比H.323具有更好的可扩缩性。SIP的地址十分灵活，它可以是电话号码，也可以是电子邮件地址、IP地址或其他类型的地址。

15携带实时音频信号的固定长度分组序列发送到因特网，每隔10ms发送一个分组。前10个分组通过网络的时延分别是45ms，50ms，53ms，46ms，30ms，40ms，46ms，49ms，55ms和51ms。

（1）用图表示出这些分组发出时间和到达时间。

（2）若在接收端还原时的端到端时延为75ms，试求出每一个分组在接收端缓存中应增加的时延。

（3）画出接收端缓存中的分组数与时间的关系。

答：（1）如图8-2所示，上面横线表示分组发出的时间，下面横线表示分组到达的时间，横坐标的单位是毫秒。

图8-2　分组的发出时间和到达时间

（2）各分组经受的时延情况如表8-1所示，表中单位均为毫秒（ms）。

表8-1　各分组经受的不同时延

分组编号	0	1	2	3	4	5	6	7	8	9
分组发送时间	0	10	20	30	40	50	60	70	80	90
分组经受的时延	45	50	53	46	30	40	46	49	55	51
分组到达时间	45	60	73	76	70	90	106	119	135	141
经过 75ms 开始重放，分组的重放时间	75	85	95	105	115	125	135	145	155	165
分组在接收端缓存中增加的时延	30	25	22	29	45	35	29	26	20	24

分组是等时发送的，如表中第2行所示；第3行是分组在互联网中实际经受的时延；第4行是分组到达的时间；若分组在接收端重放的开始时间选择在第1个分组发送后的75ms之后，即在第1个分组到达接收端30ms后，那么各分组在接收端应当重放的时间便如第5行所示；最后求得每一个分组在接收端缓存中应增加的时延分别为30，25，22，29，45，35，29，26，20，24。

（3）接收端缓存中的分组数与时间的关系如图8-3所示。

图8-3　缓存中分组数和时间的对应关系

16话音信号的采样速率为8000Hz，每隔10ms将已编码的话音采样装配成话音分组。每一个话音分组在发送之前要加上一个时间戳。假定时间戳是从一个时钟得到的，该时钟每隔Δ秒将计数器加1。试问能否将Δ取为9ms？如果行，请说明理由；如果不行，你认为Δ应取为多少？

答：不能将Δ取为9ms；Δ应小于话音分组长度10ms。如果将Δ取为9ms，则有：

时钟时间（ms）	0	9	18	27	36	45	54	63	72	81	90	99	108	…
计数器值（ms）	0	1	2	3	4	5	6	7	8	9	10	11	12	…

话音分组每隔10ms产生一个，对应的时间戳值（即计数器值）为：

语音分组产生时间(ms)	0	10	20	30	40	50	60	70	80	90	100	110	…
应加上的时间戳值	0	1	2	3	4	5	6	7	8	10	11	12	…

可以看到时间戳值在8到10之间缺了一个。可见将Δ取为略小于话音分组长度10ms是不行的。正确的做法是使2Δ或3Δ等于话音分组长度。当话音分组丢失时，时间戳值会相差4Δ或5Δ，由此来判定是否发生了分组丢失，例如可以将Δ取为5ms。

17在传送音频/视频数据时，接收端的缓存空间的上限由什么因素决定？实时数据流的数据率和时延抖动对缓存空间上限的确定有何影响？

答：接收端的缓存空间的上限取决于还原播放时所容许的时延，当还原播放时所容许的时延已确定时，缓存空间的上限与实时数据流的数据率成正比。时延抖动越大，缓存空间也应更大。

18什么是服务质量QoS？为什么说“互联网根本没有服务质量可言”？

答：（1）服务质量QoS是服务性能的总效果，此效果决定了一个用户对服务的满意程度。

（2）互联网的网络本身提供的服务是不可靠的，它只能提供“尽最大努力交付”的服务，所以根本没有服务质量可言。

19在讨论服务质量时，管制、调度、呼叫接纳各表示什么意思？

答：（1）管制：路由器对某个数据流的通信量大小进行监视和管理，使该数据流不影响其他正常数据流在网络中通过；

（2）调度：路由器明确地给不同的数据流分配固定的传输带宽，使得不同的数据流都能够得到相应的服务质量保证；

（3）呼叫接纳：数据流要预先声明它所需的服务质量，然后或者被准许进入网络，或者被拒绝进入网络。

20试比较先进先出（FIFO）排队、公平排队（FQ）和加权公平排队（WFQ）的优缺点。

答：（1）先进先出（FIFO）排队

优点：实施简单；

缺点：不能区分时间敏感分组和一般数据分组，对排在长分组后面的短分组不公平。

（2）公平排队（FQ）

优点：对每种类别的分组流设置一个队列，然后轮流使每一个队列只能一次发送一个分组，对于空队列直接跳过，这样较为公平；

缺点：长分组得到的服务时间长，而短分组得到的服务时间短，并且没有区分分组的优先级。

（3）加权公平排队（WFQ）

优点：在队列中增加“权重”，使高优先级队列中的分组有更多的机会得到服务；

缺点：实施起来很复杂。

21假定有一个支持三种类别的缓存运行加权公平队列WFQ的调度策略，并假定这三种类别的权重分别是0.5，0.25和0.25。如果是采用循环调度，那么这三个类别接受服务的顺序是123123123…

（1）如果每种类别在缓存中都有大量的分组，试问这三种类别的分组可能以何种顺序接受服务？

（2）如果第1类和第3类在缓存中有大量的分组，但缓存中没有第2类的分组，试问这两类分组可能以何种顺序接受服务？

答：（1）由于三个类别接受服务的顺序是123123123…，根据权重的不同，第一个类别接受服务的时间占总时间的1/2，第二个和第三个类别接受服务的时间各占总时间的1/4；

则接受服务的顺序可能是121312131213…，还可能是1123112311231123…。

（2）缓存中没有第二类的分组，就跳过去，接受服务的顺序是113113113113…；此时第一和第三个类别接受服务的时间占比分别为2/3和1/3，都大于相应的权值。

22漏桶管制器的工作原理是怎样的，数据流的平均速率、峰值速率和突发长度各表示什么意思？

答：（1）如图8-4所示，漏桶管制器的工作原理：漏桶管制器简称漏桶，它是一种抽象的机制。在漏桶中可装许多权标，但最多装入b个权标，只要漏桶中的权标数小于b个，新的权标就以每秒r个权标的恒定速率加入到漏桶中。但若漏桶已装了b个权标，则新的权标就不再装入，而漏桶的权标数达到最大值b。

图8-4　漏桶管制器的工作原理

（2）数据流的平均速率：指在一定的时间间隔内通过的分组数；

数据流的峰值速率：峰值速率限制了数据流在非常短的时间间隔内的流量；

数据流的突发长度：非常短的时间间隔内连续注入到网络中的分组数。

23采用漏桶机制可以控制达到某一数值的、进入网络的数据率的持续时间。设漏桶最多可容纳b个权标（token）。当漏桶中的权标数小于b个时，新的权标就以每秒r个权标的恒定速率加入到漏桶中。设分组到达速率为N pkt/s（pkt代表分组），试推导以此速率进入网络所能持续的时间T。讨论一下为什么改变权标加入到漏桶中的速率就可以控制分组进入网络的速率。

答：（1）在时间T内进入漏桶的权标数为rT，设桶内有b个权标，则在时间T内准许进入网络的分组数＝rT＋b；又因为分组速率为N pkt/s，则在时间T内到达的分组数为NT；所以有NT＝rT＋b；

因此，以此速率进入网络所能持续的时间为：T＝b/（N－r）。

（2）从NT＝rT＋b可以看出分组进入网络的速率N＝r＋b/T；

当b＝0时，分组进入网络的速率N等于权标加入到漏桶中的速率r；

当b＞0时，分组进入网络的速率N将大于权标加入到漏桶中的速率r；

综上所述，改变权标加入到漏桶中的速率就可以控制分组进入网络的速率。

24在上题中，设b＝250token，r＝5000token/s，N＝25000pkt/s。试求分组用这样的速率进入网络能够持续多长时间。若N＝2500pkt/s，重新计算本题。

答：若N＝25000pkt/s，T＝b/（N－r）＝250/（25000－5000）＝0.0125s＝12.5ms；

若N＝2500pkt/s，则T＝b/（N－r）＝250/（2500－5000）＝250/（－2500），此时分母为负，表示分组用这样的速率进入网络能持续任意长时间。

25试推导下列公式

$$d_{\max}=\frac{b_i\sum w_j}{R\times w_i}$$

答：下面是公式中各符号的含义：

R＝路由器输出链路的数据率（带宽）；

w_i＝队列i的权重；

$\sum w_j$＝所有的队列权重求和；

b_i＝漏桶i已经装满的权标数；

d_{max}＝传输b_i个分组所需要的时间。

对于分组流i，设漏桶i已经装满了b_i个权标；此时分组流i可以从漏桶中直接拿走b_i个权标，又已知分组流i得到的数据率为

$$R_i = \frac{R \times w_i}{\sum w_j}$$

这b_i个分组的最后一个分组所经受的时延最大，它等于传输b_i个分组所需的时间d_{max}，则d_{max}＝b_i/R_i，将R_i带入即可推出结果。

26假定图8-5中分组流1的漏桶权标装入速率r_1＜$Rw_1/(\sum w_i)$，试证明：25题的公式给出的d_{max}实际上是分组流1中任何分组在WFQ队列中所经受的最大时延。

图8-5　26题图

证明：如图8-6所示，分组流1的发送速度（即离开WFQ队列的速率）≥$w_1R/(\sum w_i)$。如果所有的流的队列中都有分组，那么上面公式的“≥”就应当取“＝”。如果有的队列中没有分组，WFQ就跳过这个队列，因此这个流得到的服务时间就会多一些。

图8-6　分组存储/转发示意图

现在设：

t_0＝由于队列刚刚积累了分组而需要排队等待的时刻；

t＝分组流1队列处于忙状态，$t > t_0$（队列忙就是队列中有排队的分组）；

$T_1(t_0, t)$＝在时间间隔$[t_0, t]$内，分组流1发送到网络的分组数。

显然，$T_1(t_0, t) \geq w_1R(t-t_0)/(\sum w_i)$；

令$Q_1(t)$＝在时间t时分组流1的WFQ队列中排队的分组数，则有：

$Q_1(t) = b_1 + r_1(t-t_0) - T_1(t_0, t)$

$Q_1(t) \leq b_1 + r_1(t-t_0) - w_1R(t-t_0)/(\sum w_i)$

$Q_1(t) \leq b_1 + (t-t_0)[r_1 - w_1R/(\sum w_i)]$

因为$r_1 < Rw_1/(\sum w_i)$，$Q_1(t) \le b_1$，因此分组流1在WFQ队列中排队的最大分组数是b_1。这些分组被服务的速率的最小值是$w_1R/(\sum w_i)$，因此在分组流1中任何分组的最大时延是$d_{max} = b_1(\sum w_i)/w_1R$。

27考虑教材8.4.2节讨论的管制分组流的平均速率和突发长度的漏桶管制器。现在我们限制其峰值速率p分组/秒。试说明怎样把一个漏桶管制器的输出流入到第二个漏桶管制器的输入，以便用这样串接的两个漏桶能够管制分组流的平均速率、峰值速率以及突发长度。第二个漏桶的大小和权标产生的速率应当是怎样的？

答：如图8-7所示，第二个漏桶的大小是1，权标产生的速率是p/s。

图8-7　两个漏桶串接起来

第二个漏桶的权标注入速率是p/s，从长时间来看，进入网络的分组流的最高速率为p pkt/s，这个漏桶最多只能装入一个权标，因此不能有更大的突发分组流产生；

第一个漏桶的权标注入速率是r/s，从长时间来看，最后进入第二个漏桶的分组流的最高速率也只能有这样大，即速率为r pkt/s；

我们需要使$r < p$，这时，最后进入网络的分组流的速率应为r pkt/s；

取第一个漏桶的权标注入速率r/s等于进入网络的分组流的平均速率，取第二个漏桶的权标注入速率p/s等于进入网络的分组流的峰值速率，则在时间T内，第一个漏桶输出的分组最多应等于第二个漏桶所能接纳的分组数，即$rT + b = pT$，则$T = b/(p - r)$，这便是突发长度。

28综合服务IntServ由哪几个部分组成？有保证的服务和受控负载的服务有何区别？

答：（1）IntServ共由以下四个组成部分：

①资源预留协议RSVP：IntServ的信令协议；

②接纳控制：用来决定是否同意对某一资源的请求；

③分类器：用来将进入路由器的分组进行分类，并根据分类的结果将不同类别的分组放入特定的队列；

④调度器：根据服务质量要求决定分组发送的前后顺序。

（2）有保证的服务和受控负载的服务的区别：

①有保证的服务，可保证分组在通过路由器时的排队时延有一个严格的上限；

②受控负载的服务，可以使应用程序得到比通常的“尽最大努力”更加可靠的服务。

29试述资源预留协议RSVP的工作原理。

答：一个会话必须首先声明它所需要的质量服务，以便路由器能够确定是否有足够的资源来满足这个会话的需求。RSVP进行资源预留时，采用了多播树的方式；发送端发送PATH报文，给所有的接收端指明通信量的特性；每个中间的路由器都要转发PATH报文，而接收端用RESV报文进行相应。

注意路径上的每个路由器对RESV报文的请求都可以拒绝或接受；若拒绝，路由器需发送一个差错报告报文给接收端，从而终止这一信令过程；若接受，链路带宽和缓存空间就被分配给这个分组流。

30区分服务DiffServ与综合服务IntServ有何区别？区分服务的工作原理是怎样的？

答：（1）区分服务DiffServ与综合服务IntServ的区别：

①区分服务DiffServ层次简单，伸缩性较好，而IntServ可扩展性差；

②区分服务DiffServ便于实现：把所有复杂性放在边界结点中，使核心路由器工作尽可能简单；

③区分服务DiffServ不影响路由：力图不改变网络的基础结构，而是选择在路由器中增加区分服务的功能；综合服务IntServ对现有路由器的改造十分复杂。

（2）区分服务的工作原理：

DiffServ力图不改变网络的基础结构，但在路由器中增加区分服务的功能；网络被划分为许多个DS域，DiffServ将所有的复杂性放在DS域的边界结点，而使DS域内部路由器工作尽可能快。边界路由器又分为分类器，通信量调节器两大部分。

在网络边界将数据流按QoS要求进行简单分类，不同的类别在内部节点的每次转发中实现不同的转发特性。Diffserv使得ISP能够提供给每个用户不同等级和质量的服务。用户通过设置每个数据包的DS字段的值要求特定的服务等级。

31在区分服务DiffServ中的每跳行为PHB是什么意思？EF PHB和AF PHB有何区别？它们各适用于什么样的通信量？

答：（1）DiffServ定义了在转发分组时体现服务水平的每跳行为PHB，所谓“行为”指在转发分组时路由器对分组是怎样处理的。“每跳”是强调这里所说的行为只涉及到本路由器转发的这一跳的行为，而下一个路由器再怎样处理则与本路由器的处理无关。

（2）EF PHB即迅速转发PHB，它指明离开一个路由器的通信量的数据率必须等于或大于某一数值。因此，EF PHB用来构造通过DS域的一个低丢失率、低时延、低时延抖动、确保带宽的端到端服务。EF PHB可理想地用于实时应用，如视频、VOIP或网络游戏等。

（3）AF PHB即确保转发PHB，AF用DSCP的第0～2位将通信量划分为四个等级，并给每一种等级提供最低数量的带宽和缓存空间。对于其中的每一个等级再用DSCP的第3～5位划分出三个“丢弃优先级”，当发生网络拥塞时，对于每一个等级的AF，路由器将按照“丢弃优先级”分别丢弃分组。AF PHB适用于需要速率保证，但不需要延迟或抖动限制的流量。

32假定一个发送端向2^n个接收端发送多播数据流，而数据流的路径是一个完全的二叉树，在此二叉树的每一个结点上都有一个路由器。若使用RSVP协议进行资源预留，问总共要产生多少个资源预留报文RESV（有的在接收端产生，也有的在网络中的路由器产生）？

答：根据题意，该二叉树有2^n个叶结点，故二叉树的深度为n＋1。每一个节点向其上游节点发送一个RESV报文，所以总共发送的报文数为$m = 2^{n+1} - 1$（个）。

33假定IP电话的发送方在讲话时，每秒钟产生8000字节的话音数据。每隔20毫秒把得到的数据块加上RTP首部和UDP首部后，交给IP层发送出去。假定RTP首部和IP首部都没有选项。试计算发送方在发送这种IP数据报时的数据率（kbit/s）。这个数据率比原始的话音数据率增加了百分之多少？

答：由题可知，每秒钟产生8000字节的话音数据，则20ms产生的数据为8000×0.02＝160B；

又知RTP首部为12B，UDP首部为8B，IP首部为20B；

则首部加上数据构成的IP数据报长度为160＋12＋8＋20＝200B＝1600bit；

因此发送这种IP数据报的数据率为1600/0.02＝80kbit/s；

因为增加了三个首部共40B，则该数据率相比于原始的话音数据率增加了40/160×100%＝25%。

34如图8-8所示，发送方在t＝1发送话音分组8个（等时发送，时间间隔是一个时间单位）。第1个分组在t＝8到达接收方。后续的话音分组的到达时间见图所示。

（1）分组2到分组8的时延（从发送方到接收方）各为多少？

（2）如果接收方在t＝8就开始播放，试问这8个分组中有哪几个未能按时到达赶上播放？

（3）如果接收方在t＝9就开始播放，试问这8个分组中有哪几个未能按时到达赶上播放？

（4）如果要所有的8个分组都能按时赶上播放，那么接收方应在什么时间开始播放？

图8-8　34题图

答：（1）分组2到达的时间为9，时延为7；

分组3到达的时间为12，时延为9；

分组4到达的时间为12，时延为8；

分组5到达的时间为12，时延为7；

分组6到达的时间为15，时延为9；

分组7到达的时间为15，时延为8；

分组8到达的时间为16，时延为8。

（2）未能按时到达赶上播放的分组是：3，4，6，7，8。

（3）未能按时到达赶上播放的分组是：3和6。

（4）要所有的8个分组都能赶上播放，那么接收方应该在t＝10开始播放。

35有一个RTP会话包括四个用户，他们都和同一个多播地址进行通信：发送和接收分组。每个用户发送视频的速率是100kbit/s。

（1）RTCP的通信量将被限制在多少（kbit/s）？

（2）每一个用户能够分配到的RTCP带宽是多少？

答：（1）通常使用RTCP分组的通信量不超过网络中数据分组的通信量的5%；四个用户的会话带宽共有400kbit/s，则400×0.05＝20kbit/s。

（2）每个用户能够分配到的带宽是20kbit/s的四分之一，即20/4＝5kbit/s，用来接收报告和发送报告等。

8.3 考研真题详解

本章内容不是考试重点，所以基本上没有学校的考研试题涉及到本章内容。因此，读者可以简单了解，不必作为复习重点，本部分也就没有选用考研真题。

第9章　无线网络和移动网络

9.1　复习笔记

一、无线局域网WLAN

1无线局域网的组成

无线局域网提供移动接入的功能，可分为两大类：有固定基础设施的和无固定基础设施的。

（1）IEEE 802.11

IEEE 802.11是无线以太网的标准，是有固定基础设施的，它使用星形拓扑，其中心接入点叫做AP，在MAC层使用CSMA/CA协议。凡使用802.11系列协议的局域网又称为Wi-Fi。

IEEE 802.11标准规定无线局域网的最小构件是基本服务集BSS，一个基本服务集可以是孤立的，也可通过接入点AP连接到一个分配系统DS，然后再连接到另一个基本服务集，这样就构成了一个扩展的服务集ESS。

（2）移动自组网络

移动自组网络是无固定基础设施的无线局域网，它又称做自组网络；它是由一些处于平等状态的移动站之间相互通信组成的临时网络，在军用和民用领域都有很好的应用前景。

【注意】常见名词解释（见表9-1）：

表9-1　常见的名词解释

名词	解释
固定接入	在作为网络用户期间，用户设置的地理位置保持不变
移动接入	用户设备能够以车辆速度移动时进行网络通信，当发生地理位置切换时，通信仍然是连续的
便携接入	在受限的网络覆盖面积中，用户设备能够在以步行速度移动时进行网络通信，提供有限的切换能力
游牧接入	用户设备的地理位置至少在进行网络通信时保持不变

2802.11局域网的物理层

根据物理层的不同，对应的标准也不同，如表9-2所示是对无线局域网几种标准的简单比较。

表9-2　几种常用的802.11无线局域网

标准	频段	数据速率	物理层	优缺点
802.11b	2.4GHz	最高为11Mbit/s	扩频	最高数据率较低，价格最低，信号传播距离最远，且不易受阻碍
802.11a	5GHz	最高为54Mbit/s	OFDM	最高数据率较高，支持更多用户同时上网，价格最高，信号传播距离较短，且易受阻碍
802.11g	2.4GHz	最高为54Mbit/s	OFDM	最高数据率较高，支持更多用户同时上网，信号传播距离最远，且不易受阻碍，价格比802.11b贵
802.11n	2.4/5GHz	最高为600Mbit/s	MIMO OFDM	使用多个发送和接收天线达到更高数据率，当使用双倍带宽（40MHz）时速率可达600Mbit/s

3802.11局域网的MAC层协议

（1）CSMA/CA协议概述

①无线局域网中的特殊问题

a．隐蔽站问题：因为距离等原因，不能检测出信道上其他站点信号的问题；

b．暴露站问题：无线局域网中，在不发生干扰的情况下，可允许同时多个移动站进行通信。

②CSMA/CA协议

802.11局域网使用CSMA/CA（载波侦听多路访问/碰撞避免）协议，能够尽量减少碰撞发送的概率。

802.11标准还采用虚拟载波监听机制，让源站把它要占用的信道时间（包括目的站发回确认帧所需的时间）及时通知给所有其他站，以便使其他所有站在这一段时间都停止发送数据，这样大大减少了碰撞的机会。

（2）802.11的MAC层

如图9-1所示，802.11的MAC层在物理层的上面，它包括两个子层：

①分布协调功能DCF：不采用任何中心控制，而是在每一个结点使用CSMA机制的分布式接入算法，让各个站通过争用信道来获取发送权，DCF向上提供争用服务，所有的实现都必须有DCF功能；

②点协调功能PCF：使用集中控制的接入算法，用类似于探询的方法把发送数据权轮流交给各个站，从而避免碰撞的产生；对于时间敏感的业务，如分组话音，就应使用提供无争用服务的点协调功能PCF。

图9-1　802.11的MAC层

（3）为了避免碰撞采取的措施

为尽量避免碰撞，802.11规定所有的站在完成发送后，必须再等待帧间间隔IFS后才能发送下一帧，常见两种帧间间隔为：

①SIFS（短帧间间隔）：长度为28μs，它是最短的帧间间隔；

②DIFS（分布协调功能帧间间隔）：它的长度为128μs，在DCF方式中，DIFS用来发送数据帧和管理帧。

（4）CSMA/CA算法

CSMA/CA算法归纳如下：

①若站点最初有数据要发送，且检测到信道空闲，在等待时间DIFS后，就发送整个数据帧。

②否则，站点执行CSMA/CA协议的退避算法。一旦检测到信道忙，就冻结退避计时器；只要信道空闲，退避计时器就进行倒计时。

③当退避计时器时间减少到零时，站点就发送整个帧并等待确认。

④发送站若收到确认，就知道已发送的帧被目的站正确收到了；若还要发送第二帧，就从②开始，执行CSMA/CA协议的退避算法，随机选定一段退避时间。

（5）对信道进行预约

为了更好地解决隐蔽站带来的碰撞问题，802.11允许要发送数据的站对信道进行预约。

4802.11局域网的MAC帧

802.11帧共有三种类型，即控制帧、数据帧和管理帧；如图9-2所示为802.11的几种帧格式。

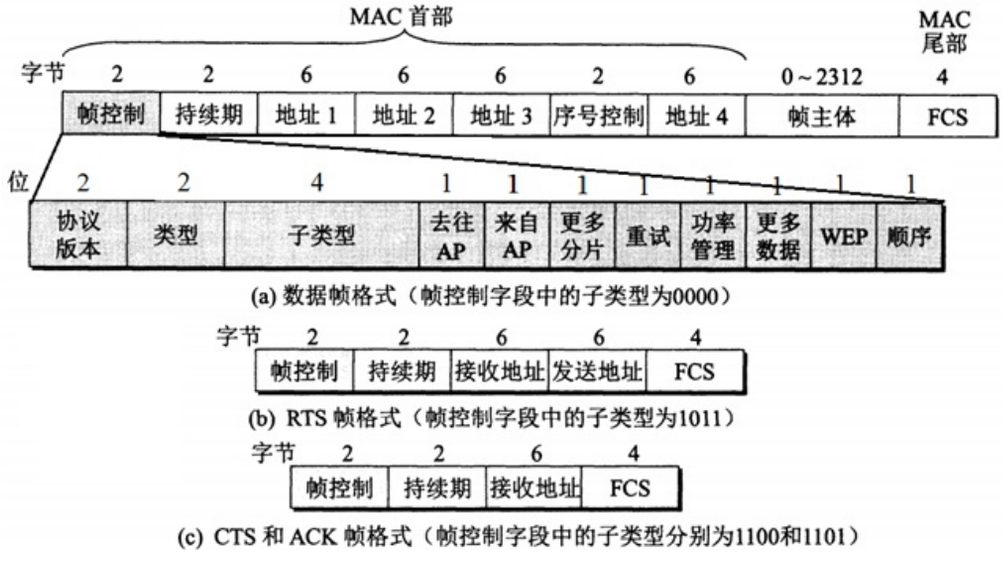

图9-2　802.11局域网的帧格式

二、无线个人区域网WPAN

无线个人区域网WPAN是指在个人工作地方把属于个人使用的电子设备用无线技术连接起来的自组网络，不需要使用接入点AP，整个网络的范围大约在10m左右；例如日常使用的蓝牙系统。

三、无线城域网WMAN

无线城域网（WMAN）是指在地域上覆盖城市及其郊区范围的分布节点之间传输信息的本地分配无线网络。

四、蜂窝移动通信网

1蜂窝无线通信技术简介

蜂窝移动通信又称为小区制移动通信，它把整个的网络服务区划分成许多小区（“蜂窝”），每个小区设置一个基站，负责本小区各个移动站的联络与控制，移动站的发送或接收都必须经过基站进行收发。

2移动IP

（1）相关概念（见表9-3）

表9-3　移动IP的相关概念

概念	解释
移动 IP	又称移动 IP 协议，它允许计算机移动到外地，但仍保留原来的 IP 地址
永久地址或归属地址	一个移动站 A 必须有的一个原始地址
归属网络	移动站原始连接到的网络称作归属网络，且它是不变的
被访网络或外地网络	当移动站 A 移动到另一个地点时所接入的网络称为被访网络或外地网络
归属代理	通常是连接在归属网络上的路由器
外地代理	被访网络中使用的代理称作外地代理，它通常就是连接在被访网络上的路由器
转交地址	外地代理为移动站 A 创建的临时地址
同址转交地址	移动站和外地代理是同一个设备时，这时的转交地址称作同址转交地址

（2）移动IP通信举例

设通信者B要与移动站A通信，则进行以下步骤：

①B发送给A的数据报被A的归属代理截获；

②归属代理知道A的转交地址，因此归属代理把B发来的数据报进行再封装，新的数据报的目的地址是A现在的转交地址；新封装的数据报发送到被访网络的外地代理；

③被访网络中的外地代理把收到的封装的数据报进行拆封，取出B发送的原始数据报，然后转发给移动站A；这个数据报的目的地址就是A的永久地址，此时A收到B，还得到了B的IP地址；

④如果现在A要向B发送数据报，那么A仍然使用自己的永久地址作为数据报的源地址，用B的IP地址作为数据报的目的地址即可。

【注意】为了支持移动性，在网络层应当增加以下的一些新功能：

①移动站到外地代理的协议；

②外地代理到归属代理的登记协议；

③归属代理数据报封装协议；

④外地代理拆封协议。

（3）移动IP的路由选择

移动IP的路由选择有间接路由选择和直接路由选择，后者需要使用通信者代理和外地代理。

3蜂窝移动通信网中对移动用户的路由选择

（1）相关概念

①归属位置寄存器HLR和来访用户位置寄存器VLR

移动交换中心MSC是蜂窝移动通信网中的核心构件，它需要维持HLR和VLR两个重要的数据库，HLR存放签约用户的所有数据信息，VLR则临时存放着当前漫游到这个MSC控制区的用户位置信息。

②移动站漫游号码MSRN

当移动用户漫游到新的MSC控制区时，VLR给该移动用户分配一个临时的移动站漫游号码MSRN来表示移动用户现在的位置信息。

（2）固定电话用户呼叫移动用户的步骤

如图9-3所示为固定用户呼叫移动用户的步骤示意图。

图9-3　固定电话用户呼叫移动用户（间接路由选择）

4GSM中的切换

切换是指移动用户与相关联的基站发生了改变，它使得呼叫的传输路由发生变化。

5无线网络对高层协议的影响

无线网络在移动站漫游时，会经常更换移动用户到无线网络的连接点（即到移动站相关联的基站），网络的连接就易发生很短时间的中断，此时举例说明对运输层的影响：在TCP连接中，只要出现TCP报文段频繁丢失，TCP的拥塞控制就会采取措施，减小其拥塞窗口，从而使TCP发送方的报文段发送速率降低。

五、两种不同的无线上网

无线上网常见有两种方式，一种是利用蜂窝移动网络，另一种是Wi-Fi上网，但两者费用差距较大。

9.2　课后习题详解

1无线局域网都由哪几部分组成？无线局域网中的固定基础设施对网络的性能有何影响？接入点AP是否就是无线局域网中的固定基础设施？

答：（1）无线局域网由无线网卡、无线接入点（AP）、计算机和有关设备组成，采用单元结构，将整个系统分成许多单元，每个单元称为一个基本服务集。

（2）“固定基础设施”是指预先建立起来的、能够覆盖一定地理范围的一批固定基站，直接影响无线局域网的性能；若固定基础设施出现故障，那么该基础设施覆盖的地理范围内所有通过AP进行转接的通信都要中断，整个网络的性能明显下降。

（3）是，但无线局域网中的固定设施并不只是接入点AP，互联AP和路由器以及互联几个AP的有线以太网也属于基础设施。

2Wi-Fi与无线局域网WLAN是否为同义词？请简单说明一下。

答：Wi-Fi在许多文献中与无线局域网WLAN是同义词。

从理论上讲，不采用IEEE 802.11协议的无线局域网就不能称为Wi-Fi，但IEEE 802.11是无线局域网的标准，事实上现在流行的无线局域网都采用了该标准，所以说它们是同义词。

3服务集标识符SSID与基本服务集标识符BSSID有什么区别？

答：（1）服务集标识符：网络管理员安装AP时为它分配的长1～32字节的标识符，表示一个无线局域网的名字，用户根据SSID能知道自己所使用的无线局域网的服务集标识符；

（2）基本服务集标识符BSSID：一个基本服务集BSS的唯一标识符，它是接入点AP的MAC地址，长度为6个字节。

4在无线局域网中的关联（association）的作用是什么？

答：在无线局域网中建立关联（association）的作用是使得某个移动站加入到选定的AP所属的子网中，并和这个接入点AP之间建立一个虚拟线路，实现移动站与AP之间，以及不同AP站点之间的数据帧传送。

5以下几种接入（固定接入、移动接入、便携接入和游牧接入）的主要特点是什么？

答：（1）固定接入：在作为网络用户期间，用户设置的地理位置保持不变；

（2）移动接入：用户设备能够以车辆速度移动时进行网络通信，当发生地理位置切换时，通信仍是连续的；

（3）便携接入：在受限的网络覆盖面积中，用户设备能够在以步行速度移动时进行网络通信，提供有限的切换能力；

（4）游牧接入：用户设备的地理位置至少在进行网络通信时保持不变。

6无线局域网的物理层主要有哪几种？

答：无线局域网的物理层主要有802.11家族谱、蓝牙新贵、家庭网络的HomeRF，其中几种常用的802.11无线局域网标准如表9-4所示。

表9-4　几种常用的802.11无线局域网

标准	频段	数据速率	物理层	优缺点
802.11b	2.4GHz	最高为11Mbit/s	扩频	最高数据率较低，价格最低，信号传播距离最远，且不易受阻碍
802.11a	5GHz	最高为54Mbit/s	OFDM	最高数据率较高，支持更多用户同时上网，价格最高，信号传播距离较短，且易受阻碍
802.11g	2.4GHz	最高为54Mbit/s	OFDM	最高数据率较高，支持更多用户同时上网，信号传播距离最远，且不易受阻碍，价格比802.11b贵
802.11n	2.4/5GHz	最高为600Mbit/s	MIMO OFDM	使用多个发送和接收天线达到更高数据率，当使用双倍带宽（40MHz）时速率可达600Mbit/s

7无线局域网的MAC协议有哪些特点？为什么在无线局域网中不能使用CSMA/CD协议而必须使用CSMA/CA协议？

答：（1）无线局域网的MAC协议的特点：

①802.11标准设计了独特的MAC层，它通过协调功能来确定在基本服务集BSS中的移动站在什么时间能发送数据或接收数据；

②MAC层在物理层的上面，包括有两个子层，分别是分步协调功能DCF子层和点协调功能PCF子层；

③为了避免碰撞，规定所有的站在完成发送后，必须再等待一段时间才能发送下一帧。

例如这里的MAC协议主要是指CSMA/CA协议，其特点有是：当一个站要发送数据时，就要检测信道，若信道忙，就按照协议推后发送；若信道空闲，等待一段时间（DIFS）再发送；接收站若正确收到该帧，就发出确认帧，发送方若收到确认帧则表明没有发送碰撞，否则就要重传这个帧，直到收到确认为止，或经过给定次数的重传后放弃。

（2）CSMA/CD协议不能用于无线局域网的原因：

①CSMA/CD协议要求一个站点在发送本站数据的同时还必须不间断地检测信道，以便发现是否有其他的站也在发送数据，这样才能实现“碰撞检测”的功能，但是在无线局域网的设备中要实现这种功能花费过大；

②以太网的碰撞检测是假定了所有站点都能够听到其他站点是否在发送数据，而无线局域网环境下这个假设不成立；即便发送数据时检测到信道是空闲的，在接收端仍然有可能发生碰撞。

因此，无线局域网不能使用CSMA/CD，而只能使用改进的CSMA/CA协议。

8为什么无线局域网的站点在发送数据帧时，即使检测到信道空闲也仍然要等待一小段时间？为什么在发送数据帧的过程中不像以太网那样继续对信道进行检测？

答：（1）这样做是为了避免和其他数据的站发生碰撞；若等待一段时间后，其他站在检测时会探测到已经有站欲发送数据，则检测结果为信道忙，这样就避免了发生碰撞。

（2）无线局域网的适配器上，接收信号的强度往往小于发送信号的强度，若因此要设计碰撞检测，则在硬件上花费过大；另外无线局域网的站点在发送数据帧时，检测到信道空闲是指这个覆盖范围内的空闲，其实可能并不空闲；因此发送数据帧的过程中不像以太网那样继续对信道进行检测。

9结合隐蔽站问题和暴露站问题说明RTS帧和CTS帧的作用。RTS/CTS是强制使用还是选择使用？请说明理由。

答：设题中A、B、C、D、E为不同的站；

（1）隐蔽站问题：如图9-4（a）所示，当A和C都检测不到无线信号时，以为是空的，向B发送数据，结果B同时收到A和C发送的数据，发生碰撞；即它未能检测出信道上其他站点信号；

暴露站问题：如图9-4（b）所示，当站B向A发送数据，而C又想和D通信时，由于C检测到了媒体上有信号，于是不能向D发送数据。

使用RTS和CTS帧后能解决上述两个问题：

如图9-5（a）所示，A在发送数据帧之前先发送一个短的控制帧RTS，若信道空闲，目的站B就响应一个控制帧CTS；

如图9-5（b）所示，A收到CTS帧后就可以发送其数据帧，C此时处于A的范围内，但不在B的范围内；因此C能够收到A发送的RTS，但并不能收到B发送的CTS帧，所以在A向B发送数据时，C也可以发送自己的数据给其他站，而不干扰B。

图中D只能收到B发送的CTS帧，而不能收到A发送的RTS帧，因此D知道B将和A通信，而它选择不干扰它们的通信。

对于站E，它能收到RTS和CTS，和D一样，在A发送数据帧和B发送确认帧的整个过程中都不能发送数据。

图9-4　隐蔽站问题和暴露站问题

图9-5　使用RTS和CTS的情况

（2）RTS/CTS是选择使用的。因为使用RTS/CTS帧，必然增加开销，而若无线局域网工作环境较好，碰撞的次数不多时，不采用这个选项会更好。

10为什么在无线局域网上发送数据帧后要对方必须发回确认帧，而以太网就不需要对方发回确认帧？

答：无线信道的通信质量远比不上有线信道，它在传输过程中很容易出现差错，因此需要收到确认帧后才开始下一数据帧的发

送；以太网因为本身信道通信质量高，就不需要这个过程。

11无线局域网的MAC协议中的SIFS，PIFS和DIFS的作用是什么？

答：（1）SIFS：即短帧间间隔，最短的帧间间隔，用来分隔开属于一次对话的各帧。

（2）PIFS：即点协调功能帧间间隔，是为了在开始使用PCF方式时（在PCF方式下使用，没有争用），使接入点AP能优先接入到媒体中。

（3）DIFS：即分布协调功能帧间间隔，在DCF方式中用来开始新的传输（数据帧和管理帧）。

12试解释无线局域网中的名词：BSS，ESS，AP，BSA，DCF，PCF和NAV。

答：（1）BSS：基本服务集，是无线局域网的最小构件；一个BSS包括一个基站和若干个移动站；

（2）ESS：扩展的服务集，一个基本服务集通过接入点AP连接到一个主干分配系统DS，再接入到另一个基本服务集，构成了一个扩展服务集；

（3）AP：接入点，基本服务集里面的基站；

（4）BSA：基本服务区，一个基本服务集BSS所覆盖的地理范围；

（5）DCF：分布协调功能，802.11标准设计的MAC层中靠下面的一个子层，它向上提供争用服务；

（6）PCF：点协调功能，PCF是MAC层的另一个子层，是选项，为的是使接入点AP集中控制整个BSS内的活动；它使用集中控制的接入算法，用类似于探询的方法将发送数据权轮流交给各个站，从而避免了碰撞的产生；

（7）NAV：网络分配向量，它指出了信道处于忙碌状态的持续时间。

13冻结退避计时器剩余时间的做法是为了使协议对所有占有站点更加公平。请进一步解释。

答：冻结退避计时器剩余时间是若检测到信道空闲，退避计时器就继续倒计时；若检测到信道忙，就停止倒计时，等到信道空闲时并再经过时间DIFS后，从剩余时间继续倒计时；

若不这样，则可能退避计时器时间减小到零时信道仍处于忙，此时需再次进行退避（重新设置退避计时器；根据退避算法，这样可能会等待更长的时间。这种做法对于没有机会发送数据的站就显得不太公平。

14为什么某站点在发送第一帧之前，若检测到信道空闲就可在等待时间DIFS后立即发送出去，但在收到对第一帧的确认后并打算发送下一帧时，就必须执行退避算法？

答：若第一个站在收到确认后立即发送下一帧数据而不执行退避算法，可能出现它长时间垄断数据的发送，这是不公平的；执行了退避算法才能保证各站点公平地发送数据。

15无线局域网的MAC帧为什么要使用四个地址字段？请用简单的例子说明地址3的作用。

答：（1）因为无线局域网除有源、目的地址以外，还包括区分不同无线网络的接入点AP地址和用于自组织网络的地址，所以无线局域网的MAC帧要使用四个地址字段。

（2）举例说明地址3的作用：

如图9-6所示，站点A向B发送数据帧，其间通过接入点AP_1转发。

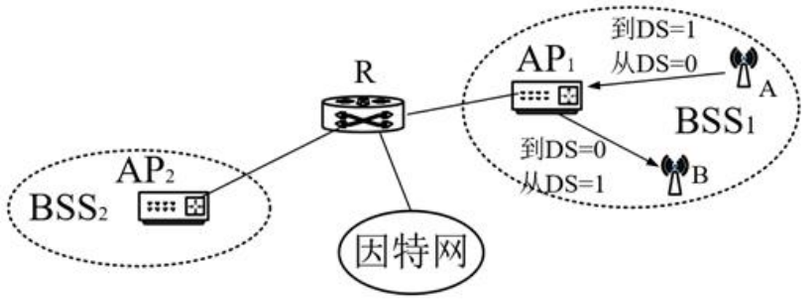

图9-6　A通过AP_1向B发送数据

此时A发送的MAC帧首部中有关的字段值如下所示。

到 DS	从 DS	…	地址 1	地址 2	地址 3
1	0	…	AP_1的 MAC 地址	A 的 MAC 地址	B 的 MAC 地址

则地址3存储的是数据最终要达到的MAC地址。

16试比较IEEE 802.3和IEEE 802.11局域网，找出它们之间的主要区别。

答：IEEE 802.3和IEEE 802.11局域网的主要区别如表9-5所示。

表9-5　IEEE 802.3和IEEE 802.11局域网的区别

比较项目	IEEE 802.3	IEEE 802.11
使用的协议	CSMA/CD	CSMA/CA
信道空闲时	立即发送数据	等一段帧间间隔后，发送或执行退避算法
检测信道的方法	边发边检测	发送之前检测
发送时是否能检测到碰撞	能，碰撞后中止发送	不能
接收方收到正确的帧	不发回确认	发回确认
何时执行退避算法	仅在检测到碰撞后执行	要发数据但检测到信道忙时执行
传输媒体	有线传输媒体	无线传输媒体
是否存在隐蔽站问题	否	是
是否需要接入点 AP	不需要	需要
安全性	很好	比 IEEE 802.3 差

17无线个人区域网WPAN的主要特点是什么，现在已经有了什么标准？

答：（1）WPAN的主要特点是低功率、小范围、低速率和低价格，不需要使用接入点AP，可以一个人使用也可以若干人共同使用。

（2）现在使用较多的WPAN是：

①蓝牙系统（标准是IEEE 802.15.1）；

②低速WPAN（标准是IEEE 802.15.4）；

③高速WPAN（标准是IEEE 802.15.3）。

18无线城域网WMAN的主要特点是什么，现在已经有了什么标准？

答：（1）WMAN的主要特点是可扩展、长距离、大容量，可提供“最后一英里”的无线接入（固定的、移动的、便携的）。

（2）已有标准包括：IEEE 802.16d（固定宽带无线接入空中接口标准）、IEEE 802.16e（支持移动性的宽带无线接入空中接口标准）。

19当计算机移动到外地时，为什么可以保留其原来的IP地址？这时需要采取哪些措施？

答：为保留其原来的IP地址，需要采用移动IP技术，下面举例说明采用了该措施即可保留原来的IP地址：

设通信者B要与移动站A通信，则进行以下步骤：

（1）B发送给A的数据报被A的归属代理截获；

（2）归属代理知道A的转交地址，因此归属代理把B发来的数据报进行再封装，新的数据报的目的地址是A现在的转交地址；新封装的数据报发送到被访网络的外地代理；

（3）被访网络中的外地代理把收到的封装的数据报进行拆封，取出B发送的原始数据报，然后转发给移动站A；这个数据报的目的地址就是A的永久地址，此时A收到B，还得到了B的IP地址；

（4）如果现在A要向B发送数据报，那么A仍然使用自己的永久地址作为数据报的源地址，用B的IP地址作为数据报的目的地址即可。

从上述过程中可以看出，利用该过程就能实现当计算机移动到外地时，可以保留其原来的IP地址。

20试解释一下名词：归属网络，永久地址，归属代理，被访网络，外地代理，转交地址。

答：（1）归属网络：移动站原始连接到的网络称作归属网络，且它是不变的；

（2）永久地址：一个移动站A必须有的一个原始地址；

（3）归属代理：通常是连接在归属网络上的路由器；

（4）被访网络：当移动站A移动到另一个地点时所接入的网络称为被访网络或外地网络；

（5）外地代理：被访网络中使用的代理称作外地代理，它通常就是连接在被访网络上的路由器；

（6）转交地址：外地代理为移动站A创建的临时地址。

21当移动站在漫游时，为了找到这个移动站，可以使用间接路由选择和直接路由选择。这两种方法有什么区别？

答：移动IP的间接路由选择和直接路由选择最主要的区别如下：

（1）间接路由选择：源站并不知道移动站的当前地址，而是把数据报发往移动站的归属网络，以后的寻址工作都由归属代理来完成；

（2）直接路由选择：通信者创建一个通信者代理，由这个通信者代理向归属代理询问移动站在被访网络的转交地址，然后由通信者代理把数据报用隧道技术发送到被访网络的外地代理，最后再由这个外地代理拆封，把数据报转发给移动站。

22试以固定电话呼叫蜂窝移动通信网中的移动电话为例，说明怎样用间接路由选择和直接路由选择的方法找到正在漫游的移动电话。

答：如图9-7所示为呼叫过程中的三个重要步骤：

（1）找到移动用户的归属网络：固定电话用户首先拨移动用户的电话号码，从这个电话号码很容易找到了移动用户电话的归属网络；所以通信者拨出某个移动用户的号码后，公用电话网的交换机就能够把呼叫传送到被叫的归属网络交换中心（归属MSC）；

（2）归属MSC向其HLR查询现在被叫移动用户的位置：HLR向归属MSC返回被叫移动用户的移动站漫游号MSRN；

（3）归属MSC按照所得到的漫游号码MSRN进行呼叫的第二段，把通信者发起的呼叫从归属MSC传送到被访网络的MSC，再传送到该移动用户所漫游到的小区的基站，这样整个的呼叫就完成了。

上述呼叫过程使用的是间接路由选择，不管被叫移动用户的位置如何，呼叫的第一步总是先找到被叫移动用户的归属MSC，呼叫的第二步再从归属MSC找到到被访网络的MSC和与该MSC相关联的被叫。

图9-7　固定电话用户呼叫移动用户

23在蜂窝移动通信网中，移动站的漫游所产生的切换，对正在工作的TCP连接有什么影响？

答：在TCP连接中，只要发生报文段的丢失或出错，TCP就要重传这个丢失或出错的报文段。移动站的漫游所产生的切换中，由于移动用户更新相关联的基站需要一定的时间，这就可能造成TCP报文段的丢失，但TCP并不知道现在出现分组丢失的原因，只要出现TCP报文段频繁丢失，TCP的拥塞控制就会采取措施，减小其拥塞窗口，从而使TCP发送方的报文段发送速率减低。

24某餐馆中有两个ISP分别设置了接入点AP_1和AP_2，并且都使用802.11b协议。两个ISP都分别有自己的IP地址块。

（1）假定两个ISP在配置其接入点时都选择了信道11。如果有用户A和B分别使用接入点AP_1和AP_2，那么这两个无线网络能够正常工作吗？

（2）若这两个AP一个工作在信道1，而另一个工作在信道11，题目的答案有变化吗？

答：（1）两个无线网络的名字一般不会是一样的，若A和B只有其中一个在通话，那么这两个无线网络可以正常工作；如果两人同时进行通话，由于信道11是共同使用的，就必然产生冲突，两个AP无法正常工作。

（2）因为两个AP工作在不同的信道，所以它们可以正常工作。

25教材中有这样的叙述：“当信道从忙态变为空闲时，任何一个站要发送数据帧时，只要不是要发送的第一个帧，不仅都必须等待一个DIFS的间隔，而且还要进入争用窗口”。试解释为什么这里要限定“只要不是要发送的第一个帧”。

答：为了防止一个站一直垄断信道，一直不停地发送大文件，所以才需要进入争用窗口，但第一个帧不需要。

26假定有一个使用802.11b协议的站要发送1000字节长的数据帧（已包括了首部和尾部），并使用RTS和CTS帧。试计算，从决定发送帧一直到收到确认帧所经历的时间（以微秒计），忽略传播时间和误码率。在数据帧首部中的持续期字段中，应写入什么二进制代码？在ACK的持续期字段中，应写入什么二进制代码？

答：（1）由题可知，这个站要发送的信息如下：

DIFS＋RTS＋SIFS＋CTS＋SIFS＋1000字节的数据帧＋SIFS＋ACK；

因为RTS长20字节，CTS和ACK各为14字节，则发送的信息有：DIFS＋3FIFS＋1048字节；

因为802.11b协议中数据率为11Mbit/s，则1048字节发送时间为1048×8/（11×10^6）≈762.2us；

又因为DIFS是128us，SIFS是28us，因此从决定发送帧一直到收到确认帧所经历的时间约为：128＋3×28＋762.2＝974.2us。

（2）在数据帧的持续期字段中，应写入00000011 0100000。

（3）在ACK的持续期字段中，应写入全0。

27有如图9-8所示的四个站点使用同一无线频率通信。每个站点的无线电覆盖范围都是图9-8所示的椭圆形。也就是说，A发送时，仅仅B能够接收；B发送时，A和C能够接收；C发送时B和D能够接收；D发送时，仅仅C能够接收。

现假定每个站点都有无限多的报文要向每一个其他站点发送。若无法直接发送，则由中间的站点接收后再转发。例如，A发送报文给D时，就必须是经过A→B，B→C和C→D这样三次发送和转发。时间被划分成等长的时隙，每个报文的发送时间恰好等于一个时隙长度。在一个时隙中，一个站点可以做以下事情中的一个：①发送一个报文；②接收一个发给自己的报文；③什么也不做。再假定传输无差错，在无线电覆盖范围内都能正确接收。

图9-8　27题图

（1）假定有一个全能的控制器，能够命令各站点的发送或接收。试计算从C到A的最大数据报文传输速率（单位为报文/时隙）。

（2）假定现在A向B发送报文，D向C发送报文。试计算从A到B和从D到C的最大数据报文传输速率（单位为报文/时隙）。

（3）假定现在A向B发送报文，C向D发送报文。试计算从A到B和从C到D的最大数据报文传输速率（单位为报文/时隙）。

（4）假定本题中的所有无线链路都换成为有线链路。重做以上的（1）至（3）小题。

（5）现在再回到无线链路的情况。假定在每个目的站点收到报文后都必须向源站点发回ACK报文，而ACK报文也要用掉一个时隙。重做以上的（1）至（3）小题。

答：（1）C→B，然后B→A，从C到A的最大数据报文传输速率为：1报文/2时隙。

（2）因为A和D的发送可以同时进行，则从A到B和从D到C的最大数据报文传输速率为：2报文/1时隙。

（3）从A到B和从C到D的最大数据报文传输速率为：1报文/1时隙；当C→D时，B也能收到信号，因此C→D和A→B不能同时进行。

（4）①1报文/1时隙。C→B和B→A这两个传输可同时运行。除了第一个报文外，以后都是A每一个时隙可收到一个报文；

②2报文/1时隙，同时传输；

③2报文/1时隙，同时传输。

（5）①1报文/4时隙。发送报文C→B，然后B→A，用两个时隙。发送ACK同样要用掉两个时隙；

②时隙1：报文A→B，报文D→C；

时隙2：ACK B→A；

时隙3：ACK C→D；

即得出结果为：2报文/3时隙；

③时隙1：报文C→D；

时隙2：ACK D→C，报文A→B；

时隙3：ACK B→A；

得出结果为：2报文/3时隙。

9.3 考研真题详解

本章内容不是考试重点，所以基本上没有学校的考研试题涉及到本章内容。因此，读者可以简单了解，不必作为复习重点，本部分也就没有选用考研真题。