期末帮《计算机网络》课程讲义

第一章 计算机网络概述

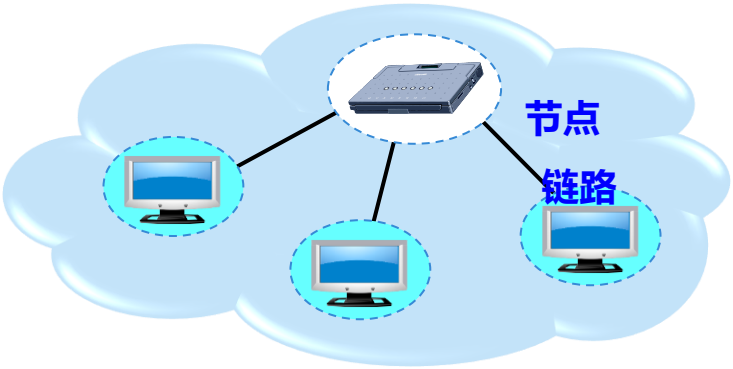
（一）互联网的概述与组成

1.互连网与互联网

internet 是互连网，通用名词，泛指由多个计算机网络互连而成的计算机网络。

Internet 是互联网，专用名词，特指全球最大的互连网。

互连网 (internet) ≠ 互联网 (Internet)



计算机网络（网络）

例题 1：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？

解：internet 是互连网，通用名词，泛指网络。Internet 是互联网，专用名词，特指全球最大的互连网。

2、互连网基础结构发展的三个阶段

（1）第一阶段：从单个网络 ARPANET 向互连网发展的过程。

（2）第二阶段：建成了三级结构的互联网。（主干网、地区网和校园网）

（3）第三阶段：逐渐形成了全球范围的多层次 ISP 结构的互联网。例如中国移动、中国联通等公司，均属于互联网服务提供商（者）。

ISP：互联网服务提供者（Internet Service Provider）

例题 2：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？

解：第一阶段：从单个网络 ARPANET 向互连网发展，TCP/IP 协议初步成型。

第二阶段：建成了三级结构的互联网，分为主干网、地区网和校园网。

第三阶段：形成了全球范围的多层次 ISP 结构的互联网，ISP 首次出现。

3、互联网的组成

（1）边缘部分：由所有连接在互联网上的主机组成，由用户直接使用，用来进行通信（传送数据、音频或视频）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（提供连通性和交换）。

例题 3：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?

解：边缘部分：由各主机构成，用户直接进行信息处理和信息共享；低速连

入核心网。

核心部分：由各路由器连网，负责为边缘部分提供高速远程分组交换。

4、互联网的边缘部分

（1）处在互联网边缘部分的就是连接在互联网上的所有的主机。这些主机又称为端系统 (end system)。

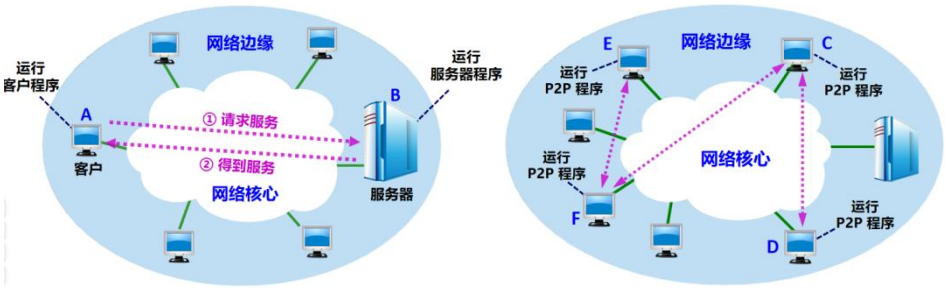
（2）边缘部分利用核心部分提供的服务进行通信，一般称为计算机之间通信。

（3）计算机之间的通信实际上是计算机 A 上某个进程和计算机 B 上另一个进程之间的通信。

（4）通信方式主要有两类：客户-服务器方式、对等连接方式（P2P）。

客户-服务器方式：客户是服务请求方，服务器是服务提供方。

对等连接方式：并不区分服务请求方和服务提供方。



5、互联网的核心部分

典型交换技术包括：

电路交换：整个报文的比特流连续地从源点直达终点，好像在一个管道中传送。

报文交换：整个报文先传送到相邻节点，全部存储下来后查找转发表，转发到下一个节点。

分组交换：单个分组（整个报文的一部分）传送到相邻节点，存储下来后查找转发表，转发到下一个节点。

互联网的核心部分采用分组交换技术。

例题 4：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。

解：电路交换：端对端通信质量因约定了通信资源获得可靠保障，对连续传送大量数据效率高。

报文交换： 无须预约传输带宽，动态逐段利用传输带宽对突发式数据通信效率高，通信迅速。

分组交换：具有报文交换高效、迅速的要点，且各分组小，路由灵活，网络生存性能好。

（二）计算机网络的类别

目前学术界并未形成公认的计算机网络定义，以下采用一个认可度较高的定义。

1、计算机网络的定义

计算机网络主要是由一些通用的、可编程的硬件互连而成的，而这些硬件并非专门用来实现某一特定目的（例如，传送数据或视频信号）。这些可编程的硬件能够用来传送多种不同类型的数据，并能支持广泛的和日益增长的应用。

（1）计算机网络所连接的硬件，并不限于一般的计算机，而是包括了智能手机或智能电视机；

（2）计算机网络并非专门用来传送数据，而是能够支持很多种应用。当然，没有数据的传送，这些应用是无法实现的。

2、计算机网络的类别

按网络作用范围分类：

广域网 WAN：互联网的核心部分，连接广域网各结点的一般使高速链路。

城域网 MAN：很多城域网采用的是以太网技术，常并入局域网进行讨论。

局域网 LAN：一般通过高速通信线路相连，地理范围较小。（校园网、企业）

个人区域网 PAN：范围很小，一般在 10m 左右。

按网络使用者分类：

公用网（public network）：电信公司出资建造的大型网络。

专用网（private network）：某个部门为满足本单位的特殊业务工作需要而建造的网络。

例题 5：下列哪些属于计算机网络的类别（　　）

A. WAN　　B. LAN　　C. PAN　　D. public network

解：ABCD

（三）计算机网络的性能

1、计算机网络的性能指标

（1）速率：数据的传送速率，也称为比特率。单位是 bit/s（比特每秒）或 b/s、bps

（2）带宽：单位时间内网络中的某信道所能通过的“最高数据率”。单位：bit/s（比特每秒）

（3）吞吐量：单位时间内通过某个网络的实际数据量。

例题 6：假定主机 A 和服务器 B 接入到互联网的链路速率分别是 100Mbit/s 和 1Gbit/s，如果互联网各链路的容量足够大，那么当 A 和 B 交换数据时，其吞吐量是多少？

解：100Mbit/s

结论：吞吐量受网络带宽或网络额定速率（瓶颈速率）的限制。

（4）时延：数据从网络的一端传送到另一端所需的时间。由以下几个部分组成：

发送时延：是主机或路由器发送数据帧所需要的时间。

$$\text{发送时延}=\frac{\text{数据帧长度（bit）}}{\text{发送速率（bit/s）}}$$

传播时延：是电磁波在信道中传播一定的距离需要花费的时间。

$$\text{传播时延}=\frac{\text{信道长度（米）}}{\text{信号在信道上的传播速率（米/秒）}}$$

处理时延：主机或路由器在收到分组时，为处理分组（例如分析首部、提取

数据、差错检验或查找路由）所花费的时间。

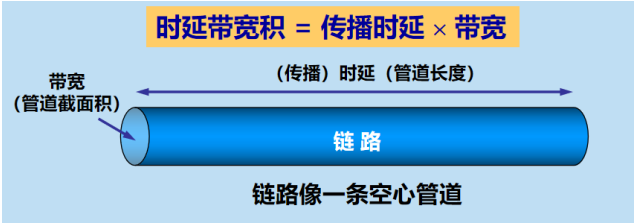
排队时延：分组在路由器输入输出队列中排队等待处理和转发所经历的时延。

例题 7：主机 A 到主机 B 的路径上有三段链路，其速率分别为 2Mbit/s，1Mbit/s 和 500kbit/s。现在 A 向 B 发送一个大文件，试计算该文件传送的吞吐量。设文件长度为 10MB，而网络上没有其他的流量。请问该文件从 A 传送到 B 大约需要多少时间？

解：因为文件的吞吐量由瓶颈链路决定，所以该文件传送的吞吐量为 500kbit/s。

传送需要时间为 168 秒。

（5）时延带宽积=传播时延×带宽



例题 8：设某段链路的传播时延为 20ms，带宽为 10Mbit/s，算出其时延带宽积。

解：时延带宽积=$20\times10^{-3}\times10\times10^{6}=2\times10^{5}$ bit

（6）往返时间 RTT：表示从发送方发送完数据，到发送方收到来自接收方的确认总共经历的时间。

例题 9：结点 A 要将一个 100 MB 数据以 100 Mbit/s 的速率发送给结点 B，B 正确收完该数据后，就立即向 A 发送确认。假定 A 只有在收到 B 的确认信息后，才能继续向 B 发送数据，且确认信息很短。如果 RTT=2，计算 A 向 B 发送数据的有效数据率。

解：发送时间=数据长度/发送速率≈8.39s

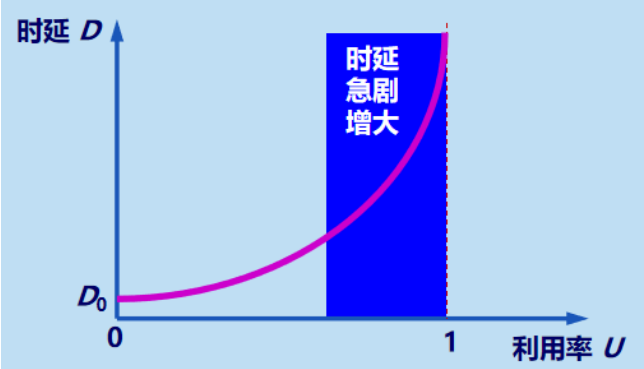
有效数据率=数据长度/（发送时间+RTT）≈80.7Mbit/s

（7）利用率：分为信道利用率和网络利用率。

信道利用率：指出某信道有百分之几的时间是被利用的。

网络利用率：全网络的信道利用率的加权平均值。

当某信道的利用率增大时，时延会迅速增加。



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

例题 10：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？

解：非性能特征有：（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

主要区别：性能指标是直接反映网络性能的，而非性能特征则不是网络所特有的指标。

（四）计算机网络体系结构

1、计算机网络体系结构的形成（非重点，了解即可）

（1）必须有一条传送数据的通路。

（2）发起方必须激活通路。

（3）要告诉网络如何识别接收方。

（4）发起方要清楚对方是否已开机，且与网络连接正常。

（5）发起方要清楚对方是否准备好接收和存储文件。

（6）若文件格式不兼容，要完成格式的转换。

（7）要处理各种差错和意外事故，保证收到正确的文件。

2、协议与划分层次

（1）网络协议 (network protocol)：简称为协议，是为进行网络中的数据交换而建立的规则、标准或约定。

（2）三个组成要素：

语法：数据与控制信息的结构或格式 。

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。

同步：事件实现顺序的详细说明。

例题 11：网络协议的三个要素是什么？各有什么含义？

解：语法：数据与控制信息的结构或格式。

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。

同步：事件实现顺序的详细说明。

（3）网络协议是分层的，分层的好处（了解）：

各层之间互相独立。

灵活性好。

结构上可分割开。

易于实现和维护。

能促进标准化工作。

（4）各层需要完成的工作包括一下的一种或多种：

差错控制：使通信更加可靠。

流量控制：发送端的发送速率必须使接收端来得及接受，不能太快。

分段和重装：发送端将数据分块，接收端还原。

复用和分用：发送端几个高层会话复用一条低层的连接，在接收端再进行分用。

连接建立和释放：交换数据前先建立一条逻辑连接，数据传送结束后再释放。

计算机网络的各层及其协议的集合就是网络的体系结构。

3、具有五层协议的体系结构

应用层：通过应用进程间的交互来完成特定网络应用。

运输层：负责向两台主机中进程之间的通信提供通用的数据传输服务。

网络层：为分组交换网上的不同主机提供通信服务。选择合适的路由。

数据链路层：将网络层交下来的 IP 数据报组装成帧，在两个相邻结点的链路上传送帧。每一帧包括数据和必要的控制信息。

物理层：实现比特（0 或 1）的传输。确定连接电缆的插头应当有多少根引脚，以及各引脚应如何连接。

例题 12： 具有五层协议的网络体系结构分别是：物理层、_____、_____、_____和应用层。

解：数据链路层；网络层；运输层。

第二章 物理层

（一）物理层的任务

1. 物理层的基本概念

（1）物理层考虑的是怎样才能在连接各种计算机的传输媒体上传输数据比特流，而不是指具体的传输媒体。

（2）作用：尽可能屏蔽掉不同传输媒体和通信手段的差异。

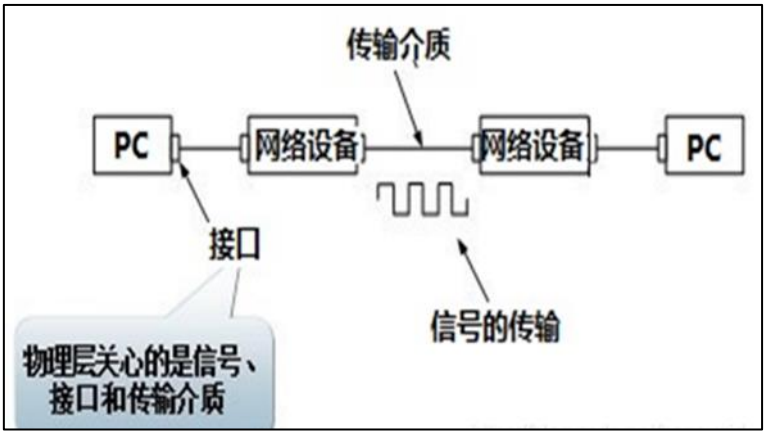
（3）用于物理层的协议也常称为物理层规程 (procedure)。

例题 1：物理层要解决什么问题？

解：物理层要尽可能地屏蔽掉物理设备和传输媒体，通信手段的不同，使数据链路层感觉不到这些差异，只考虑完成本层的协议和服务。

2、物理层的主要任务（特性）

确定与传输媒体的接口的一些特性。



（1）机械特性：指明接口所用接线器的形状和尺寸、引线数目和排列、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的意义。

（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。

例题 2：物理层的接口有哪几个方面的特性？各包含些什么内容？

解：物理层考虑的是怎样才能在连接各种计算机的传输媒体上传输数据比特流，屏蔽掉不同传输媒体和通信手段的差异。

其主要特点有：

（1）机械特性：指明接口所用接线器的形状和尺寸、引线数目和排列、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的意义。

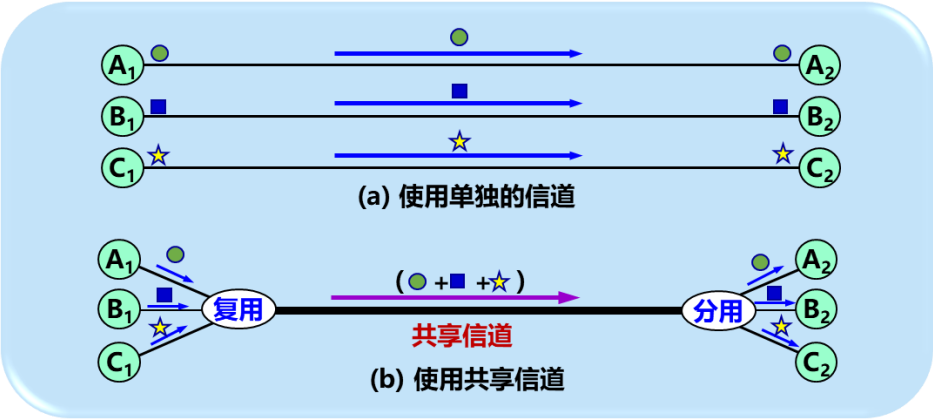
（4）过程特性：指明对于不同功能的各种可能事件的出现顺序。

（二）信道复用技术

1、复用的定义

复用 (multiplexing) ： 允许用户使用一个共享信道进行通信。

注：在进行通信时，复用器 (multiplexer) 和分用器 (demultiplexer)总是成对使用。



2、频分复用 FDM (Frequency Division Multiplexing)

（1）将整个带宽分为多份，用户在分配到一定的频带后，在通信过程中自始至终都占用这个频带。

（2）所有用户在同样的时间占用不同的带宽（即频带）资源。

例题 3：最基本的两种复用技术是什么？（　　）

A.频分复用　B.码分复用　C.时分复用　D.波分复用　E.统计时分复用

解：AC

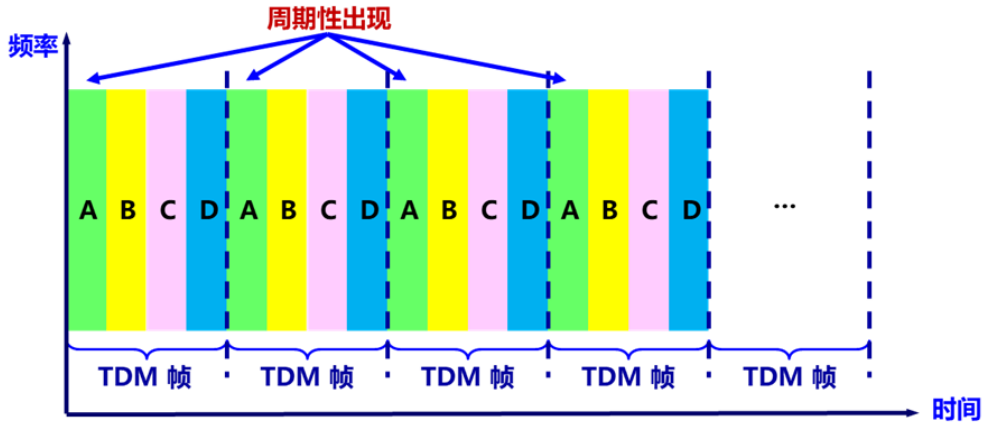
3、时分复用 TDM (Time Division Multiplexing)

（1）将时间划分为一段段等长的时分复用帧（TDM 帧）。

（2）每一个时分复用的用户在每一个 TDM 帧中占用固定序号的时隙。

（3）每一个用户所占用的时隙周期性地出现（其周期就是 TDM 帧的长度）。

（4）所有用户在不同的时间占用同样的频带宽度。

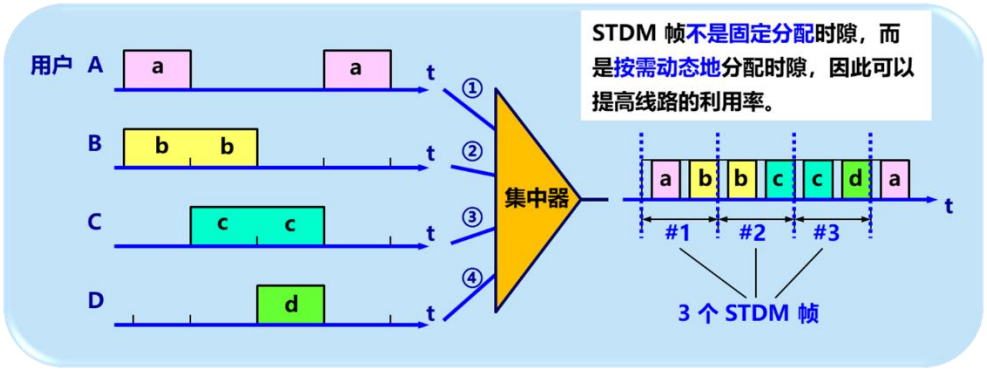


例题 4：FDM 和 TDM 的主要区别是什么？

解：频分复用 FDM：所有用户在同样的时间占用不同的带宽（即频带）资源。

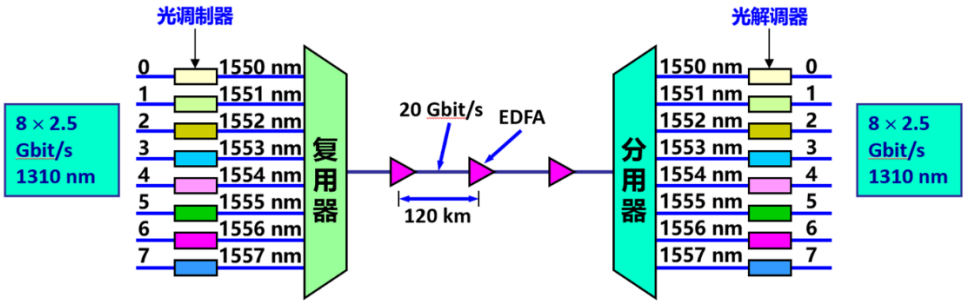
时分复用 TDM：所有用户在不同的时间占用同样的频带宽度。

4、统计时分复用 STDM (Statistic TDM)



5、波分复用 WDM (Wavelength Division Multiplexing)

光的频分复用。使用一根光纤来同时传输多个光载波信号。



6、码分复用 CDM (Code Division Multiplexing)

（1）每一个用户可以在同样的时间使用同样的频带进行通信。

（2）各用户使用经过特殊挑选的不同码型，因此不会造成干扰。

（3）当码分复用信道被多个不同地址的用户所共享时，就称为码分多址 CDMA (Code Division Multiple Access)。

7、CDMA 工作原理

（1）将每一个比特时间划分为 m 个短的间隔，称为码片 (chip)。

（2）为每个站指派一个唯一的 m bit 码片序列。

发送比特 1：发送自己的 m bit 码片序列。

发送比特 0：发送该码片序列的二进制反码。

（3）按照惯例，码片中的 0 记为-1，而 1 记为+1。

例题 5：指派给 S 站的 8 bit 码片序列是 00011011。那么，当 S 发送比特 1 时，它发送的序列是？当 S 发送比特 0 时，它发送的序列是？

解：已知，发送比特 1：发送自己的 m bit 码片序列。发送比特 0：发送该码片序列的二进制反码。因此:

当 S 发送比特 1 时，它发送的序列是 00011011

当 S 发送比特 0 时，它发送的序列是 11100100

（4）每个站分配的码片序列：各不相同，且必须互相正交 (orthogonal)。

正交：向量 S 和 T 的规格化内积 (inner product) 等于 0：

$$S \cdot T = \frac{1}{m} \sum_{i=1}^{m} SiTi = 0$$

任何一个码片向量和该码片向量自己的规格化内积都是 1 。

一个码片向量和该码片反码的向量的规格化内积值是 –1。

例题 6：常用的信道复用技术有哪些？

解：常用的信道复用技术有频分复用、时分复用、统计时分复用、码分复用和波分复用。

例题 7：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）。请问哪个站发送了数据？发送数据的站发送的是 1 还是 0？

解：A 和 D 发送 1，B 发送 0，而 C 未发送数据。

（三）宽带接入技术

1、ADSL：非对称数字用户线技术(Asymmetric Digital Subscriber Line)

（1）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。

（2）ADSL 技术把 0~4 kHz 低端频谱留给传统电话使用，而把原来没有被利用的高端频谱留给用户上网使用。

（3）非对称：下行（从 ISP 到用户）带宽远大于上行（从用户到 ISP）带宽。

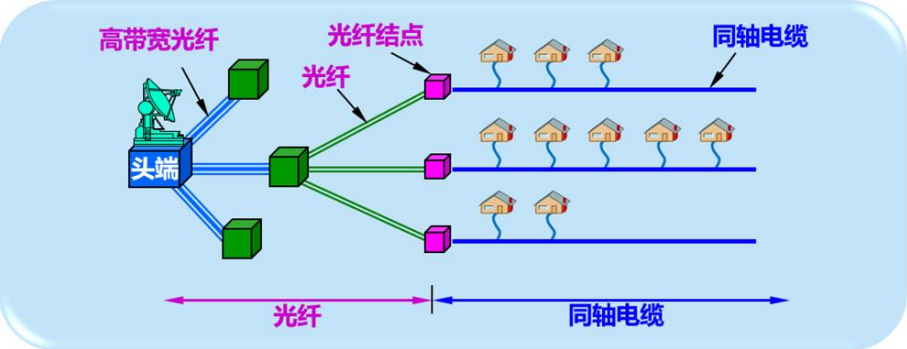
ISP：互联网服务提供者（商）

2、光纤同轴混合网（HFC 网）

（1）HFC (Hybrid Fiber Coax) 网基于有线电视网 CATV 网。

（2）改造：把原有线电视网中的同轴电缆主干部分改换为光纤。

（3）利用 HFC 网接入互联网，需要电缆调制解调器（cable modem）。



3、FTTx 技术

（1）代表多种宽带光纤接入方式。

（2）FTTx 表示 Fiber To The…（光纤到…），例如：

光纤到户 FTTH (Fiber To The Home)：在光纤进入用户的家门后，才把光信号转换为电信号。

光纤到大楼 FTTB (Fiber To The Building)

光纤到办公室 FTTO (Fiber To The Office)

光纤到桌面 FTTD (Fiber To The Desk) 等。

（3）光配线网 ODN (Optical Distribution Network)：位于光纤干线和广大用户之间。

（4）无源的光配线网常称为无源光网络 PON (Passive Optical Network)。

光配线网采用波分复用，上行和下行分别使用不同的波长。

（5）最流行的两种 PON：

以太网无源光网络 EPON (Ethernet PON) ：兼容性好，成本低，扩展性强，管理方便。

吉比特无源光网络 GPON (Gigabit PON)：可承载多业务，成本较高，但总体性能好。

例题 8：什么是 GPON 和 EPON？

解：最流行的两种无源光网络：以太网无源光网络 EPON (Ethernet PON)和吉比特无源光网络 GPON (Gigabit PON)。

第三章 数据链路层

（一）点对点信道

1.数据链路和帧

链路（link）：从一个节点到相邻节点的一段物理线路，中间没有任何其他的交换节点。链路只是一条路径的组成部分。

数据链路（data link）：既包含物理线路也包含必要的通信协议，将实现协议的软件和硬件加到链路上就构成了数据链路。

帧是点对点信道的数据链路层的协议数据单元。网络层的协议数据单元是 IP 数据报，又称分组。

例题 1：链路就是从 _____到_____的一段物理线路；数据链路既包含物理线路也包含必要的_____。

解：一个节点；相邻节点；通信协议。

2、点对点信道的数据链路层在通信时的主要步骤：

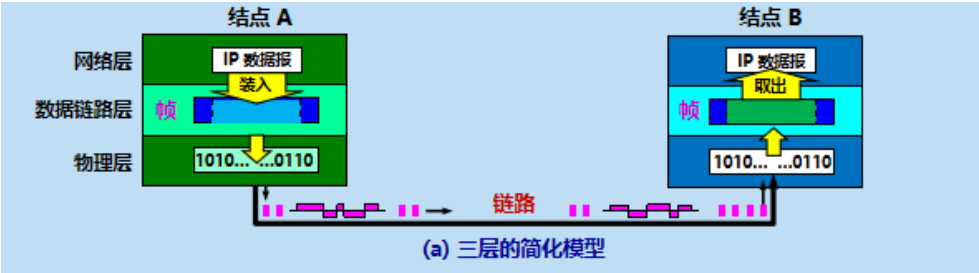
结点 A 的数据链路层把网络层交下来的 IP 数据报加上首部和尾部封装成帧。

结点 A 把封装好的帧发送给结点 B。

结点 B 对接收到的帧进行差错检验，若无差错，从帧中提取出 IP 数据报上交给网络层，若有差错丢弃这个帧。

例题 2：数据链路层把网络层交下来的 IP 数据报加上首部和尾部的操作叫做 _____。

解：封装成帧。



（二）数据链路层的基本问题

1、三个基本问题

（1）封装成帧：在数据前后加上帧头和帧尾后，接收端的数据链路层接收到物理层传来的比特流才能根据帧头帧尾识别一个帧。

（2）透明传输：防止数据中出现与帧定界符相同的比特组合导致出现帧定界错误，而在发送端数据中的帧定界符前加入转义字符，在接收端把数据中多余的转义字符去掉。这样就可以使数据按照原样无差错地通过数据链路层，即实现透明传输。

（3）差错检验：通过循环冗余检验 CRC 识别比特差错，从而节约网络资源，使错误数据到达节点或主机的数据链路层就能被尽快检测到，而不是到达主机后由主机的高层软件进行检测。这样就能使错误数据尽少的占用通信资源。

例题 3：数据链路层的三个基本问题是什么？为什么都必须加以解决？

解：封装成帧： 在数据前后加上帧头和帧尾后，接收端的数据链路层接收到物理层传来的比特流才能根据帧头帧尾识别一个帧。

透明传输：防止数据中出现与帧定界符相同的比特组合导致出现帧定界错误，而在发送端数据中的帧定界符前加入转义字符，在接收端把数据中多余的转义字符去掉。这样就可以使数据无差错地通过数据链路层，即实现透明传输。

差错检验: 为了节约网络资源，使错误数据到达节点或主机的数据链路层就能被尽快检测到，而不是到达主机后由主机的高层软件进行检测。这样就能使错误数据尽少的占用通信资源。

（三）点对点协议 PPP

1、PPP 协议（Point-to-Point Protocol）的特点

PPP 协议是用户和 ISP 通信时使用的数据链路层协议。

（1）简单 ——首要要求。

（2）封装成帧 —— 必须规定特殊的字符作为帧定界符。

（3）透明性 —— 必须保证数据传输的透明性。

（4）多种网络层协议 —— 能够在同一条物理链路上同时支持多种网络层协议。

（5）多种类型链路 —— 能够在多种类型的链路上运行。

（6）差错检测 —— 能够对接收端收到的帧进行检测，并立即丢弃有差错的帧。

（7）检测连接状态 —— 能够及时自动检测出链路是否处于正常工作状态。

（8）最大传送单元 —— 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，促进各种实现之间的互操作性。

（9）网络层地址协商 —— 必须提供一种机制使通信的两个网络层实体能够通过协商知道或能够配置彼此的网络层地址。

（10）数据压缩协商 —— 必须提供一种方法来协商使用数据压缩算法。

例题 4：PPP 协议的主要特点是什么？

解：（1）简单 ——首要要求。

（2）封装成帧 —— 必须规定特殊的字符作为帧定界符。

（3）透明性 —— 必须保证数据传输的透明性。

（4）多种网络层协议 —— 能够在同一条物理链路上同时支持多种网络层协议。

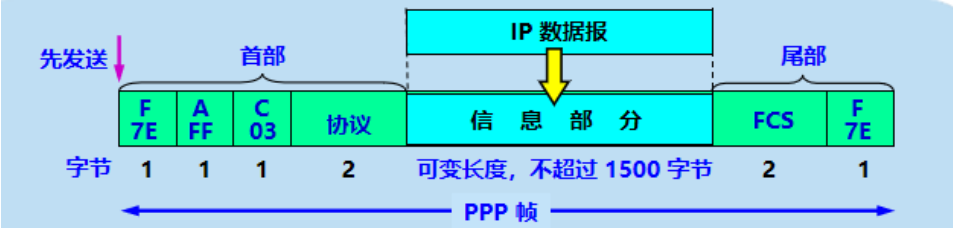
（5）多种类型链路 —— 能够在多种类型的链路上运行。

（6）差错检测 —— 能够对接收端收到的帧进行检测，并立即丢弃有差错的帧。

2、PPP 协议的帧格式——各字段的含义

PPP 的首部和尾部分别为 4 个字段和 2 个字段。

首部的第一个字段和尾部的第二个字段都是标志字段 F，规定为 0x7E，它标志着一个帧的开始或结束。两个连续的帧之间只需要一个 F，如果连续出现两个标志字段，表示这是一个空帧，应该丢弃。第四个字段是 2 字节的协议字段，它表明了信息部分的数据类型（可能是 IP 数据报也可能是其他类型的数据）。尾部的第一个字段是帧检验序列 FCS。



字节填充

当 PPP 用在异步传输时，使用字节填充，转义符为 0x7D。

（1）把信息字段中出现的每一个 0x7E 字节转变为 2 字节序列（0x7D，0x5E）。

（2）把信息字段中出现的每一个 0x7D 字节转变为 2 字节序列（0x7D，0x5D）。

（3）若信息字段中出现 ASCⅡ码的控制字符（即数值小于 0x20 的字符），则在该字符前加入一个 0x7D 字节。

例题 5：一个 PPP 帧的数据部分是 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）？

解：7E FE 27 7D 7D 65 7E

零比特填充

当 PPP 用在同步传输链路时，采用零比特填充法。

例题 6：PPP 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？若接收端收到的 PPP 帧的数据部分是 00011101111101111110110，试问删除发送端加入的零比特后会变成怎样的比特串？

解：零比特填充后：011011111011111000

删除零比特后：00011101111111111110

（四）使用广播信道的数据链路层

1、局域网的数据链路层

局域网的最主要特点：网络为一个单位所拥有，且地理范围和站点数目都有限。

以太网是局域网的一种，绝大多数局域网都是以太网。双绞线是局域网中的主流传输媒体。

实现共享信道有两种方法：

（1）静态划分信道，如频分复用、时分复用、码分复用等，但不适合局域网。

（2）动态媒体接入控制，又称多点接入。特点是信道并非在用户通信时固定分配给用户。

随机接入：特点是用户可以随机地发送消息。如果有两个用户同时发送，在共享媒体上就会产生碰撞，是发送失败。这时就需要解决碰撞的网络协议，即 CSMA/CD 协议。

受控接入：特点是用户不能随机发送信息而必须服从一定的控制。

适配器的作用：

计算机与外界局域网的连接是通过适配器进行的，适配器以前又称网卡。

适配器的一个重要功能就是进行数据串行传输和并行传输的转换。

适配器实现的功能包含了数据链路层和物理层两个层次的功能。

封装成帧、透明传输、差错检测等功能都是由适配器完成的。

适配器工作在 TCP/IP 协议中的网络接口层。

例题 7：网络适配器工作在_____。

解：TCP/IP 协议中的网络接口层。（OSI 中的数据链路层和物理层）

2、CSMA/CD 协议

（1）多点接入：多点接入说明是总线型网络，许多计算机以多点接入的方式连接在一根总线上。协议的实质就是载波监听和碰撞检测。

（2）载波监听：使用电子技术检测信道上有没有其他计算机也在发送。不管是发送前还是发送中，每个站都要不停地检测信道。

（3）碰撞检测：边发送边监听。如果几个站同时发送数据，总线上的信号电压变化会增大，就表明发生了碰撞。这时就立即停止发送。

在使用 CSMA/CD 协议时，不能同时发送和接收，因此使用 CSMA/CD 协议的以太网只能进行半双工通信（双向交替通信）。

例题 8：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 10Mb/s 以太网集线器；

(2) 10 个站都连接到一个 100Mb/s 以太网集线器;

(3) 10 个站都连接到一个 10Mb/s 以太网交换机。

解：集线器实质上是一个多端口中继器，作用是将信号整形放大转发到除输入端口外的所有端口，所以 1，2 需要共享带宽，而交换机相当于一个多端口网桥，所以每条链路独占带宽。

(1) 10 个站都连接到一个 10Mb/s 以太网集线器: 1mb/s

(2) 10 个站都连接到一个 100mb/s 以太网集线器: 10mb/s

(3) 10 个站都连接到一个 10mb/s 以太网交换机: 10mb/s

第四章 网络层

（一）网络层的两种服务

1、面向连接服务和无连接服务

面向连接：用于打电话的传统电信网使用面向连接的通信方式，它先建立连接预留出网络资源（建立一条虚电路），然后再传送信息，提供的是可靠传输的服务。

无连接：互联网采用的是无连接的方式，发送分组时不需要建立连接。

例题 1：网络层向上提供的服务有哪两种？试比较其优缺点。

解：面向连接的和无连接。

（1）面向连接：优点：通过虚电路发送分组，分组只用填写虚电路编号，分组开销较小。

缺点：一个节点出故障，所有通过该节点的虚电路均不能工作；需要昂贵复杂的网络设备。

（2）无连接：优点：网络层不提供可靠传输，路由器简单，运行方式灵活，能适应多种应用。

缺点：分组独立发送，可能出错、丢失重复或失序。

（二）网际协议 IP

1、虚拟互连网络

根据所在层次，可以将中间设备分为以下四种：

物理层使用的叫转发器。

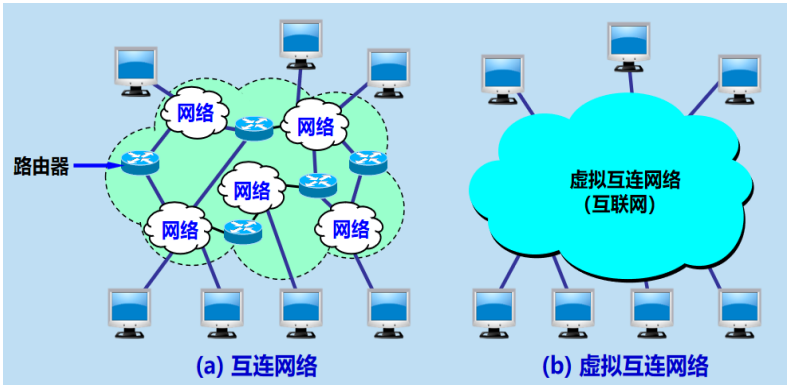
数据链路层使用的叫网桥或桥接器。

网络层使用的叫路由器。

网络层以上使用的叫网关。

由于参加互连的计算机网络都使用相同的网际协议 IP（Internet Protocol），

因此可以将其视为一个虚拟互连网络（internet）。



例题 2：作为中间设备，转发器、网桥、路由器和网关有何区别？

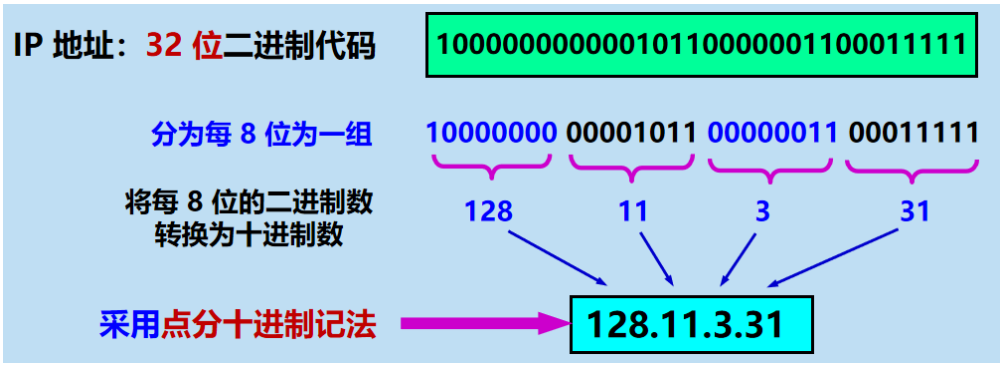
解：物理层使用的叫转发器；数据链路层使用的叫网桥或桥接器；

网络层使用的叫路由器；网络层以上使用的叫网关。

2、分类的 IP 地址

IP 地址就是给互联网上每一台主机或路由器的每一个接口分配一个全世界唯一的 32 位的标识符。

IP 地址 ＝{<网络号>，<主机号>}，它既指明了主机接口，也指明了所在网络。



例题 3：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

解：从将每个地址块的第三个字节转换为二进制，分别是：

212.56.10000100.0

212.56.10000101.0

212.56.10000110.0

212.56.10000111.0

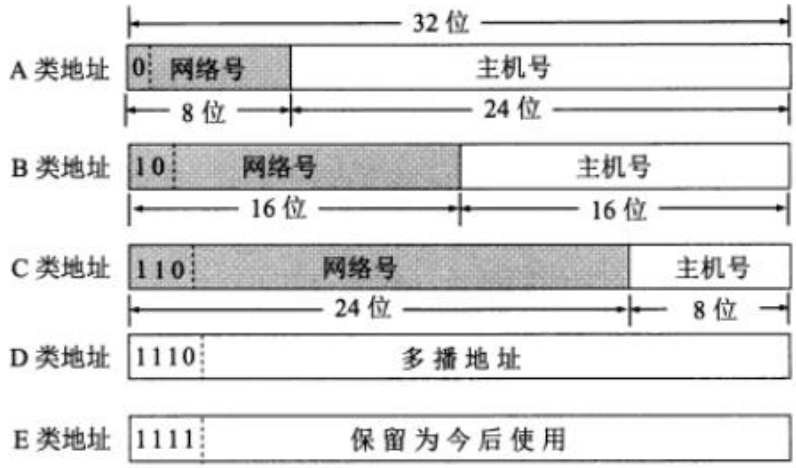
所以聚合后的地址块为 212.56.132.0/22。

分类的 IP 地址分为以下 5 类：

A 类、B 类、C 类都是单播地址，是最常用的。

D 类是用于多播（一对多通信）。

E 类地址保留为以后用。



分类是考虑到了不同网络间的差异性，有的网络主机很多，有的则很少。

IP 地址具有如下重要特点：

（1）每一个 IP 地址都是由网络号和主机号两部分组成，是一种分等级的地址结构。

（2）IP 地址是标志一台主机（或路由器）和一条链路的接口。如果一台主机同时连接到两个网络，它就有两个 IP 地址。

（3）互联网中，一个网络指的是具有相同网络号的主机的集合。所以用转发器或交换机连接起来的若干局域网仍是一个网络。

（4）IP 地址中，所有分配到网络号的网络都是平等的，不管它的范围多大或多小。

例题 4：IP 地址由_____和_____两部分组成，是一种_____

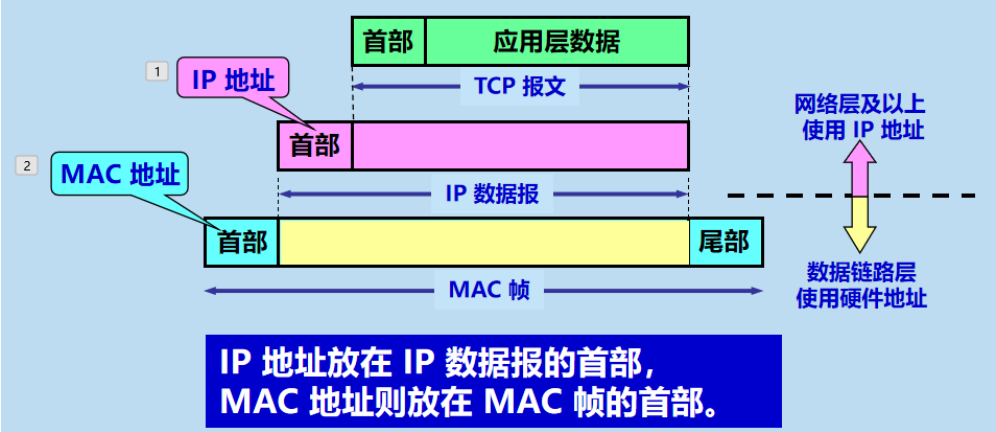
的地址结构。

解：网络号；主机号；分等级。

3、IP 地址与 MAC 地址

硬件地址（又称物理地址、MAC 地址）是数据链路层和物理层使用的地址。MAC 帧传送时使用的源地址和目的地址都属于硬件地址，放在 MAC 帧的首部。

IP 地址是网络层和以上各层使用的地址，是一种逻辑地址，放在 IP 数据报的首部。



例题 5：试说明 IP 地址与 Mac 地址的区别。为什么要使用这两种不同的地址？

解：解：IP 地址：被称为虚拟地址、软件地址或逻辑地址，IP 地址是网络层和以上各层使用的地址，是一种逻辑地址。

MAC 地址：固化在网卡的 ROM 中，称为硬件地址或物理地址。MAC 地址是数据链路层使用的地址。

IP 地址放在 IP 数据报的首部，而 MAC 地址则放在 MAC 帧的首部。

全世界存在着各式各样的网络，它们使用不同的 MAC 地址，要使这些异构网络能够互相通信就必须进行非常复杂的 MAC 地址转换工作，因此由用户或用户主机来完成这项工作几乎是不可能的事。然而 IP 编址解决了这个问题，连接到互联网的主机只需各自拥有一个 IP 地址，它们之间的通信就可以像连接在同一个网络上那样简单方便，即便必须多次调用 ARP 来找到 MAC 地址，但这个过程都是由计算机软件自动进行的，用户看不见。

4、IP 数据报的格式

（1）版本。占 4 位，通信双方使用的 IP 协议的版本必须一致。

（2）首部长度。 占 4 位，最大值是 15，注意其单位是 4 字节，也就是首部最大长度为 15*4=60 字节。首部长度必须是 4 字节的整数倍。因此可选字段后面还有一个填充字段。

（3）区分服务。占 8 位，根据字段的数值提供不同等级的服务质量。

（4）总长度。占 16 位，最大值是 65535，是首部和数据部分的长度和，单位是字节。

（5）标识 (identification)。占 16 位，同一个数据报的不同分片标识相同，因此接收方能根据标识将不同分片重装为原本的数据报。

（6）标志（flag）。占 3 位。最低位 MF=1 表示后面还有分片，MF=0 表示这是最后一个分片。中间位 DF=1 表示不能分片，为 0 表示可以分片。首位没有含义。

（7)片偏移。占 13 位。片偏移指出：较长的分组分片后，某片在原分组的相对位置。单位是 8 字节，故每个分片的长度是 8 字节的整数倍。

（8）生存时间（TTL)。占 8 位。表明数据报在网络中的寿命。单位是跳数，指明了数据报在互联网中至多可经过多少个路由器。

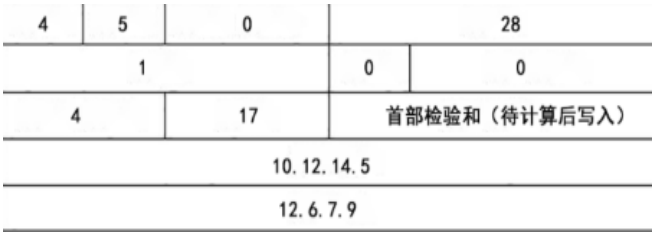
（9）协议。占 8 位。指明了数据报携带的数据使用了哪种协议。

（10）首部检验和。占 16 位。这个字段只检验首部，不包括数据部分。数据报每经过一个路由器，路由器就要重新计算一下首部检验和。

（11）源地址。占 32 位。

（12）目的地址。占 32 位。

例题 6：设 IP 数据报使用固定首部，其各字段的具体数值如图所示（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）。



0100 0101 0000 0000
0000 0000 0001 1100
0000 0000 0000 0001
0000 0000 0000 0000
0000 0100 0001 0001
0000 0000 0000 0000
0000 1010 0000 1100
0000 1110 0000 0101
0000 1100 0000 0110
0000 0111 0000 1001

解：最终结果为 1000 1011 1011 0001

（三）网际控制报文协议 ICMP

1、ICMP 报文的种类

ICMP (Internet Control Message Protocol) 允许主机或路由器报告差错情况和提供有关异常情况的报告。ICMP 是互联网的标准协议。

ICMP 报文种类	类型的值	ICMP报文的类型
差错报告报文	3	终点不可达
	11	时间超过
	12	参数问题
	5	改变路由 (Redirect)
询问报文	8 或 0	回送 (Echo) 请求或回答
	13 或 14	时间戳 (Timestamp) 请求或回答

ICMP 差错报告报文共有四种：

（1）终点不可达：当路由器或主机不能交付数据报时就向源点发送此报文。

（2）时间超过：路由器收到生存时间为 0 的报文时，除丢弃该数据报外，还要向源点发送此报文。当终点在约定时间内未收到一个数据报的全部分片时，就丢弃已收到的所有分片，并向源点发送此报文。

（3）参数问题：当路由器或目的主机收到的数据报的首部中有的字段值不正确时，就丢弃该数据报并发送此报文。

（4）改变路由（重定向）：路由器把此报文发送给主机，以告诉主机下次将数据报发给另外的路由器。

ICMP 差错报告报文的数据字段是固定格式的：把收到的需要进行差错报告的 IP 数据报的首部和数据字段的前 8 个字节提取出来作为 ICMP 报文的数据部分。

ICMP 询问报告报文共有两种：

（1）回送请求报文或回送回答：回送请求报文是由主机或路由器向一个特定目的主机发出的询问。收到此报文的主机必须给源主机发送 ICMP 回送回答报文。

（2）时间戳请求报文或时间戳回答：时间戳请求报文是请某台主机或路由器回答当前的日期和时间。通过它可以进行时钟同步和时间测量。

2、ICMP 的应用举例

ICMP 的一个重要应用是进行分组网间探测 PING（Packet InterNet Groper），以测试两台主机之间的连通性。PING 使用了 ICMP 回送请求和回送回答报文。它会连续发送 4 条回送请求报文。

使用方法：在 Windows 的 Dos 窗口中键入 ping hostname 即可测试本机与主机 hostname 之间的连通性，hostname 应该是某个主机的 IP 地址或域名。

```
C:\Documents and Settings\XXR>ping mail.sina.com.cn

Pinging mail.sina.com.cn [202.108.43.230] with 32 bytes of data:

Reply from 202.108.43.230: bytes=32 time=368ms TTL=242
Reply from 202.108.43.230: bytes=32 time=374ms TTL=242
Request timed out.
Reply from 202.108.43.230: bytes=32 time=374ms TTL=242

Ping statistics for 202.108.43.230:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 368ms, Maximum = 374ms, Average = 372ms
```

（四）IPv6

1、IPv6 的基本首部

首部长度：固定的 40 字节，称为基本首部。

首部字段数：只有 8 个。

与 IPv4 相比，IPv6 对首部的主要更改：

• 取消了首部长度字段； • 取消了服务类型字段； • 取消了总长度字段，改用有效载荷长度字段；	• 把 TTL 字段改称为跳数限制字段； • 取消了协议字段，改用下一个首部字段； • 取消了检验和字段； • 取消了选项字段，而用扩展首部来实现选项功能。

2、IPv6 的地址

（1）单播：点对点通信。

（2）多播：一点对多点的通信。

（3）任播：任播的终点是一组计算机，但是数据报只交付其中一个，一般是距离最近的一个。

IPv6 地址有 128 位，采用冒号十六进制计法：每 16 位用 16 进制表示并用冒号隔开，因此共分为了 8 段，每段是一个不超过 4 位的 16 进制数。

零压缩 (zero compression)：一串连续的零可以用一对冒号取代。在任一地址中，只能使用一次零压缩。

例如：FF05:0:0:0:0:0:0:B3 可压缩为 FF05::B3。

例题 7：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

解：（1）: :F53:6382:AB00:67DB:BB27:7332

（2）: :4D:ABCD

(3) ::AF36:7328:0:87AA:398

(4) 2819:AF::35:CB2:B271

3、从 IPv4 向 IPv6 过渡

(1)双协议栈

使一部分主机或路由器装有双协议栈：一个 IPv4 和一个 IPv6，当它与 IPv6 主机通信时使用 IPv6 地址，与 IPv4 主机通信时使用 IPv4 地址。

双协议栈使用域名系统 DNS 来查询目的主机使用哪一种地址。

(2)隧道技术

当源主机和目的主机都采用 IPv6 时，中间经过的网络有可能是 IPv4 网络。

在 IPv6 数据报要进入 IPv4 网络时，把 IPv6 数据报作为数据部分封装到 IPv4 数据报中，等离开 IPv4 网络后在把数据部分取出来。

例题 8：从 IPv4 向 IPv6 过渡的方法分别是_____和_____。

解：双协议栈；隧道技术。

第五章 运输层

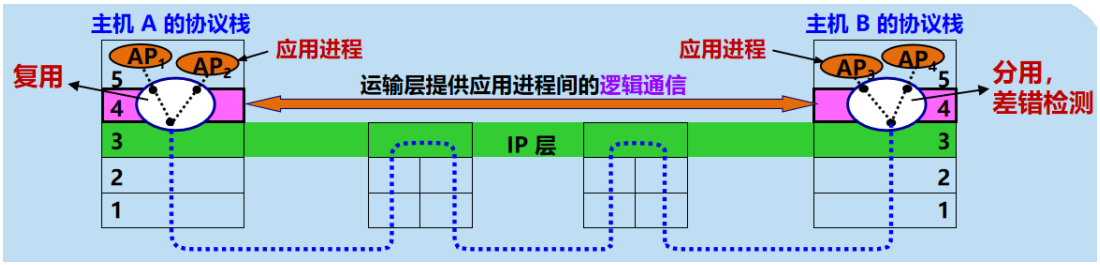
（一）运输层协议概述

1、进程之间的通信

网络层为主机之间提供通信，运输层为应用进程提供端到端的逻辑通信。

通信的真正端点是主机中的进程，即应用进程之间的通信是端到端的通信。

运输层的复用和分用：发送方的不同进程通过不同的端口号使用同一个运输层协议，接收方的运输层则把收到的报文根据端口号分发给不同的进程。



例题 1：网络层为_____之间提供通信，运输层为_____提供_____的 _____通信。

解：主机；应用进程；端到端；逻辑。

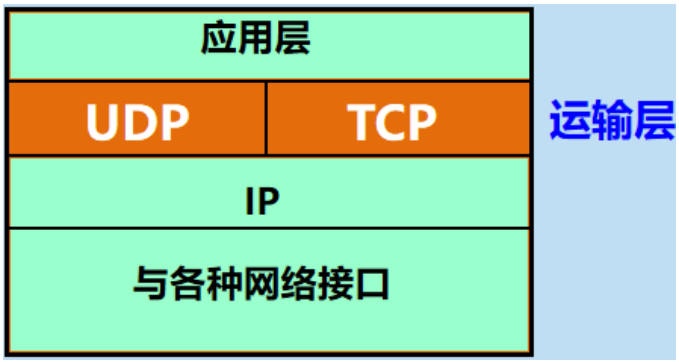
2、运输层的两个主要协议

（1）用户数据报协议 UDP (User Datagram Protocol)

- 传送数据之前不需要先建立连接。
- 收到 UDP 报后，不需要给出任何确认。
- 不提供可靠交付，但是一种最有效的工作方式。

（2）传输控制协议 TCP (Transmission Control Protocol)

- 提供可靠的、面向连接的运输服务。
- 不提供广播或多播服务。
- 开销较多。

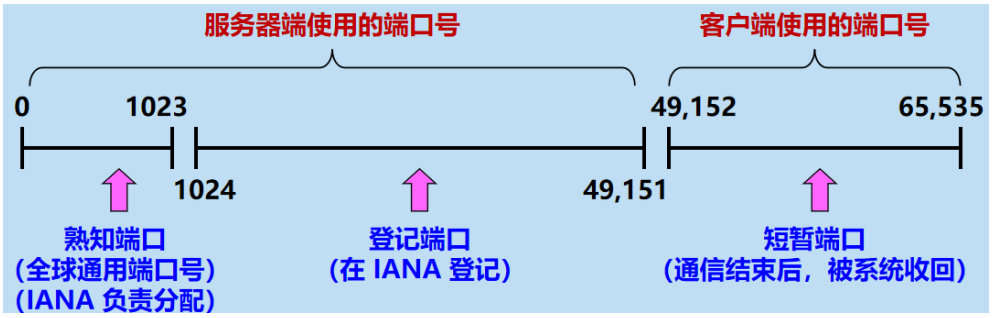


3、运输层的端口

运输层使用 16 位（即两字节）端口号来标志一个端口，允许有 65,535 个不同的端口号。端口号用来标志本计算机应用层中的不同进程。

与路由器上的硬件端口不同，这里的端口是软件端口，作为交互的地址使用。

两个计算机中的进程要互相通信，不仅必须知道对方的端口号，而且还要知道对方的 IP 地址。



例题 2：端口的作用是什么?为什么端口要划分为三种?

解：端口的作用是对 TCP/P 体系的应用进程进行统一的标志，使运行不同操作系统的计算机的应用进程能够互相通信。

熟知端口，数值一般为 0-1023，标记常规的服务进程；

登记端口号，数值为 1024-49151，标记没有熟知端口号的非常规的服务进程。

避免端口号重复，无法区分应用进程。

（二）用户数据报协议 UDP

1、UDP 概述

（1）UDP 只在 IP 的数据报服务之上增加了一些功能：复用和分用；差错检测。

（2）UDP 的主要特点：

① 无连接。发送数据之前不需要建立连接。

② 使用尽最大努力交付。即不保证可靠交付。

③ 面向报文。UDP 一次传送和交付一个完整的报文。

④ 没有拥塞控制。网络出现的拥塞不会使源主机的发送速率降低。很适合多媒体通信的要求。

⑤ 支持一对一、一对多、多对一、多对多等交互通信。

⑥ 首部开销小，只有 8 个字节。

例题 3：某个应用进程使用运输层的用户数据报 UDP，然后继续向下交给 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?

解：不可以。

IP 数据报承担了主机寻址功能，可以找到目的主机，却无法找到目的进程，分组还是停留在网络节点中，而无法到达通信实体。

UDP 提供了对进程的分用和复用功能，以及对数据报的差错检测。

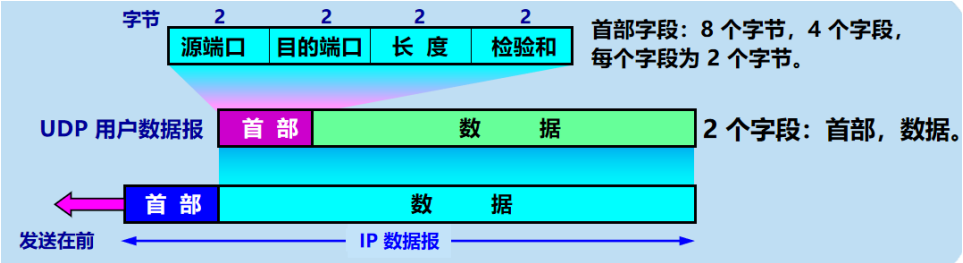
2、UDP 的首部格式

(1) 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。

(2) 目的端口：目的端口号。终点交付报文时必须使用。

(3) 长度：UDP 用户数据报的长度，其最小值是 8（仅有首部）。

(4) 检验和：检测 UDP 用户数据报在传输中是否有错。有错就丢弃。



例题 4：一个 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给服务器还是从服务器发送给客户?

解：源端口: 0*16^3+6*16^2+3*16+2*16^0 = 1586 (十进制)

目的端口: 0*16^3+0*16^2+4*16+5*16^0 = 69 (十进制)

用户数据报总长度: 0*16^3+0*16^2+1*16+12*16^0 = 28(十进制)

数据部分长度 = 总长度- 首部长度 = 20 (字节)

目的端口为 69<1023(0~1023 为款知端口)，所以数据报是从客户端发送给服务器的。

（三）传输控制协议 TCP 概述

1、TCP 最主要的特点

（1）面向连接：使用 TCP 前要先建立连接，通信完后要释放连接。

（2）点对点通信。

（3）可靠传输：无差错、不丢失、无重复、按序到达。

（4）全双工通信：TCP 的两端都设有发送缓存和接收缓存。发送时，应用程序把数据放到 TCP 的发送缓存后，TCP 在合适的时候把数据发送出去。接收时，TCP 把收到的数据放入接收缓存，应用进程合适时读取缓存中的数据。

（5）面向字节流：“流”是流入到进程或从进程流出的字节序列。TCP 把应用进程交下来的数据看成一串无结构的字节流。

2、TCP 的连接

IP 地址加上端口号称为套接字，套接字就是 TCP 连接的端点。

套接字不是应用进程，也不是端口。

套接字 socket = (IP 地址 ： 端口号)

例题 5：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 报文段的首部中的源端口和目的端口分别是什么?

解：源端口是 n，目的端口是 m。

（四）TCP 的流量控制和拥塞控制

1、利用滑动窗口实现流量控制

流量控制是为了让发送方的发送速率不要太快，要让接收方来得及接收。

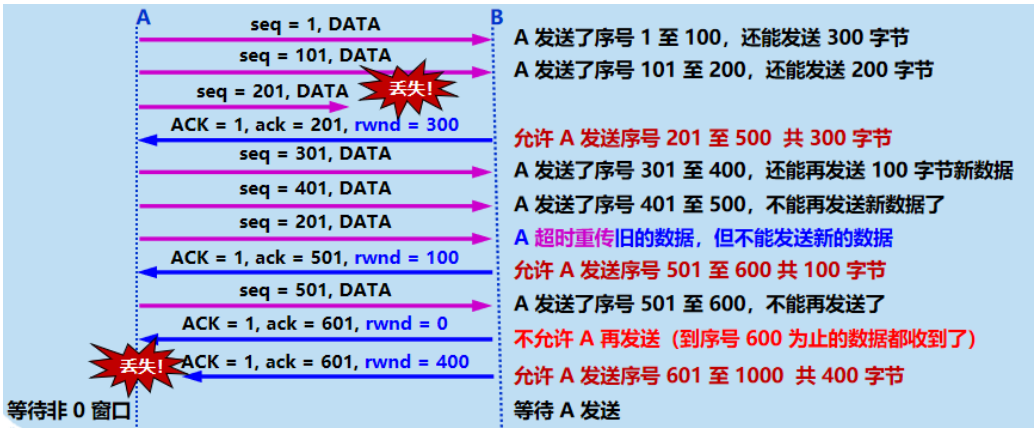
流量控制是通过滑动窗口实现的。接收方会把接收窗口的大小放到给发送方的报文的窗口字段中。

发送方的发送窗口不能超过接收方给出的窗口字段的数值。

TCP 的窗口单位是字节，不是报文段。

例题 6：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 有 1460 字节。在 TCP 的序号不重复使用的条件下，L 的最大值是多少?

解：可能的序号共 232=4GB=4294967296 个。TCP 的序号是数据字段中每一个字节的编号，而不是每一个报文段的编号。因此，这一小题与报文段的长度无关，因此用不到题目给出的 MSS 值，这个文件 L 的最大值就是可能的序号数，即 4294967296 字节。



持续计时器（persistence timer）——打破死锁僵局。

2、TCP 的传输效率

糊涂窗口综合征：每次仅发送一个字节或很少几个字节的数据时，有效数据传输效率变得很低的现象。

使用 Nagle 算法：

让接收方等待一段时间，使得或者接收缓存已有足够空间容纳一个最长的报文段，或者等到接收缓存已有一半空闲的空间。只要出现这两种情况之一，接收方就发出确认报文，并向发送方通知当前的窗口大小。

3、拥塞控制的一般原理

拥塞：在某段时间，若对网络中某资源的需求超过了该资源所能提供的可用部分，网络的性能明显变坏。

关系式：Σ 对资源需求 ＞ 可用资源

原理：

拥塞控制的前提是网络能够承受现有的网络负荷。

实践证明，拥塞控制是很难设计的，因为它是一个动态问题。

分组的丢失是网络发生拥塞的征兆，而不是原因。

在许多情况下，甚至正是拥塞控制本身成为引起网络性能恶化、甚至发生死锁的原因。

例题 7：流量控制和拥塞控制的最主要的区别是什么？

解：拥塞控制：防止过多的数据注入到网络中，避免网络中的路由器或链路过载。是一个全局性的过程，涉及到所有的主机、路由器，以及与降低网络传输性能有关的所有因素。

流量控制：抑制发送端发送数据的速率，以使接收端来得及接收。点对点通信量的控制，是个端到端的问题。

4、TCP 的拥塞控制方法

TCP 的拥塞控制采取了慢开始、拥塞避免、快重传、快恢复四种算法。

这种方法是基于窗口的拥塞控制。发送方维持一个拥塞窗口，并让自己的发送窗口等于拥塞窗口（实际上发送窗口取拥塞窗口和接收窗口中的较小者）。

发送窗口大小不仅取决于接收方窗口，还取决于网络的拥塞状况。

判断网络拥塞的依据是出现超时。当出现拥塞就使拥塞窗口减小，反之增大。

例题 8：发送窗口的大小取决于流量控制还是拥塞控制?

解：当接收窗口小于拥塞窗口时，发送窗口的大小取决于流量控制，即取决于接收端的接收能力；当拥塞窗口小于接收窗口时，则发送窗口的大小取决于拥塞控制，即取决于整个网络的拥塞状况。

（1）慢开始

目的：探测网络的负载能力或拥塞程度。

算法：由小到大逐渐增大注入到网络中的数据字节，即：由小到大逐渐增大拥塞窗口数值。

初始拥塞窗口一般不超过 2-4 个 SMSS（发送方最大报文段）长度。每收到一个新的确认后，就增加一次拥塞窗口。

使用慢开始算法，每经过一个传输轮次，拥塞窗口 cwnd 就会加倍。

（2）拥塞避免

拥塞避免算法是让拥塞窗口缓慢地增大，不像慢开始那样加倍增长。

当 cwnd（拥塞窗口） 大于一个界限值时，就使用拥塞避免算法，小于时就使用慢开始算法。

当出现超时，拥塞窗口就恢复初始值重新进行慢开始，且界限值减半。

（3）快重传

要求当接收方收到报文段后立即发送确认。

当接收方收到的报文段出现丢失，它后面不论收到什么报文段，发回的确认号都是对失序之前的那个报文段的确认。

当发送方连续收到 3 个对同一报文段的重复确认（表明下一个报文段未收到），就立即重传下一个报文段，这是就可以避免出现超时，使发送方误判为网络拥塞。

（4）快恢复

对于一般的超时，界限值减半，拥塞窗口直接置为初始值；对于快重传情况下，界限值减半，拥塞窗口设置为和界限值一样，以实现快恢复。

发送方的发送窗口实际设置为接收方窗口 rwnd 和拥塞窗口 cwnd 中较小的一个。

例题 9：下列哪些方法属于 TCP 的拥塞控制（　　）

A. 慢开始

B. 拥塞避免

C. 快恢复

D. 快重传

解：ABCD

第六章 应用层

（一）域名系统 DNS

1、域名系统概述

（1） 域名系统 DNS（Domain Name System） 是互联网使用的命名系统，用来把人们使用的机器名字转换为 IP 地址。

（2） DNS 是一个联机分布数据库系统，采用客户-服务器方式。

（3） 为互联网的各种网络应用提供了核心服务。

（4） 解析过程：当某一应用进程需要解析域名，就调用解析程序，成为 DNS 的一个客户，把待解析的域名放到 DNS 请求报文中，以 UDP 用户数据报方式发给本地域名服务器。本地域名服务器查找域名后把对应的 IP 地址发给该应用进程。应用进程获得 IP 地址后即可进行通信。

2、互联网的域名结构

互联网采用层次树状结构的命名方法，任何一台连接在互联网上的主机或路由器都有唯一一个域名。

域名结构：层次结构。由标号 (label) 序列组成，各标号之间用点（.）隔开，各标号分别代表不同级别的域名。

3、域名服务器

（1）根域名服务器是最重要的服务器，如果本地域名服务器无法解析域名，

首先求助于根域名服务器。根域名服务器使用了任播技术。

（2）为提高查询效率，并减轻根域名服务器的负荷和减少互联网上的 DNS 查询报文数量，域名服务器中广泛采用了高速缓存，存放最近查询过的域名信息。

例题 1：域名系统的主要功能是_____；

域名服务器中的高速缓存的作用是_____ 。

解：将域名解析为主机能识别的 IP 地址；提高查询效率，并减轻根域名服务器的负荷和减少互联网上的 DNS 查询报文数量。

（二）文件传送协议

1、FTP 概述

（1） 文件传送协议 FTP (File Transfer Protocol) 使用 TCP 的可靠运输服务，为客户-服务器模式。

（2） 简单文件传送协议 TFTP 使用 UDP 协议。

（3） FTP 和 TFTP 都属于文件共享协议中的一大类：复制整个文件。特点是要存取一个文件，就必须先获得一个本地的文件副本。要修改文件，只能对文件副本进行修改，然后将修改后的文件副本传送回到原节点。

2、FTP 的基本工作原理

（1）FTP 主要功能是减少或消除在不同操作系统下处理文件的不兼容性。

（2）一个 FTP 服务器进程可以同时为多个客户进程提供服务，每个进程包括一个主进程和若干个从属进程。主进程和从属进程是并发执行的。

（3）主进程负责接受新的请求。从属进程负责处理单个请求。

（4）文件传输时，FTP 的客户和服务器之间会建立两个并行的 TCP 连接：控制连接和数据连接，其中数据连接用于传输文件。因此 FTP 要使用两个端口号。

例题 2：下列哪些属于文件传送协议 FTP 的主要工作过程（ ）

A. 打开熟知端口 (端口号为 21) ，使客户进程能够连接上。

B. 等待客户进程发出连接请求

C. 启动从属进程来处理客户进程发来的请求。

D. 回到等待状态，继续接受其他客户进程发来的请求。

解：ABCD

3、简单文件传送协议 TFTP

（1）TFTP (Trivial File Transfer Protocol) 是一个很小且易于实现的文件传送协议。

（2）只支持文件传输，不支持交互，也不能对用户进行身份鉴别。

（3）优点：可用于 UDP 环境；代码所占的内存较小。

例题 3：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?

解：FTP 只提供文件传送的一些基本的服务，它使用 TCP 可靠的运输服务，主要功能是减少或消除在不同操作系统下处理文件的不兼容性。FTP 使用客户服务器方式。一个 FTP 服务器进程可同时为多个客户进程提供服务。FTP 的服务器进程由两大部分组成：一个主进程，负责接受新的请求；另外有若干个从属进程，负责处理单个请求 TFTP 是一个很小且易于实现的文件传送协议。

（三）万维网 WWW

1、万维网概述

（1）万维网 WWW (World Wide Web) 是一个大规模的、联机式的信息储藏所。万维网的简称是 Web。

（2）超文本指的是包含指向其他文档的链接的文本，一个超文本由多个信息源链接组成。超文本仅包含文本信息，超媒体扩充为包含图形、声音、视频等。

（3）万维网是一个分布式的超媒体系统。

例题 4：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_____。

解：404 Not Found

2、统一资源定位符 URL

（1）万维网使用统一资源定位符 URL 来标志万维网上的各种文档，每个文档有在互联网内唯一的 URL。

（2）URL 相当于指向互联网上任何可访问对象的一个指针。

（3）URL 的一般形式：<协议>://<主机>:<端口>/<路径>

协议：指出采用何种协议来获取该万维网文档，一般为 http，其次为 ftp

主机：即该主机的域名。

端口：通常都省略掉，HTTP 的默认端口号是 80。

路径：有时可省略。

（4） 输入 URL 时协议和 www 都可以省略，浏览器会自动补上。

例题 5：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传输层协议?

解：应用层协议需要的是 DNS。运输层协议需要的是 UDP (DNS 使用）和 TCP (HTTP 使用)。

3、超文本传送协议 HTTP

（1）HTTP 是面向事务的应用层协议。事务指的是一系列的不可分割的信息交换（即这些信息交换是一个整体）。

（2）万维网客户与服务器程序之间交互使用的协议是 HTTP 协议。万维网的客户就是浏览器。

（3）HTTP 本身是无连接、无状态的，使用可靠传输的 TCP 协议。

无连接：通信双方在交换 http 报文前不需要先建立 http 连接。

无状态：HTTP 服务器不记得曾经访问过的客户。

（四）简单网络管理协议 SNMP

1、网络管理的基本概念

（1）网络管理包括对硬件、软件和人力的使用、综合和协调。

（2）网络管理采用的协议就是 SNMP 协议。

（3）基本原理：要管理某个对象，就必然要给这个对象添加一些软件或硬件，但是这种添加的影响应该尽量小一些。SNMP 最重要的思想是尽量简单。

例题 6：网络管理包括对_____、_____和_____的使用、综合和协调。

解：硬件；软件；人力。

（4）SNMP 协议中，管理程序运行 SNMP 客户程序，代理程序运行 SNMP 服务器程序。被管对象上的 SNMP 服务器程序不停监听 SNMP 客户程序的请求和命令，一旦发现就执行对应动作。

（5）简单网络管理协议 SNMP 包括三部分：

SNMP 本身：SNMP 定义了管理站和代理间交换的分组格式，分组中包含各代理中的变量名和状态值。SNMP 负责读取和改变这些值。

管理信息结构 SMI：定义了一套通用的规则，包括如何定义命名对象、如何定义对象类型、如何对对象编码的规则。

管理信息库 MIB：用来在被管实体中创建命名对象。

2、管理信息结构 SMI

（1）被管对象的命名

SMI 规定所有的被管对象的名字都必须在一颗对象命名树上。

（2）被管对象的数据类型

SMI 把数据类型分为两大类：简单类型和结构化类型。

（3）编码方法

SMI 使用基本编码规则 BER 来进行数据编码，BER 指明了数据类型和值。

例题 7：什么是 SMI？它的作用是什么？

解：管理信息结构 SMI 是 SNMP 的重要组成部分。SMI 标准指明了所有的 MIB 变量必须使用抽象语法记法(ASN.1)来定义，SMI 定义了命名对象和定义对象类型的通用规则，以及把对象和对象的值进行编码的规则。

3、SNMP 的协议数据单元和报文

（1）实际上 SNMP 的操作只有两种基本的管理功能：

读操作：用 Get 报文来检测被管对象的状况。

写操作：用 Set 报文来改变被管对象的状况。

（2）SNMP 实现管理功能的方式：

使用探询操作：定期向被管设备发送探询信息，以了解其状况。

被管对象的代理检测到严重异常事件时主动向管理者发送报告。

例题 8：SNMP 使用 _____和_____两种基本操作。

解：读操作；写操作。

第七章 网络安全

（一）网络安全问题概述

1、计算机网络面临的威胁

（1）被动攻击：指攻击者从网络上窃听他人的通信内容。又称为截获/流量分析。

攻击者只是观察和分析某一个协议数据单元 PDU，以便了解所交换数据的某种性质，但不干扰信息流。

（2）主动攻击：常见的方式如下：

篡改：攻击者故意篡改网络上传送的报文。

恶意程序：计算机病毒、计算机蠕虫、特洛伊木马、逻辑炸弹、后门入侵和流氓软件等。

拒绝服务（DoS）攻击：攻击者向互联网上的某个服务器不停地发送大量分组，使该服务器无法提供正常服务，甚至完全瘫痪。

例题 1：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。

解：(1) 重放攻击：攻击者发送一个目的主机已接收过的包，来达到欺骗系统的目的，主要用于身份认证过程。

(2) 拒绝服务: DoS(Denial of Service)指攻击者向服务器不停地发送大量分组，使因特网或服务器无法提供正常服务。

(3) 访问控制：也叫做存取控制或接入控制。必须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所编写的一段程序。如计算机病毒、

特洛伊木马等。

2、安全的计算机网络

（1）机密性：只有信息的发送方和接收方才能懂得所发送信息的内容。是网络安全通信的最基本的内容，也是对付被动攻击必须具备的功能。需要使用各种密码技术。

（2）端点鉴别：鉴别信息的发送方和接收方的真实身份。主要用来应对主动攻击。

（3）信息的完整性：信息的内容未被篡改过。主要用来应对主动攻击。

鉴别同时包含了端点鉴别和报文完整性。

（4）运行的安全性：系统能正常运行并提供服务。访问控制 (access control) 对计算机系统的安全性是非常重要的。必须对访问网络的权限加以控制，并规定每个用户的访问权限。

例题 2：主动攻击和被动攻击的区别是什么?对于计算机网络的安全措施都有哪些?

解：主动攻击：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：观察和分析某一个协议数据单元 PDU 而不干扰信息流。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性质。这种被动攻击又称为流量分析。

对付被动攻击可采用各种数据加密技术，而对付主动攻击，则需加密技术与鉴别技术结合。

（二）两类密码体制

1、对称密钥密码体制

加密密钥与解密密钥都使用相同密钥的密码体制。

数据加密标准 DES 属于对称密钥密码体制，是一种分组密码。

- 在加密前，先对整个明文进行分组。每一个组长为 64 位。
- 然后对每一个 64 位 二进制数据进行加密处理，产生一组 64 位密文数据。
- 最后将各组密文串接起来，即得出整个的密文。

这种加密的保密性仅取决于对密钥的保密，算法是公开的。

2、公钥密码体制

又称为非对称密钥密码体制，使用不同的加密密钥与解密密钥。

公钥密码体制中加密密钥是公开的（公钥），解密密钥是保密的（私钥），加密和解密算法也是公开的。

公钥密码体制相对于对称密钥体制的优点：

（1）不需要考虑密钥分配问题：对称密钥需要安全地分配密钥。

（2）提供数字签名功能。

典型：RSA 体制，一种基于数论中的大数分解问题的体制。

例题 3：对称密钥密码体制中的加密密钥与解密密钥_____；

公钥密码体制中的加密密钥与解密密钥 _____。

解：相同；不同。

例题 4：以下哪些属于计算机网络面临的威胁（　　）

A. 截获

B. 中断

C. 伪造

D. 篡改

解：ABCD

（三）鉴别

1、报文鉴别

报文鉴别用来鉴别报文的完整性，它采用了密码散列函数。

散列函数的两个特点：

（1）输入长度可以很长，输出长度则较短且长度固定。散列函数的输出叫做散列值。

（2)不同的散列值对应不同的输入，但不同的输入可能得到相同的散列值。

密码学中的散列函数最重要的特点是：要找到两个不同的报文具有相同的散列值，在计算上是不可行的——根据散列值来求报文的逆向变换是不可能的。

散列函数的使用方法：对报文计算出散列值，将散列值附加在报文后面，将附加了散列值的整个报文加密进行发送。接收方解密后重新对报文计算散列值，如果与收到的散列值相同就没问题。

2、实体鉴别

（1）报文鉴别对每一个收到的报文都要鉴别发送者，实体鉴别只需要在整个连接的过程中鉴别一次。

（2）重放攻击

场景：A 向 B 发送带有自己身份和口令的报文，并使用对称密钥加密。B 收到报文后用对称密钥解密，鉴别 A 的身份。但是 C 可能截获 A 发出的报文并转发给 B，这样 B 就会误认为 C 是 A，之后向 C 发送了许多本该发给 A 的报文。

（3）不重数法（“一次一数”）：

可以采用一个不重复使用的大随机数来解决重放攻击。A 向 B 发送不重数（即不同会话使用不同的数），这样 C 截获后再向 B 发送，B 发现收到的是重复的，就不会被骗了。

例题 5：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?

解：（1）使用报文鉴别是为了对付主动攻击中的算改和伪造。当报文加密的时候就可以达到报文鉴别的目的，但是当传送不需要加密报文时，接收者应该能用简单的方法来鉴别报文的真伪。

（2）鉴别和保密并不相同。鉴别是要验证通信对方的确是自己所需通信的对象，而不是其他的冒充者。鉴别分为报文鉴别和实体鉴别。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)。

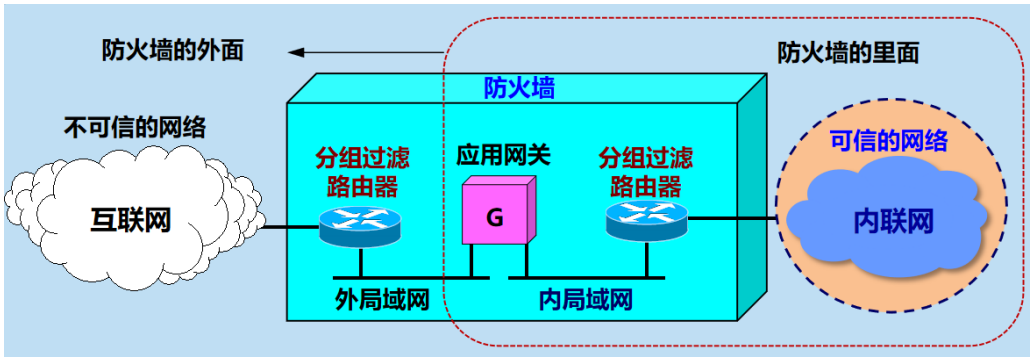
（3）报文鉴别和实体鉴别不同。报文鉴别是对每一个收到的报文都要鉴别报文的发送者，而实体鉴别是在系统接入的全部持续时间内对和自己通信的对方实体只需验证一次。

（四）系统安全

1、防火墙

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。防火墙内的网络称为可信的网络。防火墙技术包括以下两类：

（1）分组过滤路由器：它根据过滤规则（基于分组的网络层或运输层的首部信息设定）对进出内部网络的分组执行转发或丢弃。（2）应用网关：也叫代理服务器。一种网络应用需要一个应用网关。进出网络的应用程序报文都要通过应用网关，应用网关在应用层打开报文检查是否合法。



2、入侵检测系统

（1）入侵检测系统 IDS 是在入侵开始后及时检测到入侵以便尽快阻止。

（2）入侵检测系统分为两种：

基于特征的 IDS：根据已知攻击的标志性特征检测入侵。

基于异常的 IDS：根据网络流量的统计特性来检测入侵。

例题 6：试述防火墙的工作原理和所提供的功能。

解：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。

防火墙提供的功能有两个：一个是阻止，另一个是允许。阻止就是阻止某种类型的通信量通过防火墙。允许的功能与阻止的恰好相反。不过在大多数情况下防火墙的主要功能是阻止。

第八章 互联网上的音频/视频服务

（一）概述

1、多媒体信息的特点

（1）多媒体信息：内容上相互关联的文本、图形、图像、声音、动画和活动图像等所形成的复合数据信息。

（2）多媒体信息有两个特点：多媒体信息的信息量往往很大；对传输时延和时延抖动有较高要求。（边传输边播放）

（3）模拟的多媒体信号经过采样和模数转换变为数字信号，再组装成分组。这些分组的发送时间间隔是恒定的（等时的）。传统互联网中，每个分组被独立传送，到达接收端时就变成为非等时的。

（4）接收端设置适当大小的缓存。当缓存中的分组数达到一定的数量后，再以恒定速率按顺序把分组读出进行还原播放。传播时延：消除了时延的抖动，但增加了时延。

例题 1：实时数据和等时数据是一样的意思吗？为什么说因特网是不等时的？试说播放延时的作用？

解：实时数据和等时数据不是一样的意思。

模拟的音频 /视频信号只有经过数字化以后才能在因特网上传送。就是对模拟信号要经过采样和模数转换变为数字信号，然后将一定数量的比特组装成分组进行传送。这些分组在发送时的时间间隔时恒定的，但传统的因特网本身是非等时的。这是因为在时延协议的因特网中，每一个分组是独立的传送，因而这些分组在到达接收端时就变成非等时的。

播放时延的作用是消除了时延的抖动。

2、音/视频服务类型

（1）流式存储音频/视频（流媒体）：边下载边播放。

播放时并没有把“下载”的内容存储在硬盘上。

结束后，在用户的硬盘上没有留下有关播放内容的任何痕迹。

（2）流式实况音频/视频：边录制边发送、连续播放。

（3）交互式音频/视频：实时交互式通信，例如互联网电话、会议等。

例题 2：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？

解：流式存储音频 / 视频是边下载边播放，即在文件下载后不久就开始播放。

流式实况音频 / 视频是发送时边录制边发送，接受时也是能够连续播放。接受方收到的节目时间和节目中事件的发生时间可以认为是同时的。

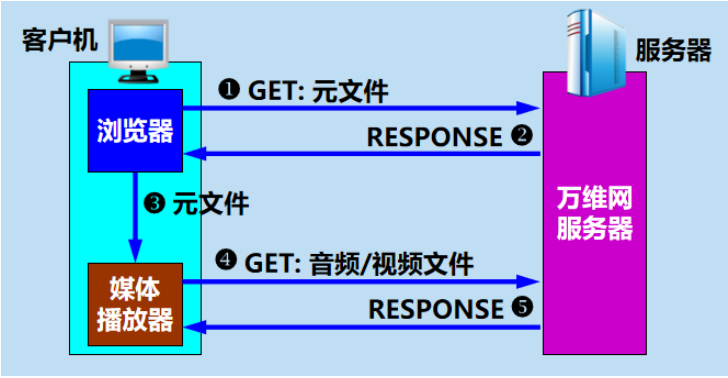
交互式音频 /视频是用户使用因特网和其他人进行实时交互通信?。

（二）流式存储音频/视频

1、具有元文件的万维网服务器

（1）“存储”音频/视频文件不是实时产生的，而是已经录制好的，通常存储在光盘或硬盘中。

（2）元文件就是一种非常小的文件，它描述或指明其他文件的一些重要信息。这里的元文件保存了有关这个音频/视频文件的信息。



2、媒体服务器

（1）使用两个分开的服务器：万维网服务器，媒体服务器。

（2）媒体服务器：也叫流式服务器 ，支持流式音频和视频的传送。

（3）媒体播放器与媒体服务器的关系：

① 客户与服务器的关系。

② 媒体播放器向媒体服务器请求音频/视频文件。

（4）媒体播放器与媒体服务器之间的交互：采用另外的协议。

例题 3：下列哪项属于媒体服务器的功能（ ）

A. 管理用户界面

B. 解压缩、消除时延抖动

C. 处理传输带来的差错

D. 请求下载浏览器所请求的音频 / 视频文件

解：D

3、实时流式协议 RTSP

实时流式协议 RTSP (Real-Time Streaming Protocol) ：

应用层的多媒体播放控制协议，不传送数据。

以客户服务器方式工作。

使用户在播放从互联网下载的实时数据时能够进行控制，如：暂停/继续、后退、前进等。

又称为“互联网录像机遥控协议”。

例题 4：实时流式协议 RTSP 的功能是_____。

解：给流式过程增加更多的功能。

（三）交互式音频/视频

1、IP 电话概述

（1） 狭义的 IP 电话：指在 IP 网络上打电话。

（2） 广义的 IP 电话：不仅仅是电话通信，而且还可以是在 IP 网络上进行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

(Instant Messaging)。

（3） IP 电话可看成是一个正在演进的多媒体服务平台，是话音、视像、数据综合的基础结构。

例题 5：狭义的 IP 电话和广义的 IP 电话都有哪些区别？

解：狭义的 IP 电话就是指在网络上打电话。广义的 IP 电话不仅仅是电话通信，而且还可以是在 IP 网络上进行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。

（4）影响 IP 电话通话质量的两个主要因素：

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。

但这两个因素是不确定的，取决于当时网络上的通信量。

例题 6：IP 电话的通话质量由_____和_____两个因素决定。

解：通话双方端到端的时延和时延抖动；话音分组的丢失率。

2、实时运输协议 RTP (Real-time Transport Protocol)

（1） RTP 采用无连接的 UDP 协议。

（2） 实时运输协议 RTP 为实时应用提供端到端的运输，但不提供任何服务质量的保证。

（3） 可以把 RTP 看成是 UDP 之上的一个运输层子层的协议。它将应用交给它的多媒体数据块封装成 RTP 分组，然后装入运输层的 UDP 数据报。

例题 7：协议能否提供应用分组的可靠传输？请说明理由。

解：不能。因为 RTP 为实时应用提供端到端的运输，但不提供任何服务质量的保证。RTP 是一个协议框架，因为它只包含了实时应用的一些共同功能，RTP 并不对多媒体数据块做任何处理而只是向应用层提供一些附加的信息，让应用层知道应当如何进行处理。

3、实时运输控制协议 RTCP(RTP Control Protocol)

（1）RTCP (RTP Control Protocol) 是与 RTP 配合使用的协议，与 RTP 协议不可分割。

（2）RTCP 也采用 UDP 服务，但并不对音频/视频分组进行封装。

（3）主要功能：

① 服务质量的监视与反馈；

② 媒体间的同步；

③ 播组中成员的标识。

类型	缩写表示	意义
200	SR	发送端报告
201	RR	接收端报告
202	SDES	源点描述
203	BYE	结束
204	APP	特定应用

例题 8：RTCP 协议使用在什么场合?它们各有何主要特点?

解：RTP 协议分别使用在：

（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。

（四）改进“尽最大努力交付”的服务

1、调度机制

（1）互联网平等对待所有分组。但不同服务要求提供不同的服务质量 QoS。

（2）调度和管制机制是使互联网能够提供服务质量的重要措施。

调度：指排队的规则。

（3）默认排队规则：先进先出 FIFO (First In First Out)。

① 先到达的分组先获得服务。

② 当队列已满时，后到达的分组就被丢弃。

（4）FIFO 的最大缺点：不能区分时间敏感分组和一般数据分组，并且也不公平。

（5）在先进先出的基础上增加按优先级排队，就能使优先级高的分组优先得到服务。

2、管制机制

（1）根据以下三个方面进行管制：

① 平均速率：指在一定的时间间隔内通过的分组数。

② 峰值速率：限制数据流在非常短的时间间隔内的流量。

③ 突发长度：限制在非常短的时间间隔内连续注入到网络中的分组数。

例题 9：下列哪项不属于数据流的管制机制（ ）

A. 传输速率

B. 平均速率

C. 峰值速率

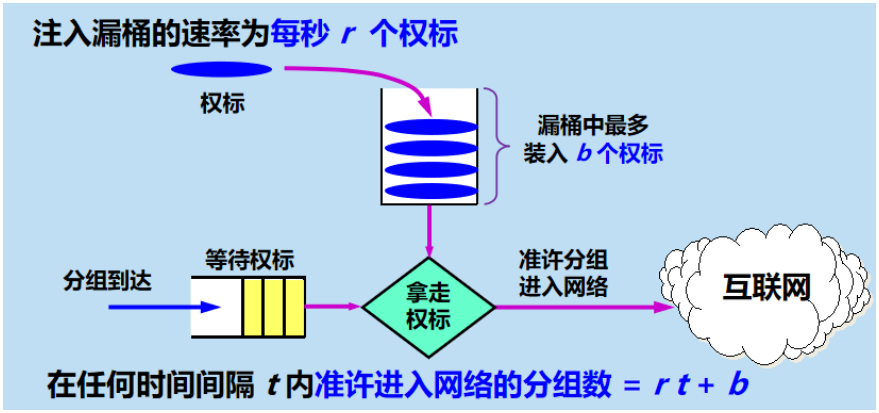
D. 突发长度

解：A

（2）漏桶管制器 (leaky bucket policer) （简称为漏桶）

（3）注意：“准许进入网络”不等于说“已经进入了网络”。

（4）控制权标进入漏桶的速率 r，就可对分组进入网络的速率进行管制。



例题 10：漏桶管制器的工作原理是怎样的？

解：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。

漏桶管制分组流进入网络的过程如下：分组进入网络前先要进入一个队列中等候漏桶中的权标，就可从漏桶取走一个权标，然后就准许一个分组从队列进入网络。若漏桶已无权标，就要等新的权标注入漏桶后，再把这个权标拿走后才能准许下一个分组进入网络。假定在时间间隔 t 中把漏桶中的全部 b 个权标都取走。但在这个时间间隔内漏桶又装入了 n 个新权标，因此在任何时间间隔 t 内准许进入网络的分组数的最大值为 ＋b。控制权标进入漏桶的速率 r 就可对分组进入网络的速率进行管制。

期末帮《计算机网络》课程讲义

第九章 无线网络和移动网络

（一）无线局域网 WLAN

1、无线局域网的组成

（1）无线局域网 WLAN (Wireless Local Area Network) ：采用无线通信技术的局域网。

（2）特点：提供了移动接入的功能；节省投资，建网速度较快；支持便携设备联网。

（3）无线局域网可以分为两类：

① 有固定基础设施的无线局域网：使用了预先建立起来的基站覆盖一定范围的固定地址，比如蜂窝移动通信网使用了电信公司建立的固定基站。

② 无固定基础设施的无线局域网：移动自组网络，比如蓝牙。（1）使用星形拓扑，中心叫做接入点 AP (Access Point)。

IEEE 802.11 是一个有固定基础设施的无线局域网的国际标准。

（4）使用星形拓扑，中心叫做接入点 AP (Access Point)。

① AP 是无线局域网的基础设施，也是一个链路层的设备。

② AP 也叫做无线接入点 WAP (Wireless Access Point)。

③ 无线局域网中的站点对网内或网外的通信都必须通过 AP。

（5）在 MAC 层使用 CSMA/CA 协议

① 基本服务集 BSS (Basic Service Set)是无线局域网的最小构件。

② 一个 BSS 包括一个接入点 AP 和若干个移动站。必须为该 AP 分配一个不超过 32 字节的服务集标识符 SSID (Service Set IDentifier) （即该 AP 的无线局域网的名字）和一个通信信道。

例题 1：无线局域网由 _____ 、_____、_____和有关设备组成。

解：无线网卡；无线接入点(AP)；计算机。

例题 2：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具体设施?

解：所谓“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。

接入点 AP 是星形拓扑的中心点，它不是固定基础设施。

（6）移动自组网络（移动分组无线网络）：服务范围通常是受限的，一般不和外界的其他网络相连接。优点：方便灵活；生存性非常好。

（7）无线传感器网络 WSN (Wireless Sensor Network) ：由大量传感器节点通过无线通信技术构成的自组网络。

（8）特点：

① 不需要很高的带宽，但大部分时间必须保持低功耗；

② 对协议栈的大小有严格的限制；

③ 对网络安全性、结点自动配置、网络动态重组等方面有一定的要求。

例题 3：WSN 是由大量_____通过 _____构成的自组网络。

解：传感器节点；无线通信技术。

2、802.11 局域网的 Mac 层协议

（1）无线局域网不能简单地搬用 CSMA/CD 协议。因为碰撞检测（CD）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，但接收到的信号强度往往会远远小于发送信号的强度，在无线局域网的设备中要实现这种功能就花费过大。

（2）802.11 无线以太网在 MAC 层使用 CSMA/CA 协议和停止等待协议。

（3）使用停止等待协议是因为无线信道的通信质量远不如有限信道，要使用停止等待来保证可靠传输。

例题 4：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？

解：CSMA/CA：载波监听多点接入/碰撞避免

CSMA/CD：载波监听多点接入/碰撞检测

（1）碰撞检测（CD）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，但接收到的信号强度往往会远远小于发送信号的强度，在无线局域网的设备中要实现这种功能就花费过大。

（2）即使能够实现碰撞检测的功能，并且在发送数据时检测到信道是空闲的时候，在接收端仍然有可能发生碰撞。

（4）802.11 的 MAC 层协议通过协调功能来确定基本服务集 BSS 中的各移动站在什么时间发送和接收数据。它包括两个子层：

① 分布协调功能 DCF：DCF 不采用中心控制，它在每一个结点使用 CSMA 机制的分布式接入算法，让各个移动站通过争用信道来获取发送权。

② 点协调功能 PCF：PCF 是选项，它用接入点 AP 集中控制整个 BSS 内各移动站的活动，使用类似探询的方法将发送数据权轮流交给各个站，以避免碰撞发生。对时间敏感的业务应该采用 PCF。

例题 5： 下列哪些属于 802.11 的 MAC 层协议包含的子层（　　）

A. PCF

B. DCF

C. BSS

D. EHT

解：AB

（二）无线个人局域网 WPAN

1、蓝牙系统

（1）无线个人区域网 WPAN (Wireless Personal Area Network) 就是把个人设备用无线技术连起来的自组网络，不需要使用接入点 AP。

（2）WPAN 都工作在 2.4GHz 频段。整个网络的范围大约在 10 m 左右。

（3）无线个人区域网包括：蓝牙系统、ZigBee、超高速 WPAN 等。

（4）WPAN 可以是一个人使用，也可以是若干人共同使用。

例题 6： WPAN 和 WLAN 的区别？

解：WPAN：是以个人为中心使用的无线个人区域网；实际上是一个低功率、小范围、低速率和低价格的电缆替代技术。

WLAN：是同时为许多用户服务的无线局域网；是一个大功率、中等范围、高速率的局域网。

（5）最早使用的 WPAN。

（6）第 1 代蓝牙：数据率 = 720 kbit/s，通信范围 = 10 米左右。

（7）蓝牙 4.0：

① 低耗能蓝牙 BLE (Bluetooth Low Energy)：适用于数据量很小的节点，电池可以连续工作 4 ~ 5 年；距离增大到 30 m，数据率可达 1 Mbit/s。

② 传统蓝牙 (classic Bluetooth)：数据率提高到 3 Mbit/s，传输距离可达 100 m。

（8）蓝牙 5.0：数据率上限达 24 Mbit/s，传输距离最高可达 300 m。

2、低速 WPAN

（1）主要用于工业监控组网、办公自动化与控制等领域，速率是 2 ~ 250 kbit/s。

（2）低速 WPAN 中最重要的就是 ZigBee。

（3）ZigBee 技术主要用于各种电子设备（固定的、便携的或移动的）之间的无线通信。

（4）ZigBee 的特点：

① 通信距离短 (10 ~ 80 m)，传输数据速率低，成本低廉。

② 功耗非常低：对于某些工作时间和总时间之比小于 1% 的情况，电池的寿命甚至可以超过 10 年。

③ 网络容量大：一个 ZigBee 的网络最多包括有 255 个结点，其中一个是主设备，其余则是从设备。若是通过网络协调器，整个网络最多可以支持超过 64000 个结点。

例题 6： 下列哪项不属于 ZigBee 的特点（　　）

A. 通信距离短

B. 损耗非常大

C. 网络容量大

D. 功耗非常低

解：B

（三）蜂窝移动通信网

1、蜂窝无线通信技术简介

（1）移动通信有多种，如蜂窝移动通信、卫星移动通信等。现在的蜂窝移动通信网采用了许多 IP 技术，可以支持手机、电脑上网。

（2）蜂窝移动通信是小区制的移动通信，它把整个网络划分成许多小区（也就是蜂窝），每个小区设置一个基站。移动站的通信都必须通过基站完成。与同一个蜂窝小区的其他用户共享带宽，每个用户实际分配到的带宽是不确定的。

（3）2G 即第二代蜂窝移动通信， 采用的是基于数字技术的时分多址（TDMA）技术和码分多址（CDMA）技术，基本只能提供电话和短信服务。它的代表是 GSM 系统。

（4）3G 使用了 IP 的体系结构和混合的交换体制（电路交换和分组交换），3G 以后的蜂窝移动通信就是以传输业务为主的通信系统了。

（5）第四代（4G）移动通信系统：2008 年，名称定为高级国际移动通信 IMT-Advanced。

特点：取消了电路交换，无论传送数据还是话音，全部使用分组交换技术，又称全网 IP 化。

例题 8：第四代蜂窝移动通信网和第三代蜂窝移动通信网有什么区别？

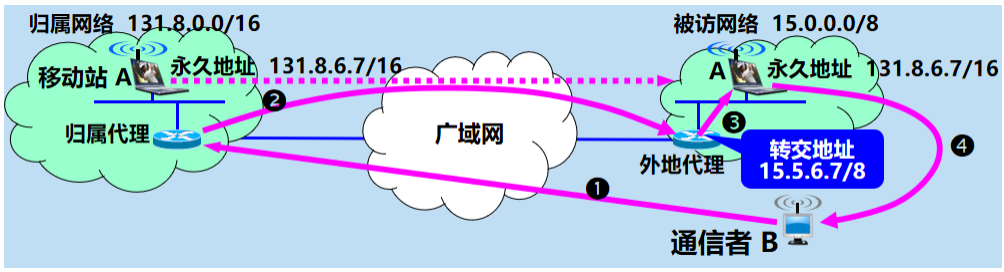
解：3G 使用了 IP 的体系结构和混合的交换体制（电路交换和分组交换），3G 以后的蜂窝移动通信就是以传输业务为主的通信系统了。

第四代（4G）移动通信系统：2008 年，名称定为高级国际移动通信 IMT-Advanced，其特点是取消了电路交换，无论传送数据还是话音，全部使用分组交换技术，又称全网 IP 化。

2、移动 IP

（1）移动 IP (Mobile IP) ：由 IETF 开发的一种技术，允许计算机移动到外地时，仍然保留其原来的 IP 地址。

（2）移动 IP 要解决的问题：使用户的移动性对上层的网络应用透明。



3、无线网络对高层协议的影响

移动站在不同无线网络间漫游时，网络的连接会发生中断。TCP 报文段会频繁丢失，TCP 的拥塞控制会受到影响，缩小拥塞窗口，而实际上网络中并不拥塞。

处理的方法：

（1）本地恢复。

（2）让 TCP 发送方知道什么地方使用了无线链路。

（3）让含有移动用户的端到端 TCP 连接拆成两个互相串接的 TCP 连接：从移动用户到无线接入点一个 TCP 连接，剩下的有线网络使用另一个 TCP 连接。

例题 9：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 连接有没有影响？

解：有。TCP 报文段会丢失；TCP 拥塞控制就会采取措施，减小其拥塞窗口，使 TCP 发送方的报文段发送速率降低。