数据科学与大数据技术

复习资料

计算机网络

小 林　黑龙江八一农垦大学 信息与电气工程学院

2025-11-24

目录

总述.....3
题型概括.....3
内容概括.....3
第一章 概述.....4
1.1 信息时代中计算机网络的概念.....4
1.2 互联网概述.....4
1.2.1 网络的网络.....4
1.2.2 互联网基础结构发展的三个阶段.....4
1.3 互联网的组成.....5
1.4 计算机网络的类别.....6
1.5 计算机网络的性能.....6
1.6 计算机网络体系结构.....7
1.6.1 协议与划分层次.....7
1.6.2 协议的体系结构.....8
1.6.3 实体、协议、服务和服务访问点.....8
第二章 物理层.....9
2.1 物理层的基本概念.....9
2.2 数据通信的基础知识.....9
2.2.1 信道的基本概念.....9
2.2.2 信道的极限容量.....10
2.3 信道复用技术.....10
2.3.1 频分复用、时分复用和统计时分复用.....10
2.3.2 波分复用.....11
2.3.3 码分复用.....11
第三章 数据链路层.....12
3.1 数据链路层的三个基本问题.....12
3.2 点对点协议 PPP.....12

3.3 使用广播信道的数据链路层 12
3.3.1 局域网的数据链路层 12
3.3.2 CSMA/CD 协议 12
3.3.3 使用集线器的星形拓扑 13
3.3.4 以太网的 MAC 层 13
3.4 扩展的以太网 13
第四章 网络层 15
4.1 网际协议 IP 15
4.1.1 IP 地址 15
4.1.2 IP 数据报的格式 16
4.2 网际控制报文协议 ICMP 16
4.3 IPv6 16
4.4 互联网的路由选择协议 17
4.5 虚拟专用网 VPN 和网络地址转换 NAT 17
第五章 运输层 18
5.1 运输层协议概述 18
5.2 UDP 和 TCP 18
5.2.1 UDP 18
5.2.2 TCP 19
第六章 应用层 21
6.1 域名系统 DNS 21
6.2 文件传送协议 21
6.3 万维网 22
6.4 电子邮件 22
第七章 网络安全 23
7.1 网络安全的知识点 23
7.2 例题 24

总述

题型概括

表格 1 题型统计

题目类型	题目数量	题目分值
填空	20	1
判断	10	1
选择	10	1
简答\计算	不定	共 60

内容概括

计算机网络是计算机考研 408 中的一本书，它解决的是计算机与计算机之间联系的问题。既然是解决计算机之间的联系交流问题，那么就会产生如：交流介质、交流手段、交流可信度、信息发送方、信息接受方等人与人之间的会出现的交流问题。本复习资料将分别从计算机网络的概述、计算机网络传输中的五层结构以及计算机网络安全等考点部分进行记录。

本复习资料参考书籍为谢希仁老师编著的计算机网络（第 8 版），适用学生范围为黑龙江八一农垦大学信息与电气工程学院数据科学与大数据技术专业学生。本复习资料仅供其他计算机大类学生参考。

第一章 概述

1.1 信息时代中计算机网络的概念

21 世纪的一些重要特征就是数字化、网络化和信息化，它是一个以网路为核心的信息时代。其中有三大类网络，**即电信网络、有线电视网络和计算机网络**，然而随着技术的发展，电信网络和有限电视网络都逐渐融入了现代计算机网络的技术。20 世纪 90 年代以后，以 Internet 为代表的计算机网络得到了飞速的发展，已经成为全球最大的和最重要的计算机网络，但是 Internet 的中文译名并不统一，以下是现有的两种译名，其含义各有不同。

1. 因特网

这个译名是全国科学技术名词审定委员会推荐的，但却长期未得到推广。

2. 互联网

这是目前流行最广的、事实上的标准译名。这个译名能够体现出 Internet 的最主要特征：**Internet 是由数量极大的各种计算机网络互连起来的。**其中互联网具有两个重要基本特点：**连通性**和**共享**。

1.2 互联网概述

1.2.1 网络的网络

计算机网络（简称为网络）**由**若干**节点**和连接这些节点的**链路**组成。**节点**可以是**计算机、集线器、交换机或路由器**等。

互连网（网络的网络）：有多个网络通过一些路由器相互连接起来，构成了一个覆盖范围更大的计算机网络。

1.2.2 互联网基础结构发展的三个阶段

1. **第一阶段是从单个网络 ARPANET 向互连网发展的过程**

其中 1983 年 TCP/IP 协议成为 ARPANET 上的标准协议，而 1983 年也被作为互联网的诞生时间。

internet（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（互联网）：专用名词，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互连网，它采用 TCP/IP 协议族作为通信的规则，其前身为美国的 ARPANET。

2. 第二阶段的特点是建成了三级结构的互联网

三级计算机网络：**主干网、地区网和校园网（或企业网）**

3. 第三阶段的特点是逐渐形成了**全球范围的多层次 ISP 结构的互联网**

1.3 互联网的组成

1. 互联网的拓扑结构按照工作方式可分为以下两大块：

1) **边缘部分**：由所有连接在互联网上的主机组成，这部分是**用户直接使用的**，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，这部分是**为边缘部分提供服务的**（提供连通性和交换）。

2. 在网络边缘的端系统之间的通信方式可以划分为以下两类：

1) **客户-服务器方式（C/S 方式）**

客户是服务请求方，服务器是服务提供方。

2) **对等连接方式（P2P 方式）**

对等连接中的每一台主机既是客户同时又是服务器。

3. **路由器**在网络核心部分起特殊作用，它是实现**分组交换**的关键构件。

4. 三种典型的交换方式：电路交换、分组交换和报文交换

1) **电路交换的主要特点**

在通话的全部时间内，通话的两个用户始终占用端到端的通信资源，当使用电路交换来传送计算机数据时，其线路的传输效率往往很低。

整个报文的比特流连续地从源点直达终点。

2) **分组交换的主要特点**

分组交换采用**存储转发技术**，在发送端发送报文前，先把较长的报文划分成较短的等长的数据段，在每个数据段前面加上首部后就构成了分组，分组又称为

“包”，而分组是互联网中传送的数据单元。

单个分组传送到相邻节点，存储下来后查找转发表，转发到下一个节点。

3) 报文交换的主要特点

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。

4) **三种交换方式的优势**

若要连续传送大量的数据，且其传送时间远大于连接建立时间，则电路交换的传输速录较快；报文交换和分组交换不需要预先分配传输带宽，在传送突发数据时可提高整个网络的信道利用路；由于一个分组的长度往往远小于整个报文的长度，因此，分组交换比报文交换的时延小，同时也具有更好的灵活性。

1.4 计算机网络的类别

1. 按照网络的作用范围进行分类

1) 广域网 WAN：作用范围通常在几十到几千公里

2) 城域网 MAN：作用范围一般是一个城市

3) 局域网 LAN：常见的为校园网和企业网

4) 个人区域网 PAN：也成为无线个人区域网 WPAN

2. 按照网络的使用者进行分类

1) 公用网：指电信公司（国有或私有）出资建造的大型网络

2) 专用网：指某个部门为满足本单位的特殊业务工作的需要而建造的不对外开放的网络

3. 用来把用户接入到互联网的网络

接入网 AN，又称为本地接入网或居民接入网。

1.5 计算机网络的性能

1. 速率：单位为 bit/s，1Byte=8bit，提到的网络速率往往指的是额定速率

2. 带宽

带宽本来指某个信号具有的频带宽度，但在计算机网络中，带宽用来表示网络中某通道传送数据的能力，因此**网络带宽表示在单位时间内网络中的某信道所**

能通过的“最高数据率”，这种意义上**带宽的单位就是数据率的单位 bit/s**。

3. 吞吐量

吞吐量表示在单位时间内通过某个网络（或信道、接口）的实际数据量，有时吞吐量还可用每秒传送的字节数或帧数来表示。

4. 时延：指数据从网络的一端传送到另一端所需的时间

1) 发送时延：主机或路由器发送数据帧所需的时间

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

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

$$\text{传播时延} = \frac{\text{信道长度(m)}}{\text{电磁波在信道上的传播速率(m/s)}}$$

3) 处理时延：主机或路由器收到分组后处理所需的时间

4) 排队时延：分组在进入路由器排队等待处理的时间和处理完等待发送的时间

$$\text{总时延} = \text{发送时延} + \text{传播时延} + \text{处理时延} + \text{排队时延}$$

5. 时延带宽积：$\textit{时间带宽积} = \textit{传播时延} \times \textit{带宽}$

6. 往返时间 RTT：双向交互一次所需的时间

$$\text{有效数据率} = \frac{\text{数据长度}}{\text{发送时间} + \text{RTT}}$$

7. 利用率：分为信道利用率和网络利用率

信道利用率指某信道有百分之几的时间是被利用的；网络利用率则是全网络的信道利用率的加权平均值。

$$\text{网络当前的时延} = \frac{\text{网络空闲的时延}}{1 - \text{网络利用率}}$$

1.6 计算机网络体系结构

1.6.1 协议与划分层次

网络协议（协议）：为进行网络中的数据交换而建立的规则、标准或约定

网络协议的三要素：语法、语义和同步

1. 语法：即数据与控制信息的结构或格式
2. 语义：即需要发出任何控制信息，完成任何动作以及做出何种响应
3. 同步：即时间实现顺序的详细说明

1.6.2 协议的体系结构

<table>
<tr><td>OSI 的体系结构</td><td>TCP/IP 的体系结构</td><td>五层协议的体系结构</td></tr>
<tr><td>7. 应用层</td><td rowspan="3">应用层
（各种应用层协议如
DNS,HTTP,SMTP 等）</td><td rowspan="3">5. 应用层</td></tr>
<tr><td>6. 表示层</td></tr>
<tr><td>5. 会话层</td></tr>
<tr><td>4. 运输层</td><td>运输层（TCP 或 UDP）</td><td>4. 运输层</td></tr>
<tr><td>3. 网络层</td><td>网际层 IP</td><td>3. 网络层</td></tr>
<tr><td>2. 数据链路层</td><td rowspan="2">链路层（网络接口层）
（这一层并没有具体内容）</td><td>2. 数据链路层</td></tr>
<tr><td>1. 物理层</td><td>1. 物理层</td></tr>
<tr><td>OSI 的七层协议</td><td>TCP/IP 的四层协议</td><td>讲述原理的五层协议</td></tr>
</table>

注：本复习资料与参考书所指的体系结构均为五层协议体系结构。

1.6.3 实体、协议、服务和服务访问点

1. 实体：任何可以发送或接受信息的硬件或软件进程
2. 协议：控制两个对等实体（或多个实体）进行通信的规则的集合
3. 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，要实现本层协议还要使用下面一层所提供的服务。即协议是水平的，服务是垂直的。

第二章 物理层

2.1 物理层的基本概念

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。

物理层的四种特性

1. 机械特性：指明接口所用的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的意义
4. 过程特性：指明对于不同功能的各种可能时间的出现顺序

2.2 数据通信的基础知识

一个数据通信系统可划分为三大部分：**源系统（发送端或发送方）、传输系统（传输网络）和目的系统（接收端或接收方）**

2.2.1 信道的基本概念

1. 三种通信的双方信息交换的方式

1) **单向通信**：又称单工通信，只能有一个方向的通信而没有反方向的交互
2) **双向交替通信**：又称半双工通信，通信的双方都可以发送信息，但不能双方同时发送（当然也不能双方同时接收）
3) **双向同时通信**：又称全双工通信，通信的双方可以同时发送和接收信息

2. **常用编码方式**

1) 不归零制：正电平代表 1，负电平代表 0
2) 归零制：正脉冲代表 1，负脉冲代表 0
3) **曼彻斯特编码**：位周期中心的向上跳变代表 0，位于周期中心的向下跳变代表 0
4) **差分曼彻斯特编码**：在每一位的中心处始终有跳变，位于开始边界有跳变代表 0，而位于开始边界没有跳变代表 1

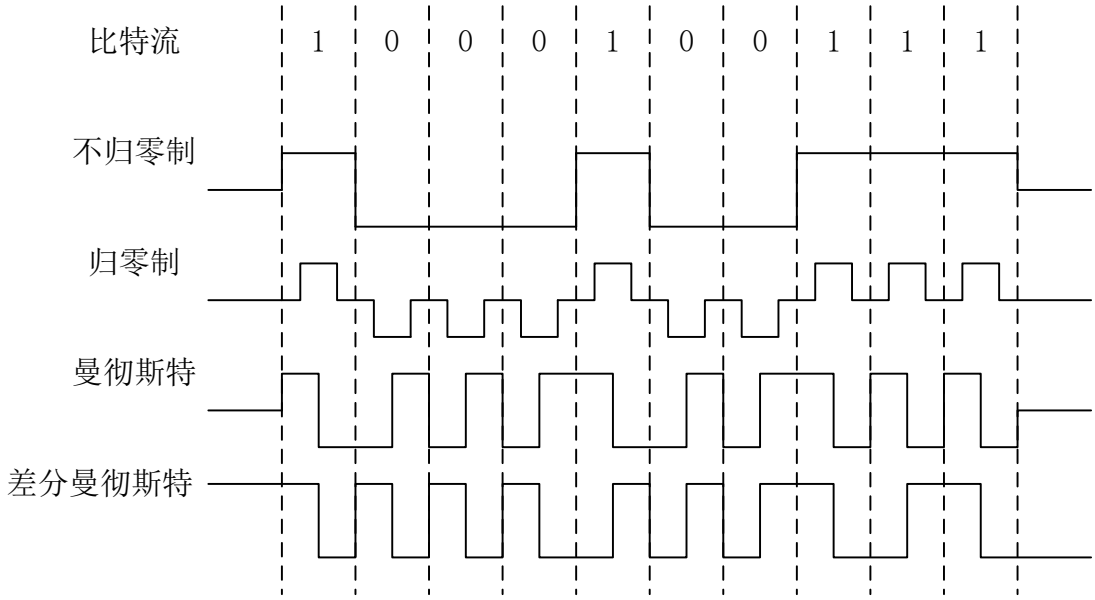


图 1 数字信号常用的编码方法

2.2.2 信道的极限容量

1. 信道能通过的频率范围

奈氏准则：在带宽为 W(Hz)的低通信道中，若不考虑噪声影响，则码元传输的最高速率是 $2W$(码元/秒)。传输速率超过此上限，就会出现严重的码间串扰的问题，使接收端对码元的判决（即识别）成为不可能。

2. 信噪比

所谓信噪比就是信号的平均功率和噪声的平均功率之比，常记为 S/N。但通常大家都是使用分贝(dB)作为度量单位。

$$\text{信噪比(dB)} = 10\log_{10}(S/N) \quad \text{(dB)}$$

香农公式指出：信道的极限信息传输速率 C 是

$$C = W\log_2(1 + S/N) \quad \text{(bit/s)}$$

香农公式表明，信道的带宽或信道中的信噪比越大，信息的极限传输速率就越高。

2.3 信道复用技术

2.3.1 频分复用、时分复用和统计时分复用

1. 频分复用 FDM：各路信号在同样的时间占用不同的带宽资源（此处的带宽

不是数据的发送速率，是频率带宽）

2. 时分复用 TDM：所有用户在不同的时间占用同样的频带宽度
3. 统计时分复用 STDM：将多个用户的不同时间的复用数据通过集中器进行整合后几种起来通过高速线路进行发送

2.3.2 波分复用

波分复用 WDM 就是光的频分复用，由于光载波的频率很高，所以习惯上用波长而不用频率来表示所使用的光载波。

2.3.3 码分复用

码分复用 CDM 是另一种共享信道的方法，当码分复用信道为多个不同地址的用户所共享时，就称为码分多址 CDMA。

优点：由于各用户使用经过特殊挑选的不同码型，因此各用户之间不会造成干扰。采用 CDMA 可提高通信的话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率。

缺点：码分复用用“带宽换共享”，在获得抗干扰与软容量优点的同时，带来了速率牺牲、远近效应、同步难题和成本上升等显著缺点。

码分复用题目计算方法：已知某站的码片序列为 S(s1,s2,s3,s4)，收到的码片序列为 W(w1,w2,w3,w4)，将 S 和 W 的按位相乘累和后除以码片长度，如果结果为+1 则发送的是 1，若结果为 0 则该站没有发送，若结果为-1 则发送的是 0。

第三章 数据链路层

3.1 数据链路层的三个基本问题

三个基本问题：封装成帧、透明传输和差错检测。

1. 封装成帧：在一段数据的前后分别添加首部和尾部，这样就构成了一个帧
2. 透明传输：通过在数据中插入转义字符或进行字节填充来解决数据中可能存在控制字符在接收端被解释为控制字符。
3. 差错检测

实际的通信链路并非是理想的，它不可能使误码率下降到零，因此，为了保证数据传输的可靠性，在计算机网络传输数据时，必须采用各种差错检测措施。目前在数据链路层广泛使用了循环冗余检验 CRC 的检错技术。

循环冗余码的检验计算和原理见书 P76~77。

3.2 点对点协议 PPP

在 TCP/IP 协议族中，可靠传输由运输层的 TCP 协议负责，因此数据链路层的 PPP 协议不需要进行纠错，不需要设置序号，也不需要进行流量控制。PPP 协议不支持多点线路（即一个主站轮流和链路上的多个从站进行通信），而只支持点对点的链路通信。此外，PPP 协议只支持全双工链路。

3.3 使用广播信道的数据链路层

3.3.1 局域网的数据链路层

局域网最主要的特点：网络为一个单位所拥有，且地理范围和站点数目均有限。

局域网工作的层次跨越了数据链路层和物理层。

3.3.2 CSMA/CD 协议

为了通信的简便，以太网采取了以下两种措施：

1. 采用较为灵活的无连接的工作方式，以太网提供的服务是尽最大努力的交付，

即不可靠的交付。

2. 以太网发送的数据都使用曼彻斯特编码的信号。

CSMA/CD 协议的要点归纳：发前先听，空闲即发送，边发边听，冲突时避退。

3.3.3 使用集线器的星形拓扑

1990 年 IEEE 制定出星形以太网 10BASE-T 的标准 802.3i，“10”代表 10Mbit/s 的数据率，BASE 表示连接线上的信号是基带定好，T 代表双绞线。

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，使用的还是 CSMA/CD 协议
2. 一个集线器有许多端口
3. 集线器工作在物理层，它的端口仅仅简单地转发比特，不进行碰撞检测

3.3.4 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。

发送给各主机的帧有三种：单播帧、广播帧和多播帧。

只有目的地址才能使用广播地址和多播地址。

2. MAC 地址的格式

以太网 V2 的 MAC 帧较为简单，由五个字段组成。前两个字段分别为 6 字节长的目的地址和源地址字段，第三个字段是 2 字节的类型字段，第四个字段是数据字段（长度在 46 到 1500 字节），最后一个字段是 4 字节的帧检验序列 FCS（使用 CRC 检验）。MAC 帧的总长度最小为 64 字节，最大为 1518 字节。

3.4 扩展的以太网

1. 碰撞域：又称冲突域，即在任一时刻，在每个碰撞域中只能有一个站在发送数据。
2. 网桥：网桥对收到的帧根据其 MAC 帧的目的地址进行转发和过滤。

3. 以太网交换机的特点

以太网交换机的每个端口都直接与一个单台主机或另一个以太网交换机相连，并且一般都工作在全双工方式；相互通信的主机都独占传输媒体，无碰撞地传输数据；以太网交换机是一种即插即用设备，其内部的帧交换表（又称地址表）是通过自学习算法自动地逐渐建立起来的。

总线以太网使用 CSMA/CD 协议，以半双工方式工作（共享式）；但以太网交换机不使用共享总线，没有碰撞问题，因此不使用 CSMA/CD 协议，而是以全双工方式工作。

第四章 网络层

4.1 网际协议 IP

互联网上交付主机的两种方式：在本网络上的直接交付（不经过路由器）；到其他网络的间接交付（经过至少一个路由器，但最后一次一定是直接交付）。

地址解析协议 ARP 把 IP 地址解析为 MAC 地址，它解决同一个局域网上的主机或路由器的 IP 地址和 MAC 地址的映射问题。ARP 的高速缓存可以大大减少网络上的通信量。

4.1.1 IP 地址

1. IP 地址及其表示方法

IP 地址就是给连接到互联网上的每一台主机（或路由器）的每一个接口，分配一个在全世界范围内是唯一的 32 位的标识符。

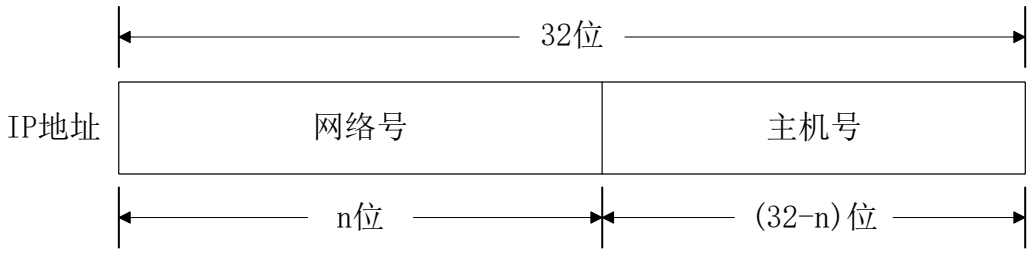


图 2 IP 地址中的网络号和主机号字段

2. 分类的 IP 地址

如图 2 所示，分类的方法非常简单，A 类（n=8）、B 类（n=16）和 C 类（n=24）地址都是单播地址（一对一通信），D 类是多播地址，E 类是保留地址。

3. 无分类编址 CIDR

目前已广泛使用无分类域间路由选择 CIDR 记法把 IP 地址后面加上斜线“/”，斜线后是前缀的位数。前缀（或网络前缀）指明网络，后缀指明主机。前缀相同的连续 IP 地址构成“CIDR 地址块”。

CIDR 的 32 位地址掩码（或子网掩码）由一串 1 和一串 0 组成，其中 1 的个数是前缀的长度。只要 IP 地址和地址掩码按位进行 AND 运算，即可得出网络地址。

4.1.2 IP 数据报的格式

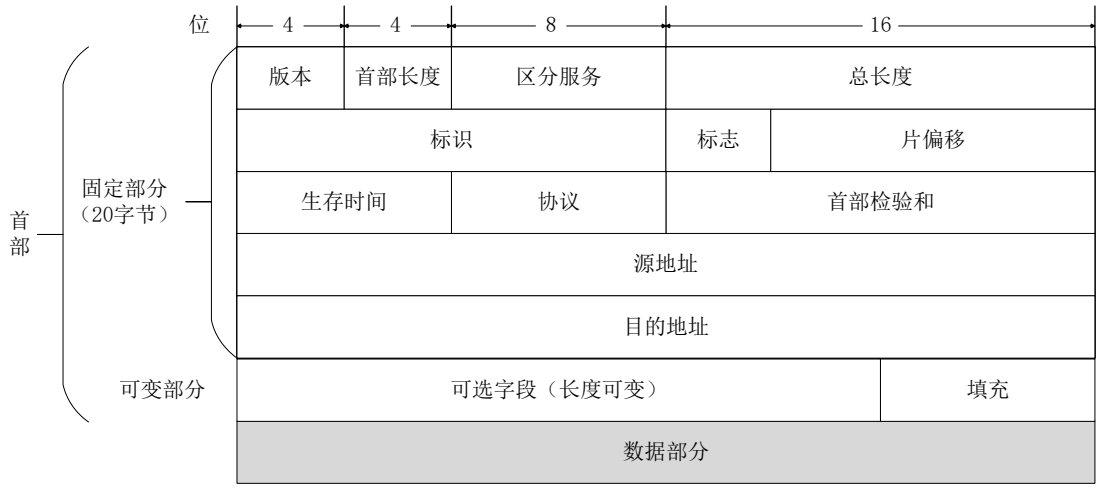


图 3 IP 数据报的格式

IP 数据报分为首部和数据两部分。首部的前一部分是固定长度，工 20 字节，是所有 IP 数据报必须具有的。

IP 首部中的生存时间字段给出了 IP 数据报在互联网中所能经过的最大路由器数，可防止 IP 数据报在互联网中无限制地兜圈子。

片偏移方式：占 13 位，较长的分组在分片后，某片在原分组中的相对位置。也就是说，相对于用户数据字段的七点，该片从何处开始。片偏移以 8 个字节为偏移单位。也就是说，除最后一个数据报片外，其他每个分片的长度一定是 8 字节的整数倍。

4.2 网际控制报文协议 ICMP

1. ICMP 报文的种类：ICMP 差错报告报文和 ICMP 询问报文
2. 分组网间探测 PING 使用了 ICMP 回送请求与回送回答报文（ICMP 的应用）

4.3 IPv6

IPv6 相对于 IPv4 的变化如下：

1. 更大的地址空间，IPv6 的地址为 128 为，使用冒号 16 进制；
2. 灵活的首部格式，首部固定 40 字节，但是运行有更多的首部扩展；
3. 改进的选项；

4. 支持即插即用（即自动配置）；
5. 支持资源的预分配；
6. IPv6 首部改为 8 字节对齐（即首部长度必须是 8 字节的整数倍），IPv4 的首部是 4 字节对齐。

IPv6 数据报由两大部分组成，即基本首部和后面的有效载荷。有效载荷也成为净负荷。有效载荷允许由零个或多个扩展首部，在后面就是数据部分。

4.4 互联网的路由选择协议

路由选择协议由两大类：内部网关协议，如 RIP 和 OSPF；外部网关协议，如 BGP-4；

RIP 是分布式的基于距离向量的路由选择协议，只适用于小型互联网。RIP 按照固定的时间间隔与相邻路由器交换信息。交换的信息是自己当前的路由表，即到达本自治系统中所有网络的（最短）距离，以及到每个网络应经过的下一跳路由器。

OSPF 是分布式的链路状态协议，适用于大型互联网。OSPF 旨在链路状态发生变化是，才向本自治系统中的所有路由器，用洪泛法发送与本路由器相邻的所有路由器的链路状态信息。

协议 BGP-4 简称为 BGP，是一种路径向量路由选择协议，用于不同自治系统 AS 之间的路由选择。BGP 力求在 AS 之间，找出一条能过够到达目的网络前缀且较好的路由（不是最佳路由，但不能兜圈子）。

4.5 虚拟专用网 VPN 和网络地址转换 NAT

虚拟专用网 VPN 利用公用的互联网作为本机构各专用网络之间的通信载体。VPN 内部使用互联网的专用地址。一个 VPN 至少要有一个路由器具有合法的全球 IP 地址，这样才能和本系统的另一个 VPN 通过互联网进行通信。所有通过互联网传送的数据都必须加密。

使用网络地址转换 NAT 技术，可以在专用网络内部使用专用 IP 地址，而仅在连接到互联网的路由器使用全球 IP 地址。

第五章 运输层

5.1 运输层协议概述

1. 进程之间的通信

真正进行通信的实体是主机中的进程，是一台主机中的应用进程和另一台主机中的应用进程在交换数据。通信的两端应当是两个主机中的应用进程。

2. 运输层的两个主要协议

用户数据报协议 UDP：在传送数据之前不需要先建立连接。

传输控制协议 TCP：提供面向连接的服务，在传输数据之前必须先建立连接。

3. 运输层的端口

运输层用一个 16 位端口号来标志一个端口，它可以允许有 65535 个不同的端口号。端口号分为服务器端使用的端口号（0~1023 指派给熟知端口，1024~49151 是登记端口号）和客户端暂时使用的端口号（49152~65535）。端口号只具有本地意义，它只是为了标志本计算机应用层中的各个进程在和运输层交互时的层间接口。在互联网的不同计算机中，相同的端口号是没有关联的。

表格 2 常用的熟知端口号

应用程序	FTP	TELNET	SMTP	DNS	TFTP
端口号	21	23	25	53	69
应用程序	HTTP	SNMP	SNMP(trap)	HTTPS	SSH
端口号	80	161	162	443	22

5.2 UDP 和 TCP

5.2.1 UDP

1. UDP 的特点

无连接；尽最大努力交付；面向报文；无拥塞控制；支持一对一、一对多、多对一和多对多的交互通信；首部开销小（只有四个字段：源端口、目的端口、长度和检验和）。

2. UDP 的首部格式

用户数据报 UDP 有两个字段：数据字段和首部字段，首部字段很简单，只有 8 个字节，由 4 个字段组成，每个字段长度都是 2 字节（源端口、目的端口、长度和检验和）。

5.2.2 TCP

1. TCP 的主要特点

面向连接；每一条 TCP 连接只能是点对点的（一对一）；提供可靠交付的服务；提供全双工通信；面向字节流。

2. TCP 报文的首部格式

TCP 报文段首部的前 20 个字节是固定的，后面有 4N 字节是根据需要而增加的选项。在一个 TCP 连接中传送的字节流中的每一个字节都按顺序编号。首部中的序号字段值则指的是本报文段所发送的数据的第一个字节的序号。首部中的确认号是期望收到对方下一个报文段的第一个数据字节的序号。若确认号为 N，则表明：到序号 N-1 为止的所有数据都已正确收到。

3. TCP 的流量控制（书 P236）

发送方的发送窗口不能超过接收方给的接收窗口的数值。

4. TCP 的拥塞控制（书 P241）

TCP 的拥塞控制采用了四种算法，即慢开始、拥塞避免、快重传和快恢复。在网络层，也可以使路由器采用适当的分组丢弃策略（如主动队列管理 AQM），以减少网络拥塞

5. TCP 的连接建立

用三次握手建立 TCP 连接的流程如图 4 所示，假定主机 A 运行的是 TCP 客户程序，而 B 运行 TCP 服务器程序。

客户端主动发送一个 SYN=1 的包，序列号为 x，表示请求建立连接，客户端进入 SYN-SENT 状态；服务器收到 SYN 包后，回复一个 SYN=1，ACK=1 的包，序列号为 y，确认号为 x+1，表示同意连接，服务器进入 SYN-RCVD 状态；客户端收到服务器的 SYN+ACK 包后，再发送一个 ACK=1 的包，序列号为 x+1，确认号为 y+1，表示连接建立完成。

客户端进入 ESTABLISHED 状态，服务器收到后也进入 ESTABLISHED 状态，之后就能进行数据传输了。

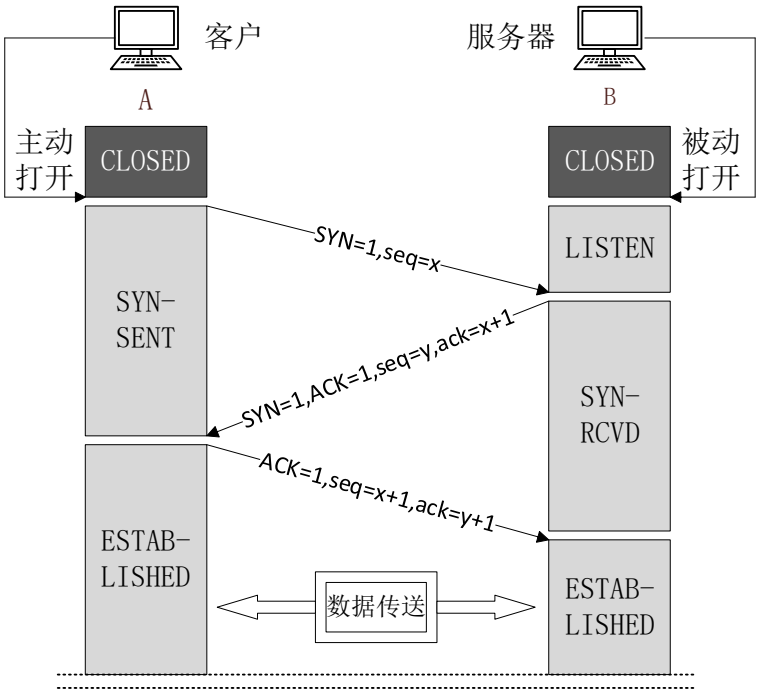


图 4 用三次握手建立 TCP 连接

6. TCP 的连接释放

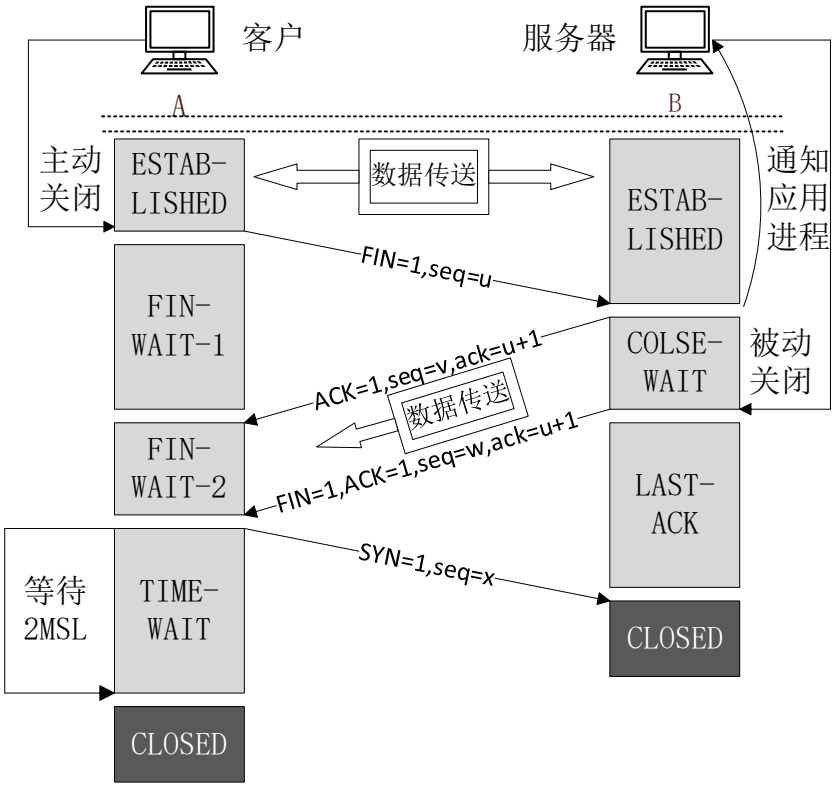


图 5 TCP 连接释放的过程

主动方 A 发 FIN=1（序号 u），发送中断请求，进入 FIN-WAIT-1；被动方 B 回 ACK=1（序号 v，确认 u+1），发送收到请求，进入 CLOSE-WAIT，A 收到后进入 FIN-WAIT-2，此时 A→B 方向已关，B 仍可继续发数据；B 数据发完，再发 FIN=1,ACK=1（序号 w，确认仍 u+1），发送关闭声明，进入 LAST-ACK；A 回 ACK=1（确认 w+1），发送确认 B 的关闭声明，进入 TIME-WAIT，B 收到后立即 CLOSED，A 等待 2MSL 后也 CLOSED，连接彻底释放。

第六章 应用层

6.1 域名系统 DNS

1. 原先的顶级域名共分为三大类

   国家顶级域名 nTLD、通用顶级域名 gTLD 和基础结构域名。

2. 域名服务器的四类

   根域名服务器、顶级域名服务器、权限域名服务器和本地域名服务器。

6.2 文件传送协议

1. FTP

文件传送协议 FTP 使用 TCP 可靠的运输服务。FTP 使用**客户服务器方式（CS 架构）**。一个 FTP 服务器进程可同时为多个客户进程提供服务。在进行文件传输时，FTP 的客户和服务器之间要建立两个并行的 TCP 连接：**控制连接（端口号 21）和数据连接（端口号 20）**。实际用于传输文件的是数据连接。

2. 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，它也使用客户服务器方式，但它使用 UDP 数据报，因此 TFTP 要有自己的差错改正措施。TFTP 只支持文件传输而不支持交互，它没有一个庞大的指令集，没有列目录的功能，也不能对用户进行身份鉴别。

TFTP 的主要特点：每次传送的数据报文中有 512 字节的数据，但最后一次可不足 512 字节；数据报文按序编号，从 1 开始；支持 ASCII 码或二进制传送；

可对文件进行读写；使用很简单的首部。

6.3 万维网

1. URL

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，并使每一个文档在整个互联网上具有唯一的标识符 URL。

2. HTTP

万维网客户程序与服务器之间进行交互所使用的协议是超文本传送协议 HTTP。HTTP **使用 TCP** 连接进行可靠的传送，它是**面向事务的应用层协议**。但 HTTP 协议本身是**无连接、无状态的**。

3. HTML

万维网使用超文本标记语言 HTML 来显示各种万维网页面。

4. **HTTP 的响应状态码**

1xx 表示通知信息，如请求收到了或正在进行处理；2xx 表示成功，如接受或知道了；3xx 表示重定向，如要完成请求还必须采取进一步的行动；4xx 表示客户的差错，如请求中有错误的语法或不能完成；5xx 表示服务器的差错，如服务器失效无法完成请求啊。

6.4 电子邮件

1. 电子邮件系统的三个主要组成构件

用户代理、邮件服务器和邮件协议（包括邮件发送协议，如 SMTP，和邮件读取协议，如 POP3 和 IMAP）。POP3 功能较少且仅在客户端内，IMAP 功能更强大且客户端与邮箱更新同步。

2. 基于万维网的电子邮件

基于万维网的电子邮件使用户能够利用浏览器收发电子邮件。用户浏览器和邮件服务器之间的邮件传送使用 HTTP 协议，而在邮件服务器之间邮件的传送仍然使用 SMTP 协议。

第七章 网络安全

7.1 网络安全的知识点

1. 计算机网络的两大威胁：被动攻击和主动攻击

   主动攻击有篡改、恶意程序、拒绝服务；被动攻击：截获。

2. 报文鉴别主要鉴别两个内容：鉴别发信者和鉴别报文的完整性。

3. 常用的散列函数：MD5 和 SHA-1

4. MD5 报文摘要 128 位，SHA-1 的长度是 160

5. 报文鉴别

   对每一个收到的报文都要鉴别报文的发送者，实体鉴别是在系统接入的全部持续时间内对自己通信的对方实体只需验证一次。

6. X.509 规定一个数字证书必须包括以下字段

   X.509 的版本、数字证书名称及序列号、本数字证书所使用的签名算法、数字证书签发者的唯一标识符、数字证书的有效期、主体名和公钥。

7. IPsec 协议族中的协议可划分三个部分

   IP 安全数据报格式的两个协议（鉴别首部 AH 和的封装安全有效载荷）；有关加密算法的三个协议；互联网密钥交换协议。

8. 安全关联在源实体和目的实体之间必须创建一条网络层的逻辑连接即安全关联

9. 运输层安全协议有两个：安全套接字 SSL、运输层安全 TLS

   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 运输的应用层数据提供安全保障。

10. 入侵检测方法：基于特征的入侵检测、基于一场的入侵检测

11. PGP 是一个完整的电子邮件安全软件包

12. 防火墙：

    是一种特殊编程的路由器，安全在一个网点的网络的其余部分之间，目的是实施访问控制策略。防火墙的功能：一个是阻止，另一个允许。

7.2 例题

1. 两类密码体制（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：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。在对称密码体制中加密密钥与解密密钥都使用相同的密钥。算法是公开的，密钥是保密的。

公钥密码体制，即加密密钥与解密密钥是不同的密码体制。在公钥密码体制中，加密密钥 PK（即公钥）是向公众公开的，而解密密钥 SK（即私钥或密钥）则是需要保密的。加密算法 E 和解密算法 D 也都是公开的。

2. 数字签名的原理？

答：数字签名必须保证能够实现以下三点功能

接收者能够核实发送者对报文的签名。也就是说，接收者能够确信该报文的确是发送者发送的。其他人无法伪造对报文的签名。这就叫报文鉴别。

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。这就叫报文的完整性。

发送者事后不能抵赖对报文的签名。这就叫不可否认。