

项目二 探索处理计算机网络问题的基本方法



项目导引

项目一从网络基本概念的角度，介绍了计算机网络的发展历程、定义、组成、分类以及网络领域目前主要研究的热点问题，回答了什么是计算机网络这一最基本的问题，在广域网的基础上提出了对网络结构进行抽象的概念：资源子网和通信子网，为我们研究计算机网络提供了初步的解决方法。随着 Internet 技术的发展，资源子网和通信子网的概念也在发生着演变。现在我们讨论 Internet 技术的发展，不再使用资源子网和通信子网的概念了，而是以“边缘部分”和“核心交换部分”代之。因此，需要在此基础上做更高层次的抽象。网络体系结构和网络协议的概念是抽象的理论研究的成果，是很多研究人员多年研究成果的总结。网络体系结构和网络协议是学习网络知识中必须要掌握的两个基本概念，它为我们提供了解决计算机网络问题的有效方法。尽管计算机网络是一个复杂的系统，利用它可以回答和解决计算机网络的基本工作原理和技术实现这个最本质的问题。

在计算机网络的发展过程中，有两种著名的网络体系结构。一是 1984 年发布的开放系统互联参考模型（Open System Interconnection/Reference Mode, OSI/RM），它为各个厂商提供了一套标准，确保全世界各公司提出的不同类型网络之间具有良好的兼容性和互操作性。二是传输控制协议/网际协议（Transmission Control Protocol/Internet Protocol, TCP/IP），起源于 20 世纪 60 年代美国国防部 DOD（U.S. Department of Defense）资助的一个网络分组交换研究项目，是至今发展最成功的通信协议，它被用于最大的开放式网络系统 Internet 之上。

本项目将从层次、服务与协议的基本概念出发，对 OSI 参考模型、TCP/IP 参考模型进行讨论和比较，使读者明白网络体系结构和网络协议这两个概念的重要性，以便读者对计算机网络的工作过程和实现（Implementation）技术建立一个整体概念，为后续学习打下基础。



项目描述

项目一已经实现两台计算机之间的物理连接，但小王仍旧不能享受两台计算机之间的文件传输功能。因此本项目在项目一基础上，能够将一台计算机的大文件通过网络传送至另一台计算机上，并能解决在网络使用过程中出现的问题，如网络中断、网络通信速度慢等问题。



项目分析

要实现本项目，首先在两台计算机上正确安装并配置网络通信协议，在确保网络连通的情况下，运行计算机操作系统内置的工具软件超级终端，或者对计算机系统进行配置，采取资源共享的方式，实现两台计算机大文件的传送要求。计算机网络在使用的过程中可能遇到一些问题，如小王家中的计算机之间不能传输文件了，应该是最常见的一种；而有些问题比较古怪，

且很难从中梳理头绪,这时候需要有科学的故障解决方法和合适的故障检测工具。解决问题的方法有多种,最为科学的故障解决方法是网络分层,将复杂的问题分解成一系列相互衔接的小任务,然后逐一解决,最终得到整个问题的解决。故障检测工具也有很多,若采用硬件故障检测工具,可能会增加投入成本;若采用开源的网络协议分析工具如 Wireshark 软件,可以在任意数量机器上使用,不用担心授权和付费问题。因此,本项目采用使用超级终端传输文件和使用 Wireshark 捕获并分析协议数据包两个任务来实现。



学习目标

通过完成本项目的操作任务,读者将:

- 了解网络层次结构的产生背景和作用。
- 理解分层模型中协议、协议数据单元、接口与服务等重要概念。
- 了解 OSI 模型的产生背景及各层功能。
- 掌握 TCP/IP 各层功能和协议分布, OSI 模型与 TCP/IP 模型的区别。
- 掌握 IP 地址的作用及 IP 协议的功能。
- 能够安装并配置 TCP/IP 协议通信参数。
- 会使用协议分析工具对计算机网络问题进行处理。

任务 1 使用超级终端传输文件

2.1.1 任务目的及要求

本任务需要将小王家中一台电脑上的大文件成功传送至另一台电脑上。通过本任务,读者可了解网络分层,掌握网络协议和网络体系结构的概念,掌握 IP 地址和 IP 协议的应用。

为了完成这一任务,首先需要在 Windows 系统上安装并配置 TCP/IP 协议,利用 Windows 自带的常见的网络测试工具 ping,检测是否正确安装 TCP/IP 通信协议和网络的连通性。然后安装并配置超级终端软件,实现两台计算机之间的文件传输。

2.1.2 知识准备

本任务知识点的组织与结构,如图 2-1 所示。

读者在学习本部分内容的时候,请认真领会并思考以下问题:

下问题:

- (1) 试分析网络分层的必要性和好处?
- (2) 协议数据单元的作用是什么? 在分层模型中,每层上的协议数据单元叫什么?
- (3) IP 地址有什么作用? 主要分为哪几类?

1. 网络的层次结构

“化繁为简,各个击破”是人们解决复杂问题的常用方法。对网络进行层次划分就是将计算机网络这个庞大的、复杂的问题划分成若干较小的、简单的问题。通过“分而治之”,解决这些较小的、简单的问题,从而解决计算机网络这个大问题。

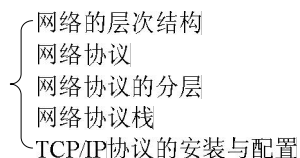


图 2-1 任务 1 知识点结构示意图

（1）邮政系统的层次结构。

为了更好地理解分层模型及协议等概念，下面以图 2-2 所示的邮政系统作为类比来说明这个问题。

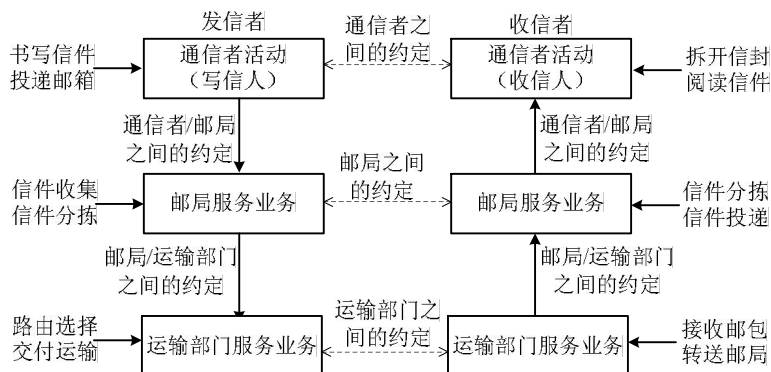


图 2-2 网络分层模型类比邮政系统模型

假设 Alice 想给重庆的朋友 Bob 写一封信，Bob 最后是怎样得到信件的呢？事实上，实际的邮政系统是一个复杂的系统，从书写信件开始，到收信人收到信件，期间要经过多个步骤，这个步骤等价于层次（Layer）。从图 2-2 可以看出，至少涉及以下几个步骤：

1) 发信方与收信方的层次是相等的，但层次的过程方向是相反的。

2) 发信人需按照国内信件的信封书写标准，在信封的相应位置写上收信人的地址、姓名和发信人的地址。

3) 各地邮局及其工作人员必须按照信封上提供的信息，并按照信件的邮寄要求，完成信件邮寄任务。

从图中我们可以清楚地看到，信件的传输工作被分为三个层次：用户、邮局和运输部门，每个层次完成各自的任务。同时，用户利用邮局的投递服务（Service），邮局利用运输部门提供的运输服务，最终完成信件的投递功能。

（2）网络分层结构的好处。

如同邮政系统一样，计算机网络也是一个复杂的系统，也采用了层次化体系结构，并有许多好处。

- 1) 根据网络实际处理过程，按功能分类，从而便于理解和掌握。
- 2) 能够定义标准接口（Interface），使不同厂商制造的硬件之间可以互联。
- 3) 工程师在设计和研发网络硬件时，可以把思维限定在一定范围之内。
- 4) 当某层内部发生变化时，不会给其他层带来影响。
- 5) 在进行网络故障分析时，分层的方法还能帮助我们分解、简化问题，定位故障点。

2. 网络协议

生活中有很多各种各样的协议，完成不同的功能，如雇佣协议、保密协议、购房协议等。这些协议有一些共同点：由双方共同商定，由双方共同认可；共同遵守协议，按协议规定办事；有针对性，有一定的法律效力和权威。

在计算机网络中，协议（Protocol）是指通信双方为了实现通信而设计的约定或会话规则。例如上述例子中的邮政系统，按照约定俗成的规则，发信人写信的时候将收信人的地址、邮编写在信封的左上角，将自己的地址和邮编写在信封的右下角，而不能反之。

每一个协议是针对某一个特定的目标和需要而解决的问题，新的网络服务出现，新的协议就会出现。因此，协议的制定和实现是计算机网络重要组成部分。执行某种通信功能所需的一组内在相关协议称为协议簇（协议栈）。协议簇由主机和网络设备在软件、硬件或同时在这两者中实施。

网络协议通常由语义、语法和时序三部分组成。

（1）语法（Syntax）：数据与控制信息的结构或格式，定义怎么做。

（2）语义（Semantics）：需要发出何种控制信息、何种动作以及做出何种应答，定义做什么。

（3）时序（Timing）：数据收发的速率匹配和接收排序，定义何时做。

下面以生活中两个人打电话的过程为例，说明协议的组成，如图 2-3 所示。

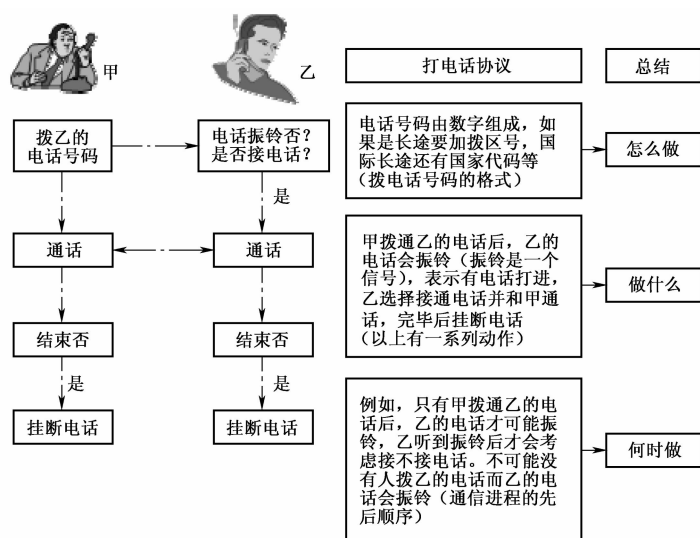


图 2-3 协议组成示例

3. 网络协议的分层

在计算机网络体系结构思想的指导下，网络协议也采用了分层结构，比如当今使用最广泛的 TCP/IP 协议，就是从原理上分为四层（该内容将在后面展开）。

（1）网络协议采用分层结构的原因。

在分层思想下，每一层都有明确的任务或相对独立的功能，不需要关心下层如何实现，只需要知道它通过层间接口（Interface）提供服务（Service）即可。灵活性好，易于实现和维护，有利于标准化。

（2）网络协议各层次之间的关系。

1) 下层为上层提供服务，而上层并不关心下层服务是如何实现的。

2) 每一对相邻层之间有一个接口（接口就是相邻层交换信息的地方，比如用户和邮局两层之间的接口为邮箱），相邻层之间通过接口交换数据，提供服务。

3) 实体（Entity）是表示任何可以发送或接收信息的硬件或软件进程。发送方和接收方处于同一层的实体叫做对等实体（Peer Entity）。数据信息传输可以发生在某一层已经建立起的对等体之间，也可以发生在同一系统的相邻层次实体之间。

4) 对等层之间的通信是虚通信，只有传输介质上完成的通信是实通信。

5) 从层次角度看数据的传输, 发送方数据往下层传递, 接收方数据向上层传递, 通常分别将发送方和接收方所历经的这种过程称为数据封装和数据拆封。

(3) 协议数据单元 (Protocol Data Unit, PDU)。

协议数据单元就是不同站点的各层对等实体之间, 为实现该层协议所交换的信息单元。考虑到协议的要求, 如时延 (Delay)、效率 (Efficiency) 等因素, 网络中的 PDU 在不同的网络层次有各自不同的名称, 其组成和功能也不同, 分别有着各自的特点, 从而组成了各种计算机网络。图 2-4 给出了后面要讨论的 OSI 参考模型各层的协议数据单元。

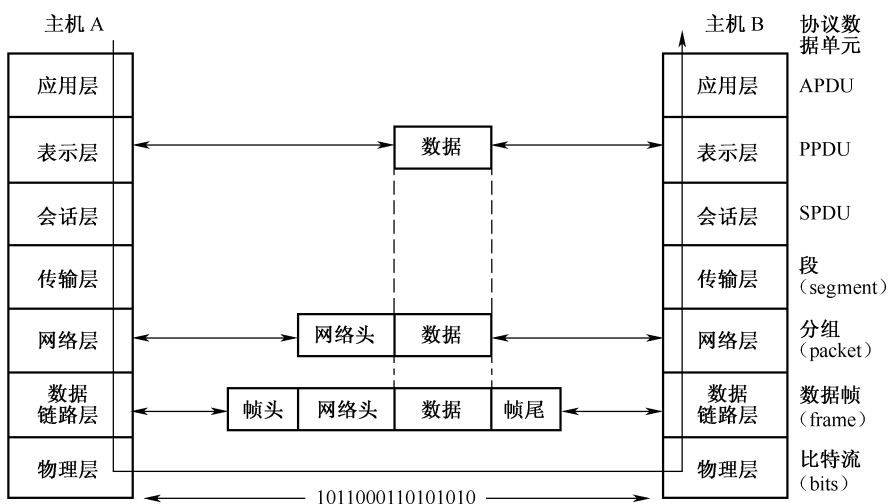


图 2-4 OSI 各层协议数据单元

知识链接：由于早期对英文名词的中文翻译缺乏标准, 在通信领域, “Packet” 一词被习惯性地翻译成“包”、“分组”、“报文”等多种形式, 本书将根据特定场合不加区分地使用这些中文名称。因此, OSI 参考模型网络层的 PDU 也称为“分组”或“数据包”或“数据报”, 而 OSI 参考模型传输层的 PDU 称为“段 (Segment)”。

(4) 层、服务与接口之间的关系。

层、服务与接口之间的关系, 如图 2-5 所示, N 层向相邻的高层提供服务, N 层向相邻的低层调用服务, 相邻的高层协议通过服务访问点 (Service Access Point, SAP) 调用低层协议 (如用户和邮局两层之间的 SAP 可看成投递信件的邮箱小孔, 而 SAP 地址可看成邮箱在这个城市中的位置)。

1) 服务的定义指明了该层做什么, 而不是上层的实体如何访问这一层, 或这一层是如何工作的。

2) 接口告诉它上面的进程应该如何访问本层, 它规定有哪些参数以及结果是什么, 但未说明本层内部是如何工作的。

3) 每一层的对等 (Peer-to-Peer) 协议是本层内部的事情, 它可以是任何协议, 只要它能够提供所承诺的服务即可。

4. 网络协议栈

接入网络的任何一台计算机需赋予一个协议栈 (Stack, 也称为协议包), 协议栈提供了使计算机能够进行网络通信的软件。这些协议栈以及连接到计算机的任何一个网络设备的驱动程序

序，提供了非常重要的软件连接，允许应用程序与网络通信。可以这么说，协议加上驱动程序等于网络接入。目前，最常见的协议包有以下几种：

(1) 传输控制协议/网际协议 (TCP/IP) 是 Internet 上使用的协议栈，也是 Windows Server 2000/2003、Windows XP 和 Novell NetWare 5 及其更高版本的默认协议。

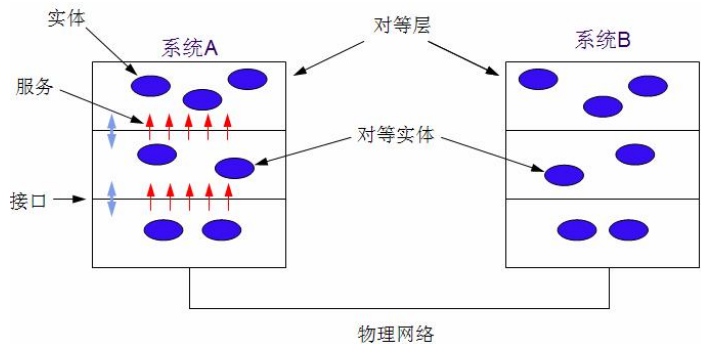


图 2-5 层、服务与接口之间关系图

(2) 互联网络分组交换/顺序分组交换 (Internetwork Packet Exchange/Sequences Packet Exchange, IPX/SPX) 是 NetWare 4.x 及其更低版本最常使用的协议栈。

(3) NetBIOS 增强用户接口 (NetBIOS Enhanced User Interface, NetBEUI) 是由 IBM 为 PC 联网开发的协议栈，一般都使用在 IBM 和 Windows 产品中，例如 Windows NT、Windows 9x 和 Windows for workgroups。

(4) AppleTalk 是由 Apple 公司为它的 Macintosh 计算机开发的协议栈，并且仍然使用在基于 Macintosh 的网络中。

(5) 系统网络体系结构 (SNA) 是由 IBM 为使用它的大型计算机开发的协议栈。

5. TCP/IP 协议栈的安装与配置

实际应用中最为广泛的协议栈是 TCP/IP，由它组成了 Internet 的一整套协议。在以 TCP/IP 协议栈为通信协议的网络上，每台连接在网络上的计算机与设备都称为“主机”，而主机与主机之间的沟通需要通过以下三个桥梁：IP 地址、掩码和默认网关。

(1) IP 地址。

1) IP 地址的作用与表示。

IP 地址是 TCP/IP 协议栈中 IP 协议定义的网络层地址。在以 TCP/IP 协议栈为通信协议的网络上，每台主机都必须拥有唯一的 IP 地址，该 IP 地址不但可以用来标识每一台主机，其中也隐含着网络的信息。TCP/IP 协议栈中的 IP 协议提供了一种通用的地址格式，该地址为 32 位的二进制数。为了方便使用，一般采用点分十进制法来表示 (将 32 位等分成四个部分，每个部分 8 位长，之间用英文句点分开，以十进制表示)，如 192.168.10.1。

2) IP 地址的组成。

32 位的 IP 地址包含了 Network ID 与 Host ID 两部分，如图 2-6 所示。

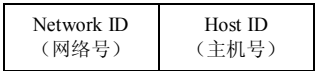


图 2-6 IP 地址的层次结构

- Network ID: 每个网络区域都有唯一的网络标识码。

- **Host ID:** 同一个网络区域内的每一台主机都必须有唯一的主机标识码。

IP 地址的编址方式明显地携带了位置信息。IP 地址不仅包含了主机本身的地址信息，而且还包含了主机所在网络的地址信息，因此，将主机从一个网络移到另一个网络时，主机 IP 地址必须进行修改以正确地反映这个变化，否则不能通信。实际上，IP 地址与生活中的邮件地址非常相似。生活中的邮件地址描述了信件收发人的地理位置，也具有一定的层次结构（如城市、区、街道等）。如果收件人的位置发生变化（如从一个区搬到了另一个区），那么邮件的地址就必须随之改变，否则邮件就不可能送达收件人。

3) IP 地址的分类。

在 32 位的 IP 地址中，哪些位代表 Network ID，哪些位代表 Host ID？这个问题看似简单，意义却很重大，因为当地址长度确定后，Network ID 长度将决定整个互联网中能包含多少个网络，Host ID 长度则决定每个网络能容纳多少台主机。

在 Internet 中，网络数是一个难以确定的因素，而不同种类的网络规模也相差很大。有的网络具有成千上万台主机，而有的网络仅仅有几台主机。为了适应各种网络规模的不同，IP 协议将 IP 地址分成 A、B、C、D 和 E 五类，它们分别使用 IP 地址的前几位加以区分，如图 2-7 所示。从图 2-7 中可以看到，利用 IP 地址的前 4 位就可以分辨出它的地址类型。

地址类	第 1 个二进制八位组范围（十进制）	第 1 个二进制八位组的比特位（绿色位不变）	地址的网络部分 (N) 和主机部分 (H)	默认子网掩码（十进制和二进制）	可能的网络数量和每个网络可能的主机数量
A	1-127**	00000000-01111111	N H H H	255.0.0.0	128 个网络 (2^7) 每个网络 16,777,214 台主机 (2^{24-2})
B	128-191	10000000-10111111	N N H H	255.255.0.0	16,384 个网络 (2^{14}) 每个网络 65,534 台主机 (2^{16-2})
C	192-223	11000000-11011111	N N N H	255.255.255.0	2,097,150 个网络 (2^{21}) 每个网络 254 台主机 (2^{8-2})
D	224-239	11100000-11101111	不适用（组播）		
E	240-255	11110000-11111111	不适用（实验）		

图 2-7 5 类 IP 地址

在五大类的 IP 地址中，只有 A、B、C 类可供 Internet 网络上的主机使用。在使用时，还需要排除以下几种特殊的 IP 地址，如表 2-1 所示。

表 2-1 特殊 IP 地址

Network ID	Host ID	源地址使用	目的地址使用	代表的意义
0	0	可以	不可	不确定的 IP 地址或默认路由
0	Host ID	可以	不可	在本网络上的某个主机
全 1	全 1	不可	可以	只在本网络上进行广播(受限广播)
Network ID	全 1	不可	可以	对特定 Network ID 上的所有主机广播（直接广播）
127	任何数	可以	可以	用作本地软件回送测试

(2) 掩码的作用。

当以 TCP/IP 协议栈为通信协议的网络上的主机相互通信时，怎么知道相互通信的主机是否在相同的网段内呢？

1) 掩码的定义。

掩码采用与 IP 地址相同的位格式，由 32 位长度的二进制位构成，也被分为 4 个 8 位组并

采用点分十进制来表示。但在掩码中，所有与 IP 地址中的网络位部分对应的二进制位取值为 1，而与 IP 地址中的主机位部分对应的位则取值为 0。

2) 默认掩码。

A、B、C 三类网络的默认掩码如表 2-2 所示。

表 2-2 A、B、C 类网络的默认掩码（二—十进制对应）

类别	二进制子网掩码	十进制子网掩码
A	11111111.00000000.00000000.00000000	255.0.0.0
B	11111111.11111111.00000000.00000000	255.255.0.0
C	11111111.11111111.11111111.00000000	255.255.255.0

3) 掩码的作用。

掩码主要有两个作用，一是用来分割 IP 地址的主机号和网络号，并且 IP 地址和掩码必须成对使用才有意义；二是掩码可以用来划分子网（Subnet）。本项目讨论第一个作用，第二个作用将在项目五中进行深入讨论。

分割 IP 地址的主机号和网络号的方法：（IP 地址）AND（掩码）=Network ID，即将给定 IP 地址与掩码对应的二进制位做逻辑“与”运算（规则：“1”和任何数相与，结果为任何数；“0”和任何数相与，结果为 0），所得的结果为 IP 地址的 Network ID。下面举例说明这一方法的使用。

假定甲主机的 IP 地址为 202.197.147.3，使用默认掩码 255.255.255.0，试问这个 IP 地址的 Network ID 是多少？解析过程如图 2-8 所示。

202.197.147.3	→	1 1 0 0 1 0 1 0	•	1 1 0 0 0 1 0 1	•	1 0 0 1 0 0 1 1	•	0 0 0 0 0 0 1 1
255.255.255.0	→	1 1 1 1 1 1 1 1	•	1 1 1 1 1 1 1 1	•	1 1 1 1 1 1 1 1	•	0 0 0 0 0 0 0 0
<hr/>								
“与”后的结果	→	1 1 0 0 1 0 1 0	•	1 1 0 0 0 1 0 1	•	1 0 0 1 0 0 1 1	•	0 0 0 0 0 0 0 0
	→	202	•	197	•	147	•	0

图 2-8 IP 地址与掩码对应的二进制位做逻辑“与”运算

若乙主机的 IP 地址为 202.197.147.18（掩码为 255.255.255.0），当甲主机要和乙主机通信时，甲主机和乙主机都会分别将自己的 IP 地址和掩码做“与”运算，得到两台主机的 Network ID 都是 202.197.147.0，因此判断这两台主机是在同一个网络区域，可以直接通信。如果两台主机不在同一个网络区域内（Network ID 不同），则无法直接通信，必须通过默认网关或路由器这一类设备进行通信。

知识链接：IP 地址和掩码必须成对使用，一个孤立的 IP 地址是没有任何意义的。有什么方法可以快速准确地将十进制表示的 IP 地址转化为二进制表示的 IP 地址？在得到 Network ID 后，如何得到 Host ID？最简单的方法：（IP 地址）-（Network ID）=Host ID。

（3）默认网关（Default Gateway）。

网关（Gateway）是一个网络通向其他网络的 IP 地址。默认网关的意思是一台主机如果找不到可用的网关，就把数据包发给默认指定的网关，由这个网关来处理数据包，因此一台主机的默认网关是不可以随随便便指定的，必须正确指定，否则无法与其他网络的主机通信。

（4）IP 地址的配置管理。

IP 地址的分配可以采用静态和动态两种方式。所谓静态分配是指由网络管理员为主机指

定一个固定不变的 IP 地址并手工配置到主机上。动态分配目前主要通过动态主机配置协议（Dynamic Host Configuration Protocol, DHCP）来实现。采用 DHCP 进行动态主机 IP 地址分配的网络环境中至少具有一台 DHCP 服务器, DHCP 服务器上拥有可供其他主机申请使用的 IP 地址资源, 客户机通过 DHCP 请求向 DHCP 服务器提出关于地址分配或租用的要求。

何时使用静态分配 IP 地址? 何时使用动态分配 IP 地址? 最重要的一个决定因素是网络规模的大小。大型网络和远程访问网络适合动态地址分配, 而小型网络适合静态地址分配。最好是普通客户机的 IP 地址采用动态分配, 而服务器等特殊主机采用静态分配, 两者相结合的方式对 IP 地址进行管理。

2.1.3 任务实施

1. 任务实施条件

装有 Windows 2003/XP 操作系统的计算机各 1 台, Windows 2003/XP CD-ROM 或者 DVD 各一张, 每台计算机已正确安装以太网卡, 连接两台计算机的交叉网线 1 条。

2. 安装 TCP/IP 协议

在操作系统的安装过程中若已自动安装了 TCP/IP 协议栈, 可以省略如下步骤。若计算机上的 TCP/IP 协议栈丢失或不可用的时候, 可以执行以下步骤, 完成 TCP/IP 协议栈的安装。

(1) 选择“开始”→“设置”→“网络和拨号连接”, 弹出如图 2-9 所示的“网络连接”窗口。



图 2-9 “网络连接”窗口

(2) 在需要进行配置的连接上单击右键并选择“属性”, 弹出如图 2-10 所示“本地连接属性”对话框。

(3) 在“此连接使用下列项目”列表框里寻找你要使用的 TCP/IP 协议, TCP/IP 协议没有勾选, 说明没有安装, 如图 2-11 所示。



图 2-10 “本地连接属性”对话框



图 2-11 查找需要安装的组件

(4) 单击“安装”按钮，弹出“选择网络组件类型”对话框，确保已经安装了网络客户和服务，选择“协议”组件，如图 2-12 所示，然后单击“添加”按钮。

(5) 在弹出的“选择网络协议”的对话框中，选择厂商“Microsoft”，选择网络协议“Microsoft TCP/IP 版本 6”，如图 2-13 所示，单击“确定”按钮。

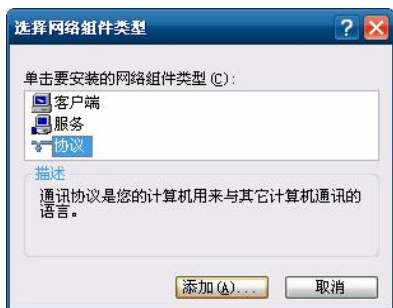


图 2-12 选择要安装的网络组件



图 2-13 选择网络协议

(6) 此时，“选择网络协议”界面中若没有我们要安装的协议选项，则单击“从磁盘安装...”按钮，安装向导会要求你给出协议包软件所在的位置，不管它是在一个硬盘、一个共享的网络磁盘、一个软盘或者可移动的驱动器、一个 CD-ROM 或者 DVD 上，如图 2-14 所示。

3. 测试 TCP/IP 协议栈

(1) 验证 TCP/IP 协议栈安装。

选择“开始”→“设置”→“网络和拨号连接”，在你想进行配置的连接上单击右键并选择“属性”，可以看见“本地连接属性”界面中 TCP/IP 协议栈已经安装，如图 2-15 所示。

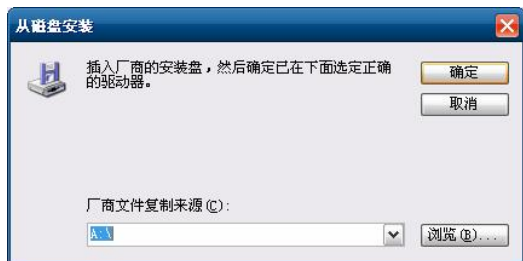


图 2-14 定位协议包软件的位置



图 2-15 TCP/IP 的安装

(2) 测试 TCP/IP 协议栈正确运行。

1) 选择“开始”→“运行”，出现如图 2-16 所示界面，在“运行”界面中输入“cmd”，回车后，出现如图 2-17 所示的 DOS 命令运行界面。

2) 在 DOS 命令运行界面中输入 ping 127.0.0.1，回车后出现如图 2-18 所示的界面。ping

是一个基于网际控制报文协议（Internet Control Message Protocol, ICMP）实现的小程序，主要用来测试网络连通性；127.0.0.1 是一个回环地址，后面将对 ping 的使用做详细解释。ping 127.0.0.1 主要用来检测 TCP/IP 协议栈是否正确安装。



图 2-16 运行界面



图 2-17 DOS 命令运行界面

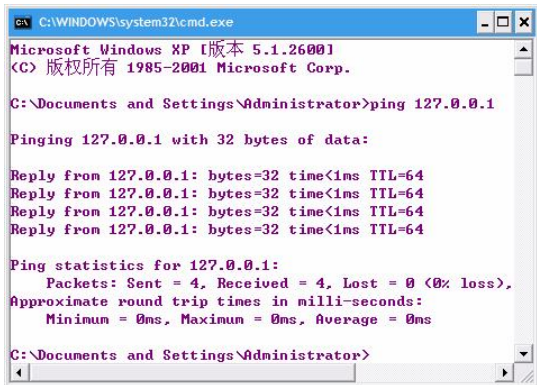




图 2-18 执行 ping 命令的输出结果

图 2-18 的输出结果说明 TCP/IP 协议栈已经正确安装。否则，说明 TCP/IP 协议栈没有安装或 TCP/IP 协议栈工作不正常。



4. 连接两台计算机

(1) 确认计算机的以太网卡已正确安装。

右键单击桌面上“我的电脑”图标，选择“属性”，弹出“系统属性界面”，单击“硬件”选项卡，弹出“设备管理器”界面，如图 2-19 所示。

在网络适配器选项，若出现 ，说明网卡已正确安装；若出现 ，说明网卡安装有问题或者没有安装，网卡处于禁用状态除外。

(2) 用网线连接计算机。

用项目一制作的交叉网线将两台计算机通过 RJ-45 接口连接起来，将网线的一端插入一台计算机的 RJ-45 接口，将网线的另一端插入另一台计算机的 RJ-45 接口。在“网络连接”窗口中，若本地连接出现 ，说明两台计算机之间的物理连接正常；若本地连接出现 ，说明两

台计算机之间的物理连接有问题，可能的原因是网线故障，或者网线的 RJ-45 接口与计算机的 RJ-45 接口接触不好。

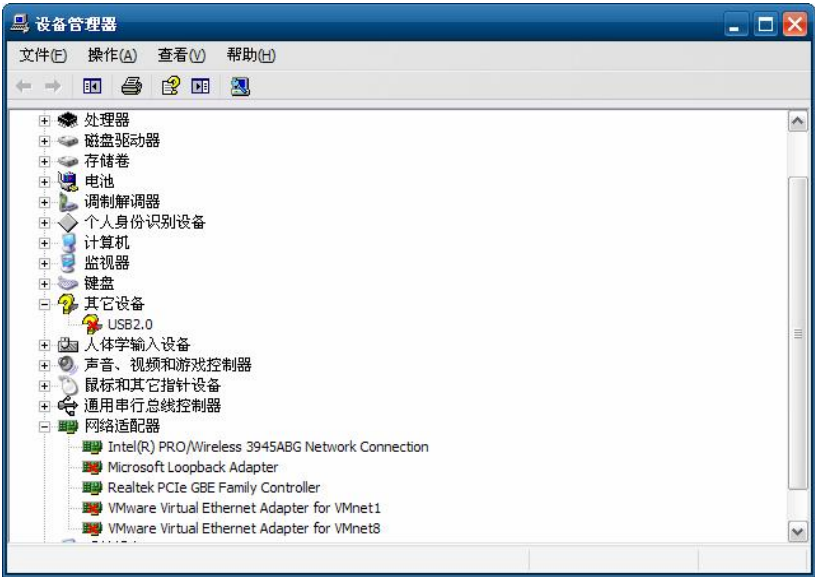


图 2-19 设备管理器界面

5. 配置计算机 TCP/IP 通信参数

(1) 右键单击桌面“网上邻居”图标，选择“属性”，弹出“网络连接”窗口，右键单击“本地连接”（一般计算机上只有一块网卡，若有多块网卡，可能出现多个“本地连接”，此时选定需要的“本地连接”即可），选择“属性”，弹出“本地连接属性”界面，选择“Internet 协议（TCP/IP）”，如图 2-20 所示，单击“属性”按钮。



图 2-20 “本地连接属性”对话框

知识链接：在“本地连接属性”对话框中，勾选“连接后在通知区域显示图标”和“此连接被限制或无连接时通知我”，以便在任务栏查看网络的连接情况，如图 2-21 所示。



图 2-21 本地连接通知

（2）在弹出的“Internet 协议（TCP/IP）属性”对话框中，选择“使用下面的 IP 地址”，如图 2-22 所示。

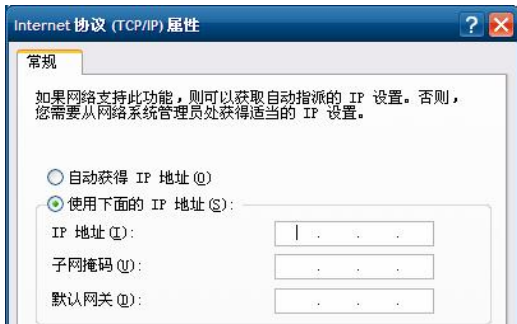


图 2-22 “Internet 协议（TCP/IP）属性”对话框

知识链接：此处因为网络中没有 DHCP 服务器，故只能采用手工的方式配置 IP 地址。

（3）在对话框的“IP 地址”栏中输入 192.168.10.10；“子网掩码”栏中输入 255.255.255.0；“默认网关”栏中不需要输入任何值，如图 2-23 所示，然后单击“确定”按钮。

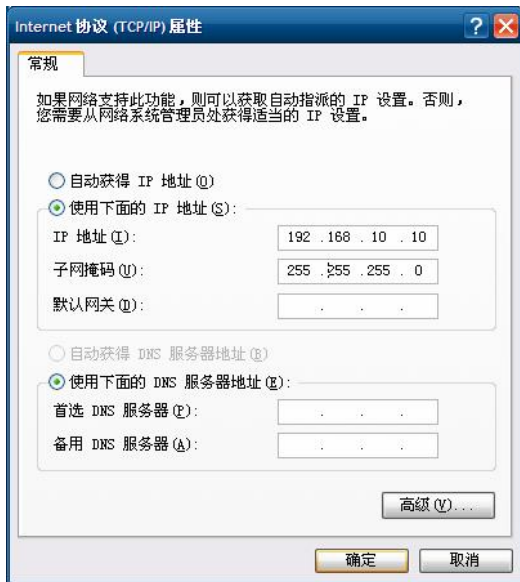


图 2-23 配置 IP 地址参数

知识链接：在同一个网络区域内通信的主机上不需要配置默认网关。

（4）验证已配置的 IP 地址。

在 DOS 界面下，使用 `ipconfig /all` 命令，可以查看 IP 地址的配置情况，如图 2-24 所示。

（5）在另一台计算机上，重复步骤（1）～（4），完成 IP 地址配置，参数为：IP 地址 192.168.10.11，掩码为 255.255.255.0。

（6）测试两台计算机之间的连通情况。

在任何一台计算机的 DOS 界面下，ping 对方 IP 地址，验证主机之间的网络连通情况，图 2-25 为在 IP 地址为 192.168.10.11 的主机上，在 DOS 界面下，执行 `ping 192.168.10.10` 的输出结果。

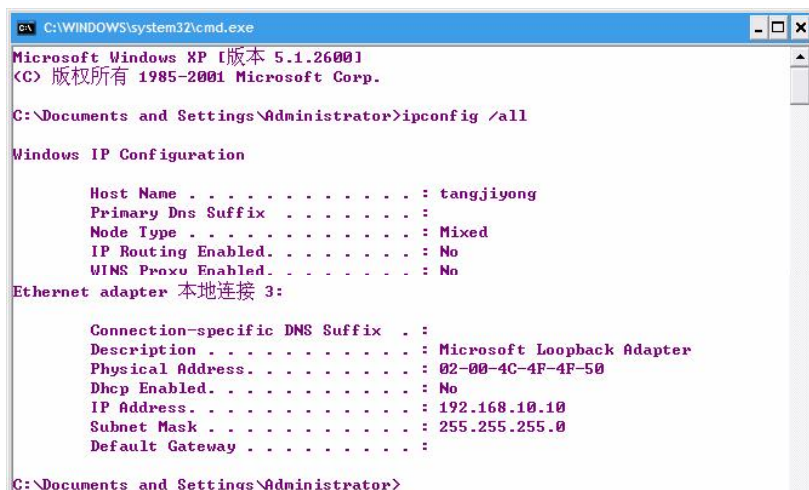


图 2-24 验证 IP 地址配置

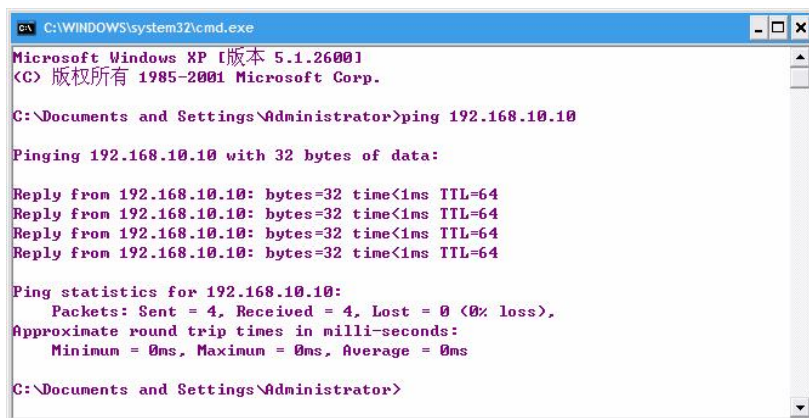


图 2-25 验证网络连通性

输出结果表明，两台计算机之间的网络连通情况正常。接下来，就可以在计算机上配置超级终端了。

6. 超级终端的配置与应用

(1) 运行“开始”→“控制面板”→“添加或删除命令”，单击“添加/删除 Windows 组件”图标，打开“Windows 组件向导”对话框，如图 2-26 所示。依次双击“附件和工具”→“通讯”选项，进入“通讯”对话框，选中“超级终端”复选框，在“通讯”、“附件和工具”对话框中依次单击“确定”按钮，在“Windows 组件向导”对话框中单击“下一步”按钮。

(2) 系统开始安装超级终端所需的组件，进程如图 2-27 所示。安装过程中，需要 Windows Server 2003 系统源程序，可由用户指定 Windows Server 2003 系统源程序所在路径，以便复制所需文件。

(3) 完成文件复制后，系统会自动打开如图 2-28 所示的向导对话框，直接单击“下一步”按钮，完成超级终端的安装过程。



图 2-26 安装 Windows 组件向导



图 2-27 安装超级终端所需的组件



图 2-28 安装超级终端组件向导

(4) 超级终端的应用。

1) 启动过程: 运行“开始”→“所有程序”→“附件”→“通讯工具”→“超级终端”命令。或者“开始”→“运行”命令, 输入 hypertrm 即可, 如图 2-29 所示。



图 2-29 超级终端运行界面

2) 将一台计算机的文件传输至另一台计算机上。注意观察传输速率的快慢情况。

3) 在两台计算机上通过超级终端体验文字传递过程。

2.1.4 课后习题

1. 网络协议包含三要素, 分别是语义、时序和 ()。
2. IP 地址由 Network ID 和 () 组成。
3. 掩码的作用是 ()。
4. 协议在数据通信中起到 () 作用。
 - A. 为每种类型的通信指定通道或介质带宽
 - B. 指定将用于支持通信的设备操作系统
 - C. 为进行特定类型通信提供所需规则
 - D. 确定电子规范以实现通信
5. 下列有关网络协议的陈述中, () 是正确的。
 - A. 网络协议定义了所用硬件类型及其如何在机架中安装
 - B. 网络协议定义了消息在源地址和目的地址之间如何交换
 - C. 网络协议都是在 TCP/IP 的网络接入层发挥作用
 - D. 只有在远程网络中的设备之间交换消息时才需要使用网络协议
6. IP 地址 10.0.10.32 和掩码 255.0.0.0 代表的是一个 ()。
 - A. 主机地址
 - B. 网络地址
 - C. 广播地址
 - D. 以上都不对
7. 若某台计算机的 IP 地址是 192.168.8.20, 子网掩码是 255.255.255.0, 则网络号和主机号分别是 ()。
 - A. 网络号: 199 主机号: 168.8.20
 - B. 网络号: 192.168 主机号: 8.20
 - C. 网络号: 192.168.8 主机号: 20
 - D. 网络号: 255.255.255 主机号: 0
8. IP 地址为 195.100.8.200 (掩码为 255.255.255.0), 这是 () 类 IP 地址。

A. A B. B C. C D. D

9. IP 地址由一组（ ）的二进制数字组成。

A. 8 位 B. 16 位 C. 32 位 D. 64 位

10. 设有两台计算机，一台计算机的 IP 地址设置为 193.100.0.18，子网掩码设置为 255.255.255.0；另一台计算机的 IP 地址设置为 193.100.0.20，子网掩码设置为 255.255.255.0。判断两台计算机是否在同一子网中？

11. 设有两台计算机，一台计算机的 IP 地址设置为 193.100.0.129，子网掩码设置为 255.255.255.192；另一台计算机的 IP 地址设置为 193.100.0.66，子网掩码设置为 255.255.255.192。判断两台计算机是否在同一子网中？

任务 2 使用 Wireshark 捕获并分析协议数据包

2.2.1 任务目的及要求

了解网络原理尤其是网络协议的内部实现机制，是解决网络问题的必要前提。通过本任务让读者掌握 OSI 参考模型的层次结构和各层功能；OSI 参考模型中数据的封装和传递；TCP/IP 体系结构的各层功能和典型协议。

针对 TCP/IP 体系结构不同层次协议的功能和特点，学会用 Wireshark 协议分析仪捕获数据包的方法，利用 Wireshark 协议分析仪了解层次模型的结构及各层主要协议，为后续学习打下坚实的基础。

2.2.2 知识准备

本任务知识点的组织与结构，如图 2-30 所示。

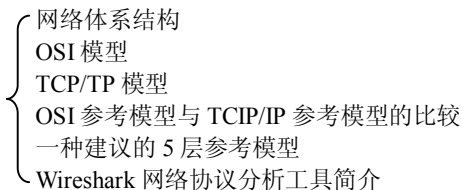


图 2-30 任务 2 知识点结构示意图

读者在学习本部分内容的时候，请认真领会并思考以下问题：

- (1) TCP/IP 参考模型产生的背景是什么？
- (2) TCP/IP 参考模型到底有几层？实际网络中使用了哪几层的 TCP/IP 参考模型？
- (3) 请对 TCP/IP 参考模型作出合理的评价？

1. 网络体系结构

引入分层模型以后，通常将计算机网络系统中的层、各层中的协议以及层次之间的接口的集合称为计算机网络体系结构（Network Architecture）。网络模型有两种基本类型：协议模型和参考模型。

(1) 协议模型提供了与特定协议栈结构精确匹配的模型，如美国国防部开发的 TCP/IP 模型，成为 Internet 赖以发展的实际标准（工业标准）。

(2) 参考模型为各类网络协议和服务之间保持一致性提供了通用的参考，如国际标准化组织(International Standard Organization, ISO)制定开发的开放系统互联参考模型(Open System Interconnection/Reference Mode, OSI/RM)。

知识链接：计算机的网络结构可以从网络体系结构、网络组织结构和网络配置三个方面来描述。网络体系结构是从功能上来描述计算机网络；网络组织结构是从网络的物理结构和实现方法来描述计算机网络；网络配置是从网络应用方面来描述计算机网络。

2. OSI 参考模型

(1) OSI 模型提出的背景。

自 IBM 在 20 世纪 70 年代推出 SNA 系统网络体系结构以来，很多公司也纷纷建立自己的网络体系结构，这些体系结构的出现大大加快了计算机网络的发展。但由于这些体系结构的着眼点往往是各自公司内部的网络连接，没有统一的标准，因而它们之间很难互联起来。在这种情况下，ISO 开发了开放系统互联参考模型 OSI/RM。“开放”这个词表示：只要遵循 OSI 标准，一个系统就可以和位于世界上任何地方遵循了 OSI 标准的其他任何系统进行互联。

OSI 参考模型为网络提供了一个可实践的模型，该模型提供了两种工具。对于网络技术人员来说，OSI 参考模型是诊断故障的一个强有力工具。技术人员掌握了这个模型后，就可以快速定位问题是出在哪一层上，因而可以有针对性地提出解决方案，从而避免因错误线索而浪费大量时间。OSI 参考模型还提供了一种用于描述网络的通用语言，这为人们相互之间交流网络功能提供了一种方法，帮助人们形成网络上许多部件的概念。如路由器工作在 OSI 参考模型中的第三层，它有时也被技术人员和 Web 站点称为第三层交换机，这里就是把 OSI 参考模型当作描述语言来使用。

(2) OSI 参考模型的结构。

OSI 参考模型如图 2-31 所示，OSI 模型是一个设计网络系统的分层次的框架，它使得所有类型的计算机系统可以互相通信。OSI 模型包括 7 个独立但又相关的层次：物理层、数据链路层、网络层、传输层、会话层、表示层和应用层。

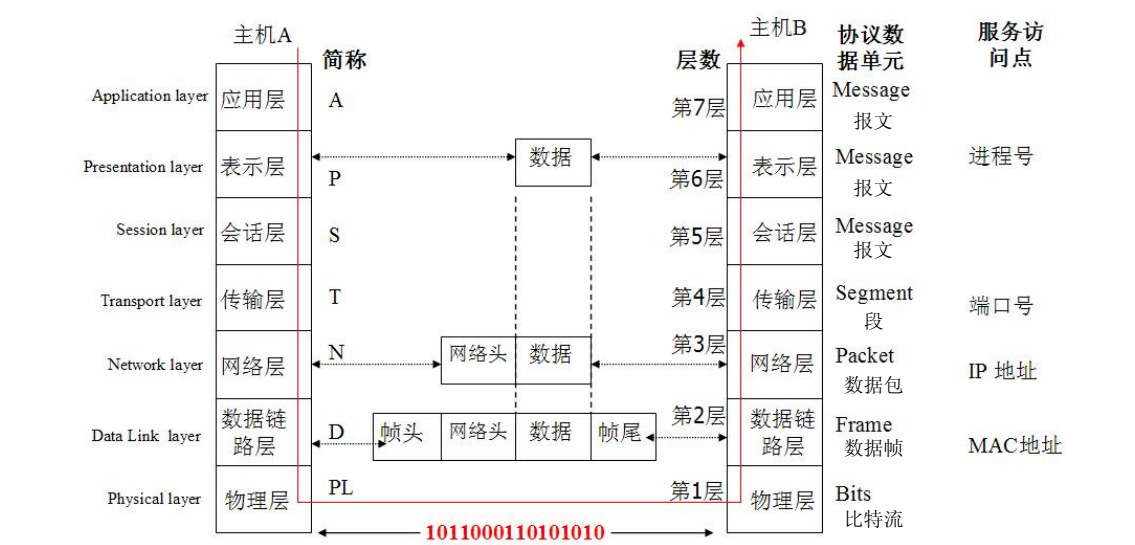


图 2-31 OSI 参考模型的层次结构

OSI 参考模型的最上层（应用层）提供了一组接口，允许网络应用程序（例如 Windows Explorer、电子邮件包或 Web 浏览器）访问网络服务。因此，应用程序驻留在参考模型之上，并且与 OSI 模型的顶层通信。OSI 参考模型的底层为物理层，是联网介质和通过这些介质的信号驻留的地方。处理网络通信所必需的所有活动都发生在顶层和底层之间。

知识链接：这里有两个记住 OSI 参考模型的 7 层的好方法。从下至上，从物理层开始，首字母缩写词是 “Please Do Not Throw Sausage Pizza Away”（请不要扔掉香肠比萨饼）。从上至下，从应用层开始，首字母缩写词是 “All People Seem To Need Data Processing”（所有人似乎都需要数据处理）。

（3）OSI 参考模型的组织。

由通信子网和资源子网组成的网络结构，是对计算机网络概念的低级抽象；由 7 个独立但相关的层次组成的网络结构，是对计算机网络概念的高级抽象。OSI 参考模型的核心包含三大层次，如图 2-32 所示。高三层由应用层、表示层和会话层组成，面向信息处理和网络应用；低三层由网络层、数据链路层和物理层组成，面向通信处理和网络通信；中间层次为传输层，为高三层的网络信息处理应用提供可靠的端（End-to-End）到端通信服务。

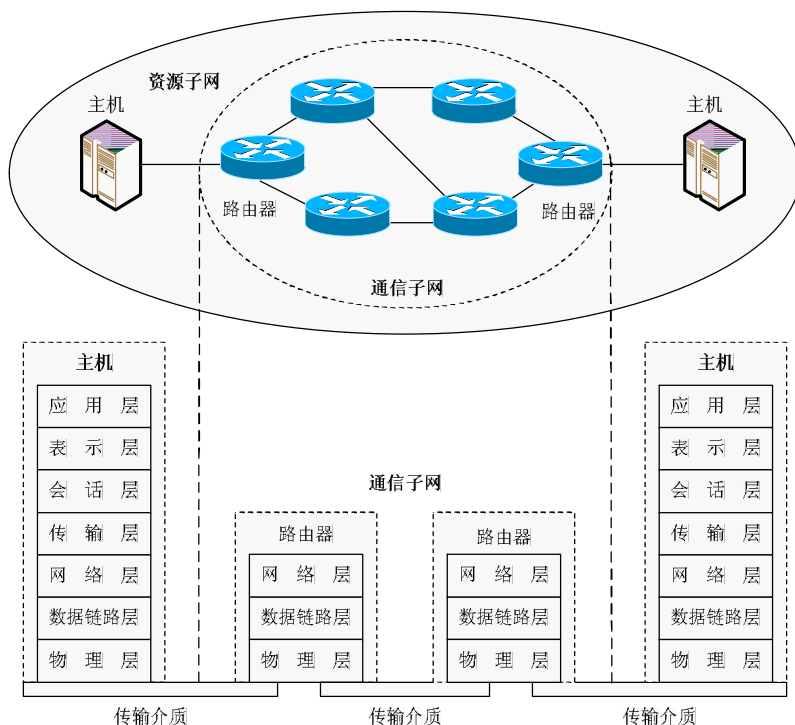


图 2-32 OSI 参考模型组织图

知识链接：点对点通信与端到端通信有何区别？相邻节点之间通过直达通路的通信，称为点对点通信。不相邻节点之间通过中间节点链接起来形成间接可达通路的通信，称为端到端通信。很显然，点对点通信是端到端通信的基础，端到端通信是点对点通信的延伸。

（4）OSI 参考模型通信过程。

在实际中，当两个通信实体通过一个通信子网进行通信时，必然会经过一些中间节点，一般来说，通信子网中的节点只涉及到低三层，因此，两个通信实体之间的层次结构如图 2-33 所示。

OSI 各层定义的通信任务是通过发送方逐层封装,接收方逐层解封装的处理过程来实现的,并且某层内部实现的功能对其他层是不可见的,发送方在某一层的封装内容只能由接收方同一层来处理,这叫做对等层通信原则。图 2-31 中收发双方相同层之间的连线代表了这个过程。读者可能会注意到,除了物理层以外的其他各层之间的连线均用虚线表示,这是因为对等层之间除物理层以外其他各层并不能直接在物理上直接通信,而是逻辑上的虚拟通信。

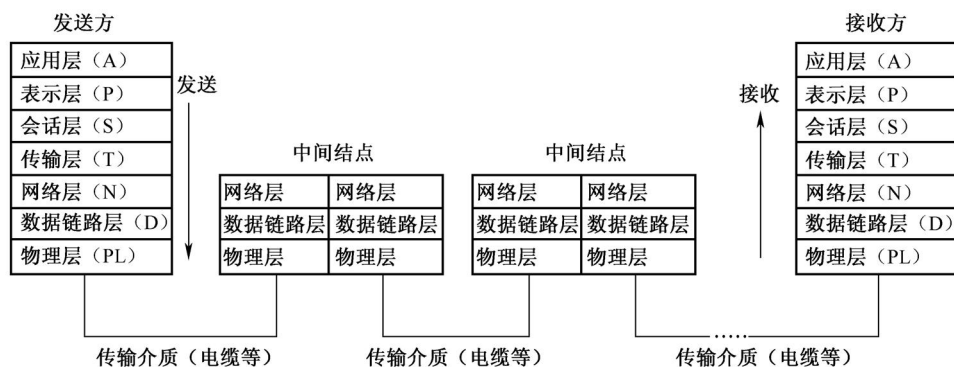


图 2-33 两个通信实体间的层次结构

(5) OSI 各层的功能概述。

OSI 参考模型各层主要功能如下。

1) 物理层 (Physical Layer, PL)。

①基于传输介质提供的信号传输服务,物理层实现相邻节点之间二进制数据流(基于比特流)的透明传输。

②物理层协议涉及与信号传输相关的机械特性、电气特性、功能特性和规程特性,包括物理接口、信号电平、引脚功能、信号时序等标准。

知识链接:“透明”一词表示某一个实际存在的事物看起来却好像不存在一样。透明传输比特流意为传输的那几个比特代表什么意思,不是物理层所要管的。另外,物理层并不是指物理设备或物理媒介,而是有关物理设备通过网络媒介进行互联的描述和规定。

知识链接:从图 2-33 中可以划分出端系统(发送方和接收方)和中间系统(若干中间节点)。传输层及其以上各层使用端到端协议实现通信,而中间系统的网络层使用逐跳(Hop-to-Hop)协议,两个端系统和每个中间节点都要使用它。

2) 数据链路层 (Data Link Layer, D)。

①基于物理层提供的相邻节点之间的数据传输服务,数据链路层确保数据的可靠传输(基于数据帧)、建立可靠的数据链路级连接。

②数据链路层协议涉及成帧和识别帧、数据链路管理(建立、维持、释放)、寻址(使用物理层 MAC 地址)、网络介质访问、差错控制、流量控制等方面的标准。

3) 网络层 (Network, N)。

①负责从源主机到目的主机的路由(基于数据包),实现跨网络数据传输,即网络互联。

②网络层协议主要涉及到如何定位主机的网络位置(使用逻辑地址或 IP 地址),如何选择传输路径等方面的标准。

4) 会话层 (Session Layer, S)。

①会话层是指通信双方一次完整的信息交互,负责发起、维护、终止应用程序之间的通

信（会话）。例如，服务器验证用户登录的过程就是会话层的一个典型实例。

②会话层协议涉及传输方式（单工、半双工、全双工）、会话质量（传输延迟、吞吐量等）、同步控制等方面的标准。会话类似于两个人之间的交谈，需要某些约定使双方有序并完整地交换信息，如通过约定俗成的表情、手势、语气等协调。

5) 表示层（Presentation Layer, P）。

①表示层负责规定通信双方信息传输时数据的组织方式。

②表示层协议主要涉及编码（ASCII、EBCDIC 等）、加密/解密、压缩/解压、格式（声音、图片、图像）等方面的标准。

知识链接：表示层中的加密与压缩任务是可选的，并不一定对所有用户都需要。此外，数据的加密与解密处理原则上也可以在其他各层中实现。

6) 应用层（Application Layer, A）。

①应用层负责为网络应用（程序）提供网络通信服务的接口。

②应用层协议涉及定义网络应用的接口。

7) 传输层（Transport Layer, T）。

依靠“物理层+数据链路层+网络层”提供的网络通信功能建立两台主机之间的连接，为“会话层+表示层+应用层”的应用程序之间的信息交互提供数据传输服务，即传输层负责端到端节点间的数据传输和控制功能。

（6）OSI 参考模型的数据传输过程。

如图 2-34 所示，假设计算机 A 上的某个应用程序要发送数据给计算机 B，则该应用程序把数据交给应用层，应用层在数据前面加上应用层的报头，形成一个应用层的数据包。

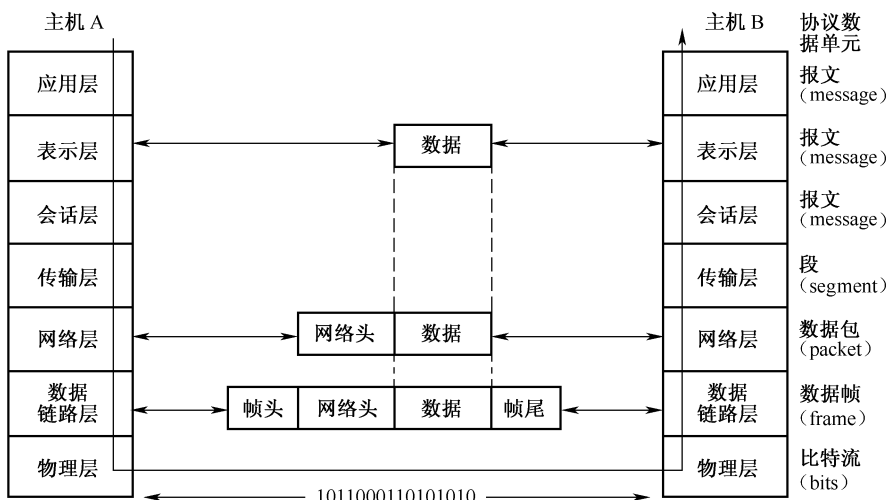


图 2-34 OSI 的数据传输

1) 发送方：将应用程序的数据分段，根据每层的功能定义协议头，逐层封装协议头。

2) 接收方（包括中间节点）：逐层拆解，利用协议封装信息实现该层协议功能，在接收方最终恢复为发送方的原始数据。

3) 通过封装与解封装 PDU 和附加协议头信息实现该层协议功能。如数据链路层通过 MAC 地址实现寻址，网络层通过 IP 地址实现路由，传输层通过端口号建立网络应用程序之间的连接。

4) 在参考模型的不同层次, PDU 是有所不同的, 在物理层叫做比特流 (Bits), 在数据链路层叫做数据帧 (Frame), 在网络层叫做数据包 (Packet), 在传输层上叫做段 (Segment), 其余各层叫做报文 (Message)。

3. TCP/IP 参考模型

(1) TCP/IP 提出的背景。

ARPA 拨出巨资开发 TCP/IP 参考模型, 因为它设想一个在任何条件下甚至核战争中都可以生存的网络, 使分组能够在任何条件下都可以通过该网络, 并且从任何一个位置到达任何其他位置。同时, 希望该网络能够适应从文件传送到实时数据传输的各种应用需求, 这种苛刻的设计要求促使了 TCP/IP 参考模型的诞生。从那时候起, TCP/IP 参考模型就成为了 Internet 赖以发展的实际标准 (工业标准)。

(2) TCP/IP 参考模型概述。

TCP/IP 也采用分层体系结构, 共分四层, 即网络接口层、Internet 层、传输层和应用层。每一层提供特定功能, 层与层之间相对独立。TCP/IP 参考模型及协议簇 (Protocol Suite) 如图 2-35 所示。

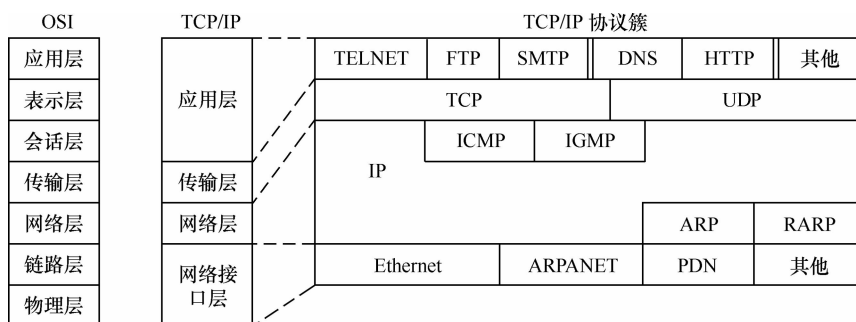


图 2-35 TCP/IP 参考模型及各层使用的协议

知识链接: TCP/IP 参考模型的特点是上下两头大而中间小: 应用层和网络接口层都有许多协议, 而中间的 IP 层很小, 这种很像沙漏计时器形状的 TCP/IP 协议栈表明: 它可以为各式各样的应用提供服务 (Everything over IP), 同时也可以连接到各式各样的网络上 (IP over Everything)。正因为如此, Internet 才发展到今天的这种全球规模。

(3) TCP/IP 参考模型各层功能及特点。

1) 网络接口层。


①没有定义任何实际协议, 仅定义了网络接口: 由于开发 TCP/IP 的主要目的是实现底层异构网络 (指 OSI 最下面两层运行不同协议的网络) 的互联, 因此, 任何已有的数据链路层协议和物理层协议都可以用来支持 TCP/IP 参考模型, 充分体现出 TCP/IP 协议的兼容性与适应性, 它也为 TCP/IP 协议的成功奠定了基础。当一种物理网被用作传送 IP 数据包的通道时, 就可以认为是这一层的内容 (完成 IP 地址与硬件地址的映射以及将 IP 分组封装成帧)。

②典型例子: 以太网 (Ethernet)、令牌环网 (Token Ring)、异步传输模式 (Asynchronous Transfer Mode, ATM)、点到点协议 (Point-to-Point Protocol, PPP)、串行线路网际协议 (Serial Line Internet Protocol, SLIP)、地址解析协议 (Address Resolution Protocol, ARP)、代理 ARP (Proxy ARP)、反向地址解析 (Reverse Address Resolution Protocol, RARP) 等。

2) 网际 (网络) 层。

①主要功能是把数据报通过最佳路径送到目的端 (寻址、路由选择、封包/拆包); 网际层是网络转发节点 (如路由器) 上的最高层 (网络节点设备不需要传输层和应用层)。

②典型例子: IP 网际控制报文协议 (Internet Control Message Protocol, ICMP)、地址解析协议 (Address Resolution Protocol, ARP)、反向地址解析 (Reverse Address Resolution Protocol, RARP)、网际组管理协议 (Internet Group Management Protocol, IGMP) 等。

 **知识链接:** 这里强调指出, 网络层中的“网络”二字, 已不是我们通常谈到的具体的网络, 而是计算机网络体系结构模型中的专用名词。本书中的网络层、网际层、IP 层都是同义语。

3) 传输层。

传输层的主要功能是提供进程间 (端到端) 的传输服务。典型例子: 传输控制协议 (Transmission Control Protocol, TCP) 和用户数据报协议 (User Datagram Protocol, UDP)。

①TCP 是面向连接的传输协议。在数据传输之前建立连接; 把数据分解为多个段进行传输, 在目的站再重新装配这些段; 必要时重新传输没有收到或错误的段, 因此它是“可靠”的。

②UDP 是无连接的传输协议。在数据传输之前不建立连接; 对发送的段不进行校验和确认, 它是“不可靠”的; 主要用于请求/应答式的应用和语音、视频应用。

4) 应用层。

①主要功能: 应用层协议为文件传输、电子邮件、远程登录、网络管理、Web 浏览等应用提供了支持; 有些协议的名称与以其为基础的应用程序同名。

②典型例子: 文件传输协议 (File Transfer Protocol, FTP)、简单邮件传输协议 (Simple Mail Transfer Protocol, SMTP)、邮局协议版本 3 (Post Office Protocol-Version 3, POP3)、远程登录 (Telnet)、超文本传送协议 (Hypertext Transfer Protocol, HTTP)、简单网络管理协议 (Simple Network Management Protocol, SNMP)、域名系统 (Domain Name System, DNS) 等。

4. OSI 参考模型与 TCP/IP 参考模型的比较

OSI 参考模型和 TCP/IP 参考模型之间有很多相似之处: 它们都是以协议栈的概念为基础, 并且协议栈中的协议是相互独立的; 两个模型中各个层次的功能也大体相似; 另外, 在两个模型中, 传输层之上的各层都是传输服务的用户, 并且都是面向应用的用户。

当然, 除了一些基本的相似之处以外, 这两个模型之间也存在着许多差异。主要表现在以下几个方面:

OSI 参考模型的最大贡献是将服务、接口和协议这 3 个概念明确区分开来。服务说明某一层提供什么功能, 接口说明上一层如何调用下一层的服务, 而协议涉及如何实现该层的服务。各层采用什么协议是没有限制的。只要向上一层提供相同的服务, 并且不改变相邻层的接口即可, 因此各层之间具有很强的独立性。然而, OSI 参考模型出现在其协议之前, 致使其协议和模型不能统一, 且 OSI 参考模型过于复杂, 以至于无法真正地加以实现。

而 TCP/IP 参考模型却正好相反, 首先出现的是协议, 模型实际上是对已有协议的描述, 因此不会出现协议不匹配模型的情况, 它们匹配得很好。唯一的问题是模型不适合描述 TCP/IP 参考模型之外的任何其他协议。

尽管 TCP/IP 协议非常流行, 但也存在许多缺点。首先是该模型没有区分服务、接口和协议这 3 个概念, 使得 TCP/IP 参考模型对于使用新技术的指导意义不够; TCP/IP 参考模型完全不是通用的, 该模型不适合描述 TCP/IP 参考模型之外的任何其他协议; 网络接口层在分层协议中根本不是通常意义下的层, 它只是处于网络层和数据链路层之间的一个接口, 根本没有提

及物理层和数据链路层。

🔗知识链接：OSI 参考模型与协议缺乏市场与商业动力，结构复杂，实现周期长，运行效率低，这是它没有能够达到预想的目标的重要原因。

5. 计算机网络的原理体系结构

通过以上的分析比较，OSI 参考模型的成功之处在于它的层次结构模型的研究思路，TCP/IP 协议体系的成功之处在于它的网络层、传输层和应用层体系成功应用于 Internet 环境中。如果将两种模型的共同点找出来和补充应该有的部分，那么这样的体系结构很容易被大家接受。如图 2-36 所示就是计算机领域著名专家、荷兰皇家艺术和科学院院士安德鲁·坦尼鲍姆（Andrew S.Tanenbaum）提出的一个 5 层网络参考模型。

OSI/RM	TCP/IP	5 层体系结构
高层（5~7）	应用层	应用层
传输层（4）	传输层	传输层
网络层（3）	网际层	网络层
数据链路层（2）	网络接口层	数据链路层
物理层（1）		物理层

图 2-36 5 层网络参考模型

6. Wireshark 网络协议分析工具简介

Wireshark 是网络包分析工具。网络包分析工具的主要作用是捕获网络协议包，并显示协议尽可能详细的信息。Wireshark 是一种开源网络分析软件。

（1）应用举例。

- 网络管理员用来解决网络问题。
- 网络安全工程师用来检测安全隐患。
- 开发人员用来测试协议执行情况。
- 用来学习网络协议。

（2）主要特性。

- 支持 Windows 和 Linux 平台。
- 实时捕获网络数据包。
- 能够显示包的详细协议信息。
- 可以打开/保存捕获的数据包。
- 通过过滤以多种色彩显示包。

（3）捕获多种网络接口。

Wireshark 可以捕获多种网络接口类型的包，包括无线局域网接口。

（4）支持多种其他程序捕获的文件。

Wireshark 可以打开多种网络分析软件捕获的包。

（5）Wireshark 不具备的功能。

- Wireshark 不是入侵检测系统。如果网络发生入侵，Wireshark 不会发出警告。但是如果发生了入侵，Wireshark 可通过查看来了解入侵的过程。
- Wireshark 不会处理网络事务，它仅仅是监视网络。Wireshark 不会发出网络包或做其他交互性的事情（名称解析除外，但也可以禁止解析）。

（6）Wireshark 的安装。

可以从网站 <http://www.wireshark.org/download.html> 下载最新版本的 Wireshark, 在 Windows 或 Linux 平台安装或运行 Wireshark, 图 2-37 为 Wireshark 捕获的协议簇。

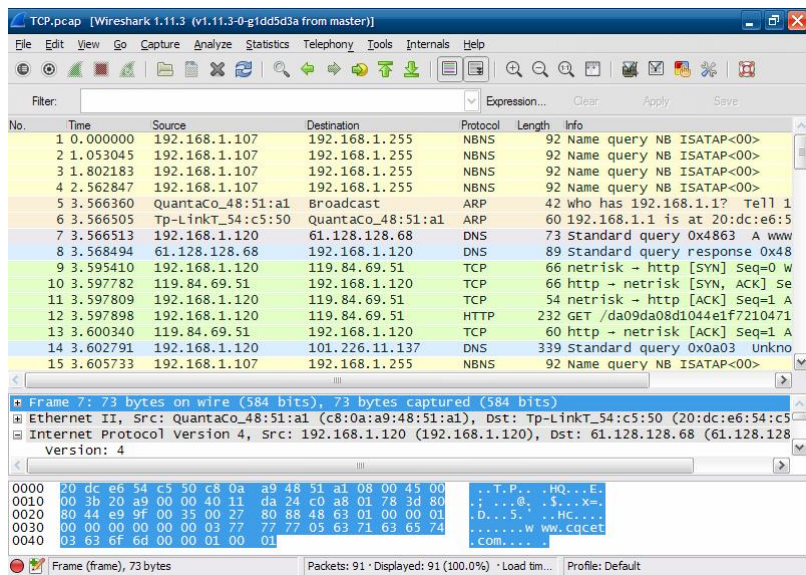


图 2-37 Wireshark 捕获包

2.2.3 任务实施

1. 任务实施条件

两台安装 Windows Server 2003/Windows XP 的计算机（一台安装有 Windows 2003，一台安装有 Windows XP）；PCI 接口的以太网卡及驱动程序；交叉线 1 条；Wireshark 软件包。两台计算机上的 IP 地址和子网掩码参考表 2-3 来进行设置。

2. 连接计算机并配置 TCP/IP 协议

根据表 2-3 进行 IP 地址的配置，参考步骤见项目二任务 1。

表 2-3 IP 地址和子网掩码

计算机	Windows XP	Windows 2003
IP 地址	192.168.1.23	192.168.1.1
子网掩码	255.255.255.0	255.255.255.0

3. 测试网络的连通性

（1）ping 命令功能。ping 命令使用 ICMP 协议的回送请求、回送应答。客户机传送一个回送请求包给服务器，服务器返回一个 ICMP 回送应答包。在默认情况下，发送请求数据包的大小为（ ）B，屏幕上回显（ ）个应答包。主要功能是用来测试网络（ ）。

（2）ping 命令格式和常见参数。在命令行中输入命令 ping /? 可以获得 ping 命令的用法和参数的一些可用选项。图 2-38 显示了 ping 命令的用法。

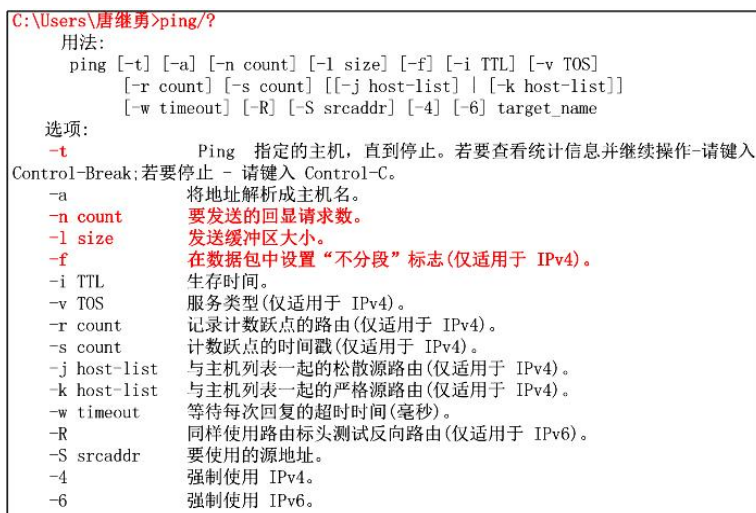


图 2-38 ping 命令的使用

(3) 测试本地主机网络的连通性。在 DOS 命令行中输入 `ping 192.168.1.2`, 输出如图 2-39 所示结果, 说明两台计算机之间是 () 的。

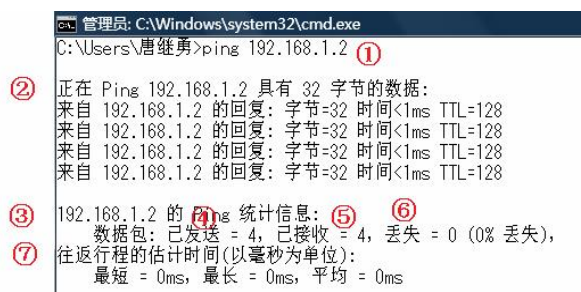


图 2-39 本地主机上的 ping 命令输出

默认情况下会向目的设备发送 4 个 ping 请求并收到应答信息。具体分析如下:

1) 目的地址, 设置为本地计算机的 IP 地址。

2) 应答信息:

字节——ICMP 数据包的大小, 默认值为 32B。

时间——传输和应答之间经过(往返)的时间。

TTL——数据包在网络中的生存时间。其值为目的设备的默认 TTL 值减去路径中的路由器数量。TTL 的最大值为 255, 较新的 Windows 计算机的默认值为 128。

3) 关于应答的摘要信息。

4) 发送的数据包——传输的数据包数量。默认发送四个数据包。

5) 接收的数据包——接收的数据包数量。

6) 丢失的数据包——发送与接收的数据包数量之间的差异。

7) 关于应答延迟的信息, 以毫秒为测量单位。往返时间越短表示链路速度越快。计算机计时器设置为每 10 毫秒计时一次。快于 10 毫秒的值将显示为 0。

4. 在 Windows Server 2003 主机上安装 Wireshark 软件

Wireshark 的安装过程非常简单, 执行默认操作即可。

5. Wireshark 的启动

单击“开始”菜单，选择“程序”，然后再单击“Wireshark”，选择“Wireshark”，启动界面如图 2-40 所示。

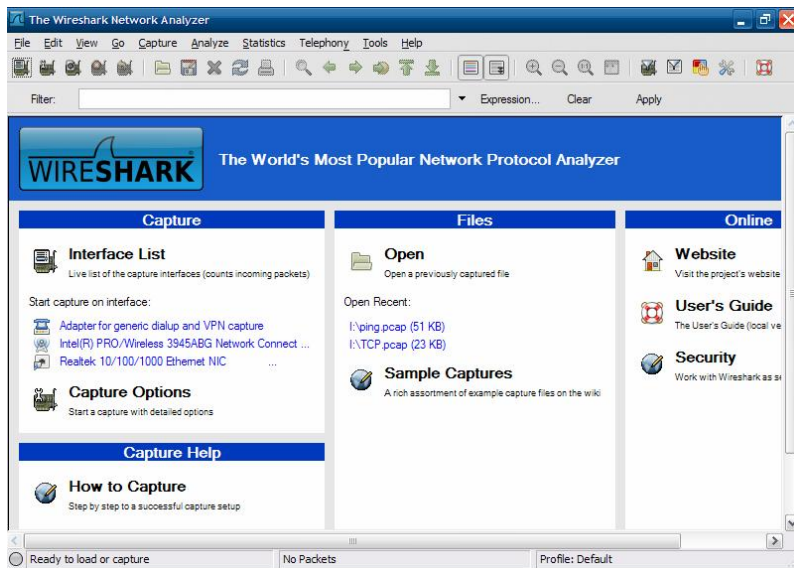


图 2-40 Wireshark 启动界面

6. 使用 Wireshark 捕获数据包

(1) 选择网络接口。

启动 Wireshark 后，在主菜单上单击“Capture”项目下的“Interfaces”，选择要捕获数据包的网络接口，如图 2-41 所示。

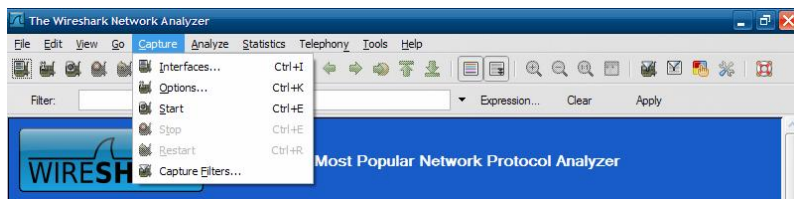


图 2-41 选择网络接口

(2) 捕获数据包。

1) 在相应的网络接口上单击“Start”按钮，指定在哪个接口（网卡）上抓包，如图 2-42 所示。

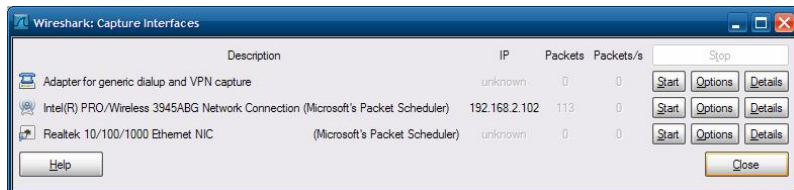


图 2-42 开始捕获数据包

2) 在安装 Windows XP 主机的 DOS 界面下执行 ping 192.168.1.1，捕获界面如图 2-43 所示。

3) 捕获到了很多与执行 ping 命令无关的数据包, 因此执行过滤, 选择我们需要的数据包进行针对性分析。在 Wireshark 的 Filter 栏中输入 icmp, 因为 ping 命令是基于 ICMP 协议实现的, 回车后出现如图 2-44 所示的界面。

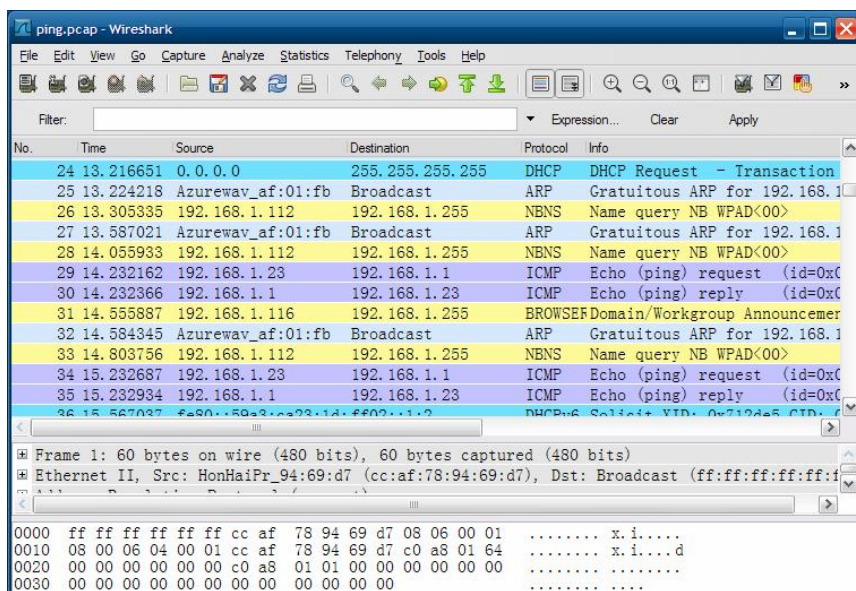


图 2-43 捕获 IP 数据包

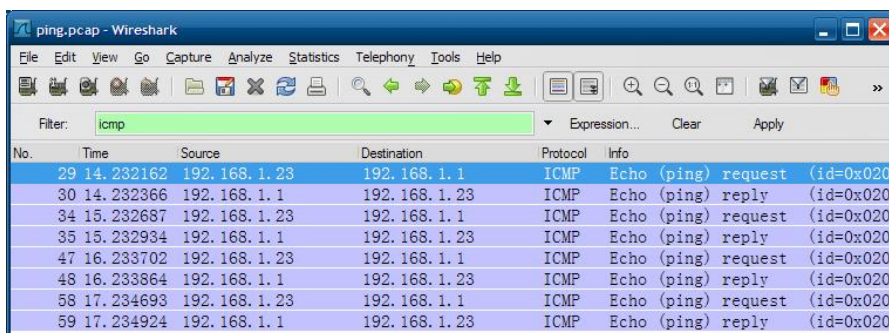


图 2-44 协议过滤

4) 执行协议过滤后, 得到了我们需要的数据, 请根据图 2-44 分析以下问题。

①ICMP 如何探测网络的可达性?

②在默认情况下, 执行 ping 命令, 主机屏幕只会回显 4 个报文, 为什么捕获的数据报却有 8 个?

5) 双击捕获到的 29 号数据包, 展开各协议字段, 如图 2-45 所示, 并分析如下问题:

在默认情况下, 执行 ping 命令, 发送数据包的大小为 32Bytes, 而捕获到的数据包大小为 74Bytes?

6) 捕获到的数据包由协议的头部和数据两部分构成, 真实的数据是封装在 ICMP 报文中的, 因此我们需要展开 ICMP 协议字段对该报文进行解码, 如图 2-46 所示, 才能看见真实的数据内容。

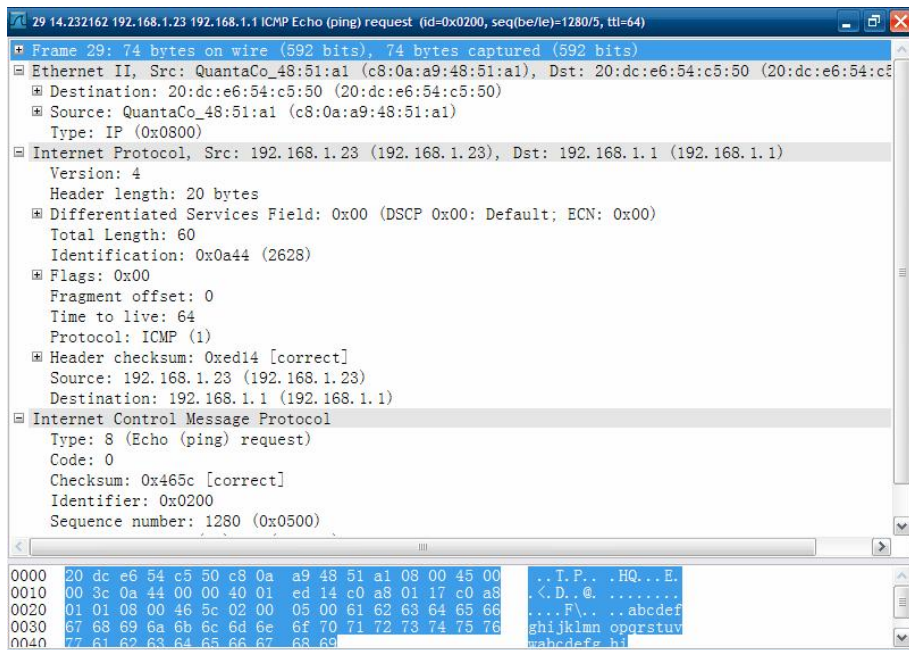


图 2-45 IP 数据包的协议字段

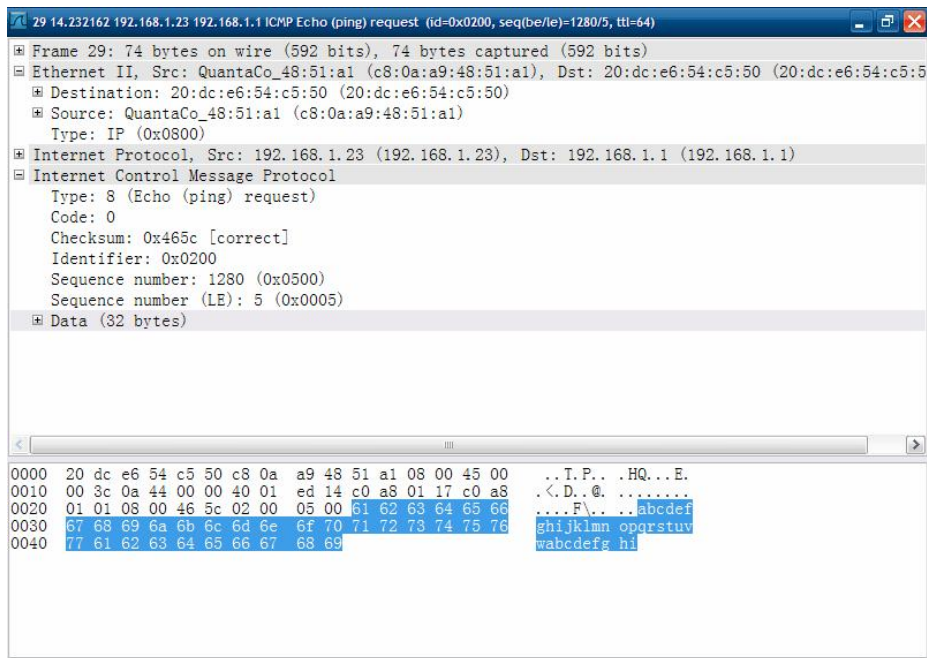


图 2-46 IP 数据包的解码

7) 请读者根据图 2-46 对 ICMP 的各协议字段进行分析, 在空白处填写相应内容。

该 ICMP 回送请求报文的类型、代码是 (), 校验和是 (), 标识号是 (), 序列号是 (), ICMP 数据是 ()。

(3) 分析网络体系分层结构。

1) 重新配置 Windows Server 2003 主机的 IP 地址参数, 确保能接入 Internet, 打开浏览器,

在地址栏中输入 `http://www.baidu.com`，使用 Wireshark 捕获数据包，如图 2-47 所示。

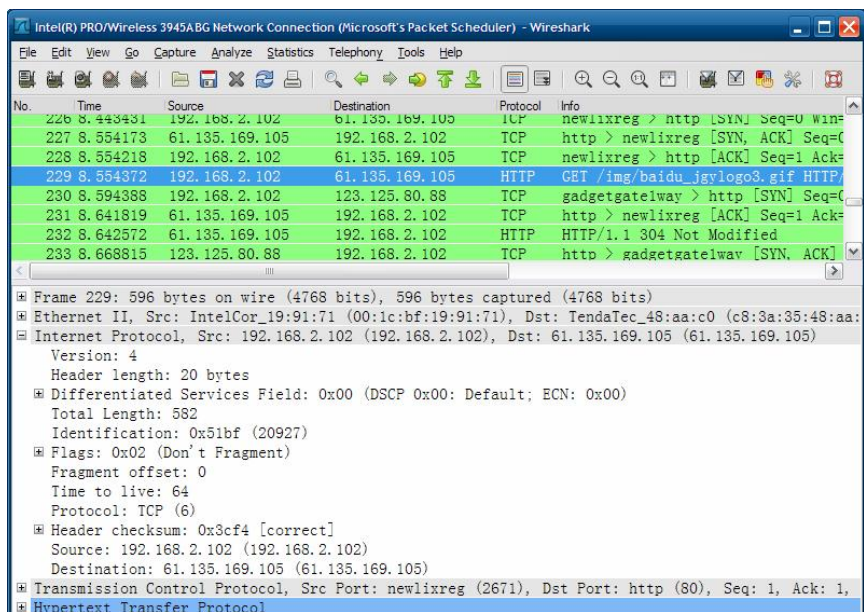


图 2-47 捕获的网络各层协议

2) 从图中可以了解到网络体系结构共分成()层,每层的名称和协议的名称是什么?

3) 根据图 2-47 简单分析网络层 IP 协议的组成。

2.2.4 课后习题

1. 在 TCP/IP 参考模型的传输层上,()协议实现的是不可靠、无连接的数据报服务,而()协议是一个基于连接的通信协议,提供可靠的数据传输。

2. 在计算机网络中,将网络的层次结构模型和各层协议的集合称为计算机网络的()。其中,实际应用最广泛的是()协议,由它组成了 Internet 的一整套协议。

3. 国际标准化组织(ISO)提出的不基于特定机型、操作系统或公司的网络体系结构 OSI 模型中,第一层和第三层分别为()。

- A. 物理层和网络层
- B. 数据链路层和传输层
- C. 网络层和表示层
- D. 会话层和应用层

4. 在下面给出的协议中,()属于 TCP/IP 的应用层协议。

- A. TCP 和 FTP
- B. IP 和 UDP
- C. RARP 和 DNS
- D. FTP 和 SMTP

5. 在下面对数据链路层的功能特性描述中,不正确的是()。

- A. 通过交换与路由,找到数据通过网络的最有效的路径
- B. 数据链路层的主要任务是提供一种可靠的通过物理介质传输数据的方法
- C. 将数据分解成帧,按顺序传输帧,并处理接收端发回的确认帧
- D. 以太网数据链路层分为 LLC 和 MAC 子层,在 MAC 子层使用 CSMA/CD 协议

6. 网络层、数据链路层和物理层传输的数据单位分别是()。

- A. 报文、帧、比特流
- B. 包、报文、比特流

- C. 包、帧、比特流 D. 数据块、分组、比特流
7. 在 OSI 参考模型中能实现路由选择、拥塞控制与互联功能的层是 ()。
- A. 传输层 B. 应用层 C. 网络层 D. 物理层
8. 在下列功能中, () 最好地描述了 OSI 模型的数据链路层。
- A. 保持数据正确的顺序、无错和完整
- B. 处理信号通过介质的传输
- C. 提供用户和网络接口
- D. 控制报文通过网络的路由选择
9. OSI 的物理层负责 () 功能。
- A. 格式化报文 B. 为数据选择通过网络的路由
- C. 定义连接到介质的特性 D. 提供远程访问介质
10. 在不同网络节点的对等层之间的通信需要 ()。
- A. 模块接口 B. 对等层协议
- C. 电信号 D. 传输介质
11. OSI/RM 共分为哪几层? 简要说明各层的功能。
12. TCP/IP 协议模型分为几层? 各层的功能是什么? 每层又包含哪些协议?
13. 将连在计算机上的网线拔除, 再执行 ping 本机 IP 地址命令, 试分析输出结果。
14. 在项目二任务 2 中, 关闭 Windows Server 2003 计算机, 执行 ping 192.168.1.3, 试分析输出结果。
15. 在项目二任务 2 中, 将 Windows XP 计算机上的 IP 地址改为 172.168.1.2, 子网掩码不变, 再执行 ping 192.168.1.3 命令, 试分析输出结果。
16. 在项目二任务 2 中, 将 Windows XP 计算机上的 IP 地址改为 192.168.1.2, 子网掩码改为 255.255.255.252, Windows Server 2003 计算机的 IP 地址改为 192.168.1.5, 子网掩码改为 255.255.255.252, 再执行 ping 192.168.1.5 命令, 试分析输出结果。
17. 一个保密机构必须向位于里昂城外 50km 的一个小镇上的另一个保密机构发送一份三页纸的信件。由于该信件是高度保密的, 所以信的每一页需要单独发送。接收方为了能够理解整封信的内容, 必须收到全部三页纸。信件的每一个单词都被发送方加密, 再由接收方对它进行解密。发送方将通过常规的邮件服务发送邮件, 但还要收到接收方的应答以确保发送安全。该信件将首先发送到巴黎, 然后再转发到这个小镇。
- (1) 比较写上了地址并且贴上了邮票的信件与数据帧之间的相似之处。
- (2) 列出 OSI 模型的层次结构, 并概略地陈述各层的功能。
- (3) 将信件通过邮政系统发送与数据包通过 OSI 模型各层传输进行比较。