第1章　网络概述

计算机网络是由许多具有信息交换和处理能力的节点互连而成的，网络中的节点可以是计算机、集线器、交换机或路由器等。它们由不同的厂家生产，使用不同的操作系统，技术实现上存在各种差异，如何实现它们之间的相互通信呢？互联网的奠基者们提出了一个技术思路：在每个异构网络内部使用各自的通信协议，异构网络之间使用 TCP/IP 协议族。

本章主要对 TCP/IP 协议族进行概述，为后续章节提供必要的背景知识。

1.1　网络互连和 TCP/IP

1.1.1　网络互连

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，从最初的免费教育科研网络逐步发展成供全球使用的有偿商业网络。Internet 给人们带来了极大的便利，那么什么是 Internet 呢？Internet 是由数量极大的各种计算机网络互连起来的，是一个世界范围的“Network of Networks”。Networks 代表各种不同的物理网络，这些网络在信道的访问方式和数据的传送方式上都存在差异，具体表现为帧格式的不同和传输介质的不同。而 Network 指的是一个单独的虚拟网络，用户能够与任意一台连接在 Internet 上的主机进行通信，不管中间间隔了多少个物理网络。

网络刚开始出现时，在典型情况下，只能在同一制造商的计算机产品之间进行通信。网络互连是指将两个以上的通信网络通过一定的方法，用一种或多种网络通信设备相互连接起来，以构成更大的网络系统。网络互连不仅仅是把计算机简单地在物理上连接起来，其最终目的是使不同网络中的用户可以互相通信、共享软件和数据等。

对用户而言，实现网络互连就是屏蔽各种异构网络的底层差异，向上提供一致性的数据格式。实现思想是把通信模块独立出来，在底层网络技术与高层应用程序之间增加一个中间层软件，以便抽象和屏蔽硬件细节，向用户提供通用网络服务。在 TCP/IP 协议族中，实现这一功能的协议是互联网协议 IP，它定义了全网统一的数据形式和地址格式。但在技术实现上，数据必须通过底层物理网络才能发送出去，要想真正实现网络互连，还必须有一个中间设备对数据包进行转换，这个设备就是路由器。路由器和 IP 实现网络互连的过程如图 1-1所示。

如图 1-1 所示，以太网中的主机 A 要和拨号网络中的主机 B 进行通信，主机 A 的应用数据被封装成 IP 数据报，最终封装成以太帧发送到网络中，经过路由器转发时，先去掉以太帧首和帧尾，从 IP 数据报首部提取目的 IP 地址，查询路由表以确定出口，然后将 IP 数

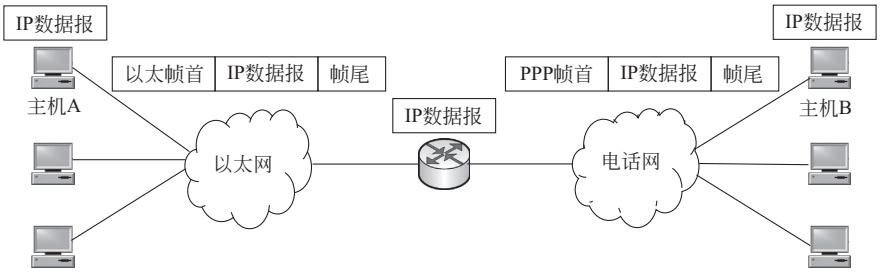

图 1-1　路由器实现网络互连

据报封装成 PPP 帧转发到拨号网络中。

综上，从用户层面看，IP 实现了网络互连；从技术层面看，路由器是实现网络互连的核心设备，整个 Internet 是由无数个物理网络通过路由器互连起来的。

1.1.2　TCP/IP 协议族

Internet 的前身是阿帕网（ARPAnet），ARPAnet 利用分组交换技术实现了计算机的互连，但由于底层硬件来自不同的生产厂商，互操作性较差，为解决网络互连问题，美国高级研究计划署（Advanced Research Project Agency，ARPA）启动了名为 Internetting 的互联网研究项目。1974 年，IP 和 TCP 问世，1977—1979 年 TCP/IP 体系结构和协议规范成形。1983 年，TCP/IP 协议成为 ARPANET 上的标准协议，使得所有使用 TCP/IP 协议的计算机都能利用互联网实现通信。

TCP/IP 协议族是 Internet 的基础，也是当今最流行的组网形式。TCP/IP 是一组协议的代名词，包括许多协议，其中比较重要的有 SLIP 协议、PPP 协议、IP 协议、ICMP 协议、ARP 协议、RIP 协议、OSPF 协议、TCP 协议、UDP 协议、FTP 协议、DNS 协议、SMTP 协议、HTTP 协议等。

IP 解决了异构网络互连问题，TCP 为网络应用提供了面向连接的可靠数据传输服务，UDP 为网络应用提供了无连接的不可靠的数据报传输服务，ICMP 用于传递网络控制和差错信息，ARP 和 RARP 用于实现 IP 地址和物理地址的相互转换，RIP、OSPF 和 BGP 等协议用于维护路由表。此外，还为一些常见的网络应用制定了标准的协议，如 DNS 协议用于域名解析，DHCP 协议用于 IP 地址分配，FTP 协议用于文件传输，SMTP 协议和 POP3 协议用于邮件传输，HTTP 协议用于超文本传送等。

1.2　网络协议与层次划分

1.2.1　网络协议的概念

计算机网络是由许多具有信息交换和处理能力的节点互连而成的，要使整个网络有条不紊地工作，相互通信的计算机系统必须高度协调工作才行，而这种“协调”是相当复杂的。这要求每个节点必须遵守一些事先约定好的数据格式及时序等规则。网络协议是为计算机网络中

进行数据交换而建立的规则、标准或约定的集合，通常由语法、语义和时序三部分组成。

（1）语法，即数据与控制信息的结构或格式。

（2）语义，即需要发出何种控制信息，完成何种动作及做出何种响应。

（3）时序，即事件实现顺序的详细说明。

网络协议是计算机网络不可缺少的组成部分，对于非常复杂的计算机网络协议，其结构应该是层次式的。网络互连是一个复杂的系统工程，包括很多的软件、硬件和相关协议，为了简化系统，设计者采用分而治之的思想来设计和描述网络体系结构，将网络协议的实现按层次进行组织，每层使用下层提供的服务完成一定的功能，并向上层提供服务。这样，协议栈中的协议就具有上下层次关系。

1.2.2　OSI 分层模型

标准的网络分层模型是 ISO（国际标准化组织）制定的 OSI（open system interconnection，开放式系统互连）参考模型。OSI 模型并不是一个标准，而只是一个在制定标准时所使用的概念性框架，定义了不同计算机互连的标准。

OSI 框架是基于 1984 年 ISO 发布的 ISO/IEC 7489 标准。该标准定义了网络互连的 7 层框架，自下而上依次为物理层、数据链路层、网络层、运输层、会话层、表示层和应用层。

1. 物理层

利用传输介质为数据链路层提供物理连接，实现比特流的透明传输。该层定义了与物理链路的建立、维护和拆除有关的机械、电气、功能和规范等特性，包括信号线的功能、介质的物理特性、传输速率、位同步、传输模式和连接规格等。

2. 数据链路层

数据链路层为网络层提供数据传输服务，完成两个相邻节点之间的通信问题。该层传送的协议数据单元称为帧（frame），具体功能包括数据成帧、介质访问控制、物理寻址、差错控制和流量控制等。

3. 网络层

网络层为传输层提供服务，负责从源主机到目的主机的端到端的数据通信，传输的协议数据单元称为数据报（packet）。具体功能包括网络逻辑地址编址、路由选择和报文转发等。

4. 运输层

运输层为上一层协议提供进程到进程的、有序的、可靠和透明的数据传输服务，传输的协议数据单元称为报文段（segment）。具体功能包括差错控制、流量控制、拥塞控制和进程寻址等。

5. 会话层

会话层负责会话的控制，具体功能包括会话的建立、维护、同步和终止。

6. 表示层

将应用处理的信息转换为适合网络传输的格式，或者将来自下一层的数据转换为上层能够处理的格式。具体功能包括数据的加密和解密、压缩和解压缩、格式转换等。

7. 应用层

为应用程序提供服务并规定应用程序相关的通信细节，通过应用程序完成用户的网络应用需求。

1.2.3 TCP/IP 分层模型

TCP/IP 协议层次结构即常说的 TCP/IP 模型，它是 ARPAnet 和其后续因特网使用的参考模型。TCP/IP 模型相对简单，共有 4 层，从下到上依次为网络接口层、网络层、运输层和应用层。图 1-2 为 TCP/IP 模型与 OSI 模型的层次对应关系。

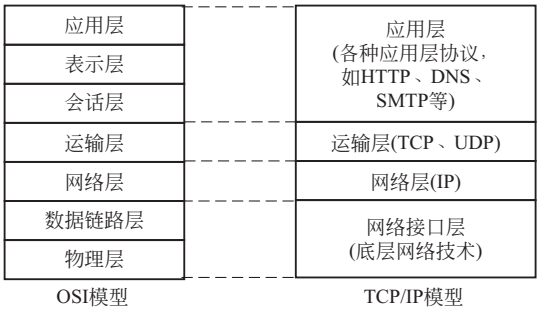

图 1-2 TCP/IP 模型与 OSI 模型的层次对应关系

1. 网络接口层

网络接口层对应 OSI 模型中的物理层和数据链路层。TCP/IP 协议栈是为支持异构网络互连而设计的，因此对网络接口层没有特别的定义，只要底层网络技术和标准支持数据帧的发送与接收，就可以作为 TCP/IP 的网络接口。

2. 网络层

网络层又称为网际层、互联网层或 IP 层，是 TCP/IP 模型的关键部分。该层主要完成 IP 数据报的封装、传输、选路和转发，使其尽可能到达目的主机。该层包括的协议主要有 IP、ARP、RARP、ICMP 和 IGMP，其中，IP 是网络层的核心。

3. 运输层

运输层位于 IP 层之上，为两台主机上的应用程序提供端到端的通信服务。目前，应用最广泛的运输层协议是 TCP 和 UDP。TCP 提供面向连接的、可靠的、基于流的数据传输服务。UDP 提供的是无连接的数据报服务，不保证可靠性和顺序性，但效率较高。

4. 应用层

TCP/IP 简化了 OSI 的会话层和表示层，将其融合到了应用层，使得通信的层次减少，从而提高了通信的效率。应用层包含了一些常用的网络应用协议，如电子邮件（SMTP）、文件传送（FTP）、远程登录（telnet）等。

1.3 互联网地址

1.3.1 IP 地址

1. 基本分类

互联网上的每个接口必须有一个唯一的 Internet 地址（也称作 IP 地址），IP 地址长度为

32 位，例如，11010011 01000111 11101001 00010101。IP 地址由两个字段组成，第一个字段是网络号，标志主机所连接到的网络，第二个字段是主机号，标志该主机。在互联网发展早期采用的是分类的 IP 地址，五类 IP 地址结构如图 1-3 所示。

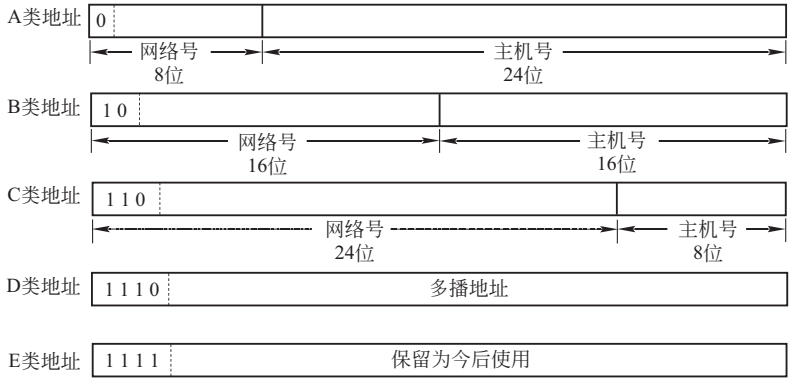

图 1-3　IP 地址分类

为了提高可读性，32 位的 IP 地址通常写成 4 个十进制整数，每个整数对应一个字节，中间用小数点隔开，这种表示方法称作“点分十进制”。上述 32 位 IP 地址可写为 211. 71. 233. 21。区分各类 IP 地址的最简单方法是看它的第一个十进制整数。表 1-1 列出了各类 IP 地址的范围。

表 1-1　各类 IP 地址的范围

网络类别	范围	适用范围
A	1. 0. 0. 0～126. 255. 255. 255	超级大网
B	128. 0. 0. 0～191. 255. 255. 255	中规模网络
C	192. 0. 0. 0～223. 255. 255. 255	小规模网络
D	224. 0. 0. 0～239. 255. 255. 255	组播地址
E	240. 0. 0. 0～247. 255. 255. 255	保留

2. 特殊的 IP 地址

除了上述 IP 地址外，还有几种特殊类型的 IP 地址。

（1）网络地址。Internet 中每个网络都有一个唯一的标志，当 IP 地址中的主机号全取 0 时，标志了一个网络，这种地址称为网络地址。211. 71. 233. 0 即为一个网络地址。

（2）广播地址。主机号全部取 1 的地址称为广播地址。若要将数据报同时发送到网络中的所有主机，则必须使用广播地址。211. 71. 233. 255 即为网络 211. 71. 233. 0 的广播地址。

（3）有限广播地址。255. 255. 255. 255 称为有限广播地址，表示在“本网络”上广播。当需要广播但又不知道所处网络的地址时，使用有限广播地址。

（4）环回地址。首字节为 127 的地址称为环回地址。该地址用于本机进程间的通信或协议软件测试，当使用该类地址时，分组永远不离开主机。常用的环回地址是 127. 0. 0. 1。

3. 私有地址

在进行 IP 地址分配时，保留了一些 IP 地址用于私有网络，这些地址称为私有地址或本地地址。私有地址只能用于内网，不可用作外网地址。A 类、B 类、C 类 3 类网络中都保留了私有地址，具体范围如下。

（1）A 类：10. 0. 0. 0～10. 255. 255. 255。

（2）B 类：172. 16. 0. 0～172. 31. 255. 255。

（3）C 类：192. 168. 0. 0～192. 168. 255. 255。

1. 3. 2 子网划分

在传统的分类网络中，同一个网络中的主机处于同一广播域。以 A 类网络为例，一个 A 类网络可能有 16 777 214 台主机，而在同一广播域中有这么多节点是不可能的，网络会因为广播通信而饱和。结果造成大量 IP 地址没有分配出去，为了更加灵活地使用 IP 地址，可以把网络进一步分成更小的子网，每个子网由路由器界定并分配一个新的子网地址。

子网划分就是将 IP 地址的主机部分进一步划分为子网部分和主机部分。其中，子网部分用来表示网络内的子网，主机部分用来表示子网中的主机。子网掩码用来指明地址中多少位用于网络号，剩余多少位用于实际的主机号。

1. 3. 3 超网编址

20 世纪 90 年代，随着互联网用户的猛增，使得 IP 地址的数量面临耗尽的风险。人们意识到分类 IP 在设计上存在很大问题，会造成 IP 地址的大量浪费。因此，一种新的无分类编址方法问世了，这种编址方法的全名是无分类域间路由选择（classless inter-domain routing，CIDR）。CIDR 取消了 IP 地址的分类，使用网络前缀来指定地址中网络号的位数，剩下的部分仍然作为主机号，用来指明主机。CIDR 把网络前缀相同的所有连续的 IP 地址组成一个“CIDR 地址块”。

CIDR 使用斜线记法，即在 IP 地址后面加上斜线“/”，斜线后面是网络前缀所占的位数，也是该地址块对应的地址掩码中 1 的个数。例如，IP 地址 211. 71. 233. 21/24，表示 32 位 IP 地址的前 24 位是网络位，后 8 位是主机位，其对应的地址掩码为 255. 255. 255. 0。

1. 4 MAC 地址

MAC 地址，又称为物理地址或硬件地址，是数据链路层的地址，用于识别链路中互连的节点。

局域网使用的 MAC 地址长 48 位，一般由网卡的生产厂商固化到网卡的 ROM 中。MAC 地址中的前 24 位表示厂商识别码，由 IEEE 分配给网卡生产厂商，每个生产厂商都有特定唯一的识别码。后 24 位是厂商内部为识别网卡而用。因此，每个网卡的 MAC 地址都是全球唯一的。

数据帧在数据链路层是根据 MAC 地址寻址的。局域网普遍采用的是由以太网交换机搭

建的星形拓扑结构。以太网交换机持有多个端口，并维护一个转发表，它们会根据帧首部中的目的 MAC 地址和转发表决定从哪个端口将数据帧转发出去。

1.5　封包与解包

网络通信的实质是应用进程之间的通信。应用进程产生的应用数据经过各层协议的封装，最后被当作一串比特流送入网络。发送方由上到下每一层对收到的数据添加相应的协议首部信息（数据链路层还要添加尾部信息），该过程称为封包。接收方由下至上每一层减去相应的协议首部或尾部，将最终的应用数据送给接收方进程，该过程称为解包。详细过程如图 1-4 所示。

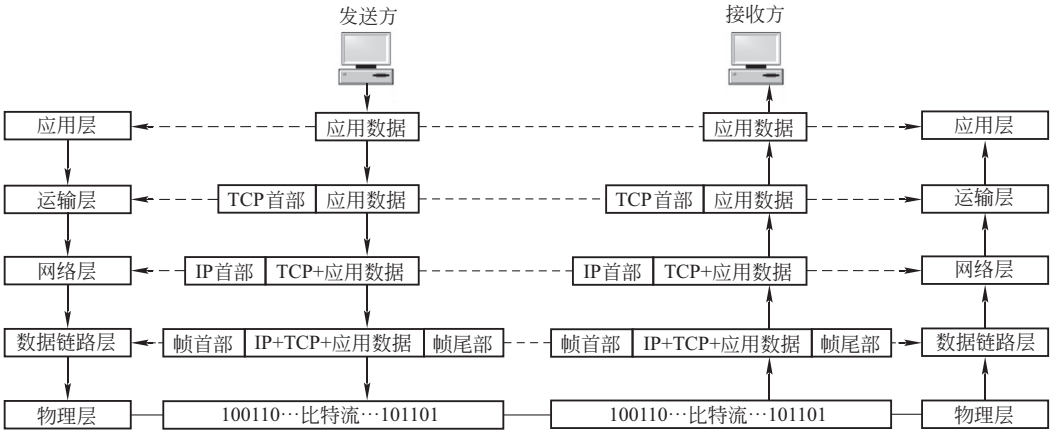

图 1-4　数据的封装与解封

发送方的应用进程向接收方的应用进程发送数据。发送方的应用进程产生应用数据，向下发送到运输层，运输层添加 TCP 首部生成 TCP 报文段，再交给网络层，网络层添加 IP 首部生成 IP 数据报，再交给数据链路层，数据链路层添加帧首和帧尾，封装成帧，最后由物理层以比特流的形式发送到网络中。

数据到达接收方，先由物理层转换成比特流，将完整的帧送到数据链路层，数据链路层完成本层功能后，去掉帧首和帧尾，将 IP 数据报送到网络层，以此类推，最终将应用数据送到接收方应用进程。

1.6　多路复用和多路分用

如果某层的一个协议对应直接上层的多个协议或实体，则需要复用和分用。

1. 多路复用

多路复用指发送方不同的上层协议可以使用同一个下层协议发送数据，如图 1-5 所示。

当发送方发送数据时，各基于 TCP 的应用多路复用 TCP，各基于 UDP 的应用多路复用

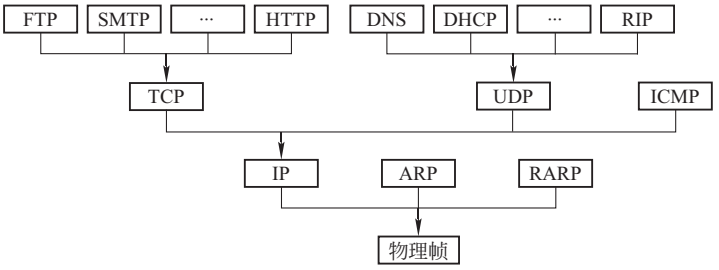

图 1-5　TCP/IP 协议的多路复用

UDP。TCP、UDP 和 ICMP 则多路复用 IP。IP、ARP 和 RARP 复用物理帧。

2. 多路分用

多路分用是多路复用的逆过程，指接收方的下层协议剥去协议首部后能够把数据正确交付给上层协议，如图 1-6 所示。

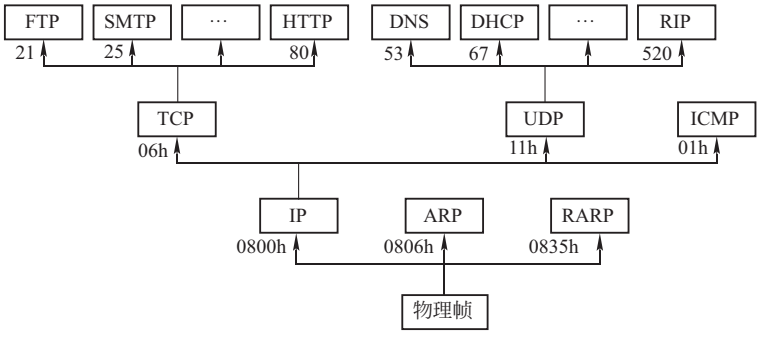

图 1-6　TCP/IP 协议的多路分用

物理帧到达接收方后，根据帧首部中的“类型”字段决定将帧中封装的数据交付给上层哪个协议。IP 模块处理完 IP 数据报后，根据 IP 首部中的“协议”字段决定将数据交付给哪个协议模块。TCP 和 UDP 协议模块处理完数据后，根据首部中的“目的端口”字段决定将数据交付给哪个应用进程。

1.7　Wireshark 简介

要深入理解网络协议的运行机制，需要从实际环境中获取真实报文进行分析。Wireshark 是目前世界上最受欢迎的协议分析软件，利用它可将捕获到的各种各样协议的网络二进制数据流翻译为人们容易读懂和理解的文字与图表等形式，极大地方便了对网络活动的监测分析和教学实验。它有十分丰富和强大的统计分析功能，可在 Windows、Linux 和 UNIX 等系统上运行。此软件于 1998 年由美国 Gerald Combs 首创研发，原名 Ethereal，至今世界各国已有 100 多位网络专家和软件人员正在共同参与此软件的升级完善和维护。它是一个开源的免费软件，任何人都可自由下载，也可参与共同开发。

图 1-7 为 Wireshark 的启动界面。

图 1-7　Wireshark 启动界面

开始捕获数据前，需要对“捕获”菜单的“选项”进行设置，为的是能在数据包捕获时提供更多的灵活性。选项分为 3 个标签页：输入、输出和选项。

“输入”标签页的主要目的是显示所有可以抓包的硬件接口和有关这些接口的基本信息。包括系统提供的接口名字，一个显示接口吞吐量的流量图，以及混杂模式状态选项等，如图 1-8 所示。

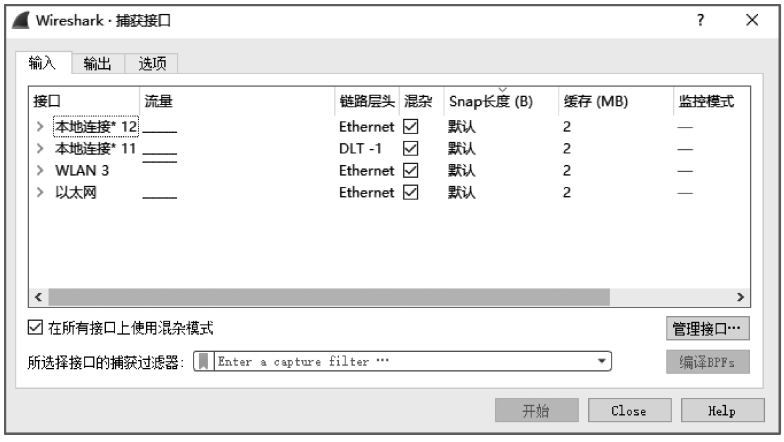

图 1-8　“输入”标签页

“输出”标签页可以选择将数据包存成一个文件、文件集或使用环状缓冲来控制创建文件的个数。可同时设置存储格式、路径及文件名称等，如图 1-9 所示。

“选项”标签页包含其他一些抓包设置，包括显示选项、解析名称和自动停止捕获，如图 1-10 所示。

Wireshark 窗口被分为 3 个区（见图 1-11），顶部是报文列表，显示的是捕获的每个数据帧中数据包的摘要信息，单击此区域内的数据包可以在另外两个区域中获得这个数据包的更多信息。中间的区域为数据包详细信息窗，显示了所选数据包在各层封包的详细信息。最下面的区域显示了该数据包的实际数据。

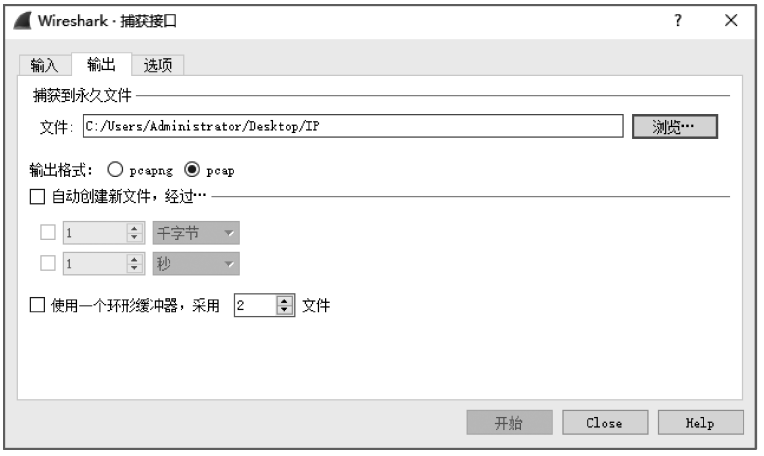

图 1-9 “捕获”的输出设置

图 1-10 “捕获”的选项设置

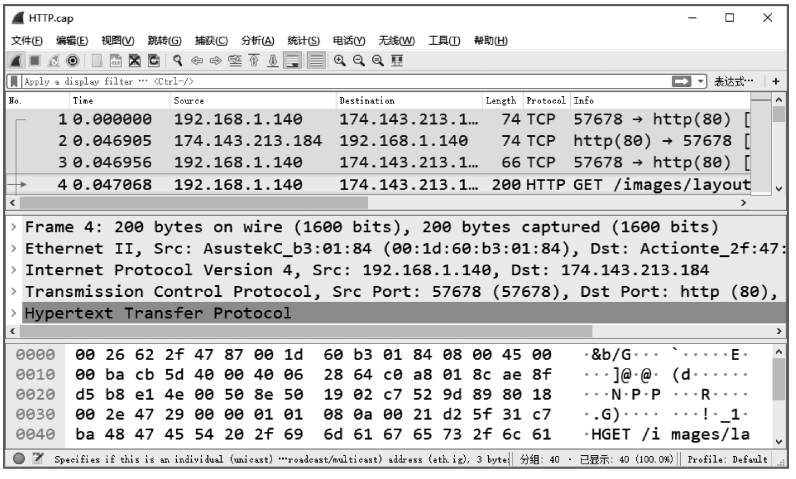

图 1-11 Wireshark 显示窗口

有时捕获到的数据包太多，但只需要某些特定的内容，则可以在“过滤”输入框里输入过滤规则。过滤语句须符合 Wireshark 的过滤表达式规则，为方便用户，可以直接在“过滤”输入框中输入，也可以单击旁边的“表达式”按钮，在打开的对话框中构造过滤语句，如图 1-12 所示。输入完后单击旁边的按钮或按回车键即可。

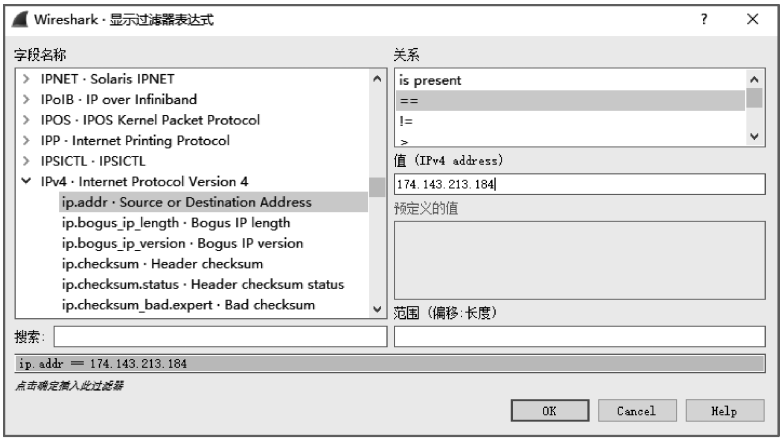

图 1-12　构造过滤语句

习题 1

1. 网络协议的定义是什么？

2. Internet 所使用的 TCP/IP 协议的基本层次有哪些？各层的作用是什么？

3. 传输层协议 TCP 和 UDP 的区别是什么？应用层如何确定使用何种传输协议？

4. 202.70.121.33 在分类 IP 中属于哪一类？在没有划分子网的情况下，其所在网络的网络地址和广播地址分别是多少？

5. 简述数据包的封装和解封过程。