TCP/IP 教程

于 京　詹晓东　胡 亦　编著

電子工業出版社
PUBLISHING HOUSE OF ELECTRONICS INDUSTRY
URL:http://www.phei.com.cn

TCP/IP 教程

于 京 詹晓东 胡 亦 编著

電子工業出版社
Publishing House of Electronics Industry
北京·BEIJING

内 容 简 介

本书内容为介绍 TCP/IP 在 Windows NT 环境下的功能及设计方案。全书共有十二章，为：TCP/IP 基础、TCP/IP 协议组概念、IP 地址、划分子网、IP 路由、动态主机配置协议 DHCP、NT 环境下的名字解析、主机名和主机名解析、实现 NT 环境下的 DNS 系统、NT 的远程访问服务 RAS、不同环境的连接、Windows NT 常用网络命令及实用程序。

本书适用于有一定网络知识、欲用 Windows NT 平台架构网络的技术人员。对参加微软 MCSE 考试的 TCP/IP 课程的读者也有所帮助。

图书在版编目(CIP)数据

TCP/IP 教程/于京等编著 . - 北京：电子工业出版社，1999.6
(教程系列)
ISBN 7 - 5053 - 5280 - 6

Ⅰ. T… Ⅱ. 于… Ⅲ. 计算机网络，传输控制协议 TCP/IP - 教材 Ⅳ. TP393

中国版本图书馆 CIP 数据核字(1999)第 05122 号

书　　名：TCP/IP 教程
编　　著：于　京　詹晓东　胡　亦
策划编辑：张　欣
责任编辑：杨逢仪
特约编辑：赖春生
排版制作：电子工业出版社计算机排版室
印 刷 者：北京隆华印刷厂
出版发行：电子工业出版社　URL：http://www.phei.com.cn
　　北京市海淀区万寿路 173 信箱　邮编 100036
经　　销：各地新华书店
开　　本：787 x 1092　1/16　印张：11.5　字数：288 千字
版　　次：1999 年 6 月第 1 版　1999 年 6 月第 1 次印刷
书　　号：ISBN 7-5053-5280-6 / TP·2635
印　　数：5000 册　　定价：16.00 元

前　言

Microsoft 的 Windows NT Server 推出以来凭借其强大的功能和友好的操作界面使其在网络操作系统中的占有率节节上升，这两年 NT 更有成为主流网络操作系统的趋势。

由于 NT 界面和与 Windows 9x 的界面非常相似，所以大多数人觉得使用 NT 是一件非常简单的事情，在实际工作中却发现 NT 中许多问题并不像图形界面表现出来的那么简单易懂，比如说：

是否可以用 NT 计算机做路由器，

如何为 NT Server 配置 DHCP 服务，

NT 计算机如何提供远程访问服务，

NT 网络如何同 NETWARE 网络集成。

想要了解网络系统的功能就必须了解支持网络通信的协议。我们想通过描述 NT 的缺省网络协议——TCP/IP 的方方面面来解决读者在构建 NT 网络的过程中可能遇到的种种网络方面的问题。

书中主要讲述了 Windows NT 环境中的缺省网络协议——TCP/IP，详细说明了 TCP/IP 协议的工作原理，特别是 TCP/IP 协议在 Windows NT 网络中应用的各种专题，比如说 WINS、DNS、DHCP、ROUTER、RAS 等。

我们相信本书可以使读者对 Windows NT 的了解程序上升到一个新的阶段，本书适用于有一定网络知识，想用 Windows NT 平台架构网络的技术人员，和想了解 TCP/IP 协议如何在 NT 环境下工作的读者。

在此，我们对在撰写过程中提供了帮助的张逢梅、曹艳芬、王宇三位同志深表谢意，他们为本书的所有示例做了大量的实际验证工作。

另外还要特别感谢给我们巨大帮助的刘爱民、王瑾琪、赵玲和杨永春四位老师。

编　者

1998.12 于北京

目　录

第 1 章　TCP/IP 基础

本章，我们将学习以下几个要点：TCP/IP 的定义、在 Microsoft Windows NT 4.0 上的优点、安装和配置 Microsoft TCP/IP、利用测试工具测试 TCP/IP、利用网络监测器分析网络性能。

1.1　TCP/IP 的优越性

TCP/IP 代表传输控制协议/互联网络协议（Transmission Control Protocol/Internet Protocol）。它用于传输 Internet 网或局域网的数据。TCP/IP 是一种网络协议的名称，它规定了各个公司的硬件和软件产品必须遵守的协议，保证在不同机型、不同软件之间的数据传输。比如 DEC 的 TCP/IP 能与 Compaq PC 进行对话。协议定义了软件之间的通信，这好比两个人在电话对话一样："我告诉你这件事，其中有一些疑问，你通过查资料，把你所查到的资料告诉我，如果你那儿也没资料，就告诉我应该到哪儿去找。"

1.1.1　TCP/IP 的历史

提到 TCP/IP 就必须从 ARPNET 网络说起，ARPNET（Advanced Research Project Agency），它支持从事军事项目的研究人员之间进行快速通信。早期的这个网络是由 Bolt、Beranek、Newman（BBN）公司开发的。

ARPNET 于 1970 年在它的主机上使用网络控制协议（NCT）；1971 年 ARPNET 进入正常服务；1972 年提出了第一份 Telnet 标准——"Ad hoc Telnet Protocol"；1973 年产生了 FTP（File Transfer Protocol）文件传输协议，它主要的功能是将文件从一台机器传输到另一台机器；1974 年传输控制协议（TCP）诞生；1981 年互联网协议（IP）标准被颁布；1982 年 DCA（Defense Communications Agency）和 ARPA 创立了传输控制协议和互联网协议作为一套 TCP/IP 协议；1983 年 UCB 公布了一个 UNIX 版本，它内嵌了 TCP/IP，由于 UNIX 得到了广泛的使用，ARPANET 从 NCT 转入 TCP/IP；1984 年引入了域名系统 DNS，同年，ARPANET 被分成了两个不同的部分，一部分称为 MILNET 专门用于一般军事通信，另一部分仍叫 ARPANET，用来研究非军事项目。

1.1.2　TCP/IP 的优点

目前非常流行的 Windows NT 4.0 上有 Microsoft TCP/IP 协议，在装有 Windows NT 的计算机之间能够进行企业组网与连接。在 NT 中 TCP/IP 有以下几个优点。

（1）标准的、可路由的企业网络协议。TCP/IP 是现有的协议中最完整的，所有的现代操作系统都支持 TCP/IP（NT、UNIX），大多数网络依赖 TCP/IP 管理它们的网络通信。

（2）可以连接不同的系统。文件传输协议（FTP）和 Telnet 等许多标准的连接工具可用来在不同的系统之间传输数据，在 NT Server 中也包含了几个工具。

（3）强大的、广泛的、交叉平台式的客户机/服务器框架。Microsoft TCP/IP 提供插槽

（Windows Sockets）界面，它可以较好地用于开发运行于插槽之上的客户机/服务器应用程序。

（4）进入 Internet 的方法。TCP/IP 与 Internet 紧密交织在一起。

1.2 安装配置 Microsoft 的 TCP/IP

1.2.1 安装 Microsoft TCP/IP 的步骤

（1）在“开始(Start)”菜单中，选择“设置(Setting)”，然后点击“控制面板(Control Panel)”，“控制面板(Control Panel)”的窗口就出现了。

（2）双击“网络(NetWork)”，出现“网络(Network)”对话框。

（3）点击“协议(Protocol)”。

（4）点击“增加(Add)”，出现“选择网络协议(Select Network Protocol)”对话框。

（5）选择 TCP/IP Protocol 并点击“确定(OK)”按钮。

（6）弹出窗口，要求输入 NT Server 的源文件的路径，选择一正确路径。

（7）点击“继续(Contiune)”按钮，安装程序将从你提供的路径中安装文件。

（8）点击“关闭(Close)”按钮，出现 Microsoft TCP/IP 属性对话框。

（9）输入你分配的 IP 地址、子网掩码和缺省网关。

（10）点击“确定(OK)”按钮，提示你重新启动计算机。

（11）选择“确定(Yes)”按钮，重新启动计算机后，使用的就是你设好的 IP 地址。

1.2.2 手工配置 TCP/IP

如果你的网络中没有 DHCP 服务器，必须进行手工配置 TCP/IP 协议，使用 TCP/IP 协议的计算机的网络适配卡都需要 IP 地址和子网掩码，如果连接本地网之外的主机，还需要指定一个缺省网关。我们将使用控制面板的网络选项配置这些参数。IP 地址是 32 位逻辑地址，用于辨别 TCP/IP 主机，每个 IP 地址由两部分组成：网络 ID 与主机 ID。网络 ID 标识所有在同一物理网络中的主机，主机 ID 标识网络中的某台主机。IP 地址如 192.171.1.1，在一个物理网络中 IP 地址是唯一的。子网掩码用于掩盖 IP 地址中的一部分，使 TCP/IP 能够区分网络 ID 与主机 ID。

配置图如图 1-1 所示。

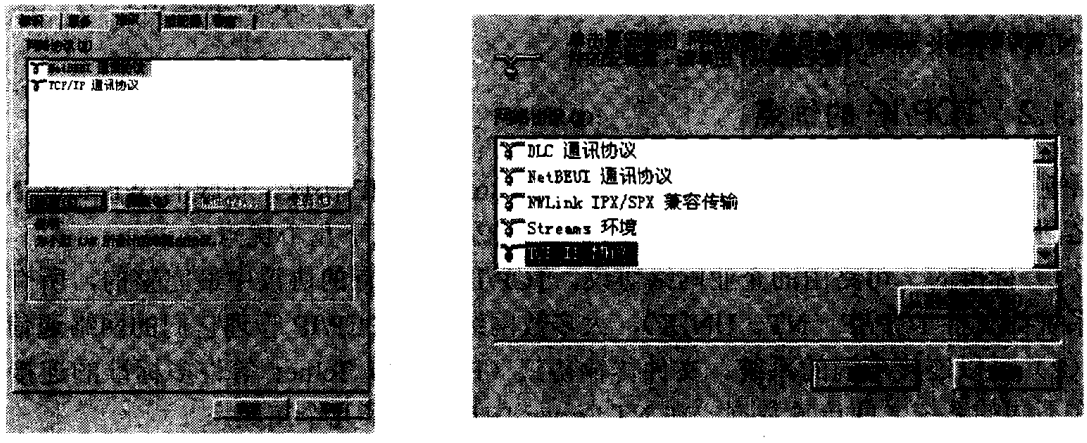


图 1-1

1.3 测试 TCP/IP

在 Windows NT 中装好 TCP/IP 后，你怎样才能发现你的 TCP/IP 是否安装正确？在 Windows NT 4.0 中带有 PING 和 IPCONFIG 两个工具可以测试你的 TCP/IP 安装是否正确。

1.3.1 IPCONFIG

使用 IPCONFIG 来验证主机的 TCP/IP 配置参数，包括 IP 地址、子网掩码和缺省网关，用这个工具可以看 IP 地址是否重复。

在命令处键入 IPCONFIG

如果配置已经初始化且 IP 地址没有重复，屏幕将显示如下内容：

Windows NT IP Configuration

Ethernet adapter E100B1:

IP Address.....:137.132.109.100

Subnet Mask.....:255.255.0.0

Default Gateway.....:137.132.109.2

如果你的 IP 地址是重复的，那么上面显示的子网掩码（Subnet Mask）将出现 0.0.0.0。

在 Windows95 中有一个 WINIPCFG 应用程序，也可以验证 TCP/IP 的配置。它显示的结果如图 1-2。

在窗口中可以看出这台主机配置的 IP 地址和子网掩码以及网关。

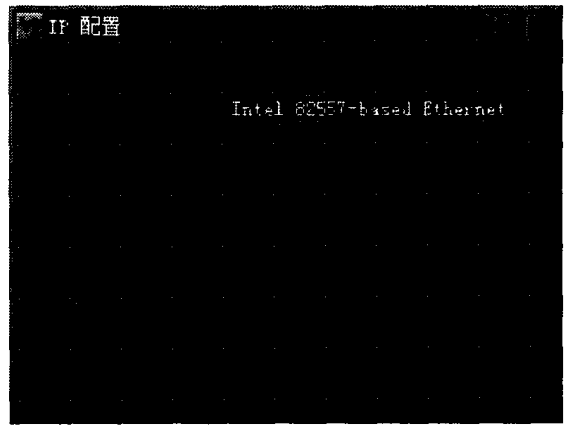


图 1-2

1.3.2 PING

PING 是一个 DOS 程序，它可以向另一计算机发送特殊的 IP 包。这个请求包会引起对方计算机返回一个应答包。

用 IPCONFIG 应用程序验证 TCP/IP 的配置后，可以使用 PING 来验证连接。PING 的命令格式如下：

PING　IP 地址

如果 PING 成功，屏幕将显示如下信息：

PING IP 地址 with 32 bytes of data:

Reply from IP 地址:bytes=32 time<10ms TTL=128

Reply from IP 地址:bytes=32 time<10ms TTL=128

Reply from IP 地址:bytes=32 time<10ms TTL=128

如果 PING 不成功，屏幕将显示如下信息：

PING IP 地址 with 32 bytes of data:

Request time out.

Request time out.

Request time out.

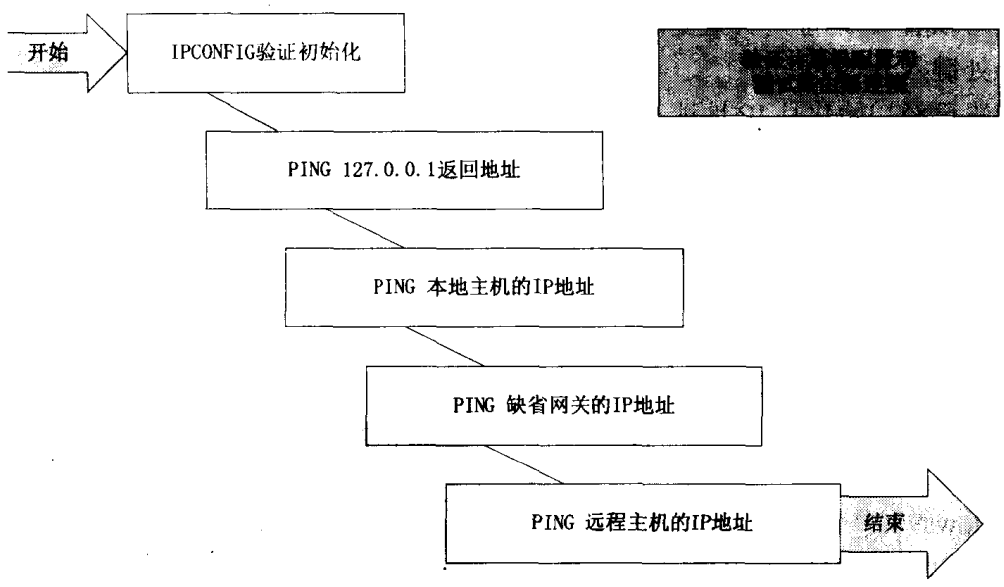
或显示如下内容：

Destination host unreachable.

Destination host unreachable.

Destination host unreachable.

现在以一个网络的检测过程举例说明 PING 的过程（如图 1-3）：



PING 远程主机的 IP 地址

图 1-3

（1）用 IPCONFIG 验证 TCP/IP 设置是否已经初始化；

（2）用 PING 返回地址来验证是否安装正确，在 DOS 提示符下输入 PING 127.0.0.1；

（3）PING 主机的 IP 地址，验证主机是否正确地加入，输入 PING 本地主机的 IP 地址；

（4）PING 缺省网关的 IP 地址，确定缺省网关是否工作以及能否与本地网络主机联系，输入 PING 缺省网关的地址；

（5）PING 远程主机的 IP 地址，确定是否能通过路由器与它联系。

1.4 监测网络

在 Windows NT 中带有一个工具软件来监测和分析网络，那就是 Microsoft Network Monitor，你可以利用这个软件把复杂的网络监测变成较轻松的工作。它通过设置网卡捕获进出信息包的方式来监测网络。

1.4.1 安装 Network Monitor

安装 Monitor 的步骤如下：

（1）用管理员身份登录到 NT Server；

（2）打开控制面板（Control Panel），选择网络（Network），点击服务（Services）；

（3）按增加（Add），出现选择网络服务（Select Network Services）对话框，如图 1-4；

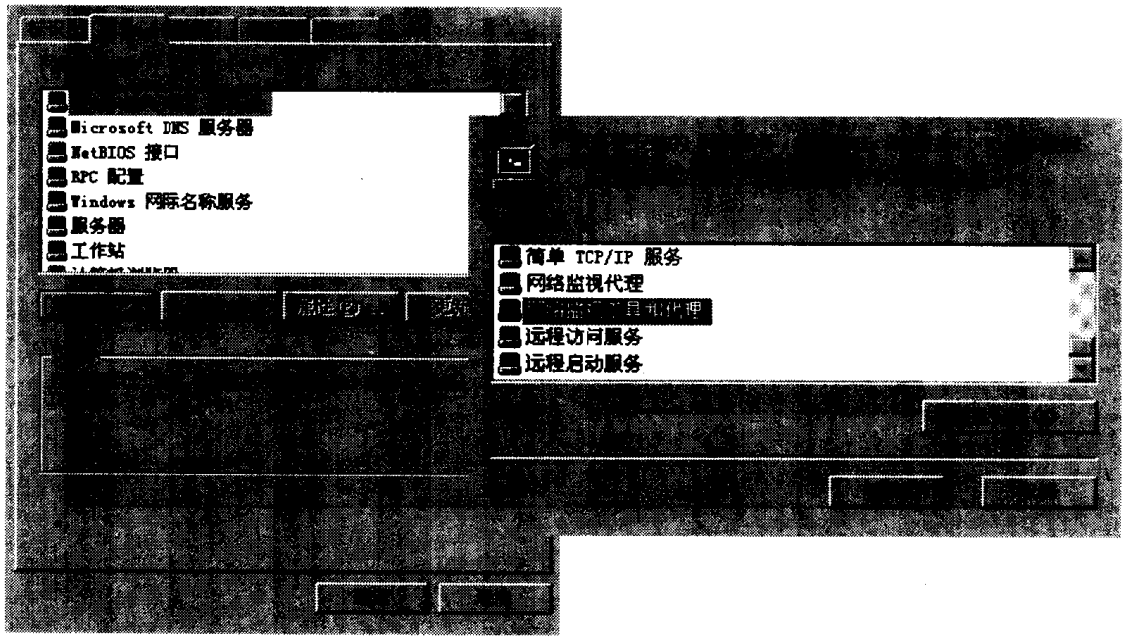


图 1-4

（4）在网络服务（Network Service）列表中选择 Network Monitor Tools and Agent。并按确定（OK）按钮，安装程序显示输入源文件的路径，插入你的 NT Server 光盘，输入源文件路径；

（5）安装完后，将重新启动计算机。

1.4.2 分析网络交通

用 Network Monitor 分析网络交通，首先要启动 Network Monitor，在 Start 菜单中选择 Programs，然后选择 Administrative Tools(Common)中的 Network Monitor。进入以后，显示的窗口是 Captrue 窗口，在 Captrue 窗口的上方有工具条，选择开始捕获按钮 ▶，捕获开始，在 Capture 窗口中显示出统计信息。当你发现你所要分析的网络交通之后，按工具条的停止按钮。怎样查看捕获的数据呢？选择 Capture 菜单中的 Display Capture Data 菜单,会显示出一个 Summary 窗口，显示出每一帧捕获，在它的窗口中可以看到帧数目、帧接收时间、来源地址、目的地址、最高层协议以及帧的描述。如果想看更详细的内容，在工具条上点击 Zoom Pane，会显示出 2 个附加的窗口，在上方的是 Detail 窗口，显示详细的协议信息；下方是 Hex 窗口，显示帧中的原始字节数，如图 1-5 所示。

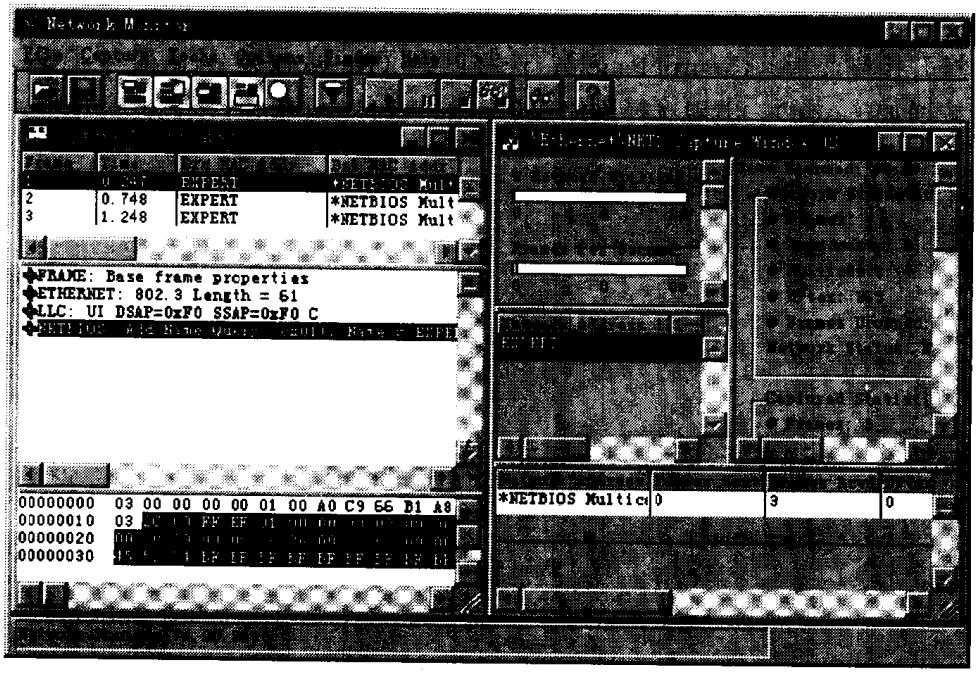


图 1-5

1.5 复习题

1. 用什么工具观察本机的 IP 信息设置?
2. 简述使用 PING 工具的顺序及每一步的用途
3. 运行 TCP/IP 必须有什么参数?

第 2 章　TCP/IP 协议组

在本章中我们将介绍以下几个内容：TCP/IP 协议的组成部分、每个协议做什么工作以及协议之间的联系、地址的解释过程。

2.1　TCP/IP 协议组

TCP/IP 协议组主要由 ICMP、IGMP、IP、TCP、UDP 等组成。这些协议分别应用于四层同构模型中：应用层、传输层、网间和网络接口。应用层为网络应用程序提供 WINDOWS SOCKETS 和 NETBIOS 两个接口来使用 TCP/IP 协议服务。传输层包括 TCP 和 UDP 两个协议，其作用是提供计算机之间的会话服务。INTENET 层包括四个协议，他们是 ICMP、IGMP、IP 和 ARP，它们负责完成数据包在发送过程中的路由和错误控制。网络接口层包含了网络类型等信息，作用是在网络和计算机之间进行桢的上传和下载。

各层为处理数据块，都要在数据块前加入一数据块，指明涉及哪一层，以及其他层和接收主机正确处理消息所需的信息位，每层都在源数据外加一层信息外壳，这一过程称为封装。

2.1.1　ICMP

ICMP（Internet Control Message Protocol）协议是为 IP 处理状态信息的协议，影响路由选择的网络硬件错误和变化，它位于网间层（Ineternet）。ICMP 消息以 IP 数据包形式传输，是不可靠的。

IP 协议本身不具备错误报告和错误纠正的功能，它是应怎样发现传输数据包的错误呢？它靠网际控制信报文协议来处理一个数据传输过程中发生的错误和状态。又在什么情况下发生作用？当数据包无法被递交或当一个网关采用较短的路径传输通信数据，或者网关没有足够的空间可以存放并转发数据的时候。

虽然，ICMP 能报告 IP 的一些错误，但它并不能增强 IP 的可靠性，不过 IP 必须得使用 ICMP，因为传输数据可靠性是上层协议的任务（如 TCP）。

ICMP 数据包的结构如表 2-1。

表 2-1　ICMP 数据包的结构

域	功　　能
类型	ICMP 数据包的类型，是 8 位的类型域
代码	指示在给定的类型中有哪些功能，如果只有一种功能，Code 为零，是 8 位的类型域，表示差错信息或状态信息的类型
校验	一个 16 位的校验和
Type-Specific	随类型变化的附加数据
Data	数据（可变长度）

2.1.2 IGMP

IGMP(Internet Group Management Protocol)用于 IP 主机向本地路由器报告主机组成员，允许路由器和主机相互报告有关多址传输操作的信息。它通知路由器在网络中特定多重广播组的主机可以使用，IGMP 数据包以 IP 数据包形式传输，是不可靠的。

IGMP 数据包的结构如表 2-2。

表 2-2 IGMP 数据包的结构

域	功 能
版本	IGMP 的版本是 0x1（固定）
类型	IGMP 的消息类型，0x1 类型是 Host Membership Query，用于特定的多重广播组中的任何成员的投票网络；0x2 类型是 Host Membership Report，用来声明成员属于特定的组或用来对 0x1 类型作出响应
未用	发送者置为 0，接收者忽略
校验和	8 字节 IGMP 头中的 16 位校验和
组地址	被主机用于在 0x2 类型中存储 IP 多重广播地址。在 0x1 类型中被设为 0

2.1.3 IP

IP（Internet Protocol）主要负责在主机与网络之间寻址和选择路径，处理数据的实际传输。它是一个无连接的协议，在数据交换之前相互之间没有联络，因此它的传递是没有保证的、是不可靠的。

IP 通过反复向目标 IP 地址传递数据包，直到目标主机接受数据或它在网络中的生存期结束。目标主机在收到数据包后，不通知发送者或接收者（包括数据包接收有错误），因此用这种方法传递数据包，数据包可能会丢失、发送顺序错误、重复或延迟。

IP 要传递一个数据包，在数据包前面要加入几个 IP 的域，如表 2-3。

表 2-3 IP 传递一个数据包的方法

域	功 能
版本	标识 IP 的版本（如 Ipv4）
Internet 报头长度	指定 IP 报头的长度
服务类型	约定 TOS 功能
总长度	指定包括报头在内的 IP 数据包的总长度
标识符	与地址字段一起，用于唯一标识该数据单元
标志	用于分段操作
分段偏移量	描述该数据包在原 PDU 中的位置
源 IP 地址	数据的发送者
目标 IP 地址	数据的接收者
协议	告诉目标主机 IP 是否将数据包传送给 TCP 或 UDP
校验和	用来简单验证数据包是否完整
生存期（TTL）	数据包在被抛弃之前允许在网络上停留的时间。防止数据包在网络内的无限循环。TTL 中存放的是秒值，WINDOWS NT 缺省的 TTL 是 128s

2.1.4 主要的 IP 服务

（1）网际报头检查。

当一个路由器接收到一个数据包时，它检查报头确定该数据包的类型，如果是一个网际数据包，路由器就把该数据包交给网际检查程序，报头检查模块对 IP 数据包报头进行一系列的编辑和有效性测试，如：有效的报头长度、正确的 IP 版本号、有效的 IP 报头长度、有效的 IP 报头校验和、非零生存时间的有效性。

（2）IP 源路由选择。

IP 通过源路由选择机制允许一个上层协议（ULP）决定 IP 路由器如何为数据包选择路径。当 IP 接受一个数据包时，它使用源路由选择字段确定下一个中间站点，IP 使用一个指针字段获得下一个 IP 地址，如果表中的地址用完，则使用目的 IP 地址字段进行路由选择，如果表中的地址没有用完，则 IP 模块使用指针所指向的 IP 地址作为下一个站点的地址。

（3）除了有上述两个功能外，还有路径记录、路由选择、路由记录选项、时间戳选项、路径跟踪、分段与重组等功能。

2.1.5 IP 地址和路由选择

IP 使用路由选择表和地址表在 Internet 上发送数据。路由选择表存储路径，地址表存储一个网络中实体（主机、路由器等）的地址。

IP 地址表是由 IAB 在 RFC1213 中发表的，表 2-4 描述的就是这 IP 地址表。

表 2-4 IP 地址表

	地址	接口索引	子网掩码	广播地址	数据包的最大尺寸
地址 1					
地址 2					
. . .					
地址 n					

其中 n 必须≥1，每一个地址（一个实体）占一行，如果某个实体占有多个 IP 地址，则该实体可以占多行。

地址：接口的 IP 地址；

接口索引：该实体的一个连接所使用的接口号；

子网掩码：包含表项地址列中的 IP 地址所对应的子网掩码；

广播地址：用于在本地接口上发送数据包并和本行的 IP 地址结合在一起；

数据包的最大尺寸：表示 IP 模块处理的数据包的最大尺寸。

IP 路由选择表随着 MIB（Internet）发表，出现正式的 IP 路由选择表的定义。

在 IP 路由选择表中主要有下面几项。

- 目的：该路径目的端口的 IP 地址，如果值为 0.0.0.0，表示该路径为缺省路径；
- 接口索引：标识了到达该路径中的下一个主机需要使用的本地接口；
- 尺度：共有 5 项表示尺度，用来确定路径的代价信息。代价尺度是到达目的端口所经过的站点数；
- “下一站点”：标识该路径中下一个站点的 IP 地址；
- 路径类型：它的值可为下面的 4 种值之一，1 不属于下面 3 种情况之一；2 一个

无效路径；3　一个直接连接的路径；4　间接；

- 路由选择协议：标识该路径所使用的路径发现协议；
- 路径年龄：从路径被更新或验证之后到现在的时间（s）；
- 路径掩码：将目的 IP 地址与 IP 数据包中包含的目的地址进行比较之前，用掩码与 IP 数据包中的目的地址进行“与”运算；
- 路径信息：取决于路由选择协议。

2.1.6　在路由器上的 IP

当路由器接收到数据包后，数据包被传送到 IP，IP 将做如下工作：

- IP 将生存期减 1 或根据实际路由器阻塞情况减去更多，如果生存期减到 0，该数据包被废弃。
- 如果数据包对网络来说太大，IP 会把它分割为更小的数据包。如果数据包被分割了，IP 为每个数据包生成新的报头。它包括：一个指示下一块的标志；一个用来辨别属于整个的所有部分 Fragment ID；一个通知接收主机如何重组数据包的 Fragment offset。
- IP 计算新的校验和。
- IP 获得下一个路由器的目标硬件地址。
- IP 转发数据包。

在每一个路由器上，这个过程将重复直到数据包到达目的地。

2.1.7　SOCKET

插槽应用程序通过协议端口号码识别，比如，在 Bullet Proof FTP（一个 FTP 应用软件）软件中需要输入一个 PORT（端口）地址号码，这样才能与 TCP 端口通信。

端口号码可以使用 0~65536（2^{16}）之间的任意数字。当有服务请求时，操作系统动态分配客户端的应用程序的端口号码，服务器一端的应用程序的端口号码是由 IANA 预先分配且不会改变的。注意：0~1023 范围的端口号码保留，应避免使用它们。常用的端口如表 2-5。

表 2-5　常用端口

端口号	名　称	描　述	端口号	名　称	描　述
5	RJD	远程作业表	68	BOOTPC	引导协议客户
7	ECHO	回声	69	TFTP	简单文件传输
11	USERS	活动用户	79	FINGER	Finger
13	DAYTIME	日期时间	101	HOSTNAME	NIC 主机名服务器
20	FTP-DATA	文件传输的数据	102	ISO-TSAP	ISO TSAP
21	FTP	文件传输	103	X400	X400
23	TELNET	TELNET	104	X400SND	X400 SND
25	SMTP	简单邮件传输	105	CSNET-NS	CSNET 邮箱名字服务器
37	TIME	时间	109	POP2	邮局协议 2
42	NAMESERV	主机名服务器	111	RPC	SUN RPC 端口图
43	NICKNAME		137	NETBIOS-NS	NETBIOS 名字服务
53	DOMAIN	域名服务器	138	NETBIOS-DG	NETBIOS 数据包服务
67	BOOTPS	引导协议服务器	139	NETBIOS-SS	NETBIOS 会话服务