
HZ BOOKS
Hack Attacks Revealed, Second Edition
网络与信息安全技术丛书
黑客攻击
揭秘篇
(美) John Chirillo 著
万静 胡春华 等译
附赠 CD-ROM
机械工业出版社
China Machine Press

网络与信息安全技术

黑客攻击揭秘篇

（美） John Chirillo 著
万 静 胡春华 等译

机械工业出版社
China Machine Press

本书由安全专家兼黑客John Chirillo根据现在自身的安全防范经验及过去黑客生涯中的攻击经历编著而成。内容极富实用性，详细地介绍了当前各种操作系统中的安全漏洞以及防火墙、代理、网关、路由器等网络设备面临的安全问题。本书详细给出了各种漏洞、病毒、蠕虫的来龙去脉，详细描述了黑客利用这些漏洞及弱点进行攻击的具体过程，并给出了相应的防范措施。本书内容翔实，讲解透彻，是一本在UNIX、Windows和Linux中定制安全工具集的完全参考手册。

John Chirillo: Hack Attacks Revealed, Second Edition (ISBN: 0-471-23282-3)
Authorized translation from the English language edition published by John Wiley & sons, Inc.

本书版权登记号：图字：01-2002-4873

图书在版编目（CIP）数据

黑客攻击揭秘篇/（美）切里罗（Chirillo, J.）著；万静等译. -北京：机械工业出版社，2003.4
（网络与信息安全技术丛书）
书名原文：Hack Attacks Revealed, Second Edition
ISBN 7-111-11804-9

Ⅰ.黑… Ⅱ.①切…②万… Ⅲ 计算机网络－安全技术 Ⅳ TP393.08

中国版本图书馆CIP数据核字（2003）第017233号

机械工业出版社（北京市西城区百万庄大街22号 邮政编码 100037）
责任编辑：周 睿
北京昌平奔腾印刷厂印刷·新华书店北京发行所发行
2003年4月第1版第1次印刷
787mm×1092mm 1/16·41.5印张
印数：0 001 - 4 000册
定价：69.00元（附光盘）

前　言

我们专攻技术，鄙视常规，至少这是我们处事的态度。我们擅长操作计算机。每件事对我们来说都很容易，并且当万事无忧时，世界看起来很不真实。或许，这就是我们为什么寻找阴谋的原因，并且当阴谋不存在时，我们自己来制造阴谋。或许，我会开动另外一个军事开关。

我们为什么会这样？

我们不同于其他人，其他人不会接受我们的行为。我们本身不是种族主义者、男性至上主义者或者理想主义者。我们不会在意其他人是否理解我们。我们在虚拟世界中聚集起来，而在现实世界中我们相互间却又是如此陌生、遥远，以至于我们不适应正常的社会生活。

我们能快速掌握概念，并且由于喜欢控制的天性，我们能够很快识破对我们撒谎的人。他们不能欺骗我们。我们不在意。需要干掉的系统有的是。实际上，我们关心更多东西，但是不能有效地影响它们。

我们对等待上天指示的技术大话感觉到眼花缭乱和困惑。什么时候才会实现？我们准备着，也希望早日得到它。如果它不出现……我们就感觉像被人抛弃一样。也许我们将创建它，或者至少梦想到它。这很混乱吗？

无知的幻想来自一群缺乏兴趣的人。

我们还不是技术无知者，茫然间等待遥远和可怕的未来。我们活着，并且渴望生活。我十分厌倦有些人说我们“与众不同”。我们是正迈入新千年的新一代，我们因技术而聚集，并生活在技术世界里，在这个世界上“与众不同”并没有什么关系。我们全都是“与众不同”的，全都不同寻常……但这并没有什么影响。我们这些处于技术尖端中的一些人极力嘲笑那些不懂得技术者。他们代表旧世界，被前卫和竞争所驱使。我们嘲笑他们，因为他们对人与人之间的差异漠不关心。他们为什么不能像我们这样？

微软想问我究竟目的何在。我只想着明天。我是未来的黑客，这就是我的宣言。

—Mindgame

随着世界变得日益网络化，竞争对手、间谍、不满意的雇员、无聊的年轻人，以及黑客会更加频繁地借助于因特网入侵别人的计算机，以便于偷窃信息、进行破坏工作、发泄以及捣乱。现在，因特网和万维网提供了一个新后门，通过该后门，远程攻击者可以入侵家庭计算机或者公司网络，并且偷窃数据。按照我的经验，大约85%的连接到因特网的网络都易于受这种类型的攻击。

随着因特网的成长以及技术的发展，攻击会变得愈发普遍。今天，外部攻击是任何连接到因特网的公司都要面临的问题。为了保证远程访问是安全的，保证系统本身的安全性，以及保证安全策略的实施，生活中每个人都应该理解攻击的含义。

本书的主要目标是向人们提供安全的基础知识。

本版的新内容

本书是英文版的第2版，与上一版相比，除了更正一错误之外，本版还提供70多个知识点、高级发现技术，以及Myparty、Goner、Sircam、BadTrans、Nimda、Code Red I/II等代码分析；路由器、操作系统（包括Windows 2000/ Pro和XP、Solaris和LINUX）和服务器软件守护程序等的脆弱点、建议、攻击试验，以及其他图解说明和技术介绍。本书还介绍了最常见的75种黑客攻击。在新版本中为了容纳新信息，大多数与

主题无关的信息、列表以及部分源代码已经转移到随书光盘中。

除了新信息之外，你还会看到新提供的完整的联网安全工具集——TigerSuit Pro3.5。该工具集包含用于发现、扫描、渗入、揭露、控制、窥探、洪水、欺骗、嗅探、感染、报告、监控等各种软件模块。以下是标准的TigerSuite工具：

工　具	扫 描 器
Finger Query（Finger查询）	Ping Scanner（Ping扫描器）
DNS Query（DNS查询）	IP Range Scan（IP地址范围扫描）
IP/ Hostname Finder（IP/主机名查找器）	IP Port Scanner（IP端口扫描器）
NS Lookup（NS查找）	Network Port Scanner（网络端口扫描器）
Telnet Session（Telnet会话）	Site Query Scan（站点查询扫描）
Trace Route（跟踪路由）	Proxy Scanner（代理扫描器）
WhoIs Query（WhoIs查询）	Trojan Scanner（特洛伊木马扫描器）
TigerWipe	
入 侵 器	**模 拟 器**
Buffer Overloader（缓冲区负载）	TigerSim:
FTP Cracker（FTP解密器）	Virtual Server Simulator（虚拟服务器模拟器）
FTP Flooder（FTP洪水器）	系统状态
HTTP Cracker（HTTP解密器）	CMOS
HTTP Flooder（HTTP洪水器）	Drive Space（驱动器空间）
Mail Bomber（邮件炸弹）	Volume Info（卷信息）
Mail Spoofer（邮件欺骗器）	Memory（内存）
Password Crackers（口令解密器）	Power（电源）
Ping Flooder（Ping洪水器）	Processor（处理器）
Server Side Crasher（服务器端崩溃器）	Network（网络）
TCP Flooder（TCP洪水器）	IP、ICMP、TCP和UDP
TigerBreach Penetrator（TigerBreach入侵器）	**侦　探**
UDP Flooder（UDP洪水器）	PortSpy Communication Sniffer（PortSpy通信嗅探器）
Win Crasher（Win 崩溃器）	

TigerSuite特殊版本（本书提供）包括如下更新特性和新特性：

改进特性	新增特性
DNS Query（DNS查询）	FTP Server Benchmark Testing（FTP服务器基准测试）
Trace Route（跟踪路由）	HTTP Server Benchmark Testing（HTTP服务器基准测试）
Trojan horse detection（特洛伊木马检测）	IP Stealth Port Scanner（IP秘密端口扫描器）
TCP Flooder（TCP洪水器）	UDP Port Scanner（UDP端口扫描器）
UDP Flooder（UDP洪水器）	Web CGI Vulnerability Scanner（Web CGI弱点扫描器）
Mail Spoofer（邮件欺骗器）	Web Custom HTTP Scanner（Web定制HTTP扫描器）
Mail Bomber（邮件炸弹）	IPX Flooder（IPX洪水器）
Ping Flooder（Ping洪水器）	SNMPWalk

Server Side Crasher（服务器端崩溃器）
Trojan Scanner（特洛伊木马扫描器）
TigerSim Virtual Server Simulator（TigerSim虚拟服务器模拟器）
TigerBreach Penetrator（TigerBreach入侵器）
PortSpy Communication Sniffer（PortSpy通信嗅探器）
TigerWipe Active Processes（TigerWipe活动进程）
TigerSuite VNC Remote Control（TigerSuite VNC远程控制）
PDA Viewers for remote handheld access（远程手持式访问的PDA查看器）
Network Quick Stats（网络快速状态）

注意：www.TigerTools.net/ support.htm是TigerSuit的技术支持站点。

本书读者对象

俗语“最好的防御是最好的进攻”肯定适用于网络安全领域。本书的评价者认为本书也许会成为管理者、网络管理员（CNA和MCP）、网络工程师（CNE和MCSE）、联网工程师（CCNA/P和CCIE）、安全咨询员（CISSP），甚至对此感兴趣的相关人士的必备参考书。本书提供的材料有助于读者更好地理解如何确定网络中的弱点。

更确切地说，本书的读者有：

- 家庭或者小型家庭办公（SOHO）的狂热推崇者。
- 经常考虑安全问题的网络工程师和安全工程师。
- 黑客、骇客以及朋客，对于他们本书既有教育意义，也有娱乐性。
- 非技术管理者，其工作也许依赖于本书提供的信息。
- 《Sneakers》、《黑客帝国》、《Hackers》和《箭鱼行动》这类电影的爱好者。
- 聪明好奇的年轻人，当读完本书之后他们的目的就明确了。

关于作者

John Chirillo从12岁就开始从事计算机职业，经过一年自学之后，他编写了名为Dragon's Tomb的游戏。该游戏在Color Computer System市场上销售了数千份。在接下来的5年中，John编写了一些其他软件包，包括The Lost Treasure（一个游戏编写教程）、Multimanager（一个记账、库房和财务管理软件包）、Sorcery（RPG探险游戏）、PC Notes（用于教授数学的GUI，范围从代数到微积分）、Falcon's Quest I和II（可以发音的图形化探险游戏）、Genius（一个完整的基于Windows的单击操作的操作系统），以及其他等等。John逐渐获得众多语言的证书，有QuickBasic、VB、C++、Pascal、汇编语言和Java。John后来开发了PC Optimization Kit（可以把标准Intel 486处理器芯片的速度提高200%）。

在开办两家公司（Software Now和Geniusware）之后，John成了大公司的顾问，专门负责安全和分析，需要进行安全分析、嗅探器分析，以及LAN/WAN设计、实现和解决问题。在该阶段内，John取得了很多网络技术证书，其中有：Cisco的CCNA、CCDA和CCNP，Intel Certified Solutions Consultant，Compaq ASE Enterprise Storage UNIX证书，以及即将获得的CISSP，等等。他目前是某技术管理公司的高级网络工程师。

本书除封面署名外，还有以下人员参加翻译工作：方建、刘辉、辛冉、周鹏、李家峻、郝丽杰、蒋佳、刘新喜、杨吉龙、张兴凯、吴淑英、邓多多、李欣、成洁易、王政、桂黎明、方巍巍、孙淑芳、王胜利、章波、曾心洁、陈安然、梁天天、刘洁威、武威、傅蓉、李克雅、周木。

目　录

第二部分 发 现

第三部分 入 侵

第五部分 黑客的工具箱

第六部分 附 录

第一部分

技　术

第1章 理解通信协议

大约30年前，通信协议就已被开发出来，用来连接单个站点以形成局域网（LAN，local area network）。在局域网中，一组计算机和其他设备分布在相对有限的范围内，通过通信链路连接在一起，而且在网络中，任何站点都可以和其他站点进行交互。这样的网络可以让站点共享像激光打印机、硬盘驱动器这样的资源。

在本章和下一章中，我们将讨论通信协议。通信协议是一组规则或标准，用于将站点与其他站点连接起来，以便进行信息交换。开放系统互连模型（OSI，open system interconnection model）是公认的计算机通信标准，它由7个协议层组成。在能够准确地定义、实施、测试安全防护措施之前，你必须完全理解这些协议。这两章包括了与以下主题相关的基础知识：IP、TCP、UDP、ARP、RARP、ICMP、IPX、SPX、NetBIOS和NetBEUI。

1.1 因特网简史

20世纪60年代，美国国防部高级研究计划署（ARPA，Advanced Research Projects Agency）（后来被称为国防部高级研究计划局，DARPA）开始建立了一个试验用的横跨整个美国的广域网（WAN，wide area network）。这个广域网被简称为ARPANET。它最初的目标是使政府机关、教育机构和研究试验室通过文件共享和电子邮件来共享计算资源，以促进这些机构的合作。但是没过多久，DARPA就认识到ARPANET具有的巨大潜力，而且有可能在世界范围内提供这种网络连接。

到20世纪70年代，DARPA继续提供资金支持，开展对ARPANET的研究，推动联网技术通信框架的发展。得到的框架就是传输控制协议/网际协议（TCP/IP，Transmission Control Protocol/Internet Protocol）系列（协议被定义成用于在计算机网络中进行通信的一组规则）。为了增加人们对这些协议的接受程度，DARPA向计算界公开了该计划的一个相对便宜的实现。加州大学伯克利分校伯克利软件设计（BSD，Berkeley Software Design）UNIX系统是该实验的一个主要目标。DARPA资助了一个名为Bolt Beranek and Newman的公司，该公司协助开发用于BSD UNIX系统的TCP/IP系列。

当这种新的技术出现时，许多机构正在开发局域网技术，以连接公共站点的两台或多台计算机。到了1983年1月，连接在ARPANET上的所有计算机都使用新的TCP/IP协议簇进行通信。在1989年，欧洲粒子物理研究所、欧洲高能物理实验室研究开发出了万维网（WWW，World Wide Web）。CERN此项研究的主要目的是通过使用超级文本，为世界上的物理学家提供更有效的通信方法。此时的超级文本只包括带有命令

行标签的包含在角括号“<> ”中的文档文本。标签用来表示文档的逻辑元素，例如题目、标题和段落。很快，它就发展成为了超文本标记语言（HTML，Hypertext Markup Language），程序员可以用它来生成可视化的信息页。1993年2月，伊利诺伊州立大学的全国超级计算应用中心（NCSA，National Center for Supercomputing Applications ）发布了著名的浏览器Mosaic。使用浏览器，用户可以浏览用图表表示的HTML信息页。

此时，大约有50台Web服务器可同时提供可视的HTML文件。9个月之后，这个数目上升到了500多台。大约一年之后，由84个国家的10 000多台Web服务器组成了万维网，它们运行在ARPANET的名为因特网的主干线上。

今天，因特网为世界上上百万台主机提供了合作的方法。因特网的主干基础设施可以提供的传输速率超过了45Mbp，这是ARPANET带宽的1000倍（带宽用来度量介质在某一时刻可以处理的通信量。在数字通信中，它描述了在通信链路中每秒可传输的数据量，简写成bps。“Bit”（位）是“binary digit”的简写形式，代表计算机中最小的信息单元。位由0或1组成；一个字节代表连续的8位）。

1.1.1 开放系统互连参考模型

国际标准化组织（ISO，International Standards Organization）开发了7层开放系统互连（OSI，Open Systems Interconnection）模型，用来描述在数据通信中执行的功能。理解每一层的工作原理很重要，因为它们合在一起就能实现成功的通信。分层有助于将联网复杂性分解成可以管理的部分，使得问题易于被发现；而且，分层允许特殊化——也就是允许开发商开发新的针对某一领域的产品。换句话说，OSI模型像一个调解人，允许不同的硬件和应用在一起很好地工作。

现在我们从上向下定义这7层：

- **第7层：应用层** 该层提供用户接口，将联网技术引入到应用中，执行应用同步和系统处理。该层定义的公共服务包括文件传输协议（FTP，File Transfer Protocol）、简单邮件传输协议（SMTP，Simple Mail Transfer Protocol），以及万维网（WWW，World Wide Web）。
- **第6层：表示层** 该层负责向第7层提供数据。该层使用像GIF、JPEG、ASCII和MPEG这样的编码方案，对数据进行编码、解码、压缩以及加密。
- **第5层：会话层** 第6层使用的会话机构在该层形成、管理和中止。该层主要定义表示层节点间的数据协调。Novell的服务访问点（SAP，Service Access Points）和NetBEUI是在该层起作用的协议。
- **第4层：传输层** TCP和用户数据报协议（UDP，User Datagram Protocol）在该层起作用。因此，该层负责节点间可靠的、面向连接的通信，并且为来自上层的数据提供透明的数据传输和错误校正。
- **第3层：网络层** 路由选择协议和逻辑网络寻址在该层运行。IP地址和交互网络包交换（IPX，Internetwork Packet Exchange）地址都是逻辑网络寻址。在该层定义的路由选择协议的一个例子是路由选择信息协议（RIP，Routing Information Protocol）（在后面会讨论这个话题）。
- **第2层：数据链路层** 该层提供可靠的数据传输，数据转换成位，通过物理层在物理网络中传输。该层具有如下两个子层：
- 介质访问控制（MAC，Media Access Control）子层：该子层负责将分组划分为带有MAC地址的帧、检测错误，以及定义物理拓扑结构（总线型、星型还是环型）。
- 逻辑链路控制（LLC，Logical Link Control）子层：该子层的主要目标是维护上层协议的标准化，使它独立于各种LAN。
- **第1层：物理层**。该层负责在物理通讯介质上比特的电子和机械传输。网络接口卡（NIC，network interface cards）、屏蔽线、非屏蔽线，以及拓扑结构（例如以太网和令牌网）都是物理介质。

1.1.2 网际协议

TCP/IP协议簇中的网际协议（IP，Internet Protocol）（RFC 791中有相应的描述）是4层模型（图1-1）。IP用来互连网络，形成因特网来回传输数据。IP包括寻址和控制信息，使分组可以在因特网上路由。分组被定义为是一种信息的逻辑组合，它包括带有控制信息的分组头和用户数据。遇到分组的设备（路由器）分离出分组头并检查其中包含的敏感路由信息。在传递过程中，这些分组头被不断修改，并被重新表示。

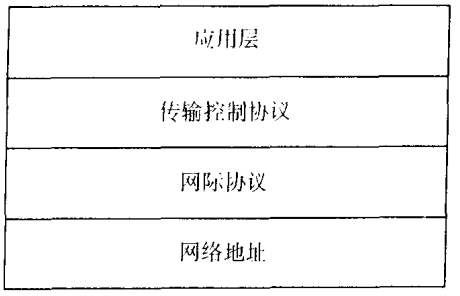

图1-1 4层的TCP/IP模型

黑客提示 分组头含有控制信息（路由说明）和用户数据。入侵者可以复制、修改和/或欺骗（伪装）这些信息。在本书后面的部分，我们将学到更多的剥窃手段。

IP的一个主要功能是提供永久建立的连接（称为无连接），在因特网上非可靠、高效地发送数据报。数据报可以被描述成是信息的逻辑分组，被当作一个网络层单元在通信介质上发送。IP数据报是因特网上的主要信息单元。IP的另一个重要功能是分片和重新组装数据报，以支持具有不同传输规模的链接。

在分析会话或嗅探器捕获（sniffer capture）中，区分不同类型的分组是必要的。下面描述了IP分组和其中的14个域，如图1-2所示。

- **版本号** 当前使用的IP版本。
- **IP分组头长度** 以32位字长表示分组头长度。
- **服务类型**（ToS，Type-of-Service） 上层协议（紧邻该层的上层协议，例如传输协议TCP和UDP）试图处理当前的数据报并试图指定其重要性。
- **总长度** 整个IP分组的长度，单位是字节。
- **标识符** 它是一个整数，用来帮助将分片的数据报组合在一起。
- **标志段** 长度为3位，第一位指定分组是否可以被分片。第二位指定分组是否是最后一片。第三位暂时还未使用。
- **报片偏移** 指出当前报片中的数据在初始数据报中的位置。用来重新组装原始数据报。
- **生存时间**（TTL，Time-to-Live） 一个递减的计数器，数值最小为0，防止分组无限循环。当值为0时，分组被丢弃。
- **协议** 指出正在接收的到来分组的上层协议。
- **分组头校验和** 用来保证IP分组头的完整性。
- **源地址** 发送IP分组的节点（站点、服务器、和/或路由器）地址。
- **目标地址** 接收IP分组的节点（站点、服务器、和/或路由器）的地址。
- **选项** 一般包含安全选项。

• **数据** 上层信息。

黑客提示 值得特别注意的部分是源地址、目标地址、选项和数据。

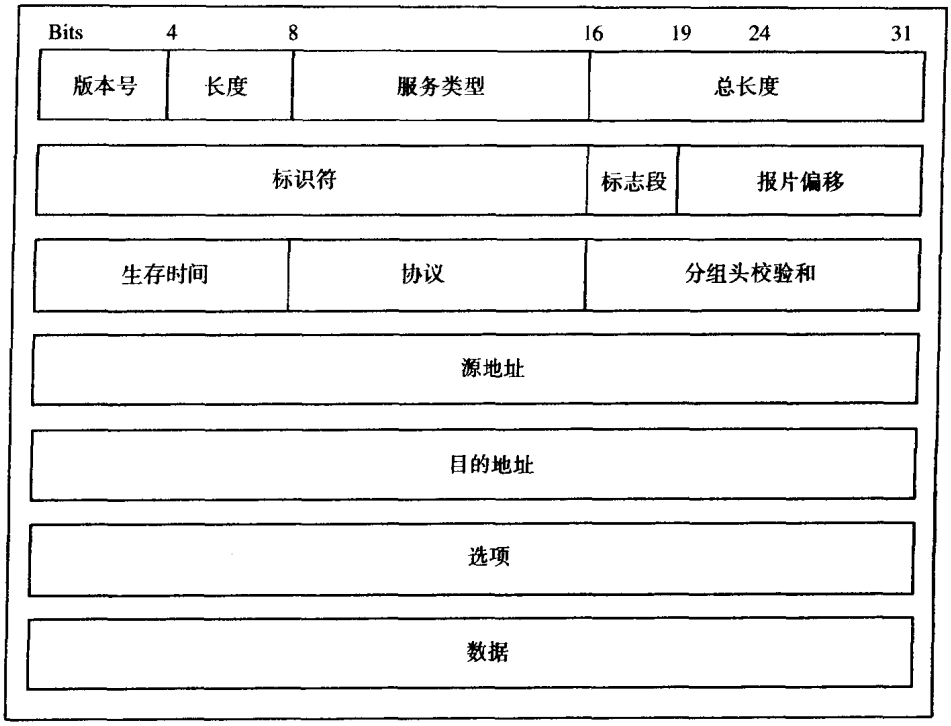

图1-2 IP分组

现在让我们看一下图1-3a和1-3b中用嗅探器得到的实际的IP分组头并和前一个图的各部分做一下比较。

```
------ IP Header ------
IP:
IP: Version = 4, header length = 20 bytes
IP: Type of service = 00
IP:       000. .... = routine
IP:       ...0 .... = normal delay
IP:       .... 0... = normal throughput
IP:       .... .0.. = normal reliability
IP: Total length    = 60 bytes
IP: Identification  = 59136
IP: Flags           = 0X
IP:       .0.. .... = may fragment
IP:       ..0. .... = last fragment
IP: Fragment offset = 0 bytes
IP: Time to live    = 32 seconds/hops
IP: Protocol        = 1 (ICMP)
IP: Header checksum = 0376 (correct)
IP: Source address      = [172.29.44.14]
IP: Destination address = [172.29.44.2]
IP: No options
```

图1-3a 在因特网控制消息协议（ICMP，Internet Control Message Protocol）Ping测试的传输中，用嗅探器得到的IP分组头

```
----- IP Header -----
IP:
IP: Version = 4, header length = 20 bytes
IP: Type of service = 00
IP:       000. .... = routine
IP:       ...0 .... = normal delay
IP:       .... 0... = normal throughput
IP:       .... .0.. = normal reliability
IP: Total length    = 112 bytes
IP: Identification  = 4864
IP: Flags           = 4X
IP:       .1.. .... = don't fragment
IP:       ..0. .... = last fragment
IP: Fragment offset = 0 bytes
IP: Time to live    = 32 seconds/hops
IP: Protocol        = 6 (TCP)
IP: Header checksum = FA8F (correct)
IP: Source address      = [10.55.28.117]
IP: Destination address = [10.55.28.22]
IP: No options
```

图1-3b 在NetBIOS用户数据报协议（UDP，User Datagram Protocol）会话请求（这些协议将在本章的后半部分和第2章中介绍）的传输中，用嗅探器得到的IP分组头

1.1.3 IP数据报、封装、大小和分片

IP数据报是因特网最基本的传输单元。IP数据报是IP组件之间的数据交换单元。IP数据报具有报头，报头包含像路由器这样的基础设备使用的路由信息（请参考图1-4）。

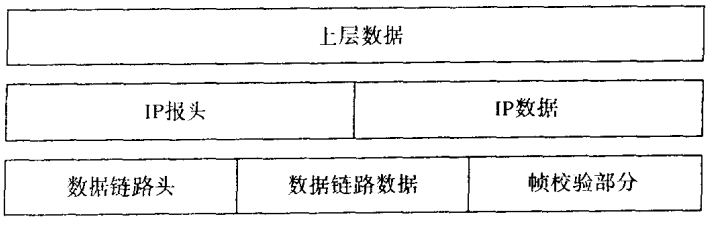

图1-4 IP数据报图

分组中的数据不是IP关心的内容。IP关心的是控制信息，它们与上层协议有关。控制信息包含在IP分组头中，用来在本地网或因特网上把数据报发送到目标地址。为了理解这种关系，可以将IP看成是方法，将数据报看成是工具。

黑客提示 IP头是收集信息，获得控制的主要部分。

理解数据报在网络中传播的方法很重要。为了充分地在因特网的物理介质上传播，我们需要保证每一个数据报以一个物理帧的形式传播。数据报在介质中以一个帧的形式传播的过程称作封装。

现在让我们看一下实际的数据报传播情况，以进一步解释传播数据报的方法（请参考图1-5）。这个例子包括三个分支部门间的共同连通性，它们通过因特网、链接以太网、令牌环网和光纤分布式数据接口（FDDI，Fiber Distributed Data Interface）或光纤冗余令牌环网连接。

理想的情况是一个完整的IP数据报刚好装满一帧；它通过的网络支持特定的传输尺寸。但是，这种理想的情况非常少见。问题其中一个是对数据报而言的，网络对传输尺寸规定了最大传输单元（MTU，