

# 第一部分 TCP/IP 及其安全需求： 防火墙

## 第1章 网络互连协议和标准概述

因特网是一个发展非常活跃的领域。在 1968 年，它的早期研究成果开始崭露头角，后来便出现了它的前身 ARPANET，ARPANET 为表现因特网特性的试验平台做出了重大贡献，1973 年，因特网正式面世。

从那时起，关于因特网的研究和努力就一直没有间断过，其中大部分努力都是围绕着被称为网络的一个新型赛博空间所需要的标准而进行的。当然，你必须明白，在因特网环境中“成就”一词的意义已超出了这个词在字典里原来的意义。因为因特网有着无限的生机，它对问题和困难的解决总是超过预想的标准，Lynch 与 Rose 所写的书“*Internet system Handbook*” (1993) 中引用 David Croker 的一句话：“因特网标准的进化过程把实用的工程风格与广泛的社会支持结合在了一起”。“成就”一词所代表的更是一种个人的成功，而不是某个机构筹划的结果。

因特网协议及其标准与世界上任何其他事物的结构不同，它总是由一些机构或专业人士中的个人首先提出的。为了了解新的协议是如何出现并最终成为标准的，应该首先熟悉缩写词 RFC，即 Request for Comment。它的发展变迁过程要追溯到 1969 年，起因是由于因特网的成员过于分散。正如这个词的字面意思所示，这些文档是一些实用文档、方法、测试结果、模型甚至完整的规范。因特网社会的成员可以阅读，也可以把意见反馈给 RFC，如果这些想法（或基本原理）被社会接受，就有可能成为标准。

在因特网社会中关于 RFC 的用法（MO）以及如何操作并没有太大的变化。1969 年，当时只有一个网络，整个社会不超过一百位专业人员；随着因特网的飞速发展，因特网不但需要一个机构来集中和协调这些成果，并且需要制定一个最低要求的准则，至少能在成员之间进行有效的通信并取得相互了解。

1974 年前后，摆在 ARPANET 面前的形势很清晰了，通信联络需要进一步扩展，它需要的不仅是要能容纳成倍增加的通信媒体，而且要了解早已存在于群组中的许多领域的意义。这个领域需要一个管理者。大约在 1977 年，随着作为因特网实验备忘录（IEN）一部分的许多实验的进行，著名的 TCP/IP 协议获得了发展的动力。

没过多久（1986 年），为了 RFC 讨论的需要，需要建立一个由工程技术人员组成的、对标准的发展负责的工作机构，以便有效地引导因特网的发展成长，这样，因特网工程工作组（INENG）成立了。

今天，因特网工程部（IETF）和因特网研究部（TRTF）成为对因特网近期工程需求和远期研究目标负责、并担负重任的两个工作组。这两个组织曾直接隶属于国际网络执行委员会（IAB），现在属于因特网协会（1992 年成立），这个协会最终也是为因特网技术的发展负责的。但是，如果你是一个因特网上的常客，可能对缩略词 IAB 并不满意，的确，在 IAB 的逐步发展

并走向成熟过程中，IAB将它的名字改为“Internet Architecture Board”(由“Activities”改为“Architecture”)，因为IAB在因特网发展的运作方面并没起多大作用。

谈到RFC标准，那么首先考虑到的应该是RFC 733。如果有关于标准的想法或对因特网有益的新技术，可以把它作为RFC提交给因特网社会。作为IAB成员之一的RFC编辑，决定着RFC的发表，对任一正式文档，RFC都有一种确定的风格和格式。

**提示** 如果想得到RFC格式指南，请参考RFC 1111。有关RFC提交方面的信息，请发邮件到rfc-editor@isi.edu。要得到RFC目录，可以检索文件rfc/rfc-index.txt。

**注意** 关于IAB、IETF和IRTF更详细的信息，建议查阅Lynch与Rose所著的《Internet System Handbook》，这不属于本书所讨论的范围。

本书并不讨论因特网上所用到的每一个协议，这是因为：

这些协议太多且一直在不停地变化，全部列出来对你并没有太多帮助。

我们的主要目的是集中在每个协议具体的安全缺陷上。通过对它们安全特性的评估，不但会使你在选择一个协议时做出更明确的决定，而且也会使你明白为什么诸如密码、防火墙和代理服务器等技术会成为系统安全决策时的必要选择。

因此，本章集中讨论主要的因特网协议及它们的特性、缺陷、强度以及在因特网上它们是如何对连通性和数据交换产生影响的。表 1-1 列出了因特网上用到的主要协议。

表1-1 提交给IETF 的关于IP 支持的RFC

RFC号	文档内容描述
768	用户数据报协议(UDP)
783	次要文件传输协议(TFTP)
791	网际协议(IP)
792	因特网控制报文协议(ICMP)
793/1323	传输控制协议(TCP)
826	地址转换协议(ARP)
854	虚终端协议(Telnet)
877/1356	X.25 网络IP over
903	反向地址转换协议(RARP)
904	外部网关协议(EGP)版本2
950	IP子网扩展
951	引导协议(BootP)
1001	TCP/UDP中NetBIOS 服务协议标准 传输：概念和方法
1002	TCP/UDP中NetBIOS 服务协议标准 传输：详细规范
1009	因特网网关需求
1042	IP over IEEE 802 网络
1058	路由信息协议(RIP)
1063	最大传播单元发现选项
1075	距离向量多播路由协议(DVMRP)
1084	引导协议厂商扩展
1108	修订网际协议安全选项(RIPSO)
1112	因特网群组管理协议
1155	管理信息的结构和鉴别

(续)

RFC号	文档内容描述
1156	因特网管理信息基础
1157	简单网络管理协议(SNMP)
1188	IP over FDDI
1247	开放式最短路径优先(OSPF)版本2
1256	路由器的发现
1267	边界网关协议(BGP)版本3
1519	无类域间路由选择(CIDR)
1532	分类和扩展BootP for 引导协议
1533	DHCP选项和自举协议扩展
1542	分类和扩展BootP for DHCP
1654	边界网关协议版本 4 (BGP-4)

## 1.1 网际协议

网际协议(IP)是广泛用于公司、政府部门和因特网上的网络协议。它支持许多个人、专业以及商业上的应用系统,像电子邮件、数据处理以及图像、声音的传输等。

IP是一个无连接的数据报(报文)传输协议。用它来进行网上的寻址、路由选择以及对传输和接收数据报进行控制。每个数据报都包括源地址和目的地址、控制信息以及传向主机层或来自主机层的真实数据。IP数据报是进行网上(包括因特网)传送的基本单位。由于IP是一个无连接协议,所以它不需要预定义一个与逻辑网络连接的关联路径。由于信息包是由路由器接收的,因此IP寻址信息常用来确定信息包到达其最终目的地址的最佳路由。这样,尽管IP没有关于数据路径用法的控制,但当一个资源不可用时,它能为数据报重选路由。

### 1.1.1 IP寻址

在IP中有一种机制,它能使主机和网关通过网络路由数据报。IP的这种传递是根据每个数据报的目的地址进行的。当IP接收到一份数据报时,便检查它的报头(报头存在于每个数据报中),查找目的网络号和路由表。IP数据报的包头格式如下(见图1-1):

版本	包头长度	服务类型	总长	识别码	标志	标志偏移量	生存时间	协议	头部校验和	源IP地址	目的IP地址	IP选项	填充	数据
(4位)	(4位)	(1)	(2)	(2)	(13位)	(13位)	(1)	(1)	(2)	(4)	(4)	(可变)	(可变)	(65 500位)
(# bytes)														

图1-1 IP包头格式

用来创建数据报的IP协议的版本号。

包头长度。

数据报需要的服务类型。

数据报长。

数据报标识号。

段控制信息。

数据报在因特网/内部网中传输的最大跳数。

数据域协议格式。

源地址、目的地址。

IP选项。

所有具有本地地址的数据报都可用 IP 直接传送，而具有外部地址的数据报则根据路由表信息向着目的地址的方向传向下一站。

IP 还管理着数据报的大小，如果数据报的大小超过实际网络能传送的最大长度，IP 将会根据网络硬件的处理能力把数据报分成更小的段，这些数据报在最终被传送到目的地址后又重新被组装在一起。

IP 连接由 IP 地址控制。每个 IP 地址唯一标识网络上的一个节点，这在受保护的网（局域网，广域网和内部网）和诸如因特网的不受保护的网络上都是一样的。IP 地址是用来沿网络传递信息包的，就像美国邮局向全国和全世界按邮政编码顺次递送信件和包裹那样。

在一个诸如 LAN 的受保护的网络环境中，一个节点可以是一台使用 DOS 局域网工作区（LWPD）的 PC，这里的 IP 地址是在 LWPD 软件安装过程中经过对配置文件的修改而设置的。

IP 协议是 TCP/IP 的基础。TCP/IP 的特别之处在于它能用于连接非同类的计算机系统，这将在本章后面部分详细介绍。

### 1.1.2 IP 安全风险

如果在因特网上没有关于连接的安全风险，也就没必要有防火墙和其他防范机制了。基于 IP 协议的安全解决方案虽然可以广泛地由商业渠道获得并且能随意使用，但从本书中你可以认识到，在大部分时间内，一个系统还需要行政管理的力量，从而尽可能地把黑客挡在门外。

计算机安全越来越成为一个公众关注的问题，我们不可能全部列出处理基于 IP 协议安全问题的工具及其实用程序。本书介绍一些安全机制、硬件技术和应用软件以帮助审核所在网络的安全性。现在，让我们把注意力集中到因特网连接协议的安全缺陷上来，看一看缺陷的鉴别及其可能的解决方案。

IP Watcher：IP 协议的劫持

如图 1-2 所示，这里有一个称之为 IP Watcher 的商业产品。无论何时，只要管理员（或黑客）需要，IP Watcher 就可通过监视因特网会话以终止或取得对它们的控制，从而劫持 IP 连接。在公开的连接表上迅速点一下，就可显示当前的会话和所有键入的信息。再点一下，当 IP Watcher 接管会话时，用户已经彻底被控制了。不用说，这种软件的罪恶用途几乎是无限的。

但是，当考虑 IP 连接的安全时，所要关注的不仅仅是 IP Watcher，在黑客团体中，还有很多用来劫持连接的工具。而 IP Watcher 的方便之处（实在是一种威胁）在于它能被很容易地通过点击而加以利用。

尽管被 IP Watcher 监视时所产生的痕迹很少，很容易骗过你，但还是可以发觉的。如果发往服务器的数据报严重超时，这就是一个明显的迹象，说明你的 IP 连接被劫持了；还有，如果你是一个很警觉的网络管理员，就能看到通常提到的 ACK 风暴：即当某人劫持了一个 IP 连接，由于试图要在服务器（或工作站）上试着重建会话连接而造成的一种风暴。这会引起网

络上信息的严重泛滥和阻塞。

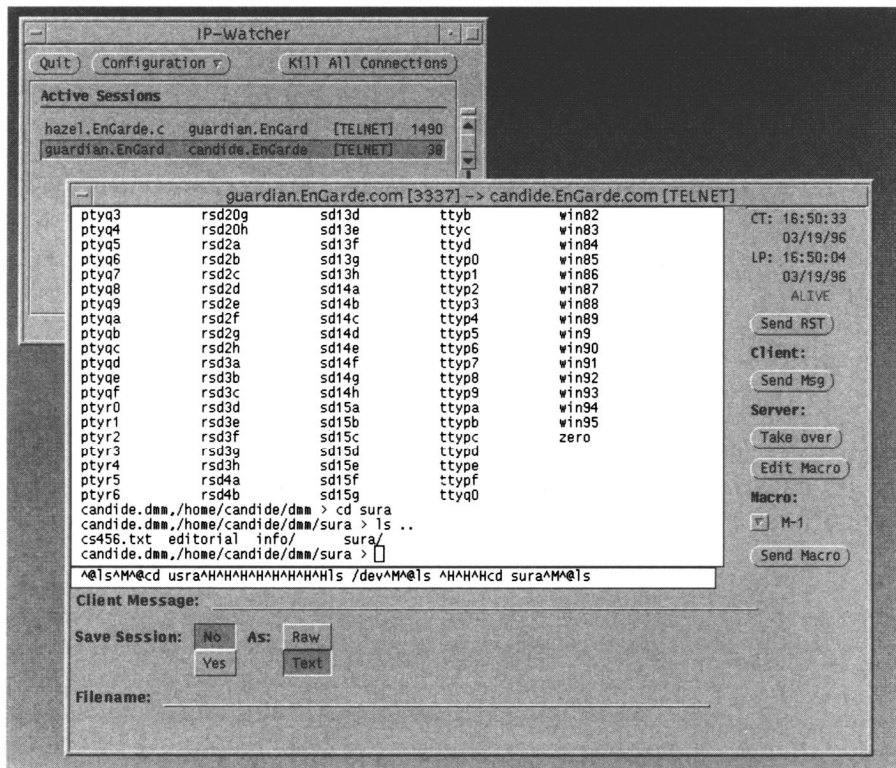


图1-2 IP Watcher，一个黑客引擎

还有一些出自黑客的高级工具，用来拦截 IP 连接，但使用起来并不是很容易；甚至还有一些工具能够在阅读电子邮件时将数据插入到连接中。例如，你的文件突然可通过网线传到远程网站，你所觉察到的迹象仅仅是信息包传送时有些延时，但当阅读电子邮件时，却不会觉察到它。不过劫持 IP 连接并不像说起来那样简单，这需要攻击者直接进入连接的数据流中，因此，大多数情况下，攻击者若想劫持 IP，必须进入你的站点。

**提示** 如果想在因特网或受保护的网络上得到更多的关于管理或劫持 IP 连接的工具，请查询下列站点：

<http://cws.iworld.com>——此站点提供了一些 16 位和 32 位 Windows (NT 或 Windows 95) 因特网工具。

<http://www.uhsq.uh.edu>——此站点提供了一些 UNIX 安全工具，并对工具作了简短的综合描述。

<ftp://ftp.bellcore.com/pub/nmh>, <ftp://primal.iems.nwu.edu/pub/skey>——此站点支持 S/Key 核心软件。

<ftp://ftp.funet.fi>——在这里你会找到一些普通的关于安全 / 破坏的实用程序，诸如 npasswd、passwd+、traceroute (如图 1-3 所示)、whois、tcpdump、SATAN 以及 Crack。为了在实用程序中进行快速查找，一旦进入站点，使用引用站点查找 < find >，



find > 是查找文件系统的语句。若使用 Web 客户，则使用 `http://ftp.funet.fi/search:<find>站点`。

```
[root@luxor /root]# traceroute www.whitehouse.gov
traceroute: Warning: www.whitehouse.gov has multiple addresses; using 198.137.240.92
traceroute to www.whitehouse.gov (198.137.240.92): 30 hops max, 40 byte packets
 1 em1 (192.55.214.202)  2.836 ms  2.039 ms  2.030 ms
 2 mtnet-50T0.MF.Net (204.220.21.137)  15.486 ms  9.490 ms  17.263 ms
 3 M10Net-gw.MF.Net (137.192.3.254)  9.136 ms  10.129 ms  9.496 ms
 4 t3-gw.mci.net.net (198.174.96.5)  9.055 ms  11.301 ms  13.271 ms
 5 border5-hssi1-0.Chicago.mci.net (204.70.186.5)  17.112 ms  18.046 ms  17.842 ms
 6 core2-fddi-0.Chicago.mci.net (204.70.186.49)  20.949 ms  18.465 ms  20.048 ms
 7 core2-hssi-3.NorthRoyalton.mci.net (204.70.1.253)  24.453 ms  23.439 ms  29.226 ms
 8 bordercore2-loopback.Atlanta.mci.net (168.48.48.1)  188.168 ms  43.909 ms  67.561 ms
 9 core3.Atlanta.mci.net (204.70.4.9)  43.264 ms  44.555 ms  42.790 ms
10 * ast-ps1-map.Atlanta.mci.net (206.157.77.50)  209.006 ms  190.108 ms
11 mcr-rt-30.ps1.net (38.1.3.7)  110.631 ms  102.360 ms  131.482 ms
12 * se-30.ps1.net (38.1.3.5)  562.659 ms *
13 rc5-southeast.us.ps1.net (38.1.25.5)  295.153 ms * 168.730 ms
14 38.25.11.2 (38.25.11.2)  161.114 ms  166.938 ms *
15 * 198.137.240.33 (198.137.240.33)  183.045 ms  166.193 ms
16 www2.whitehouse.gov (198.137.240.92)  169.966 ms  174.018 ms  175.163 ms
[root@luxor /root]#
```

图1-3 运行中的路由跟踪工具的界面

对于提供给因特网网络信息中心（InterNIC）的信息一定要注意。如果要在因特网上建立一个站点，则必须向InterNIC申请一个域名，这时，必须提供所在机构的管理和技术联系方面的信息，以及他们的电话、电子邮件地址和网站的物理地址。尽管这是一个很好的安全方法，但如果有人使用UNIX命令“`whois <domainname>`”，其结果将如图1-4所示，将列出你提供给InterNIC的所有信息。

```
[root@luxor /root]# whois "WHITEHOUSE-HST"
Executive Office of the President USA (WHITEHOUSE-HST)
  Room NE0B 4208
  725 17th Street NW
  Washington, D.C. 20503

  Hostname: WHITEHOUSE.GOV
  Address: 198.137.241.30
  System: SUN running SUNOS

  Host Administrator:
    Fox, Jack S. (JSF) fox_j@H1.EOP.GOV
    (202) 395-5417

  Record last updated on 19-Oct-95.

To see this host record with registered users, repeat the command with
a star (*) before the name; or, use % to show JUST the registered users.

The InterNIC Registration Services Host contains ONLY Internet Information
(Networks, HSN's, Domains, and POC's).
Please use the whois server at nic.ddn.mil for MILNET Information.
[root@luxor /root]#
```

图1-4 UNIX 中whois命令的使用

但这意味着你可以拒绝向 InterNIC 提供信息。向 InterNIC 提供信息是必需的，并且反过来也能用来为你提供保护。不过，当你提交完这个信息时必须记住，黑客通常就是用它来找到一个网站的基本信息的。因此，一定要谨慎。例如，对于联系名，可以用一个缩写或用绰号。向 InterNIC 进行信息咨询，通常是你的网络遭受攻击的开端。

1997年春，我的函件发往南方，去协调从 MS Mail 到 MS Exchange 的转换，结果有少数几个邮寄列表服务器出现信息垃圾。几个小时内，我们的一个系统管理员在家接到一个投诉电话，拨的就是他家的电话号码，投诉者很清楚要找谁。通过使用“whois”，遭受信息垃圾攻击的列表服务器的系统操作员能够识别出我所在公司的名字和地址，因为是周末，他找不到别人讨论这个问题，只能根据系统管理员的名字和我们公司所在的城市，快速搜索（如：Four 这样的搜索引擎 <http://www.four11.com>）以获悉我们系统管理员的家庭地址和电话号码。

## 1.2 用户数据报协议

RFC 768 中记录的用户数据报协议（UDP），为 IP 提供了一种不可靠、无连接的数据报传输服务。因此，此协议通常应用于面向事务的实用程序，如 IP 标准“简单网络管理协议（SNMP）”和“次要文件传输协议（TFTP）”。

同下一节要讨论的 TCP 一样，UDP 与 IP 协同工作用来传送报文到目的地址，并提供协议端口以区分运行于单个主机上的软件应用程序。然而，与 TCP 不同的是，UDP 并不保证数据不丢失和不被复制，因此，如果要使数据传输可靠的话，一定要用 TCP 而不是 UDP。图 1-5 给出了 UDP 报头格式。

0	7	8	15	16	23	24	31
源端口				目的端口			
长度				校验和			
数 据...							

图1-5 用户数据报报头格式

### 1.2.1 攻击用户数据报协议服务：SATAN 轻松应对

SATAN，一个流行的用于 UNIX 系统网络审查的免费工具。它是一个基于因特网的工具，能够审视运行于系统上开放的用户数据报协议（UDP）服务（同 TCP 一样），并且在它发现的服务上能进行低层的脆弱性检测。

尽管当前操作系统中被检测出的脆弱之处大多数已被修正，SATAN 仍广泛地用于系统配置的检查。这个工具用起来简单，但有点慢，当网络不稳定时，也不太精确。

SATAN 运行于 UNIX 的 X-windows 下，为使它更具特色，需要有一个能为 Linux 提供补丁的版本。当用这个工具进行繁重的审查设置时要当心，因为它经常对过时的脆弱之处不给予报警。

### 1.2.2 用于 UNIX 和 Windows NT 上的因特网安全系统

因特网安全系统（ISS），如图 1-6 所示，是一套用于审查 Web 服务器、防火墙和内部主机的商业产品。这套产品包括许多最新的探查 UDP 服务（同 TCP 一样）的因特网攻击工具和检

查系统脆弱性的工具。经过配置它可以进行周期性检查，并有几个选项可用于报告的生成，其中也包括输出到数据库。

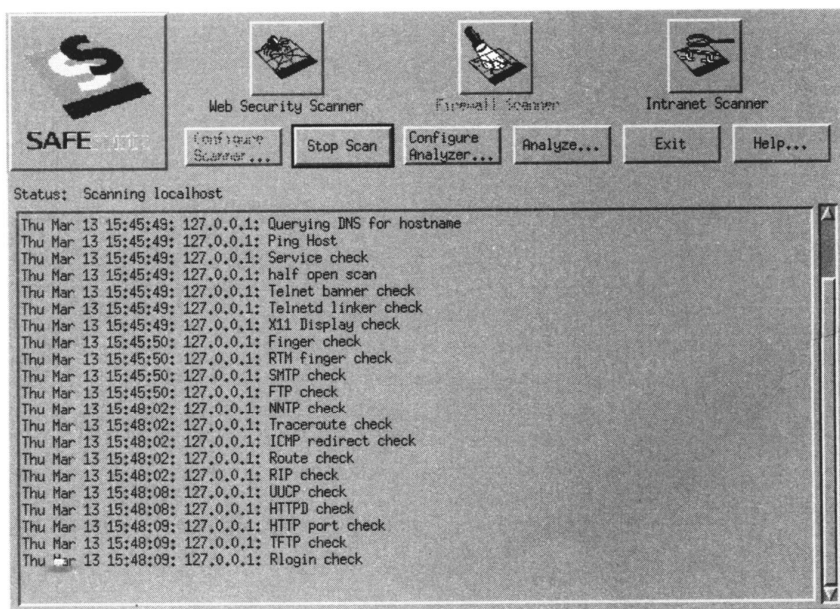


图1-6 ISS 扫描本地主机的界面

作为一种审查工具，ISS的攻击水平和高度可定制的特点远远超过 SATAN。如图1-7显示

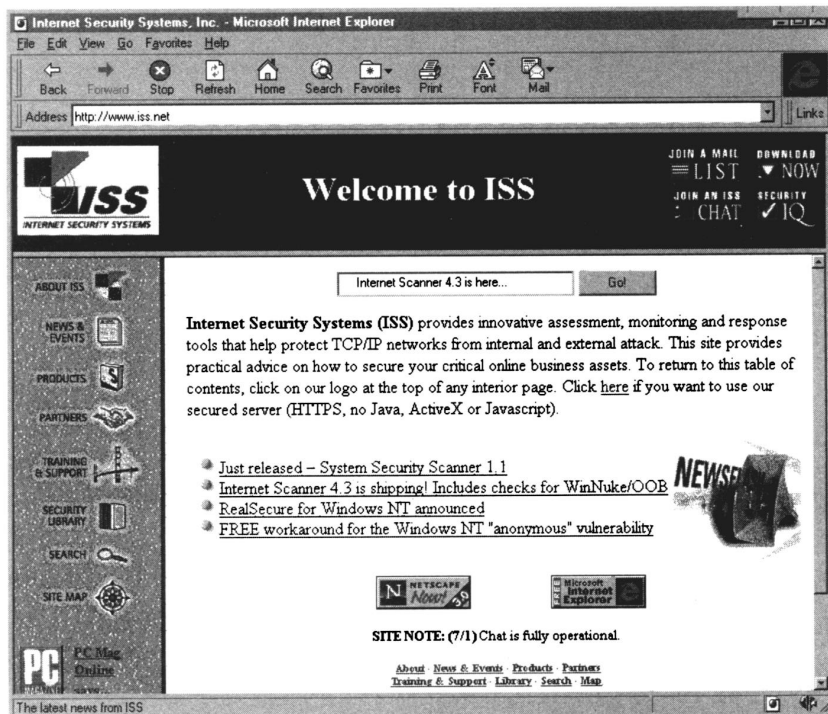


图1-7 ISS Web 站点免费提供审查产品的测试版



了ISS网站的一个界面，在这里可以下载此产品的测试版，这个程序只能审查安装本程序的机器，若要审查另外的机器，可以向ISS购买它的密钥。

一些大公司内部使用本产品用来审查本公司系统的配置以及用于验证他们使用的或要出售的防火墙。当前此产品用于各种风格的UNIX和Windows NT系统，它的售价是根据站点的大小来定的。

### 1.3 传输控制协议

传输控制协议（TCP）为IP提供了一种可靠的面向连接的传输层服务。由于它为非同类的计算机系统和网络之间提供了很高的互操作能力，TCP/IP得到了迅速发展，从而使它走出学术理论领域而进入市场。

该协议通过使用一个握手方案，提供了一种在主机之间建立、维护和终止逻辑连接的机制。另外，TCP提供了协议端口，从而可以通过每个包含目的端口和源端口号的消息，辨别运行于单一设备上的多道程序。TCP还通过单一的网络连接对字节流、数据流的界定、数据确认、数据再传输以及多路复用的多重连接提供了可靠的传输。

当然，本节不准备为你讲述TCP/IP网络互连的所有内容，有关内容可以参考RFC 1323（Van Jacobson TCP）和本书后所列出的参考书。但是，为了使你理解本协议安全上的脆弱性，让我们回顾一下通用的TCP/IP的概念和术语，这样既可以使我们了解它被广泛接受的原因，也可以使我们了解它在安全上的缺陷。

#### IP地址

所有基于IP的网络（因特网、LAN和WAN）都用一个统一的全球编址方案，每一个主机或服务器，必须拥有唯一的IP地址。这个地址方案的主要特点如下：

地址不能重复，以确保与因特网上的其他网络不发生冲突。

IP编址允许连接到因特网和其他网络上的主机或网络的数目不受限制。

IP地址允许网络使用不同的硬件编址方案，从而成为其他非同类网络的一部分。

规则 IP地址由点分十进制法隔开的四个单字节域组成。

例：1.3.0.2    192.89.5.2    142.44.72.8

IP地址必须遵守下列规则：

地址由32位二进制数组成，且这32位又分为四个域，每个域一个字节（8位）。

地址内容包括两部分：一个网络号和一个主机号或机器号。

在同一网络上的主机必须具有相同的网络号。

在同一网络上的两台主机不能有相同的主机号。

无论怎样连接，任意两个网络不能有相同的网络号。

要记住这些号码是很困难的，因此，在IP编址时，代表主机名地址的字符串与IP地址相关联。使用主机名地址的另一好处是当网络增长时，IP地址能够改变。主机全名由主机名和域名组成。

例如，Process Software的Web服务器的主机全名“CHEETAH.PROCESS.COM”是由主机名“CHEETAH”和域名“PROCESS.COM”构成，转换成IP地址是“198.115.138.3”，如

图1-8所示。

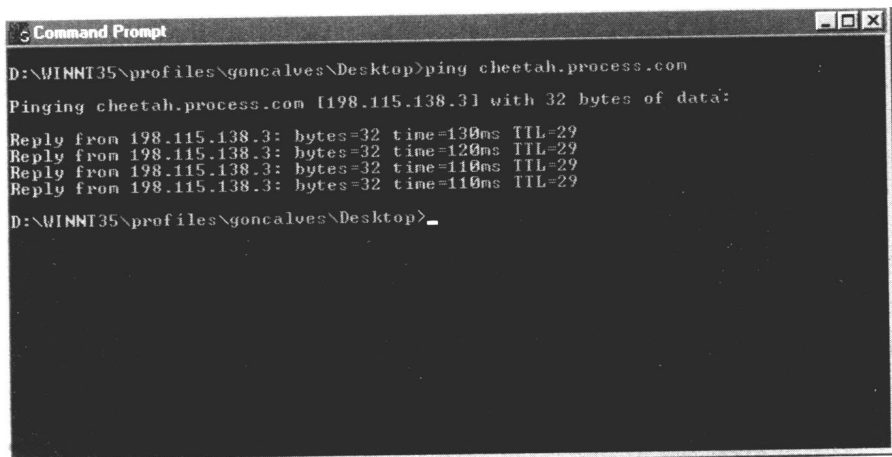


图1-8 通过PING 命令获取一个主机的IP地址

提示 也可用“PING”命令在因特网上查找一个主机或节点的IP地址，如图1-8所示。

不要把具体的用户名或计算机的位置指定为主机名，因为这些都是经常变化的；另外，还要使主机名简短易拼，命名时可随意使用数字和符号。

主机名通常由局域网管理员决定，因为他要加一个新的节点到网络，并且用它在域名服务（DNS）数据库中的地址进入该网络。

#### 分类和掩码

IP地址主要有三类。IP地址的分类是由因特网站点上与主机号相对应的网络号决定的。像因特网这样大的网络中，三类地址都可以使用。地址分类如下：

A类：第一字节用做网络号，其余三个字节用做主机号。第一字节的十进制取值范围为0~127，网络的最多数目可达128个，每个网络的主机数可达16 777 216个。

B类：前两个字节用做网络号，后两个字节用做主机号。第一字节取值128~191，这样，允许网络数目可达到16 384个，每个网络中主机数目可达65 536个。

C类：前三个字节用做网络号，最后一个字节用做主机号。第一个字节取值192~223，这样可允许网络数目达到2 097 152个，每个网络中的主机数目则不超过256个。

不同的地址种类决定了每类地址不同的网络掩码，主机和网关根据不同的网络掩码通过以下方法路由因特网信息包：

提取一个因特网地址的网络号。

把网络号与它们自己的路由选择信息相比较，以确定此地址是否与信息包要发往的地址相符。

网络掩码是一个32位因特网地址，这里，用于网络号的那些位都设成“1”，用于主机号的那些位都设成“0”。

表1-2列出了每类地址的值及相应的网络掩码。地址的第一个字节决定了地址种类。图1-9以十进制数形式给出了A、B、C三类因特网地址。

表1-2 因特网地址类

类 别	第一字节取值	网络掩码
A	1~127	255.0.0.0
B	128~191	255.255.0.0
C	192~233	255.255.255.0
D	224~239	无

注意 D类地址用于多播，数值240~255是为正处于实验中的当前还没应用的E类地址所保留的。

	8	16	24	32
A类	网络号	主机号	主机号	主机号
	1. ~ 127.	0. ~ 255.	0. ~ 255	0. ~ 255
B类	网络号	网络号	主机号	主机号
	128. ~ 191.	0. ~ 255.	0. ~ 255.	0. ~ 255.
C类	网络号	网络号	网络号	主机号
	192. ~ 223.	0. ~ 255.	0. ~ 255.	0. ~ 255.

图1-9 A、B、C三类因特网地址的十进制形式

## 1.4 通过CIDR扩展IP地址

1992年，因特网工程指导组（IESG）做出了将B类地址分配给主机的决定，但很快发现，用起来并没有什么效率可言。此时需要一个快速的解决方案，这促使了一种称之为无类域间路由选择（CIDR）的因特网标准跟踪协议的发展。

CIDR用地址前缀代替了地址类别，网络掩码必须随地址在一起。这种策略有效地利用了地址空间，且减慢了路由表的增长速度。例如，CIDR可以会聚一个称之为超级网络的IP地址，格式为：192.62.0.0/16，这里192.62.0.0代表地址前缀，16是前缀的位长。用这样一个地址代表从192.62.0.0到192.62.255.255。CIDR得到了开放式最短路径优先协议（OSPF）和边界网关协议（BGP-4）的支持。关于这两个协议在本章的后面部分将进一步讨论。

### 1.4.1 TCP/IP安全风险及其对策

可能你已经看出，安全性并不是TCP/IP的强项，至少当前的IP协议（IPv4）是这样。尽管做到百分之百安全的网络是不可能的，但是必须做到使网络上的信息易于访问。因而，可访问性和安全性的平衡确定了一种折衷的管理，它必须考虑安全策略，反过来，做决定时也

必须根据安全策略。在访问因特网时，这个安全策略支持公司的风险需求。

众多全球性的因特网安全漏洞来自最初的设计。IPv4本身并没有安全特性，并且其他TCP/IP协议中的安全特性也是很脆弱的。一个完善的网络互连安全性，需要详细计划并开发一个安全策略，从而阻止非授权访问或使其很难达到目的，并且能很容易地监测到它。

已经开发出很多设备用来增强TCP/IP网络的安全性。另外，内部策略一般是允许用户在受保护的网络上与在同一网络上的其他用户自由进行交流，但是与远程和外部网络（因特网）的访问则根据不同的访问安全性级别进行控制。

访问策略从简单的到复杂的都有，进入一个系统需要的可以是一个口令，或者也可用一个复杂的加密方案，如第3章中所述。

因特网安全机制中最常采用的是防火墙，在本节最后将对其作一简单论述，在第4章将进行详细讨论。防火墙的种类较多，包括用于各种环境下的多种产品。TCP/IP协议中的大多数安全特性是建立在认证机制基础上的，但是，最常用的认证格式是基于不安全的IP地址和域名的，而这却是很容易被攻破。

### 1. IP 欺骗

IP欺骗（IP Spoofing）是一种常用的攻击方法。它通过伪造“可信赖”主机和路由器的IP地址访问受保护的信息资源。用于电子欺骗攻击的一个途径就是利用IPv4的“源路由选择”这一特性，它允许数据报的制造者描述数据报传送到目的地址途中必经的某些甚至全部的路由器，而目的地址的路由器的应答数据报也必须经过同样的中间路由器。通过细心地构造源路由，攻击者能够模仿网上任何主机或路由器的组合，这样就可以击败基于地址或基于域名的认证方案。

因此，当有人绕过源路由选择，用欺骗性的IP地址建立信息包侵入时，你就被欺骗了。但“IP欺骗”到底是什么呢？

从根本上讲，电子欺骗是一种降低网络开销的技术，特别是在WAN中，通过电子欺骗，可以利用网桥和路由器去减少远程设备所需的带宽数。这种技术欺骗LAN上的设备，使它们把已断开的远程设备仍认为处于连接状态，因而，黑客也可用这种技术去攻击你的站点。

图1-10解释了欺骗技术是怎样进行的。黑客能够运用IP欺骗，通过用欺骗性的IP地址建立信息包，从而获得了通向根部的访问。这种基于IP地址认证的诡计应用程序，造成了非授权使用，且很可能进行对目标系统的根部访问。当信息包的源地址在本地的域内时，若防火墙没有配置到信息包的过滤器中，欺骗甚至可以成功地通过防火墙。

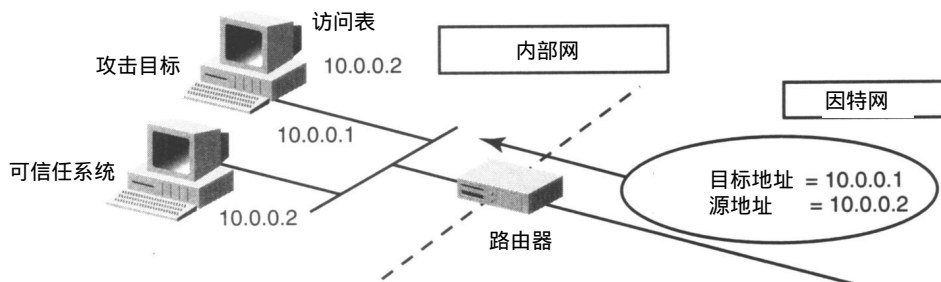


图1-10 IP 欺骗的一个例子

当路由器连到外部网上且支持内部接口时，还要当心这些路由器。在内部网络上，如果路由器有支持子网的两个接口时，必须警惕，因为这正是IP欺骗所要攻击的薄弱环节。



提示 关于IP 欺骗的其他信息，请查阅Robert Morris的论文“ A Weakness in the 4.2BSD UNIX TCP/IP Software”，URL如下：[ftp://research.att.com:/dist/internet\\_security/117.ps.zo](ftp://research.att.com:/dist/internet_security/117.ps.zo)。

当为了入侵一个受保护的网路而欺骗 IP 时，黑客通过等待一个合法用户进行连接和输入指令到远程站点，就能够绕过一次性口令和认证方案。一旦用户完成认证，黑客就控制了连接，这就会危及到站点的安全性。在 SunOS 4.1-x 系统中经常发生这种事，当然其他系统中也存在这种可能。

通过监视信息包可以监测 IP 欺骗。可以使用网络日志或类似的网络监视软件，在外部接口上查看信息包，若发现在本地的域内它既有源地址又有目的地址，这就意味着有人正在侵犯你的系统。

提示 网络日志可以通过匿名FTP从下述URL下载：

<ftp://net.tamu.edu:/pub/security/TAMU/netlog-1.2.tar.gz>。

另一种监测 IP 欺骗的方法是比较内部网上系统之间的日志记录的过程，如果有 IP 欺骗，你能够看到目标机器远程访问记录上没有任何关于发起这次远程访问的响应记录。

前面提到过，防止站点遭到 IP 欺骗的最好方法就是安装一个过滤路由器，它对输入到外部接口上的数据进行严格控制。如果一个信息包在内部网上有源地址，它就禁止此信息包通过。计算机应急行动小组（CERT）还推荐，应该过滤从内部网络发出的具有源地址的信息包，以防止源 IP 欺骗的攻击从你的站点发起（如图 1-11 所示）。在随后的几章里，将对此作进一步讨论。

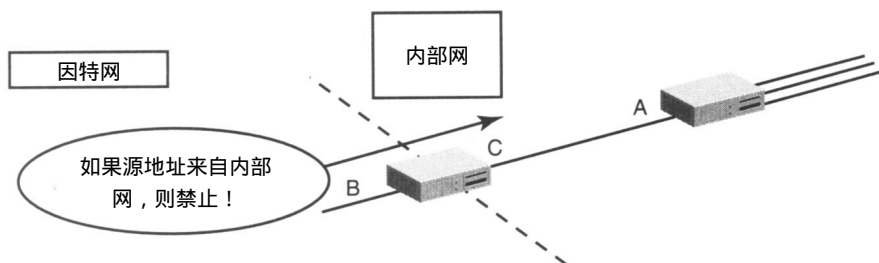


图1-11 CERT关于防止IP 欺骗的建议

## 2. 失密风险

IP层的确提供了一些保密性支持，最常用的一种是来自 Motorola的网络加密系统（NES），它可对数据报进行加密，但是存在的一个问题是 NES加密彻底封闭了受保护的网路。

警告 如果认为你的系统遭受过欺骗，应该同CERT协调中心或与事件反馈及安全小组论坛（FIRST）中你的代表联系。

CERT人员强烈建议，电子邮件需要加密，CERT协调中心可提供共享的DES密钥、PGP（公共密钥，可通过匿名FTP在[info.cert.org](http://info.cert.org)得到）或PEM（详细信息请与CERT人员联系）。

因特网电子邮件：[cert@cert.org](mailto:cert@cert.org)

尽管NES一定程度上可用于军事设施，为不同级别的数据提供 IP网络安全；但是，这个

策略对于协作应用而言几乎是不能接受的。另外，NES有一个很复杂的配置方案，带宽也窄，且不支持IP多播。

### 3. 丢失完整性风险

TCP/IP协议中还有一些方案，其作用是通过使用校验和进行错误监测来保护传输层中数据的完整性。但是，今天复杂的因特网环境与80年代初大不相同，仅有简单的校验和是不够的，现在，完整性的保证可以通过电子签名获得，事实上，这并不是IPv4的一部分。

尽管如此，IPv4的安全特性中仍有完整性机制的原形（已被合并到IPv6中），它是由IETF IPSEC工作组开发的。

### 4. tcpdump——一个基于文本的对策

有时，对于网络上的问题，需要有敏感的洞察力去发现攻击系统的信息包。程序 tcpdump 产生了一个令人费解的输出，如图 1-12所示，通常需要一本好的网络手册来解码，对于那些敢于挑战这种输出的人，这可以帮助他解决网络问题，特别是在源地址和目的地址都已知的情况下；对于那些仅仅是浏览信息的人，则没什么太大的用途。

```
16:38:20.713383 luxor.1377 > hrisc02.6393: S 3884707742:3884707742(0) win 512 <ms
s 1460>
16:38:20.713383 hrisc02.6875 > luxor.1348: R 0:0(0) ack 1034577935 win 0
16:38:20.713383 hrisc02.6876 > luxor.1350: R 0:0(0) ack 3624648839 win 0
16:38:20.713383 hrisc02.6877 > luxor.1351: R 0:0(0) ack 533598542 win 0
16:38:20.713383 luxor.1378 > hrisc02.6894: S 2857164548:2857164548(0) win 512 <ms
s 1460>
16:38:20.713383 hrisc02.6878 > luxor.1352: R 0:0(0) ack 3799663586 win 0
16:38:20.713383 luxor.1379 > hrisc02.6896: S 4196575263:4196575263(0) win 512 <ms
s 1460>
16:38:20.713383 luxor.1380 > hrisc02.6896: S 1276478647:1276478647(0) win 512 <ms
s 1460>
16:38:20.713383 luxor.1381 > hrisc02.6897: S 3055046481:3055046481(0) win 512 <ms
s 1460>
16:38:20.723383 hrisc02.6879 > luxor.1353: R 0:0(0) ack 2858009840 win 0
16:38:20.723383 luxor.1382 > hrisc02.6898: S 3880767338:3880767338(0) win 512 <ms
s 1460>
16:38:20.753383 hrisc02.6880 > luxor.1354: R 0:0(0) ack 1354475889 win 0
16:38:20.753383 luxor.1383 > hrisc02.6899: S 3233160253:3233160253(0) win 512 <ms
s 1460>
16:38:20.763383 b.domain > gateway.domain: 5909- 0/4/4 (214)
16:38:20.763383 hrisc02.6884 > luxor.1358: R 0:0(0)
64 packets received by filter
0 packets dropped by kernel
[root@luxor /root]#
```

图1-12 运行中的tcpdump:尽管输出令人费解，但却很有用

从许多UNIX安全档案中可以查到 tcpdump，它要求分发出去在各种系统中进行编译，但对于特定的机器，如Suns，则必需进行特别的修改以捕获装有 tcpdump的机器上发来的信息。

### 5. strobe:用于UNIX的对策

strobe是一个有用的工具，如图 1-13所示，可以从许多 UNIX档案获得它，仅用来检查系统上的TCP服务，有时也完全可用于检查系统的配置。它只是作为一个用于 UNIX的文本工具且没有用于UDP，这是DNS的主要部分和其他服务的一小部分。它是一个比较受欢迎且好用的系统脚本管理工具，它可以把从系统中所获得的信息逐行打印。

strobe很容易运行且可以在众多 UNIX上编译，从许多流行的 UNIX安全档案中都可以找到它。

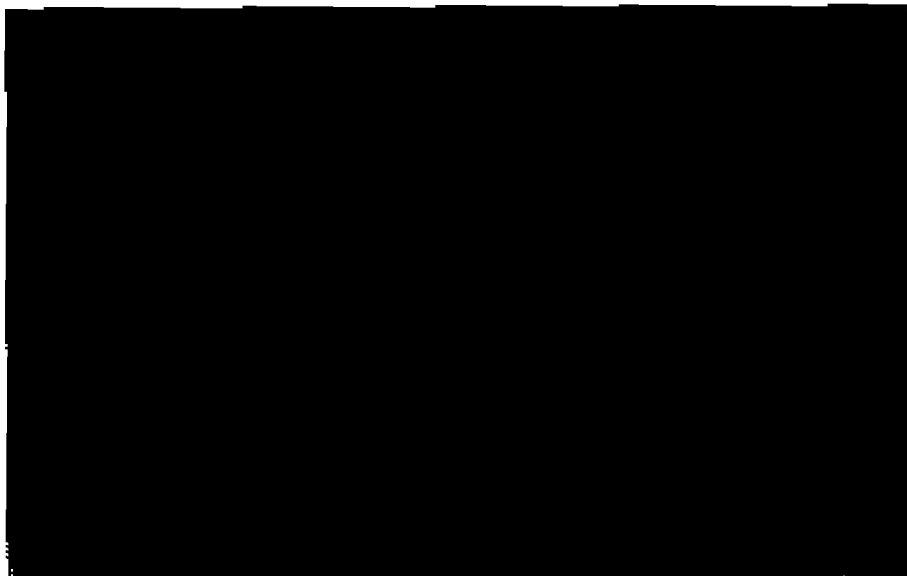


图1-13 检查系统TCP服务的工具：strobe

#### 1.4.2 IPSEC——IETF提出的IP安全对策

IP协议安全体系（IPSEC）是IETF安全工作组努力的结果，他们意识到IP需要比现在更强安全性。1995年，IPSEC作为IPv4的一个选项和IPv6的扩展头被提出（IPv6将在本章后面的部分进行介绍）。

在数据报这一级，IPSEC支持认证、完整性和保密性。通过向数据报加入一个认证头选项，从而提供了认证和完整性的功能，反过来，这又使得公钥加密和公开算法得到了充分应用。IP有效负荷安全封装（ESP）也提供了保密性，ESP对数据报的有效负荷和报头进行加密，并把另一明文包头接在这个加密的数据报上，这也可用于在因特网内设置专用虚拟网络。

#### 1.4.3 IPSO——（美）国防部IP安全对策

IP安全选项（IPSO）是（美）国防部（DOD）1991年作为IPv4套件的一组安全特性提出的。为使它与因特网协议共同使用，IPSO由如下两个协议组成：

国防部基本安全选项（BSO）——BSO协议定义了访问控制敏感标志的内容，把它附在进入系统和离开系统的IP数据报上。

国防部扩展安全选项（ESO）——ESO协议描述了关于增加安全分类层次和保护特权数目的需求及其机制。

此方案是由根据敏感等级做了标志的数据报组成，多数情况下，政府机构也用同样的方法标记、控制文档的分类（绝密、机密、秘密以及非保密），但是没有使用任何加密方案。也许因为这一点，IPSO没有成为因特网的一个标准，也没有得到进一步应用。

### 1.5 路由信息协议

路由信息协议（RIP）是一个距离向量、内部网关协议（IGP），路由器用它来交换路由选

择信息，如图 1-14 所示。通过 RIP 向终端站和路由器提供在不同网络进行动态选择最佳路径的信息。

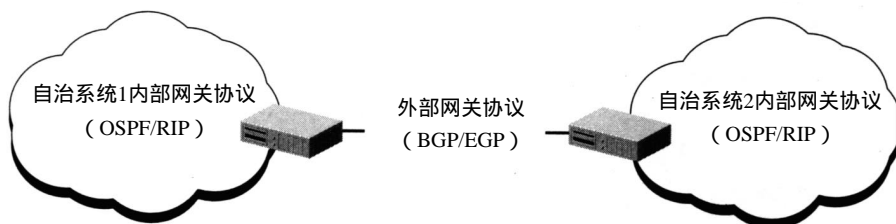


图1-14 RIP——确定在不同网络间定义的最佳路由

在确定最佳路由时，RIP把源网络与目的网络之间总的跳数作为开销，跳数最少的那条网络路径就是总开销最少的路径。

一个信息包通过一个 IP 网络时，RIP 所允许的最大跳数是 15。通过指定最大跳数，RIP 可避免路由选择回路。数据报根据每个路由器路由表中的某种算法在互联网中进行路由。一个路由器的路由表内容包括：在自治系统中所有已知的网络信息、到达目的网络的总跳数以及沿着目的网络方向下一个跳的路由器地址。

在一个使用 RIP 的网络中，每一个路由器每隔 30 秒就要向其相邻的路由器广播它的整个 RIP 表。当一个路由器接收到相邻路由器的 RIP 表时，它就用这个信息去更新自己的表，然后把更新过的表再传送给与它相邻的路由器。

这个过程一直继续下去，直到所有路由器在网络拓扑结构中取得一致。一旦达到这种情形，这个网络就获得了会聚，如图 1-15 所示。

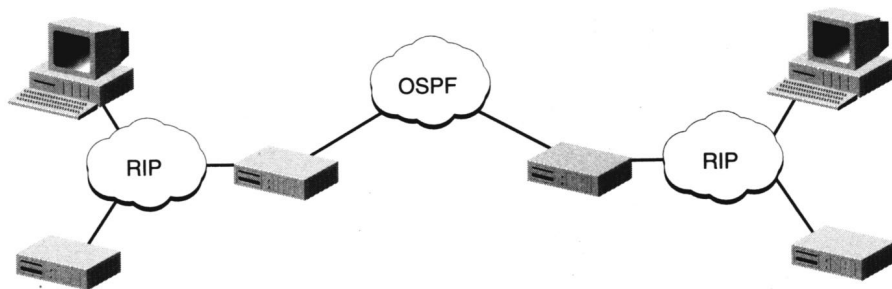


图1-15 用RIP完成网络会聚

## 1.6 MBONE——多播骨干网

当在因特网上进行音频和视频传输时，多播骨干网（MBONE）起着很重要的作用。它起源于 IETF 最初的两个“音频广播”试验，即把 IETF 会议站点的音频和视频信号向全世界目的站点进行现场多播。整个想法就是要建立一个半永久性的 IP 多播试验台，用以 IETF 的信息传输以及为继续进行的会议之间的实验提供帮助，顺便说一下，这是一个自愿协作者所做的尝试。

作为一个虚拟网络，MBONE 处在因特网物理层顶部，以支持 IP 多播信息包的路由选择。



从拓扑结构看，网络事实上是由点到点的“隧道”连接起来的各个“岛”组成的。这些隧道一直通向支持IP多播的操作系统和运行着多播路由选择守护进程的操作系统。

也许你想将你的Web站点注册为其中一员。它允许你的Web用户通过音频/视频信息包参加IETF的音频广播和其他一些试验，也可帮助你以及你的用户用相对较低的花费获得通过IP多播的经验。

加入MBONE并不复杂，你需要提供一个以上IP多播路由器连接到与你的用户以及与其他参加者相连的隧道上。由于大多数路由器不支持多播，所以多播路由器通常与主路由器分开；另外，你还需要有运行着多播程序的工作站。

你应专门分配一台工作站完成多播的路由选择工作，这可以阻止一些其他的行为干扰多播的传输。你也不用担心核心补丁的安装或新代码的发行会影响其他应用系统的功能。

你可以对MBONE进行配置，使有多播功能的机器与隧道连接，经外部DMZ和物理的主干网络通向其他地域的网络，也可经隧道连接到内部DMZ低层的能多播的机器，在那里分离复制的信息包。

注意 下面列出的是加入到MBONE的一部分因特网服务提供商（ISP）：

*AlterNet*——ops@uunet.uu.net  
*CERFnet*——mbone@cerf.net  
*CICNet*——mbone@cic.net  
*CONCERT*——mbone@concert.net  
*Cornell*——swb@nr-tech.cit.cornell.edu  
*JANET*——mbone-admin@noc.ulcc.ac.uk  
*JvNCnet*——multicast@jvnc.net  
*Los Nettos*——prue@isi.edu  
*NCAR*——mbone@ncar.ucar.edu  
*NCSAnet*——mbone@cic.net  
*NEARnet*——nearnnet-eng@nic.near.net  
*OARnet*——oarnet-mbone@oar.net  
*PSCnet*——pscnet-admin@psc.edu  
*PSInet*——mbone@nisc.psi.edu  
*SESQUINET*——sesqui-tech@sesqui.net  
*SDSCnet*——mbone@sdsc.edu  
*SURAnet*——multicast@sura.net  
*UNINETT*——mbone-no@uninett.no

MBONE的一个局限性是在音频处理能力上仍存在问题，特别是用Windows NT系统时，因为要听到它必须下载全部的音频程序。不过，现在已有解决这个问题的系统了，音频下载时就可以播放。下面列出了一些在Windows 98、Windows NT和企业版上测试过的系统：

*RealAudio*——由Progressive Networks开发，可由<http://www.realaudio.com>下载一个测试版，为在下载时，播放音频，这个播放器与一专用的RealAudio服务器通信，这减小了下载过程中的延迟，特别当用速度很慢的调制解调器时。它还支持各种质量等级的音频和一些非音频特性。例如与音频同步显示的HTML页面。RealAudio播放器可用于

Microsoft Windows、Macintosh和一些UNIX平台。

Winplay——Winplay使用MP3压缩技术，提供了高质量的音频。据本人所知，这个特点是其他同类产品所没有的。可由 <ftp://ftp.uoknor.edu> 下载，或从德国 Institute for Integrated Circuits的主页<http://www.iis.fhg.de/departs/amm/layer3/winplay> 下载。

VocalTec ——这是一个有名的播放器，它为 Web提供了音频流技术。但它只用于 Microsoft Windows，其查询站点为：<http://www.vocaltec.com>。

多播信息包设计时使用了专门的 IP地址范围：224.0.0.0到239.255.255.255。前面提到过，处于这个范围的是因特网的 D类地址。因特网编号管理局（IANA）将D类子网地址224.2.\*.\*给了MBONE（广泛应用于远程会议中）。在此地址范围内，主机在 MBONE上用一个IP地址有选择地进行相互间的通信，从而建立会话。这样，多播 IP地址就用来标明由通信链接而结合起来的一组主机，而不是由实际的 LAN连接结合起来的一组主机。每一主机临时采用相同的IP地址，当会话终止后，IP地址被归还到一个“池”中，以备包含不同主机的其他会话再用。

在MBONE彻底用于因特网之前，仍然还有一些问题要解决。因为，在不同子网的多类主机之间的多播必须完全在因特网上传输，而且并不是所有的路由器都能多播。多播 IP信息包必须经隧道传送（这使 MBONE成为一个虚拟网络），看起来就像单播信息包传送到一般路由器那样。因而，这些多播 IP数据报要被源端-终端的多播路由器封装到一个单播的 IP头内，此IP头具有目的地址区和源地址区，且要设置到隧道终点路由器的 IP地址内；还有个别的将协议区设置到IP中，这说明信息包中的下一个协议也是 IP。然后，目的地的多播路由器剥去头部去读“内部”多播会话的 IP地址，并且把信息包转发到它自己网络的主机上，或者再封装数据报转发到其他能提供服务的多播路由器，或者转发到会话组成员那里。

注意 关于MBONE更多的信息，请查阅Vinary Kumar的《Interactive Multimedia on the Internet》，由New Riders于1996年出版。

## 1.7 因特网控制报文协议

在RFC 792中定义的因特网控制报文协议（ICMP）是IP的一部分，其作用是处理错误报文和系统级报文，并将报文发送到纠错网关或主机。它用的是 IP的基本支持，看上去好像是一个更高级的协议，但是，ICMP确实是IP不可分割的一部分，且 IP的每一部分都必须执行它。

控制报文的传送是在这么几种情况下，例如：当数据报不能到达它的目的地时，或当网关转发数据报失败时（一般是由于没有足够的缓冲容量）。

## 1.8 因特网组管理协议

因特网组管理协议（IGMP）定义于RFC 1112，它的形成是为了使多路访问网络上的主机能够命令具有它们群组成员信息的本地路由器，它是通过主机多播 IGMP的主机成员报告来实现的。这些多播路由器侦听到这些信息后能够与其他多播路由器交换群组成员信息，这里允许形成分发树去传递多播数据报。

我们所知的IGMP版本2，几乎没有什么扩充，在 IP多播的后期发行中，为了包括简明的

用户快速修整离开报文和多播跟踪路由报文，IGMP版本2才被开发出来并且发行。如图 1-16 给出了IGMP的头部信息。

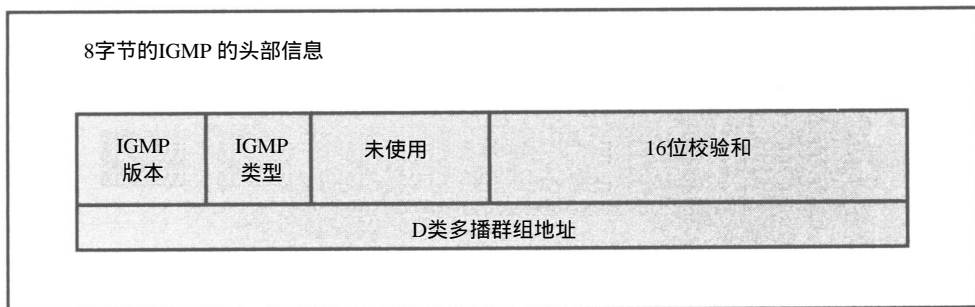


图1-16 8字节IGMP的头部信息

典型的IGMP语句如下所示：

```
igmp yes | no | on | off [ {  
    queryinterval sec;  
    timeoutinterval sec;  
    interface interface_list enable | disable;  
    traceoptions trace_options;  
}];
```

第一行的igmp语句允许或禁止IGMP协议，若igmp语句没有指定，则缺省为igmp off；如果是允许，则IGMP缺省情况下允许单播和多播的所有接口都有效，这些接口由IFF\_BROADCAST和IFF\_MULTICAST接口标志标识。在一个IP多播路由选择协议有效之前必须使IGMP有效。

注意 关于IGMP的功能和选项的完整信息，请查阅RFC1112或Intergate的站点：

<http://intergate.ipinc.com/support/gated/new/node29.html>。

## 1.9 开放式最短路径优先

开放式最短路径优先（OSPF）是一个基于第二代标准的IGP（内部网关协议），用于一个自治系统内部各路由器间进行路由信息的交换。“自治系统”指的是那些由一群路由器组成，在单一权力机构管理控制下的系统。OSPF最大限度地减少了穿过巨大的IP互联网时的网络会聚次数。

不要把OSPF与RIP混淆，因为它不是一个距离向量路由选择协议。进一步讲，OSPF是一个链路状态路由选择协议，它允许路由器之间相互交换关于其他网络的可达能力及到达其他网关的开销和距离等信息。在RFC 1247中OSPF是被作为IGP的一个标准而定义的。

提示 内部网关协议（IGP）是一个因特网协议，它是用来在一个自治系统内向路由器分发路由信息，为更好地理解这个IP协议的特性，它的名字可用“网关”代替，这更是一个历史上形成的定义，而“路由器”则是一个更确切的术语。

在一个自治系统中，仅当拓扑结构发生变化时，所有支持OSPF的路由器通过发布路由更

新信息去使用链路状态表进行路由信息的交换。在这种情况下，觉察到这种变化的路由器应立即把拓扑结构的变化而不是全部的路由表通知相邻的路由器，这些相邻的路由器再用相同的方法把更新信息传给与它相邻的路由器，如此一直进行下去。这减少了因特网上的流量。它的主要特点是，由于拓扑结构变化是立即被传播的，这就使得比用于 RIP 上的基于时间片的机制更快地获得整个网络的会聚。

因此，OSPF 越来越多地被曾经依靠 RIP 路由选择服务的自治系统所采用，特别是因为 OSPF 路由器同时支持 RIP 的路由器-终端通信和路由器-路由器通信。它确保了因特网内的通信，并为 OSPF 进入其他网络提供了畅通的渠道。

## 1.10 边界网关协议版本4 (BGP-4)

边界网关协议版本 4 (BGP-4) 是一个能使处于不同自治系统中的路由器进行路由信息交换的外部网关协议。BGP-4 还提供了一系列机制以方便 CIDR，这是因为它提供了广播一个任意长 IP 前缀的能力且由此消除了 BGP 中网络“类”的概念。

BGP 使用 TCP 以确保交互式自治系统的信息的传递。仅当拓扑结构发生变化时产生更新信息，且更新信息只包含变化了的那部分信息，这减少了网上的通信量，也降低了为了使路由器间的路由表保持一致所需的开销。

## 1.11 地址转换协议

地址转换协议 (ARP) 是一种从主机因特网地址获得其以太网地址的方法。发方广播一个含有另一个主机因特网地址的 ARP 数据包，并等待它送回其以太网地址。每个主机都持有一个地址转换高速缓存，以减少延迟和负载。ARP 允许因特网地址独立于以太网地址，但只有当所有主机都支持它时才能工作。

如 RFC 826 中定义，一个路由器和主机必须连到同一网段去实现 ARP，且广播不能被另一路由器转发到不同的网段。

### 1.11.1 反向地址转换协议

如 RFC 903 中定义，反向地址转换协议 (RARP) 提供了与前面所述的 ARP 相反的功能。RARP 映像一硬件地址，也称为 MAC 地址，到一 IP 地址。RARP 主要用于无盘节点，当其首次初始化时，用来查找它们的因特网地址，其功能与 BOOTP 很相似。

### 1.11.2 通过路由器传递 IP 数据报的安全风险

处理网络安全时，常常忽略了路由器，而它们是因特网连接所必不可少的。路由器提供了从网络路径到外界的全部数据，这也使它们成为很好的攻击目标，因为许多网站都有一路由器与外界相连，所以可以通过毁坏连接去攻击站点。

应保持使用最新版的路由器软件。新发行的版本能对付当前大量的拒绝服务攻击。这些攻击常常烦琐地执行，且只要有几个信息包通过连接就能够引发。有时，路由器的升级意味着在内存和硬件升级上的更多的花销，但是作为设备至关重要的一部分，不应忽视。

与更新软件不同，使远程管理无效是一种常用的对付通过拒绝服务和远程攻击获得路由控制的方法。通过一个开放的远程管理端口，攻击者可以进入路由器。一些路由器在遭受到



对它们管理口令的强烈攻击时作出了牺牲！用一快速的脚本对所有的口令进行尝试，为避免被发现，每次尝试只能进入路由器一次。人工管理太多的路由器也是个问题，或许采用网络交换技术是一个明智的选择，用当今的交换机代替以前骨干网上的路由器将有助于问题的解决。

### 1.12 简单网络管理协议

如RFC 1157，STD 15中定义：简单网络管理协议（SNMP）用于管理IP网络上的节点。在IP安全因素中，某种程度上忽视了网络设备自身的保护。SNMPv2使得对网络设备的管理方法得到明显加强。但由于略有争议，SNMP的安全特性还有待于进一步完善。

注意 SNMPv2最初提出的一些方面的安全性被做成了可选择的，有的在1996年3月根据因特网标准从SNMPv2的描述中清除掉了。现在新的SNMPv2又有一个实验性安全协议被提出。

尽管如此，SNMP仍是一个用于监视和控制IP路由器和连接网络的标准协议。这个面向事务的协议描述了SNMP管理者与代理之间结构化管理信息的传递。驻留于工作站上的SNMP管理者发出查询去收集路由器的状态、配置和执行信息。

### 1.13 监视ISP连接

当购买Internet Service Provider时，大多数订购者曲解了它所提供的安全方法。它们的安全等级很快可以决定顾客的安全等级，如果上行的数据遭到威胁，那么所有流向因特网的数据就可以被警觉的攻击者发觉，当看到有信息从客户那里发进发出，确实感到惊讶。私人邮件被读，以Web形式提交的信息被读，下载文件被拦截，任何发向因特网的数据都能被偷窃。

还有一种更恶劣的趋势，即，不仅仅是对信息进行偷窃，而且还要劫持连接。一个用户登录到远程帐户，其文件突然开始改变。劫持水平越来越高，一个会话可以被清晰地劫持，而用户则仅认为是网络速度有些慢。这类劫持需要攻击者处于数据流中的某个位置，而ISP恰是一个很好的栖息处。

### 1.14 下一代IP协议IPv6

在1973年，TCP/IP被引入ARPANET，当时连接了250个站点，750台计算机，而今天的因特网取得了巨大的发展，全世界连接到它的用户已超过6000万，估计有几十万站点和数千万台计算机。这种增长现象就把前所未有的压力放在了因特网的底层结构和内在的技术上。

由于因特网的这种典型增长，潜在的网络技术的不足也越来越明显。当前的IP协议第4版最后一次修订是在1981年（RFC 791），从那时起，由于协议的老化，因特网工程部（IETF）一直在为出现的缺陷寻找解决方案，这一系列方案被命名为IPv6，并且将成为下一代通信应用系统的主干部分。

到21世纪初，因特网将以一种不同于今天的难以预测的方式继续使用，并且希望它的使用扩展到多媒体笔记本电脑，蜂窝式调制解调器及家用电气，诸如电视、烤箱、咖啡机（记住，IBM最新台式PC模型已具备了一些远程控制家用电器的功能）。

实际上，我们在家、在工作中、在玩的时候用到的设备都可连到因特网上，这种可能性

是无穷尽的，但实现的道路上也是比较崎岖的，特别是就安全性和保密性方面而言。

对于在这些新的应用方面的功能，TCP/IP必须对其能力进行开发和扩展，首先最重要的一步就是开发下一代“IP协议”，IPv6。

IPv6的开始出现并不意味着IPv4已无能为力，但是，有一些迫不得已的原因使你会尽快采用IPv6。当然，这个过程存在着挑战，实际上，因特网技术的任何发展都需要与IPv4无缝兼容，特别是对于易管理性的迁移，这样，可以允许我们在不必使整个因特网同时升级的情况下，方便地使用IPv6的功能。

#### 1.14.1 地址扩展

IPv6的主要原因解决就要用完的IPv4网络地址这一问题。为了给每辆汽车、机器工具、烤箱、电视、交通灯、EKG监视器以及每部电话都分配一网络地址，我们需要数亿新的网络地址。IPv6可以彻底解决这个问题，它用128位的地址结构提供了足够的地址。

从32位增长到128位的地址表足以满足快速增长的因特网社会对地址增长的需求。IPv6所支持的地址位数是IPv4的4倍（ $128:32$ ）。它的地址空间比IPv4大的倍数是惊人的。这个地址空间算出来是：

340 282 366 920 938 463 463 374 607 431 768 211 456

这是一个极大的地址空间，理论上讲，在地球表面的每平方米大约有 665 570 793 348 866 943 898 599个地址（假设地球表面积为 511 263 971 197 990平方米）。

实际中，地址的分配和路由选择需要建立一种体系结构，这可以减少地址空间的使用。假设其效率范围与其他寻址结构相同的话，IPv6可容纳从  $8 \times 10^{17} \sim 2 \times 10^{33}$  个节点。

#### 1.14.2 网络设备的自动配置

人工控制和管理大量连接到公用或私用网络上的主机不是件容易的事。多数公司的网络管理员（如Internet Provider），对此头疼之极。IPv6的自动配置能力可以大大减轻这种负担，其做法是，当一个新设备连到网络上时，就对其进行确认并且自动对其配置，以使其可以通信，对于移动或无线用户，IPv6显示了它更流畅的功能和强大的能力。

#### 1.14.3 安全性

高级IT界专业人员和CEO共同面对的一个主要问题是把通过内部网连接起来的机构连到因特网上时的安全问题。尽管如此，对于连接到因特网的每一个人来说，秘密入侵也是一个忧虑，当IP连接开始侵入咖啡机时就是一个例子。幸运的是，IPv6将安全特性植入整个主机内，包括系统间的认证和私有数据的加密。这些能力对于使用因特网进行安全计算是至关重要的。

#### 1.14.4 实时性能

把TCP/IP用于实时或接近实时的应用系统的一个障碍是响应时间和服务质量。通过使用IPv6的信息包优先权特性，现在可以把TCP/IP用于这些应用系统。

#### 1.14.5 多播

当前网络技术的策划是基于一对一或一对全部通信这个前提的，这意味着那些分发信息到大量用户的应用系统必须建立一个从服务器到每个客户的分开的网络连接。IPv6提供了建立应用系统的能力，从而通过“多播”选项更有效地使用服务器和网络资源。这允许一个应用系统在网络上进行数据“广播”，数据只能被那些有正当授权的客户接收。多播为潜在的应用系统开辟了一个全新的领域，从新闻和金融数据的分发，到视频和音频的分发等等。

IPv6有许多特性和成果，根据我们的目的，将集中讨论IPv6的约定，特别是安全性方面的约定。

#### 1.14.6 IPv6安全性

用户想知道他们的事务处理和访问他们自己的站点是安全的。用户还想增加访问协议层的安全性。正如本书中所讨论的，直到有了IPv6，仅通过添加应用程序和服务就可获得安全性。

IPv6提供的安全特性可用于两个领域：

认证——它要求发送方登录到接收方，如果发送方没有被确认，则访问不能进行；如果允许访问，这就保证了数据是由被承认的发送方所发的，且其内容在传送中没有改变。

保密——保密是采用加密的方式，且保护数据不被用户无意识地破坏。信息包在离开一个站点时被加密，进入一个站点时被认证。

保密和认证都可应用于“安全协商”，对于一个发送方和一个接收方之间的单向交换，需要一个协商；对于一个双向交换，则需要两次协商。当兼有认证和保密时，哪个用在先都可以，如果加密在先，则整个信息包被认证，包括加密部分和未加密部分；如果认证在先，则认证用于整个信息包。

IPv6正在由IETF和其参与者进行反复测试，随着其核心规范的最后定案，IPv6将在一年内完成，因特网服务提供将在今后3~4年内提供IPv6链接。

### 1.15 网络时间协议

网络时间协议（NTP）是一个建立在TCP/IP之上的协议，通过在因特网上参考无线电装置、原子时钟以及其他时钟，确保对本地时间的准确记录。此协议能在很长一段时间内使分布式时钟同步在毫秒级。它在STD 12，RFC 1119中定义。

### 1.16 动态主机配置协议

动态主机配置协议（DHCP）实际上是1994年末由Microsoft在3.5版本的NT服务器上所介绍的一个协议。

这个协议提供了一种动态分配IP地址到IBM PC的一种方法，前提是这些PC上运行的是Microsoft Windows并且处于局域网中。

系统管理员分配一个IP地址范围给DHCP，且在LAN上的每一客户PC都配有各自的TCP/IP软件，这些软件的作用是从DHCP服务器请求一个IP地址请求和授权过程使用可控时间段的租用概念。更多的信息可以从Microsoft的NT Server文档中找到。

## 1.17 Windows套接字 (Winsock) 标准

Winsock是Microsoft Windows网络软件的一个规范，描述了应用系统如何获得网络服务，特别是TCP/IP服务。Winsock是想提供一个单一的API用于应用程序开发者要开发的程序和提供商确认的多种网络软件。对于任一 Microsoft Windows的版本，它定义了一个二进制接口 (ABI)，这样，一个写入 Windows套接字标准的API就能与来自任一网络软件厂商的有效协议一同工作了。

Microsoft Windows 98、Windows NT和Windows 2000都支持Windows套接字标准。这个标准还支持TCP/IP以外的其他协议。

## 1.18 域名系统

在RFC 1034，RFC 1035中定义的域名系统提供了一种分布式、复杂的数据查询服务，主要用于因特网上将主机名（或站名），如：process.com，解释成它的IP地址，如：192.42.95.1。DNS经过配置后，可使用名字服务器序列，根据域的名字进行查询，直到找到一个匹配为止。

DNS通常是作为Sun Microsystem网络信息系统（NIS）所提供的用于主机名解释的一个替代品被安装的。但是，NIS依靠一个单一的服务器，而DNS是一个分布式数据库。使用命令nslookup可以对其进行相互之间的查询。

域名系统涉及到了主机命名方法以及服务器与客户对通过因特网信息的管理两方面内容。

### DNS信息限定

InterNIC持有一个站点的主要信息和DNS的次要信息。参照InterNIC去学习是哪一个系统把地址解释成机器名，这对于国外用户来说是一种典型的方法。一定要注意由外部主要和次要的DNS提供的地址，如果列出国外用户能访问的DNS记录中重要的资源，就能给攻击者以暗示，使他决定应该对哪个系统进行攻击。给一个系统明确地命名为“main-server”或“modem-dialout”是不明智的。

因此，我建议你为主机内部地址建立第三个DNS服务器，仅允许系统从本地站点访问这些信息，这可以防止内部名字泄漏到因特网。可以给主机取两个不同的名字，且都可被因特网访问到。只要系统外在的名字没有明显的信息表明主机是什么（如：“ftp”或“www”），就可在内部将一个重要的系统命名为“main-server”。如果机器不多，则可以只让少数几个系统列出在外面这是很容易做到的。

## 1.19 防火墙概念

到现在为止只对网络协议及其标准作了概述，但你应该能够感觉到在因特网上所发送的每一段数据都可以被偷窃和修改。因特网的组织方式，是要每个站点都要为自身安全负责。如果黑客占领了一个用于通信的关键地方的站点，那么用户发出的所有通过该站点的数据就完全由黑客随意处置了。黑客可以截获未加密的信用卡、Telnet会话、FTP会话、发给祖母的信件以及其他任何通过这条线路的信息。

就像不要相信你的上行信息那样，也一定要仔细对待发往远程站点的信息。由谁控制目的地系统，这是一个一直在讨论的问题。



设计防火墙的目的就是不要让那些来自不受保护的网路如因特网上的多余的未授权的信息进入专用网络，如LAN或WAN，而仍能允许本地网络上的你以及其他用户访问因特网服务。图1-17显示了防火墙的基本目的。

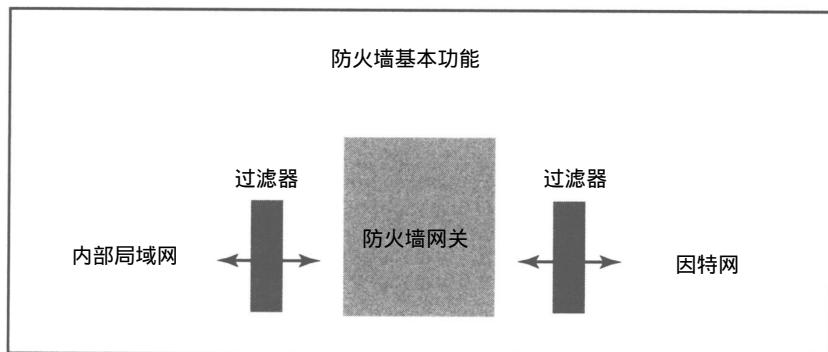


图1-17 防火墙的基本功能

如图1-18所示，大多数防火墙就是一些路由器，它们根据数据报的源地址、目的地址、更高级的协议，或根据由专用网络安全管理员制定的标准，或安全策略，过滤进入网络的数据报。

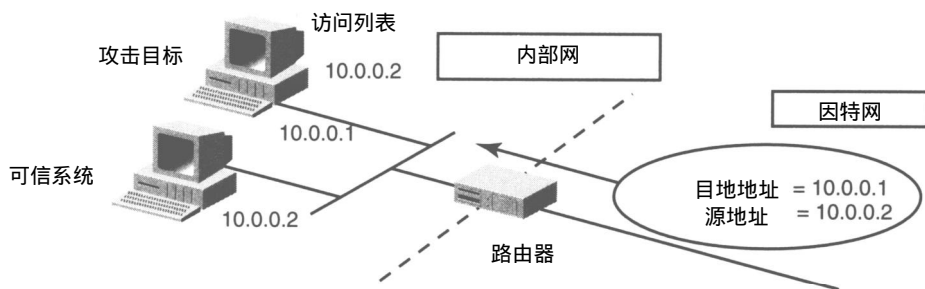


图1-18 路由器级包过滤

许多复杂的防火墙使用了代理服务器，也称作堡垒主机，如图 1-19所示，堡垒主机可以

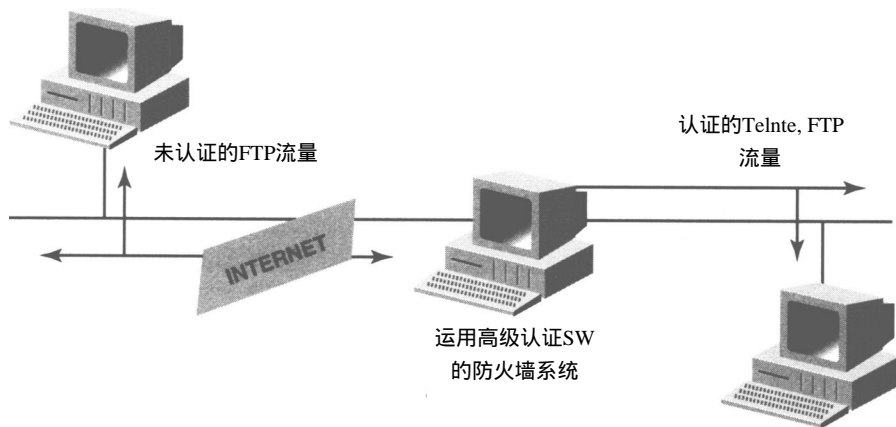


图1-19 代理服务器（堡垒主机）防止来自互联网的直接访问

防止内部用户直接访问因特网服务，其作用就像一个代理，过滤掉未授权的要进入因特网的流量。

防火墙的目的就是使它像一扇安全门，保证门内各组件的安全，此外，还控制着谁（或什么）可以进入和谁（或什么）可以走出这个受保护的环境。它就像门前的一个安全卫士，控制和确认谁能或不能进入这个站点。

防火墙的建立提供了对网络流量的可控过滤，以限制访问特定的因特网端口号，而其余则被堵塞。为做到这一点，要求它必须是唯一的入口点，这就是你为什么多次发现防火墙与路由器是一个整体的原因。

因此，选择防火墙应该根据装在站点的硬件、本部门专业性的意见和可信任的销售商。

通常，配置防火墙是用来阻止未经认证的外部登录。用防火墙保护站点是一种最容易使“门”对安全和审计起作用的方法。

利用防火墙，你可以防止站点的任意连接，并且还能建立跟踪工具，它可以根据日志摘要帮助你，因为日志中记载着连接的起点、服务器提供的服务量，甚至还包含是否有攻击进入等信息。

防火墙的一个基本目的是保护站点不被黑客攻击，如前所述，站点暴露于大量的威胁面前，防火墙可为你提供保护，但对那些绕过它的连接，则无能为力。因此，要警惕后门，如：调制解调器连到你的 LAN 上时，特别是如果你的远程访问服务（RAS）处于受保护的 LAN 内时，这就是一个典型的例子。

然而，防火墙并不是绝对有效的。它的目的是增强安全性，而不是保证安全。如果有很重要的信息在 LAN 上，首先服务器就不应该与它连接。必须注意那些允许你从机构内部进入服务器的群件应用程序，反之亦然。

另外，如果在内部 LAN 上有 Web 服务器，要警惕内部攻击，对企业服务器也是这样。这是因为防火墙不能对付来自机构内的威胁，例如，一个捣乱的职员可以拔掉企业服务器上的插头，使其暂时停止工作，对此，防火墙则无能为力！

包过滤是一个简单有效的用于过滤多余信息包的方法：通过拦截信息包、读信息包和拒绝那些与路由器中规则不匹配的信息包。

遗憾的是，包过滤不足以保证站点的安全，因为许多威胁、许多新协议几乎不费劲就可以绕过这些过滤器。

例如，包过滤用于 FTP 协议并没有效，因为它允许用端口 20 与外部服务器联系以建立连接，从而完成数据的传输。即使在路由器上加一条规则，内部网络机器上的端口 20 仍能被外界探查。还有，如前所述，黑客可以很容易地“欺骗”这些路由器。今后，防火墙将会进一步增强这些方面的安全策略。

然而，当你决定实现一个防火墙时，首先你要决定所要用的防火墙的类型（当然，防火墙的类型很多）和结构。相信本书会带给你很大的帮助。

你应知道，还有一些商用的防火墙产品，常称为 OS Shields，装于操作系统上。尽管它们比较流行，通过代理应用系统与包过滤相结合能够监视任一协议的数据和命令流，从而达到对站点的保护，但 OS Shields 并不是一个很成功的产品，原因是它那独特的配置：由于是在核心级进行的配置，所以对管理员来说是不可见；另外，管理员不得不引入其他产品以帮助服务器的安全管理。

防火墙技术已走过了很长的路，包括所谓传统的，或者说是静态的防火墙，今天已经有了“动态防火墙技术”。

动态防火墙同静态防火墙相比，主要区别在于，后者的目的是“许可任何服务，除非遭到明确拒绝”或“拒绝任何服务，除非有明确许可”，而前者的主要目的是“许可/拒绝任何服务，只要你需要”。

它这种适应网络流量和设计结构的能力，提供了比静态包过滤模式更便利的特色。

### 1.19.1 防火墙缺陷

本书用大量的篇幅讲述了有关防火墙的事宜，特别是由于所有最新一代的防火墙所表现出来的基本问题：它们可以控制获得一定授权的站点在一定的时间与哪个服务会话，但可怕的是作为一个整体提供到因特网的服务能够被公开。

当前的防火墙不能辨别出完成有效服务的数据，对防火墙来说一个邮件就是邮件。数据过滤是最近一些防火墙中的新发明，关于它更多的信息请看第10章。

使用一个防火墙且清除所有含诸如“黑客”这个词的报文，已经成为可能，但并不是所有防火墙都有过滤 applets 的能力，当今，这些 applet 对于任一受保护的内部网络是一个主要的威胁。

还有，如果一个黑客连接到防火墙内系统的一个有效服务或端口上，例如 SMTP 端口，那么黑客就能用一有效数据去进行攻击或用 Shell 命令去利用那个有效服务。

作为例子来看一下 Web 服务器。phf 攻击是当前众多针对 NCSA Web 服务器的攻击之一。服务器有一个缺省实用程序 phf，它允许攻击者运行系统上的命令。这个攻击看上去就像一个正常的 Web 查询，除非 phf 上有一个管理者邮件过滤器在防火墙上放置了高级命令，否则，今天的防火墙不能阻止这类攻击。

对付这个局限性的关键是要把防火墙当作一种理解内部服务配置的方式。防火墙只允许特定的服务被因特网上的用户访问，但必须确保这些已知的服务是能够得到的最新的、最安全的版本。这样，就可以把我们的注意力从加固整个网络转移到仅仅加固几个内部的机器和服务上来。

关于这方面的内容，你将在后面的第4章、第5章和第8章继续学习。

### 1.19.2 停火区

停火区（DMZ）用在这样的位置，有少数机器服务于内部网络，且其余机器隔离于一些设备（通常是防火墙）之后。这些机器或者在公开的地方，或者有另外一个防火墙对 DMZ 进行保护。从安全角度看，这是一个很好的安排，因为只有接受返回连接的机器才是“牺牲品”。

如果机器能省去这些努力，有高风险目标的机构就可以从这个方案获益。经证明，它对保护内部资源的安全是极其有效的。还有一个建议是改变机器的类型和安全软件的出版商，以保护在 DMZ 内部和外部的安全。例如，在一个性质倾向于相同的社区中，采用这种方法是很有帮助的，如果使用两个相同的防火墙，则它们可以被一个违法者同时破坏掉。

建立 DMZ 的唯一缺陷是机器的维护。为了使 Web 服务器和 FTP 服务器容易更新，大多数管理员喜欢文件系统的本地访问。若在两者之间加一个防火墙，则使得实现维护有些难度，

特别是当不只是一个人维护服务器时。总之，外部信息的驻留还算稳定，也很少有管理上的烦恼。

### 1.19.3 认证问题

防火墙和过滤路由器的工作越来越趋于合二为一。是否允许连接进入系统，认证允许服务连接是建立在对用户认证的基础上，而不是建立在它们的源地址和目的地址基础上。利用一些软件，用户的认证可以允许到达某些服务和机器，而另外的则只能访问基本系统。在基于用户的服务认证中，防火墙常扮演一个重要的角色，但也可以配置一些服务器去理解这些信息。当前的 Web 服务器经配置也可用于控制允许哪个用户访问哪棵子树和把用户限制于适当的安全等级。

认证有多种，其形式有密码令牌、一次性口令及（最常用且安全性也最低的）简单文本口令。由站点管理员决定哪个用户用哪种认证方式，这也是得到公认的。正确的认证可允许国外站点的管理员进入网络改正错误，这类连接是使用密码令牌这种性能强的认证方法的首选对象。

### 1.19.4 周边信任

今天，整体安全的焦点在周边上。坚固的外表和柔弱的中央是一种普遍存在的现象。坚固外表的实现借助于防火墙、认证设备、强固的拨号堤、虚拟专用通道、虚拟网络以及许多隔离网络的其他方法。而在内部，则只有供人侵占的份了。内部安全没有被恰当地管理，且普遍令人担心，因为如果有人越过了边界，堡垒就失陷了。这是一个众所周知的问题，也是今后要继续努力解决的问题。

关于这个问题的解决方案无需多讲了。内部安全问题一直是一个敏感的麻烦事，且都不情愿投资去寻求解决方案。解决它的唯一途径是通过广泛的宣传和高度的热情使这项工作下去。快速或永久解决这个问题是不现实的，但事实上，对周边的信任最终还是靠不住的。

有关破坏防火墙的问题也一直在讨论，且认证方法也不是一点用没有。对一个站点物理安全的信赖实在是一个灾难，对外部人员的鉴别水平还是不够的。电话维修员常来检修吗？能让维修员进入一个机构最敏感的区域吗？从安全上讲，周边并不是唯一的底线。

### 1.19.5 内部网

在信息系统组中，内部网提供的资源很快成了一个主要的利益来源。它们允诺提供每个人都能访问的单一资源，从而能改善他们的生活。向无纸信息系统的转变没有看上去那样伟大。把一个机构内部的所有文档放入一个地方，无异于给这些文件划上醒目的红色标记，但又希望人们不会注意到它。

也许是我造了一个新词，但“ Intra-Intranets ”的确是解决这个问题一个明智的方案。把重要数据保存于工作组内，不重要的数据保存在隔离开的内部网内，这是一个可行的选择。用不同的系统去存储子群组，且整个机构使用一个主系统。对于在主系统上什么是可允许的需要制定相应的政策，以保护资料不被公开访问。

本章综合概述了许多广泛使用的网络协议及其标准、与之相关的安全问题以及防火墙在提高连接安全性方面的基本作用。

对于许多机构来说，基础连接成为一个很重要的问题。的确，连接到因特网有许多方法，其中一些比另一些更有效，这是由于它们具备与各种环境和各种计算机进行交互的能力。

第2章“基础连接”，讨论了通过UUCP、SLIP、PPP、Rlogin和Telnet用于因特网上的基础连接的特点。