

移动IP

- ▶ **Mobile IP: The Internet Unplugged**
- ▶ (美) James D. Solomon 著
- ▶ 裘晓峰 等译



机械工业出版社
China Machine Press

Prentice Hall

TP393
S98

461181

IP 网络技术丛书

移动 IP

所著
(美) James D. Solomon 著

袁晓峰等 译



机械工业出版社
China Machine Press

1528000

本书提供了从不同层次理解移动IP所需的完整内容。介绍了移动IP运行的环境,描述了移动IP需解决的各种问题、解决问题的方式以及在若干配置实例中移动IP应用的方式。还介绍了移动IP应用过程中遇到的各种安全威胁的情况,并列举了解决安全威胁的各种技术。

本书共分四部分14章,内容丰富、实用,是网络管理员、网络设计者和准备实现移动IP的人员的必备之书。

James D. Solomon : Mobile IP: The Internet Unplugged.

Authorized translation from the English language edition published by Prentice Hall.

Copyright © 1999 by Prentice Hall, Inc.

All rights reserved.

Chinese simplified language edition published by China Machine Press.

Copyright © 2000 by China Machine Press.

本书中文简体字版由美国Prentice Hall公司授权机械工业出版社独家出版。未经出版者书面许可,不得以任何方式复制或抄袭本书内容。

版权所有,侵权必究。

本书版权登记号: 图字: 01-1999-2862

图书在版编目(CIP)数据

移动IP / (美)索罗门 (Solomon, J. D.) 著; 裘晓峰等译. — 北京: 机械工业出版社, 2000.1

(IP网络技术丛书)

书名原文: Mobile IP: The Internet Unplugged

ISBN 7-111-07694-X

I. 移… II. ①索… ②裘… III. 计算机网络-传输控制协议 IV. TP393

中国版本图书馆CIP数据核字(1999)第53962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: 卢志坚

北京市南方印刷厂印刷·新华书店北京发行所发行

2000年1月第1版·2000年3月第2次印刷

787mm×1092mm·1/16·14.25印张

印数: 5 001-9 000

定价: 30.00元

凡购本书, 如有倒页、脱页、缺页, 由本社发行部调换

译者序

因特网是人类历史上影响最为深远的发明之一，它的触角已渐渐深入到人们日常生活的方方面面。它突破了时间和空间的限制，利用它，可以查阅最新的科技资料，可以看到最新的国际时事新闻，可以找到自己最喜欢的朋友，可以与世界各地的网友切磋游戏技巧……。当前，对于因特网相关技术的研究也受到了各个商业公司、大学、研究院所的高度重视。

让人们能够随时、随地访问因特网，是当前因特网技术研究的一个热点，也是下一代真正的个人通信技术的目标。移动IP技术就是这样的一种技术。它将人们从计算机机房、电话插座的限制中解放出来，不用重新启动计算机、不用重新配置，甚至不用中断当前的网络浏览、正在进行的网友聊天，就能随处移动，不管是在家中、在办公室、在火车上还是在飞机上。

移动IP技术在利用各种路由技术提供随时随地的连通性的同时，还设计了强大的认证和加密体系来对付因特网上人们越来越关心的安全问题，其中使用到了各种先进的密码算法技术，可以说是当前因特网技术的集大成者！

本书深入浅出，概念清晰，从TCP/IP连网技术的入门，到隧道封装、防火墙、公开密钥算法、移动IP体系中的各种专门概念和技术等，都做了非常详尽的叙述和严密的分析，指出了原有的标准文件中存在的错误和不明之处。阐述了当前正在进行的各种研究工作的内容，是讲述移动IP技术的一本非常好的专著。

本书作者作为移动IP技术的官方研究组织——因特网工程任务组移动IP任务工作小组的前任主席之一，全面参与了该技术的研究工作，并为本书的写作付出了巨大的努力。

本书的翻译工作由裘晓峰主笔，参加翻译工作的还有赵粮、罗伟光、何慈信、李明之、张侃、徐大勇等。我们在翻译中尽量忠实原著，文中的专业术语都在第一次出现时标注了英文，以方便读者理解。对于尚未标准化的专业术语翻译，从前后文的语义出发，也请教了不少专家，尽量做到准确、精练。

本书不仅是移动IP技术，也是因特网安全技术一本不可多得的参考书。通过它的翻译出版，我们希望能够为感兴趣的读者提供学习和研究工作上的帮助。

译者

1999年11月

序

在当今社会中，移动包括各种各样的移动形式，正成为日益关注的话题。所有的物体都在移动着，越来越快地移动着。

刚开始设计连网技术时，我们认为所有的计算机和通信设备都是固定不动的，这是很自然的事情，当然，如果当时能考虑得完善些，情况就会好得多。现在，许多计算机一直在移动着，其中还有许多要求在移动中进行通信，因此，我们现在使用的通信协议就必须适应这种移动通信需求。

现在应用最为广泛的一种通信方法是采用IP协议簇，利用IPv4、TCP和UDP以及在它们之上的一系列应用。随着移动通信需求的增长，IP协议簇也应适应移动通信的要求。

因特网工程任务组（IETF）成立了一个工作小组，开始讨论这个问题，许多解决方案被提了出来，并进行了讨论。在整个过程中，本书作者都参与了这方面的工作。

这个工作小组一直在讨论各种各样的解决方法，工作小组中的一些负责人转向了其他方面的研究，James Solomon则于1994年夏天成为这方面工作的主席之一，从那时起，他就一直领导着这个小组。在其他主席的帮助下，这个工作小组制订了一个协议来解决移动IP通信的需要，他们从一堆存在冲突的提议中理出了一个现实可行的解决方法。由于他对所涉及问题的理解和对该团体中的所做的领导工作，James Solomon在上述研究中起了关键作用。

正是由于上述原因，他成为您手中这本书的唯一适合的作者。他考虑得非常周详，并对研究中所做的折中和取舍有较深理解。事实上，作为主席，他的工作就是理解所涉及的方方面面，而不仅仅是喜欢的那些东西。因此，James Solomon对这个协议有非常透彻的理解，包括它工作的方式、之所以这样定稿的原因等，这些都在本书中做了交代。并且，他从头到尾地看到了所有的争论，以及人们对这个协议产生困惑的原因，因此，James Solomon在这些关键地方加入了特别额外的细节说明。

移动正在变得无处不在。从简单的形式看，您将便携机网线从办公室或园区网中拔下来，回家后再插到家里的网上，这样，您的便携机就实现了移动。也有可能您是通过旅馆房间里的电话，或者通过蜂窝电话，或者通过机场的公共电话接入网络。最近，我们看到了带有内置的无线或红外网络接口的计算机，它们随时都可以移动。很明显，对于家庭通信软件开发者、网络设备制造者以及负责建设和运行我们正在使用的网络的工程师们来说，移动中的通信已经成为一个目标，他们需要具有移动能力的技术，以及如何应用这些技术的信息。这本书与其作者一样，非常公正地阐述了上述问题。

您手中的这本书非常详细地论述了从因特网协议簇的各个组成部分一直到移动及其解决方案的宏大范围内的各种技术，因此，它能够带给读者理解移动IP解决方案所需的技术信息。作者在本书中还描述了移动IP技术当前的发展，包括推广相关应用的积极工作。甚至还告诉了读者我们还不知道怎样去做的东西，不管怎样，让大家了解问题的所在总是有意义的。

——Joel M. Halpern

Routing Area Director for the IETF

Director ,Internetworking Architecture, Newbridge Networks, Inc.

前言

笔记本电脑在尺寸、重量和复杂程度上的巨大提高；对计算机网络，尤其是因特网上信息的依赖性的持续增长；远程办公和移动办公人员数量的迅猛增加；这些都是移动计算和联网技术标准创立的推动力量。

本书就是关于这样一个标准的。移动IP允许移动节点（例如膝上型或笔记本电脑）在不重新启动和不中断任何正在进行的通信的同时就能够移动自己的位置，当前的因特网协议簇尚不能提供这些功能。移动IP用来增强现存的IP协议以便提供移动性，这项技术目前正处于标准研究开发阶段。

本书提供了从不同层次来理解移动IP所需要的完整内容。本书首先介绍了移动IP运行的环境，然后描述了移动IP需要解决的各种问题、解决问题的方式以及在若干种配置实例中移动IP应用的方式。本书还介绍了移动IP应用过程中会遇到的各种安全威胁的详细情况，并列举了解决安全威胁的各种技术。本书还论述了移动计算的一些尚未形成定论的问题，并对需要继续研究的领域提出了可能的解决方案。

本书的目的在于三个方面：首先是揭开了定义移动IP的因特网标准文档，即RFC文档的神秘性，使每个需要了解这项新技术的人，都能发现本书的内容容易理解而且论述得很透彻。其次是向考虑安装移动IP的读者介绍移动IP在管理方面和安全方面的问题。这部分读者对象包括网络管理员、企业（网络）安全官员、网络设计工程师、有线或无线服务提供商等。第三是帮助准备实现移动IP的技术人员理解当前标准文档中哪些地方解释得不够清楚、哪些地方根本没有解释或哪些地方解释得不正确。

本书的范围因而限制在移动IP及其应用和安全问题。本书中没有复制其他著作中很容易看到的信息，例如协议栈中各层协议的详细描述等。并且，本书没有提供移动IP可以运行其上的各种可能的物理层媒介的详细介绍，因为这些资料随处可得，并且，移动IP完全不依赖于这些媒介。

读者可能会喜欢较少使用缩略语，那样可能会像许多其他的计算机网络著作一样带来含混不清的地方。本书使用了非常朴素的语言来描述移动IP专业性很强的内容，并提供了例子和插图来阐明其要点。本书在提出某个问题的解决方案之前，会提供有关该问题详细的背景信息，以便读者能透彻地理解该问题的特性。本书还尽可能地提供了对没有覆盖到的资料的参考索引，这样，当读者在对某个章节理解不清时就不会孤立无援了。本书尽量避免使用计算机行话，书中的所有术语都使用了详尽的词汇表进行定义。

本书的开篇是一个计算机网络技术的初级读本，解释了网络分层模型，尤其是IP协议。随后是详细的移动IP讨论，准备实现移动IP的技术人员会觉得这部分非常有用。接下来，本书介绍了在解决用户、用户网络、服务提供商的安全威胁的条件下，移动IP的应用情况。再往后是更深入的话题，包括IPv6的移动性以及移动IP中尚未解决的问题等。最后，本书对在全世界都实现移动IP技术的前景进行了展望。

英文原书书号：ISBN0-13-856246-6

原书出版社网址：<http://www.prenhall.com>

目 录

译者序
序
前言

第一部分 导 论

第1章 绪论	1
1.1 推动移动通信发展的力量	1
1.2 阅读本书所需要的知识	2
1.3 本书面向的读者	2
1.4 本书的目的	2
1.5 书中所用的标记	3
1.6 IPv4还是IPv6	3
1.7 如何得到RFC文件或因特网草案	3
1.8 本书其他部分的组织结构	4
第2章 计算机网络教程	6
2.1 计算机是如何进行通信的	6
2.1.1 协议层	6
2.1.2 每一层的功能	7
2.1.3 本书关系到哪些协议层	8
2.1.4 网络层提供的服务	9
2.2 因特网协议 (IP)	10
2.2.1 ICMP	10
2.2.2 IP的功能	11
2.2.3 IP包格式	11
2.2.4 节点如何得到一个IP地址	13
2.3 IP路由技术的工作原理	14
2.3.1 什么是路由表	14
2.3.2 存在多个匹配表项时怎么办	14
2.3.3 选路实例	16
2.3.4 IP路由技术总结	17
2.4 路由表是如何生成的	17
2.5 为什么选路依赖于网络前缀	19
2.6 如何将域名解析成地址	19
2.7 如何决定数据链路层地址	20

2.7.1 地址解析协议	20
2.7.2 代理ARP和ARP	20
2.8 本章总结	21
第3章 移动IP的作用	22
3.1 当节点换了一条链路时会发生什么	22
3.2 用特定主机路由能否解决移动问题	23
3.2.1 特定主机路由如何解决移动问题	23
3.2.2 特定主机路由解决方案好吗	24
3.3 为什么不只是改变节点的IP地址	26
3.3.1 改变IP地址时能否保持现有连接	26
3.3.2 如何找到IP地址不断变化的节点	27
3.4 在数据链路层能否解决移动问题	27
3.5 只需要漫游功能的情况	29
3.6 本章总结	29

第二部分 移动IP

第4章 移动IP总述	31
4.1 移动IP是否是官方标准	31
4.2 移动IP解决的问题	31
4.3 移动IP的应用范围	32
4.3.1 移动IP可用于哪些媒介	32
4.3.2 移动IP是否是一个完整的移动通信方案	32
4.4 移动IP的设计要求	33
4.5 移动IP的设计目标	33
4.6 移动IP做了什么假设	33
4.7 移动IP的功能实体	34
4.7.1 代理是主机还是路由器	36
4.7.2 谁拥有移动节点和代理	36
4.8 移动IP的工作机制	37
4.9 本章总结	39
第5章 技术细节	41
5.1 移动IP的设计思想	41
5.2 代理搜索	42

5.2.1 代理搜索包括的消息	42
5.2.2 移动节点如何判定自己的移动	44
5.2.3 移动节点收不到任何广播消息时 怎么办	45
5.2.4 总结	46
5.3 注册	46
5.3.1 注册消息	47
5.3.2 注册过程	50
5.3.3 移动节点如何得到家乡代理 的地址	54
5.3.4 节点如何知道注册消息的真正 发送者	55
5.3.5 移动节点如何向家乡代理或外地 代理提供额外信息	56
5.3.6 移动节点在无线蜂窝间频繁切 换时怎么办	56
5.3.7 “R”比特的处理	57
5.4 数据包的选路	59
5.4.1 移动节点在家乡链路上时包 的选路	59
5.4.2 移动节点在外地链路上时包 的选路	59
5.4.3 移动节点如何发送数据包	63
5.4.4 IP包的路由与它们的源地址无关吗	65
5.4.5 为什么用隧道而不是源路由	65
5.4.6 为什么用三角路由	66
5.4.7 移动节点收发广播和组播	67
5.4.8 Van Jacobson 压缩的工作机制	70
5.5 本章总结	71
第6章 隧道技术	73
6.1 IP分片	73
6.1.1 分片的工作原理	73
6.1.2 IPv4如何确定路径的MTU	74
6.2 IP的IP封装	75
6.2.1 生成一个封装的数据包	75
6.2.2 ICMP报文的中继	76
6.2.3 防止递归封装	77
6.2.4 小结	77
6.3 最小封装	77

6.3.1 产生一个经过封装的数据包	78
6.3.2 分片	78
6.3.3 生存时间和隧道长度	79
6.3.4 中继ICMP报文	79
6.3.5 防止递归封装	79
6.3.6 小结	79
6.4 通用路由封装	79
6.4.1 多协议封装	80
6.4.2 防止递归封装	80
6.4.3 小结	81
6.5 本章总结	81

第三部分 移动IP的应用

第7章 安全入门	83
7.1 安全的概念	83
7.2 密码学	83
7.2.1 密码系统	84
7.2.2 秘密密钥和公开密钥算法	84
7.3 机密性的含义	85
7.3.1 秘密密钥加密	85
7.3.2 公开密钥加密	86
7.4 认证、完整性检查和不可抵赖	87
7.4.1 授权	87
7.4.2 认证	87
7.4.3 认证系统的功效	88
7.4.4 秘密密钥认证	88
7.4.5 公开密钥认证	90
7.5 密钥的安全管理	92
7.5.1 公开密钥管理中的难点	92
7.5.2 手工方法	92
7.5.3 受信任的第三方	93
7.6 因特网中使用的安全协议	93
7.6.1 安全协定	93
7.6.2 IP认证头 (AH)	94
7.6.3 IP封装安全净荷 (ESP)	94
7.6.4 其他因特网安全协议	95
7.6.5 ISAKMP/Oakley	95
7.6.6 SKIP	96
7.7 防火墙	97

7.7.1 防火墙的简单历史.....	97	9.3.2 移动节点作为VPN的特例	116
7.7.2 包过滤路由器.....	98	9.4 移动节点如何穿越防火墙而又	
7.7.3 应用层中继.....	99	不牺牲网络的安全性.....	118
7.7.4 安全隧道	100	9.4.1 穿越防火墙的假设和要求	118
7.8 本章总结.....	101	9.4.2 用SKIP穿越防火墙	119
第8章 园区内的移动：移动IP的一个		9.4.3 采用ISAKMP/Oakley穿越防火墙	127
简单应用	102	9.5 本章总结和结论	128
8.1 应用模型.....	102	第10章 服务提供商对移动IP的应用	129
8.1.1 什么是园区内部网	102	10.1 商用移动IP服务的模型	129
8.1.2 移动IP是如何应用的	103	10.2 窃取服务	130
8.1.3 为什么要网络管理员这样来		10.2.1 蜂窝“克隆”欺骗.....	130
配置移动IP	104	10.2.2 服务提供商如何使用移动	
8.1.4 本章的安全模型	104	IP防止窃取服务攻击.....	131
8.2 内部攻击.....	104	10.3 重新考察拒绝服务攻击	135
8.3 移动节点的拒绝服务攻击.....	105	10.3.1 Flooding攻击的原理	136
8.3.1 什么是拒绝服务攻击	105	10.3.2 服务提供商对Flooding攻击	
8.3.2 移动IP可防止哪种拒绝服务攻击	105	的防御	136
8.3.3 移动IP如何阻止拒绝服务攻击	106	10.3.3 入口过滤对移动IP的影响	136
8.3.4 重发攻击	107	10.3.4 入口过滤有关的移动IP改进	137
8.3.5 小结	107	10.4 MOTOROLA公司的iDEN™	
8.4 窃取信息：被动地偷听.....	108	系统：案例分析	138
8.4.1 威胁的特性	108	10.4.1 iDEN提供的服务类型	138
8.4.2 数据链路层加密	108	10.4.2 iDEN分组数据	139
8.4.3 端到端加密	109	10.4.3 iDEN分组数据的工作方式	139
8.5 窃取信息：会话窃取攻击		10.5 本章总结	141
(Takeover)	110	第11章 移动IP的其他应用	142
8.5.1 外地链路上的会话窃取	110	11.1 移动IP框架中对其他协议的支持	142
8.5.2 其他地方的会话窃取攻击	110	11.1.1 为什么要支持其他协议	142
8.6 其他主动攻击	111	11.1.2 其他协议	142
8.7 本章总结	112	11.1.3 要求和假设	143
第9章 因特网上的移动：一个更复杂		11.1.4 集成移动扩展	143
的应用	113	11.1.5 用其他协议注册	144
9.1 应用模型	113	11.1.6 向移动节点路由其他协议	
9.1.1 假设和要求	113	的数据包	144
9.1.2 如何应用移动IP达到这些要求	114	11.1.7 为什么要用GRE	146
9.1.3 为什么要这么做	114	11.1.8 为什么用隧道	147
9.2 有哪些安全威胁.....	115	11.1.9 小结	147
9.3 如何保护防火墙外的移动节点.....	115	11.2 移动网络（不是移动主机）.....	147
9.3.1 VPN回顾	115	11.2.1 家乡链路上的移动路由器	148

11.2.2 外地链路上的移动路由器	148	12.6.6 移动节点何时发送绑定更新	175
11.2.3 移动网络的路由表	149	12.7 数据包的选路	176
11.2.4 运动网络的情况	152	12.7.1 知道转交地址的通信伙伴如 何向移动节点发送数据包	176
11.2.5 小结	153	12.7.2 不知道转交地址的通信伙伴 如何向移动节点发送数据包	177
11.3 移动IP作为二层隧道建立协议	153	12.7.3 移动节点如何发送数据包	178
11.3.1 什么是远程拨入	154	12.8 本章总结	178
11.3.2 虚拟隧道协议的工作原理	155	第13章 尚无定论的话题	179
11.3.3 虚拟隧道协议的安全考虑	157	13.1 TCP的性能和移动性	179
11.3.4 为什么不只是用移动IP	157	13.1.1 什么是TCP	179
11.3.5 L2TP与VTP的不同	157	13.1.2 TCP的工作原理	180
11.3.6 小结	159	13.1.3 TCP有关拥塞的假设是否正确	181
11.4 本章总结	159	13.1.4 移动节点如何提高TCP性能	182
		13.1.5 小结	184
		13.2 RSVP和实时业务	184
		13.2.1 什么是实时业务	184
		13.2.2 IP为何不太适用于实时业务	185
		13.2.3 RSVP	186
		13.2.4 移动IP对实时业务的影响	188
		13.2.5 小结	190
		13.3 服务定位	191
		13.3.1 服务定位协议的功能	191
		13.3.2 服务定位的工作原理	192
		13.3.3 服务定位的安全问题	194
		13.3.4 服务定位和移动	195
		13.3.5 小结	195
		13.4 本章总结	196
		第14章 总结和最后的问题	197
		14.1 移动IP总结	197
		14.1.1 背景、内容和目的	197
		14.1.2 术语和操作	197
		14.1.3 移动IP应用	199
		14.1.4 正在进行的工作和尚无定 论的话题	200
		14.2 移动IP的将来	200
		术语	203

第四部分 有关将来的话题

第12章 IPv6的移动性

12.1 IPv6和IPv4的不同

12.1.1 IPv6基本报头

12.1.2 IPv6扩展报头

12.1.3 IPv6地址类型

12.2 设计移动IPv6时关系到哪些区别

12.2.1 大地址空间的好处

12.2.2 新的选路报头的作用

12.2.3 认证报头的作用

12.3 有了地址自动配置就无需移动

IPv6了吗

12.4 移动IPv6的工作原理

12.4.1 移动IPv6的组成

12.4.2 IPv6的邻节点搜索

12.5 移动节点如何确定它的位置

12.5.1 ICMPv6路由器搜索

12.5.2 移动节点如何得到转交地址

12.6 移动节点如何将转交地址告诉

别的节点

12.6.1 布告

12.6.2 一般的布告过程

12.6.3 布告协议

12.6.4 布告中用到的消息

12.6.5 移动节点如何知道家乡代理

的地址

第一部分 导 论

第1章 绪 论

想象一下，你正要休个长假或要出差一年，由于要离开家很长一段时间，所以必须作出些安排，以确保你的邮件能随时送到你手中，而你可能每两个星期就会换个地址。在这种情况下，又如何保证邮件能送到你那里呢？

一种方法是寄明信片给每一位可能给你写信的人，包括公用事业公司、信用卡公司、朋友和亲戚，通知他们地址变更情况，还要特别小心，千万不能告诉那些可能寄送垃圾邮件的人。这种方法存在许多问题。首先，每次换地方就要寄一遍明信片。其次，必须给每一位能想到的、可能给你写信的人寄上明信片，否则等回家时，就可能发现有人在几个月前给你家寄了一份非常紧急的通知。第三，在这种方式中，没有任何办法来防止恶作剧者以你的名义发出这种明信片，从而使得你的信件被送到他们手中，或是送到你的商业对手的手中，或是任何你所不希望的地方。

更好的方法是在你家所在的邮局留下一个转发通知，这样，所有寄来的信件都将被转发到你当前的新地址。这种方法的好处在于，将新地址只告诉邮局，而无需通知每一位可能给你写信的人。邮局可以提供一些安全措施，保证用户的真实身份，确保不是别人假冒你，并且还可以通过认证，确保你确实有改动转发地址的权限。

诚然，如果一些邮件按你先前的地址进行了转发，可当它们在半路上时，你却又换了新地址，那么，这些邮件就可能暂时丢失。解决这个问题的方法是：在你离开之前，通知邮局将信件再转发到你的新地址上。当然，也可以通知给你写信的人，如果在一定的时间内没有收到回信，就请再给你重发一次。

这里，如果将“信件”改为“因特网数据包”，将“转发”改为“隧道技术”，将“邮局”改为“具有移动IP功能的路由器”，那么前面所讨论的情况就和移动IP一样了。下面我们将用整本书来进一步作详尽的描述。

1.1 推动移动通信发展的力量

过去几年中，笔记本电脑的数目迅速增加，因特网也有了迅猛发展。笔记本电脑在体积、重量和性能方面都在不断改进，同时，因特网也正在以惊人的速度发展着。

现在，人们越来越依赖于网络计算。大多数企业都建立了先进的网络，连接各个雇员和他们的计算机、工作站。有时，我们工作中的重要信息只能通过网络得到，这些信息可能在企业的专用网Intranet上，也可能在因特网上。因特网是一个公用网络，连接着全世界的各个公司、大学、非盈利性组织、个人和政府机关。

此外，越来越多的人成为了移动办公的一分子，包括远程计算人员、移动售货人员以及其他一些经常需要跑来跑去的人，这些人急切地希望能从企业网的计算机中或是因特网上得

到所需的数据。

不断增加的移动办公人群、对网络计算越来越强的依赖和移动计算技术的发展，这三方面一起推动着将移动的计算机与其他计算机相连的需求，包括与固定的和移动的计算机连接。

人们为两台或多台计算机之间交换信息定义了一套复杂的规则，这就是网络协议。问题是，在大多数网络协议制定的时代，几乎所有的计算机都不需要经常移动，所以许多通信协议都应付不了快速移动中的计算机通信。

本书介绍了移动IP (Mobile IP)，一个为移动的计算机传送信息的解决方案，它是一个由因特网工程组制定的因特网 协议标准。移动IP与移动计算机通信时所采用的物理媒介无关，它允许移动计算机在不中断通信和不重新启动应用程序的情况下改变地理位置。在本书的第一部分中，我们将定义所有有关的术语和概念。

1.2 阅读本书所需要的知识

阅读本书需要有关计算机技术的基础知识，稍懂计算机连网的计算机专家会发现他们有足够的知识来理解本书的绝大多数内容，具备一些二进制代数方面的知识也会很有帮助，这是计算机认识和计算数字的基本方法。

本书还为那些在计算机连网、计算机通信和计算机安全方面知识有限的读者准备了一些教学内容。本书并不需要读者了解因特网协议的细节，也不需要了解对付安全威胁的加密方法。但是，那些具备这方面知识的读者也会发现本书内容详尽，具有一定的深度和广度。

1.3 本书面向的读者

作者尽力研究了有关移动IP的标准文件，并用通俗的文字将它描述出来，因此，那些只了解移动IP以及用它能解决哪些问题的读者会发现很容易在本书中找到他们想要的信息，而且非常易懂。

另外，那些想对移动IP有详细了解的读者也会在本书中发现他们想要的信息。这里，我们列出两类读者：

- 对于任何一个想在网络中采用移动IP技术的读者，都可以在本书中找到详细的实现方法，包括具体应用和安全措施。这些读者一方面包括网络管理人员、网络维护人员、公司的安全人员，另一方面包括有线和无线业务提供商中的网络设计人员。
- 那些想通过硬件或软件实现移动IP的人也可以得益于本书，这些人包括主机软件、协议、路由器、网络接入设备的销售公司，特别是那些本地和广域无线通信设备、接入点、骨干设备制造商中的工程师和管理人员。这部分读者会喜欢本书对标准文件中一些错误之处、遗漏之处和令人疑惑的地方所作的解释，他们还会发现本书对移动IP的来龙去脉和应用所做的描述是必不可少的。

1.4 本书的目的

本书的主要目的是从技术本身到应用和安全措施详细地描述移动IP。要读透标准文件是很困难的，在对标准文档的来龙去脉不太了解的情况下要读透它就更困难了，本书提供了移

动IP的来龙去脉的情况。

如上一节所说,本书还从实现者的角度出发,力图澄清移动IP标准文件中的明显错误、用词不当之处和令人疑惑的地方;还力图帮助那些想采用移动IP技术的人了解其中的安全隐患,并解释了消除和减轻这些安全隐患的方法。

本书的另一个目的是介绍因特网工程任务组中负责定义移动IP的工作小组的情况,介绍标准制订工作的进展过程。

本书详细地描述了移动IP,并介绍了与它有关的技术。但本书尽力避免花太多的篇幅去讨论那些别的文献中已介绍过的技术。

- 那些想了解CDPD和其它无线连接技术的细节的读者可以考虑去阅读[Daye1]或[TaWaBa97]。
- 若想了解计算机连网技术各层协议的细节,可以考虑阅读[Come5]、[Stev94]或[Tane96]。
- 若想了解各种加密和认证算法的数学基础,可以考虑阅读[KaPeSp95]或[Schneier95]。

1.5 书中所用的标记

本书中尽量避免使用缩写,例如,我们从不把移动IP(Mobile IP)缩写成MIP,也不把移动节点缩写成MNs,或把外地代理缩写成Fas。一个通贯全书的缩写就是IP,它表示因特网协议(Internet Protocol)。书中其他缩写包括PPP、UDP和TCP,但为了帮助读者阅读,本书多处写出了它们的全称。

1.6 IPv4还是IPv6

目前,因特网几乎全由采用因特网协议版本4的节点构成,包括主机和路由器。因特网协议版本4也写成IPv4。因特网的发展如此之快,因此迫切需要一个新版本的协议来解决IPv4的缺陷,如对可寻址的最大节点数目的限制,这个新版本称为IPv6。目前它正在标准化的进程中。

除了极个别的情况,本书讨论的是因特网协议的版本4(IPv4)。因此在谈到IPv4时,只是简写为IP。在讨论因特网协议版本6的那些章节中,如第12章IPv6的移动性,或在可能存在混淆的情况下,我们会清楚地标明采用的版本号,如IPv4或IPv6。

1.7 如何得到RFC文件或因特网草案

本书经常参考RFC(Request For Comments)文件,RFC包括一些官方的因特网标准协议和其他许多有趣的东西,这些RFC文件可以通过多种途径得到。

能连接到World Wide Web上的读者,可以在Web浏览器上输入下面的地址得到RFC文件:
`ftp://ds.internic.net/rfc/rfcNNNN.txt`。这里的NNNN表示想要的RFC的文件号,例如,[RFC2002]可以从以下地址检索到:`ftp://ds.internic.net/rfc/rfc2002.txt`。有一个文件特别有用,它是所有已发表的RFC文件的“索引”,这个文件可以从以下地址得到:
`ftp://ds.internic.net/rfc/rfc-index.txt`。

类似地,因特网草案(这是因特网工程任务的各个工作小组产生的各种原始文档)可以从以

下地址得到: <ftp://ds.internic.net/internet-drafts/document-name>, 其中, document-name是你想要的草案的文件名。例如, [draft-ietf-mobileip-firewall-trav-00.txt]可以从以下地址检索到:
<ftp://ds.internic.net/internet-drafts/draft-ietf-mobileip-firewall-trav-00.txt>。

另外, RFC文件和Internet草案还可以通过E-mail得到, 只需简单地给下面地址发一个邮件就可以: mailserv@ds.internic.net。邮件的主题栏为空, 邮件内容包括“FILE filename”, 其中filename是你想要的文件名字。例如, 上面所说的两个文件可以用下面的邮件得到:

To: mailserv@ds.internic.net

Subject:

FILE /rfc/rfc2002.txt

FILE /internet-drafts/draft-ietf-mobileip-firewall-trav-00.txt

因特网草案在被修订后的六个月内你还可以得到它。经过修订后, 它要么成为RFC文件, 要么就被删除了。本书或其他书的参考文献中列出的因特网草案都应被看作是正在处理中的。列出这类参考文献只是为了让有兴趣也有条件的读者得到更多的信息, 并不意味着它们会被发表为因特网标准。

由于因特网草案常常产生又被删除, 往往没有正式公布, 本书参考的文献也可能会过期, 因此可以访问一下有关本书的站点 <http://www.prenhall.com/solomon>, 从那里你可以发现那些过期的草案。

最后从 <http://www.ietf.org/> 可以得到有关因特网工作组的更多信息, 移动IP工作组的情况则在: <http://www.ietf.org/html.charters/mobileip-charter.html>, 那里有该工作组的RFC文件和因特网草案。

1.8 本书其他部分的组织结构

本书由以下四个部分组成:

1) 第一部分是全书的导论。第1章表明了本书的目的、面对的读者群和阅读本书所需的背景知识。第2章为那些对计算机连网协议、因特网网上信息传送的方法不熟悉的人们提供了一个教程。在这一章中, 我们详细地描述了IP路由技术, 因为移动IP的最主要目的就是为了克服IP的缺点。最后, 第3章解释了为什么需要像移动IP这样的技术, 为什么目前那些解决因特网中移动通信问题的方法都不令人满意。

2) 第二部分极详细地介绍了移动IP本身。第4章通过定义移动IP所解决的问题和解决方法的应用范围, 给出了移动IP的概况。第4章还定义了移动IP用到的一些术语及其高层操作。第5章中描述了移动IP的三个部件: 代理搜索、注册、路由技术。第6章提供了有关隧道技术的细节, 这是移动IP中将数据包路由到移动计算机上所用的技术。

3) 第三部分介绍了在各种情形中如何应用移动IP以及应用它的好处, 并且详细研究了在各种应用中的安全策略。第7章为那些不熟悉计算机安全或加密技术的人提供了一条安全原则。第8章展示了在一个园区网中采用移动IP的简单例子, 在这一章中, 为使事情简单化, 忽略了防火墙和与因特网的连接。第9章将防火墙加了进去, 使得问题变得更复杂也更有意思了, 这里讨论了移动IP中如何穿越安全防火墙。第10章从商业服务提供商提供业务的角度来描述移动IP, 并讲述了一些服务提供商特别关注的问题: 在第8章和第9章中已经介绍过的对用户的威胁。第11章展示了两个移动IP的高级应用。首先, 描述了移动IP对多协议的支持(如

AppleTalk), 而不是仅仅支持IP。其次, 第11章说明了移动IP如何为整个移动网络提供连接, 而不仅仅是为一台移动计算机。第11章的最后描述了一个对终端用户来说不可见但却非常重要的移动IP应用。

4) 第四部分介绍了移动IP将来的发展。第12章详尽描述移动IPv6的细节, 它为下一个版本的因特网协议提供了可移动性。然后, 在第13章中, 讲述了移动IP面对三个主要问题: TCP的性能、对实时业务的支持(如音频和视频)和服务定位。第14章总结了全书的要点, 并向读者描述了一个广泛采用移动IP的世界的情景, 以及在那个世界中我们可以做的一些事情。

第2章 计算机网络教程

本章讨论计算机通信的特点和机制。首先介绍OSI参考模型，并将其与因特网通信模型进行对比。接下来考察一下路由技术的概念和因特网在各个子网间传送信息的原理。这些练习是为后面的章节作准备的。在那些章节中，我们将看到为什么在因特网的选路体系中需要移动IP这样的技术。

不管怎样，本章不可能完整论述计算机通信，要想更全面地了解这方面的技术可以参阅[Tane96]，[Come95]或[Stev94]。如果你已经对计算机连网和IP路由技术有了基本了解，就可以跳过本章直接转入下一章。

2.1 计算机是如何进行通信的

计算机通过在网络上发送和接收数字信息进行通信，这些信息包括二进制数字，称为比特，它们的取值只能是0或1。比特被分为8个一组，称为字节，多个字节又捆扎在一起构成帧或数据包，在后面我们还将对数据包作更详细的描述。

两台计算机交换数据包之前，它们首先必须通过某种物理媒介连接起来，例如铜线、光纤或者电磁波。在少数情况下，两台计算机由同一段不中断的物理线路或无线链路直接连接，这时，它们也就可以直接互相发送数据包了。但是在大多数情况下，计算机发出的数据包通常要经过一个或者多个中间交换设备才能到达它们的目的地。

在实际环境中，两台计算机互相通信可能会变得非常困难，尤其是在它们使用不同的硬件、不同的操作系统、不同的应用软件时。要使两台计算机能互相通信必须解决下面的问题：

- 1) 计算机互相通信的速率以及使用什么样的物理媒介？
- 2) 如果使用的通信媒介是多台计算机共享的，如何决定在某一个时刻该由哪台计算机发送数据包？
- 3) 如何对计算机进行编址，以便唯一地区分开每个数据包的发送者和接收者？
- 4) 如果两台计算机不是直连在一起的，数据包如何选出一条从起点到目的地的合适通路？
- 5) 如何检测通信过程中的错误，检测到错误后又如何去校正错误？
- 6) 通信过程中使用什么数字格式来表示数据？

计算机科学中研究上述这些问题的分支通常称为计算机连网技术，或者简单称为连网技术。由于同时解决上述所有问题非常困难，计算机科学家们将它们分解成可以分别独立解决的若干子问题，每个子问题就构成了通信中的一个层，每个层由严格限定的一组原则和规程来定义。

2.1.1 协议层

图2-1所示为国际标准化组织ISO (International Organization for Standardization) 为计算

机连网所定义的开放系统互连模型OSI (Open System Interconnection)。七层中的每一层都完成一组特定的功能,从而为上一层提供一定的服务。规定各层如何操作的那些原则和规程就称为协议。

从理论上来说,这个模型中每一层的协议都与它的上层或下层的协议无关。这使得每一层可以独立地采用新技术,而不影响其他层,只要这些新技术提供的服务不少于原来的协议就可以了。这只是理论上的情况,从本书后面的章节中我们可以看出,考虑到效率等因素,各层之间多多少少有些关联。

2.1.2 每一层的功能

图2-1所示各层的功能如下:

1. 物理层

它通过通信设施或媒介把比特流从一个地方传到另一个地方。物理层协议定义了传输媒介的电气和机械特性,如比特率、电平等等。

2. 数据链路层

这一层利用物理层提供的比特传送功能,在同一条链路的相邻两台计算机之间传送数据帧。一个帧由网络层数据包加上一个较短的数据链路层帧头构成。数据链路层协议确保数据帧的可靠传送,并在多台计算机共享同一个媒介的情况下,在各台计算机之间作出访问媒介的仲裁。

3. 网络层

这一层利用数据链路层提供的帧传送功能,在通信的源和目的之间传送数据包(可能需要经过一条或多条中间链路)。数据包由高层数据加上一个较短的网络层报头构成。网络层协议规定了一台网络设备如何才能找到网络中的另一台网络设备,并规定了如何选择路由将数据包送到它的目的地。

4. 传输层

传输层使得网络层提供的端到端的包传送功能是可靠的。送入传输层,并通过可靠的端到端传输功能到达对端,然后从对端传输层送出的数据称为数据流。传输层将数据流分批传送,传输层每一次能传送的一段数据称为数据段,由高层协议数据加上一个较短的传输层报头构成。因此,一个数据段构成了网络层数据包的净负荷。传输层协议规定了检错和纠错方法。

5. 会话层

会话层接收从传输层送来的可靠的数据流,并向高层提供丰富的、面向应用的服务。例如,有的会话层提供周期性的检测点,使得网络发生灾难性的故障后通信仍能恢复,当通过不可靠的网络来传送一个大文件时,这种功能是非常有用的。由于网络故障,在文件的绝大部分已经传送完时,又不得不从头开始传送,这是对网络资源的极大浪费。

6. 表示层

这一层定义了在一个应用中互相交换的信息的语义和语法,也就是说,表示层定义了某个应用中的整数、文本消息和其他数据是如何进行编码和通过网络传送的,这使得无论它们各自存储数据的方式是否不同,使用不同硬件和操作系统的计算机之间都可以交换信息。

7. 应用层