HZ BOOKS

IP网络技术丛书

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

IP网络技术丛书

移动 IP

(美) James D.Solomon 著

裘晓峰等 译

机械工业出版社
China Machine Press

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。

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

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连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

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，这些邮件就可能会暂时丢失。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，那些只想了解移动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-mbileip-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趣了，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面对的三个主要问题：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，并向高层提供非富的、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

这一层传送用户运行的某个计算机程序的特定信息。有的应用层协议定义如何交换电子邮件（E-mail），有的应用层协议定义计算机之间如何传送文件，有的则定义Web客户（浏览器）如何从Web服务器上取下Word Wide Web页面。

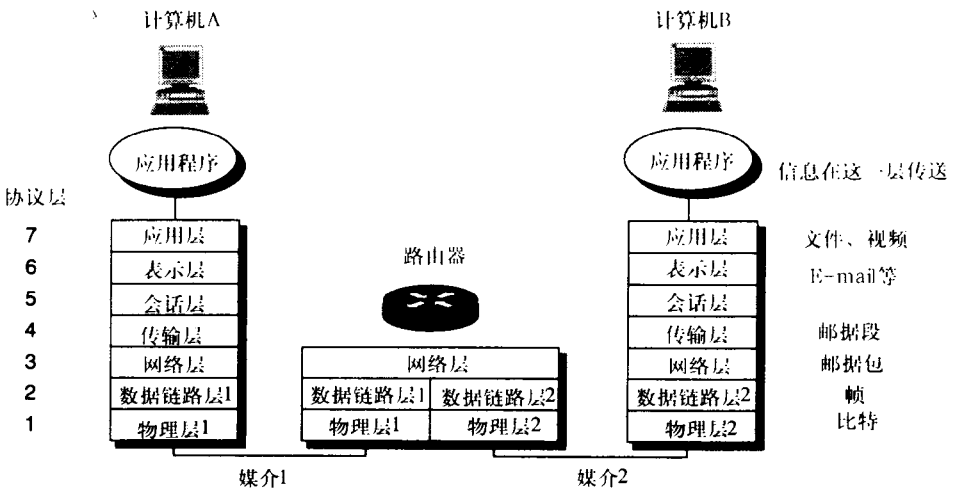

图2-1　OSI参考模型

实现一个协议的一部分硬件或软件称为协议实体，计算机的同层协议实体之间利用低几层提供的服务通过网络传送信息。从逻辑上看，我们可以认为一台计算机的协议实体和另一台计算机的同层协议实体之间直接进行对话。两个可以通过网络互相通信的协议实体称为对等实体。

例如在图2-1中，从逻辑上讲，计算机A的网络层与路由器的网络层进行通信，为了完成这个通信，网络层利用数据链路层1通过媒介1传送数据包，因此计算机A的网络层实体和路由器的网络层实体是对等实体。

典型的情况下，各层协议从高层接收数据，并通过在前面加上一个较短的报头来实现本层协议的功能，然后将加了报头的信息传给网络另一端的同等实体。加上的报头告诉同等实体对接收到的数据做什么处理，这个报头可能包括协议地址、数据部分的长度以及用于检错和纠错的校验和。同等实体接收到信息后，剥去协议头，恢复出原始数据再送给高层。

最后还有一个术语，如图2-1中所示，从低到高的一系列协议常称为一个协议栈。当各层被具体的协议所代替时（如网络层协议采用因特网协议IP），我们就称这一系列具体的协议为一个协议簇。例如，Internet协议栈各层所采用的协议统称为TCP/IP协议簇。

2.1.3　本书关系到哪些协议层

本书主要关系到网络层协议，以及将数据包从源计算机传到目的端所需的各种技术。然而，如前所述，为了传送数据包，网络层依赖于数据链路层提供的服务，因此，本书还将讨论各种链路的一些重要特性，以及它们对传输层协议产生的影响。想更多地了解其他各层协议的读者可以参阅[Tane96]。

2.1.4 网络层提供的服务

网络层的目的是隐藏各种链路的具体特性，向传输层提供一个逻辑上的网络，它将数据包通过一条或多条链路从源计算机传送到目的计算机。一个数据包包括从传输层送来的数据段和网络层的协议头。因此，从传输层向下看网络层时，看到的是一种将数据段从源端传送到目的地的服务。

1. 节点

一个网络设备就是一个节点。为完成网络层的功能，网络层协议为每个网络设备分配一个或多个逻辑地址。所谓逻辑地址，是指与节点的物理地址无关。有时，为实现一个数据链路或物理层协议，我们需要物理地址（如以太网地址）。

如图2-2所示，网络层定义的网络设备（或节点）有两类：

1) 主机　包括PC机、工作站、主机、文件服务器以及其他各种计算机。

2) 路由器　它在主机和其他路由器之间转发数据包，使得主机不必和通信所用的链路直接相连。

转发是路由器将接收到的数据包又发送出去的过程，目的是为了使数据包离它的目的地更近一些。

2. 路由

路由器之间通过路由协议交换信息，以报告它们各自所连接的网络和主机每个路由器都建立有一张路由表。路由器利用路由表为各个数据包选择从源端到目的地的路径。

3. 逐跳和端到端

如图2-2所示，在任意两台主机之间的路径上可能有多台路由器，每台路由器只负责决定应将数据包转发到哪一台主机或路由器上（即下一跳），以使它能到达目的地。这种方法称为逐跳的路由选择，以区别于那些在数据包发送之前就决定好整条路径的技术。

回到图2-1，我们可以发现只有协议栈的高层，即从传输层到应用层，才采用端到端的协议。也就是说，这些层的协议实体只存在于通信的源和目的主机上，比如说图2-1所示的两台计算机。协议栈的低层，即从物理层到数据链路层，则采用逐跳的方法，这几层的协议实体只和同一条链路上与它相邻的下一个对等实体通信。

网络层则同时具有端到端和逐跳协议的特性。一方面，网络层的数据包由一个端点产生并传送到另一个端点，这是端到端协议的特性；另一方面，两端点间沿途的各台路由器都要检查数据包，这使网络层协议又有了逐跳协议的特性。

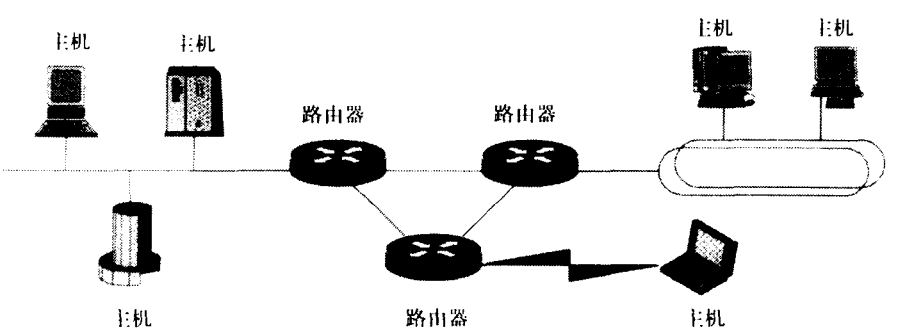

图2-2　网络实体：主机和路由器

4. 路由器和网桥

最后，为严格起见，本书将路由器定义为运行在网络层的设备。也就是说，路由器根据数据包中的网络层协议头转发数据包。网桥则运行在数据链路层，即网桥按照数据包的数据链路层头对数据链路层帧进行中继。

如图2-3所示，对网络层来说网桥是不可见的，比如，主机1和路由器上的网络层软件对于它们之间有一台网桥一无所知，对它们来说，经过桥接的媒介只是一条链路。网桥将数据帧从一个物理段中继到另一个物理段上，并使主机1和路由器相信它们是直连的。

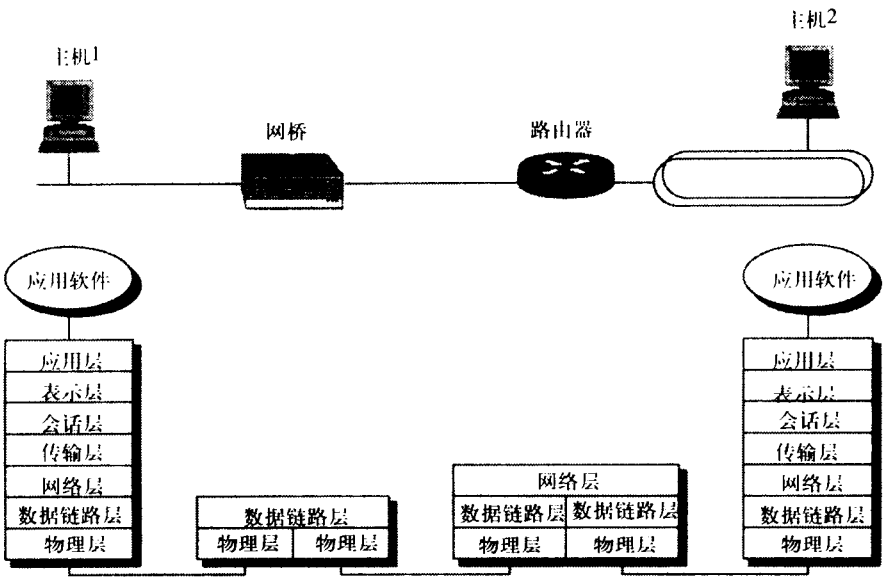

图2-3　网桥、路由器和主机

2.2　因特网协议（IP）

TCP/IP协议簇所体现的因特网通信模型与OSI模型有相似之处，但又有些不同。因特网通常将OSI模型中的高三层合并成一个应用层，但就本书而言，这两种模型可以看作是一样的。

因特网网络层协议称为因特网协议（IP）[RFC 791]。第4层，即传输层，因特网中有两种广泛采用的协议：传输控制协议（TCP）[RFC 793]，它为高层提供可靠的、面向数据流的服务；而用户数据报协议（UDP）[RFC 768]则为高层提供没有可靠性保证的、无连接的服务。因特网的网络协议（IP）和有可靠性保证的传输层协议（TCP）一起构成了因特网协议簇的名称。

2.2.1　ICMP

ICMP（Internet Control Message Protocol）(RFC 792)网间网控制报文协议定义了一套差错报文和控制报文，用来表示数据包传输过程中发生了错误，另外还有一些ICMP报文为节点提供诊断信息。实现IP的节点必须实现ICMP，以保证于因特网标准兼容。因此，当我

们谈到IP时，就表示也同时包括ICMP。图2-4表明了TCP/IP参考模型以及各种因特网协议间的关系。

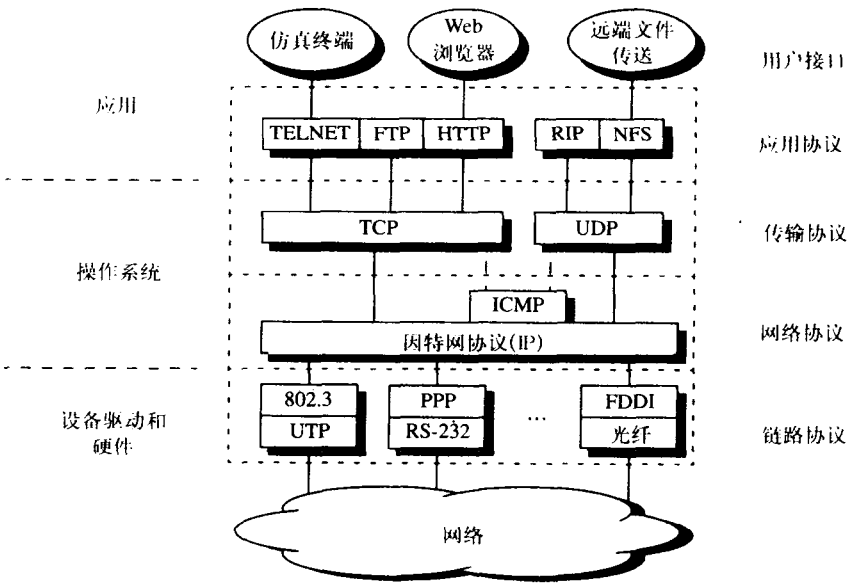

图2-4 因特网（TCP/IP）参考模型

2.2.2 IP的功能

和其他所有的网络层协议一样，IP将数据包从源端发送到目的端点，这种业务有时也称为“端到端的包传送”。IP所提供的可靠性服务称为“尽力而为”，也就是说IP将尽力将数据包传送到目的端，但并不保证它一定能无差错地到达目的端。

简而言之，IP和高层达成的服务协定如下：“IP将尽力把带有数据的包送到目的地，最终可能会有一个或多个数据包的拷贝到达目的端。数据包也可能会丢失，而且到达的每一个拷贝都可能有错误。如果你觉得这种服务质量不可接受，就请自己想办法来保证一定有一个正确的数据包到达目的端。”

因此，如果一个应用要求可靠通信，就应由传输层来保证无差错的端到端传输。在因特网中，传输控制协议(TCP）提供了可靠的端到端的数据传送。

2.2.3 IP包格式

IP包包括从传输屋或更高层送来的一段数据，以及加在数据前面的一个IP报头。[RFC791]中定义的IP报头包括图2-5中所示的各个域，其中最主要的域是源地址和目的地址。这些地址的作用和邮政系统中信封上的地址作用相似，表明了发送者和接收者的地址。

1. IP地址

IP地址是一个32比特（4字节）的数。每一个节点的每个网络端口都有一个IP地址，端口是节点与链路的硬件和软件连接点，像路由器那样具有多个网络端口的节点也就有多个IP地址，每个端口一个地址。

(1) 带点的十进制标识法

IP地址常被写成由点分开的十进制数，4字节中的每个字节写成一个十进制数，中间用点分隔开。例如，一个IP地址用十六进制表示为 C0 13 F1 12，用带点的十进制标识法表示时就成为192.19.241.18，因为 $C0_{(hex)}=192_{(dec)}$，$13_{(hex)}=19_{(dec)}$，$F1_{(hex)}=241_{(dec)}$，$12_{(hex)}=18_{(dec)}$。

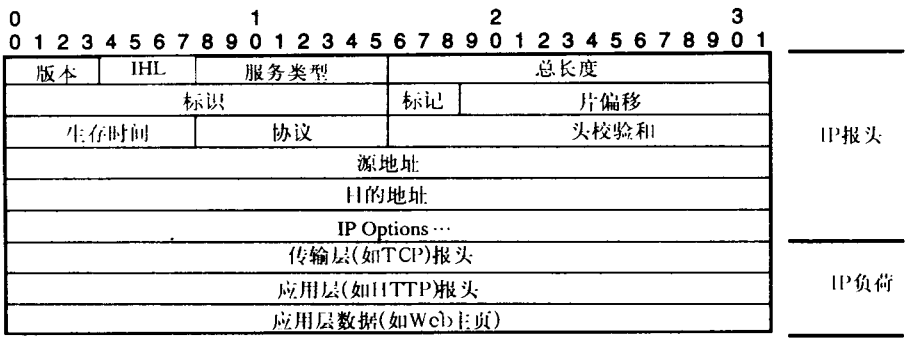

图2-5　IP包：报头和净荷

(2) 网络前缀和主机部分

如图2-6所示，IP地址有两个部分：网络前缀部分和主机部分。网络地址是一串连续的比特，连在同一条链路上的所有节点有相同的网络前缀，因此要求这些节点的IP地址具有唯一的、不同的主机部分。你可以把网络前缀看成是用来标识一条链路的，而主机部分是用来标识连接在链路上的一台特定主机或路由器的。

这条原则并不是一成不变的，虽然通常给每一条链路分配一个网络前缀，但并不排除给一条链路分配多个网络前缀。这时，可以把一条物理链路看成包含多条虚拟链路，而每一条虚拟链路都分配了一个网络前缀，这样我们就可以认为一个网络前缀只对应于一条链路（物理的或虚拟的）。在本书中，忽略了一条链路有多个网络前缀的情况，而假设每条链路只有一个网络前缀，这种假设并不会失去普遍性。

为了更清楚地表示网络前缀的概念，来看一下IP地址“129.61.18.26”。我们被告知网络前缀的长度为24比特（3字节），这时 p = 24，h = 8，因此网络前缀为“129.61.18”，主机部分为“26”。

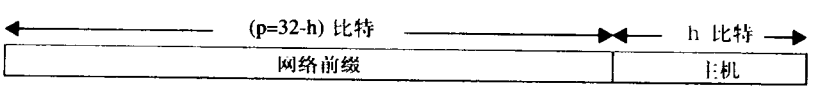

图2-6　IP地址格式

(3) 前缀长度

前缀长度指明了一个IP地址网络前缀部分的比特数，因此IP地址主机部分的比特数为：32 - 前缀长度。仍以上一个例子来看，129.61.18.26的前缀长度为24比特。另一种IP地址及其前缀长度的简写方式为：地址/前缀长度，在这个例子中就写成129.61.18.2/24。

2. IP报头的其他域

版本域（Version）表明了一个数据包采用的是因特网协议的哪个版本。对于IPv4，这个域的值为4。将来对于其他版本的因特网协议这个域也会随版本号增加。IHL（Internet

Header Length）域表示以32比特（4字节）为计数单位的IP报头的长度，因此，IHL的最小值为5，即20字节，这是一个不带IP可选项的IP报头。

服务类型（Type of Service）域决定了IP包在提供多种服务质量（如最小时延、高可靠性）的网络中将受到何种处理。总长度（Total Length）域则给出了整个IP包的字节数，包括IP报头本身的长度。

标记（Flag）域和片偏移（Fragment Offset）用于将大IP包分割成几个称为片的小块，以保证它可以顺利地穿过无力处理大IP包的网络。标识（Identification）域是发送端填写的值，以便接收端重组那些不得不分成几个片的包。

生存时间TTL（Time to Live）用于限制一个IP包的转发时间。想想看，当第一台路由器认为到达某一目的端的路径要经过第二台路由器，而第二台路由器又认为该路径应经过第一台路由器，这时会发生什么情况呢？当第一台路由器接收到一个发往该目的地址的数据包时，它会将数据包转发给第二台路由器，而第二台路由器就会将数据包重新转发给第一台路由器，然后第一台路由器又将包转发回第二台路由器。如果没有TTL，这个包就会在这两台路由器构成的环中永远转下去。这样的环在大的网络中经常会出现。

协议类型（Protocol）被IP层用来区分IP包中的负荷是由哪个高层协议产生的。当接收到一个IP包时，这个域使得接收节点上的IP软件可以将IP包送给相应的高层协议处理。例如，这个域取值为1表示ICMP，6表示TCP，17表示UDP。

头校验和（Header Checksum）被接收节点用来确认接收到的IP报头中有没有差错。头校验和只由IP报头中的各个域计算得来，而与IP包的净荷无关，IP包净荷的校验则是高层协议的工作。

3. IP选项

在上面介绍的各固定长度的域之后，IP报头中有时还有多个可选项。虽然可选项可以用来实现一些非常有趣的功能，但实际上还是很少用到它。在后面我们将介绍一种可选项“Loose Source and Record Route”，其他的可选项包括安全、与时间有关的数据、各种诊断功能等。

2.2.4 节点如何得到一个IP地址

节点可以通过手工和自动两种方法得到它们的IP地址。手工配置的方法在企业网中比较通用。在这种网络中，一个网络管理员负责为整个网络中所有主机和路由器分配IP地址，手工配置时通常只是将IP地址（或下面章节中将介绍的其他参数）输入到节点的配置文件中，或像在许多个人计算机上能看到的那样，输入到用户端口配置界面的某一个域中。

自动配置IP地址通常有两种方法。第一种方法是，用户用调制解调器、电话线和家用个人计算机拨到ISP（Internet Service Provider）上，这时PC机会在点到点协议PPP（Point- to-Point Protocol）[RFC 1332]的IPCP（IP Control Protocol）[RFC 1661]阶段向ISP的拨入设备请求一个IP地址。另一种方法是采用动态主机配置协议DHCP（Dynamic Host Configuration Protocol）[RFC 2131]。在大型的企业网或园区网中常可以看到DHCP，这些网络有许多节点而且网络速率比较快。在DHCP中，节点可以向DHCP服务器发出请求，要求它暂时分配一个IP地址。DHCP可以和BOOTP（Bootstrap Protocol）[RFC 951]同时使用。BOOTP也是用于动态IP地址分配的，目前在许多地方仍然用它。