移动IP穿越网络防火墙实证研究

YIDONG IP CHUANYUE WANGLUO FANGHUOQIANG SHIZHENG YANJIU

王育欣◎著

航空工业出版社

移动IP穿越网络防火墙实证研究

王育欣 著

航空工业出版社

北京

内 容 提 要

本章提出了利用 IPSEC 技术保护移动 IP 穿越防火墙的方案。全书共分 6 个部分，包括：① 绪论，简要说明了移动 IP 的相关概念和工作原理，以及在应用中出现的问题；② 移动 IP 穿越防火墙问题分析；③ IPSEC 技术应用于移动 IP 穿越；④ 移运 IP 穿越防火墙方案的设计；⑤ 实现具有 IPSEC 保护的移动 IP 穿越防火墙；⑥ 结论，对前面所讲解的内容进行了总结。

图书在版编目（CIP）数据

移动 IP 穿越网络防火墙实证研究 / 王育欣著. -- 北京 : 航空工业出版社，2014.6
ISBN 978-7-5165-0492-5

Ⅰ. ①移… Ⅱ. ①王… Ⅲ. ①移动通信－通信协议－研究 Ⅳ. ①TN915.04

中国版本图书馆 CIP 数据核字(2014)第 124733 号

移动 IP 穿越网络防火墙实证研究
Yidong IP Chuanyue Wangluo Fanghuoqiang Shizheng Yanjiu

航空工业出版社出版发行
（北京市朝阳区北苑 2 号院 100012）
发行部电话：010-84934379 010-84936353
北京忠信印刷有限责任公司印刷 全国各地新华书店经售
2014 年 6 月第 1 版 2014 年 6 月第 1 次印刷
开本：787×1092 1/16 印张：6.25 字数：144 千字
印数：1－2000 定价：35.00 元

随着移动通信技术和因特网技术的不断发展，两种技术互相融合产生了移动 IP 技术。移动 IP 虽然有很广泛的发展前景，但还没有充分地得到应用，很重要的原因就是移动 IP 在应用中遇到了问题。其中之一就是移动 IP 在穿越防火墙时防火墙阻断了移动 IP 隧道，这不仅给移动 IP 带来了难题，也给网络的安全性造成了很大的威胁。为了实现移动 IP 穿越防火墙的同时又保证网络的安全性，本书提出了利用 IPSEC 技术保护移动 IP 穿越防火墙的方案。

本书首先分析了移动 IP 穿越防火墙的问题和目前解决方法的不足，分析了 IPSEC 应用于移动 IP 的优势，并根据移动 IP 穿越防火墙三种不同的情况对该方案进行了详细设计，最后在 Linux 上模拟实现了移动 IP 穿越防火墙的方案。

本书主要内容如下：

第一章主要介绍移动 IP 的技术和它的原理机制，以及移动 IP 的特性和实体，然后给出了移动 IP 难以大规模应用的原因。

第二章首先介绍防火墙的概念，然后引入移动 IP 穿越防火墙的问题，介绍了反向隧道穿越防火墙的方法，但是这种方法同时存在移动 IP 穿越时的安全问题，接着给出了 SKIP 穿越防火墙的方案并分析了 SKIP 方案的优缺点，引出了基于 IPSEC 的思想。

第三章主要介绍了如何把 IPSEC 技术应用于移动 IP 穿越防火墙方案中，分析了 IPSEC 技术的具体细节，研究了移动 IP 穿越防火墙的安全问题，指出了应用 IPSEC 技术的优势。首先设计了 IPSEC 技术和移动 IP 技术的结合方案，然后结合 IPSEC 技术和防火墙技术为实现穿越设计了一个安全的平台。

第四章主要基于应用 IPSEC 的思想，详细设计了移动 IP 穿越防火墙的方案。分析了移动 IP 穿越防火墙的环境，根据移动节点在无外地代理，移动节点利用同一安全体系的外地代理和移动节点利用不在同一安全体系的外地代理的三种不同的情况分别设计了移动 IP 穿越防火墙的方法。最后给出了移动 IP 穿越防火墙方案的优点和不足，以及有待解决的问题。

第五章在 Linux 上模拟移动节点穿越防火墙的方案。首先分析了 Linux 防火墙实现的技术基础——Netfilter HOOK 机制，给出了 IPSEC 防火墙在 Linux 上的实现，通过对防

火墙规则的静态的修改实现了 IPSEC 数据包穿越 IPSEC 防火墙；然后在实验室条件下模拟了移动节点利用同一安全体系的外地代理与家乡代理通信情况下的注册过程，并且在此过程中实现了防火墙规则的动态修改。在此基础上实现了具有 IPSEC 保护的移动 IP 穿越防火墙的过程；最后对具有 IPSEC 保护的移动 IP 数据包的传输效率进行了测试与分析。

著　者

2014 年 5 月

目　录

1 绪 论

1.1 移动 IP 的出现

人类通信的最高目标是个人通信，就是利用各种可能的网络技术，实现任何人在任何时间、任何地点与任何人进行任何种类的信息交换。随着社会的不断前进，Internet 现已深入到社会的各个层面，笔记本电脑以及其他便携式电脑的功能已经越来越强大、携带越来越方便，移动通信技术也得到飞速发展，人们利用便携电脑为终端，以移动通信技术来支持用户在任意移动的环境中，通过 Internet 实现与他人的各类信息交换已经成为可能。移动 IP 技术已经成为实现个人通信这一人类通信最高目标的最佳技术方案。

在当今的信息社会中，移动通信技术和 Internet 技术迅猛发展。几乎最新的信息、通信、电子、计算机方面的一切新技术，无不为这两大支柱产业所吸收和采纳。它们有着前途美好的未来。移动 IP 不是移动通信技术与 Internet 技术的简单叠加，也不是无线话音和无线数据的简单叠加，它是移动通信和 IP 的深层融合。移动 IP 技术综合了这两种技术，具有广泛的发展前景。

使用传统 IP 技术的主机使用固定的 IP 地址和 TCP 端口号进行相互通信，在通信期间，它们的 IP 地址和 TCP 端口号必须保持不变，否则 IP 主机之间的通信将无法继续。而移动 IP 的基本问题是 IP 主机在通信期间可能需要在网路上移动，它的 IP 地址也许经常会发生变化，而 IP 地址的变化最终会导致通信的中断。

如何解决因节点移动（即 IP 地址的变化）而导致通信中断的问题？蜂窝移动电话提供了一个非常好的解决问题的先例。因此，解决移动 IP 问题的基本思路与处理蜂窝移动电话呼叫相似，都使用了漫游、位置登记、隧道、鉴权等技术，从而使移动节点使用固定不变的 IP 地址，一次登录即可实现在任意位置（包括移动节点从一个 IP 子网漫游到另一个 IP 子网时）上保持与 IP 主机的单一链路层连接，使通信持续进行。

在移动 IP 之前的网络模式 TCP/IP 中并没有提供主机的移动性。它是为固定环境设计的，而这些使得移动性难以实现，因为原有的 IP 路由体系有一个重要的规则：路由选择只依据目的 IP 地址的网络部分，而不是整个 IP 地址，即路由是针对网络的。一台主机的 IP 地址包括网络前缀，如果把主机的位置从原来的网络移动到新的网络中，将意味着它的 IP 地址不能反映它的当前位置，由此引发的后果就是现有的 IP 路由体系不能把报文

投递给该主机。在这种情况下，主机必须配置一个新的属于当前子网的 IP 地址来反映它的新位置。对于 TCP/IP 连接来说，有四个元素来唯一地标识它：源 IP 地址、目的 IP 地址、TCP 源端口号、TCP 目的端口号，改变其中任何一个都会导致 TCP/IP 连接的中断或丢失。因此，要保持移动主机移动时传输层的连接，必须保持 IP 地址不变。这两种情况是互相矛盾的，那么，如何为主机配置一个新的 IP 地址又不中断 TCP/IP 连接呢？为此，IETF 提出了移动 IP 技术。

移动 IP 技术分两种形式，一种与无线蜂窝系统类似，移动主机不断变换自己的位置；另一种是本书重点研究的，移动主机在某一个位置固定停留一段时间，而不是频繁地更换自己的位置。

移动 IP 技术的发展过程大致如下：

第一步 IP 业务与移动通信结合，在电路交换的移动通信网络中引入 IP 电话业务。

IP 电话是一种新的电话业务，是在 IP 网络承载话音技术创新的产物。它把话音进行压缩编码，打包分组，路由分配，存储交换，解包解压缩等变换处理，在 IP 网络上实现话音通信。因为它的分组特性有效地利用了网络资源，降低了话音传输的成本，所以与传统电话相比有成本价格上的优势。在固定网中，IP 电话业务正在崛起。基于成本上的考虑，在移动网络中引入 IP 电话业务也是颇有发展前景的新业务。在我国，GSM 移动网络中引入 IP 电话是用户关注的新业务，也是运营商需要解决的技术问题。

第二步 GSM 网络中引入 IP 分组数据业务—GPRS，GPRS 是移动通信网络向分组化发展的一个里程碑。GPRS 是一个从空中接口到地面接入网再到核心网络部分都分组化的数据通信网络。GPRS 的分组化实质，使得空中接口频谱利用率与地面接入网带宽利用效率都得到极大的提高。同时诞生了“按流量计费”这种更加合理的资费政策，使得运营商可以宣称：让用户 24 小时在线，只有点击的时候才计费。GPRS 扫除了阻碍无线互联网应用得到普及在技术和成本两方面的障碍，必将加快移动互联网应用的普及和推广。GPRS 的骨干网将借助于 IP 网络和互联网络实现无缝互通互联。对用户来说，移动终端使得原先需要庞大昂贵的 PC 才能使用的互联网以一种更为简单便捷、亲切易用和廉价实用的方式出现，也更加易于为广大普通用户所接受。移动性将大大促进互联网应用的普及。可以大胆地预言，互联网和移动通信的结合，会使得以前曲高和寡的数据业务以廉价实用的方式进入寻常百姓家。

接下来，第三代移动通信网络的发展方向将是一个全 IP 的分组网络。第三代移动通信的发展是在固定网络向宽带电信级 IP 网络发展的大背景下进行的。第三代移动通信的核心网络将采用宽带 IP 网络。在此 IP 网上，承载着从实时话音、视频到 Web 浏览、电子商务等多种业务，是电信级的多业务统一网络。宽带的 IP 网络将是分层的：物理承载可以是 IP over DWDM、IP over SDH、IP over ATM 等多种方式，IP 协议是主导的网络路由与寻址协议，网络控制由 Call Server 服务器实现，而网上的业务则由众多的第三方智能业

务提供商提供。实现了传输网络、网络控制、业务提供的分离。相对于传统网络，全部分组网络的安全性、业务质量保证、新业务提供的便利性、业务种类的丰富性以及开放系统带来的广阔商机都是传统网络无法达到的。

第三代移动网络发展的初期将继承现有移动网络的基础设施，如移动交换机（MSC/VLR），归属位置登记（HLR）数据库等；在业务发展初期，电路型业务如话音，电路型多媒体业务将仍然由 MSC 网络承载，而分组数据业务将由 GSN 分组交换机承载，形成电路和分组两套网络并存的局面。但随着分组业务量的急剧增长和 IP 技术的完全成熟，所有的业务将会统一到 IP 网络，形成一个真正的综合业务网络。

1.2 移动 IP 的特性及实体

1.2.1 移动 IP 的特性及重要名词

移动IP包括以下几个特性：

（1）透明性。对于应用程序和传输层协议以及变动中涉及不到的路由器，移动性是透明的[1]。

（2）与 IPV4 的可互操作性。使用移动 IP 的主机可以与运行常规的 IPV4 的软件的固定主机进行互操作。

（3）宏移动性。移动 IP 重点关注持续时间较长的移动的问题。对于带着便携式计算机进行商业旅行，并把计算机连接到这个位置达一周的用户来说，移动 IP 十分适用。

移动 IP 如果要保持 TCP/IP 的连接，那么原来的 IP 地址不能改变。如果要为数据包找到新的地址又必须按照新的 IP 地址进行路由，IETF 把这两种地址都保留了下来。第一个地址就是计算机的主地址，它是永久的、固定的。这是应用层和传输层所用的地址，如此一来，TCP/IP 连接就不会中断了。第二个地址是临时地址，它是随着计算机的移动而改变，它的任务是找到主机的最新的移动地址。

移动 IP 的重要名词：

归属代理（Home Agent）：一个在移动节点归属网上的路由器，它至少有一个接口在归属网上，当移动节点离开归属网时，它通过“IP 通道（IP Tunnel）”把数据包传给移动节点，并且负责维护移动节点的当前位置信息。

外区代理（Foreign Agent）：移动节点当前所在网络上的路由器，它向已登记的移动节点提供选路服务。当使用外区代理转交地址时，外区代理负责解除原始数据包的隧道封装，取出原始数据包，并将其转发到该移动节点。对于那些由移动节点发出的数据包而言，外区代理可作为已登记的移动节点的缺省路由器使用。

归属地址（Home Address）：这是用来识别端到端连接的静态地址，也是移动节点与归属网连接时使用的地址。不管移动节点连至网络何处，其归属地址保持不变。

转交地址（Care of Address）：转交地址即隧道终点地址。它可能是外区代理转交地址，也可能是驻留本地的转交地址。外区代表转交地址是外区代理的一个地址，移动节点利用它进行登记。在这种地址模式中，外区代理就是隧道的终点，它接收隧道数据包，解除数据包的隧道封装，然后将原始数据包发到移动节点。由于这种地址模式可使很多移动节点共享同一个转交地址，而且不对有限的 IPv4 地址空间提出不必要的要求。所以这种地址模式被优先使用。驻留本地的转交地址是一个临时分配给移动节点的地址。它由外部获得（如通过 DHCP），移动节点将其与自身的一个网络接口相关联。当使用这种地址模式时，移动节点自身就是隧道的终点，执行解除隧道功能，取出原始数据包。一个驻留本地的转交地址仅能被一个移动节点使用。转交地址是仅供数据包选路使用的动态地址，也是移动节点与外区网连接时使用的临时地址。每当移动节点接入到一个新的网络，转交地址就发生变化。

位置登记（Registration）：移动节点必须将其位置信息向其归属代理进行登记，以便被找到。在移动 IP 技术中，依不同的网络连接方式，有两种不同的登记规程。一种是通过外区代理进行登记。即移动节点向外区代理发送登记请求报文，外区代理接收并处理登记请求报文，然后将报文中继到移动节点的归属代理；归属代理处理完登记请求报文后向外区代理发送登记答复报文（接受或拒绝登记请求），外区代理处理登记答复报文，并将其转发到移动节点。另一种是直接向归属代理进行登记，即移动节点向其归属代理发送登记请求报文，归属代理处理后向移动节点发送登记答复报文（接受或拒绝登记请求）。登记请求和登记答复报文使用用户数据报协议（UDP）进行传送。当移动节点收到来自其归属代理的代理通告报文时，它可判断其已返口到归属网络。此时，移动节点应向归属代理撤销登记。在撤销登记之前，移动节点应配置适用于其归属网络的路由表。

代理发现（Agent Discoery）：为了随时随地与其他节点进行通信，移动节点必须首先找到一个移动代理。移动 IP 定义了两种发现移动代理的方法：一是被动发现，即移动节点等待本地移动代理周期性地广播代理通告报文；二是主动发现，即移动节点广播一条请求代理的报文。移动 IP 使用扩展的“ICMP Router Discovery”机制作为代理发现的主要机制。要注意的是，使用以上任何一种方法都可使移动节点识别出移动代理并获得转交地址，从而获悉移动代理可提供的任何服务，并确定其连至归属网还是某一外区网上。使用代理发现可使移动节点检测到它何时从一个 IP 网络（或子网）漫游（或切换）到另一个 IP 网络（或子网）。

所有移动代理（不管其能否被链路层协议所发现）都应具备代理通告功能，并对代理请求作出响应。所有移动节点必须具备代理请求功能。但是，移动节点只有在没有收到移动代理的代理通告，并且无法通过链路层协议或其他方法获得转交地址的情况下，方可发

送代理请求报文。

隧道技术（Tunneling）：当移动节点在外区网上时，归属代理需要将原始数据包转发给已登记的外区代理。这时，归属代理使用 IP 隧道技术，将原始 IP 数据包（作为净负荷）封装在转发的 IP 数据包中，从而使原始 IP 数据包原封不动地转发到处于隧道终点转交地址处。在转变地址处解除隧道，取出原始数据包，并将原始数据包发送到移动节点。当转交地址为驻留本地的转交地址时，移动节点本身就是隧道的终点，它自身进行解除隧道，取出原始数据包的工作。IETF RFC2003 和 RFC2004 各自定义了一种利用隧道封装数据包的技术。

在 RFC2003 中规定，为了实现在 IP 数据包中封装作为净负荷的原始 IP 数据包，需要在原始数据包的现有头标前插入一个外层 IP 头标。外层头标中的源地址和目的地址分别标识隧道的两个边界节点。内层 IP 头标（即原始 IP 头标）中的源地址和目的地址则分别标识原始数据包的发送节点和接收节点。除了减小 TTL 值之外，封装节点不改变内层的 IP 头标。内层 IP 头标在被传送到隧道出口节点期间保持不变，从而使原始 IP 数据包原封不动地转发到处于隧道终点的转交地址。

使用 RFC2004 定义的 IP 内最小封装有一个前提条件，就是当原始数据包被分片时，不能使用这种封装技术。也就是说，数据包在封装之前不能被分片。因此，对移动 IP 技术来讲，最小封装技术是可选的。为了使用最小封装技术来封装数据包，移动 IP 技术需要在原始数据包经修改的 IP 头标和未修改的净负荷之间插入最小转发头标。显然，这种最小封装技术比 RFC2003 定义的封装技术节省开销。

当拆装数据包时，隧道的出口节点将最小转发头标的字段保存到 IP 头标中，然后移走这个转发头标。

1.2.2 移动 IP 的实体

移动 IPV4 定义了三个特定的实体：

（1）移动节点（Mobile Node），一台主机，它保持主地址不变，从一个网络移动到另一个网络。

（2）家乡代理（Home Agent），有一个端口在移动节点家乡链路上的一台主机或路由器。当移动节点离开家乡链路时，它截获发往移动节点的分组并转发到移动节点上，它还保持有关移动节点当前位置的记录。

（3）外地代理（Foreign Agent），位于移动节点访问的链路上的一台主机或路由器，它为移动节点提供路由服务，作为移动节点在该链路上的缺省路由器，帮助移动节点通知它的家乡代理其转交地址，和家乡代理合作将分组传送给离开家乡网络的移动节点。

1.3 移动 IP 的工作原理

在移动 IP 中，主要有三个工作阶段：

代理发现（Agent Discovery）——移动节点发现它的外地代理（Foreign Agent）和家乡代理（Home Agent）[1、19]。

注册（Registration）——移动节点通过外地代理或者家乡代理注册当前的位置。

建立隧道（Tunneling）——当移动节点漫游时，家乡代理（Home Agent）建立到转交地址（移动节点在外部网络的接入点地址）的隧道，将分组路由到移动节点。

1.3.1 代理发现

移动 IP 发现过程是在路由器通告消息基础上建立的，它只是对路由器通告消息进行了扩展，将路由器通告消息与移动功能相关联。在代理发现阶段，移动代理（家乡代理和外地代理）通过使用 ICMP 路由器发现协议（ICMP Router Discovery Protocol）向网络通告业务。移动节点侦听这些通告，获知自己目前的位置，即判断出目前是连接在家乡网络上还是连接在外部网络上。

ICMP 路由器发现协议通告携带移动 IP 扩展字段，这个扩展字段指明代理的类型（家乡代理还是外地代理，亦或者是混合型代理）；代理的转交地址（Care-of Address）；代理提供的业务类型，例如，建立反转隧道、通用路由封装（GRE），移动节点可允许的注册生命期。家乡代理和外地代理会周期地发送代理通告。在代理通告的发送间隔，移动节点可以以广播或者多播的方式主动发送请求消息。任何一个家乡代理或者外地代理收到移动节点的请求消息后，都会立即给予回复，向该移动节点发送代理通告消息。

移动节点决定连接到外部网络，则需要获得一个转交地址。有两种转交地址：一种是外地代理的转交地址，即移动节点正在访问的外部网络的一个接口，也可以认为是外地代理的 IP 地址；另一种是合作定位转交地址（co-located care of address），即临时分配给移动节点端口上的 IP 地址。外地代理的转交地址可以被多个移动节点所共享，而 co-located 转交地址仅限于一个移动节点在一段时间内单独使用。当移动节点检测出自己的接入点地址改变，或者注册时间即将过期，都需要向代理注册。

1.3.2 注册

移动 IP 的注册过程就是移动节点告知家乡代理自己目前的接入点转交地址，并通知外地代理自己正在对其进行访问。移动节点、外地代理和家乡代理之间互相交换注册消息。

移动节点可以通过外地代理向家乡代理进行注册，也可以直接向家乡代理进行注册。

这两种注册程序都会使用注册请求消息和注册回复消息。

通过外地代理进行注册，移动节点会向每一个可能需要的外地代理发送注册请求消息，开始注册过程；外地代理处理这些注册请求消息，然后将它们转发给家乡代理；家乡代理给外地代理发送注册回复消息，接受或者拒绝移动节点的注册请求；外地代理处理这些注册回复，然后将它们转发给移动节点。

移动节点直接向家乡代理注册时，直接向家乡代理发送注册请求消息；家乡代理给移动节点发送注册回复消息，接受或者拒绝移动节点的注册请求。

1.3.3 建立隧道

移动节点给它的通信节点发送分组时使用家乡 IP 地址作为源地址，这样移动节点仿佛始终连接在家乡网络中。即使移动节点漫游到外部网络，通信节点仍然不会意识到它的移动。

以移动节点为目的地址的数据分组首先会到达家乡网络，由家乡网络中的家乡代理截获，然后将这些数据分组用隧道方式传送到移动节点所在接入点的转交地址。建立隧道有两个主要功能：在隧道起始处，对发送到隧道末梢端点的数据进行封装；在隧道终结处，对已到达隧道末梢端点的数据进行解封装。缺省的隧道模式是 IP in IP 封装模式，可选的封装技术有：GRE 技术和在 IP 内的最小封装。移动节点发送至通信节点的分组，首先会发送到外地代理，然后由外地代理将这些分组发送至最终的目的地址，即通信节点处。

1.3.4 无外地代理的特殊情况

如果移动节点连到了一条外地链路上但却收不到任何外地代理广播消息，或者移动节点根本不需要外地代理，那么移动节点可以绕过外地代理直接和家乡代理联系。移动节点可以设法通过动态主机配置协议 DHCP（Dynamic Host Configuration Protocol）服务器得到一个地址，如果成功了，移动节点就可以将这个地址作为配置转交地址，向它的家乡代理注册，这种情况比较特殊。

1.4 移动 IP 应用中出现的问题

移动 IP 在应用中遇到了一些困难，为移动 IP 的进一步的普及和应用带来了很大的困难，在这些问题中可分为两种问题：第一种是移动 IP 协议本身的问题，第二种是移动 IP 和现有的应用的冲突。

1.4.1 三角路由问题

移动 IP 中经常遇到“三角路由”问题，即通信对端发送数据报到移动节点时，首先要到达家乡代理，而后由家乡代理通过隧道转发给移动节点，而移动节点可以直接向通信对端发送数据报。“三角路由”问题会增加数据报传输的时延，占用网络资源并且加重家乡代理的处理负担。一种解决方法是采用路由优化技术，即移动节点将其转交地址通知通信对端，使通信对端可以通过隧道直接发送数据报到移动节点。但是路由优化将会带来新的安全问题，为了加强安全性能，移动节点必须和通信对端相互认证，即它们需要一对密钥。当移动节点和通信对端数目较多时，为每一个移动节点和通信对端分配一对密钥的方法是不可行的。另外，只有当移动节点与家乡代理比较远而与通信对端较近时采用路由优化才有较大意义。因此，应根据实际的网络拓扑结构并在考虑安全性的前提下来决定是否采用路由优化。

三角路由问题属于移动 IP 技术本身问题。容易发现，在移动 IPv4 中存在一个严重的问题，即通信节点发往“离家在外”移动节点的数据总是要建立三角路由（Triangle Routing）。如果我们要实现通信节点和移动节点的直接路由，需要保证移动节点转交地址向通信节点注册的安全性。可是，在 IPv4 中没有自动的密钥配置机制，为移动节点和它的每一个通信节点都分配一对密钥是不可能的。因此，我们需要专门的路由优化协议来实施优化路由。

1.4.2 外地代理的平滑切换问题

由于移动节点的移动频率可能很高，移动节点有时不能及时将当前的新转交地址注册到家乡代理，此时发往移动节点的数据报将会丢失。这个问题可以通过实现代理之间的平滑切换来解决。一种简单的实现方法是新的外地代理在得到移动节点认证前就发送绑定更新给旧外地代理，而后旧外地代理就开始向新外地代理转发数据。这种方法的切换时延较短，但存在很大的安全缺陷。如果一个攻击者假冒了新的外地代理，则可能会截获送往移动节点的数据。为增加代理切换的安全性能，同时尽量减少切换过程中的数据丢失，必须要求新外地代理首先得到移动节点的认证。移动节点可以在向新的外地代理发送注册请求的同时向旧外地代理发送绑定更新消息，并通知旧外地代理暂时缓存数据。而后移动节点对新外地代理进行认证，如果认证成功，移动节点将通知旧外地代理转发它缓存的数据到新外地代理，从而实现了一种更平滑、安全的切换。

1.4.3 网络性能问题

移动 IP 是一种与媒介无关的协议，可以工作在多种环境。当移动 IP 工作在无线网络