移动IPv6原理及基于MIPL的实现*)

谢 晟 吴中福 李 华 田凤斌
(重庆大学计算机学院 重庆400044)

摘 要 本文介绍了移动IPv6的基本原理和主要实现细节,并利用Linux和MIPL搭建了一个移动IPv6实验床,通过实验验证了移动IPv6的工作机制。

关键词 移动IPv6,邻居发现,MIPL,NGN

The Principle of Mobile IPv6 and its Implementation Based on MIPL

XIE Sheng WU Zhong-Fu LI Hua TIAN Feng-Bin
(College of Computer, Chongqing University, Chongqing 400044)

Abstract In this paper, we introduce the basic principle of Mobile IPv6 as well as its main implementing details and build a Mobile IPv6 testbed with Linux and MIPL. The mechanism of Mobile IPv6 is also validated through our experiments.

Keywords Mobile IPv6, Neighbor discovery, MIPL, NGN1

1 引言

随着互联网业务的进一步发展以及移动电话、PDA和笔记本等移动数据通信终端数量的增加,将会有越来越多的互联网用户希望能在任何地点、以任意的接入方式(有线或无线)、用固定的帐号和网络配置参数连接到Internet或企业网络,并且在移动的过程中不中断正在进行的应用。IETF在1996年就制定了IPv4移动性支持的标准,但是由于IPv4地址空间紧缺,移动IPv4实现较复杂,稳定性和安全性也较差,而IPv4的替代者IPv6能够较好地克服这些缺点,因此要实现移动IP,最好是基于IPv6。IETF从1996年就开始研究移动IPv6,到目前为止最新的草案是2003年6月发表的draft-ietf-mobileip-ipv6-24。这是草案的最后一个版本并已提交给IESG审议。

2 移动IPv6的基本工作原理

2.1 移动IPv6的设计目标

移动IP中的"移动"是指主机的网络接入点在不同的链路(网段)上切换,即在网络层上的移动。由于现有的网络路由技术是基于网络前缀而不是主机地址的,因此在节点的接入点切换到新的链路上后,如果不相应地改变IP地址,则发往该节点的数据包将无法正确路由到其当前所在链路。但上层连接,比如TCP是通过套接字对(源端口,源IP地址,目的端口,目的IP地址)来标识的,修改IP地址会使已经建立的连接中断,无法实现实时切换。移动IPv6的设计目标就是让节点能够使用固定的IP地址在不同的链路上切换,同时对上层应用保持透明,并与底层协议无关,即如果硬件允许的话,移动节点可以在异构的网络间切换(比如从以太网切换到蜂窝网络)。

2.2 移动IPv6的功能实体

移动IPv6中有3个主要的功能实体:

(1)移动节点MN(Mobile Node):接入点能够在不同链路上切换的节点。

(2)通信节点CN(Correspondent Node):与MN通信的对端节点,可以是固定或移动的节点。

(3)家乡代理HA(Home Agent):MN的家乡链路上的一台路由器,当MN不在家乡链路上时,HA把目的地为MN的IP包通过隧道发送给MN,并接收MN通过反向隧道发送过来的数据包,再转发给CN。

2.3 移动检测(Move Detection)

MN原先所在的链路称为家乡链路(Home Link),在这条链路上的地址称为家乡地址(Home Address)。当MN位于它的家乡链路时,不需要移动IPv6的处理,接收和发送数据包将按普通的路由进行转发。

MN可通过邻居发现(Neighbor Discovery)机制[5]和链路层信息来检测其是否切换了链路。当下面情况之一发生时,MN认为自己切换了链路[9]:

(1)连续几次(预设值)在预定的路由器通告间隔时间内没有收到缺省路由器的路由器通告。

(2)通过邻居不可达检测[5](Neighbor Unreachability Detection)确认缺省路由器已不可达。

(3)某些链路层协议能够向上层提供链路层切换的信息,这可能是发生了网络层切换的预示,MN可据此立即对缺省路由器进行不可达检测。

确认发生切换后,MN立即通过无状态[6]或有状态[7]地址自动配置机制获得在外地链路(Foreign Link)上的一个转交地址(Care-of Address)。MN每次切换到新的外地链路时,都将得到一个新的转交地址。

*)本文受重庆大学研究生创新实践基地"MIPL环境下移动IP延迟性能分析与改进"项目资助。谢 晟 硕士研究生,研究方向:计算机网络、移动IP。吴中福 教授,博士生导师,主要研究方向:计算机网络、计算机安全。李 华 副教授,硕士生导师,主要研究方向:计算机网络、远程教育系统。田凤斌 硕士研究生,研究方向:计算机网络、移动IP。

2.4 家乡注册(Home Registration)

MN 家乡地址和转交地址的关联称为绑定(Binding)。当 MN 得到转交地址后,就向 HA 发送绑定更新(Binding Update)。HA 维持着一个绑定缓存(Binding Cache),主要包括的域有:MN 的家乡地址、MN 的转交地址、生存时间值。当 HA 收到绑定更新后,就在绑定缓存中添加一个相应的表项,记录 MN 的绑定信息。之后,HA 向 MN 发送绑定确认(Binding Acknowledgement),表示注册成功。每条绑定表项都有生存时间,在其到期之前,如果 MN 希望继续使用该绑定,则需要再次发送绑定更新,否则 HA 将删除对应的表项。为此,MN 要维持一个绑定更新列表(Binding Update List)以存储 MN 发送的每一个绑定更新的信息。注册过程如图1。

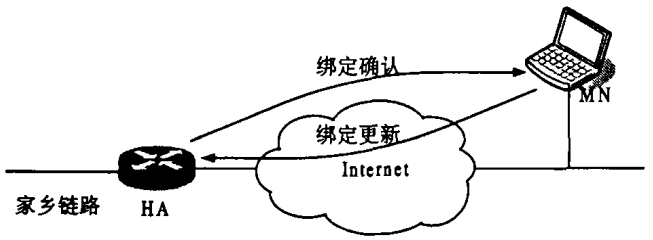

图1 家乡注册过程

2.5 通过双向隧道转发数据包(Bidirectional Tunneling)

注册之后,MN 就可以和 CN 进行通信了。CN 发送的 IP 包经过普通的路由到达 MN 的家乡链路后,被 HA 截获。HA 再对 IP 包进行封装[8],即将整个 IP 包作为数据装入新的 IP 包中。此时,原始(内层)IP 包的源地址是 CN 地址,目的地址是 MN 的家乡地址;隧道(外层)IP 包的源地址是 HA 将转发该包的接口的地址(隧道入口),目的地址是 MN 的转交地址(隧道出口)。MN 接收到从隧道发送过来的 IP 包,将外层 IP 拆封得到原始的 IP 包后交给上层处理。同样,MN 发送的 IP 包通过反向隧道(Reverse Tunnel)发送给 HA,HA 拆封后将原始的 IP 包按照正常路由转发给 CN。这样对于上层应用来说,节点的移动是透明的。CN 无须提供移动性支持就能和 MN 通信。采用双向隧道转发的过程如图2。

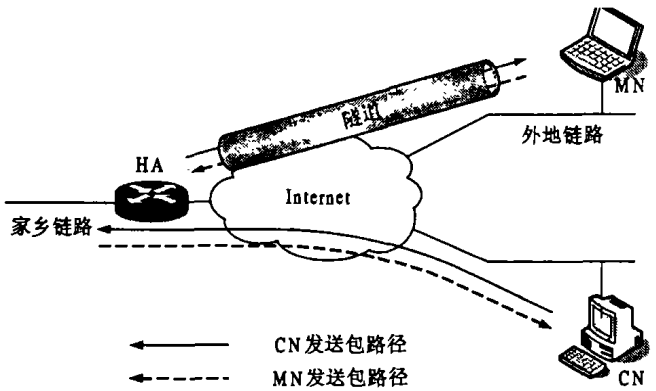

图2 双向隧道通信模式

2.6 路由优化(Route Optimization)

MN 和 CN 之间采用双向隧道模式通信必须经过 HA 转发而不能直接路由到目的地,这样延长了转发路径,增加了转发延迟,形成三角路由问题。为解决这个问题,MN 和 CN 还可以采用路由优化模式进行通信,前提是 CN 有移动性支持。MN 完成了家乡注册之后,如果从隧道出口接收到 CN 的数据包,便可以根据相应的策略启动通信节点注册(Correspondent Registration)过程。MN 向 CN 发送绑定更新,CN 也维持着一个和 HA 中结构相同的绑定缓存。CN 在缓存中添加相应绑定表项,记录 MN 的家乡地址、转交地址和绑定生存时间。MN 也在其绑定更新列表中添加相应表项。

绑定成功之后,CN 在发送 IP 包到 MN 时,在 IP 包中增加类型2路由扩展头[9],里面记录 MN 的家乡地址,并将 IP 包的目的地址换成 MN 的转交地址,然后按普通方式将其转发。IP 包经过正常的路由到达 MN,MN 将扩展头中的地址和 IP 头中的目的地址互换,此时扩展头中存放的是 MN 的转交地址,而 IP 头中的目的地址变成了它的家乡地址。然后 IP 包被交给上层处理。

MN 在发送 IP 包到 CN 时,在 IP 包中增加含有家乡地址选项[9](Home Address Option)的目的地选项扩展头(Destination Option Header)[1],里面记录 MN 的家乡地址,再把 IP 头中的源地址设为转交地址,然后按照普通方式转发该包。CN 接收到后就将选项内的地址与 IP 头的源地址互换。这时 IP 头中的源地址是 MN 的家乡地址,目的地址是 CN 的地址。然后 IP 包被交给上层继续处理。

通过路由优化,CN 和 MN 就能够直接进行通信而无须经过 HA 的转发。这样减少了 IP 包转发的中间跳数,缩短了转发延迟,同时减轻了 HA 的工作负载。另外,对于 MN 和 CN 的上层应用来说,移动始终保持了透明性。路由优化的过程如图3。

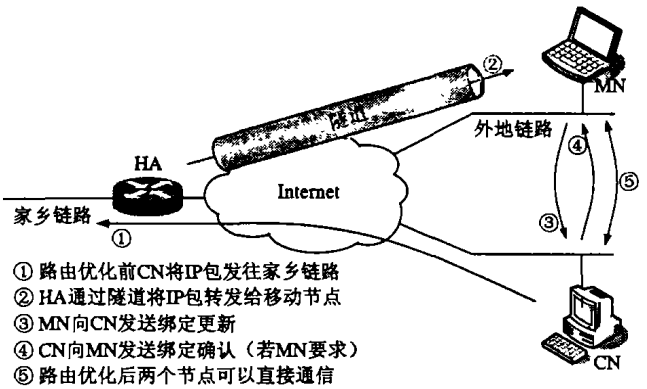

图3 路由优化过程

3 主要实现细节

3.1 HA 截获和转发 IP 包

为了截获发往 MN 的 IP 包,家乡注册后 HA 必须在家乡链路上多播(Multicast)代理邻居通告[5](Proxy Neighbor Advertisement),将 MN 的家乡地址映射到 HA 连接家乡链路的接口的 MAC 地址。在绑定有效生存时间内,HA 还应对所有针对 MN 家乡地址的邻居请求(Neighbor Solicitation)发送应答邻居通告(Solicited Neighbor Advertisement),同样将 MN 的家乡地址映射到 HA 连接家乡链路的接口的 MAC 地址。这样,所有封装有发往 MN 家乡地址的 IP 包的帧都会到达 HA 上的指定接口。

家乡注册后,HA 和 MN 之间建立起一条 IPv6隧道,实际上是在系统中创建了一个伪接口(Pseudo-interface)。和普通的物理接口不同,伪接口指向的是一组软件(移动性模块)而不会向物理介质发送比特流[13]。HA 还会在其路由表中为该 MN 添加一条特定的主机路由表项(前缀匹配长度为128),目

的地址为MN的家乡地址，转发接口为建立的隧道，这样就将伪接口合成到了路由表当中。HA截获IP包之后根据其目的地址匹配到该路由表项，将其“转发”到伪接口。IP包被交给移动性模块，经过封装后再转发到MN的转交地址。从反向隧道发送过来的IP包的目的地址就是HA，HA将其拆封后得到原始的IP包，再按照普通的路由方式将其转发出去。

3.2 MN发送和接收IP包

移动性模块会在MN上自动创建一个伪接口，该接口的IP地址和MN的真实物理接口IP地址相同，也是MN的家乡地址。当MN在家乡链路时收发IP包和普通节点一样，不需要移动性模块对其进行处理。当MN切换到外地链路并完成了家乡注册之后，MN将添加一条缺省路由，将缺省网关设为伪接口，因为MN和先前的缺省路由器已不在同一链路，现在所发送的IP包都要交给移动性模块进行处理。通过把伪接口合成到路由表中，移动性模块就能够在原始IP包发送之前将其“拦截”，并根据绑定信息进行不同的处理(封装或加入目的地选项扩展头)后再转发出去。

无论是隧道方式还是路由优化方式，MN接收到的IP包的目的地址都是其转交地址，在交给上层处理之前，移动性模块都要对其进行处理(拆封或者处理类型2路由头)。

3.3 CN发送和接收IP包

即使CN没有移动性支持也能够和MN通信。上层应用只需要知道MN固定的家乡地址并将其设为IP包的目的地址，IP包就能到达MN的家乡链路，并由HA通过隧道发送给MN。MN发送的IP包经过反向隧道到达HA，经HA拆封后再转发给CN，这时CN收到的IP包的源地址仍然是MN的家乡地址。CN不知道也无须知道MN是否移动。若CN提供移动性支持，则可以采用路由优化方式同MN通信，这时CN在把IP包发送出去或者把接收到的IP包交给上层处理之前，都需要将其“拦截”并交给移动性模块处理(加入类型2路由头或处理目的地扩展头)。“拦截”的方法因系统而异，MIPL利用了Linux下分析处理特定协议数据包的框架Netfilter[10,12]。

4 移动IPv6实验床

4.1 MIPL简介

MIPL(Mobile IPv6 for Linux)是由芬兰赫尔辛基大学(HUT)开发的移动IPv6软件[10]，起源于1999年该大学软件项目课程的一个学生项目，其最初目的是设计一个有限功能的移动IPv6原型。2000年后，该项目被纳入HUT通信软件及多媒体实验室的GO/Core项目继续开发。这是研究人员和爱好者使用最多的一个系统，更新很快，目前最新版本是1.0，遵循草案24版本，支持Linux 2.4.22内核，可从www.mobile-ipv6.org下载。MIPL由内核补丁和用户空间工具两部分组成，内核补丁在Linux内核中加入移动性支持，用户空间工具则用于运行时的调试和配置。

4.2 实验环境

我们实验的目的是测试和验证移动IPv6的基本工作原理和主要实现细节，所以建立了比较简单的实验环境，包括两台路由器和两台主机，网络拓扑结构如图4。

HA和Router实际上是两台安装有双网卡的主机，采用Red Hat Linux 8.0操作系统并配置了路由转发功能。HA上还安装了MIPL使其支持移动IPv6的HA功能。MN和CN也安装了Linux和MIPL。HA的eth0接口连接家乡链路2001:250:f006:5020::/64，eth1连接Router的eth0，该网段地址前缀为2001:250:f006:5021::/64，Router的eth1再连接一条外地链路2001:250:f006:5022::/64。MN最初连接在家乡链路上，地址为2001:250:f006:5020::100/64，CN地址为2001:250:f006:5022::200/64。

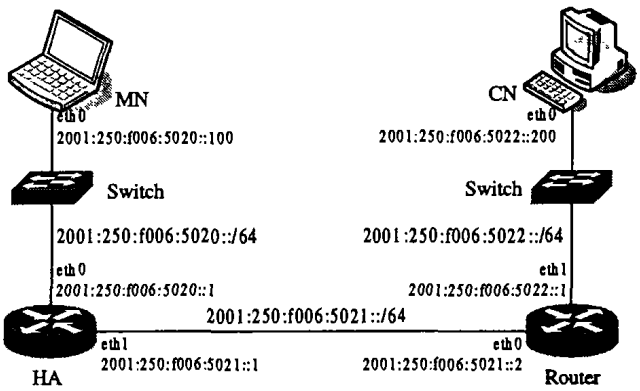

图4 实验环境网络拓扑图

4.3 实验步骤

(1)在HA上将MIPL内核补丁加入到Linux 2.4.22内核源码当中，编译新内核并配置使其具有家乡代理功能。同样在MN和CN上安装和配置MIPL，使MN具有移动节点功能，CN只需支持基本的移动IPv6功能即可。在HA和Router上安装路由器通告守护进程软件Radvd-0.7.2并作相应配置。根据拓扑图连接并配置各个接口。

(2)在CN上关闭移动IPv6服务，使其没有移动性支持。在CN上ping6 MN，在此过程中将MN的网线从家乡链路上断开并接入外地链路2001:250:f006:5022::/64。在此过程中分别用ifconfig、route和MIPL的用户工具mipdiag检测和分析HA和MN的接口配置情况、路由表内容和移动IPv6相关信息，在MN上用tcpdump命令观测网络通信情况。

(3)在CN上启动移动IPv6服务，使CN提供移动性支持。重复(2)中的步骤。

4.4 实验结果及分析

(1)CN关闭移动IPv6服务时

在MN上可以看到移动IPv6创建了一个伪接口mip6-mnha1，IPv6地址与eth0的家乡地址相同。在HA上系统创建了一个IPv6隧道的伪接口ip6tnl1，这实际上是一个空闲的隧道，当MN切换到外地链路并进行家乡注册后，移动IPv6会占用这个隧道并新建一个空闲隧道。每一个MN家乡地址和转交地址的绑定都会在HA中占用一个隧道。

MN在家乡链路时，MN和CN按照正常路由方式通信，不需要移动性模块处理。MN上的tcpdump输出采样如下：

①2001:250:f006:5022::200>2001:250:f006:5020::100:icmp6:echo request (len 64, hlim 64)

②2001:250:f006:5020::100>2001:250:f006:5022::200:icmp6:echo reply (len 64, hlim 64)

将MN切换到外地链路2001:250:f006:5022::/64后，再次查看MN的接口配置，eth0通过无状态地址自动配置得到一个转交地址2001:250:f006:5022:2e0:4cff:fed4:a4c/64。

查看HA的绑定缓存，里面已经添加了一条绑定表项，其中Type为2表示这是一条家乡注册：

Mobile IPv6 Binding cache

```
Home Address    2001:250:f006:5020::100
Care-of Address 2001:250:f006:5022:2e0:4cff:fed4:a4c
Lifetime        24
Type            2
```

CN 没有移动性支持，所以不能查看绑定缓存。

如3.1节所述，HA 的路由表内添加了一条特定主机路由：

```
Kernel IPv6 routing table
Destination                Next Hop        Iface
2001:250:f006:5020 ::      100/128::ip6tnl1
```

如3.2节所述，MN 的路由表内添加了一条缺省路由：

```
Kernel IPv6 routing table
Destination                Next Hop     Iface
::/0                       ::           mip6mnha1
```

CN 上的 ping6短暂中断后继续，MN 上的 tcpdump 输出采样如下：

①2001:250:f006:5022::200>2001:250:f006:5020::100:icmp6:echo request (len 64, hlim 64)
②2001:250:f006:5020::1>2001:250:f006:5022:2e0:4cff:fed4:a4c:2001:250:f006:5022::200>2001:250:f006:5020::100:icmp6:echo request (len 64, hlim 63)
③(len 104, hlim 255)2001:250:f006:5022:2e0:4cff:fed4:a4c>2001:250:f006:5020::1:2001:250:f006:5020::100>2001:250:f006:5022::200:icmp6:echo reply (len 64, hlim 64)(len 104, hlim 255)
④2001:250:f006:5020::100>2001:250:f006:5022::200:icmp6:echo reply (len 64, hlim 63)

第一条信息是CN 发送的原始 IP 包，目的地址是 MN 的家乡地址。第二条是经 HA 封装了的 IP 包，如3.1节所述，外层 IP 头源地址是 HA 地址，目的地址是 MN 转交地址。两个 len 的差值正好是 IPv6报头长度40字节[1]。第三条是 MN 封装后通过反向隧道发送给 HA 的 IP 包，第四条是 MN 发送给 CN 的原始 IP 包。这说明 MN 和 CN 正采用双向隧道方式通信。

(2)CN *启动移动* IPv6*服务时*

与(1)中相同，MN 和 HA 上分别建立了伪接口 mip6mnha1和 ip6tnl1。MN 在家乡链路时，MN 上 tcpdump 输出也与(1)中相同。

将 MN 切换到外地链路2001:250:f006:5022::/64后，eth0得到一个转交地址2001:250:f006:5022:2e0:4cff:fed4:a4c/64。HA 的绑定缓存内添加了一条家乡注册信息：

```
Mobile IPv6 Binding cache
Home Address    2001:250:f006:5020::100
Care-of Address 2001:250:f006:5022:2e0:4cff:fed4:a4c
Lifetime        19
Type            2
```

CN 上的 ping6短暂中断后继续。查看 CN 的绑定缓存，里面增加了一条信息，类型1表示是通信节点注册：

```
Mobile IPv6 Binding cache
Home Address    2001:250:f006:5020::100
Care-of Address 2001:250:f006:5022:2e0:4cff:fed4:a4c
Lifetime        34
Type            1
```

与(1)相同，HA 和 MN 的路由表中都添加了特定表项。

MN 上的 tcpdump 输出采样如下：

①2001:250:f006:5022::200>2001:250:f006:5022:2e0:4cff:fed4:a4c:srcrt (len=2,type=2,segleft=1[|srcrt][|icmp6](len 88, hlim 64)
②2001:250:f006:5022:2e0:4cff:fed4:a4c>2001:250:f006:5022::200:DSTOPT (padn)(homeaddr:2001:250:f006:5020::100)icmp6:echo reply (len 88, hlim 64)

第一条信息是CN 发给 MN 的 IP 包，目的地址是 MN 的转交地址，载荷是 icmp6(echo request)，“srcrt”和“type=2”表示含有类型2路由扩展头，包长度为88字节，由64字节的原始 IP 包和24字节的类型2路由扩展头组成。第二条信息是 MN 应答 CN 的 IP 包，源地址是 MN 的转交地址，“DSTOPT”表示含有目的地选项扩展头，里面放置的是含有 MN 家乡地址的家乡地址选项，IP 包长度中包括了24字节的目的地选项扩展头。这说明 MN 和 CN 正采用路由优化方式通信。

总结 3G 标准化组织3GPP(The 3rd Generation Partnership Project)已经将 Internet 无线接入定为3G 的基本服务之一，而且将 IPv6作为多媒体业务的必选承载协议，所以移动 IPv6具有非常广阔的应用前景。本文介绍了移动 IPv6的基本原理和主要的实现细节，并利用 MIPL 搭建了一个简单的实验环境，通过实验来验证移动 IPv6的工作机制。我们计划在下一步的研究中利用实验床做一些移动 IPv6性能优化方面的分析。

参 考 文 献

1 Deering S, Hinden R. Internet Protocol, Version 6 (IPv6) Specification. RFC 2460, 1998
2 Hinden R, Deering S. Internet Protocol Version 6 (IPv6) Addressing Architecture. RFC3513, 2003
3 Hinden R, Deering S, Nordmark E. IPv6 Global Unicast Address Format. RFC3587, 2003
4 Conta A, Deering S. Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification. RFC2463, 1998
5 Narten T, Nordmark E, Simpson W. Neighbor Discovery for IP Version 6 (IPv6). RFC2461, 1998
6 Thomson S, Narten T. IPv6 Stateless Address Autoconfiguration. RFC2462, 1998
7 Droms R, Bound J, Volz B, Lemon T, Perkins C, Carney M. Dynamic Host Configuration Protocol for IPv6(DHCPv6). RFC3315, 2003
8 Conta A, Deering S. Generic Packet Tunneling in IPv6 Specification. RFC2473, 1998
9 Johnson D, Perkins C, Arkko J. Mobility Support in IPv6, draft-ietf-mobileip-ipv6-24, work in progress, 2003
10 Tuominen A J, Petander H. MIPL Mobile IPv6 for Linux in HUT Campus Network MediaPoli. In: Proc. of Ottawa Linux Symposium 2001, Canada, 2001
11 何涛，杨寿保. IPv6的移动性支持及实现. 小型微型计算机系统，2003,24(3):415～418
12 代刚，马严. 移动 IPv6技术的研究及其在 Linux 环境下的实现. 中兴通讯技术，2002(3):24～27
13 裘晓峰译. 移动 IP. 北京：机械工业出版社，2000