

基于Linux的移动IP家乡代理的研究与实现

刘冰月

(大连东软信息学院 计算机系, 辽宁 大连 116023)

摘要:移动IP是一个用来支持节点移动性的因特网协议。它的设计目标是使节点无论在什么位置都可以无缝地接入因特网,并且可以不用改变节点原来的IP地址。文中的主要工作是实现移动IP中定义的一个功能实体——家乡代理,在原有的路由协议基础之上通过修改家乡代理的IP层处理机制,使其具有移动代理的功能。这样做的好处在于可以不必对现有的设备作任何硬件和软件的更新就可以将其它节点发给移动节点的数据包转发到它现在所处的位置。

关键词:移动IP;家乡代理;隧道

中图分类号:TP393

文献标识码:A

文章编号:1673-629X(2009)09-0200-04

Investigation and Implementation of Mobile IP Home Agent Based on Linux

LIU Bing-yue

(Dept. of Computer, Dalian Neusoft Institute of Information, Dalian 116023, China)

Abstract: Mobile IP is a protocol that supports a node's mobility. Its target is causing a node to connect Internet anywhere and needn't change its IP. Based on the route mechanism of IP protocol to realize a function entity in mobile IP - the home agent. Make a router to a home agent through modifying its processing mechanism of IP layer. So it can transmit packets to the mobile node without renewing any hardware or software.

Key words: Mobile IP; Home Agent; Tunnel

1 移动IP出现的背景

移动IP技术是IP技术和移动通信技术的完美结合,它使得数据通信发生着与语音通信一样的变革。它将使得人类最终实现在任何时间、任何地点、用任何一种媒体与任何一个人进行通信的梦想。

由于传统的IPv4协议有一个非常不好的约定,即节点必须使用固定的IP地址和TCP端口号进行相互通信,否则节点之间的通信将无法继续^[1]。因此,当移动节点改变IP地址时,它和别的节点之间正在进行的通信将中断,必须由移动节点以新的IP地址建立一条新连接才能继续进行通信,为了解决这一问题,IETF的移动IP工作组于1992年6月制定移动IP协议,从而使Internet上的移动接入成为可能^[2]。

移动IP的出现主要为了解决以下两个问题:

(1)当节点在切换链路时不改变它的IP地址就无

法在新链路上接收数据包。

(2)当节点在移动过程中改变了它的IP地址就不得不每次都中断和重启正在进行的通信。

2 移动IP中定义的几个主要的实体

移动IP中定义的几种重要的功能实体有:

(1)移动节点:可以将接入因特网的位置从一条链路切换到另一条链路上而仍然保持所有正在进行的通信,并且只使用它的家乡地址的那些节点。

(2)家乡代理^[3]:有一个端口与移动节点家乡链路相连的路由器。

(3)家乡地址:即移动节点的永久IP地址,当移动节点切换链路时家乡地址并不改变。

(4)转交地址:是指移动节点连接在外地链路上时的相关IP地址。这是一个完全正确,却没有多少实质内容的定义。从概念上讲有两种转交地址:外地代理转交地址和配置转交地址。文中所采用的就是配置转交地址。

(5)隧道:当一个数据包被封装在另一个数据包的净荷中进行传送时所经过的路径称为隧道。移动IP

收稿日期:2009-01-14;修回日期:2009-03-08

基金项目:新世纪优秀人才支持计划资助项目(ACET-04-0301);

吉林省科技发展项目基金(20080107)

作者简介:刘冰月(1978-),女,山东高密人,讲师,硕士,主要研究方向为计算机网络及系统结构。

中使用了三种隧道技术:IP的IP封装、最小封装和通用路由封装。文中所采用的是IP的IP封装。

文中的主要工作是,对移动IP中定义的家乡代理实体的功能的研究与实现,主要包括以下三个方面:

1)家乡代理对移动节点的注册注销方面的工作。

2)注册成功后家乡代理利用隧道封装技术进行数据包的发送。

3)家乡代理利用代理ARP截获其他节点发往移动节点的数据包。

3 开发环境和设计思想

由于移动IP是一个对节点移动性的网络层解决方案,因此其主要功能的实现应该在网络层完成,这样既保证了系统的安全性可靠性,也实现了应用透明性,使得无论上层应用程序采用何种协议都可以不受节点移动的影响。由于Linux操作系统的内核源代码开放的特性,因此选择在Linux系统平台上进行开发,通过修改其IP层源代码,使其增加对节点移动性的支持。文中使用的是Redhat 9.0, Linux操作系统内核版本2.4.20-8。

文中是对[RFC 2002]文档^[3]中定义的移动IP协议中的一个实体——家乡代理的具体的实现。主要分为三个层次:第一部分是在用户层上运行的一些应用程序来完成移动节点的注册过程;第二部分是在系统内核中做一定的修改即在网络层做处理来实现对数据包的隧道封装;第三部分是在数据链路层上发送代理ARP消息来截获发往移动节点的数据包。

4 移动节点的注册

当移动节点发现它连在一条外地链路上时,它就得到一个转交地址,并向家乡代理注册这个地址^[3]。移动IP的注册包括两种消息的交互:注册请求消息(Registration Request)和注册应答消息(Registration Reply)。注册消息放在UDP数据段的数据部分,UDP数据段则放在IP包的净荷中。

4.1 文中所使用的注册表存储结构

注册表是用来存储移动节点家乡地址和转交地址对应关系的结构。在文中其表项的数据结构定义如下:

```
struct register_node{
    struct sockaddr_in home_addr; /* 移动节点家乡地址信息 */
    struct sockaddr_in foreign_addr; /* 移动节点转交地址信息 */
    u_short lifetime; /* 绑定生存时间 */
}
```

}

4.2 文中采用的注册机制

文中采用的注册机制如下:

移动节点注册时,使用事先规定好的固定端口号(434)向家乡代理发送注册请求UDP包,家乡代理启动监听程序循环监听434端口,如果有数据包到来,则判断该数据包类型:

* 如果是注册数据包即生存时间 >0 ,则做以下处理:

首先判断该包的合法性,并对其身份进行认证。

如果认证成功,若生存时间 >0 并且 $S=0$,则根据UDP包的数据部分对该表项进行更新。若生存时间 >0 并且 $S=1$,则插入一个新表项。之后,家乡代理向移动节点发送注册成功消息,即发送注册应答UDP包,其中Code域置1表明接受请求。

移动节点接收到注册应答消息后同样要进行包的合法性认证以及对应答消息中标识域值的对比。这样,就避免了其他节点以假冒身份进行的恶意攻击,保证了移动IP实现过程中的安全性、可靠性。

如果认证不成功,则直接返回一个注册应答消息,其中Code域置0,告知该请求被拒绝。

* 如果是注销包即生存时间 $=0$,则做以下处理:

首先,同样进行一系列安全认证,然后查找注册表。若找到匹配表项,则删除该表项。否则,向移动节点发送应答UDP包,告之“该节点已经注销”。

* 如果既不是注册包也不是注销包则不对该包做任何修改,继续监听。

4.3 用户空间与内核空间共同访问注册表解决方法

由于对数据包的隧道封装操作是在内核空间中完成的,而注册表是建立于用户空间的存储结构,对移动节点注册请求消息的接收和处理是由用户层的守护进程来完成的,这样就涉及到用户态和内核态之间如何进行通信的问题。文中采用的解决方法是使用文件来存储注册表,这样内核和用户层就可以通过对同一个文件的操作达到共同对注册表进行访问的目的。

首先为用户层创建一个用来存储注册表内容的文件——regtable,并以可读写方式打开它,然后根据到来的注册消息对该文件进行相应的添加、修改或删除操作。

与此同时家乡代理的IP层不断有数据包到来,需要根据包头的目的地址域来判断该包是否是发往移动节点的数据包,如果是,则同样需要访问注册表。首先在内核中以只读方式打开注册表文件regtable,顺序查找是否有相匹配的内容,如果找到则根据其中相应的转交地址对数据包进行隧道封装。

5 家乡代理利用隧道封装技术进行数据包的发送

由于移动节点在移动到外地链路之后仍以自己原来的 IP 地址与其它节点进行通信,因此其它节点给移动节点发送数据包时仍然将移动节点的家乡地址作为目的地址。要想利用传统的路由机制将这些数据包路由到移动节点,家乡代理就必须对它们进行隧道封装,使其目的地址符合现有的 IP 协议规则之后再进行发送^[4]。

文中采用的封装机制如下:当家乡代理收到一个数据包后,首先根据 IP 头中的目的地址查找注册表文件,若没有找到匹配项则认为是发给普通节点的包,可以根据传统路由规则进行转发;否则对该数据包进行封装,源地址域填入家乡代理的 IP 地址,目的地址域填入查找注册表后得到的移动节点的转交地址。

封装后的数据包格式如图 1 所示。其中:

- src——源 IP 地址或源 UDP 端口号域
- dst——目的 IP 地址或目的 UDP 端口号域
- MN——移动节点的家乡地址
- COA——转交地址
- HA——家乡代理的 IP 地址
- CN——通信对端的 IP 地址

新 IP 头 [src = HA, dst = COA]	原 IP 头 [src = CN, dst = HA]	TCP/UDP 头	数据 部分	移动-家乡 认证扩展
------------------------------------	-----------------------------------	--------------	----------	---------------

图 1 封装后的数据包格式

由于需要修改数据包的 IP 头等信息,所以需要在 IP 层截获数据包,加以处理之后再交给系统进行路由。

在 Linux 平台中,当位于以太网上的一个节点接收到另一个节点发送的数据包时,该包必定由低到高依次经过 Linux 网络堆栈中的数据链路层、IP 层、TCP/UDP 层、socket 层。因此选择在 IP 层的内核处理函数 ip_rcv(位于内核文件 net/ipv4/ip_input.c 中)中对家乡代理截获的其它节点发往移动节点的数据包进行隧道封装,封装之后再交由内核处理。这时由于数据包的目的地址是一个合法的外地链路地址,所以利用传统的 IPv4 路由协议就可将包发送给移动节点。

6 家乡代理利用代理 ARP 截获发往移动节点的数据包

使用代理 ARP 的方法来截获发往移动节点的数据包。当有一台位于移动节点的家乡链路上的主机想向移动节点发送数据包时,该主机将广播一个 ARP 请求消息以得到移动节点的数据链路层地址。然而如果

移动节点这时不在家乡链路上,它就不可能收到这条 ARP 请求,因为路由器从不转发 ARP 消息。这时需要由移动节点的家乡代理发送一个 ARP 应答即用家乡代理的数据链路层地址对移动节点的家乡地址作应答,这个代理 ARP 使得移动节点不在家乡链路上时,发送给它的数据包都送给家乡代理^[5]。

6.1 文中的代理 ARP 应答帧结构

家乡代理发送的代理 ARP 应答帧结构如图 2 所示。其中:

- Ecn——通信对端以太网地址
- Eha——家乡代理以太网地址
- 帧类型——对于 ARP 请求或应答,该字段的值为 0x0806
- 硬件类型——它的值为 1 即表示以太网地址
- 协议类型——它的值为 0x0800 即表示 IP 地址
- 操作字段——ARP 请求值为 1,ARP 应答值为 2
- MA——移动节点的家乡地址
- CN——通信对端的 IP 地址

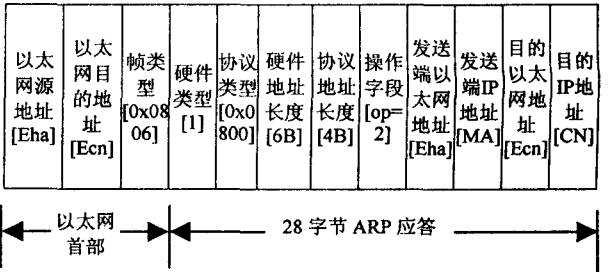


图 2 代理 ARP 应答帧结构

6.2 Linux 中的代理 ARP 实现

在网络接口设备的硬件层之间能够直接进行包交换的设备构成了一个局域网,局域网中的每一设备具有唯一的硬件地址。对 TCP/IP 协议来说,局域网中的每一设备都具有唯一的 IP 地址,当数据包要从某一节点发向局域网中具有另一 IP 地址的节点时,源节点必须获得目的节点的数据链路层地址,这就需要硬件地址解析。ARP 协议是根据节点的 IP 地址获取其硬件地址的方法。源节点向局域网广播 ARP 请求,局域网中其余节点都收到该请求,具有所请求 IP 地址的节点会向源节点做出应答,提供它自己的数据链路层地址。由于 ARP 请求的广播特性,某一节点可以对不是自己 IP 地址的请求做出应答,这就是代理 ARP。文中的家乡代理就是要实现这一功能。

文中利用了 Linux 中提供的 socket 接口来收发 ARP 帧只要建立一个类型为 SOCK_PACKET 的 socket 套接字即可:

```
int sockfd;  
sockfd = socket(AF_INET, SOCK_PACKET, htons(ETH_
```

P_ARP)); //监听 ARP 帧

定义 arp_packet 数据结构来存储 ARP 帧:

```
# define ETH_HW_ADDR_LEN 6
# define IP_ADDR_LEN 4
# define ARP_FRAME_TYPE 0x0806
# define ETHER_HW_TYPE 1
# define IP_PROTO_TYPE 0x0800
# define OP_ARP_REPLY 2
# define DEFAULT_DEVICE "eth0"

struct arp_packet {
    u_char targ_hw_addr[ETH_HW_ADDR_LEN];
    u_char src_hw_addr[ETH_HW_ADDR_LEN];
    u_short frame_type;
    u_short hw_type;
    u_short prot_type;
    u_char hw_addr_size;
    u_char prot_addr_size;
    u_short op;
    u_char sndr_hw_addr[ETH_HW_ADDR_LEN];
    u_char sndr_ip_addr[IP_ADDR_LEN];
    u_char rcpt_hw_addr[ETH_HW_ADDR_LEN];
    u_char rcpt_ip_addr[IP_ADDR_LEN];
    u_char padding[18];
}
```

对代理 ARP 的具体实现过程如下:

* 首先利用 recvfrom() 函数在链路层上直接监听网络上的 ARP 帧并将接收到的 ARP 帧放入缓冲区 buf 中;

* 之后判断存放在缓冲区中帧的 op 字段,如果是请求帧则判断它的目的 IP 地址域,如果这个 IP 地址是已经向家乡代理注册过的移动节点的家乡地址,那么家乡代理利用 ioctl() 函数得到自己的硬件地址;

* 最后利用 sendto() 函数来代替移动节点发送一

个 ARP 应答帧,其中的源硬件地址域填写家乡代理自己的硬件地址。

通过这种方式,家乡代理就可以截获到位于移动节点家乡链路上的其它节点发往移动节点的数据包。

7 结束语

根据 RFC 2002 文档中对移动 IP 协议的描述^[6],实现了移动 IP 中规定的一个功能实体——家乡代理的基本功能^[7]。在实现的过程中也存在着一些问题,比如,移动 IP 中的路由优化问题^[8]、网络性能和可靠性方面的问题、对 IPV6 协议的支持问题^[9]以及安全性问题^[10]等等。这些都有待进一步的完善,也是今后将要努力的方向。

参考文献:

- [1] Perkins C. Mobile IP[J]. IEEE Communications Magazine, 1997, 35(5): 84-99.
- [2] Perkins C. Mobile Networking through Mobile IP[J]. IEEE Internet Computing, 1998, 2(1): 58-69.
- [3] Perkins C. IP Mobility Support for IPv4[S]. The Internet Engineering Task Force, RFC 3344, 2002.
- [4] Perkins C, Johnson D B. Route Optimization in Mobile IP [DB/DK]. draft-ietf-mobileip-optim-10.txt, Internet Draft, IETF, 2000.
- [5] Solomon J D. 移动 IP[M]. 北京:机械工业出版社, 2000.
- [6] Perkins C. IP Mobility Support[S]. The Internet Engineering Task Force, RFC 2002, 1996.
- [7] 邱新平, 阮传概, 张振海. 移动 IP 技术研究[J]. 移动通信, 2000(3): 26-29.
- [8] 孙利民. 移动 IP 技术[M]. 北京:电子工业出版社, 2003.
- [9] 李庆, 曾志纯. IPv6 协议对移动性的支持[J]. 微机发展 (现更名: 计算机技术与发展), 2003, 13(11): 90-92.
- [10] 周贤伟. 移动 IP 与安全[M]. 北京:国防工业出版社, 2005.

(上接第 127 页)

高查询的准确度,下一步将研究用形状进一步检索心脏图像,以提高查准率。

参考文献:

- [1] Lobodzinski S S, Meszaros G N. Context indexing of digital cardiac ultrasound records in PACS[J]. SPIE, 1998, 3339: 500-507.
- [2] Abate A F, Michele N, Genny T, et al. IME an image management environment with content based access[J]. Image and Vision Computing, 1999, 17: 967-980.
- [3] 李顺山, 庄天戈, 陈辉. 基于灰度直方图和互相关方法的医学图像检索[J]. 上海交通大学学报, 2001, 35(5): 695-698.

- [4] Pincus S M, Goldberger A L. Physiological time-series analysis: What does regularity quantify? [J]. Am J Physiol, 1994, 266: 1643-1656.
- [5] 汪蕙, 金丰年. 基于灰度和边界方向直方图的医学图像检索[J]. 信号处理 2004, 20(1): 74-77.
- [6] 任艳斐. 直方图均衡化在图像处理中的应用[J]. 计算机与信息技术, 2007(4): 37-38.
- [7] 金磊, 陈优广, 严敏. 一种基于用户感兴趣区域的图像检索算法[J]. 计算机技术与发展, 2006, 16(3): 104-106.
- [8] 张恒博. 一种基于色彩和灰度直方图的图像检索方法[J]. 计算机工程, 2004, 30(10): 20-22.
- [9] 汪慧兰, 赵海峰, 罗斌. 基于局部颜色空间特征的图像检索[J]. 计算机技术与发展, 2006, 16(1): 76-79.