Submit to: Workshop on Computer Networks

Paper title: Address Sharing enabled Mobile IP utilizing NAPT

Authors: Fu-Yuan Lee, Shiuhpyng Shieh and Lin-Yi Wu

Contact author: Fu-Yuan Lee

Department of Computer Science and Information Engineering

National Chiao Tung Univserity, Hsinchu, Taiwan 300

E-mail: {leefy, ssp, lywu}@csie.nctu.edu.tw

Phone: (03) 5712121 ext. 54750

Fax: (03)5724176

Abstract

The IP depletion problem is getting more serious with the increase in the number of mobile network devices connecting to the IP networks. To cope with this problem, we incorporate NAPT with Mobile IP to enable address sharing. In the proposed scheme, mobile nodes use private addresses as their home addresses and access Internet services using a shared public IP address. Since private addresses can be utilized without coordination, our scheme is designed to work in the presence of address collision. Furthermore, our scheme is transparent to mobile nodes and correspondent nodes. Therefore, it can be easily deployed because the protocol stacks of mobile nodes and correspondent nodes need not to be modified. Briefly, Mobile IP can accommodate more mobile nodes by adopting the scheme presented in this paper.

Keywords: Mobile IP, NAPT, regional registration, address sharing

Address Sharing enabled Mobile IP utilizing NAPT *

Fu-Yuan Lee, Shiuhpyng Shieh and Lin-Yi Wu

Department of Computer Science and Information Engineering
National Chiao Tung Univserity, Hsinchu, Taiwan 300
E-mail: {leefy, ssp, lywu}@csie.nctu.edu.tw
Phone: (03) 5712121 ext. 54750
Fax: (03)5724176

Abstract

The IP depletion problem is getting more serious with the increase in the number of mobile network devices connecting to the IP networks. To cope with this problem, we incorporate NAPT with Mobile IP to enable address sharing. In the proposed scheme, mobile nodes use private addresses as their home addresses and access Internet services using a shared public IP address. Since private addresses can be utilized without coordination, our scheme is designed to work in the presence of address collision. Furthermore, our scheme is transparent to mobile nodes and correspondent nodes. Therefore, it can be easily deployed because the protocol stacks of mobile nodes and correspondent nodes need not to be modified. Briefly, Mobile IP can accommodate more mobile nodes by adopting the scheme presented in this paper.

Keywords: Mobile IP, NAPT, regional registration, address sharing

1 Introduction

With the increasing demand on mobility and rapid development of Internet applications in IP networks, building an All-IP access network with mobility support has received considerable research interests in recent years. Integrating traditional wired IP networks with other heterogeneous networks such as PSTN and wireless networks allows users to access Internet services any where and any time. Due to the convenience, more and more mobile network devices will

*This work is supported in part by Lee and MTI Center for Internetworking Research (Global Crossing), Ministry of Education, and National Science Council under Contract NSC 90-2213-E-009-145 and NSC 89-E-FA04-1-4

connect to the IP networks in the near future. In the All-IP based mobile network architecture, Mobile IP [4] is adopted as one technique to support seamlessly roaming among alternative access networks [7]. Using Mobile IP, a mobile device, called mobile node (MN), can maintain its network connectivity regardless of its link layer point of attachment. According to the Mobile IP protocol specification, each mobile node requires a unique and permanent IP address as its home address which is considered as a globally unique identifier of the mobile node. However, this requirement intensifies the IP depletion problem because IP version 4 (IPv4) address space can not fulfill the need of IP addresses when the number of mobile network devices becomes large.

To solve the IP depletion problem, two techniques was proposed, address space expansion and address sharing. IP version 6 (IPv6) [2] is a solution based on address space expansion. In IPv6, the length of an IPv6 address is extended to 128 bits and therefore 2^{128} addresses are supported. However, using IPv6 is still infeasible in current stage because the routers that support IPv6 are not widely deployed. In the schemes based on address sharing, multiple hosts can share the same IP address. Network Address Port Translation (NAPT) [9] is the most widely used address sharing scheme. It is a variance of traditional Network Address Translation (NAT) [1] whereas the translation in NAPT is extended to IP addresses and transport identifiers. It translates (local IP address, local transport port number) to (public IP address, assigned transport port number). In this way, a group of intranet hosts using private addresses can share a single public IP address to access Internet services. NAPT provides a simple and efficient solution to the IP depletion problem.

In NAPT setup, NAPT server is deployed in the border of the intranet to perform address and port translation. An example of address and port translation is shown in Figure 1. Intranet host 10.0.0.1 connects to host 140.113.1.1 using 2002 as the source port and 10.0.0.1 as the source address. NAPT server intercepts the outgoing packet and replaces the source address 10.0.0.1 and source port 2002 with a globally unique IP address, 140.113.1.253 and a uniquely assigned port, 3456. Subsequently, NAPT server forwards this packet to the router. In the return path, NAPT server changes the destination address from 140.113.1.253 to 10.0.0.1 and destination port from 3456 to 2002.

There are some schemes that introduce the use of private addresses and NAT operations in Mobile IP. In 1999, Teo et al. proposed a scheme allowing a mobile node with a private home address to move to a private foreign network and maintains the same network connectivity [6]. Teo's scheme uses reverse tunnel [10] to transmit packets between a mobile node and a correspondent node. Every IP packet is transferred via foreign agent and home agent. Therefore,

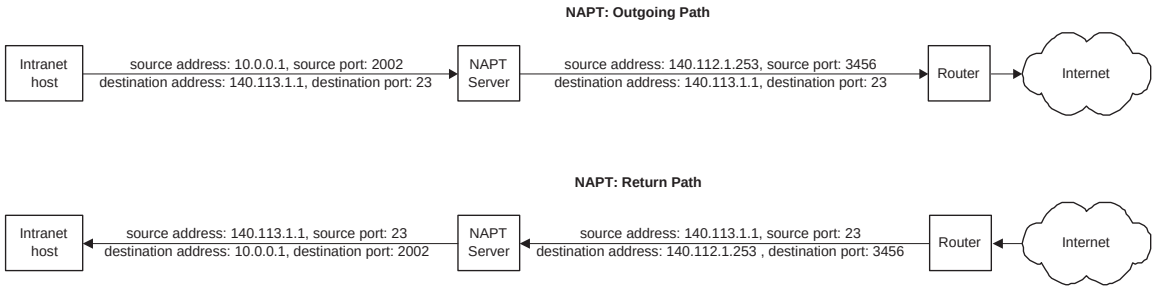

Figure 1: NAPT operations

Teo's scheme does not support route optimization [8] and has poor transmission efficiency. In 2001, Kato et al. proposed approaches that allow assigning private addresses to mobile nodes and support route optimization [11, 12]. However, in their approaches, every mobile node must acquire a distinct public IP address from the address pool of its home network. In this way, the size of the address pool becomes an upper bound to the number of mobile node that can connect to the Internet in the same time. In 2002, Levkowetz et al. proposed a scheme that enables a NAT device to uniquely identify a mobile node which resides behind it [14]. Similar with Teo's scheme, a reverse tunnel is required. Therefore, Levkowetz's scheme can not support route optimization.

In this paper, we present our solution to the IP depletion problem in mobile networks. By integrating Mobile IP and NAPT, our scheme allows mobile nodes with private addresses to access Internet services using the same public IP address in the same time. Moreover, route optimization is supported in our scheme. This paper is organized as follows. Section 2 elaborates requirements of a feasible scheme. In section 3, we describe the network model. Section 4 shows detail operations of the proposed scheme. In section 5, summary and brief conclusions are presented.

2 Requirements

To design a feasible scheme that incorporates Mobile IP with NAPT, there are three general requirements must be satisfied.

Connective Mobile node must be able to initiate connections or accept connections regardless of its current point of attachment. In other words, the mobile node can have the same network connectivity as it were in its home network.

Transparent Making the movement of a mobile node transparent to correspondent nodes and Internet routers is an important design principle of Mobile IP. On the other hand, hiding

the operation of address and port translation from the communicating entities is also an important design consideration in NAPT. Being transparent to communicating entities can avoid changing protocol stacks for adapting Mobile IP and NAPT. In other words, correspondent nodes and routers need not to be aware of the use of private address nor the movement of a mobile node. Also, address and port translation should not influence normal operations of mobile nodes and correspondent nodes. This can significantly reduce the difficulty of deployment.

Address Collision Tolerant Since intranets can use private addresses without any coordination with IANA [3], the same private address space can thus be utilized by many different intranets, i.e. mobile nodes belonging to different home network can use the same private address as their home address. Address collision might occur when two or more mobile nodes using the same private home address visit the same foreign network simultaneously. Moreover, address collision can also take place if a mobile node uses the same private address with one of the intranet hosts in the visited foreign network. Address collision tolerance is a fundamental requirement that must be satisfied.

3 Network Configurations and Operational Overview

In this section, we present our network model and provide an operational overview. In the proposed scheme, we classify all the mobile nodes into two categories. A mobile node that provides Internet services is considered as a *mobile server* or it is considered as a *mobile client*. Without specification, the term "mobile node" represents both mobile servers and mobile clients. Procedures that only applied to mobile servers or mobile clients will be specified particularly.

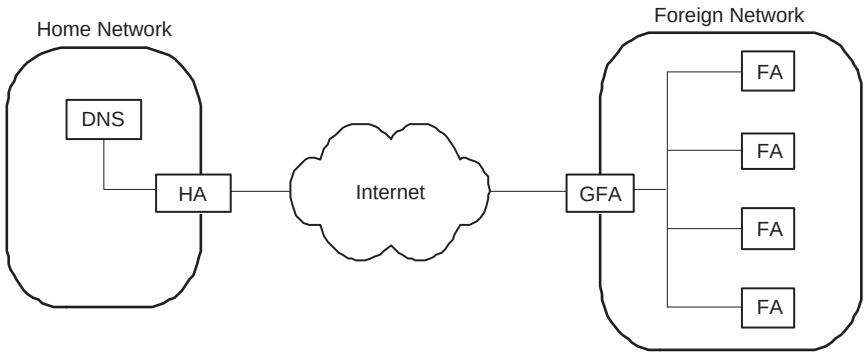

Figure 2: General network model

Our network model is depicted in Figure 2, showing one home network and one foreign network. In a mobile node's home network, home agent (HA) maintains location information

for the mobile node and tunnels messages to the mobile node when it is away from home. A home agent has a public IP address and manages a pool of public IP addresses. The public address pool is shared by the mobile nodes belonging to the home network. A mobile node has two home addresses, one private home address and one public home address. Private home address is a permanent private IP address assigned by HA uniquely. On the contrary, public home address is temporarily assigned to the mobile node for a pre-defined lifetime. When assigning public home address, home agent also specifies a list of port numbers to the mobile node. The assigned port numbers compose a *port partition*. By using disjointed port partitions, multiple mobile nodes can share the same public IP address without any confusion. Size of a port partition is determined by HA. A mobile client may have tens or hundreds of ports numbers in its assigned port partition while a mobile server always has a full-scaled port partition, i.e. 0-65535. Moreover, a mobile server must have a fully qualified domain name (FQDN). When the DNS server receives a DNS query containing the FQDN of a mobile server, it responds the query with the assigned public home address of the mobile server. Sometimes it might occur that the FQDN of a mobile server is not associated with a public home address, the DNS server must notify HA so that HA can assign a public home address to the mobile server. Therefore, DNS server in the home network must support dynamic update [5] such that the HA can update or insert address bindings in the DNS server when necessary.

In a foreign network, two hierarchy levels of foreign agents (FAs) are adopted to support regional registration [13]. With regional registration, propagation delay and overhead for exchanging registration messages is significantly reduce when a mobile node roams among the second level foreign agents. It also indirectly benefits HAs because number of registration requests is also reduced.

At the top level of the hierarchy, there is a gateway foreign agent, GFA. GFA acts as an edge router and a NAPT server of the foreign network. It must have a public IP address. At the second level of the hierarchy is a set of FAs. Each second level FA has a private address and acts as an access router of a private network. Since it has a network interface in the same link with hosts in the private network, it thus can obtain the MAC address of a visited mobile node and communicate with the mobile node via link layer transmission. To announce the presence of the GFA and FA, each FA must periodically broadcast the agent advertisement message containing the IP address of GFA and its own private address. When a mobile node first visits a new foreign network, it performs *home registration* to its HA. If the mobile node moves to another FA under the same GFA, it performs *regional registration* to the visited GFA.

In home registration, a mobile node registers the IP address of the visited GFA as its care-of

address. In the following context, we call this address as the *global care-of address* (GCOA) of the mobile node. A mobile node's GCOA changes only when it moves to a new foreign network dominated by another GFA. Moreover, the mobile node obtains a private address from the visited FA. The obtained private address is called *local care-of address* (LCOA) of the mobile node. LCOA indicates which second level FA that the mobile node resides and provides GFA local connectivity to the mobile node. In regional registration, the new visited FA assigns a new LCOA to the mobile node and GFA updates the registered LCOA. Briefly, through home registration and regional registration, HA keeps latest GCOA and GFA keeps latest LCOA of a mobile node.

Now, we briefly describe how a mobile node connects to a correspondent node. The mobile node starts the communication by sending a packet using its home private address as the source address. The access route of the private network, visited FA, intercepts the packet and forwards it to the GFA. In GFA, the source address is replaced with mobile node's public home address and source port is replaced with an unused port in the assigned port partition. After that, GFA forwards the packet. In the return path, packets destined to the mobile node's public home address are delivered to the home network. HA intercepts the packets and determines MN.GCOA according to the public home address and port number. Then, the packets are delivered to the visited GFA via a GRE tunnel. Similarly, GFA determines the LCOA of the mobile node and replaces the destination address and destination port of the packets. The packets are then transmitted to the visited FA via another GRE tunnel. Finally, visited FA transfers the packets to the mobile node by filling the MAC address of the mobile node in the link layer destination address.

4 Protocol Operations

In this section, we present the procedures of registration and communications. First, home registration which is performed when a mobile node arrives in a foreign network is presented. And then follows the regional registration. To start communication, a public home address and a port partition is obtained through the address allocation procedure. Finally, two communication procedures including mobile node originated packet transmission and mobile server terminated packet transmission are presented.

Before we detail each procedure, notations for describing our work are listed.

MN.MAC A MAC address of MN

MN.HA The public IP address of MN's home agent.

MN.PrHAddr MN's private home address.

MN.PuHAddr MN's temporarily assigned public home address.

MN.GCOA MN's global care-of address.

MN.LCOA MN's local care-of address.

MN.PP The port partition assigned to MN.

CN A correspondent node.

GFA.IP An IP address of a GFA.

Figure 3 illustrates an example of the general network model. In this setting, 140.113.1.0/24 is the address space of the home network and 140.113.1.1 is the IP address of the HA1. HA1 assigns private addresses in 192.168.1.0/24 to mobile nodes. In the foreign network, there are one GFA1 and two FAs. 140.112.1.1 is the IP address of GFA1. 10.0.1.254 is the IP address of FA1-1 and 10.0.1.0/24 is the private address space in the subnet of FA1-1. 10.0.2.254 is the IP address of FA1-2 and 10.0.2.0/24 is the private address space in the subnet FA1-2. In the following, we use this network configuration for illustrations.

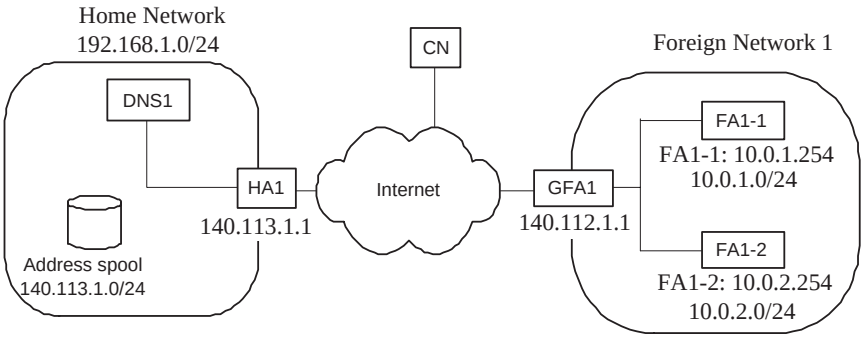

Figure 3: An example of network configuration

4.1 Home Registration

Figure 4 shows the procedure of home registration. MN performs home registration when it moves from its home network to a foreign network or moves from one foreign network to another with different GFA. IP address of the visited GFA is registered as GCOA of MN by home registration. Upon receipt of the home registration request from MN, the visited FA assigns a private address as LCOA of MN and forwards the packets via a GRE tunnel to GFA. GFA records MN.LCOA and forwards the home registration request to MN's HA after rewriting

the source address and source port of the packet. After the home registration, GFA records MN.LOCA, and HA records MN.GCOA.

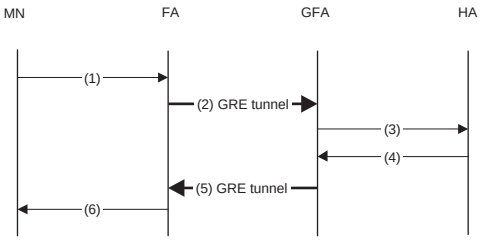

Figure 4: Procedure of home registration

1. After receiving the agent advertisement containing the IP addresses of the visited GFA and FA, MN sends home registration request containing GFA.IP as its GCOA to HA. In the packet header, MN.PrHAddr is the source address and an unused port, p1, is the source port.

2. Upon receipt of MN's home registration request, the visited FA allocates an unused private address as MN.LCOA, and maintains the mapping of assigned MN.LCOA and MN.MAC. In our example, If a mobile node, 192.168.1.1, visits FA1-1 in foreign network 1 and FA1-1 assigns 10.0.1.1 as the MN.LCOA, then FA1-1 must maintain the table illustrated below:

MN.HA	MN.PrHAddr	MN.LOCA	MN.MAC
140.113.1.1	192.168.1.1	10.0.1.1	00:d0:b7:2c:70:dc

   After assigning LCOA to MN, the visited FA encapsulates the home registration request by using GRE tunneling. The GRE tunnel uses GFA.IP and MN.LCOA as the end point addresses. Therefore, GFA will receive the home registration request at the opposite end of the tunnel.

3. After decapsulating the home registration request, GFA performs address and port translation. The source address and port are changed to GFA.IP and an unused port of GFA, $p1'$. The modified message will be delivered to HA through normal routing mechanism. Like FA does, GFA must maintain a mapping of (MN.HA, MN.PrHAddr) to MN.LCOA.

4. After successfully authenticating the registration request, HA updates GCOA of MN to GFA.IP. After that, HA sends the registration reply to MN using GFA.IP as the destination address and $p1'$ as destination port.

5. GFA performs address and port translation on the registration reply. According to the destination address (GFA.IP) and destination port ($p1'$), GFA replaces the destination

address and destination port with MN.PrHAddr and p1. GFA also determines MN.LCOA and tunnels the modified packets by using MN.LCOA as the destination address in the GRE header.

6. Visited FA decapsulates the packets and determines MN.MAC according to the destination address in the GRE tunnel. Then, FA sends the registration reply to MN using the MAC address as the link layer destination address.

4.2 Regional Registration

MN performs regional registration for registering a new LCOA to GFA when it moves to a new FA beneath the same GFA. Figure 5 shows the detail of regional registration.

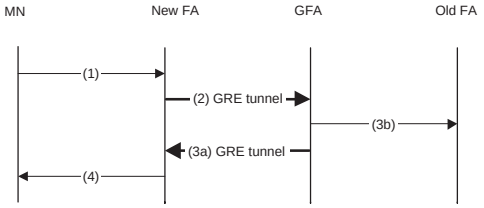

Figure 5: Procedure for regional registration

1. MN sends the regional registration request to visit GFA using MN.PrHAddr as the source address.

2. The new visited FA selects an unused private address as the new LCOA of MN. Similar with home registration, the new visited FA maintains a mapping of MN.LCOA to MN.MAC and tunnels the registration request to GFA using the new MN.LCOA as source address.

3. Upon receipt of the regional registration request, GFA updates the LCOA of MN and sends two messages to MN and old visited FA respectively.

   (3a) GFA informs the old FA to release old LCOA assigned to MN.

   (3b) GFA tunnels the regional registration reply by using new MN.LCOA as the destination address of the GRE tunnel.

4. The visited FA decapsulates the reply message and determines MN.MAC address according to the destination address of the GRE tunnel. FA sends the regional registration reply to MN by link layer transmission.

4.3 Address Allocation

Address allocation procedure is for assigning a public home address and a port partition to MN. Assigning disjointed port partitions allows a single IP address to be shared by multiple mobile nodes. Assigned public home address and port partition of MN must be recorded both in HA and the visited GFA. As a result, when receiving packets from CNs, HA can determine which MN is the receiver by examining the destination address and destination port of the packet. Furthermore, HA can tunnel the packet to GFA by using MN.GCOA. In the foreign network, when receiving tunneled packets from HA, GFA can perform address and port translation operations according to source address of the GRE tunnel, destination address and destination port in the inner packet header.

Address allocation is triggered by two events. First, when MN wants to connect to CN before obtaining a public home address and an assigned port partition from its HA , GFA must start the address allocation procedure, called GFA initiated address allocation. Second, when CN wants to connect to a mobile server and the mobile server has not gotten its public home address, DNS server in the home network should notify HA to start the address allocation procedure, called DNS initiated address allocation. Following, we present the detail of the two address allocation procedure.

4.3.1 GFA Initiated Address Allocation

As shown in Figure 6, GFA sends the address allocation request to MN's HA for allocating a public home address and a port partition.

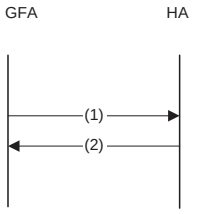

Figure 6: Procedure of GFA initiated address allocation

1. GFA sends the address allocation request containing MN.PrHAddr to MN's HA.

2. After receiving the request from GFA, HA authenticates the request and examines MN.PrHAddr. If MN is a mobile client, HA picks up a public IP address with one unused port partition. If MN is a mobile server, HA picks up an unused public IP from the address spool. Then, HA sends the reply containing the selected public home address and port partition. GFA

receives the reply and constructs the mapping of (MN.HA, MN.PrHAddr, MN.PuHAddr, MN.PP) to MN.LCOA.

4.3.2 DNS Initiated Address Allocation

Figure 7 shows the procedure that DNS triggers the address allocation.

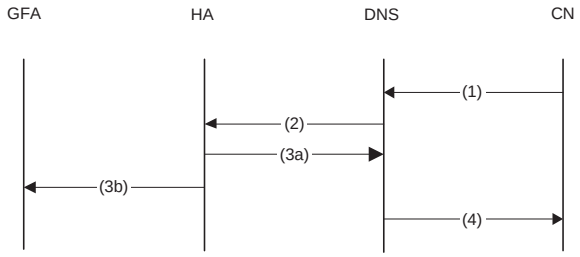

Figure 7: Procedure of DNS initiated address allocation

1. CN sends a DNS query message containing mobile server's FQDN to the DNS hierarchy. The query will be forwarded to the DNS server in MN's home network.

2. If the FQDN is associated with a public IP address, DNS server responds the query with the public IP address. Otherwise, DNS server sends notification to HA.

3. Upon receipt of the notification message from DNS server, HA selects an unused public IP address as MN's public home address and sends two messages to GFA and DNS respectively.

   (3a) HA sends dynamic update message to the DNS server for updating the address binding of the mobile server.

   (3b) HA sends address allocation message containing MN.PrHAddr and MN.PuHAddr to GFA. GFA records address translation mappings.

4. DNS server replies CN with MN.PuHAddr.

After a successful address allocation, MN can initiate connections or accept connections. To manipulate the packets transferred between MN and CN, HA, GFA and FA must construct their own address translation tables to record addresses and assigned port partition of a mobile node. We use Figure 3 to illustrate the operations. We assume that there are four mobile nodes,denoted as MN_1, MN_2, MN_3 and MN_4. Address information about the four mobile nodes are listed in table 1. Among the four mobile nodes, MN_1, MN_2 and MN_3 belong to the

MN	MN.HA	MN.PrHAddr
MN_1	140.113.1.1	192.168.1.1
MN_2	140.113.1.1	192.168.1.2
MN_3	140.113.1.1	192.168.1.3
MN_4	140.111.1.1	192.168.1.1

Table 1: Address information of mobile nodes.

same home network and MN_4 belongs to another. MN_4 has the same private home address with MN_1. Moreover, we assume that MN_3 is a mobile server while others are mobile clients.

Consider that all of the mobile nodes move to the private network of FA1-1 in foreign network 1. After home registration and address allocation, the four mobile nodes obtain their LCOAs and register IP address of the GFA in their home agents. Moreover, MN_1 and MN_2 share 140.113.1.2 as their public home address and obtain port partitions, 100-200 and 200-300 respectively. Since MN_3 is a mobile server, it occupies 140.113.1.3 as its public home address and a full scaled port partition, 0-65535. MN_4 obtains 140.111.1.2 as its public home address and 100-200 as its port partition. The address translation tables in HA1, GFA1 and FA1-1 are shown in table 2, table 3 and table 4. MN_4's home agent has similar table with HA1.

MN.PrHAddr	MN.COA(MN.GCOA)	MN.PuHAddr	MN.PP
192.168.1.1	140.112.1.1	140.113.1.2	100-200
192.168.1.2	140.112.1.1	140.113.1.2	200-300
192.168.1.3	140.112.1.1	140.113.1.3	0-65535

Table 2: Address translation table in HA1

MN.HA	MN.PrHAddr	MN.LCOA	MN.PuHAddr	MN.PP
140.113.1.1	192.168.1.1	10.0.1.1	140.113.1.2	100-200
140.113.1.1	192.168.1.2	10.0.1.2	140.113.1.2	200-300
140.113.1.1	192.168.1.3	10.0.1.3	140.113.1.3	0-65535
140.111.1.1	192.168.1.1	10.0.1.4	140.111.1.2	100-200

Table 3: Address translation table in GFA1

According to table 2, when HA1 receives a packet with destination address 140.113.1.2 and destination port 101, HA1 can determine the receiver, MN_1 , and tunnel the packet to 140.112.1.1. In foreign network 1, GFA1 receives the tunneled packet and determines the receiver according to (source address in the GRE tunnel, destination address in the inner packet

MN.HA	MN.PrHAddr	MN.LCOA	MN.MAC
140.113.1.1	192.168.1.1	10.0.1.1	00:d0:b7:2c:70:dc
140.113.1.1	192.168.1.2	10.0.1.2	00:90:cc:0b:32:bd
140.113.1.1	192.168.1.3	10.0.1.3	00:02:b3:4d:44:c0
140.111.1.1	192.168.1.1	10.0.1.4	00:a1:b2:2d:44:cd

Table 4: Address translation table in FA1-1

header, destination port number in the inner packet header). In this way, GFA1 can distinguish MN_1 and MN_4 and then can determine MN_1 as the receiver of the packet. Before tunneling the inner packet to 10.0.1.1, GFA1 replaces the destination address with MN.PrHAddr, 192.168.1.1, and rewrites the destination port if necessary. Subsequently, the packet can be delivered to the visited FA, FA1-1. Then, FA1-1 determines the MAC of the receives by (destination address of the GRE tunnel, destination address of the inner packet header). Finally, FA1-1 decapsulates the tunneled packet and delivers the packet to MN_1 using MN.MAC as link layer destination address.

4.4 Mobile node originated packet transmission

Figure 8 shows the procedure that MN connects to CN.

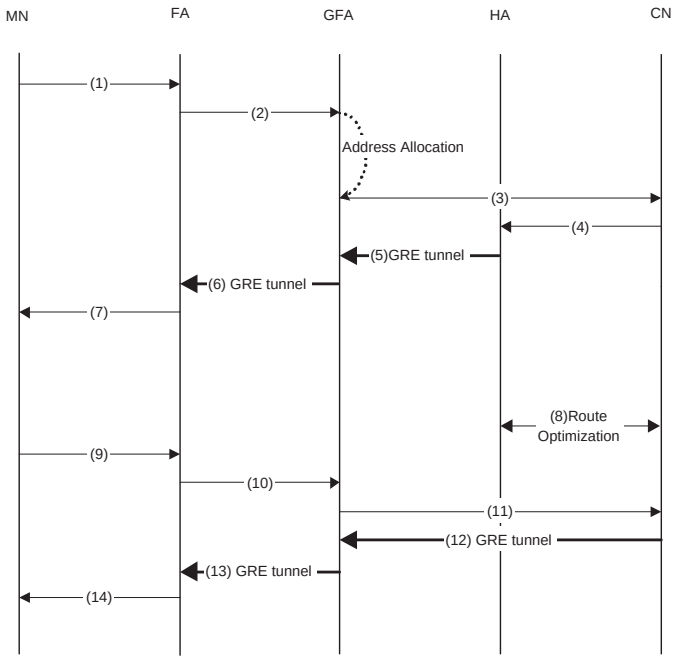

Figure 8: A mobile node connects to a correspondent node

1. MN sends packets to CN using MN.PrHAddr as source address.

2. FA forwards the packet to GFA.

3. Upon receipt of the packet, GFA looks for MN.PuHAddr in its address translation table. If the MN does not have a public home address and a port partition, GFA starts the address allocation procedure. After allocating a public home address and a port partition for MN, GFA replaces the source address of the outgoing packet with MN.PuHAddr and the source port with a port number in the assigned port partition. Then, GFA forwards this packet to CN.

4. In the return path, CN sends the packet to MN using MN.PuHAddr as the destination address. The packet will be routed to MN's home network.

5. HA uses (destination address, destination port number) of the packet to determine MN.GCOA and tunnels the packet to the address found. In this way, the packet will be delivered to GFA.

6. After decapsulating the packet, GFA uses (source address of the GRE tunnel, destination address in the inner packet header, port of the inner packet header) to map to MN.PrHAddr and MN.LCOA. Then, GFA rewrites the destination address and port of the inner packet header. Subsequently, GFA tunnels the modified packet using MN.LCOA as the destination address of the tunnel.

7. FA decapsulates the packet and uses (destination address of the GRE tunnel, destination address of the inner packet header) to map to MN.MAC. Then, the packet is delivered to MN using the MAC address.

Steps 8-14 are optional. If CN, HA and GFA support route optimization, following steps can be adopted to increase transmission efficiency.

8. In this step, HA and CN exchange *Binding Update* and *Binding Acknowledge* [8] messages for route optimization.

9. This step is the same with step 1.

10. This step is the same with step 2.

11. This step is the same with step 3.

12. CN sends the packets to MN via GFA instead of via HA. Packets are transferred to GFA through a GRE tunnel between CN and GFA.

13. This step is the same with step 6.

14. This step is the same with step 7.

4.5 Mobile server terminated packet transmission

Figure 9 shows the procedure that a mobile server accepts a connection from CN.

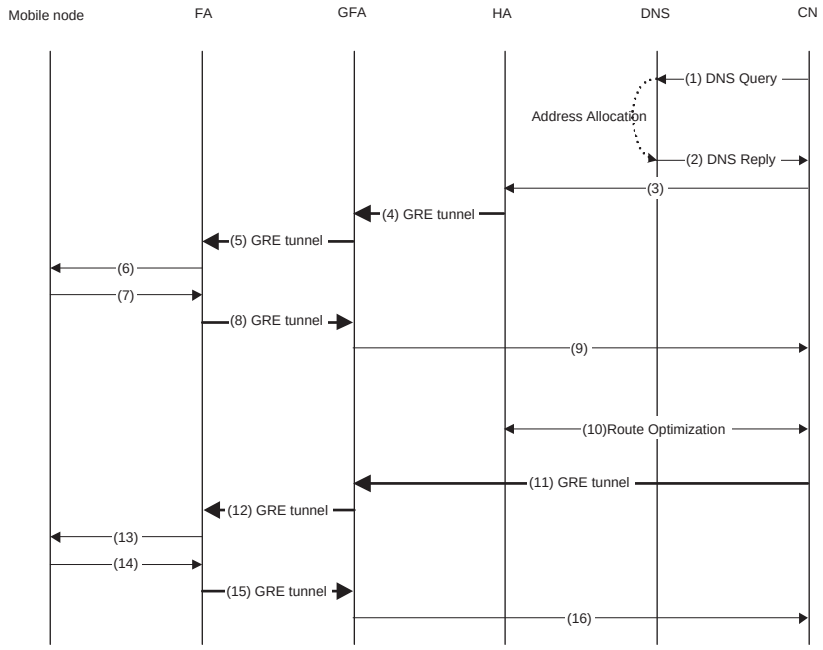

Figure 9: A mobile server accepts a connection from a correspondent node

1. To connect to a mobile server, CN must send DNS query to the DNS hierarchy for mobile server's IP address. This would trigger the assignment of a public home address to the mobile server if the mobile server does not have a public home address. The procedure can be found in section 4.3.

2. The DNS replies the assigned public home address to CN.

3. After receiving the DNS reply, CN sends the packet to the mobile server using the MN.PuHAddr as the destination address. The packet will be routed to mobile server's home network.

4. HA uses the (destination address, destination port number) to determine MN.GCOA. Then, HA tunnels the packet by using MN.GCOA as the destination of the GRE tunnel.

5. GFA decapsulates the packet and replaces the destination address of the packet with mobile server's private home address. Then, GFA tunnels the packet to mobile server using MN.LCOA

6. FA decapsulates the packet and sends the packet to mobile server using MN.MAC.

7. In the return path, MN sends the packet using its MN.PrHAddr as the source address.

8. FA relays the packet to GFA.

9. GFA replaces the source address with MN.PuHAddr and forwards the modified packet to CN.

Steps 10-16 are optional. If CN, HA and GFA support route optimization, following steps can be adopted to increase transmission efficiency.

10. In the step, HA and CN exchange *Binding Update* and *Binding Acknowledge* [8] messages for route optimization.

11. CN sends the packets to MN via GFA instead of via HA. Packets are transferred to GFA through a GRE tunnel between CN and GFA.

12. This step is the same with step 5.

13. This step is the same with step 6.

14. This step is the same with step 7.

15. This step is the same with step 8.

16. This step is the same with step 9.

5 Conclusions

In this paper, we have proposed a scheme that incorporates Mobile IP with NAPT to realize address sharing for mobile nodes. Procedures for registration and packet transmission are presented. Briefly, our scheme has the following features:

- To satisfy the requirement of connectivity, we classify all the mobile node into two categories: mobile client and mobile server. Multiple mobile clients belonging to the same home network can access Internet services using the same public home IP address and disjointed port partitions. For mobile servers, the ability to accept connections is reserved.

- Our scheme is designed to tolerant to address collision because two or more mobile nodes using the same private home address can coexist in the same network. GFA can distinguish packets of different mobile nodes with the same private home address according to the

source address of the GRE tunnel. Similarly, FA can achieve this by the destination address in the GRE tunnel, MN.LCOA.

- Our scheme is transparent to mobile nodes, correspondent nodes and Internet routers. It is unnecessary to change their protocol stacks for supporting our scheme.
- Hierarchical network configuration is adopted in our network model for supporting of regional registration. Thus signaling overhead and propagation delay of registration messages is significantly reduced when mobile node moves from one FA to another beneath the same GFA.
- Our scheme supports route optimization. This can further improve the transmission efficiency.

Integrating Mobile IP and NAPT is an effective solution for Mobile IP to accommodate more network devices. But there are two issues left for more study. First, the size of a port partition must be set appropriately. It determines how many mobile nodes can share one public IP address simultaneously and how many connections a mobile node can have in the same time. Second, a mechanism to manage the lifetime of the assigned public home address is required. With an effective lifetime management, a port partition can be released in time when another mobile node needs it. The two issues is worthy of more investigation for a more robust scheme.

References

[1] K. Egevant and P. Francis, "The IP Network Address Translator," IETF RFC 1631, May 1994.

[2] S. Deering and R. Hinden, "Internet Protocol version 6 (IPv6) Specification," IETF RFC 1883, Dec. 1995.

[3] Y. Rekhter, B. Moskowitz, D. Karrenberg, G. J. de Groot and E. Lear, "Address Allocation for Private Internets," IETF RFC 1918, Feb. 1996.

[4] C.Perkins, "IP Mobility Support," IETF RFC 2002, Oct. 1996.

[5] P. Vixie, S. Thomson, Y. Rekhter and J. Bound, "Dynamic Updates in the Domain Name System (DNS UPDATE)," IETF RFC 2136, Mar. 1997.

[6] W. T. Teo and Y. Li, "Mobile IP extensions for Private Internets Support(MPN)," IETF Internet-Draft: draft-teoyli-mobileip-mvpn-02.txt, Sep. 1999.

[7] 3rd Generation Partnership Project 2, "Wireless IP Architecture Based on IETF Protocols," Jul. 2000.

[8] C. Perkins and D. Johnson, "Route Optimization in Mobile IP," IETF Internet-Draft: draft-ietf-mobileip-optim-11.txt, Nov. 2000.

[9] P. Srisuresh and K. Egevang, "Traditional IP Network Address Translator(NAT)," IETF RFC 3022, Jan. 2001.

[10] G. Montenegro, "Reverse Tunneling for Mobile IP, revised," IETF RFC 3024, Jan. 2001.

[11] Kato, T., Idoue, A. and Yokota, H., "Mobile IP Using Private Addresses," *Sixth IEEE Symposium on Computers and Communications*, pp. 491–497, 2001.

[12] Idoue, A., Yokota, H. and Kato, T., "Mobile IP Network Supporting Private IP Addresses Utilizing Regional Registration and NAT Function," *Eigth International Conference on Parallel and Distribution Systems*, pp. 141–146, 2001

[13] Eva Gustafsson, Annika Jonsson and Charles E. Perkins, "Mobile IPv4 Regional Registration," IETF Internet-Draft: draft-ietf-mobileip-reg-tunnel-06.txt, Mar. 2002.

[14] H. Levkowetz and S. Vaarala, "Mobile IP NAT/NAPT Traversal using UDP Tunnelling," IETF Internet-Draft: draft-ietf-mobileip-nat-traversal-02.txt, Apr. 2002.