Mobile IP Using Private Care-of Addresses

Yu-Huei Tseng and Wen-Shyang Hwang

Department of Electrical Engineering,
National Kaohsiung University of Applied Sciences, Kaohsiung, ROC

Abstract

Mobile networking is becoming popular. The increasing mobile communications make the lack problem of the number of addresses in IPv4 more serious. In order to improve the problem, this paper proposes an approach to fulfill a mobile IP protocol by using a private IP address for the care-of address. The address is assigned by the foreign agent while a mobile node visits the foreign network. In this approach, the foreign agent uses the NAT (Network Address Translation) technology to allow a correspondent node making a connection to a mobile node. This paper will describe the detailed design of the approach.

1. INTRODUCTION

1.1 Motivation

There is no doubt that the networking world's ultimate goal is anywhere, anytime, continuously connected computing, hence the mobility is becoming a requirement rather than a comfort. With the cellular phone, people have tasted the flexibility roaming provides, and the freedom from a fixed network. The demand for laptop computers with connectivity to the Internet is yet another example. In fact, IP implicitly assumes that a host location is fixed, and the IP address registered to the host is a direct function of the network that the host is connected to. This provides the underlying mechanism for datagrams to be properly routed.

People would like to be able to roam from network to network seamlessly. The Mobile-IP working group of the Internet Engineering Task Force (IETF) has developed a standard to do just that. The standard, now called Mobile IP [1], is an enhancement to the standard IP, is used as a basis for the architecture of mobile networks. Accordingly, experts forecast the number of IPv4 addresses, using in the currently mobile IP, will be exhausted before 2005. In order to resolve this problem, the use of IPv6 [2] is widely considered and the mobile IP using IPv6 is being standardized in IETF [3]. However, IPv6 and mobile IPv6 are not widely spread in the current stage. In convention, the private IP addresses and NAT (Network Address Translator) [4] are used for IPv4 networks, that is non-mobile, to resolve the IP address starvation problem. There is a specific range of IP addresses are used as the private IP addresses [5], and a closed network can be constructed using those addresses without paying any attentions to the overlap of IP addresses in other closed networks. Only when a node in a closed network wants to communicate with other nodes located outside of the closed network, a router with NAT function (a NAT router) at the border of the closed network assigns to the node one of the global IP addresses which the NAT router maintains.

Therefore, it is considered that the IP address starvation in the mobile IPv4 can also be resolved by introducing private IP addresses for mobile nodes. There are some approaches for the mobile IP using private IP addresses proposed so far. In IETF, the private IP-in-IP encapsulation (PIPE) [6] is proposed by cooperating with reverse tunneling in the direction from FA (Foreign Agent) to HA (Home Agent) [7], it can allow IP packets to be forwarded from a MN (Mobile Node) with private home IP address to HA with private IP address. The paper [8] expands this mechanism using reverse tunneling and PIPE to the environment where a hierarchical FA levels are introduced for the regional registration [9]. However, they cannot use the route optimization [10], which allows an IP packet to be transferred directly between a correspondent node and FA in both directions, since an IP packet between a mobile node and a correspondent node is always transferred via FA and HA. Therefore, the private mobile IP approaches mentioned above are considered to be insufficient. In order to improve private IP performance mentioned above, Mobile IP using private IP addresses [11], which allows to assign a private IP address to a mobile terminal, no need to use reverse tunneling, so route optimization [10] can be used to the network, but foreign agent and home agent must install NAT function, and home agent also need to install DNS server inside itself. This obviously heavily weighted the workload of foreign agent and home agent, especially home agent.

In this paper, we proposed a middle solution for the shortage of IP addresses. Only foreign agent needs to install NAT function. This paper describes the details of procedures for the mobile IPv4, which allows a mobile node to use a private care-of address. This paper consists of the following sections. Section 1 is introduction for mobile IP, including motivation and mobile IP characteristics. Section 2 and 3 describe design principle and the detail procedures for mobile IPv4 with private care-of addresses, respectively. Section 4 describes the discussions on management of lifetime.

1.2 Mobile IP Characteristics

The general characteristics of mobile IP address include the following [12]:

- **Transparency**. Mobility is transparent to applications and transport layer protocols as well as to routers not involved in the change. In particular, as long as they remain idle, all open TCP connections survive a change in network and are ready for further use.
- **Interoperability with IPv4**. A host using mobile IP can interoperate with stationary hosts that run conventional IPv4 software as well as with other mobile hosts. Furthermore, no special addressing is required– the addresses assigned to mobile hosts do not differ from addresses assigned to fixed hosts.
- **Scalability**. The solution scales to large Internets. In particular, it permits mobility across the global Internet.
- **Security**. Mobile IP provides security facilities that can be used to ensure all messages are authenticated (i.e., to prevent an arbitrary computer from impersonating a mobile host).
- **Macro Mobility**. Rather than attempting to handle rapid network transitions such as one encounters in a wireless cellular system, mobile IP focuses on the problem of long-duration moves. For example, mobile IP works well for a user who takes a portable computer on a business trip, and leaves it attached to the new location for a week.

2. DESIGN PRINCIPLES

2.1 Requirements

We identify the following requirements to fulfill the mobile IP using private care-of addresses (private IP for care-of addresses). When a mobile node communicates with a node through a global IP network, a global care-of address (global IP for care-of address) will be temporarily assigned to this mobile node, and the mapping between the global home address (global IP for home address), global care-of address and private care-of address will be maintained during this communication. According to the mobile IP characteristics, mobile IP is designed for macroscopic mobility rather than high-speed movement.

As described above, the call acceptance by a mobile node with global home address and private care-of address is essential in this situation. NAT function is used by FA only to assign a global care-of address for the case that a node with global home address and private care-of address accesses a server in the global Internet. Therefore, it is required to allow a correspondent node to make a call to a mobile node with private care-of address. A mobile node in a visited network will not always communicate with other nodes but will be waiting for accepting a call. While accepting a call, it needs to register its location to its HA. Therefore, the lifetime of registration of the mobile IP and that of global care-of address assignment need to be managed independently. The requirements described above needs to be fulfilled by a procedure which is consistent with the mobile IP and which does not impose any limitations on the mobile IP and related procedures.

2.2 Design Principles

Based on the requirements described above, we adopted the following design principles to fulfill mobile IP using private care-of address.

(1) Each mobile node has a global/unique IP address as home address assigned in its home network. If the mobile node moves away from home network, it obtains a new secondary address, and informs the home agent of its new location by Registration Request message [1]. When the mobile returns home, it must contact the home agent to deregister, meaning that the home agent will stop intercepting datagrams. While a mobile node is connected to its home network, it works as fixed-host non-mobile way.
(2) HA and FA work as a router located at the border of its network. In addition, they provide mobility agent function. FA must support NAT function.
(3) When a mobile node moves to a visited network, it obtains a private care-of address by FA, and uses this address to register with its related HA.
(4) When the mobile node communicates with a correspondent node (CN) located outside of the visited network, the private care-of address of the mobile node will be mapped to temporarily global care-of address by FA with NAT function. And the result will inform its related HA.
(5) FA's NAT function assigns a global care-of address corresponding to the private care-of address of a mobile node, when the node communicates with CN. We maintain the lifetime of this global care-of address independent of the location registration of the mobile node. While a mobile node communicates using the global care-of address, its lifetime will continue to be expanded. Since the maintenance of the global care-of address is to be performed by the NAT function of FA, we introduce the coordination procedure for

synchronizing the lifetime of global care-of address.

3. COMMUNICATION PROCEDURE

Based on the design principles described in the previous section, we have designed the following procedures and data structures in order to fulfill the mobile IP using private care-of addresses.

3.1 Procedure for Mobile Node Registration

Figure 1 shows the procedure that a Mobile Node (MN) registers its location to Home Agent (HA) when it moves to a visited network.

(1) When MN moves to a visited network, it maybe sends Agent Solicitation message in order to discover, or it discovers an Agent Advertisement message sent by FA [1]. So MN obtains the IP address of FA and a related private COA by this message.

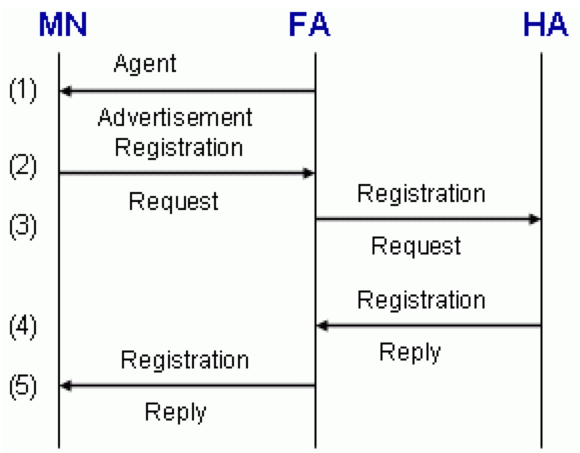

Figure 1. *Procedure for Registration*

(2) MN sends a Registration Request message to FA. In this message, the source and destination addresses are the global IP addresses of MN and FA, respectively. The care-of address of this message is the private IP address assigned by FA.

(3) FA receives this Registration Request message and it relays it to HA. In this message, the source and destination addresses are the global IP addresses of FA and HA, respectively.

(4) If the Registration Request is valid, then HA updates the MN's binding entry. And HA responds the Registration Request message by a Registration Reply message. In this message, the source and destination addresses are the global IP addresses of HA and FA, respectively.

(5) FA sends a Registration Reply message to MN.

It can be said that the Registration procedures of the mobile IP works well even if a mobile node uses a private care-of address.

3.2 Procedure for Mobile Node Initiated Communication

Figure 2 shows the procedure of communication where a mobile node MN with a global home address and a private care-of address accesses to a correspondent node CN which is connected to the global IP network.

(1) MN sends an IP packet containing higher level protocol data to CN. The source IP address of this packet is the global IP address of MN IP_{glo}(MN) and the destination IP address is the global IP address of CN IP_{glo}(CN). This packet is transferred to FA with NAT function, which works as a border router.

(2) FA checks whether a global COA address is already assigned to MN. If not, FA will select one of the global IP addresses and assign it to MN as a global COA address. We call it IP_{gCOA}(MN). Then FA informs HA of sending a global COA address assigned message, including the lifetime of the IP_{gCOA}(MN). After that, FA maintains the mapping among IP_{pCOA}(MN), IP_{gCOA}(MN), its lifetime, IP_{glo}(HA) and IP_{glo}(MN). And HA maintains the mapping among IP_{pCOA}(MN), IP_{gCOA}(MN), its lifetime, IP_{glo}(FA) and IP_{glo}(MN).

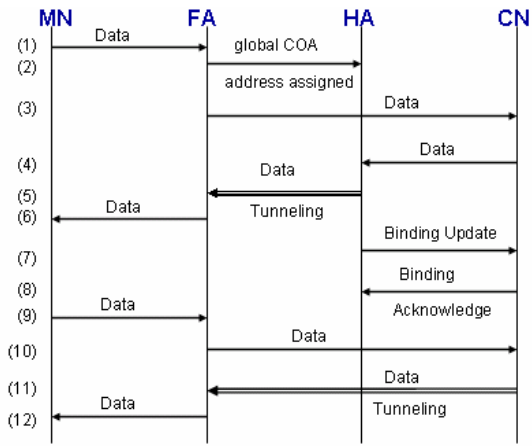

Figure 2. *Procedure for MN Initiated Communication*

(3) The IP packet will be delivered from FA to CN by normal IP routing.

(4) CN sends a reply IP packet to IP_{glo}(MN). Since IP_{glo}(MN) is an IP address maintained by HA, this reply packet will be delivered to the home network and be intercepted by HA. This is a normal procedure of the mobile IP.

(5) HA forwards the incoming IP packet to FA using IP-within-IP encapsulation, which has the IP_{gCOA}(MN) as the care-of address.

(6) When FA receives this encapsulated IP packet, it

will take the original IP packet which CN transmitted. Then FA sends this packet to MN.

(7) If the route optimization is supported by HA and CN, HA will require CN to transfer IP packets destined to MN directly to FA using IP-within-IP encapsulation. This is a normal procedure of the route optimization of the mobile IP. Actually, this is fulfilled by the exchange of a Binding Update message and a Binding Acknowledgement message. HA send a Binding Update message to CN.

(8) CN responds a Binding Acknowledge message to HA.

(9) MN sends an IP packet in response to the packet received in (6).

(10) FA receives this IP packet and forwards it to CN by normal IP routing. This will be received by CN.

(11) When CN replies to this IP packet, it will send the reply to FA using IP-within-IP encapsulation, which has the IP_{gCOA}(MN) as the care-of address. This is a normal procedure of the route optimization.

(12) FA decapsulates the packet transmitted by CN to FA. Then FA will forward the original packet to MN.

3.3 Procedure for Correspondent Node Initiated Communication

Figure 3 shows the procedure of communication where a mobile node MN with a global home address and a private Care-of address accepts a call initiated by a correspondent node CN which is connected to the global IP network.

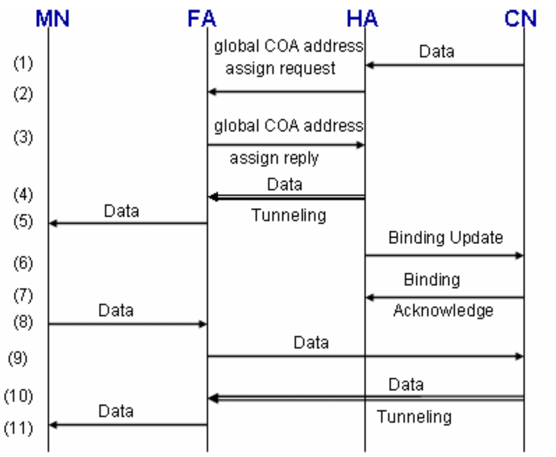

Figure 3. *Procedure for CN Initiated Communication*

(1) CN sends an IP packet to MN. The source IP address of this packet is the global IP address of CN (IP_{glo}(CN)) and the destination IP address is the global IP address of MN (IP_{glo}(MN)). Firstly, this packet will be delivered to the home network and be intercepted by HA. This is a normal procedure of the mobile IP.

(2) HA checks whether a global COA address is already assigned to MN. If not, it will send a global COA address assign request message to FA with NAT function.

(3) FA has several global IP addresses used by mobile nodes belonging to this FA. FA will select one of the global IP addresses and assign it to MN as a global COA address IP_{gCOA}(MN). Then FA informs HA of sending a global COA address assign reply message, including the lifetime of the IP_{gCOA}(MN). After that, FA maintains the mapping among IP_{pCOA}(MN), IP_{gCOA}(MN), its lifetime, IP_{glo}(HA) and IP_{glo}(MN). And HA maintains the mapping among IP_{pCOA}(MN), IP_{gCOA}(MN), its lifetime, IP_{glo}(FA) and IP_{glo}(MN).

(4) HA forwards the incoming IP packet to FA using IP-within-IP encapsulation, which has the IP_{gCOA}(MN) as the care-of address.

(5) When FA receives this encapsulated IP packet, it will take the original IP packet which CN transmitted. Then FA sends this packet to MN.

(6) This step shows route optimization. HA requires CN to transfer IP packet directly to FA by sending a Binding Update message to CN.

(7) CN responds a Binding Acknowledge message to HA.

(8) MN sends an IP packet in response to the packet received in (5).

(9) FA receives this IP packet and forwards it to CN by normal IP routing. This will be received by CN.

(10) When CN replies to this IP packet, it will send the reply to FA using IP-within-IP encapsulation, which has the IP_{gCOA}(MN) as the care-of address. This is a normal procedure of the route optimization.

(11) FA decapsulates the packet transmitted by CN to FA. Then FA will forward the original packet to MN.

3.4 Date Structures

The following data structures are required to fulfill the procedures described above.

3.4.1 Data Structure in FA

FA has a data structure managing the mobile nodes currently locating under its network. This structure has an entry corresponding to one mobile node and each entry contains the following fields:

- The home address of the mobile node IP_{glo}(MN).
- The MAC (Media Access Control) address of the mobile node. FA obtains this address when the mobile node sends a Registration Request message at the registration procedure.
- The address of HA IP_{glo}(HA).

- The lifetime of the registration to HA, indicating when this registration expires to exist.
- The global IP address IP_{gCOA}(MN) assigned for the mobile node by FA with NAT function, if the node is communicating.
- The lifetime of the global IP_{gCOA}(MN) address of the mobile node, indicating the remaining lifetime for the use of this address.
- The private IP address IP_{pCOA}(MN) assigned for the mobile node by FA when the mobile node moves to this corresponding area.

3.4.2 Data Structure in HA

HA has a data structure managing the mobile nodes belonging to it. This structure has an entry corresponding to one mobile node and each entry contains the following fields:

- The home address of the mobile node IP_{glo}(MN).
- The address of FA IP_{glo}(FA), if the mobile node is away from the home network..
- The lifetime of the registration by FA, indicating when this registration expires to exist.
- The global IP address IP_{gCOA}(MN) for the mobile node if assigned.
- The lifetime of the global IP_{gCOA}(MN) address of the mobile node if assigned.
- The private IP address IP_{pCOA}(MN) for the mobile node if the mobile node moves to a visited network.

4. MANAGEMENT OF LIFETIME

In the proposed approach, there are two kinds of lifetime; the lifetime of the MN registration, and the lifetime of the global Care-of address assignment. In order to keep them consistent, we adopt the following ways:

(1) The lifetime of the MN registration is handled according to the mobile IP standard. That is, the lifetime of MN registration is maintained by MN, FA, and HA. The lifetime value will be determined during the registration procedure. If the lifetime becomes close to the expiration and MN continues to being located in this visited network, MN will send another Registration Request message to renew the registration.

(2) The lifetime of global care-of address assignment needs to be managed independent of that of the MN registration. A global care-of address will be assigned to a MN only while it is actually communicating with other nodes connected to the global IP network. Even if a MN is registered to HA, a global care-of address is not assigned if it is not communicating. In order to fulfill this requirement, we adopt the following procedures:
    - When FA with NAT function assigns a global care-of address, it informs HA of the address and its lifetime.
    - The lifetime of this global care-of address needs to be expanded while MN communicates using it. Basically, FA can detect this communication, but HA can't always detect it because HA does not join IP packet transfer from MN to CN in the case of route optimization. Therefore, we have decided that FA handles the expansion of the lifetime of global care-of addresses. After a global care-of address assigned to MN, FA expands the lifetime of this care-of address if MN sends or receives any IP packets. FA also maintains the latest lifetime value of which it informs HA. We call this value the Latest Care-of address lifetime. If the latest care-of address lifetime becomes close to the expiration and the actual lifetime managed by FA is larger than that, FA sends a Care-of Address Assign Expansion message to HA in order to inform the new lifetime value.
    - When the lifetime of MN registration expires at FA, FA will clear the lifetime of global care-of address. Before clearing it, FA sends a Care-of Address Assign Expansion message to HA in order to inform latest care-of address lifetime value.

5. CONCLUSIONS

In this paper, we have proposed an approach to assign the private care-of addresses to individual mobile nodes when they are visiting the networks and to allocate global care-of addresses to them only during they communicate with correspondent nodes (CNs) in the global IP networks. So far, there are some proposals on private IP address based mobile IP, but they are based on the reverse tunneling where the communication of mobile nodes in both directions is transferred between home agents (HAs) and foreign agents (FAs), or weighted the workload of foreign agents (FAs) and home agents (HAs) if no need reverse tunneling.

This approach proposed a middle solution for the lack of IP addresses. It introduces NAT functions in FA only. When a MN in a visited network, it will obtain a private care-of address, and then register the address to its HA. When a MN starts communication with a CN in the global IP network, or a CN starts communication with a MN, FA with NAT function assigns a global care-of address to this mobile node and informs this to its HA. After communication, the global care-of address will be released.

This paper describes the detailed design of the proposed approach that includes the methods to coordinate among lifetimes for MN registration and the global care-of address assignment. This approach is an effective technique for resolving the IP address starvation in the mobile IP version 4.

REFERENCES

[1] C. Perkins, editor, "IP Mobility Support," RFC 2002, October 1996.

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

[3] D. Johnson and C. Perkins, “Mobility Support in IPv6,” work in progress, available at draft-ietf-mobileip-ipv6-12.txt, April 2000.

[4] K. Egevang and P.Francis, “The IP Network Address Translator (NAT),” RFC 1631, May 1994.

[5] Y. Rekhter, et al., ”Address Allocation for Private Internets,” RFC 1597, March 1994.

[6] B. Petri, “Private IP Encapsulation within IP (PIPE),” work in progress, available at draft-petri-mobileip-pipe-00.txt, July 2000.

[7] G. Montenegro, Editor, “Reverse Tunneling for Mobile IP, revised,” RFC 3024, January 2001.

[8] J. Malinen, “Using Private Addresses with Hierarchical Mobile IPv4,” Master’s Thesis at Helsinki University of Technology, available at http://www.cs.hut.fi/Research/Dynamics/publications.html, March 2000.

[9] E. Gustafsson, A. Jonsson and C. Perkins, et al., “Mobile IPv4 Regional Registration,” work in progress, available at draft-ietf-mobileip-reg-tunnel-06.txt, March 2002.

[10] C. Perkins and D. Johnson, “Route Optimization in Mobile IP,” work in progress, available at draft-ietf-mobileip-optim-10.txt, February 2000.

[11] *Kato, T.; Idoue, A.; Yokota, H.* ,” Mobile IP using private IP addresses**,”** Computers and Communications, 2001. Proceedings. Sixth IEEE Symposium on , 2001.

[12] Douglas E. Comer, “Internetworking with TCP/IP principles, protocols, and architectures,” Chapter 19 mobile IP, fourth edition, Prentice Hall International, Inc. 2000.