Journal of Computer Science 2 (2): 211-217, 2006
ISSN 1549-3636
© 2006 Science Publications

On using Mobile IP Protocols

Fayza A. Nada
Faculty of Computers and Information, Suez Canal University, Ismailia, Egypt

Abstract: The recent advances in wireless communication technology and the unprecedented growth of the Internet have paved the way for wireless networking and IP mobility. Mobile Internet protocol has been designed within the IETF to support the mobility of users who wish to connect to the Internet and maintain communications as they move from place to place. This study describes and summarizes the current Internet draft for mobile IP (MIPv4) with its major components: agent discovery, registration and tunneling. In addition, we outline the available encapsulation techniques and route optimization procedure. In the end, we describe the design of the new protocol for transparent routing of IPv6 packets to mobile IPv6 nodes operating in the Internet.

Key words: Mobile IP, MIPv4, MIPv6, mobile networking, encapsulation, route optimization

INTRODUCTION

Mobile communications services have experienced remarkable growth and among these, services providing Internet access from mobile terminals are steadily increasing by tens of thousands of subscribers per day[1]. To create IP-based mobility management mechanism, efforts are being made to implement mobility management at the IP level (so called IP mobility) by using IP addresses, for example, instead of managing the movement of terminals within a mobile network according to the conventional mobile terminal number or subscriber number[2]. Advantages of implementing IP mobility include the ability to implement universal mobility management mechanisms independent of specific access networks and the ability to provide seamless mobile services spanning wireless access network generations and even heterogeneous access networks including both mobile and fixed networks. Since IP mobility supports the implementation of network integration and services between mobile and fixed networks, it is becoming an important technology not only for mobile networks but also for fixed networks[3].

Mobile IP is an Internet protocol designed to support host mobility. Its goal is to provide the ability of a host to stay connected to the Internet regardless of its location. Mobile IP is able to track a mobile host without needing to change the mobile host's long term IP address[4]. IP addresses are used to identify a particular end system. One can use an IP address to identify one particular node out of the tens of millions of computer nodes making up the Internet. Popular transport protocols such as Transmission Control Protocol (TCP)[5] keep track of their internal session state between the communicating endpoints by using the IP address of the two endpoints, however, IP addresses are also used to find a route between the endpoints. The route does not have to be the same in both directions; the route selected for a datagram depends only on the IP destination address and not on the IP source address. These two uses of IP addresses result in the following contradiction for mobile computing. On one hand, a mobile computer needs to have a stable IP address to be identified to other Internet nodes. On the other, if the address is fixed, the datagrams routing to the mobile computer will always go to the same place, thus no mobility. Mobile IP extends IP by allowing the mobile computer to have two addresses, one for identification and the other for routing.

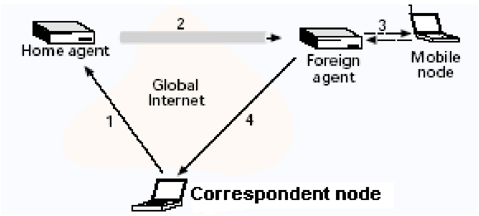


Fig. 1: Mobile IP overview

We can outline the operation of the basic mobile IP protocol (MIPv4) as follows[6]: Mobility agents send agent advertisement messages. After receiving an agent advertisement, a mobile node can determine whether it is attached to the home network or to a foreign network. When a mobile node is attached to a foreign network, it obtains a care-of address on that foreign network. The mobile node registers its care-of address with its home agent. As shown in Fig. 1, the home agent receives all datagrams distended to the mobile node's home address and tunnels them to the mobile node's care-of address. In order for the home agent to deliver a datagram to the care-of address, it uses a procedure called encapsulation or tunneling (shown by the thick tube in the figure).

Corresponding Author: Fayza A. Nada, Faculty of computers and information, Suez Canal University, Ismailia, Egypt

The original datagram is encapsulated by another IP header with the destination is the care-of address and then delivered by the home agent. When the foreign agent receives the encapsulated datagram, it decapsulates it, removing the encapsulating IP header and delivers the inner datagram to the mobile node which is presumed to be on the same link as one of the foreign agent's network interfaces. Datagrams sent the mobile node are delivered to their destination using standard IP routing mechanism[7].

MOBILE IP OVERVIEW

Mobile IP is considered as a cooperation of the three procedures: Agent discovery, Registration and Tunneling. When a mobile node moves within range of foreign agent, it listens for advertisements which contain a care-of address. If no advertisements are detected, the mobile node may solicit for a care-of address. In many cases the only way the mobile node can detect whether it has moved is by comparing new advertisements with previous ones and determining whether the offered care-of address has changed[8].

Agent discovery: The method of detecting a mobility agent is quite similar to that used by Internet nodes to detect routers by running Internet control message protocol (ICMP) Router discovery (RFC 1256)[9]. The basic operation involves periodic broadcasts of advertisements by the routers onto their directly attached networks. Protocol engineer try to reuse existing system components to avoid old errors and benefit from the experience of others. So that, the Mobile IP working group supports the special additional needs of mobility agents by attaching special extensions to the standard ICMP[10] messages. That is, mobile service advertisements and solicitations are transported via ICMP messages, with the ICMP payload containing one or more special mobile extensions[7].

Agent solicitation: Mobile nodes use router solicitations ICMP messages to detect any changes in the set of mobility agents available at the current point of attachment. If advertisements are no longer detectable from a foreign agent that previously had offered a care-of address to the mobile node, the mobile node should presume that foreign agent is no longer within range of the mobile node's network interface. In this case, the mobile node should hunt for a new care-of address or use a care-of address known from advertisements it is still receiving[11]. The mobile node may choose to wait for another advertisement if it has not received any recently advertised care-of addresses or it may send agent solicitation, the mobile IP agent solicitation message format is illustrated in Fig. 2.

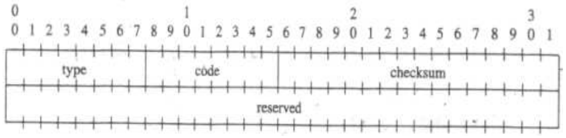
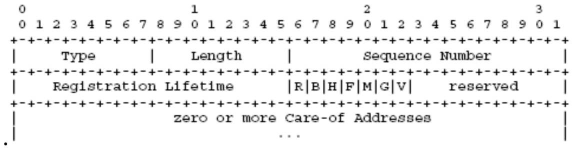


Fig. 2: Agent solicitation (from RFC 1256)

Agent advertisement: The mobile IP discovery process has been built on top of the existing standard protocol Router Advertisement, specified in RFC 1256[12]. Mobile IP Agent discovery does not change the original fields of existing router advertisements but extends them to associate mobility functions. A router advertisement can carry information about routers and carry further information about one or more care-of addresses and in this case they are called agent advertisements. Home agents and foreign agents broadcast agent advertisements at regular intervals. To get a care-of address, a mobile node can either waits to get an agent advertisement or broadcasts a solicitation that will be answered by any foreign agent or home agent that receives it. Mobility agent extension format is shown in Fig. 3.



```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|     Type      |    Length     |        Sequence Number        |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|    Registration Lifetime      |R|B|H|F|M|G|V|    reserved     |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                 zero or more Care-of Addresses                |
|                              ...                              |
```

Fig. 3: Mobility agent advertisement extension

Registration: Mobile IP provides a mechanism by which the mobile node can send information to its home agent. Registration process (shown in Fig. 4) enables the mobile node to:

- * Inform the home agent about its current care-of address.
- * Renew the registration when moving to a new point of attachment.
- * Deregister when returning back to its home network.

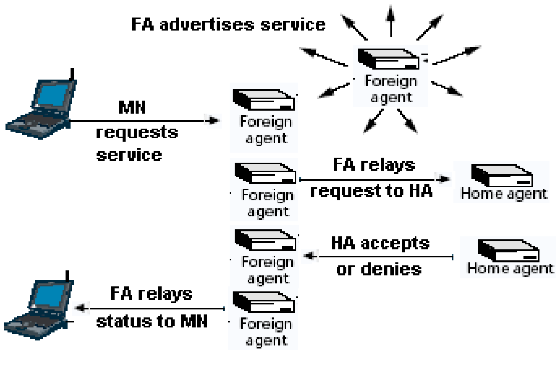


Fig. 4: Registration overview

Registration request: The registration messages use the User Datagram Protocol (UDP). A nonzero UDP checksum should be included in the header and not checked by the recipient. A mobile node registers with its home agent using a registration request message so that its home agent can create or modify binding for that mobile node.

The registration process is almost the same whether the mobile node has obtained its care-of address from a foreign agent, or alternatively has acquired it from another independent service such as DHCP. After the IP and UDP headers, the registration request has the structure illustrated in Fig. 5.

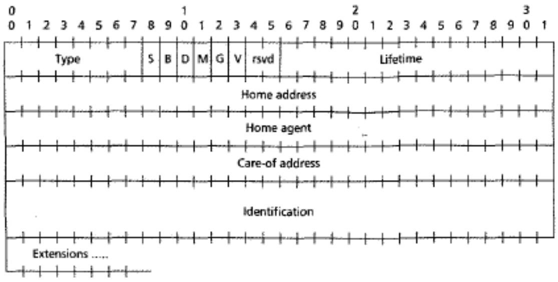


Fig. 5: Registration request packet format

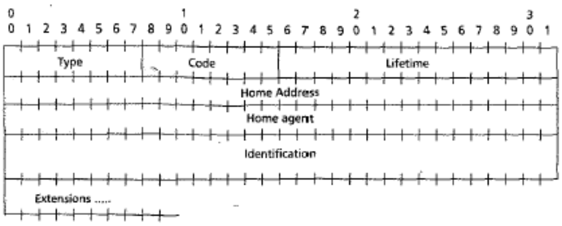


Fig. 6: Registration reply packet format

Registration reply: A mobility agent returns a registration reply message to a mobile node which has sent a registration request message. If the mobile node is requesting service through a foreign agent, that foreign agent will receive the reply and relay it to the mobile node. The reply message is shown in Fig. 6, it contains the necessary codes to inform the mobile node about the status of its request, along with the lifetime granted by the home agent, which may be smaller than the original request. The foreign agent should not increase the lifetime selected by the mobile node in the registration request, since the lifetime is covered by the mobile-home authentication extension which can not be correctly recomputed by the foreign agent. The home agent must not increase the lifetime selected by the mobile node in the registration request since doing so could increase it beyond the maximum registration lifetime allowed by the foreign agent. If the lifetime received in the registration reply is greater than that in the registration request, the lifetime in the request should be used. When the lifetime received in the registration reply is less than that in the registration request, the lifetime in the reply should be used[13].

Tunneling and routing: Mobile IP specifies a method by which an IP datagram may be encapsulated (carried as payload) within an IP datagram. Encapsulation is a means to change the normal IP routing for datagrams, by delivering them to an intermediate destination that would otherwise not be selected based on the IP Destination Address field in the original IP header. Once the encapsulated datagram arrives at this intermediate destination node, it is decapsulated, yielding the original IP datagram, which is then delivered to the destination indicated by the original Destination Address field. This use of encapsulation and decapsulation of a datagram is frequently referred to as "tunneling" the datagram and the encapsulator and decapsulator are then considered to be the "endpoints" of the tunnel, with the source, encapsulator, decapsulator and destination being separate nodes[14].

IP within IP encapsulation: To encapsulate an IP datagram using IP within IP encapsulation, an outer IP header[15] is inserted before the datagram's existing IP header, as shown in Fig. 7. The outer IP header Source Address and Destination Address identify the "endpoints" of the tunnel, the inner IP header Source Address and Destination Addresses identify the original sender and recipient of the datagram, respectively. The inner IP header is not changed by the encapsulator, except to decrement the TTL as noted below and remains unchanged during its delivery to the tunnel exit point. No change to IP options in the inner header occurs during delivery of the encapsulated datagram through the tunnel. If needed, other protocol headers such as the IP Authentication header[16] may be inserted between the outer IP header and the inner IP header. Note that the security options of the inner IP header may affect the choice of security options for the encapsulating (outer) IP header.

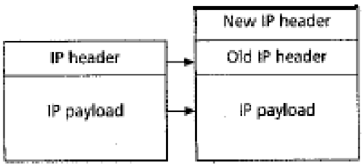
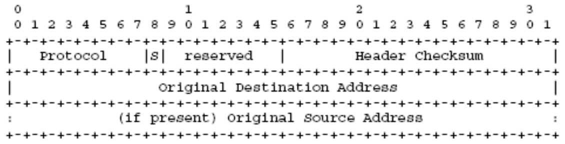


Fig. 7: IP within IP encapsulation

Minimal encapsulation: A minimal forwarding header is defined for datagrams which are not fragmented prior to encapsulation. Use of this encapsulation method is optional. Minimal encapsulation must not be used when an original datagram is already fragmented, since there is no room in the minimal forwarding header to store fragmentation information. To encapsulate an IP datagram using minimal encapsulation, the IP header of the original datagram is modified and the minimal forwarding header is inserted into the datagram after the IP header, followed by the unmodified IP payload of the original datagram. No additional IP header is added to the datagram. The format of the minimal forwarding header is shown in Fig. 8.



```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|   Protocol    |S|  reserved   |        Header Checksum        |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                 Original Destination Address                  |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
:            (if present) Original Source Address               :
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Fig. 8: Minimal encapsulation header format

When decapsulating a datagram, the fields in the minimal forwarding header are restored to the IP header and the minimal forwarding header is removed from the datagram. In addition, the Total Length field in the IP header is decremented by the size of the minimal forwarding header removed from the datagram and the Header Checksum field in the IP header is recomputed[15] or updated to account for the changes to the IP header described here for decapsulation. The encapsulator may use existing IP mechanisms appropriate for delivery of the encapsulated payload to the tunnel exit point. In particular, use of IP options are allowed and use of fragmentation is allowed unless the "Don't Fragment" bit is set in the IP header[17].

PROBLEMS OF BASE MOBILE IP PROTOCOL

Mobile IP still has many items that need to be worked on and enhanced such as the security issue and the routing issue. The IETF has been working on the problems which had been found on the base Mobile IP protocol.

Triangle routing: As noted above, datagrams going to the mobile node have to travel through the home agent when the mobile node is away from home, but datagrams from the mobile node to other stationary Internet nodes can be routed directly to their destinations. This additional routing, called triangle routing and shown in Fig. 9, is generally far from optimal, especially in cases when the correspondent node is very close to the mobile node. Route Optimization is the protocol suggested to eliminate the triangle routing problem and is described here.

Duplicating fields in "IP within IP": To encapsulate the datagram, we put the original datagram inside another IP envelope, then the whole packet consists of the outer IP header plus the original datagram. The fields in the outer IP header add too much overhead to the final datagram -- several fields are duplicated from the inner IP header. This waste of unnecessary space is uneconomical. Minimal Encapsulation scheme is defined to overcome this problem and becomes another option to encapsulate the datagram.

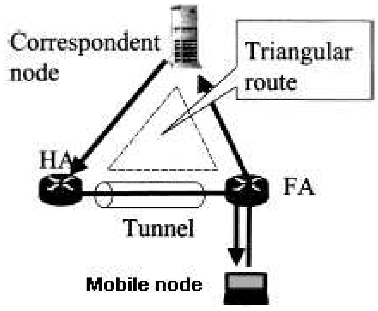


Fig. 9: Triangle routing

Fragility: Although single home agent model is simple and easy to configure, it has the disadvantage of fragility. The mobile node becomes unreachable once the home agent breaks down. One possible solution is to support multiple home agents. If one conventional home agent fails, there are still other home agents who can take over the duty and route the datagram to the mobile node.

Dogleg routing: If a mobile node happens to move to the same subnetwork as its correspondent node that wants to send it datagrams, this is what will happen in order for the datagram to be received by the mobile node, based on the base Mobile IP protocol: the correspondent node will send the datagram all the way to the mobile node's home agent, which may be a half globe away; its home agent will then forward the datagram to its care-of-address, which might just take a half second to reach if the datagram is sent directly from the correspondent node. This kind of "indirect routing" is inefficient and undesirable.

Security issues: The most pressing outstanding problem facing Mobile IP is that of security. A great deal of attention is being focused on making Mobile IP coexist with the security features coming into use within the Internet. Firewalls[18] in particular cause difficulty for Mobile IP because they block all classes of incoming packets that do not meet specified criteria. Enterprise firewalls are typically configured to block packets from entering via the Internet that appear to emantate from internal computers. Although this permits management of internal Internet nodes without great attention to security, it presents difficulties for mobile nodes wishing to communicate with other nodes within their home enterprise networks. such communications, originating from the mobile node, carry the mobile node's home address and would thus be blocked by the firewall[11].

ROUTE OPTIMIZATION

Mobile IP suffers from the Triangle Routing, shown in Fig. 9. Packets sent from the mobile node to a correspondent node are delivered by normal Internet routing rules. But, when a correspondent node needs to send a datagram to a mobile node, it has to go through the home agent, This additional network travel increases the delays for incoming packets, increases the network congestion and create a routing bottleneck at the home agent[8]. The IETF is investigating the route optimization method for dealing with this problem[19]. The operation of the IETF method is as follows:

When the Home Agent receives a packet destined to the mobile node from a correspondent node, it reports (Binding Update) a combination of the relevant mobile node's home address and care-of address (Binding Information), which the Home Agent itself is maintaining, to the correspondent node.

The correspondent node maintains the Binding Information of the mobile node and tunnels subsequent packet transmissions to the mobile node's care-of address.

Although the correspondent node maintains the Binding Information for a fixed interval, it will update the timer before a time-out occurs when it receives another Binding Update from the Home Agent. In the above description, the Home Agent decides to send out a Binding Update. However, there is also an option in which the correspondent node issues a request (Binding Request) to the Home Agent to send out a Binding Update. These functions described above enable the correspondent node to directly send packets to the mobile node without routing them through the Home Agent[3]. Thus, Route Optimization protocol uses the following four messages:

Binding warning message: It is sent to the home agent to show a correspondent node that does not know the mobile node's care-of address. A binding warning message (Fig. 10) informs the recipient that the target node could benefit from obtaining a fresh binding for the mobile node.

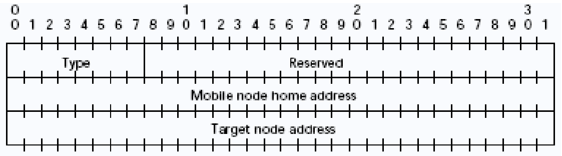


Fig. 10: Binding warning message format

Binding request message: Any time a correspondent node determines that its binding is stale, or is going stale, it can issue a binding request message (Fig. 11) to the home agent. The correspondent node sends a 64-bit number (the identification) to the home agent for use in protecting against replay attacks and also to help match pending requests with subsequent updates.

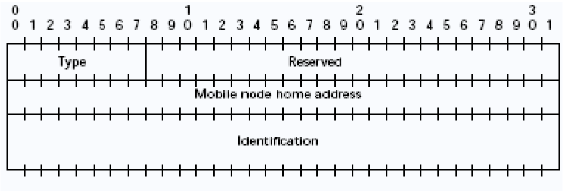


Fig. 11: Binding request message format

Binding update message: The home agent sends an authenticated binding update message (Fig. 12) containing the mobile node's current care-of address to a correspondent node that needs it. This happens when the home agent receives a datagram addressed to a mobile node from the correspondent node, which subsequently has to be tunneled by the home agent to the mobile node's current care-of address. If the home agent has a security relationship with the correspondent node, it can send a binding update directly without waiting for any binding warning message or binding request. The binding included in the update must contain an associated lifetime, after which the binding is to be purged by the recipient.

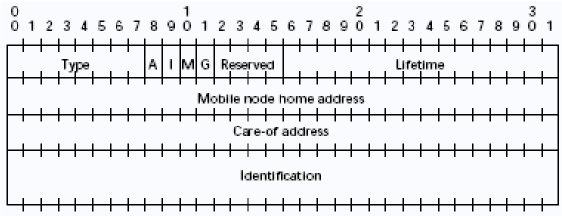


Fig. 12: Binding update message format

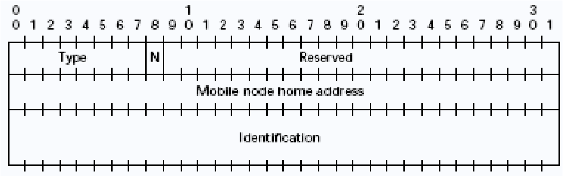


Fig. 13: Binding acknowledgment message format

Binding acknowledgment message: Figure 13 is used to acknowledge the reception of binding update messages. The 64-bit identification field protects against replays and allows the acknowledgment to be associated with a pending binding update. The N bit allows the recipient of the binding update to satisfy the A bit of the binding update, while informing the updating agent that the update was not acceptable[7].

OVERVIEW ON MOBILE IPv6

IPv6 is derived from IPv4 and is in many ways similar to it. As such, the IETF Mobile IP Working Group's current protocol design[20] for mobility of IPv4 nodes could be adapted for use in IPv6, with only the straightforward changes needed to accommodate differences between IPv4 and IPv6 such as the size of addresses. The most visible difference is that IPv6 addresses are all 128 bits long, instead of 32 bits long as in IPv4. Within this huge address space, a tiny part is reserved for all current IPv4 addresses and another tiny part is reserved for the Link-Local addresses, which are not routable but are guaranteed to be unique on the local network. IPv6 defines several kinds of extension headers, which may be used to include additional information in the headers of an IPv6 packet. The Routing header is particularly useful for our mobility protocol and is similar to the Source Route options defined for IPv4.

Mobile IPv6 basic operation: Mobile nodes should assign three IPv6 addresses to their network interface(s) at least whenever they are roaming away from their home subnet. One is its home address, which is permanently assigned to the mobile node in the same way as any IP node. The second address is the mobile node's current Link-Local address. The third address, known as the mobile node's care-of address, which is associated with the mobile node only while visiting a particular foreign subnet. The central data structure used in Mobile IPv6 is a cache of mobile node bindings, maintained by each IPv6 node, known as a Binding Cache. While away from home, a mobile node registers with a router in its home subnet, requesting this router to function as the home agent for the mobile node. While it has a home registration entry in its Binding Cache, the home agent uses proxy Neighbor Discovery to intercept any IPv6 packets addressed to the mobile node's home address on the home subnet and tunnels each intercepted packet to the mobile node's primary care-of address indicated in this Binding Cache entry. To tunnel the packet, the home agent encapsulates it using IPv6 encapsulation[21].

In addition, Mobile IPv6 provides a mechanism for IPv6 correspondent nodes communicating with a mobile node to dynamically learn the mobile node's binding. The correspondent node adds this binding to its Binding Cache. When sending a packet to any IPv6 destination, a node checks its Binding Cache for an entry for the packet's destination address and if a cached binding for this address is found, the node routes the packet directly to the mobile node at the care-of address indicated in this binding; this routing uses an IPv6 Routing header[22] instead of IPv6 encapsulation. If no Binding Cache entry is found , the correspondent node instead sends the packet normally (with no Routing header) and the packet is then intercepted and tunneled by the mobile node's home agent as described above.

Mobile IPv6 introduces two new IPv6 Destination options to allow a mobile node's home agent and correspondent nodes learn and cache the mobile node's binding. After configuring a new care-of address, a mobile node must send a Binding Update option containing that care-of address to its home agent and to any correspondent nodes that may have an out-of-date care-of address for the mobile node in their Binding Cache. Receipt of a Binding Update must be acknowledged using a Binding Acknowledgement option, if an acknowledgement was requested in the Binding Update[23].

The binding update option: A mobile node sends a Binding Update to an other node to inform it of its current binding. Since the Binding Update is sent as an IPv6 Destination option, the mobile node may include it in any existing packet that it is sending to that destination node, or it may send the Binding Update in a packet by itself. The Binding Update is used by a mobile node to register its primary care-of address with its home agent and to notify correspondent nodes of its binding so that they may create or update entries in their Binding Cache for use in future communication with the mobile node.

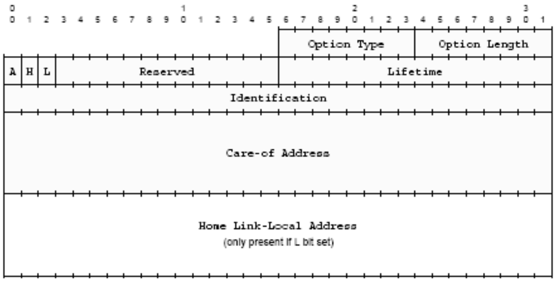


Fig. 14: Binding update destination option format

The format of the Binding Update option is shown in Fig. 14. The sending mobile node's home address must be the source address in the IPv6 header of the packet containing the Binding Update and thus need not be duplicated within the data of the Binding Update option.

The binding acknowledgement option: The Binding Acknowledgement option is sent by a node to acknowledge receipt of a Binding Update. When a node receives a Binding Update addressed to itself, in which the Acknowledge (A) bit is set, it must return a Binding Acknowledgement. The destination address in the IPv6 header of the packet carrying the Binding Acknowledgement must be the care-of address from the Binding Update, causing the Binding Acknowledgement to be returned directly to the mobile node sending the Binding Update. The format of the Binding Acknowledgement option is shown in Fig. 15.

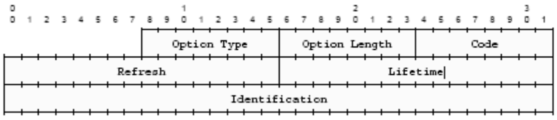


Fig. 15: Binding acknowledgment destination option format

CONCLUSION

Mobile IP is a proposal standard protocol that builds on the Internet protocol by making mobility transparent to applications and higher level protocols (like TCP). It is still in the process of being standardized and there are still many items that need to be worked on and enhanced such as the security issue and the routing issue. The IETF has been working on the problems which had been found on the base Mobile IP protocol. In this study we have presented an introduction to the base Mobile IP protocol (MIPv4) with it three major procedures: Agent discovery, Registration and Tunneling. we have outlined the alternative encapsulation techniques and route optimization procedure as well. In the end we have summarized Mobile Internet Protocol version 6 (MIPv6) with its basic operations and enhancements that allow transparent routing of IPv6 packets to mobile nodes, taking advantage of the opportunities made possible by the design of a new version of IP.

REFERENCES

1. NTT DoCoMo Gateway Business Department. DoCoMo i-mode. 3GPP SA2 S2-99E94.
2. Combined GSM and Mobile IP Mobility Handling in UMTS IP CN (3G TR 23.923 version 1.2.0).
3. Takagi, Y., Takeshi Ihara and Hiroyuki Ohnishi, 2003. Mobile ip route optimization method for next-generation mobile networks. Electronics and Communications in Japan, Part 1, 86: 2.
4. Chen, Y., 1996. A Survey Paper on Mobile IP.
5. Postel, J.B., (Ed.), 1981. Transmission Control Protocol. RFC 793.
6. Perkins, C., Mobile IP Design Principles and Practices. Addison Wesley Wireless Communications Series.
7. Perkins, C., 1997. Mobile IP. IEEE Comm., 35: 84-99.
8. Perkins, C., 1998. Mobile IP. Intl. J. Commnun. Syst., 11: 3-20.
9. Eastlake, D.E. and C.W. Kaufman, 1996. Domain name system protocol security extensions, draft-ietf-dnssec-secext-09.txt.
10. Postel, J.B., (Ed.), 1981. Internet Control Message Protocol, RFC 792..
11. Perkins, C., 1998. Mobile networking through Mobile IP. IEEE Internet Computing J.,
12. Deering, S.E., (Ed.), 1991. ICMP Router Discovery Messages, IETF RFC 1256.
13. Perkins, C., (Ed.), 1996. IP Mobility Support, RFC 2002.
14. Perkins, C., 1996. IP Encapsulation Within IP, IETF RFC 2003.
15. Postel, J., (Ed.), 1981. Internet Protocol, STD 5, RFC 791.
16. Atkinson, R., 1995. IP Authentication Header, RFC 1826.
17. Perkins, C., 1996. Minimal Encapsulation Within IP, IETF RFC 2004.
18. Cheswick, W.R. and S. Bellovin, 1994. Firewalls and Internet Security. Addison-Wesley, Reading, Mass.
19. Perkins, C., Route optimization in mobile IP. IETF draft.ietf.mobileip.optim-09.txt.
20. Perkins, C., (Ed.), 1996. IPv4 Mobility Support. ietf-draft-mobileip-protocol-17.txt.
21. Conta, A. and S. Deering, 1996. Generic Packet Tunneling in IPv6. ftp://ftp.ietf.org/internet-drafts/draft-ietf-ipngwg-ipv6-tunnel-07.txt.
22. Deering, S. and R. Hinden, 1995. Internet Protocol. Version 6 (IPv6) Specification. RFC 1883.
23. Johnson, D. and C. Perkins, 1996. Mobility support in IPv6. ACM Mobi-Com 96, ACM, pp: 27-37.