Mobile IP Survey

Chakchai So-In, *s_chakchai@yahoo.com*

Abstract:

Mobile Internet Protocol (MIP) is a standard protocol that allows users to maintain nonstop connectivity with their home IP addresses regardless of physical movement. In this paper, we give an overview of Mobile IP: terminology, functionality, and operation. Comprehensive surveys on Mobile IP issues are discussed: Quality of Service (QOS), Multicast, Security, Voice, and TCP over Mobile IP. The Mobile IPv6 basic concept is also explained. Finally, IP-based mobility and Mobile IP implementations are reviewed.

Table of Contents

1. Introduction

We want to keep our IP addresses wherever we are, but a traditional IP design does not support mobility. So, whenever we change our location, we also need new IP addresses. Changing IP addresses is undesirable for several reasons. As we know, most Internet traffic is TCP, and changing the IP address forces TCP to establish a new connection. As a result, packets might get lost during this change. Moreover, a mobile node will be assigned a foreign IP address instead of a local IP address. Then, using

the foreign IP address makes it difficult for users to gain access to their private or local networks, such as local printers.

The first attempt was to use the Host Specific Route, so a mobile node could keep its IP address permanently. However, whenever the mobile node changed its location, numerous host specific updated routes might be created to propagate throughout the Internet. Also, most importantly, this technique raises of security concerns since all packets may be forwarded to the new location over an unknown network.

Mobile IP was designed to solve all these problems. Mobile IP (MIP) is an Internet Engineering Task Force (IETF) standard protocol which allows users to keep their own IP addresses even though they move from one network to the other. Users can use their local IP addresses permanently regardless of having a link-layer point of attachment. Mobile IP supports a current Internet Protocol in both wired and wireless networks. There is no need to make a modification for other nodes in order to communicate with the nodes with Mobile IP functionality. Mobile IP is scalable for large number of users, and users can be confident that no one can read their messages or use their resources.

In this paper, we describe Mobile IP basic concepts in Section 2. Section 3 points out main Mobile IP issues: quality of service (QOS), multicast, security, voice over Mobile IP, and TCP over Mobile IP. Mobile IPv6 is explained in Section 4. IP-based mobility and Mobile IP implementations are reviewed in Sections 5 and 6. Finally, conclusions are drawn in Section 7.

Back to Table of Contents

---

2. Mobile IPv4 Fundamentals

This section explains Mobile IP basic concepts. It applies to either Mobile IPv4 or Mobile IPv6. This section is divided into three subsections: Section 2.1 shows Mobile IP terms which also used for the rest of this paper. Section 2.2 gives details of Mobile IP functionality. Section 2.3 describes Mobile IP operation.

2.1 Mobile IP Terminology

There are many potentially unfamiliar terms and acronyms in the mobile world, used in Requests for Comments, Internet Drafts, technical papers, and throughout this paper. Taken from [RFC3344, 2002], Table 2.1 shows common Mobile IP terms.

Table 2.1: Mobile IP Terminology

Mobility Agent(MA)	Home Agent or Foreign Agent
Home agent(HA)	A router on a mobile node□s home network. It delivers packets through a tunnel to a mobile node. It also maintains mapping between the mobile node□s home address and its care-of address.
Foreign agent(FA)	A router on a mobile mode□s visited network. It works as the default router of the mobile node.
Mobile Node(MN)	A host or router that changes its point of attachment. It keeps its home IP address regardless of the change of location.
Correspondent	

Node(CN)	Either a fixed or mobile host which is communicating with the MN
Care-of Address (COA)	IP Address that is sent to the HA
Foreign agent-based COA(FCOA)	IP Address of the FA (Packets are detunneled at the FA and the FA sends them to the MN by Layer 2 address).
Colocated COA (CCOA)	IP Address which belongs to the address in the FA network which the MN obtains in a registration process (Packets are detunneled at the MN). The FA acts as the default router.
Gratuitous ARP	Sent by the HA to update Address Resolution Protocol (ARP) tables for all connected hosts
Mobility Binding	Mapping of the HA and the COA
Tunnel	Virtual private channel with an encapsulated packet
Security Parameters Index(SPI)	Identifies the Security Association (SA) for datagrams between two nodes. SPI selects the authentication algorithm and secret either shared key or public key to compute an authenticator.

2.2 Mobile IP Functionality

This section describes Mobile IP functionality. Typically, there are three main Mobile IP functions. For the first function, Location Discovery, the MN must know where it is, whether local or foreign. For the second function, Move Detection, the MN also has to recognize if it has moved from one network to another or just moved inside the network. And finally, the MN has to inform its own HA of its new location, so the HA can forward packets to the right address. Tunneling takes care of the communication process between the MN and the HA.

2.2.1 Location Discovery

The MN is responsible for discovering whether the MN is in a home or foreign network. This process is done by either the Agent Advertisement or Agent Solicitation communication process. Usually, the FA periodically broadcasts the Internet Router Discovery Protocol (IRDP) message [RFC 1256, 1991] in its own network to let the visited MN know the FA is here and what services the FA provides (Agent Advertisement). Thus, the MN knows which network it belongs to. In case the MN does not receive this message, it can request the service by sending a solicitation message to inform the FA directly (Agent Solicitation). If there is no answer back during a limited time, the MN attempts to use the Dynamic Host Configuration Protocol (DHCP) to acquire a new IP address. Both the advertisement and the solicitation protocols are the same as the IRDP with Time to Live (TTL) set to 1. A destination address in the IRDP packet can be used as either a multicast address, 224.0.0.1 (all systems on this link), or a broadcast address, 255.255.255.255 (all nodes). Figure 2.1 and Tables 2.2a, and 2.2b show the Agent Advertisement and Agent Solicitation protocols.

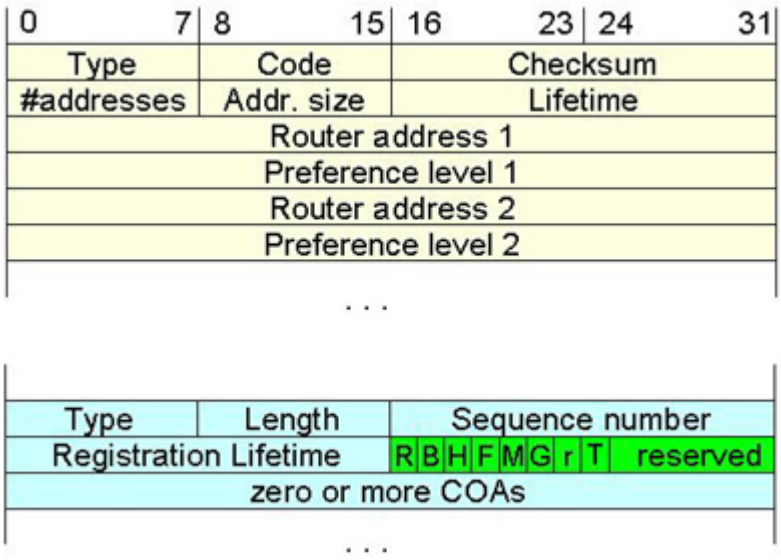


Figure 2.2: Agent Advertisement/ Agent Solicitation protocol

Table 2.2a: Agent Advertisement/ Agent Solicitation protocol

IRDP :	
Type	9 = Agent Advertisement, 10 = Agent Solicitation
Code	0 = Advertising Agent is a fully capable router. 16 = only a Mobile IP agent
Checksum	The 16-bit one's complement of the one's complement sum of the ICMP /IRDP message, starting with the ICMP/IRDP Type
Num Addrs	The number of router addresses advertised in this message
Addr Entry Size	The number of 32-bit words of information per each router address
Lifetime	The maximum number of seconds that the router addresses may be considered valid.
Router Address [i]	The sending router's IP address (es) on the i = 1..Num Addrs interface from which this message is sent.
Preference Level[i]	The preferability of each Router Address[i]
Mobility Extension :	
Type	16 (Mobility Advertisement Extension)
Length	6+4*#COAs (6 = the number of bytes in the sequence number, Registration Lifetime, Flags, and Reserved fields + another 4 bytes per each COA)
Sequence Number	The count of Agent Advertisement messages sent since the agent was initialized.
Registration Lifetime	The longest lifetime in seconds that the Registration Request will be accepted by this agent. 0xffff = infinity.

Table 2.2b: Agent Advertisement protocol/ Agent Solicitation protocol (continue)

S	MN is requesting the use of simultaneous bindings. This requires the HA to duplicate all packets and then forward them to multiple COAs (The purpose is to avoid lost packet).
B	MN is requesting broadcast datagrams from its home network be delivered to it.
D	MN is specifying that it can perform Mobile IP tunnel decapsulation. The MN is using a CCOA so the tunnel ends at the MN.
M	MN is requesting that HA uses the Minimal Encapsulation, as defined in RFC 2004, instead of IP-in-IP encapsulation for Mobile IP tunneling.
G	MN is requesting that HA uses the GRE, as defined in RFC 1701, instead of IP-in-IP encapsulation for Mobile IP tunneling.
r	Sent as zero; ignored on reception.
T	MN is requesting the Reverse Tunneling for packets originated by the MN.
x	Sent as zero; ignored on reception.

After a discovery phase, the MN has to send a registration or deregistration request message with its updated COA back to the HA. After that, a registration reply message will be sent back to the MN to confirm the registration process. The HA then updates its mapping address between the home address of the MN and the updated COA. Both registration messages use the UDP protocol in which a destination port is set to 434. The registration request and reply protocols are shown in Figure 2.3, Tables 2.3, and 2.2b. In case the MN returns to its home network, the MN still sends the registration message to deregister it from the HA (Lifetime is set to 0).

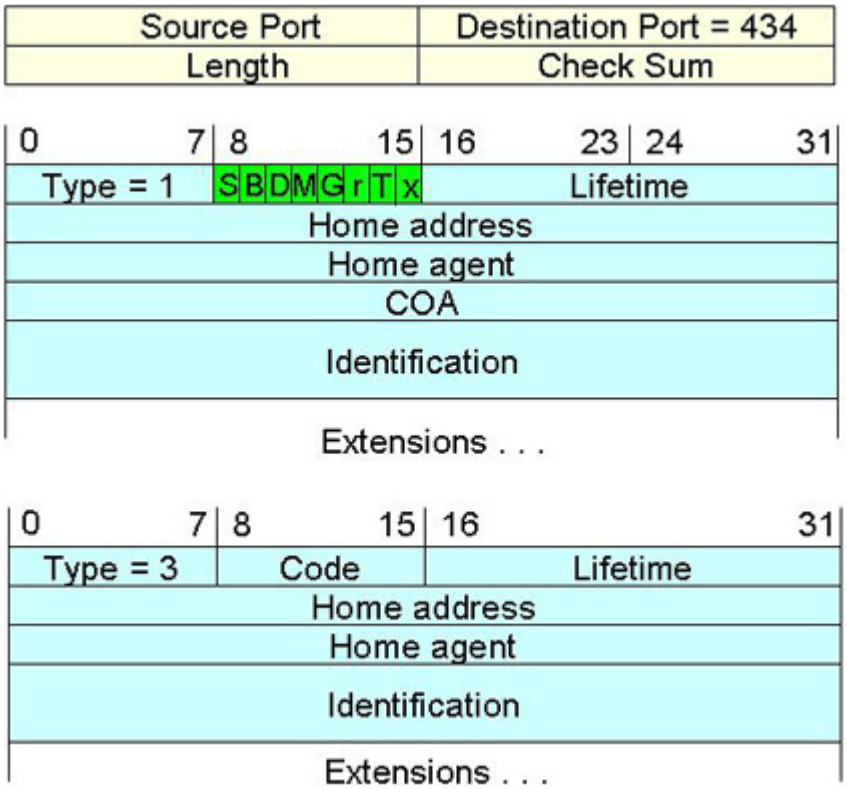


Figure 2.3: UDP (top), Registration Request (middle), and Registration Reply (bottom) protocols

Table 2.3: Registration Protocols

Type	1 = Registration Request, 3 = Registration Reply
Lifetime	The number of seconds remaining before the registration is considered expired. 0 = a request for deregistration. 0xffff = infinity. If the Code field indicates that the registration was denied, the contents of the Lifetime field are unspecified and must be ignored on reception.
Identification	Unique identification to match the Registration Request with Registration Reply, and unique identification of MN

Since a registration process might make the MN transmit packets over an unknown network through a tunneling process (which we will describe in the next section), Mobile IP is vulnerable if the registration messages are not authenticated or even encrypted properly. Basically, there are three types of authentication: the authentication of the registration messages between the MN and the HA (Mobile-Home), between the MN and the FA (Mobile-Foreign), and between the FA and the HA (Foreign-Home). However, due to the difficulty of key distribution management, it is not necessary to authenticate the FA [RFC 3344, 2002]. In this recommendation, to prevent a node from pretending to be either the HA or the FA, HMAC-MD5 (Keyed-hash message authentication code with Message-Digest algorithm 5) is also used as a default authentication algorithm, with 128 bit key size and manual key distribution (shared key). Figure 2.4 and Table 2.4 show the Authentication Extension protocol.

Figure 2.4: Authentication Extension protocol

Table 2.4: Authentication Extension protocol

Type	31 = Mobile-Home, 33 = Mobile-Foreign, 34 = Foreign-Home
Length	4 plus the number of bytes in the Authenticator
Security parameter index (SPI)	Identifies the Security Association (SA) for datagrams between two nodes. SPI selects the authentication algorithm and secret keys either shared or public to compute the Authenticator
Authenticator	A code used to authenticate the message. (variable length)

Moreover, to prevent a replay attack on the registration messages (either the FA or the MN uses the repetition of the registration messages), an identification field plays an important. First, the identification field is divided into two parts of 32 bits each. With the help of the Network Time Protocol (NTP), whenever the MN does the registration process, it puts a timestamp in the lower order 32 bits in the identification field. The MN also generates a nonce (random) number and puts it in the higher order 32 bits. The message uses the authentication code to protect against alteration. Once the HA receives that packet, it checks the identification field for validity. If it is valid, the HA copies it to the identification field in the reply message, and sends it back to the MN.

2.2.2 Move Detection

Whenever the MN changes its location, the MN itself has to be responsible for location tracking. The MN must also inform the HA to update its COA, so the HA can send packets back to the right COA which is destined for the MN. [RFC 3344, 2002] proposed two such algorithms. In the first, the registration process is based on the lifetime indicated in the Lifetime field inside the ICMP header. If the MN does not receive any Agent Advertisement messages from the FA within the lifetime, the MN can assume it has lost contact to the current FA, and it tries to register with the new FA after receiving another Agent Advertisement message.

In the second algorithm, the MN uses a network prefix feature of the Prefix Length Extension (Prefix type = 19) of the Agent Advertisement protocol. The MN can identify whether it has moved and hands off when its network is different from the current FA network. Since these two mechanisms are based on ICMP messages, the MN sometimes has to wait for either an expired timeout or the advertisement protocol time interval. To make the mobility detection process fast, [Raab and Chandra, 2005] and [Yu et al., 2003] proposed new ideas for using Layer 2 information with the Agent Solicitation message to indicate whether the MN should be handed over (The MN has moved), since technically the MN can detect link state effectively. However, this scheme involves not only Layer 2 but also ICMP functionalities; therefore, it might not be useful in practice.

Typically, the primary concerns of the handoff process are to minimize packet loss and handoff latency. The MN might lose packets during the handoff because the HA keeps sending the packets through the previous FA. With route optimization functionality, [Perkins, 2002a] described how to do a smooth handoff (Mobile IP route optimization with smooth handoff extension) to mitigate the packet loss problem (Figure 2.10c). Basically, the FA allows the MN to do a handoff before the new registration process is completed. During the handoff, the previous FA still maintains the binding for the former MN. Whenever the MN moves to another network, the MN informs the new FA to send a binding update to the previous FA. Then, the previous FA reencapsulates the packets with the right COA and sends them to the MN. To prevent loss of the packets, the buffer scheme may have to be implemented at the FA.

Since the route optimization mechanism requires that the MN always report to the HA and also that the messages be sent to the previous FA, it causes a lot of signaling throughout the network. In a buffer scheme concept, [Cao et al., 2004] presented a mailbox-based scheme, which they claim outperforms the route optimization with a smooth handoff extension scheme. Instead of sending the packets to the MN directly, the sender sends them to the mailbox, and then the mailbox forwards the packets to the MN. The MN associates itself with the mailbox whenever the MN has moved. During the handoff, the MN can choose to contact both the mailbox and the HA. Alternatively, it may choose to contact the mailbox only in order to reduce the load of the HA and the traffic between the MN and the HA.

All techniques above are concerned about packet loss. However, in consideration of the handoff latency, the time during the switching delay and IP protocol operation, [Koodli and Perkins, 2006] and [Koodli, 2006] proposed the Fast Hand Over technique, not only to reduce packet loss but also to reduce the handover delay. This technique is widely used for real time traffic such as voice over IP, where timing delay is very critical. Basically, this technique allows the MN to send the packets as soon as it detects a new network, and also makes the FA deliver the packets to the MN whenever it detects a new MN attachment.

During the handoff, once again, the MN sends an updated registration message back to the HA to update its COA. All of the handoff mechanisms above might create a lot of traffic during the registration process if the MN frequently moves. This not only wastes bandwidth, but also takes a long time to do the registration process, especially if the MN is far from the HA. Apart from the mailbox-based scheme, [Gustafsson et al., 2006] proposed the regionalized registration concept (Hierarchy of Foreign Agents).

This technique can reduce both total signaling messages to the HA and the signaling delay by performing registrations locally in the regional domain. The Gateway Foreign Agent (GFA) is a new network node which acts as the gateway for each domain. All FAs within local network know this address. Then, when the MN first registers with the HA, it sends the GFA address as its COA rather than either FCOA or CCOA. So, the MN only informs the GFA whenever it moves between different FAs within the regional domain.

2.2.3 Tunneling

In order to deliver packets from the MN to the HA and vice versa, either the FA (with FCOA) or the MN (with CCOA) has to do tunneling to avoid the route propagation problem. After the tunnel is established, it is considered as just only one hop end-to-end from either the FA or the MN to the HA. Basically, there are three kinds of encapsulation technique. First, a traditional IP-in-IP encapsulation [RFC 2003, 1996] simply encapsulates the original IP packet within the new IP header (Figure 2.5), decrements TTL by 1, and sets the outer protocol field to 4 (IP-in-IP). This technique does not support IP fragmentation so path MTU discovery must be enabled before its use.

Since the IP-in-IP encapsulation doubles IP packet sizes, this leads to inefficiency for a small IP packet, for example, a voice packet. Apart from the header compression technique, [RFC 2004, 1996] Perkins proposed the idea of the Minimal Encapsulation, used to avoid the repetition of the IP fields. The original IP header is modified as shown in Figure 2.6. The protocol field is set to 55 (min. encap.). For *S* If 0, the original source address is not present, so the length of this inner header (purple in Figure 2.6) is eight octets. If 1, the original source address is present and twelve octets for the inner header length. The Generic routing encapsulation (GRE) [RFC 2784, 2000] (Figure 2.7) is another tunneling protocol, which supports various kinds of transport protocols over IP network.

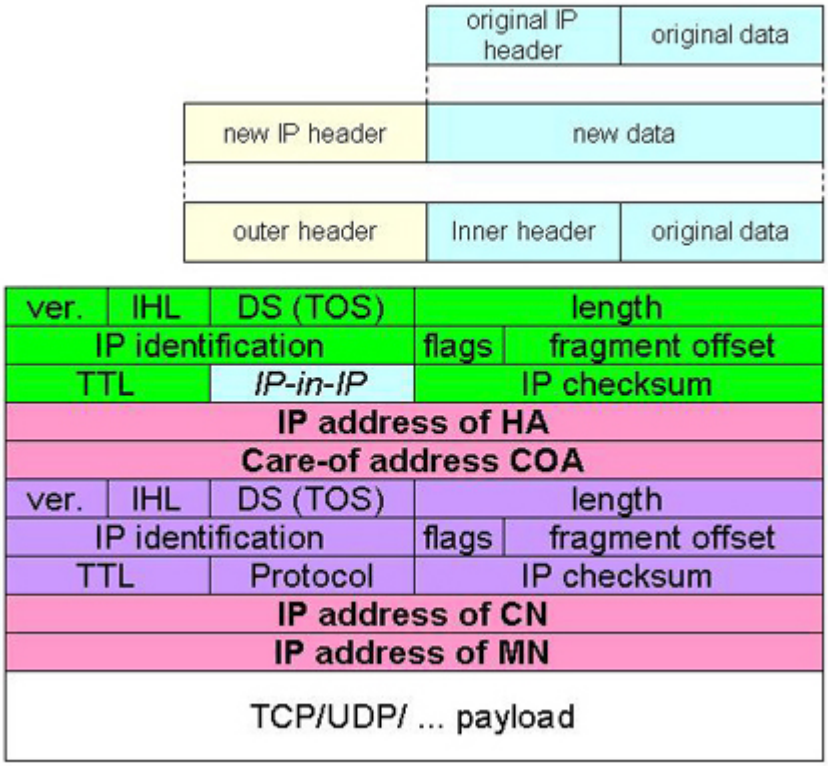


Figure 2.5: IP-in-IP encapsulation

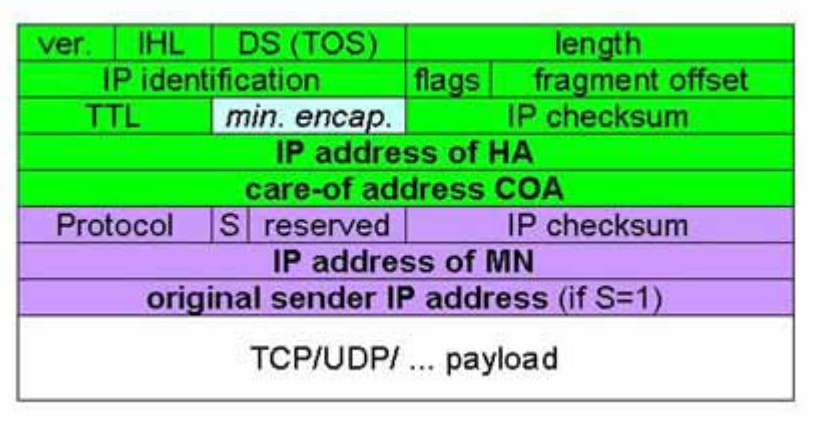


Figure 2.6: Minimal encapsulation

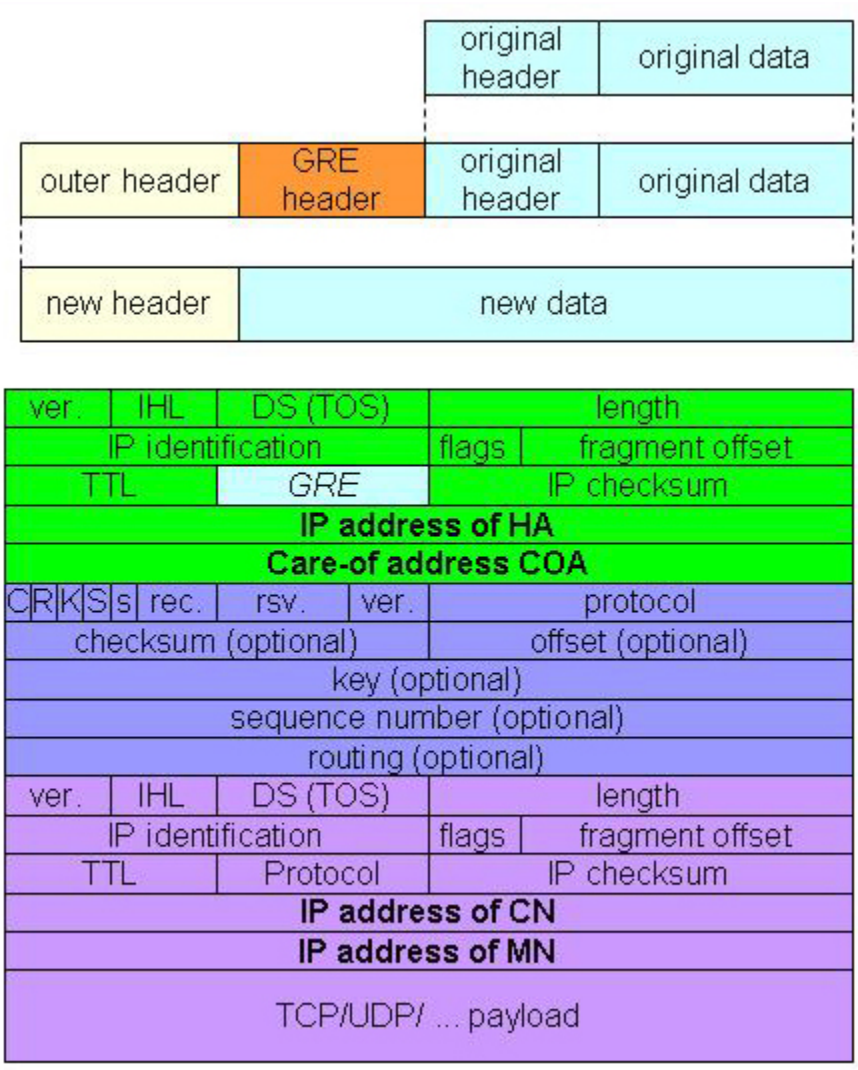


Figure 2.7: GRE encapsulation

2.3 Mobile IP Operation

This section summarizes Mobile IP operation, as shown in Figure 2.8. First, the CN wants to send

messages to the MN. It sends IP packets destined for the MN□s home address. These packets will be forwarded to the home network (1 and 2) by normal routing. Since the HA knows the MN is not in this network, the HA will intercept these packets, using the features of Gratuitous ARP and Proxy ARP. The updating ARP table indicates that the HA Layer 2 address is the MN Layer 2 address, so IP packets sent to the MN, will be sent directly to the HA. After that, the HA makes a tunnel (encapsulates the original packets inside a new IP packet), and forwards the packets (3) to the COA (The source IP address is the HA address, and the destination IP address is the COA). After taking off the outer header, the FA forwards the packets directly to the MN by link layer address if it is the FCOA (4). However, if it is the CCOA, the HA forwards the packets directly to the MN where the packets are deencapsulated. Finally, the MN sends the packets back to the CN as usual (5, 6, and 7).

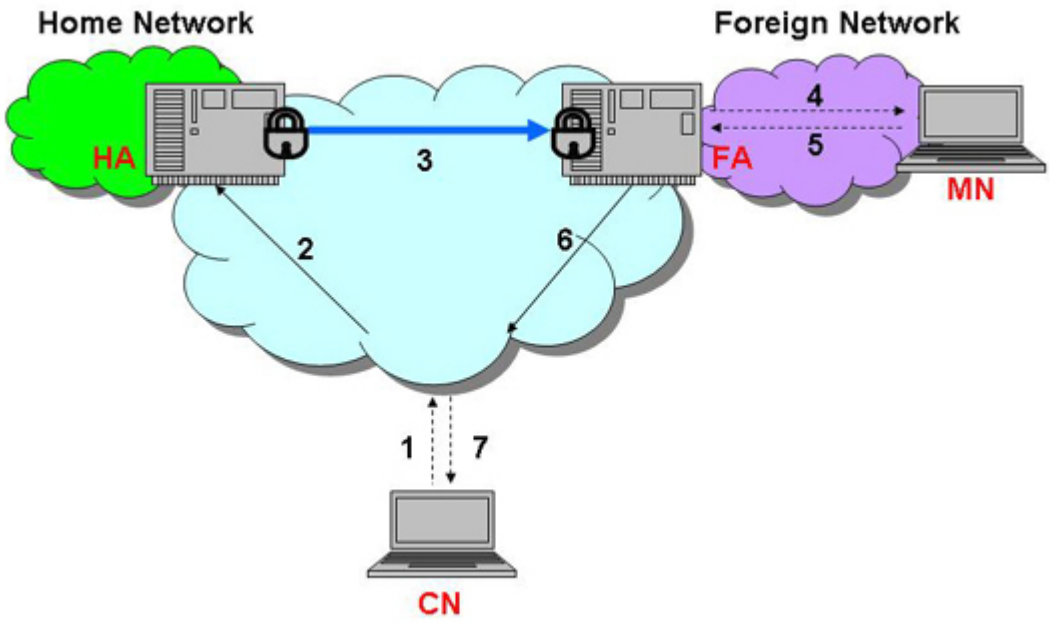


Figure 2.8: Mobile IP operation

Although it seems that Mobile IP can operate properly in this model, it turns out that due to the Ingress Filtering [RFC 2827, 2000] and location management issues, if the Firewall is setup, this technique can not be used. This problem is called the Triangle Routing problem because the way the packets are forwarded forms a triangle (From the CN to the HA, then to the FA, and finally back to the CN). Typically, a firewall does not allow an outgoing packet whose source address is different from its network addresses. Also, it is unusual to have outgoing and incoming packets in different paths (1, 2 and 6, 7). To solve these problems, [RFC 3024, 2001] recommends the Reverse Tunneling technique. Instead of sending the packets directly to the CN, the MN sends the packets back to the HA, and then the HA forwards them to the CN (Figure 2.8). However, considering routing inefficiency, the Reverse Tunneling technique might not be a good answer because it creates unnecessary delay if the CN is very close to the MN but is far from the HA.

[Perkins and Johnson, 2001] proposed a new technique called route optimization using the binding message mechanism shown in Figure 2.10a. With HA authorization, the CN can keep the binding cache of the MN home address and the COA. Within its lifetime, the CN can send messages directly to the COA rather than the HA. In case the MN has moved (Figure 2.10b), the FA sends a binding warning to the HA about the new binding, and then the HA sends a binding update to the CN for the right COA. If the lifetime has expired, the CN will send the binding update to the HA to refresh its binding cache. This binding message technique can also apply to the smooth handoff technique described in section 2.2.2

(Figure 2.10c).

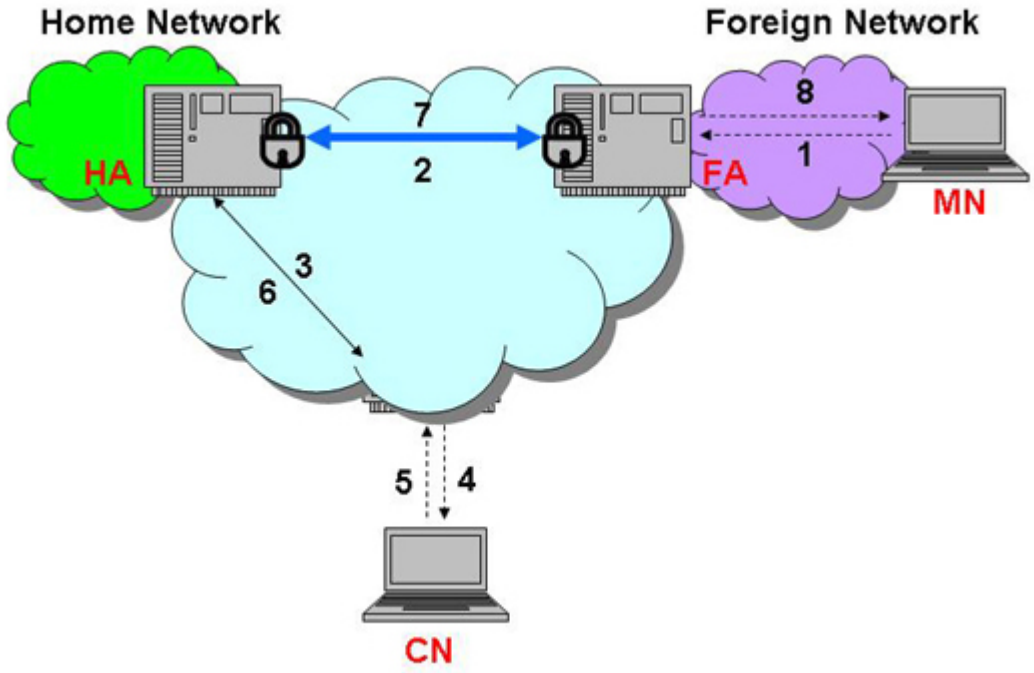
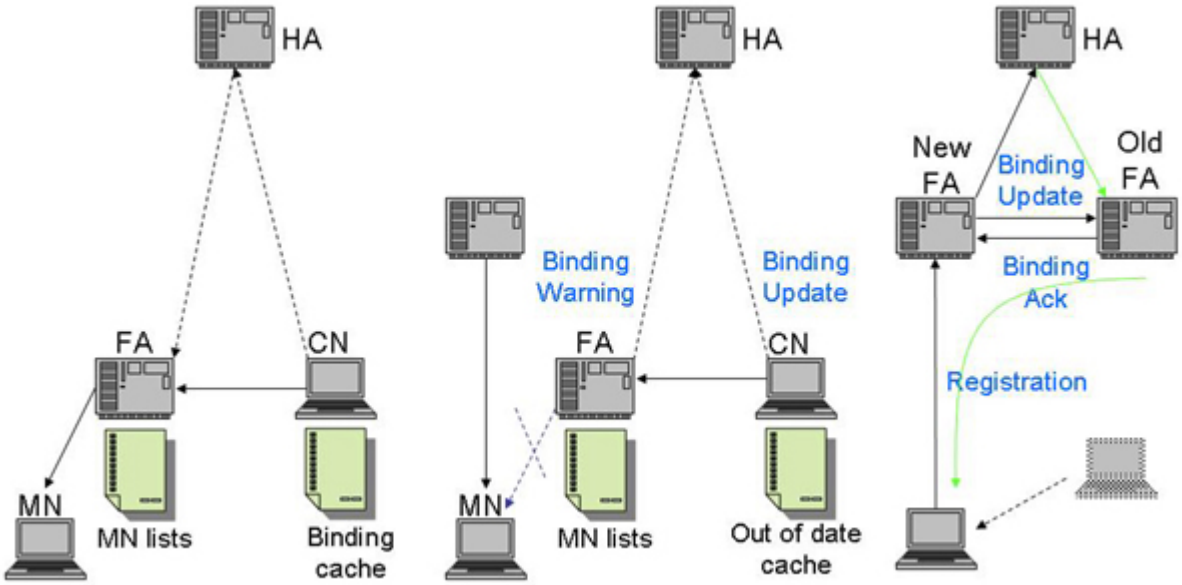


Figure 2.9: Reverse Tunneling



a) Binding Cache b) Binding Update/Warning c) Smooth handoff

Figure 2.10: Route Optimization

Back to Table of Contents

3. Concerns about Mobile IP

In this section, we survey the primary issues of Mobile IP: quality of service (QOS), multicast, security,

voice over Mobile IP, and TCP over Mobile IP.

3.1 Quality of Service (QOS)

Aside from the major problem in Mobile IP, disruption during the handoff, QOS is the next greatest, especially to guarantee traffic flow. Basically, there are three Internet QOS techniques: Integrated Services (IntServ), Differentiated Service (DiffServ), and Multiprotocol Label Switching (MPLS). The Resource ReSerVation Protocol (RSVP) is used as a signaling protocol for IntServ. PATH messages and ResV message are sent back and forth in order to negotiate QOS requirements before establishing the connection. DiffServ uses the information in the IPv4 header (TOS field) to differentiate the QOS. MPLS is a recent technique which simulates the circuit switching in an IP network. Instead of routing, the MPLS does switching based on the label inside each packet.

Just like IP, Mobile IP can use all the techniques above to provide quality of service; however, some special modifications might have to be applied. For example, after encapsulating a voice packet with high priority, in practice the intermediate routers might treat the packet as an IP-in-IP packet, and then they might modify the priority level for that packet. The tunnel template is used to solve this problem [Raab and Chandra, 2005]. The QOS survey on Mobile IP by Abd-Elhamid M Taha et al. [M. Taha et al., 2005] is very precise and also covers almost all QOS topics. They list current QOS techniques and describe the QOS Extensions for Mobile IP: IntServ, DiffServ, and Mobile IP-Specific MPLS Extension. Eight of RSVP Extensions are analyzed comparatively: Mobile Extension to RSVP, Mobile RSVP (and with modification), HMRSVP (and with modification), RSVP-MP, Localized RSVP, and RSVP for MIPv6. Current MPLS Extensions are also considered: MPLS/MIP, Mobility Aware MPLS, HM-MPLS, and MMPLS-Based Hierarchical MIP (Tables 3.1 and 3.2).

Table 3.1: Comparison of RSVP Extensions [Raab and Chandra, 2005]

	Considers intradomain mobility?	**Relies on passive states?**	**Prereservation Basic?**	**MIPv6-compatible?**	**Route recovery for handoff?**
Mobile Extension to RSVP	No	Yes, but could be temporarily reassigned.	Generic	No: heavily relies on an FA	N/A
Mobile RSVP	No	Yes	Node knows whole path a priori.	Yes	N/A
Mobile RSVP with modifications	No	Yes	Six neighboring cells	Yes	N/A
HMRSVP	Yes	No	Only during coverage overlaps	Yes	Up to GFA for local movements. Total path when GFA changed.
Modified	Yes	No	Only during coverage	Yes	Up to GFA for local movements.

HMRSVP			overlaps		Total path when GFA changed.
RSVP-MP	Yes	No	-	Yes	None
Localized RSVP	Yes	No	-	Yes	Only up to a crossover router
RSVP for MIPv6	No	No	-	Yes	Only up to a crossover router

Table 3.2: Comparison of MPLS Extensions [Raab and Chandra, 2005]

	Considers intradomain mobility?	**Reliance on static LSPs**	**MIPv6-compatible?**	**Route recovery for handoff?**	**Notes**
MPLS/MIP	No	No	No: requires FA functionality.	Total path.	-
Mobility Aware MPLS	Yes	Yes	Yes: GW could be an edge LSR.	Only up to a crossover router.	-
HM-MPLS	Yes: two-tier only.	No	No: requires FA functionality	Only up to a crossover router.	Extended for IntServ over DiffServ solution and RSVP-TE
MMPLS-Based Hierarchical MIP	Yes	No	Yes	Total path.	

3.2 Multicast

IP multicast is an efficient way to send packets from one host to multiple hosts. However, in Mobile IP, traditional multicasting techniques (DVMRP, MOSPF, CBT, and PIM) increase the difficulty when the mobile nodes frequently leave and join the multicast tree. [Montenegro, 1996] proposed the first two Mobile IP multicast techniques, Bi-directional Tunneling and Remote Subscription. The first technique depends only on a MN subscription. Whenever the MN joins a new network, it sends an Internet Group Management Protocol (IGMP) message directly to a multicast router (MR) in its foreign network to join the multicast group. Then, the distribution tree is recomputed. Although the routing path is optimal, it causes more transmission delays and packet losses. The second technique depends on the HA. The MN sends the multicast packets through the unicast tunneling between the MN and its HA. So, whenever the MN moves, there is no need to reconstruct the multicast distribution tree; however, it might cause a non-optimal routing path and the tunnel convergence problem.

[Harrison et al., 1997] proposed the Mobile Multicast (MoM) scheme. It basically selects one of the

HAs as the Designated Multicast Service Provider (DMSP), which forwards the multicast packets to the MNs. As a result, network traffic is reduced substantially. [Chikarmane et al., 1998] and [Xylomenos and Polyzos, 1997] compared the three techniques aboveas shown in Table 3.3. Remote Subscription outperforms the other techniques; however, Bi-Directional Tunneling offers good security.

Table 3.3: Comparison of three mobile multicast techniques [Chikarmane et al., 1998] and [Xylomenos and Polyzos, 1997]

Category	Remote Subscription	Bi-Directional Tunneling	Mobile Multicast
Optimal Routing	Yes	No	No
Transparency	No	Yes	Yes
Redundant packet delivery	No	Yes	Minimal
Delivery of scoped multicast	No	Yes	Yes
Multicast protocol independent	Yes	Yes	Yes
Join and graft delays	Yes	No	No
Entities modification	FA	HA, MN	HA, FA, MN
Security Support	No	Yes	No
Protocol Overhead	No	Yes	Yes
Delivery Overhead	No	Yes	No
Multicast Routing	Optimum	Suboptimum	Suboptimum

[Richard and Wang, 2002] proposed the Range-based Mobile Multicast Protocol (RBMoM). This technique attempts to combine both traditional techniques above (Bi-directional Tunneling and Remote Subscription) and also to overcome the MoM disadvantages, especially the non-optimal routing path. The RBMoM makes a trade off between the optimal routing path and the frequency to update the multicast distribution tree by controlling the service range of the multicast home agent (MHA). The MHA controls the multicast forwarding packets through the tunnels to all FAs. Another technique, Mobile Multicast Gateway (MMG) [Ye et al., 2003] was introduced to replace MHA. This gateway works as both Mobile IP and multicast. They claim that this technique not only eliminates the tunnel convergence problem and optimizes routing efficiency, but also gives superior results.

3.3 Security

Security is always a big concern for Mobile IP wireless networks. Anybody can intercept the packets, so the Mobile IP has a number of vulnerabilities. This section discusses the application and security aspects of the Mobile IP. First we briefly describe the security architecture for Internet Protocol known as IPSec which is defined by the IETF (The IPSec concept can be applied to secure the Mobile IP). The IPSec defines a suite of protocols which describe security mechanisms and services for the IPv4 and the IPv6 and upper layers. Figure 3.1 shows the IPSec security architecture, in which three protocols are defined: Encapsulating Security Payload (ESP), Authentication Header (AH), and Internet Key Exchange (IKE).

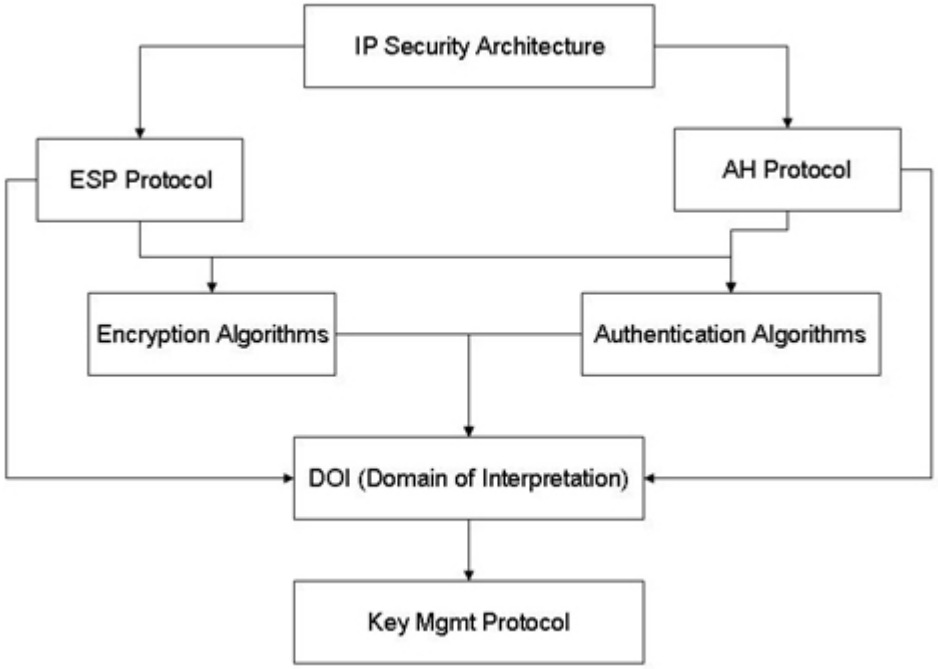


Figure 3.1: IPSec security architecture [Tuquerres et al., 1999]

Basically, there are two modes of encapsulation, Tunnel Mode and Transport Mode. For Tunnel Mode, the AH is put in between the new IP header and the original IP header if IPv4, but after the extension header and the original IP header if IPv6. For Transport Mode, if IPv4, the AH is put after the original IP header, and before the Destination Option if IPv6. ESP is put in the same place as the AH for both modes, but the ESP trailer and ESP authentication are required after the data portion.

Figure 3.1 also shows that the AH does not support encryption (authentication only) for protecting confidentiality; the ESP may be used to provide both privacy and authentication. Basically, both the AH and the ESP protocols need the concept of sharing keys among the parties. The IKE protocol has been defined to establish the session key. Security Association is used as a unidirectional agreement between the parties that specifies a set of policies and keys. Table 3.4 shows a SA example.

Table 3.4: Security Association [Tuquerres et al., 1999]

SPI	Authentication Algorithm	Authentication Key	Replay Protection	Encryption Algorithm	Encryption Key
01234567	E.g., Keyed MD$	(a secret key)	Timestamp		
89ABCDEF				e.g., RSA	(public/private key)

Concerning Mobile IP, [Solomon, 1997] describes various kinds of possible attacks and recommended solutions. As described above (Section 2.2.1), a strong authentication technique (HMAC-MD5) is used to prevent a bogus registration which results in a Denial of Service (DOS) attack. With either the timestamp or nonce concept, replay attack can also be prevented. Passive eavesdropping is commonly used to attack. The attackers may listen on the exchanged traffic between the MN and the HA, and possibly can gain physical access either to wired networks, such as a shared Ethernet, or to wireless networks. As a result, Mobile IP is required to use end-to-end encryption for all traffic to avoid this kind of attack.

Moreover, strong cryptography can thwart another kind of attack called Session Stealing where the attackers wait for the MN to register with its HA, then eavesdrop to see the useful information. After that, the attackers send out a huge number of packets to put the MN out of action. Finally the attacker can capture the session and communicate with other nodes as a legitimate node.

With the Agent Advertisement feature of Mobile IP, attackers can figure out what the network prefixes are if there is no authentication with either HA or FA. They can then guess the available host number to use. After listening for a while, they can possibly figure out what addresses are currently not being used. To prevent this attack, the □R□ bit in Agent Advertisement message has to be enforced, so that all visiting MNs are required to register with the FA. Then, all MNs who wish to connect to the FA have to perform link layer encryption to the FA.

[Islam, 2005] did a brief security survey on Mobile IP. Security Mobile IP (Sec MIP) was also proposed by using IPSec. The MN has to authenticate either the FA or the Firewall by IPSec functionality. Islam also listed several current security proposals using either the AH or the ESP in IPSec to enhance the Mobile IP security. Public key encryption and key certificates are also used to secure the Mobile IP communication. Also, he proposed a system to secure mobility support (Security Border Gateway) with the use of IPSec, Ingress Filtering, and symmetric bi-directional route optimization.

3.4 Voice over Mobile IP

Deploying voice over Mobile IP seems to be a simple way to add value to an integrated mobile network. However, due to the major weaknesses of Mobile IP, route optimization and handoff latency, Mobile IP may need to be optimized in order to improve voice quality by minimizing the end-to-end delay, delay jitter, and packet loss. [Seol et al., 2002] investigated the possibility of deploying Internet telephony over Mobile IP. SIP-based mobility support [Wedlund and Schulzrinne, 1999] was used in this investigation. They found that the packet size has the main impact on increasing the packet transmission delay. Also, to optimize the delay and network load on the network, they recommended the packet size should be set to three frames (33 bytes each) per packet.

[Fathi et al., 2005] evaluated Mobile IPv4 and Mobile IPv6 in terms of handoff delay performance. Considering only the handoff delay performance, Mobile IPv4 is appropriate use for Voice over IP service, but Mobile IPv6 is preferable if considering end-to-end delay performance. Also, they recommended that Hierarchical MIPv6 for optimizing both performances. They found that the handoff performance depends on the frame error rate, so the Adaptive Retransmission Timer scheme was also proposed to reduce the frame error rate by reducing the back-off timer adaptively.

For Mobile IP on wireless networks (IEEE 802.11based networks), there are currently two techniques to improve handoff performance. First, the Scalable QOS Provisioning Scheme (SQPS) for mobile networks uses wireless sensors based on location tracking. The FA can make a resource reservation in advance to reduce the packet loss during handoff. However, this scheme needs the FA to inform the previous FA where to forward the traffic. A second scheme is the Low-latency Guarantee Handoff Scheme (LHSQ). This technique can reduce the packet loss rate substantially with the Wireless Rether QOS mechanism; however, extra bandwidth is needed for the active application.

[Wang and Kuo, 2005] proposed the new scheme not only to reduce the delay but also to decrease the occupied bandwidth for voice over Mobile IP applications for Infrastructure-Mode Wireless LANs. This scheme optimizes the header caching for the packetization process and uses low-latency LHSQ to reduce the delay. With end-to-end delay, delay jitter, and packet loss as main measurement metrics, they claim that this scheme outperforms both SQPS and LHSQ. Compared to 3.88 for SQPS and 4.19 for

LHSQ, the AMOS (sum of the MOS values divided by number of the calls) for this scheme can be up to 4.35.

3.5 TCP over Mobile IP

Many versions of TCP (Tahoe, Reno, NewReno, Vegas, Sack, and so on) have been released to improve performance, reduce loss late, increase throughput, and provide fair shares for each connection. However, all these versions works on wired networks. This section describes the TCP enhancement technique and TCP performance issues used to adapt the TCP to work on Mobile IP in both wired and wireless networks, with the original goal of Mobile IP, to maintain the TCP session.

[Mohamed et al., 2002] investigated the effects of the Retransmission Timeout (RTO) on TCP performance during the handoff. In contrast to Van Jacobson and standard TCP retransmission timeout algorithms which use adaptively changing RTO, they claim that using the FxRTO (Fixed RTO) algorithm which RTO is set to *RTT*p* (RTT is the round trip time of the first segment and p is a constant between 3 and 4) can reduce the long pauses in TCP communication during handoff. Pauses can cause a large timeout in wireless communication. As a result, the average throughput is much higher with this algorithm.

[Parameswaran and Sankar, 2004] did simulations to observe the effect of TCP flavors on the throughput of FTP data on a wireless LAN. TCP Tahoe, NewReno, Sack, and Vegas were examined in the experiment. Generally, with increasing distance, the throughput also increases for all TCP versions. However, by combining the delayed acknowledgement functionality, overall throughput increases substantially. The delay acknowledgement interval just makes the throughput slightly decrease. They also reported that TCP Vegas exhibits the least throughput.

[Ho et al., 2005] investigated how to improve TCP Vegas efficiency after handoff, since TCP Vegas is sensitive to RTT change. In wireless networks, TCP Vegas can not tell whether the variability of RTT is due to the network congestion or to the change of routing update. They also proposed Demo-Vegas protocol which provides higher throughput. The Demo-Vegas can detect the movement of the connection. If needed, it updates the BaseRTT (Minimum Route Trip Time) with the use of the exiting one unused bit (SIG bit) in the TCP header. Whenever MN has moved or changed its COA, it will tell the sender to re-measure BaseRTT by setting its SIG bit.

[Chang et al., 2005] evaluated TCP performance in terms of dropped packets and maintenance of lasting the connection with the MN and the CN on Mobile IPv4 and Mobile IPv6. They claim that the TCP performance on Mobile IPv6 outperforms that on Mobile IPv4. Then, due to the broad unavailability of Mobile IPv6 network, they also designed a virtual Mobile IPv6 network over Mobile IPv4 infrastructure with the 6-to-4 tunneling capability for all access routers in a fixed IPv4 network.

Back to Table of Contents

---

4. Mobile IPv6

In addition to supporting all Mobile IPv4 functionalities, Mobile IPv6 also provides many mobility protocol improvements [RFC 3775, 2004]. Unlike Mobile IPv4, Mobile IPv6 itself is a part of the IPv6 address, not just the UDP message for registration processes (Figure 2.3). There is no need for the FA, since the MN obtains its new IPv6 address (CCOA) by auto-configuration (DHCP) called Stateless

Address Auto Configuration [RFC 2462, 1998]. Consequently all routers must perform the router advertisement function. In terms of route optimization, Mobile IPv6 defines the Destination Options. With binding update, binding acknowledgements, and the Return Routability mechanisms integrated in the IP6 packet, the MN can communicate directly to the CN. Figure 4.1 shows a typical Mobile IPv6 operation.

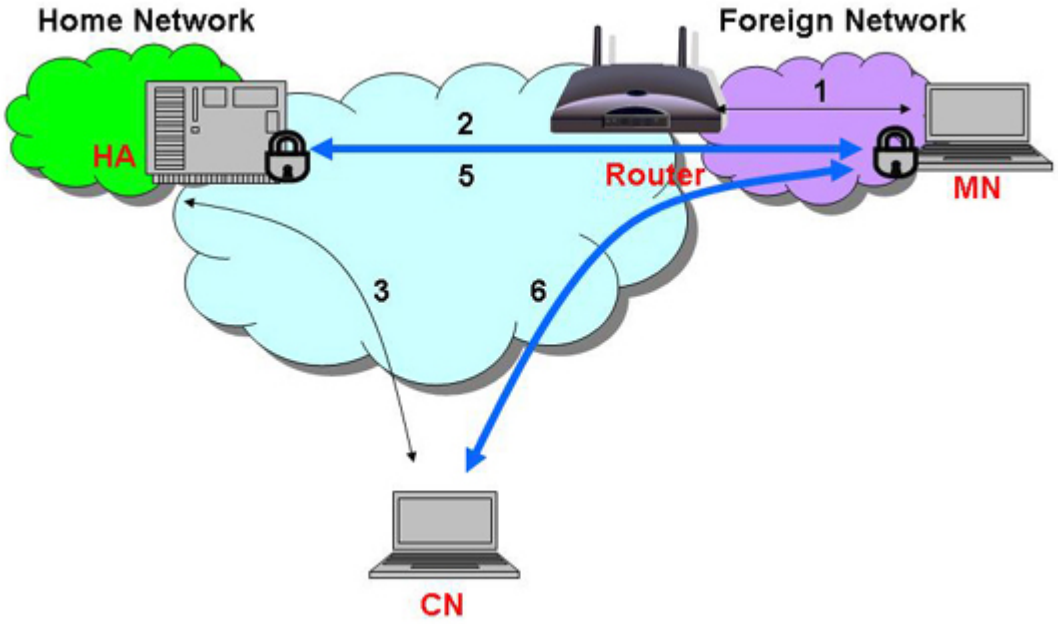


Figure 4.1: Mobile IPv6 operation

First, by Neighbor Discovery [RFC 2461, 1998], the MN detects the movement by network prefix functionality. Then, the MN obtains the CCOA (1). The MN sends the binding update to the HA (2). The HA updates its binding list and sends the acknowledgement message back. If the CN wants to send the packets to the MN, it sends them to the MN home address as usual. The HA intercepts the packets and checks its binding list with the data□s destination address. The HA then makes a tunnel to the MN□s COA. When the MN receives a packet, with the Destination Option, it sends the binding update to the CN. Finally, the CN can send the packets to the MN□s COA directly.

Mobile IPv6 also reduces the signaling traffic between the MN, the CN, and the HA by localizing registration within the region, a technique called the Hierarchical Mobile IPv6 (HMobile IPv6) [Soliman et al., 2004]. Together with Mobile IPv6 Fast handover [Koodli, 2006], the handoff latency is improved substantially. In terms of security, apart from Mobile IPv4 security support such as DOS and replay attack, Mobile IPv6 fully supports end-to-end IPSec [RFC 3776, 2004] and [Zao and Condell, 1997]. Also, Cookie and Token concepts with HMAC_SHA1 instead of HMAC_MD5 are used to protect the binding update message.

Back to Table of Contents

---

5. Mobility Support in IP

[Debashis et al., 2004] surveyed IP-related Mobility protocols. Mobile IP, HAWAII, Cellular IP, Hierarchical MIP, TeleMIP, Dynamic Mobility Agent, and Terminal Independent MIP are

comparatively analyzed for location update, handoff latency, and signaling overhead. They grouped the protocols into three different categories: Micro mobility (Intrasubnet mobility), in which MN moves within a subnet; Macro mobility (Intradomain mobility), in which MN moves within a domain but different subnets; and Global mobility (Interdomain mobility), in which MN moves across the different domains. Figure 5.1 shows the Mobility protocol classification.

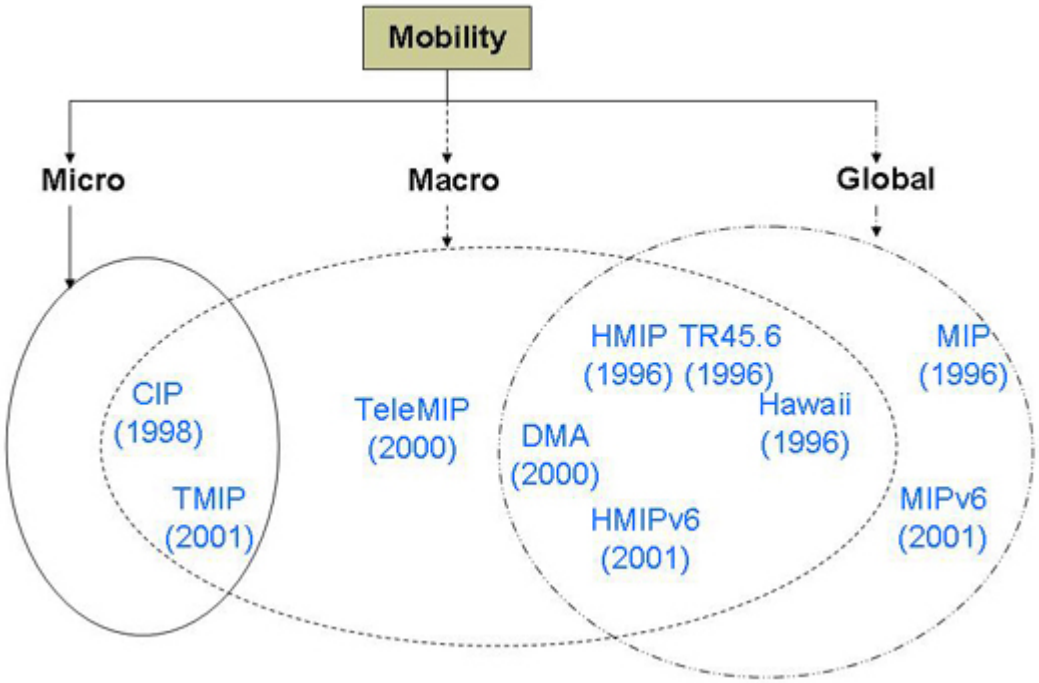


Figure 5.1: Mobility classification of protocols [Debashis et al., 2004]

The IP Mobility protocols have their own advantages and disadvantages which depend on their protocol goal; for example, the Mobile IP goal targets the global mobility but it causes delays and packet losses. In Debashis et al., the comparison of each IP-based mobility protocol was shown in Table 5.1. Overall, TeleMIP is better for macromobility management in terms of the overhead signaling but not for the security and QOS issues.

Table 5.1: Comparison of IP mobility support [Debashis et al., 2004]
(Y = valid, N = non-valid)

	MIP	HMIP	TR45.6	CIP	HAWAII	TeleMIP	DMA
Global connectivity	Y	Y	Y	Y	Y	Y	Y
AAA and security	Y	N	Y	N	N	N	N
Global roaming facility	Y	Y	Y	Y	Y	Y	Y
Stable point of attachment	N	N	N	N	N	Y	Y
Real-time traffic	N	N	N	N	N	N	N

management							
QOS support	N	N	N	N	N	N	Y
Dynamic address allocation	N	N	N	N	N	Y	Y
Protocol layers	L3	L3.5	L3	L3	L3	L3	L3
Paging Support	N	Y	N	Y	Y	N	Y
LU	Datagram tunneling	Update Message	Update Message	Data Packet	Update Message	Update Message	Binding Update
Route optimization	Mobility binding	N	Y	N	N	Non optimal	N
Mobility Management	Global	Global /Macro	Global	Macro/Micro	Global /Macro	Macro	Global /Macı
Handoff Control	Smooth handoff by special tunnel binding	Hard	Hard	Hard / and Soft	Path setup schemes	Hard	Soft (proactive multicasting
Signaling Overhead	Higher	Highest	Higher	Lowest	Lower	Lowest	Low
Latency	High	High	Low	Low	Low	Low	Low

Back to Table of Contents

6. Mobile IP availability

Since Mobile IP has existed for over a decade, in this section, the previous and current implementations are surveyed. In 1994, [Perkins et al., 1994] proposed the Internet Mobile Host Protocol (IMHP) which supports both the route optimization and integrated authentication of all management information. Security is the main disadvantage for this protocol. [Gupta, 1998] proposed the Solaris Mobile IP which mainly supports the firewall traversal. Though named Solaris, this system is run on the Linux operating system. The MosquitoNet Research Group at Stanford University developed the Mobile IP implementation [Baker et al., 1999] for the Linux operating system that assumes the lack of the FA, and so uses the collocated care-of address scheme. Another free Mobile IP implementation in the Linux operating system for both Mobile IPv4 and Mobile IPv6, is in the Monarch Research Project at the Carnegie-Mellon group website http://www.monarch.cs.cmu.edu/. This implementation also includes both IP-in-IP and Minimal encapsulations.

The Portland State Secure Mobile Networking Project provided security (IPSec) for the Mobile IP. The implementation can be found at http://www.cs.pdx.edu/research/SMN/index.html. [Su-xiang et al., 2004] added the tunneling scheme into the Linux kernel to improve speed and security. [Forsberg et al.,

1999] at Helsinki University of Technology developed a hierarchical version of the Mobile IP called The Dynamics Mobile IP system for Linux. Some parts of this project can be ported to a Microsoft Windows based system. The source code is available at: http://dynamics.sourceforge.net/. This scheme supports both private addresses and fast handoffs and also allows hierarchical agents for fast registration. [Valko et al., 1999] at Columbia University proposed the new simplicity and scalability protocol, Cellular IP, which supports host mobility in a Cellular Wireless Network. This scheme is suitable for environments where the MN moves frequently. [Mondal, 2003] describes some of the current Mobile IP implementations and also did the comparison among their features shown in Table 6.1.

On the commercial side, most of the networking companies support Mobile IP: [Cisco, 2003], [Nokia, 2005], [Siemens, 2005], [Hewlett-Packard, 2003], and so on.], and so on. In terms of Mobile IP client services, providers [BirdStep, 2005], [Secgo, 2005], and [ipUnplugged, 2005] are the three top most products which are compatible to most of the network. Although [Microsoft, 2004] claims that Microsoft Research has been developing Mobile IPv6 technology, only the CN support is included in Microsoft Windows XP with Service Pack 1, Windows XP with Service Pack 2, and Windows Server 2003. Also, currently Mobile IPv6 Technology will not be available until there is enough customer demand.

Even though current network equipment fully supports Mobile IP, there is still a need to update the network operating system, which might require upgrading or replacing routers and switches [Cisco, 2003]. Another concern is that users do not see the need to use Mobile IP as [Microsoft, 2004] claims. As a result, we currently do not see real implementation of Mobile IP happening globally.

Table 6.1: Comparison of Mobile IP implementations [Mondal, 2003]

Feature	Dynamic	MosquitoNet	Solaris MIP	Cellular IP	IMHP
Compatibility with existing protocols	High	High	Medium	Medium	Medium
Dependency on network support	High	Low	Medium	High	High
Support for Optimal routing	Average	High	Above average	Low	Above average
Support for Security	High	Low	Medium	Low	High
Scalability	Highest	Above average	Average	Lowest	Average
Speed of Handoff	Fast	Average	Average	Above Average	Slow
Overheads	High	Low	Below Average	High	Average

Back to Table of Contents

7. Summary

In this paper, we give a summary on Mobile IP concepts, terminology, functionality, and operation.

Various networking issues are also surveyed: Quality of Service (QOS), Multicast, Security, Voice over Mobile IP, and TCP over Mobile IP. Mobile IPv6 concepts and operation are also explained. Surveys of IP-based Mobility and Mobile IP implementations are presented.

Mobile Internet Protocol research is still ongoing, and there are new standards to be developed. We recommend going to the Mobile IP IETF website for updated Request for Comments and Internet Drafts at http://www.ietf.org/html.charters/mip4-charter.html and http://www.ietf.org/html.charters/mip6-charter.html.

Back to Table of Contents

References

[Perkins, 2002a] Charles E. Perkins, "Mobile IP," Communications Magazine, IEEE Volume 40, Issue 5, Part Anniversary, May 2002 Pages: 66 - 82.
This paper describes the mobility support for IPv4 and IPv6.

[RFC 3344, 2002] Charles E. Perkins, "IP Mobility Support for IPv4," Request for Comments (Proposed Standard) 3344, Internet Engineering Task Force, August 2002. available online at http://www.ietf.org/rfc/rfc3344.txt.
This RFC specifies the mobility support for IPv4.

[RFC 3775, 2004] D. Johnson, C. Perkins, and J. Arkko, "Mobility Support in IPv6," Request for Comments (Proposed Standard) 3775, Internet Engineering Task Force, June 2004. available online at http://www.rfc-editor.org/rfc/rfc3775.txt.
This RFC specifies the mobility support for IPv6.

[Raab and Chandra, 2005] Stefan Raab and Madhavi W. Chandra, "Mobile IP Technology and Applications," Cisco Press, 2005.
This book presents and discusses various kinds of Mobile IP overview and techniques.

[Yu et al., 2003] Liu Yu, Ye Min-hua, and Zhang Hui-min, "The handoff schemes in mobile IP," Vehicular Technology Conference, 2003. VTC 2003 Spring. The 57th IEEE Semiannual Volume 1, 22-25 April 2003 Pages: 485 - 489.
This paper describes the current handoff scheme in Mobile IP and also proposed new scheme.

[Koodli and Perkins, 2006] Rajeev Koodli and Charles E. Perkins, "Mobile IPv4 Fast Handovers," Internet Draft, Internet Engineering Task Force, draft-ietf-mip4-fmipv4-00.txt, February 2006. available online at http://www.ietf.org/internet-drafts/draft-ietf-mip4-fmipv4-00.txt.
This draft specifies how to make the handover fast in Mobile IPv4.

[Koodli, 2006] Rajeev Koodli, "Fast Handovers for Mobile IPv6," Internet Draft, Internet Engineering Task Force, draft-ietf-mipshop-fast-mipv6-03.txt, October 2005. available online at http://www.ietf.org/internet-drafts/draft-ietf-mipshop-fast-mipv6-03.txt.
This draft specifies how to make the handover fast in Mobile IPv6.

[Cao et al., 2004] Jiannong Cao, Liang Zhang, Henry Chan, and Das, S.K,"Design and performance evaluation of an improved mobile IP protocol," INFOCOM 2004. Twenty-third AnnualJoint Conference

of the IEEE Computer and Communications Societies Volume 1, March 2004 Pages: 7-11.
This paper presented the mailbox-based scheme in order to reduce the signal message and also reduce the load of HA.

[Gustafsson et al., 2006] E. Gustafsson, A. Jonsson, and C. Perkins, "Mobile IPv4 Regional Registration," Internet Draft, Internet Engineering Task Force, draft-ietf-mip4-reg-tunnel-01.txt, June 2006. available online at http://www.ietf.org/internet-drafts/draft-ietf-mip4-reg-tunnel-01.txt.
This draft specifies the way to make a registration process locally (within a region).

[RFC 1256, 1991] S. Deering, "ICMP Router Discovery Messages," Request for Comments (Proposed Standard) 1256, Internet Engineering Task Force, September 1991. available online at http://www.rfc-editor.org/rfc/rfc1256.txt.
This RFC specifies the original IRDP which Agent Advertisement and Solicitation protocols are based on.

[RFC 2003, 1996] Charles E. Perkins, "IP Encapsulation within IP," Request for Comments (Proposed Standard) 2003, Internet Engineering Task Force, October 1996. available online at http://www.rfc-editor.org/rfc/rfc2003.txt.
This RFC specifies one of the Mobile IP encapsulation techniques, IP-in-IP, by which an IP datagram is encapsulated within a new IP datagram.

[RFC 2004, 1996] Charles E. Perkins, "Minimal Encapsulation within IP," Request for Comments (Proposed Standard) 2004, Internet Engineering Task Force, October 1996. available online at http://www.rfc-editor.org/rfc/rfc2004.txt.
This RFC specifies one of the Mobile IP encapsulation techniques, Minimal Encapsulation, by which an IP datagram is modified to avoid the repetition in the IP datagram.

[RFC 2784, 2000] D. Farinacci, T. Li, S. Hanks, D. Meyer, and P. Traina, "Generic routing encapsulation GRE," Request for Comments (Proposed Standard) 2784, Internet Engineering Task Force, March 2000. available online at http://www.rfc-editor.org/rfc/rfc2784.txt.
This RFC specifies one of the Mobile IP encapsulation techniques, GRE, by which a special header is added in between the original IP header and new IP header to support various transport layer protocols.

[RFC 2827, 2000] P. Ferguson and D. Senie, "Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing," Request for Comments (Proposed Standard) 2827, Internet Engineering Task Force, May 2000. available online at http://www.rfc-editor.org/rfc/rfc2827.txt.
This RFC specifies the Network Ingress Filtering at the Firewall and also shows the modification for Mobile IP.

[RFC 3024, 2001] G. Montenegro, "Reverse Tunneling for Mobile IP, revised," Request for Comments (Proposed Standard) 3024 Internet Engineering Task Force, January 2001. available online at http://www.rfc-editor.org/rfc/rfc3024.txt.
This RFC shows the technique to overcome if the Firewall setup Network Ingress Filtering.

[Perkins and Johnson, 2001] Charles E. Perkins and David B. Johnson, "Route Optimization in Mobile IP," Internet Draft, Internet Engineering Task Force, draft-ietf-mobileip-optim-11.txt, September 2001. available online at http://www.ietf.org/internet-drafts/draft-ietf-mobileip-optim-11.txt.
This draft specifies an extension to the operations of the base Mobile IP protocol to allow for optimal routing when CN wants to send the message to MN directly.

[M. Taha et al., 2005] Abd-Elhamid M. Taha, Hossam S. Hassanein, and Mouftah T. Mouftah, "Extensions for Internet QoS paradigms to mobile IP: a survey," Communications Magazine, IEEE Volume 43, Issue 5, May 2005 Pages: 132 - 139
This paper reviews an extension of QOS on Mobile IP and also the authors did the comparison for QOS techniques on Mobile IP.

[Montenegro, 1996] G. Montenegro, "Bi-directional Tunneling for Mobile IP", Internet Draft, Internet Engineering Task Force, draft-montenegro-tunneling-01.txt, September 1996. available online at http://www.ietf.org/internet-drafts/draft-montenegro-tunneling-01.txt.
This paper presents the original technique for Multicast on Mobile IP, Bi-directional Tunneling for Mobile IP.

[Harrison et al., 1997] Tim G. Harrison, Carey L. Williamson, Wayne L. Mackrell, and Richard B. Bunt, "Mobile Multicast (MoM) Protocol: Multicast Support for Mobile Hosts," Proceedings of ACM/IEEE MOBICOM'97, September 1997 Pages: 151-160.
This paper presents new technique for Multicast on Mobile IP, MoM.

[Chikarmane et al., 1998] Vineet Chikarmane, Carey L. Williamson, Richard B. Bunt, Wayne Mackrell, "Multicast Support for Mobile Hosts Using Mobile IP: Design Issues and Proposed Architecture," ACM Mobile Networks and Application, March 1998, Pages: 365-379.
This paper reviews two Multicast techniques on Mobile IP and also the authors did the comparison on Remote Subscription, Bi-Directional Tunneling, and MoM.

[Xylomenos and Polyzos, 1997] G. Xylomenos and G. Polyzos, "IP Multicast for Mobile Hosts," IEEE Communications, January 1997, Pages: 55 -58.
This paper presents the comparison for Remote Subscription, Bi-Directional Tunneling, and MoM.

[Richard and Wang, 2002] Chunhung Richard and Kai-Min Wang, "Scalable multicast protocol in IP-based mobile networks," ACM Wireless Networks, Vol. 8, Issue 1 January 2002, Pages: 27-36.
This paper presents another scheme for Multicast technique for Mobile IP, Range-based Mobile Multicast Protocol.

[Ye et al., 2003] Min-hua Ye, Lv-yun Yang, Yu Liu, and Hui-min Zhang, "The implementation of multicast in mobile IP," WCNC 2003 - IEEE Wireless Communications and Networking Conference, Vol. 1, March 2003 Pages: 1796-1800.
This paper presents another scheme for Multicast technique for Mobile IP by using Mobile Multicast Gateway in Range-based Mobile Multicast Protocol.

[Solomon, 1997] J. D. Solomon, "MobileIP - The Internet Unplugged," Prentice-Hall, 1997.
This books presents security issues on Mobile IP and some techniques to solve the problems.

[Islam, 2005] Rafiqul Islam, "Enhanced Security In Mobile IP Communication," Master of Science Thesis, Royal Institute of Technology, Stockholm University, Sweden February 2005
This thesis presents some security issues on Mobile IP and proposed new scheme to o secure the mobility support.

[Tuquerres et al., 1999] Gloria Tuquerres, Rogerio Salvador, and Ron Sprenkels, "MOBILE IP: SECURITY & APPLICATION," University of Twente, The Netherlands, December 1999.
This thesis presents some security issues on Mobile IP and proposed new scheme to o secure the mobility support.

[Zao and Condell, 1997] John K. Zao and Matt Condell, "Use of IPSec in Mobile IP," Internet Draft, Internet Engineering Task Force, draft-ietf-mobileip-ipsec-use-00.txt, November 1997. available online at http://www.ietf.org/internet-drafts/draft-ietf-mobileip-ipsec-use-00.txt.
This draft specifies the use of IPsec in Mobile IP.

[RFC 3776, 2004] J. Arkko, V. Devarapalli, and F. Dupont, "Using IPsec to Protect Mobile IPv6 Signaling Between Mobile Nodes and Home Agents," Request for Comments (Proposed Standard) 3776, Internet Engineering Task Force, June 2004. available online at http://www.rfc-editor.org/rfc/rfc3776.txt.
This RFC specifies how to use IPsec to secure the signaling message between MN and HA.

[Fathi et al., 2005] Hanane Fathi, Shyam Chakraborty, and Ramjee Prasad, "Mobility management for VOIP: Evaluation of Mobile IP-based protocols," Communications, 2005. (ICC 2005) 2005 IEEE International Conference, Vol. 5, May 2005 Pages: 3230 - 3235.
This paper presents the evaluation of Mobile IPv4 and Mobile IPv6 in terms of the performance of handoff delay.

[Wang and Kuo, 2005] Min Wang and Geng-Sheng (G.S.) Kuo, "Enhancement of voice over mobile IP for infrastructure-mode wireless LANs," Global Telecommunications Conference, 2005. GLOBECOM'05. IEEE Vol. 5, December 2005 Pages: 2642 - 2646
This paper presents new scheme for voice over Mobile IP applications for Infrastructure-Mode Wireless LANs.

[Seol et al., 2002] Soonuk Seol, Myungchul Kim, Chansu Yu, and Jong-Hyun Lee, "Experiments and analysis of voice over Mobile IP," Personal, Indoor and Mobile Radio Communications, 2002. The 13th IEEE International Symposium, Vol. 2, 15-18 September 2002 Pages: 977 - 981.
This paper presents the investigation of the possibility to deploy Internet telephony over Mobile IP.

[Wedlund and Schulzrinne, 1999] Elin Wedlund and Henning Schulzrinne, "Mobility support using SIP," In Proceedings of the 2nd ACM international workshop on Wireless mobile multimedia, 1999, Pages: 76 -82.
This paper specifies how to use SIP-based in mobility support.

[Chang et al., 2005] Sujeong Chang, Jaehyung Park, Yonggwan Won, Mijeong Yang, and Min Young Chung, "Performance Comparison of TCP Traffic over Mobile IPv4 and IPv6 Networks and a Mobile Network Deployment Approach," Computer and Information Technology, 2005. (CIT 2005) The Fifth International Conference, September 2005 Pages: 469 - 473.
This paper presents the evaluation of the TCP performance in terms of dropped packets and lasting the connection with MN and CN on Mobile IPv4 and Mobile IPv6.

[Ho et al., 2005] Cheng-Yuan Ho, Yi-Cheng Chan, and Yaw-Chung Chen,"An efficient mechanism of TCP-Vegas on mobile IP networks," INFOCOM 2005, 24th Annual Joint Conference of the IEEE Computer and Communications Societies. In Proceedings IEEE Vol. 4, March 2005 Pages: 2776 - 2780.

This paper presents the investigation of how to improve TCP Vegas efficiency.

[Parameswaran and Sankar, 2004] Parmeswaran, A.K.; Sankar, R.,"Mobile IP throughput studies on a wireless LAN," SoutheastCon, 2004. In Proceedings. IEEE, Mar 2004 Pages: 234 - 238.
This paper specifies how to use SIP-based in mobility support.

[Mohamed et al., 2002] Yazid Mohamed, Norsheila Fisal, and Alias Mohd, "Performance of TCP on Mobile IP network during handoffs," Research and Development, 2002. (SCOReD 2002) July 2002 Pages: 390 - 393.
This paper specifies how to use SIP-based in mobility support.

[RFC 2461,1998] T. Narten, E. Nordmark, and W. Simpson, "Neighbor Discovery for IP Version 6 (IPv6)," Request for Comments (Proposed Standard) 2461, Internet Engineering Task Force, December 1998. available online at http://www.rfc-editor.org/rfc/rfc2461.txt.
This paper presents the observation of the effect of the TCP flavors on the throughput of FTP data on Wireless LAN.

[RFC 2462,1998] S. Thomson and T. Narten, "IPv6 Stateless Address Autoconfiguration" Request for Comments (Proposed Standard) 2462, Internet Engineering Task Force, December 1998. available online at http://www.rfc-editor.org/rfc/rfc2462.txt.
This RFC specifies an auto configuration on Mobile IPv6.

[Soliman et al., 2004] Hesham Soliman, Claude Catelluccia, Karim El Malki, and Ludovic Bellier, "Hierarchical Mobile IPv6 mobility management (HMobile IPv6)," Internet Draft, Internet Engineering Task Force, draft-ietf-mipshop-hmipv6-04.txt, December 2004. available online at http://www.ietf.org/internet-drafts/draft-ietf-mipshop-hmipv6-04.txt.
This draft specifies an auto configuration on Mobile IPv6

[Debashis et al., 2004] S. Debashis, M. Amitava, M. I Saha, and C. Mohuya, "Mobility Support in IP: A Survey of Related Protocols," IEEE Network, November 2004.
This paper presents the survey of the IP-related Mobility protocols.

[Reinbold and Bonaventure, 2002] Pierre Reinbold and Olivier Bonaventure,"A Survey of IP micro-mobility protocols," Technical report at Infonet group, University of Namur, Belgium, March 2002.
This paper presents the survey of the IP micro-mobility protocols.

[Baker et al., 1999] Mary G. Baker, Xinhua Zhao, Stuart Cheshire, and Jonathan Stone Stanford University, "Supporting Mobility in MosquitoNet," USENIX Annual Technical Conference 1999. available at the group web site at http://mosquitonet.stanford.edu/software/mip.html
This paper presents the Mobile IP implementation technique.

[Forsberg et al., 1999] D. Forsberg, J.T. Malinen, T. Weckstrom, M. Tiusanen, "Distributing Mobility Agents Hierarchically under Frequent Location Updates," Sixth IEEE International Workshop on Mobile Multimedia Communications (MOMUC'99), San Diego 1999.
This paper presents the Mobile IP implementation technique.

[Su-xiang et al., 2004] Weng Su-xiang, Liu Shu-fen, and Yao Zhi-lin, "An implementation of mobile IP's tunnel technology in Linux kernel," Computer Supported Cooperative Work in Design, 2004. Proceedings. The 8th International Conference, Vol. 1, May 2004 Pages: 459 - 461.
This paper presents the Mobile IP implementation technique.

[Gupta, 1998] Vipul Gupta, "Solaris Mobile IP: Design and Implementation," SUN Microsystems, Inc. February 1998, available online at http://playground.sun.com/mobile-ip/sunlabs/SolarisMobileIP.pdf
This paper presents the Mobile IP implementation technique.

[Perkins et al., 1994] Charles E. Perkins, Andrew Myles, and David B. Johnson, "The Internet Mobile

Host Protocol (IMHP)," In Proceeding INET June 1994 Pages: 642 - 651.
This paper presents the Mobile IP implementation technique.

[Valko et al., 1999] A. Valko, A. Campbell, and J. Gomez, "Cellular IP," Internet Draft, Internet Engineering Task Force, draft-valko-cellularip-00.txt, November 1998. available online at http://www.ctr.columbia.edu/~andras/cellularip/.
This paper presents the Mobile IP implementation technique on cellular network.

[Mondal, 2003] Abdul Sakib Mondal, "Mobile IP: Present State and Future," Springer, 2003.
This book describes the comparison of Mobile IP implementations.

[Cisco, 2003] "Mobile IP (Cisco)" available online at http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120t/120t1/mobileip.htm.
This article describes an overview of Mobile IP and the configuration of Mobile IP on Cisco network.

[Nokia, 2005] "Mobile VOIP: IP Convergence Goes Mobile" available online at http://www.nokia.com/NOKIA_COM_1/About_Nokia/Press/White_Papers/pdf_files/backgrounder_voip

This article describes an overview of Mobile IP and the configuration of Mobile IP on Nokia network.

[Hewlett-Packard, 2003] "HP-UX Mobile IPv4 A.02.01" available online at http://docs.hp.com/en/mobile-IPV4ad2/mobile-IPV4ad2.pdf.
This article describes an overview of Mobile IP and the configuration of Mobile IP on Hewlett-Packard network.

[Siemens, 2005] "Mobile IP Centrex" available online at http://www.siemens.com/Daten/siecom/HQ/COM/Internet/Mobile_Networks/WORKAREA/com_mnen/20IP%20Centrex%20White%20Paper_1351013.pdf.
This article describes an overview of Mobile IP and the configuration of Mobile IP on Siemens network.

[BirdStep, 2005] "Birdstep Intelligent Mobile IP Client v2.0, Universal Edition," available online at http://www.birdstep.com/collaterals/Mobile-IP-Universal-Edition-Business%20Whitepaper.pdf.
This article describes an overview of Mobile IP and the configuration of Mobile IP on Birdstep network.

[Secgo, 2005] "Internet Mobility Management with Secgo Mobile IP," available online at http://www.secgo.com/docs/secgo_mip_whitepaper.pdf.
This article describes an overview of Mobile IP and the configuration of Mobile IP on Sego network.

[ipUnplugged, 2005] "ipUnplugged Product Brief" available online at http://www.ipunplugged.com/pdf/ProductSheet43_Letter_G.pdf.
This article describes an overview of Mobile IP and the configuration of Mobile IP on Unplugged network.

[Microsoft, 2004] "The Cable Guy □ September 2004: Introduction to Mobile IPv6," available online at http://www.microsoft.com/technet/community/columns/cableguy/cg0904.mspx.
This article describes an overview of Mobile IP and Mobile IP implementation in Microsoft Windows.

Back to Table of Contents

List of Acronyms

MA	Mobility Agent
HA	Home Agent
FA	Foreign Agent
GFA	Gateway Foreign Agent
LSR	Label Switch Router
COA	Care-of-Address
FCOA	Foreign agent-based Care-of-Address
CCOA	Colocated Care-of-Address
MN	Mobile Node
CN	Correspondent Node
HN	Home Network
FN	Foreign Network
ARP	Address resolution protocol
SPI	Security Parameters Index
VOIP	Voice over Internet Protocol
HMAC	Keyed-hash message authentication code
MD5	Message-Digest algorithm 5
SHA1	Secure Hash Algorithm 1
IP	Internet Protocol
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
QOS	Quality of Service
IGMP	Internet Group Management Protocol
ICMP	Internet Control Message Protocol
IRDP	Internet Router Discovery Protocol
Mobile IP	Mobile Internet Protocol
Mobile IPv4	Mobile Internet Protocol version 4
Mobile IPv6	Mobile Internet Protocol version 6
TTL	Time to Live
RTT	Round Trip Time
GRE	Generic routing encapsulation
DHCP	Dynamic Host Configuration Protocol
DVMRP	Distance Vector Multicast Routing Protocol
MOSPF	Multicast Open Shortest Part First
CBT	Core Based Trees
PIM	Protocol Independent Multicast
IPSec	Internet Protocol Security
MOS	Mean Opinion Score

SIP	Session Initiation Protocol
LU	Location Update
LAN	Local Area Network
IETF	Internet Engineering Task Force
IEEE	Institute of Electrical and Electronics Engineers
ESP	Encapsulating Security Payload
AH	Authentication Header
IKE	Internet Key Exchange
RFC	Request for Comments
RSA	Rivest, Shamir, and Adleman

Back to Table of Contents

Last Modified: April 20, 2006.

Note: This paper is available on-line at http://www.cse.wustl.edu/~jain/cse574-06/mobileIP/index.html.