Handbook of Wireless Networks and Mobile Computing, Edited by Ivan Stojmenović

ISBNs: 0-471-41902-8 (Paper); 0-471-22456-1 (Electronic)

CHAPTER 25

Mobile IP Protocols

CHRISTOS DOULIGERIS and THANOS VASILAKOS
Institute of Computer Science, FORTH, Heraklion, Crete, Greece

25.1 INTRODUCTION

The Internet currently offers access to a variety of information worldwide in an efficient and, through the use of web technologies, user-friendly manner. It is based on the Transport Control/Internet Protocol (TCP/IP) protocol stack [6] which has been developed with data communications and fixed access location points in mind. The wide use of wireless technologies for voice communications and the proliferation of handheld and other devices that can provide access to the Internet call for a new paradigm for connecting mobile users to the Internet. Such an endeavor needs to take into account the existing Internet protocols, compatibility issues, and the requirements of mobile users.

Mobile IP, as proposed by the Internet Engineering Task Force (IETF) in RFC 2002 [1] and subsequent RFCs [2], provides an efficient, scalable mechanism for node mobility within the Internet. Nodes may move and change their point of attachment to the Internet without changing their IP address. This allows them to maintain transport and higher-layer connections while moving. Node mobility is realized without the need to propagate host-specific routes throughout the Internet routing fabric. The mobile node uses two IP addresses: a fixed home address and a care-of address that changes at each new point of attachment.

Mobile IP is intended to solve node mobility issues over the IP layer. It is just as suitable for mobility across homogeneous media as it is for mobility across heterogeneous media. Mobile IP facilitates node movement from one Ethernet segment to another as well as handling node movement from an Ethernet segment to a wireless local area network (LAN).

One can think of mobile IP as solving the "macro" mobility management problem. It is less well suited for more "micro" mobility management applications, for example, handoff amongst wireless transceivers, each of which covers only a very small geographic area. In this situation, link layer mechanisms for link maintenance (i.e., link layer handoff) might offer faster convergence and fewer overheads than mobile IP.

Finally, it is noted that mobile nodes are assigned (home) IP addresses largely the same way in which stationary hosts are assigned long-term IP addresses; namely, by the authority that owns them. Properly applied, mobile IP allows mobile nodes to communicate using only their home address, regardless of their current location. Mobile IP, therefore,

makes no attempt to solve the problems related to local or global addressing (IP address, renumbering etc).

In brief, mobile IP routing works as follows. Packets destined to a mobile node are routed first to their home network—a network identified by the network prefix of the mobile node's (permanent) home address. At the home network, the mobile node's home agent intercepts such packets and tunnels them to the mobile node's most recently reported care-of address. At the endpoint of the tunnel, the inner packets are decapsulated and delivered to the mobile node. In the reverse direction, packets sourced by mobile nodes are routed to their destination using standard IP routing mechanisms.

The mobile IP protocol defines the following:

- An authenticated registration procedure by which a mobile node informs its home agent(s) of its care-of address(es).
- An extension to Internet Control Message Protocol (ICMP) Router Discovery [9], which allows mobile nodes to discover prospective home agents and foreign agents.
- The rules for routing packets to and from mobile nodes, including the specification of one mandatory tunneling mechanism [4] and several optional tunneling mechanisms [7, 2].

This chapter will present the mobile IP standard as well as current efforts within the IETF to provide connectivity in the future wireless world. In the next section, an introduction to the requirements and constraints imposed by IP in a mobile environment are presented, as well as necessary functions a mobile protocol should perform and principles it should adhere to. Section 25.3 presents in detail the mobile IP protocol as defined in RFC2002 and its revisions. The following sections present issues that the mobile IP community faces regarding route optimization, transferring to an Ipv6 environment, organization of databases, and security.

25.2 MOBILITY REQUIREMENTS AND CONSTRAINTS IN AN IP ENVIRONMENT

IP Version 4, which is the current, most implemented version of IP, assumes that a node's IP address uniquely identifies the node's point of attachment to the Internet. A node must be located on the network indicated by its IP address in order to receive datagrams destined for it; otherwise, datagrams destined to the node would be undeliverable. If a node changes its point of attachment, in order not to lose its ability to communicate, one of the two following mechanisms must typically be employed:

1. The node must change its IP address whenever it changes its point of attachment.
2. Host-specific routes must be propagated throughout much of the Internet.

The first alternative makes it impossible for a node to maintain transport and higher-layer connections when the node changes location. The second does not scale very well.

A mobile node must be able to communicate with other nodes after changing its link layer point of attachment to the Internet, yet without changing its IP address. A mobile node must be able to communicate with other nodes that do not implement these mobility functions. No protocol enhancements are required in hosts or architectural entities. All messages used to update another node as to the location of a mobile node must be authenticated in order to protect against remote redirection attacks.

Wireless links have substantially lower bandwidth and higher error rates than traditional wired networks. Minimizing power consumption is important for battery powered mobile nodes. Therefore, signaling and processing should be minimized. Integration of mobility with IP should also place no additional constraints on the assignment of IP addresses. The companies or organizations that own the mobile nodes should assign IP addresses.

25.3 MOBILE IP PROTOCOL OVERVIEW

25.3.1 Mobile IP New Architectural Entities

Mobile IP introduces three new functional entities:

1. *Mobile Node.* A host or router that changes its point of attachment from one network or subnetwork to another. A mobile node may change its location without changing its IP address; it may continue to communicate with other Internet nodes at any location using its (constant) IP address, assuming link layer connectivity to a point of attachment is available.
2. *Home Agent.* A router on a mobile node's home network that tunnels datagrams for delivery to the mobile node when it is away from home, and maintains current location information for the mobile node.
3. *Foreign Agent.* A router on a mobile node's visited network that provides routing services to the mobile node while registered. The foreign agent detunnels and delivers datagrams to the mobile node that were tunneled by the mobile node's home agent. For datagrams sent by a mobile node, the foreign agent may serve as a default router for registered mobile nodes.

A mobile node is given a long-term IP address on a home network. This home address is administered in the same way that a "permanent" IP address is provided to a stationary host. When away from its home network, a "care-of address" is associated with the mobile node that reflects the mobile node's current point of attachment. The mobile node uses its home address as the source address of all IP datagrams that it sends and for datagrams sent for certain mobility management functions.

The following terminology is used in the mobile IP documents.

Agent Advertisement. An advertisement message constructed by attaching a special Extension to a router advertisement message.

Care-of Address. The termination point of a tunnel toward a mobile node, for datagrams forwarded to the mobile node while it is away from home. The protocol can use two different types of care-of addresses: a "foreign agent care-of address" is an address of a foreign agent with which the mobile node is registered, and a "colocated care-of address" is an externally obtained local address that the mobile node has associated with one of its own network interfaces.

Correspondent Node. A peer with which a mobile node is communicating. A correspondent node may be either mobile or stationary.

Foreign Network. Any network other than the mobile node's home network.

Home Address. An IP address that is assigned for an extended period of time to a mobile node. It remains unchanged regardless of where the node is attached to the Internet.

Home Network. A network, possibly virtual, having a network prefix matching that of a mobile node's home address. Note that standard IP routing mechanisms will deliver datagrams destined to a mobile node's home address to the mobile node's home network.

Link Layer Address. The address used to identify an endpoint of some communication over a physical link. A facility or medium over which nodes can communicate at the link layer.

Link. Typically, the link layer address is an interface's media access control (MAC) address.

Mobility Agent. Either a home agent or a foreign agent.

Mobility Binding. The association of a home address with a care-of address, along with the remaining lifetime of that association.

Mobility Security Association. A collection of security contexts between a pair of nodes that may be applied to mobile IP protocol messages exchanged between them. Each context indicates an authentication algorithm and mode, a secret (a shared key or appropriate public/private key pair), and the style of replay protection in use.

Node. A host or a router.

Nonce. A randomly chosen value, different from previous choices, inserted in a message to protect against replays.

Security Parameter Index (SPI). An index identifying a security context between a pair of nodes among the contexts available in the Mobility Security Association. SPI values 0 through 255 are reserved and must not be used in any Mobility Security Association function.

Tunnel. The path followed by a datagram while it is encapsulated. It is routed to a knowledgeable decapsulating agent, which decapsulates the datagram and then correctly delivers it to its ultimate destination.

Virtual Network. A network with no physical instantiation beyond a router (with a physical network interface on another network). The router (e.g., a home agent) generally advertises reachability to the virtual network using conventional routing protocols.

Visited Network. A network other than a mobile node's home network, to which the mobile node is currently connected.

Visitor List. The list of mobile nodes visiting a foreign agent.

25.3.2 Operation of Mobile IP

Mobile IP provides two basic functions: agent discovery and registration. During agent discovery, home agents and foreign agents may advertise their availability on each link for which they provide service. A newly arrived mobile node can send a solicitation on the link to learn if any prospective agents are present. When the mobile node is away from home, it registers its care-of address with its home agent during the registration phase. Depending on its method of attachment, the mobile node will register either directly with its home agent, or through a foreign agent that forwards the registration to the home agent.

The following steps provide a rough outline of operation of the mobile IP protocol [1]:

- Mobility agents (i.e., foreign agents and home agents) advertise their presence via agent advertisement messages. A mobile node may optionally solicit an agent advertisement message from any locally attached mobility agents through an agent solicitation message.
- A mobile node receives these agent advertisements and determines whether it is on its home network or a foreign network.
- When the mobile node detects that it is located on its home network, it operates without mobility services. If returning to its home network from being registered elsewhere, the mobile node deregisters with its home agent through exchange of a registration request and registration reply message with it.
- When a mobile node detects that it has moved to a foreign network, it obtains a care-of address on the foreign network.The care-of address can either be determined from a foreign agent's advertisements (a foreign agent care-of address), or by some external assignment mechanism such as the dynamic configuration protocol (DHCP) [6] (a colocated care-of address).
- The mobile node operating away from home then registers its new care-of address with its home agent through exchange of a registration request and registration reply message with it, possibly via a foreign agent.
- Datagrams sent to the mobile node's home address are intercepted by its home agent, tunneled by the home agent to the mobile node's care-of address, received at the tunnel endpoint (either at a foreign agent or at the mobile node itself), and finally delivered to the mobile node.
- In the reverse direction, datagrams sent by the mobile node are generally routing mechanisms, not necessarily passing through the home agent.

When away from home, mobile IP uses protocol tunneling to hide a mobile node's home address from intervening routers between its home network and its current location.

The tunnel terminates at the mobile node's care-of address. The care-of address must be an address to which datagrams can be delivered via conventional IP routing. At the care-of address, the original datagram is removed from the tunnel and delivered to the mobile node.

Mobile IP provides two alternative modes for the acquisition of a care-of address:

- A "foreign agent care-of address" is a care-of address provided by a foreign agent through its agent advertisement messages. In this case, the care-of address is an IP address of the foreign agent.
- A "colocated care-of address" is a care-of address acquired by the mobile node as a local IP address through some external network interfaces.

The mode of using a colocated care-of address has the advantage that it allows a mobile node to function without a foreign agent, for example, in networks that have not yet deployed a foreign agent. It does, however, place additional burden on the IPv4 address space because it requires a pool of addresses within the foreign network to be made available to visiting mobile nodes. It is difficult to efficiently maintain pools of addresses for each subnet that may permit mobile nodes to visit.

Figure 25.1 illustrates the routing of datagrams to be registered with the home agent. In the figure, the mobile node is using a foreign agent care-of address. In Step 1, a datagram to a mobile node arrives on the home network via standard IP routing. In Step 2, the datagram is intercepted by home agent and is tunneled to the care-of address. In Step 3, the datagram is detunneled and delivered to the mobile node. In Step 4, for datagrams sent by the mobile node, standard IP routing delivers each of them to its destination. Note that the foreign agent is the mobile node's default router.

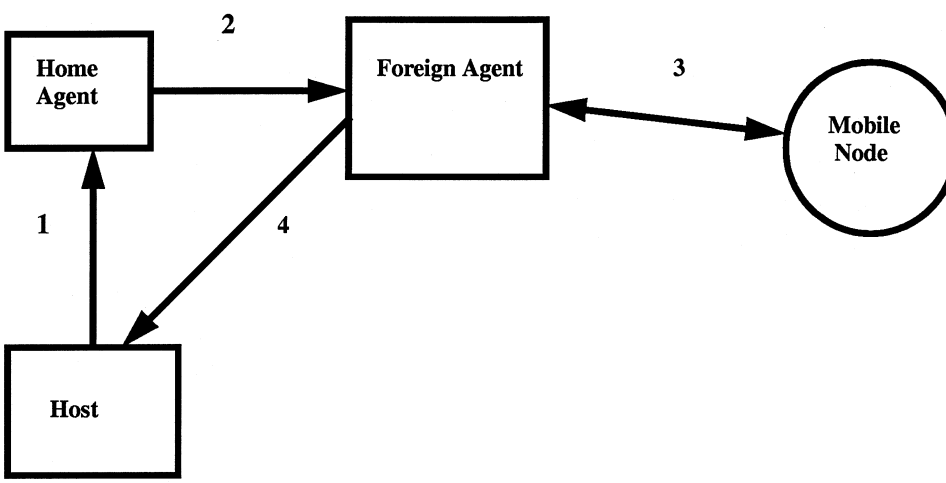


Figure 25.1 Transmission of messages in a mobile IP environment.

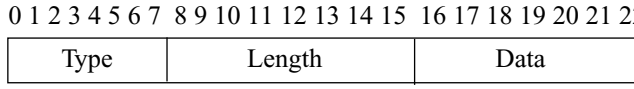
25.3.3 Message Formats

Mobile IP defines a set of new control messages, sent with the user datagram protocol (UDP) [17]. Currently, the following two message types are defined:

1. Registration request
2. Registration reply

In addition, for agent discovery, mobile IP makes use of the existing router advertisement and router solicitation messages defined for ICMP router discovery [4].

Mobile IP defines a general extension mechanism to allow optional information to be carried by mobile IP control messages or by ICMP router discovery messages. Extensions allow variable amounts of information to be carried within each datagram. Each of these extensions (with one exception) is encoded in the following type–length–value format:



Type indicates the particular type of extension.

Length indicates the length (in bytes) of the data field within this extension. The length does not include the type and length bytes.

Data indicates the particular data associated with this extension. This field may be zero or more bytes in length. The type and length fields determine the format and length of the data field.

The total length of the IP datagram indicates the end of the list of extensions.

Two separately maintained sets of numbering spaces, from which extension type values are allocated, are used in mobile IP:

The first set consists of those extensions that may appear only in mobile IP control messages. Currently, the following types are defined for extensions appearing in mobile IP control messages:

32	Mobile Home Authentication
33	Mobile Foreign Authentication
34	Foreign Home Authentication

The second set consists of those extensions that may appear only in ICMP router discovery messages [4]. Currently, mobile IP defines the following types for extensions appearing in ICMP router discovery messages:

0	One-byte Padding (encoded with no length nor data field)
16	Mobility Agent Advertisement
19	Prefix Lengths

25.3.4 Agent Discovery

Agent discovery is the method by which a mobile node determines whether it is currently connected to its home network or to a foreign network, and by which a mobile node can detect when it has moved from one network to another. When connected to a foreign network, the methods specified in this section also allow the mobile node to determine the foreign agent care-of address being offered by each foreign agent on that network.

Mobile IP extends ICMP router discovery [4] as its primary mechanism for agent discovery. Including a mobility agent advertisement extension in an ICMP router advertisement message forms an agent advertisement. An agent solicitation message is identical to an ICMP router solicitation [with IP time-to-live (TTL) set to 1]. Agent advertisement and agent solicitation may not be necessary for link layers that already provide this functionality

25.3.4.1 Agent Advertisement

To advertise its services on a link, a mobility agent transmits agent advertisements. Mobile nodes use these advertisements to determine their current point of attachment to the Internet. An agent advertisement is an ICMP router advertisement that has been extended to also carry a mobility agent and, optionally, a prefix length extension, one-byte padding extension, or other extensions that might be defined in the future.

Within an agent advertisement message, ICMP router advertisement fields of the message are required to conform to the following additional specifications:

Link Layer Fields

Destination Address. The link layer destination address of a unicast agent advertisement must be the same as the source link layer address of the agent solicitation that prompted the advertisement.

IP Fields

TTL. The TTL for all agent advertisements must be set to 1.

Destination Address. As specified for ICMP router discovery [4], the IP destination address of an agent advertisement must be either the "all systems on this link" multicast address (224.0.0.1) [5] or the "limited broadcast" address (255.255.255.255). The subnet-directed broadcast address of the form <prefix>.<-1> cannot be used since mobile nodes will not generally know the prefix of the foreign network.

ICMP Fields

Code. The Code field of the agent advertisement is interpreted as follows:

0 = The mobility agent handles common traffic, that is, it acts as a router for IP datagrams not necessarily related to mobile nodes.

16 = The mobility agent does not route common traffic. However, all foreign agents must (minimally) forward to a default router any datagrams received from a registered mobile node.

Lifetime. The maximum length of time that the advertisement is considered valid in the absence of further advertisements.

Router Address(es). Addresses that may appear in this portion of the agent advertisement.

Num Addrs. The number of router addresses advertised in this message. Note that in an agent advertisement message, the number of router addresses specified in the ICMP router advertisement portion of the message may be set to 0.

The protocol also specifies the periodicity of the transmission of these messages. A home agent must always be prepared to serve the mobile nodes for which it is the home agent. When a foreign agent wishes to require registration even from those mobile nodes that have acquired a colocated care-of address, it sets a special bit, the "R" bit, to one. An agent solicitation is identical to an ICMP router solicitation (with the IP TTL field set to 1).

Foreign Agent and Home Agent Considerations

Any mobility agent that cannot be discovered by a link layer protocol must send agent advertisements. An agent, which can be discovered by a link layer protocol, should also implement agent advertisements. However, the advertisements need not be sent, except when the site policy requires registration with the agent, or as a response to a specific agent solicitation. All mobility agents should respond to agent solicitations. If the home network is not a virtual network, then the home agent for any mobile node should be located on the link identified by the mobile node's home address, and agent advertisement messages sent by the home agent on this link must have the "H" bit set. In this way, mobile nodes on their own home network will be able to determine that they are indeed at home.

If the home network is a virtual network, mobile nodes are always treated as being away from home.

Mobile Node Considerations

Every mobile node must implement agent solicitation. Solicitations should only be sent in the absence of agent advertisements and when a care-of address has not been determined through a link-layer protocol or other means. The mobile node uses the same procedures, defaults, and constants for agent solicitation as specified for ICMP router solicitation messages [4], except that the mobile node may solicit more often than once every three seconds, and a mobile node that is currently not connected to any foreign agent may solicit more times than a specified maximum number. The mobile node must limit the rate at which a mobile node sends solicitations.

A mobile node can detect that it has returned to its home network when it receives an agent advertisement from its own home agent. If so, it should deregister with its home agent.

25.3.5 Registration

Mobile IP registration provides a flexible mechanism for mobile nodes to communicate their current reachability information to their home agent. It is the method by which mobile nodes request forwarding services when visiting a foreign network, inform their home

agent of their current care-of address, renew a registration that is due to expire, and/or deregister when they return home.

Registration messages exchange information between a mobile node (optionally), a foreign agent, and the home agent. Registration creates or modifies a mobility binding at the home agent, associating the mobile node's home address with its care-of address for the specified lifetime.

Several other (optional) capabilities are available through the registration procedure; these enable a mobile node to: maintain multiple simultaneous registrations, deregister specific care-of addresses while retaining other mobility bindings, and discover the address of a home agent if the mobile node is not configured with this information.

25.3.5.1 Registration Overview

Mobile IP defines two different registration procedures, one via a foreign agent that relays the registration to the mobile node's home agent, and one directly with the mobile node's home agent. The following rules determine which of these two registration procedures to use in any particular circumstance.

- If a mobile node is registering a foreign agent care-of address, the mobile node must register via that foreign agent.
- If a mobile node is using a colocated care-of address, and receives an agent advertisement from a foreign agent on the link on which it is using this care-of address, the mobile node should register via that foreign agent (or via another foreign agent on this link) if the "R" bit is set in the received agent advertisement message.
- If a mobile node is otherwise using a colocated care-of address, the mobile node must register directly with its home agent.
- If a mobile node has returned to its home network and is (de)registering with its home agent, the mobile node must register directly with its home agent.

Both registration procedures involve the exchange of registration request and registration reply messages. When registering via a foreign agent, the registration procedure requires the following four messages:

- The mobile node sends a registration request to the prospective foreign agent to begin the registration process.
- The foreign agent processes the registration request and then relays it to the home agent.
- The home agent sends a registration reply to the foreign agent to grant or deny the request.
- The foreign agent processes the registration reply and then relays it to the mobile node.

When the mobile node instead registers directly with its home agent, the registration procedure requires only the following two messages:

- The mobile node sends a registration request to the home agent.
- The home agent sends a registration reply to the mobile node, granting or denying the request.

25.3.5.2 Authentication

Each mobile node, foreign agent, and home agent must be able to support a mobility security association for mobile entities, indexed by their SPI and IP address. Registration messages between a mobile node and its home agent must be authenticated with the mobile home authentication extension. This extension immediately follows all nonauthentication extensions, except those foreign agent-specific extensions that may be added to the message after the mobile node computes the authentication.

25.3.5.3 Registration Request

A mobile node registers with its home agent using a registration request message so that its home agent can create or modify a mobility binding for that mobile node (e.g., with a new lifetime). The request may be relayed to the home agent by the foreign agent through which the mobile node is registering, or it may be sent directly to the home agent in the case in which the mobile node is registering a colocated care-of address.

25.3.5.4 Registration Reply

A mobility agent returns a registration reply message to a mobile node that has sent a registration request message. If the mobile node is requesting a service from a foreign agent, that foreign agent will receive the reply from the home agent and subsequently relay it to the mobile node. The reply message 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.

25.3.5.5 Mobile Node Considerations

A mobile node must be configured with its home address, a netmask, and a mobility security association for each home agent. In addition, a mobile node may be configured with the IP address of one or more of its home agents; otherwise, the mobile node may discover a home agent using specific procedures.

For each pending registration, the mobile node maintains the following information:

- The link layer address of the foreign agent to which the registration request was sent, if applicable
- The IP destination address of the registration request
- The care-of address used in the registration
- The identification value sent in the registration
- The originally requested lifetime
- The remaining lifetime of the pending registration

25.3.5.6 Foreign Agent Considerations

The foreign agent plays a mostly passive role in mobile IP registration. It relays registration requests between mobile nodes and home agents, and, when it provides the care-of address, decapsulates datagrams for delivery to the mobile node. It should also send periodic agent advertisement messages to advertise its presence, if not detectable by link layer means.

A foreign agent must not transmit a registration request except when relaying a registration request received from a mobile node to the mobile node's home agent. A foreign agent must not transmit a registration reply except when relaying a registration reply received from a mobile node's home agent, or when replying to a registration request received from a mobile node in the case in which the foreign agent is denying service to the mobile node. In particular, a foreign agent must not generate a registration request or reply because a mobile node's registration lifetime has expired. A foreign agent also must not originate a registration request message that asks for deregistration of a mobile node; however, it must relay valid (de)registration requests originated by a mobile node.

Each foreign agent must be configured with a care-of address. In addition, for each pending or current registration, the foreign agent must maintain a visitor list entry containing the following information obtained from the mobile node's registration request:

- The link layer source address of the mobile node
- The IP source address (the mobile node's home address)
- The IP destination address
- The UDP source port
- The home agent address
- The identification field
- The requested registration lifetime
- The remaining lifetime of the pending or current registration

25.3.5.7 Home Agent Considerations

Home agents play a reactive role in the registration process. The home agent receives registration requests from the mobile node (perhaps relayed by a foreign agent), updates its record of the mobility bindings for this mobile node, and issues a suitable registration reply in response to each.

A home agent must not transmit a registration reply except when replying to a registration request received from a mobile node. In particular, the home agent must not generate a registration reply to indicate that the lifetime has expired.

25.3.6 Routing Considerations

This section describes how mobile nodes, home agents, and (possibly) foreign agents cooperate to route datagrams to/from mobile nodes that are connected to a foreign network. The mobile node informs its home agent of its current location using the registration procedure described in the previous sections. Home agents and foreign agents must

support tunneling datagrams using IP in IP encapsulation [14]. Any mobile node that uses a colocated care-of address must support receiving datagrams tunneled using IP in IP encapsulation. Minimal encapsulation [15] and GRE encapsulation [8] are alternate encapsulation methods that may optionally be supported by mobility agents and mobile nodes.

The protocol specifies unicast, broadcast, and multicast datagram routing. In this chapter, we focus on the procedures for unicast datagram routing.

25.3.6.1 Unicast Datagram Routing

Mobile Node Considerations

When connected to its home network, a mobile node operates without the support of mobility services. That is, it operates in the same way as any other (fixed) host or router. The method by which a mobile node selects a default router when connected to its home network, or when away from home and using a colocated care-of address, is outside the scope of this document. ICMP router advertisement [4] is one such method.

When registered on a foreign network, the mobile node chooses a default router by the following rules.

1. If the mobile node is registered using a foreign agent care-of address, then the mobile node must choose its default router from among the router addresses advertised in the ICMP router advertisement portion of that agent advertisement message. The mobile node may also consider the IP source address of the agent advertisement as another possible choice for the IP address of a default router, along with the (possibly empty) list of router addresses from the ICMP router advertisement portion of the message. In such cases, the IP source address must be considered to be the worst choice (lowest preference) for a default router.
2. If the mobile node is registered directly with its home agent using a colocated care-of address, then the mobile node should choose its default router from among those advertised in any ICMP router advertisement message that it receives for which its externally obtained care-of address and the router address match under the network prefix. If the mobile node's externally obtained care-of address matches the IP source address of the agent advertisement under the network prefix, the mobile node may also consider that IP source address as another possible choice for the IP address of a default router, along with the (possibly empty) list of router addresses from the ICMP router advertisement portion of the message. If so, the IP source address must be considered to be the worst choice (lowest preference) for a default router. The network prefix may be obtained from the prefix lengths extension in the router advertisement, if present. The prefix may also be obtained through other mechanisms beyond the scope of this document.

Foreign Agent Considerations

Upon receipt of an encapsulated datagram sent to its advertised care-of address, a foreign agent must compare the inner destination address to those entries in its visitor list. When the destination does not match the address of any mobile node currently in the visitor list,

the foreign agent must not forward the datagram without modifications to the original IP header, because otherwise a routing loop is likely to result. The datagram should be silently discarded. ICMP destination unreachable must not be sent when a foreign agent is unable to forward an incoming tunneled datagram. Otherwise, the foreign agent forwards the decapsulated datagram to the mobile node.

The foreign agent must not advertise to other routers in its routing domain, nor to any other mobile node, the presence of a mobile router.

The foreign agent must route datagrams it receives from registered mobile nodes. At a minimum, this means that the foreign agent must verify the IP header checksum, decrement the IP time to live, recompute the IP header checksum, and forward such datagrams to a default router. In addition, the foreign agent should send an appropriate ICMP redirect message to the mobile node.

Home Agent Considerations

The home agent must be able to intercept any datagrams on the home network addressed to the mobile node while the mobile node is registered away from home. Proxy and gratuitous ARP may be used in enabling this interception.

The home agent must examine the IP destination address of all arriving datagrams to see if it is equal to the home address of any of its mobile nodes registered away from home. If so, the home agent tunnels the datagram to the mobile node's currently registered care-of address capability of multiple simultaneous mobility bindings, it tunnels a copy to each care-of address in the mobile node's mobility binding list. If the mobile node has no current mobility bindings, the home agent must not attempt to intercept datagrams destined for the mobile node, and thus will not in general receive such datagrams. However, if the home agent is also a router handling common IP traffic, it is possible that it will receive such datagrams for forwarding onto the home network. In this case, the home agent must assume that the mobile node is at home and simply forward the datagram directly onto the home network.

If the lifetime for a given mobility binding expires before the home agent has received another valid registration request for that mobile node, then that binding is deleted from the mobility binding list. The home agent must not send any registration reply message simply because the mobile node's binding has expired. The entry in the visitor list of the mobile node's current foreign agent will expire naturally, probably at the same time as the binding expired at the home agent. When a mobility binding's lifetime expires, the home agent must delete the binding, but it must retain any other (non-expired) simultaneous mobility bindings that it holds for the mobile node.

When a home agent receives a datagram, intercepted for one of its mobile nodes registered away from home, the home agent must examine the datagram to check if it is already encapsulated. If so, the following special rules apply in the forwarding of that datagram to the mobile node. If the inner (encapsulated) destination address is the same as the outer destination address (the mobile node), then the home agent must also examine the outer source address of the encapsulated datagram (the source address of the tunnel). If current care-of address is the same as the mobile node's, the home agent must silently discard that datagram in order to prevent a likely routing loop. If, instead, the outer source address is not the same as the mobile node's current care-of address, then the home agent should for-

ward the datagram to the mobile node. In order to forward the datagram in this case, the home agent may simply alter the outer destination address to the care-of address, rather than reencapsulating the datagram. Otherwise (the inner destination address is not the same as the outer destination address), the home agent should encapsulate the datagram again (nested encapsulation), with the new outer destination address set equal to the mobile node's care-of address.

25.3.7 Security Considerations

The mobile computing environment is potentially very different from the ordinary computing environment. In many cases, mobile computers will be connected to the network via wireless links. Such links are particularly vulnerable to passive eavesdropping, active replay attacks, and other active attacks.

25.3.7.1 Message Authentication Codes

Home agents and mobile nodes must be able to perform authentication. The default algorithm is keyed MD5 [21], with a key size of 128 bits. The default mode of operation is to both precede and follow by the 128-bit key the data to be hashed; that is, MD5 is to be used in "prefix + suffix" mode. The foreign agent must also support authentication using keyed MD5 and key sizes of 128 bits or greater, with manual key distribution. More authentication algorithms, algorithm modes, key distribution methods, and key sizes may also be supported.

25.3.7.2 Areas of Security Concern in this Protocol

The registration protocol described in RFC 2002 will result in a mobile node's traffic being tunneled to its care-of address. This tunneling feature could be a significant vulnerability if the registration were not authenticated. Such remote unauthenticated redirection, for instance, as performed by the mobile registration protocol, is widely understood to be a security problem in the current Internet [2]. The use of "gratuitous ARP" brings with it all of the risks associated with the use of ARP. Since it is not authenticated, it can potentially be used to steal another host's traffic.

25.3.7.3 Key Management

This specification requires a strong authentication mechanism (keyed MD5) which precludes many potential attacks based on the mobile IP registration protocol. However, because key distribution is difficult in the absence of a network key management protocol, messages with the foreign agent are not all required to be authenticated. In a commercial environment, it might be important to authenticate all messages between the foreign agent and the home agent, so that billing is possible, and service providers do not provide service to users that are not legitimate customers of that service provider.

25.3.7.4 Replay Protection for Registration Requests

The identification field is used to let the home agent verify that the mobile node, not replayed by an attacker from some previous registration, has freshly generated a registration message. Two methods are described in this section: time stamps (mandatory) and

"nonces" (optional). All mobile nodes and home agents must implement time-stamp-based replay protection. These nodes may also implement nonce-based replay protection.

The style of replay protection in effect between a mobile node and its home agent is part of the mobile security association. A mobile node and its home agent must agree on which method of replay protection will be used. The interpretation of the identification field depends on the method of replay protection as described in the subsequent subsections.

Whatever method is used, the low-order 32 bits of the identification must be copied unchanged from the registration request to the reply. The foreign agent uses those bits (and the mobile node's home address) to match registration requests with corresponding replies. The mobile node must verify that the low-order 32 bits of any registration reply are identical to the bits it sent in the registration request.

The identification in a new registration request must not be the same as that in an immediately preceding request, and should not repeat while the same security context is being used between the mobile node and the home agent.

25.4 ROUTE OPTIMIZATION

The base mobile IP protocol [12], allows any mobile node to move about, changing its point of attachment to the Internet, while continuing to be identified by its home IP address. Correspondent nodes send IP datagrams to a mobile node at its home address in the same way as with any other destination. This scheme allows transparent interoperation between mobile nodes and their correspondent nodes, but forces all datagrams for a mobile node to be routed through its home agent, usually through very long and inefficient routes, placing a heavy burden on the network.

Route optimization extensions to the mobile IP protocol [16] provide a means for nodes to cache the binding of a mobile node and to then tunnel their own datagrams directly to the mobile node's home agent. Extensions are also provided to allow datagrams in flight when a mobile node moves, and datagrams sent based on an out-of-date cached binding, to be forwarded directly to the mobile node's new binding.

All operations of route optimization change the routing of IP datagrams to the type of mechanisms defined in the base mobile IP protocol. This authentication generally relies on a mobility security association established in advance between the sender and receiver of such messages. The association can be created using ISAKMP [7], or any of the registration key establishment methods specified in [11].

25.4.1 Route Optimization Overview

Route optimization can be seen to have two different parts:

1. Updating binding caches (a cache of mobility bindings of mobile nodes, maintained by a node for use in tunneling datagrams to those mobile nodes)
2. Managing smooth handoffs between foreign agents

25.4.1.1 Binding Caches

Route optimization provides a means for any node to maintain a binding cache containing the care-of address of one or more mobile nodes. When sending an IP datagram to a mobile node, if the sender has a binding cache entry for the destination mobile node, it may tunnel the datagram directly to the care-of address indicated in the cached mobility binding.

In the absence of any binding cache entry, datagrams destined for a mobile node will be routed to the mobile node's home network in the same way as any other IP datagram, and then tunneled to the mobile node's current care-of address by the mobile node's home agent. This is the only routing mechanism supported by the base mobile IP protocol. With route optimization, as a side effect of this indirect routing of a datagram to a mobile node, the original sender of the datagram may be informed of the mobile node's current mobility binding, giving the sender an opportunity to cache the binding.

Any node may maintain a binding cache to optimize its own communication with mobile nodes. A node may create or update a binding cache entry for a mobile node only when it has received and authenticated the mobile node's mobility binding. As before, each binding in the binding cache also has an associated lifetime, specified in the binding update message in which the node obtained the binding. After the expiration of this time period, the binding is deleted from the cache. In addition, a node cache may use any reasonable strategy for managing the space within the binding cache. When a new entry needs to be added to the binding cache, the node may choose to drop any entry already in the cache, if needed, to make space for the new entry. For example, a least recently used (LRU) strategy for cache entry replacement is likely to work well.

When sending an IP datagram, if the sending node has a binding cache entry for the destination node, it should tunnel the datagram to the mobile node's care-of address using the encapsulation techniques used by home agents, described in [9, 10, 4].

25.4.1.2 Foreign Agent Smooth Handoff

When a mobile node moves and registers with a new foreign agent, the base mobile IP protocol does not notify the mobile node's previous foreign agent. IP datagrams intercepted by the home agent after the new registration are tunneled to the mobile node's new care-of address, but datagrams in flight that had already been intercepted by the home agent and tunneled to the old care-of address when the mobile node moved are likely to be lost and are assumed to be retransmitted by higher-level protocols if needed. The old foreign agent eventually deletes its visitor list entry for the mobile node after the expiration of the registration lifetime.

Route optimization provides a means for the mobile node's previous foreign agent to be reliably notified of the mobile node's new mobility binding, allowing datagrams in flight to the mobile node's previous foreign agent to be forwarded to its new care-of address. This notification also allows any datagrams tunneled to the mobile node's previous foreign agent, from correspondent nodes with out-of-date binding cache entries for the mobile node, to be forwarded to its new care-of address. Finally, this notification allows any resources consumed by the mobile node at the previous foreign agent (such as radio channel reservations) to be released immediately, rather than waiting for its registration lifetime to expire.

25.5 MOBILITY SUPPORT FOR IPv6

IPv6 includes many features for streamlining mobility support that are missing in IP Version 4 (current version), including stateless address autoconfiguration [14] and neighbor discovery [15]. IPv6 [5] also attempts to drastically simplify the process of renumbering, which could be critical to the future routability of the Internet.

The design of mobile IP support in IPv6 (Mobile IPv6) represents a natural combination of the experiences gained from the development of mobile IP support in IPv4 (Mobile IPv4) [19, 18, 20], together with the opportunities provided by the design and deployment of a new version of IP itself (IPv6) and the new protocol features offered by IPv6. Mobile IPv6 thus shares many features with Mobile IPv4, but the protocol is now fully integrated into IP and provides many improvements over Mobile IPv4. This section summarizes the major differences between Mobile IPv4 and Mobile IPv6 [3]:

- Support for what is known in Mobile IPv4 as "route optimization" [21] is now built in as a fundamental part of the protocol, rather than being added on as an optional set of extensions that may not be supported by all nodes as in Mobile IPv4.
- Support is also integrated into Mobile Ipv—and into IPv6 itself—for allowing mobile nodes and mobile IP to coexist efficiently with routers that perform "ingress filtering" [7]. A mobile node now uses its care-of address as the source address in the IP header of packets it sends, allowing the packets to pass normally through ingress filtering routers. The ability to correctly process a home address option in a received packet is required in all IPv6 nodes, whether mobile or stationary, host or router.
- The use of the care-of address as the source address in each packet's IP header also simplifies routing of multicast packets sent by a mobile node. With Mobile IPv4, the mobile node had to tunnel multicast packets to its home agent in order to transparently use its home address as the source of the multicast packets. With Mobile IPv6, the use of the home address option allows the home address to be used but still be compatible with multicast routing that is based in part on the packet's source address.
- There is no longer any need to deploy special routers as "foreign agents," as in Mobile IPv4. In Mobile IPv6, mobile nodes make use of IPv6 features, such as neighbor discovery [17] and address autoconfiguration [27], to operate in any location away from home without any special support required from its local router.
- Unlike Mobile IPv4, Mobile IPv6 utilizes IP Security (IPsec) [11, 12, 13] for all security requirements (sender authentication, data integrity protection, and replay protection) for binding updates (which serve the role of both registration and route optimization in Mobile IPv4). Mobile IPv4 relies on its own security mechanisms for these functions, based on statically configured "mobility security associations."
- The movement detection mechanism in Mobile IPv6 provides bidirectional confirmation of a mobile node's ability to communicate with its default router in its current location (packets that the router sends are reaching the mobile node, and packets that the mobile node sends are reaching the router).
- Most packets sent to a mobile node while away from home in Mobile IPv6 are sent using an IPv6 routing header rather than IP encapsulation, whereas Mobile IPv4 must use encapsulation for all packets.

- While a mobile node is away from home, its home agent intercepts any packets for the mobile node that arrive at the home network, using IPv6 neighbor discovery [17] rather than ARP [23], as in Mobile IPv4. The use of neighbor discovery improves the robustness of the protocol.
- The dynamic home agent address discovery mechanism in Mobile IPv6 uses IPv6 anycast [10] and returns a single reply to the mobile node, rather than the corresponding Mobile IPv4 mechanism that used IPv4 directed broadcast and returned a separate reply from each home agent on the mobile node's home link. The Mobile IPv6 mechanism is more efficient and more reliable, since only one packet need be sent back to the mobile node. The mobile node is less likely to lose one of the replies because no "implosion" of replies is required by the protocol.
- Mobile IPv6 defines an advertisement interval option on router advertisements (equivalent to agent advertisements in Mobile IPv4), allowing a mobile node to decide for itself how many router advertisements (agent advertisements) it is willing to miss before declaring its current router unreachable.
- The use of IPv6 destination options allows all Mobile IPv6 control traffic to be piggybacked on any existing IPv6 packets, whereas in Mobile IPv4 and its route optimization extensions, separate UDP packets were required for each control message.

25.6 CONNECTIVITY WITH 3G NETWORKS

Mobile IP requires link layer connectivity between the mobile node and the foreign agent. If another wireless network is used, then [30] proposes a protocol for achieving this. In particular, this protocol applies to CDMA2000 networks in which the physical layer terminates at a radio network node (RNN) and the FA resides inside a separate packet data serving node (PDSN). The PDSN is responsible for establishing, maintaining, and terminating the link layer to the mobile node. A RNN is responsible for relaying the link layer protocol between a mobile node and its corresponding PDSN.

The interface between the RNN and the PDSN is called the RP interface. This interface requires mobility management for handling handoff from one RNN to another without interrupting end-to-end communication. It also requires the support of the link layer protocol encapsulation.

The messages used for mobility management across the RP interface include registration request, registration reply, registration update, and registration acknowledge. Both registration request and registration update messages must be sent with UDP using the well-known port number 699.

The high-level architecture of a third generation CDMA2000 network RP interface is shown in Figure 25.2. In the figure, the PDSN will be responsible for establishing, maintaining, and terminating the link layer to the mobile node. It initiates the authentication, authorization, and accounting for the mobile node and optionally, securely tunnels to the home agent.

The RNN is responsible for mapping the mobile node identifier reference to a unique link layer identifier used to communicate with the PDSN. RNN validates the mobile station for access service and manages the physical layer connection to the mobile node.

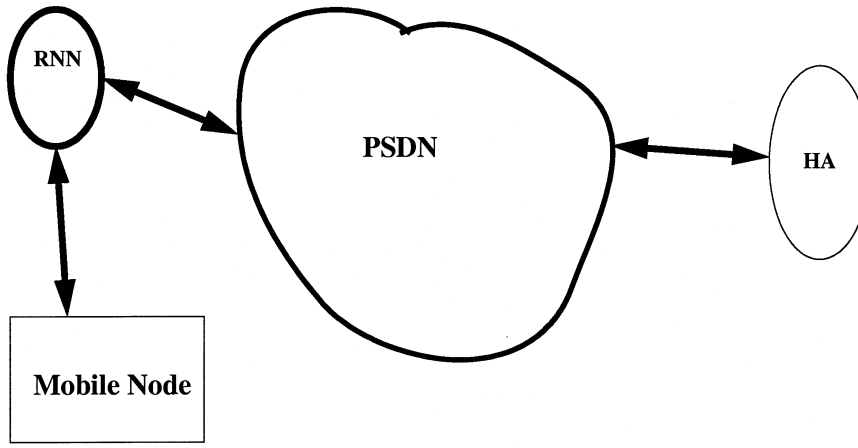


Figure 25.2 The third generation cdma200 network RP interface.

The extensions to mobile IP include enabling general routing encapsulation (GRE) and reverse tunneling during registration. A new extension called session-specific extension is defined and is mandatory in the registration acknowledge messages. The home address field must be set to zero in the registration request, registration reply, and registration update, and registration acknowledge messages.

Two new messages (registration update and registration acknowledge) are defined to support the RP session disconnection in order to speed up resource reclamation.

25.6.1 GRE Encapsulation

GRE encapsulation, as described in [8], is supported during user data transmission. A new protocol type might be required to support the link layer protocol defined for the third generation CDMA2000 network. The key field is required, and its value is the same as the one from the session-specific extension as described above. The sequence number may be required, depending on the requirement of the protocol encapsulated within the GRE frame.

During traffic tunneling, the sender inserts the key value from the registration request message into the key field of the GRE header. The receiver uses the key value from the GRE header to decide where to forward the user data.

25.6.2 Security Considerations

The protocol presented in [30] is designed for use over a protected, private network between RNN and PDSN. Prearranged security associations in the style of Mobile IPv4 are

assumed to exist among every (RNN, PDSN) pair that will form an RP connection. Also, it is assumed that the session-specific information is authenticated by means outside the scope of this draft.

Several potential vulnerabilities exist if these assumptions are not met. First, if the network connecting the RNN and PDSN is accessible to an attacker, user traffic may be intercepted and/or spoofed if there are no other end-to-end security mechanisms in place. Second, the mobile IP control messages must be authenticated to prevent tunnel set-up and tear-down by unauthorized parties. Mobile IP authentication extensions are used to provide this additional protection for control messages. Finally, if session-specific information is not authenticated, a denial-of-service attack is possible if a RNN unknowingly sends a registration request to the PDSN with a spoofed session-specific extension. The PDSN would then send an explicit tunnel tear-down to the previous RNN, causing user traffic to be misdirected to the new RNN. This would cause a loss of service and possibly interception of traffic, depending on what other security measures are in place.

25.7 MANAGEMENT OF INFORMATION BASES

The required objects for the management information base (MIB) for use with network management protocols in TCP/IP-based internets is proposed in RFC 2006 [25]. In particular, it describes managed objects used for managing the mobile node, foreign agent, and home agent of the mobile IP protocol.

The Internet standard network management framework (SNMP) presently consists of three major components. The SMI, described in RFC 1902 [26], presents the mechanisms used for describing and naming objects for the purpose of management. The MIB-II, STD 17, RFC 1213 [28] gives the core set of managed objects for the Internet suite of protocols. The protocols RFC 1157 [22] and/or RFC 1905 [24], describe the way to access managed objects. The framework permits new objects to be defined for the purpose of experimentation and evaluation.

25.7.1 Objects

Managed objects are accessed via a virtual information store, termed the management information base or MIB. Objects in the MIB are defined using the subset of Abstract Syntax Notation One (ASN.1) defined in the SMI. In particular, an object identifier, an administratively assigned name, names each object type. The object type together with an object instance serves to uniquely identify a specific instantiation of the object. For human convenience, we often use a textual string, termed the descriptor, to refer to the object type.

To be consistent with the Internet Advisory Board (IAB) directives and good engineering practice, some criteria have been applied to select managed objects for the mobile IP protocol:

- Partition management functionality among the mobile node, home agent, and foreign agent according to the partitioning seen in the mobile IP protocol.
- Require that objects be essential for either fault or configuration management.
- Exclude objects that are simply derivable from others in this or other MIBs.

RFC 2006 [25] specifies the objects used in managing these entities, namely, the mobile node, the home agent, and the foreign agent.

Objects in this MIB are arranged into groups. Each group is organized as a set of related objects. The overall structure and the relationship between groups and the mobile IP entities are shown below:

Groups	Mobile node	Foreign agent	Home agent
mipSystemGroup	X	X	X
mipSecAssociationGroup	X	X	X
mipSecViolationGroup	X	X	X
mnSystemGroup	X		
mnDiscoveryGroup	X		
mnRegistrationGroup	X		
maAdvertisementGroup		X	X
faSystemGroup		X	
faAdvertisementGroup		X	
faRegistrationGroup		X	
haRegistrationGroup			X
haRegNodeCountersGroup			X

25.8 CONCLUSIONS

Wireless communications and Internet technologies are combined in an efficient manner in the mobile IP framework. The mobile IP specification establishes the mechanisms that enable a mobile host to maintain and use the same IP address as it changes its point of attachment to the network. Standardization efforts in the IETF are addressing a variety of issues in order to provide for a lightweight, efficient, and effective protocol that will be compatible with other technologies and will allow users a secure, fast access to a network wherever they are.

Current efforts address optimization of the routing functions, integration with modern high-speed wireless networks, and providing access through firewalls [16].

Mobility implies higher security risks than with static operation, because the traffic may at times take unforeseen network paths with unknown or unpredictable security characteristics. The mobile IP specification makes no provisions for securing data traffic. Current effort suggest mechanisms (see RFC 2356 [29]) that allow a mobile node out on a public sector of the Internet to negotiate access past a firewall and construct a secure channel into its home network. In addition to securing traffic, these mechanisms allow a mobile node to roam into regions that impose ingress filtering and use a different address space.

Connection and interoperability with existing and future broadband wireless networks are topics that are increasingly receiving attention in the mobile IP community.

REFERENCES

1. C. Perkins (Ed.), IP mobility support, IETF RFC 2002, Oct. 1996 and revised in September 2000.
2. C. Perkins, *Mobile IP: Design Principles and Practice,* Addison-Wesley Longman, Reading, MA, 1998.
3. D. Johnson and C. Perkins, Mobility support for IPv6, IETF Internet Draft, Nov. 2000.
4. S. Deering and R. Hinden, Internet Protocol, Version 6 (IPv6) Specification, IETF RFC 1883, Dec. 1995.
5. R. Hinden and S. Deering, IP Version 6 addressing architecture, IETF RFC 1884, Dec. 1995.
6. J. B. Postel (Ed.), Internet Protocol, IETF RFC 791, Sept. 1981.
7. CDPD Consortium, Cellular digital packet data specification, PO Box 809320, Chicago, Ill., July 1993, http://www.cdpd.org/public/specification/index.html.
8. Hanks, S., Generic routing encapsulation (GRE), RFC 1701, Oct. 1994.
9. S. E. Deering (Ed.), ICMP Router discovery messages, IETF RFC 1256, Sept. 1991.
10. C. Perkins, IP Encapsulation within IP, IETF RFC 2003, May 1996.
11. C. Perkins, Minimal Encapsulation within IP, IETF RFC 2004, May 1996.
12. V. L. Voydock and S. T. Kent, Security mechanisms in high-level networks, *ACM Computer Surveys, 15,* 2, pp. 135–171, 1983.
13. R. L. Rivest, The MD5 message-digest algorithm, IETF RFC 1321, Apr. 1992.
14. S. Thomson and T. Narten, IPv6 stateless address autoconfiguration, IETF RFC 1971, Aug. 1996.
15. T. Narten, E. Nordmark, and W. Simpson, Neighbor discovery for IP Version 6 (IPv6), IETF RFC 1970, Aug. 1996.
16. C. Perkins, Route optimization in mobile IP, IETF Internet Draft, Nov. 2000.
17. S. Bradner and A. Mankin, The recommendation for the IP next generation protocol, IETF RFC 1752, Jan. 1995.
18. D. Johnson and C. Perkins, Mobility support in IPv6, *ACM Mobicom 96,* ACM, Nov. 1996, pp. 27–37.
19. A. Conta and S. Deering, Generic packet tunneling in IPv6, ftp://ftp.ietf.org/internet-drafts/draft-ietf-ipngwg-ipv6-tunnel-07.txt, July 1996.
20. M. Khalil (Ed.), Mobile IP Extensions rationalization (MIER), IETF Internet Draft, May 2000.
21. S. Kent and R. Atkinson, IP authentication header, ftp://ftp.ietf.org/internet-drafts/draft-ietf-ipsec-auth-header-03.txt, Nov. 1997 (work in progress).
22. Case, J., Fedor, M., Schoffstall, M., and J. Davin, Simple network management Protocol, RFC 1157, May 1990.
23. C. Perkins and P. Bhagwat, A Mobile Networking system based on Internet protocol (IP), in *Proceedings USENIX Symposium on Mobile and Location-Independent Computing,* Aug. 1993, USENIX Assoc., pp. 69–82.

24. J., McCloghrie, K., Rose, M., and S. Waldbusser, Protocol operations for version 2 of the simple Network Management Protocol (SNMPv2), RFC 1905, Jan. 1996.

25. D. Cong and M. Hamlen C. Perkins, The definitions of managed objects for IP mobility support, Using SMIv2, IETF RFC 2006, October 1996.

26. J. Case, K. McCloghrie, M. Rose, and S. Waldbusser, Structure of management information for Version 2 of the simple network management protocol (SNMPv2), RFC 1902, Jan. 1996.

27. W. R. Cheswick and S. Bellovin, *Firewalls and Internet Security,* Addison-Wesley, Reading, MA, 1994.

28. McCloghrie, K., and M. Rose (Eds.), Management information base for network management of TCP/IP-based internets: MIB-II, STD 17, RFC 1213, March 1991.

29. G. Montenegro and V. Gupta, Sun's SKIP firewall traversal for mobile IP, IETF RFC 2356, June 1998.

30. Y. Xu (Ed.), Mobile IP based micro mobility management protocol in the third generation wireless network, IETF Internet Draft, Nov. 2000.