ELSEVIER

Computer Networks and ISDN Systems 27 (1994) 479-491

COMPUTER NETWORKS and ISDN SYSTEMS

IMHP: A mobile host protocol for the Internet

Charles Perkins [a], Andrew Myles [b], David B. Johnson [c,*]

[a] T.J. Watson Research Center, IBM Corporation, P.O. Box 218, Yorktown Heights, NY 10598, USA
[b] Department of Electronics, Macquarie University 2109, Sydney, Australia
[c] School of Computer Science, Carnegie Mellon University, 5000 Forbes Avenue, Pittsburgh, PA 15213-3891, USA

Abstract

This paper describes a protocol that allows transparent routing of IP packets to mobile hosts in the Internet, while using only the mobile host's *home* IP address. The protocol, called IMHP (Internet Mobile Host Protocol), requires no changes in stationary hosts that communicate with mobile hosts, and requires no changes in mobile hosts above the IP level. IMHP quickly converges to optimal routing following the movement of a mobile host, while preserving the current level of security in the Internet. Detailed examples of operation are presented.

Keywords: Mobile hosts; Mobile networking; TCP/IP; Internetworking; Network protocol

1. Introduction

Within the last few years, there has been impressive growth in the number of portable computers in use. Moreover, the fact that a computer is portable no longer implies that it has limited processing power. Today's mobile computers have hundreds of megabytes of disk space, window-based user interfaces, color displays, and sophisticated devices for data communications. The combination of power and mobility promise to reshape the way we think of computing within the next few years.

Existing computer resources are made available by a worldwide collection of computer networks and protocols. People using portable computers will naturally expect to have access to this global network of computer resources, and at no loss of performance, without concern for the fact that their movement tends to violate the basic assumptions upon which the global network was built in the first place.

The first problem encountered is that internetworking protocols such as IP assume that the computer's network address logically encodes the computer's location. This is a side effect of the way the "network number" is encoded into the network-layer address; in the past, networks were thought of as physical entities that were unlikely to move. Indeed, until recently computers moved so rarely that the network impact of any movement could be handled by manual reconfiguration of routers and other administrative equipment.

For maximal flexibility, we must consider movements across domains consisting of multiple independent networks. This is a more difficult case to solve than merely allowing movement

[*] Corresponding author. E-mail: dbj@c.cmu.edu.

SSDI 0169-7552(94)00052-2

along the area defined by a single broadcast local area network. In the latter case, it would be sufficient simply to use transparent MAC-level bridges to connect one or more compatible wireless networks to the existing local area network. Similarly, in order to provide convenient mobility to the mobile user, we wish to avoid any need for rebooting or reconfiguring the mobile computer after each movement from one point of connection to the network to another.

Our vision is that of a large population of mobile users, each expecting and obtaining the highest level of service from their mobile computers and their existing (stationary) computer resources, unconstrained by and unaware of the new problems caused by the incompatibility of their network requirements and the original design goals of their internetworking protocols.

This paper describes a protocol, called IMHP (Internet Mobile Host Protocol), that we have developed to allow mobile hosts to move transparently and rapidly around both the local and the wide area network in an IP environment. The protocol contains many features drawn from the proposal of Carnegie Mellon University [6,7] and from the proposal of Macquarie University and IBM [8]. It uses the general architecture proposed by IBM [9], and includes aspects also drawn from the proposals of Sony [12–14] and of Columbia University [4,5]. IMHP has been submitted to the Mobile IP Working Group of the Internet Engineering Task Force (IETF) in its efforts toward standardizing a protocol for mobile hosts in the Internet.

2. Requirements

Any host operating using new mobile internetworking protocols must remain compatible with existing hosts. This means that we cannot specify any changes to the base IP or TCP protocols, and that we cannot require any changes to existing routers or hosts. A mobile host using IMHP will be able to communicate successfully with all existing Internet hosts.

Existing applications must continue to work without interruption when a mobile host moves between adjacent cells, as long as the uninterrupted operation is physically possible. This means that even though the route to the mobile host might change, no disconnection/reconnection will be visible to transport layer entities. Thus, application programs can expect to operate continuously over a single session even though the network attachment point of the mobile host changes.

We must avoid introducing any additional security holes into the mechanisms that operate in the Internet. This means that our protocol need not protect against intrusions by other hosts that can promiscuously "snoop" on physically passing packets, but we must ensure that hosts that do not have physical access to data or management packets sent to or from the mobile host cannot corrupt such packets.

3. Definitions

The following specific terms are used in this paper: **Node.** A device in the network that implements the Internet Protocol, IP [11]. **Router.** A node that forwards IP datagrams, as specified in Ref. [2]. This does not include nodes that, though capable of IP forwarding, have that capability turned off, nor does it include nodes that perform IP forwarding only in processing IP Source Route options. **Host.** Any node that is not a router. **Mobile host.** A host that may connect to the Internet in networks other than its own home network, while still using its home address. **Stationary host.** A host that is not a mobile host. **Correspondent host.** A host communicating with another host. This term is used when it is not relevant whether a host is a mobile host or stationary host. **Home address.** An address used to identify a mobile host, no matter where it may currently be located. **Home network.** The (logical) network on which a mobile host's home address resides. **Care-of address.** An address that defines the location of a mobile host at some particular instant in time. Packets addressed to the mobile host will arrive at this address. **Foreign agent.** A function within any node that offers a care-of address for visiting mobile hosts, and delivers arriving packets addressed to one of these mobile hosts locally to the mobile host. **Home agent.** A function within any node that maintains information about the current care-of address of each of the mobile hosts that it is configured to serve with this home network, and that forwards packets (addressed to any of these mobile hosts) to the care-of address for that mobile host. **Cache agent.** A function within any node that caches the location of one or more mobile hosts and forwards packets to these mobile hosts. **Triangle routing.** The routing of a correspondent host's packets to a mobile host by forwarding through the mobile host's home agent, rather than following the shortest path directly to the mobile host.

4. Basic operation

4.1. Infrastructure

A mobile host is the IMHP entity that may move through the IP internetwork. It is assigned a constant IP address on a home network, known as its home address. Correspondent hosts may always use the home address to address packets to a mobile host.

Each mobile host has a *home agent* on its home network. Each home agent maintains a list known as a *home list*, which identifies those mobile hosts that it is configured to serve, along with the current location of each of these mobile hosts, if known. IMHP makes no assumptions about whether mobile hosts use wired or wireless interfaces for connection to the network.

The home network configuration may correspond to a physical subnet or a virtual subnet. For example, the home network may be a physical network connected to the Internet through an IP router, which is responsible for advertising connectivity to the home network. The home agent may be a separate node attached to the physical home network, or may be implemented by the same node as the IP router. Alternatively, the home network may be a virtual network, which means that mobile hosts never connect directly to their home network. These example configurations are illustrated in Fig. 1. Other configurations are also possible in which the home agent is replicated or distributed, or the home

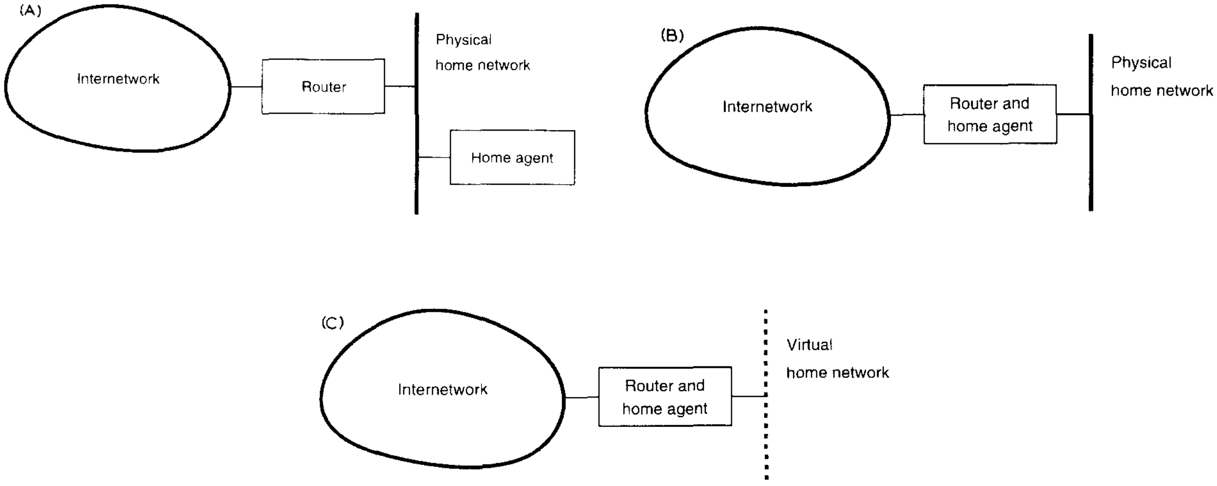


Fig. 1. Example home network configurations: (a) home agent as a separate node on the home network; (b) home agent in the router to the home network; (c) a virtual home network.

network is distributed, but such configurations are not discussed in this paper.

When a mobile host connects to the network, it must perform a registration process with a *foreign agent* on that network before packets will be delivered to the mobile host. The mechanisms used to identify that the mobile host has connected to a new network depend in part on the sub-network layer technology being used. Either the potential foreign agent or the home agent may reject a registration attempt. Typically the grounds for rejection will be security based, although other factors such as load may also be considered. During the registration process, the mobile host will specify whether or not its new location should be made available to other IMHP entities for the purposes of route optimization (Section 4.2).

Each foreign agent maintains a list known as a *visitor list*, which identifies those mobile hosts that are currently registered with it. The address of the foreign agent, supplied as the mobile host's care-of address, defines the mobile host's current location. The combination of a home address and a care-of address is known as a *binding*. The binding between a mobile host and a foreign agent is also tagged by a logical timestamp, which is generated by the mobile host by incrementing its previous timestamp value each time it attempts to register with a foreign agent. The timestamp is always included with any binding stored or passed through the network. Timestamps may be used to compare bindings for a given mobile host to determine which is the most recent.

The registration protocol ensures that a mobile host's home agent learns about the new binding of any mobile host it serves. The registration protocol also notifies the previous foreign agent that the mobile host has moved. This mechanism allows the previous foreign agent to forward packets, destined to a mobile host that has moved elsewhere, to the mobile host's new location. Optionally, instead of notifying the previous foreign agent of the mobile host's new location, the registration protocol may simply notify it that the mobile host has moved, without revealing its new location; in this case, the previous foreign agent simply removes the mobile host from its list of visiting mobile hosts. The exchange of packets used by the registration protocol is illustrated in Fig. 2 for a typical IMHP configuration.

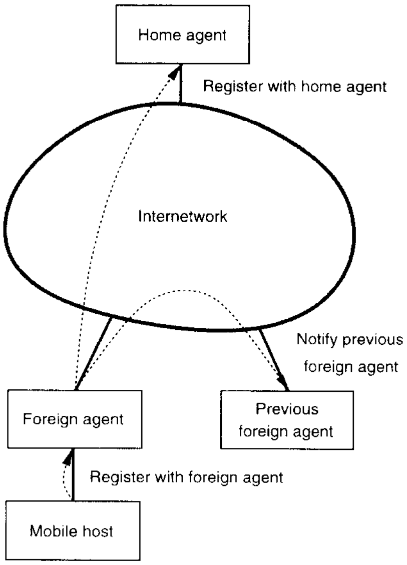


Fig. 2. Example registration process.

Any node may function as a *cache agent* by caching the current binding of one or more mobile hosts in order to be able to forward packets directly to those mobile hosts. A mobile host's previous foreign agent (functioning as a cache agent) may cache the new binding of that mobile host from the notification sent during its registration with its new foreign agent. This cache entry serves as a "forwarding pointer" to allow packets arriving at the mobile host's old location to be forwarded to its new location. Any correspondent host that implements IMHP (for example, another mobile host) may also function as a cache agent by similarly maintaining a cache of bindings for other mobile hosts; the IMHP management protocol sends a Binding Notify packet (Section 5.1) to correspondent hosts as needed to build and maintain these caches. The cache of bindings maintained by a cache agent is known as a *location cache*.

Each entry in the visitor list or location cache of a node has a lifetime period associated with it, after which the entry expires and is deleted by the node, ensuring that a stale entry does not persist forever. The lifetime period is reset whenever the entry is reconfirmed by the IMHP management protocol or by the registration protocol. The mobile host is responsible for ensuring that its visitor list entry in its current foreign agent does not expire.

A cache agent may actively attempt to reconfirm bindings in its location cache using the IMHP management protocol. Active reconfirmation methods may be appropriate when a location cache entry is used often and expiration of the entry (along with the subsequent rediscovery process) would disrupt communications.

The notification to a mobile host's previous foreign agent must be sent reliably, because otherwise packets for the mobile host might be lost until the previous foreign agent expires its visitor list entry. Until a previous foreign agent receives this notification, it will continue to transmit arriving packets for to the mobile host onto the local network where the mobile host was visiting, but the mobile host is no longer there to receive them. The notification is thus periodically retransmitted either until it is acknowledged or until the previous foreign agent can be assumed to have expired its visitor list entry for the mobile host. The lifetime period that a foreign agent uses for a visitor list entry is established by negotiation when a mobile host registers with it.

When a mobile host is connected to its physical home network it may, after notifying its home agent, revert to operating as a host using conventional protocols without any IMHP overheads, if certain minimal conditions are met. Most notably, when a mobile host departs from its home network, any ARP cache entries for the mobile host stored at existing nodes on the home network must be updated. This can be done by having the home agent send an ARP reply packet on behalf of the mobile host, specifying that the home address of the mobile host is to be associated with the MAC address of the home agent. This use of ARP is known as a *gratuitous* ARP.

Foreign agents, home agents, and mobile hosts, although described separately in this section, may be located together in various combinations within any node.

4.2. Packet routing

IMHP entities must direct packets destined to a mobile host to the mobile host's current known location (i.e., care-of address). IMHP entities send packets to a mobile host's current location using *tunnelling*. As a general rule, tunnelling involves the use of an encapsulation protocol. All IMHP entities must support the default IMHP tunnelling protocol described in Section 5.2.

IMHP establishes a few rules for forwarding packets. These rules help ensure that optimal routes are used when possible. In general, a node uses whatever location cache, visitor list, home list, and normal IP routing table information it has available to forward packets, with a small number of restrictions. If none of the rules below apply to a particular packet, then normal IP routing rules are followed.

The following two basic rules apply to all IMHP nodes, which allow for the delivery of packets addressed to these nodes and for the decapsulation of tunnelled packets:

- If a node receives a tunnelled packet, and the destination of the tunnel is one of the node's own addresses, then the node decapsulates the packet and continues processing the packet according to the remaining forwarding rules.

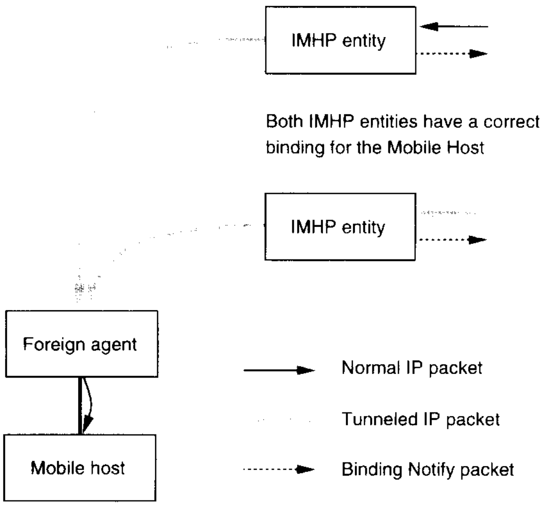


Fig. 3. IMHP routing and lazy update example.

- If a node receives a packet that is not tunnelled, and the destination of the packet is one of the node's own addresses, then the node passes the packet to higher layer protocols for processing.

A home agent will generally have a current authenticated binding for the mobile hosts in its home list. A home agent must also serve as a cache agent for these mobile hosts, and may be a foreign agent for the mobile hosts it serves as well. These properties serve to define the following forwarding rules for a home agent, when dealing with packets addressed to the mobile hosts in its home list:

- If a home agent receives a tunnelled packet for a mobile host in its home list, in which the original destination is the same as the encapsulated destination, then the home agent decapsulates the packet and continues processing the packet according to the remaining forwarding rules.
- If a home agent (acting as a foreign agent) has a visitor list entry for the mobile host, then the home agent delivers the packet locally using the network interface indicated by the visitor list entry.
- If a home agent (acting as a cache agent) has a location cache entry for the mobile host, then the home agent tunnels the packet to the care-of address indicated in the location cache entry, subject to the restriction in the following rule.
- A home agent must never tunnel a packet to a foreign agent if the packet was just tunnelled to the home agent from that same foreign agent. This rule avoids looping between a home agent and a foreign agent that no longer thinks it serves some mobile host. The home agent may also undertake appropriate actions (here undefined) to further handle the packet or locate the mobile host.
- If a home agent does not have a location cache entry or a visitor list entry for the destination mobile host, further action is undefined. The home agent may in this case undertake appropriate actions to further handle the packet or locate the mobile host.

Foreign agents and cache agents use forwarding rules that are similar to those used by a home agent. The differences from the rules used by a home agent are primarily due to the fact that a foreign agent or a cache agent might not have an authenticated binding for the mobile host, if that agent is not also the home agent serving that mobile host. The following forwarding rules apply to packets received by a foreign agent or a cache agent:

- If a foreign agent receives a tunnelled packet, and the foreign agent has an entry in its visitor list for the packet's destination after decapsulating the packet, then the foreign agent delivers the packet locally using the network interface indicated by the visitor list entry.
- If a foreign agent receives a (non-tunnelled) packet, and the foreign agent has an authenticated visitor list entry for the packet's destination, then the foreign agent delivers the packet locally to the interface indicated by the visitor list entry.
- If a cache agent receives a packet, and the cache agent has a location cache entry for the packet's destination, then the cache agent tunnels the packet to the care-of address indicated in the location cache entry.
- If a cache agent or a foreign agent receives a tunnelled packet, and the cache agent or foreign agent is unable to forward the packet using the above rules after decapsulating the packet, then the cache agent or foreign agent tunnels the packet to the mobile host's home agent by sending the packet with both the original destination and the encapsulated destination set to the mobile host's home address.

The philosophy of IMHP is to perform lazy updating of location caches, since cached bindings for a mobile host need not be updated until they are used. If a stale binding is used, the packet will experience non-optimal routing until the stale binding is updated, but the natural action of IMHP entities causes bindings to be updated as soon as possible whenever they are in use. If one IMHP entity discovers that another IMHP entity might be holding incorrect information about the location of a mobile host, it should attempt to correct the other IMHP entity. The only exceptions to the use of lazy updating are that a mobile host usually attempts to notify its previous foreign agent that it has moved, and a mobile host always tells its home agent that it has moved.

For example, if an IMHP entity receives a packet that needs to be tunnelled to a mobile host, it may conclude that the source (the source of tunnel in case of tunnelled packets) does not have a correct binding for the destination mobile host. The IMHP entity should return an IMHP Binding Notify packet, containing a current binding, to the IMHP entity suspected of having the incorrect binding, as illustrated in Fig. 3. The Binding Notify packet is part of the IMHP management protocol, and is described more fully in Section 5.1.

An IMHP entity must not flood the network with IMHP management protocol packets. Most existing hosts will ignore these packets; and hosts that do understand them may be busy, for example authenticating a binding from a previous notification. Even if an IMHP entity receives a packet through a tunnel, it cannot conclude that the source will understand IMHP management protocol packets sent to it, as Internet hosts are free to use tunnelling for other purposes. Thus, IMHP entities must use a backoff algorithm to limit the frequency with which they send IMHP management protocol packets containing the same binding to any individual node.

4.3. Security considerations

IMHP must provide some form of authentication for bindings received. Without authentication, an IMHP entity could use any binding or other information it received from the management protocol or from the registration protocol. This would allow for faster convergence to optimal routes and would simplify implementation; however, any malicious or mischievous host could then easily forge IMHP management protocol packets containing a false binding, allowing such a host to intercept or otherwise redirect packets intended for the mobile host. This risk is unacceptable in the Internet where nothing may be assumed about other users.

Strong authentication could be provided for all bindings received, for example using public and private keys with a key distribution infrastructure. Using such a mechanism, IMHP entities must authenticate any bindings they receive. Although strong authentication is highly desirable, such mechanisms could be slow and difficult to administer, and no standard key distribution infrastructure has yet been defined for use in the Internet. The wide-spread use of strong authentication mechanisms in the Internet is also currently impeded by patent and international export restrictions on encryption technology.

As an interim measure, until use of standard strong authentication mechanisms becomes feasible, IMHP defines a simple authentication mechanism that preserves the current level of security in the Internet. In effect, all nodes on networks on the normal routing path of a packet are assumed to be trustworthy, and no other host can change this path; for nodes connected to the normal routing path of the packet, however, many other security holes already exist in the protocols used in the Internet [1]. The rest of this section discusses the details of this authentication mechanism in IMHP.

There are two cases in particular that require some level of authentication to guard against spoofing. First, a home agent must have confidence in a binding for a mobile host it serves, and second, other IMHP entities need to authenticate bindings which are received in Binding Notify packets.

In IMHP, each mobile host is configured with a simple password (a shared secret) that both the mobile host and its home agent know. This secret is used in authenticating IMHP management and registration messages between the mobile host and its home agent, and is no worse than a password being passed in clear text across today's Internet.

Other IMHP entities may not share such a secret, but can obtain an authenticated binding for a mobile host by sending a Binding Request packet (Section 5.1) to the mobile host's home agent, along with a random value as an authenticator for the Binding Notify message. If the reply contains the same authenticator, the included binding can be considered to be authenticated, since the normal routing path of packets in the Internet is assumed to be trusted; the random authenticator value in the request and reply guards against forged reply packets being sent by malicious hosts not on this routing path.

When a mobile host moves, its previous foreign agent should be quickly notified of its new binding so that packets in flight are not lost. The speed of notification can be increased by including a random authenticator, established when the mobile host registered with this previous foreign agent (with an implied trust of the local foreign agent to mobile host link), in the update packet. If a foreign agent receives a notification with that authenticator, the new binding can be considered to be authenticated.

These three authentication methods are illustrated in Fig. 4. When location privacy is required, or route optimization is not important, the mobile host may also arrange with its home agent to not advertise its binding; the previous foreign agent would not learn the new location of the mobile host when the mobile host moves.

5. IMHP packet descriptions

5.1. Management packets

The IMHP management protocol operates as an extension of ICMP [10] through the definition of an additional ICMP message type for each of the three IMHP management packet types: Binding Request, Binding Notify, and Binding Acknowledge. Like ICMP error messages, IMHP management protocol packets should never cause the generation of other IMHP management protocol packets (including Binding Notify), and IMHP management protocol packets are only sent with regard to fragment zero of fragmented packets. For brevity, the syntax and functions of the IMHP management protocol packets are given here only in outline.

The destination address of a Binding Request packet should be set to the address of the mobile host for which the binding is being requested. A control bit is also set in the packet to prevent the packet being rerouted by any location cache or visitor list entries. The packet will thus reach the mobile host's home network, where it will be received by its home agent. When the home agent receives such a Binding Request for a mobile host in its home list, the home agent replies on the mobile host's behalf.

If an IMHP entity receives a packet that it must tunnel to reach the destination mobile host, it may suspect that the source of the packet has an incorrect binding or no binding for the destination mobile host; it may then send that entity an updated binding for that mobile host using an IMHP Binding Notify packet. The Binding Notify packet is also used as the reply to a Binding Request packet, and to notify a mobile host's previous foreign agent that it has moved to a new foreign agent. Bindings are shown in the Binding Notify packet by including the address of the foreign agent, the address of the mobile host, the binding's logical timestamp, and the lifetime re-

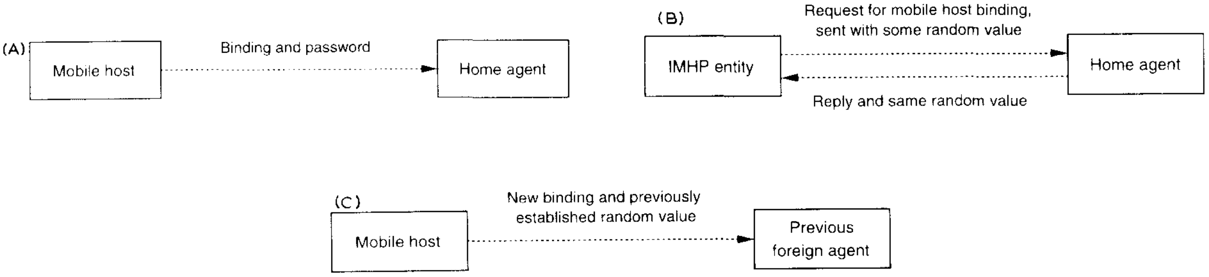
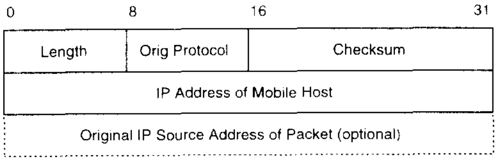

(A)
Mobile host
Binding and password
Home agent
(B)
IMHP entity
Request for mobile host binding, sent with some random value
Reply and same random value
Home agent
(C)
Mobile host
New binding and previously established random value
Previous foreign agent

Fig. 4. Authentication methods used in IMHP: (a) mobile host sending a new binding to its home agent; (b) IMHP entity requesting an authenticated binding for a mobile host; (c) mobile host notifying its previous foreign agent of its new binding.



0	8	16 31
Length	Orig Protocol	Checksum
IP Address of Mobile Host		
Original IP Source Address of Packet (optional)		

Fig. 5. IMHP encapsulation header format.

maining for the validity of the binding. If the mobile host is connected to its home network, the mobile host's own address will be used in the Binding Notify as the foreign agent's address. An authenticator will be included when available or supplied in a Binding Request to which the Binding Notify is replying.

A control bit may be set in a Binding Notify packet to request an acknowledgment from the recipient. An IMHP entity receiving such a Binding Notify packet acknowledges the receipt by sending an IMHP Binding Acknowledge containing the same binding. This acknowledged form of Binding Notify is used when sending the notification to a mobile host's previous foreign agent during its registration with a new foreign agent.

5.2. Tunnelling protocol

The default IMHP tunnelling protocol uses a very efficient form of encapsulation; it adds only 8 bytes to each packet sent to a mobile host if the sender has a location cache entry for the destination mobile host, and otherwise adds only 12 bytes to each packet. Fig. 5 illustrates the IMHP encapsulation header format.

To encapsulate a packet, rather than adding a new IP header to the packet, the encapsulation header is inserted into the packet immediately *following* the existing IP header. The original Destination Address and Protocol number in the IP header are moved into the encapsulation header, and if the IP address of the encapsulating agent differs from the current Source Address in the IP header, the Source Address is likewise moved into the encapsulation header. The Length in the encapsulation header is set to either 8 bytes or 12 bytes, depending on whether or not the Source Address was moved. In the IP header, the Protocol number is set to indicate the IMHP tunnelling protocol, the Destination Address is set to the mobile host's care-of address, and the Source Address is set to the IP address of the encapsulating agent. Finally, the IP header Checksum and Length fields are adjusted to reflect the changes to the packet.

Intermediate routers need not understand the tunnelling protocol, since after being encapsulated, the packet is simply a normal IP packet addressed to the mobile host's care-of address. Once delivered to that destination, the packet will be handled by the IMHP protocol software on that node, based on the Protocol number in the IP header.

6. Packet transmission examples

The following subsections describe examples of the actions that the various IMHP entities (mobile hosts, foreign agents, and home agents) are required to perform under a range of typical scenarios. In each example, the same line styles used in Fig. 3 are used to represent the different types of packets. It is assumed in these examples that mobile hosts and foreign agents maintain location caches.

6.1. Mobile host to mobile host communication

Fig. 6 illustrates the basic operation when a mobile host, MH1, within range of a foreign agent, FA1, having a home agent, HA1, wants to communicate with another mobile host, MH2, within range of a foreign agent, FA2, having a

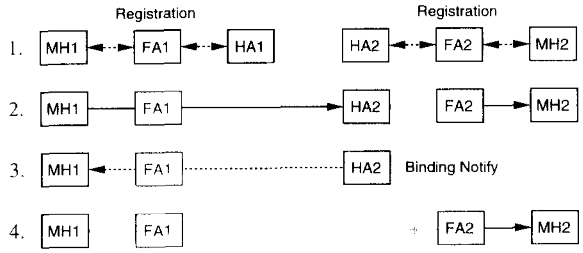


Fig. 6. Mobile host to mobile host communication.

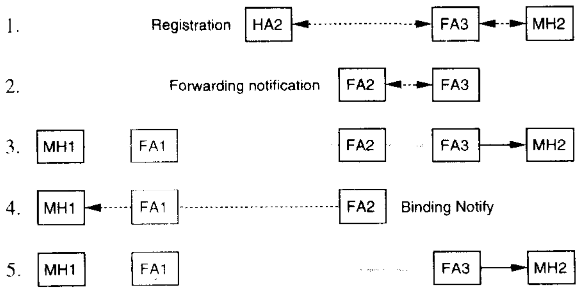


Fig. 7. Mobile host movement.

home agent, HA2. The following operations are shown in Fig. 6:

(1) MH1 and MH2 both register independently with their foreign agents (FA1 and FA2, respectively) and notify their home agents (HA1 and HA2, respectively), of their new bindings.

(2) Suppose MH1 wants to send a packet to MH2, and MH1 does not have a binding cached for MH2. MH1 transmits the packet relying on existing IP routing protocols, using FA1 as its default router. The packet is eventually received by MH2's home agent, HA2, which tunnels the packet to MH2's foreign agent, FA2. When FA2 receives the tunnelled packet, it decapsulates it and delivers it locally to MH2.

(3) When HA2 receives and then tunnels the packet, it also sends to the source (here, MH1) an IMHP Binding Notify packet containing MH2's binding, as MH1 seems not to have a binding cached for MH2. When MH1 receives the Binding Notify packet containing the binding for MH2, it may need to authenticate the binding using the methods described in Section 4.

(4) Assuming MH1 is satisfied that the received binding is genuine, MH1 can transmit future packets for MH2 by tunnelling them directly to MH2's current foreign agent, FA2. A close to optimum route is thus established.

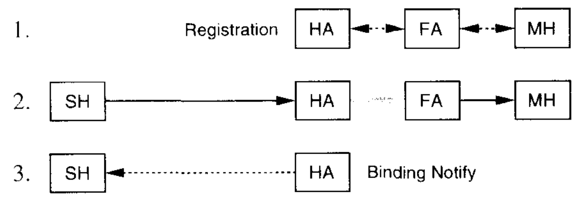


Fig. 8. Stationary host to mobile host communications.

6.2. Mobile host movement

Fig. 7 extends the example of Fig. 6 to show the movement of MH2 to a new location. The following operations are shown in Fig. 7:

(1) MH2 detects that it is connected to a new network. The registration protocol is used to register with a new foreign agent, FA3, and to notify MH2's home agent, HA2.

(2) MH2's previous foreign agent, FA2, is also reliably notified of MH2's new binding. The notification to FA2 may include authentication information.

(3) Suppose MH1 wants to send a packet to MH2. MH1 tunnels the packet to where it believes MH2 is located at FA2. FA2 forwards the packet to FA3, using the binding that it received in the notification from MH2's new registration with FA3. Finally, FA3 decapsulates the packet and delivers it locally to MH2.

(4) FA2 recognizes that MH1 must have an old binding for MH2, since otherwise MH1 would not have tunnelled the packet to FA2. FA2 thus sends MH1 a Binding Notify packet notifying it of MH2's new binding at FA3. MH1 may need to authenticate this binding before using it.

(5) Once the new binding is authenticated, future packets to MH2 are tunnelled directly to FA3.

HA1 is not involved in any of the messages related to the movement of MH2 and the subsequent update of bindings held by MH1.

6.3. Stationary host to mobile host communication

Fig. 8 illustrates the case in which a stationary host, SH, that does not implement IMHP, wants to communicate with a mobile host, MH, within range of a foreign agent, FA, having a home agent, HA. The following operations are shown in Fig. 8:

(1) MH detects it is connected to a new network

and uses the registration protocol to register with a new foreign agent, FA, and to notify its home agent, HA.

(2) Suppose SH wants to send a packet to MH. Since SH does not implement IMHP, it does not have MH's location cached. SH therefore sends the packet to MH using conventional protocols. The packet is eventually received by HA, which tunnels it MH's current location, FA. FA decapsulates the packet and delivers it locally to MH.

(3) When HA tunnels the packet from SH to FA, it also sends a Binding Notify back to the source of the packet, SH. Since SH does not implement IMHP, HA may eventually surmise that the Binding Notify packets it is sending to SH are having no effect; HA's backoff algorithm will cause it send a new Binding Notify packet to SH only infrequently, not sending one at all for most new packets it receives from SH for MH. The packets from SH will continue to follow a "triangle routing" path, which is likely to be non-optimum, but no changes are required in SH to communicate with MH.

6.4. Routing loop resolution

Suppose, perhaps because of some incorrect implementation of the protocol, that two or more cache agents had location cache entries forming a loop for a particular mobile host. Consider the case of three cache agents (CA1, CA2, and CA3) that have such bindings in their location caches for a mobile host, MH. The resolution of the loop is illustrated in Fig. 9.

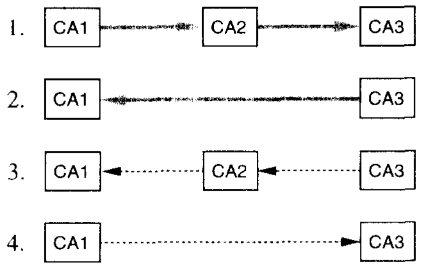


Fig. 9. Routing loop resolution.

The following operations are shown in Fig. 9:

(1) CA1 tunnels a packet destined for MH to CA2, and CA2 then tunnels it to CA3.

(2) When CA3 receives the packet, it will tunnel the packet on again to CA1.

(3) When CA2 tunnels the packet to CA3, it also sends a Binding Notify back to CA1, since CA1 appears not to have a current binding for MH (otherwise, CA1 would have tunnelled the packet there rather than to CA2). Similarly, when CA3 tunnels the packet to CA1, it also sends a Binding Notify back to CA2.

(4) Finally, CA1 likewise sends a Binding Notify to CA3. Each cache agent that receives a Binding Notify packet uses the logical timestamp in the binding to decide whether its current binding is out of date. If so, it replaces its location cache entry with the new binding, possibly after authenticating it. The loop is thus broken by these Binding Notify packets.

7. Extensions

7.1. Popups

Some areas of the Internet may not have IMHP facilities, such as foreign agents, available for use. When this situation arises, a mobile host may, in effect, act as its own foreign agent to maintain connectivity. This technique, which has been called *popup* [4], requires a mobile host using IMHP to acquire a temporary local address from a local address server (for example, a server implementing DHCP [3]) and to report the allocated address to its home agent as its care-of address. Packets for the mobile host that are then tunnelled to this care-of address are received directly by the mobile host, which decapsulates the packets itself before processing. Only the mobile host need know that no separate foreign agent is in use.

This binding can be distributed using Binding Notify messages in the same way as any other binding, allowing optimal routing of packets to the mobile host using this temporary address.

However, when the mobile host subsequently moves to a new network, packets sent to the mobile host might be lost until all location cache entries pointing to this temporary address expire. This movement of the mobile host would appear to correspondent hosts as a crash of the foreign agent, since no node would then be responding to the temporary address. This problem may be solved by instead not distributing this new binding to nodes other than the mobile host's home agent, but this would require all packets to the mobile host to be forwarded through its home agent, resulting in routing that is likely to be non-optimal.

In either case, true mobile functionality depends on the ability of the mobile host to detect automatically that it has moved. Without a real foreign agent, this might be difficult, or might require user intervention. One possible method in this case for the mobile host to detect that it has moved to a new network would be to monitor the source address of received broadcast packets such as ARP requests.

7.2. *Intermediate cache agents*

Different types of intermediate agents have been suggested by a number of proposals [6,8,13] as a way of optimizing routes between stationary hosts and mobile hosts.

In IMHP, the functionality of a cache agent may also be implemented in intermediate routers not otherwise functioning as home agents, foreign agents, or mobile hosts. When such an intermediate router receives a packet for normal IP forwarding, it can instead tunnel the packet directly to the foreign agent currently serving the destination mobile host, if it has a location cache entry for that mobile host. Intermediate routers serving as cache agents initially discover new bindings by snooping on IMHP Binding Notify packets as they forward them.

8. Summary and conclusions

We have proposed mechanisms useful for enabling computers to maintain network connections even as they move about from one location to another. The model we have developed fits naturally within the existing Internet and allows mobile hosts to communicate with existing computing resources without requiring any changes to existing nodes. We have transformed the problem of providing seamless connectivity to mobile hosts, into a problem of maintaining dynamic location information for the mobile host at the home agent and optionally at cache agents.

By enabling hosts to also cache bindings for mobile hosts, we provide mechanisms for better routing which bypasses the default reliance on routes through the home agent. Thus, as more new equipment is deployed that incorporates these techniques for avoiding "triangle routing", the routing inefficiency associated with maintaining network connections with mobile hosts will disappear. This new feature, which is roughly analogous to the current ICMP "Host Redirect" message, requires careful authentication, since otherwise a malicious user might issue an intentionally incorrect binding in order to intercept or otherwise redirect a data stream intended for a mobile host.

The user of a mobile host need not perform any unusual procedures or operations to achieve the benefits of seamless mobility wherever allowed by the physics of the network medium. By providing mechanisms for distributing the mobile host's care-of address just to the places where it is in use, IMHP eliminates the likelihood that the home agent would be a bottleneck in the operation of the home network. Schemes that rely on the home agent for transmission of every packet destined to the mobile host are likely to provide poorer performance, present extra load to the interconnected networks, and offer traffic characteristics tied to the vagaries of the processing load carried by the home agent. We have tried to take great care to make sure that the maintenance of the distributed bindings in IMHP location caches is simple, effective, and reliable.

Acknowledgements

We gratefully acknowledge the interactions we have had with Al Quirt, Kannan Alagappan, and others in the IETF Mobile IP Working Group who have helped shape the ideas within this paper.

References

[1] S.M. Bellovin, Security problems in the TCP/IP protocol suite, *Computer Commun. Rev.* **19** (2) (1989) 32–48.

[2] R.T. Braden and J.B. Postel, Requirements for Internet gateways, Internet Request For Comments RFC 1009, June 1987.

[3] Ralph Droms, Dynamic host configuration protocol, Internet Request For Comments RFC 1531, October 1993.

[4] J. Ioannidis, D. Duchamp, G. Maguire and S. Deering, Protocols for mobile internetworking, Internet Draft, June 1992.

[5] John Ioannidis, Dan Duchamp and Gerald Q. Maguire Jr, IP-based protocols for mobile internetworking, in: *Proc. SIGCOMM '91 Conf. Communications Architectures and Protocols*, 1991, pp. 235–245.

[6] David B. Johnson, Transparent Internet routing for IP mobile hosts, Internet Draft, July 1993.

[7] David B. Johnson, Scalable and robust internetwork routing for mobile hosts, in: *Proc. 14th Int. Conf. on Distributed Computing Systems*, June 1994, pp. 2–11.

[8] Andrew Myles and Charles Perkins, Mobile IP, Internet Draft, August 1993.

[9] C. Perkins and Y. Rekhter, Support for mobility with connectionless network layer protocols, Internet Draft, November 1992.

[10] J.B. Postel, Internet control message protocol, Internet Request For Comments RFC 792, September 1981.

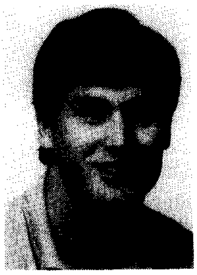
[11] J.B. Postel, Internet Protocol, Internet Request For Comments RFC 791, September 1981.

[12] F. Teraoka, Kim Claffy and M. Tokoro, Design, implementation, and evaluation of Virtual Internet Protocol, in: *Proc. 12th Int. Conf. on Distributed Computing Systems*, June 1992, pp. 170–177.

[13] Fumio Teraoka, VIP: IP extensions for host migration transparency, Internet Draft, July 1992.

[14] Fumio Teraoka, Yasuhiko Yokote and Mario Tokoro, A network architecture providing host migration transparency, in: *Proc. SIGCOMM '91 Conf.: Communications Architectures and Protocols*, September 1991, pp. 209–220.

Charles Perkins received the B.A. degree and the M.E.E. degree from Rice University, and the M.A. degree from Columbia University. Since 1984, he has worked for IBM on a variety of projects related to networks, multiprocessors, and mobile computing. He is a member of USENIX, IEEE, ACM, and the Internet Society.



Andrew Myles received the B.Sc. degree in 1984 and the B.E. (Electrical) degree with First Class Honours and University Medal in 1986 from the University of Sydney. From 1987 to 1989 he worked at Hewlett Packard Laboratories in Bristol, UK, before returning to Australia. He is currently working towards the Ph.D. degree at Macquarie University, with a special interest in MAC and network layer protocols for wireless and mobile networks. He is a member of the IEEE and the IEEE Communications Society.

David Johnson received the B.A. degree in computer science and mathematical sciences in 1982, and the M.S. and Ph.D. degrees in computer science in 1985 and 1990, respectively, all from Rice University. He is currently an Assistant Professor of Computer Science at Carnegie Mellon University, where he has been since 1992. Prior to joining the faculty at Carnegie Mellon, he was a Research Scientist and Lecturer at Rice University for three years. His research interests include network protocols, distributed systems, and operating systems. Dr. Johnson is a member of the IEEE Computer Society, IEEE Communications Society, ACM, USENIX, Sigma Xi, and the Internet Society.