The Internet Mobile Host Protocol (IMHP)

Charles E. Perkins <perk@watson.ibm.com>
Andrew Myles <andrewm@mpce.mq.edu.au>
David B. Johnson <dbj@cs.cmu.edu>

Abstract

This paper describes the Internet Mobile Host Protocol (IMHP), which allows transparent routing of IP packets to mobile hosts in the Internet, while using only the mobile host's home IP address. No changes are required in stationary hosts that communicate with mobile hosts, and no changes are required in mobile hosts above the IP level. IMHP quickly converges to optimal routing following the movement of a mobile host, while maintaining the weak security model of today's Internet. Detailed examples of operation are presented.

I. 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 that 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 along the area defined by a single network. In the latter case, it would be sufficient to provide bridges between the mobile computer and the single network. By giving the mobile computer a network address compatible with the network number assigned to the single network of interest, packets to and from the mobile computer could be delivered as long as the bridges know whether or not the mobile computer is within their individual range. Similarly, in order to provide convenient mobility to the mobile user, we wish to avoid any need for rebooting the computer after each network reconnection (i.e., after each move from one attachment point 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.

Our Internet Mobile Host Protocol (IMHP), allows 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 proposals of Carnegie Mellon University [5, 6] and of Macquarie University and IBM [7]. It uses the general architecture proposed by IBM [8], and includes aspects also drawn from the proposals of Sony [13, 12, 11] and of Columbia University [4, 3].

II. Requirements

Any host operating using these 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 which operate the Internet. This means that our protocol need not protect against intrusions by other hosts which can promiscuously "snoop" on physically passing packets, but that no other external agents can corrupt data or management packets communicated with the mobile host.

III. Definitions

The following specific terms are used in this paper:

Node A device in the network that implements the Internet Protocol, IP [10].

Router A node that forwards IP datagrams, as specified in [1]. 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 a 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 of time. Packets addressed to the mobile host will arrive at this address.

Foreign agent An agent 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 An agent that maintains information about the current care-of address of each of the mobile hosts it is configured to serve, and that forwards packets (addressed to any of these mobile hosts) to the care-of address for that mobile host.

Triangle routing A situation in which a correspondent host's packets to a mobile host are forwarded through the mobile host's home agent, rather than following the shortest path directly to the mobile host.

Cache agent An agent that caches the location of one or more mobile hosts and forwards packets to these mobile hosts.

IV. Basic Operation

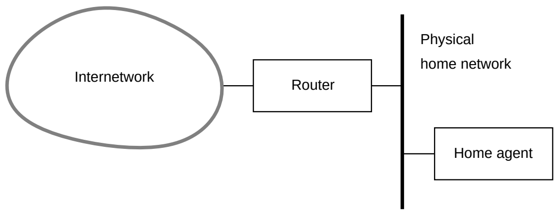
IV.A. Infrastructure

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.

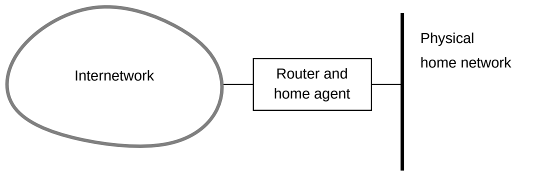
A mobile host has a home agent, which is attached to its home network. Each home agent maintains a list known as a *home list*, which identifies those mobile hosts that it is configured to serve, along with the current location of each of these mobile hosts, if known. IMHP makes no assumptions about 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 Figure 1. Other configurations are also possible in which the home agent is replicated or distributed, or the home network is distributed, but such configurations are not discussed in this paper.

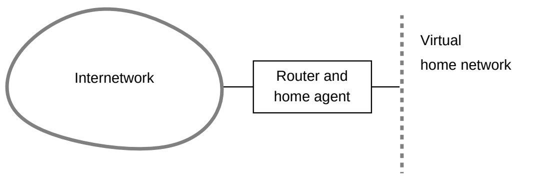
When a mobile host connects to the network, it must perform a registration process before packets will be delivered to it. The mechanisms used to identify that the mobile host has connected to the a new network depend on the sub-network layer technology being used. Either the potential foreign agent 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 IV.C).



(a) Home agent as a separate system on the home network



(b) Home agent in the router to the home network



(c) A virtual home network

Figure 1 Example home network configurations

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(s) that the mobile host's 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. 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 Figure 2 for a typical IMHP configuration.

Any node may cache the current binding of a mobile host in order to be able to forward packets directly to that mobile host. A mobile host's previous foreign agent (functioning as a cache agent) may cache the new binding of the mobile host from the notification sent during the new registration; 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 maintain a cache of bindings for other mobile hosts; the IMHP management protocol sends a Binding Notify packet (Section V.A) 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*.

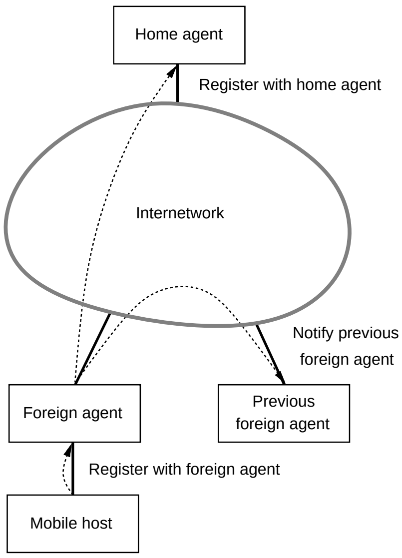


Figure 2 Example registration process

Each entry in the visitor list or location cache of a node has a time out associated with it, ensuring that a stale entry does not persist forever. The time out 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 is not timed out.

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 a time out (along with the subsequent rediscovery process) would disrupt communications.

The notification to a mobile host's previous foreign agents must be sent reliably, because otherwise packets might be lost until the previous foreign agent times out its visitor list entry for the mobile host. The notification is thus periodically retransmitted either until it is acknowledged or until the previous foreign agent can be assumed to have timed out its visitor list entry for the mobile host. The timeout period that a foreign agent uses for a visitor list entry is established by negotiation when a mobile host registers with the foreign agent.

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 out 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 ARP reply is known as a *gratuitous* ARP.

Foreign agents, home agents, and mobile hosts, although described separately in this section, may be combined together within the same node for many purposes. The IMHP management protocol discussed in this section is described more fully in Section V.A.

IV.B. Packet Routing

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

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 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 tunneled packets:

- If a node receives a tunneled 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.
- If a node receives a packet that is not tunneled, 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 tunneled 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 has a visitor list entry for the mobile host, then the home agent delivers the packet locally to the network interface indicated by the visitor list entry.
- If a home 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 tunneled 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 tunneled 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 to the interface indicated by the visitor list entry.
- If a foreign agent receives a 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 data packet (not an IMHP management 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 tunneled 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 this rule 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 tunneled to a mobile host, it may conclude that the source (the source of tunnel in case of tunneled packets) does not have a correct binding for the destination mobile host. The IMHP entity should return an IMHP Binding Notify protocol packet containing a current binding to the IMHP entity that has the suspected incorrect binding, as illustrated in Figure 3. The Binding Notify packet is part of the IMHP management protocol, and is described more fully in Section V.A. The same principle does not apply to the receipt of any IMHP management protocol packets, which should not cause the generation of further IMHP management packets. This is similar to the operation of ICMP error messages.

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 tunneling 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 mobile host.

IV.C. Security Considerations

IMHP is designed to support a range of security models, ranging from no security to *weak security* to strong security. This section defines the various security models and outlines their advantages, disadvantages, and possible implementation.

If an IMHP entity is operating with no security, it may use any binding or other information it receives from the IMHP management protocol or from the registration protocol. This allows for faster convergence to optimal routes and simplifies implementation. However, a malicious or mischievous host may then intercept a packet stream to a mobile host, by simply sending a forged IMHP management protocol packet containing a false binding. This risk is unacceptable in the Internet where nothing may be assumed about other users.

Under the strong security model, IMHP entities authenticate any bindings or other information they receive about a mobile host, by using public and private keys and trusted servers. This can be much slower and difficult to administer.

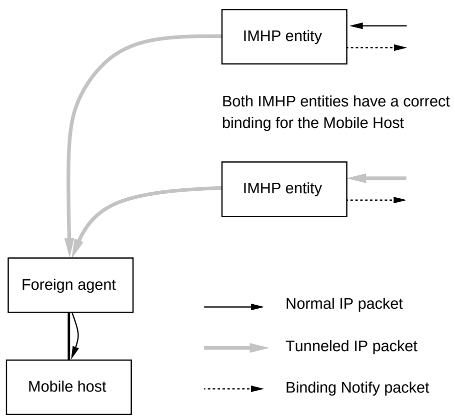


Figure 3 IMHP routing and lazy update example

The *weak security* model provides security that is at least as good as that provided by the Internet today. 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. The rest of this section discusses the details of a weak security model as it applies to 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; thus it will require a shared secret. Second, other IMHP entities need to authenticate bindings which are received in Binding Notify packets.

A mobile host includes a simple password (a shared secret) that both the mobile host and the home agent know. This method of authentication is no worse than a password being passed in clear text across today's network, and so it may be considered to satisfy the weak security model.

Other IMHP entities may not share such a secret, but can obtain an authenticated binding for a mobile host by sending its home agent a Binding Request packet (Section V.A) 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 authentic under the weak security model. For such requests, a control bit is set in the Binding Notify packet (Section V.A) to prevent the packet being tunneled by cache agents. Under the assumptions of weak security, the request is then guaranteed to reach the mobile host's home agent.

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. This process can be sped up by including a random authenticator, established when the mobile host registered with this previous foreign agent (with an implied trust of

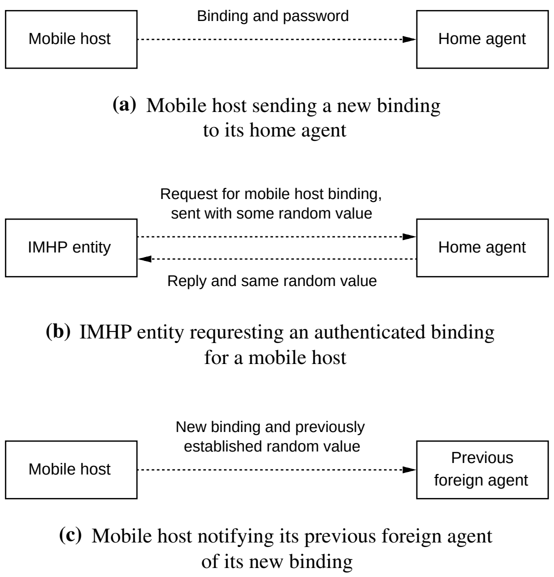


Figure 4 Weak security methods in IMHP

the mobile host to foreign agent link), in the update packet. If a foreign agent receives a notification with that authenticator, the new binding can be considered to be authentic under the weak security model.

These three methods used in the weak security model are illustrated in Figure 4. When location privacy is required, or route optimization is not important, the mobile host may also arrange with its home agent to never advertise its binding; previous foreign agents would not learn the new location of the mobile host as it moves.

V. IMHP Packet Description

V.A. Management Packets

The IMHP management protocol would operate as an extension of ICMP [9] through the definition of additional message types. For brevity, the syntax and functions of the IMHP management protocol packets are given here only in outline. Like ICMP error messages, IMHP management protocol packets should never cause the generation of other IMHP management protocol packets, and IMHP management protocol packets are only sent with regard to fragment zero of fragmented packets.

Three types of management packets are used in IMHP: Binding Notify, Binding Request, and Binding Acknowledgement.

The destination address of a Binding Request packet should be the same as the address of the mobile host in the packet for which the binding is being requested. The packet will thus reach that mobile host’s home network, where it will be received by the 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 then must tunnel to a mobile host, it may suspect that the source IMHP entity has an incorrect binding or no binding for a mobile host. It may then send that entity an IMHP Binding Notify for this mobile host. An IMHP entity acknowledges the receipt of an IMHP Binding Notify with an IMHP Binding Acknowledge containing the same binding. Bindings are shown by including the addresses of the foreign agent, the mobile host, and the lifetime remaining for the validity of the binding. If the mobile host is connected to its home network, its address will also be used in the Binding Notify as the foreign agent’s address. An authenticator will be included when available or supplied in the Binding Request.

A control bit may be set in any IMHP management packet to specify that no location caches are to be used to redirect the packet. This bit can be used when addressing an IMHP management packet to a mobile host, to insure that the packet will arrive at the mobile host’s home agent.

Another control bit may be set in a Binding Notify packet, to request an acknowledgment from the recipient. This acknowledged form of Binding Notify is used when sending the notifying to mobile host’s previous foreign agent during its registration with a new foreign agent.

V.B. Encapsulation Protocol

The default IMHP tunneling protocol is an encapsulation protocol that is very efficient in terms of overhead; 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. Figure 5 illustrates the IMHP encapsulation tunneling header format.

To encapsulate a packet, rather than adding a new IP header to the packet, the tunneling 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 tunneling 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 tunneling header. The Length in the tunneling 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 encapsulation tunneling 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 tunneling 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.

VI. Packet Transmission Examples

The following subsections describe examples of the actions that the various IMHP entities (mobile hosts, foreign agent,s and home agents) are required to perform under a range of typical scenarios.

In each example, the same line styles used in Figure 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.

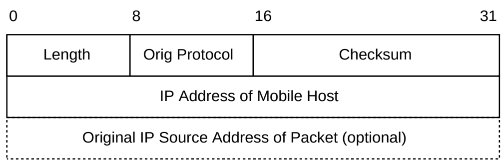


Figure 5 IMHP encapsulation tunneling header format

VI.A. Mobile Host to Mobile Host

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

1. MH1 and MH2 both register 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 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 tunneled packet, it decapsulates it and delivers it locally.
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 IMHP management protocol packet containing the binding for MH2, it may need to authenticate the binding using methods described in Section IV.
4. Assuming MH1 is satisfied that the received binding is genuine, MH1 can transmit future packets for MH2 by tunneling them directly to MH2's current foreign agent, FA2. A close to optimum route is thus established.

VI.B. Mobile Host Movement

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

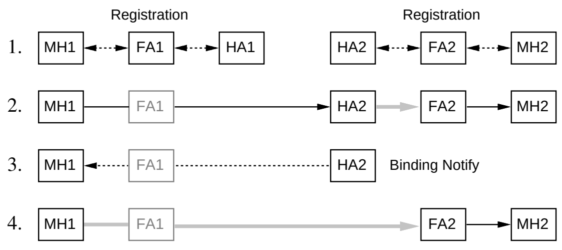


Figure 6 Mobile host to mobile host communication

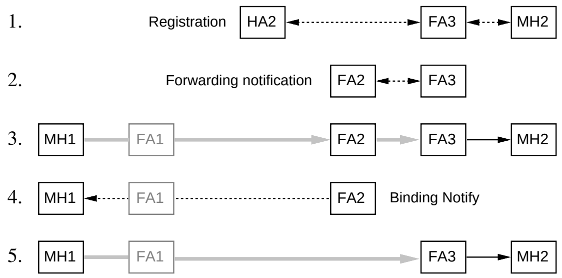


Figure 7 Mobile host movement

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 tunneled 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 tunneled 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.

VI.C. Stationary Host to Mobile Host

Figure 8 illustrates the case in which a stationary host, SH, which 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 Figure 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 the MH's known location, FA. FA decapsulates the packet and delivers it locally to MH.

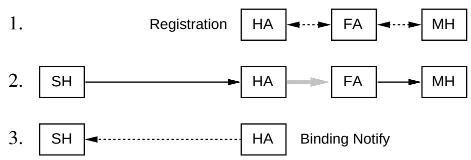


Figure 8 Stationary host to mobile host communications

3. When HA receives the packet from SH, it sends a Binding Notify to the source, 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.

VI.D. 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 Figure 9.

The following operations are shown in Figure 9:

1. If CA1 tunnels a packet destined for MH to CA2, CA2 will tunnel the packet to CA3.
2. When CA3 receives the packet, it will tunnel the packet on again to CA1.
3. The loop is broken by the Binding Notify packets that are sent to the source of each tunnel. CA2 sends a Binding Notify to CA1, and CA3 sends a Binding Notify to CA2.
4. Finally, CA1 sends a Binding Notify to CA3. Each foreign agent that receives a Binding Notify packet uses the logical timestamp to decide whether its current binding is out of date. If so, the foreign agent replaces this location cache entry, possibly after authenticating the new binding.

VII. Extensions

VII.A. 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 use a technique called *popup* [3] to maintain connectivity. The popup method applied to IMHP requires the mobile host to acquire a temporary local address from a local address server (for example, a server implementing DHCP [2]) and to then report the allocated address to its home agent as its care-of address. The mobile host, in effect, acts as its own foreign agent, using this temporary address.

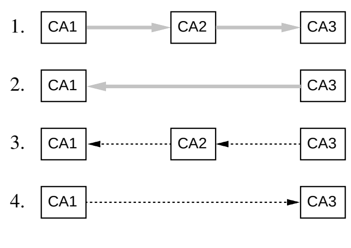


Figure 9 Routing loop resolution

If the home agent is allowed to distribute this binding to other nodes in Binding Notify messages, optimal routing of packets to the mobile host using this temporary address is possible. However, when the mobile host subsequently moves to a new network, communication to the mobile host might be lost for up to the timeout period on the location cache entry. This movement of the mobile host would appear to the correspondent hosts as a crash of the foreign agent, since no node would then be responding to this 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 the 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 method that might be used would be to monitor the source address of received broadcast packets such as ARP requests.

VII.B. Intermediate Cache Agents

Different types of intermediate agents have been suggested by a number of proposals [12, 5, 7] 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 then tunnel the packet directly to the foreign agent currently serving the destination mobile host. Intermediate routers serving as cache agents discover new bindings by snooping on IMHP Binding Notify packets as it forwards them.

VIII. 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 new 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 disrupt or usurp a data stream intended for a mobile host.

The user of the 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.

Acknowledgments

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

References

[1] R. Braden and J. Postel. Requirements for Internet Gateways. RFC 1388, June 1987.

[2] Ralph Droms. Dynamic Host Configuration Protocol. RFC 1531, October 1993.

[3] J. Ioannidis, D. Duchamp, G. Maguire, and S. Deering. Protocols for Mobile Internetworking. Internet Draft, June 1992.

[4] John Ioannidis, Dan Duchamp, and Gerald Q. Maguire Jr. IP-based Protocols for Mobile Internetworking. In *Proceedings of the SIGCOMM '91 Conference: Communications Architectures & Protocols*, pages 235–245, 1991.

[5] David B. Johnson. Transparent Internet Routing for IP Mobile Hosts. Internet Draft, July 1993.

[6] David B. Johnson. Scalable and Robust Internetwork Routing for Mobile Hosts. In *Proceedings of the 14th International Conference on Distributed Computing Systems*, June 1994.

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

[8] C. Perkins and Y. Rekhter. Support for Mobility with Connectionless Network Layer Protocols. Internet Draft, November 1992.

[9] J. Postel. Internet Control Message Protocol. RFC 792, September 1981.

[10] J. Postel. Internet Protocol. RFC 791, September 1981.

[11] F. Teraoka, Kim Claffy, and M. Tokoro. Design, implementation, and evaluation of virtual internet protocol. In *Proceedings of the 12th International Conference on Distributed Computing Systems*, pages 170–177, June 1992.

[12] Fumio Teraoka. VIP: IP Extensions for Host Migration Transparency. Internet Draft, July 1992.

[13] Fumio Teraoka, Yasuhiko Yokote, and Mario Tokoro. A Network Architecture Providing Host Migration Transparency. In *Proceedings of the SIGCOMM '91 Conference: Communications Architectures & Protocols*, pages 209–220, September 1991.

Author Information

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, and ACM.

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 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, and Sigma Xi.