Network Working Group | Mobile IP Working Group
Request for Comments: DRAFT | December 1993

Routing Support for IP Mobile Hosts

Abstract

This document specifies protocol enhancements that allow transparent routing of IP packets to and from mobile hosts in the Internet. A mobile host is always identified by its home IP address, regardless of its current point of attachment to the Internet. While situated away from its home area, a mobile host is also associated with a foreign IP address, which provides information about its current point of attachment to the Internet.

Mobility functions are defined for four entities: a) a mobile host, b) a home agent, c) a foreign agent, and d) a mobile-aware correspondent host. No protocol enhancements are required in conventional hosts or routers that are not serving in one of these roles. In particular, no additional protocols are needed by a conventional (non-mobile) host in order for it to communicate with a mobile host. Similarly, no additional protocols are needed by a conventional router (that is not acting as a home agent or a foreign agent) in order for it to route packets to or from a mobile host.

The protocols defined in this document place no additional requirements on assignment of IP addresses: that is, a mobile host will be assigned a permanent Internet address by the organization that owns it, and will be able to use that IP address regardless of its current point of attachment to the Internet.

Status of This Memo

Contents

1. Introduction

Computers are becoming smaller, less expensive, and portable. Notebooks and portable computers are on the market today that are both portable and extremely powerful. People will no longer be constrained to using their computers only in a fixed location.

At the same time, computer networking is becoming indispensable to more and more computer users. The ability to access information and communicate globally is being demanded by more and more computer users, and in the emerging environment these users will want to attach their computers to the network wherever they happen to be working, while maintaining the same level of service that they received at their desktops.

A user might usually connect to the network at their desk, but occasionally will take their computer to a conference room in another part of the building, or even at another site. However, today's IP protocol was designed under the tacit assumption that a computer is always attached to the network at a single physical location, and IP uses the IP address to identify this point of attachment. Host migration has been assumed to occur so rarely that it can be handled manually. For example, consider an IP host that is relocated from the user's desktop to a conference room. If the user's desk and the conference room have direct access to the same IP subnet, the migration process is trivial because the original IP address of the computer can still be used. However, if the user's desk and the conference room are on different subnets, then the original IP address is no longer valid. The user must acquire a new IP address from the appropriate local authority, which may not be an easy task. Then, multiple configuration files on the migrating machine, on various name servers, and on other machines that were using the original IP address to identify the migrating machine will all need to be modified. In this environment, migration tends to be a slow, error prone process, and the average user does not have the skills or the desire to carry it out.

In an environment where movement of machines from one place to another is a common occurrence, new protocols will be needed to ensure that migration can be achieved transparently, with little or no direct user involvement in the process. The emergence of wireless networks will underscore the need for ease of migration even more. When a user is no longer constrained by cable, host migration may not even be under the user's direct control. For example, the provider of a wireless RF service may move the computer's point of attachment from one cell to another, based on dynamic factors such as load and noise, even though the user has not changed the physical location of his computer.

Finally, individual networks are being interconnected into a single global network. In the Internet, users already have access to network facilities around the world. Therefore, the new protocols will need to be able to operate efficiently in both a local (intra-network) environment and a global (inter-network) environment. That is, hosts must be able to move to new locations, both within their own local network and within any of the globally interconnected networks.

2. Requirements for Mobility Support

The protocols specified in this document satisfy the following requirements:

a) A mobile host using its home IP address shall be able to communicate with other Internet hosts after having been disconnected from the internet and then reconnected at a different point.
b) A mobile host shall be capable of communicating with existing hosts that do not implement the mobility functions described in this document.
c) A mobile host shall provide at least weak security, that is, a level of security at least as good as that provided by the Internet today. See Appendix A for a general treatment of security.

3. Definitions

For this document, the following definitions apply:

Correspondent Host: The remote host with which a given host is communicating. The correspondent host may be either mobile or non-mobile.

Direct Routing: A path followed by a packet destined for a mobile host, when the packet is encapsulated by the originator and sent directly to the Foreign Agent serving the mobile host.

Foreign Agent: A host or router that will forward packets to a locally reachable mobile host that is away from its home network, is registered with the Foreign Agent, and shares a common subnet with the Foreign Agent. It supports the registration service for such hosts, and also updates the mobile host's Home Agent with the current binding of the mobile host to the Foreign Agent.

The Foreign Agent will decapsulate incoming packets. If the inner packet is addressed to a mobile host which it is currently serving, the Foreign Agent will deliver the inner packet to the mobile host.

Foreign Agent Address: The address of the Foreign Agent that is currently servicing a mobile host that is away from its home. The Foreign identifies the point of attachment of a mobile host to the Internet. The Foreign Agent Address is not related in any way to either the mobile host′s Home IP Address or the address of its Home Agent.

Foreign Subnet: Any subnet other to which a mobile host is attached, other than its home subnet.

Forwarding List: A list maintained by a Home Agent that records the mobility bindings in force, if any, for each of its mobile hosts that is away from home.

Home Agent: A host or router on a network that 1) advertises reachability for a mobile host, 2) maintains a record of the current binding between the IP address of the mobile host and the IP address of the Foreign Agent currently serving that host while it is away from home, and 3) encapsulates packets for delivery to a Foreign Agent for eventual delivery to a mobile host that is away from home.

Home IP Address: A permanent IP address that is assigned to a mobile host. It remains unchanged regardless of where the host is attached to the Internet. When a mobile host is attached to the network identified by its home address, it is said to be ″at home″ or ″in its home area″ or ″in its home network″. When it is attached to the Internet at a point not identified by its home address, then the mobile host is said to ″be away from its home network″ or ″at a foreign network″ or ″away from home″.

Home Subnet: The home subnet for a given mobile host is the subnet pointed to by the permanent IP address of that host.

Ignorant Host: A host that does not implement any of the functions described in this document; a host which does not understand or react to the elements of procedure described in this document.

Location List: A list maintained by a Foreign Agent or a Mobile Host that records mobility bindings that are in force for mobile hosts that are not currently attached to a common subnetwork with the host or agent that is maintaining this list.

Mobile Host: An IP host that implements at least the base set of functions described in this document. In cooperation with a Home Agent and a Foreign Agent, such a host is able to attach to the Internet at a point other than the one denoted by its permanent IP address.

Mobile-aware Host: A host that is able to support a Location List and provide encapsulation functions, but is not necessarily able to support registration or beaconing protocols.

Mobility Binding: The association of a mobile host with the Foreign Agent that is currently providing service to it.

Triangle Routing: A path followed by a packet destined for a mobile host, when that packet is forwarded first to the mobile host′s Home Agent and then is encapsulated and forwarded by the Home Agent to the Foreign Agent serving that host.

Visitor List: A list maintained by a Foreign Agent that records the mobility bindings in force, if any, for each mobile hosts that it is currently serving.

Weak Security: A level of security which is at least as good at that provided by the Internet today.

4. Overview of Mobility Support

IP host addresses are composed of a network number, identifying the network to which the host is attached, and a host number, identifying the particular host within that network. Because IP makes an implicit assumption that the host′s attachment point remains fixed, currently defined routing protocols select a path to a host based on the network number contained in the host′s IP address. If a host moves while keeping its IP address unchanged, its network number will not reflect its new point of attachment, and existing routing protocols will not be able to route packets to it correctly.

This document defines new functions that allow a mobile host to interoperate correctly and conveniently on the IP Internet, without the need to acquire new IP addresses as it changes its attachment point. The functions fall into several classes:

— Beaconing/Solicitation
— Registration
— Route Optimization
— Packet Forwarding/Encapsulation

The functions specified in this document apply to four entities:

a) Mobile Host
b) Mobile-aware Host
c) Home Agent
d) Foreign Agent

This paper also provides a framework on which authentication procedures can be applied to the registration and route optimization messages.

4.1 Infrastructure

The mobility protocols described in this paper are predicated upon a topology model in which:

— Home Agents and Foreign Agents are part of a static (wired) backbone: that is, their point of attachment to the Internet remains fixed
— Mobile hosts are assumed to be able to change their point of attachment to the Internet on a relatively frequent basis: that is, they are assumed to move around
— Mobile-aware hosts are assumed to be static: that is, their point of attachment to the Internet remains fixed.

This protocol does not address a topology in which Home Agents and Foreign Agents can change their attachment points on a frequent basis.

4.2 Beaconing/Solicitation Overview

To send a registration request to a specific Foreign or Home Agent, a mobile host must know the IP address of that agent. This document does not limit the means by which the mobile host can acquire this information. It does, however, define an optional dynamic method that can be used by a mobile host and a prospective agent to learn the agent's IP address.

Agents advertise their capabilities on a periodic basis on each subnet to which they allow mobile hosts to attach themselves. Alternatively, a mobile host may multicast a query over the subnet to learn if any prospective agents are present.

The procedures assume that a data link connection has been established between the agent and the mobile host on the subnet on which the beaconing and solicitation will take place. The methods used to establish such a data link connection are not specified in this document, but are left as a local option.

4.3 Registration Overview

The registration function controls the exchange and maintenance of information between mobile hosts, Foreign Agents, and Home Agents. This function creates a mobility binding, linking the mobile host's Home IP Address and the address of the Foreign Agent currently serving the mobile host. Other hosts, called correspondent hosts, communicate with a mobile host by sending it packets addressed to the mobile host's Home IP Address.

When a Mobile Host connects to the network, it must perform a registration process before packets can be delivered to it. Depending on its point of attachment, the mobile host will register with either its Home Agent or a Foreign Agent. The registration protocol defines the methods for exchanging information between the mobile host, its Home Agent, and its actual or potential Foreign Agent.

In the most common situation, a mobile host will move away from its Home Subnet and attempt to establish communication over the Foreign Subnet to which it has moved. To accomplish this, it must initiate the registration process with the Foreign agent.

The registration process involves the exchange of four messages, as illustrated in Figure 1:

a) The mobile host sends a MH_REG_REQ message to the prospective Foreign Agent to begin the registration process
b) The Foreign Agent sends a FA_REG_REQ message to the Home Agent to inform it of the mobile host's request and to ask permission from the Home Agent to provide the requested service
c) The Home Agent sends a FA_REG_REPLY message to the Foreign Agent to grant or deny permission for the Foreign Agent to provide service
d) The Foreign Agent sends an MH_REG_REPLY message to the mobile host to inform it of the disposition of its registration request.

After a successful registration, the Home Agent and Foreign Agent are both aware of the mobility binding for the mobile host. Hence, the same mobility binding will have been included in both the Home Agent's Forwarding List and the Foreign Agent's Visitor List. At this time, correspondent hosts are able to communicate with the mobile host.

A Foreign Agent must maintain a Visitor List of mobile hosts that are currently registered with itself and that share a common subnetwork with itself. In addition, it may maintain a Location List that keeps track of the prospective Foreign Agent to which a mobile host has moved.

When the Foreign Agent receives a packet addressed to itself, it can decapsulate it and consult its Visitor List and Location List. It will then take one of three actions: a) deliver the inner packet directly to a system named in its Visitor List, b) encapsulate the packet to the prospective Foreign named in the Location List, or c) hand the inner packet over for further processing by the routing protocol in use in the local Autonomous System.

The Home Agent for a given mobile host must be located on the network identified by the network number in the mobile host's Home IP Address. The Home Agent operates in conjunction with a conventional router, which advertises reachability to mobile hosts served by the Home Agent. The router attracts packets addressed to the mobile host; the Home Agent intercepts these packets and encapsulates them for delivery to the Foreign Agent, if any, currently serving the mobile host.

A Home Agent keeps a Forwarding List for its mobile hosts that are away from home, and can therefore encapsulate packets addressed to the mobile host, sending them to the Foreign Agent currently serving that mobile host.

Several possible configurations are shown in Figure 2. The home network configuration may correspond to a physical subnet or a virtual subnet:

— In (a), the home network is a physical network connected to the Internet through a router, and the Home Agent is a separate entity attached to the physical Home Network.
— In (b), the router and the Home Agent are colocated in the same system on the home network.
— In (c), the home network is a virtual network: that is, there is no actual physical home network to which the mobile host can attach itself.

CAUTION

This document does not define any message flows or elements of procedure to be used in configuration (a) between a non-colocated Home Agent and router. Such procedures are not within the scope of this document.

4.4 Forwarding and Encapsulation of Packets

After completion of the registration process, the Home Agent and the Foreign Agent each know about the current mobility binding. Acting cooperatively, they can therefore deliver packets to the mobile host using encapsulation and decapsulation.

In the base mode of operation, a correspondent host creates a packet addressed to the Home IP Address of a mobile host with which it wishes to communicate. When the mobile host is away from home and has completed the registration process, the following sequence of events will occur, as illustrated in Figure 3:

a) The conventional host will place the permanently assigned IP address of the mobile host in the packet's destination address field.
b) Conventional routing protocols will deliver the packet to the Home Agent/Router, because the router has advertised reachability to the mobile host.
c) The Home Agent/Router will intercept the packet, consult its Forwarding List, and encapsulate the packet for delivery to the Foreign Agent, using the IP address of the Foreign Agent as the destination address. (If the mobile host is at home, the Home Agent will deliver the packet to it. If the mobile host is not at home, and the Home Agent has no mobility for it, then the Home Agent will not be able to deliver the packet.)
d) Conventional routing protocols will deliver the encapsulated packet to the Foreign Agent.
e) The Foreign Agent will decapsulate the packet, see that there is an entry in its Visitor List for the mobile host, and deliver the inner packet to the mobile host, which shares a common data link medium with itself.

If the route optimization procedures have been invoked, then a prior Foreign Agent can encapsulate packets for delivery to a mobile host's new prospective Foreign Agent; and a correspondent agent can encapsulate packets destined for a given mobile host so that they will be routed directly to its Foreign Agent.

4.5 Route Optimization

Sections 10.7 through 10.10 define an optional method by which a prospective Foreign Agent can notify a mobile host's prior Foreign Agent that the mobile host is trying to register with a new Foreign Agent. Since the notification will include the prospective new mobility binding, the prior Foreign Agent can optionally forward packets destined for the mobile host to the prospective Foreign Agent.

This paper defines an optional method by which a Home Agent can inform a correspondent, mobile-aware host of the current binding in force between a destination mobile host and its Foreign Agent. Upon receiving an advertised binding, a correspondent mobile-aware host will establish its validity before using it. These procedures give the correspondent (source) host the option of encapsulating packets directly to the Foreign Agent, rather than sending it to the host's Home Agent for forwarding to the Foreign Agent. That is, it provides a method for avoiding the phenomenon of triangle routing (see Figure 4, and compare Figure 3.)

4.6 Authentication Framework

Although it does not define the specific details of the authentication processes, this paper does define a framework within which the authentication processes must work. This framework is as follows:

— No authentication framework is defined for the beaconing and solicitation process.

— Within the registration process, all messages are assumed to be "self-authenticating": that is, they contain enough information within them to provide the receiving system to authenticate the message and its sender. In other words, the authentication framework does not involve a challenge/response mechanism.

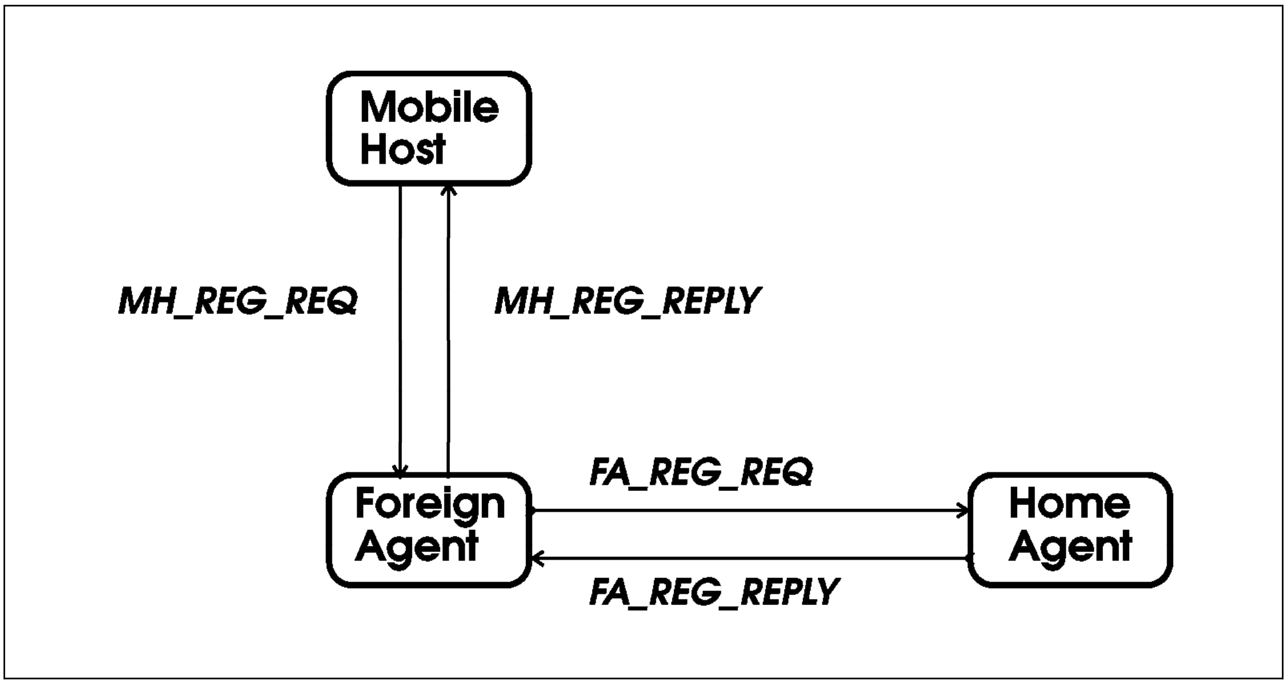

Figure 1. Flow of Registration Messages

— Within the route optimization process, the authentication model involves a challenge, followed by a response. The recipient of an advertised mobility binding will send a challenge to the mobile host named in that binding. The named mobile host, in turn, must respond positively to the challenge before the recipient can consider the binding to be valid.

The basic mechanism is illustrated in Figure 5, which shows the authentication flows involved when a Home Agent advertises a mobility binding to a correspondent host.

BRIEF DIGRESSION

An alternate strategy had been suggested: namely, that the BID_VAL message in step 2 would, in the absence of intermediate cache agents, go to the Home Agent, who could respond to it immediately instead of forwarding it to the mobile host. I did not adopt that approach because it would have required the Home Agent to parse *EVERY* incoming IP packet addressed to the mobile host--1) to see if it contained the UDP header, and 2) to see if the message behind the UDP header was in fact a BIND_VAL message.

5. Mobility Message Formats

Message formats and usage rules are defined to support the beaconing/solicitation functions, registration functions, and route optimization functions. Unless otherwise indicated, all messages are transmitted as the data portion of an IP datagram; the messages themselves are UDP datagrams. Each message carries the 8 byte each supported message type, as shown in Figure 6. UDP header, followed by specific message fields for

The types of messages are:

— Beacon/Solicitation Messages:

a) BEACON
b) SOLICIT

— Registration Messages:

a) MH_REG_REQ
b) MH_REG_REPLY
c) FA_REG_REQ
d) FA_REG_REPLY

— Route Optimization Messages:

a) BIND_ADV
b) BIND_VAL

No messages are used in support of the forwarding/encapsulation process.

All messages contain an integral number of bytes. The bytes of a message are numbered consecutively in increasing order, starting with 1. The bits within a byte are numbered from 0 to 7, where bit 0 is the high order (leftmost) bit. When consecutive bytes are used to represent a binary number, the lowest numbered byte contains the most significant binary digits.

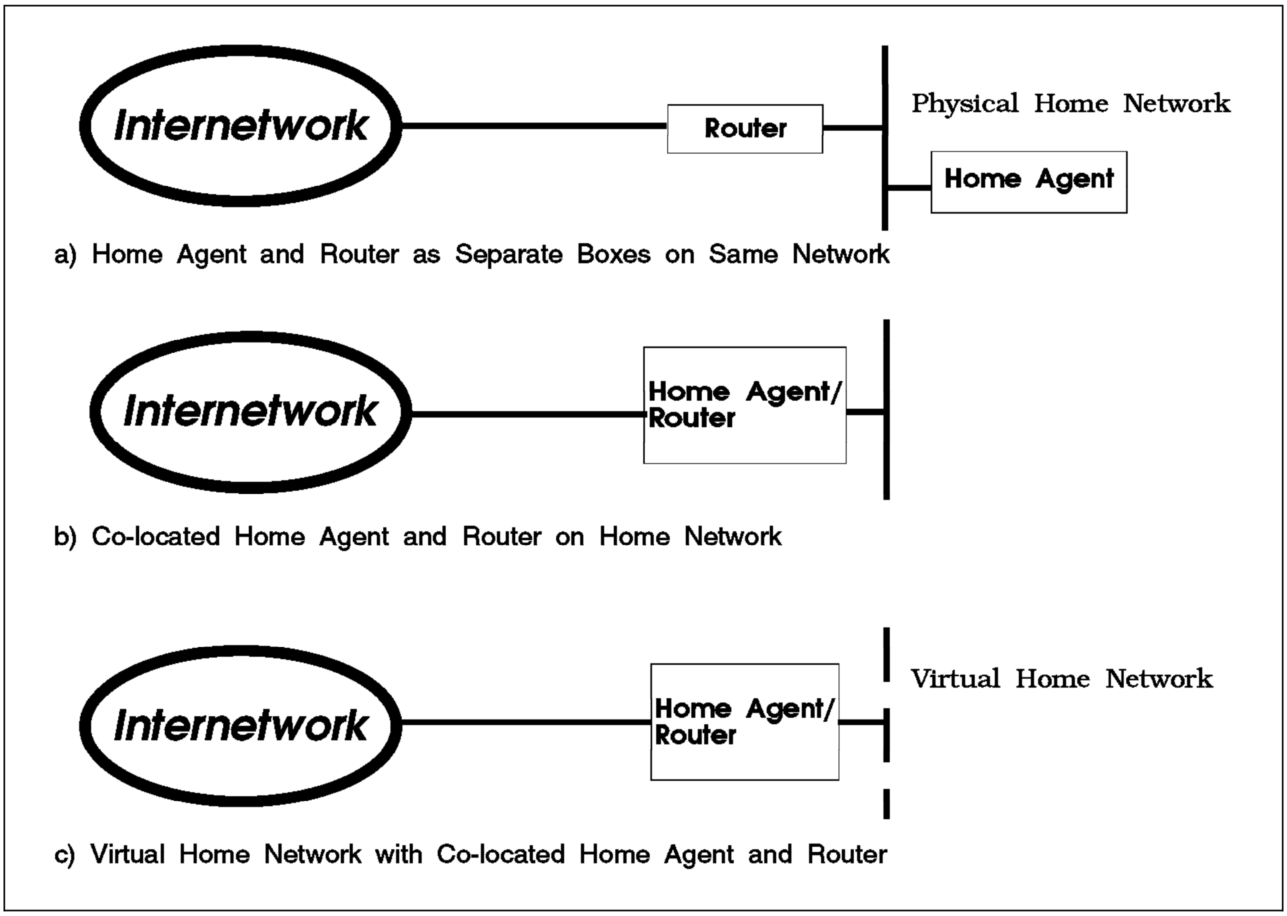

Figure 2. Home Network Configurations

Values of fields are given in decimal, and all numeric fields are unsigned, unless otherwise noted.

Each message must always contain a UDP header; the header is followed by additional data fields, which will vary by message type and which may not always be present in every message of a given type.

5.1 UDP Header

The UDP header contains 4 fields, each 2 bytes in length, that are defined in RFC 768 and are illustrated below. The UDP Destination Port shall be set to the value X′????′.

```
     0     0     1     1     1     2     2     3
     3     7     1     5     9     3     7     1
+-+-+-+-|-+-+-+-|-+-+-+-|-+-+-+-|-+-+-+-|-+-+-+-|-+-+-+-|-+-+-+-+
+ UDP Source Port               | UDP Destination Port          +
+-+-+-+-|-+-+-+-|-+-+-+-|-+-+-+-|-+-+-+-|-+-+-+-|-+-+-+-|-+-+-+-+
+ UDP Message Length            | UDP Checksum                  +
+-+-+-+-|-+-+-+-|-+-+-+-|-+-+-+-|-+-+-+-|-+-+-+-|-+-+-+-|-+-+-+-+
```

The UDP header is followed by a variable length data field whose contents are defined in the following sections for each of the supported message types.

5.2 BEACON Message

The message contains a UDP Header followed by the fields shown below:

```
     0     0     1     1     1     2     2     3
     3     7     1     5     9     3     7     1
+-+-+-+-|-+-+-+-|-+-+-+-|-+-+-+-|-+-+-+-|-+-+-+-|-+-+-+-|-+-+-+-+
+ TYPE  | OP_CODE       | INCARN_NUM . . .                      +
+-+-+-+-|-+-+-+-|-+-+-+-|-+-+-+-|-+-+-+-|-+-+-+-|-+-+-+-|-+-+-+-+
+ INCARN_NUM      (cont′d)      |
+-+-+-+-|-+-+-+-|-+-+-+-|-+-+-+-+
```

The descriptions of these fields are as follows:

TYPE: The value 1 indicates that this is an BEACON message.

OP_CODE: The value 1 indicates that this is an advertisement sent by a Home Agent; the value 2 indicates that it is an advertisement by a Foreign Agent; the value 3 indicates it is an advertisement by a system in which the Home Agent and Foreign Agent functions are both present.

INCARN_NUM: A 4 byte unsigned integer chosen by the agent and changed each time the agent is rebooted.

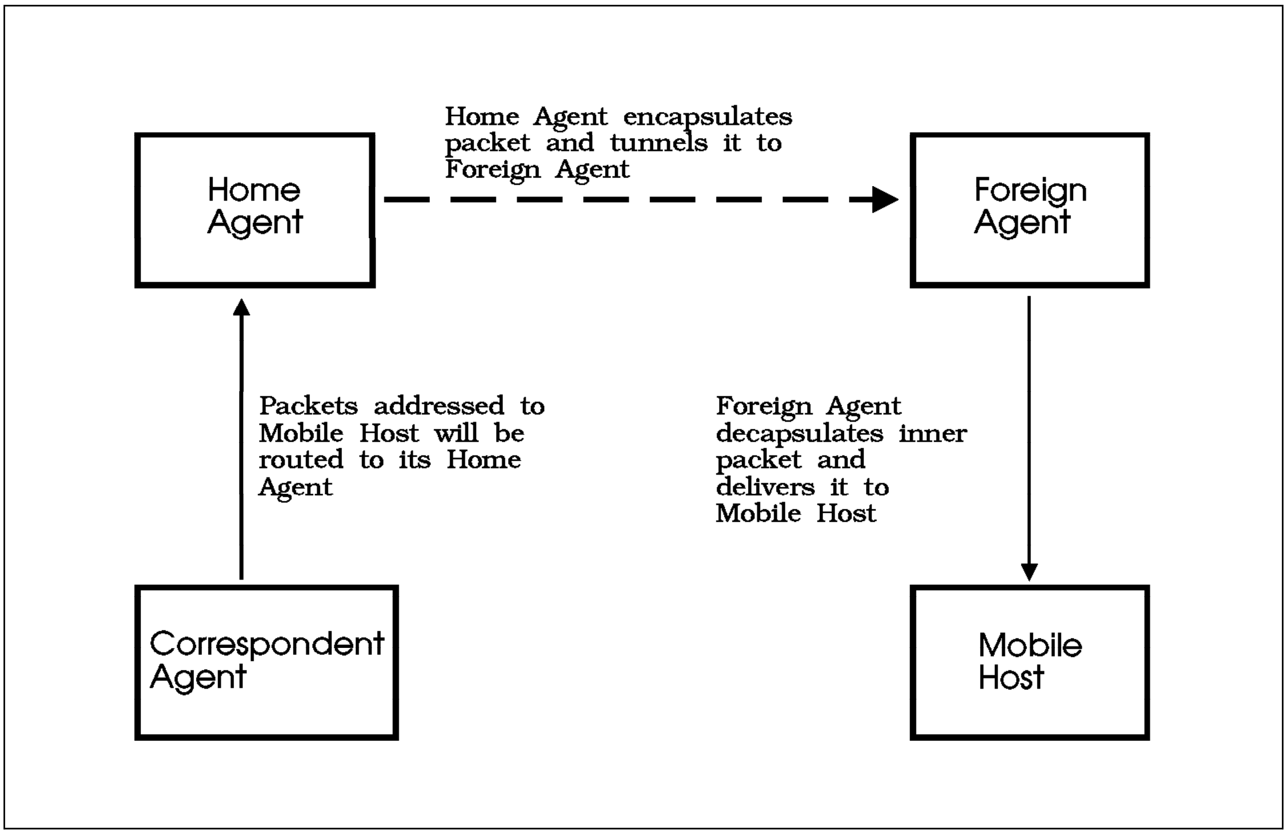

Figure 3. Tunneling a Packet to a Foreign Agent. A Home Agent will encapsulate a packet destined for a mobile host that is away from home, and will tunnel it to the appropriate Foreign Agent.

5.3 SOLICIT Message

The message contains a UDP Header followed by the additional fields shown below:

```
      0     0     1     1     1     2     2     3
      3     7     1     5     9     3     7     1
+-+-+-+-|-+-+-+-|-+-+-+-|-+-+-+-|-+-+-+-|-+-+-+-|-+-+-+-|-+-+-+-+
+ TYPE          | OP_CODE       |
+-+-+-+-+-+-+-+-|-+-+-+-|-+-+-+-|
```

The descriptions of these fields are as follows:

TYPE: The value 2 indicates that this is a SOLICIT Message.

OP_CODE: The value 1 indicates that Home Agents should replay to this Solicit message;the value 2 indicates that only Foreign Agents should reply to this message; and the value 3 indicates that either a Home Agent or a Foreign Agent can respond to this message.

5.4 MH_REG_REQ Message

The message contains a UDP header followed by the fields shown below:

```
      0     0     1     1     1     2     2     3
      3     7     1     5     9     3     7     1
+-+-+-+-|-+-+-+-|-+-+-+-|-+-+-+-|-+-+-+-|-+-+-+-|-+-+-+-|-+-+-+-+
+ TYPE       | OP_CODE       |   MH_REG_NUM                +
+-+-+-+-+-+-+-+-|-+-+-+-|-+-+-+-|-+-+-+-|-+-+-+-|-+-+-+-|-+-+-+-+
+HA_ADD_LGTH    |PFA_ADD_LGTH   |M-H_AUTH_LGTH  |M-F_AUTH_LGTH  +
+-+-+-+-|-+-+-+-|-+-+-+-|-+-+-+-|-+-+-+-|-+-+-+-|-+-+-+-|-+-+-+-+
+               HA_ADD (variable)                               +
+-+-+-+-+-+-+-+-|-+-+-+-|-+-+-+-|-+-+-+-|-+-+-+-|-+-+-+-|-+-+-+-+
+         PFA_ADD (variable)                                    +
+-+-+-+-+-+-+-+-|-+-+-+-|-+-+-+-|-+-+-+-|-+-+-+-|-+-+-+-|-+-+-+-+
+         M-H_AUTH_DATA (variable)                              +
+-+-+-+-+-+-+-+-|-+-+-+-|-+-+-+-|-+-+-+-|-+-+-+-|-+-+-+-|-+-+-+-+
+         M-F_AUTH_DATA (variable)                              +
+-+-+-+-+-+-+-+-|-+-+-+-|-+-+-+-|-+-+-+-|-+-+-+-|-+-+-+-|-+-+-+-+
```

The descriptions of these additional fields are:

TYPE: The value 3 indicates that this is a MH_REG_REQ message.

OP_CODE: The operation field consists is divided in two parts. The leftmost (high-order bits 0. 1, and 2) are used to define whether registration options are in effect, as follows:

- — If bit 0 is equal to 1, then the Prior Foreign Agent should be notified when a new registration request is initiated; if 0, no notification will be sent to the Prior Foreign Agent
- — If bit 1 is equal to 1, then the Home Agent may notify correspondent hosts of the mobility

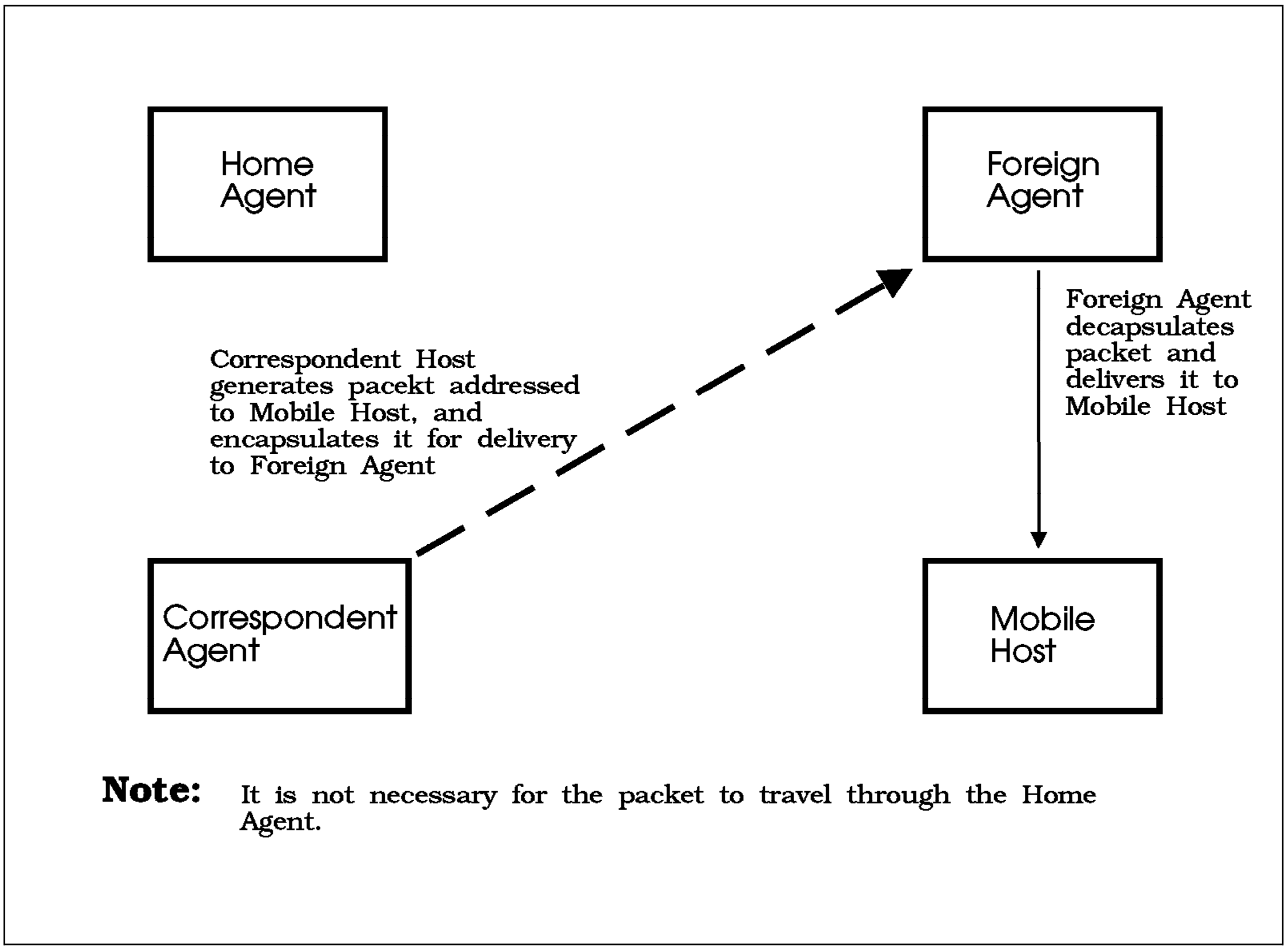

Figure 4. Avoiding Triangle Routing. A Home Agent will encapsulate a packet destined for a mobile host that is away from home, and will tunnel it to the appropriate Foreign Agent.

binding; if 0, then no binding notifications may be sent to a correspondent host

— If bit 2 is equal to 1, then this mobile host supports multiple concurrent bindings with different Foreign Agents; if 0, then the host supports only a single binding at a time.

The five rightmost (low order bits 3, 4, 5, 6, and 7) are treated as an unsigned integer code value, with the following meanings:

— 0 is a request to terminate service
— 1 is a request to initiate the registration protocol in its entirety
— 2 is a request to reconfirm an existing registration with the Home Agent
— 3 is a request to reconfirm an existing registration with the current Foreign Agent

MH_REG_NUM: This 2 byte field contains an unsigned integer whose value is the registration number associated with this message.

HA_ADD_LGTH: The unsigned integer in this field gives the length in bytes of the Home Agent's IP Address.

PFA_ADD_LGTH: The unsigned integer in this field gives the length in bytes of the Prior Foreign Agent's IP Address.

M-H_AUTH_LGTH: The unsigned integer value in this field defines the length in bytes of the Mobile-Home Authentication Data field. If set to the value 0, then the Mobile-Home Authentication Data field will not be present in the message.

M-F_AUTH_LGTH: The unsigned integer value in this field defines the length in bytes of the Foreign Authentication Data field. If set to the value 0, then the Mobile-Foreign Authentication Data field will not be present in the message.

HA_ADD: This field contains the IP address of the Home Agent with which this mobile unit is associated. This field must always be present.

M-H_AUTH_DATA: This variable length field contains data that can be used by the Home Agent to authenticate the mobile host. Both its contents and their interpretation are outside the scope of this specification.

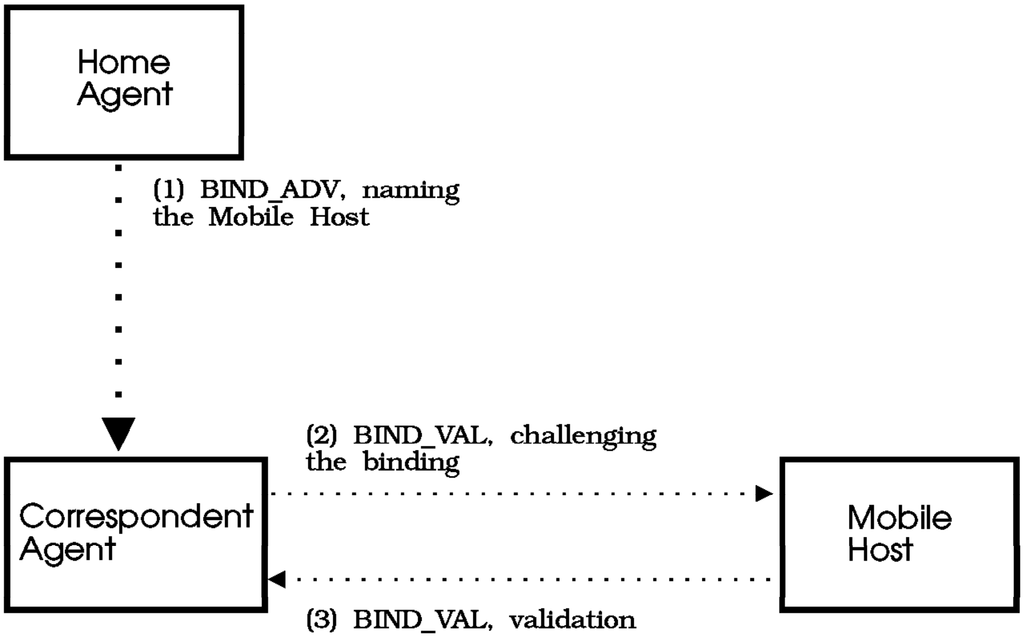

Figure 5. Authentication Example for an Advertised Binding. The Home Agent advertises the binding, which is validated by the mobile host named in the binding.

M-F_AUTH_DATA: This variable length field contains data that can be used by the Foreign Agent to authenticate the mobile host. Both its contents and their interpretation are outside the scope of this specification.

PFA_ADD: This field contains the IP address of the Foreign Agent with which the mobile unit had most recently registered. If the mobile host does not wish to disclose this information, it may set this field to X'00 00 00 00'.

5.5 MH_REG_REPLY Message

The MH_REG_REPLY message consists of a UDP header (see 5.1) followed by the fields shown below:

```
       0       0       1       1       1       2       2       3
       3       7       1       5       9       3       7       1
+-+-+-+-|-+-+-+-|-+-+-+-|-+-+-+-|-+-+-+-|-+-+-+-|-+-+-+-|-+-+-+-+
+ TYPE          | OP_CODE         | MH_REG_NUM                  +
+-+-+-+-+-+-+-+-|-+-+-+-|-+-+-+-|-+-+-+-|-+-+-+-|-+-+-+-|-+-+-+-+
+FA_SVC_LIFE                     | HA_SVC_LIFE                  +
+-+-+-+-|-+-+-+-|-+-+-+-|-+-+-+-|-+-+-+-|-+-+-+-|-+-+-+-|-+-+-+-+
+A-H_AUTH_LGTH  |H-H_AUTH_LGTH   | A-H_AUTH_DATA....            +
+-+-+-+-|-+-+-+-|-+-+-+-|-+-+-+-|-+-+-+-|-+-+-+-|-+-+-+-|-+-+-+-+
+         A-H_AUTH_DATA (cont'd)                                +
+-+-+-+-+-+-+-+-|-+-+-+-|-+-+-+-|-+-+-+-|-+-+-+-|-+-+-+-|-+-+-+-+
+         H-H_AUTH_DATA (variable)                              +
+-+-+-+-+-+-+-+-|-+-+-+-|-+-+-+-|-+-+-+-|-+-+-+-|-+-+-+-|-+-+-+-+
```

The descriptions of these additional fields are:

TYPE: The value 4 indicates that this is an MH_REG_REPLY message.

OP_CODE: The operation codes shown below are supported; codes not shown are reserved for future use.

CODE	**OPERATION**
0	Service will be provided
1	Service denied: reason unspecified
2	Service denied: foreign agent has insufficient resources available
3	Service denied: authentication failure with Home Agent

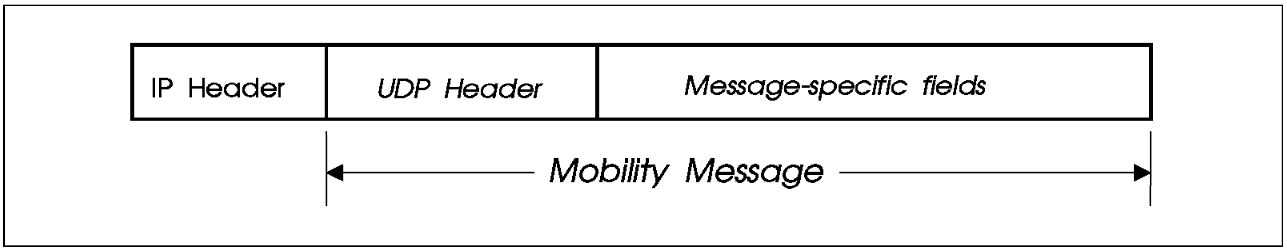

Figure 6. Message Structure

4	Service denied: authentication failure with Foreign Agent
5	Registration pending

MH_REG_NUM: This 2 byte field contains an unsigned integer whose value is the registration number associated with this message.

FA_SVC_LIFE: This 2 byte field contains an unsigned integer whose value is equal to the number of seconds that the Foreign Agent will provide service to the mobile host without receiving a reconfirmation.

HA_SVC_LIFE: This 2 byte field contains an unsigned integer whose value is equal to the number of seconds that the Home Agent will provide encapsulation and forwarding service to a mobile host away from home without receiving a reconfirmation.

A-H_AUTH_LGTH: The unsigned integer value in this field defines the length in bytes of the Agent-Host Authentication Data field. A value of 0 indicates that the Agent-Host Authentication Data field is not present.

H-H_AUTH_LGTH: The unsigned integer value in this field defines the length in bytes of the Agent-Host Authentication Data field. A value of 0 indicates that the Host-Home Authentication Data field is not present.

A-H_AUTH_DATA: This variable length field contains data that can be used by the mobile host to authenticate the Agent. Both its contents and their interpretation are outside the scope of this specification.

H-H_AUTH_DATA: This variable length field contains data that can be used by the mobile host to authenticate the Agent. Both its contents and their interpretation are outside the scope of this specification.

5.6 FA_REG_REQ Message

The FA_REG_REQ message consists of the UDP Header (5.1) and the following additional fields:

```
       0       0       1       1       1       2       2       3
       3       7       1       5       9       3       7       1
+-+-+-+-|-+-+-+-|-+-+-+-|-+-+-+-|-+-+-+-|-+-+-+-|-+-+-+-|-+-+-+-+
+ TYPE            | OP_CODE         | MH_REG_NUM                +
+-+-+-+-+-+-+-+-|-+-+-+-|-+-+-+-|-+-+-+-|-+-+-+-|-+-+-+-|-+-+-+-+
+MH_ADD_LGTH      |F-H_AUTH_LGTH    |H-H_AUTH_LGTH    | MH_ADD ...+
+-+-+-+-|-+-+-+-|-+-+-+-|-+-+-+-|-+-+-+-|-+-+-+-|-+-+-+-|-+-+-+-+
+...MH_ADD (cont'd)                                             +
+-+-+-+-|-+-+-+-|-+-+-+-|-+-+-+-|-+-+-+-|-+-+-+-|-+-+-+-|-+-+-+-+
+       F-H_AUTH_DATA (variable)                                +
+-+-+-+-+-+-+-+-|-+-+-+-|-+-+-+-|-+-+-+-|-+-+-+-|-+-+-+-|-+-+-+-+
+       H-H_AUTH_DATA (variable)                                +
+-+-+-+-+-+-+-+-|-+-+-+-|-+-+-+-|-+-+-+-|-+-+-+-|-+-+-+-|-+-+-+-+
```

The description of these fields are:

TYPE: The value 5 indicates that this is a FA_REG_REQ message.

OP_CODE: The operation field consists is divided in two parts. The leftmost (high-order bits 0. 1, and 2) are used to define whether registration options are in effect, as follows:

- If bit 0 is equal to 1, then the Prior Foreign Agent should be notified when a new registration request is initiated; if 0, no notification will be sent to the Prior Foreign Agent
- If bit 1 is equal to 1, then the Home Agent may notify correspondent hosts of the mobility binding; if 0, then no binding notifications may be sent to a correspondent host
- If bit 2 is equal to 1, then this mobile host supports multiple concurrent bindings with different Foreign Agents; if 0, then the host supports only a single binding at a time.

The five rightmost (low order bits 3, 4, 5, 6, and 7) are treated as an unsigned integer code value, with the following meanings:

- 0 is a request to terminate service
- 1 is a request to initiate a new registration
- 2 is a request to reconfirm an existing registration with the Home Agent

MH_REG_NUM: This 2 byte field contains an unsigned integer whose value is the registration number associated with this message.

MH_ADD_LGTH: This field contains an unsigned integer giving the length in bytes of the Mobile Address field.

F-H_AUTH_LGTH: The unsigned integer value in this field defines length in bytes of the Foreign-Home Authentication Data Field.

H-H_AUTH_LGTH: The unsigned integer value in this field defines length in bytes of the Host-Home Authentication Data Field. This field must be present. A value of 0 indicates that the Mobile-Home Authentication Data field will not be present.

MH_ADD: This field contains the Home IP Address of the mobile unit on whose behalf the Foreign Agent is acting. It must be present. This field must be present. A value of 0 indicates that the Foreign-Home Authentication Data field will not be present.

F-H_AUTH_DATA: This variable length field contains data that can be used by the Home Agent to authenticate the Foreign Agent. Both its contents and their interpretation are outside the scope of this specification.

H-H_AUTH_DATA: This variable length field contains data that can be used by the Home Agent to authenticate the mobile host. Both its contents and their interpretation are outside the scope of this specification.

5.7 FA_REG_REPLY Message

The FA_REG_REPLY message contains a UDP header (see 5.1) followed by additional fields.

```
      0      0      1      1      1      2      2      3
      3      7      1      5      9      3      7      1
+-+-+-+-|-+-+-+-|-+-+-+-|-+-+-+-|-+-+-+-|-+-+-+-|-+-+-+-|-+-+-+-+
+ TYPE          | OP_CODE       | MH_REG_NUM                    +
+-+-+-+-+-+-+-+-|-+-+-+-|-+-+-+-|-+-+-+-|-+-+-+-|-+-+-+-|-+-+-+-+
+   HA_SVC_LIFE                 |H-F_AUTH_LGTH  |H-H_AUTH_LGTH  +
+-+-+-+-|-+-+-+-|-+-+-+-|-+-+-+-|-+-+-+-|-+-+-+-|-+-+-+-|-+-+-+-+
+MH_ADD_LGTH    |   MH_ADD....(variable)                        +
+-+-+-+-+-+-+-+-|-+-+-+-|-+-+-+-|-+-+-+-|-+-+-+-|-+-+-+-|-+-+-+-+
+ ... H-F_AUTH_DATA (variable)                                  +
+-+-+-+-+-+-+-+-|-+-+-+-|-+-+-+-|-+-+-+-|-+-+-+-|-+-+-+-|-+-+-+-+
+     ...H-H_AUTH_DATA (variable)                               +
+-+-+-+-+-+-+-+-|-+-+-+-|-+-+-+-|-+-+-+-|-+-+-+-|-+-+-+-|-+-+-+-+
```

The description of these fields are:

TYPE: The value 6 indicates that this is a FA_REG_REPLY message.

OP_CODE: The operation codes shown below are supported; codes not shown are reserved for future use.

CODE	**OPERATION**
0	Permission granted
1	Permission denied: reason unspecified
2	Permission denied: authentication failure with Foreign Agent
3	Permission denied: authentication failure with mobile host
4	Permission denied: mobile host failed to reconfirm existing registration

MH_REG_NUM: This 2 byte field contains an unsigned integer whose value is the registration number associated with this message.

HA_SVC_LIFE: This 2 byte field contains an unsigned integer whose value is equal to the number of seconds that the Home Agent will provide encapsulation and forwarding service to a mobile host away from home without receiving a reconfirmation. It may not be present in all messages.

H-F_AUTH_LGTH: The unsigned integer value in this field defines the length in bytes of the Home-Foreign Authentication Data field. This field must be present. A value of 0 indicates that the Home-Foreign Authentication Data field is not present.

H-H_AUTH_LGTH: The unsigned integer value in this field defines the length in bytes of the Home-Host Authentication Data field. This field must be present. A value of 0 indicates that the Home-Host Authentication Data field is not present.

MH_ADD_LGTH: The unsigned integer value gives the length in bytes of the Mobile Address field.

MH_ADD: This field contains the Home IP Address of the mobile host.

H-F_AUTH_DATA: This variable length field contains data that can be used by the Foreign Agent to authenticate the Home Agent. Both its contents and their interpretation are outside the scope of this specification.

H-H_AUTH_DATA: This variable length field contains data that can be used by the Foreign Agent to authenticate the Home Agent. Both its contents and their interpretation are outside the scope of this specification.

5.8 BIND_ADV Message

The message contains a UDP header (see 5.1) followed by additional fields, as shown:

```
      0      0      1      1      1      2      2      3
      3      7      1      5      9      3      7      1
+-+-+-+-|-+-+-+-|-+-+-+-|-+-+-+-|-+-+-+-|-+-+-+-|-+-+-+-|-+-+-+-+
+ TYPE          | OP_CODE       | MH_REG_NUM                    +
+-+-+-+-+-+-+-+-|-+-+-+-|-+-+-+-|-+-+-+-|-+-+-+-|-+-+-+-|-+-+-+-+
+   BIND_LIFE                   |FA_ADD_LGTH    |MH_ADD_LGTH    +
+-+-+-+-|-+-+-+-|-+-+-+-|-+-+-+-|-+-+-+-|-+-+-+-|-+-+-+-|-+-+-+-+
+AUTH_LGTH      |   FA_ADD (variable)...                        +
+-+-+-+-+-+-+-+-|-+-+-+-|-+-+-+-|-+-+-+-|-+-+-+-|-+-+-+-|-+-+-+-+
+  ...                  | MH_ADD...(variable)                   +
+-+-+-+-+-+-+-+-|-+-+-+-|-+-+-+-|-+-+-+-|-+-+-+-|-+-+-+-|-+-+-+-+
+  ...          | AUTH_DATA...(variable)                        +
+-+-+-+-+-+-+-+-|-+-+-+-|-+-+-+-|-+-+-+-|-+-+-+-|-+-+-+-|-+-+-+-+
```

The description of these fields are:

TYPE: The value 7 indicates that this is a BIND_ADV Message.

OP_CODE: The following operation codes are defined:

- **0** Advertisement from Home Agent to mobile-aware correspondent host
- **1** Advertisement from prospective Foreign Agent to Prior Foreign Agent that mobile host is attempting to register
- **2** Binding implied by decapsulation is not supported by this system

BIND_LIFE: This 2 byte field contains an unsigned integer whose value is equal to the maximum amount of time, in seconds, during which the binding contained in this message may be assumed to be valid.

FA_ADD_LGTH: This field contains an unsigned integer that gives the length in bytes of the Foreign Agent IP Address field.

MH_ADD_LGTH: This field contains an unsigned integer that gives the length in bytes of the Home IP Address field.

FA_ADD: This field contains the Foreign Agent's IP Address.

MH_ADD: This field contains the Home IP Address of the mobile host.

AUTH_LGTH: The unsigned integer value in this field defines the length in bytes of the Authentication Data field. This field must be present. A value of 0 indicates that the Authentication Data field is not present.

AUTH_DATA: This variable length field contains data that can be used by the recipient of this message to authenticate the sender of this message. Both its contents and their interpretation are outside the scope of this specification.

5.9 BIND_VAL Message

The BIND_VAL message contains a UDP header (see 5.1) followed by additional fields, as shown:

```
        0       0       1       1       1       2       2       3
        3       7       1       5       9       3       7       1
+-+-+-+-|-+-+-+-|-+-+-+-|-+-+-+-|-+-+-+-|-+-+-+-|-+-+-+-|-+-+-+-+
+ TYPE          | OP_CODE       | MH_REG_NUM                    +
+-+-+-+-+-+-+-+-|-+-+-+-|-+-+-+-|-+-+-+-|-+-+-+-|-+-+-+-|-+-+-+-+
+   BIND_LIFE                   |FA_ADD_LGTH    |MH_ADD_LGTH    +
+-+-+-+-|-+-+-+-|-+-+-+-|-+-+-+-|-+-+-+-|-+-+-+-|-+-+-+-|-+-+-+-+
+AUTH_LGTH      |  FA_ADD (variable)...                         +
+-+-+-+-+-+-+-+-|-+-+-+-|-+-+-+-|-+-+-+-|-+-+-+-|-+-+-+-|-+-+-+-+
+  ...                  | MH_ADD...(variable)                   +
+-+-+-+-+-+-+-+-|-+-+-+-|-+-+-+-|-+-+-+-|-+-+-+-|-+-+-+-|-+-+-+-+
+  ...          | AUTH_DATA...(variable)                        +
+-+-+-+-+-+-+-+-|-+-+-+-|-+-+-+-|-+-+-+-|-+-+-+-|-+-+-+-|-+-+-+-+
```

The description of these fields are:

TYPE: The value 8 indicates that this is a BIND_VAL message.

OP_CODE: The following operation codes are defined:

- **0** Challenge to sender of BIND_ADV Message host
- **1** Positive Response to Challenge
- **2** Negative response to Challenge

BIND_LIFE: This 2 byte field contains an unsigned integer whose value is equal to the maximum amount of time, in seconds, during which the binding contained in this message may be assumed to be valid.

FA_ADD_LGTH: This field contains an unsigned integer that gives the length in bytes of the Foreign Agent IP Address field.

MH_ADD_LGTH: This field contains an unsigned integer that gives the length in bytes of the Home IP Address field.

FA_ADD: This field contains the Foreign Agent's IP Address.

MH_ADD: This field contains the Home IP Address of the mobile host.

AUTH_LGTH: The unsigned integer value in this field defines the length in bytes of the Authentication Data field. This field must be present. A value of 0 indicates that the Authentication Data field is not present.

AUTH_DATA: This variable length field contains data that can be used by the recipient of this message to authenticate the sender of this message. Both its contents and their interpretation are outside the scope of this specification.

6. Message Usage

6.1 Message Rejection

All messages contain a UDP checksum, and may optionally contain data fields that can be used for authentication. A mobile host, Home Agent, or Foreign Agent that receives a message with an incorrect UDP checksum or with authentication data that is incorrect with respect to the authentication procedures in force between the message originator and the message recipient shall ignore such messages.

6.2 Beaconing and Solicitation Messages

The beaconing and solicitation procedures are carried out between a mobile host and a prospective agent. After establishing a data link connection on a given subnet that supports the attachment of mobile host, the host must learn if there are any prospective Foreign Agents available to serve it when it is away from home. If the mobile host is returning home, it must learn if its Home Agent is available to serve it.

This exchange of information is accomplished through the BEACON message and the SOLICIT message.

Home Agents and Foreign Agents must be able to 1) generate BEACON messages, and 2) receive and respond to SOLICIT messages.

Mobile hosts must be able to receive BEACON messages; as an option, mobile hosts may also generate SOLICIT messages.

6.2.1 BEACON Messages

The BEACON message informs mobile hosts about the existence of the agent, its address, and its capabilities. The BEACON is used in two ways:

a) Unsolicited Advertisement: In the absence of any specific request from a mobile host, Foreign Agents and Home Agents must broadcast a BEACON message periodically on each subnet to which they allow mobile hosts to attach themselves. The periodicity of the BEACON messages is not defined by this document, but should be chosen to be consistent with the properties of the subnet over which it will be carried.
b) Solicited Advertisement: In response to an explicit request from a mobile host via a Host Solicit message, the agent shall respond as soon as possible with a BEACON message. The Operation field of the SOLICIT message specifies the type of agent that should reply to the SOLICIT message.

The advertising agent shall set the OP_CODE field of the BEACON message to match its capabilities, and shall include its incarnation number in the Incarnation Number field. The Incarnation Number shall remain unchanged between successive boots of the agent, and shall be changed upon reboot. The methods used by the agent to select an incarnation number are a local option not specified by this document.

The source address of the IP packet that carries the BEACON message shall contain the IP address of the advertising agent; the destination address shall be "_____", indicating all hosts on the subnet.

6.2.2 SOLICIT Messages

The mobile host can, but is not required to, send out a SOLICIT message if it has not heard a BEACON within a reasonable amount of time after establishing a data link connection on the subnet. By sending the SOLICIT message, a mobile host can request the prospective agent, if any, to respond immediately, rather than waiting until the next periodic broadcast of the BEACON message would take place.

A mobile host sends out a SOLICIT message on the subnetwork to which it is attached. The response to this message, if any, will be a BEACON message.

The OP_CODE field of the SOLICIT message shall be set to indicate if the mobile host is seeking to learn about Home Agents only, Foreign Agents only, or both.

The source address of the IP packet that carries the SOLICIT message shall use the Home IP Address of the mobile host as its source address; it shall use X'____', indicating all agents on the subnet, as its destination address.

QUESTION

Is there such a multicast address defined for IP? We need to reach the prospective agents before the host knows the network number of the subnet, and we need to limit the multicast to just a single subnet.

6.3 Registration Messages

The registration process is carried out cooperatively by the mobile host, its Foreign Agent, and its Home Agent. The messages exchanged among the participants are: MH_REG_REQ messages, MH_REG_REPLY messages, FA_REG_REQ Messages, and FA_REG_REPLY messages.

6.3.1 MH_REG_REQ Message

Home Agents and Foreign Agents must multicast a BEACON message to all (prospective) hosts on each subnetwork to which mobile hosts may attach themselves. The periodicity of the advertisement is not constrained by this document. It should be chosen by the advertiser to be consistent with the type of subnet over which it will be carried.

A mobile host uses a MH_REG_REQ message for several purposes:

— Whenever a mobile host changes its point of attachment to the Internet, it must initiate the registration process. If it is away from home, it must register with a Foreign Agent; if it is returning home, it must register with its Home Agent.
— If a mobile host detects a change in the Incarnation Number of the Foreign Agent with which it is registered, it must initiate a new registration with that Foreign Agent
— A mobile host must reconfirm an existing registration with its Home Agent and its Foreign Agent before the respective service lifetime expires
— A mobile host can ask a Foreign Agent to stop providing service to itself

6.3.1.1 Registration Request When Away From Home

The mobile host initiates the registration process by sending a MH_REG_REQ message to the prospective Foreign Agent. The IP packet carrying the MH_REG_REQ message uses the mobile host's Home IP address as the source and the Foreign Agent's IP address as the destination.

The message (described in section 5.4) must include all of the following fields: Type Code, Operation, Registration Number, the four length fields, and the Home Agent IP Address field. The remaining fields are only present if the corresponding length field is non-zero.

The mobile host shall set bits 0, 1, and 2 of the Operation field according to its local policy, and shall set bits 3 through 7 to indicate a request to initiate the registration protocol in its entirety. When bit 0 of the Operation field is equal to zero, then the Prior Foreign Agent Length field must be set to the value 0.

The value in the Registration Number field shall be incremented by 1. This will be the normal case as the mobile host moves from one point of attachment to another. However, if the immediately prior registration number is unknown (for example, immediately after the host is rebooted), the registration number shall be set to the value 0.

If the mobile host and its Home Agent have previously agreed to use a specific authentication procedure, then the mobile unit will put the appropriate data in the MH_AUTH_LGTH and the MH_AUTH_DATA fields. Otherwise, the MH_AUTH_LGTH field shall be set to the value 0, and the MH_AUTH_DATA field will not be present in the message.

If the mobile host and the prospective Foreign Agent have previously agreed to use a specific authentication procedure, then the mobile unit will put the appropriate data in the M-F_AUTH_LGTH and the M-F_AUTH_DATA fields. Otherwise, the M-F_AUTH_LGTH field shall be set to the value 0, and the M-F_AUTH_DATA field will not be present in the message.

6.3.1.2 Registration Request When At Home

A mobile host at times will need to attach itself to its home subnet. Since a mobile host that is at home has no Foreign Agent, an abbreviated registration procedure is used between the mobile host and its Home Agent.

The mobile host will send a MH_REG_REQ message to its Home Agent. The IP packet carrying the MH_REG_REQ message uses the mobile host's Home IP address as the source and the Home Agent's IP address as the destination.

The contents of the MH_REG_REQ message are the same as described in section 6.3.1.1 with one exception: since no Foreign Agent is involved, the M-F_AUTH_LGTH field shall be set to the value 0, and the M-F_AUTH_DATA field will not be present in the message.

6.3.1.3 Reconfirming an Existing Registration

A mobile host that has successfully completed the registration procedure has been informed of its Home Service Lifetime and its Foreign Service Lifetime. If the mobile host has not reconfirmed its registration with the Home Agent or Foreign Agent before the respective service lifetime expires, then service will be terminated. Therefore, to continue to receive service, the mobile host must reconfirm its registration in a timely fashion. A successful reconfirmation will assign a new service lifetime to the mobile host.

The mobile host reconfirms an existing registration with its Foreign Agent by sending a MH_REG_REQ to the Foreign Agent, setting the value of the five low-order bits of the Operation field to the value 3 (reconfirmation with Foreign Agent). Similarly, a mobile host reconfirms its registration with its Home Agent by a MH_REG_REQ to the Home Agent, setting the five low-order bits of the Operation field to the value 2 (reconfirmation with Home Agent).

The MH_REG_NUM field carried in the MH_REG_REQ message shall be set to the same value that was used in the original registration request. Since the mobile host has not changed Foreign Agents, the PFA_ADD_LGTH field shall be set to zero. Since the Home Agent is not involved in the reconfirmation the MH_ADD_LGTH field shall be set to zero. The M-F_AUTH_LGTH and M-F_AUTH_DATA fields shall be set in accordance with the authentication procedures in force.

6.3.1.4 Requesting Termination of Service

A mobile host can use a MH_REG_REQ message to inform a Foreign Agent that it no longer wishes to use its services. The Operation field shall be set to 0, and the MH_REG_NUM field shall contain the current registration number. The MH_ADD_LGTH field, PFA_ADD_LGTH field, and the M-H_AUTH_LGTH field shall all be set to 0. The M-F_AUTH_LGTH field and M-F_AUTH_DATA field shall be set in accordance with the security procedures in force between the mobile host and the Foreign Agent.

6.3.2 MH_REG_REPLY Message

This message is sent by a Home Agent or a Foreign Agent to a mobile unit to inform the mobile unit if a pending request for service has been accepted or denied. It contains data that can be used to authenticate the agent to the mobile host. It also contains information telling the mobile unit how long it can expect to be serviced by the agent before needing to reconfirm its registration.

Since the MH_REG_REPLY message is carried with an IP packet, the header of the IP packet will use the agent's IP address as the source, and will use the mobile unit's Home IP address as the

The MH_REG_REPLY message can be sent by either a Home Agent or a Foreign Agent to a mobile host that shares a subnet with it. It is used to inform the mobile host about the status of a registration:

— it informs the mobile host if a registration request has been accepted or denied
— it informs the mobile request if a registration request is in the process of being acted upon

6.3.2.1 Confirmation to a Mobile Host at Home

After receiving a MH_REG_REQ from a mobile host that is at home, the Home Agent informs the mobile request of the progress of that request by means of an MH_REG_REPLY message. The OP_CODE field indicates the disposition of the registration request. The FA_SVC_LIFE filed shall be set to 0; the HA_SVC_LIFE field shall be set in accordance with the Home Agent's policy. The A-H_AUTH_LGTH field shall be set to 0, and the H-H_AUTH_LGTH and H-H_AUTH_DATA fields shall be set in accordance with the authentication policy in force.

6.3.2.2 Confirmation to a Mobile Host Away from Home

A Foreign Agent will generate an MH_REG_REPLY message either in response to a FA_REG_REPLY message or because the Foreign Agent wished to withdraw service from an already attached mobile host.

Since the MH_REG_REPLY message is carried with an IP packet, the header of the IP packet will use the Foreign Agent's IP address as the source, and will use the mobile host's IP address as the destination. The OP_CODE field in the header of the MH_REG_REPLY message shall be set by the Foreign Agent to indicate the whether it will provide service to the mobile host. If service will not be provided, then the Foreign Agent may, as a local option. use code 1 ("reason unspecified") in all cases, rather than replying with the specific reason for denying the service.

6.3.3 FA_REG_REQ Message

This message is generated by a Home Agent in response to a previous FA_REG_REQ message. It is used by the Home Agent to grant or refuse permission to the Foreign Agent to provide services to the mobile host, in the case where the Foreign Agent has requested permission to service the mobile host. If permission is granted, the Home Agent will inform the Foreign Agent of the time interval during which permission is in force (HA_SVC_LIFE field).

The message carries information that will allow the Home Agent to authenticate itself to the Foreign Agent and to the mobile host which is requesting service from the Foreign Agent.

When the FA_REG_REQ message has informed the Home Agent that the Foreign Agent is no longer servicing the mobile host, the Home Agent need not respond.

A Foreign Agent uses the FA_REG_REQ message for several purposes:

— To ask permission from the Home Agent to provide service to one of its mobile hosts
— To request permission to continue to provide service to an already registered mobile host
— To inform the Home Agent that it is no longer providing service to a given mobile host

6.3.3.1 Requesting Permission to Provide Service

A Foreign Agent that wishes to provide service to a newly registering mobile host must obtain permission to do so from the mobile host's home agent. It requests permission by sending a Foreign-Home Update message to the Home Agent whose address was carried in the Home Agent IP Address field of the MH_REG_REQ message that started the registration process.

The format of the FA_REG_REQ message is described in section 5.6. The Operation field shall be set to the value 1. The MH_REG_NUM field shall be set to the value that was carried in the MH_REG_NUM field of the MH_REG_REQ message.

The MH_ADD field shall contain the mobile unit's IP address (that is, the IP source address that was used in the IP packet that carried the MH_REG_REQ message).

If the Foreign Agent and the Home Agent have previously agreed to use a specific authentication procedure, then the Foreign Agent will put the appropriate data in the F-H_AUTH_LGTH and the F-H_AUTH_DATA fields. Otherwise, the F-H_AUTH_LGTH field shall be set to the value 0, and the F-H_AUTH_DATA field will not be present in the message. The contents of the H-H_AUTH_LGTH and

H-H_AUTH_DATA fields shall be copied from the corresponding fields of the MH_REG_REQ message that initiated the registration process.

6.3.3.2 Termination of Service

When a Foreign Agent stops providing service to a mobile host, it shall inform the mobile host's Home Agent by means of a Foreign-Home Update message whose OP_CODE field is set to 0 (service no longer being provided). The update must include the mobile host's Home IP Address and registration number. The F-H_AUTH_LGTH and F-H_AUTH_DATA fields shall be set in accordance with the authentication policies in force. The H-H_AUTH_LGTH field shall be set to 0.

6.3.4 FA_REG_REPLY Message

The FA_REG_REPLY message is sent from a Home Agent to a Foreign Agent. This message will be issued in response to requests from a Foreign Agent to begin providing service to a mobile host. The disposition of the request is contained in the OP_CODE field of the FA_REG_REPLY message. The information in the MH_REG_NUM field and the MH_ADD field are derived from the equivalent information in the MH_REG_REQ message which is being answered.

6.4 Routing Optimization Messages

6.4.1 BIND_ADV Message

The BIND_ADV message is used to advertise mobility bindings:

- A prospective Foreign Agent can advertise to the Prior Foreign Agent that a given mobile host has initiated the registration process with the new prospective Foreign Agent. This will allow the prior Foreign Agent to encapsulate and forward packets to the New Foreign Agent, rather than sending them back to the Home Agent for encapsulation and subsequent delivery.
- A Home Agent can advertise to a correspondent host the current mobility binding for a given mobile host. This information will allow a correspondent host the option of encapsulating a packet destined for a given mobile host and sending it directly to the appropriate Foreign Agent, rather than relying on an indirect route where the Home Agent provides the encapsulation function.

6.4.1.1 Notifying a Prior Foreign Agent

When a mobile host requests a prospective Foreign Agent to begin the registration procedure, bit 0 of the Operation field of the Mobile Request message will indicate whether the prospective Foreign Agent should notify the prior Foreign Agent that a new registration has been requested.

If notification is requested, then the prospective Foreign Agent must send a BIND_ADV message to the prior Foreign Agent whose IP address was carried in PFA_ADD field of the MH_REG_REQ message. The prospective Foreign Agent shall include its own IP address in the FA_ADD field of the message and shall include the mobile host's Home IP Address in the MH_ADD field. The amount of time that the Prior Foreign Agent can make use of the advertised mobility binding is specified in the BIND_LIFE field. Authentication fields shall be included in accordance with the authentication policy in force between the prospective Foreign Agent and the Prior Foreign Agent.

The MH_REG_NUM field shall contain the registration number used by the mobile host in its registration request to the prospective Foreign Agent. Information placed in the authentication fields shall be in accordance with the authentication policies in force between the prospective and the prior Foreign Agents.

QUESTION

This mode of operation allows the prospective Foreign Agent to notify the Prior Foreign Agent before the new registration request has been approved by the Home Agent. Should we place a very tight upper limit on the Binding Lifetime--that is, not much bigger than the roundtrip time for the prospective FA to request permission from the HA and get back an answer?

6.4.1.2 Notifying a Correspondent Host

Because a Home Agent advertises reachability for its mobile hosts, both when they are at home and when they are away, IP packets whose destination address is that of a mobile host will be routed along a path that takes them to the Home Agent for that host. If the mobile host is away from home and the Home Agent is aware of its current binding, then the Home Agent will encapsulate the original packet for delivery to the Foreign Agent serving that host.

The Home Agent may also optionally inform the correspondent host of the mobile host's current mobility binding, thus affording it an opportunity to encapsulate the packet for direct delivery to the mobile host's Foreign Agent, rather than relying on the Home Agent to perform the encapsulation. To take advantage of this optional information, the correspondent host must at least be mobile-aware.

The Home Agent will send a BIND_ADV message addressed to the correspondent host. The MH_ADD and FA_ADD fields define the current mobility binding for the mobile host. The BIND_LIFE field indicates the time interval over which the correspondent host is authorized to use the mobility binding. The authentication fields are filled in accordance with the authentication policy in force between the Home Agent and the correspondent host.

The Home Agent shall maintain a record of those correspondent hosts to whom it has sent BIND_ADV messages, and it shall maintain an entry in the list until such time that the corresponding binding lifetime expires.

A Home Agent should limit the rate at which it sends BIND_ADV messages to a correspondent host. The Home Agent should not send a duplicate message to the same correspondent host until enough time has elapsed for the original BIND_ADV to have been received and acknowledged by the correspondent host.

6.4.2 BIND_VAL Message

This message is generated by the recipient of a BIND_ADV message to challenge the sender to validate both the advertised binding and its own identity.

The recipient of a challenge, in turn, will reply to the challenger with a BIND_VAL method that indicates if the challenged binding was valid or invalid.

The BIND_VAL message is used for two purposes:

— to challenge the validity of a BIND_ADV message
— to respond to such a challenge.

6.4.2.1 Issuing a Challenge

A mobile-aware host that receives a BIND_ADV message must validate the enclosed binding before using it. The recipient does this by sending a BIND_VAL challenging message (OP_CODE 0) to the mobile host named in the MH-ADD field of the BIND_ADV message. The local system shall not make use of the advertised binding until the authentication process has succeeded. The challenge message shall include the same MH_REG_NUM, BIND_LIFE, MH_ADD, and FA_ADD fields that were carried in the message that advertised the binding. The authentication fields shall be set in accordance with the authentication policy in force between the sender and the recipient.

6.4.2.2 Responding to a Challenge

A system that receives a BIND_VAL challenge addressed to itself shall respond immediately to the sender of the challenge, using a BIND_VAL response. If the recipient of the challenge determines that the binding is invalid, the response must be negative (Operation Code 1); if the binding is valid, the response will be positive (Operation Code 2).

The body of the BIND_VAL response message will include the same the MH_REG_NUM, FA_ADD, MH_ADD, and BIND_LIFE fields that appeared in the BIND_VAL challenge message. The authentication fields will contain data that is consistent with the policy in force between the sender and receiver of this message.

6.4.2.3 Receiving a Response to a Challenge

If the response to a BIND_VAL challenge is positive, the local system may place that binding in its Location List; if it is negative, then the local system shall immediately discard that binding, making no further use of it.

7. Encapsulation Procedures

....TO BE ADDED LATER..........................

8. Mobile Host Processing

8.1 Receiving BEACON Messages

A mobile host listens for BEACONs at all times that it has a data link connection up and running on a given subnetwork: that is, a mobile host listens both before and after initiating a registration request:

— Before making a registration request:

In order to generate a MH_REG_REQ message to start the registration process, a mobile host must know the IP address of a prospective agent on the subnet to which it is attached. After establishing a data link connection on the subnet, the host will listen for a BEACON message from the appropriate type of agent: a Home Agent when the mobile host is attached to its home subnet, or a Foreign Agent when the mobile host is away from home.

When the mobile host hears a valid BEACON, it will note the agent's IP address, which is carried as the source address of the IP packet that carried the BEACON message. It shall also note the Incarnation Number of the agent.

— After initiating a registration request:

  The mobile host will continue to check for BEACONs after it has initiated its registration request. If it receives a BEACON from the same agent with which it is currently registered or has a registration request in progress, it shall check if the Incarnation Number in the most recent message differs from the Incarnation Number in the previous BEACON received from the same agent. If it has, then the mobile host must initiate a new registration request; if it has not, no action needs to be taken.

8.2 Sending SOLICIT Messages

A mobile host that has not yet learned the identity of an available agent on the subnetwork to which it is attached can either continue to listen for BEACON messages (see section 8.1) or it can multicast a SOLICIT message which will cause any available agent to respond with a BEACON message as soon as possible after receipt of the SOLICIT message.

8.3 Requesting a New Registration

A mobile host will need to initiate a new registration request in several situations, for example:

— it has lost contact with its current agent
— it has moved to a new subnetwork
— it has noticed that the Incarnation Number of the agent has changed

The mobile host initiates a request for a new registration by sending a MH_REG_REQ message to the Home Agent or Foreign Agent that it wants to register with (see sections 6.3.1.1 or 6.3.1.2, as appropriate).

8.4 Receiving MH_REG_REPLY Messages

When a mobile host receives an MH_REG_REPLY message that will be rejected according to 6.1, the message shall be ignored.

If an MH_REG_REPLY message contains a Registration Number which is not equal to the Registration Number currently in use by the mobile host, then the message shall be ignored.

Values contained in the HA_SVC_LIFE field and the FA_SVC_LIFE field shall be retained locally, when present.

The mobile host is not required to issue any message in reply to an MH_REG_REPLY message.

If the MH_REG_REPLY message indicates that service will be provided, then the mobile host may begin forwarding data packets to the agent for subsequent delivery to a correspondent host. If the MH_REG_REPLY message indicates that service has been denied, then the mobile host shall not forward any packets to the agent, other than subsequent MH_REG_REQs for registration.

8.5 Reconfirming an Existing Registration

If a mobile host wishes to continue to receive services from its Home Agent or its current Foreign Agent, it must reconfirm its registration with that agent before the associated service lifetime expires, as described in section 6.3.1.3.

8.6 Receiving a BIND_ADV

A mobile-aware host that receives a BIND_ADV message addressed to itself shall note the mobility binding and its associated lifetime. Then it shall request validation from the sender of the BIND_ADV, using a BIND_VAL challenge (see section 6.4.2.1) addressed to the source IP address of the BIND_ADV message.

Until a positive BIND_VAL response is received, the mobile-aware host shall treat the advertised mobility binding as invalid. After receiving a positive response, the host shall then place the mobility binding in its Location List, and may use it to encapsulate packets for delivery directly to a mobile host's Foreign Agent until the Binding Lifetime expires.

8.7 Receiving BIND_VAL Message

A mobile host that receives a BIND_VAL message that challenges a given binding shall determine if the binding in question is valid, and shall then respond appropriately to the system that sent the BIND_VAL challenge, as described in section 6.4.2.2.

8.8 Sending BIND_VAL Message

A mobile host shall reply to a BIND_VAL challenge by sending a BIND_VAL response to the sender of the challenge, as outlined in section 6.4.2.2.

8.9 Encapsulation

A mobile-aware host may use the validated information in its Location List to encapsulate packets for direct delivery to the Foreign Agent serving a mobile host with which it wishes to communicate. A mobility binding in the Location List shall be deleted when its binding lifetime expires.

9. Home Agent Processing

A Home Agent must be able to receive and react to F-H_REG_REQ messages, receive and react to MH_REG_REQ messages sent by mobile hosts that are at home, generate MH_REG_REPLY messages to mobile hosts that are at home, generate FA_REG_REPLY messages, and encapsulate packets for delivery to the Foreign Agent currently serving a mobile host that is away from home. It may also optionally inform correspondent hosts of the current mobility bindings for mobile hosts that are away from home by using the BIND_ADV and BIND_VAL messages.

9.1 Advertising Reachability

A Home Agent must advertise reachability to each mobile host for which it is serving as Home Agent, whether such hosts are at home or away from home. The advertisement will be carried as part of the routing protocol in force within the Home Agent's Autonomous System.

9.2 Receiving SOLICIT Messages

A Home Agent that receives a SOLICIT message asking for Home Agents to identify themselves shall respond as soon as possible by sending a BEACON message on the subnetwork over which the SOLICIT message was received.

9.3 Sending BEACON Messages

BEACON messages shall be sent on a regular basis on all subnetworks to which mobile hosts can attach, and shall also be sent as soon as possible in response to a SOLICIT message (see 6.2.1).

9.4 Receiving a MH_REG_REQ Message

If a Home Agent receives a MH_REG_REQ message from a mobile host that is at home, the Home Agent shall verify that satisfies the authentication criteria currently in force. If it does not, then the message shall be ignored.

If the message was sent by a currently attached mobile host, the message shall be ignored when its MH_REG_NUM field is both a) not equal to zero and b) less than the registration number currently in use by the Home Agent for that mobile host.

If the MH_REG_REQ message requests termination of service, the Home Agent shall remove the associated mobility binding from its Forwarding List.

If the MH_REG_REQ message asks for a new registration or reconfirmation of an existing registration, the Home Agent shall reply to the Mobile Host with an MH_REG_REPLY message whose operation code indicates the action taken by the Home Agent.

9.5 Sending an MH_REG_REPLY Message

A Home Agent shall send an MH_REG_REPLY to a mobile host that is at home in response to a registration or reconfirmation request from that host. The Operation field of the MH_REG_REPLY message shall be set to indicate the Home Agent's response to the mobile host's request (see section 6.3.2.1).

9.6 Receiving a FA_REG_REQ Message

A FA_REG_REQ message that will be rejected according to 6.1 shall be ignored.

The response to the FA_REG_REQ message depends on the operation code of the message:

a) If a FA_REG_REQ message indicates that a given mobile host is requesting a new registration, the Home Agent shall reply to this request by sending a FA_REG_REPLY message to the Foreign Agent whose IP address was the source of the FA_REG_REQ message (see section 6.3.4). If permission is granted for the Foreign Agent to provide service to the mobile host, the Home Agent shall update its Forwarding List with the identity of the mobile host (carried in the MH_ADD field of the FA_REG_REQ message) and the identity of the Foreign Agent (carried in the source address of the IP packet). The HA_SVC_LIFE field must be present in the message. Unless the Operation Code of the FA_REG_REQ message prohibits it, the Home Agent shall notify the previous Foreign Agent, if known, that it is no longer authorized to provide service to the mobile host. The identity of the previous Foreign Agent, if any, will be available in the Home Agent's Forwarding List.
b) If the FA_REG_REQ message is reconfirming an existing registration, the Home Agent shall reply to the Foreign Agent with a FA_REG_REPLY message (see section 6.3.4). If reconfirmation is denied, then the Home Agent shall remove the associated mobility binding from its Forwarding List.
c) If the FA_REG_REQ message indicates that the Foreign Agent is no longer providing service to the mobile host, then the Home Agent shall remove that mobility binding from its Forwarding List.

9.7 Generating a FA_REG_REPLY Message

A Home Agent generates a FA_REG_REPLY message to respond to a previously received FA_REG_REQ message, as outlined in section 9.6.

A Home Agent also sends a FA_REG_REPLY message to a Foreign Agent when the HA_SVC_LIFE has expired without the mobile host′s reconfirming an existing registration, informing the Foreign Agent that it may no longer provide service to the mobile host.

The MH_REG_NUM field of the FA_REG_REPLY message will contain the same value that was carried in the FA_REG_REQ message to which the Home Agent is replying.

9.8 Sending BIND_ADV Messages

If a Home Agent receives a data packet whose destination address is contained in its Forwarding List (that is, it is the address of a mobile host that is away from home), the Home Agent may send a BIND_ADV message to the correspondent host named in the source address field of the data packet, as described in section 6.4.1.2. However, if the binding in the Forwarding list indicates that the Home Agent may not advertise it, then the Home Agent shall not send a BIND_ADV message to the correspondent host.

9.9 Receiving a BIND_ADV Message

The actions to be taken by a Home Agent that receives a Binding Update message addressed to itself are not specified in this paper. As a local option, the Home Agent may either retain the advertised binding, or discard it.

9.10 Encapsulating Outbound Data Packets

If the Home Agent has a valid binding in its Forwarding List for a mobile host that is away from home, then it shall encapsulate data packets destined for that mobile host. The outer packet shall use the Home Agent′s IP address as the source, and the current Foreign Agent′s IP address as the destination. The newly encapsulated packet shall then be handed over to the IP routing protocol in use by the local Autonomous System for further handling.

9.11 Registration Expiration

If the HA_SVC_LIFE for a given mobile host expires before the Home Agent has received a reconfirmation request, then the associated mobility binding shall be erased from the Forwarding List, and a FA_REG_REPLY message shall be sent to the Foreign Agent telling it that it may no longer provide service to that mobile host (see also section 9.7).

10. Foreign Agent Processing

A Foreign Agent must be able to generate FA_REG_REQ messages, generate MH_REG_REPLY messages, receive and react to Home-Foreign Confirm messages, and receive and react to MH_REG_REQ messages. It must also optionally be able to notify a Prior Foreign Agent that a mobile host has moved.

10.1 Sending BEACON Messages

BEACON messages shall be sent on a regular basis on all subnetworks to which mobile hosts can attach, and shall also be sent as soon as possible in response to a SOLICIT message (see 6.2.1)

10.2 Receiving SOLICIT Messages

A Foreign Agent that receives a SOLICIT message asking for Foreign Agents to identify themselves shall respond as soon as possible by sending a BEACON message on the subnetwork over which the SOLICIT message was received.

10.3 Receiving MH_REG_REQ Messages

When a Foreign Agent receives a MH_REG_REQ message that will be rejected according to 6.1, the message shall be ignored.

If the message is a registration request from a currently registered mobile host, the message shall be discarded if the Registration Number contained in the message is not equal to zero and is also less than the Registration Number currently in use.

Upon receipt of a MH_REG_REQ message from a mobile host that has an operation code of 1 (registration request), the Foreign Agent has two options: as a local matter, it may immediately deny service to the mobile host, or it may request permission from the Home Agent (named in the MH_REG_REQ message) to provide service to the mobile host.

The actions to be taken are as follows:

— If service is being denied, then the Foreign Agent shall send an MH_REG_REPLY message to the mobile host indicating that service has been denied. The contents of this message are defined in 10.6.3.

— If the Foreign Agent is willing to provide service, it shall send a FA_REG_REQ message to the mobile host′s Home Agent. The contents of this message are defined in 10.4.1. The Foreign Agent shall not begin such service until authorized by the mobile host's Home Agent through a FA_REG_REPLY message.

10.4 Generating FA_REG_REQ Messages

A Foreign Agent will generate a FA_REG_REQ message for one of two reasons: a) in response to a MH_REG_REQ message from a mobile unit for which the Foreign Agent wishes to provide service, or b) to inform the Home Agent of a mobile host for whom the Foreign Agent had been providing service that the Foreign Agent will no longer provide such services for that host. The actions taken by the Foreign Host in each of these cases are described in sections 10.4.1 and 10.4.2.

10.4.1 Updating the Home Agent

After receiving a MH_REG_REQ message from a mobile host for whom it wishes to provide service, the Foreign Agent shall send a FA_REG_REQ message to the Home Agent to request permission to provide this service (see section 6.3.3.1).

10.4.2 Denying Service

When a Foreign Agent stops providing service to a previously registered mobile host, it shall notify the Home Agent by means of a FA_REG_REQ message, as described in 6.3.3.2. Termination of service may be invoked for several reasons: for example, the FA_SVC_LIFE may have expired.

10.5 Receiving FA_REG_REPLY Messages

A FA_REG_REPLY message that will be rejected according to 6.1 shall be ignored.

The Foreign Agent shall ignore a FA_REG_REPLY message which does not relate to a pending registration request or to a currently registered mobile host.

When a Foreign Agent receives a FA_REG_REPLY message for a pending registration request, the Foreign Agent shall promptly inform the mobile host about the disposition of its request through an MH_REG_REPLY message, using the method defined in 10.6.2

If the FA_REG_REPLY message gave permission to the Foreign Agent to provide service to the mobile host, then the Foreign Agent shall update its Visitor List accordingly.

10.6 Generating MH_REG_REPLY Messages

A Foreign Host sends an MH_REG_REPLY message to a mobile host to advise it of the status of a pending or current registration.

10.6.1 Pending Registration Request

As soon as possible after it receives a MH_REG_REQ message from a mobile host that requests a registration to be begun, the Foreign Agent shall reply to the mobile host with a MH_REG_REPLY message indicating that the registration is pending. By telling the mobile host that processing of its request has started, it will be possible for the mobile host to forestall generation of new registration requests until it has allowed sufficient time for the pending request to have been handled.

10.6.2 Relaying Information from Home Agent

When a Foreign Agent receives a FA_REG_REPLY message for a mobile unit that the Foreign Agent is currently providing service to, or for which it has sought permission from the Home Agent to provide service to, it shall relay the pertinent information contained in the FA_REG_REPLY message to the mobile host by means of an MH_REG_REPLY message.

The operation code of the MH_REG_REPLY shall be set in accordance with the operation code carried in the FA_REG_REPLY message.

If service is being denied, then the HA_SVC_LIFE field and the FA_SVC_LIFE field will not be present.

If service will be provided, then the HA_SVC_LIFE field of the FA_REG_REPLY message shall be copied into the corresponding field of the MH_REG_REPLY message. The Foreign Agent shall determine a value for the FA_SVC_LIFE field of the MH_REG_REPLY message.

The H-H_AUTH_LGTH field and H-H_AUTH_DATA field, if present, shall be copied from the FA_REG_REPLY message into the corresponding field(s) of the MH_REG_REPLY message.

10.6.3 Terminating Service

A Foreign Agent may deny or withdraw services to an already

When a Foreign Agent stops providing service to a previously registered mobile host, it shall notify the mobile host by means of an MH_REG_REPLY message, as described in 6.3.3.2. Termination of service may be invoked for several reasons: for example, the FA_SVC_LIFE may have expired.

The MH_REG_REPLY message sent to the mobile host will use the same Registration Number that the mobile host used when the registration was initially accepted. The FA_SVC_LIFE field and the HA_SVC_LIFE field will not be present.

If the mobile host and the Foreign Agent have previously agreed to use a specific authentication procedure, then the Foreign Agent will put the appropriate data in the A-H_AUTH_LGTH and A-H_AUTH_DATA fields. Otherwise, the A-H_AUTH_LGTH field shall be set to the value 0, and the A-H_DATA field will not be present in the message.

10.7 Sending a BIND_ADV Message

A Foreign Agent uses a BIND_ADV message to inform a Prior Agent (named in a MH_REG_REQ for registration) that a given mobile host is requesting a new registration. The current Foreign Agent shall not send a BIND_ADV message to a Prior Foreign Agent if the Operation field of the MH_REG_REQ message prohibits it from doing so.

The BIND_ADV to the prior Foreign Agent should be sent as soon as possible after receipt of the MH_REG_REQ message. Message content is described in section 6.4.1.1.

10.8 Receiving a BIND_ADV Message

A BIND_ADV message that will be rejected according to 6.1 shall be ignored. A BIND_ADV message whose OP_CODE field indicates that it was not sent by a prospective Foreign Agent shall be ignored.

The binding advertised in a BIND_ADV message shall not be used until it has been verified by an exchange of BIND_VAL messages with the system who sent the BIND_ADV message.

10.9 Sending a BIND_VAL Message

A Foreign Agent that receives a BIND_ADV message may choose to ignore it, and no further action will be necessary. However, if it wishes to make use of the mobility binding that it contains, it must send a Binding Validation message to the system named in the IP source address of the BIND_ADV message, challenging it to verify the advertised binding (see section 6.4.2.1).

10.10 Receiving a BIND_VAL Message

A Foreign Agent may receive a BIND_VAL message that either a) challenges a binding that the Foreign Agent is alleged to have advertised in a previous BIND_ADV message, or b) responds to challenge issued by the Foreign Agent.

10.10.1 Receiving a Challenge

The Foreign Agent shall respond to the challenge as soon as possible, as described in section 6.4.2.2.

10.10.2 Receiving a Response

If the response to a previously issued challenge is negative, then the Foreign Agent may not use the associated mobility binding. If the response is positive, then the Foreign Agent may add the mobility binding to its Location List. It may use the information to encapsulate packets to the current Foreign Agent, subject to the BIND_LIFE constraint.

If the Foreign Agent has a binding for the mobile host, then that binding shall be removed from its Mobility Information Base. The Foreign Agent shall then start a BIND_LIFE timer associated with validated binding.

10.11 Decapsulation

A Foreign Agent shall decapsulate packets addressed to itself:

a) if the received packet contains an inner packet addressed to a system named in the Foreign Agent's Visitor List, the Foreign Agent shall deliver the inner packet to the named system.
b) If the received packet contains an inner packet addressed to a system named in the Foreign Agent's Location List, it shall encapsulate the inner packet. The new outer packet shall use the Foreign Agent's IP address as the source, and shall use the address of the Prior Foreign Agent (learned from the Location List) as the destination. Then the Foreign Agent shall hand the outer packet over to the routing Protocol in use by the local Autonomous System for further processing.
c) if the received packet contains an inner packet addressed to a system that is not named in either the Visitor List or the Location List, then the Foreign Agent shall hand the inner packet to the routing function for further processing. It shall also send a BIND_ADV message to the system named in the source address field or the original outer packet, indicating that the binding consisting of the pair <destination IP address of outer packet (alleged Foreign Agent), destination address of inner IP packet (alleged mobile host)> is invalid.

11. Correspondent Host Processing

A correspondent host can either be a mobile host, a mobile-aware host, or an ignorant host:

a) A correspondent mobile host provides the processing described in section 6.2, including all its subsections.
b) A correspondent mobile-aware host must be able to receive and understand BIND_ADV messages (see section 8.6), challenge the received binding (see section 6.4.2.1), and receive and understand the response to that challenge (see section 6.4.2.3).
c) The actions of a correspondent ignorant host are not constrained by this specification.

12. Registration Numbers

The header of each message carries a registration number. Registration numbers are generated by the mobile hosts in the Mobile Request message. Home Agents and Foreign Agents do not generate new registration numbers: they simply use the appropriate registration number which they have learn from messages that they have already received.

The registration number 0 has special significance. For purposes of this protocol, the registration number 0 signifies that this message is to be recognized by all entities that receive it: that is, the registration number ″0″ is considered to be higher in value than any other registration number.

The mobile host will use the registration number 0 as the next number after the value 255.

13. Mobile Host′s Mobility Information Base

The Mobility Information Base for a mobile host contains the following information, and is indexed by the current registration number used by the mobile host:

— Host′s Home IP Address
— Current Registration Number
— Address of the current Foreign Agent
— FA_SVC_LIFE value
— HA_SVC_LIFE value
— Location List (if route optimization is supported)
— BIND_LIFE values (one per entry in Location List)

14. Home Agent′s Mobility Information Base

The Mobility Information Base for a Home Agent contains the following information, and is indexed by the Home IP address of a mobile host.

— Home IP Address of mobile host
— Address of Current Foreign Agent
— Current Registration Number
— IP address of prior Foreign Agent (if known)
— HA_SVC_LIFE value
— BIND_LIFE values (one for each binding advertised to a correspondent host)
— List of correspondent host′s to whom bindings have been advertised

15. Foreign Agent′s Mobility Information Base

The Mobility Information Base for a Foreign Agent contains the following information, and is indexed by the Home IP address of a mobile host. There is one entry for each mobile host currently served by the Foreign Agent.

— Home IP address of mobile host
— IP address of Home Agent
— Current Registration Number
— IP address of prior Foreign Agent (if known)
— HA_SVC_LIFE (one per mobile host served)
— FA_SVC_LIFE (one per mobile host served)

16. Open and/or Unfinished Items

There are several open items for which some preliminary work has taken place, but for which all relevant details are not yet available. The information that the editor was able to locate has been placed in the Appendix. Pending action by the group, these items will either be integrated into the text, or dropped.

The items are:

a) Appendix B: Operating Mobile Hosts on Their Home Networks
b) Appendix C: Direct Communication Between Mobile Hosts Away from their Home Network
c) Appendix D: Temporary Home Agents
d) Appendix E: Co-located Mobile Host/Foreign Agent
e) Appendix F: Multiple Simultaneous Registrations

17. Conformance Requirements

---Left for discussion at next interim meeting
---We need to agree on the mandatory/optional features, etc.

Appendix A. Security Models

This protocol can support a range of security models, ranging from no security to weak security to strong security. This section describes the various security models and outlines their advantages, disadvantages, and possible implementation.

The ″no security model″ implies that a recipient believes every message that it receives, making no attempt to authenticate the source. This model allows very fast convergence of routes to the most optimum possible and is very easy to implement. Its main problem is that it allows a malicious or mischievous host to intercept a packet stream to a Mobile Host by simply sending a forged protocol message containing a false binding. Although this model might be appropriate in a private network, it is unacceptable in the Internet where nothing may be assumed about other users.

The ″strong security model″ implies that recipients never believe any protocol message unless they can authenticate it. Authentication under the strong security model almost certainly requires the use of public and private keys and trusted servers. Its main disadvantage is its complexity and speed of operation. In particular, convergence to close to optimum routes may be a very slow process.

The ″weak security model″ is based on the idea that the protocol should provide security that is at least as good as provided by the Internet today. In effect, this means that all entities on the normal path of a packet through the Internet are assumed to be trustworthy. In effect, the weak security model merely requires an entity to perform relatively simple authentication procedures when it receives new information about the location of a Mobile Host.

The rest of this section discusses examples of how one might conform to a weak security model using the protocol specified in this paper. Routing support for mobile hosts requires authentication services for three reasons under the weak security model:

— A Home Agent needs to be able to authenticate a binding it receives from a Mobile Host it serves.
— Entities need to be able to acquire an authenticated binding for a Mobile Host.
— Entities need to be able to authenticate the source of a protocol message.

A Mobile Host may help its Home Agent authenticate the binding that it sends to its Home Agent under the weak security model by including 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.

In general, entities will not have a shared secret, such as a password, that can be used to authenticate received bindings. However, an entity can obtain an authenticated binding for a Mobile Host under the weak security model by sending the Mobile Host (or the Mobile Host′s Home Agent acting on behalf of the Mobile Host) a request that also contains a random authentication pattern. If the reply contains the same authentication pattern, the included binding can be authenticated under the weak security model. The reception of incorrect authentication patterns is an indication of a possible attack.

Sometimes it is important for an entity to know that another entity really holds the information it claims to hold. In this case the source rather than the information is being authenticated. An entity can authenticate the source by sending it a request for the same information with a random authentication pattern. If the reply contains the same information and authentication pattern, it can be authenticated.

One optimization may be made to the weak security methods described above. It is desirable that when a Mobile Host moves, its previous Foreign Agent is quickly updated with its new binding so that packets in flight are not lost. Without an additional mechanism a Foreign Agent receiving the new binding would need to authenticate it with the Mobile Host or its Home Agent, which takes time. This process can be sped up by including a random authentication pattern, which is established when the Mobile Host registered with its previous Foreign Agent (with an implied trust of the Mobile Host to Foreign Agent link), in the update packet. Thus, if a Foreign Agent receives an update with a correct authentication pattern, the new binding can be considered to be authenticated under the weak security model.

Appendix B. Operating Mobile Hosts on Their Home Networks

B.1 Preferred mode of operation

Many people will use their computers most often on their Home Networks. When doing so, they will expect the same level of service from their infrastructure as they receive today with, say, desktop workstations. In order to allow Mobile Hosts to reside comfortably on their Home Networks, special care has to be taken with handling ARP requests from corresponding hosts on the Home Network.

A problem can arise if a Mobile Host, which has previously answered an ARP request, then moves away from its Home Network and leaves behind a stale entry in a Correspondent Host′s ARP cache. If a router which forwards packets into the Home Network has a stale ARP cache entry for the Mobile Host, any unencapsulated packets forwarded to the Home Network for the Mobile Host would be lost after travelling through that router. Thus, it is important for ARP caches of hosts populating the Home Network be updated as soon as possible.

Define a gratuitous ARP as an ARP reply which is broadcast to all hosts on a local subnet, but not in response to any ARP request. Suppose all non Mobile Hosts listen to gratuitous ARPs, and use them to update any relevant entries in their local ARP caches whether or not the ARP reply was issued in response to an ARP request they had issued. Mobile Hosts, whether or not they are currently situated on their Home Network, are required to correctly process gratuitous ARPs.

Then a reasonably good solution is to make sure that a gratuitous ARP is issued on behalf of a Mobile Host whenever it moves away from it Home Network. The gratuitous ARP will indicate that all remaining hosts should associate the IP address of the Mobile Host with the MAC address of the Home Agent that had formerly served the Mobile Host before it moved. The gratuitous ARP can be repeated as many times as needed to insure that all the hosts on the Home Network reliably receive it.

When a Mobile Host returns to its Home Network it can issue a gratuitous ARP on its own behalf. In addition the Home Agent can issue unicast ARPs on behalf of the Mobile Host when the Home Agent receives a packet from a Correspondent Host that could be sent directly rather than through the Home Agent.

While the Mobile Host is away from its Home Network, the Home Agent has to perform Proxy ARP replies for the Mobile Host. Otherwise, whenever a Correspondent Host which also resides on the Home Network (or a router which would forward a packet into the Home Network) needs to send a packet to the Home Address of the Mobile Host, the transmission would fail unless the sender could obtain some Layer 2 address for the Mobile Host's Home Address. In this way, all packets destined to Mobile Hosts will end up at the Home Agent for further processing during the times when the Mobile Host is situated away from its Home Network.

B.2 Operation when Gratuitous ARP is not reliable

If the non-mobile hosts on the Home Network do not correctly process gratuitous ARPs, then Mobile Hosts must be configured to ignore all ARP requests. Thus, no non-Mobile Host will ever store the MAC address of a Mobile Host within its ARP cache. In this situation, the Home Agent must forever perform proxy ARP duties on behalf of the Mobile Hosts it serves. All packets destined to Mobile Hosts will end up at the Home Agent, even it they could otherwise have been transmitted directly to the Mobile Host on the same network. The Home Agent must then forward the packets to the Mobile Host on behalf of the corresponding host. The Home Agent will have obtained the MAC address of its Mobile Hosts when they registered.

Sometimes non Mobile Hosts do not correctly process gratuitous ARPs, but nevertheless have a sufficiently small timeout value for entries in their ARP caches. Then it may be preferable to allow the Mobile Hosts to answer ARP requests even though there will be a break in communications whenever a Mobile Host moves.

Appendix C. Operating Mobile Hosts Away from their Home Networks

Suppose two Mobile Hosts, with Home Addresses that may or may not be on the same Home Network, share a data communications medium and at least one of the Mobile Hosts is not connected to its Home Network. It is advantageous, for processing and transmission bandwidth reasons, for them to send packets directly to each other. The problems resemble those of a Mobile Host communicating directly with other hosts on the Mobile Host's Home Network, discussed in the previous section.

This section proposes a mechanism for direct communication between any two Mobile Hosts when they are both registered with the same Foreign Agent. It is assumed that all Mobile Hosts process gratuitous ARP replies correctly. It is not required that other hosts process gratuitous ARP replies correctly.

Consider the example of two Mobile Hosts, MH1 and MH2, with Home Addresses on different Home Networks registered with a single Foreign Agent. Now suppose MH1 sends a packet to MH2. As MH2 is on a different Home Network, MH1 will route the packet to the Foreign Agent acting as its default router.

The Foreign Agent will discover that MH2 is in its Visitor List and so it delivers the packet directly to MH2. The Foreign Agent can also discover that MH1 is also in its Visitor List and is connected to the same communications medium as MH2. The Foreign Agent may then send MH1 a redirect message telling it to create a special host route for MH2 which indicates MH2 is directly reachable to MH1. Like a Visitor List entry the host route is specified to eventually time out.

The next time MH1 tries to send MH2 a packet, it will find the host route and ARP for MH2. Assuming MH2 replies to ARP requests when not connected to its Home Network, MH1 will learn MH2's MAC address and thus send packets to MH2 directly rather than through the Foreign Agent. The same process works in reverse for packets from MH2 to MH1.

If one of the Mobile Hosts is connected to its Home Network, the same process works on the condition that the Foreign Agent and the Home Agent are in the same box and that both Mobile Hosts use the combined entity as their first hop router.

Now suppose MH2 moves to a new location and registers with a new Foreign Agent. MH2 must first delete all special host routes created by the redirect packet and the associated ARP cache entries. MH2 also notifies it previous Foreign Agent that is has moved. The Previous Foreign Agent on receiving the notification broadcasts a small number of gratuitous ARP replies that cause any mobile hosts with a special host route for MH2 to delete it along with the associated ARP cache entry.

Once the various updates have been completed communications between MH1 and MH2 will continue normally. If all the gratuitous ARP replies are lost then communications to MH2 will be lost for the time period of the special host route in MH1; thus the gratuitous ARP should be repeated often enough to avoid this loss.

Notice that during these operations, there is no need for the Foreign Agent to perform any Proxy ARP operations. When the gratuitous ARP entries, in its remaining clients, time out, the Foreign Agent will again receive packets just by its natural recognition as the local default router by its client Mobile Hosts.

Finally, it is important to point out that in the particular case of movement of wireless Mobile Hosts, it is possible for two Mobile Hosts to lose communication with each other even though they are registered with the same Foreign Agent. When an indication is received that two Mobile Hosts, which were previously in direct communication, lower layer facilities will need to be invoked to indicate the deletion the host route (and ARP cache entry) for the affected host.

Appendix D. Temporary Home Agents

Temporary Home Agents can be used to localize the flow of registration messages when a mobile host moves around within a limited space: for example, within a routing domain.

In the baseline protocol, each time a mobile host moves to a new Foreign Agent, it must initiate a new registration sequence, which involves exchange of messages between the Foreign Agent and the Home Agent. This method certainly will work correctly, but it may be sub-optimum in certain cases. For example, consider the case where a mobile host has roamed to a new routing domain which is physically far away from the domain where its Home Agent is located. If a system in the "remote" domain can serve as a Temporary Home Agent for all the conventional Foreign Agents in that domain, then the flow of registration messages can be largely confined to the remote domain--that is, if the mobile host elects to use the services of the Temporary Home Agent, then the FA_REG_REQUEST and FA_REG_REPLY messages can flow between the current Foreign Agent and the Temporary Home Agent, thus minimizing the flow of messages across domain boundaries.

The following sequence of events illustrate how the process would work:

a) The BEACON message from the Foreign Agent will include a new bit to indicate if the Foreign Agent can also serve as a Temporary Home Agent

b) A mobile host requests registration from a Foreign Agent, as in normal operation, using a MH_REG_REQ message.

c) The Foreign Agent will send a conventional FA_REG_REQ message to the Home Agent, which already includes authentication data. ** The FA-REG_REPLY message will also include a new field to tell the Home Agent that it wants to serve as a Temporary Home Agent for one of its mobile hosts.**

d) The Home Agent responds to the FA_REG_REQ message with an FA_REG_REPLY message, as normal. There will need to be more granularity in the OP_CODES: permission to serve as T-HA will need a new code point.

e) The Foreign Agent tells the mobile host that:
   - the registration was successful (MH_REG_REPLY message), and
   - The Foreign Agent will (or will not) serve as a Temporary Home Agent.

f) Now when a mobile host moves to a new location, it can tell the prospective Foreign Agent (via the HA_ADD field of the MH_REG_REQ message) that its "Home Agent" is either the real Home Agent or the properly authorized Temporary Home Agent.

g) The prospective Foreign Agent then continues the registration process as normal with the agent whose address appears in the HA_ADD field of the registration request.

The basic data packet flows to the Home Agent, who encapsulates it for delivery to the co-located Temporary Home Agent/Foreign Agent. The

Temporary Home Agent receives the encapsulated packet, decapsulates it, and then re-encapsulates the inner packet for delivery to the Foreign Agent. who then decapsulates and delivers it to the mobile host.

If the mobile host moves to a different Foreign Agent (say FA2) and tells it that its Home Agent is T-HA, then then the FA_REG_REQ and FA_REG_REPLY messages flow between FA2 and T-HA. No new registration messages need to flow between T-HA and HA: that is, as far as the real Home Agent is concerned, the mobile host has not changed attachment points. However, the T-HA will know that the mobile host has moved to Foreign Agent 2, and thus can still deliver data packets to it.

Appendix E. Co-located Mobile Host/Foreign Agent

In cases where a mobile host away from home is able to dynamically acquire a temporary IP address, the mobile host can then serve as its own Foreign Agent, using the temporary address as the address of the Foreign Agent. Thus, the Foreign Agent function and the Mobile Host function can be co-located in a single box. This eliminates altogether the need to deploy separate entities that can perform the Foreign Agent functionality. The procedures for acquiring a temporary address are outside the scope of this document. A possible method for acquiring a temporary address is DHCP.

Because these functions are co-located, all communication between the mobile host and its Foreign Agent is internal to the box, and there is no need to use the following external messages: MH_REG_REQ, MH_REG_REPLY, BEACON, and SOLICIT.

The only messages that need to be supported are the FA_REG_REQ and FA_REG_REPLY. These messages will still flow between the MH/FA box and its Home Agent. The mobility binding will associate the Home IP address of the mobile host with the temporary address obtained for the Foreign Agent.

It is assumed that a mobile host has mechanisms to detect changes in its Link Layer connectivity and to initiate acquisition of a temporary address each time such a change occurs. The mechanisms will be specific to the particular Link Layer technology, and are outside the scope of this document. For example, some link layer protocols provide inactivity timers that can be used to infer whether connectivity has been lost.

Appendix F. Simultaneous Registrations

This option has only been accommodated to the extent that a bit has been set aside in the OP_CODE field of the MH_REG_REQ message. Presumably, the actions (not yet defined) would be along the lines of: don′t erase an old binding from the Forwarding list or the Visitor List without an explicit message to do so. That is, we can no longer assume that receipt of a new mobility binding invalidates a previous binding.

It also assumes that a Home Agent (or a correspondent host who knows about the multiple simultaneous bindings) has a local mechanism available to select one of them for each incoming packet (maybe round-robin or some such mechanism.)