Internet Engineering Task Force (IETF)
Request for Comments: 5944
Obsoletes: 3344
Category: Standards Track
ISSN: 2070-1721

C. Perkins, Ed.
WiChorus Inc.

November 2010

IP Mobility Support for IPv4, Revised

Abstract

This document specifies protocol enhancements that allow transparent routing of IP datagrams to mobile nodes in the Internet. Each mobile node is always identified by its home address, regardless of its current point of attachment to the Internet. While situated away from its home, a mobile node is also associated with a care-of address, which provides information about its current point of attachment to the Internet. The protocol provides for registering the care-of address with a home agent. The home agent sends datagrams destined for the mobile node through a tunnel to the care-of address. After arriving at the end of the tunnel, each datagram is then delivered to the mobile node.

Status of This Memo

This is an Internet Standards Track document.

This document is a product of the Internet Engineering Task Force (IETF). It represents the consensus of the IETF community. It has received public review and has been approved for publication by the Internet Engineering Steering Group (IESG). Further information on Internet Standards is available in Section 2 of RFC 5741.

Information about the current status of this document, any errata, and how to provide feedback on it may be obtained at http://www.rfc-editor.org/info/rfc5944.

Table of Contents

1. Introduction

IP version 4 assumes that a node's IP address uniquely identifies the node's point of attachment to the Internet. Therefore, a node must be located on the network indicated by its IP address in order to receive datagrams destined to it; otherwise, datagrams destined to the node would be undeliverable. For a node to change its point of attachment without losing its ability to communicate, currently one of the two following mechanisms must typically be employed:

- the node must change its IP address whenever it changes its point of attachment, or
- host-specific routes must be propagated throughout much of the Internet routing fabric.

Both of these alternatives are often unacceptable. The first makes it impossible for a node to maintain transport and higher-layer connections when the node changes location. The second has obvious and severe scaling problems, especially relevant considering the explosive growth in sales of notebook (mobile) computers.

A new, scalable mechanism is required for accommodating node mobility within the Internet. This document defines such a mechanism, which enables nodes to change their point of attachment to the Internet without changing their IP address.

Changes between this revised specification for Mobile IP and the original specifications (see [44], [14], [15], [20], [4], and [50]) are detailed in Appendix F.

1.1. Protocol Requirements

A mobile node must be able to communicate with other nodes after changing its link-layer point of attachment to the Internet, yet without changing its IP address.

A mobile node must be able to communicate with other nodes that do not implement these mobility functions. No protocol enhancements are required in hosts or routers that are not acting as any of the new architectural entities introduced in Section 1.5.

All messages used to update another node as to the location of a mobile node must be authenticated in order to protect against remote redirection attacks.

1.2. Goals

The link by which a mobile node is directly attached to the Internet may often be a wireless link. This link may thus have a substantially lower bandwidth and higher error rate than traditional wired networks. Moreover, mobile nodes are likely to be battery powered, and minimizing power consumption is important. Therefore, the number of administrative messages sent over the link by which a mobile node is directly attached to the Internet should be minimized, and the size of these messages should be kept as small as is reasonably possible.

1.3. Assumptions

The protocols defined in this document place no additional constraints on the assignment of IP addresses. That is, a mobile node can be assigned an IP address by the organization that owns the machine.

This protocol assumes that mobile nodes will generally not change their point of attachment to the Internet more frequently than once per second.

This protocol assumes that IP unicast datagrams are routed based on the Destination Address in the datagram header (and not, for example, by source address).

1.4. Applicability

Mobile IP is intended to enable nodes to move from one IP subnet to another. It is just as suitable for mobility across homogeneous media as it is for mobility across heterogeneous media. That is, Mobile IP facilitates node movement from one Ethernet segment to another, as well as from an Ethernet segment to a wireless LAN, as long as the mobile node’s IP address remains the same after such a movement.

One can think of Mobile IP as solving the "macro" mobility management problem. It is less well suited for more "micro" mobility management applications -- for example, handoff amongst wireless transceivers, each of which covers only a very small geographic area. As long as node movement does not occur between points of attachment on different IP subnets, link-layer mechanisms for mobility (i.e., link-layer handoff) may offer faster convergence and far less overhead than Mobile IP.

1.5. New Architectural Entities

Mobile IP introduces the following new functional entities:

Mobile Node

A host or router that changes its point of attachment from one network or subnetwork to another. A mobile node may change its location without changing its IP address; it may continue to communicate with other Internet nodes at any location using its (constant) IP address, assuming link-layer connectivity to a point of attachment is available.

Home Agent

A router on a mobile node's home network that tunnels datagrams for delivery to the mobile node when it is away from home, and maintains current location information for the mobile node.

Foreign Agent

A router on a mobile node's visited network that provides routing services to the mobile node while registered. The foreign agent detunnels and delivers to the mobile node datagrams that were tunneled by the mobile node's home agent. For datagrams sent by a mobile node, the foreign agent may serve as a default router for registered mobile nodes.

A mobile node is given a long-term IP address on a home network. This home address is administered in the same way that a "permanent" IP address is provided to a stationary host. When away from its home network, a "care-of address" is associated with the mobile node and reflects the mobile node's current point of attachment. The mobile node uses its home address as the source address of all IP datagrams that it sends, except where otherwise described in this document for datagrams sent for certain mobility management functions (e.g., as in Section 3.6.1.1).

1.6. Terminology

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119 [1].

In addition, this document frequently uses the following terms:

Authorization-Enabling Extension

An authentication that makes a (registration) message acceptable to the ultimate recipient of the registration message. An authorization-enabling extension MUST contain a Security Parameter Index (SPI).

In this document, all uses of authorization-enabling extension refer to authentication extensions that enable the Registration Request message to be acceptable to the home agent. Using additional protocol structures specified outside of this document, it may be possible for the mobile node to provide authentication of its registration to the home agent, by way of another authenticating entity within the network that is acceptable to the home agent (for example, see RFC 2794 [2]).

Agent Advertisement

An advertisement message constructed by attaching a special Extension to a Router Advertisement [5] message.

Authentication

The process of verifying (using cryptographic techniques, for all applications in this specification) the identity of the originator of a message.

Care-of Address

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

Correspondent Node

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

Foreign Network

Any network other than the mobile node’s home network.

Gratuitous ARP

An Address Resolution Protocol (ARP) packet sent by a node in order to spontaneously cause other nodes to update an entry in their ARP cache [45]. See Section 4.6.

Home Address

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

Home Network

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

Link

A facility or medium over which nodes can communicate at the link layer. A link underlies the network layer.

Link-Layer Address

The address used to identify an endpoint of some communication over a physical link. Typically, the link-layer address is an interface's Media Access Control (MAC) address.

Mobility Agent

Either a home agent or a foreign agent.

Mobility Binding

The association of a home address with a care-of address, along with the remaining Lifetime of that association.

Mobility Security Association

A collection of security contexts, between a pair of nodes, which may be applied to Mobile IP protocol messages exchanged between them. Each context indicates an authentication algorithm and mode (Section 5.1), a secret (a shared key, or appropriate public/private key pair), and a style of replay protection in use (Section 5.7).

Node

A host or a router.

Nonce

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

Security Parameter Index (SPI)

An index identifying a security context between a pair of nodes, among the contexts available in the Mobility Security Association. SPI values 0 through 255 are reserved and MUST NOT be used in any Mobility Security Association.

Tunnel

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

Virtual Network

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

Visited Network

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

Visitor List

The list of mobile nodes visiting a foreign agent.

1.7. Protocol Overview

The following support services are defined for Mobile IP:

Agent Discovery

> Home agents and foreign agents may advertise their availability on each link for which they provide service. A newly arrived mobile node can send a solicitation on the link to learn if any prospective agents are present.

Registration

> When the mobile node is away from home, it registers its care-of address with its home agent. Depending on its method of attachment, the mobile node will register either directly with its home agent, or through a foreign agent that forwards the registration to the home agent.

Silently Discard

> The implementation discards the datagram without further processing, and without indicating an error to the sender. The implementation SHOULD provide the capability of logging the error, including the contents of the discarded datagram, and SHOULD record the event in a statistics counter.

The following steps provide a rough outline of operation of the Mobile IP protocol:

- Mobility agents (i.e., foreign agents and home agents) advertise their presence via Agent Advertisement messages (Section 2). A mobile node may optionally solicit an Agent Advertisement message from any locally attached mobility agents through an Agent Solicitation message.

- A mobile node receives these Agent Advertisements and determines whether it is on its home network or a foreign network.

- When the mobile node detects that it is located on its home network, it operates without mobility services. If returning to its home network from being registered elsewhere, the mobile node deregisters with its home agent, through exchange of a Registration Request and Registration Reply message with it.

- When a mobile node detects that it has moved to a foreign network, it obtains a care-of address on the foreign network. The care-of address can either be determined from a foreign agent's

advertisements (a foreign agent care-of address), or by some external assignment mechanism such as DHCP [34] (a co-located care-of address).

- The mobile node operating away from home then registers its new care-of address with its home agent through exchange of a Registration Request and Registration Reply message with the home agent, possibly via a foreign agent (Section 3).

- Datagrams sent to the mobile node's home address are intercepted by its home agent, tunneled by the home agent to the mobile node's care-of address, received at the tunnel endpoint (either at a foreign agent or at the mobile node itself), and finally delivered to the mobile node (Section 4.2.3).

- In the reverse direction, datagrams sent by the mobile node are generally delivered to their destination using standard IP routing mechanisms, not necessarily passing through the home agent.

When away from home, Mobile IP uses protocol tunneling to hide a mobile node's home address from intervening routers between its home network and its current location. The tunnel terminates at the mobile node's care-of address. The care-of address must be an address to which datagrams can be delivered via conventional IP routing. At the care-of address, the original datagram is removed from the tunnel and delivered to the mobile node.

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

a. A "foreign agent care-of address" is a care-of address provided by a foreign agent through its Agent Advertisement messages. In this case, the care-of address is an IP address of the foreign agent. In this mode, the foreign agent is the endpoint of the tunnel and, upon receiving tunneled datagrams, decapsulates them and delivers the inner datagram to the mobile node. This mode of acquisition is preferred because it allows many mobile nodes to share the same care-of address and therefore does not place unnecessary demands on the already limited IPv4 address space.

b. A "co-located care-of address" is a care-of address acquired by the mobile node as a local IP address through some external means, which the mobile node then associates with one of its own network interfaces. The address may be dynamically acquired as a temporary address by the mobile node, such as through DHCP [34], or may be owned by the mobile node as a long-term address for its use only while visiting some foreign network. Specific external methods of acquiring a local IP address for use as a co-located

care-of address are beyond the scope of this document. When using a co-located care-of address, the mobile node serves as the endpoint of the tunnel and itself performs decapsulation of the datagrams tunneled to it.

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

It is important to understand the distinction between the care-of address and the foreign agent functions. The care-of address is simply the endpoint of the tunnel. It might indeed be an address of a foreign agent (a foreign agent care-of address), but it might instead be an address temporarily acquired by the mobile node (a co-located care-of address). A foreign agent, on the other hand, is a mobility agent that provides services to mobile nodes. See Sections 3.7 and 4.2.2 for additional details.

A home agent MUST be able to attract and intercept datagrams that are destined to the home address of any of its registered mobile nodes. Using the proxy and gratuitous ARP mechanisms described in Section 4.6, this requirement can be satisfied if the home agent has a network interface on the link indicated by the mobile node’s home address. Other placements of the home agent relative to the mobile node’s home location MAY also be possible using other mechanisms for intercepting datagrams destined to the mobile node’s home address. Such placements are beyond the scope of this document.

Similarly, a mobile node and a prospective or current foreign agent MUST be able to exchange datagrams without relying on standard IP routing mechanisms; that is, those mechanisms that make forwarding decisions based upon the network-prefix of the Destination Address in the IP header. This requirement can be satisfied if the foreign agent and the visiting mobile node have an interface on the same link. In this case, the mobile node and foreign agent simply bypass their normal IP routing mechanism when sending datagrams to each other, addressing the underlying link-layer packets to their respective link-layer addresses. Other placements of the foreign agent relative to the mobile node MAY also be possible using other mechanisms to exchange datagrams between these nodes, but such placements are beyond the scope of this document.

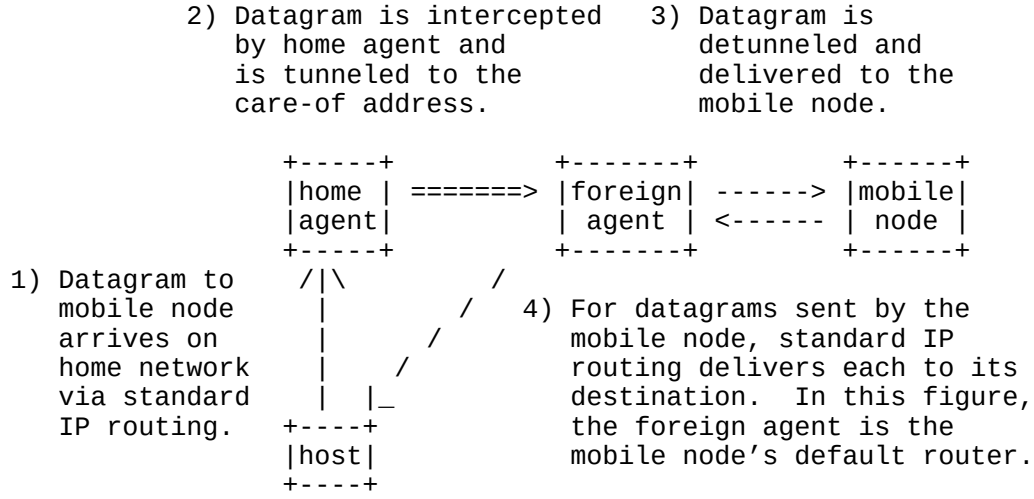


Figure 1: Operation of Mobile IPv4

If a mobile node is using a co-located care-of address (as described in item (b) above), the mobile node MUST be located on the link identified by the network prefix of this care-of address. Otherwise, datagrams destined to the care-of address would be undeliverable.

For example, Figure 1 illustrates the routing of datagrams to and from a mobile node away from home, once the mobile node has registered with its home agent. In Figure 1, the mobile node is using a foreign agent care-of address, not a co-located care-of address.

1.8. Message Format and Protocol Extensibility

Mobile IP defines a set of new control messages, sent with UDP [17] using well-known port number 434. The following two message types are defined in this document:

1 Registration Request

3 Registration Reply

Up-to-date values for the message types for Mobile IP control messages are specified in the IANA online database [48].

In addition, for Agent Discovery, Mobile IP makes use of the existing Router Advertisement and Router Solicitation messages defined for ICMP Router Discovery [5].

Mobile IP defines a general Extension mechanism to allow optional information to be carried by Mobile IP control messages or by ICMP Router Discovery messages. Some extensions have been specified to be encoded in the simple Type-Length-Value format described in Section 1.9.

Extensions allow variable amounts of information to be carried within each datagram. The end of the list of extensions is indicated by the total length of the IP datagram.

Two separately maintained sets of numbering spaces, from which Extension Type values are allocated, are used in Mobile IP:

- The first set consists of those Extensions that may appear in Mobile IP control messages (those sent to and from UDP port number 434). In this document, the following types are defined for Extensions appearing in Mobile IP control messages:

  0 One-byte Padding (encoded with neither Length nor Data field)
  32 Mobile-Home Authentication
  33 Mobile-Foreign Authentication
  34 Foreign-Home Authentication

- The second set consists of those Extensions that may appear in ICMP Router Discovery messages [5]. In this document, the following types are defined for Extensions appearing in ICMP Router Discovery messages:

  0 One-byte Padding (encoded with neither Length nor Data field)
  16 Mobility Agent Advertisement
  19 Prefix-Lengths

Each individual Extension is described in detail in a separate section later in this document. Up-to-date values for these Extension Type numbers are specified in the IANA online database [48].

Due to the separation (orthogonality) of these sets, it is conceivable that two Extensions that are defined at a later date could have identical Type values, so long as one of the Extensions may be used only in Mobile IP control messages and the other may be used only in ICMP Router Discovery messages.

The Type field in the Mobile IP extension structure can support up to 255 (skippable and non-skippable) uniquely identifiable extensions. When an Extension numbered in either of these sets within the range 0 through 127 is encountered but not recognized, the message containing that Extension MUST be silently discarded. When an Extension

numbered in the range 128 through 255 is encountered that is not recognized, that particular Extension is ignored, but the rest of the Extensions and message data MUST still be processed. The Length field of the Extension is used to skip the Data field in searching for the next Extension.

Unless additional structure is utilized for the extension types, new developments or additions to Mobile IP might require so many new extensions that the available space for extension types might run out. Two new extension structures are proposed to solve this problem. Certain types of extensions can be aggregated, using subtypes to identify the precise extension, for example as has been done with the Generic Authentication Keys extensions [46]. In many cases, this may reduce the rate of allocation for new values of the Type field.

Since the new extension structures will cause an efficient usage of the extension type space, it is recommended that new Mobile IP extensions follow one of the two new extension formats whenever there may be the possibility of grouping related extensions together.

The following subsections provide details about three distinct structures for Mobile IP extensions:

- The simple extension format
- The long extension format
- The short extension format

1.9. Type-Length-Value Extension Format for Mobile IP Extensions

The Type-Length-Value format illustrated in Figure 2 is used for extensions that are specified in this document. Since this simple extension structure does not encourage the most efficient usage of the extension type space, it is recommended that new Mobile IP extensions follow one of the two new extension formats specified in Section 1.10 or Section 1.11 whenever there may be the possibility of grouping related extensions together.

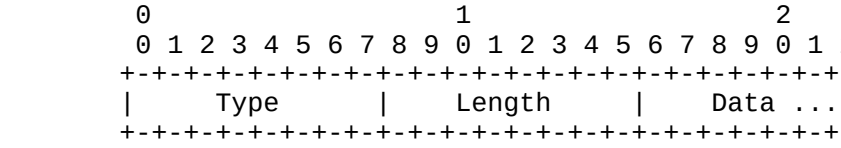


Figure 2: Type-Length-Value Extension Format for Mobile IPv4

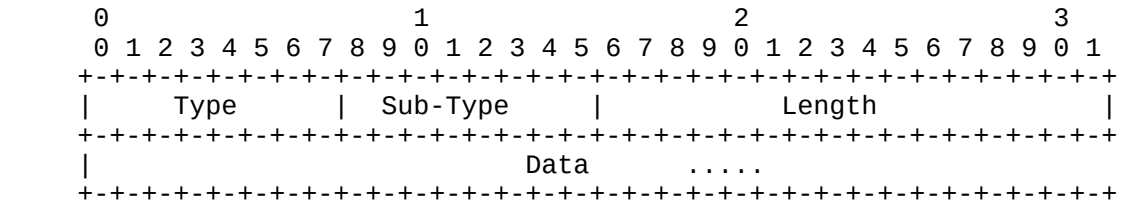
Type Indicates the particular type of Extension.

Length Indicates the length (in bytes) of the Data field within this Extension. The length does NOT include the Type and Length bytes.

Data The particular data associated with this Extension. This field may be zero or more bytes in length. The format and length of the Data field is determined by the Type and Length fields.

1.10. Long Extension Format

This format is applicable for non-skippable extensions that carry information of more than 256 bytes. Skippable extensions can never use the long format, because the receiver is not required to include parsing code and is likely to treat the 8 bits immediately following the Type as the Length field.



The Long Extension format requires that the following fields be specified as the first fields of the extension.

Type is the type, which describes a collection of extensions having a common data type.

Sub-Type is a unique number given to each member in the aggregated type.

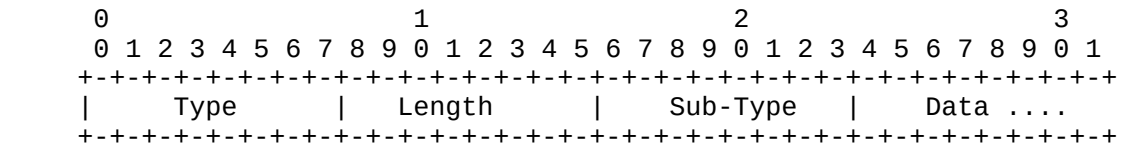
Length indicates the length (in bytes) of the Data field within this Extension. It does NOT include the Type, Length, and Sub-Type bytes.

Data is the data associated with the subtype of this extension. This specification does not place any additional structure on the subtype data.

Since the Length field is 16 bits wide, the extension data can exceed 256 bytes in length.

1.11. Short Extension Format

This format is compatible with the skippable extensions defined in Section 1.9. It is not applicable for extensions that require more than 256 bytes of data; for such extensions, use the format described in Section 1.10.



The Short Extension format requires that the following fields be specified as the first fields of the extension:

Type is the type, which describes a collection of extensions having a common data type.

Sub-Type is a unique number given to each member in the aggregated type.

Length 8-bit unsigned integer. Length of the extension, in bytes, excluding the extension Type and the extension Length fields. This field MUST be set to 1 plus the total length of the Data field.

Data is the data associated with this extension. This specification does not place any additional structure on the subtype data.

2. Agent Discovery

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

Mobile IP extends ICMP Router Discovery [5] as its primary mechanism for Agent Discovery. An Agent Advertisement is formed by including a Mobility Agent Advertisement Extension in an ICMP Router Advertisement message (Section 2.1). An Agent Solicitation message is identical to an ICMP Router Solicitation, except that its IP Time

to Live (TTL) MUST be set to 1 (Section 2.2). This section describes the message formats and procedures by which mobile nodes, foreign agents, and home agents cooperate to realize Agent Discovery.

Agent Advertisement and Agent Solicitation may not be necessary for link layers that already provide this functionality. The method by which mobile nodes establish link-layer connections with prospective agents is outside the scope of this document (but see Appendix A). The procedures described below assume that such link-layer connectivity has already been established.

No authentication is required for Agent Advertisement and Agent Solicitation messages. They MAY be authenticated using the IP Authentication Header [9], which is unrelated to the messages described in this document. Further specification of the way in which Advertisement and Solicitation messages may be authenticated is outside of the scope of this document.

2.1. Agent Advertisement

Agent Advertisements are transmitted by a mobility agent to advertise its services on a link. Mobile nodes use these advertisements to determine their current point of attachment to the Internet. An Agent Advertisement is an ICMP Router Advertisement that has been extended to also carry a Mobility Agent Advertisement Extension (Section 2.1.1) and, optionally, a Prefix-Lengths Extension (Section 2.1.2), One-byte Padding Extension (Section 2.1.3), or other Extensions that might be defined in the future.

Within an Agent Advertisement message, ICMP Router Advertisement fields of the message are required to conform to the following additional specifications:

- Link-Layer Fields

  Destination Address

  The link-layer Destination Address of a unicast Agent Advertisement MUST be the same as the source link-layer address of the Agent Solicitation that prompted the Advertisement.

- IP Fields

  TTL The TTL for all Agent Advertisements MUST be set to 1.

Destination Address

As specified for ICMP Router Discovery [5], the IP Destination Address of a multicast Agent Advertisement MUST be either the "all systems on this link" multicast address (224.0.0.1) [6] or the "limited broadcast" address (255.255.255.255). The subnet-directed broadcast address of the form <prefix>.<-1> cannot be used since mobile nodes will not generally know the prefix of the foreign network. When the Agent Advertisement is unicast to a mobile node, the IP home address of the mobile node SHOULD be used as the Destination Address.

- ICMP Fields

Code The Code field of the Agent Advertisement is interpreted as follows:

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

16 The mobility agent does not route common traffic. However, all foreign agents MUST (minimally) forward to a default router any datagrams received from a registered mobile node (Section 4.2.2).

Lifetime

The maximum length of time that the Advertisement is considered valid in the absence of further Advertisements.

Router Address(es)

See Section 2.3.1 for a discussion of the addresses that may appear in this portion of the Agent Advertisement.

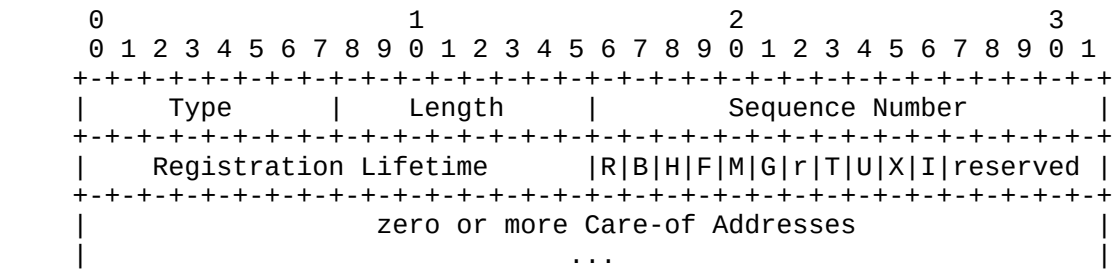
Num Addrs

The number of router addresses advertised in this message. Note that in an Agent Advertisement message, the number of router addresses specified in the ICMP Router Advertisement portion of the message MAY be set to 0. See Section 2.3.1 for details.

If sent periodically, the nominal interval at which Agent Advertisements are sent SHOULD be no longer than 1/3 of the advertisement Lifetime given in the ICMP header. This interval MAY be shorter than 1/3 the advertised Lifetime. This allows a mobile node to miss three successive advertisements before deleting the agent from its list of valid agents. The actual transmission time for each advertisement SHOULD be slightly randomized [5] in order to avoid synchronization and subsequent collisions with other Agent Advertisements that may be sent by other agents (or with other Router Advertisements sent by other routers). Note that this field has no relation to the "Registration Lifetime" field within the Mobility Agent Advertisement Extension defined below.

2.1.1. Mobility Agent Advertisement Extension

The Mobility Agent Advertisement Extension follows the ICMP Router Advertisement fields. It is used to indicate that an ICMP Router Advertisement message is also an Agent Advertisement being sent by a mobility agent. The Mobility Agent Advertisement Extension is defined as follows:



Type 16

Length (6 + 4*N), where 6 accounts for the number of bytes in the Sequence Number, Registration Lifetime, flags, and reserved fields, and N is the number of care-of addresses advertised.

Sequence Number

The count of Agent Advertisement messages sent since the agent was initialized (Section 2.3.2).

Registration Lifetime

The longest lifetime (measured in seconds) that this agent is willing to accept in any Registration Request. A value of 0xffff indicates infinity. This field has no relation to the "Lifetime" field within the ICMP Router Advertisement portion of the Agent Advertisement.

R Registration required. Registration with this foreign agent (or another foreign agent on this link) is required even when using a co-located care-of address.

B Busy. The foreign agent will not accept registrations from additional mobile nodes.

H Home agent. This agent offers service as a home agent on the link on which this Agent Advertisement message is sent.

F Foreign agent. This agent offers service as a foreign agent on the link on which this Agent Advertisement message is sent.

M Minimal encapsulation. This agent implements receiving tunneled datagrams that use minimal encapsulation [15].

G Generic Routing Encapsulation (GRE) encapsulation. This agent implements receiving tunneled datagrams that use GRE encapsulation [13].

r Sent as zero; ignored on reception. SHOULD NOT be allocated for any other uses.

T Foreign agent supports reverse tunneling as specified in [12].

U Mobility agent supports UDP Tunneling as specified in [27].

X Mobility agent supports Registration Revocation as specified in [28].

I Foreign agent supports Regional Registration as specified in [29].

reserved
Sent as zero; ignored on reception.

Care-of Address(es)

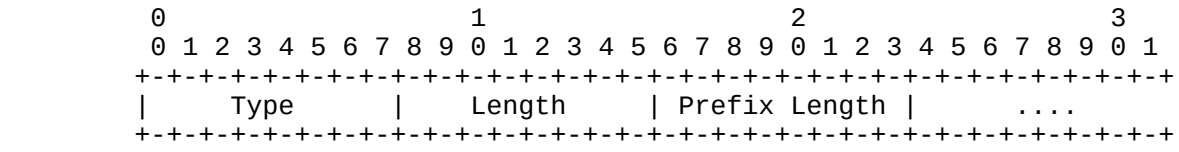
The advertised foreign agent care-of address(es) provided by this foreign agent. An Agent Advertisement MUST include at least one care-of address if the 'F' bit is set. The number of care-of addresses present is determined by the Length field in the Extension.

A home agent MUST always be prepared to serve the mobile nodes for which it is the home agent. A foreign agent may at times be too busy to serve additional mobile nodes; even so, it must continue to send Agent Advertisements, so that any mobile nodes already registered with it will know that they have not moved out of range of the foreign agent and that the foreign agent has not failed. A foreign agent may indicate that it is "too busy" to allow new mobile nodes to register with it, by setting the 'B' bit in its Agent Advertisements. An Agent Advertisement message MUST NOT have the 'B' bit set if the 'F' bit is not also set. Furthermore, at least one of the 'F' bit and the 'H' bit MUST be set in any Agent Advertisement message sent.

When a foreign agent wishes to require registration even from those mobile nodes that have acquired a co-located care-of address, it sets the 'R' bit to one. Because this bit applies only to foreign agents, an agent MUST NOT set the 'R' bit to one unless the 'F' bit is also set to one.

2.1.2. Prefix-Lengths Extension

The Prefix-Lengths Extension MAY follow the Mobility Agent Advertisement Extension. It is used to indicate the number of bits of network prefix that applies to each router address listed in the ICMP Router Advertisement portion of the Agent Advertisement. Note that the prefix lengths given DO NOT apply to care-of address(es) listed in the Mobility Agent Advertisement Extension. The Prefix-Lengths Extension is defined as follows:



Type 19 (Prefix-Lengths Extension)

Length N, where N is the value (possibly zero) of the Num Addrs field in the ICMP Router Advertisement portion of the Agent Advertisement.

Prefix Length(s)

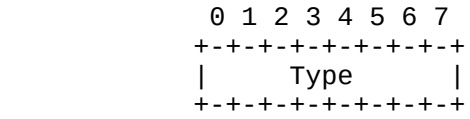
The number of leading bits that define the network number of the corresponding router address listed in the ICMP Router Advertisement portion of the message. The prefix length for each router address is encoded as a separate byte, in the order that the router addresses are listed in the ICMP Router Advertisement portion of the message.

See Section 2.4.2 for information about how the Prefix-Lengths Extension MAY be used by a mobile node when determining whether it has moved. See Appendix D for implementation details about the use of this Extension.

2.1.3. One-Byte Padding Extension

Some IP protocol implementations insist upon padding ICMP messages to an even number of bytes. If the ICMP length of an Agent Advertisement is odd, this Extension MAY be included in order to make the ICMP length even. Note that this Extension is NOT intended to be a general-purpose Extension to be included in order to word- or long-align the various fields of the Agent Advertisement. An Agent Advertisement SHOULD NOT include more than one One-byte Padding Extension and if present, this Extension SHOULD be the last Extension in the Agent Advertisement.

Note that, unlike other Extensions used in Mobile IP, the One-byte Padding Extension is encoded as a single byte, with no Length nor Data field present. The One-byte Padding Extension is defined as follows:



Type 0 (One-byte Padding Extension)

2.2. Agent Solicitation

An Agent Solicitation is identical to an ICMP Router Solicitation with the further restriction that the IP TTL Field MUST be set to 1.

2.3. Foreign Agent and Home Agent Considerations

Any mobility agent that cannot be discovered by a link-layer protocol MUST send Agent Advertisements. An agent that can be discovered by a link-layer protocol SHOULD also implement Agent Advertisements.

However, the Advertisements need not be sent, except when the site policy requires registration with the agent (i.e., when the 'R' bit is set), or as a response to a specific Agent Solicitation. All mobility agents MUST process packets that they receive addressed to the Mobile-Agents multicast group, at address 224.0.0.11. A mobile node MAY send an Agent Solicitation to 224.0.0.11. All mobility agents SHOULD respond to Agent Solicitations.

The same procedures, defaults, and constants are used in Agent Advertisement messages and Agent Solicitation messages as specified for ICMP Router Discovery [5], except that:

- o a mobility agent MUST limit the rate at which it sends broadcast or multicast Agent Advertisements; the maximum rate SHOULD be chosen so that the Advertisements do not consume a significant amount of network bandwidth, AND

- o a mobility agent that receives a Router Solicitation MUST NOT require that the IP Source Address is the address of a neighbor (i.e., an address that matches one of the router's own addresses on the arrival interface, under the subnet mask associated with that address of the router).

- o a mobility agent MAY be configured to send Agent Advertisements only in response to an Agent Solicitation message.

If the home network is not a virtual network, then the home agent for any mobile node SHOULD be located on the link identified by the mobile node's home address, and Agent Advertisement messages sent by the home agent on this link MUST have the 'H' bit set. In this way, mobile nodes on their own home network will be able to determine that they are indeed at home. Any Agent Advertisement messages sent by the home agent on another link to which it may be attached (if it is a mobility agent serving more than one link), MUST NOT have the 'H' bit set unless the home agent also serves as a home agent (to other mobile nodes) on that other link. A mobility agent MAY use different settings for each of the 'R', 'H', and 'F' bits on different network interfaces.

If the home network is a virtual network, the home network has no physical realization external to the home agent itself. In this case, there is no physical network link on which to send Agent Advertisement messages advertising the home agent. Mobile nodes for which this is the home network are always treated as being away from home.

On a particular subnet, either all mobility agents MUST include the Prefix-Lengths Extension or all of them MUST NOT include this Extension. Equivalently, it is prohibited for some agents on a given subnet to include the Extension but for others not to include it. Otherwise, one of the move detection algorithms designed for mobile nodes will not function properly (Section 2.4.2).

2.3.1. Advertised Router Addresses

The ICMP Router Advertisement portion of the Agent Advertisement MAY contain one or more router addresses. An agent SHOULD only put its own addresses, if any, in the advertisement. Whether or not its own address appears in the router addresses, a foreign agent MUST route datagrams it receives from registered mobile nodes (Section 3.7).

2.3.2. Sequence Numbers and Rollover Handling

The sequence number in Agent Advertisements ranges from 0 to 0xffff. After booting, an agent MUST use the number 0 for its first advertisement. Each subsequent advertisement MUST use the sequence number one greater, with the exception that the sequence number 0xffff MUST be followed by sequence number 256. In this way, mobile nodes can distinguish a reduction in the sequence number that occurs after a reboot from a reduction that results in rollover of the sequence number after it attains the value 0xffff.

2.4. Mobile Node Considerations

Every mobile node MUST implement Agent Solicitation. Solicitations SHOULD only be sent in the absence of Agent Advertisements and when a care-of address has not been determined through a link-layer protocol or other means. The mobile node uses the same procedures, defaults, and constants for Agent Solicitation as specified for ICMP Router Solicitation messages [5], except that the mobile node MAY solicit more often than once every three seconds, and that a mobile node that is currently not connected to any foreign agent MAY solicit more times than MAX_SOLICITATIONS.

The rate at which a mobile node sends solicitations MUST be limited by the mobile node. The mobile node MAY send three initial solicitations at a maximum rate of one per second while searching for an agent. After this, the rate at which solicitations are sent MUST be reduced so as to limit the overhead on the local link. Subsequent solicitations MUST be sent using a binary exponential backoff mechanism, doubling the interval between consecutive solicitations,

up to a maximum interval. The maximum interval SHOULD be chosen appropriately based upon the characteristics of the media over which the mobile node is soliciting. This maximum interval SHOULD be at least one minute between solicitations.

While still searching for an agent, the mobile node MUST NOT increase the rate at which it sends solicitations unless it has received a positive indication that it has moved to a new link. After successfully registering with an agent, the mobile node SHOULD also increase the rate at which it will send solicitations when it next begins searching for a new agent with which to register. The increased solicitation rate MAY revert to the maximum rate, but then MUST be limited in the manner described above. In all cases, the recommended solicitation intervals are nominal values. Mobile nodes MUST randomize their solicitation times around these nominal values as specified for ICMP Router Discovery [5].

Mobile nodes MUST process received Agent Advertisements. A mobile node can distinguish an Agent Advertisement message from other uses of the ICMP Router Advertisement message by examining the number of advertised addresses and the IP Total Length field. When the IP total length indicates that the ICMP message is longer than needed for the number of advertised addresses, the remaining data is interpreted as one or more Extensions. The presence of a Mobility Agent Advertisement Extension identifies the advertisement as an Agent Advertisement.

If there is more than one advertised address, the mobile node SHOULD pick the first address for its initial registration attempt. If the registration attempt fails with a status code indicating rejection by the foreign agent, the mobile node MAY retry the attempt with each subsequent advertised address in turn.

When multiple methods of agent discovery are in use, the mobile node SHOULD first attempt registration with agents including Mobility Agent Advertisement Extensions in their advertisements, in preference to those discovered by other means. This preference maximizes the likelihood that the registration will be recognized, thereby minimizing the number of registration attempts.

A mobile node MUST ignore reserved bits in Agent Advertisements, as opposed to discarding such advertisements. In this way, new bits can be defined later, without affecting the ability for mobile nodes to use the advertisements even when the newly defined bits are not understood.

2.4.1. Registration Required

When the mobile node receives an Agent Advertisement with the 'R' bit set, the mobile node SHOULD register through the foreign agent, even when the mobile node might be able to acquire its own co-located care-of address. This feature is intended to allow sites to enforce visiting policies (such as accounting) that require exchanges of authorization.

If formerly reserved bits require some kind of monitoring/enforcement at the foreign link, foreign agents implementing the new specification for the formerly reserved bits can set the 'R' bit. This has the effect of forcing the mobile node to register through the foreign agent, so the foreign agent could then monitor/enforce the policy.

2.4.2. Move Detection

Two primary mechanisms are provided for mobile nodes to detect when they have moved from one subnet to another. Other mechanisms MAY also be used. When the mobile node detects that it has moved, it SHOULD register (Section 3) with a suitable care-of address on the new foreign network. However, the mobile node MUST NOT register more frequently than once per second on average, as specified in Section 3.6.3.

2.4.2.1. Algorithm 1

The first method of move detection is based upon the Lifetime field within the main body of the ICMP Router Advertisement portion of the Agent Advertisement. A mobile node SHOULD record the Lifetime received in any Agent Advertisements, until that Lifetime expires. If the mobile node fails to receive another advertisement from the same agent within the specified Lifetime, it SHOULD assume that it has lost contact with that agent. If the mobile node has previously received an Agent Advertisement from another agent for which the Lifetime field has not yet expired, the mobile node MAY immediately attempt registration with that other agent. Otherwise, the mobile node SHOULD attempt to discover a new agent with which to register.

2.4.2.2. Algorithm 2

The second method uses network prefixes. The Prefix-Lengths Extension MAY be used in some cases by a mobile node to determine whether or not a newly received Agent Advertisement was received on the same subnet as the mobile node's current care-of address. If the prefixes differ, the mobile node MAY assume that it has moved. If a mobile node is currently using a foreign agent care-of address, the

mobile node SHOULD NOT use this method of move detection unless both the current agent and the new agent include the Prefix-Lengths Extension in their respective Agent Advertisements; if this Extension is missing from one or both of the advertisements, this method of move detection SHOULD NOT be used. Similarly, if a mobile node is using a co-located care-of address, it SHOULD NOT use this method of move detection unless the new agent includes the Prefix-Lengths Extension in its Advertisement and the mobile node knows the network prefix of its current co-located care-of address. On the expiration of its current registration, if this method indicates that the mobile node has moved, rather than re-registering with its current care-of address, a mobile node MAY choose instead to register with the foreign agent sending the new Advertisement with the different network prefix. The Agent Advertisement on which the new registration is based MUST NOT have expired according to its Lifetime field.

2.4.3. Returning Home

A mobile node can detect that it has returned to its home network when it receives an Agent Advertisement from its own home agent. If so, it SHOULD deregister with its home agent (Section 3). Before attempting to deregister, the mobile node SHOULD configure its routing table appropriately for its home network (Section 4.2.1). In addition, if the home network is using ARP [16], the mobile node MUST follow the procedures described in Section 4.6 with regard to ARP, proxy ARP, and gratuitous ARP.

2.4.4. Sequence Numbers and Rollover Handling

If a mobile node detects two successive values of the sequence number in the Agent Advertisements from the foreign agent with which it is registered, the second of which is less than the first and inside the range 0 to 255, the mobile node SHOULD register again. If the second value is less than the first but is greater than or equal to 256, the mobile node SHOULD assume that the sequence number has rolled over past its maximum value (0xffff), and that re-registration is not necessary (Section 2.3).

3. Registration

Mobile IP registration provides a flexible mechanism for mobile nodes to communicate their current reachability information to their home agent. It is the method by which mobile nodes:

- request forwarding services when visiting a foreign network,
- inform their home agent of their current care-of address,

- renew a registration that is due to expire, and/or
- deregister when they return home.

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

Several other (optional) capabilities are available through the registration procedure, which enable a mobile node to:

- discover its home address, if the mobile node is not configured with this information,
- maintain multiple simultaneous registrations, so that a copy of each datagram will be tunneled to each active care-of address,
- deregister specific care-of addresses while retaining other mobility bindings, and
- discover the address of a home agent if the mobile node is not configured with this information.

3.1. Registration Overview

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

- If a mobile node is registering a foreign agent care-of address, the mobile node MUST register via that foreign agent.
- If a mobile node is using a co-located care-of address, and receives an Agent Advertisement from a foreign agent on the link on which it is using this care-of address, the mobile node SHOULD register via that foreign agent (or via another foreign agent on this link) if the 'R' bit is set in the received Agent Advertisement message.
- If a mobile node is otherwise using a co-located care-of address, the mobile node MUST register directly with its home agent.

- o If a mobile node has returned to its home network and is (de)registering with its home agent, the mobile node MUST register directly with its home agent.

Both registration procedures involve the exchange of Registration Request and Registration Reply messages (Section 3.3 and Section 3.4). When registering via a foreign agent, the registration procedure requires the following four messages:

a. The mobile node sends a Registration Request to the prospective foreign agent to begin the registration process.

b. The foreign agent processes the Registration Request and then relays it to the home agent.

c. The home agent sends a Registration Reply to the foreign agent to grant or deny the Request.

d. The foreign agent processes the Registration Reply and then relays it to the mobile node to inform it of the disposition of its Request.

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

a. The mobile node sends a Registration Request to the home agent.

b. The home agent sends a Registration Reply to the mobile node, granting or denying the Request.

The registration messages defined in Sections 3.3 and 3.4 use the User Datagram Protocol (UDP) [17]. A nonzero UDP checksum SHOULD be included in the header, and MUST be checked by the recipient. A zero UDP checksum SHOULD be accepted by the recipient. The behavior of the mobile node and the home agent with respect to their mutual acceptance of packets with zero UDP checksums SHOULD be defined as part of the Mobility Security Association that exists between them.

3.2. Authentication

Each mobile node, foreign agent, and home agent MUST be able to support a Mobility Security Association for mobile entities, indexed by their SPI and IP address. In the case of the mobile node, this must be its home address. See Section 5.1 for requirements for support of authentication algorithms. Registration messages between a mobile node and its home agent MUST be authenticated with an authorization-enabling extension, e.g., the Mobile-Home Authentication Extension (Section 3.5.2). This extension MUST be the

first authentication extension; other foreign-agent-specific extensions MAY be added to the message after the mobile node computes the authentication.

3.3. Registration Request

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

IP fields:

Source Address

Typically the interface address from which the message is sent.

Destination Address

Typically that of the foreign agent or the home agent.

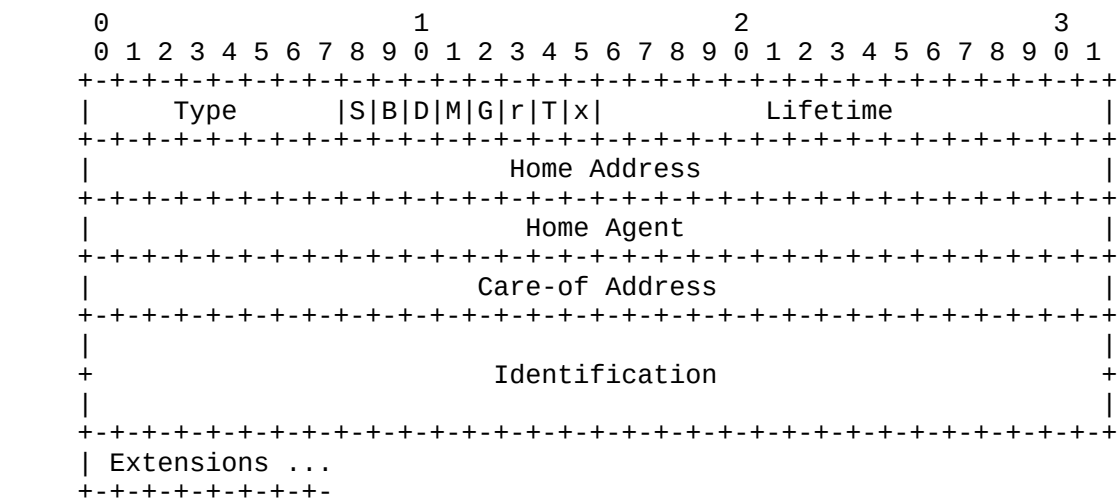
See Sections 3.6.1.1 and 3.7.2.2 for details.

UDP fields:

Source Port variable

Destination Port 434

The UDP header is followed by the Mobile IP fields shown below:



Type 1 (Registration Request)

S Simultaneous bindings. If the 'S' bit is set, the mobile node is requesting that the home agent retain its prior mobility bindings, as described in Section 3.6.1.2.

B Broadcast datagrams. If the 'B' bit is set, the mobile node requests that the home agent tunnel to it any broadcast datagrams that it receives on the home network, as described in Section 4.3.

D Decapsulation by mobile node. If the 'D' bit is set, the mobile node will itself decapsulate datagrams that are sent to the care-of address. That is, the mobile node is using a co-located care-of address.

M Minimal encapsulation. If the 'M' bit is set, the mobile node requests that its home agent use minimal encapsulation [16] for datagrams tunneled to the mobile node.

G GRE encapsulation. If the 'G' bit is set, the mobile node requests that its home agent use GRE encapsulation [13] for datagrams tunneled to the mobile node.

r Sent as zero; ignored on reception. SHOULD NOT be allocated for any other uses.

T Reverse Tunneling requested; see [12].

x Sent as zero; ignored on reception.

Lifetime

The number of seconds remaining before the registration is considered expired. A value of zero indicates a request for deregistration. A value of 0xffff indicates infinity.

Home Address

The IP address of the mobile node.

Home Agent

The IP address of the mobile node's home agent.

Care-of Address

The IP address for the end of the tunnel.

Identification

A 64-bit number, constructed by the mobile node, used for matching Registration Requests with Registration Replies, and for protecting against replay attacks of registration messages. See Sections 5.4 and 5.7.

Extensions

The fixed portion of the Registration Request is followed by one or more of the Extensions listed in Section 3.5. An authorization-enabling extension MUST be included in all Registration Requests. See Sections 3.6.1.3 and 3.7.2.2 for information on the relative order in which different extensions, when present, MUST be placed in a Registration Request message.

3.4. Registration Reply

A mobility agent typically returns a Registration Reply message to a mobile node that has sent a Registration Request message. If the mobile node is requesting service from a foreign agent, that foreign agent will typically receive the Reply from the home agent and

subsequently relay it to the mobile node. Reply messages contain the necessary codes to inform the mobile node about the status of its Request, along with the lifetime granted by the home agent, which MAY be smaller than the original Request.

The foreign agent MUST NOT increase the Lifetime selected by the mobile node in the Registration Request, since the Lifetime is covered by an authentication extension that enables authorization by the home agent. Such an extension contains authentication data that cannot be correctly (re)computed by the foreign agent. The home agent MUST NOT increase the Lifetime selected by the mobile node in the Registration Request, since doing so could increase it beyond the maximum Registration Lifetime allowed by the foreign agent. If the Lifetime received in the Registration Reply is greater than that in the Registration Request, the Lifetime in the Request MUST be used. When the Lifetime received in the Registration Reply is less than that in the Registration Request, the Lifetime in the Reply MUST be used.

IP fields:

Source Address

Typically copied from the Destination Address of the Registration Request to which the agent is replying. See Sections 3.7.2.3 and 3.8.3.2 for complete details.

Destination Address

Copied from the source address of the Registration Request to which the agent is replying.

UDP fields:

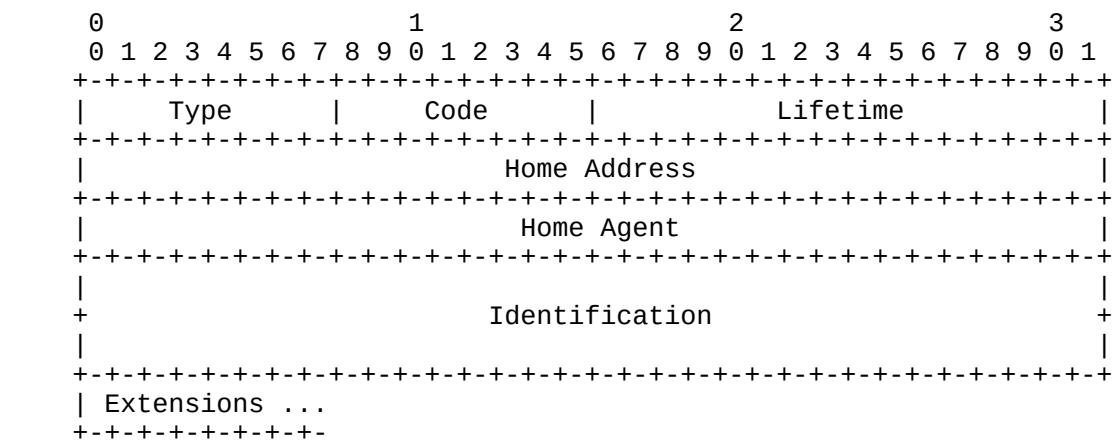
Source Port

Copied from the UDP Destination Port of the corresponding Registration Request.

Destination Port

Copied from the source port of the corresponding Registration Request (Section 3.7.1).

The UDP header is followed by the Mobile IP fields shown below:



Type 3 (Registration Reply)

Code

A value indicating the result of the Registration Request. See below for a list of currently defined code values.

Lifetime

If the Code field indicates that the registration was accepted, the Lifetime field is set to the number of seconds remaining before the registration is considered expired. A value of zero indicates that the mobile node has been deregistered. A value of 0xffff indicates infinity. If the Code field indicates that the registration was denied, the contents of the Lifetime field are unspecified and MUST be ignored on reception.

Home Address

The IP address of the mobile node.

Home Agent

The IP address of the mobile node’s home agent.

Identification

A 64-bit number used for matching Registration Requests with Registration Replies, and for protecting against replay attacks of registration messages. The value is based on the Identification field from the Registration Request message from the mobile node, and on the style of replay protection used in the security context between the mobile node and its home agent (defined by the Mobility Security Association between them, and SPI value in the authorization-enabling extension). See Sections 5.4 and 5.7.

Extensions

The fixed portion of the Registration Reply is followed by one or more of the Extensions listed in Section 3.5. An authorization-enabling extension MUST be included in all Registration Replies returned by the home agent. See Sections 3.7.2.2 and 3.8.3.3 for rules on placement of extensions to Reply messages.

The following values are defined for use within the Code field. Registration successful:

0 registration accepted
1 registration accepted, but simultaneous mobility bindings unsupported

Registration denied by the foreign agent:

64 reason unspecified
65 administratively prohibited
66 insufficient resources
67 mobile node failed authentication
68 home agent failed authentication
69 requested Lifetime too long
70 poorly formed Request
71 poorly formed Reply
72 requested encapsulation unavailable
73 reserved and unavailable
77 invalid care-of address
78 registration timeout
80 home network unreachable (ICMP error received)
81 home agent host unreachable (ICMP error received)
82 home agent port unreachable (ICMP error received)
88 home agent unreachable (other ICMP error received)
194 Invalid Home Agent Address

Registration denied by the home agent:

128 reason unspecified
129 administratively prohibited
130 insufficient resources
131 mobile node failed authentication
132 foreign agent failed authentication
133 registration Identification mismatch
134 poorly formed Request
135 too many simultaneous mobility bindings
136 unknown home agent address

Up-to-date values of the Code field are specified in the IANA online database [48].

3.5. Registration Extensions

3.5.1. Computing Authentication Extension Values

The Authenticator value computed for each authentication Extension MUST protect the following fields from the registration message:

- the UDP payload (that is, the Registration Request or Registration Reply data),
- all prior Extensions in their entirety, and
- the Type, Length, and SPI of this Extension.

The default authentication algorithm uses HMAC-MD5 [10] to compute a 128-bit "message digest" of the registration message. The data over which the HMAC is computed is defined as:

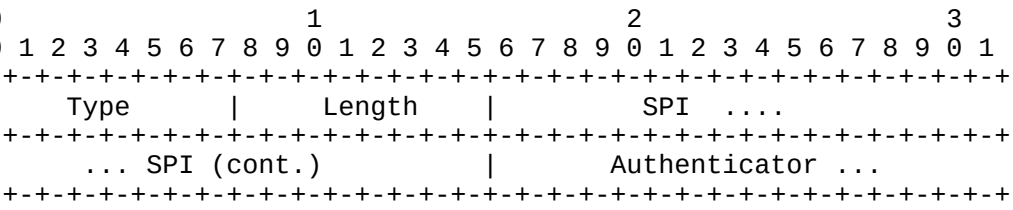
- the UDP payload (that is, the Registration Request or Registration Reply data),
- all prior Extensions in their entirety, and
- the Type, Length, and SPI of this Extension.

Note that the Authenticator field itself and the UDP header are NOT included in the computation of the default Authenticator value. See Section 5.1 for information about support requirements for message authentication codes, which are to be used with the various authentication Extensions.

The Security Parameter Index (SPI) within any of the authentication Extensions defines the security context that is used to compute the Authenticator value and that MUST be used by the receiver to check that value. In particular, the SPI selects the authentication algorithm and mode (Section 5.1) and secret (a shared key, or appropriate public/private key pair) used in computing the Authenticator. In order to ensure interoperability between different implementations of the Mobile IP protocol, an implementation MUST be able to associate any SPI value with any authentication algorithm and mode that it implements. In addition, all implementations of Mobile IP MUST implement the default authentication algorithm (HMAC-MD5) specified above.

3.5.2. Mobile-Home Authentication Extension

At least one authorization-enabling extension MUST be present in all Registration Requests, and also in all Registration Replies generated by the home agent. The Mobile-Home Authentication Extension is always an authorization-enabling extension for registration messages specified in this document. This requirement is intended to eliminate problems [30] that result from the uncontrolled propagation of remote redirects in the Internet. The location of the authorization-enabling extension marks the end of the data to be authenticated by the authorizing agent interpreting that authorization-enabling extension.



Type 32

Length 4 plus the number of bytes in the Authenticator.

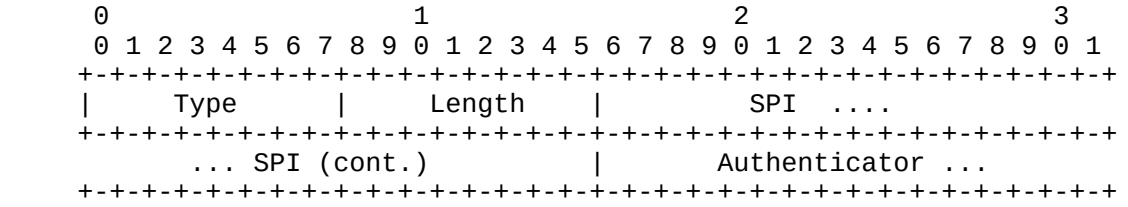
SPI Security Parameter Index (4 bytes). An opaque identifier (see Section 1.6).

Authenticator

(variable length) (See Section 3.5.1.)

3.5.3. Mobile-Foreign Authentication Extension

This Extension MAY be included in Registration Requests and Replies in cases in which a Mobility Security Association exists between the mobile node and the foreign agent. See Section 5.1 for information about support requirements for message authentication codes.



Type 33

Length 4 plus the number of bytes in the Authenticator.

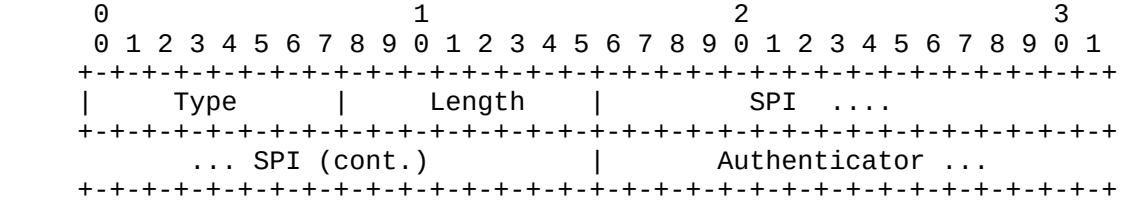
SPI Security Parameter Index (4 bytes). An opaque identifier (see Section 1.6).

Authenticator

(variable length) (See Section 3.5.1.)

3.5.4. Foreign-Home Authentication Extension

This Extension MAY be included in Registration Requests and Replies in cases in which a Mobility Security Association exists between the foreign agent and the home agent, as long as the Registration Request is not a deregistration (i.e., the mobile node requested a nonzero Lifetime and the home address is different than the care-of address). The Foreign-Home Authentication extension MUST NOT be applied to deregistration messages. See Section 5.1 for information about support requirements for message authentication codes.



Type 34

Length 4 plus the number of bytes in the Authenticator.

SPI Security Parameter Index (4 bytes). An opaque identifier (see Section 1.6).

Authenticator

(variable length) (See Section 3.5.1).

In order to perform the authentication, the home agent and the foreign agent are configured with a Mobility Security Association that is indexed by the SPI (in the appended Foreign-Home Authentication Extension) and the IP Source Address of the Registration Request. When the extension is used with a Registration Reply message, the foreign agent address MUST be used as the Destination IP Address in the IP header.

When this extension is applied to a Registration Request message, the Mobility Security Association for verifying the correctness of the authentication data is selected by the home agent based on the value of the Source IP Address field of the Registration Request and the SPI of the Authentication extension. The Source IP Address will be the same as the Care-of Address field of the Registration Request (see Section 3.7.2.2).

When this extension is applied to a Registration Reply message, the Mobility Security Association for verifying the correctness of the authentication data is selected by the foreign agent based on the value of the home agent Address field of the Registration Reply.

If the Care-of Address in the Registration Request is not in the Agent Advertisement, then the foreign agent MUST NOT append the Foreign-Home Authentication Extension when relaying the message to the home agent. Moreover, for a deregistration message (i.e., Lifetime = 0), the foreign agent MUST NOT append the Foreign-Home Authentication Extension when relaying the message to the home agent. Consequently, when the home agent (HA) receives a deregistration request that does not contain a Foreign-Home Authentication Extension, it MUST NOT for this reason discard the request as part of security association processing.

3.6. Mobile Node Considerations

A mobile node MUST be configured (statically or dynamically) with a netmask and a Mobility Security Association for each of its home agents. In addition, a mobile node MAY be configured with its home address, and the IP address of one or more of its home agents; otherwise, the mobile node MAY discover a home agent using the procedures described in Section 3.6.1.2.

If the mobile node is not configured with a home address, it MAY use the Mobile Node Network Access Identifier (NAI) extension [2] to identify itself, and set the Home Address field of the Registration Request to 0.0.0.0. In this case, the mobile node MUST be able to assign its home address after extracting this information from the Registration Reply from the home agent.

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

- the link-layer address of the foreign agent to which the Registration Request was sent, if applicable,
- the IP Destination Address of the Registration Request,
- the care-of address used in the registration,
- the Identification value sent in the registration,
- the originally requested Lifetime, and
- the remaining Lifetime of the pending registration.

A mobile node SHOULD initiate a registration whenever it detects a change in its network connectivity. See Section 2.4.2 for methods by which mobile nodes MAY make such a determination. When it is away from home, the mobile node's Registration Request allows its home agent to create or modify a mobility binding for it. When it is at home, the mobile node's (de)Registration Request allows its home agent to delete any previous mobility binding(s) for it. A mobile node operates without the support of mobility functions when it is at home.

There are other conditions under which the mobile node SHOULD (re)register with its foreign agent, such as when the mobile node detects that the foreign agent has rebooted (as specified in Section 2.4.4) and when the current registration's Lifetime is near expiration.

In the absence of link-layer indications of changes in point of attachment, Agent Advertisements from new agents SHOULD NOT cause a mobile node to attempt a new registration, if its current registration has not expired and it is still also receiving Agent Advertisements from the foreign agent with which it is currently registered. In the absence of link-layer indications, a mobile node MUST NOT attempt to register more often than once per second.

A mobile node MAY register with a different agent when transport-layer protocols indicate excessive retransmissions. A mobile node MUST NOT consider reception of an ICMP Redirect from a foreign agent that is currently providing service to it as reason to register with a new foreign agent. Within these constraints, the mobile node MAY register again at any time.

Appendix C shows some examples of how the fields in registration messages would be set up in some typical registration scenarios.

3.6.1. Sending Registration Requests

The following sections specify details for the values that the mobile node MUST supply in the fields of Registration Request messages.

3.6.1.1. IP Fields

This section provides the specific rules by which mobile nodes pick values for the IP header fields of a Registration Request.

IP Source Address:

- When registering on a foreign network with a co-located care-of address, the IP source address MUST be the care-of address.
- Otherwise, if the mobile node does not have a home address, the IP source address MUST be 0.0.0.0.
- In all other circumstances, the IP source address MUST be the mobile node’s home address.

IP Destination Address:

- When the mobile node has discovered the agent with which it is registering, through some means (e.g., link-layer) that does not provide the IP address of the agent (the IP address of the agent is unknown to the mobile node), then the "All Mobility Agents" multicast address (224.0.0.11) MUST be used. In this case, the mobile node MUST use the agent’s link-layer unicast address in order to deliver the datagram to the correct agent.
- When registering with a foreign agent, the address of the agent as learned from the IP source address of the corresponding Agent Advertisement MUST be used. This MAY be an address that does not appear as an advertised care-of address in the Agent Advertisement. In addition, when transmitting this Registration

Request message, the mobile node MUST use a link-layer Destination Address copied from the link-layer source address of the Agent Advertisement message in which it learned this foreign agent's IP address.

- o When the mobile node is registering directly with its home agent and knows the (unicast) IP address of its home agent, the Destination Address MUST be set to this address.

- o If the mobile node is registering directly with its home agent, but does not know the IP address of its home agent, the mobile node may use dynamic home agent address resolution to automatically determine the IP address of its home agent (Section 3.6.1.2). In this case, the IP Destination Address is set to the subnet-directed broadcast address of the mobile node's home network. This address MUST NOT be used as the Destination IP Address if the mobile node is registering via a foreign agent, although it MAY be used as the home agent address in the body of the Registration Request when registering via a foreign agent.

IP Time to Live:

- o The IP TTL field MUST be set to 1 if the IP Destination Address is set to the "All Mobility Agents" multicast address as described above. Otherwise, a suitable value should be chosen in accordance with standard IP practice [18].

3.6.1.2. Registration Request Fields

This section provides specific rules by which mobile nodes pick values for the fields within the fixed portion of a Registration Request.

A mobile node MAY set the 'S' bit in order to request that the home agent maintain prior mobility binding(s). Otherwise, the home agent deletes any previous binding(s) and replaces them with the new binding specified in the Registration Request. Multiple simultaneous mobility bindings are likely to be useful when a mobile node using at least one wireless network interface moves within wireless transmission range of more than one foreign agent. IP explicitly allows duplication of datagrams. When the home agent allows simultaneous bindings, it will tunnel a separate copy of each arriving datagram to each care-of address, and the mobile node will receive multiple copies of datagrams destined to it.

The mobile node SHOULD set the 'D' bit if it is registering with a co-located care-of address. Otherwise, the 'D' bit MUST NOT be set.

A mobile node MAY set the 'B' bit to request its home agent to forward to it a copy of broadcast datagrams received by its home agent from the home network. The method used by the home agent to forward broadcast datagrams depends on the type of care-of address registered by the mobile node, as determined by the 'D' bit in the mobile node's Registration Request:

- If the 'D' bit is set, then the mobile node has indicated that it will decapsulate any datagrams tunneled to this care-of address itself (the mobile node is using a co-located care-of address). In this case, to forward such a received broadcast datagram to the mobile node, the home agent MUST tunnel it to this care-of address. The mobile node detunnels the received datagram in the same way as any other datagram tunneled directly to it.

- If the 'D' bit is NOT set, then the mobile node has indicated that it is using a foreign agent care-of address, and that the foreign agent will thus decapsulate arriving datagrams before forwarding them to the mobile node. In this case, to forward such a received broadcast datagram to the mobile node, the home agent MUST first encapsulate the broadcast datagram in a unicast datagram addressed to the mobile node's home address, and then MUST tunnel this resulting datagram to the mobile node's care-of address.

  When decapsulated by the foreign agent, the inner datagram will thus be a unicast IP datagram addressed to the mobile node, identifying to the foreign agent the intended destination of the encapsulated broadcast datagram, and will be delivered to the mobile node in the same way as any tunneled datagram arriving for the mobile node. The foreign agent MUST NOT decapsulate the encapsulated broadcast datagram and MUST NOT use a local network broadcast to transmit it to the mobile node. The mobile node thus MUST decapsulate the encapsulated broadcast datagram itself, and thus MUST NOT set the 'B' bit in its Registration Request in this case unless it is capable of decapsulating datagrams.

The mobile node MAY request alternative forms of encapsulation by setting the 'M' bit and/or the 'G' bit, but only if the mobile node is decapsulating its own datagrams (the mobile node is using a co-located care-of address) or if its foreign agent has indicated support for these forms of encapsulation by setting the corresponding bits in the Mobility Agent Advertisement Extension of an Agent Advertisement received by the mobile node. Otherwise, the mobile node MUST NOT set these bits.

The Lifetime field is chosen as follows:

- If the mobile node is registering with a foreign agent, the Lifetime SHOULD NOT exceed the value in the Registration Lifetime field of the Agent Advertisement message received from the foreign agent. When the method by which the care-of address is learned does not include a Lifetime, the default ICMP Router Advertisement Lifetime (1800 seconds) MAY be used.

- The mobile node MAY ask a home agent to delete a particular mobility binding, by sending a Registration Request with the care-of address for this binding, with the Lifetime field set to zero (Section 3.8.2).

- Similarly, a Lifetime of zero is used when the mobile node deregisters all care-of addresses, such as upon returning home.

The Home Address field MUST be set to the mobile node's home address, if this information is known. Otherwise, the Home Address field MUST be set to zeroes.

The Home Agent field MUST be set to the address of the mobile node's home agent, if the mobile node knows this address. Otherwise, the mobile node MAY use dynamic home agent address resolution to learn the address of its home agent. In this case, the mobile node MUST set the Home Agent field to the subnet-directed broadcast address of the mobile node's home network. Each home agent receiving such a Registration Request with a broadcast Destination Address MUST reject the mobile node's registration and SHOULD return a rejection Registration Reply indicating its unicast IP address for use by the mobile node in a future registration attempt.

The Care-of Address field MUST be set to the value of the particular care-of address that the mobile node wishes to (de)register. In the special case in which a mobile node wishes to deregister all care-of addresses, it MUST set this field to its home address.

The mobile node chooses the Identification field in accordance with the style of replay protection it uses with its home agent. This is part of the Mobility Security Association the mobile node shares with its home agent. See Section 5.7 for the method by which the mobile node computes the Identification field.

3.6.1.3. Extensions

This section describes the ordering of any mandatory and any optional Extensions that a mobile node appends to a Registration Request. This ordering is REQUIRED:

a. The IP header, followed by the UDP header, followed by the fixed-length portion of the Registration Request, followed by

b. If present, any non-authentication Extensions expected to be used by the home agent or other authorizing agent (which may or may not also be useful to the foreign agent), followed by

c. All authorization-enabling extensions (see Section 1.6), followed by

d. If present, any non-authentication Extensions used only by the foreign agent, followed by

e. The Mobile-Foreign Authentication Extension, if present.

Note that items (a) and (c) MUST appear in every Registration Request sent by the mobile node. Items (b), (d), and (e) are optional. However, item (e) MUST be included when the mobile node and the foreign agent share a Mobility Security Association.

3.6.2. Receiving Registration Replies

Registration Replies will be received by the mobile node in response to its Registration Requests. Registration Replies generally fall into three categories:

- the registration was accepted,
- the registration was denied by the foreign agent, or
- the registration was denied by the home agent.

The remainder of this section describes the Registration Reply handling by a mobile node in each of these three categories.

3.6.2.1. Validity Checks

Registration Replies with an invalid, non-zero UDP checksum MUST be silently discarded.

In addition, the low-order 32 bits of the Identification field in the Registration Reply MUST be compared to the low-order 32 bits of the Identification field in the most recent Registration Request sent to the replying agent. If they do not match, the Reply MUST be silently discarded.

Also, the Registration Reply MUST be checked for presence of an authorization-enabling extension. For all Registration Reply messages containing a status code indicating status from the home agent, the mobile node MUST check for the presence of an authorization-enabling extension, acting in accordance with the Code field in the Reply. The rules are as follows:

a. If the mobile node and the foreign agent share a Mobility Security Association, exactly one Mobile-Foreign Authentication Extension MUST be present in the Registration Reply, and the mobile node MUST check the Authenticator value in the Extension. If no Mobile-Foreign Authentication Extension is found, or if more than one Mobile-Foreign Authentication Extension is found, or if the Authenticator is invalid, the mobile node MUST silently discard the Reply and SHOULD log the event as a security exception.

b. If the Code field indicates that service is denied by the home agent, or if the Code field indicates that the registration was accepted by the home agent, exactly one Mobile-Home Authentication Extension MUST be present in the Registration Reply, and the mobile node MUST check the Authenticator value in the Extension. If the Registration Reply was generated by the home agent but no Mobile-Home Authentication Extension is found, or if more than one Mobile-Home Authentication Extension is found, or if the Authenticator is invalid, the mobile node MUST silently discard the Reply and SHOULD log the event as a security exception.

If the Code field indicates an authentication failure, either at the foreign agent or the home agent, then it is quite possible that any authenticators in the Registration Reply will also be in error. This could happen, for example, if the shared secret between the mobile node and home agent was erroneously configured. The mobile node SHOULD log such errors as security exceptions.

3.6.2.2. Registration Request Accepted

If the Code field indicates that the request has been accepted, the mobile node SHOULD configure its routing table appropriately for its current point of attachment (Section 4.2.1).

If the mobile node is returning to its home network and that network is one that implements ARP, the mobile node MUST follow the procedures described in Section 4.6 with regard to ARP, proxy ARP, and gratuitous ARP.

If the mobile node has registered on a foreign network, it SHOULD re-register before the expiration of the Lifetime of its registration. As described in Section 3.6, for each pending Registration Request, the mobile node MUST maintain the remaining lifetime of this pending registration, as well as the original Lifetime from the Registration Request. When the mobile node receives a valid Registration Reply, the mobile node MUST decrease its view of the remaining lifetime of the registration by the amount by which the home agent decreased the originally requested Lifetime. This procedure is equivalent to the mobile node starting a timer for the granted Lifetime at the time it sent the Registration Request, even though the granted Lifetime is not known to the mobile node until the Registration Reply is received. Since the Registration Request is certainly sent before the home agent begins timing the registration Lifetime (also based on the granted Lifetime), this procedure ensures that the mobile node will re-register before the home agent expires and deletes the registration, in spite of possibly non-negligible transmission delays for the original Registration Request and Reply that started the timing of the Lifetime at the mobile node and its home agent.

3.6.2.3. Registration Request Denied

If the Code field indicates that service is being denied, the mobile node SHOULD log the error. In certain cases, the mobile node may be able to "repair" the error. These include:

Code 69: (Denied by foreign agent, requested Lifetime too long)

In this case, the Lifetime field in the Registration Reply will contain the maximum Lifetime value that the foreign agent is willing to accept in any Registration Request. The mobile node MAY attempt to register with this same agent, using a Lifetime in the Registration Request that MUST be less than or equal to the value specified in the Reply.

Code 133: (Denied by home agent, registration Identification mismatch)

In this case, the Identification field in the Registration Reply will contain a value that allows the mobile node to synchronize with the home agent, based upon the style of replay protection in effect (Section 5.7). The mobile node MUST adjust the parameters it uses to compute the Identification field based upon the information in the Registration Reply, before issuing any future Registration Requests.

Code 136: (Denied by home agent, unknown home agent address)

This code is returned by a home agent when the mobile node is performing dynamic home agent address resolution as described in Sections 3.6.1.1 and 3.6.1.2. In this case, the Home Agent field within the Reply will contain the unicast IP address of the home agent returning the Reply. The mobile node MAY then attempt to register with this home agent in future Registration Requests. In addition, the mobile node SHOULD adjust the parameters it uses to compute the Identification field based upon the corresponding field in the Registration Reply, before issuing any future Registration Requests.

3.6.3. Registration Retransmission

When no Registration Reply has been received within a reasonable time, another Registration Request MAY be transmitted. When timestamps are used, a new registration Identification is chosen for each retransmission; thus, it counts as a new registration. When nonces are used, the unanswered Request is retransmitted unchanged; thus, the retransmission does not count as a new registration (Section 5.7). In this way, a retransmission will not require the home agent to resynchronize with the mobile node by issuing another nonce in the case in which the original Registration Request (rather than its Registration Reply) was lost by the network.

The maximum time until a new Registration Request is sent SHOULD be no greater than the requested Lifetime of the Registration Request. The minimum value SHOULD be large enough to account for the size of the messages, twice the round-trip time for transmission to the home agent, and at least an additional 100 milliseconds to allow for processing the messages before responding. The round-trip time for transmission to the home agent will be at least as large as the time required to transmit the messages at the link speed of the mobile node’s current point of attachment. Some circuits add another 200 milliseconds of satellite delay in the total round-trip time to the home agent. The minimum time between Registration Requests MUST NOT be less than 1 second. Each successive retransmission timeout period SHOULD be at least twice the previous period, as long as that is less than the maximum as specified above.

3.7. Foreign Agent Considerations

The foreign agent plays a mostly passive role in Mobile IP registration. It relays Registration Requests between mobile nodes and home agents, and, when it provides the care-of address,

decapsulates datagrams for delivery to the mobile node. It SHOULD also send periodic Agent Advertisement messages to advertise its presence as described in Section 2.3, if not detectable by link-layer means.

A foreign agent MUST NOT transmit a Registration Request, unless the request is being relayed from a mobile node to that mobile node's home agent. A foreign agent MUST NOT transmit a Registration Reply except when relaying a Registration Reply received from a mobile node's home agent, or when replying to a Registration Request received from a mobile node in the case in which the foreign agent is denying service to the mobile node. In particular, a foreign agent MUST NOT generate a Registration Request or Reply because a mobile node's registration Lifetime has expired. A foreign agent also MUST NOT originate a Registration Request message that asks for deregistration of a mobile node; however, it MUST relay well-formed (de)Registration Requests originated by a mobile node.

3.7.1. Configuration and Registration Tables

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

- the link-layer source address of the mobile node
- the IP Source Address (the mobile node's home address) or its co-located care-of address (see description of the 'R' bit in Section 2.1.1)
- the IP Destination Address (as specified in Section 3.6.1.1)
- the UDP Source Port
- the home agent address
- the Identification field
- the requested registration Lifetime, and
- the remaining Lifetime of the pending or current registration

If there is an NAI extension in the Registration Request message (often, for example, when the mobile node's Home Address is zero), then the foreign agent MUST follow the procedures specified in RFC

2794 [2]. In particular, if the foreign agent cannot manage pending Registration Request records with such a zero Home Address for the mobile node, the foreign agent MUST return a Registration Reply with a code indicating NONZERO_HOMEADDR_REQD (see [2]).

The foreign agent MAY configure a maximum number of pending registrations that it is willing to maintain (typically 5). Additional registrations SHOULD then be rejected by the foreign agent with Code 66. The foreign agent MAY delete any pending Registration Request after the request has been pending for more than 7 seconds; in this case, the foreign agent SHOULD reject the Request with Code 78 (registration timeout).

As with any node on the Internet, a foreign agent MAY also share Mobility Security Associations with any other nodes. When relaying a Registration Request from a mobile node to its home agent, if the foreign agent shares a Mobility Security Association with the home agent, it MUST add a Foreign-Home Authentication Extension to the Request. In this case, when the Registration Reply has nonzero Lifetime, the foreign agent MUST check the required Foreign-Home Authentication Extension in the Registration Reply from the home agent (Sections 3.3 and 3.4). Similarly, when receiving a Registration Request from a mobile node, if the foreign agent shares a Mobility Security Association with the mobile node, it MUST check the required Mobile-Foreign Authentication Extension in the Request and MUST add a Mobile-Foreign Authentication Extension to the Registration Reply to the mobile node.

3.7.2. Receiving Registration Requests

If the foreign agent accepts a Registration Request from a mobile node, it checks to make sure that the indicated home agent address does not belong to any network interface of the foreign agent. If not, the foreign agent then MUST relay the Request to the indicated home agent. Otherwise, if the foreign agent denies the Request, it MUST send a Registration Reply to the mobile node with an appropriate denial code, except in cases where the foreign agent would be required to send out more than one such denial per second to the same mobile node. The following sections describe this behavior in more detail.

If the foreign agent has configured one of its network interfaces with the IP address specified by the mobile node as its home agent address, the foreign agent MUST NOT forward the Request again. If the foreign agent serves the mobile node as a home agent, the foreign agent follows the procedures specified in Section 3.8.2. Otherwise,

if the foreign agent does not serve the mobile node as a home agent, the foreign agent rejects the Registration Request with Code 194 (Invalid Home Agent Address).

If a foreign agent receives a Registration Request from a mobile node in its visitor list, the existing visitor list entry for the mobile node SHOULD NOT be deleted or modified until the foreign agent receives a valid Registration Reply from the home agent with a code indicating success. The foreign agent MUST record the new pending Request as a separate part of the existing visitor list entry for the mobile node. If the Registration Request asks for deregistration, the existing visitor list entry for the mobile node SHOULD NOT be deleted until the foreign agent has received a successful Registration Reply. If the Registration Reply indicates that the Request (for registration or deregistration) was denied by the home agent, the existing visitor list entry for the mobile node MUST NOT be modified as a result of receiving the Registration Reply.

3.7.2.1. Validity Checks

Registration Requests with an invalid, non-zero UDP checksum MUST be silently discarded. Requests with non-zero bits in reserved fields MUST be rejected with Code 70 (poorly formed Request). Requests with the 'D' bit set to 0, nonzero Lifetime, and specifying a care-of address not offered by the foreign agent, MUST be rejected with Code 77 (invalid care-of address).

Also, the authentication in the Registration Request MUST be checked. If the foreign agent and the mobile node share a Mobility Security Association, exactly one Mobile-Foreign Authentication Extension MUST be present in the Registration Request, and the foreign agent MUST check the Authenticator value in the Extension. If no Mobile-Foreign Authentication Extension is found, or if more than one Mobile-Foreign Authentication Extension is found, or if the Authenticator is invalid, the foreign agent MUST silently discard the Request and SHOULD log the event as a security exception. The foreign agent also SHOULD send a Registration Reply to the mobile node with Code 67.

3.7.2.2. Forwarding a Valid Request to the Home Agent

If the foreign agent accepts the mobile node's Registration Request, it MUST relay the Request to the mobile node's home agent as specified in the Home Agent field of the Registration Request. The foreign agent MUST NOT modify any of the fields beginning with the fixed portion of the Registration Request up through and including the Mobile-Home Authentication Extension or other authentication extension supplied by the mobile node as an authorization-enabling

extension for the home agent. Otherwise, an authentication failure is very likely to occur at the home agent. In addition, the foreign agent proceeds as follows:

- It MUST process and remove any extensions that do not precede any authorization-enabling extension,
- It MAY append any of its own non-authentication Extensions of relevance to the home agent, if applicable, and
- If the foreign agent shares a Mobility Security Association with the home agent, and the Request has Lifetime != 0, then it MUST append the Foreign-Home Authentication Extension.

Specific fields within the IP header and the UDP header of the relayed Registration Request MUST be set as follows:

IP Source Address

The care-of address offered by the foreign agent for the mobile node sending the Registration Request.

IP Destination Address

Copied from the Home Agent field within the Registration Request.

UDP Source Port

variable

UDP Destination Port

434

After forwarding a valid Registration Request to the home agent, the foreign agent MUST begin timing the remaining lifetime of the pending registration based on the Lifetime in the Registration Request. If this lifetime expires before receiving a valid Registration Reply, the foreign agent MUST delete its visitor list entry for this pending registration.

3.7.2.3. Denying Invalid Requests

If the foreign agent denies the mobile node's Registration Request for any reason, it SHOULD send the mobile node a Registration Reply with a suitable denial code. In such a case, the Home Address, Home Agent, and Identification fields within the Registration Reply are copied from the corresponding fields of the Registration Request.

If the Reserved field is nonzero, the foreign agent MUST deny the Request and SHOULD return a Registration Reply with Status Code 70 to the mobile node. If the Request is being denied because the requested Lifetime is too long, the foreign agent sets the Lifetime in the Reply to the maximum Lifetime value it is willing to accept in any Registration Request, and sets the Code field to 69. Otherwise, the Lifetime SHOULD be copied from the Lifetime field in the Request.

Specific fields within the IP header and the UDP header of the Registration Reply MUST be set as follows:

IP Source Address

Copied from the IP Destination Address of the Registration Request, unless the "All Agents Multicast" address was used. In this case, the foreign agent's address (on the interface from which the message will be sent) MUST be used.

IP Destination Address

If the Registration Reply is generated by the foreign agent in order to reject a mobile node's Registration Request, and the Registration Request contains a Home Address that is not 0.0.0.0, then the IP Destination Address is copied from the Home Address field of the Registration Request. Otherwise, if the Registration Reply is received from the home agent, and contains a Home Address that is not 0.0.0.0, then the IP Destination Address is copied from the Home Address field of the Registration Reply. Otherwise, the IP Destination Address of the Registration Reply is set to be 255.255.255.255.

UDP Source Port

434

UDP Destination Port

Copied from the UDP Source Port of the Registration Request.

3.7.3. Receiving Registration Replies

The foreign agent updates its visitor list when it receives a valid Registration Reply from a home agent. It then relays the Registration Reply to the mobile node. The following sections describe this behavior in more detail.

If upon relaying a Registration Request to a home agent, the foreign agent receives an ICMP error message instead of a Registration Reply, then the foreign agent SHOULD send to the mobile node a Registration Reply with an appropriate "home agent unreachable" failure code (within the range 80-95, inclusive). See Section 3.7.2.3 for details on building the Registration Reply.

3.7.3.1. Validity Checks

Registration Replies with an invalid, non-zero UDP checksum MUST be silently discarded.

When a foreign agent receives a Registration Reply message, it MUST search its visitor list for a pending Registration Request with the same mobile node home address as indicated in the Reply. If there are multiple entries with the same home address, and if the Registration Reply has the Mobile Node NAI extension [2], the foreign agent MUST use the NAI to disambiguate the pending Registration Requests with the same home address. If no matching pending Request is found, and if the Registration Reply does not correspond with any pending Registration Request with a zero mobile node home address (see Section 3.7.1), the foreign agent MUST silently discard the Reply. The foreign agent MUST also silently discard the Reply if the low-order 32 bits of the Identification field in the Reply do not match those in the Request.

Also, the authentication in the Registration Reply MUST be checked. If the foreign agent and the home agent share a Mobility Security Association, exactly one Foreign-Home Authentication Extension MUST be present in the Registration Reply, and the foreign agent MUST check the Authenticator value in the Extension. If no Foreign-Home Authentication Extension is found, or if more than one Foreign-Home Authentication Extension is found, or if the Authenticator is invalid, the foreign agent MUST silently discard the Reply and SHOULD log the event as a security exception. The foreign agent also MUST reject the mobile node’s registration and SHOULD send a Registration Reply to the mobile node with Code 68.

3.7.3.2. Forwarding Replies to the Mobile Node

A Registration Reply that satisfies the validity checks of Section 3.8.2.1 is relayed to the mobile node. The foreign agent MUST also update its visitor list entry for the mobile node to reflect the results of the Registration Request, as indicated by the Code field in the Reply. If the code indicates that the home agent has accepted the registration and the Lifetime field is nonzero, the foreign agent SHOULD set the Lifetime in the visitor list entry to the minimum of the following two values:

- the value specified in the Lifetime field of the Registration Reply, and
- the foreign agent's own maximum value for allowable registration Lifetime.

If, instead, the code indicates that the Lifetime field is zero, the foreign agent MUST delete its visitor list entry for the mobile node. Finally, if the code indicates that the registration was denied by the home agent, the foreign agent MUST delete its pending registration list entry, but not its visitor list entry, for the mobile node.

The foreign agent MUST NOT modify any of the fields beginning with the fixed portion of the Registration Reply up through and including the Mobile-Home Authentication Extension. Otherwise, an authentication failure is very likely to occur at the mobile node. In addition, the foreign agent SHOULD perform the following additional procedures:

- It MUST process and remove any Extensions that are not covered by any authorization-enabling extension,
- It MAY append its own non-authentication Extensions that supply information to the mobile node, if applicable, and
- It MUST append the Mobile-Foreign Authentication Extension, if the foreign agent shares a Mobility Security Association with the mobile node.

Specific fields within the IP header and the UDP header of the relayed Registration Reply are set according to the same rules specified in Section 3.7.2.3.

After forwarding a valid Registration Reply to the mobile node, the foreign agent MUST update its visitor list entry for this registration as follows. If the Registration Reply indicates that

the registration was accepted by the home agent, the foreign agent resets its timer of the lifetime of the registration to the Lifetime granted in the Registration Reply; unlike the mobile node's timing of the registration lifetime as described in Section 3.6.2.2, the foreign agent considers this lifetime to begin when it forwards the Registration Reply message, ensuring that the foreign agent will not expire the registration before the mobile node does. On the other hand, if the Registration Reply indicates that the registration was rejected by the home agent, the foreign agent deletes its visitor list entry for this attempted registration.

3.8. Home Agent Considerations

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

A home agent MUST NOT transmit a Registration Reply except when replying to a Registration Request received from a mobile node. In particular, the home agent MUST NOT generate a Registration Reply to indicate that the Lifetime has expired.

3.8.1. Configuration and Registration Tables

Each home agent MUST be configured with an IP address and with the prefix size for the home network. The home agent MUST be configured with the Mobility Security Association of each authorized mobile node that it is serving as a home agent.

When the home agent accepts a valid Registration Request from a mobile node that it serves as a home agent, the home agent MUST create or modify the entry for this mobile node in its mobility binding list containing:

- the mobile node's home address
- the mobile node's care-of address
- the Identification field from the Registration Reply
- the remaining Lifetime of the registration

The home agent MAY optionally offer the capability to dynamically associate a home address to a mobile node upon receiving a Registration Request from that mobile node. The method by which a home address is allocated to the mobile node is beyond the scope of

this document, but see [2]. After the home agent makes the association of the home address to the mobile node, the home agent MUST put that home address into the Home Address field of the Registration Reply.

The home agent MAY also maintain Mobility Security Associations with various foreign agents. When receiving a Registration Request from a foreign agent, if the home agent shares a Mobility Security Association with the foreign agent, the home agent MUST check the Authenticator in the required Foreign-Home Authentication Extension in the message, based on this Mobility Security Association, unless the Lifetime field equals 0. When processing a Registration Request with Lifetime = 0, the HA MAY skip checking for the presence and validity of a Foreign-Home Authentication Extension. Similarly, when sending a Registration Reply to a foreign agent, if the home agent shares a Mobility Security Association with the foreign agent, the home agent MUST include a Foreign-Home Authentication Extension in the message, based on this Mobility Security Association.

3.8.2. Receiving Registration Requests

If the home agent accepts an incoming Registration Request, it MUST update its record of the mobile node's mobility binding(s) and SHOULD send a Registration Reply with a suitable code. Otherwise (the home agent has denied the Request), it SHOULD in most cases send a Registration Reply with an appropriate code specifying the reason the Request was denied. The following sections describe this behavior in more detail. If the home agent does not support broadcasts (see Section 4.3), it MUST ignore the 'B' bit (as opposed to rejecting the Registration Request).

3.8.2.1. Validity Checks

Registration Requests with an invalid, non-zero UDP checksum MUST be silently discarded by the home agent.

The authentication in the Registration Request MUST be checked. This involves the following operations:

a. The home agent MUST check for the presence of at least one authorization-enabling extension, and ensure that all indicated authentications are carried out. At least one authorization-enabling extension MUST be present in the Registration Request, and the home agent MUST either check the Authenticator value in the extension or verify that the Authenticator Value has been checked by another agent with which it has a security association.

If the home agent receives a Registration Request from a mobile node with which it does not have any security association, the home agent MUST silently discard the Registration Request.

If the home agent receives a Registration Request without any authorization-enabling extension, the home agent MUST silently discard the Registration Request.

If the Authenticator is invalid, the home agent MUST reject the mobile node's registration. Further action to be taken in this case depends upon whether the Request has a valid Foreign-Home authentication extension (as follows):

* If there is a valid Foreign-Home authentication extension, the home agent MUST send a Registration Reply with Code 131.

* Otherwise, if there is no Foreign-Home Security Association, the home agent MAY send a Registration Reply with Code 131. If the home agent sends a Registration Reply, it MUST contain a valid Mobile-Home Authentication Extension. In constructing the Reply, the home agent SHOULD choose a security association that is likely to exist in the mobile node; for example, this may be an older security association or one with a longer lifetime than the one that the mobile node attempted to use in its Request. Deployments should take care when updating security associations to ensure that there is at least one common security association shared between the mobile node and home agent. In any case of a failed Authenticator, the home agent MUST then discard the Request without further processing and SHOULD log the error as a security exception.

b. The home agent MUST check that the registration Identification field is correct using the context selected by the SPI within the authorization-enabling extension that the home agent used to authenticate the mobile node's Registration Request. See Section 5.7 for a description of how this is performed. If incorrect, the home agent MUST reject the Request and SHOULD send a Registration Reply to the mobile node with Code 133, including an Identification field computed in accordance with the rules specified in Section 5.7. The home agent MUST do no further processing with such a Request, though it SHOULD log the error as a security exception.

c. If the home agent shares a Mobility Security Association with the foreign agent, and this is a Registration Request (has non-zero Lifetime), the home agent MUST check for the presence of a valid Foreign-Home Authentication Extension. Exactly one Foreign-Home Authentication Extension MUST be present in the Registration

Request in this case, and the home agent MUST check the Authenticator Value in the Extension. If no Foreign-Home Authentication Extension is found, or if more than one Foreign-Home Authentication Extension is found, or if the Authenticator is invalid, the home agent MUST reject the mobile node's registration and SHOULD send a Registration Reply to the mobile node with Code 132. The home agent MUST then discard the Request and SHOULD log the error as a security exception.

d. If the home agent and the foreign agent do not share a Mobility Security Association, and the Registration contains a Foreign-Home Authentication Extension, the home agent MUST discard the Request and SHOULD log the error as a security exception.

In addition to checking the authentication in the Registration Request, home agents MUST deny Registration Requests that are sent to the subnet-directed broadcast address of the home network (as opposed to being unicast to the home agent). The home agent MUST discard the Request and SHOULD return a Registration Reply with a Code of 136. In this case, the Registration Reply will contain the home agent's unicast address, so that the mobile node can re-issue the Registration Request with the correct home agent address.

Note that some routers change the IP Destination Address of a datagram from a subnet-directed broadcast address to 255.255.255.255 before injecting it into the destination subnet. In this case, home agents that attempt to pick up dynamic home agent discovery requests by binding a socket explicitly to the subnet-directed broadcast address will not see such packets. Home agent implementors should be prepared for both the subnet-directed broadcast address and 255.255.255.255 if they wish to support dynamic home agent discovery.

3.8.2.2. Accepting a Valid Request

If the Registration Request satisfies the validity checks in Section 3.8.2.1, and the home agent is able to accommodate the Request, the home agent MUST update its mobility binding list for the requesting mobile node and MUST return a Registration Reply to the mobile node. In this case, the code in the Registration Reply will be either 0 if the home agent supports simultaneous mobility bindings, or 1 if it does not. See Section 3.8.3 for details on building the Registration Reply message.

The home agent updates its record of the mobile node's mobility bindings as follows, based on the fields in the Registration Request:

- If the Lifetime is zero and the Care-of Address equals the mobile node's home address, the home agent deletes all of the entries in the mobility binding list for the requesting mobile node. This is how a mobile node requests that its home agent cease providing mobility services.

- If the Lifetime is zero and the Care-of Address does not equal the mobile node's home address, the home agent deletes only the entry containing the specified Care-of Address from the mobility binding list for the requesting mobile node. Any other active entries containing other care-of addresses will remain active.

- If the Lifetime is nonzero, the home agent adds an entry containing the requested Care-of Address to the mobility binding list for the mobile node. If the 'S' bit is set and the home agent supports simultaneous mobility bindings, the previous mobility binding entries are retained. Otherwise, the home agent removes all previous entries in the mobility binding list for the mobile node.

In all cases, the home agent MUST send a Registration Reply to the source of the Registration Request, which might indeed be a different foreign agent than that whose care-of address is being (de)registered. If the home agent shares a Mobility Security Association with the foreign agent whose care-of address is being deregistered, and that foreign agent is different from the one that relayed the Registration Request, the home agent MAY additionally send a Registration Reply to the foreign agent whose care-of address is being deregistered. The home agent MUST NOT send such a Reply if it does not share a Mobility Security Association with the foreign agent. If no Reply is sent, the foreign agent's visitor list will expire naturally when the original Lifetime expires.

When a foreign agent relays a deregistration message containing a care-of address that it does not own, it MUST NOT add a Foreign-Home Authentication Extension to that deregistration. See Section 3.5.4 for more details.

The home agent MUST NOT increase the Lifetime above that specified by the mobile node in the Registration Request. However, it is not an error for the mobile node to request a Lifetime longer than the home agent is willing to accept. In this case, the home agent simply reduces the Lifetime to a permissible value and returns this value in the Registration Reply. The Lifetime value in the Registration Reply informs the mobile node of the granted Lifetime of the registration, indicating when it SHOULD re-register in order to maintain continued

service. After the expiration of this registration Lifetime, the home agent MUST delete its entry for this registration in its mobility binding list.

If the Registration Request duplicates an accepted current Registration Request, the new Lifetime MUST NOT extend beyond the Lifetime originally granted. A Registration Request is a duplicate if the home address, care-of address, and Identification fields all equal those of an accepted current registration.

In addition, if the home network implements ARP [16], and the Registration Request asks the home agent to create a mobility binding for a mobile node that previously had no binding (the mobile node was previously assumed to be at home), then the home agent MUST follow the procedures described in Section 4.6 with regard to ARP, proxy ARP, and gratuitous ARP. If the mobile node already had a previous mobility binding, the home agent MUST continue to follow the rules for proxy ARP described in Section 4.6.

3.8.2.3. Denying an Invalid Request

If the Registration Request does not satisfy all of the validity checks in Section 3.8.2.1, or the home agent is unable to accommodate the Request, the home agent SHOULD return a Registration Reply to the mobile node with a Code that indicates the reason for the error. If a foreign agent was involved in relaying the Request, this allows the foreign agent to delete its pending visitor list entry. Also, this informs the mobile node of the reason for the error such that it may attempt to fix the error and issue another Request.

This section lists a number of reasons the home agent might reject a Request, and provides the code value it should use in each instance. See Section 3.8.3 for additional details on building the Registration Reply message.

Many reasons for rejecting a registration are administrative in nature. For example, a home agent can limit the number of simultaneous registrations for a mobile node, by rejecting any registrations that would cause its limit to be exceeded, and returning a Registration Reply with a Code of 135. Similarly, a home agent may refuse to grant service to mobile nodes that have entered unauthorized service areas by returning a Registration Reply with a Code of 129.

Requests with non-zero bits in reserved fields MUST be rejected with Code 134 (poorly formed Request).

3.8.3. Sending Registration Replies

If the home agent accepts a Registration Request, it then MUST update its record of the mobile node's mobility binding(s) and SHOULD send a Registration Reply with a suitable Code. Otherwise (the home agent has denied the Request), it SHOULD in most cases send a Registration Reply with an appropriate Code specifying the reason the Request was denied. The following sections provide additional detail for the values the home agent MUST supply in the fields of Registration Reply messages.

3.8.3.1. IP/UDP Fields

This section provides the specific rules by which home agents pick values for the IP and UDP header fields of a Registration Reply.

IP Source Address

Copied from the IP Destination Address of the Registration Request, unless a multicast or broadcast address was used. If the IP Destination Address of the Registration Request was a broadcast or multicast address, the IP Source Address of the Registration Reply MUST be set to the home agent's (unicast) IP address.

IP Destination Address

Copied from the IP Source Address of the Registration Request.

UDP Source Port

Copied from the UDP Destination Port of the Registration Request.

UDP Destination Port

Copied from the UDP Source Port of the Registration Request.

When sending a Registration Reply in response to a Registration Request that requested deregistration of the mobile node (the Lifetime is zero and the Care-of Address equals the mobile node's home address) and in which the IP Source Address was also set to the mobile node's home address (this is the normal method used by a mobile node to deregister when it returns to its home network), the IP Destination Address in the Registration Reply will be set to the mobile node's home address, as copied from the IP Source Address of the Request.

In this case, when transmitting the Registration Reply, the home agent MUST transmit the Reply directly onto the home network as if the mobile node were at home, bypassing any mobility binding list entry that may still exist at the home agent for the destination mobile node. In particular, for a mobile node returning home after being registered with a care-of address, if the mobile node's new Registration Request is not accepted by the home agent, the mobility binding list entry for the mobile node will still indicate that datagrams addressed to the mobile node should be tunneled to the mobile node's registered care-of address; when sending the Registration Reply indicating the rejection of this Request, this existing binding list entry MUST be ignored, and the home agent MUST transmit this Reply as if the mobile node were at home.

3.8.3.2. Registration Reply Fields

This section provides the specific rules by which home agents pick values for the fields within the fixed portion of a Registration Reply.

The Code field of the Registration Reply is chosen in accordance with the rules specified in the previous sections. When replying to an accepted registration, a home agent SHOULD respond with Code 1 if it does not support simultaneous registrations.

The Lifetime field MUST be copied from the corresponding field in the Registration Request, unless the requested value is greater than the maximum length of time the home agent is willing to provide the requested service. In such a case, the Lifetime MUST be set to the length of time that service will actually be provided by the home agent. This reduced Lifetime SHOULD be the maximum Lifetime allowed by the home agent (for this mobile node and care-of address).

If the Home Address field of the Registration Request is non-zero, it MUST be copied into the Home Address field of the Registration Reply message. If the home agent cannot support the specified nonzero unicast address in the Home Address field of the Registration Request, then the home agent MUST reject the Registration Request with a Code of 129.

Otherwise, if the Home Address field of the Registration Request is zero as specified in Section 3.6, the home agent SHOULD arrange for the selection of a home address for the mobile node, and insert the selected address into the Home Address field of the Registration Reply message. See [2] for further relevant details in the case where mobile nodes identify themselves using an NAI instead of their IP home address.

If the Home Agent field in the Registration Request contains a unicast address of this home agent, then that field MUST be copied into the Home Agent field of the Registration Reply. Otherwise, the home agent MUST set the Home Agent field in the Registration Reply to its unicast address. In this latter case, the home agent MUST reject the registration with a suitable code (e.g., Code 136) to prevent the mobile node from possibly being simultaneously registered with two or more home agents.

3.8.3.3. Extensions

This section describes the ordering of any required and any optional Mobile IP Extensions that a home agent appends to a Registration Reply. The following ordering MUST be followed:

a. The IP header, followed by the UDP header, followed by the fixed-length portion of the Registration Reply,

b. If present, any non-authentication Extensions used by the mobile node (which may or may not also be used by the foreign agent),

c. The Mobile-Home Authentication Extension,

d. If present, any non-authentication Extensions used only by the foreign agent, and

e. The Foreign-Home Authentication Extension, if present.

Note that items (a) and (c) MUST appear in every Registration Reply sent by the home agent. Items (b), (d), and (e) are optional. However, item (e) MUST be included when the home agent and the foreign agent share a Mobility Security Association.

4. Routing Considerations

This section describes how mobile nodes, home agents, and (possibly) foreign agents cooperate to route datagrams to/from mobile nodes that are connected to a foreign network. The mobile node informs its home agent of its current location using the registration procedure described in Section 3. See the protocol overview in Section 1.7 for the relative locations of the mobile node’s home address with respect to its home agent, and the mobile node itself with respect to any foreign agent with which it might attempt to register.

4.1. Encapsulation Types

Home agents and foreign agents MUST support tunneling datagrams using IP in IP encapsulation [14]. Any mobile node that uses a co-located care-of address MUST support receiving datagrams tunneled using IP in IP encapsulation. Minimal encapsulation [15] and GRE encapsulation [13] are alternate encapsulation methods that MAY optionally be supported by mobility agents and mobile nodes. The use of these alternative forms of encapsulation, when requested by the mobile node, is otherwise at the discretion of the home agent.

4.2. Unicast Datagram Routing

4.2.1. Mobile Node Considerations

When connected to its home network, a mobile node operates without the support of mobility services. That is, it operates in the same way as any other (fixed) host or router. The method by which a mobile node selects a default router when connected to its home network, or when away from home and using a co-located care-of address, is outside the scope of this document. ICMP Router Advertisement [5] is one such method.

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

- If the mobile node is registered using a foreign agent care-of address, it MAY use its foreign agent as a first-hop router. The foreign agent's MAC address can be learned from the foreign agent's Agent Advertisement message. Otherwise, the mobile node MUST choose its default router from among the router addresses advertised in the ICMP Router Advertisement portion of that Agent Advertisement message.

- If the mobile node is registered directly with its home agent using a co-located care-of address, then the mobile node SHOULD choose its default router from among those advertised in any ICMP Router Advertisement message that it receives for which its externally obtained care-of address and the router address match under the network prefix. If the mobile node's externally obtained care-of address matches the IP source address of the Agent Advertisement under the network prefix, the mobile node MAY also consider that IP source address as another possible choice for the IP address of a default router. The network prefix MAY be obtained from the Prefix-Lengths Extension in the Router Advertisement, if present. The prefix MAY also be obtained through other mechanisms beyond the scope of this document.

While they are away from the home network, mobile nodes MUST NOT broadcast ARP packets to find the MAC address of another Internet node. Thus, the (possibly empty) list of router addresses from the ICMP Router Advertisement portion of the message is not useful for selecting a default router, unless the mobile node has some means not involving broadcast ARP and not specified within this document for obtaining the MAC address of one of the routers in the list. Similarly, in the absence of unspecified mechanisms for obtaining MAC addresses on foreign networks, the mobile node MUST ignore redirects to other routers on foreign networks.

4.2.2. Foreign Agent Considerations

Upon receipt of an encapsulated datagram sent to its advertised care-of address, a foreign agent MUST compare the inner Destination Address to those entries in its visitor list. When the Destination does not match the address of any mobile node currently in the visitor list, the foreign agent MUST NOT forward the datagram without modifications to the original IP header, because otherwise a routing loop is likely to result. The datagram SHOULD be silently discarded. ICMP Destination Unreachable MUST NOT be sent when a foreign agent is unable to forward an incoming tunneled datagram. Otherwise, the foreign agent forwards the decapsulated datagram to the mobile node.

The foreign agent MUST NOT advertise to other routers in its routing domain, nor to any other mobile node, the presence of a mobile router (Section 4.5) or mobile node in its visitor list.

The foreign agent MUST route datagrams it receives from registered mobile nodes. At a minimum, this means that the foreign agent must verify the IP Header Checksum, decrement the IP Time To Live, recompute the IP Header Checksum, and forward such datagrams to a default router.

A foreign agent MUST NOT use broadcast ARP for a mobile node’s MAC address on a foreign network. It may obtain the MAC address by copying the information from an Agent Solicitation or a Registration Request transmitted from a mobile node. A foreign agent’s ARP cache for the mobile node’s IP address MUST NOT be allowed to expire before the mobile node’s visitor list entry expires, unless the foreign agent has some way other than broadcast ARP to refresh its MAC address associated with the mobile node’s IP address.

Each foreign agent SHOULD support the mandatory features for reverse tunneling [12].

4.2.3. Home Agent Considerations

The home agent MUST be able to intercept any datagrams on the home network addressed to the mobile node while the mobile node is registered away from home. Proxy and gratuitous ARP MAY be used in enabling this interception, as specified in Section 4.6.

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

For multihomed home agents, the source address in the outer IP header of the encapsulated datagram MUST be the address sent to the mobile node in the Home Agent field of the Registration Reply. That is, the home agent cannot use the address of some other network interface as the source address.

See Section 4.1 regarding methods of encapsulation that may be used for tunneling. Nodes implementing tunneling SHOULD also implement the "tunnel soft state" mechanism [14], which allows ICMP error messages returned from the tunnel to correctly be reflected back to the original senders of the tunneled datagrams.

Home agents MUST decapsulate packets addressed to themselves, sent by a mobile node for the purpose of maintaining location privacy, as described in Section 5.5. This feature is also required for support of reverse tunneling [12].

If the Lifetime for a given mobility binding expires before the home agent has received another valid Registration Request for that mobile node, then that binding is deleted from the mobility binding list. The home agent MUST NOT send any Registration Reply message simply because the mobile node's binding has expired. The entry in the visitor list of the mobile node's current foreign agent will expire naturally, probably at the same time as the binding expired at the home agent. When a mobility binding's lifetime expires, the home

agent MUST delete the binding, but it MUST retain any other (non-expired) simultaneous mobility bindings that it holds for the mobile node.

When a home agent receives a datagram, intercepted for one of its mobile nodes registered away from home, the home agent MUST examine the datagram to check if it is already encapsulated. If so, special rules apply in the forwarding of that datagram to the mobile node:

- If the inner (encapsulated) Destination Address is the same as the outer Destination Address (the mobile node), then the home agent MUST also examine the outer Source Address of the encapsulated datagram (the source address of the tunnel). If this outer Source Address is the same as the mobile node's current care-of address, the home agent MUST silently discard that datagram in order to prevent a likely routing loop. If, instead, the outer Source Address is NOT the same as the mobile node's current care-of address, then the home agent SHOULD forward the datagram to the mobile node. In order to forward the datagram in this case, the home agent MAY simply alter the outer Destination Address to the care-of address, rather than re-encapsulating the datagram.

- Otherwise (the inner Destination Address is NOT the same as the outer Destination Address), the home agent SHOULD encapsulate the datagram again (nested encapsulation), with the new outer Destination Address set equal to the mobile node's care-of address. That is, the home agent forwards the entire datagram to the mobile node in the same way as any other datagram (encapsulated already or not).

4.3. Broadcast Datagrams

When a home agent receives a broadcast datagram, it MUST NOT forward the datagram to any mobile nodes in its mobility binding list other than those that have requested forwarding of broadcast datagrams. A mobile node MAY request forwarding of broadcast datagrams by setting the 'B' bit in its Registration Request message (Section 3.3). For each such registered mobile node, the home agent SHOULD forward received broadcast datagrams to the mobile node, although it is a matter of configuration at the home agent as to which specific categories of broadcast datagrams will be forwarded to such mobile nodes.

If the 'D' bit was set in the mobile node's Registration Request message, indicating that the mobile node is using a co-located care-of address, the home agent simply tunnels appropriate broadcast IP datagrams to the mobile node's care-of address. Otherwise (the 'D' bit was NOT set), the home agent first encapsulates the broadcast

datagram in a unicast datagram addressed to the mobile node's home address, and then tunnels this encapsulated datagram to the foreign agent. This extra level of encapsulation is required so that the foreign agent can determine which mobile node should receive the datagram after it is decapsulated. When received by the foreign agent, the unicast encapsulated datagram is detunneled and delivered to the mobile node in the same way as any other datagram. In either case, the mobile node must decapsulate the datagram it receives in order to recover the original broadcast datagram.

4.4. Multicast Datagram Routing

As mentioned previously, a mobile node that is connected to its home network functions in the same way as any other (fixed) host or router. Thus, when it is at home, a mobile node functions identically to other multicast senders and receivers. This section therefore describes the behavior of a mobile node that is visiting a foreign network.

In order to receive multicasts, a mobile node MUST join the multicast group in one of two ways. First, a mobile node MAY join the group via a (local) multicast router on the visited subnet. This option assumes that there is a multicast router present on the visited subnet. If the mobile node is using a co-located care-of address, it SHOULD use this address as the source IP address of its IGMP [6] messages. Otherwise, it MAY use its home address.

Alternatively, a mobile node that wishes to receive multicasts MAY join groups via a bidirectional tunnel to its home agent, assuming that its home agent is a multicast router. The mobile node tunnels IGMP messages to its home agent, and the home agent forwards multicast datagrams down the tunnel to the mobile node. For packets tunneled to the home agent, the source address in the IP header SHOULD be the mobile node's home address.

The rules for multicast datagram delivery to mobile nodes in this case are identical to those for broadcast datagrams (Section 4.3). Namely, if the mobile node is using a co-located care-of address (the 'D' bit was set in the mobile node's Registration Request), then the home agent SHOULD tunnel the datagram to this care-of address; otherwise, the home agent MUST first encapsulate the datagram in a unicast datagram addressed to the mobile node's home address and then MUST tunnel the resulting datagram (nested tunneling) to the mobile node's care-of address. For this reason, the mobile node MUST be capable of decapsulating packets sent to its home address in order to receive multicast datagrams using this method.

A mobile node that wishes to send datagrams to a multicast group also has two options: (1) send directly on the visited network; or (2) send via a tunnel to its home agent. Because multicast routing in general depends upon the IP source address, a mobile node that sends multicast datagrams directly on the visited network MUST use a co-located care-of address as the IP source address. Similarly, a mobile node that tunnels a multicast datagram to its home agent MUST use its home address as the IP source address of both the (inner) multicast datagram and the (outer) encapsulating datagram. This second option assumes that the home agent is a multicast router.

4.5. Mobile Routers

A mobile node can be a router that is responsible for the mobility of one or more entire networks moving together, perhaps on an airplane, a ship, a train, an automobile, a bicycle, or a kayak. The nodes connected to a network served by the mobile router may themselves be fixed nodes or mobile nodes or routers. In this document, such networks are called "mobile networks".

A mobile router MAY act as a foreign agent and provide a foreign agent care-of address to mobile nodes connected to the mobile network. Typical routing to a mobile node via a mobile router in this case is illustrated by the following example:

a. A laptop computer is disconnected from its home network and later attached to a network port in the seat back of an aircraft. The laptop computer uses Mobile IP to register on this foreign network, using a foreign agent care-of address discovered through an Agent Advertisement from the aircraft’s foreign agent.

b. The aircraft network is itself mobile. Suppose the node serving as the foreign agent on the aircraft also serves as the default router that connects the aircraft network to the rest of the Internet. When the aircraft is at home, this router is attached to some fixed network at the airline’s headquarters, which is the router’s home network. While the aircraft is in flight, this router registers from time to time over its radio link with a series of foreign agents below it on the ground. This router’s home agent is a node on the fixed network at the airline’s headquarters.

c. Some correspondent node sends a datagram to the laptop computer, addressing the datagram to the laptop’s home address. This datagram is initially routed to the laptop’s home network.

d. The laptop's home agent intercepts the datagram on the home network and tunnels it to the laptop's care-of address, which in this example is an address of the node serving as the router and foreign agent on the aircraft. Normal IP routing will route the datagram to the fixed network at the airline's headquarters.

e. The aircraft router and foreign agent's home agent there intercept the datagram and tunnel it to its current care-of address, which in this example is some foreign agent on the ground below the aircraft. The original datagram from the correspondent node has now been encapsulated twice: once by the laptop's home agent and again by the aircraft's home agent.

f. The foreign agent on the ground decapsulates the datagram, yielding a datagram still encapsulated by the laptop's home agent, with a Destination Address of the laptop's care-of address. The ground foreign agent sends the resulting datagram over its radio link to the aircraft.

g. The foreign agent on the aircraft decapsulates the datagram, yielding the original datagram from the correspondent node, with a Destination Address of the laptop's home address. The aircraft foreign agent delivers the datagram over the aircraft network to the laptop's link-layer address.

This example illustrates the case in which a mobile node is attached to a mobile network. That is, the mobile node is mobile with respect to the network, which itself is also mobile (here with respect to the ground). If, instead, the node is fixed with respect to the mobile network (the mobile network is the fixed node's home network), then either of two methods may be used to cause datagrams from correspondent nodes to be routed to the fixed node.

For the fixed node, a home agent MAY be configured to have a permanent registration that indicates the mobile router's address as the fixed host's care-of address. The mobile router's home agent will normally be used for this purpose. The home agent is then responsible for advertising connectivity using normal routing protocols to the fixed node. Any datagrams sent to the fixed node will thus use nested tunneling as described above.

Alternatively, the mobile router MAY advertise connectivity to the entire mobile network using normal IP routing protocols through a bidirectional tunnel to its own home agent. This method avoids the need for nested tunneling of datagrams.

4.6. ARP, Proxy ARP, and Gratuitous ARP

The use of ARP [16] requires special rules for correct operation when wireless or mobile nodes are involved. The requirements specified in this section apply to all home networks in which ARP is used for address resolution.

In addition to the normal use of ARP for resolving a target node's link-layer address from its IP address, this document distinguishes two special uses of ARP:

- A Proxy ARP [49] is an ARP Reply sent by one node on behalf of another node that is either unable or unwilling to answer its own ARP Requests. The sender of a Proxy ARP reverses the Sender and Target Protocol Address fields as described in [16], but supplies some configured link-layer address (generally, its own) in the Sender Hardware Address field. The node receiving the Reply will then associate this link-layer address with the IP address of the original target node, causing it to transmit future datagrams for this target node to the node with that link-layer address.

- A Gratuitous ARP [45] is an ARP packet sent by a node in order to spontaneously cause other nodes to update an entry in their ARP cache. A gratuitous ARP MAY use either an ARP Request or an ARP Reply packet. In either case, the ARP Sender Protocol Address and ARP Target Protocol Address are both set to the IP address of the cache entry to be updated, and the ARP Sender Hardware Address is set to the link-layer address to which this cache entry should be updated. When using an ARP Reply packet, the Target Hardware Address is also set to the link-layer address to which this cache entry should be updated (this field is not used in an ARP Request packet).

  In either case, for a gratuitous ARP, the ARP packet MUST be transmitted as a local broadcast packet on the local link. As specified in [16], any node receiving any ARP packet (Request or Reply) MUST update its local ARP cache with the Sender Protocol and Hardware Addresses in the ARP packet, if the receiving node has an entry for that IP address already in its ARP cache. This requirement in the ARP protocol applies even for ARP Request packets, and for ARP Reply packets that do not match any ARP Request transmitted by the receiving node [16].

While a mobile node is registered on a foreign network, its home agent uses proxy ARP [49] to reply to ARP Requests it receives that seek the mobile node's link-layer address. When receiving an ARP Request, the home agent MUST examine the target IP address of the Request, and if this IP address matches the home address of any

mobile node for which it has a registered mobility binding, the home agent MUST transmit an ARP Reply on behalf of the mobile node. After exchanging the sender and target addresses in the packet [49], the home agent MUST set the sender link-layer address in the packet to the link-layer address of its own interface over which the Reply will be sent.

When a mobile node leaves its home network and registers a binding on a foreign network, its home agent uses gratuitous ARP to update the ARP caches of nodes on the home network. This causes such nodes to associate the link-layer address of the home agent with the mobile node's home (IP) address. When registering a binding for a mobile node for which the home agent previously had no binding (the mobile node was assumed to be at home), the home agent MUST transmit a gratuitous ARP on behalf of the mobile node. This gratuitous ARP packet MUST be transmitted as a broadcast packet on the link on which the mobile node's home address is located. Since broadcasts on the local link (such as Ethernet) are typically not guaranteed to be reliable, the gratuitous ARP packet SHOULD be retransmitted a small number of times to increase its reliability.

When a mobile node returns to its home network, the mobile node and its home agent use gratuitous ARP to cause all nodes on the mobile node's home network to update their ARP caches to once again associate the mobile node's own link-layer address with the mobile node's home (IP) address. Before transmitting the (de)Registration Request message to its home agent, the mobile node MUST transmit this gratuitous ARP on its home network as a local broadcast on this link. The gratuitous ARP packet SHOULD be retransmitted a small number of times to increase its reliability, but these retransmissions SHOULD proceed in parallel with the transmission and processing of the mobile node's (de)Registration Request.

When the mobile node's home agent receives and accepts this (de)Registration Request, the home agent MUST also transmit a gratuitous ARP on the mobile node's home network. This gratuitous ARP also is used to associate the mobile node's home address with the mobile node's own link-layer address. A gratuitous ARP is transmitted by both the mobile node and its home agent, since in the case of wireless network interfaces, the area within transmission range of the mobile node will likely differ from that within range of its home agent. The ARP packet from the home agent MUST be transmitted as a local broadcast on the mobile node's home link, and SHOULD be retransmitted a small number of times to increase its reliability; these retransmissions, however, SHOULD proceed in parallel with the transmission and processing of the mobile node's (de)Registration Reply.

While the mobile node is away from home, it MUST NOT transmit any broadcast ARP Request or ARP Reply messages. Finally, while the mobile node is away from home, it MUST NOT reply to ARP Requests in which the target IP address is its own home address unless the ARP Request is unicast by a foreign agent with which the mobile node is attempting to register or a foreign agent with which the mobile node has an unexpired registration. In the latter case, the mobile node MUST use a unicast ARP Reply to respond to the foreign agent. Note that if the mobile node is using a co-located care-of address and receives an ARP Request in which the target IP address is this care-of address, then the mobile node SHOULD reply to this ARP Request. Note also that, when transmitting a Registration Request on a foreign network, a mobile node may discover the link-layer address of a foreign agent by storing the address as it is received from the Agent Advertisement from that foreign agent, but not by transmitting a broadcast ARP Request message.

The specific order in which each of the above requirements for the use of ARP, proxy ARP, and gratuitous ARP are applied, relative to the transmission and processing of the mobile node's Registration Request and Registration Reply messages when leaving home or returning home, are important to the correct operation of the protocol.

To summarize the above requirements, when a mobile node leaves its home network, the following steps, in this order, MUST be performed:

- The mobile node decides to register away from home, perhaps because it has received an Agent Advertisement from a foreign agent and has not recently received one from its home agent.

- Before transmitting the Registration Request, the mobile node disables its own future processing of any ARP Requests it may subsequently receive requesting the link-layer address corresponding to its home address, except insofar as necessary to communicate with foreign agents on visited networks.

- The mobile node transmits its Registration Request.

- When the mobile node's home agent receives and accepts the Registration Request, it performs a gratuitous ARP on behalf of the mobile node, and begins using proxy ARP to reply to ARP Requests that it receives requesting the mobile node's link-layer address. In the gratuitous ARP, the ARP Sender Hardware Address is set to the link-layer address of the home agent. If, instead, the home agent rejects the Registration Request, no ARP processing (neither gratuitous nor proxy) is performed by the home agent.

When a mobile node later returns to its home network, the following steps, in this order, MUST be performed:

- The mobile node decides to register at home, perhaps because it has received an Agent Advertisement from its home agent.
- Before transmitting the Registration Request, the mobile node re-enables its own future processing of any ARP Requests it may subsequently receive requesting its link-layer address.
- The mobile node performs a gratuitous ARP for itself. In this gratuitous ARP, the ARP Sender Hardware Address is set to the link-layer address of the mobile node.
- The mobile node transmits its Registration Request.
- When the mobile node's home agent receives and accepts the Registration Request, it stops using proxy ARP to reply to ARP Requests that it receives requesting the mobile node's link-layer address, and then performs a gratuitous ARP on behalf of the mobile node. In this gratuitous ARP, the ARP Sender Hardware Address is set to the link-layer address of the mobile node. If, instead, the home agent rejects the Registration Request, the home agent MUST NOT make any change to the way it performs ARP processing (neither gratuitous nor proxy) for the mobile node. In this latter case, the home agent should operate as if the mobile node has not returned home, and continue to perform proxy ARP on behalf of the mobile node.

5. Security Considerations

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

5.1. Message Authentication Codes

Home agents and mobile nodes MUST be able to perform authentication. The default algorithm is HMAC-MD5 [10], with a key size of 128 bits. The foreign agent MUST also support authentication using HMAC-MD5 and key sizes of 128 bits or greater, with manual key distribution. Keys with arbitrary binary values MUST be supported.

The "prefix+suffix" use of MD5 to protect data and a shared secret is considered vulnerable to attack by the cryptographic community. Where backward compatibility with existing Mobile IP implementations

that use this mode is needed, new implementations SHOULD include keyed MD5 [19] as one of the additional authentication algorithms for use when producing and verifying the authentication data that is supplied with Mobile IP registration messages, for instance, in the extensions specified in Sections 3.5.2, 3.5.3, and 3.5.4.

More authentication algorithms, algorithm modes, key distribution methods, and key sizes MAY also be supported for all of these extensions.

5.2. Areas of Security Concern in This Protocol

The registration protocol described in this document will result in a mobile node's traffic being tunneled to its care-of address. This tunneling feature could be a significant vulnerability if the registration were not authenticated. Such remote redirection, for instance, as performed by the mobile registration protocol, is widely understood to be a security problem in the current Internet if not authenticated [30]. Moreover, the Address Resolution Protocol (ARP) is not authenticated, and can potentially be used to steal another host's traffic. The use of gratuitous ARP (Section 4.6) brings with it all of the risks associated with the use of ARP.

5.3. Key Management

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

5.4. Picking Good Random Numbers

The strength of any authentication mechanism depends on several factors, including the innate strength of the authentication algorithm, the secrecy of the key used, the strength of the key used, and the quality of the particular implementation. This specification requires implementation of keyed MD5 for authentication, but does not preclude the use of other authentication algorithms and modes. For keyed MD5 authentication to be useful, the 128-bit key must be both secret (that is, known only to authorized parties) and pseudo-random.

If nonces are used in connection with replay protection, they must also be selected carefully. RFC 4086 [8] written by Eastlake, et al. provides more information on generating pseudo-random numbers.

5.5. Privacy

Users who have sensitive data that they do not wish others to see should use mechanisms outside the scope of this document (such as encryption) to provide appropriate protection. Users concerned about traffic analysis should consider appropriate use of link encryption. If absolute location privacy is desired, the mobile node can create a tunnel to its home agent. Then, datagrams destined for correspondent nodes will appear to emanate from the home network, and it may be more difficult to pinpoint the location of the mobile node. Such mechanisms are all beyond the scope of this document.

5.6. Ingress Filtering

Many routers implement security policies such as "ingress filtering" [35] that do not allow forwarding of packets that have a Source Address that appears topologically incorrect. In environments where this is a problem, mobile nodes may use reverse tunneling [12] with the foreign agent supplied care-of address as the Source Address. Reverse-tunneled packets will be able to pass normally through such routers, while ingress filtering rules will still be able to locate the true topological source of the packet in the same way as packets from non-mobile nodes.

5.7. Replay Protection for Registration Requests

The Identification field is used to let the home agent verify that a registration message has been freshly generated by the mobile node, not replayed by an attacker from some previous registration. Two methods are described in this section: timestamps (mandatory) and "nonces" (optional). All mobile nodes and home agents MUST implement timestamp-based replay protection. These nodes MAY also implement nonce-based replay protection.

The style of replay protection in effect between a mobile node and its home agent is part of the Mobility Security Association. A mobile node and its home agent MUST agree on which method of replay protection will be used. The interpretation of the Identification field depends on the method of replay protection as described in the subsequent subsections.

Whatever method is used, the low-order 32 bits of the Identification field MUST be copied unchanged from the Registration Request to the Reply. The foreign agent uses those bits (and the mobile node’s home

address) to match Registration Requests with corresponding replies. The mobile node MUST verify that the low-order 32 bits of any Registration Reply are identical to the bits it sent in the Registration Request.

The Identification field in a new Registration Request MUST NOT be the same as in an immediately preceding Request, and SHOULD NOT repeat while the same security context is being used between the mobile node and the home agent. Retransmission as in Section 3.6.3 is allowed.

5.7.1. Replay Protection Using Timestamps

The basic principle of timestamp replay protection is that the node generating a message inserts the current time of day, and the node receiving the message checks that this timestamp is sufficiently close to its own time of day. Unless specified differently in the security association between the nodes, a default value of 7 seconds MAY be used to limit the time difference. This value SHOULD be greater than 3 seconds. Obviously the two nodes must have adequately synchronized time-of-day clocks. As with any messages, time synchronization messages may be protected against tampering by an authentication mechanism determined by the security context between the two nodes.

If timestamps are used, the mobile node MUST set the Identification field to a 64-bit value formatted as specified by the Network Time Protocol [11]. The low-order 32 bits of the NTP format represent fractional seconds, and those bits that are not available from a time source SHOULD be generated from a good source of randomness. Note, however, that when using timestamps, the 64-bit Identification used in a Registration Request from the mobile node MUST be greater than that used in any previous Registration Request, as the home agent uses this value as a sequence number. Without such a sequence number, it would be possible for a delayed duplicate of an earlier Registration Request to arrive at the home agent (within the clock synchronization required by the home agent), and thus be applied out of order, mistakenly altering the mobile node’s current registered care-of address.

Upon receipt of a Registration Request with an authorization-enabling extension, the home agent MUST check the Identification field for validity. In order to be valid, the timestamp contained in the Identification field MUST be close enough to the home agent’s time-of-day clock, and the timestamp MUST be greater than all previously accepted timestamps for the requesting mobile node. Time tolerances and resynchronization details are specific to a particular Mobility Security Association.

If the timestamp is valid, the home agent copies the entire Identification field into the Registration Reply it returns to the mobile node. If the timestamp is not valid, the home agent copies only the low-order 32 bits into the Registration Reply, and supplies the high-order 32 bits from its own time of day. In this latter case, the home agent MUST reject the registration by returning Code 133 (registration Identification mismatch) in the Registration Reply.

As described in Section 3.6.2.1, the mobile node MUST verify that the low-order 32 bits of the Identification field in the Registration Reply are identical to those in the rejected registration attempt, before using the high-order bits for clock resynchronization.

5.7.2. Replay Protection Using Nonces

The basic principle of nonce replay protection is that node A includes a new random number in every message to node B, and checks that node B returns that same number in its next message to node A. Both messages use an authentication code to protect against alteration by an attacker. At the same time, node B can send its own nonces in all messages to node A (to be echoed by node A), so that it too can verify that it is receiving fresh messages.

The home agent may be expected to have resources for computing pseudo-random numbers useful as nonces [8]. It inserts a new nonce as the high-order 32 bits of the Identification field of every Registration Reply. The home agent copies the low-order 32 bits of the Identification field from the Registration Request message into the low-order 32 bits of the Identification field in the Registration Reply. When the mobile node receives an authenticated Registration Reply from the home agent, it saves the high-order 32 bits of the Identification field for use as the high-order 32 bits of its next Registration Request.

The mobile node is responsible for generating the low-order 32 bits of the Identification field in each Registration Request. Ideally, it should generate its own random nonces. However, it may use any expedient method, including duplication of the random value sent by the home agent. The method chosen is of concern only to the mobile node, because it is the node that checks for valid values in the Registration Reply. The high-order and low-order 32 bit values of the identification chosen SHOULD both differ from their previous values. The home agent uses a new high-order value, and the mobile node uses a new low-order value for each registration message. The foreign agent uses the low-order value (and the mobile host’s home address) to correctly match registration replies with pending Requests (Section 3.7.1).

If a registration message is rejected because of an invalid nonce, the Reply always provides the mobile node with a new nonce to be used in the next registration. Thus, the nonce protocol is self-synchronizing.

6. IANA Considerations

Mobile IP specifies several new number spaces for values to be used in various message fields. These number spaces include the following:

- Mobile IP message types sent to UDP port 434, as defined in Section 1.8.
- types of extensions to Registration Request and Registration Reply messages (see Sections 3.3 and 3.4, and also consult [12], [43], [2], [3], and [7]).
- values for the code in the Registration Reply message (see Section 3.4, and also consult [12], [43], [2], [3], and [7]).
- Mobile IP defines so-called Agent Solicitation and Agent Advertisement messages. These messages are in fact Router Discovery messages [5] augmented with Mobile-IP-specific extensions. Thus, they do not define a new name space, but do define additional Router Discovery extensions as described below in Section 6.2. Also see Section 2.1, and consult [3] and [7].

There are additional Mobile IP numbering spaces specified in [3].

Information about assignment of Mobile IP numbers derived from specifications external to this document is given by IANA at http://www.iana.org/protocols. From that URL, see the "Mobile Internet Protocol (IP) Numbers" section.

In this revised specification, a new code value (for the field in the Registration Reply message) is needed within the range typically used for foreign agent messages. This error code is needed to indicate the status "Invalid Home Agent Address". See Section 3.7.2 for details.

6.1. Mobile IP Message Types

Mobile IP messages are defined to be those that are sent to a message recipient at port 434 (UDP or TCP). The number space for Mobile IP messages is specified in Section 1.8. Approval of new extension

numbers is subject to Expert Review, and a specification is required [22]. The currently standardized message types have the following numbers, and are specified in the indicated sections.

Type	Name	Section
1	Registration Request	3.3
3	Registration Reply	3.4

6.2. Extensions to RFC 1256 Router Advertisement

RFC 1256 defines two ICMP message types, Router Advertisement and Router Solicitation. Mobile IP defines a number space for extensions to Router Advertisement, which could be used by protocols other than Mobile IP. The extension types currently standardized for use with Mobile IP have the following numbers.

Type	Name	Section
0	One-byte Padding	2.1.3
16	Mobility Agent Advertisement	2.1.1
19	Prefix-Lengths	2.1.2

Approval of new extension numbers for use with Mobile IP is subject to Expert Review, and a specification is required [22].

6.3. Extensions to Mobile IP Registration Messages

The Mobile IP messages specified within this document and listed in Sections 1.8 and 6.1 may have extensions. Mobile IP message extensions all share the same number space, even if they are to be applied to different Mobile IP messages. The number space for Mobile IP message extensions is specified within this document. Approval of new extension numbers is subject to Expert Review, and a specification is required [22].

Type	Name	Section
0	One-byte Padding	
32	Mobile-Home Authentication	3.5.2
33	Mobile-Foreign Authentication	3.5.3
34	Foreign-Home Authentication	3.5.4

6.4. Code Values for Mobile IP Registration Reply Messages

The Mobile IP Registration Reply message, specified in Section 3.4, has a Code field. The number space for the Code field values is also specified in Section 3.4. The Code number space is structured according to whether the registration was successful, the foreign agent denied the Registration Request, or the home agent denied the Registration Request, as follows:

Code #s	Guideline
0-8	Success Codes
9-63	Allocation guidelines not specified in this document
64-127	Error Codes from the Foreign Agent
128-192	Error Codes from the Home Agent
193-200	Error Codes from the Gateway Foreign Agent [29]
201-255	Allocation guidelines not specified in this document

Approval of new code values requires Expert Review [22].

Table 1: Guidelines for Allocation of Code Values

7. Acknowledgments

Special thanks to Steve Deering (Xerox PARC), along with Dan Duchamp and John Ioannidis (JI) (Columbia University), for forming the working group, chairing it, and putting so much effort into its early development. Columbia’s early Mobile IP work can be found in [37], [38], [39].

Thanks also to Kannan Alaggapan, Greg Minshall, Tony Li, Jim Solomon, Erik Nordmark, Basavaraj Patil, and Phil Roberts for their contributions to the group while performing the duties of chairperson, as well as for their many useful comments.

Thanks to the active members of the Mobile IP Working Group, particularly those who contributed text, including (in alphabetical order)

Ran Atkinson (Naval Research Lab)
Samita Chakrabarti (Sun Microsystems)
Ken Imboden (Candlestick Networks, Inc.)
Dave Johnson (Carnegie Mellon University)
Frank Kastenholz (FTP Software)
Anders Klemets (KTH)
Chip Maguire (KTH)
Alison Mankin (ISI)
Andrew Myles (Macquarie University)
Thomas Narten (IBM)
Al Quirt (Bell Northern Research)
Yakov Rekhter (IBM)
Fumio Teraoka (Sony)
Alper Yegin (NTT DoCoMo)

Thanks to Charlie Kunzinger and to Bill Simpson, the editors who produced the first drafts of this document, reflecting the discussions of the working group. Much of the new text in the later revisions preceding RFC 2002 is due to Jim Solomon and Dave Johnson.

Thanks to Greg Minshall (Novell), Phil Karn (Qualcomm), Frank Kastenholz (FTP Software), and Pat Calhoun (Sun Microsystems) for their generous support in hosting interim working group meetings.

Sections 1.10 and 1.11, which specify new extension formats to be used with aggregatable extension types, were included from a specification document (entitled "Mobile IP Extensions Rationalization (MIER)", which was written by

Mohamed Khalil (Nortel Networks)
Raja Narayanan (nVisible Networks)
Haseeb Akhtar (Nortel Networks)
Emad Qaddoura (Nortel Networks)

Thanks to these authors, and also for the additional work on MIER, which was contributed by Basavaraj Patil, Pat Calhoun, Neil Justusson, N. Asokan, and Jouni Malinen.

Thanks to Vijay Devarapalli, who put in many hours to convert the source for this text document into XML format.

8. References

8.1. Normative References

[1] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[2] Calhoun, P. and C. Perkins, "Mobile IP Network Access Identifier Extension for IPv4", RFC 2794, March 2000.

[3] Perkins, C., Calhoun, P., and J. Bharatia, "Mobile IPv4 Challenge/Response Extensions (Revised)", RFC 4721, January 2007.

[4] Cong, D., Hamlen, M., and C. Perkins, "The Definitions of Managed Objects for IP Mobility Support using SMIv2", RFC 2006, October 1996.

[5] Deering, S., Ed., "ICMP Router Discovery Messages", RFC 1256, September 1991.

[6] Deering, S., "Host extensions for IP multicasting", STD 5, RFC 1112, August 1989.

[7] Dommety, G. and K. Leung, "Mobile IP Vendor/Organization-Specific Extensions", RFC 3115, April 2001.

[8] Eastlake 3rd, D., Schiller, J., and S. Crocker, "Randomness Requirements for Security", BCP 106, RFC 4086, June 2005.

[9] Kent, S., "IP Authentication Header", RFC 4302, December 2005.

[10] Krawczyk, H., Bellare, M., and R. Canetti, "HMAC: Keyed-Hashing for Message Authentication", RFC 2104, February 1997.

[11] Mills, D., Martin, J., Ed., Burbank, J., and W. Kasch, "Network Time Protocol Version 4: Protocol and Algorithms Specification", RFC 5905, June 2010.

[12] Montenegro, G., Ed., "Reverse Tunneling for Mobile IP, revised", RFC 3024, January 2001.

[13] Farinacci, D., Li, T., Hanks, S., Meyer, D., and P. Traina, "Generic Routing Encapsulation (GRE)", RFC 2784, March 2000.

[14] Perkins, C., "IP Encapsulation within IP", RFC 2003, October 1996.

[15] Perkins, C., "Minimal Encapsulation within IP", RFC 2004, October 1996.

[16] Plummer, D., "Ethernet Address Resolution Protocol: Or Converting Network Protocol Addresses to 48.bit Ethernet Address for Transmission on Ethernet Hardware", STD 37, RFC 826, November 1982.

[17] Postel, J., "User Datagram Protocol", STD 6, RFC 768, August 1980.

[18] Postel, J., "Internet Protocol", STD 5, RFC 791, September 1981.

[19] Rivest, R., "The MD5 Message-Digest Algorithm", RFC 1321, April 1992.

[20] Solomon, J., "Applicability Statement for IP Mobility Support", RFC 2005, October 1996.

[21] Perkins, C., Ed., "IP Mobility Support for IPv4", RFC 3344, August 2002.

[22] Narten, T. and H. Alvestrand, "Guidelines for Writing an IANA Considerations Section in RFCs", BCP 26, RFC 5226, May 2008.

8.2. Informative References

[23] Solomon, J. and S. Glass, "Mobile-IPv4 Configuration Option for PPP IPCP", RFC 2290, February 1998.

[24] Montenegro, G., Dawkins, S., Kojo, M., Magret, V., and N. Vaidya, "Long Thin Networks", RFC 2757, January 2000.

[25] Allman, M., Glover, D., and L. Sanchez, "Enhancing TCP Over Satellite Channels using Standard Mechanisms", BCP 28, RFC 2488, January 1999.

[26] Paxson, V. and M. Allman, "Computing TCP’s Retransmission Timer", RFC 2988, November 2000.

[27] Levkowetz, H. and S. Vaarala, "Mobile IP Traversal of Network Address Translation (NAT) Devices", RFC 3519, April 2003.

[28] Glass, S. and M. Chandra, "Registration Revocation in Mobile IPv4", RFC 3543, August 2003.

[29] Fogelstroem, E., Jonsson, A., and C. Perkins, "Mobile IPv4 Regional Registration", RFC 4857, June 2007.

[30] Bellovin, S., "Security Problems in the TCP/IP Protocol Suite", ACM Computer Communications Review, 19(2), March 1989.

[31] Border, J., Kojo, M., Griner, J., Montenegro, G., and Z. Shelby, "Performance Enhancing Proxies Intended to Mitigate Link-Related Degradations", RFC 3135, June 2001.

[32] Caceres, R. and L. Iftode, "Improving the Performance of Reliable Transport Protocols in Mobile Computing Environments", IEEE Journal on Selected Areas in Communication, 13(5):850-857, June 1995.

[33] Dawkins, S., Montenegro, G., Kojo, M., Magret, V., and N. Vaidya, "End-to-end Performance Implications of Links with Errors", BCP 50, RFC 3155, August 2001.

[34] Droms, R., "Dynamic Host Configuration Protocol", RFC 2131, March 1997.

[35] Ferguson, P. and D. Senie, "Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing", BCP 38, RFC 2827, May 2000.

[36] Jacobson, V., "Compressing TCP/IP Headers for Low-Speed Serial Links", RFC 1144, February 1990.

[37] Ioannidis, J., Duchamp, D., and G. Maguire, "IP-Based Protocols for Mobile Internetworking", In Proceedings of the SIGCOMM ’01 Conference: Communications Architectures and Protocols, pages 235-245, September 1991.

[38] Ioannidis, J. and G. Maguire, "The Design and Implementation of a Mobile Internetworking Architecture", In Proceedings of the Winter USENIX Technical Conference, pages 489-500, January 1993.

[39] Ioannidis, J., "Protocols for Mobile Internetworking", PhD Dissertation - Columbia University in the City of New York, July 1993.

[40] Jacobson, V., "Congestion Avoidance and Control", In Proceedings of the SIGCOMM ’88 Workshop, ACM SIGCOMM, ACM Press, pages 314-329, August 1998.

[41] McCloghrie, K. and F. Kastenholz, "The Interfaces Group MIB", RFC 2863, June 2000.

[42] McGregor, G., "The PPP Internet Protocol Control Protocol (IPCP)", RFC 1332, May 1992.

[43] Montenegro, G. and V. Gupta, "Sun's SKIP Firewall Traversal for Mobile IP", RFC 2356, June 1998.

[44] Perkins, C., Ed., "IP Mobility Support", RFC 2002, October 1996.

[45] Stevens, R., "TCP/IP Illustrated, Volume 1: The Protocols", Addison-Wesley, Reading, Massachusetts, 1994.

[46] Perkins, C. and P. Calhoun, "Authentication, Authorization, and Accounting (AAA) Registration Keys for Mobile IPv4", RFC 3957, March 2005.

[47] Simpson, W., Ed., "The Point-to-Point Protocol (PPP)", STD 51, RFC 1661, July 1994.

[48] IANA, "Mobile IPv4 Numbers", http://www.iana.org.

[49] Postel, J., "Multi-LAN address resolution", RFC 925, October 1984.

[50] Perkins, C., Ed., "IP Mobility Support for IPv4", RFC 3220, January 2002.

Appendix A. Link-Layer Considerations

The mobile node MAY use link-layer mechanisms to decide that its point of attachment has changed. Such indications include the Down/Testing/Up interface status [41], and changes in cell or administration. The mechanisms will be specific to the particular link-layer technology, and are outside the scope of this document.

The Point-to-Point-Protocol (PPP) [47] and its Internet Protocol Control Protocol (IPCP) [42] negotiate the use of IP addresses.

The mobile node SHOULD first attempt to specify its home address, so that if the mobile node is attaching to its home network, the unrouted link will function correctly. When the home address is not accepted by the peer, but a transient IP address is dynamically assigned to the mobile node, and the mobile node is capable of supporting a co-located care-of address, the mobile node MAY register that address as a co-located care-of address. When the peer specifies its own IP address, that address MUST NOT be assumed to be a foreign agent care-of address or the IP address of a home agent. PPP extensions for Mobile IP have been specified in RFC 2290 [23]. Please consult that document for additional details for how to handle care-of address assignment from PPP in a more efficient manner.

Appendix B. TCP Considerations

B.1. TCP Timers

When high-delay (e.g., SATCOM) or low-bandwidth (e.g., High-Frequency Radio) links are in use, some TCP stacks may have insufficiently adaptive (non-standard) retransmission timeouts. There may be spurious retransmission timeouts, even when the link and network are actually operating properly, but just with a high delay because of the medium in use. This can cause an inability to create or maintain TCP connections over such links, and can also cause unneeded retransmissions that consume already scarce bandwidth. Vendors are encouraged to follow the algorithms in RFC 2988 [26] when implementing TCP retransmission timers. Vendors of systems designed for low-bandwidth, high-delay links should consult RFCs 2757 and 2488 [24], [25]. Designers of applications targeted to operate on mobile nodes should be sensitive to the possibility of timer-related difficulties.

B.2. TCP Congestion Management

Mobile nodes often use media that are more likely to introduce errors, effectively causing more packets to be dropped. This introduces a conflict with the mechanisms for congestion management found in modern versions of TCP [40]. Now, when a packet is dropped, the correspondent node's TCP implementation is likely to react as if there were a source of network congestion, and initiate the slow-start mechanisms [40] designed for controlling that problem. However, those mechanisms are inappropriate for overcoming errors introduced by the links themselves, and have the effect of magnifying the discontinuity introduced by the dropped packet. This problem has been analyzed by Caceres, et al. [32]. TCP approaches to the problem of handling errors that might interfere with congestion management are discussed in documents from the PILC working group [31] [33]. While such approaches are beyond the scope of this document, they illustrate that providing performance transparency to mobile nodes involves understanding mechanisms outside the network layer. Problems introduced by higher media error rates also indicate the need to avoid designs that systematically drop packets; such designs might otherwise be considered favorably when making engineering tradeoffs.

Appendix C. Example Scenarios

This section shows example Registration Requests for several common scenarios.

C.1. Registering with a Foreign Agent Care-of Address

The mobile node receives an Agent Advertisement from a foreign agent and wishes to register with that agent using the advertised foreign agent care-of address. The mobile node wishes only IP-in-IP encapsulation, does not want broadcasts, and does not want simultaneous mobility bindings:

```
IP fields:
  Source Address = mobile node's home address
  Destination Address = copied from the IP source address of the
    Agent Advertisement
  Time to Live = 1
UDP fields:
  Source Port = <any>
  Destination Port = 434
Registration Request fields:
  Type = 1
  S=0,B=0,D=0,M=0,G=0
  Lifetime = the Registration Lifetime copied from the
    Mobility Agent Advertisement Extension of the
    Router Advertisement message
  Home Address = the mobile node's home address
  Home Agent = IP address of mobile node's home agent
  Care-of Address = the Care-of Address copied from the
    Mobility Agent Advertisement Extension of the
    Router Advertisement message
  Identification = Network Time Protocol timestamp or Nonce
Extensions:
  An authorization-enabling extension (e.g., the Mobile-Home
    Authentication Extension)
```

C.2. Registering with a Co-Located Care-of Address

The mobile node enters a foreign network that contains no foreign agents. The mobile node obtains an address from a DHCP server [34] for use as a co-located care-of address. The mobile node supports all forms of encapsulation (IP-in-IP, minimal encapsulation, and GRE), desires a copy of broadcast datagrams on the home network, and does not want simultaneous mobility bindings:

```
IP fields:
  Source Address = care-of address obtained from DHCP server
  Destination Address = IP address of home agent
  Time to Live = 64
UDP fields:
  Source Port = <any>
  Destination Port = 434
Registration Request fields:
  Type = 1
  S=0,B=1,D=1,M=1,G=1
  Lifetime = 1800 (seconds)
  Home Address = the mobile node's home address
  Home Agent = IP address of mobile node's home agent
  Care-of Address = care-of address obtained from DHCP server
  Identification = Network Time Protocol timestamp or Nonce
Extensions:
  The Mobile-Home Authentication Extension
```

C.3. Deregistration

The mobile node returns home and wishes to deregister all care-of addresses with its home agent:

```
IP fields:
  Source Address = mobile node's home address
  Destination Address = IP address of home agent
  Time to Live = 1
UDP fields:
  Source Port = <any>
  Destination Port = 434
Registration Request fields:
  Type = 1
  S=0,B=0,D=0,M=0,G=0
  Lifetime = 0
  Home Address = the mobile node's home address
  Home Agent = IP address of mobile node's home agent
  Care-of Address = the mobile node's home address
  Identification = Network Time Protocol timestamp or Nonce
Extensions:
  An authorization-enabling extension (e.g., the Mobile-Home
    Authentication Extension)
```

Appendix D. Applicability of Prefix-Lengths Extension

Caution is indicated with the use of the Prefix-Lengths Extension over wireless links, due to the irregular coverage areas provided by wireless transmitters. As a result, it is possible that two foreign agents advertising the same prefix might indeed provide different connectivity to prospective mobile nodes. The Prefix-Lengths Extension SHOULD NOT be included in the advertisements sent by agents in such a configuration.

Foreign agents using different wireless interfaces would have to cooperate using special protocols to provide identical coverage in space, and thus be able to claim to have wireless interfaces situated on the same subnetwork. In the case of wired interfaces, a mobile node disconnecting and subsequently connecting to a new point of attachment may well send in a new Registration Request no matter whether the new advertisement is on the same medium as the last recorded advertisement. And, finally, in areas with dense populations of foreign agents it would seem unwise to require the propagation via routing protocols of the subnet prefixes associated with each individual wireless foreign agent; such a strategy could lead to quick depletion of available space for routing tables,

unwarranted increases in the time required for processing routing updates, and longer decision times for route selection if routes (which are almost always unnecessary) are stored for wireless "subnets".

Appendix E. Interoperability Considerations

This document specifies revisions to RFC 2002 that are intended to improve interoperability by resolving ambiguities contained in the earlier text. Implementations that perform authentication according to the new more precisely specified algorithm would be interoperable with earlier implementations that did what was originally expected for producing authentication data. That was a major source of non-interoperability before.

However, this specification does have new features that, if used, would cause interoperability problems with older implementations. All features specified in RFC 2002 will work with the new implementations, except for V-J compression [36]. The following list details some of the possible areas of compatibility problems that may be experienced by nodes conforming to this revised specification, when attempting to interoperate with nodes obeying RFC 2002.

- A client that expects some of the newly mandatory features (like reverse tunneling) from a foreign agent (FA) would still be interoperable as long as it pays attention to the 'T' bit.

- Mobile nodes (MNs) that use the NAI extension to identify themselves would not work with old mobility agents.

- Mobile nodes that use a zero home address and expect to receive their home address in the Registration Reply would not work with old mobility agents.

- Mobile nodes that attempt to authenticate themselves without using the Mobile-Home authentication extension will be unable to successfully register with their home agent.

In all of these cases, a robust and well-configured mobile node is very likely to be able to recover if it takes reasonable actions upon receipt of a Registration Reply with an error code indicating the cause for rejection. For instance, if a mobile node sends a Registration Request that is rejected because it contains the wrong kind of authentication extension, then the mobile node could retry the registration with a mobile-home authentication extension, since the foreign agent and/or home agent in this case will not be configured to demand the alternative authentication data.

Appendix F. Changes since RFC 3344

The following revisions to details of the specification in this document were made after RFC 3344 was published. A list of changes from RFC 2002 made during the development of RFC 3344 [21] may be found in the latter document. For items marked with issue numbers, more information is available by consulting the MIP4 mailing list archives.

- Showed more bit definitions in the Agent Advertisement message structure (see Section 2.1.1). New advertisement bits have been defined by other specification documents, but not reflected in previous publications of this specification; this has led to confusion. Citations for the other specification documents have also been included.

- (Issue 6) The behavior of the home agent was changed to avoid mandating error replies to Registration Requests that were invalidated because the foreign agent failed authentication. The intention is to make the home agent more robust against Denial of Service attacks in which the malicious device has no intention of providing a valid Registration Request but only wants to congest traffic on the home network. See Section 3.8.2.1.

- Due to non-unique assignment of IPv4 addresses in many domains, it is possible for different mobile nodes to have the same home address. If they use the NAI, the foreign agent can still distinguish them. Language was added to Section 3.7.1 and Section 3.7.3.1 to specify that the foreign agent MUST use the NAI to distinguish mobile nodes with the same home address.

- (Issue 45) Specified that a foreign agent MUST NOT apply a Foreign-Home Authentication extension to a mobile node's deregistration request. Also, the foreign agent MUST NOT apply a Foreign-Home Authentication extension unless the Care-of Address in the Registration Request matches an address advertised by the foreign agent.

- Specified that the Mobility Security Association to be used by the foreign agent and home agent depends upon values contained in the message data, not the IP headers.

- (Issues 9, 18) Created a new error code for use by the foreign agent, for the case when the foreign agent does not serve the mobile node as a home agent. Formerly, the foreign agent could use an error Code of 136 for this case.

- (Issue 17) Specified that, if the home agent cannot support the requested nonzero unicast address in the Home Address field of the Registration Request, then it MUST reject the registration with an error Code of 129. See Section 3.8.3.2.

- (Issue 19) Specified that multiple authorization-enabling extensions may be present in the Registration Request message, but that the home agent has to (somehow) ensure that all have been checked (see Section 3.8.3.1).

- (Issue 20) Specified that the foreign agent SHOULD NOT modify any of the fields of the Registration Reply message that are covered by the Mobile-Home Authentication Extension, when it relays the packet to the mobile node.

- (Issue 21) Clarified that the foreign agent removes extensions that do not precede any authorization-enabling extension, not just the Mobile-Home Authentication extension (Section 3.7.3.2).

- (Issue 44) Specified that the address advertised by the foreign agent in Agent Advertisements is the care-of address offered on that network interface, not necessarily the address of the network interface (Section 3.7.2.2).

- (Issue 45) Clarification in Section 3.7.2.1 that Code 77 can only apply to a Registration Request with nonzero Lifetime.

- Created a new error code for use when a foreign agent can detect that the Home Agent address field is incorrect.

- Prohibited the use of the Foreign-Home Authorization Extension on deregistration messages.

- Cleaned up some more wording having to do with authorization-enabling extensions.

- For consistency, changed some wording about copying UDP ports.

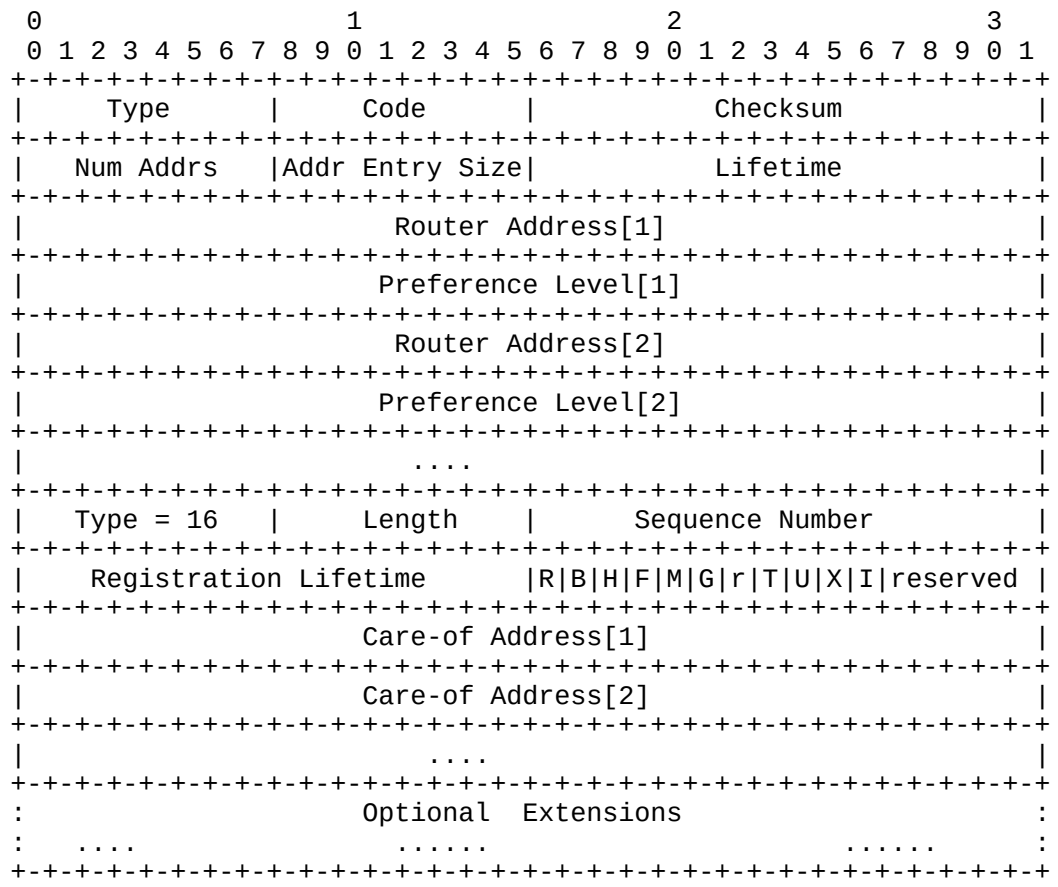
- Added wording to clearly not disallow dynamically configuring netmask and security information at the mobile node.

- Revamped Changes section.

- Updated citations.

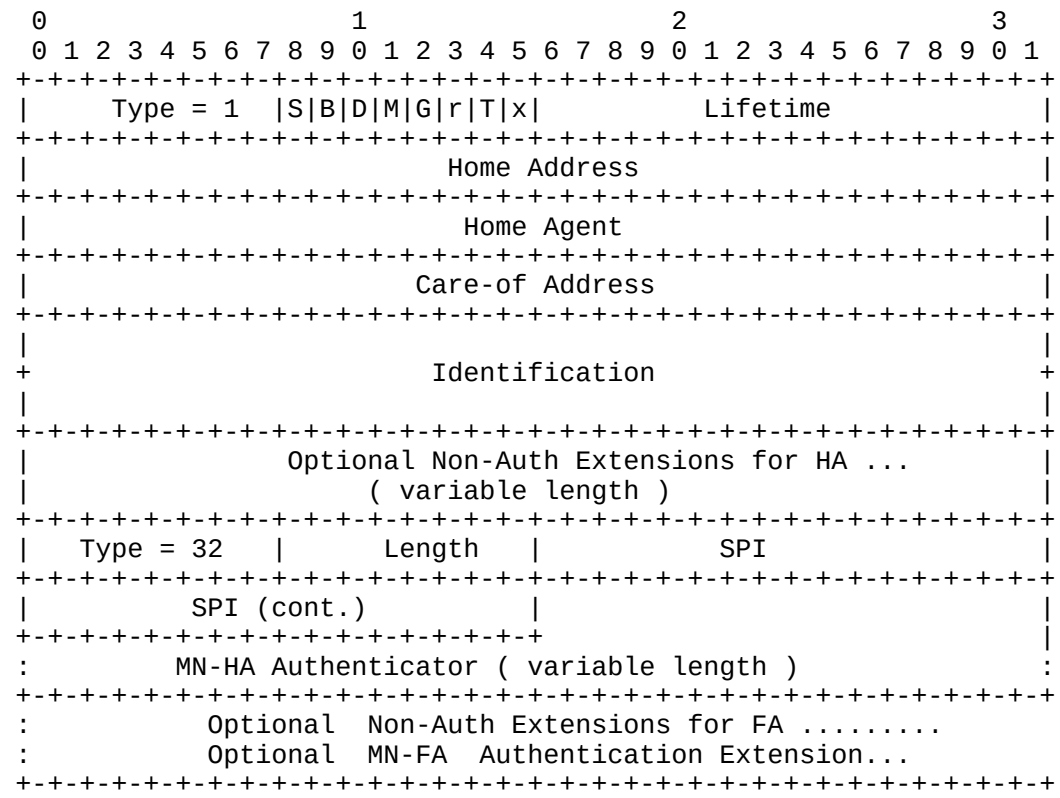
Appendix G. Example Messages

G.1. Example ICMP Agent Advertisement Message Format



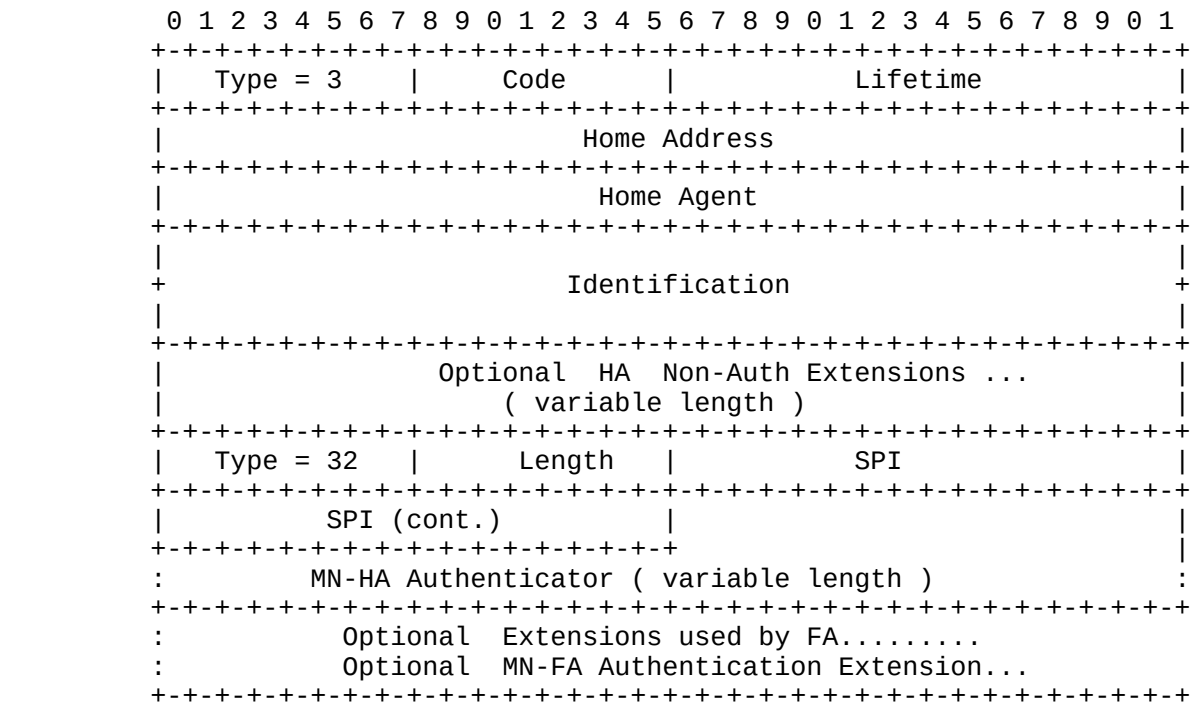
G.2. Example Registration Request Message Format

The UDP header is followed by the Mobile IP fields shown below:



G.3. Example Registration Reply Message Format

The UDP header is followed by the Mobile IP fields shown below:



Author’s Address

Charles E. Perkins (editor)
WiChorus Inc.
3590 N. 1st Street, Suite 300
San Jose, CA 95134
USA

EMail: charliep@computer.org