

Distributed Registration Extension to Mobile IP
draft-chuahli-mobileip-dremip-00.txt

Status of This Memo

This document is a submission to the Mobile-IP Working Group of the Internet Engineering Task Force (IETF). Comments should be submitted to the mobile-ip@smallworks.com mailing list.

Distribution of this memo is unlimited.

This document is an Internet-Draft. Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as ``work in progress.''

To learn the current status of any Internet-Draft, please check the ``1id-abstracts.txt' listing contained in the Internet-Drafts Shadow Directories on ftp.is.co.za (Africa), nic.nordu.net (Europe), munnari.oz.au (Pacific Rim), ds.internic.net (US East Coast), or ftp.isi.edu (US West Coast).

Abstract

This document proposes an extension to the Mobile IP base protocol. The features in this extension allow us to (i) reduce frequent distant registrations at the mobility agents, (ii) be more scalable by a separation of registration and forwarding services, (iii) ease the key management problem among mobility agents, and (iv) be interoperable with other mobility agents/mobile nodes running standard Mobile-IP specified in [RFC2002](#).

Contents

Abstract	i
1. Introduction	1
1.1. Architectural Entities	2
1.3. Terminology	2
1.3. Design Goals	4
1.3.1 Reduce Distant Registration Frequency	4
1.3.2 Ease of Key Management	5
1.3.3 Increase Scalability	5
2. Protocol Overview	6
2.1. Agent Discovery	6
2.2. Local Registration	6
2.3. Home Registration	7
2.4. Transit Registration	7
2.5. Datagram Routing	8
2.6. Local/Home Service.....	8
2.7. Foreign Server Smooth Handoffs	9
2.8. Optimizing Registrations	9
2.9. Interoperability with the Base Protocol	10
3. Message Formats	11
3.1. Agent Advertisement	11
3.2. Registration Request	11
3.3. Registration Reply	12
3.4. Route Request	12
3.5. Route Reply	13
4. Newly Defined Extensions	14
4.1. Registration Server Extension	14
4.2. Care-of Address Extension	14
4.3. Agent-Server Authentication Extension	16
4.4. Mobile-Server Authentication Extension	16
4.5. Server-Server Authentication Extension	17
5. Care-of Agent Considerations	17
5.1. Receiving Route Request	17
5.2. Binding Route Enable/Disable.....	18
6. Registration Server Considerations	18
6.1. Data Structure	19
6.2. Receiving Registration Request as a Binding Registrar	19
6.3. Receiving Registration Request as a Binding Relay	20
6.4. Sending Route Request	21
6.5. Receiving Route Reply	21
6.6. Load Balancing	22

Expires April 1998

[Page ii]

7. Mobility Agent Considerations	22
7.1. Sending Agent Advertisement	22
7.2. Receiving Registration Request as a Foreign Agent	22
7.3. Receiving Registration Request as a Home Agent	22
7.4. Receiving Registration Reply	22
7.5. Receiving Route Request	22
8. Mobile Node Considerations	23
8.1. Receiving Agent Advertisement	23
8.2. Sending Registration Request	23
8.3. Receiving REgistration Reply	24
8.4. Handoff	24
Appendix A Registration Server Discovery Procedure	25
Appendix B Care-of Agent Discovery Procedure	25
Appendix C Key Distribution Between Registration Servers	25
Appendix D Example Scenarios	26
Appendix D.1 Local/Home Registrations	26
Appendix D.2 Transit/Home Registrations	27
Appendix D.3 Optimizing Registrations	31
Appendix D.4 Interoperability with RFC2002	32
Reference	33
Acknowledgement	34
Authors's Address	34

Expires April 1998

[Page iii]

1. Introduction

Mobile IP base protocol [[1](#)] provides an efficient, scalable mechanism for node mobility within the Internet. However, the key management between the home and foreign agents, and between the foreign agents and the mobile node is still a problem.

Secondly, as Perkins [[2](#)] addresses in the hierarchical foreign agents model, each time the mobile node moves, a Registration Request message has to be approved by the mobile node's Home Agent. In cases where the home agent is far away, it may become too expensive or even impossible to complete these frequent registrations. This document proposes an extension to the Mobile IP base protocol to solve these problems.

In this internet draft, we introduce some extensions to the base protocol to provide a more scalable solution to the mobility management problem. Our proposed extension separates the the registration and forwarding services. The registration service can be provided additionally by a network entity called registration server while the forwarding service can be provided by a network entity called care-of agents. The introduction of registration servers allow us to reduce the number of trusted entities in the network and hence enable us to ease the key management problem. It also allows us to do authentications such that illegal use of routing services. The introduction of care-of agents allow us to do load-balancing according to the dynamically changing traffic needs. In addition, we define 3 types of registrations, namely local, home and transit registrations. By having these different types of registrations, we are able to reduce the frequency of distant registrations. Our new features are introduced in such a way that the mobile nodes and mobility agents supporting our new features can still interoperate with mobile nodes and mobility agents supporting the base protocol specified in [RFC2002](#).

1.1. Architectural Entities

The memo introduces the following new architectural entities:

Registration Server (RS)

An entity providing registration service within a routing domain. A registration server in the mobile node's home routing domain is called a Home Registration Server. A registration server in the routing domain that the mobile node is visiting is called a Local Registration Server. Otherwise, it is called a Transit Registration Server.

Care-of Agent (COA)

An entity providing forwarding service and hence care-of addresses. In the base protocol, a care-of agent is the foreign agent itself. However, we propose here to separate it from the foreign agent.

1.2. Terminology

Care-of Address

The care-of address is redefined, in this memo, as an IP address from which datagrams can be relayed to the mobile node, whether or not through one or more intermediate nodes.

Mobility Binding

The mobility binding is redefined the same as in the base protocol except that the care-of address takes the above definition.

Registration

The registration is redefined as a procedure for mobile node to register a mobility binding with a registration server or a home agent and to obtain a care-of address closer to the home agent, by exchange of Registration Request and Registration Reply messages. In the base protocol, this is a registration with a home agent.

The care-of address submitted in the Registration Request is called the CHILD care-of address of the registration. The one obtained by this registration is called the PARENT care-of address of the registration.

Binding Registrar

A registration server or home agent, with which the mobile node

registers a mobility binding. In the base protocol, this is the home agent, with which a mobility binding is associated.

Expires April 1998

[Page 2]

Binding Relay

A foreign agent or registration server, through which the Registration Reply for a mobility binding can be delivered to the mobile node. In the base protocol, this is the foreign agent.

A mobile node is allowed to register a mobility binding with a binding registrar via a binding relay.

Home/Local/Transit Registration

A registration where the binding registrar is in the mobile node's home routing domain is called a home registration. A registration where the binding registrar is in the routing domain that is visited by the mobile node is called a local registration. Otherwise, the registration is called a transit registration.

Complete Registration

The combination of one or more registrations, which allows tunnels to be built such that there will be at least one forwarding path from the home agent to the visiting mobile node.

Binding Route Enabled/Disabled

A binding route is enabled by a care-of agent if, a datagram destined for the mobile node is relayed by this care-of agent from the parent care-of address of a registration to the child care-of address. In the base protocol, this means to build a tunnel from the home agent to the care-of address and to add a routing entry to the care-of address for the mobile node.

A binding route is disabled by a care-of agent if, the care-of agent functions as a regular router disregarding the existence of a mobility binding if any. Thus, a datagram destined for the mobile node will be forwarded to the mobile node's home network or simply discarded with an ICMP message bounced if the datagram was tunneled to the care-of agent.

1.3 Design Goals

There are 5 major design goals for this protocol, namely,

- (i) reduce frequent distant registrations,
- (ii) ease key management,
- (iii) prevent illegal use of routing services,
- (iv) increase scalability,
- (iv) interoperable with [RFC2002](#).

This protocol separates the the registration and forwarding services. The registration service is provided by the registration server while the forwarding service is provided by the care-of agents. Since each routing domain may only have one registration server and many care-of agents, the number of trusted entities in mobile networks are reduced and hence enable us to ease the key management problem. It also allows us to do authentications such that illegal use of routing services can be prevented.

1.3.1 Reduce Frequent Distant Registrations

To reduce frequent distant registrations, we define 3 types of registrations, namely local, home and transit registrations. When the mobile node moves from one routing domain to another, it needs to perform a home registration with the home registration server (HRS) to inform the HRS of the identity of the local Registration Server it is currently registered.

When the mobile node moves within the same routing domain, even though its point of attachment may change from one foreign agent to another, the mobile node only needs to perform local registrations. As long as the parent care-of address in the local Registration Reply message matches with the one obtained previously, the mobile node needs not perform any home registrations. That way, the number of distant registrations with HRS can be reduced.

The transit registrations are used when the mobile node's home registration server does not have security association with the local registration server. The local server will give the mobile node the identity of a registration server which can act as a middleman for the home registration. The mobile node will first perform a transit registration with this transit registration server to get a parent care-of address. Using this allocated care-of address from the transit registration, the mobile node can then do a home registration via the transit registration server.

In our proposed registration extension MobileIP protocol, we assume that the home registration life time exceeds the transit registration life time which exceeds the local registration life time.

1.3.2 Ease of Key Management/Prevent Illegal Usage

One of the design goals in this protocol is to prevent replay attacks in the mobile node's registration procedure, and to prevent an illegal mobile node from stealing services from a routing domain. The existing mobile IP base protocol does not require an existence of security associations between the mobile node and the foreign agent, and between the home agent and the foreign agent.

If there are already such security associations, this protocol works exactly the same way as the base protocol. Otherwise, this protocol provides a means to compensate for a lack of such security associations. We assume that there are security associations between registration servers. Since the number of registration servers are much less than the number of mobility agents, we have a reduction in key management problem. This makes the our enhanced Mobile-IP model more scalable.

If there is no security association between the mobile node and the foreign agent or no security association between the foreign agent and the home agent, the mobile node will not be allowed to register directly with its home agent, but to first register with a registration server in the local routing domain. This local server in turn allocates a parent care-of address and returns to the mobile node via the registration reply.

If there is a security association between the foreign server and the mobile node's home agent, the mobile node can subsequently register the parent care-of address allocated by the foreign server with the home agent.

Otherwise, the mobile node is advised to register with its home registration server via the foreign server. This is feasible because there are security associations between the foreign server and the home server, and between the mobile node and the home server. Thus, a completely secured binding is established, which allows packets to be delivered to the mobile node.

1.3.3 Increase Scalability

As mentioned above, the introduction of registration servers reduces the number of trusted entities and hence reduce the severity of key management problem. Hence, our enhanced Mobile-IP model is more scalable than the Base protocol. In addition, by separating the

registration service with the forwarding services and introducing as many care-of agents as we need, we can perform some load-balancing to cater to the dynamically changing traffic needs.

Expires April 1998

[Page 5]

2. Protocol Overview

A mobile node should have a complete registration when it moves away from its home network. A complete registration consists of local registrations, home registrations and/or transit registrations. A registration starts with receiving Agent Advertisements. Thus, changes for this protocol will apply to both the Agent Discovery and the Registration procedures.

2.1 Agent Discovery

In the base protocol, the foreign agents advertise their presence via Agent Advertisement messages. The mobile node obtains a care-of address (which usually is the foreign agent's address) from the advertisements. The mobile node may initiate a registration using this care-of address.

In this proposal, the care-of address obtained from the Agent Advertisement and used in a registration request is referred to as the child care-of address of this registration.

In addition to the care-of addresses in the Agent Advertisement message, our proposal requires that the Agent Advertisement message includes a registration server extension so that prospective mobile nodes can choose a registration server for the local registration. The registration extension contains one or more registration server addresses. There is a priority value and a lifetime associated with each registration server's address.

2.2 Local Registrations

When the mobile node detects a change in the point of attachment, it performs a local registration with the local registration server via a foreign agent. The mobile node sends a Registration Request message to the local server. The local server replies with a Registration Reply message. This message contains a parent care-of address which usually is the IP address of a care-of agent that has been assigned to provide forwarding service for the visiting mobile node. One can consider this care-of agent as the local home agent in terms of forwarding. Note that if the local registration server happens to be the home agent or the Home Registration Server of the mobile node, then usually the care-of agent assigned will be the home agent of the mobile node.

The local server may request the assigned care-of agent to enable the binding route via an exchange of Route Request and Route Reply messages with the care-of agent. Thereafter, packets from any node within the local routing domain may be able to reach the mobile node. This may additionally require changes to relevant intra-domain

routing protocols, which is beyond the scope of this document.

For any registration, we require that a care-of address, called the parent care-of address, be returned to the mobile node by means of the registration reply.

Expires April 1998

[Page 6]

2.3 Home Registrations

If the parent care-of address obtained via local registration is not the same as the address of the mobile node's home agent, and the parent care-of address is also different from that obtained previously, then, the mobile node should perform home registrations. The mobile node builds a new mobility binding using this parent care-of address by registering this binding with its home registration server, via the local server. The mobile node does so via an exchange of Registration Request and Registration Reply message with the home server.

In this home registration, the parent care-of address obtained through a previous local registration becomes the child care-of address. The care-of address returned from the home registration server is a new parent care-of address which usually is the address of the mobile node's home agent. In this manner, a complete registration is performed among the mobile node, the foreign agent, the local server, the home server and the home agent.

The home server may request the home agent to enable the binding route, that is, to build a tunnel from the new parent care-of address (the home agent's address) to the child care-of address (a care-of agent's address at the visiting domain) via an exchange of Route Request and Route Reply messages.

2.4 Transit Registrations

There are two scenarios where transit registrations may be used. Type 1 Transit Registrations are used when the mobile node moves from one routing domain to another and has a valid mobility binding with a previous foreign server. In this case, the mobile node may issue a transit registration request to that previous foreign server to enable a binding route from the previous parent care-of address to the current one.

Such a mobility binding is transitional and helps to ensure that data that has been delivered to the previous parent care-of address can be forwarded to the new parent care-of address. This transitional binding can be removed once the mobile node has completed its registration of the new parent care-of address with the home registration server.

Type 2 Transit Registrations are used when a foreign server in the visiting domain has no security association with the home server. In this case, the mobile node may register, via the local server, the local parent care-of address with a transit registration server, which in turn allocates a new parent care-of address to the mobile

node. The mobile node then registers, via the transit server, this new parent care-of address with the home server. It is expected that the mobile node has security association with the transit registration server.

2.5 Datagram Routing

Through a series of local, transit and home registrations, the mobile node obtains a path from the home agent to the foreign agent. The path consists of a sequence of tunnels with the starting point of the first tunnel being the home agent, and the termination point of the last tunnel being the foreign agent, and each of the tunnels begins with a parent care-of address and ends with a child care-of address.

Datagrams sent to the mobile node's home address are intercepted by its home agent, tunnelled from one care-of agent to another until they reach the foreign agent, and finally being delivered to the mobile node by the foreign agent.

These tunnels fall into three categories: home tunnels, transit tunnels, and local tunnels. A home tunnel begins with a home agent or a care-of agent allocated by a home registration server, and ends with a care-of agent allocated by another registration server. A transit tunnel begins with a care-of agent allocated by a transit registration server and ends with a care-of agent allocated by the current visiting registration server. A local tunnel begins with a care-of agent allocated by the current visiting registration server and ends at the foreign agent. Each of these tunnels is authorised by two registration servers or by a registration server and a mobility agent.

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 care-of agents, the home or foreign agent.

2.6 Local/Home Service

In some cases, the mobile node may just be interested in communicating with the hosts in its visiting domain but not interested in having home traffic forwarded to its visiting location. For such scenarios, if the visiting network has pre-arrangement with the mobile node's home registration server to provide local services to mobile nodes that belong to that home registration server, then the mobile node only needs to perform local registration.

2.7 Foreign Server Smooth Handoffs

When a mobile node moves and discovers that the local registration server does not change, then it only needs to perform a local registration.

When a mobile node moves and discovers that the local registration server has changed, then it not only performs a local registration, it also performs a home registration. As in the route optimization draft [6], a Previous Foreign Server Notification option can be implemented so that the new foreign server can notify the old foreign server about the mobile node's new mobility binding. This notification can be used by the previous server to tear down existing tunnels. Such notification also allows any datagrams that have been delivered to the previous care-of agent to be delivered to the new care-of agent.

If the new foreign registration server does not have a security association with the home registration server, then all 3 types of registrations, namely local, transit and home registrations have to be performed.

2.8 Optimizing Registrations

In earlier sections, we describe how DREMIP supports local, transit and home registrations. In this section, we elaborate a bit on how a mobile node can combine both the local and home registrations within one Registration Request message.

A mobile node who wishes to make a local and home registrations can send a Registration Request message with a registration server extension. The binding registrar in the Registration Request message will be the local server and a MN/Local Server authentication extension can be appended. The Home Registration Server identity is contained in the Registration Server Extension. The Mobile Node can also attach the MN/Home Server Extension at the back of the Registration Server Extension.

We refer the readers to [Appendix D.3](#) for more details on such registration optimizations.

In addition, it is a requirement in DREMIP that the following inequality holds for local, home and transit registration lifetimes:

Local Registration LifeTimes <= Transit Registration LifeTimes

<= Home Registration LifeTimes

Note also that the lifetimes of the different tunnels: local, transit and home tunnels can be set according to the local, transit and home registration lifetimes respectively. If the Previous Foreign Agent Notification feature is implemented, then the tunnel lifetimes can be set to infinity and the deregistration message can be used to tear down the tunnel.

Expires April 1998

[Page 9]

2.9 Interoperability with the Base Protocol

To make the this protocol compatible with the base protocol, a few requirements apply to the mobile node, foreign agent and home agent.

Upon receipt of an Agent Advertisement message without registration server extension, the mobile node should be able to register with a home agent via the foreign agent as in the base protocol. In this case, the mobile node should not check for the presence of any care-of address extension in the Registration Reply.

In addition, the Registration Request should be sent as a Home Registration Request. The binding registrar address field should be the home registration server address or the home agent address. If there is no security association between the mobile node and the home agent, but there exists one between the mobile node and the home server, then the Registration Request should be directed to the home server.

A home or foreign agent should check the R-bit in the Registration Request message to determine whether the mobile node is supported by this protocol. A foreign agent, upon receipt of a Registration Request with R-Bit cleared, should not require that there be a mobile-foreign authentication extension in the request and a foreign-home authentication extension in the further reply message.

In [Appendix D.4](#), we give two example scenarios and explain in greater details how a mobile node without DREMIP feature can use the Mobile-IP service in a DREMIP network and how a mobile node with DREMIP feature can use the Mobile-IP service in a [RFC2002](#)-compliant foreign network.

3. Message Formats

3.1 Agent Advertisement

The Agent Advertisement messages additionally include a registration server extension, which contains one or more registration server addresses. Thus, the mobile node can be informed of the registration server addresses and register its mobility binding with one of them.

3.2. Registration Request

One bit is added to the Registration Request message to indicate the registration is supported by this distributed registration extension protocol. The IP and UDP fields of the Registration Request message is the same as described in [RFC2002](#). The UDP header is followed by the Mobile IP fields shown below:

```

      0               1               2               3
    0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
|      Type      |S|B|D|M|G|V|R|r|      Lifetime      |
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
|                                     Home Address        |
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
|                                     Binding Registrar    |
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
|                                     Care-of Address      |
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
|                                     Identification        |
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
| Extensions ...                                         |
+---+---+---+---+---+

```

distributed Registration extension (R):

The R-bit is set by a mobile node or a binding registrar to indicate that the procedure is supported by this registration extension protocol. This bit is for the purpose of interoperability with the base protocol.

Reserved (r):

The r-bit should be set to 0.

Binding Registrar:

A home agent or a registration server.

Expires April 1998

[Page 11]

3.3. Registration Reply

There is no change in the format of the Registration Reply message except that, the "Home Agent" field is renamed to "Binding Registrar" field.

In addition to a few authentication extensions, the Registration Reply MUST include a care-of address extension so that a registration server can allocate a parent care-of address to the mobile node. The Registration Reply MAY additionally append a registration server extension to advise the mobile node to choose a registration server address as the next binding registrar.

3.4. Route Request Message

Route Request is sent by a registration server to a care-of agent to enable a binding route between the care-of agent and a child care-of address of a registration.

IP fields:

Source Address	Typically the interface address from which the message is sent.
----------------	---

Destination Address	Typically the IP address of the care-of agent.
---------------------	--

UDP fields:

Source Port <variable>

```
Destination Port      434
```

The UDP header is followed by the fields shown below:

[illegible]

Type 32 (Route Request)

Reserved sent as zero; ignored on reception.

Lifetime

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

Destination Address

The home address of the mobile node.

Next Hop Address

The child care-of address of a registration

Identification

A 64-bit number, constructed by the server, used for matching Route Requests with Route Replies, and for protecting against replay attacks of these messages.

Extensions

The fixed portion of the Route Request is followed by one or more of the Extensions.

3.5. Route Reply Message

The care-of agent returns a Route Reply message to the server which has sent a Route Request ([Section 3.4](#)) message. The Reply message contains the necessary codes to inform the server about the status of its request, along with the lifetime granted by the care-of agent, which MAY be smaller than the original Request.

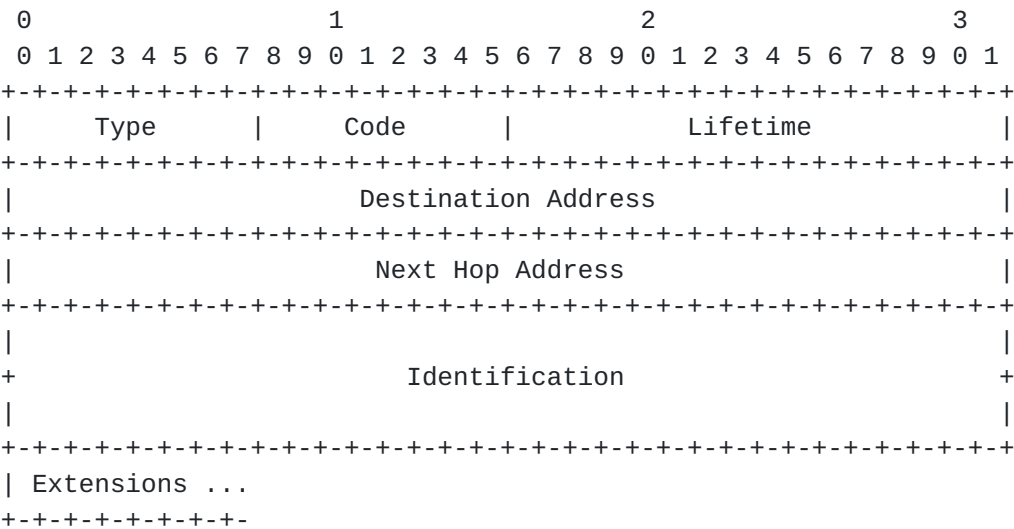
IP fields:

Source Address	Typically copied from the destination address of the Route Request to which the care-of agent is replying.
Destination Address	Copied from the source address of the Route Request to which the care-of agent is replying

UDP fields:

Source Port	<variable>
Destination Port	Copied from the source port of the corresponding Route Request

The UDP header is followed by the fields shown below:



Type	33 (Route Reply)
Code	A value indicating the result of the Route Request. See below for a list of currently defined Code values.

Lifetime

If the Code field indicates that the care-of agent agrees to add the route capability, the Lifetime field is set to the number of seconds remaining before the route is considered expired. A value of zero indicates that the route has been disabled. A value of 0xffff indicates infinity.

If the Code field indicates that the route was denied, the contents of the Lifetime field are unspecified and MUST be ignored on reception.

Destination Address

The home address of the mobile node.

Next Hop Address

The child care-of address of a registration

Identification

A 64-bit number used for matching Route Requests with Route Replies, and for protecting against replay attacks of tunnel messages. The value is based on the Identification field from the Route Request message from the client.

Extensions

The fixed portion of the Route Reply is followed by one or more of the Extensions.

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

0 route added

64 reason unspecified

65 administratively prohibited

67 server failed authentication

68 requested Lifetime too long

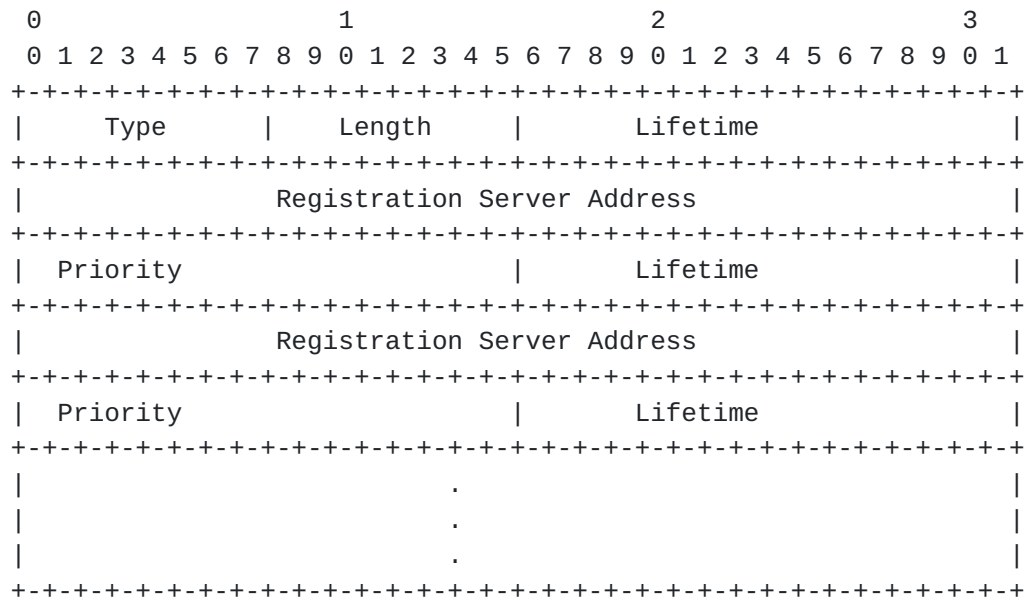
69 poorly formed message

Up-to-date values of the Code field are specified in the most recent "Assigned Numbers" [\[5\]](#).

4. Newly Defined Extensions

4.1. Registration Server Extension

This extension is placed in the Agent Advertisement message or Registration Reply message, and is used to provide the mobile node with addresses of a collection of available registration servers. Note that we have included a priority level for different registration servers. One can use this priority level to provide hierarchical registrations or as an congestion-level indicator to prevent mobile nodes from registering with an overloaded registration server.



Type 81

Length 2 + 8 * number of registration server addresses

Lifetime

The number of seconds remaining before the registration server is considered invalid. A value of zero indicates the registration server doesn't provide service to more mobile nodes. A value of 0xffff indicates infinity.

Priority

The level of authorization.

4.2. Care-of Address Extension

This extension is placed in the Registration Reply so that a registration server can allocate a care-of address to the mobile

[illegible]

Length 6

```
care-of address
    parent care-of address or home agent address
```

4.3. Agent-Server Authentication Extension

This extension is included in the Registration Request and Registration Reply messages between the foreign agent and the foreign registration server, and between the home agent and the home registration server. The protocol here requires that there exists a security association between an agent and a registration server in the same routing domain.

The extension **MUST** also be included in the Route Request and Route Reply messages between a registration server and a care-of agent.

```

0             1             2             3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
|   Type   |   Length   |   SPI   ....
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
... SPI (cont.) |   Authenticator ...
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+

```

Type 83

Length 4 plus the number of bytes in the Authenticator.

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

Authenticator
 (variable length)

4.4. Mobile-Server Authentication Extension

This extension is included in the Registration Request and Registration Reply messages between the mobile node and the foreign registration server, and between the mobile node and the home registration server. The protocol here requires that there exists a security association between a mobile node and a registration server whether they are in the same routing domain or not.

```

0             1             2             3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
|   Type   |   Length   |   SPI   ....
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
... SPI (cont.) |   Authenticator ...
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+

```

Type 84

Length 4 plus the number of bytes in the Authenticator.

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

Authenticator
 (variable length)

Expires April 1998

[Page 16]

4.5. Server-Server Authentication Extension

This extension is included in the Registration Request and Registration Reply messages between two registration servers, especially between the foreign registration server and the home registration server. The protocol here requires that there exists a security association between two registration servers whether they are in the same routing domain or not.

```

      0               1               2               3
      0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
|   Type   |   Length   |   SPI   ....
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
... SPI (cont.) |   Authenticator ...
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+

```

Type 85

Length 4 plus the number of bytes in the Authenticator

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

Authenticator
(variable length)

5. Care-of Agent Considerations

The care-of agent could be an OSPF area border router, an autonomous system border router or a backbone router. In the base Mobile-IP protocol, the care-of address was originally associated with a foreign agent and a foreign agent has the responsibility of forwarding the traffic destined to the mobile node. In this registration extension protocol, the care-of agent is designed to forward traffic destined to the mobile node.

5.1. Receiving Route Request

Upon receipt of a Route Request, the care-of agent MUST check the validity of the message. The request is valid if

- the UDP checksum is valid; AND
- the message MUST include an Agent-Server Authentication extension at the end and the Authenticator is valid.

An invalid request SHOULD be discarded and an error SHOULD be logged.

On receipt of a valid Route Request message, the care-of agent SHOULD

respond with a Route Reply with the lower 32-bit identification copied from the original request.

If the care-of agent is not able to honor the request, it SHOULD put a proper code in the reply.

Expires April 1998

[Page 17]

If the care-of agent denies the request and disable the binding route to the child care-of address, it SHOULD set the code to a positive value (0) and the lifetime to 0.

Otherwise, if the care-of agent agrees to enable a binding route to the child care-of address, it SHOULD set the code to a positive value (0) and the lifetime to a value not greater than that in the original Request. The binding route is valid within the granted lifetime and SHOULD be disabled upon its expiry.

5.2. Binding Route Enable/Disable

In general, a care-of agent MAY enable or disable a binding route using tunneling mechanism ([4]). Within a routing domain, however, the care-of agent MAY take advantage of underlying routing protocols instead. This approach may be discussed elsewhere. In this document, we assume a care-of agent uses the tunneling mechanism.

To enable a binding route, the care-of agent MAY first build a tunnel to the next hop address specified in the Route Request message if such a tunnel does not exist previously. The care-of agent then installs in its forwarding cache an entry with the tunnel as the outgoing circuit. To disable the registration delivery, the care-of agent can simply remove the entry from its forwarding cache. If there is no entry associated with the tunnel, the care-of agent SHOULD additionally remove this tunnel.

6. Registration Server Considerations

A registration server MAY not be a router. It is designed to be independent of the forwarding path for mobile traffic, and to monitor and switch the forwarding path. A registration server performs local registrations at most times but less frequently does home and transit registrations.

The local registration is used to establish the local mobility binding of a mobile node, that is, the association of the mobile node with a local registration server, a foreign agent, and the lifetime of this association. The local mobility binding MAY create the mobile node's connectivity to the local routing domain.

The local registration server, taking the advantage of the above local mobility binding, then establishes a home mobility binding, that is, the association of the mobile node with the home agent or the home registration server of the mobile node, the local registration server, and the lifetime of the association.

The registration server MAY be configured with one or more care-of

agent addresses, which are allocated to mobile nodes such that traffic load can be balanced.

Expires April 1998

[Page 18]

6.1. Data Structure

For each registration server and each visiting mobile node, there are generally two registrations: one where the registration server acts as the binding registrar and the other where the registration server acts as a binding relay. Each registration creates an entry in the registration server cache. Since the mobile node may perform multiple registrations (home and/or transit) based on an existing local registration, a registration server SHOULD NOT merge the two entries into one. The entry created by a local registration where the registration server is the binding registrar consists of

- mobile node's home address
- child care-of address and
- parent care-of address
- lifetime, and
- the forwarding status over the tunnel between parent and child care-of address.

Each entry created by the home or transit registration where the registration server is the binding relay should have a pointer to the above entry, and additionally includes

- binding registrar, and - lifetime

6.2. Receiving Registration Request as a Binding Registrar

Upon receiving a valid registration request where the registration server is the binding registrar, the server should check if the mobile node is previously associated with any care-of agent. If it is not, the server should choose a parent care-of address. The server SHOULD exchange a pair of Route Request and Route Reply with the relevant care-of agent in order for the care-of agent to enable a binding route for the lifetime requested by the mobile node. The server SHOULD NOT return Registration Request to the mobile node until it receives a Route Reply from the care-of agent.

After the server receives a positive Route Reply from the care-of agent, the server will verify that the tunnel lifetime is consistent with the registration life time. Then, the server SHOULD send a positive Registration Reply to the mobile node if there is a security association between itself and the mobile node. The server SHOULD deny this request by sending a negative Registration Reply to the mobile node. In this case, the server SHOULD additionally ask the care-of agent to disable the binding route by exchange of negative Route Request and Route Reply.

For this case, if the registration server previously does not have

a mobility binding yet with the mobile node, it SHOULD allocate a parent care-of address, put it in a care-of address extension, and append the extension to the Registration Reply. However, if the registration server has a binding with the mobile node previously, the old care-of address SHOULD be put in that extension. This ensures that the mobile node can obtain the same parent care-of address if repeatedly registering with the registration server.

The registration server MAY include a registration server extension in the Registration Reply message for the mobile node to perform further transit/home registrations.

The registration server SHOULD include an agent-server or server-server authentication extension in the reply if the binding relay is the foreign agent or another registration server, respectively.

If there is no tunnel currently between the parent and child care-of address, the registration server SHOULD direct the care-of agent, by issuing a Route Request message, to build a tunnel from the parent care-of address to the child care-of address of the mobile node. The child care-of address is specified in the Registration Request while the parent care-of address is allocated by the binding registrar.

If the registration server is a home server, the parent care-of address it allocates MAY be the home agent address. In this case, the care-of agent is the home agent.

6.3. Receiving Registration Request as a Binding Relay

Upon receiving a valid registration request where the registration server is the binding relay, the registration server MUST verify that there is already an entry for this mobile node where it acts as a binding registrar. If not, the Registration Request MUST deny this request. The registration server SHOULD also verify that there is a security association between itself and the binding registrar. If not, the server SHOULD deny this request. The binding lifetime SHOULD

not be greater than the one with the current mobility binding where the registration server acts as a binding registrar. Otherwise, the server SHOULD deny this request.

If the Registration Request message meets all the requirements above, the registration server MAY relay this request to the binding registrar in the same way as the foreign agent deals with the Registration Request in the base protocol.

The registration server MAY deny the request and include a registration server extension for the mobile node to perform a transit registration with another server. The mobile node can then perform further home registration via this transit server.

The registration server SHOULD include a server-server authentication extension in the request to be relayed, or a mobile-server authentication extension in the reply if the server denies the

request above.

Expires April 1998

[Page 20]

6.4. Sending Route Request

To ensure the care-of agent can forward traffic to the mobile node, the server SHOULD send a Route Request to the care-of agent. The server SHOULD copy lifetime from the Registration Request to the Route Request.

The server SHOULD retransmit Route Request if it has not received a matched Route Reply in a reasonable time. Failure in receipt of such a Route Reply message after a maximum of retransmissions SHOULD be logged for further administrative option. The server MAY choose another care-of agent and repeat the procedure above until no care-of agent is available. In this case, the server SHOULD send a negative Registration Reply to the mobile node.

The server MUST append an Agent-Server Authentication extension to the Route Request message. The SOMIP model requires that there be a security association between the server and the care-of agent.

6.5. Receiving Route Reply

Upon receipt of a Route Reply, the server MUST check the validity of the message. The reply is valid if

- the UDP checksum is valid;
- the low-order 32 bits of the Identification field in the Route Reply equals to the low-order 32 bits of the Identification field in the most recent Route Request sent to the care-of agent; AND
- the reply MUST include a Agent-Server Authentication extension.

If the code field is negative or the lifetime is zero, the server MUST send a Registration Reply message with a negative code or lifetime set to 0.

Otherwise, the server must check for consistency between the tunnel life time and the registration lifetime. If no previous agent notification feature is implemented, then the tunnel life time should not exceed the remaining registration life time. Otherwise, it may be allowed to exceed to reduce the bandwidth overhead required in refreshing tunnel lifetimes.

6.6. Load Balancing

Each registration server occasionally probes their care-of agents on the traffic load that each of them is supporting. The care-of agents each return a metric that has a higher value when the traffic load is

higher. Based on such replies, the server can order the list of care-of addresses with the least loaded one being at the top of the list. When the server receives a local registration request, it assigns the least loaded care-of address to that request.

7. Mobility Agent Considerations

7.1 Sending Agent Advertisement

A mobility agent SHOULD include a registration server extension in the Agent Advertisements. This can facilitate the mobile node in finding a registration server with whom it has security association for subsequent registrations.

7.2. Receiving Registration Request As a Foreign Agent

Upon receiving a Registration Request, a foreign agent SHOULD verify that there is a security association between itself and the binding registrar. If there is, the agent works exactly the same as the foreign agent in the base protocol.

Otherwise, the agent SHOULD deny the Registration Request. The agent MAY include a registration server extension in the Registration Reply

message for the mobile node to choose another binding registrar and to perform further registrations.

7.3. Receiving Registration Request as a Home Agent

The home agent deals with a received Registration Request in the same way as the home agent in the base protocol.

7.4. Receiving Registration Reply

The mobility agent deals with a received Registration Reply in the same way as in the base protocol.

7.5. Receiving Route Request

The foreign agent SHOULD disregard this message.

The home agent SHOULD deal with the Route Request in the same way as the care-of agent. The home agent SHOULD additionally send proxy ARP and gratuitous ARP on the home network. The procedure SHOULD be the same as in the base protocol.

Expires April 1998

[Page 22]

8. Mobile Node Considerations

8.1. Receiving Agent Advertisement

When a mobile node receives an agent advertisement, it SHOULD check to see if the mobility agent is its home agent. If it is, it does nothing since it is at home. Otherwise, it checks to see if there is a registration server extension in the agent advertisement. If yes, the mobile node SHOULD choose one of the registration servers whose addresses appear in the registration server extension and perform a local registration with the selected server. Note that if the mobile node is in its home domain i.e. the home registration server appears in the registration server extension, then the mobile node SHOULD choose its home registration server.

8.2 Sending Registration Request

The mobile node SHOULD choose a proper binding relay and a binding registrar from previously received Agent Advertisement messages. For local registrations, the binding relay is the foreign agent, and the binding registrar is one of the local registration servers whose addresses appear in the registration server extension. Note that if the mobile node is in its home domain, then the binding registrar that the mobile node chooses SHOULD be its home registration server.

For the case where the mobile node is visiting a foreign network, the mobile node will use the local registration server as the binding relay and the home registration server as the binding registrar in the mobile node's home registration request.

For transit registrations, the binding registrar is a registration server with whom the mobile node has previously established a mobility binding or with whom the mobile node has a security association, while the binding relay could be a foreign agent or another registration server.

If the mobile node previously receives a negative Registration Reply, which includes a registration server extension, it SHOULD choose a proper binding registrar to proceed further registration.

The mobile node SHOULD include a mobile-server authentication extension in the request if the binding relay is a registration server.

Expires April 1998

[Page 23]

8.3 Receiving Registration Reply

Upon receiving a valid local registration reply, the mobile node SHOULD check to see if the binding registrar or the parent care-of address returned in the reply is its home agent. If yes, this is a complete registration. If it is not, however, the mobile node SHOULD check to see if it has previously established a mobility binding with its home registration server or home agent, using this parent care-of address.

If it has, nothing needs to be done since the mobile node just changes its point of attachment locally. Otherwise, the mobile node SHOULD perform a home registration using this parent care-of address. In this second registration, the local server will be used as the binding relay and the binding registrar will be set to the home registration server's address. The mobile node SHOULD make sure that the home registration life time exceeds the local registration life time.

If the reply includes a registration server extension, it means the the binding registrar advises the mobile node to perform further registration with one of the registration servers in the extension. In this case, the mobile node SHOULD choose one of them and proceed with a registration with the local server set to the binding relay, and the selected registration server set to the binding registrar. Again, the mobile node SHOULD make sure that the transit registration life time exceeds the local registration lifetime. Later, if the mobile node needs to perform home registration, the mobile node SHOULD make sure that the home registration lifetime exceeds the transit registration lifetime.

8.4. Handoff

When a mobile node moves from one foreign routing domain to another, the mobile node performs a local registration with the new local server. Then, it can first do a transit registration with its previous foreign registration server such that a tunnel can be built from the previous foreign server's care-of address to the new local server's care-of address. This tunnel is a transitional tunnel that enables the forwarding of packets that have been sent to the previous

foreign server but have not been delivered to the mobile node. Later,

it performs a home registration with its home registration server using the new local server's care of address. After establishing a complete binding with the home registration server, the transitional tunnel can be torn down.

Expires April 1998

[Page 24]

Appendix A Registration Server Discovery Procedures

Here, we describe a procedure for mobility agents to discover the registration servers. We assume that a multicast address has been assigned to all registration servers. A mobility agent merely needs to send a Neighbor Request message to the multicast address of the registration servers. All registration servers that can hear this Neighbor Request message will respond with a unicast Neighbor Reply message. The Neighbor Reply message contains a priority level field. The mobility agent then puts the addresses of all registration servers and their associated priority levels in the Agent Advertisement messages that it broadcasts. The Neighbor Request message can be repeated periodically with a period long enough to limit the overhead bandwidth consumption. Details of this registration server discovery procedure will be provided in another upcoming internet draft.

Appendix B Care-of Agent Discovery Procedures

In practice, we may just manually configure care-of agents. However, when there are a lot of care-of agents available and more than one registration servers exist, we may want a more dynamic assignment of care-of agents to registration servers. Here, we describe a procedure for registration servers to discover the presence of care-of agents in its vicinity. Again, we assume that a multicast address is defined for registration server and all care-of agents in a routing domain. The registration server can send a Care-of Agent Solicit message to that multicast address. All care-of agents that can hear this Care-of Agent Solicit message will have to respond to the Registration Server with a unicast Care-of Agent Advertisement message.

Appendix C Key Distribution between Registration Servers

We assume that all cooperating registration servers share a public key and has a private key. We can use the same approach discussed in [\[6\]](#).

Appendix D Example Scenarios

This section shows example Registration Requests for several common scenarios.

D.1 Local/Home Registrations

D.1.1 Local Registration

The mobile node receives an Agent Advertisement from a foreign agent which has a registration server extension showing RS2 as the local registration server. Assume that the mobile node has a security association with RS2. The mobile node 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, does not want simultaneous mobility bindings:

IP fields:

Source Address = mobile node's home address

Destination Address = copied from 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, R=1

Lifetime= the Registration Lifetime copied from the Mobility Agent Advertisement Extension of the Router Advertisement message

Home Address = the mobile node's home address

Binding Registrar = IP address of RS2 copied from Registration Server extension

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:

The Mobile-Foreign(RS2) Authentication Extension

The Mobile-Agent Authentication Extension (?)

The foreign agent will relay the Registration Request to RS2. The mobile node upon hearing a positive registration reply from RS2 (which is relayed by the foreign agent) will copy the parent care-of address (COA1) allocated from the Care-of Address Extension in the Registration Reply. The mobile node will create an entry to record the local registration server's IP address, the parent care-of address, and the local registration life time.

If we allow for local service and that the foreign network prefers a tunnel to be built between the care-of agent and the foreign agent for routing mobile node's traffic packets, then RS2 will direct the care-of agent whose IP address is the parent care-of address (COA1) to build a tunnel to the foreign agent.

D.1.2 Home Registration

Then, the mobile node will send another Registration Request

IP fields:

Source Address = mobile node's home address

Destination Address = RS2's IP address

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, R=1

Lifetime= 0xffff

Home Address = the mobile node's home address

Binding Registrar = MN's Home Server (RS1) 's IP address

Care-of Address = the allocated parent care-of address extracted
from the Care-of Address extension in the Local Registration
Reply.

Identification = Network Time Protocol timestamp or Nonce

Extensions:

The Mobile-Home (RS1) Authentication Extension

The Mobile-Foreign(RS2) Authentication Extension

The local server, RS2, will relay the Home Registration Request to the MN's Home Server (RS1) by adding the Server (RS2)-Server (RS1) Authentication Extension. The MN's Home Server will check for the validity of the Registration Request and sends a Registration Reply via the local server to the mobile node. The Registration Reply will contain the MN/Home Server Authentication Extension and the Server/Server Authentication Extension. If the Home Server approves the home registration, then the Home Registration Reply will contain a Care-of Address extension that gives the home agent's IP address as the parent care-of address. The Home Server will direct the home agent to build a tunnel to COA1. The Home Server does so by sending a Route Request Message with Server/Agent Authentication Extension (if the Home Server does not trust the Home

D.2 Transit/Home Registration

D.2.1 Transit Registration

Assume that RS2 does not have any server/server authentication with RS1 in Example D.1.2 above. Then, RS2 will reject the Home Registration Request and attaches a Registration Server Extension in its reply:

Registration Reply from RS2 will be as follows:

IP fields:

Source Address = copied from destination address of the
Registration Request to which RS2 is replying

Destination Address = copied from the source address of the
Registration Request to which RS2 is replying

UDP fields:

Source Port = <any>

Destination Port = 434

Registration Request fields:

Type = 3

Code = 67

Lifetime= ignored

Home Address = the mobile node's home address

Binding Registrar = MN's Home Server (RS1) 's IP address

Identification = copied from Registration Request message

Extensions:

Registration Server Extension which gives RS3 as the
transit registration server.

The Mobile-Home (RS1) Authentication Extension

The Mobile-Foreign(RS2) Authentication Extension

The mobile node will then send a Registration Request with RS3 as the binding registrar.

IP fields:

Source Address = mobile node's home address

Destination Address = RS2's IP address

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, R=1

Lifetime= 0xffff

Home Address = the mobile node's home address

Binding Registrar = RS3's IP address

Care-of Address = the allocated parent care-of address extracted
from the Care-of Address extension in the Local Registration
Reply.

Identification = Network Time Protocol timestamp or Nonce

Extensions:

The Mobile-Home (RS1) Authentication Extension

The Mobile-Foreign(RS3) Authentication Extension

The Mobile-Foreign(RS2) Authentication Extension

The local server, RS2, will relay the Transit Registration Request to RS3. RS3 will validate the Registration Request and sends a Registration Reply to MN. If RS3 approves the transit registration, it will attach a Care-of Address extension which contains information on the new parent care-of address (COA2).

D.2.2 Home Registration

The mobile node then sends a Home Registration Request to its Home Server via RS3

IP fields:

Source Address = mobile node's home address

Destination Address = RS3's IP address

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, R=1

Lifetime= 0xffff

Home Address = the mobile node's home address

Binding Registrar = MN's Home Server

Care-of Address = the allocated parent care-of address, COA2
extracted from the Care-of Address extension in the Transit
Registration Reply.

Identification = Network Time Protocol timestamp or Nonce

Extensions:

The Mobile-Home (RS1) Authentication Extension

The Mobile-Foreign(RS3) Authentication Extension

If the Home Server approves the registration, it will send a Registration Reply with an attached Care-of Address Registration that gives home agent address as the parent care-of address. The Home Server will also instruct the Home Agent to build a tunnel to COA2. When RS3 receives the Registration Reply, it will also instruct COA2 to build a tunnel to COA1. If local service is not provided by the local server, then we can let transit server notifies the local server upon successful home registration and the local server can then instruct COA1 to build a tunnel to the foreign agent.

D.3 Optimizing Registrations

Based on the examples described above, we describe in this section how the number of registrations can be reduced.

D.3.1 Local/Home Registration

With the requirement that the Agent Advertisement contains all registration servers' addresses that the local server has authentication with, a mobile node can decide if it can perform a home registration together with a local registration. If the mobile node finds its Home Server's address in the Agent Advertisement, it can send a Registration Request Message with an attached Registration Server Extension which contains the Home Server address and its life time.

IP fields:

Source Address = mobile node's home address

Destination Address = foreign agent's IP address

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, R=1

Lifetime= LifeTime copied from Agent Advertisement

Home Address = the mobile node's home address

Binding Registrar = local server (RS2)'s IP address

Care-of Address = foreign agent address

Identification = Network Time Protocol timestamp or Nonce

Extensions:

The Registration Server Extension with Home Server information and Home Registration Lifetime

The Mobile-Home (RS1) Authentication Extension

The Mobile-Agent Authentication Extension(?)

The Mobile-Foreign(RS2) Authentication Extension

If the local server RS2 approves the registration, it will change the binding registrar to the Home Server's IP address (extracted from Registration Server Extension), replaces the Lifetime with Home Registration Lifetime, and change the care-of address to a newly allocated parent care-of address. Then, it relay this registration request message (without the registration server extension) to the Home Server. Upon receiving a reply from the Home Server, the local server formulates the following Registration Reply:

IP fields:

Source Address = copied from destination address of the
Registration Request to which RS2 is replying
Destination Address = copied from the source address of the
Registration Request to which RS2 is replying

UDP fields:

Source Port = <any>

Destination Port = 434

Expires April 1998

[Page 31]

Registration Request fields:

Type = 3
Code =
Lifetime= Local Registration LifeTime
Home Address = the mobile node's home address
Binding Registrar = RS2's IP address
Identification = copied from Registration Request message

Extensions:

Registration Server Extension which gives Home Server's
IP address as well as Home Registration LifeTime
The Mobile-Home (RS1) Authentication Extension
The Mobile-Foreign(RS2) Authentication Extension

Similar optimizations can be done for the case of transit registrations.

D.4 Interoperability with [RFC2002](#)

D.4.1 Mobile Node with DREMIP feature in a [RFC2002](#)-compliant network

Assume that MN1 which has DREMIP feature visits a foreign network that runs [RFC2002](#)-compliant base Mobile-IP protocol. MN1 receives an Agent Advertisement without Registration Server Extension. Hence, it issues a Registration Request Message with R bit cleared to its Home Agent/Home Registration Server via the Foreign Agent. The Registration Request Message will not have a Registration Server Extension. To the foreign agent, the binding registrar's field is like the Home Agent field in the base protocol. MN1 attaches the MN/Server or MN/Home Agent Authentication extension. If there exists authentication extension between MN1 and the Foreign Agent, MN1 will also attach that extension. The Foreign Agent will then deliver the Registration Request to the binding registrar which can either be the Home Registration Server or Home Agent. If the binding registrar is the Home Registration Server (HRS), then the HRS will issue a Registration Reply which has the MN's home address and its home agent address just like in base Mobile-IP protocol without attaching any Care-of Address extension.

D.4.2 Mobile Node without DREMIP feature in a DREMIP compliant network

The mobile node will ignore the registration server extension in the Agent Advertisement. The mobile node will issue a Registration Request with R bit cleared to the foreign agent. The Registration Request contains the MN's home address and MN's home agent address. The mobile node attaches the MN/Home Agent Authentication and the MN/Foreign Agent Authentication extensions. Note that here, we assume that unless there is a MN/Foreign Agent Authentication extensions, the mobile node cannot use the service in this foreign network. The foreign agent in the DREMIP network notices that the R-bit is clear and hence just relays the Registration Request message to the MN's Home Agent. The Home Agent issues a Registration Reply which doesn't contain Care-of-Address extension to the Foreign Agent. The Foreign Agent faithfully delivers the Registration Reply message to the mobile node.

References

- [1] Charles Perkins, editor. IP mobility support. [RFC 2002](#), Oct 1996.
- [2] Charles Perkins. Mobile-IP Local Registration with Hierarchical Foreign Agents. Internet Draft, [draft-perkins-mobileip-hierfa-00.txt](#), February 1996. Work in progress.
- [3] Charles Perkins. IP Encapsulation within IP. [RFC 2003](#), October 1996.
- [4] David B. Johnson and Charles Perkins. Route Optimization in Mobile IP. Internet Draft, [draft-ietf-mobileip-optim-04.txt](#), February 1996. Work in progress.
- [5] Joyce K. Reynolds and Jon Postel. Assigned Numbers. [RFC 1700](#), October 1994.
- [6] J. Zao, etc. A Public-Key Based Secure Mobile IP, Proceedings of Mobicom97, October, 1997.
- [7] D. Johnson, etc. Route Optimizations in Mobile-IP networks Internet Draft. [draft-optim-05.txt](#), October, 1997. Work in progress.

Expires April 1998

[Page 33]

Acknowledgement

The authors wish to thank Wee Tuck Teo from National University of Singapore for some useful comments on an earlier draft.

Authors' Address

Questions about this memo can also be directed to:

M. C. Chuah,
Performance Analysis Department,
Room 3K-320,
Bell Laboratories,
Lucent Technologies,
101, Crawfords Corner Road,
Holmdel, NJ 07733, USA.
Phone: 732-949-7206
Fax: 732-834-5906
Email: chuah@lucent.com

Y. Li
Protocol Development Group
Engineering Department
Bay Networks, Inc.
BL60-304, 600 Technology Park Drive
Billerica, MA 01821
Phone: (508) 916-1130
Fax: (508) 670-8760
Email: yli@BayNetworks.COM

