Network Working Group Y. Rekhter
INTERNET-DRAFT (T.J. Watson Research Center, IBM Corp.)
Richard Colella (NIST)

TUBA Mobility Support

(draft-ietf-tuba-mobility-00.txt)

(Posted: May 16, 1994/Expires: November 16, 1994)

Status of this Memo

This document is a submission to the TUBA Working Group of the Internet Engineering Task Force (IETF). Comments should be submitted to the tuba@lanl.gov mailing list.

Distribution of this memo is unlimited.

Abstract

This document specifies protocol enhancements that allow transparent routing of CLNP datagrams to Mobile Nodes in the Internet. The 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 the Home Agent. The Home Agent tunnels traffic destined for the Mobile Node to the Care-Of-Address.

Acknowledgements

This document is taken almost verbatim from the draft-ietf-mobileip-protocol-02.txt Internet Draft. The latter is the product of the mobile-ip WG.

1. Introduction

If a node moves while keeping its address unchanged, the address may not reflect its new point of attachment. The routing protocols will not be able to route datagrams to it correctly.

This document defines new functions that allow a node to roam on the Internet, without changing its network layer address (NSAP).

The following entities are defined:

Mobile Node

A TUBA host or router that changes connections from one network or subnetwork to another.

Home Agent

A router on a network that advertises reachability for a Mobile Node, maintains a registry of the current Mobility Bindings for that node while it is away from home, and tunnels datagrams for delivery to a Mobile Node.

Foreign Agent

A router that assists a locally reachable Mobile Node that is away from its home network.

The following support services are defined:

Agent Discovery

Agents advertise their availability on each link.

A newly arrived Mobile Node can send a solicitation on the link to learn if any prospective Agents are present.

Care-Of-Address Assignment

The Care-Of-Address terminates the end of a tunnel toward a Mobile Node. Depending on the foreign network configuration, the Care- Of-Address may be dynamically assigned to the Mobile Node, or associated with a Foreign Agent.

Registration

When the Mobile Node is away from home, it registers the Care-Of- Address with the Home Agent.

Depending on its method of attachment, the Mobile Node will register either directly with a Home Agent, or through a Foreign Agent which forwards the registration to the Home Agent.

Encapsulation

Once a Mobile Node has registered a Care-Of-Address with a Home Agent, the Home Agent intercepts datagrams destined for the Mobile Node, formulates another datagram with the intercepted datagram enclosed within, and forwards the resulting datagram to the Care- Of-Address.

Decapsulation

At the Care-Of-Address, the enclosed datagram is extracted.

When the Mobile Node has its own Care-Of-Address, it decapsulates its own datagrams.

When the Care-Of-Address is associated with a Foreign Agent, the Foreign Agent decapsulates the datagrams. If the datagram is addressed to a Mobile Node which the Foreign Agent is currently serving, it will deliver the datagram to the Mobile Node.

Otherwise, the datagram MUST be silently discarded (rather than being further forwarded). CLNP ER Destination Unreachable MUST NOT be sent when a Foreign Agent is unable to forward a datagram.

1.1. Requirements

A Mobile Node using its Home-Address shall be able to communicate with other nodes after having been disconnected from the Internet, and then reconnected at a different point.

A Mobile Node shall continue to be capable of communicating directly with existing nodes that do not implement the mobility functions described in this document.

A Mobile Node shall provide authentication in its registration messages.

1.2. Goals

As few administrative messages as possible are sent between a Mobile Node and a Foreign Agent. The link is likely to be bandwidth limited.

The size of messages on the Mobile Node's directly attached link are to be kept as short as possible. The link is likely to be bandwidth limited.

1.3. Assumptions

The protocols defined in this document place no additional requirements on assignment of addresses (NSAPs). That is, a Mobile Node will be assigned an address (NSAP) by the organization that owns the machine, and will be able to use that address (NSAP) regardless of the current point of attachment.

Mobile Nodes are able to change their point of attachment to the Internet as frequently as once per second.

No protocol enhancements are required in hosts or routers that are not serving any of the mobility functions. Similarly, no additional protocols are needed by a router (that is not acting as a Home Agent or a Foreign Agent) to route datagrams to or from a Mobile Node.

The operation of this specification assumes that CLNP datagrams are routed to a destination without regard to the source of the datagram.

If desired, the Mobile Node can tunnel to its Home Agent. The

definition of such tunneling mechanisms is outside the scope of this specification.

1.4. Specification Language

In this document, several words are used to signify the requirements of the specification. These words are often capitalized.

MUST This word, or the adjective "required", means that the definition is an absolute requirement of the specification.

MUST NOT This phrase means that the definition is an absolute prohibition of the specification.

SHOULD This word, or the adjective "recommended", means that there may exist valid reasons in particular circumstances to ignore this item, but the full implications must be understood and carefully weighed before choosing a different course.

MAY This word, or the adjective "optional", means that this item is one of an allowed set of alternatives. An implementation which does not include this option MUST be prepared to interoperate with another implementation which does include the option.

silently discard

The implementation discards the packet 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 packet, and SHOULD record the event in a statistics counter.

1.5. Terminology

This document frequently uses the following terms:

Authentication Type

This includes the algorithm and algorithm mode. Note that a single algorithm (such as DES) might have several modes (for example, CBC and ECB).

Correspondent Host

The peer with which a Mobile Node is communicating. The

Correspondent Host may be either mobile or stationary.

Home-Address

A long term address (NSAP) that is assigned to a Mobile Node. It remains unchanged regardless of where the node is attached to the Internet. The Home-Address is intercepted by the Home Agent while the Mobile Node is registered with that Home Agent.

Link

A communication facility or medium over which nodes can communicate at the link layer; underlying the network layer.

Mobility Binding

The association of a Home-Address with a Care-Of-Address, and the remaining LifeTime of the association.

Mobility Security Association

The security relationship between two nodes that is used with Mobile CLNP protocol messages. This relationship includes the authentication type (including algorithm and algorithm mode), the secret (such as a shared key, or appropriate public/private key pair), and possibly other information such as labelling.

Triangle Routing

A path followed by a datagram destined for a Mobile Node, when that datagram arrives first at the Home Agent, and then is encapsulated and tunneled by the Home Agent.

2. Agent Discovery

To communicate with a Foreign or Home Agent, a Mobile Node must learn either the network layer address (NSAP) or the link layer address of that Agent.

It is assumed that a link-layer connection has been established between the Agent and the Mobile Node. The method used to establish such a link-layer connection is not specified in this document.

After establishing a link-layer connection that supports the attachment of Mobile Nodes, the node must learn if there are any prospective Foreign Agents available to serve it while it is away from home. If the Mobile Node is returning home, it must learn if its Home Agent is available.

There are often several methods of learning the availability of an Agent. Those described here are recommended.

Multi-Point Link-Layers
Link establishment protocol, IEEE 802.11, might yield the link address of an agent. This link-layer address is used to attempt registration.

ES-IS

Configuration information provided by ES-IS protocol allows a Mobile Node to discover the existence and reachability of a Foreign Agent, and permits a Foreign Agent to discover the existence and reachability of a Mobile Node.

It is recommended that as few messages as possible which duplicate functionality be sent on mobile links. This is particularly important on wireless and congested links.

When multiple methods are in use, the Mobile Node SHOULD first attempt registration with routers sending ISH packets in preference to those sending link-layer advertisements. This ordering maximizes the likelihood that the registration will be recognized, thereby minimizing the number of registration attempts.

An Administrative Domain MAY require registration with a Foreign Agent even when another registration method is in use. This facility is envisioned for service providers with packet filtering fire-walls, or visiting policies (such as accounting) which require exchanges of authorization.

2.1. Authentication

No authentication is required for the advertisement and solicitation process.

These messages MAY be authenticated using a TUBA Authentication mechanism (as described in draft-ietf-inlsp-tuba-00.txt), which is external to the messages described here. Further work on authentication of advertisement and solicitation is outside of the scope of this document.

Whenever an externally authenticated message fails authentication, the message is silently discarded.

2.2. Agent Solicitation

Every Mobile Node is required to implement ES-IS. However, the ESH packet is only sent when no link-layer identification has been received.

Any Foreign Agent and Home Agent which is not identified by a link-layer protocol MUST implement ES-IS.

2.3. Agent Advertisement

Every Mobile Node is required to correctly process ES-IS packets.

Any Foreign Agent and Home Agent which is not identified by a link-layer protocol MUST implement ES-IS.

An Agent which is identified by a link-layer protocol SHOULD also implement ES-IS.

It is assumed that the ISH packet format is extended as to allow an indication of whether a router is willing to act as an Agent.

The Mobile Node chooses a Care-Of-Address from among advertising Agents in the same fashion as it would choose a first hop router.

3. Registration

The registration function exchanges information between Mobile Nodes and Home Agents. This function creates a Mobility Binding, linking the Home-Address with the Care-Of-Address currently used by the Mobile Node.

When assigned a transient Care-Of-Address, a Mobile Node can act without a Foreign Agent. When registering or deregistering directly with the Home Agent, the registration process involves the exchange of only 2 messages.

a) The Mobile Node sends a Registration Request to the Home Agent, to ask the Home Agent to provide the requested service.

b) The Home Agent sends a Registration Reply to the Mobile Node to grant or deny service.

An Administrative Domain MAY require registration through a Foreign Agent, as indicated in Agent Advertisements.

When the Care-Of-Address is associated with a Foreign Agent, the Foreign Agent acts as a relay between the Mobile Node and Home Agent. The extended registration process involves the exchange of 4 messages:

a) The Mobile Node sends a Registration Request to the prospective Foreign Agent to begin the registration process.

b) The Foreign Agent relays the request by sending a Registration Request to the Home Agent, to ask the Home Agent to provide the requested service.

c) The Home Agent sends a Registration Reply to the Foreign Agent to grant or deny service.

d) The Foreign Agent sends a copy of the Registration Reply to the Mobile Node to inform it of the disposition of its request.

3.1. Authentication

Each Mobile Node, Foreign Agent, and Home Agent MUST support an internal table holding a list of NSAP addresses, and the Mobility Security Association for each address.

Mobile Node to Home Agent registration messages are required to be authenticated with the Mobile-Home Authentication Extension. The Mobile Node and Home Agent MUST support authentication using keyed MD5 and key sizes of 128 bits or greater, with manual key distribution. Additional authentication algorithms, algorithm modes, and key distribution methods MAY also be supported.

In addition, the Foreign Agent SHOULD support authentication using keyed MD5 and key sizes of 128 bits or greater, with manual key distribution. Additional authentication algorithms, algorithm modes, and key distribution methods MAY also be supported.

Only one Mobility Security Association exists between any given pair of participating nodes at any given time.

Whenever a Mobility Security Association exists between a pair of nodes, all registration messages between these nodes MUST be authenticated, using the appropriate authentication extension.

3.2. UDP

The Registration messages defined herein use the User Datagram Protocol header [RFC-768]. The UDP well-known port <TBD> is used.

The UDP checksum is required. Any mobility message with an incorrect or zero UDP checksum is silently discarded.

3.3. Registration Request

The UDP Header is followed by the 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     |     Code      |           LifeTime            |
      +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
      |HAg Addr Len  |         Home Agent Address (variable)...      |
      +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
      |                         ....                                  |
      +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
      |HA Addr Len    |         Home Address (variable)...            |
      +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
      |                         ....                                  |
      +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
      |CO Addr Len    |         Care-Of-Address (variable)...         |
      +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
      |                         ....                                  |
      +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
      |                                                               |
      +                       TimeStamp                               +
      |                                                               |
      +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
      |Extensions ...
      +-+-+-+-+-+-+-+-
```

CLNP fields:

Source   The Home-Address of the Mobile Node.

Destination   The NSAP address of the Agent, when known. When the NSAP address is unknown (i.e., the agent was discovered via a link-layer protocol), the "all Mobile Agents" multicast address. The link-layer

unicast address is used to deliver the datagram to the correct Agent.

UDP fields:

Source Port variable

Destination Port <TBD>

MobileTUBA fields:

Type

1 when sent by the Mobile Node
2 when sent by the Foreign Agent

Code Optional capabilities:

0 - remove prior registrations
1 - retain prior registrations

LifeTime The seconds remaining before the registration is considered expired. A value of zero indicates a request for de-registration. A value of all ones indicates infinity.

The LifeTime SHOULD NOT be set to greater than the LifeTime learned in an Agent Advertisement.

HAg Addr Len The length of the Home Agent Address (in octets)

Home Agent The NSAP address of the Home Agent.

HA Addr Len The length of the Home NSAP address of the Mobile Node (in octets)

Home-Address The Home NSAP address of the Mobile Node.

CO Addr Len The length of the Care-Of-Address (in octets)

Care-Of-Address The NSAP address for the decapsulation end of a tunnel.

TimeStamp 64 bits. A sequence number assigned by the Mobile Node. A Network Time Protocol [RFC-1305] value is preferred, but the elapsed time since system startup, or any other monotonically increasing

counter MAY be used. The value MUST NOT be the same as an immediately preceeding request.

The Mobile-Home Authentication Extension is required, and immediately follows all non-authentication extensions.

Authenticator   A hash value taken over a stream of bytes consisting of the shared secret between the Mobile Node and Home Agent, followed by (concatenated with) the fields in the message beginning with the Code field, including all prior extensions, and the Type and Length of this extension, but not including the Authenticator field itself, and finally the shared secret again.

The Mobile-Foreign or Foreign-Home Authentication Extension is optional, and immediately follows the Mobile-Home Authentication Extension.

When forwarded by a Foreign Agent, fields and extensions are copied from the Registration Request without modification.

3.4. Registration Reply

The UDP Header is followed by the 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      |      Code     |           LifeTime            |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |HA Addr Len    |         Home-Address (variable)...            |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |                         ....                                  |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |                                                               |
   +                       TimeStamp                               +
   |                                                               |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |Extensions ...
   +-+-+-+-+-+-+-+-
```

CLNP fields:

The Source and Destination of the Request message are swapped for the Reply message.

Note that the Source of the original Registration Request must be saved in order for the Foreign Agent to return the reply to the correct Mobile Node.

UDP fields:

The Source Port and Destination Port of the Request message are swapped for the Reply message.

Note that the Source Port of the original Registration Request must be saved in order for the Foreign Agent to return the reply to the correct Mobile Node port.

MobileTUBA fields:

Type 3

Code One of the following codes:

0 service will be provided.

denied by Foreign Agent,
16 reason unspecified.
17 administratively prohibited.
18 insufficient resources.
19 Mobile Node failed authentication.
20 Home Agent failed authentication.
21 Request LifeTime too long.

denied by Home Agent,
32 reason unspecified.
33 administratively prohibited.
34 insufficient resources.
35 Mobile Node failed authentication.
36 Foreign Agent failed authentication.

Up-to-date values of the Code field are specified in the most recent "Assigned Numbers" RFC [2].

LifeTime The seconds remaining before the registration is considered expired. A value of zero confirms a request for de-registration. A value of all ones indicates infinity.

May be modified by the Home Agent.

HA Addr Len Copied from the Request message.

Home-Address Copied from the Request message.

TimeStamp Copied from the Request message.

The Mobile-Home Authentication Extension is required, and immediately follows all non-authentication extensions.

Authenticator A hash value taken over a stream of bytes consisting of the shared secret between the Mobile Node and Home Agent, followed by (concatenated with) all of the fields in the message beginning with the Code field, including all prior extensions, and the Type and Length of this extension, but not including the Authenticator field itself, and finally the shared secret again.

Note that the Care-Of-Address and Home Agent are not present in the message. This provides a separate calculation value for mutual authentication from the Home Agent to the Mobile Node.

The Mobile-Foreign or Foreign-Home Authentication Extension is optional, and immediately follows the Mobile-Home Authentication Extension.

When forwarded by a Foreign Agent, fields and extensions are copied from the Registration Reply without modification.

4. Mobility Message Extensions

To promote extensibility, each message begins with a short fixed part, which is followed by one or more extensions in Type-Length-Value format.

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 CLNP datagram.

```
     0                   1                   2
     0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2
    +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-
    |  Extension    |   Length      | Data ...
    +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-
```

Extension Current values are assigned as follows:

16	Mobility
32	Mobile-Home Authentication
33	Mobile-Foreign Authentication
34	Foreign-Home Authentication
65	GRE Encapsulation

Up-to-date values are specified in the most recent "Assigned Numbers" RFC [2].

Length Indicates the length of the Data field. The Length does not include the Extension and Length bytes.

Data This field is zero or more bytes and contains the value(s) for this Extension. The format and length of the Data field is determined by the Extension and Length fields.

When an extension is encountered which is not recognized, it is ignored. The length field is used to skip the data field in searching for the next extension.

4.1. Mobility Extension

```
 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
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|  Extension    |    Length     |        Sequence Number        |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|R|  Reserved   |
+-+-+-+-+-+-+-+-+
```

Extension 16

Length 3

Sequence Number Contains the number of advertisement messages sent since the node was initialized. This number MUST include this advertisement.

When this value decreases, the Mobile Node MUST assume that any current registration has been lost. This field cannot roll over in less than 2**16 seconds, and rollover is unambiguously indicated by

the value zero.

R — Registration required bit. When this bit is set to 1, registration with the Foreign Agent is required, even when the Mobile Node has acquired a transient Care-Of-Address.

Reserved — Sent as zero; ignored on reception.

4.2. Authentication Extensions

```
 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
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|  Extension    |     Length    |  Authenticator
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Extension

32 Mobile-Home
33 Mobile-Foreign
34 Foreign-Home

Length — The number of data bytes in the Extension (16 when MD5 is used).

Authenticator — Variable length (128 bits for MD5).

For Mobile-Home authentication, the value differs depending on the direction the message is sent. These calculations are defined in the Registration Request and Reply messages.

For Mobile-Foreign and Foreign-Home authentication, a hash value taken over a stream of bytes consisting of the shared secret, followed by (concatenated with) the Source, the Destination, the remaining fields in the message beginning with the UDP header, including all prior extensions, and the Type and Length of this extension, but not including the Authenticator field itself, and finally the shared secret again.

5. Forwarding Datagrams to the Mobile Node

5.1. CLNP in CLNP Encapsulation

Support for CLNP in CLNP encapsulated tunneling is required.

The format of the CLNP header is as described in [ISO8473]. The outer CLNP header Source and Destination addresses identify the "end-points" of the tunnel. The inner CLNP header Source and Destination addresses identify the sender and recipient of the datagram.

The Destination field in the CLNP header is replaced by the Care-Of-Address of the Mobile Node.

If the encapsulating agent is not the original source of the datagram, the Source field in the CLNP header is replaced by the CLNP address of the encapsulating agent.

When the Home Agent encapsulates the datagram, it sets the CLNP Lifetime (CLNP TTL) field to be the same as the original datagram.

When decapsulating, the outer CLNP TTL minus one is inserted into the inner CLNP TTL. Thus, CLNP hops are counted, but the actual routers interior to the tunnel are not identified.

5.2. Tunneling Management

It is possible that one of the routers along the tunnel interior might encounter an error while processing the datagram, causing it to return a CLNP ER message to the source end of the tunnel. The three types of CLNP errors that can occur in this circumstance are:

- Segmentation needed but not permitted.
- Lifetime expired.
- Destination address unreachable.

Unfortunately, CLNP ER only requires routers to return the CLNP header of the datagram. This is not enough to include the encapsulated header, so it is not generally possible for the Home Agent to immediately reflect the CLNP ER message from the interior of a tunnel back to the source host.

However, by carefully maintaining "soft state" about its tunnels, a Home Agent can return accurate CLNP ER messages in most cases. The

Home Agent SHOULD maintain at least the following soft state information about each tunnel:

- MTU of the tunnel.
- TTL (path length) of the tunnel
- Reachability of the end of the tunnel.

The Home Agent uses the CLNP ER messages it receives from the interior of a tunnel to update the soft state information for that tunnel. When subsequent datagrams arrive that would transit the tunnel, the router checks the soft state for the tunnel. If the datagram would violate the state of the tunnel (such as, the TTL is less than the tunnel TTL) the Home Agent sends a CLNP ER message back to the source, but also forwards the datagram into the tunnel.

Using this technique, the CLNP ER messages sent by Home Agents will not always match up one-to-one with errors encountered within the tunnel, but they will accurately reflect the state of the network.

6. Mobile Node Considerations

A Mobile Node listens for ISH messages at all times that it has a link connection. In this manner, it can learn that its Foreign Agent has changed, or that it has arrived home.

Whenever a Mobile Node changes its point of attachment to the Internet, it must initiate the registration process. If it is away from home, it must register with a Foreign Agent. If it is returning home, it must deregister with its Home Agent.

A Mobile Node will operate without the support of mobility functions when it is at home.

6.1. Configuration and Registration Tables

Each Mobile Node will need:

- Home-Address

- one or more Home Agents

For each pending registration:

- Media Address of Agent

- Care-Of-Address
- TimeStamp used
- LifeTime

For each Mobility Security Association:

- Authentication Type
- Authentication Key

6.2. Registration When Away From Home

A Mobile Node SHOULD re-register with its Foreign Agent(s) before the LifeTime of its registration expires. The Mobile Node MAY re- register with its Foreign Agent(s) at any time. A Mobile Node can ask the Home Agent to terminate forwarding service through a particular Care-Of-Address, by sending a registration with a LifeTime of zero.

6.3. Registration without a Foreign Agent

In cases where a Mobile Node away from home is able to dynamically acquire a transient CLNP address, the Mobile Node can serve without a Foreign Agent, using the transient address as the Care-Of-Address. Thus, the registration function and the tunnel decapsulation function can be co-located in a single node. This eliminates the need to deploy separate entities as Foreign Agents.

The direct registration process involves the exchange of only two messages:

a) The Mobile Node sends a Registration Request to the Home Agent, to ask the Home Agent to provide the requested service.

b) The Home Agent sends a Registration Reply to the Mobile Node to grant or deny service.

All communication between the Mobile Node and its Home Agent is direct, and there is no need to use the Agent Solicitation, Agent Advertisement, and Registration Request.

It is assumed that such a Mobile Node has mechanisms to detect changes in its link-layer connectivity, and to initiate acquisition

of a new transient address each time such a change occurs. The mechanisms will be specific to the particular link-layer technology, and are outside the scope of this document.

6.4. De-registration When At Home

At times, a Mobile Node will attach itself to its home link. Since a Mobile Node that is at home needs no forwarding, a de-registration procedure MAY be used between the Mobile Node and its Home Agent.

The de-registration process involves the exchange of only two messages:

a) The Mobile Node sends a Registration Request directly to its Home Agent, with the LifeTime set to zero, and the Code field set to 0, to indicate that the Home Agent remove all related entries.

b) The Home Agent sends a Registration Reply to the Mobile Node to grant or deny service.

In this special case, for Authenticator calculation, the Care-Of-Address is set to the Home-Address.

This procedure is specified for the sake of convenience. The Mobile Node is not required to register with its Home Agent. It MAY de-register with each Foreign Agent, or it MAY allow its Mobility Bindings to simply expire.

It is not necessary to re-register with a Home Agent when a change of Incarnation Number occurs, or the Advertisement LifeTime expires, since the Mobile Node is not seeking tunneling service.

6.5. Registration Replies

When a Mobile Node receives a Registration Reply which has a TimeStamp which is not the same as the TimeStamp of its most recent Registration Request to the putative sender, the message is silently discarded.

When a Reply is received which has a Code indicating information from the Foreign Agent, the Mobile-Home Authenticator will be missing or invalid. However, if no other reply has as yet been received, the reason for denial SHOULD be accepted, and result in an appropriate

action. If a later authenticated reply is received, that reply supercedes the unauthenticated reply.

When a Reply is received which has a Code indicating that authentication failed with the Home Agent, the reason for denial SHOULD result in an appropriate action.

Otherwise, when a Reply is received with an invalid Authenticator, the message is silently discarded.

When the LifeTime of the reply is greater than the original request, the excess time SHOULD be ignored. When the LifeTime of the reply is smaller than the original request, re-registration SHOULD occur before the LifeTime expires.

The Mobile Node is not required to issue any message in reply to a Registration Reply.

6.6. Simultaneous Registrations

Under normal circumstances, sending a new Registration Request removes other unexpired registrations for a Mobile Node from the Home Agent.

An optional capability is to allow multiple simultaneous registrations. For example, this is particularly useful when a Mobile Node is on a border between multiple cellular systems.

In order to request simultaneous registrations, the Mobile Node sends the Registration Request with a Code set to 1.

The return Code in the Registration Reply is the same. No error occurs if the Home Agent is unable to fulfill the request.

IP explicitly allows duplication of datagrams. When the Home Agent is able to fulfill the request, the Home Agent will encapsulate a copy of each arriving datagram to each Care-Of-Address, and the Mobile Node will receive multiple copies of its datagrams.

7. Foreign Agent Considerations

It is the intent that Foreign Agent involvement be as minimal as possible. The role of the Foreign Agent is passive, passing registration requests to the Home Agent, and decapsulating tunneled datagrams

to pass to the Mobile Node.

When no Mobility Security Association exists, this also reduces the risks resulting from absence of authentication from Foreign Agent messages.

The Foreign Agent MUST NOT originate a Request or Reply that has not been prompted by the Mobile Node. No Request or Reply is generated to indicate that the service LifeTime has expired.

A Foreign Agent MUST NOT originate a message which revokes the registration of a different Foreign Agent. A Foreign Agent SHOULD forward such revocations without modification when such revocation messages originated from an appropriate Mobile Node or Home Agent.

7.1. Configuration and Registration Tables

Each Foreign Agent will need:

- Care-Of-Address

For each pending or current registration, the Foreign Agent will need a Visitor List:

- Media Address (aka SNPA) of Mobile

- Home-Address

- Home Agent

- LifeTime

A Foreign Agent that has implemented and is using authentication will also need to have the Mobility Security Association information for each pending or current authenticated registration. Even if a Foreign Agent implements authentication, it might not use authentication with each registration, because of the key management difficulties.

7.2. Receiving Registration Requests

Upon receipt of a Registration Request, the Foreign Agent may:

- immediately deny service to the Mobile Node, by sending a

Registration Reply with the appropriate Code set.

- request permission from the Home Agent to provide service to the Mobile Node, by sending a Registration Request.

If the Foreign Agent is unable to satisfy the request for some reason, such as the Mobile Node proposes a Lifetime longer than the Foreign Agent has advertised, then the Foreign Agent sends a Registration Reply with an appropriate Code, and does not forward the request to the Home Agent.

The Foreign Agent must maintain a list of pending Requests, which includes the Source NSAP Address and UDP Source Port, in order that the Reply can be returned to the Mobile Node.

7.3. Receiving Registration Replies

A Registration Reply which does not relate to a pending Registration Request, or to a currently registered Mobile Node, is silently discarded.

If the Registration Reply granted permission to provide service to the Mobile Node, then the Foreign Agent updates its Visitor List accordingly.

8. Home Agent Considerations

It is the intent that the Home Agent have primary responsibility for processing and coordinating services.

The Home Agent for a given Mobile Node SHOULD be located on the link identified by the Home-Address. This link MAY be virtual.

8.1. Configuration and Registration Tables

Each Home Agent will need:

- an NSAP Address

For each authorized Mobile Node, the Home Agent will need:

- Home-Address assigned to that Node

For each registered Mobile Node, the Home Agent will need a Forwarding List:

- Home-Address

- Care-Of-Address

- LifeTime

For each Mobility Security Association:

- Authentication Type

- Authentication Key

8.2. Receiving Requests from the Foreign Agent

Upon receipt of a Registration Request from the Foreign Agent, the Home Agent grants or denies the service requested by sending a Registration Reply to the sender of the request, with the appropriate Code set.

When a Registration Request has an invalid Authenticator for the Mobile Node, a Reply is sent to the Foreign Agent, in order that the Foreign Agent can clear its pending request list.

If permission is granted for the Foreign Agent to provide service to the Mobile Node, the Home Agent will update its Forwarding List with the Home-Address of the Mobile Node, and the Care-Of-Address of the tunnel.

The Home Agent MAY shorten the LifeTime of the request.

If the Request asks for termination of service by indicating a LifeTime of zero, the Home Agent removes the Mobility Binding for that Care-Of-Address from its Forwarding List.

8.3. Receiving Requests from the Mobile Node

Upon receipt of a Registration Request from the Mobile Node, the Home Agent grants or denies the service requested by sending a Registration Reply to the sender of the request, with the appropriate Code set.

In this special case, for Authenticator calculation, the Care-Of-Address is a copy of the Home-Address.

The Home Agent MAY shorten the LifeTime of the request.

If the Request asks for termination of service by indicating a Life-Time of zero, and the Code field set to 0, the Home Agent removes the Mobility Bindings for all Foreign Agents associated with that Mobile Node from its Forwarding List.

No special Reply is sent to associated Foreign Agents. The entries in their Visiting Lists are allowed to expire naturally.

8.4. Simultaneous Registrations

When a Home Agent supports the optional capability of multiple simultaneous registrations, any datagrams forwarded are simply duplicated, and a copy is sent to each Care-Of-Address.

The return Code in the Registration Reply is the same. No error occurs if the Home Agent is unable to fulfill the request, and earlier entries in the Forwarding List are removed.

8.5. Registration Expiration

If the LifeTime for a given Mobile Node expires before the Home Agent has received a re-registration request, then the associated Mobility Binding is erased from the Forwarding List.

No special Registration Reply is sent to the Foreign Agents. The entries in the Visiting Lists will expire naturally, and probably at the same time.

Appendix A. TCP Timers

Most hosts and routers which implement TCP/IP do not permit easy configuration of the TCP Timer values. When high-delay (e.g. SATCOM) or low-bandwidth (e.g. High-Frequency Radio) links are in use, the default TCP Timer values in many systems will cause retransmissions or timeouts when the link and network is actually operating properly, though with greater than usual delays because of the media in use. This can cause an inability to create or maintain connections over

such links, and can also cause unneeded retransmissions which consume already scarce bandwidth. Vendors are encouraged to make TCP Timers more configurable. Vendors of systems designed for the mobile computing markets should pick default timer values more suited to low-bandwidth, high-delay links. Users of Mobile Nodes should be sensitive to the possibility of timer-related difficulties.

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.

The registration protocol described here will result in a host's traffic being source routed to its mobile location. Such traffic redirection could be a significant vulnerability when the registration were not authentic. Also, source routing is widely understood to be a security problem in the current Internet. [Bellovin89].

This specification includes a strong authentication mechanism (keyed MD5) which precludes many potential attacks based on the Mobile TUBA registration protocol. However, because key distribution is difficult in the absence of a network key management protocol, not all messages with the Foreign Agent are authenticated. Vulnerabilities remain in the registration protocol whenever a registration message is not authenticated. For example, 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 don't provide service to users that are not legitimate customers of that service provider.

The strength of any authentication mechanism is dependent 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 authorised parties) and pseudo-random. RFC-XXXX provides more information on generating pseudo-random numbers.

Users who have sensitive data that they do not wish others to see should use mechanisms outside the scope of this specification (such

as encryption) to provide appropriate protection. Users concerned about traffic analysis should consider appropriate use of link encryption.

References

[Voydock83] "V.L. Voydock & S.T. Kent, "Security Mechanisms in High-level Networks", ACM Computing Surveys, Vol. 15, No. 2, June 1983."

[Bellovin89] Steven M. Bellovin, "Security Problems in the TCP/IP Protocol Suite", ACM Computer Communications Review, Vol. 19, No. 2, March 1989."

[ISO9542] ISO9542 "End System to Intermediate System Routeing Exchange protocol for use in conjuction with the Protocol for providing the connectionless-mode network service (ISO8473)"

[ISO8473] ISO8473 "Protocol for providing the connectionless-mode network service"

[Glenn] Glenn, K., R., "Intergrated Network Layer Security Protocol for TUBA", draft-ietf-tuba-inlsp-00.txt (work in progress)