Network Working Group
Internet Draft
expires in six months

W A Simpson
Daydreamer
November 1994

IPv6 Mobility Support
draft-simpson-ipv6-mobility-00.txt

Status of this Memo

This document is a submission to the IPv6 Working Group of the Internet Engineering Task Force (IETF). Comments should be submitted to the ipng@sunroof.eng.sun.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 not appropriate to use Internet Drafts as reference material, or to cite them other than as a ``working draft'' or ``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 ds.internic.net (US East Coast), nic.nordu.net (Europe), ftp.isi.edu (US West Coast), or munnari.oz.au (Pacific Rim).

Abstract

This document specifies protocol enhancements that allow transparent routing of IPv6 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 a Home Agent. The Home Agent sends traffic destined for the Mobile Node through a tunnel to the Care-Of-Address.

1. Introduction

The following actors participate in roaming on the Internet:

Mobile Node

A host or router that changes its point of attachment from one link to another.

Home Agent

A router that advertises reachability for a Mobile Node, maintains a registry of the current point of attachment of that Mobile Node, and encapsulates datagrams for delivery to the Mobile Node while it is away from home.

Foreign Agent

A router that assists a locally reachable Mobile Node while it is away from home.

The following support services are needed:

Agent Discovery

All Agents advertise their availability on each link for which they provide service. Since all agents are routers, this is provided by the Router Advertisement.

A Mobile Node which changes its point of attachment can send a Router Solicitation to learn if any routers are present.

Care-Of-Address Assignment

The Care-Of-Address identifies the point of attachment of a Mobile Node. Depending on the foreign network configuration, the Care-Of-Address may be either 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 a 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, 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.

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 of attachment.

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

A Mobile Node shall provide authentication in its registration messages.

1.2. Goals

The Mobile Node's directly attached link is likely to be bandwidth limited. Few administrative messages are sent between a Mobile Node and an Agent. The size of these messages are kept as short as possible.

As few messages as possible which duplicate functionality are sent on mobile links. This is particularly important on low bandwidth and congested links.

1.3. Assumptions

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

Mobile Nodes are able to change their point of attachment to the Internet no more frequently than once per 4 seconds, which is also the default frequency of advertisements [D-Send].

Changes in topology which occur more frequently must be handled at the link layer transparently to the internetwork layer. It is further noted that engineering margins may require the link layer to handle all changes at a frequency in the neighborhood of 10 seconds.

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 Internet datagrams are routed to a Destination without regard to the Source of the datagram.

If desired, the Mobile Node can create tunnel(s) to its Home Agent. Such mechanisms are beyond the scope of this document.

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
A peer with which a Mobile Node is communicating. The Correspondent may be either mobile or stationary.

Home-Address
A long-term Internet Address that is assigned to a Mobile Node. It remains unchanged regardless of where the node is attached to the Internet. Datagrams addressed to the Home-Address are 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.

Routing Prefix
The high-order bits in an address, which are used by routers to locate a link for delivery of a datagram.

Mobility Security Association

The security relationship between two nodes that is used with Mobile Registration 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 forwarded by the Home Agent.

2. Agent Discovery

To communicate with a Foreign or Home Agent, a Mobile Node must learn either the Internet Address or the link 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. Recommended link-layer facilities are described in the Appendices.

After establishing a link-layer connection that supports the attachment of Mobile Nodes, the node learns whether there are any Agents available. If the Home Agent is recognized, the Mobile Node is at home.

All Agents MUST implement Router Advertisements [D-Send]. The Router Advertisements indicate whether the router is also an Agent.

When multiple methods of Agent identification are in use, the Mobile Node SHOULD first attempt registration with routers sending Router Advertisements 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 the IPv6 Authentication Header [IPv6-AH].

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

There is the potential for a key management problem:

- if the Mobile Node doesn't know the authentication type and key used by the advertiser.

- if the Foreign Agent doesn't know the authentication type and key used by the Mobile Host.

This key management issue is simplified when asymmetric authentication algorithms are used, because each node's public authentication key can published without enabling masquerading attacks. However, asymmetric algorithms are often more computationally intensive than symmetric algorithms.

2.2. Agent Solicitation

Every Mobile Node is required to implement IPv6 Router Solicitation [D-Send].

However, the Router Solicitation is only sent when no Care-Of-Address has been determined through a link-layer protocol or prior Router Advertisement.

All Foreign Agents and Home Agents MUST respond to Router Solicitations.

The same procedures, defaults, and constants are used as described in [D-Send].

2.3. Agent Advertisement

Every Mobile Node is required to correctly process IPv6 Router Advertisements.

All Foreign Agents and Home Agents MUST implement IPv6 Router Advertisements.

When an Agent is identified by a link-layer protocol, the Router Advertisements need not be sent, except when the site policy requires registration with the Agent, or as a response to a specific Router Solicitation.

The same procedures, defaults, and constants are used as described in [D-Send], except as specified herein.

The Mobility Extension is required, and indicates that the router is an Agent. Other extensions indicate optionally supported features.

The Mobile Node examines the Router Advertisement. If any Routing-Information extension exactly matches a Home Agent in its list, the Mobile Node is at home.

Otherwise, the Care-Of-Address is chosen from among advertising Agents in the same fashion as the Mobile Node would choose a first hop router.

If a Cluster-prefix exactly matches the Home-Address prefix extracted by the same Prefix-Size, then that router is one of the preferred routers for that Home-Address. The Mobile Node selects the highest preference such IPv6 Cluster for the Care-Of-Address.

It is very likely that no Cluster-prefix matches when the Mobile Node is not at home. In this case, the highest preference non-matching Router Identifying-Address and Prefix-Size is used to calculate the IPv6 Cluster-Address to be used for the Care-Of-Address.

A Home Agent which does not provide Foreign Agent services will have preference values less than the highest Foreign Agent preference.

3. Registration

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

3.1. Direct

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

a) The Mobile Node sends a Registration Request to a Home Agent, to ask that 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.

This method may also be less desirable when the link is low bandwidth. The encapsulation will not be removed on the final hop.

3.2. Relayed

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. This 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 that 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.

3.3. Authentication

Each Mobile Node, Foreign Agent, and Home Agent MUST support an internal table holding a list of Internet 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.

Mobile-Foreign and Foreign-Home Authentication use the IPv6 Authentication Header [IPv6-AP].

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.

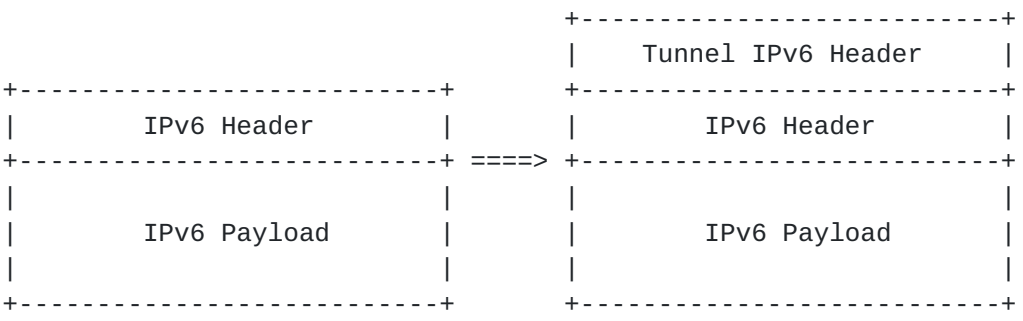
3.4. ICMP Message Formats

The Packet format and basic facilities are already defined for ICMP as modified for IPv6 [IPv6-ICMP].

The Mobility Registration and Reply message formats are documented in [D-Form].

4. Forwarding Datagrams to the Mobile Node

Support for IPv6 in IPv6 encapsulated datagrams is required.



The format of the IPv6 Header is described in [IPv6-Base]. The outer IPv6 Source and Destination identify the "endpoints" of the tunnel. The inner IPv6 Source and Destination identify the sender and recipient of the datagram.

The Protocol field in the outer IPv6 header is set to Payload number 41 for the direct IPv6 encapsulation.

The outer IPv6 Header Destination is set to the Care-Of-Address of the Mobile Node.

The outer IPv6 Header Source is set to the Internet Address of the encapsulating agent.

When the datagram is encapsulated, the outer IPv6 Header Hop Count field is set to be the same as the original datagram.

When decapsulating, the outer Hop Count minus one is inserted into the inner Hop Count.

4.1. Tunnel 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 an ICMP error message to the source end of the tunnel. The three types of ICMP errors that can occur in this circumstance are:

- Datagram too big.
- Time Exceeded.
- Destination Unreachable.

Unfortunately, IPv6 ICMP only requires routers to return 8 bytes (64

bits) of the datagram beyond the IPv6 header. This is not enough to include the encapsulated header, so it is not generally possible for the Home Agent to immediately reflect the ICMP message from the interior of a tunnel back to the source host.

However, by carefully maintaining "soft state" about its tunnels, the encapsulating router can return accurate ICMP messages in most cases. The router 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 router uses the ICMP 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 router sends an ICMP error message back to the source, but also forwards the datagram into the tunnel.

Using this technique, the ICMP error messages sent by encapsulating routers will not always match up one-to-one with errors encountered within the tunnel, but they will accurately reflect the state of the network.

The Don't Fragment bit is always set within the tunnel. This enables the proper MTU of the tunnel to be determined.

Fragmentation which occurs because of the size of the encapsulation header is done before encapsulation, preventing more than one layer of fragmentation in a single datagram.

5. Mobile Node Considerations

A Mobile Node listens for Agent Advertisements 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. The determination that the point of attachment is at home or away from home is entirely at the discretion of the Mobile Node, based on the information obtained from Agent Advertisements.

Whenever a Mobile Node detects a change in its point of attachment, it MUST initiate the registration process. If it is away from home, it MUST either register through a Foreign Agent where required, or directly with a Home Agent. If it is returning home, it MUST de-register with its Home Agent.

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

The Mobile Node primarily uses link-layer mechanisms to decide that its point of attachment has changed. Such indications include the Down/Testing/Up interface status [RFC-1573], and changes in cell or administration. The mechanisms will be specific to the particular link-layer technology, and are beyond the scope of this document.

In the absence of link-layer indications of changes in point of attachment, Agent Advertisements from new Agents do not affect a current registration. A Mobile Node which has already registered MUST NOT register with a different Agent until:

a) transport-layer protocols indicate excessive re-transmissions.

b) the current Registration LifeTime has expired.

The Mobile Node MUST NOT register with a new Agent simply because a higher preference Agent has appeared, or the preference values change for the Agent with which it is currently registered. The preference value is used only for initial selection of an Agent.

Receipt of a Local Redirect from a registered Agent MUST NOT affect the choice of Agent for re-registrations. Local Redirect only affects the choice of preferred router for forwarding decisions.

5.1. Configuration and Registration Tables

Each Mobile Node will need:

- Home-Address
- Prefix-Size
- one or more Home Agents

For each pending registration:

- Media Address of Agent
- Care-Of-Address
- Identification used
- LifeTime

For each Mobility Security Association:

- Authentication Type
- Authentication Key

5.2. Registration When Away From Home

If a Mobile Node detects a reduction in the Sequence Number of an Agent Advertisement from a Foreign Agent through which it has registered, the Mobile Node SHOULD re-register. Such a reduction does not include the wrap of the Sequence Number to zero.

The LifeTime of the registration SHOULD NOT be set to greater than the LifeTime learned in an Agent Advertisement. When the method by which the Care-Of-Address is learned does not include a LifeTime, the default Router Advertisement LifeTime (1800 seconds) is used.

The LifeTime MAY be modified by the Home Agent in its reply.

A Mobile Node SHOULD re-register before the LifeTime of its registration expires. The Mobile Node MAY re-register at any time.

A Mobile Node MAY ask a Home Agent to terminate forwarding service to a particular Care-Of-Address, by sending a registration with a LifeTime of zero.

5.3. Registration without a Foreign Agent

In cases where a Mobile Node away from home is able to dynamically acquire a transient Internet Address, the Mobile Node can serve without a Foreign Agent, using the transient address as the Care-Of-Address.

This feature MUST NOT be used unless the 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.

In these cases, all communication between the Mobile Node and its Home Agent is direct. This eliminates the need to deploy separate entities as Foreign Agents.

The LifeTime of such a registration is chosen by the Mobile Node. By default, the Router Advertisement LifeTime (1800 seconds) is used.

The LifeTime MAY be modified by the Home Agent in its reply.

However, on those links where the Mobile Node detects an Agent Advertisement that has the "F" bit set in the Mobility Extension, the Mobile Node SHOULD register through an appropriate Foreign Agent, even when it could otherwise register directly with a Home Agent.

5.4. De-registration When At Home

At times, a Mobile Node might attach itself to its home link. Since a Mobile Node that is at home needs no forwarding, a de-registration procedure MUST 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, 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 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 Sequence Number occurs, or the Advertisement LifeTime expires, since the Mobile Node is not seeking encapsulating service.

5.5. Registration Replies

When a Mobile Node receives a Registration Reply which has an Identification which is not the same as the Identification 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.

5.6. Registration Retransmission

When no Reply has been received within a reasonable time, the Registration Request is re-transmitted. A new Identification is chosen for each retransmission.

The preferred technique is to re-register each time a new Agent Advertisement is received. By default, the advertisements occur at 1/3 the LifeTime. This gives sufficient protection from missed advertisements, or lost registration requests and replies.

The minimum retransmission time SHOULD be related to the speed of the link. The minimum value SHOULD be large enough to account for the size of the packets, twice the round trip time for transmission at the link speed, and at least an additional 100 milliseconds to allow for processing the packets before responding. Some circuits add another 200 milliseconds of satellite delay.

The initial time MUST NOT be less than 1 second. At 9,600 bps or less, the recommended initial time is 3 seconds. At 1,200 bps or less, the recommended initial time is 5 seconds.

Each successive value less than the maximum value SHOULD be at least twice the previous value.

The maximum retransmission time SHOULD be no greater than the LifeTime of the Registration Request.

5.7. 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 the 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.

IPv6 explicitly allows duplication of datagrams. When the Home Agent is able to fulfill the request, the Home Agent will encapsulate a separate copy of each arriving datagram to each Care-Of-Address, and the Mobile Node will receive multiple copies of its datagrams.

When the need for multiple registrations has passed, the Mobile Node SHOULD re-register with the Code set to 0, to remove the other registrations.

5.8. Mobile Routers

A Mobile Node can be a router, which is responsible for the mobility of an entire network moving together, such as on an airplane, a ship, a train, an automobile, a bicycle, or a kayak.

Provision for a Routing-Prefix in registration messages is needed when a Mobile Node registers through a Foreign Agent. This allows a Foreign Agent to recognize all addresses attached to the Mobile Node

when they are decapsulated at the Care-Of-Address.

When a transient Internet Address has been assigned, the Mobile Node can register directly with the Home Agent, as described previously. Such a Mobile Node MAY advertise to other routers in the foreign routing domain.

The Mobile Node MAY register multiple times with different Home-Addresses and Routing-Prefixes. This permits multiple prefixes to be routed through the Mobile Node.

When the Mobile Node returns home, and de-registers with the Home Agent, it participates directly in routing with other routers in its home routing domain.

6. 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 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.

The Foreign Agent SHOULD NOT advertise the presence of the Mobile Node which is a router to other routers in its routing domain.

The Agent Advertisement preference is used to regulate the number of Mobile Nodes which register with the Foreign Agent. When the Foreign Agent would otherwise need to reject new registrations because of insufficient resources, the Foreign Agent SHOULD reduce its preference values until resources become available.

6.1. 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 entry:

- Media Address of Mobile
- Home-Address
- Prefix-Size
- Home Agent
- Identification used
- 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.

6.2. Receiving Registration Requests

Upon receipt of a Registration Request, if the Foreign Agent is unable to satisfy the request for some reason, then the Foreign Agent sends a Registration Reply to the Mobile Node with an appropriate Code, and does not forward the Request to the Home Agent. Otherwise, the Foreign Agent will forward the Request to the Home Agent.

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

6.3. Receiving Registration Replies

The fields of the Registration Reply MUST be examined for validity. 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.

6.4. Decapsulation

Every Foreign Agent MUST examine all arriving encapsulated traffic for both the Home-Address and Routing-Prefix in order to forward to the correct Mobile Node.

When the Destination does not match any node currently in the Visitor List, the datagram MUST be silently discarded (rather than being further forwarded). IPv6 Destination Unreachable MUST NOT be sent when a Foreign Agent is unable to forward a datagram.

6.5. Mobility

The Foreign Agent can be mobile, if the link identified by the Care-Of-Address is mobile. The Foreign Agent could be either a node on a mobile network, or another Mobile Node itself.

7. Home Agent Considerations

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

The Home Agent SHOULD advertise the presence of the Mobile Node which is a router to other routers in its routing domain.

7.1. Configuration and Registration Tables

Each Home Agent will need:

- an IPv6 Address
- Prefix-Size for the Home Network, if any

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

- Home-Address
- Prefix-Size for the Mobile Network, if any

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

- Care-Of-Address
- Identification used
- LifeTime

For each Mobility Security Association:

- Authentication Type
- Authentication Key

7.2. Receiving Registration Requests

Upon receipt of a Registration Request, 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.

The Request is validated by checking that the Identification is not the same as a preceeding Request, and the Mobile-Home Authentation Extension is correct. Other Authentication Extensions are also validated when present.

The Home Agent MAY shorten the LifeTime of the request.

If service permission is granted, the Home Agent will update its Forwarding List with the Care-Of-Address of the tunnel.

If the Request asks for termination of service by indicating a LifeTime of zero, and the Code field set to 1, the Home Agent removes the Mobility Binding for that Care-Of-Address from its Forwarding List.

If the Request asks for termination of service by indicating a LifeTime 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.

On termination, no special Reply is sent to additional associated Foreign Agents. The entries in their Visiting Lists are allowed to expire naturally.

7.3. Receiving Requests through a Foreign Agent

When a Registration Request is invalid, a Reply is sent to the Foreign Agent, in order that the Foreign Agent can clear its pending request list.

7.4. 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.

7.5. 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.

7.6. Encapsulation

Every Home Agent MUST examine all arriving traffic for both the Home-Address and Routing-Prefix in order to forward to the correct Mobile Node.

When previously encapsulated datagrams arrive which are associated with the Routing-Prefix of the Mobile Node, the Home Agent simply alters the Destination to the Care-Of-Address. This avoids recursive encapsulation.

Previously encapsulated datagrams which are not associated with the Routing-Prefix are recursively encapsulated.

7.7. Mobility

The Home Agent can be mobile, if the link identified by the Home-Address it serves is mobile. The Home Agent could be either a node on a mobile network, or another Mobile Node itself.

A datagram would be encapsulated on its way to the mobile network, decapsulated for delivery to the Mobile Node, intercepted by the Home Agent, and re-encapsulated to the Mobile Node.

A. Point-to-Point Link-Layers

The Point-to-Point-Protocol (PPP) [RFC-1548] Internet Protocol Control Protocol (IPCP) [RFC-1332], does not yet negotiate the use of IPv6 addresses.

Instead, IPv6 Neighbor Discovery [D-Send] is used to exchange identities with the peer. IPv6 Router Advertisements indicate whether the router is also an Agent.

When a transient IPv6 Unicast Address is dynamically assigned, that address MAY be used as the Care-Of-Address in registration.

B. Multi-Point Link-Layers

Another link establishment protocol, IEEE 802.11, might yield the link address of an Agent. This link-layer address SHOULD be used to attempt registration.

The receipt of a Router Advertisement supercedes the link-layer address, and a new registration MUST occur.

C. 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] The Address Resolution Protocol (ARP) is not authenticated, and can potentially be used to steal another host's traffic.

This specification includes a strong authentication mechanism (keyed MD5) which precludes many potential attacks based on the Mobile IP registration protocol. However, because key distribution is difficult in the absence of a network key management protocol, 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. [Eastlake] provides more information on generating pseudo-random numbers.

Users who have sensitive data that they do not wish others to see should use mechanisms (such as encryption) to provide appropriate protection. Users concerned about traffic analysis should consider appropriate use of link encryption.

References

[Atkinson] Atkinson, R., "Authentication Header", work in progress.

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

[Eastlake] Eastlake, D.E.3, S.D. Crocker, J.I. Schiller, "Randomness Requirements for Security", work in progress.

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

[RFC-768]

[RFC-791]

[RFC-826]

[RFC-1122]

[RFC-1144]

[RFC-1256]

[RFC-1310]

[RFC-1305]

[RFC-1321]

[RFC-1332]

[RFC-1573]

[RFC-1661]

Acknowledgements

Special thanks to John Ioannidis (Columbia University), for his inspiration and experimentation which began this most recent round of IP mobility development.

Special thanks also to Steve Deering (Xerox PARC), for his early support as Chair of the Simple-IP and Mobile-IP Working Groups.

Charlie Perkins (IBM) coalesced the terms of Home and Foreign Agents.

Security details are primarily the work of Randall Atkinson (Naval Research Laboratory).

Tunnel soft state was originally developed for the "IP Address Encapsulation (IPAE)" specification, by Robert E. Gilligan, Erik Nordmark, and Bob Hinden (all of Sun Microsystems).

Much of the text of this specification is derived from earlier drafts by Charlie Kunzinger (IBM), and the verbose members of the Mobile-IP Working Group who contributed text, including Dave Johnson (Carnegie Mellon University), Tony Li (Cisco Systems), Andrew Myles (Macquarie University), John Penners (US West), Fumio Taraoka (Sony), and John Zao (Harvard).

Finally, the Editor wishes to thank Phil Karn (Qualcomm), whose decade of IP mobility experimentation in the amateur radio community, and widespread freeware dissemination of his KA9Q software, provided the impetus and availability for many thousands throughout the world to join the Internet community.

Author's Address

Questions about this memo can also be directed to:

William Allen Simpson
Daydreamer
Computer Systems Consulting Services
1384 Fontaine
Madison Heights, Michigan 48071

Bill.Simpson@um.cc.umich.edu
bsimpson@MorningStar.com

Table of Contents