

IPng Mobility Considerations

Status of this Memo

This memo provides information for the Internet community. This memo does not specify an Internet standard of any kind. Distribution of this memo is unlimited.

Abstract

This document was submitted to the IPng Area in response to RFC 1550. Publication of this document does not imply acceptance by the IPng Area of any ideas expressed within. Comments should be submitted to the big-internet@munari.oz.au mailing list. This RFC specifies criteria related to mobility for consideration in design and selection of the Next Generation of IP.

Table of Contents

1.	Introduction	2
2.	Addressing	2
2.1	Ownership	2
2.2	Topology	3
2.3	Manufacturer	3
2.4	Numbering	3
2.5	Configuration	3
3.	Communication	3
3.1	Topological Changes	4
3.2	Routing Updates	4
3.3	Path Optimization	5
3.4	At Home	5
3.5	Away From Home	5
4.	Security	5
4.1	Authentication	5
4.2	Anonymity	6
4.3	Location Privacy	6
4.4	Content Privacy	6
5.	Bandwidth	6
5.1	Administrative Messages	7
5.2	Response Time	7
5.3	Header Prediction	8
6.	Processing	8
6.1	Fixed Location	8

6.2	Simple Fields	9
6.3	Simple Tests	9
6.4	Type, Length, Value	9
Acknowledgements		9
Security Considerations		9
Author's Address		9

1. Introduction

Current versions of the Internet Protocol make an implicit assumption that a node's point of attachment remains fixed. Datagrams are sent to a node based on the location information contained in the node's IP address.

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

A number of considerations arise for routing these datagrams to a Mobile Node.

2. Addressing

Each Mobile Node must have at least one Home-Address which identifies it to other nodes. This Home-Address must be globally unique.

2.1. Ownership

The presence of ownership information in the Home-Address would be beneficial. A Mobile Node will be assigned a Home-Address by the organization that owns the machine, and will be able to use that Home-Address regardless of the current point of attachment.

The ownership information must be organized in such a fashion to facilitate "inverse" lookup in the Domain Name Service, and other future services.

Ownership information could be used by other nodes to ascertain the current topological location of the Mobile Node.

Ownership information could also be used for generation of accounting records.

2.2. Topology

There is no requirement that the Home-Address contain topological information. Indeed, by the very nature of mobility, any such topological information is irrelevant.

Topological information in the Home-Address must not hinder mobility, whether by prevention of relocation, or by wasting bandwidth or processing efficiency.

2.3. Manufacturer

There is no requirement that the Home-Address contain manufacturer information.

Manufacturer information in the Home-Address must not hinder mobility, whether by prevention of relocation, or by wasting bandwidth or processing efficiency.

2.4. Numbering

The number of mobile nodes is expected to be constrained by the population of users within the lifetime of the IPng protocol. The maximum world-wide sustainable population is estimated as $16e9$, although during the lifetime of IPng the population is not expected to exceed $8e9$.

Each user is assumed to be mobile, and to have a maximum combined personal mobile and home network(s) on the order of $4e3$ nodes.

The expectation is that only 46 bits will be needed to densely number all mobile and home nodes.

The size of addressing elements is also constrained by bandwidth efficiency and processing efficiency, as described later.

2.5. Configuration

Since the typical user would be unlikely to be aware of or willing and able to maintain $4e3$ nodes, the assignment of Home-Addresses must be automatically configurable. Registration of the nodes must be dynamic and transparent to the user, both at home and away from home.

3. Communication

A Mobile Node must continue to be capable of communicating directly with other nodes which do not implement mobility functions.

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.

A Mobile Node using its Home-Address must 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 using its Home-Address must be able to communicate with other nodes while roaming between different points of attachment, without loss of transport connections.

3.1. Topological Changes

In order that transport connections be maintained while roaming, topological changes must not affect transport connections.

For correspondent nodes which do not implement mobility functions, topological changes should not be communicated to the correspondent.

For correspondent nodes which implement mobility functions, the correspondent should be capable of determining topological changes.

Topological change information must be capable of insertion and removal by routers in the datagram path, as well as by the correspondent and Mobile Node.

3.2. Routing Updates

Mobile Nodes are expected to be able to change their point of attachment no more frequently than once per second.

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.

Changes in topology which occur less frequently must be immediately reflected in the mobility updates. This may preclude the use of the Domain Name Service as the repository of mobility topological information.

It must be noted that global routing updates do not operate at this frequency. As old topological information may be obsoleted faster than global routing updates, access to the repository of mobility topological information must be independent of prior topological information.

The mobility specific repository should use ownership information in the Home-Address for access to the repository.

3.3. Path Optimization

Optimization of the path from a correspondent to a mobile node is not required. However, such optimization is desirable.

For correspondent nodes which implement mobility functions, the correspondent should be capable of determining the optimal path.

The optimization mechanism is also constrained by security, bandwidth efficiency and processing efficiency, as described later.

3.4. At Home

Mobile Nodes do not require special "virtual" home network addresses. The assumption that extra addresses or multiple routers are available is unwarranted in small networks.

Mobile Nodes must operate without special assistance from routers in order to communicate directly with other nodes on the home subnetwork link.

3.5. Away From Home

When a router is present, and the correspondent does not implement mobility functions, the router must be capable of redirecting the correspondent to communicate directly with the Mobile Node.

When no router is present, Mobile Nodes must be capable of communicating directly with other nodes on the same link.

Mobility must not create an environment which is less secure than the current Internet.

Changes in topology must not affect internode security mechanisms.

4. Security

4.1. Authentication

Mobility registration messages must be authenticated between the home topological repository and Mobile Node.

When the correspondent implements mobility functions, redirection or path optimization must be authenticated between the correspondent and Mobile Node.

4.2. Anonymity

The capability to attach to a foreign administrative domain without the awareness of the foreign administration is not prohibited. However, any mobility mechanism must provide the ability to prevent such attachment.

4.3. Location Privacy

The capability to attach to a foreign administrative domain without the awareness of correspondents is not prohibited. However, any mobility mechanism must provide the ability for the home administration to trace the current path to the point of attachment.

4.4. Content Privacy

Security mechanisms which provide content privacy must not obscure or have a dependency on the topological location of Mobile Nodes.

5. Bandwidth

Mobility must operate in the current link environment, and must not be dependent on bandwidth improvements. The Mobile Node's directly attached link is likely to be bandwidth limited.

In particular, radio frequency spectrum is already a scarce commodity. Higher bandwidth links are likely to continue to be scarce in the mobile environment.

Current applications of mobility using radio links include HF links which are subject to serious fading and noise constraints, VHF and UHF line of sight radio between ships or field sites, and UHF Satellite Communications links.

The HF radio bandwidth is fixed at 1200 or 2400 bps by international treaty, statute, and custom, and is not likely to change.

The European standard for cellular radio is 2400 bps GSM.

The most prevalent deployed analog cellular and land-line modulation used by mobile nodes is 2400 bps.

Current digital cellular deployment is 19,200 bps CDPD shared among many users. At early installations, under light loads, effective FTP throughput has been observed as low as 200 bps.

Future digital cellular deployment is 9,600 and 14,400 bps CDMA, which is shared between voice and data on a per user basis.

Effective FTP throughput has been measured as low as 7,200 bps.

Future Personal Communications Services (PCS) will also have relatively little bandwidth. In industrialized nations, the bandwidth available to each user is constrained by the density of deployment, and is commensurate with planned digital cellular deployment.

It appears likely that satellite-based PCS will be widely deployed for basic telephony communications in many newly-industrialized and lesser-developed countries. There is already significant PCS interest in East and SouthEast Asia, India, and South America.

Van Jacobson header prediction is widely used, and essential to making the use of such links viable.

5.1. Administrative Messages

The number of administrative mobility messages sent or received by the Mobile Node must be limited to as few as possible. In order to meet the frequency requirement of changing point of attachment once per second, registration of changes must not require more than a single request and reply.

The size of administrative mobility messages must be kept as short as possible. In order to meet the frequency requirement of changing point of attachment once per second, the registration messages must not total more than 120 bytes for a complete transaction, including link and internet headers.

5.2. Response Time

For most mobile links in current use, the typical TCP/IPv4 datagram overhead of 40 bytes is too large to maintain an acceptable typing response of 200 milliseconds round trip time.

Therefore, the criteria for IPng mobility is that the response time not be perceptably worse than IPv4.

This allows no more than 6 bytes of additional overhead per datagram to be added by IPng.

This was a primary concern in the design of mobility forwarding headers. Larger headers were rejected outright, and negotiation is provided for smaller headers than the default method. Topological headers are removed by the Foreign Agent prior to datagram transmission over the slower link to the Mobile Node, which also aids header prediction, as described below.

5.3. Header Prediction

Header prediction can be useful in reducing bandwidth usage on multiple related datagrams. It requires a point-to-point peer relationship between nodes, so that a header history can be maintained between the peers.

Header prediction is less effective in mobile environments, as the header history is lost each time a Mobile Node changes its point of attachment. The new Foreign Agent will not have the same history as the previous Agent.

In order for header prediction to operate successfully, changing topological information must be removed from datagram overhead prior to transmission of the datagram on any final hop's directly attached link. This applies to both the Mobile Node peering with a Foreign Agent, and also the final link to a Correspondent. Otherwise, header prediction cannot be relied upon to improve bandwidth utilization on low-speed Mobile and Correspondent links.

Since the changing topological information cannot be removed in the forwarding path of the datagram, header prediction will also be affected at any other pair of routers in the datagram path. Each time that a Mobile Node moves, the topological portion of the header will change, and header history used at those routers will be updated. Unless topological information is limited to as few headers as possible, this may render header prediction ineffective as more Mobile Nodes are deployed.

6. Processing

Mobility must operate in the current processor environment, and must not be dependent on hardware improvements.

Common hardware implementations of Mobile Nodes include lower speed processors, and highly integrated components. These are not readily upgradable.

The most prevalent mobile platform is a low speed i86, i286 or i386.

The most common ASIC processor is a low speed i186.

6.1. Fixed Location

The processing limitations require that datagram header fields which are frequently examined by Mobile Nodes, or used for datagram forwarding to or from Mobile Nodes, are in a fixed location and do not require lengths and offsets.

Varied number of fields was explicitly rejected in the design of mobility registration and forwarding headers.

6.2. Simple Fields

The processing limitations require that datagram header fields which are frequently examined by Mobile Nodes, or used for datagram forwarding to or from Mobile Nodes, are simple and fixed size.

Varied length of fields was explicitly rejected in the design of mobility forwarding headers.

6.3. Simple Tests

Because the most prevalent processors are "little-endian", while network protocols are in practice "big-endian", the field processing must primarily use simple equality tests, rather than variable shifts and prefix matches.

6.4. Type, Length, Value

Fields which are not frequently examined, whether due to infrequent transmission or content that is not relevant in every message, must be of the Type, Length, Value format.

Acknowledgements

This compilation is primarily based on the work in progress of the IETF Mobile IP Working Group.

Security Considerations

Security issues are discussed in section 4.

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

EMail: Bill.Simpson@um.cc.umich.edu or
bsimpson@MorningStar.com

