Internet Engineering Task Force
INTERNET DRAFT

W. T. Teo
National University
of Singapore
Y. Li
Nortel Networks, Inc.

Mobile IP extension for Private Internets Support (MPN)

Status of This Memo

This document is an Internet-Draft and is in full conformance with all provisions of Section 10 of RFC2026.

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

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

The list of current Internet-Drafts can be accessed at http://www.ietf.org/ietf/1id-abstracts.txt

The list of Internet-Draft Shadow Directories can be accessed at http://www.ietf.org/shadow.html.

Abstract

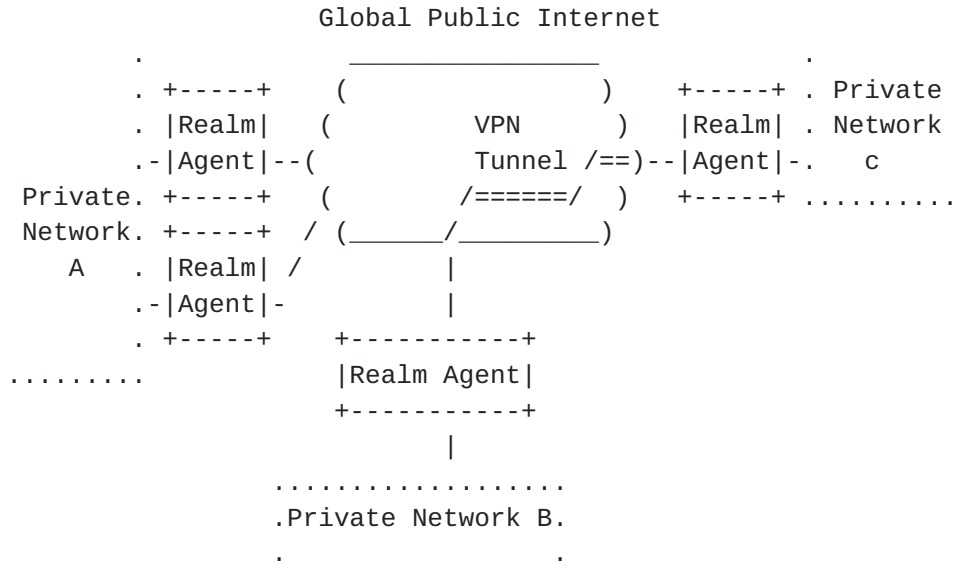
This memo specifies enhancements to Mobile IP that allow IP mobility support across routing realms. The protocol allows a mobile node to have the same home network connectivity, regardless of its current routing realm network point of attachment. It is designed to work in the presence of address collisions and network address translations. Private networks connected to the public Internet can extend IP mobility support to cover the public Internet and other private networks. Movement from a private home network to the public foreign network, from a private home network to another private foreign network or from the public home network to a private foreign network are possible under the MPN framework.

1. Introduction

Mobile IP [1] allows a node to move from its home network, the IP subnet indicated by its home address. When away from the home network, datagrams destined to the node are tunnelled to a care-of address in the visited network. This assumes a node's address is sufficient to identify the node's location in the Internet and IP unicast datagrams can be routed solely based on the destination address in the datagram header. This is only true when the node's mobility is constrained within a common routing realm. For example, this routing realm could be the global public Internet or a localized private network.

These assumptions are not valid beyond the mobile node's routing realm. Therefore, Mobile IP cannot ensure mobility across different routing realms. MPN is an extension to the Mobile IP base protocol that enables this mobility support spanning multiple routing realms.

1.1 MPN Framework



In MPN, the central routing realm is the global public Internet. All other routing realms (private routing realms) depend on this global routing infrastructure for wide area mobility.

Unlike the central routing realm which has numerous public networks, each private network constitutes an independent routing realm. Examples of private networks are intranets, extranets and virtual private networks.

These private routing realms are globally identified in the public Internet by their public agents. Realm agents are the private

networks link to the public Internet. For example, the public agent may be a border router or an Internet service provider network point of presence.

An independent private network (e.g. private network A) may have more than one link to the public Internet, i.e. there are more than one public agents.

A private routing realm may consists of multiple networks physically located in separate sites. For example, private network B and private network C may form a virtual private network. There will be a VPN tunnel established between the two networks, to route traffic between the two different physical sites. This VPN tunnel is transparent in the MPN framework. For such network configurations, in the context of MPN, the networks represent a single private routing realm. There is no cross routing realm movement if a node moves to another physical site within such a network.

All the realm agents in a private routing realm should be advertised in the realm agents advertisement extension [ref Section 3.1]. In MPN, realm agents provide the tunnel routing required by visiting mobile nodes. The realm agents' addresses are also used in the identification of routing realms. Mobile nodes from a private network are configured with the realm agents' addresses in their routing realm. These addresses are used to determine the mobile node's current routing realm.

1.2 Addressing Concerns

IP addresses are topologically significant and unique only within a routing realm. By enabling mobility across multiple routing realms, there may be address collisions due to overlapping address space in the visited routing realm.

MPN is designed to work in the presence address collisions and solve the problem of tunneling across independent routing realms. However, MPN is not intended to provide communication across routing realms [ref Section 1.4]. The determination of the end host and the routing mechanisms for end-to-end communication in the home routing realm is independent of MPN. There are other protocols that provide communication across routing realms such as NAT [6] and PAID [8]. Their operation is transparent to MPN.

1.3 Mobile Node Concerns

When a mobile node enters a foreign routing realm and its visited network link is broadcast-oriented (such as Ethernet), the mobile node MUST use a co-located care-of address, instead of a local

foreign agent care-of address, for reverse GRE tunnels [ref Section 2.2]. This is to avoid address ambiguity on the broadcast link due to home address collisions.

A private mobile node should use a co-located care-of address (if possible) even when the foreign routing realm visited network link is not broadcast-oriented. As the local foreign agent is not the forward or reverse tunnel endpoint, end-to-end encryption can be supported.

1.4 Mobility Support

The mobility support in Mobile IP allows a mobile node to be always identified by its home address, when it roams from its home network. The mobile node's reachability by other nodes and its accessibility to other nodes is not explicit in Mobile IP. This is because a common routing fabric is assumed.

In MPN, mobility support is more accurately defined as maintaining the same home network connectivity. The mobile node should have access to all nodes that is reachable within its home network, even when it migrates into another routing realm. Similarly, all nodes that can reach the mobile node within its home network, should be able to reach the mobile node when it moves to another routing realm (if MPN mobility support is available in the visited network).

1.5 Design Goals

The design goals of MPN are:

1. The MPN protocol shall require minimum changes and support all functions of the Mobile IP base protocol.

2. The MPN protocol must not affect the operation of Mobile IP mobile nodes and mobility agents.

2. The MPN protocol shall be migratory. It will enable the upgrading of a private network in phases while maintaining backward compatibility with a basic MPN deployment.

1.6 Protocol Requirements

No protocol enhancements are required for realm agents in a basic MPN deployment. However, there are security risks involved when permitting unrestricted tunneling into a private network, for a basic MPN deployment. The reverse tunneling is required in MPN to maintain home network connectivity.

1.7 New Architectural Entity

Realm Agent

A router or firewall that connects a private network to the global public Internet [ref Section 1.1]. A realm agent may be located at the private network's border or at the private network's ISP. The realm agent MUST have a public IP address, which is reachable from the global public Internet. All nodes within the private network MUST be able to reach the realm agent using this public IP address. The realm agent MUST be able to route to all local home agents and care-of addresses within the private network.

1.8 Terminology

Unless otherwise specified, the document adopts all the terminology defined in "IP Mobility Support" [1] [2].

This document introduces the following terms:

Private Network

A network separated from the global public Internet with access restrictions. A private network typically assigns nodes private addresses specified in RFC 1918 [9] and the addresses may not be routable by the general public Internet. For this document, private networks only refer to private networks connected to the global public Internet and not physically isolated networks.

Private Mobile Node

A mobile node whose home network is in a Private Network.

Public Mobile Node

A mobile node whose home network is in the global public Internet.

Routing Realm

The global public Internet and each private network constitute individual routing realms [ref Section 1.1] This document operates on the paradigm that interconnecting routing realms may have overlapping address space but within a routing realm, all IP addresses are unique and unicast datagrams are routable solely based on the destination address in the datagram header.

Home Routing Realm

A routing realm which the mobile node's home network is located.

Foreign Routing Realm

Any routing realm other than the mobile node's Home Routing Realm.

Visited Routing Realm

A network other than the mobile node's Home Routing Realm, which the mobile node is currently located.

Passive Realm Agent

A GRE [10] router. In a basic MPN deployment, a passive realm agent route GRE tunnels (where IP is both the delivery and payload protocol). A passive agent is not aware of nodes movement and it need not process MPN registration messages or maintain any mobility binding and security associations. This enables the immediate deployment of realm agents since there are no specific MPN protocol enhancements required.

Active Realm Agent

A GRE router. In addition, an active agent processes and relay MPN registration messages. It MUST maintain mobility bindings of successful registrations and may have security associations. Security policies for visiting mobile nodes may be enforced for the whole network at the active realm agent. An active realm agent may provide routing optimizations and tunnel circuit switching [ref Section 7].

Home Realm Agent

A realm agent in the mobile node's Home Routing Realm. All Private Mobile Nodes MUST be assigned one or more realm home agents. A realm mobile node may be assigned a realm home agent located at its home network domain.

Foreign Realm Agent

Any realm agent other than the mobile node's Home Realm Agent.

Mobility Binding

The association of a home address with a care-of address and any intermediate tunnel destinations (realm home/foreign agent

address), along with the remaining lifetime of that association.

Local Home Agent

A home agent in Mobile IP terminology.

Local Foreign Agent

A foreign agent in Mobile IP terminology.

Mobility Agent

Either a local home agent, local foreign agent or a realm agent.

2. Tunneling

Tunneling is a means to alter the normal IP routing for datagrams, by delivering them to intermediate destinations that would otherwise not be selected by the (network part of the) IP destination address in the original IP header.

2.1 Reverse tunneling

A bidirectional tunnel is established when a mobile node is in a foreign routing realm. In order for the mobile node to have the same level of network connectivity as it does when in its home network, nodes that are reachable only when the mobile node is in the home routing realm or home network, should be accessible in the visited network. Packets destined to a node's address in another routing realm will probably not be delivered using the existing routing mechanism in the visited routing realm. A reverse tunnel [5] is used to deliver datagrams originating from the mobile node back to the home routing realm or home network. This will allow the datagrams to be routed to the correct correspondent nodes in the presence of address collisions and security restrictions. The reverse tunnel exit point need not be the mobile node's local home agent.

2.2 GRE encapsulation

IP in IP encapsulation [3] is the default tunneling mechanism used in Mobile IP. While it is useful for re-routing a datagram from one point to another, the mechanism is unsuitable when multiple transitional points are required, to traverse across different routing realms. To achieve such functionality, the encapsulation method must support source routing or the intermediate destinations must be dynamically configured to forward the datagram to the next

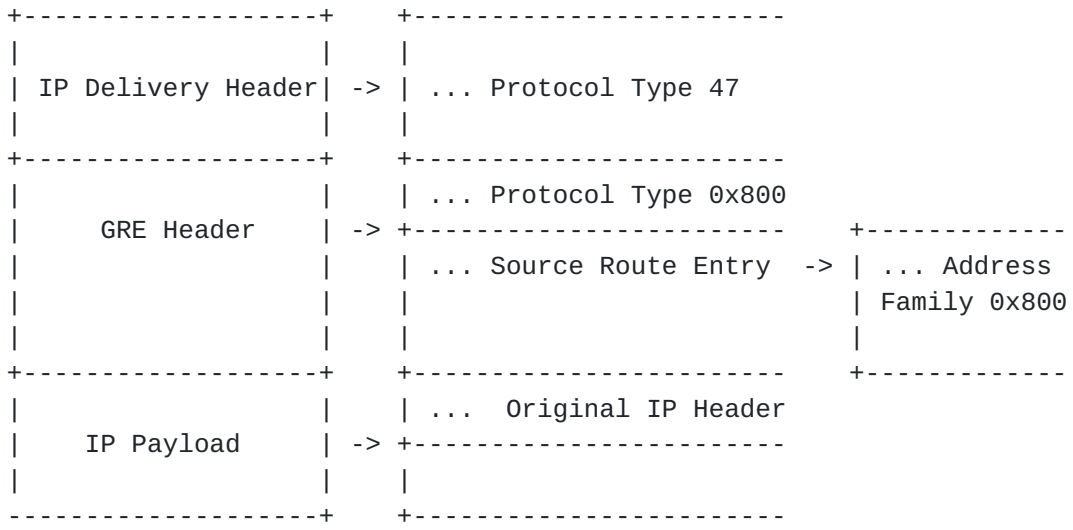
correct tunneling point.

MPN uses Generic Routing Encapsulation [10] as the default encapsulation method to tunnel across different routing realms. GRE provides a Source Route Entry (SRE) in the tunnel header. Using a SRE with an Address Family indicating an IP loose source route (Strict Source Route flag cleared), the intermediate destinations can be specified.

In the case of MPN, the SRE's IP address list will include any realm agent along the tunnel route and the tunnel endpoint. Typically the tunnel endpoint is the local home agent (for a reverse tunnel) or the care-of address (for a forward tunnel).

2.3 Overall Encapsulated Packet

The diagram below provides an overview of the GRE tunnelled packet layout.



2.4 GRE SRE Processing

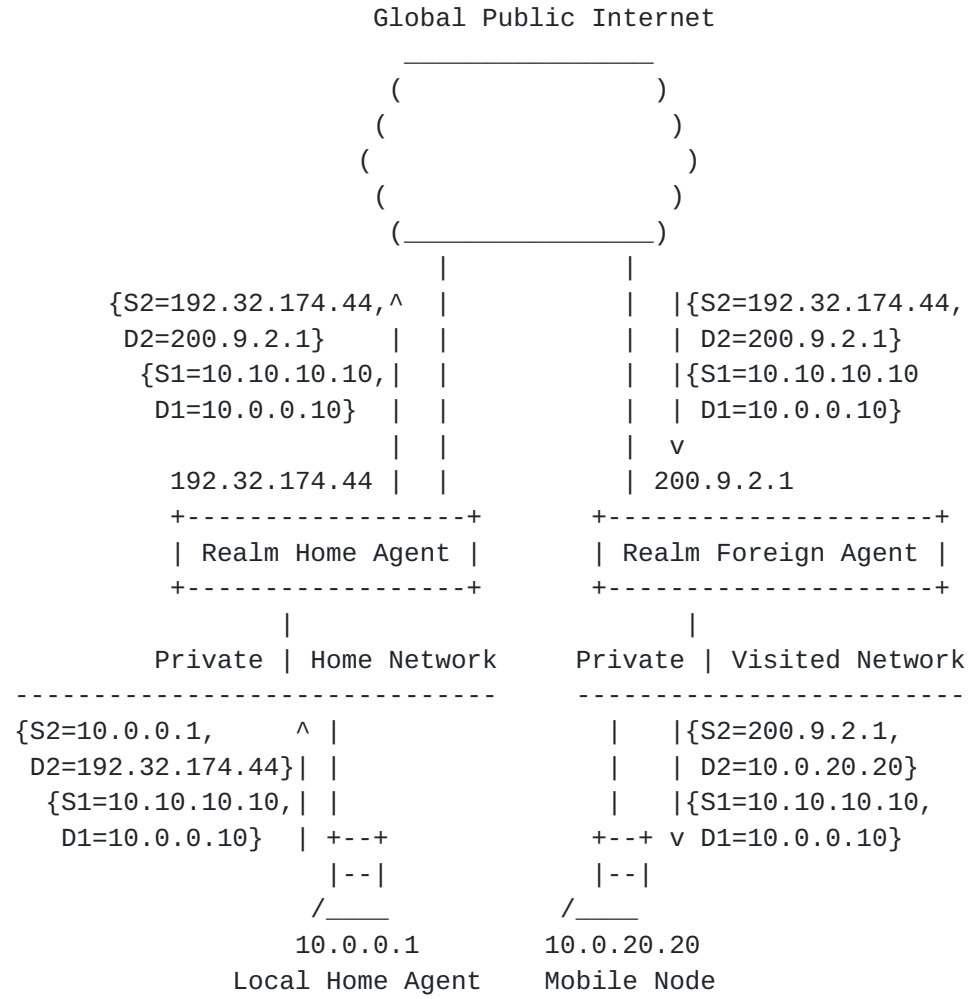
All the intermediate tunnel destinations (the realm agents) MUST process the GRE header as specified in [10, 11]. The local home agent and the mobile node MUST be able to perform GRE encapsulation and decapsulation.

The diagram below illustrates forward GRE tunneling (from the local home agent to the mobile node co-located care-of address) when the mobile node moves from the private home routing realm into a private visted routing realm with overlapping address space. The same route but in reverse is typically taken by the reverse GRE tunnel.

Private Home Routing Realm
---
private home network: 10.0.0.0/8
correspondent node address: 10.10.10.10
MN home address: 10.0.0.10
MN local home agent address: 10.0.0.1
MN realm home agent address: 192.32.174.44

Private Visited Routing Realm
---
private visited network: 10.0.0.0/16
advertised realm foreign agent address: 200.9.2.1
MN co-located care-of address: 10.0.20.20

S1 and D1 represent the original IP header's source and destination addresses respectively. S2 and D2 represent the IP delivery header's source and destination addresses respectively.



2.5 ICMP messages

The realm agents should handle ICMP messages from within the GRE tunnel as specified in [3], including the maintenance of tunnel "soft state".

3. MPN Agent Advertisement

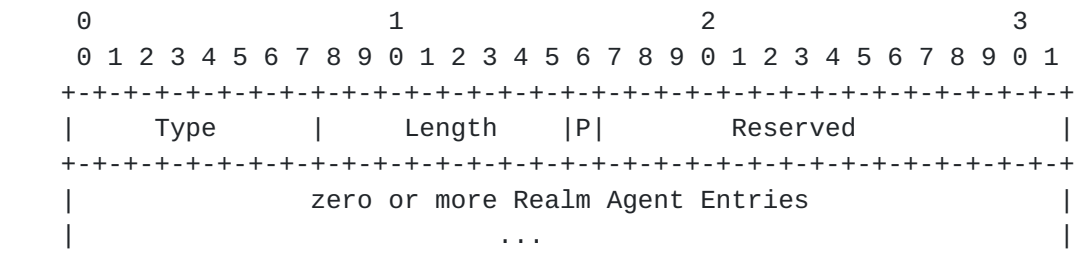
Mobile IP's agent advertisements allow a mobile node to detect movement across IP subnets. MPN includes a realm agent advertisement extension to Mobile IP's agent advertisements. This allows a mobile node to determine its current routing realm.

All MPN extension type values are selected from the range 128 to 255. As specified in Mobile IP, values in this range can be silently ignored by mobile nodes supporting only the Mobile IP based protocol.

3.1 Realm Agent Extension

This extension MUST be included in all local home agents' and local foreign agents' agent advertisements. All realm agents that serve as a realm home agent for any mobile node in the routing realm MUST be included in the list of Realm Agent Entries. The presence of this extension also indicates that the advertiser supports MPN.

The Realm Agent Advertisement Extension is defined as follows:

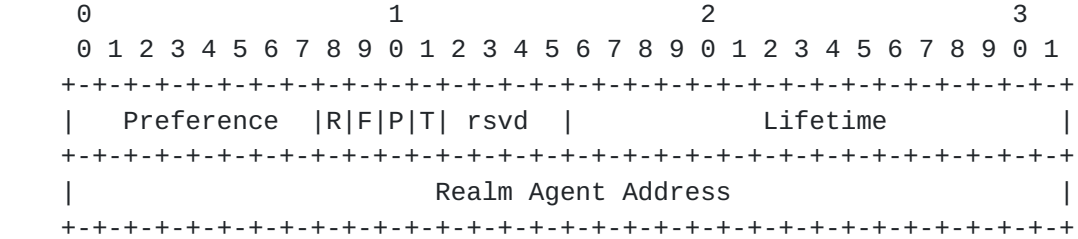


Type 128

Length (2 + 8*N), where N is the number of realm agent entries.

P Public Network. The network is accessible from the global public Internet (not a private network)

The Realm Agent Entry is defined as follows:



Preference	cost indicator. 0 means the realm foreign agent is busy and will not tunnel datagrams for additional mobile nodes.
Lifetime	The longest lifetime (measured in seconds) that this realm foreign agent is willing to accept in any registration request. A value of 0xffff indicates infinity.
R	Registration required. Registration with the realm foreign agent is required. The realm foreign agent will maintain the mobility binding of successful registrations. If the 'R' bit is not set, the Lifetime field is undefined and can be assumed to be infinite. If the 'R' bit is set, the 'P' bit can be assumed to be set.
F	Foreign Realm Agent. This realm agent offers service as a foreign realm agent in this routing realm.
P	Registration Proxy. This realm agent will relay the registration message to the next mobility agent or mobile node (registration reply).
T	Tunnel Circuit Switching. This realm agent supports tunnel circuit switching [ref Section 7].

The Realm Agent Address MUST be a public IP address reachable from the global public Internet.

A realm agent MUST always be prepared to serve the mobile nodes for which it is the realm home agent.

The Realm Agent Advertisement Extension MUST be before the Mobility Agent Advertisement Extension [1].

3.2 Choosing a Realm Agent

Having only one realm agent for a routing realm will be a single point of failure and possible bottleneck device.

The realm agent entries [refer Section 3.1] carry with each realm agent address a preference identifier. To select a realm agent, one has to rely on heuristics approaches. The easiest may be to always choose the "preferred realm foreign agent" - the realm agent entry with the maximum preference value or alternatively chose the realm home/foreign agent randomly. This will spread the tunneled traffic on

different routes and introduce better load sharing and more redundancy to the network.

3.3 Absent Agent Advertisment

Agent advertisements are needed to determine the current routing realm. If there is no agent advertisement detected, a mobile node should send agent solicitations, even when it acquires a co-located care-of address. This is to determine if the mobile node is within its home routing realm.

In the absence of agent advertisements, a mobile node should proceed as if the current routing realm is the global public Internet. This implies, a public mobile node should proceed as specified in Mobile IP, and a private mobile node should proceed as specified in the private home routing realm to public visited routing realm movement scenario [ref Section 6.3].

3.4 Movement Detection

To determine the current routing realm, a mobile node should check the 'P' bit in the Realm Agent Advertisement Extension.

Public Mobile Node

If the 'P' bit is set, the mobile node is in its home routing realm (the global public Internet) and it can proceed as specified in Mobile IP.

If the 'P' bit is not set, the mobile node is in a private routing realm and it should proceed as specified in the public home routing realm to private visited routing realm movement scenario [ref Section 6.1]

Private Mobile Node

If the 'P' bit is set, the mobile node is in the global public Internet and it should proceed as specified in the private home routing realm to public visited routing realm movement scenario [ref Section 6.3]

If the 'P' bit is not set, the mobile node MUST search all the Realm Agent Entries. If one of the realm agent addresses advertised matches the mobile node's assigned realm home agent address, it is in its home routing realm and can proceed as specified in Mobile IP. If there is no matching realm agent address, the mobile node is in a private foreign routing realm and it should proceed as specified in the private home routing realm to private foreign routing realm

movement scenario [ref Section 6.2]

Once the current routing realm is determined, the mobile node can detect movement between IP subnets as specified in Mobile IP.

4. MPN Registration

Registration allows mobile nodes to communicate their current reachability information to the mobility agents. The following sections describes registration across routing realms.

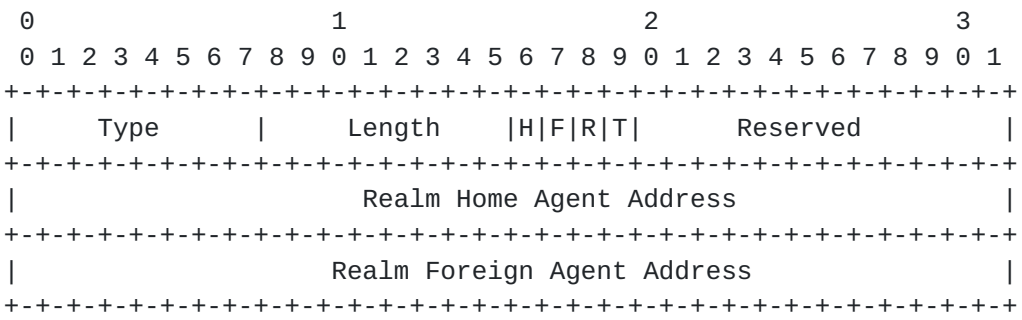
There are two registration procedures. One via the mobility agents that relay the registration to the mobile node's local home agent, and another by tunneling the registration to the mobile node's local home agent. By default, the registration messages are tunneled unless all intermediate tunnel destinations (the realm agents) support registration relay ('P' bit is set in the Realm Agent Entry [ref Section 3.1]).

4.1 Realm Agent Registration Extension

All registration request and reply MUST include the Realm Agent Registration extension. This extension MUST be before the Mobile-Home Authentication extension. The extension is an explicit notification of the source route (realm agents) that SHOULD be traversed between the home routing realm and visited routing realms.

There may be additional routing realms crossed implicity but they are transparent to MPN and no additional intermediate tunnel destinations are specified i.e. not included in the Realm Agent Registration extension.

The Realm Agent Registration extension is defined as follows:



Type 128

Length 10

H Realm Home Agent Present

If the Realm Home Agent Present bit is set to 1, then the realm home agent address field is valid and indicate an intermediate tunnel destination requested.

F Realm Foreign Agent Present

If the Foreign Home Agent Present bit is set to 1, then the realm home agent address field is valid and represent an intermediate tunnel destination requested.

R Registration Relay. If the 'R' bit is set, the mobile node or local home agent requests that the realm agents relay the registration messages.

T Tunnel Circuit Switching. If the 'T' bit is set, the mobile node requests that the mobility agents use tunnel circuit switching [ref Section 7].

4.2 Registration Considerations

Tunneling of Registration Messages

All mobility agents except the local foreign agent MUST be able to process GRE tunneled packets. This enables the mobile node to reverse tunnel the registration request to its local home agent and for the local home agent to forward tunnel the registration reply in a basic MPN deployment.

Registration Relay

A private mobile node MUST NOT request a realm foreign agent to relay its registration request (set 'R' bit in Realm Agent Registration extension) if its realm home agent does not support registration relay.

Realm Foreign Agent

A realm foreign agent that requires registration ('R' bit is set in the Realm Agent Entry) MUST tunnel the registration message to the local home agent if the 'H' bit is set but the 'R' bit is not set in the Realm Agent Registration extension, with the realm home agent as the intermediate tunnel destination.

Local Foreign Agent

A local foreign agent that requires registration ('R' bit is set in

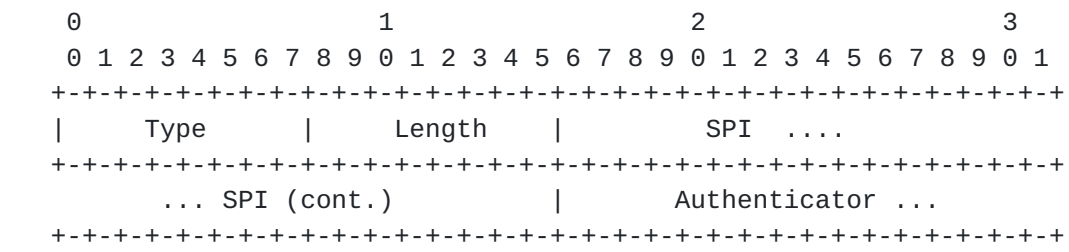
the Mobility Agent Extension) MUST process the Realm Agent Registration Extension and relay the registration message to the next mobility agent.

Local Home Agent

The local home agent MUST return the same realm agent registration extension (in the registration request) for all registration replies.

5. Security Extensions

There can be security associations between realm agents and Mobile IP mobility agents.



Mobile-Realm Home Authentication Extension

Type 35

Mobile-Realm Foreign Authentication Extension

Type 36

Realm Foreign-Realm Home Authentication Extension

Type 37

6. Movement Scenarios

Only movement across routing realms need to be considered. Mobility support within the home routing realm is provided by the Mobile IP base protocol. Only the differences from Mobile IP is illustrated.

The movement detection algorithm is specified in Section 3.4 In all the scenarios, the mobile node will typically establish a bidirectional tunnel with its local home agent.

6.1 Public Home Routing Realm to Private Visited Routing Realm

A realm foreign agent 200.9.2.1 is selected from the realm agent entries ('F' bit is set) advertised.

Registration Request

IP fields:

Source Address MN co-located care-of address

Destination Address MN local home agent address

Mobile IP fields:

The 'D' bit, 'G' bit and 'R' bit are set.

Realm Agent Registration extension fields:

The 'F' bit is set.

Realm Foreign Agent Address 200.9.2.1

If the realm foreign agent 200.9.2.1 supports registration relay, the the mobile node's local home agent.

Registration Reply

Realm Agent Registration extension fields:

If the 'R' bit is not set, the registration message must be GRE tunneled in the reverse direction.

Bidirectional Tunnel

On successful registration, a bidirectional GRE tunnel is established between the mobile node and local home agent.

Mobile Node <--> Realm Foreign Agent <--> Local Home Agent

Routing Optimization

The realm foreign agent may be the reverse tunnel endpoint. This should be determined by the mobile node.

6.2 Private Home Routing Realm to Private Visited Routing Realm

The scenario is similar to Section 6.1 except there is now a realm home agent. Using the same example in Section 2.4:

Registration Request

The Realm Agent Registration fields:

The 'H' bit and 'F' bit are set.

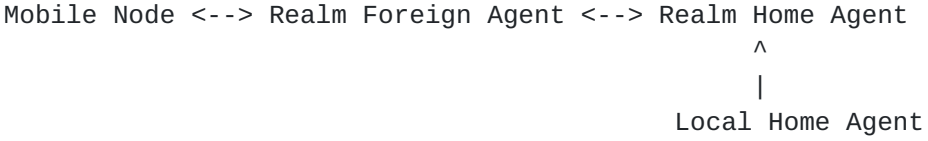
Realm Foreign Agent Address 200.9.2.1

Realm Home Agent Address 192.32.174.44

If both the realm home agent and realm foreign agent support registration relay, the 'R' bit set, else the registration message must be GRE tunneled to the mobile's node local home agent.

Bidirectional Tunnel

On successful registration, a bidirectional GRE tunnel is established between the mobile node and local home agent.



Routing Optimization

The realm home agent may be the reverse tunnel endpoint. This should be determined by the mobile node.

6.3 Private Home Routing Realm to Public Visited Routing Realm

The scenario is similar to Section 6.2 except there is now no realm foreign agent.

Registration Request

IP fields:

Source Address MN co-located care-of address

Destination Address 192.32.174.44

Mobile IP fields:

The 'D' bit, 'G' bit and 'R' bit are set.

Realm Agent Registration extension fields:

The 'H' bit is set.

Realm Home Agent Address MN realm home agent

If the realm home agent supports registration relay, the 'R' bit is set, else the registration message must be tunneled to the mobile node's local home agent.

Bidirectional Tunnel

On successful registration, a bidirectional GRE tunnel is established between the mobile node and local home agent.

Mobile Node <--> Realm Home Agent <--> Local Home Agent

Routing Optimization

The realm home agent may be the reverse tunnel endpoint. This should be determined by the mobile node.

7. Tunnel Circuit Switching

This section describes an alternative encapsulation mechanism to tunnel across multiple routing realms. Tunnel circuit switching is an extension of Minimal Encapsulation for IP [4].

In MPN, bidirectional tunneling is used to deliver datagrams between the mobile node and its local home agent. In tunnel circuit switching, the bidirection tunnel is a virtual routing circuit with the mobile node and its local home agent as the circuit end points. When the mobile node and its local home agent are in different routing realms, the virtual circuit must be routed through realm agent(s).

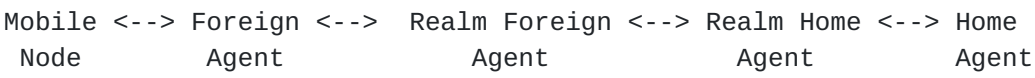
The diagram illustrates all the MPN entities in a virtual circuit that crosses three separate routing realms - private home network to global public internet to private visited network.

Mobile node with co-located care-of address

Mobile Node <--> Realm Foreign Agent <--> Realm Home Agent <--> Home Agent

For the reverse tunnel, the mobile node encapsulates the original datagram with the care-of address as the source address of the modified IP header.

Mobile node with local foreign agent as care-of address



For the reverse tunnel, the mobile node encapsulates the original datagram with the home address as the source address and the local foreign agent or the realm foreign agent as the destination address of the modified IP header.

For the forward tunnel, the local foreign agent or the mobile node may be the tunnel endpoint. The local foreign agent MUST forward the datagram with the mobile node's link layer address (learnt from the mobile node registration request) as the destination link layer address.

7.1 Conventional Datagram Tunneling

Typically, there are only two entities involved in tunneling - the encapsulator and decapsulator - as the tunnel is established within a common routing realm. There is generally no benefit to establishing a virtual circuit since the tunnel header already stores both tunnel endpoints addresses.

In MPN, to tunnel from the home agent to the care-of address and vice versa, the IP addresses of each of the intermediate tunnel destinations which routes the tunneled packet are required.

In the conventional approach, all these routing information are recorded in the tunnel header. However, this information is duplicated for every datagram tunneled. The additional information is also only relevant to the realm agents. Establishing a tunnel circuit can reduce this overhead.

7.2 Tunnel Identifier

Tunnel identifiers (TIDs) are assigned by realm agents. They are used by MPN entities to correctly switch the tunnel circuits. The TIDs are unique to a realm agent and have no relation to the TIDs assigned by other realm agent.

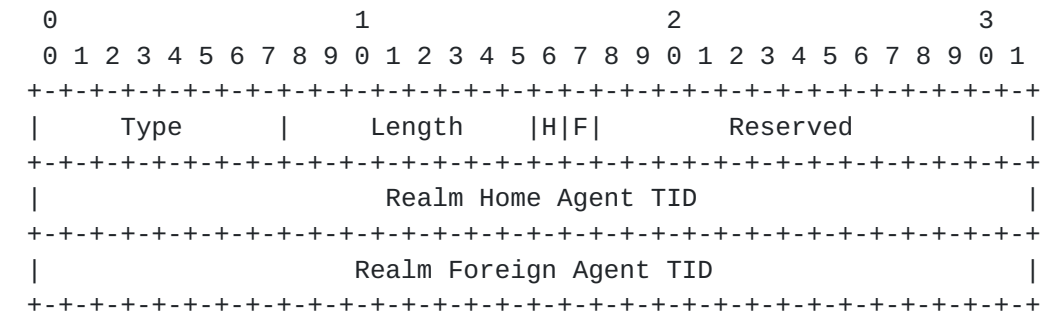
IP fragmentation must not occur at a tunnel circuit switching point as the TID is stored within the IP payload. The same requirement applies to GRE tunnels.

The TID assigned must be authenticated to prevent modification during tunnel circuit establishment. Since a Mobile-Home security association MUST exist in Mobile IP, it can be used for the TID authenticaton.

During the mobile node registration process, the realm agents allocate their TIDs in the TID extension [ref to Section 7.3] of the registration request. The TID extension MUST NOT be included in the Mobile-Home Authentication extension. If the registration process is successful, the home agent MUST include the TID extension in the Mobile-Home Authentication extension of the registration reply.

The realm agents MUST verify that the TID in the TID extension of the registration reply is the original value allocated. If the value is changed, the realm agent MUST indicate a registration failure in the code field of the registration reply.

7.3 Tunnel Identifier Extension



Type 129

Length 10

H Realm Home Agent TID Present

If the Realm Home Agent TID Present bit is set to 1, then the realm home agent TID field is valid.

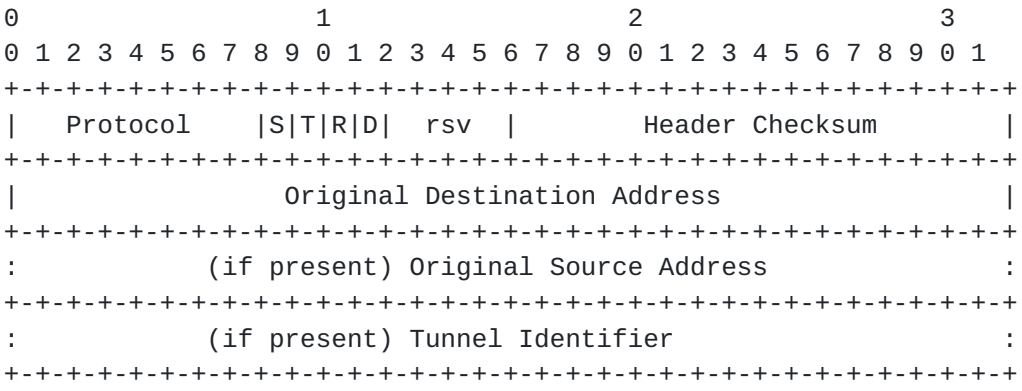
F Realm Foreign Agent TID Present

If the Foreign Home Agent TID Present bit is set to 1, then the realm home agent TID field is valid.

7.4 Minimal Forwarding Header

The minimal forwarding header is inserted into a datagram as specified by [4].

The format of the extended minimal forwarding header is as follows:



The new extensions are defined as follows:

T TID Bit
If set, the Tunnel Identifier field is present.

R Reverse Bit
If set, the packet is tunneled from the mobile node to its local home agent (reverse tunneling).

D Decapsulation Bit
If set, the packet SHOULD be decapsulated and forwarded using the existing routing mechanism.

7.5 Data Structures

A realm agent MUST associate the TID with the following information:

Index	H	R	Next Hop IP Address	Next Hop TID
TID	0	0	Care-of Address	Unchanged
	0	1	Realm Home Agent	Realm Home Agent TID
	1	0	Realm Foreign Agent	Realm Foreign Agent TID
	1	1	Home Agent	Unchanged

H If set, the realm agent is a Realm Home Agent. R If set, the tunnel circuit is a reverse tunnel ('R' bit is set in the extended minimal forwarding header).

A local home agent MUST associate the mobile node's home address with

the TID assigned by the (forward tunnel) next hop realm agent in the registration request.

A local foreign agent MUST associate the TID assigned by the (reverse tunnel) next hop realm agent in the registration reply with the mobile node's link layer address.

8. Security Considerations

GRE is a cleartext encapsulation mechanism and does not protect the data from eavesdroppers. The mobile node and its local home agent should establish an end-to-end bidirectional tunnel and encrypt it if privacy is a concern.

Due to the current lack of trust for the Internet at large, a secure channel should be established from a private mobile node to its private home routing realm. Traffic between the private mobile node and its realm home agent's external interface should be encrypted.

Firewall Filter Rules

Access control at the realm agents into the private network should be provided as any node that gains access to it, can access the private network as well.

Firewalls can deny mobile traffic on a per private routing realm basis or per public network basis. To control the visitor list on a per mobile node basis, the realm agents MUST be active realm agents. It is also possible to filter traffic based on the TID.

Implementation Status

A prototype implementation of MPN by W. T. Teo, one of the authors, is now undergoing testing.

Acknowledgements

Many thanks to Y. C. Tay at the National University of Singapore for supporting this joint work as well as for his valuable comments.

This work was supported in part by National University of Singapore ARF grant RP960683.

References

[1] Perkins, C., Editor, "IP Mobility Support", RFC 2002, October 1996

[2] C. Perkins. "IP Mobility Support Version 2", <draft-ietf-mobileip-v2-00.txt>, November 1997

[3] C. Perkins, "IP Encapsulation within IP", RFC 2003, May 1996

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

[5] G. Montenegro, "Reverse Tunneling for Mobile IP", RFC 2344, May 1998.

[6] P. Srisuresh, K. Egevang, "Traditional IP Network Address Translator (Traditional NAT)", <draft-ietf-nat-traditional-01.txt> - work in progress, November 1998

[7] P. Srisuresh, M. Holdrege, "IP Network Address Translator (NAT) Terminology and Considerations", <draft-ietf-nat-terminology-01.txt> - work in progress, October 1998

[8] Y. Li, W. T. Teo, "IP Private Address Identification", <draft-yliteo-mobileip-paid-01.txt> - work in progress, November 1998

[9] Rekhter, Y., Moskowitz, B. Karrenberg, D., G. de Groot, and Lear, E. "Address Allocation for Private Internets", RFC 1918, February 1996

[10] S. Hanks, T. Li, D. Farinacci and P. Traina, "Generic Routing Encapsulation over IPv4 networks", RFC 1702, October 1994

[11] S. Hanks, T. Li, D. Farinacci, P. Traina, "Generic Routing Encapsulation (GRE)", RFC 1701, October 1994

Author's Address

W. T. Teo
School of Computing
National University of Singapore
Lower Kent Ridge Crescent
SINGAPORE 119260

E-mail: teoweetu@comp.nus.edu.sg
Y. Li
Nortel Networks
BL60-304
600 Technology Park Drive
Billerica, MA 01821

Phone: 1-978-916-1130
Fax: 1-978-670-8760
E-mail: yunli@NortelNetworks.COM