Internet Engineering Task Force
INTERNET DRAFT
<draft-adrangi-mipv4-midbox-traversal-00>
Date: July 2001
Expires: January 2002

Farid Adrangi
Prakash Iyer
Intel Corp.

Mobile IPv4 Traversal Across NAT and VPN Gateways

Status of this Memo

Abstract

Wireless LANs or hot spots are starting to be widely deployed in Enterprise Intranets and public areas such as airports, coffee shops, shopping malls etc. based on IPv4. This combined with the availability of multi-mode networked devices and applications that can take advantage of continuous mobility and constant reachability, is driving the need for Mobile IP in these networks. At the same time, middleboxes (NAT and VPN gateways for example) are also seeing widespread usage. Mobile IPv4 has known functional and performance limitations in the

presence of these middleboxes. This draft proposes a solution framework that enables seamless operation of Mobile IPv4 across middleboxes without requiring any changes to the middleboxes themselves. Although the solution is generically extensible,

---

the draft specifically focuses on NAT and VPN traversal. The solution has no link layer dependencies and can be applied to other 802.3-compatible physical media as well.

Table Of Contents

---

1. Introduction

The deployment of 802.3-based wired LANs and wireless LAN hot spots and WAN packet data networks based on 2.5G and 3G technologies and the availability of multi-mode networked

devices is driving new application scenarios that require Mobile IPv4 support. These networks are also seeing widespread use of NAT and VPN gateways. For example, many Enterprises are deploying wireless LANs outside their corporate DeMilitarized Zone (DMZ), requiring mobile nodes to "VPN" back into the Intranet, from NATÆed subnets. Wireless WAN operators are setting up to offer routable IPv4 addresses to corporate clients for remote access back to their Enterprise networks, while offering NAT-based access to their core network and the Internet to consumers. NAT and firewall-enabled residential networks are another example where mobile nodes could encounter such middleboxes. Mobile IPv4 has known functional and performance limitations, traversing these middleboxes. It is often unacceptable to deploy workarounds that require any software or hardware changes to these middleboxes or compromise their functionality in any way.

The solution proposed in this draft introduces a logical component called the MIP Proxy to enable seamless Mobile IPv4 functionality across such middleboxes, without requiring any changes to these middleboxes.

The important sections of this draft are organized as follows:
Section 4 describes the MIP proxy.
Section 5 discusses seamless traversal through NAT gateways.
Section 6 discusses seamless traversal through VPN gateways.
These two solutions can be deployed independently or in combination depending on specific network configurations, as discussed in section 7.

2. Terminology

Administrative Domain:
A Mobile IP administrative domain specifies the Mobile IP security parameters for one or more home agents and their corresponding mobile nodes. The security parameters are used for authentication or encryption to provide a secure channel for the Mobile IP control and data traffic between the home agent and mobile nodes.

Actual Home Agent:
It is the mobile nodeÆs real home agent, as defined by [RFC2002].

NAT-Router:
It is an IPv4 Router with NAT functionality.

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this draft are to be interpreted as described in [RFC2119].

3. Acronyms

GRE: Generic Routing Encapsulation
ISP: Internet Service provider
MIPv4: Mobile IP for IPv4
MIPv6: Mobile IP for IPv6
NAT: Network Address Translator

MN-Perm: Permanent home address of the MN
MN-COA: Co-located care-of address of the MN
MIPP-Priv: MIP Proxy interface address on the private (HA) side
MIPP-Pub: MIP Proxy interface address on the public side
NATGW-Priv: NAT gatewayÆs IP address on the private (LAN) side
NATGW-Pub: NAT gatewayÆs IP address on the public (WAN) side
IP-D: IP Destination Address
IP-S: IP source Address
VPNGW-Pub: VPN Gateway Public/External IP Address
VPNGW-Priv: VPN Gateway Private/Intranet IP Address

4. The MIP Proxy

The MIP Proxy is a functional entity that is introduced in the path between a MN and itÆs corresponding HA as depicted in the figure below. The MIP Proxy serves two primary functions: that of a surrogate MN and a surrogate HA to essentially "stitch" an end-to-end connection between a MN and itÆs HA. A single MIP Proxy can serve multiple MNs and HAs and can consequently be associated with multiple home subnets. The MIP Proxy does not replace any existing HAs. The MIP Proxy MUST belong to the same administrative domain as any of its associated home agents. It

MUST share SAs for various MIPv4 registration extensions with its associated HA(s).

+----+

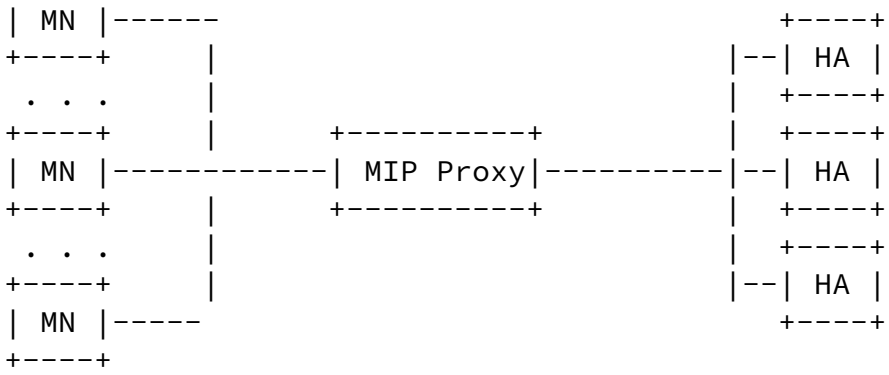


Figure 4.0 : MIP Proxy serving multiple MNs and HAs

A MIP Proxy MAY support additional functionality in the context of support for a specific type of middlebox. For NAT and VPN gateways, additional functionality, if any, is described in relevant sections of this draft.

The MIP Proxy will nominally run on a dual-homed host. It MAY be possible to instantiate the MIP Proxy on a singly homed host.

4.1. Surrogate MN Functionality

One of the primary functions of the MIP Proxy is to serve as a MNÆs surrogate when it roams into a foreign network.

As a surrogate MN, the MIP Proxy MUST perform the following MN compliant functions:

- It MUST perform registration request and reply protocol, specified by [RFC2002]
- It MUST perform reverse tunneling, defined by [RFC3024]
- It MUST perform authentication mechanism(s) for the MN and HA, required by [RFC2002]
- It MUST perform replay protection for registration request, defined by [RFC2002]

The MIP Proxy MUST NOT perform the following MN functions:

- It MUST NOT perform agent solicitation, defined by [RFC2002]
- It MUST NOT perform any functions related to agent discovery, defined by [RFC2002]
- It MUST NOT perform registration retransmission, defined by [RFC2002]
- It MUST NOT perform move detection mechanisms, defined by [RFC2002]

4.2. Surrogate HA Functionality

The other primary function of the MIP Proxy is to serve as a surrogate HA to a roaming MN that is outside its home network, and with an intervening middlebox such as a NAT or VPN gateway.

As a surrogate HA, the MIP Proxy MUST perform the following MN compliant functions:

- It MUST perform registration request and reply protocol, defined by [RFC2002]
- It MUST perform authentication mechanism(s) for the (MN & HA and the HA & FA), required by [RFC2002]
- It MUST maintain registration binding table, defined by [RFC2002]
- It MUST perform replay protection for registration request, defined by [RFC2002]

The MIP Proxy MUST NOT perform the following MN functions:

- It MUST NOT perform agent advertisement, defined by [RFC2002]
- It MUST NOT perform gratuitous ARP, defined by [RFC2002]
- It MUST NOT perform Proxy ARP, defined by [RFC2002]
- It MUST NOT perform Route Optimization [ROUTE-OPT]

4.3. Deploying a MIP Proxy

A MIP Proxy MAY be deployed in a public network serving multiple HAs in that network as conceptually depicted in the figure above. It MUST be deployed in a DMZ to supported authenticated firewall traversal for MIPv4 packets traversing the DMZ from an MN with an intervening NAT gateway in itÆs foreign network. It MUST be deployed in parallel with an IPsec-compatible VPN gateway in a DMZ. Trivially, a subset of the MIP Proxy functionality MAY be co-located with a HA if appropriate.

The MIP Proxy MAY be located in the same or a different subnet from any of its associated home agents.

4.4. Discovering a MIP Proxy

A MN MUST be statically configured with the MIPP-Pub address of the MIP Proxy. Dynamic discovery of the MIP ProxyÆs public IP address is outside the scope of this draft.

4.5. MIP Proxy Redundancy

A MIP Proxy redundancy protocol is desirable to effect high availability in public and Enterprise deployment. Details of such a protocol are beyond the current scope of this draft.

5. MIPv4 Traversal Through NAT Gateways

5.1. NAT Traversal Problem Statement

When an MN roams from its home network (which may or may not be in a routable IP address space) to a foreign network behind a NAT gateway, it acquires a non-routable care-of address (most likely through [DHCP]). The acquired non-routable care-of address is passed to the HA through a registration request. This causes the MN to lose its connectivity to its home network, since the HA will not be able to forward the MNÆs packets to the non-routable care-of address. The scenario is depicted in Figure 5.1 below.

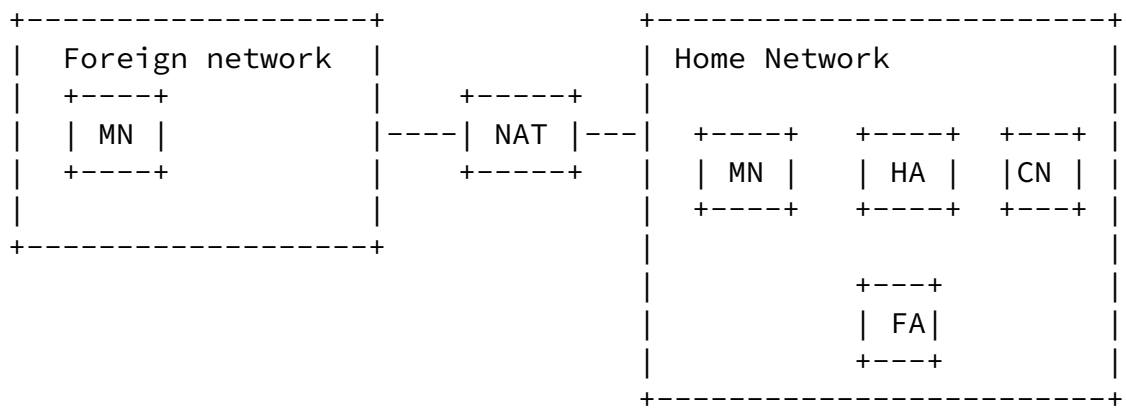


Figure 5.1 : MN has moved from its home network to a foreign network

Even if we overcome this problem somehow by using the NAT gatewayÆs public routable address in the care-of address field of the registration request, the NAT gateway will not always be able to demultiplex inbound MIPv4 data traffic properly. Consider two MNs behind the NAT gateway registered with the same HA. The inbound IP-in-IP tunneled MIPv4 packets from the HA to the two MNs will have the source and destination IP address, making it difficult for the NAT gateway to route the packets to the appropriate MN.
The implications on Minimal IP [RFC2004] and GRE encapsulation

[RFC1701] modes of MIPv4 are similar to IP-in-IP tunneling.

5.2. Assumptions and Applicability

The solution proposed in the draft is targeted toward network environments where the following are true.
- The NATÆed foreign network SHOULD NOT be modified. This implies that no software or hardware changes to the NAT gateway are feasible and adding a new routing entity (dedicated to MIPv4 nodes) to such a network is unacceptable. Most residential and small business networks are typical examples of such NATÆed networks, wherein an embedded broadband router (supporting local DHCP and NAT) is employed and additional resources such as a routable IP address and/or a system are not obtainable.
- The NAT gateway is capable of doing address and port mapping.

- The NATÆed network MUST provide DHCP service to the foreign subnet or a mobile node MUST be capable of self-assigning or acquiring by other means, a non-routable care-of address when it roams behind the NAT.
- The NATÆed network MAY NOT include a foreign agent.
- The NATÆed network MAY NOT be in the same administrative domain as the MN, MIP Proxy and HA.
- The NATÆed network MUST be configured with the IP addresses reserved for private Internets by IANA ([RFC1918], [LOCAL-LINK]).
- If the NATÆed network is multi-subnetted, the routers within that network cannot be compromised.
- The HA SHOULD NOT be modified.
- MNÆs home network MUST be in a routable IP address domain. This address domain MAY be behind a firewall/DMZ.
- A FA MAY NOT be available in the ISP access or core network.
- Security implications should not be worse than direct comm. With HA.

Applicability in other network environments has not been verified; however it is not explicitly precluded. Furthermore, the proposed solution MAY be used in combination with other NAT traversal solutions as appropriate.

If the MNÆs home network is in a non-routable IP address domain, an appropriate solution (outside the scope of this

draft) MUST be deployed to make the home network accessible from an external public or private network.

5.3. Using the MIP Proxy for NAT Traversal

The MIP Proxy acts as an intermediate node between a MN in foreign network behind NAT and itÆs HA. MIPv4 registration requests from the MN are sent to the MIP Proxy, instead of the actual HA. The MIP Proxy terminates the registration request and validates the payload. If the registration request is acceptable, the MIP Proxy creates a new registration request and forwards it to the HA on behalf of the MN. The registration response from the HA is translated into a new response from the MIP Proxy back to the MN.

All subsequent MIPv4 data traffic between the MN and the MIP Proxy SHOULD be encapsulated in a UDP tunnel, in order to help the NAT gateway demultiplex return inbound MIPv4 traffic NAT/NAPT mechanisms.

The solution is detailed in the following sections.

5.3.1. When does a MN register with the MIP Proxy?

A mobile node MUST register with the MIP Proxy when it roams to a foreign network behind a NAT gateway. Mechanisms to detect

the presence of a NAT gateway are beyond the scope of this draft.

5.3.1.1. Selection of the COA Field in the Registration Request Payload

As explained in the problem statement, the use of a non-routable address as the COA causes the MN to lose its connectivity to its home network. Therefore, the MN MUST use the NAT gatewayÆs routable (WAN) as the COA in its registration payload. The MN MAY be configured with the NAT gatewayÆs routable IP address a priori. However, if this is not feasible, it is imperative for the MN to use a secured discovery scheme to realize the NAT gatewayÆs routable address to avoid potential Denial-of-Service (DoS) attacks. The following diagrams show one possible method for dynamically discovering and verifying the NAT gatewayÆs routable address.

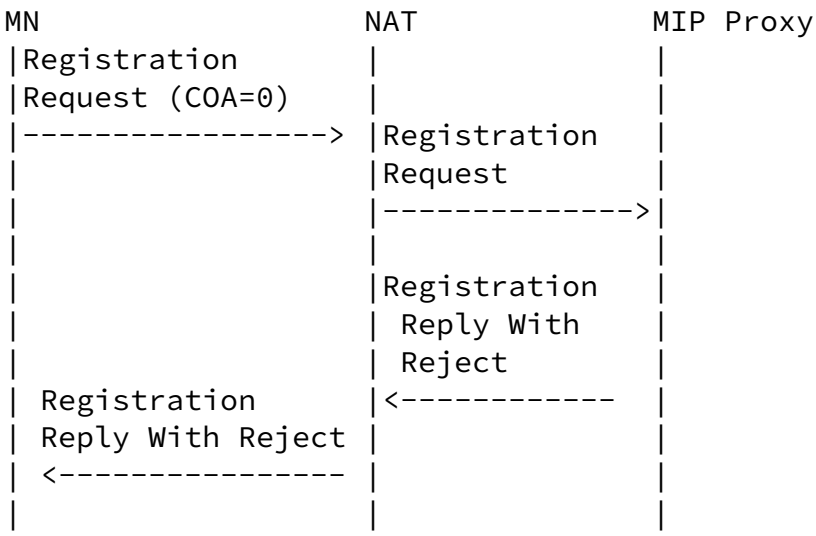


Figure 5.3a : Discovery of the NAT gatewayÆs routable address

Figure 5.3b : Verification of the NAT gatewayÆs routable address

The NAT gatewayÆs routable address discovery (as depicted in Figure 5.3a) is accomplished as a part of the registration request protocol initiated when the MN roams to a foreign

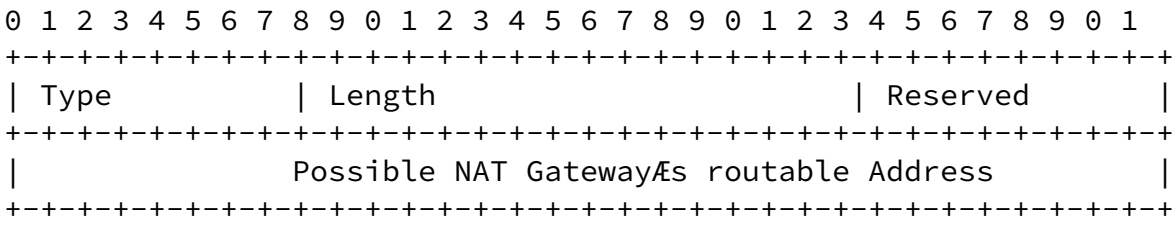
network behind a NAT gateway. The MN MUST send a registration request to the MIP Proxy with the COA set to a zero. As the registration payload contains an invalid COA, the MIP Proxy MUST send a registration reply with error code 134 (Poorly Formatted). The MIP Proxy MUST also include the NAT Discovery extension in its reply (see section 5.3.1.2). The MIP Proxy

employs this extension to notify the MN about the possible NAT gatewayÆs routable address, obtained from the source IP address of the registration request.

The MN MAY verify this IP address, before it can use it as the COA in its registration payload. With NAT-router gateways, The MN MAY achieve this by analyzing the trace-route log (i.e., a series of ICMP echo and reply messages) from the MN to the possible NAT gatewayÆs routable address obtained form the registration discovery extension.

5.3.1.2. Discovery Registration Extension

The following shows the format of the NAT Discovery extension used in the registration reply from the MIP Proxy to the MN.



Type: 180
Length: Indicates (in bytes) of the data fields within the extension, excluding the Type and Length bytes.
Reserved: For future user.
Possible NAT GatewayÆs routable Address: An IP address

Once the MN obtains and verifies the NAT gatewayÆs public address, it MUST send a registration request with the COA set to the NAT gatewayÆs routable address.

5.3.2. MIPv4 registration protocol between MN and HA

Once the MN obtains and verifies the NAT gatewayÆs routable address, the MN MUST register with its actual home agent via the MIP Proxy. Therefore,
the normal flow of MIPv4 registration messages between a MN and a HA are altered as depicted in the figure below.

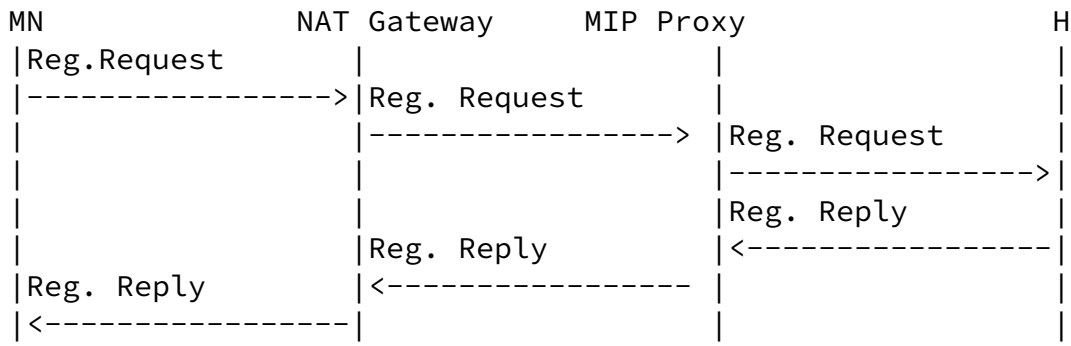


Figure 5.3.2 : Mobile IP registration protocol between MN and HA

5.3.2.1. Establishing UDP Tunnel Parameters for MIPv4 Data Traffic

To support multiple, simultaneous MIPv4 data sessions from MNs behind a NAT gateway to a home network via the same HA, a UDP tunnel MUST be established between the MN and MIP Proxy. The MN MUST use the parameter registration extension (see section 5.3.2.3) to notify the MIP Proxy about the UDP port number ought to be used to establish a UDP tunnel for the Mobile IP data traffic between the MN and MIP Proxy.

The UDP port number 434 MAY be used to tunnel the data traffic between the MN and MIP Proxy. However, this MAY have some performance implications. If any UDP port numbers other than 434 is used, a new entry in the NAT gatewayÆs address/port mapping MUST be created right after a successful registration. This can be done, by sending a NULL UDP packet (i.e, an empty payload) from the MN to the MIP proxy.

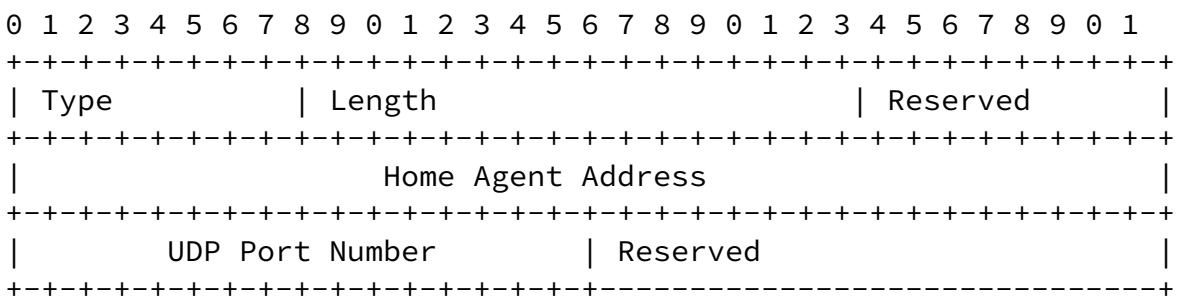
The mobile node MUST maintain the selected UDP port number for the lifetime of the registration request. The MN SHOULD ensure that the NAT gatewayÆs lifetime for the UDP tunnel port mapping does not expire prior to the expiry of the Registration lifetime. This MAY be done through some sort of periodic KeepAlive messages from the MN to MIP Proxy.

5.3.2.2. Discovering the MNÆs actual home agent by the MIP Proxy

The MN MUST notify the MIP Proxy about its actual home agent address, via the parameter registration extension. The following shows the parameter registration extension format.

5.3.2.3. Parameter Registration Extension

The following shows the format of the parameter extension used in the registration request from MN to the MIP Proxy.

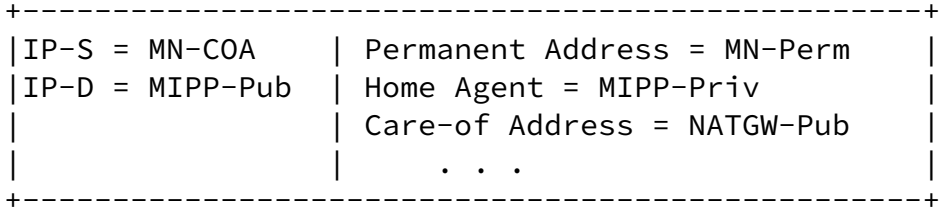


Type : 181
Length :
Indicates (in bytes) of the data fields within the extension, excluding the Type and Length bytes.
Reserved: For future use.
Home Agent Address: An IP address of the MNÆs actual home agent
UDP Port Number: Used to establish UDP tunnel
Reserved: For future use.

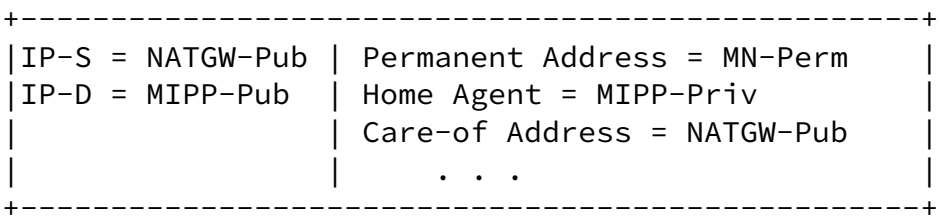
5.3.2.4. MIPv4 Registration Request Packet Flow From MN to HA

The MN sends the Registration Request to the MIP Proxy. The intervening NAT gateway modifies the source IP address (and possibly the UDP source port).

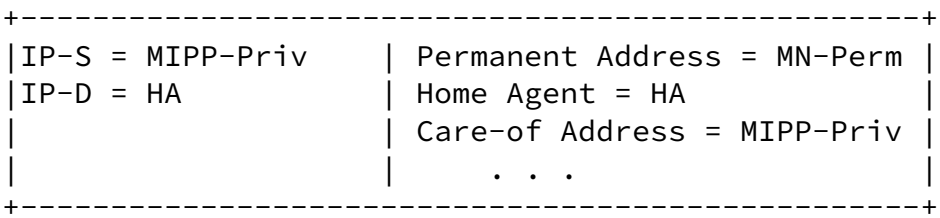
From MN to the MIP Proxy:



The NAT gateway modifies the source IP address, and possibly UDP source port number.



The MIP Proxy terminates and authenticates the Registration Request received from the MN. It then modifies the registration request payload and forwards a new registration request to the HA associated with the MN. The MIP Proxy MUST set the Home Agent and Care-of Address fields of the registration request to the MNÆs actual HA (learned from the parameter registration extension) and the MIP ProxyÆs private address respectively. The packet format is shown below.

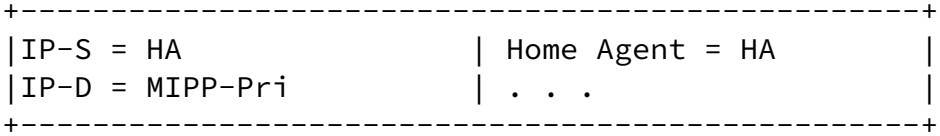


The MIP Proxy maintains a registration binding cache similar to the one specified by [RFC2002] for a HA, in order to forward the registration replies and subsequent MIPv4 data traffic. In addition, the MIP Proxy MUST also record the UDP port number (learned form the parameter registration extension) for the UDP tunnel between the MN and the MIP Proxy in the registration binding cache. The MIP Proxy MUST not manage registration lifetimes and MUST NOT reinitiate a registration request with a HA prior to its expiration. A MN MUST continue to manage Registration lifetimes as specified in [RFC2002].

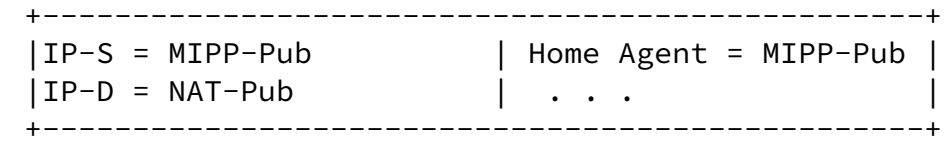
5.3.2.5. MIPv4 Registration Reply Packet Flow From HA to MN

If the actual HA were to accept the registration request, the reply flow sequence will be as follows:

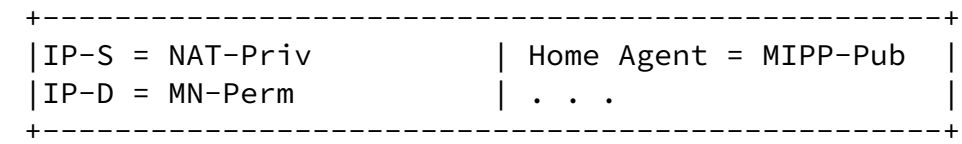
From the HA to the MIP Proxy:



From the MIP Proxy to the NAT



From the NAT to the MN:



5.3.3. MIPv4 data traffic from MN to CN

The normal flow of MIPv4 data flow between a MN and a HA are altered as depicted in the figures below. Note that the data traffic form the MN to MIP Proxy is encapsulated in a UDP tunnel.

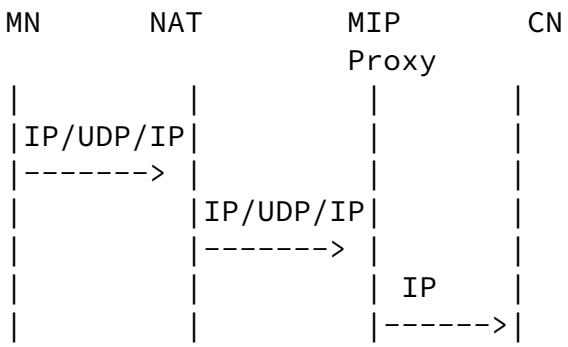
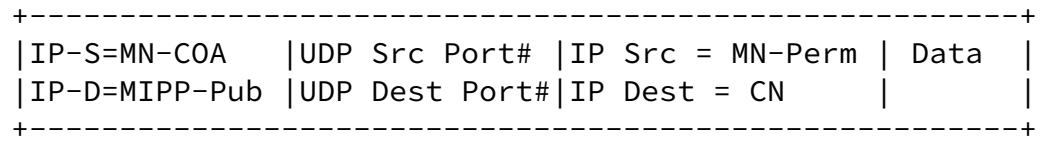


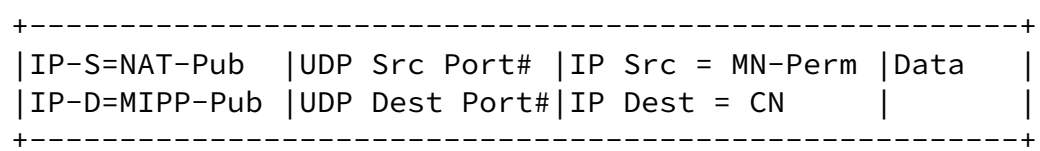
Figure 5.3.5 : MIP Proxy forwards data packet directly to CN

All MIPv4 data traffic between the MN and MIP Proxy will be encapsulated in a UDP tunnel. The MIP Proxy will strip off the outer IP and UDP headers, and re-encapsulate the detunneled packet in an IP header (from MIPP-Pub to MN or from MIPP-Priv to HA as the case may be) before forwarding it to the MN or HA respectively. The following figures illustrate the traffic flow from the MN to the MIP Proxy, and the MIP Proxy to the actual HA.

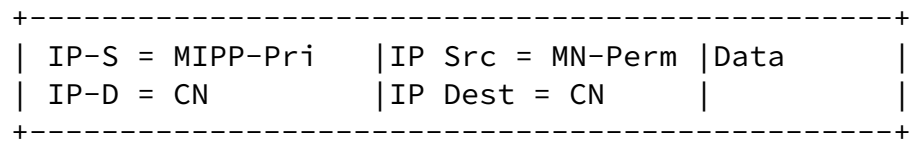
MIPv4 data packet flow from the MN to the MIP Proxy:



The intermediate NAT gateway will apply address and port mapping on the packet, and forward the packet, as follows:



MIPv4 data packet flow from the MIP Proxy to CN is as follows:

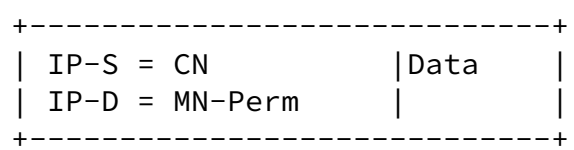


5.3.4. MIPv4 data traffic from CN to MN

MIPv4 data traffic will be tunneled from the actual HA to the MIP Proxy IP-in-IP tunnel is illustrated in the figure above, however the discussion applies to other MIPv4 encapsulation modes as well). The MIP Proxy strips off the outer IP header, and forwards the inner IP packet to the MN in a UDP tunnel.

The following figures illustrate the traffic flow from the CN to the MN (via the actual HA and the MIP Proxy).

The data packets from the CN will be sent to the MNÆs permanent address, MN-Perm.



The MNÆs home agent will intercept the data packet, and will forward it to its current care-of address (i.e., MIP Proxy) as follows:

```
+-----------------------------------------------+
| IP-S = HA          |IP Src = MN-Perm |Data    |
| IP-D = MIPP-Priv   |IP Dest = CN     |        |
+-----------------------------------------------+
```

From the MIP Proxy to the NAT gateway:

```
+-------------------------------------------------------------+
|IP-S = MIPP-Pub    |UDP Src Port# |IP Src = MN-Perm |Data |
|IP-D = NAT-Pub     |UDP Dest Port#|IP Dest = CN     |     |
+-------------------------------------------------------------+
```

The NAT gateway unapplies address and port mapping on the packet, and forwards the packet, as follows:

From the NAT gateway to the MN:

```
+-------------------------------------------------------------+
| IP-S = MIPP-Pub    |UDP Src Port# |IP Src = MN-Perm |Data |
| IP-D = MN-COA      |UDP Dest Port#|IP Dest = CN     |     |
+-------------------------------------------------------------+
```


5.4. Summary of changes on MIPv4 components required by this solution

This solution requires changes on the mobile node, and of course an addition of a new component, the MIP Proxy.

5.4.1. Required Changes to a MN

- The MN MUST be configured with the static IP address of the MIP Proxy. A mechanism for MIP Proxy discovery MAY be defined in future.
- The MN MUST be able to determine if it has roamed to a private address space behind a NAT gateway.
- The MN MUST implement the registration extension as specified in this draft.
- The MN SHOULD be able to extend the lifetime of the NAT gatewayÆs address and port mapping entries for the UDP tunnel

beyond the registration lifetime determined with itÆs HA.

5.4.2. Required Configuration for the MIP Proxy

- The MIP Proxy MUST be configured with all of the SAs of an MN and a HA that it represents as a surrogate.
- The MIP Proxy SHOULD be configured with static IP addresses to avoid periodic reconfiguration on MNs.

5.5. Performance Implications of MIP Proxy assisted NAT Traversal

- The proposed method creates a layer of indirection (i.e., the MIP Proxy), which MAY have some performance implications.
- An eight bytes UDP header is added to the Mobile IP data traffic from the MN to MIP Proxy.
- Discovery and verification method of the NAT gatewayÆs public address will degrade the registration hand-off performance.

5.6. Implications of Twice NAT between the MN and MIP Proxy

The proposed solution MAY not work if Twice NAT is encountered in the path between the MN and the MIP proxy.

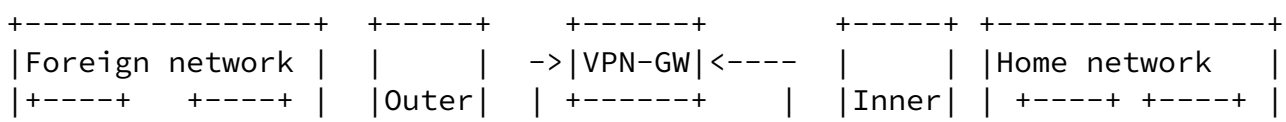
6. MIPv4 Traversal Through IPsec VPN Gateways

A MN whose home network is in a routable IP address space behind a VPN gateway could roam to an external public or private address space. An example would be a user who roams from within a Corporate Intranet to an external wired or wireless hot spot. In this case, the MNÆs HA is located in the Corporate Intranet behind the firewall/DMZ complex, as illustrated in the figure below.

It is desirable in this scenario to connect back to the Intranet via a VPN and stay connected even as the user roams from one external IP subnet to another. The integration of MIPv4 and IPsec has not been standardized and several issues

---

have to overcome to support seamless end-to-end IPsec. This draft describes a solution based on the use of the MIP Proxy to enable seamless traversal across IPsec-based VPNs.



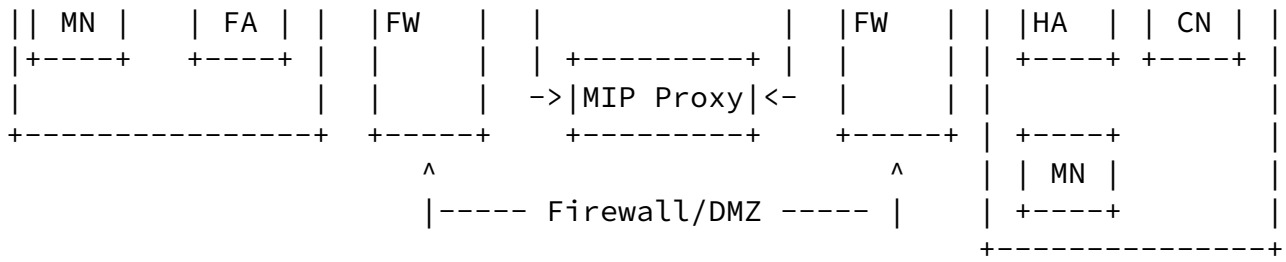


Figure 6.0 : MN has moved from its home network to a foreign network outside the DMZ

6.1. IPsec VPN Traversal Problem Statement

With respect to Figure 6.0 above, the problem can be summarized in the following 2 scenarios:

Scenario 1: The MN could roam into a foreign subnet without a FA and obtain a COA at its point of attachment (via DHCP or other means). In an end-to-end security model, an IPsec tunnel that terminates at the VPN gateway in the DMZ MUST protect the IP traffic originating at the MN. If the IPsec tunnel is associated with the COA, the tunnel SA MUST be refreshed after each subnet handoff which could have some performance implications on real-time applications.

Scenario 2: The MN could roam into a foreign subnet with a FA. If the MN were to associate a VPN tunnel with its COA, the FA (which is likely in a different administrative domain) cannot parse the IPsec, will not be able to setup SAs with the MNÆs VPN gateway and will consequently be not able to relay MIPv4 packets between the MN and the VPN gateway.

6.2. Integration of MIPv4 and IPsec

Clearly there are several schemes to apply IPsec to MIPv4 packets. [MIPv4-SEC-GUIDE] describes different segments where

IPsec could be applied to MIPv4 packets. This draft is based on the premise that the most likely acceptable scenario is the one in which IPsec is applied end-to-end.

6.3. Assumptions and Applicability

The solution is derived based on the following assumptions and

applicability criteria:
- End-to-end IPsec tunnel mode MUST be applied to MIPv4 data flows; i.e. between the MN and the VPN gateway at the edge of its home network.
- MIPv4 registration packets MAY NOT require IPsec tunnel as they are authenticated and integrity protected. However, they MUST be terminated inside the DMZ to enable authenticated firewall traversal.
- FA-assisted routing and MN co-located modes of operation MUST be supported.
- The MN MUST be configured with the MIP Proxy and the VPN gatewayÆs external IP addresses, and route the MIPv4 traffic through the MIP Proxy when it is outside the corporate intranet.
- The MN SHOULD be able to determine if it has roamed outside the corporate network by some method (e.g., by comparing its current COA against address blocks used by the corporate intranet).
- The MN MUST be able to determine when it should exercise its key exchange protocol to establish the IPsec tunnel SA to the VPN gateway.

6.4. Solution Considerations

In addition to enabling the use of end-to-end IPsec with MIPv4, the use of the MIP Proxy in the DMZ enables a solution that can meet the following criteria:

6.4.1. Fast Handoffs

To support fast handoffs across IP subnets, it is imperative to keep the key management overhead down to a minimum. In this draft, we propose a mechanism whereby the IPsec tunnel SA can be bound to the invariant permanent IP address of the MN. Doing so, enables the reuse of the SA across IP subnet handoffs and also minimizes the protocol handshake between the VPN gateway, actual HA and the MIP Proxy.

6.4.2. Preserve Existing VPN Infrastructure

This implies the following:
- Preserves the investment in existing VPN gateways
- Requires no software upgrades to VPN gateways to explicitly support MIPv4 users
- Preserves IPsec VPN security requirements that are not inferior to what is already provided to existing "nomadic

computing" remote access users, i.e. for confidentiality, primary and secondary authentication, message integrity, protection against replay attacks and related security services

6.4.3. Preserve Existing DMZ Traversal Policies

Most Corporate DMZ policies recommend authenticated firewall traversal for protocols that traverse the DMZ. Placing devices outside the outer DMZ firewall to assist with DMZ traversal exposes the device to hackers and is generally not an acceptable solution. IT departments prefer that solutions adhere to and can be accommodated with existing or compliant DMZ ACLs.

6.5. Deploying the MIP Proxy to support VPN Traversal

As shown in Figure 6.0, the MIP Proxy is deployed in parallel to an existing VPN gateway in the DMZ to support MIPv4.

6.5.1. Mobile IPv4 Registration

The MN sends MIPv4 registration requests directly to the MIP Proxy. The MIP Proxy terminates and authenticates the registration requests. It then generates a new registration request and forwards it to the corresponding HA. The registration request MUST include the discovery registration extension (see section 5.3.1.2.) to notify the MIP Proxy about the MNÆs actual home agent. The registration replies from the HA will also go through the MIP Proxy bypassing the VPN gateway. Note that the MN and the MIP Proxy MUST share the SA for the MN-HA authentication extension.

This solution also works if the MN were to use a FA in the foreign network.
A rail-road diagram illustrating the MIPv4 registration process is shown below.

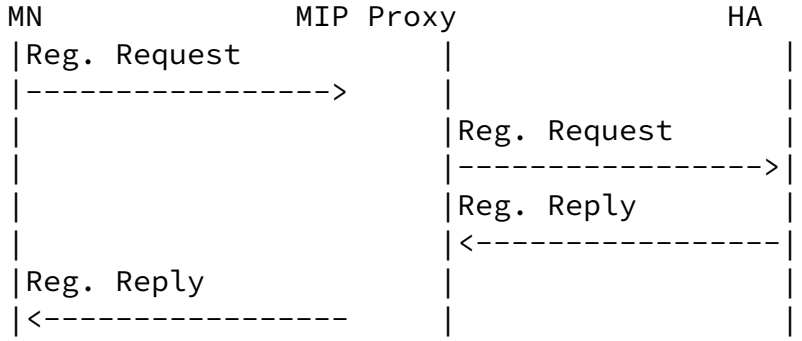


Figure 6.5.1 : Mobile IP registration protocol between MN and HA

6.5.1.1. MIPv4 Registration Request Packet Flow from MN to HA

This draft illustrates the sequence from MN to HA via a FA û it can be easily extended to describe the flow for a co-located COA mode MN.

From the MN to a FA:

```
+-------------------------------------------------+
|IP-S = MN-Perm   | Permanent Address = MN-Perm   |
|IP-D = FA_COA    | Home Agent = MIPP-Pub         |
|                 | Care-of Address = FA COA      |
|                 |     . . .                     |
+-------------------------------------------------+
```

From the FA to the MIP Proxy:

```
+-------------------------------------------------+
|IP-S = FA COA    | Permanent Address = MN-Perm   |
|IP-D = MIPP-Pub          | Home Agent = MIPP-Pub |
|                 | Care-of Address = FA COA      |
|                 |     . . .                     |
+-------------------------------------------------+
```

From the MIP Proxy to the actual HA:

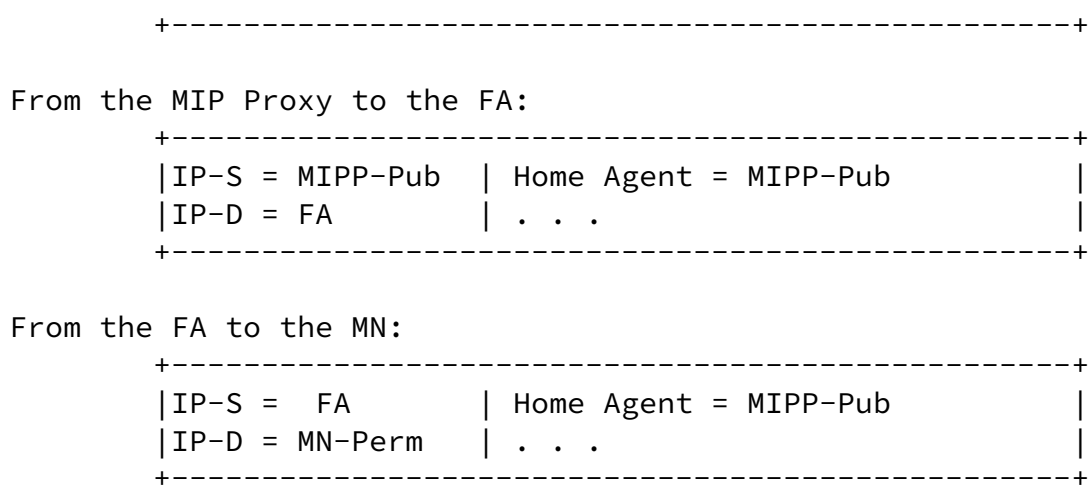
```
+-------------------------------------------------+
|IP-S = MIPP-Priv | Permanent Address = MN-Perm   |
|IP-D = HA        | Home Agent = HA               |
|                 | Care-of Address = MIPP-Priv   |
|                 |     . . .                     |
+-------------------------------------------------+
```

6.5.1.2. MIPv4 Registration Reply Packet Flow from HA to MN

If the actual HA were to accept the registration request, the reply flow sequence will be as follows:

From the HA to the MIP Proxy:

```
+-------------------------------------------------+
|IP-S = HA         | Home Agent = HA              |
|IP-D = MIPP-Priv  | . . .                        |
```



6.5.1.3. DMZ Configuration Requirements for MIPv4 Registration Packets

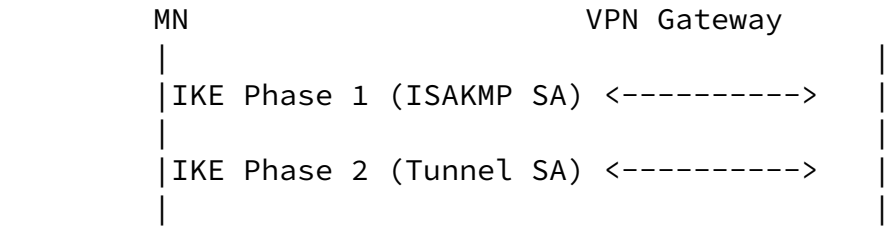
The DMZ ACLs MUST be setup for the following:
- Inbound UDP registration packets (destination port = 434 and destination address = MIPP-Pub) MUST be permitted.
- The DMZ inner firewall MUST permit the forwarding of registration request and reply packets from the MIP Proxy to one or more HAs.

6.5.2. Mobile IPv4 Data Processing

The following railroad diagram illustrates the sequence of steps to establish secured MIPv4 traffic between a MN and a CN. The process initially occurs in 3 sequential steps: MIPv4 registration, IPsec tunnel SA establishment and MIPv4 data forwarding. Registration and SA refreshes may subsequently occur independent of each other.

MIPv4 Registration- see Figure 6.5.1
Note that the VPN gateway is not involved in the MIPv4 Registration process.

IPsec Tunnel SA Establishment:

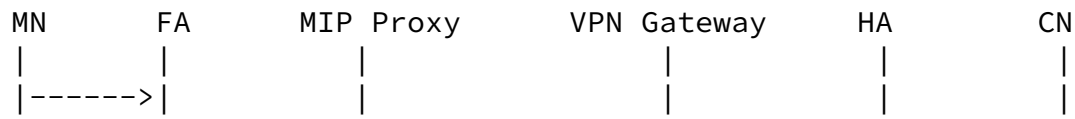


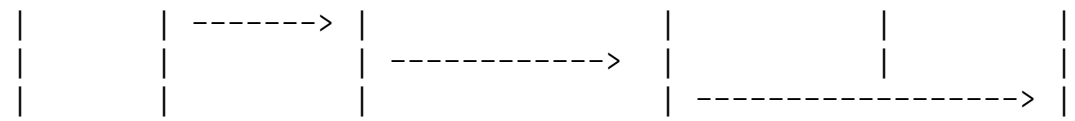
Note that the MIP proxy is not involved in the Tunnel SA establishment and will not be involved in SA refreshes.

The data forwarding is described in the following 2 sub-sections.

6.5.2.1. MIPv4 Data Traffic from MN to CN

The MN generates an IP packet from the MN-Perm interface and destined to the CN. This packet is encapsulated in an IPsec-ESP tunnel from MN-Perm to VPNGW-Pub. The packet in turn is encapsulated in an IP header from MN COA to the MIP Proxy. The MIP Proxy strips off the outermost IP header and forwards the inner IP packet (which is from the MNÆs permanent address to the VPN gateway) to the VPN gateway. The VPN gateway in turn processes the IPsec VPN tunnel, strips off the IP and ESP headers and forwards the inner most IP packet to the destination CN. The railroad diagram depicts the packet flow sequence, followed by a description of packets as they traverse the network.

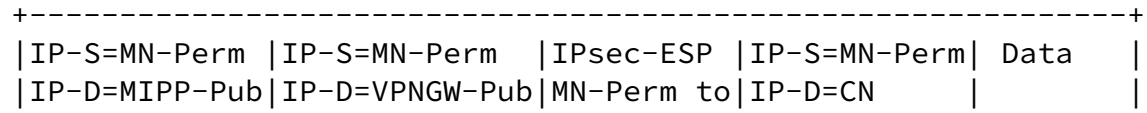




From the MN to MIP Proxy: IP-IP-ESP-IP-TCP/UDP-Data
From MIP Proxy to VPN: IP-ESP-IP
From VPN Gateway to CN: IP

The packet flow from the MN to the CN is described below. The analysis assumes than the MN employs reverse tunneling to the HA (which is the MIP Proxy in this case) and that packets are routed via a FA.

From the MN to the FA:



```
|             |              |VPNGW-Pub |            |        |
+-------------------------------------------------------------+
```

In this case, the layer-2 destination address is set to the MAC address of the FA.

From the FA to the MIP Proxy:

```
+-------------------------------------------------------------+
|IP-S=FA COA  |IP-S=MN-Perm  |IPsec-ESP |IP-S=MN-Perm| Data   |
|IP-D=MIPP-Pub|IP-D=VPNGW-Pub|MN-Perm to|IP-D=CN     |        |
|             |              |VPNGW-Pub |            |        |
+-------------------------------------------------------------+
```

Clearly, the FA does not need to know the IPsec tunnel SA to process the packet.

From the MIP Proxy to the VPN gateway:
The MIP Proxy strips off the outermost IP header and forwards the packet to the VPN gatewayÆs outer interface using the layer-2 address corresponding to VPNGW-Pub.

```
+-----------------------------------------------+
|IP-S=MN-Perm  |IPsec-ESP |IP-S=MN-Perm| Data   |
|IP-D=VPNGW-Pub|MN-Perm to|IP-D=CN     |        |
|              |VPNGW-Pub |            |        |
+-----------------------------------------------+
```

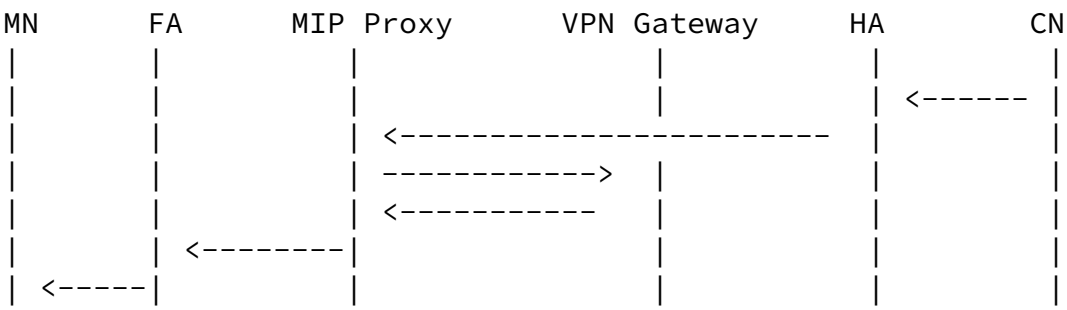
From the VPN gateway to the CN:
The VPN gateway completes IPsec tunnel processing on the packet, strips off the outermost IP and ESP headers and forwards the encapsulated IP datagram to the CN.

```
+---------------------+
|IP-S=MN-Perm| Data   |
|IP-D=CN     |        |
+---------------------+
```


6.5.2.2. MIPv4 Data Traffic from CN to MN

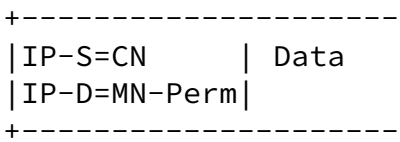
The outbound MIPv4 data traffic destined to the MNÆs co-located address is always tunneled to the MIP Proxy (which appears as a surrogate MN to the actual HA). The MIP Proxy forwards the inner IP packet (with MN-Perm as the destination address) to the VPN gateway. The VPN gateway applies the IPsec ESP tunnel SA on the packet. The VPN gateway forwards the packet back to the MIP Proxy on its MIPP-Pub interface û this is accomplished by a routing table update on the VPN gateway. The MIP Proxy in

turn tunnels the IPsecÆed packet to the MNÆs COA. The railroad diagram depicts the packet flow sequence, followed by a description of packets as they traverse the network.



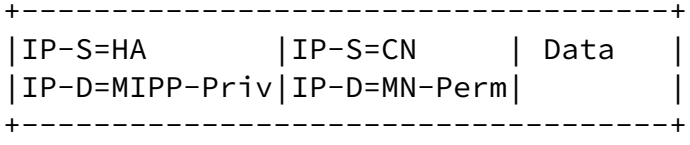
From the HA to the MIP Proxy: IP-IP
From the MIP Proxy to the VPN gateway: IP
From the VPN gateway to the MIP Proxy: IP-ESP-IP
From the MIP Proxy to the MN: IP-IP-ESP-IP

The packet flow from the CN to the MN is described below.
From the CN to the actual HA:

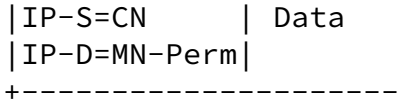


The CN sets the layer-2 destination address to that of the actual HA.

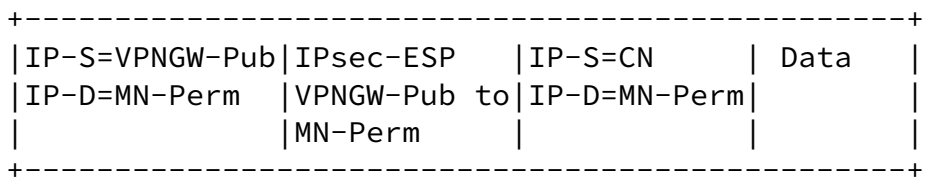
From the actual HA to the MIP Proxy:



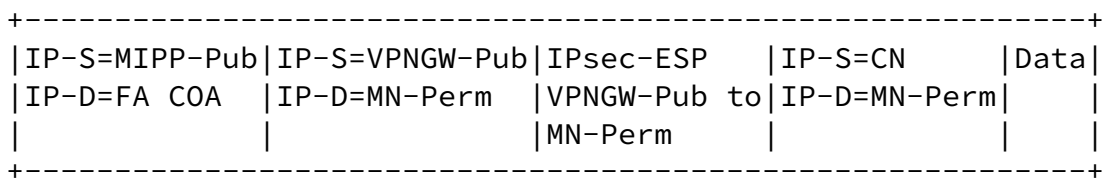
From the MIP Proxy to the VPN gateway:
The MIP Proxy strips off the outermost IP header and forwards the packet to the VPNGW-Priv interface using the corresponding layer-2 address.



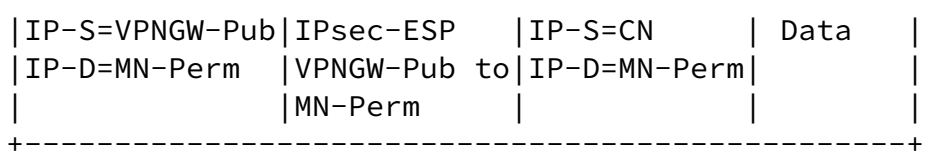
From the VPN gateway to the MIP Proxy:
The VPN gateway applies an IPsec ESP tunnel SA to the IP packet and forwards it back to the MIP Proxy on the MIPP-Pub interface based on its routing table.



From the MIP Proxy to the FA:
The MIP Proxy adds an outer encapsulating IP header to the FA COA.



From the FA to the MN:
The FA strips off the outermost IP header and forwards the packet to the MN.



The MN terminates the IPsec tunnel and processes the MIPv4 data as always.

6.5.3. Support For Route Optimization

The MIP Proxy MUST NOT support Route Optimization [ROUTE-OPT]. However, the Route Optimization between the correspondent node and the mobile nodeÆs actual home agent MAY be performed.

6.6. Key Management and SA Preservation

The scheme described in the previous section binds the IPsec tunnel SA to the normally invariant permanent IP address of the MN. This implies that the tunnel SA can be preserved even when the MN changes its co-located COA or connects via a FA in a different IP subnet. The SA however must be refreshed prior to its lifetime expiration. Also, many VPN gateway implementations

support some keep-alive mechanism to detect the presence of a VPN client and "retire" the SA if the VPN client is not detected for a period of time. If an MN loses link connectivity for a period extending the keep-alive timeout interval, it MUST reestablish the tunnel SA, regardless of whether it reconnects to the same IP subnet or not.

The scheme also preserves any secondary authentication mechanisms that may be in the place to authenticate a remote access user.

6.7. DMZ and VPN Gateway Configuration Requirements

The solution described in this section makes the following assumptions on the configurability of the VPN gateway and the DMZ ACLs:
- It MUST be possible to configure the VPN gatewayÆs routing table to deliver the outbound IPsecÆed MIPv4 packets destined to MN-Perm to the MIP ProxyÆs MIP-Pub interface, if MIP Proxy is not co-located with the VPN gateway.
- The outer firewall MUST allow inbound tunneled IP packets destined to the MIP Proxy
- The MIP Proxy MUST be able to forward packets (destined to MN) to VPN gateway via layer 2 mechanism. This implies that the MIP Proxy and VPN Gateway MUST be on the same subnet.

6.8. Supporting Other IPsec-based VPN Configurations

The scheme currently described in this draft assumes a native IPsec VPN scheme extended to support secondary authentication schemes. Its applicability to other IPsec VPN configurations such as L2TP over IPsec transport and ESP-in-UDP tunneling is yet to be determined.

6.9. Considerations for Integrating the MIP Proxy and VPN Gateway

The MIP Proxy as described in this draft is a logical functional component and as such can be deployed in the DMZ in one of 2 possible ways:
- As a standalone device in parallel with the VPN gateway as depicted in Figure 6.0. This decouples support for MIPv4 users from any software or hardware upgrades to the VPN gateway itself and also enables multi-vendor interoperability. The scheme however adds some overhead to the end-to-end communication path between an MN and a CN and requires minimal support from the VPN gateway software (i.e. a mechanism to make routing table updates).
- Integrated as a software component with the VPN gateway. This clearly reduces the communication overhead but tightly couples

support for MIPv4 users with any software upgrades to the VPN gateway itself.

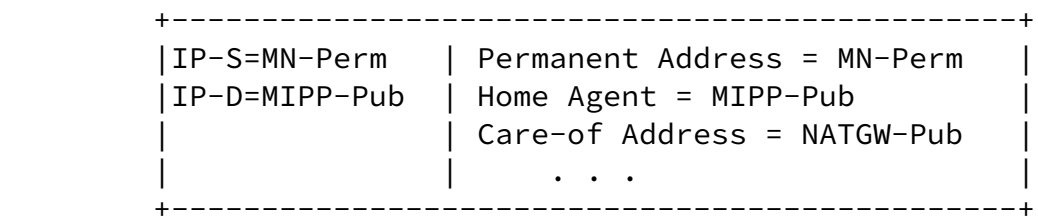
7. Using the MIP Proxy for combined NAT and VPN Traversal

The discussion in the draft would be incomplete without describing a scenario in which a MN roams into a foreign NATÆed network and has to connect back to itÆs home network which is behind a DMZ. Many Enterprises are deploying wireless LANs as a private NATÆed network outside their DMZ-users that roam into such a network will be forced to VPN back into their Intranet. Such a scenario can be supported with the MIP Proxy enabling simultaneous NAT and VPN traversal. The network configuration would be a combination of Figures X and Y. The analysis assumes that there is no FA in the NATÆed network.

7.1. MIPv4 Registration Message Flow

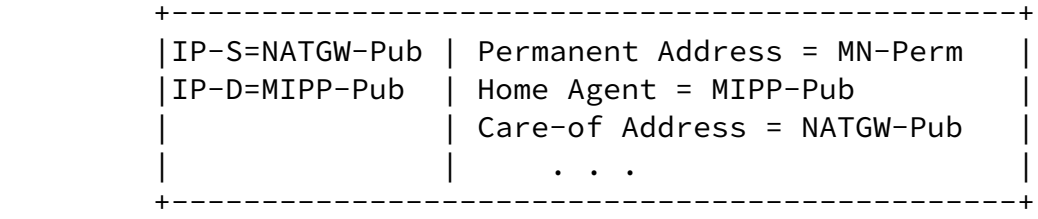
7.1.1. MIPv4 Registration Requests

From the MN to the NAT gateway:



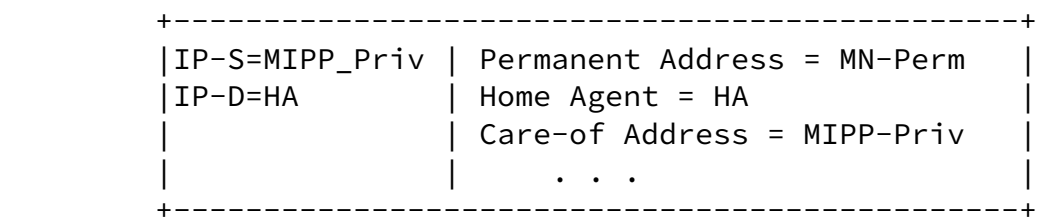
Please see the discussion in section 5 for possible mechanisms for an MN to determine the NAT gatewayÆs external (public) routable IP address.

From the NAT gateway to the MIP Proxy:
The NAT gateway performs source address and source UDP port translation before forwarding the packet to the MIP Proxy.



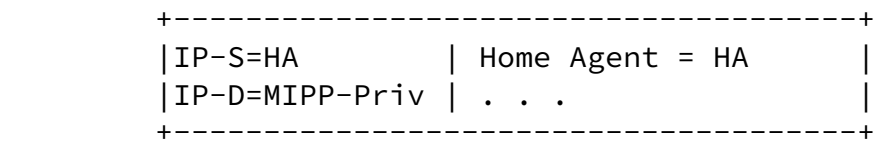
From the MIP Proxy to the actual HA:

The MIP Proxy terminates and authenticates the registration request (as described in previous sections). It then creates a new registration request and forwards it to the actual HA.

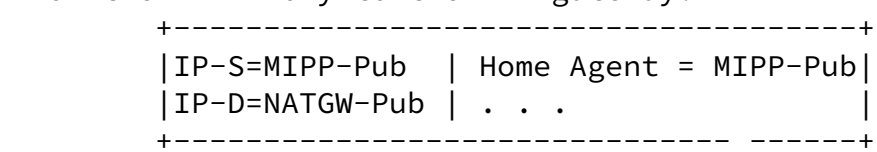


7.1.2. MIPv4 Registration Replies

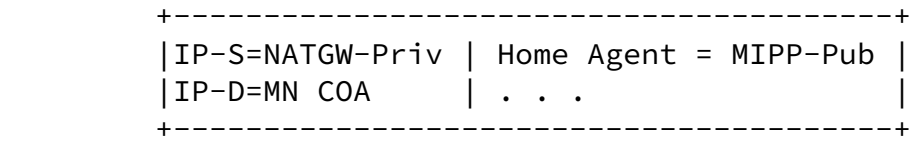
From the actual HA to the MIP Proxy:



From the MIP Proxy to the NAT gateway:



From the NAT gateway to the MN:

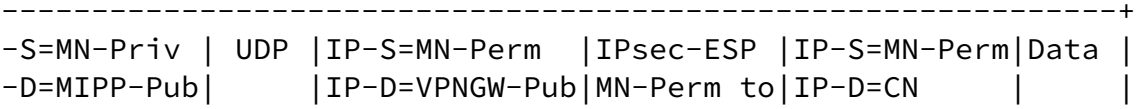


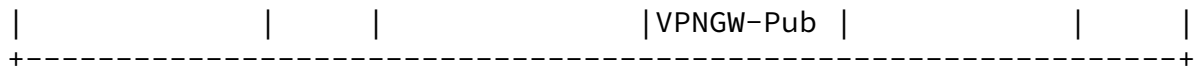
7.2. MIPv4 Data Flow

Reverse tunneling is assumed in the packet flow descriptions that follow.

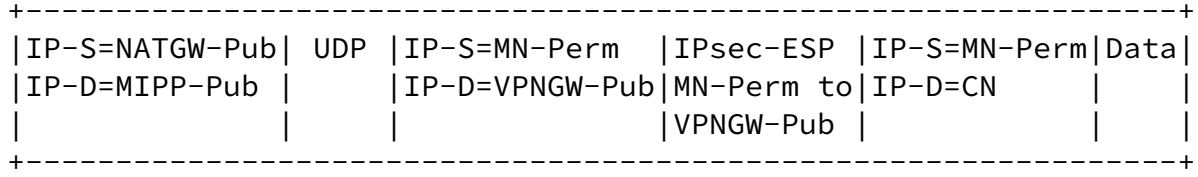
7.2.1. Data Flow from the MN to the CN

From MN to the NAT gateway:

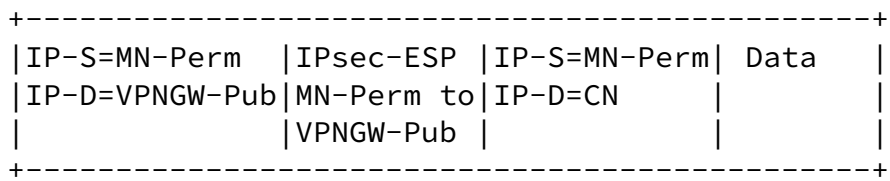




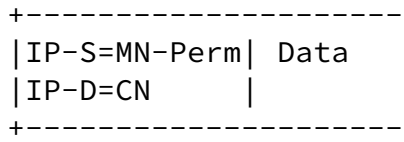
From the NAT gateway to the MIP Proxy:



From the MIP Proxy to the VPN gateway:

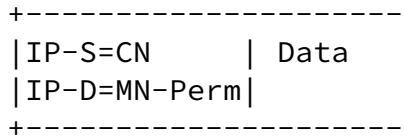


From the VPN gateway to the CN:

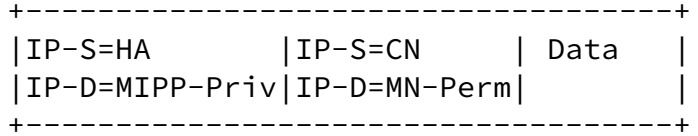


7.2.2. Data Flow from the CN to the MN

From the CN to the actual HA:

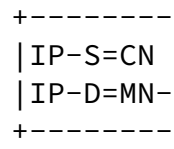


From the actual HA to the MIP Proxy:

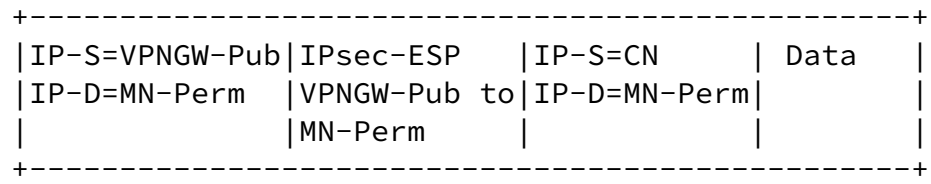


From the MIP proxy to the VPN gateway:
The MIP proxy strips off the outer IP header and forwards the

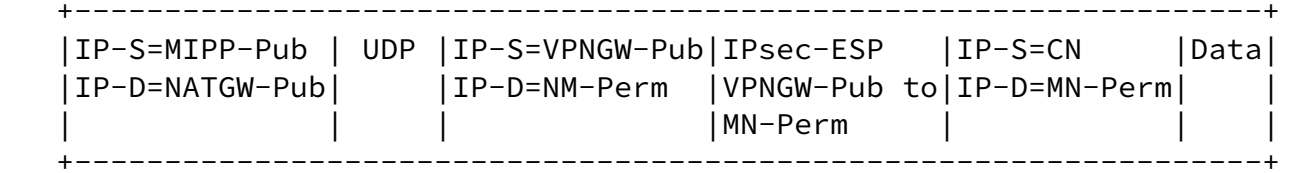
packet on the layer-2 address for VPNGW-Priv.



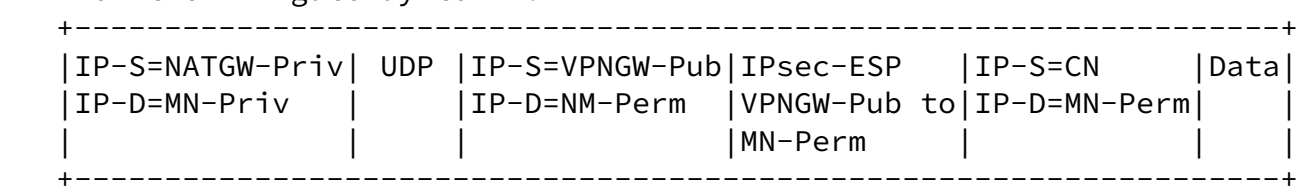
From the VPN gateway to the MIP Proxy:



From the MIP Proxy to the NAT gateway:



From the NAT gateway to MN:



8. Security Implications

The MIP Proxy is a functional entity that MUST be implemented on a secure device especially if it is deployed in the DMZ. The MIP Proxy is assumed to belong to the same (security) administrative domain as the MN and the actual HA. The protocol extensions specified in the draft do not introduce any new vulnerabilities to the mobile IP protocol.

9. Acknowledgements

The authors would like to thank Mike Andrews and Changwen Liu of Intel Corporation for their review and feedback on this draft.

10. Patents

Intel Corporation is in the process of filing one or more patent applications that may be relevant to this IETF draft.

11. References

[RFC2002] RFC 2002 : IP mobility support
[RFC3024] RFC 3024 : Reverse tunneling for mobile IP
[RFC2004] RFC 2004 : Minimal encapsulation within IP
[RFC1701] RFC 1701 : Generic Routing encapsulation
[RFC2119] RFC 2119 : Key words for use in RFCs to Indicate Requirement Levels
[RFC1918] RFC 1918 : Address Allocation for Private Internets
[DHCP] RFC 2131 : Dynamic Host Configuration Protocol
[MIPv4-SEC-GUIDE] draft-bpatil-mobileip-sec-guide-01.txt - Requirements / Implementation Guidelines for Mobile IP using IP Security
[[LOCAL-LINK] : Dynamic Configuration of Iv4 Link-Local Addresses, <draft-ietf-zeroconf-ipv4-linklocal-03>
[ROUTE-OPT] : Route Optimization in Mobile IP, <draft-ietf-mobileip-optim-10.txt>

Authors:

Farid Adrangi
Intel Corporation
2111 N.E. 25th Avenue
Hillsboro, OR
USA

Phone: 503-712-1791
Email: farid.adrangi@intel.com

Prakash Iyer
Intel Corporation
2111 N.E. 25th Avenue
Hillsboro, OR
USA

Phone: 503-264-1815
Email: prakash.iyer@intel.com