Internet Engineering Task Force
INTERNET DRAFT
<draft-adrangi-mobileip-vpn-traversal-02>
Date: July 17 2002
Expires: January 2003

Farid Adrangi
Prakash Iyer
Intel Corp.

Kent Leung
Milind Kulkarni
Alpesh Patel
Cisco Systems

Qiang Zhang
Liqwid Networks

Joe Lau
Hewlett Packard Corp.

Mobile IPv4 Traversal Across IPsec-based VPN Gateways

Status of this Memo

Abstract

Multi-subnetted IEEE 802.11 WLAN networks are being widely

deployed in Enterprise Intranets û(in many cases requiring a VPN tunnel to connect back and access Intranet resources), and public areas such as airports, coffee shops, convention centers and shopping malls. Many of these WLAN networks also employ NAT

to translate between non-routable and routable IPv4 care-of (point of attachment) addresses. WWAN networks such as those based on GPRS, 1xRTT and eventually EDGE, 1xEV, CDMA2000 and UMTS are also starting to see deployment. These deployments are paving the way for applications and usage scenarios requiring TCP/IP session persistence and constant reachability while connecting back to a secured (VPN protected), target ôhomeö network. This in turn drives the need for a mobile VPN solution that is multi-vendor interoperable, providing seamless access with persistent VPN sessions - through NAT gateways when needed. This draft proposes a solution framework that enables efficient, seamless operation of Mobile IPv4 when combined with an IPsec-based VPN and supporting NAT traversal when needed. The solution has no link layer dependencies and can be applied to other 802.3-compatible wired and wireless physical media as well.

Table Of Contents

1. Introduction

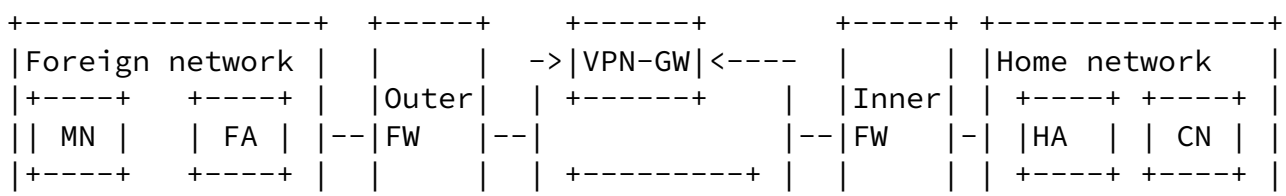
The problem statement and solution requirements for MIPv4 traversal across VPN gateways are articulated in [15]. To understand the motivation and rationale for the solution proposed in this draft, we strongly encourage the audience to read [15] first.

This draft introduces a logical component called the Mobile IP Proxy (MIP Proxy) to enable seamless Mobile IPv4 functionality across VPN gateways, without requiring any IPsec VPN protocol changes to VPN gateways. The solution aims specifically at extending the use of deployed IPsec-based VPN gateways, a feature that is much desired by corporate IT departments. The solution also leverages [11] to support Mobile traversal across ôNAT and VPNö gateways. The ôNAT and VPNö refers to a network topology where Mobile IP traffic has to traverse one or more NAT gateway(s) followed by a VPN gateway in the path to its final destination. While the discussion in this draft is limited to IPsec-based VPN gateways, it should be compatible with other IP-based VPN solutions as well.

1.2. Goals

A MN whose home network is in a protected 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 (i.e, the HA is not directly reachable by the MN), as illustrated in Figure 1.2.

It is desirable in this scenario to connect back to the Intranet via a VPN while maintaining the transport connections prior to the move, and stay connected as the user roams from one external IP subnet to another outside the DMZ, or the user decides to roam back inside the DMZ.



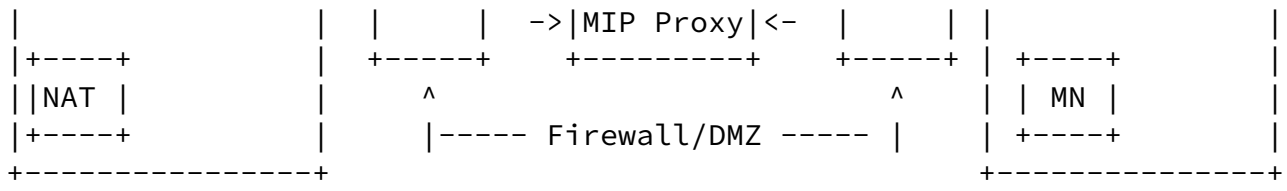


Figure 1.2 û MN moves from its home network to a foreign network outside the DMZ

1.3. Problem Description

With respect to Figure 1.2 above, the problem can be summarized in the following 3 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 undesirable 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 and will not be able to setup SAs with the MNÆs VPN gateway and will consequently not be able to relay MIPv4 packets between the MN and the VPN gateway.

Scenario 3: The MN could roam into a NATÆed network that may or may not employ a FA. In this scenario, the MIPv4 traffic has to traverse a NAT followed by a VPN gateway. The problem statement

and solution for MIPv4 traversal across NAT gateways is articulated in [11].

1.4. Solution Overview

The solution introduces a new Mobile IP logical entity, called Mobile IP Proxy (MIP Proxy). With respect to Figure 1.2 above, the MIP Proxy is placed in the DMZ, co-located or running in parallel with the VPN. The MIP Proxy is in the path between a MN

outside the DMZ and its corresponding actual HA.

The MIP Proxy serves two primary functions: that of a surrogate MN and a surrogate HA to essentially ôstitchö an end-to-end connection between the MN and its actual 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 SHOULD belong to the same administrative domain as any of its associated home agents and their corresponding MNs. It MUST share SAs for various MIPv4 registration extensions with its associated HA(s).

The MIP Proxy will nominally run on a dual-homed host - one of its interfaces on the private (LAN) side, and the other on the public (WAN) side. The MIP Proxy can be instantiated on a singly homed host - however in this document we assume that the MIP Proxy is instantiated on a dual-homed host. The MIP Proxy MAY be implemented as a standalone device or combined with a VPN gateway.

1.4.1. Assumptions and Applicability

The solution is derived based on the following assumptions and applicability criteria:

- An 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 an IPsec tunnel as they are authenticated and integrity protected. However, they MUST be terminated inside the DMZ to enable authenticated firewall traversal.

- The DMZ outer firewall MUST allow inbound tunneled IP packets destined to the MIP Proxy.

- The DMZ outer firewall MUST permit inbound UDP registration packets (destination port = 434 and destination address = MIP Proxy interface on the public (WAN) side).

- The DMZ inner firewall MUST permit the forwarding of registration request and reply messages from the MIP Proxy to one or more HAs.

1.5. Terminology

Administrative Domain:
In the context of this draft an administrative domain is the entity that specifies security parameters for Mobile IP registration extensions for one or more Home Agents and their corresponding mobile nodes. The administrative domain also manages policies that govern negotiation of security associations for VPN sessions that terminate or initiate at the edge of the network under its jurisdiction.

Actual Home Agent:
It is the mobile nodeÆs real home agent, as defined by [1].

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 [5].

1.6. Acronyms

DMZ: De-Militarized Zone
FA-COA: Foreign Agent care-of address
FA-Routed: FAÆs interface address on the routed network
FA-Visited: FAÆs interface address on the visited network
GRE: Generic Routing Encapsulation
IP-D: IP Destination Address
IP-S: IP source Address
ISP: Internet Service provider
MIPv4: Mobile IP for IPv4
MIPv6: Mobile IP for IPv6
MN-COA: Co-located care-of address of the MN
MN-Perm: Permanent home address of the MN
MIPP-Priv: MIP Proxy interface address on the private (HA) side
MIPP-Pub: MIP Proxy interface address on the public (Internet) side
NAT: Network Address Translation
NATGW-Priv: NAT gatewayÆs IP address on the private (LAN) side
NATGW-Pub: NAT gatewayÆs IP address on the public (WAN) side
VPNGW-Priv: VPN Gateway Private/Intranet IP Address
VPNGW-Pub: VPN Gateway Public/External IP Address

2. Registration

The MN roaming outside the DMZ sends MIPv4 registration requests directly to the MIP Proxy. The registration messages are not protected by an IPsec tunnel, and MUST be excluded from the tunnel SA applied to flows between the MN and any correspondent hosts via the VPN gateway. The MIP Proxy terminates and authenticates the

registration requests. It then generates a new registration request and forwards it to the corresponding actual HA. The

registration replies from the actual HA will also go through the MIP Proxy bypassing the VPN gateway.

A railroad diagram illustrating the MIPv4 registration process is shown below.

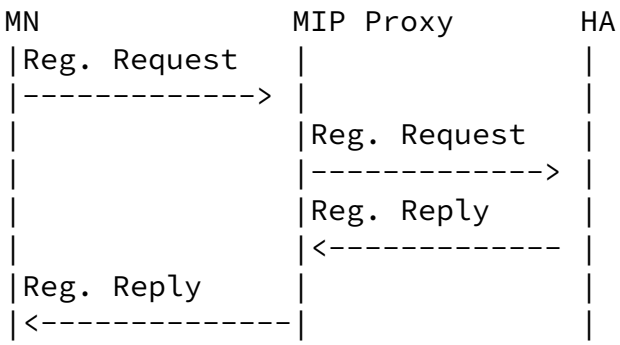


Figure 2. û Mobile IP registration protocol between MN and HA

2.1. Authentication

Each MN and the MIP proxy MUST share the SA for the MN-HA authentication extension. The MIP Proxy MUST authenticate received Registration Requests or Replies before processing them. The mechanisms to share SAs are beyond the current scope of this draft. 2.2. Registration Request Process

The MIP Proxy MUST relay all valid Registration Requests received from a MN to its actual HA, after updating its pending registration request list. Here, relaying means that the MIP Proxy creates a new Registration Request on the behalf of the MN and sends it to the MNÆs actual HA. The MIP Proxy MUST be compliant with [1], and it MUST adhere to the rules specified in the following sub-sections in creating the new Registration Request.

2.2.1. Registration Request Bits

- The new Registration Request header MAY have the same æMÆ,

æGÆ, rsv bit values included in the Registration Request received from the MN.

- The æBÆ bit in new Registration Request header MUST be set ifthe æBÆ bit in the Registration Request received from the MN is set and the MIP Proxy supports broadcast.

- The æDÆ bit in the new Registration Request MUST NOT be set, if the æBÆ bit is set. Although the surrogate MN side of the MIP Proxy always uses a co-located care-of address (i.e, MIPP-Priv), this restriction is enforced to cause the actual HA to encapsulate a broadcast or a multicast IP datagram in a unicast datagram addressed to the MNÆs home address, and then tunnel

this encapsulated datagram to the MIP Proxy (i.e, MIPP-Priv). Otherwise, the MIP Proxy will not be able to route the broadcast or multicast IP datagrams received from the HA(s), as it cannot determine to which MN the packet should be routed.

- The æTÆ bit in the new Registration Request MUST be set, if the MIP Proxy may route the MIPv4 data traffic received from the MN to CN in reverse tunneling mode.

- The new Registration Request MUST NOT set the æSÆ bit, as the actual HA will always have the same care-of address (MIPP-Priv) for all its MNs roaming outside the DMZ. Please see section 2.7.1. for more details.

2.2.2. Registration Request Fields

- The new Registration Request header MUST have equal or smaller lifetime value included in the registration request received from the MN.

- The new Registration Request header MUST have the same identification value included in the Registration Request received from the MN.

- The new Registration Request header MUST have the same Home Address value included in the Registration Request received from the MN.

- The new Registration Request headerÆs HA address field MUST be set to the MNÆs actual HA address.

- The new Registration Request headerÆs care-of address field MUST be set to MIPP-Priv.

2.2.3. Registration Request Extensions

- The new Registration Request MUST contain all Registration extensions included in the Registration Request received from the MN, with the exception of the ones specific to the MN and the MIP Proxy protocol negotiation and the authentication extension protecting the registration message between the MN and the MIP Proxy.

- The new Registration Request MUST include the MN-HA authentication extension.

2.2.4. Registration Request Validity Check

When a Registration Request is received from a MN, the MIP proxy MUST validate the registration request and respond to a malformed registration request as a HA would, as specified in [1]. In addition, the MIP proxy MUST also check the Registration Request for the following:

- The æTÆ bit MUST be set in the Registration Request. If not, the MIP Proxy MUST return a Registration Reply to the MN with an appropriate error code specified in[2].

- The MIP proxy MUST check for the existence of the HA Parameter extension, specified in section 2.6.3. In the absence of a valid HA Parameter extension, the MIP proxy MUST return a Registration Reply to the MN with an appropriate error code specified in section 2.4.1 if MIP Proxy cannot determine an appropriate HA to service the MN.

2.3. Registration Reply Process

The MIP proxy MUST relay Registration Replies received from actual HAs to appropriate MNs. Here, relaying means that the MIP Proxy creates a new Registration Reply on the behalf of the MNÆs actual HA and sends it to the MN. The MIP proxy MUST update its record of mobility bindings associated with a MN, before relaying the registration reply to the MN.

In processing a registration reply, the MIP proxy MUST be compliant with [1]. And, it MUST adhere to the rules specified in the following sub-sections.

2.3.1. Registration Reply Fields

- The new Registration Reply header MUST have the same Code value as in the Registration Reply received from the MNÆs actual HA, except when MIP Proxy received accepted Registration Reply from the actual HA but cannot service the MN (eg. create mobility binding, route, tunnel). In this case, insufficient resource (133) error code should be set in the Registration Reply to the MN.

- The new Registration Reply header MUST have the same lifetime value as in the Registration Reply received from the MNÆs actual HA. If the lifetime value is zero, the MIP Proxy should also retire the entry/entries in its mobility-binding list for the MN, as specified in [1].

- The new Registration Reply header MUST have the same Home Address value as in the Registration Reply received from the MNÆs actual HA.

- The new Registration Reply headerÆs Home Agent address field MUST be set to MIPP-Pub.

- The new Registration Reply header MUST have the same identification value as the Registration Reply received from the MNÆs actual HA.

- The new Registration Reply MUST contain all non-authentication extensions included in the Registration Reply received from the MNÆs actual HA.

- The new Registration Reply MUST include the ôMN-HAö authentication extension.

- The new Registration Reply MAY include the ôFA-HAö authentication extension, as needed.

2.4. Registration Reply Initiated by the MIP Proxy

The MIP proxy MAY deny a Registration Request for various reasons. If so, the MIP Proxy MUST use an appropriate registration denied code, specified in the following section.

2.4.1. New Registration Reply Codes

The following values are defined for use within the Code field.

Registration denied by the MIP Proxy:

200 missing HA Parameter extension
201 non zero HA address Required in HA Parameter extension
202 home agent unreachable (when ICMP unreachable received)
203 MISSING-NAI
204 MISSING-HOMEADDR
205 MISSING-HOME-AGENT
206 ASSIGNED-HOME-AGENT

2.5. Mobile Node Considerations

2.5.1. Location Detection

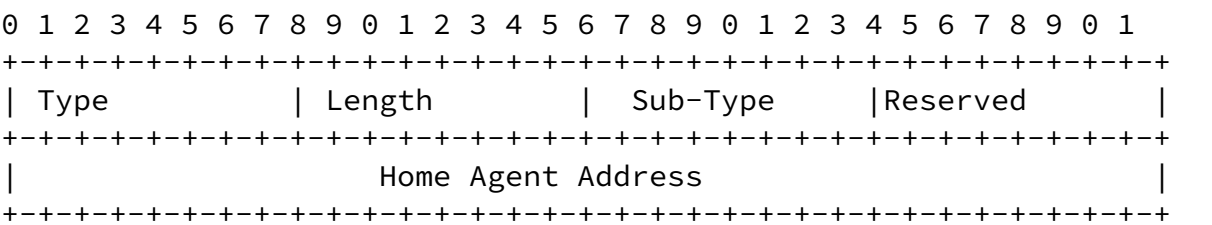
Location detection is done by MIP Proxy and MN is aware of its location as per the response from MIP Proxy. Please see section 2.6.1 for more details.

2.5.2. New Configuration Requirement

A mobile node MUST be configured with the MIPP-Pub, unless dynamic MIPP-Pub discovery is used, which is outside the scope of this draft.

2.5.3. HA Parameter Extension

When a MN registers with the MIP Proxy, it MUST include the non-skippable HA Parameter extension. This extension is used to indicate the IP address of the actual HA to the MIP Proxy. HA address in the extension MAY be set to zero, to request dynamic HA assignment û please see section 2.7.3. for more details.



Type : To be assigned by IANA (non-skippable)

Length :

Indicates the length (in bytes) of the data fields within the extension, excluding the Type and Length bytes.

Sub-Type: To be assigned by IANA

Reserved: For future use.

Home Agent Address: IP address of the MNÆs actual HA

2.6. MIP Proxy Considerations

2.6.1. Algorithm for location detection

MN always communicates to the MIP Proxy (public address), whether on internal or external network. MIP Proxy detects location of MN either by 1) care-of address in the Registration Request or source address if MN registers using NAT traversal or 2) inside or outside interface receiving the Registration Request.

As per #1 above, MIP Proxy does location detection based on care-of-address in Registration Request. Internal addresses (enterprise private and public addresses) are known at the MIP Proxy and so MIP Proxy can determine if the care-of-address is internal. If the Registration Request from MN indicates NAT traversal (mismatch of source and care-of-address), MIP Proxy uses the source address to determine the location of MN.

If the network design can guarantee that internal traffic reaches the MIP Proxy on internal interface and external traffic reaches the MIP Proxy on external interface, then the MIP Proxy can interpret the MNÆs location based on the interface on which it receives Registration Request, as mentioned in #2 above.

Regardless of location detection algorithm, if the Registration Request originates from external network, MIP Proxy forwards the Registration Request to the appropriate HA. If the Registration Request originates from internal network, MIP Proxy rejects the Registration Request with error code 206. This informs MN to use the HA address

specified in HA Parameter Extension.

If MN is registering using dynamic HA assignment (HA address in HA Parameter Extension set to zero) and if MN is registering from internal network, MIP Proxy selects the home agent and puts that address in home agent field in HA Parameter Extension in Registration Reply with error code 206. If MN is registering using dynamic HA assignment from external network, HA includes the home agent address in HA Parameter Extension in Registration Reply (if successful).

If MN receives a Registration Reply with code set to 206, MN interprets as being in internal network and registers directly with the home agent. If MN is behind NAT in internal network, it will register with the specified home agent using UDP tunnel extension. The home agent in this case SHOULD support NAT traversal.

When MN re-registers due to a change in care-of-address, MN always registers with the MIP Proxy and includes the HA Parameter extension. If MN is just renewing its registration, MN registers with HA or MIP Proxy, the entity with which it last registered.

HA Parameter Extension is always present in both Registration Request and Registration Reply.

2.6.2. Simultaneous Mobility Binding

The MIP proxy MAY support simultaneous mobility bindings, regardless of if a MNÆs actual HA supports this feature or not.

When a Registration Request with an æSÆ bit set (i.e. simultaneous binding requested by a MN) is received, the MIP proxy MUST NOT set the æSÆ bit in the new Registration Request, whether or not it support simultaneous mobility bindings.

If the MIP Proxy supports simultaneous bindings and it receives a Registration Request with an æSÆ set, it MUST set the lifetime value in the relayed Registration Request to the maximum of the remaining lifetime values of all existing mobility bindings for this MN and the lifetime value of the new Registration Request received from the MN. Any subsequent

Registration Request refreshes received for any of the existing simultaneous mobility bindings MUST follow the same rule with respect to setting the lifetime value in the Registration Request to be relayed to the MNÆs actual home agent.

When the Registration Reply is received from the MNÆs actual HA, the lifetime value in the mobility bindings list for this MN MUST be set to the lesser value of the accepted lifetime (reflected in the Registration Reply) and the existing lifetime (the request lifetime through the Registration Request) in the mobility bindings list of the MIP proxy.

If the MIP Proxy does not support simultaneous bindings and it receives a Registration with an æSÆ bit set, it MUST send a Registration Reply to the MN as specified in[1].

2.6.3. Mobile IP NAI Extension

The MIP proxy MAY support the Mobile IP NAI extension, specified in [14].

If the MIP Proxy receives a Registration Request whose Home Address is zero and includes the Mobile IP NAI extension, it MUST use NAI instead in its pending registration request list. If the Registration Reply has a non-zero Home Address and includes the Mobile IP NAI extension, the MIP Proxy MUST update its mobility bindings list for this MN, and relay the Registration Reply to the MN.

The MIP Proxy MUST do the following validity checks, if it supports the Mobile IP NAI extension.

- If Home Address is zero in the Registration Request and the MIP Proxy does not support the Mobile IP NAI extension, the MIP Proxy MUST silently discard the Request since there is no SA.

- If the MIP Proxy receives a Registration Request with a value of zero in the Home Address field and no NAI extension, it MUST silently discard the Request since there is no SA.

- If the Registration Reply from the MNÆs actual HA does not include the Mobile Node NAI extension, the MIP proxy SHOULD send the Registration Reply to the mobile node with an error

code indicating MISSING-NAI, as defined in section 2.4.1.

- If the Registration Reply from the MNÆs actual HA includes a zero Home Address or zero Home Agent address, the MIP proxy SHOULD send the Registration Reply to the mobile node with an error code indicating MISSING-HOMEADDR or MISSING-HOME-AGENT, as defined in section 2.4.1.

2.6.4. Dynamic HA Assignment

The MIP proxy MAY support dynamic HA assignment in conjunction with dynamic home address assignment for a MN. If the MN sends a Registration Request with the Home Agent field set to zero in the HA Parameter extension and includes a valid NAI extension, the MIP Proxy can dynamically assign a HA from a pool of HA IP addresses. The selection of a HA is beyond the scope of this draft. The selected HA MUST support the NAI extension in the Registration Request. However, this scheme is NOT intended to support dynamic HA handovers.

2.6.5. Pending Registration List

For each pending registration, the MIP Proxy maintains the following information:

- The IP destination address of the actual HA
- The care-of address in the received Registration Request
- The identification in the received Registration Request
- The lifetime in the received Registration Request, and
- The remaining Lifetime of the pending registration

2.6.6. Mobility Bindings

The MIP Proxy MUST maintain a mobility binding list similar to the one specified in [1] for a HA, in order to forward the registration replies and subsequent MIPv4 data traffic. The MIP Proxy updates its binding table, when a successful Registration Reply is received from an actual HA.

For each mobility binding entry, the MIP Proxy maintains the following information:

- The IP destination address of the actual HA

- The home address of the MN
- NAI if in the received Registration Request
- The care-of address in the received Registration Request
- The identification in the received Registration Request
- The lifetime in the received Registration Request, and

The MIP Proxy MUST also use the same methods defined in [1] for deleting or retiring the entries in its mobility-binding list(s).

2.6.7. Handling ICMP Error Messages

When the MIP Proxy sends a Registration Request to an actual HA on the behalf of a MN, it may receive an ICMP error message indicating that the actual HA is not reachable for a specific reason (i.e., network unreachable, host unreachable, port unreachable, protocol unreachable). If so, the MIP Proxy MUST send a Registration Reply to the MN with Code indicating why the actual HA was not reachable.

2.7. MIPv4 Registration Packet Flow

2.7.1. MIPv4 Registration Request Packet Flow from MN to HA

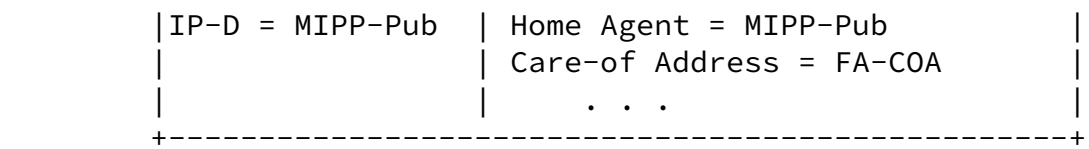
This draft illustrates the sequence from MN to HA via a FA û it can be easily extended to describe the flow for a co-located COA mode MN.

From the MN to a FA:

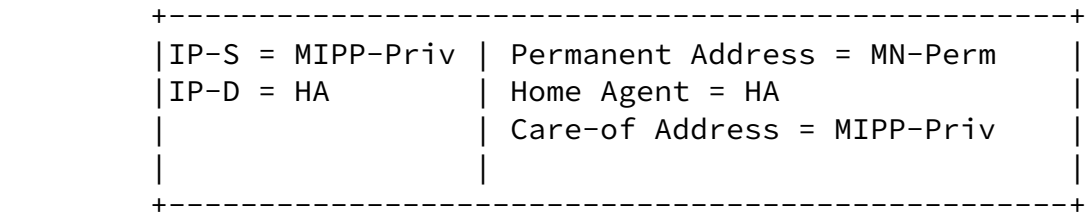
```
+-------------------------------------------------+
|IP-S = MN-Perm    | Permanent Address = MN-Perm  |
|IP-D = FA-Visited| Home Agent = MIPP-Pub         |
|                  | Care-of Address = FA-COA     |
|                  |     . . .                    |
+-------------------------------------------------+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

From the FA to the MIP Proxy:

```
+-------------------------------------------------+
|IP-S = FA-Routed | Permanent Address = MN-Perm    |
```



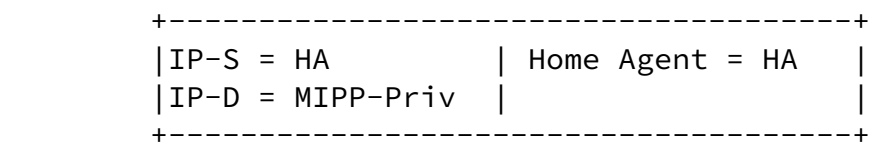
From the MIP Proxy to the actual HA:



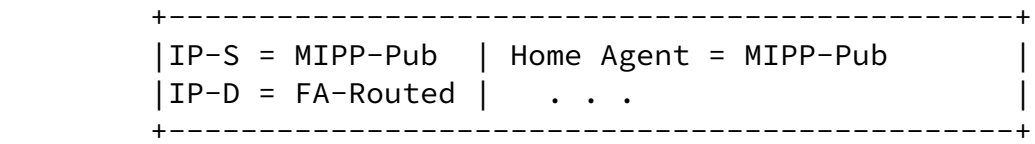
2.7.2. MIPv4 Registration Reply Packet Flow from HA to MN

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

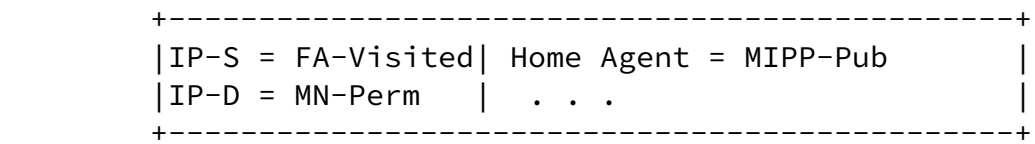
From the HA to the MIP Proxy:



From the MIP Proxy to the FA:



From the FA to the MN:



3. Functions Not Performed By The MIP Proxy

The MIP Proxy MUST NOT perform the following HA functions, as defined in [1]:

- It MUST NOT generate agent advertisements
- It MUST NOT send gratuitous ARPs

- It MUST NOT perform Proxy ARP

- It MUST NOT support Route Optimization [10]

The MIP proxy MUST NOT perform the following MN functions, as specified by [1]:

- It MUST NOT generate agent solicitations or functions pertaining to agent discovery
- It MUST NOT implement any move detection mechanisms
- The MIP Proxy MUST NOT manage registration lifetimes and MUST NOT reinitiate a registration request with the actual HA prior to its expiration.

4. MIP Proxy Integration with VPN

The MIP Proxy as described in this draft is a logical functional entity and as such can be integrated with VPN in 2 possible ways, which are one-box and two-box solutions.

4.1. One-Box Integration

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. Figure 4.1. depicts a network stack resulted from the one-box integration of the MIP proxy with the VPN gateway. Please note that IPsec and the MIP Proxy layers can be combined into one layer (tightly coupled integration), or they can be layered as shown in figure 4.1. (loosely coupled integration).

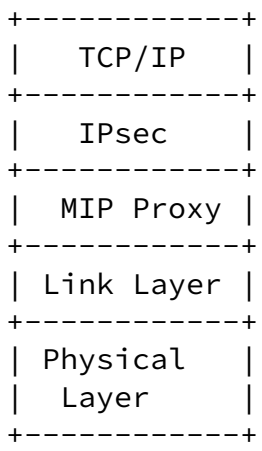


Figure 4.1. û One-Box Integration of MIP Proxy with VPN

4.1.1. Redundancy

A MIP Proxy redundancy protocol is desirable to effect high availability in public and Enterprise deployments, when two box solution approach is used. Details of such a protocol are beyond the current scope of this draft.

4.2. Two-Box Integration

Implemented as a standalone device deployed in parallel with the VPN gateway as depicted in Figure 1.2. 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 a MN and a CN.

4.2.1. Two-Box Integration Requirements

- 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.

- 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.

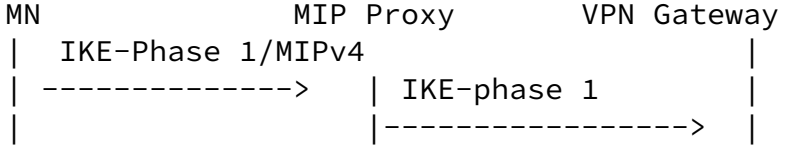
5. MIPv4 Data Traffic Routing Through VPN

This section describes MIPv4 data traffic flow through VPN with the aid of the MIP Proxy. For clarity, this section assumes a two-box solution approach.

5.1. Establishment of Secured MIPv4 Traffic

There are two steps that MUST be successfully completed in order to establish secured MIPv4 traffic between a MN and a CN.

The first step is that the MN MUST complete MIPv4 registration with its actual home agent through the MIP Proxy, as discussed in section 2. The second step is that the MN MUST establish IPsec tunnel SA to the VPN gateway through the MIP Proxy, as shown in Figure 3.a. Any subsequent registration and SA refreshes may occur independent of each other.



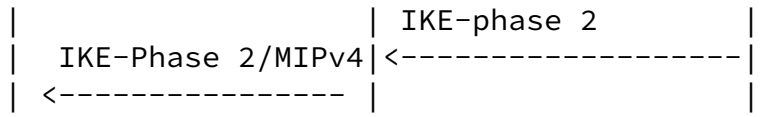


Figure 3.a û IPsec Tunnel SA Establishment
(Two Box Solution)

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

5.2. Association Between VPN Inner and MN Home IP Address

To support continuous mobility and constant reachability, the tunnel inner IP address assigned to a MN MUST be the same as the home IP address.

5.3. MIPv4 Data Traffic from MN on External Network 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 or FA-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 MIP Proxy MUST perform the following validity checks on received MIP data packets whose destination IP address is set to MIPP-Pub (i.e., packets received from outside the DMZ).

- The received packet MUST be encapsulated by an appropriate method (e.g., IP-in-IP, Minimal Encapsulation, GRE) that the MIP Proxy supports
- The inner IP packetÆs destination IP address MUST be set to a VPN gateway IP address that the MIP Proxy supports
- An ESP header MUST follow the inner IP header

If any of above validity checks fail, then the MIP Proxy MUST silently drop the packet.

The packet routing from the MIP Proxy to the CN may differ depending on whether the CN belongs to any of ômobility subnetsö

that the MIP Proxy supports. The following railroad diagrams depict the packet flow sequence for both cases, followed by a description of packets as they traverse the network.

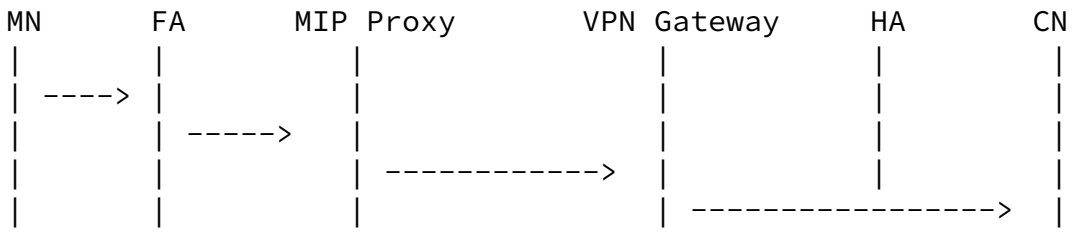


Figure 5.2a – Packet flow from MN to CN, where the CN does not belong to any of "Mobility subnets" that the MIP Proxy supports

From the MN to FA: IP-ESP-IP-Data
From the FA to MIP Proxy: IP-IP-ESP-IP-Data
From MIP Proxy to VPN: IP-ESP-IP-Data
From VPN Gateway to CN: IP-Data

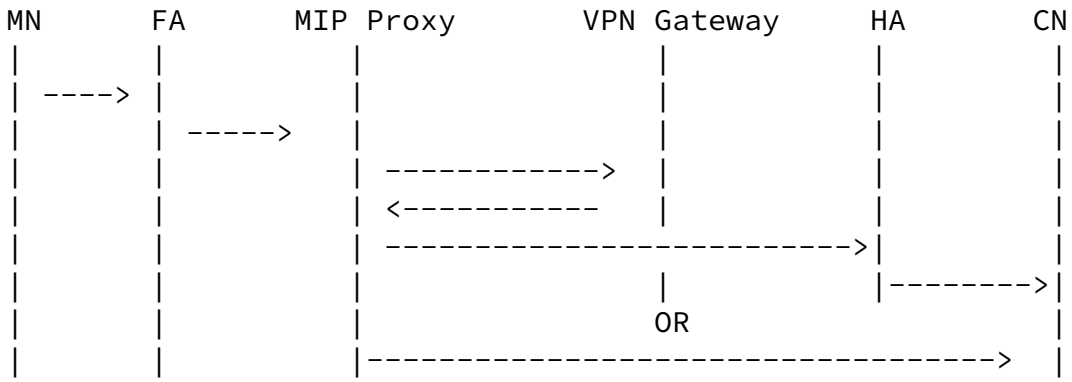


Figure 5.2b – Packet flow from MN to CN, where the CN belongs to a "Mobility subnet" that the MIP Proxy supports

From the MN to FA: IP-ESP-IP-Data
From the FA to MIP Proxy: IP-IP-ESP-IP-Data
From MIP Proxy to VPN: IP-ESP-IP-Data
From VPN Gateway to MIP Proxy: IP-Data
(forwarded back to the MIP Proxy using via Network route installed on the VPN gateway)

Reverse tunneling delivery method is used:

```
-----------------------------------------
From MIP Proxy to HA:     IP-IP-Data
From HA to CN:            IP-Data

Non-Reverse Tunneling delivery method is used:
-----------------------------------------------
From MIP Proxy to CN:     IP-Data
```

The packet flow analysis from the MN to the CN is described below. The analysis assumes that the CN does not belong to any ômobility subnetsö that the MIP Proxy supports.

From the MN to the FA:

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

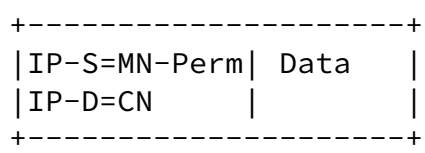
Clearly, the FA does not need to know the IPsec tunnel SA to process the packet. FA only reverse tunnel traffic to the MIP Proxy.

From the MIP Proxy to the VPN gateway:
The MIP Proxy strips off the outermost IP header and forwards the packet (whose destination address is set to VPNGW-Pub) to the VPN gateway.

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

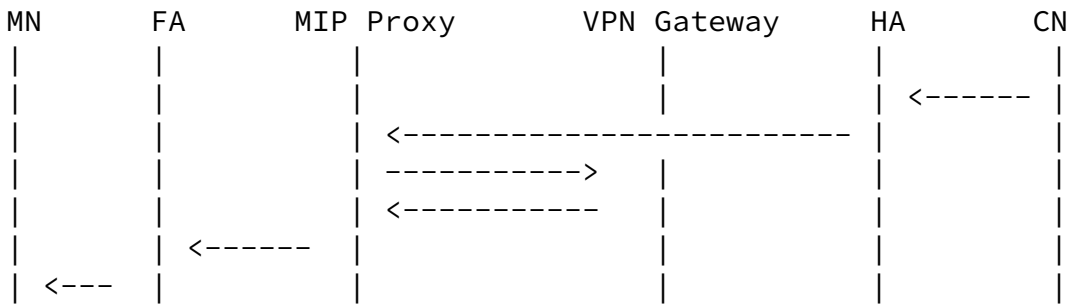
From the VPN gateway to the CN:

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



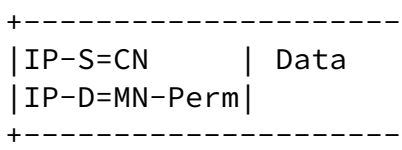
5.4. MIPv4 Data Traffic from CN to MN on External Network

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

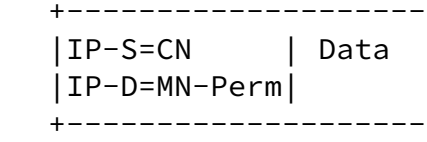
The packet flow from the CN to the MN is described below.
From the CN to the actual HA:



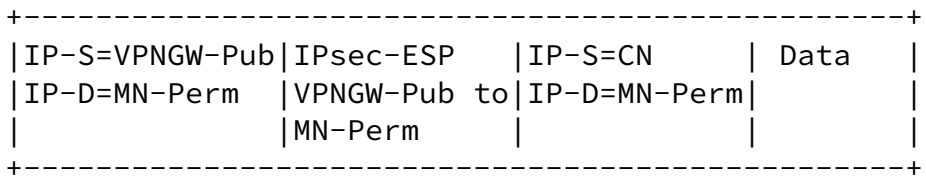
The packet is intercepted by the actual HA, as the MN has moved outside its home subnet.

From the actual HA to the MIP Proxy:

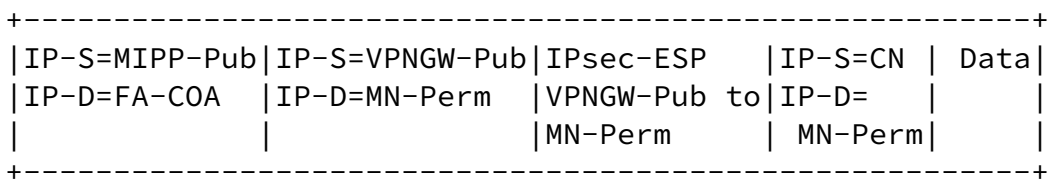
From the MIP Proxy to the VPN gateway:
The MIP Proxy strips off the outermost IP header and forwards the packet to the VPNGW-Priv interface using the corresponding layer-2 address.



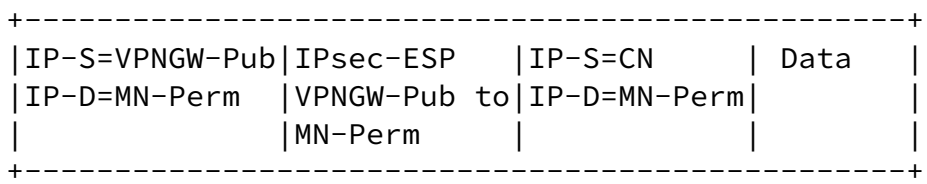
From the VPN gateway to the MIP Proxy:
The VPN gateway applies an IPsec ESP tunnel SA to the IP packet and forwards it back to the MIP Proxy on the MIPP-Pub interface based on its routing table.



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.

5.5. Key Management and SA Preservation

The MIPv4 data traffic routing described in the previous section binds the IPsec tunnel SA to the normally invariant permanent (home) 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 ôretireö the SA if the VPN client is not detected for a period of time. If a 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.

5.6. 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. However the solution should apply to L2TP over IPsec transport [12] and ESP-in-UDP VPN [13] configurations as well.

Note that ESP-in-UDP VPN is not necessary when Mobile IP UDP tunnels [11] are in use.

5.7 Routing Considerations

VPN gateway must insert a route for the home network(s) to point

to the MIP Proxy. This route MUST not be redistributed via an IGP.

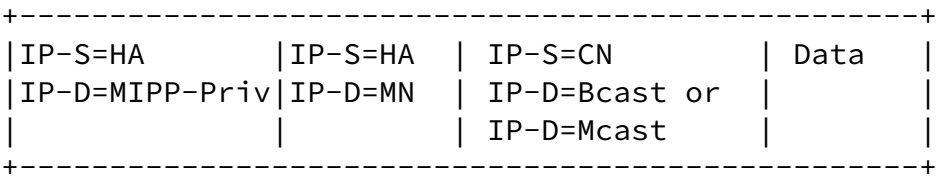
On the MIP Proxy, packets that come from a MIP tunnel (on either the Public or Private interface) must be forwarded (via layer-two mechanism) to the VPN Gateway for IPSec tunnel encapsulation/decapsulation.

5.7.1. Broadcast / multicast Datagrams

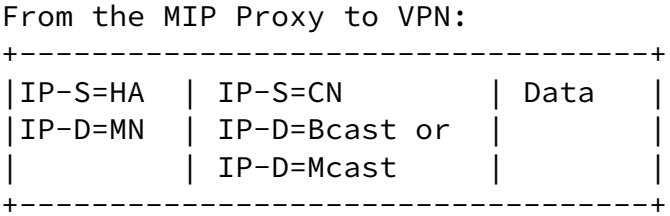
When an actual HA receives a broadcast or a multicast datagram, it forwards the datagram to the MIP proxy for any qualified MNs outside the DMZ.

Since the MIP proxy always unsets the æDÆ bit in a Registration Request that it sends to the actual HA on the behalf of the MN (see section 2.2.1), the actual home agent applies double encapsulation on broadcast or multicast packets that need to be forwarded to the MN, as specified in [1]. When the MIP Proxy receives the double encapsulated packets from an actual HA, it decapsulates the outer IP header, and then forwards the packet to the VPN as shown below.

From Actual HA to the MIP Proxy:



From the MIP Proxy to VPN:



5.7.2. MN Registration through a Trusted FA

A MN may roam into a network served by a trusted FA. The trusted FA refers to a FA that has SA with the VPN-GW or a FA whose hosting network has SA with VPN-GW and an IPsec tunnel

will be established between the FA or its hosting network and the VPN-GW while necessary to protect any traffic between. In this case, the MN MUST use the NAI extension in the FA route advertisement or other mechanisms which are out of the scope of this draft to determine that the FA is a trusted FA. The MN MUST not use the MIP Proxy in this scenario, the FA is responsible for properly tunneling the traffic including the MIP signaling and data through the VPN-GW.

6. MIPv4 Traversal Through IPsec ôNAT and VPNö Gateways

This section extends MIPv4 VPN traversal solution described in section 5 to support MIPv4 traversal across ôNAT and VPNö scenario, in which MN has to traverse one or more NAT gateway(s) followed by a VPN gateway in the path to its final destination.

A solution for MIPv4 traversal across intervening NAT gateways is provided in [11] through a MN/HA protocol extension. The solution cannot be directly applied here, since the MNÆs home agent is not

directly reachable. However, the solution can be leveraged by simply corresponding the MIP Proxy surrogate HA to the HA in [11].

The following sub-sections show MIPv4 control and data packets flow between a MN and a CN.

6.1. MIPv4 Registration Message Flow

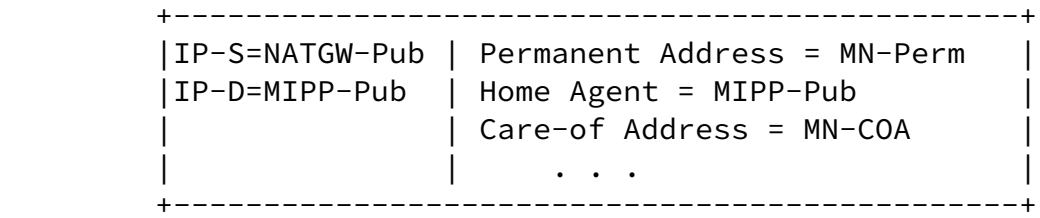
6.1.1. MIPv4 Registration Requests

From the MN to the NAT gateway:

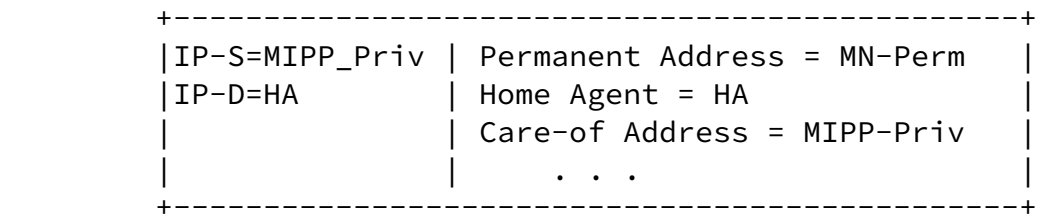
```
+-----------------------------------------------+
|IP-S=MN-Perm   | Permanent Address = MN-Perm   |
|IP-D=MIPP-Pub  | Home Agent = MIPP-Pub         |
|               | Care-of Address = MN-COA      |
|               |   . . .                       |
+-----------------------------------------------+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

Please refer to section 4.5 and the [11] draft for detailed discussion of required registration extensions.

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.

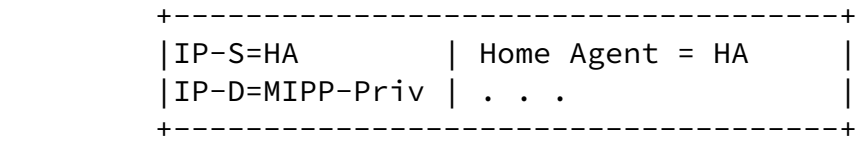


From the MIP Proxy to the actual HA:
The MIP Proxy terminates and authenticates the registration request (as described in previous sections). It then creates a new registration request and forwards it to the actual HA.

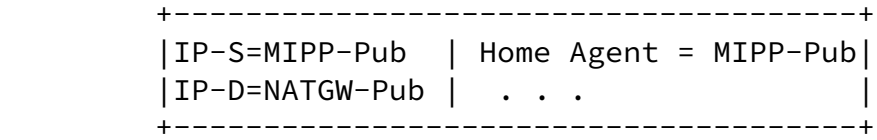


6.1.2. MIPv4 Registration Replies

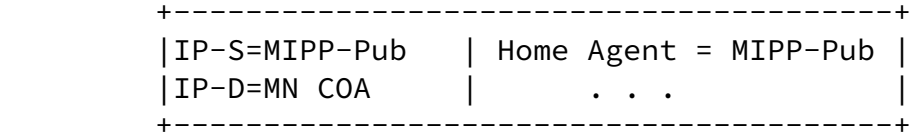
From the actual HA to the MIP Proxy:



From the MIP Proxy to the NAT gateway:



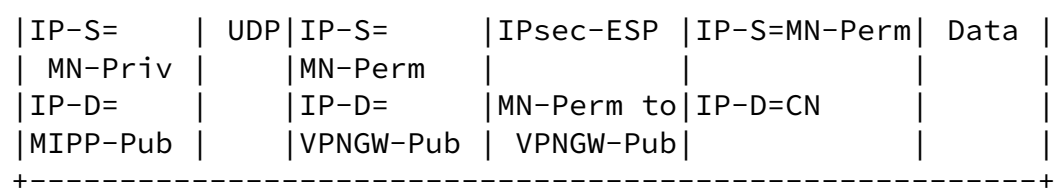
From the NAT gateway to the MN:



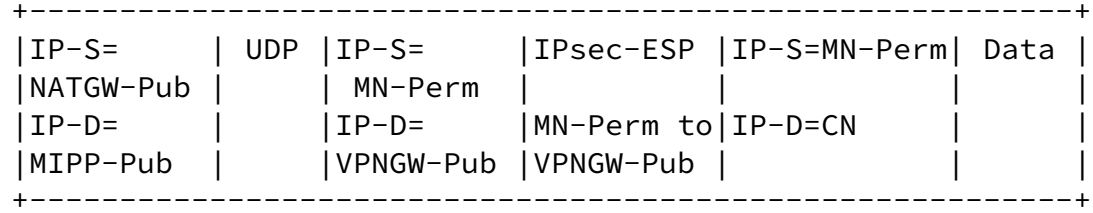
6.2. MIPv4 Data Flow

6.2.1. Data Flow from the MN to the CN

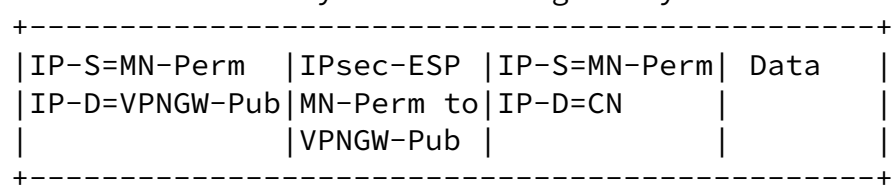
From MN to the NAT gateway:



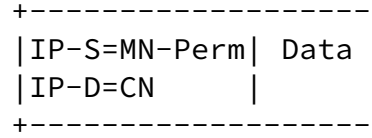
From the NAT gateway to the MIP Proxy:



From the MIP Proxy to the VPN gateway:

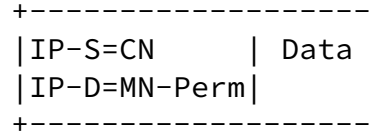


From the VPN gateway to the CN:

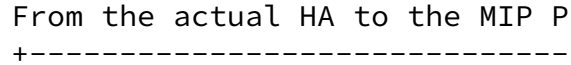


6.2.2. Data Flow from the CN to the MN

From the CN to the actual HA:



From the actual HA to the MIP Proxy:



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

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.

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

From the VPN gateway to the MIP Proxy:

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

From the MIP Proxy to the NAT gateway:

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

From the NAT gateway to MN:

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

7. 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 vulnerability to the mobile IP protocol.

8. Acknowledgements

The authors would like to thank Mike Andrews, Changwen Liu and Ranjit Narjala of Intel Corporation, Sami Vaarala of Netseal, Alexis Oliverean of Motorola for their review and feedback on this draft.

9. Intellectual Property Rights

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

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

10. Revision History

1) Initial Version
9/2001

2) Second Version 3/2002
+ Modified the draft to meet requirements defined in [15]
+ General Clean up
+ Made changes to reflect comments/feedbacks from Sami Vaarala of Netseal, Qiang Zhang of Ecutel, Alexis Oliverean of Motorola

11. References

[1] Perkins. IP mobility support for IPv4. RFC 3220, January 2002
[2] Montenegro. Reverse tunneling for mobile IP. RFC 3024, January 2001
[3] Perkins. Minimal encapsulation within IP. RFC 2004, October 1996
[4] Hanks, Farinacci, Traina. Generic Routing encapsulation. RFC 1701, October 1994
[5] Bradner. Key words for use in RFCs to Indicate Requirement Levels. RFC 2119, March 1997
[6] Rekhter, Moskowitz, Karrenberg. Address Allocation for Private Internets. RFC 1918, Feburary 1996
[7] Droms. Dynamic Host Configuration Protocol. RFC 2131, March 1997
[8] <draft-bpatil-mobileip-sec-guide-01.txt> - Requirements / Implementation Guidelines for Mobile IP using IP Security

[9] Cheshire, Aboba. Dynamic Configuration of IPv4 Link-Local Addresses. <draft-ietf-zeroconf-ipv4-linklocal-03>, April 2002
[10] Perkins, Johnson. Route Optimization in Mobile IP. <draft-ietf-mobileip-optim-11.txt>, September 2001
[11] Levkowetz, Vaarala. Mobile IP NAT/NAPT Traversal using UDP Tunneling. <draft-ietf-mobileip-nat-traversal-01.txt>, March 2002
[12] Patel, Aboba, Zorn, Booth, RFC 3193 û Securing L2TP with IPsec
[13] Huttunen , Dixon, Swander. UDP Encapsulation of IPsec Packets <draft-ietf-ipsec-udp-encaps-02>, April 2002

[14] Calhoun, Perkins. Mobile IP Network Access Identifier Extension for IPv4. RFC 2794, March 2000
[15] Adrangi, Leung, Kulkarni, Patel, Zhang, Lau. Problem Statement and Requirements for Mobile IPv4 Traversal Across VPN Gateways. <draft-ietf-mobileip-vpn-problem-statement-00.txt>, March 2002

Authors:

Farid Adrangi Email: farid.adrangi@intel.com
Phone: 503-712-1791
Prakash Iyer Email: prakash.iyer@intel.com
Phone: 503-264-1815

Intel Corporation
2111 N.E. 25th Avenue
Hillsboro, OR 97124
USA

Kent Leung Email: kleung@cisco.com Phone: 408-526-5030
Milind Kulkarni Email: mkulkarn@cisco.com Phone: 408-527-8382
Alpesh Patel Email: alpesh@cisco.com Phone: 408-853-9580

Cisco Systems
170 W. Tasman Drive,
San Jose, CA 95134

Qiang Zhang Email: qzhang@liqwidnet.com
Phone:703 8641327
Liqwid Networks Inc.

Joe Lau Email: jlau@cup.hp.com Phone: 408 447-2159

Hewlett-Packard Company
19420 Homestead Road, MS 4301
Cupertino, CA 95014