Mobile IP Working Group
INTERNET DRAFT
25 June 1999

Charles E. Perkins
G. Montenegro
Pat R. Calhoun
Sun Laboratories

Private Addresses in Mobile IP

draft-ietf-mobileip-privaddr-00.txt

Status of This Memo

This document is a submission by the mobile-ip Working Group of the Internet Engineering Task Force (IETF). Comments should be submitted to the MOBILE-IP@STANDARDS.NORTELNETWORKS.COM mailing list.

Distribution of this memo is unlimited.

This document is an Internet-Draft and is in full conformance with all provisions of Section 10 of RFC2026. Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

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

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

Abstract

The use of possibly non-unique private addresses (i.e., addresses that are not globally routable in the internet) for mobile nodes, foreign agents, or home agents is not handled by RFC 2002. This document specifies changes to enable Mobile IP to handle such addresses.

1. Introduction

Full-scale deployment of Mobile IP would benefit from an ability to provide mobility across differing address spaces, sometimes called "realms", especially because corporate networks often use private address spaces. A solution is needed to handle such addresses consistently with regionalized registrations and firewall traversal. The mechanisms proposed in this note aim to solve this problem.

We use use the following model:

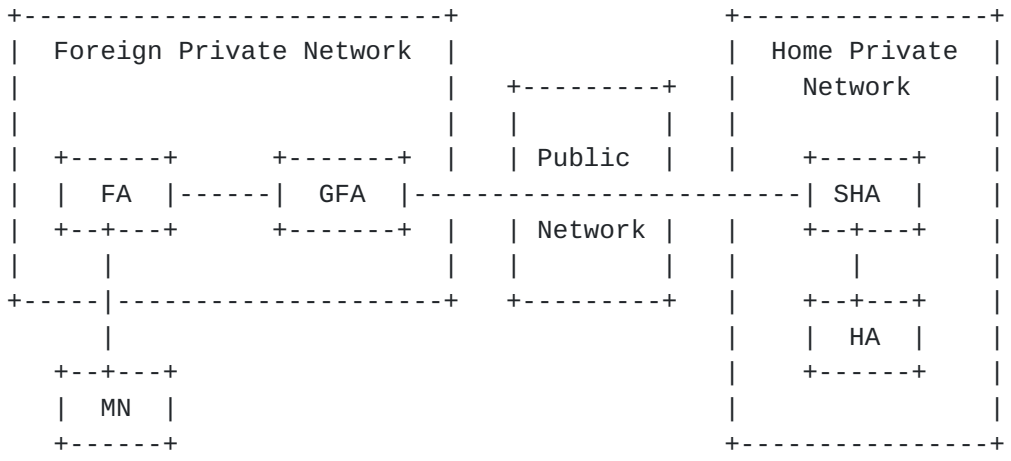

Figure 1: Mobility with Private Networks

A Home Agent using a private address cannot be the destination of any packets transmitted by a foreign agent in a different addressing domain. Thus, such a home agent has to rely on the presence of a Surrogate Home Agent (a SHA). Furthermore, every mobile node on the Home Network served by such a home agent will also have a private address.

This means that Registration Requests for the mobile node have to be sent to the SHA. Then, the SHA has to know how to forward such requests to the home agent.

In this document, the GHAA (Global Home Agent Address) is defined to be either the HA, if the HA has a globally routable IP address, or else the SHA, if the HA does not have a globally routable IP address.

Mobile IP has two distinct phases:

1. tunnel setup via a UDP-based (registration) protocol, and

2. data transfer via tunneled packets.

2. Data Transfer

Let's examine first the data transfer phase. Given that only systems within the same address space have direct reachability, the packets do not travel along an end-to-end tunnel. Instead, the tunnel from HA to FA is a compound tunnel, used as in a previous proposal, Tunnel Establishment Protocol (TEP) [2].

The segments of the tunnel are always within any given address space. If the home agent has a private address, there are 3 tunnel segments:

HA->SHA, SHA->GFA, and GFA->FA

Otherwise, if the home agent has a globally routable IP address, only two tunnel segments are necessary:

HA->GFA and GFA->FA

It is also possible that additional tunnel segments will be needed between the GFA and the FA, but setting up such additional tunnel segments is outside the scope of this document.

The order and endpoints of the compounds tunnels are reversed when packets flow in the reverse direction. Data transfer, then, proceeds from the correspondent node to the home agent through the SHA along to the FA in the manner to be described next. In this section, MN refers to a particular mobile node which needs to receive data at a particular care-of address, which may itself be a private address from a separate address space than the one from which MN's IP address is allocated.

In sections 2.3 through 2.5, the IP node sending the packet the GFA is designated as the GHAA, as defined in section 1.

2.1. From HA to SHA

Say a correspondent node CN (not shown in figure 1) sends a packet to MN. If the home agent (HA) has a private address, then it MUST know the address of a SHA, and MUST cause the tunneled data packet to the MN's care-of address to seem to originate from the SHA. The HA first encapsulates the packet with an IP header that indicates that origination. Then, the HA encapsulates it and sends it towards SHA as illustrated in figure 2.

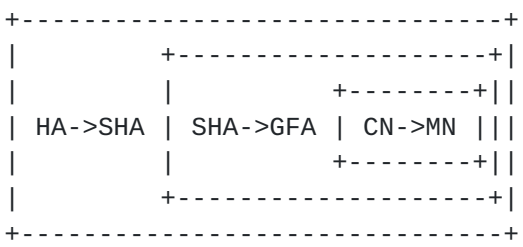

Figure 2: IP-in-IP tunneled packet from HA to SHA

2.2. From SHA to GFA

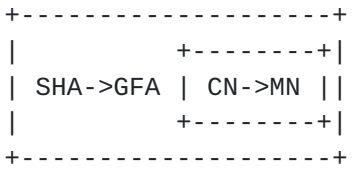

Figure 3: IP-in-IP tunneled packet from SHA to GFA

Once the packet reaches SHA, the packet is decapsulated, exposing the still encapsulated packet with SHA as the source IP address. The packet from SHA to GFA is illustrated in figure 3.

2.3. From GFA to FA

When GFA decapsulates the packet, it looks for a binding for MN, the inner destination. Following the discussion in [6], MN's IP address does not necessarily uniquely identify the mobile node. The reason is that the GFA may have another binding in place for a mobile node from another private address space that is using the same IP address as MN. The GFA has to identify the correct visitor list entry based on a tuple (i.e., an ordered set of information) which is guaranteed to be unique. One such tuple sufficient for demultiplexing IP-within-IP packets [7] (protocol 4) is (MN,GHAA), where:

- MN is the destination IP address of the innermost header, and

- GHAA is the source IP address of the encapsulating header.

The destination IP address of the innermost header is the mobile node's home address. The source IP address of the encapsulating header is GHAA. The ordered pair (MN,GHAA) is presumed unique among all of GFA's Mobile IP clients.

GFA requires (MN,GHAA) to fetch the next tunnel endpoint, FA. This tuple continues to be required for any foreign agent beyond GFA, as such agents MAY reside in a separate address space from MN's home address. Accordingly, GFA encapsulates again so that GHAA will still be visible in the intermediate header. The packet that arrives at FA is illustrated in figure 4.

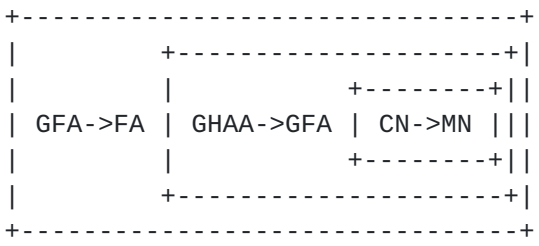

Figure 4: IP-in-IP tunneled packet from GFA to FA

2.4. From FA to MN

Before delivering the packet to the mobile node, the FA MUST check that the outer source IP address (GFA) matches the intermediate destination IP address. The FA MAY require that the same GFA always be associated with the MN, by storing this information in its routing table. Note that a routing loop would result from indiscriminately forwarding the decapsulated packet after the outer (GFA->FA) header was removed, because the GFA would keep doing the same thing to the packet. RFC 2002 includes language to prohibit this indiscriminate forwarding, and the mobility agents handling private addresses require at least as much care as RFC 2002 mobility agents when dealing with encapsulation.

Like the GFA, the FA searches based on (MN,GHAA). Once the FA identifies the ultimate destination of the packet, MN, it delivers the packet using link-level mechanisms.

2.5. Using GRE tunnels

GRE packets with a Routing field are outside the scope of this document. GRE packets [4, 5] (protocol 47) without a Key field are only handled if their Protocol Type field has a value of 0x800 (other values are outside the scope of this document), and can be demultiplexed based on the same tuple (MN,GHAA) as IP-within-IP packets. GRE packets with a Key field could be demultiplexed based on that field used as a tunnel identifier [2] negotiated at registration time.

Question: how is the tunnel identifier negotiated?

In this case, by absorbing the cost of negotiating the tunnel identifier and setting up the necessary routing for the GRE header, extra encapsulation steps can be avoided by providing a single GRE header, as illustrated in figure 5.

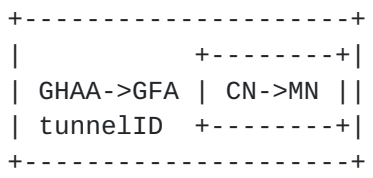

Figure 5: GRE tunneled packet from GFA to FA

3. Tunnel Establishment

Even if the HA cannot address FA directly, the HA has to send tunneled packets so that they eventually arrive at the FA so that the FA can deliver them to the mobile node. These packets are delivered via GHAA and GFA. Configuring this tunnel is initiated by the Mobile IP Registration Request message, as defined in [8].

If mobile node MN is registering with home agent HA, the GFA should be used as the care-of address, because the GHAA sends packets to MN via GFA.

The mobility agents FA and GFA create the mapping (MN,GHAA) for each mobile node. This information is available from the registration messages. If the mobile node has acquired a co-located address, any foreign agent issuing agent advertisements MUST use the 'R' bit to force the mobile node's Registration Request to go through it. If a mobile node using a co-located address is not receiving any advertisements, then one of two things must be true:

- the co-located care-of address is globally routable, or

- the mobile node discovers the GFA; the protocol for this discovery operation is not specified within this document.

3.1. Privately Addressed Mobile Nodes

Foreign agents that comply with Mobile IP as specified in RFC 2002 are not required to handle mobile nodes with private IP addresses. Doing so requires additional mechanism, because it is possible for two mobile nodes to show up with the same identical private IP address. Fortunately, at least delivery from the foreign agent's network interface to the mobile node will still be possible, based on the MAC address of the mobile node. However, once the Foreign Agent has decapsulated the packets it receives for the mobile node(s) with a duplicated private IP address, it cannot determine which mobile node should receive the packet based only the value of the destination IP address (MN) in the inner IP header,

In order to handle private addresses, a Foreign Agent MUST be able to identify its visitor list entry for the mobile node by using (MN,GHAA) as defined in section 2.3. Pending Registration Requests using private addresses MUST be able to be identified by using the the Identification field along with either:

- the NAI [1] supplied by the mobile node, or

- (MN,GHAA)

A new `P' bit is defined, from the currently reserved field of the Agent Advertisement defined in RFC 2002 [8], for use by Foreign Agents that have the mechanisms specified herein. If the mobile node has a private address, then it SHOULD send registration requests only to a foreign agent that has advertised the ability to handle private addresses by setting the `P' bit. If the mobile node has a private address, then it SHOULD include the NAI extension [3] in its Registration Request.

When a Registration Reply is determined to match a request from a Mobile Node (MN) with a private address, the foreign agent MUST associate GHAA with its (new) visitor list entry for MN.

DISCUSSION:

cep: I am not surewe should tie together the NAI with the use of private addresses in this way. And, I think that the

FA has to advertise its willingness to handle such nasty, unfriendly things such as private addresses.

cep: We could make the home agent append a Private Address extension to the Registration Reply, in the range 128-255. That would avoid making the mobile nodes have to be smart, and it would avoid requiring the foreign agents make the more difficult routing determination for mobile nodes with unique IP addresses.

3.2. Privately Addressed Home Agents

Suppose the home agent has a private address. Then, the home agent MUST perform the encapsulation steps specified in section 2.1. The mobile node MUST be able to discover the address of its SHA. This discovery MAY occur in one of the following ways:

1. The home agent can advertise an SHA's address in advertisements received by the mobile node when the mobile node is at home. This document does not specify any method by which a home agent can advertise a SHA.

2. The SHA can be returned in the Home Agent field of the Registration Reply, when the mobile node asks for dynamic allocation of a Home Agent.

3. The mobile node can be statically configured to contain the address of a SHA, at the same time that it is configured with a security association with a home agent or with a home AAA server.

3.3. Foreign Agents with Private Addresses

A foreign agent with a private address SHOULD NOT advertise its care-of address within its agent advertisements (beacons), because the beacons are assumed to offer connectivity for mobile nodes that may belong in a different addressing domain. Instead, it SHOULD advertise a care-of address that is reachable by the GHAA. This globally reachable care-of address is associated with a distinguished foreign agent known as the Gateway Foreign Agent (GFA).

DISCUSSION:
The FA could use one of three methods to indicate to the mobile node the necessary information about the foreign domain/GFA:

- can advertise FA@domain

- can advertise GFA

- can reject registration and send GFA

If the foreign agent advertises a care-of address which is not associated with one of its own network interfaces, the mobile node must be given some other method to detect when it moves to a different foreign agent. A foreign agent advertising a GFA as its care-of address SHOULD use the FA-NAI extension, specified in section 4.

In order to advertise the GFA as a care-of address, the foreign agent has to find find out what it is. This MAY be done by any of the following methods:

1. The GFA can list its care-of address in advertisements received by the foreign agent.

2. The GFA can be returned in the Care-of Address field of the Registration Reply. This requires that the care-of address be made known to the home agent, in order for the Registration Reply to be properly authenticated.

3. The foreign agent can be statically configured to contain the care-of address of a GFA.

   [gab - does an MN need to know the GFA?. maybe not. just issue the request with care-of address 0 and have the FA figure it out via AAA or whatever, precisely as outlined in the next section.]

This document does not (yet) specify any method by which the home agent may obtain the GFA's globally routable care-of address.

3.4. Alternative GFAs

If a foreign agent has access to multiple GFAs, the appropriate GFA for a particular mobile node MAY may be selected depending upon the NAI given by the mobile node, or the home agent address given by the mobile node. In this case, the foreign agent MAY advertise a care-of address of zero, and include the FA-NAI extension specified in section 4. When the mobile node first attempts to make a connection in a particular foreign domain, it is typically unaware of any nearby care-of address. When the foreign agent advertises a zero care-of address, the care-of address that the mobile node uses during its initial registration MUST be zero. Before the Registration Request reaches the home domain, the care-of address (say, of a GFA), MUST be inserted by an agent (call it AAAX) trusted and authenticated by the home domain, or an associate in the foreign domain trusted and

verified by AAAX. The home agent, then, includes that care-of address in the Registration Reply, for subsequent use by the mobile node.

DISCUSSION:

This should perhaps go into a separate document. It could depend on AAA. We need to define error numbers for the following cases:

- nonzero COA at private FA

- zero COA at GHAA

3.5. Protocol between SHA and HA

In this section we assume that the home agent has a private address, and thus that every packet tunneled to the mobile node has the IP address of the SHA as the source IP address in the tunnel header.

If a SHA receives a Registration Request, and it is not the home agent for the initiating mobile node, the SHA has to have an entry for the mobile node and a record of the associated home agent in its home list. This record can be created in the following ways:

1. Manual configuration

2. The SHA can receive a Registration Request from a AAA agent in the home domain (call it AAAH) during the initial registration sequence for the mobile node in the foreign domain. In this case, the AAAH will send the address of the appropriate home agent along with the Registration Request.

When the home agent receives a data packet for delivery to the mobile node, the home agent MUST first deliver this packet to the SHA. It does this by iterated encapsulation:

1. Encapsulate using the care-of address as the tunnel destination and the SHA as the tunnel source address, and then

2. Encapsulate using the SHA as the tunnel destination and the home agent's private address as the tunnel source address

When the SHA receives this tunneled packet, it only has to remove the outermost IP header from the packet and forward the (still at least singly encapsulated) result to the care-of address.

4. Foreign Agent NAI

The Foreign Agent NAI Extension to the Agent Advertisement contains the foreign agent's host name following the format defined in [1]. The NAI is used to identify the foreign agent and can be used by a mobile node to determine whether or not it has moved out of the domain in which its previous foreign agent was configured to provide mobility service.

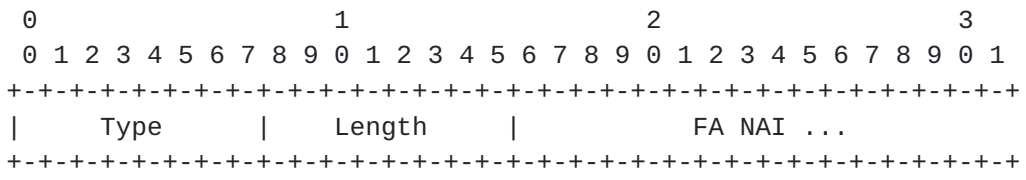

Figure 6: The FA NAI Extension

Type TDB

Length The length in bytes of the FA NAI field

FA NAI Contains the foreign agent's NAI in the format defined in [1].

5. Security Considerations

Since private addresses are typically administered to prevent access to networks inside an enterprise, privately addressed mobile nodes with Mobile IP must be handled with great care to avoid break-ins. For instance, the mobile node should probably not offer any IP forwarding services while registered at an external care-of address. It is difficult to imagine how forwarding traffic between the foreign and home domain could be logically consistent with the raison d'etre for the private address space in the home domain.

The SHA and GFA offer access mechanisms into a private address space. Packets sent to the SHA or GFA for further handling may, therefore, require authentication and possibly encryption to maintain the existing security policy which originally dictated the choice of using a private address space within the enterprise.

6. IPv6 Considerations

It is hoped that IPv6 will not offer any such private addresses as have been brought about by perceived unavailabilty of enough IPv4 addresses.

References

[1] B. Aboba and M. Beadles. RFC 2486: The network access identifier, January 1999. Status: PROPOSED STANDARD.

[2] P. Calhoun and C. Perkins. Tunnel Establishment Protocol (TEP). draft-ietf-mobileip-calhoun-tep-00.txt, December 1997. (work in progress).

[3] Pat R. Calhoun and Charles E. Perkins. Mobile IP Network Address Identifier Extension. draft-ietf-mobileip-mn-nai-01.txt, February 1999. (work in progress).

[4] Stan Hanks, Tony Li, Dino Farinacci, and Paul Traina. Generic Routing Encapsulation (GRE). RFC 1701, October 1994.

[5] Stan Hanks, Tony Li, Dino Farinacci, and Paul Traina. Generic Routing Encapsulation over IPv4 networks. RFC 1702, October 1994.

[6] G. Montenegro. Negotiated Address Reuse (NAR). draft-montenegro-aatn-nar-00.txt, May 1998. (work in progress).

[7] Charles Perkins. IP Encapsulation within IP. RFC 2003, May 1996.

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

Addresses

The working group can be contacted via the current chairs:

Erik Nordmark
Sun Microsystems, Inc.
17 Network Circle
Menlo Park, California 94025
USA

Phone: +1 650 786-5166
Fax: +1 650 786-5896
E-mail: nordmark@sun.com

Basavaraj Patil
Nortel Networks Inc.
2201 Lakeside Blvd.
Richardson, TX. 75082-4399
USA

+1 972-684-1489

bpatil@nortelnetworks.com

Questions about this memo can be directed to:

Charles E. Perkins
Sun Microsystems Laboratories
15 Network Circle
Menlo Park, California 94025
USA

Phone: +1-650 786-6464
EMail: cperkins@eng.sun.com
Fax: +1 650 786-6445

Pat R. Calhoun
Sun Microsystems Laboratories
15 Network Circle
Menlo Park, California 94025
USA

Phone: +1 650-786-7733
EMail: pcalhoun@eng.sun.com

Gabriel Montenegro
Sun Microsystems Laboratories
15 Network Circle
Menlo Park, California 94025
USA

Phone: +1-650-786-6288
EMail: gab@eng.sun.com