MIPv6: from hindsight to foresight?

<draft-nordmark-mobileip-mipv6-hindsight-00.txt>

Status of this Memo

This Internet Draft expires May 14, 2002.

Abstract

This document captures the authors personal opinions and is intended to serve as input to the discussion in the Mobile IP Working Group. It proposes several, in may cases completely independent, things which might be deemed radical changes to Mobile IPv6 based on watching Mobile IPv6 evolve over the last 5 years.

Contents

1. INTRODUCTION

The Mobile IPv6 specification has evolved incrementally over at least 5 years. During that time several things have changed that could be used to provide additional benefits for mobile IPv6.

An example is IP tunneling which was first specified for Mobile IPv4. Since then the understanding of IP tunneling has increased significantly over the years due to being used for both IPsec and IPv6 transition. This has lead to a greater understanding of e.g., the security issues in decapsulating packets.

This document proposes a set of largely independent changes to Mobile IPv6 that are on the author's "wish list". Many of the changes can be viewed as just using a different packet format to encode the same information thus the impact on implementations might not be that large as one would otherwise think. But it is the author's opinion that these changes make the protocol fit better with other IP protocol hence easier to understand. The hope is that this will reduce the probability of implementation problems relating to robustness, security, etc.

If the working group thinks these simplifications are worth-while it would make sense to apply them before Mobile IPv6 becomes a proposed standard. Delaying this type of "cleanup" until after there is a mobile IPv6 standard is not likely to be beneficial since then one would have to be concerned with compatibility between the old and the new scheme, carry around the code for the old scheme, etc. Thus it makes sense for the WG to look carefully at these suggestions and make a conscious decision whether to reject them or accept them, and not try to postpone this discussion until later.

These ideas are not mine alone - most of them have been suggested by others on the Mobile IPv6 or IPNG mailing lists over the years but have not resulted in much of discussion.

With one notable exception the suggested changes do not change the set of features available in Mobile IPv6. The exception is the suggestion to remove the "update of previous default router" which, in the author's opinion, is a pre-mature optimization. Given the "securing binding updates in the absence of a global PKI" discussion that the working group is having it less clear than ever whether the use of the previous default router as a temporary Home Agent for the previous Care of Address will reduce the packet loss due to handoffs - securely updating the previous default router is likely to take at least one round-trip time and which point the number of packets in transit between the CNs and MN's old CoA is likely to be very small. In any case, there are separate efforts to make handoffs smoother.

1.1. Goals and Requirements

The goals for the proposed changes are:

- Simplify things to the extend possible without loosing functionality.

- Use existing protocol mechanisms such as tunneling. In general make Mobile IPv6 less different than other existing protocol mechanisms.

- o Allow IPsec to be used to authenticate control traffic in the cases when a trust relationship exists e.g. between the MN and its HA.

- o Address the concerns about the use of routing headers and home address options expressed in [RH-HA].

1.2. Proposed Changes

Replace the binding update specific piggybacking in [MIPv6] with generic end-to-end piggybacking i.e. the ability to send two IP packet payloads in a single IP packet.

Make the Mobile IPv6 control packets (Binding Request, Update, Acknowledgement, etc) use either a UDP port, new ICMP types, or a new payload type.

Replace the use of the Routing Header in Mobile IPv6 with IPinIP tunneling. Specify a new tunneling header which omits the source address since, in this case, the conceptual outer source address and inner source address are identical. The resulting header adds 24 bytes to the packet which is the same as a the size of the routing header and it allows sites and hosts to have separate security policy for processing these headers than processing routing headers as [RH-HA] suggests they need.

Replace the use of the Home Address option conceptually with tunneling. Avoid an increase in packet size by specifying a new tunneling header which omits the destination address, since in this case the inner and outer destination addresses would be identical.

For mobile to mobile communication, where both a routing header and a home address option is used today this conceptual use of tunneling just becomes regular IPinIP tunneling since in that case all four IPv6 need to be carried; two care of addresses and two home addresses in each packet.

There is also one idea that could be added to Mobile IPv6 at a later stage, which is to make the movement detection more explicit. The idea is to configure the routers on each link to advertise a single global IPv6 address as the "identity" of the link in each Router Advertisement. This can be done by defining a new Neighbor Discovery option. Thus a Mobile Node when it receives a Router Advertisement can immediately tell whether it has moved - the global identity will be different for each link.

2. GENERIC END-TO-END PIGGYBACKING

This is based on the work in [PAYLOAD].

The idea is to define a new extension header that is capable of carrying multiple IP packet payloads between a pair of IP addresses, that is defined such that IPsec can be used independently on the different payloads. Thus it would be possible to have a mobile IPv6 control packet protected by ESP and a TCP SYN packet without any IPsec protection in the same IP packet.

2.1. Piggybacking Packet Format

Extracted from [PAYLOAD].

```
        0              7 8            15 16                            31
        -----------------------------------------------------------------
        |               |               |                               |
        |    Nxt Hdr    |  Int Nxt Hdr  |            Length             |
        |               |               |                               |
        -----------------------------------------------------------------
        |                                                               |
        |    Data  (Length octets) ...                                  |
        |                                                               |
        |                          /------------------------------------|
        |                         /       Trailing Padding              |
        -------------------------/---------------------------------------
```

IP Fields:

Nxt Hdr
The payload type for the header that follows the trailing padding.

Int Nxt Hdr
The payload type for the Data field.

Length
The length of the Data field in octets.

Data
Some payload of type "Int Nxt Hdr".

Trailing Padding
If the length of the whole extension header is not

a multiple of 8 octets this field will be present so that the total length of the extension header becomes a multiple of 8 octets.

Note that [PAYLOAD] defines the above format as the `General Payload Header'' (GPH) and also defines the ``Aligned Payload Header'' with 32 bits of reserved field between the length field and the data field. The reason for this is to provide different alignment with respect to the beginning of the Data field.

2.2. Sending Payload Headers

When a sender sees a benefit of using piggybacking it can include multiple payloads in the packet independent whether the payloads use IPsec or not.

However, some firewalls might drop any packet containing the payload header and other firewalls will drop such a packet if any of the contained payloads violate the security policy. Hence this form of piggybacking SHOULD NOT be used when retransmitting packets since that could result in repeated retransmissions all being dropped by a firewall when individual packets would make it through.

The payload header, when sent, SHOULD be placed after any fragmentation header but before any IPsec headers.

2.3. Processing Received Payload Headers

Conceptually the processing of a payload header can be described as using the payload header to create two separate IP packets and processing those packets independently.

This can be described as forming two IPv6 headers (and other headers like HopByHop options that precede the payload header) and appending the payload from the Data field in the payload header to one of the headers and the appending rest of the packet to the other header. Finally adjusting the IPv6 payload length for the two headers.

Note that in general there can be more than one payload header per packet in which case this simple way of describing the processing needs to be recursive.

Once the two packets have been generated they are processed as they had just been received from the link-layer i.e., any IPsec processing takes place on the individual packets.

3. NO MORE DESTINATION OPTIONS IN MOBILE IPv6

The use of Destination options for Binding Update and other MIPv6 control messages allowed the use of Binding Update specific piggybacking. With the introduction of the generic end-to-end piggybacking above there is no longer such a need. Thus it makes sense to make the Mobile IPv6 control messages use a protocol that allows them both to be treated separately by IPsec [IPSEC-SA] implementations, and make it easier to implement this processing separately from the main "ip_input" code path.

This can be accomplished by using UDP or by using one or more new ICMP types (assuming IPsec implementations support selecting on ICMP types; it is not required according to [IPSEC-SA]), or by defining a new payload/protocol type for this purpose.

4. USE REGULAR TUNNELING BETWEEN MOBILE NODES

Currently when two mobile nodes are communicating using route optimization the packet ends up containing a destination options extension header with a home address option, which gets padded out to 24 bytes, and a routing header which is also 24 bytes. The suggestion to conceptually use tunneling instead means that for this mobile to mobile communication an extra IPv6 header is all that is needed. In addition to the conceptual simplifications of using tunneling there is an added bonus in this case; saving of 8 bytes per packet.

5. IP TUNNELING WITH REDUNDANT SOURCE OR DESTINATION ADDRESSES

When IPinIP tunneling is used [TUNNEL] the packet ends up containing four IP addresses. However, when sending packets between a non-mobile CN and a MN there is only need for three IP addresses; for packets from the CN to the MN there needs to be a source address, the CoA of the MN, and the Home Address (HoA) of the MN. Similarly, from packets from the MN to the CN the same set of addresses are needed but the source and destination sense of them is inverted.

5.1. Three Address Tunneling Packet Format

The message format is the same for the two cases. Which one is used is identified by the Next Header value in the previous extension header. The two values are:

```
   IPinIPnoSRC     TBD [Assigned by IANA]
```

IPinIPnoDST   TBD [Assigned by IANA]

```
       0                   1                   2                   3
       0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
      +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
      |  Next Header  |   Length = 3  |           Reserved            |
      +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
      |                            Reserved                           |
      +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
      |                                                               |
      +                                                               +
      |                                                               |
      +                              Address                          +
      |                                                               |
      +                                                               +
      |                                                               |
      +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

TBD: Does it make sense to include transport class and flowid in the reserved fields above?

5.2. Sending Rules

A possible sending rule is that based on the assumption that the sender somehow knows that the receiver supports both [TUNNEL] and the above two new payload types. For Mobile IPv6 once could just require that all nodes participating in Mobile IP (i.e. the same set of nodes that support the Home Address Option and Route Optimization today) also support encapsulation including the two new extension headers. Presumably Mobile IPv6 needs a mechanism, such as an ICMP error, to detect when a receiver does not support the home address option. A similar mechanism could be used to detect that a receiver doesn't support these headers. When the headers are not supported then in the case of sending packets from a MN, the only choice would be to reverse tunnel the packet through the HA. When sending packets to a MN after establishing a Binding Cache Entry it would be a more or less fatal error if the MN did not support the IPinIPnoSRC payload type.

When sending a packet through a conceptual tunnel as described in [TUNNEL], and the sender has reason to believe that the receiver, it would compare the inner source with the inner destination as well as the outer source and outer destination addresses. If the source addresses match it would use a IPinIPnoSRC extension header with the "Address" field in the extension header being the inner destination address (the Home Address when sending to a MN). If the destination

addresses match the sender would use a IPinIPnoDST extension header with the "Address" field being the inner source address (the Home Address when sending a packet from a MN). If neither addresses match then a regular [TUNNEL] packet would be sent.

5.3. Receiving Rules

A conceptual way of describing the receive side behavior is to expand the above extension headers to a regular IPinIP header and then process that IPinIP header by the usual rules. Such a scheme allows the sending implementation to use IPinIP in all cases and the use of IPinIPnoSRC and IPinIPnoDST are optimizations that the sender can use to save bytes on the wire.

For IPinIPnoSRC this step involves replacing the IPinIPnoSRC header with an IPinIP header and copying the source address from the outer IP header into that new header while copying the Address field in the IPinIPnoSRC to the destination field in the new header and updating the payload length etc.

The same step for IPinIPnoDST just copies the outer IP destination into the new inner header and takes the new inner header source from the above Address field.

5.4. When to Accept Tunneled Packets

When Mobile IPv6 is using tunneling a conservative approach security-wise would be to only accept the tunneled packets, unless the node has other policies that are more permissive, based on the content of the Binding Cache and Binding Update List [MIPv6].

Packets where the inner and outer source match and the inner and outer destinations differ, whether or not IPinIPnoSRC or IPinIP was used to deliver the packet, SHOULD only be accepted if all of these are true:

- o The <outer destination, inner destination> is the CoA and HoA for an entry that is in the Binding Update list. Thus only nodes that have been sent an unexpired binding update should be tunneling such entries towards the node.

- o The outer destination and inner destination belong to the same zone [SCOPED-ARCH]. The reasons for this is in [RH-HA].

- o If the receiver is a security gateway i.e. treats some network interfaces as being on the "inside" and others as the "outside"

(or perhaps has more that two such "domains") it SHOULD also verify that the inner and outer destinations are in the same such "domain".

Packets where the inner and outer destinations match and the inner and outer sources differ, whether or not IPinIPnoDST or IPinIP was used to deliver the packet, SHOULD only be accepted if all of these are true:

- The <outer source, inner source> matches a <CoA, HoA> in the Binding Cache. This restriction says that only nodes that have managed to securely create a Binding Cache entry in the correspondent can send packets directly to it using this form of tunneling. If this is not the case an MN needs to tunnel packets through the home agent so the packets will delivered to the CN without any tunneling header.

Packets where both the inner and outer source and destinations are different SHOULD only be accepted if all of these are true:

- The above rules in the case of matching destinations are satisfied.

- The above rules in the case of matching source addresses are satisfied.

When a packet is dropped because it does not satisfy the above requirements an ICMP error (type and code TBD) should be sent back to the outer source address. This message is then used by the sender to detect e.g. when a CN has garbage collected a Binding Cache entry. [TBD: This makes packet delivery depend on ICMP errors not being discarded by firewalls! If this is an issue an option is to not allow CNs to garbage collect binding cache entries until the lifetime expire.]

Packets where both the inner and outer source and destinations are the same SHOULD be dropped.

6. EXPLICIT MOVEMENT DETECTION

Note that unlike the other ideas presented in this document this particular one can presumably be done at a later point in time. But it would simplify the Mobile Nodes if they could use this movement detection scheme instead of relying on a combination of the IPv6 addresses of the individual routers and the on-link prefixes that the routers advertise as specified in [MIPv6].

6.1. Location Indication Option Format

This specification defines a new Location Indication option for Neighbor Discovery [ND]. This option is used in Router Advertisement messages to help mobile nodes quickly detect when they appear in a different link without resorting to ``guessing'' based on the advertised prefixes in the router advertisements and Neighbor Unreachability Detection specified in [MIPv6].

```
     0                   1                   2                   3
     0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
    +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
    |     Type      |    Length     | Location Type |  Reserved     |
    +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
    |                           Reserved                            |
    +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
    |                                                               |
    +                                                               +
    |                                                               |
    +                     Identifying Address                       +
    |                                                               |
    +                                                               +
    |                                                               |
    +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Fields:

Type 8-bit identifier of the type of option. Value TBD.

Length 8-bit unsigned integer. The length of the option (including the type and length fields) in units of 8 octets. Always 5 for this option.

Location Type

8-bit field specifying what level type of location (granularity etc) that is captured in the

Identifying Address. The following types are defined in this document:

Link Location	1
AAA domain indication	2

Identifying Address

128-bit IPv6 address. An IPv6 address which together with the location type uniquely identifies the location.

A mobile node would track the last received Identifying Address of type "link location". When it receives a Location Indication of that type with a different Identifying Address it should as quickly as possible form a new care of address. If the Router Advertisement contains Prefix options with the A-bit set it can immediately so this. Otherwise it needs to send one or more Router Solicitations in order to receive one or more such Prefix options. Once the mobile node has a new care of address it can discard the old care of address and the old default router list (the default routers which have not been heard from after it received the new link location) and proceed to send binding updates to the home agent and correspondents in the Binding Update list as specified in [MIPv6].

Routers that are configured to send Location Indication options should verify, in addition to what is specified in the Section on Router Advertisement Consistency in [ND], that other routers on the same link use the same Identifying Address for the same Location Type. If these is a mismatch this should be reported to system management.

7. SECURITY CONSIDERATIONS

The generic end-to-end piggybacking allows arbitrary IP payloads to be included in the same packet. Thus firewalls that care about IP payloads need to inspect all of them. If the firewall is not capable of doing this it is likely to drop the whole packet, and if the firewall has the capability to inspect the multiple payloads it is likely to drop the whole packet if any payload needs to be rejected. Thus any use of this multiple payload header needs to be able to have retransmission policies that avoid repeatedly trying to use the header for retransmitted packets.

As pointed out in [RH-HA] the issues of processing Routing Headers as used by Mobile IP and Home Address Options seem rather similar to the

concerns that exist for decapsulating and optionally forwarded packets when using tunneling.

Using the framework that exists for tunneling to express this makes Mobile IPv6 be able to leverage security mechanisms. However, the specific policies for when to decapsulate packets are quite different for the Mobile IP use of tunneling as outlined in Section 5.4.

The suggestion do to explicit movement detection allows any node on the link, in the absence of authenticated and authorized Router Advertisements, to send Location Indication options which would make a Mobile Node think it has moved and attempt to form new Care of Addresses. However, similar attacks can be launched against the movement detection mechanisms in [MIPv6]. None of these attacks are possible for off-link senders.

8. ACKNOWLEDGEMENTS

This document is mostly a collection of ideas that others have suggested that I've tried to capture or this virtual paper.

Robert Elz wrote [PAYLOAD] many years back and Francis Dupont found a copy of the old draft.

Bill Sommerfeld suggested using encapsulation instead of Routing Headers and Home Address options on the mobileip mailing list.

TBD: List more names.

REFERENCES

[RH-HA] P. Savola, "Security of IPv6 Routing Header and Home Address Options", draft-savola-ipv6-rh-ha-security-00.txt

[TUNNEL] A. Conta, and S. Deering, "Generic Packet Tunneling in IPv6 Specification", RFC 2473, December 1998.

[PAYLOAD] R. Elz, "The IPv6 Payload Header", Expired Internet Draft, draft-kre-ipv6-payload-01.txt, October 1995.

[ICMPv6] A. Conta, and S. Deering, "Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification", draft-ietf-ipngwg-icmp-v3-01.txt.

[IPv6] S. Deering, R. Hinden, Editors, "Internet Protocol, Version 6

(IPv6) Specification", RFC 2460, December 1998.

[MIPv6] D. Johnson, C. Perkins. "Mobility Support in IPv6", draft-ietf-mobileip-ipv6-14.txt.

[ND] T. Narten, E. Nordmark, W. Simpson, "Neighbor Discovery for IP Version 6 (IPv6)", RFC 2461, December 1998.

[IPSEC-SA] R. Atkinson. "Security Architecture for the Internet Protocol". RFC 2401, November 1998.

[KEYWORDS] S. Bradner, "Key words for use in RFCs to Indicate Requirement Levels", RFC 2119, March 1997.

[INGRESS] P. Ferguson, D. Senie, "Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing.", RFC 2827, May 2000.

AUTHORS' ADDRESSES

Erik Nordmark
Sun Microsystems Laboratories, Europe
29 Chemin du Vieux Chene
38240 Meylan, France

phone: +33 (0)4 76 18 88 03
fax: +33 (0)4 76 18 88 88
email: Erik.Nordmark@sun.com