

Mobility in IPv6

Rachid Ait Yaiz and Osman Öztürk
 {yaiz, osman }@ctit.utwente.nl

Abstract- This document deals with mobility related issues in IPv6. IPv6 has some differences with IPv4. The major differences are the IPv6 Base Header, the IPv6 Extension Headers and the IPv6 Address Types. These differences help in the design of Mobile IPv6. Good solutions could be found for the location determination by a mobile node, for the registration of a mobile node on a foreign link, for the packet interception by a home agent and for the notification of correspondent hosts, by a mobile node, of its current location. Good solutions could also be found for routing to and from a mobile host.

1. Introduction

The Internet has experienced an enormous growth during the last few decades. The number of available Internet addresses seemed to be insufficient to meet the future needs of the Internet. As a response, the Internet Engineering Task Force (IETF) introduced the Internet Protocol version 6 (IPv6) as a replacement for the current Internet protocol (IPv4). Besides the much higher number of available IP addresses within IPv6 (2^{128} instead of 2^{32}), IPv6 differs in several ways from IPv4. In this paper we will describe these differences in Section 2. We will show the components of Mobile IPv6 in Section 3. In the Sections 4 through 7 we will show how differences, mentioned in Section 2, help in the design of Mobile IPv6. Finally we draw some conclusions in Section 8. Note that the ideas presented in this paper are not ideas of the authors but rather extracted from [Sol98] and [IDMIPv6].

2. Differences between IPv6 and IPv4

There are three major differences between IPv6 and IPv4:

- IPv6 Base Header
- IPv6 Extension Header
- IPv6 Address Types

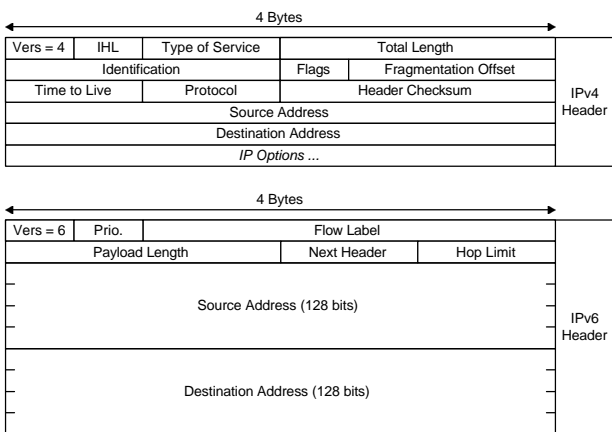


Figure 1. IPv6 Base Header vs. Ipv4 Header [Sol98]

Figure 1 shows the IPv6 Base Header versus the IPv4 Header.

Several differences are perceivable. For instance, the version number in both headers is different, the IPv6

Header includes a Next Header field and the address fields in the IPv6 Base Header are much larger than in the IPv4 Header. The Next Header Field in the IPv6 Base Header points to an extension header which can be one of the following headers:

- Hop-by-Hop Options Header, which contains options that are examined by every router along the path.
- Destination Options Header, which contains options that are only examined by the destination.
- Routing Header, which is used in case of source routing
- Fragment Header, which is used by the source node when packets that are larger than the path Maximum Transfer Unit are to be sent.
- IP authentication Header, which is used to provide authentication.
- IP Encapsulation Security Payload, which is used to provide confidentiality of the IP payload.
- Upper-Layer Header, which is for instance the TCP header or the UDP header.

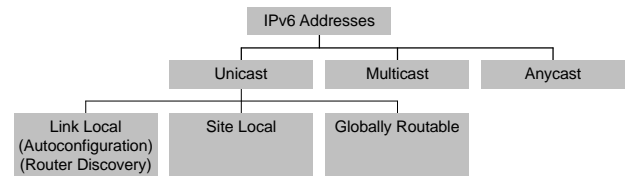


Figure 2: IPv6 Address Types

Figure 2 shows the IPv6 Address Types which slightly differs from the address types of IPv4. IPv6 treats broadcast as a special case of multicast. As a result, there is no broadcast address type. On the other hand IPv6 defines an Anycast address which can be seen as a special version of a Multicast Address. When an Anycast address is used, a packet is sent to only one member of the group depicted by the Anycast address. Furthermore, a Unicast address can be divided into three different types of addresses:

- Link Local addresses which have only local link significance. This means that the packets using a Link Local address are never forwarded by routers. Link Local addresses are used in case of Autoconfiguration and Router Discovery.
- Site Local addresses which have only site local significance. This means that packets using a Site

Local address can be forwarded by every router within a site except by the egress routers connecting to the global Internet.

- Globally Ratable addresses which are globally unique.

The most important differences between IPv4 and IPv6 in relation to the design of Mobile IPv6 are:

- Larger Addresses, which allows for new techniques to be used in order for the Mobile Node (MN) to obtain a care-of address. Now, MNs can always get a co-located care-of address, a fact that removes the need for a Foreign Agent (FA).
- New Routing Header, which allows for proper use of source routing. This was not possible with IPv4 [SOL98].
- Authentication Header, which allows for the authentication of the binding messages.
- Destination Options Header, which allows for the use an options without significant performance degradation. Performance degradation occurred in IPv4 because every router along the path had to examine the options even when they are only destined for the receiver of the packet.

3. Components of Mobile IPv6

The functioning of Mobile IPv6 is similar to that of Mobile IPv4. A MN must determine its current location. When a MN is on its home link it must act as a Fixed Host. When a MN is on a foreign link, it must acquire a co-located care-of address and notify this address to the Home Agent (HA). The MN also reports this acquired care-of address to selected correspondents. The last component of Mobile IPv6 is the routing of packets to and from MNs.

The following question can be extracted:

- How does a MN determine its current location?
- How does the HA intercept packets that are destined for a mobile node.
- How does a MN inform other nodes of its care-of address?
- How are packets routed to and from a MN?

These questions will be answered in the following sections.

4. ICMPv6 Router Discovery

ICMPv6 has several functions which can be used by Mobile IPv6. These functions include:

- Router Advertisements
- Router Solicitations
- Address Autoconfiguration (stateful and stateless)
- Neighbor advertisements

A MN can determine its current location by listening to the Router Advertisements and comparing the network prefix of the source address within this advertisements with the network prefix of its Home Link (HL). If the network prefix of the source address within the Router Advertisement equals the network prefix of the home address of the MN then the MN is on its HL. Otherwise the MN is on a Foreign Link (FL).

Similarly the MN can detect its movement from a FL to another FL when the network prefix of the source address within a Router Advertisement changes to another network prefix that is not its Home Link network prefix.

If the MN does not want to wait for a Router Advertisement, it can send a Router Solicitation asking the routers to send a Router Advertisement.

To obtain a care-of address the MN can use either stateful or stateless Address Autoconfiguration. In the first situation the MN obtains a care-of address from an address server like a DHCP server. In the latter situation, the MN extracts the network prefix from the Router Advertisements en concatenates it with its MAC layer address to form a care-of address.

After a care-of address is obtained or formed, it must be checked whether this is a unique address or not.

When the MN is not on its home link, the HA must intercept packets destined for the MN. In order to enable this packet interception, the HA must multicast a “gratuitous” Neighbor Advertisement on the home link containing the home address of the MN and its own MAC layer address. In fact, the HA is telling the nodes on the home link that the IP address of the MN must be associated with the MAC address of the HA, and hence packets destined to the MN (depicted by the IP address) are delivered to the HA (depicted by MAC address). The process of a node A letting other nodes associate the IP address of node B with the MAC address of node A is called the process of proxy Neighbor Discovery [IDMIPv6].

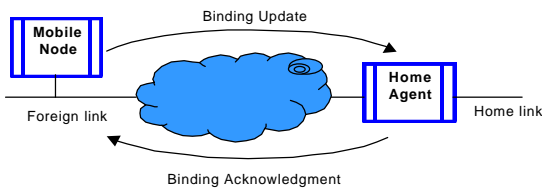
When the MN returns to its home link, the MN must multicast a “gratuitous” Neighbor Advertisement containing its own MAC layer address and its home address.

5. Notification in IPv6

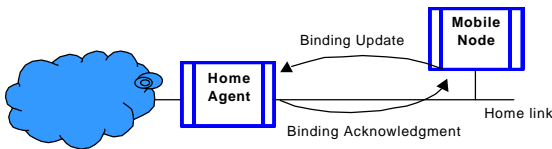
To transparently route packets to the mobile node's care-of address (which are destined to a mobile node's home address) three new procedures are introduced in IPv6. These are the binding update, the binding acknowledgment and the binding request procedures. The three procedures form the notification procedure, which is the association of the home address and the care-of address of a mobile node with the lifetime of the association, in which the mobile node informs (notifies) other nodes of its current location. This is done when a mobile node moves to another link, as is shown in figure 3A and C, where the mobile node moves to a foreign link and notifies its home agent (A) and the correspondent node (C) of its new location. The home

agent must be informed in order to be able to reroute (tunnel) the packets destined to the mobile node that arrive at the home agent. In IPv6 it is possible that the correspondent node can communicate directly with the mobile node. For this the mobile node informs the correspondent node of its current location (care-of address). The correspondent node will then use this care-of address as the destination address and will send its packets directly to the mobile node. In figure 3B is shown that the mobile node returns back to its home link and notifies its home agent.

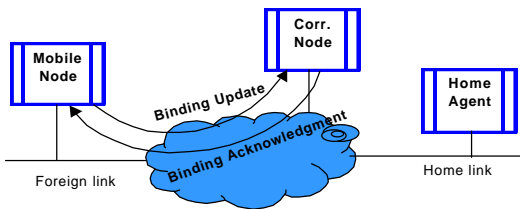
The binding messages are transferred in the new IPv6 extension header, available as Destination Option Header. This header contains binding specific information, which is only examined and processed by the ultimate destination. The binding messages can be either send as a stand-alone packet (without user data) or can be included (piggybacked) within any IPv6 packet carrying any payload (with user data).



A: Mobile node at a foreign link informing the HA



B: Mobile node back at its home link informing the HA



C: Mobile node at a foreign link informing the CN

Figure 3: Notification procedures

When a mobile node moves to a new link, it sends a binding update to its home agent or other correspondent nodes in its list to inform them about its current care-of address. As shown in figure 4, the destination option header containing the mobile IPv6 binding update option consists of an A an H and an L bit and the fields: lifetime, identification, mobile node's Home Address and Care-of Address. The A bit indicates whether the receiver should reply with a binding Acknowledgement or not. The H bit is used if the mobile node wants the receiving node to be its home agent. The L bit is sent if the mobile node also

wants to receive packets destined to its link-local home address.

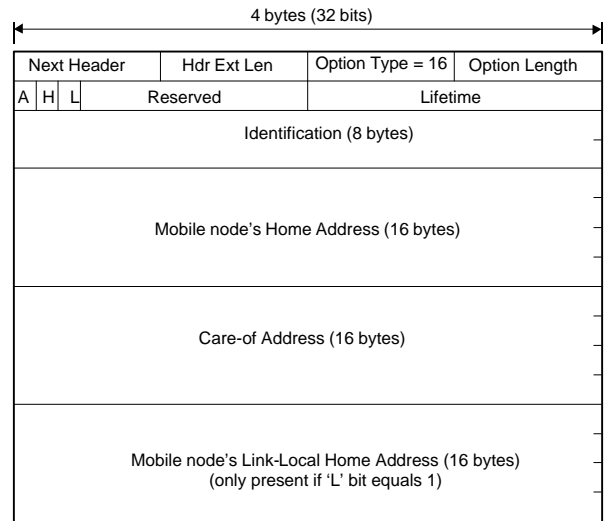


Figure 4: Destination Option Header Containing the Mobile IPv6 Binding Update Option

The identification field, the home address field and the care-of address field is the same as in the registration request field of IPv4.

A binding Acknowledgement is sent to the mobile node by its home agent or any other correspondent node to indicate that the Binding Update was successfully received and whether it was accepted or not. The status field is used for this purpose. This is shown in figure 5.

The lifetime, identification and mobile node's home address are the other fields of this option, which are copied from the received binding update. An extra field is the refresh field, which indicates how long the sender of the binding acknowledgement will store the care-of address of the mobile node. This is used as an indication for the mobile node how often it has to send a binding update to that node. A binding acknowledgement is required if the A bit in the binding update is set to 1.

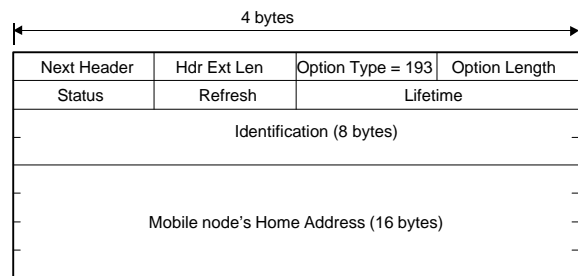


Figure 5: Destination Option Header Containing the Mobile IPv6 Binding Acknowledgement option

If a correspondent node wants to know the care-of address of a mobile node, it sends a binding request to that mobile node. The only information in this request is the request itself so the binding request only contains the option type and the option length fields, as shown in figure 6. The

mobile node does not necessarily have to respond to the request by sending a binding update. The request is also used to get new lifetime and refresh fields, when they are expired or need to be refreshed.

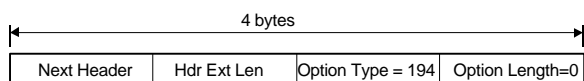


Figure 6: Destination Option Header Containing the Mobile IPv6 Binding Request Option

6. Routing in IPv6

Another option in IPv6 is the routing header option. The routing header contains a list of intermediate destinations that a packet must visit along its path to the ultimate destination [Sol98]. The ultimate destination is the mobile node's home address, which is noted as address[1] in the routing header (figure 7).

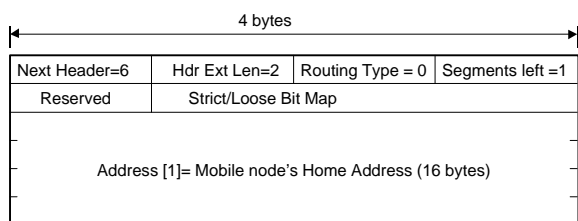


Figure 7: IPv6 "Type 0" Routing Header

As an intermediate destination the mobile node's current location (care-of address) is used, since the care-of address is collocated with the mobile node itself. So, as a destination address, the care-of address of the mobile node is used. No other node reacts on the packet except those at the destination. At the destination the mobile node sees its home address in the routing header and gets the packet. If the correspondent node knows the care-of address of the mobile node, it can send packets directly to the mobile node using the routing header. If the correspondent node does not know the care-of address of the mobile node, then it will send the packets just like in IPv4 by using the home address of the mobile node as the destination address and the packet will be sent to the home agent, which will encapsulate the packet for tunneling the packet to the current location of the mobile node. After receiving a packet via its home agent the mobile node knows that the correspondent node is not aware of its current care-of address. In that case in IPv6 it is possible, that the mobile node can consider whether to send a binding update to the correspondent node to inform the correspondent node of its current care-of address, so that the correspondent node can send packets to the mobile node directly.

A mobile node can generate and send packets to any router at its current link it has received a router advertisement from. The routing table at the mobile node is configured in such a way that the mobile node will send all its packets to that router, which will forward the packets to the right destination.

7. Dynamic home agent address discovery

The nodes in a IPv6 network can be reconfigured and so it can happen that the node which functioned as the home agent of a mobile node is not active or is removed from the link. In that case it is possible for the mobile node to dynamically obtain the address of another node at the home link which can function as the mobile nodes new home agent. This is done with the dynamic home agent address discovery option available in IPv6. For this the mobile node builds a packet destined to all the nodes on its home link (multicast address) in which it places a binding update option with the H bit set. This packet is encapsulated in another packet, which has as destination address the subnet-router anycast address, which will be delivered at any router at its home link. Upon receiving this packet, the router will decapsulate it and multicast the inner packet to all the nodes on that link. All nodes with home agent functionality will reply to the binding update by sending a binding acknowledgement in which they reject the mobile node's request, because they received the request within a multicast packet. The binding acknowledgement packet however will contain the globally routable IPv6 unicast address of each node. The mobile node will collect these addresses and select one of the home agents to which it directly sends a subsequent binding update. This time the node will accept the request to be the mobile nodes home agent.

8. Conclusions

With the introduction of IPv6, a lot of the disadvantages of IPv4 were taken away. The design of Mobile IPv6 benefits, among others, from the new Routing Header, which allows sending packets from a Correspondent Node to a Mobile Node using source routing instead of encapsulation. Furthermore, the larger address space within IPv6 allows for new technique to be used, which eliminated the need for a foreign agent.

The Authentication Header is the first step in making it possible to authenticate binding messages preventing denial-of-service attacks. The second step is to find a key distribution mechanism, which is not realized yet.

The design of Mobile IPv6 also benefits from the introduction of the Destination Options Header within IPv6. This allows the binding messages to only being examined at the ultimate destination. Hence, the intermediate routers between source and destination are spared the performance degradation caused by examining options contained in the binding messages.

9. References

- [IDMIPv6] Internet Draft, Mobility Support in IPv6, D Johnson and C. Perkins, IETF 1999
- [Sol98] Mobile IP, The Internet Unplugged, James D. Solomon, Prentice Hall 1998