IPv6 Working Group
INTERNET DRAFT

Charles Perkins
IBM Corporation
David B. Johnson
Carnegie Mellon University
26 January 1996

Mobility Support in IPv6

<draft-ietf-mobileip-ipv6-00.txt>

Abstract

This document specifies mobility messages that allow transparent routing of IP datagrams to mobile nodes in the Internet. Each mobile node is always identified by its home address, regardless of its current point of attachment to the Internet. While situated away from its home, a mobile node is also associated with a care-of address, which provides information about its current point of attachment to the Internet. The protocol provides for notifying the mobile node's home agent, and any other interested IPv6 addressable entities, about the care-of address of the mobile node. When necessary, the home agent sends packets destined for the mobile node through a tunnel to the care-of address. After arriving at the end of the tunnel, the packets are then delivered to the mobile node.

Status of This Memo

1. Introduction

A new version of the Internet Protocol, IPv6, is being developed with 128-bit addresses, which remedies perceived flaws with the existing version (that is, IPv4). This document specifies messages and a simple protocol for the operation of mobile computers for IPv6. Mobile computers are likely to account for a substantial fraction of the population of the Internet during the lifetime of IPv6.

The development of IPv6 presents a rare opportunity, in that there is no existing installed base of IPv6 hosts or routers with which compatibility must be maintained, and all IPv6 nodes may be assumed to perform the few operations needed to support Internet-wide mobility. The most important function needed to support mobility is the reliable and timely notification of a mobile node's current location those other nodes that need it. The home agent needs this location information in order to forward intercepted packets from the home network to the mobile node, and correspondent nodes need this information in order to send their own packets directly to the mobile node.

In this document, we specify the way that the mobile node can notify other nodes about its current whereabouts, using a Destination option which fits naturally in IPv6. We describe the mechanism by which a routing header can be used to deliver packets to the mobile node at its current whereabouts. All IPv6 nodes and routers are assumed to perform the few operations required for mobility, since doing so adds little additional overhead. This leads to dramatic simplifications in the required protocols, compared to the methods required for IPv4.

2. Basic Operation

From the model of operation developed for enabling mobile networking for IPv4, we borrow the concepts of home network, home address, home agent, care-of address, and binding. Mobile computers will have assigned to their interface(s) (at least) two IPv6 addresses whenever they are roaming away from their home network. One (the home address) is permanent; the other (the IPv6 link-local address) is used temporarily. In addition, the mobile node will typically autoconfigure a globally-routable address at each new point of attachment [12]. Every IPv6 router supports encapsulation, so every router is capable of serving as a home agent on the network(s) to which it is attached.

In brief, using the IPv4 language, we have a basic model of operation in which a mobile node can always be reached by sending packets to its home (permanent) address. Assuming the mobile node is not

present on its home network, packets arriving for it there will be intercepted by the home agent, and tunneled to a care-of address.

Care-of addresses can be constructed by the mobile node using the methods of automatic address configuration [12]. If the mobile node receives router advertisments, it MUST use automatic address configuration to construct a globally unique, routable address. This routable address can be used by the mobile node as its care-of address. After determining its care-of address, a mobile node must send a binding update containing that care-of address to the home agent (and any other correspondent nodes that may have out-of-date bindings in their binding cache). By default, correspondent nodes send packets to mobile nodes by using routing headers instead of encapsulation. As detailed in the next section, correspondent nodes are usually expected to deliver packets directly to the mobile node's care-of address, so that the home agent is rarely involved with packet transmission to the mobile node.

It is essential for scalability and minimizing network load that correspondent nodes be able to learn the care-of address of a mobile node, and to be able to cache this information for use in sending future packets to the mobile node's care-of address. By caching the care-of address of a mobile node, optimal routing of packets can be achieved between the correspondent node and the mobile node. Routing packets directly to the mobile node's care-of address also eliminates congestion at the home agent and thus contributes significantly to the overall health of the Internet. Moreover, many communications between the mobile nodes and its correspondent nodes can be carried out with no assistance from the home agent. Thus, the impact of failure at the home agent can be drastically reduced; this is important because many administrative domains will have a single home agent to serve a particular home network, and thus a single point of failure for communications to nodes using that home agent. Besides that, communications between the home agent and a mobile node may depend on a number of intervening networks; thus, there are many more ways that packets can fail to reach a mobile node when the home agent is required as an intermediate node. This would be particularly relevant on, say, trans-oceanic links between home agent and mobile node. Caching the binding of a mobile node at the correspondent node enables communication with the mobile nodes even if the home agent fails or is difficult to contact over the Internet.

In the typical case when a mobile node has configured its care-of address at one of its own interfaces, transferring data to the mobile node means no more work for routers on link at its current point of attachment, than transferring data to any other node on that link. This affords another substantial performance improvement in the typical case.

3. Terminology

Mobile IPv6 defines these terms:

Binding

The association of a home address with a care-of address, along with the remaining lifetime of that association.

Care-of Address

The care-of address is the termination point of a tunnel toward a mobile node that is away from its home network.

Correspondent

A peer with which a mobile node is communicating. The correspondent may be either mobile or stationary.

Foreign Network

Any network other than the mobile node's Home Network.

Home Address

An IPv6 address that is assigned for an extended period of time to a mobile node. It remains unchanged regardless of where the node is attached to the Internet.

Home Agent

A router on a mobile node's home network which tunnels packets for delivery to the mobile node when it is away from home, and maintains current location information for the mobile node.

Home Network

A network, possibly virtual, having a network prefix matching that of a mobile node's home address. Note that standard IP routing mechanisms will deliver packets destined to a mobile node's Home Address to the mobile node's Home Network.

Link

A facility or medium over which nodes can communicate at the link layer. A link underlies the network layer.

Mobile Node

A host or router that changes its point of attachment from one network or subnetwork to another. A mobile node may change its location without losing connectivity and without changing its IPv6 address.

Node

A host or a router.

Tunnel

The path followed by a packet while it is encapsulated. The model is that, while it is encapsulated, a packet is routed to a knowledgeable decapsulating agent, which decapsulates the packet and then correctly delivers it to its ultimate destination.

4. Binding Updates

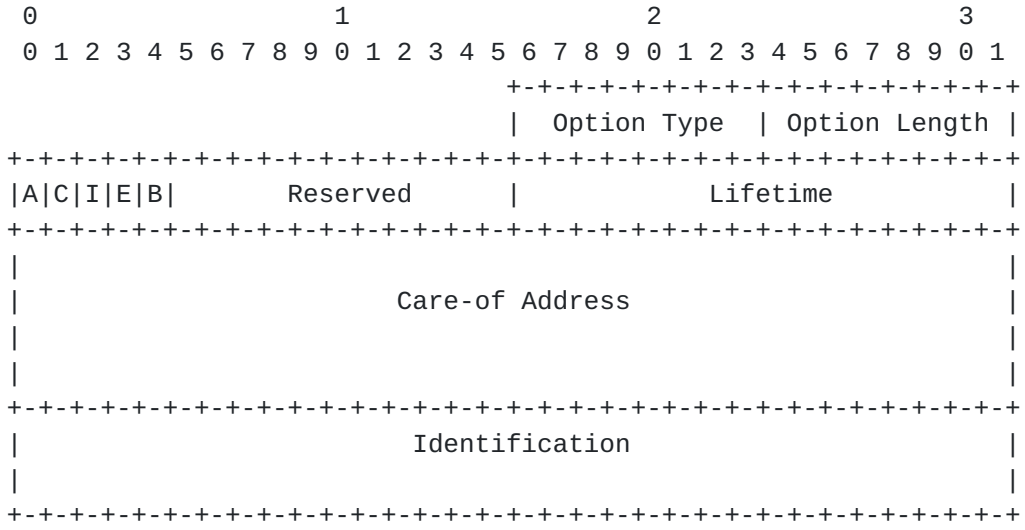
In IPv6, all IPv6 nodes must be capable of caching the care-of address of mobile nodes with which they want to communicate. This cached address information can be integrated with the node's Destination Cache [9]. Binding updates should be considered a form of routing updates; thus, handled incorrectly, they could be a source of security problems and routing loops. Therefore, packets which include binding updates MUST also include an IPv6 authentication header [1]; replay protection is then achieved by use of the Identification field in the binding update.

4.1. Binding Update Option Format

The Binding Update Option is an option within the Destination Header [5].

A mobile node uses the Binding Update destination option to notify another node (e.g., correspondent node or home agent) of its current care-of address. The binding update should be placed in the IPv6 packet after any routing header, since the binding update should only be processed by the destination node rather than by each hop along the path. The binding update is encoded as destination option type 16 (TBD). By encoding the binding update in this way, it can be included in any normal data packet or can be sent in a separate packet containing no data. The binding update contains the mobile node's care-of address, an identification for the update (to protect

against attempts to replay it), and a lifetime for the binding. This option format is adapted from that used in the IPv4 Route Optimization [7]. Note that the home address MUST be the source address of the IPv6 packet containing the binding update, and thus is not required to be located within the data of the destination option.



Option Type

8-bit identifier of the type of option. The first three bits of the option are 000, indicating first that a node receiving the option may discard the option and still process the rest of the packet, and second that the option may not be modified enroute.

Option Length

8-bit unsigned integer. Length of the Option Data field of this option, in octets.

Acknowledge (A)

The Acknowledge (A) bit is set by a node if it wants a a Binding Acknowledge message to be returned upon receipt of the Binding Update Option.

Co-location (C)

The mobile node is itself the agent receiving datagrams at the care-of address.

Identification Present (I)

The (I) bit is set by the node sending the Binding Update option to indicate whether or not the Identification field is present.

Encapsulation (E)

The (E) bit is set by the mobile node to request that the receiving node use IPv6-within-IPv6 encapsulation when sending any future packets to the mobile node's care-of address, instead of packets containing the care-of address in a routing header. See subsection 7.

"All-Nodes Multicast" (B)

The (B) bit is set by the mobile node to request that the home agent encapsulate and send "all-nodes multicast" packets to the mobile node at its care-of address. The (B) bit must only be used when sending binding updates to the home agent. Note that the home agent may be manually configured to send only a subset of such packets to the mobile node -- for instance, the home agent may inspect the port number of UDP packets, or the ICMP packet type, to determine whether or not the packet should be forwarded to the mobile node.

Reserved

Sent as 0; ignored on reception.

Lifetime

The number of seconds remaining before the binding must be considered expired. A value of all ones indicates infinity. A value of zero indicates that the indicated binding (or route table entry, in the case of a mobile node's previous router) for the mobile node should be deleted. The lifetime is typically equal to the remaining lifetime of the mobile node's binding with its care-of address.

Care-of Address

The current care-of address of the mobile node. When set equal to the home address of the mobile node, the Binding Update option instead indicates that any existing binding for the mobile node should be deleted; no binding for the mobile node should be created.

Identification

If present, a 64-bit number used to protect against replay attacks.

The receiver of this message must be able to determine that the mobile node is truly the agent which has generated the binding update, by verifying a subsequent IPv6 authentication header [1] within the packet.

Extensions to the Binding Update Options format may be included after the fixed portion of the Binding Update option. The presence of such extensions will be indicated by the option length field. When the option length is greater than the size of the fixed fields of the Binding Update Option, the remainder is interpreted as extensions. Currently no extensions have been defined.

5. Sending Binding Updates

After moving away from its home network to a new location (see subsection 5.1), the mobile node registers its new binding with its home agent by sending a packet containing a binding update to its home agent. This binding update MUST have the (A) bit set, instructing the home agent to send an acknowledgement. If not already doing so, the home agent must send out onto the Home Network a proxy Neighbor Advertisment on behalf of the mobile node, with the Override flag set [9]. This will ensure that other nodes on the home network are able to send packets to the mobile node by using the services of the home agent.

In the case when the mobile node is returning to its home network, the binding update sent to its home agent MUST contain the mobile node's home address in place of any care-of address. The mobile node MUST also send out the appropriate Neighbor Advertisment packets with the Override flag set, so that its neighbors on its home network will update the relevant information for the mobile node in their Neighbor Caches. This Neighbor Advertisement packet can be repeated a small number of times to guard against occasional loss of packets on the home network.

A binding update may also be included, whenever necessary, in a normal data packet sent to a correspondent node. For each correspondent node, information is kept by the mobile node to determine whether or not the correspondent node has been sent a fresh binding update since the last time any movement by the mobile node to a new care-of address has occurred. When a packet is to be sent to a correspondent node which hasn't been sent a fresh binding update, the mobile node SHOULD include the update within the packet, and indicate that the update has been sent. Thus, correspondent nodes are generally kept updated and can send almost all data packets directly to the mobile node. Such binding updates are not generally required to be acknowledged. However, if the mobile node wants to be sure, an acknowledgment can be requested.

The binding update can also be sent in an otherwise empty packet whenever the mobile node wishes to update its correspondents. This is normally done only if the mobile suspects that its home agent is not operational, too far away, a correspondent node is not sending the traffic to the proper care-of address, or there is an immediate need for the correspondent node to obtain the binding. The mobile node must not send binding updates more often than MAX_UPDATE_RATE to any correspondent host, since it is not allowed to change its point of attachment more often than MAX_UPDATE_RATE. A mobile node can detect that a correspondent node is not sending packets to the proper care-of address because in that case the packets arrive at the mobile

node's care-of address by encapsulation instead by inclusion in a routing header within the packet.

The mobile node may choose to keep its location private from certain correspondent nodes. The mobile node need not send binding updates to those correspondents. No other IPv6 nodes are authorized to send binding updates on behalf of the mobile node.

When sending binding updates, a mobile node uses the Identification field of the destination option, in conjunction with the IPv6 Authentication Header, to protect against replays. One style of replay protection involves the use of a timestamp as the Identification data. The result would be that the mobile node and the target of its binding update would have to roughly agree on the current time, and that stale binding updates would have to be rejected. The exact mechanisms by which the Identification field is created and interpreted by the sending and receiving parties depends on the Security Association existing between them. This subject is discussed thoroughly in the mobile-IPv4 specification [6].

5.1. Detecting movement

A mobile node may detect that it has changed its point of attachment to the Internet by several means. The usual method involves reception of router advertisements from previously undetected routers. This may also be augmented by a determination that a previously accessible router is no longer accessible (using Neighbor Unreachability Detection (NUD) as specified in [9]).

It is also possible that indications about changes of point of attachment can be obtained from lower-level protocol or device driver software.

6. Binding Acknowledgement Message

A Binding Acknowledge message is used to acknowledge acceptance of a Binding Update (section 4.1) option, if that option has the Acknowledge (A) bit set. Binding Acknowledgement messages should be sent addressed to the mobile node originating the Binding Update, using if necessary a routing header containing the care-of address given in the Binding Update.

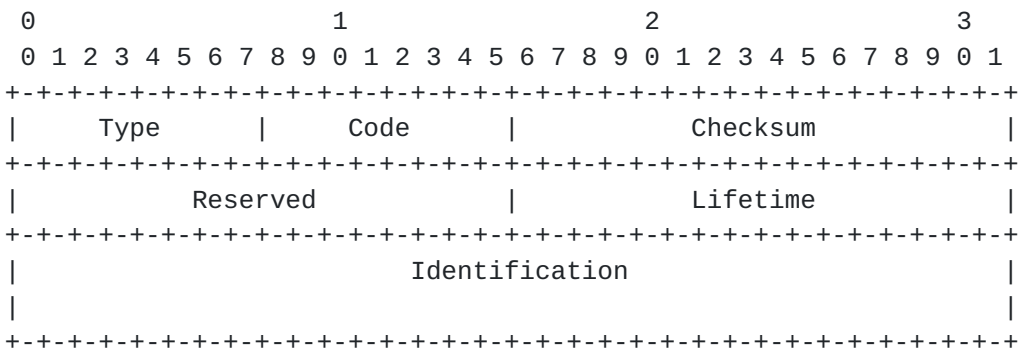
Since the Binding Acknowledgement is mostly used by home agents and is not associated with any transmission of data packets, it is specified here as an informational ICMP message to the mobile node. However, all of the error conditions specified in the Registration

Reply message of the IPv4 mobile-IP protocol may apply, so the general format and codes of that message are adapted here to fit the ICMP packet layout for IPv6 [4].

The acknowledgement message contains the necessary codes to inform the mobile node about the status of its binding. Additionally, the home agent MAY shorten the lifetime to be smaller than indicated in the original binding update. When the lifetime of the reply is greater than what was contained in the binding update, the excess time MUST be ignored. When the lifetime of the reply is smaller than the original request, another binding update SHOULD be sent before the lifetime expires.

If a mobile node fails to receive an acceptable Binding Acknowledgement within INITIAL_BINDACK_TIMEOUT seconds after transmitting the binding update, it must retransmit the binding update with the same identification, and begin an exponential back-off process of retransmission. The time-out period is doubled upon each retransmission until the target of the binding update sends an acknowledgement, or the time-out period reaches the value MAX_BINDACK_TIMEOUT.

The ICMP Binding Acknowledgment packet has the following format:



Type 192 (TBD)

Code One of the following codes:

0 service will be provided
128 service denied: reason unspecified
129 service denied: administratively prohibited
130 service denied: insufficient resources
133 service denied: identification mismatch
134 service denied: poorly formed request
136 service denied: unknown home agent address

Lifetime	The seconds remaining before the binding is considered expired. A value of zero indicates removal of a binding. A value of all ones indicates infinity.
Identification	The acknowledgment identification is derived from the binding update message, for use by the mobile node in matching the acknowledgment with an outstanding Binding Update.

Up-to-date values of the Code field are to be specified in the most recent "Assigned Numbers" [10].

7. Delivering Packets to a Mobile Node

If a routing header is not present, the routing infrastructure will route packets addressed to a mobile node to its home network. Since the mobile node's location is known on the home network (namely, by the home agent), packets can be addressed to the mobile node and intercepted by the home agent without the sender knowing that the node is mobile.

Correspondent nodes that have accepted a binding update for a mobile node, can send packets directly to that mobile node's current care-of address by including a routing header in them. To use the routing header for delivery of packets to a mobile node, a correspondent host just specifies the care-of address as the (last) intermediate routing point and the mobile node as the destination. When the packet arrives at the care-of address, normal processing of the routing header will ensure delivery to the mobile node. IPv6 routing headers do not carry the semantics which require reversal of source routes.

Home agents cannot use routing headers to deliver packets to the mobile node, because they can't modify the packet and add to it in flight. They must always use encapsulation [3] for this purpose (section 8).

If a packet to the mobile node is encapsulated, it uses the care-of address as the destination address in the outer IPv6 header. Then, when the the encapsulated packet arrives at the care-of address, the encapsulation is stripped away and the packet delivered (if possible) to the mobile node. Of course, if the mobile node is itself receiving packets at the care-of address, the delivery path is trivial.

If a correspondent node receives ICMP Host Unreachable or Network Unreachable after sending a packet to a mobile node using its cached care-of address, it SHOULD delete the cache entry until information about the mobile node's current care-of address becomes available (via a binding update).

7.1. Smooth Handoffs

If a mobile node obtains a new care-of address from an stateful address allocation authority (e.g, [2]), it should soon explicitly deallocate the previous care-of address. For smooth handoffs, a mobile client may still accept packets at both addresses for a short time after configuring its newly allocated IPv6 address. If the previous address is allocated by such a stateful address server, then such a mobile client may not wish to release the address immediately upon acquisition of a new care-of address. The stateful address server will allow mobile clients to acquire new addresses while still using previously allocated addresses.

Routers must (just as any IPv6 node) be able to accept authenticated binding updates for the mobile node and, subsequently, act on the cached binding by encapsulating packets for intermediate delivery to the care-of address specified in the binding. In cases where a mobile node moves from one care-of address to another with no delay, but without being able to maintain simultaneous connectivity at both care-of addresses, it SHOULD send a binding update to the router servicing the previous care-of address, so that packets for the mobile node can be delivered to the new care-of address immediately. For example, a mobile node may move from one radio link to another on a different channel, and be unable to monitor packets delivered over two channels at once. In this example, the mobile node should send a binding update to the entity delivering packets over the previous radio channel so that those packets will instead be delivered via a new care-of address. This binding update associates the mobile node's previous care-of address to the mobile node's new care-of address, and is authenticated using the IPv6 Authentication Header with whatever security association the previous router had with the mobile node's previous care-of address.

For this purpose, the mobile node must have some security association with the entity serving the previous care-of address. In the typical case specified within this document, a mobile node has obtained a care-of address via autoconfiguration and is receiving tunneled packets at that care-of address. When the mobile node moves, routers serving the link at its previous point of attachment may find that the mobile node's previous care-of address has become inaccessible.

Note that the previous router does not necessarily know anything about the mobile node's home address as part of this sequence of events; the routers may only know about things associated with the (e.g., autoconfigured) care-of addresses used by the mobile node at the previous and current points of attachment.

Since only one binding update is expected to be sent to the previous router, the mobile node MAY elect to omit the Identification field. If the mobile node omits the Identification field from the binding update, there is no replay protection and the security association with the previous router can only be used one time. In this case, the router should only accept the binding update if the mobile node's care-of address is still present in its Neighbor Cache. In this situation, the mobile node SHOULD request an acknowledgment for the binding update. Thus, the previous router should keep the security association around for the mobile node's previous care-of address in case the mobile node loses the acknowledgment and retransmits the binding update (with the same new care-of address).

The previous router then operates the same way as when the mobile node's home agent receives a binding update from the mobile node. That is, the previous router must inspect packets, and redirect the packets destined for the care-of address indicated in the binding update. Packets which need to be redirected to the mobile node's new care-of address are encapsulated and sent to the new care-of address. In fact, the previous router is temporarily acting as a home agent for the mobile node's previous care-of address. In particular, the previous router does not use any routing header to effect the redirected delivery. Moreover, the previous router should issue Neighbor Advertisement packets for the previous care-of address, so that on-link neighbors will send packets destined to the mobile node to the previous router for encapsulation and further delivery to the new care-of address.

Once the mobile node receives the encapsulated packet, it can then typically follow the routing header contained in the decapsulated packet and deliver the final payload to internal protocol handling using its IPv6 home address. The mobile node must ensure that a binding update is sent to each source of such packets so that the previous router is relieved of its duties at the earliest possible moment.

8. Home Agent Considerations

When the home agent, or any other routing agent, receives a packet destined to a mobile node for which it has a binding cached, it encapsulates the packet for delivery to the mobile node's

care-of address. The agent cannot insert a routing header, or modify the destination address of the mobile node, because of IPv6 authentication mechanisms [1]. Moreover, the home agent is expected to be involved only rarely with the transmission of data to the mobile node, because the mobile node will send binding updates as soon as possible to its correspondent hosts.

It is useful to be able to send a packet to a mobile node's home agent without explicitly knowing the home agent's address. For example, a mobile node must communicate with its home agent to send it a binding update; but since the mobile node was last at home, it may have become necessary to replace the node serving as its home agent due to the failure of the original node or due to reconfiguration of the home network. It thus may not always be possible or convenient for a mobile node to know the exact address of its own home agent.

Mobile nodes can dynamically discover the address of a home agent by sending a binding update to the anycast address on their home network. Each router on the home network which receives this binding update MUST reject the binding update and include its address in the Binding Acknowledgement packet indicating the rejection. The mobile node is assumed to know a proper anycast address on its home network before making use of this method for determining a particular home agent's address.

Other routers on the home network must be instructed to forward packets to the current router which is serving as the mobile node's home agent. This can be done using the same proxy mechanisms already made available in Neighbor Discovery. The current home agent multicasts the equivalent of a Proxy ARP onto the home network, and subsequently the other routers on the home network will forward packets destined to the mobile node to the particular router which is serving as the home agent for that mobile node.

8.1. Renumbering the Home Network

Neighbor Discovery [9] specifies a mechanism by which all nodes on a network can gracefully autoconfigure new addresses, say by combining a new routing prefix with their existing MAC address. As currently specified, this mechanism works when the nodes are on the same link as the router issuing the necessary multicast packets to advertise the new routing prefix(es) appropriate for the link.

However, for mobile nodes not currently attached to the same link as their home agent, special care must be taken to allow the mobile nodes to renumber gracefully. The most direct method of insuring

this is for the home agent to tunnel the multicast packets to the care-of address of the mobile node as necessary. The rules for this are as follows:

- A mobile node assumes that its routing prefix has not changes unless it receives authenticated router advertisement messages from its home agent that the prefix has changed.

- When the mobile node is at home, the home agent does not tunnel router advertisements to it.

- When a home network prefix changes, the home agent tunnels router advertisement packets to each mobile node which is currently away from home and using a home address with the affected routing prefix. Such tunneled router advertisements MUST be authenticated [1].

- When a mobile node receives a tunneled router advertisement containing a new routing prefix, it must perform the standard autoconfiguration operation to create its new address

- When a mobile node returns to its home network, it must again perform Duplicate Address Detection at the earliest possible moment after it has registered with its home agent.

- A mobile node may send a router solicitation to its home agent at any time, within the constraints imposed by rate control in the Neighbor Discovery specification [9]

Note that a mobile node is guaranteed that its home address is unique and used by no other mobile node. However, in some circumstances it may nevertheless be true that other nodes on its home network form the same link-local address as the mobile node during the time when the mobile node is away from its home network. Thus, there is the requirement above that the mobile node perform Duplicate Address Detection when it returns again to its home network.

9. Multicast Packet Routing

A mobile node that is connected to its home network functions just like any other (stationary) host or router. Thus, when it is at home, a mobile node functions identically to other multicast senders and receivers. This section therefore describes the behavior of a mobile node that is not on its home network.

In order receive multicasts, a mobile node must join the multicast group. Mobile nodes MAY join multicast groups in order to receive

transmissions in one of two ways. First, they MAY join the group via a (local) multicast router on the visited subnet. This option assumes that there is a multicast router present on the visited subnet. The mobile node SHOULD use its dynamically acquired care-of address (if it has acquired one) as the source IP address of its multicast group membership control message packets. Otherwise, it MAY use its home address.

Alternatively, a mobile node which wishes to receive multicasts can join groups via a bi-directional tunnel to its home agent, assuming that its home agent is a multicast router. The mobile node tunnels the appropriate multicast group membership control packets to its home agent and the home agent forwards multicast packets down the tunnel to the mobile node. The home agent must tunnel the packet directly to the mobile node's dynamically acquired care-of address, or, the packet must be tunneled first to the mobile node's home address and then recursively tunneled to the mobile node's care-of address.

A mobile node which wishes to send packets to a multicast group also has two options: (1) send directly on the visited network; or (2) send via a tunnel to its home agent. Because multicast routing in general depends upon the IP source address, a mobile node which sends multicast packets directly on the visited network MUST use a dynamically acquired care-of address as the IP source address. Similarly, a mobile node which tunnels a multicast packet to its home agent MUST use its home address as the IP source address of both the (inner) multicast packet and the (outer) encapsulating packet. This second option assumes that the home agent is a multicast router.

10. Compatibility with ICMP

When sending a packet to a mobile node, it is important to correctly return to the original sender any ICMP error messages generated by this packet. Since in most cases such packets use a routing header containing the care-of address, this is usually not a problem.

However, when a packet encapsulated at the home agent encounters such an error condition, ICMP error messages are returned to the sender as specified in [3]. ICMP for IP version 6 has been specified to return as much of the original packet as will fit in the ICMP error message without the ICMP packet exceeding 576 octets [4]. This size should be sufficient for correctly returning ICMP error messages backwards along the tunnel.

11. Protocol Requirements

This section summarizes the requirements introduced by the above protocol operations for IPv6 nodes and for routers.

11.1. Requirements for IPv6 Nodes

Every IPv6 node must be able to interpret Binding Update packets. Every IPv6 node must be able to maintain Security Associations for use in IPv6 Authentication Headers [1] which are used to authenticate Binding Updates and protect against replay attacks. Every IPv6 node must be able to associate care-of addresses with IPv6 target addresses, and use routing headers to deliver packets to IPv6 target addresses (e.g., mobile node addresses) using the care-of address as an intermediate router address.

11.2. Requirements for IPv6 Mobile Nodes

Every IPv6 mobile node must be able to perform IPv6 decapsulation. Every mobile node must be able to send Binding Updates as outlined above, and receive Binding Acknowledgements from routers. Every IPv6 mobile node must keep track of which other IPv6 nodes may need to receive Binding Updates as a result of recent movement by the mobile node. In particular, every IPv6 mobile node must be able to send Binding Updates when a packet is received that does not use a routing header to specify its care-of address.

11.3. Requirements for IPv6 Routers

Every IPv6 router must perform the mobility-related functions listed in the previous subsection (11.1) for IPv6 nodes, but not necessarily the functions for mobile nodes.

Every IPv6 router must be able to issue Binding Acknowledgements in response to Binding Updates received and accepted from a mobile node. Every IPv6 router must be able to encapsulate packets in order to tunnel them to a care-of address known for a mobile node from which it has received a binding update. Every IPv6 router must be able to maintain security associations for the mobile nodes from which it will accept binding updates.

A. Constants

INITIAL_BINDACK_TIMEOUT == 1 second

MAX_BINDACK_TIMEOUT == 256 seconds

MAX_UPDATE_RATE == 1 per second

B. Open issues

B.1. Using Encapsulation Protocols

Should alternative encapsulation techniques be defined for use with these protocols? Should a minimal encapsulation be defined and specified as the default?

There is only one possible advantage afforded by the use of encapsulation, compared to the use of the existing routing header defined for IPv6, and it only occurs when a mobile node uses a care-of address associated with a router attached to the same link as the mobile node's point of attachment as in B.3. If a mobile node has a link to a router over a low speed wireless link, and the router receives encapsulated packets for the mobile node, the encapsulation is stripped away before final delivery is made to the mobile node. In that case, fewer bytes are transmitted over the low-speed link, than would be the case for a normally processed routing header specifying the care-of address. Perhaps this would be better taken care of by defining something like TCP header compression over the link from the router to the mobile node. Such a compression scheme would eliminate the need to include the routing header information in every packet delivered over a slow-speed connection between a router and a mobile node.

Another alternative would be to provide another type of routing header (routing type == 2, say) which would allow an intermediate node to delete itself from the list instead of just rearranging the list. This would completely eliminate the need for encapsulation for normal datagrams from correspondent host to mobile node. However, having routers remove addresses to shrink the packet size may be a slow operation (relatively speaking).

B.2. Session keys with local routers

In the IPv4 route optimization proposal, a mechanism is outlined whereby a session key can be established between foreign agents and mobile clients, without requiring any pre-established security

relationship between them. A similar mechanism should be defined for IPv6, to avoid the need for a possibly time-consuming negotiation between routers and mobile nodes for the purpose of obtaining the session key, which under many circumstances would only be used once. This mechanism, if needed, can be specified completely outside the mobile-IPv6 protocol and would amount to a way of creating a dynamic SPI between two nodes which do not share a trust relationship, but which need to agree on a key for some particular purpose (here, allowing the future authentication of a binding update). Hopefully, Photuris [8] will allow this function to be performed appropriately for mobile nodes, say by a Diffie-Hellman key exchange.

B.3. Local Router Considerations

In previous versions of this specification, routers local to the current point of attachment of the mobile node ("local routers") were expected to offer services to mobile nodes. That is still quite feasible, and requires only that the routers support the decapsulation procedure required to extract the packet for final delivery to the mobile node. If every router supports decapsulation (in addition to the operations required from every IPv6 router and IPv6 node), then addresses formed using any prefix advertised by the router could be used as a care-of address except the router's link-local address. Enabling this style of care-of address acquisition will likely require some straightforward enhancements to the IPv6 Neighbor Discovery packet formats. In particular, a Router Advertisement should probably define another per-prefix bit to specify whether the prefix is available to the mobile nodes for constructing a care-of address. For stateful address configuration, an option could be defined to allow the stateful server to notify a mobile node of a legitimate care-of address appropriate for use at the new point of attachment.

Many other operations, related to registration of the mobile node in a new service area, are likely to become important as mobile nodes become more prevalent. For instance, it may be required to:

- authenticate the identity of mobile clients
- charge for connection services
- produce or share a session key for use by new mobile clients (say, for encryption)
- negotiate a compression algorithm
- manage the resources of router's communications devices

B.4. Source Address Filtering by Firewalls

The current specification does nothing to permit mobile nodes to send their packets through firewalls which filter out packets with the "wrong" source IPv6 addresses in the IPv6 packet header. The mobile node's home address may be unlikely to fall within the ranges required to satisfy the firewall's criteria for further delivery.

This subject needs serious discussion soon. As indicated by recent discussion, such firewalls are unlikely to disappear. Any standardized solution [11] to the firewall problem based on hiding the non-local source address outside the source addres field of the IPv6 header is likely to fail. Any vendor or facilities administrator wanting to filter based on the address in the IPv6 source address field would also quickly begin filtering on hidden source addresses.

C. Acknowledgments

Thanks to Thomas Narten for contributing valuable discussion and reviewing this draft, as well as helping to shape some recent changes relevant to the operation of Neighbor Discovery.

References

[1] R. Atkinson. IP Authentication Header. RFC 1826, August 1995.

[2] J. Bound. Dynamic Host Configuration Protocol for IPv6. draft-ietf-dhc-dhcpv6-03.txt -- work in progress, November 1995.

[3] A. Conta and S. Deering. Generic Packet Tunneling in IPv6. draft-ietf-ipngwg-ipv6-tunnel-00.txt - work in progress, November 1995.

[4] A. Conta and S. Deering. Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6). RFC 1885, December 1995.

[5] S. Deering and R. Hinden. Internet Protocol, Version 6 (IPv6) Specification. RFC 1883, December 1995.

[6] IETF Mobile-IP Working Group. IPv4 Mobility Support. ietf-draft-mobileip-protocol-12.txt - work in progress, September 1995.

[7] David B. Johnson and Charles E. Perkins. Route Optimization in Mobile-IP. draft-ietf-mobileip-optim-03.txt -- work in progress, November 1995.

[8] P. Karn and B. Simpson. draft-ietf-ipsec-photuris-08.txt. Internet Draft -- work in progress, November 1995.

[9] T. Narten, E. Nordmark, and W. Simpson. IPv6 Neighbor Discovery. draft-ietf-ipngwg-discovery-03.txt -- work in progress, November 1995.

[10] J. Reynolds and J. Postel. Assigned Numbers. RFC 1700, October 1994.

[11] Fumio Teraoka. draft-teraoka-ipv6-mobility-sup-02.txt. Internet Draft -- work in progress, January 1996.

[12] S. Thomson and T. Narten. IPv6 Stateless Address Autoconfiguration. draft-ietf-addrconf-ipv6-auto-06.txt - work in progress, November 1995.

Authors' Addresses

Charles Perkins
Room J1-A25
T. J. Watson Research Center
IBM Corporation
30 Saw Mill River Rd.
Hawthorne, NY 10532

Work: +1 914 789-7350
Fax: +1 914 784-7007
E-mail: perk@watson.ibm.com

David B. Johnson
Computer Science Department
Carnegie Mellon University
5000 Forbes Avenue
Pittsburgh, PA 15213-3891

Work: +1 412 268-7399
Fax: +1 412 268-5576
E-mail: dbj@cs.cmu.edu