Journal of Mobile Communication 2 (2): 59-63, 2008
ISSN: 1990-794X

Optimal Routing In Mobile IP With Mobile IPv6

[1]P. Harini and [2]O.B.V. Ramanaiah
[1]Department of Information Technology,
St. Ann's College of Engineering and Technology, Chirala, A.P, India
[2]Department of CSE, JNTUCE, Ananthapur, A.P, India

Abstract: In this study, we describe the design of a new protocol for transparent routing of IPv6 packets to mobile IPv6 nodes operating in the Internet. IP is the protocol which provides packet routing and delivery services for the Internet and IP version 6 (IPv6) is a new version of IP intended to replace the current version of IP (IPv4). We have designed protocol enhancements for IPv6, known as Mobile IPv6, that allow transparent routing of IPv6 packets to mobile nodes, taking advantage of the opportunities made possible by the design of a new version of IP. In Mobile IPv6, each mobile node is always identified by its home address, regardless of its current point of attachment to the Internet. While away from its home IP subnet, a mobile node is also associated with a care-of address, which indicates the mobile node's current location. Mobile IPv6 enables any IPv6 node to learn and cache the care-of address associated with a mobile node's home address and then to send packets destined for the mobile node directly to it at this care-of address using an IPv6 Routing header. All IPv6 nodes, whether mobile or stationary, can communicate with mobile nodes.

Key words: Home agent, care-of address, correspondent node, mobile node, cache, binding

INTRODUCTION

This study specifies a protocol which allows nodes to remain reachable while moving around in the IPv6 Internet. With out specific support for mobility in IPv6, packets destined to a mobile node would not be able to reach it while the mobile node is away from its home agent. In order to solve the problems with mobility of nodes, in this study we propose a cache technique. The protocol defined in this study, known as Mobile IPv6, allows a mobile node to move from one link to another with out changing the mobile node's "home address". The mobile IPv6 enables the nodes to cache the binding of a mobile node's home address with its care-of address and to send packets destined for the mobile node directly to it at this care-of address. The Mobile IPv6 protocol is just as suitable for mobility across homogeneous media as for mobility across heterogeneous media. One can think of the Mobile IPv6 protocol as solving the network layer mobility management problem. The design of Mobile IP support in IPv6 also includes some experiences gained from Mobile IPv4 (Perkins, 2002).

BASIC OPERATION

A mobile node is always expected to be addressable at its home address, whether it is currently attached to its home link or is away from home. While a mobile node is at home, packets addressed to its home address are routed to the mobile node's home link, using conventional Internet mechanisms. While a mobile node is attached to some foreign link away from home, it is also addressable to one or more care-of addresses. The Mobile node can acquire its care-of address through conventional IPv6 mechanisms, such as stateless or stateful auto-configuration. Any node communicating with a mobile node is referred to in this document as a "correspondent node" of the mobile node and may itself be either a stationary node or a mobile node. Mobile nodes can provide information about their current location to correspondent nodes. This happens through the correspondent registration. There are two possible modes for communications between the mobile node and a correspondent node. First mode is Bidirectional tunneling and the second mode is "route optimization".

REQUIREMENTS FOR TYPES OF IPV6 NODES

Mobile IPv6 places some special requirements (Brander, 1997) on the functions provided by different types of IPv6 nodes.

The requirements are set for the following groups of nodes:

Corresponding Author: Professor P. Harini, Department of Information Technology, St. Ann's College of Engineering and Technology, Chirala, A.P, India

- All IPv6 nodes.
- All IPv6 nodes with support for route optimization.
- All IPv6 routers.
- All mobile IPv6 home agents.
- All mobile IPv6 mobile nodes.

All IPv6 nodes: Any IPv6 node may at any time be a correspondent node of a mobile node, either sending a packet to a mobile node or receiving a packet from a mobile node.

Ipv6 nodes with support for route optimization: Nodes that implement route optimization are a subset of all IPv6 nodes on the Internet. The ability of a correspondent node to participate in route optimization is essential for the efficient operation of the IPv6 Internet, for the following reasons:

- Avoidance of congestion in the home network and enabling the use of lower-performance home agent equipment even for supporting thousands of mobile nodes.
- Reduction network load across the entire Internet, as mobile devices begin to predominate.
- Reduction of jitter and latency for the communications.
- Greater Likelihood of success for QoS signaling as tunneling is avoided and, again, fewer sources of congestion.
- Improved robustness (Eastlake *et al*., 1994) against network partitions, congestion and other problems, since fewer routing path segments as traversed.

These effects combine to enable much better performance and robustness for communications between mobile nodes and IPv6 correspondent nodes.

All IPv6 routers: All IPv6 routers, even thow not serving as a home agent for Mobile IPv6, have an effect on how well mobile nodes can communicate:

- Every IPv6 router should be able to send an Advertisement Interval Option in each of its Router Advertisements, to aid movement detection by mobile nodes.
- Every IPv6 router should be able to support sending unsolicited multicast Router Advertisements at the faster rate.
- Each router should include at least one prefix with the Router Address (R) bit set and with full IP address in its Router Advertisements.

IPv6 home agents: In order for a mobile node to operate correctly while away from home, at least one IPv6 router on the mobile node's home link must function as a home agent for the mobile node.

IPv6 mobile nodes: The following requirements apply to all IPv6 capable of functioning as mobile nodes:

- The node must maintain a Binding Update List.
- The node must support sending packets containing a Home Address option and follow the required IPSec interaction.
- The node must be able to perform IPv6 encapsulation and decapusulation.
- The node must be able to process type2 routing header.
- The node must support receiving a Binding Error message.
- The node must support receiving ICMP errors.

NEW IPv6 PROTOCOL

Mobility header: The mobility Header is an extension header used by mobile nodes, correspondent nodes and home agents in all messaging related to the creation and management of bindings (Fig. 1).

Format

Payload proto: Eight-bit selector. Identifies the type of header immediately following the mobility header. This is intended to be used by a future extension.

Header len: Eight-bit unsigned integer, representing the length of the Mobility Header in units of 8 octets, excluding the first 8 octets. The length of the Mobility Header must be a multiple of 8 octets.

MH type: Eight-bit selector. Identifies the particular mobility message in question. An unrecognized MH Type field causes an error indication to be sent.

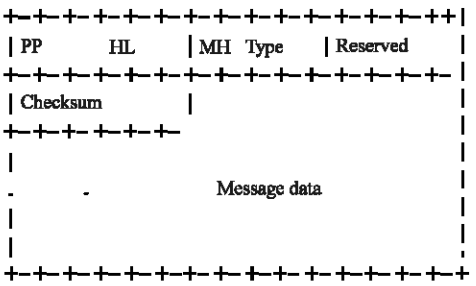

Fig. 1: Frame format of mobility header, PP : Payload Proto, HL: Header Len

Reserved: Eight-bit field reserved for future use. The value must be initialized to zero by the sender and must be ignored by the receiver.

Checksum: Sixteen-bit unsigned integer. This field contains the checksum of the Mobility header.

Message data: A variable length field containing the data specific to the indicated Mobility Header type.

This header is used to carry the following messages:

- Home Test Init.
- Home Test.
- Care-of Test Init.
- Care-of Test.

These 4 messages are used to perform the return rout ability procedure form the mobile node to a correspondent node.

Binding update: A Binding update is used by a mobile node to notify a correspondent node or the mobile node's home agent of its current binding (Perkins, 1996). The Binding Update sent to the mobile node's home agent to register its primary care-of address is marked as a "home registration".

Binding acknowledgement: A Binding Acknowledgement is used to acknowledge receipt of a Binding Update, if an acknowledgement was requested in the Binding Update, the binding update was sent to a home agent, or an error occurred.

Binding refresh request: A Binding Refresh Request is used by a correspondent node to request a mobile node to re-establish its binding with the correspondent node.

Binding error: The Binding Error is used by the correspondent node to signal an error related to mobility, such as an inappropriate attempt to use the Home Address destination option with out an existing binding.

New IPv6 ICMP messages: Mobile IPv6 also introduces 4 new ICMP message types, two for use in the dynamic home agent address discovery mechanism and two for renumbering and mobile configuration mechanisms. The following two new ICMP message types are used for home agent address discovery:

- Home Agent Address Discovery Request.
- Home Agent Address Discovery Reply.

The next two message types are used for network renumbering and address configuration on mobile node.

- Mobile Prefix Solicitation.
- Mobile Prefix Advertisement.

Node keys: Each correspondent node has a secret key, kcn, called the "node key" (Bellovin, 2003), which it uses to produce the keygen tokens sent to the mobile nodes. A correspondent node MAY generate a fresh node key at any time; this avoids the need for secure persistent key storage.

Cookies and tokens: The return rout ability address test procedure uses cookies and keygen tokens (Harkins and Carrel, 1998) as opaque values within the test init and test messages, respectively.

The "home init cookie" and "care-of init cookie" are 64 bit values sent to the correspondent node from the mobile node and later returned to the mobile node.

The "home keygen token" and "care-of keygen token" are 64-bit values sent by the correspondent node to the mobile node via the home agent and the care-of address.

CORRESPONDENT NODE OPERATION

IPv6 nodes with route optimization support maintain a Binding Cache of bindings for other nodes. A separate Binding Cache should be maintained by each IPv6 (Hinden and Deering, 2003) node for each of its unicast routable addresses. Each Binding Cache entry conceptually contains the following fields:

- The home address of the mobile node for which this is the Binding Cache entry. This field is used as the key for searching the Binding Cache for the destination address of a packet being sent.
- The care-of address for the mobile node indicated by the home address field in this Binding Cache entry.
- A lifetime value, indicating the remaining lifetime for this Binding Cache entry.
- A flag indicating whether or not this Binding Cache entry is a home registration entry.

Processing mobility headers: Mobility Header processing (Kent and Atkinson, 1998 a-c) must observe the following rules:

- The checksum must be verified.
- The MH type field must have a known value.
- The Payload proto field must be IPPROTO_NONE.

Packet processing: In this we will describe how the correspondent node sends packets to the mobile node and receives packets from it. In this we will follow:

- Receiving Packets with Home Address Option.
- Sending Packets to a Mobile Node.
- Sending Binding Error Messages.
- Receiving ICMP Error Messages.
- Return Routability Procedure.
- Processing Bindings.
- Receiving Binding Updates.
- Requests to Cache a Binding.
- Requests to Delete a Binding.
- Sending Binding Acknowledgements.
- Sending Binding Refresh Requests.
- Cache Replacement Policy.

HOME AGENT OPERATION

Each home agent must maintain a Binding Cache and Home Agents List. The Home Agents List is maintained by each home agent, recording information about each router on the same link that is acting as a home agent.

Processing mobility headers: All IPv6 home agents are same as correspondent node operation. In this we will follow:

- Processing Bindings.
  - Primary Care-of Address Registration.
  - Primary Care-of Address De-Registration.
- Packet Processing.
  - Intercepting Packets for a Mobile node.
  - Processing Intercepted Packets.
  - Multicast Membership control.
  - Stateful Address Auto configuration.
  - Handling Reverse Tunneled Packets.
  - Protecting Return Routability Packets.
- Dynamic Home Agent Address Discovery.
- Sending Prefix Information to the Mobile Node.

MOBILE NODE OPERATION

Each Mobile node must maintain a Binding Update List. The Binding Update List records information for each Binding Update sent by this mobile node, in which the life time of the binding has not yet expired.

This Mobile Node Operation happens in the following way:

- Packet Processing.
- Home Agent and Prefix Management.
- Movement.
- Return Routability Procedure.
- Processing Bindings.
- Retransmissions and Rate Limiting.

Mobile IPv6 does not attempt to solve all general problems related to the use of mobile computers or wireless networks.

CONCLUSION

Mobile IPv6 enables any IPv6 node to learn and cache the care-of address associated with a mobile node's home address and then to send packets destined for the mobile node directly to it at this care-of address using an IPv6 Routing header. In this Mobile IPv6 there is no need to deploy special routers as "foreign routers" as in IPv4. Mobile IPv6 operates in any location with out any special support required from the local router. Mobile IPv6 route optimization can operate securely even with out pre-arranged security associations. It is expected that route optimization can be deployed on a global scale between all mobile nodes and correspondent nodes. In particular, this protocol does not attempt to solve Handling links with unidirectional connectivity or partial reachability, Access control on a link being visited by a mobile node, Local or hierarchical forms of mobility management, Assistance for adaptive.

REFERENCES

Aura, T. and J. Arkko, 2002. MIPv6 BU Attacks and Defenses. Work in Progress.

Bellovin, S., 2003. Guidelines for Mandating Automated Key Management. Work in Progress.

Brander, S., 1997. Key words for use in RFCs to Indicate Requirement Levels. BCP 14, RFC 2119.

Eastlake, D., S. Crocker and J. Schiller, 1994. Randomness Recommendations for Security. RFC 1750.

Harkins, D. and D. Carrel, 1998. The Internet Key Exchange (IKE), RFC 2409.

Hinden, R. and S. Deering, 2003. Internet Protocol Version 6 (Ipv6) Addressing Architecture. RFC 3513.

Kent, S. and R. Atkinson, 1998a. Security Architecture for the Internet Protocol. RFC 2401.

Kent, S. and R. Atkinson, 1998b. IP Authentication Header. RFC 2402.

Kent, S. and R. Atkinson, 1998c. IP Encapsulating Security Payload (ESP). RFC 2406.

Maugham, D., M. Schertler, M. Schneider and J. Turner, 1998. Internet Security Association and Key Management Protocol (ISAKMP). RFC 2408.

Perkins, C., 2002. IP Mobility Support for Ipv4, RFC 3344.

Perkins, C., 1996. IP Encapsulation within IP, RFC 2003.

Perkins, C., 1996. Minimal Encapsulation within IP, RFC 2004.

Piper, D., 1998. The Internet IP Security Domain of Interpretation for ISAKMP. RFC 2407.