Asian Journal of Information Technology 5(5) : 540-543, 2006

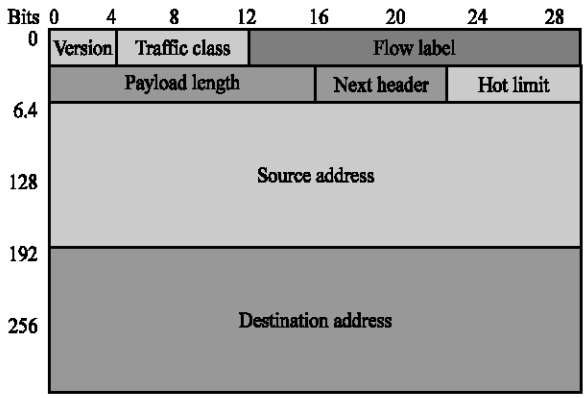
Mobile Ipv6 Protocol and Mobility

Faheem, S.M. and M. Nawaz Brohi
Department of Information Technology, Preston University, Ajman-UAE

Abstract: IPv6 is a protocol which allows nodes to remain reachable while moving around in the Ipv6 Internet. Mobile IPv6 (MIPv6) enables a node to roam around in home and foreign networks while maintaining the active sessions. The network layer hides the change of addresses, while the node is on move, from the upper layers. This study introduces the basic structure of IPv6 header, the concept behind the mobility of a node, the difference in IPv4 and IPv6 headers with respect to mobility. The study also discusses the mechanism of mobility in IPv6, shows how the registration process takes place within the home and foreign networks. Like any other development this protocol too is not a perfect one, and has pros and cons both which are discussed in the end of this study.

Key words: Mobility, care-of-address, binding, home agent, bi-directional tunneling, on-link assumption, general packet radio service (GPRS), Wideband Code Division Multiple Access WCDMA)

IPV6 HEADER STRUCTURE



The IPv6 header is much simpler than that of its predecessor. It contains eight fields at minimum which may form a complete packet structure. There are optional fields known as extension headers. The eight fields are defined as[1]:

Version: 4-bit, Internet protocol number which is equal to 6 for IPv6.

Traffic class: 8-bit ID, which defines how the packet should be handled.

Flow label: 20-bit label, to allow the source to label the packet for special handling.

Payload length: 16-bit, determines the length of the payload.

Next header: 8-bit selector, identifies the type of header following the IPv6 header.

Hop limit: 8-bit unsigned integer, determines the number of forwarding nodes.

Source address: 128-bit, address of the originator

Destination address: 128-bit, address of the recipient

EXTENSION HEADERS

Optional information regarding internet layer is encoded in separate headers that may be placed between the IPv6 header and the upper layer header in a packet. An IPv6 packet may contain 0, 1 or more extension headers. These extension headers are only examined by the end nodes with one exception that Hop-by-Hop header is processed by the interim routers. A complete implementation of IPv6 includes the implementation of the following extension headers:

Hop-by-Hop options: Normally only the terminal node processes extension header. The only exception to this rule is the Hop-by-Hop option header. This header, as the name suggests, specifies a process that must be performed every time the packet goes through a router. It is possible to specify any type of processing. An example of the use of this header is the Jumbogram option (RFC2675). The Payload Length field (specifies the length of the packet excluding the IPv6 header) in IPv6 basic header is 16 bits, so it can only specify up to 65536 octets.

Corresponding Author: Faheem, S.M., Department of Information Technology, Preston University, Ajman-UAE

When it is necessary to send a packet that is larger than this size, Jumbogram option allows you to specify the length of the packet in the extension header.

Routing: The Routing header is used to specify routing path. For example, it is possible to specify which Internet service provider to use, and secure performance for specific purposes. Source node used the Routing header to list addresses of routers that the packet must go through. Addresses specified in this list will be used as destination addresses of this IPv6 packet in the order of the listing and the packet will be sent from one router to another accordingly.

Fragment: The Fragment header is used when the source of IPv6 packet needs to send a packet larger than Path MTU and tells how to reconstruct the packet from its fragments.

Destination options: The destination option header is used to specify a process that needs to be performed by the destination node. It is possible to specify any type of processing.

Authentication and ESP: IPsec is a security mechanism used at the IP layer. All IPv6 node must have IPsec implementation. However, implementation and utilization is a different story, and whether IPsec will be actually used in the communication or not will depend on time and circumstances. When IPsec is used, the Authentication header used for the packet authentication and securing the consistency of data, and the ESP header used for specifying the information relating to data encryption, will be incorporated as extension headers. IPsec is defined as a mechanism that can coexist with IPv4. However, in IPv4, information is placed in Options field.

There is an order of processing the headers and the recommended numbering is:

Ipv6 Header
Hop-by-Hop Options Header
Destination Options Header
Routing Header
Fragment Header
Authentication Header
Encapsulating Security Payload
Destination option Header
Upper Layer Header

Each extension header should occur once with the exclusion that destination header could occur twice at the max.

CONCEPT OF THE MOBILITY OF A NODE

The basic idea behind mobility is the global connectivity of a cellular node, without losing its sessions. There are two widely practiced standards in General Packet Radio Service (GPRS) and Wideband Code Division Multiple Access (WCDMA) mobile networks which are link layer and IP layer mobility. The two systems provide link layer connectivity which could result in loss of IP communication if the node moves out of native network. Mobile IPv6 is the solution to such problem and to facilitate the end-to-end connectivity without losing the sessions between the two nodes. It has been designed to not only to assign static IPv6 addresses but to handle the mobility in GPRS/WCDMA or Multi-access networks. The major benefits include the efficient roaming, IPv6 address assignment, reachability via home address and peer to peer services.

THE DIFFERENCE IN IPV4 AND IPV6 HEADERS WITH RESPECT TO MOBILITY

The design of Mobile IP support in IPv6 (Mobile IPv6) benefits both from the experiences gained from the development of Mobile IP support in IPv4 (Mobile IPv4) and from the opportunities provided by IPv6[2]. Mobile IPv6 thus shares many features with Mobile IPv4, but is integrated into IPv6 and offers many other improvements. This section summarizes the major differences between Mobile IPv4 and Mobile IPv6[3]:

- There is no need to deploy special routers as foreign agents, as in Mobile IPv4. Mobile IPv6 operates in any location without any special support required from the local router.
- Support for route optimization is a fundamental part of the protocol, rather than a nonstandard set of extensions.
- Mobile IPv6 route optimization can operate securely even without pre-arranged security associations. It is expected that route optimization can be deployed on a global scale between all mobile nodes and correspondent nodes.
- Support is also integrated into Mobile IPv6 for allowing route optimization to coexist efficiently with routers that perform ingress filtering.
- The IPv6 neighbor un-reachability detection assures symmetric reachability between the mobile node and its default router in the current location.
- Most packets sent to a mobile node while away from home in Mobile Ipv6 are sent using an Ipv6 routing header rather than IP encapsulation,

reducing the amount of resulting overhead compared to Mobile IPv4.

- Mobile IPv6 is decoupled from any particular link layer, as it uses IPv6 Neighbor Discovery instead of ARP. This also improves the robustness of the protocol.
- The use of IPv6 encapsulation (and the routing header) removes the need in Mobile IPv6 to manage tunnel soft state.
- The dynamic home agent address discovery mechanism in Mobile IPv6 returns a single reply to the mobile node. The directed broadcast approach used in IPv4 returns separate replies from each home agent.

MOBILITY MECHANISM

A mobile node is required to be connected and reachable when needed while it is connected to its native network or outside to other network.

The address assigned by the native network is called the home address, and similarly the address assigned by the outside or foreign network is called care-of-address. A mobile node is recognized by either of these addresses. If a node is in its native network, then the conventional internet routing takes place and the packets are delivered in normal fashion at the home address. The prefix of the node is in accordance with the home network. While the node is moving, it is now recognized by its care-of-address. This address is generated by adding the foreign network suffix to host part. The host part of address can be obtained by stateful or stateless configurations of IPv6. In this case packed destined for this node will now be delivered at its care-of-address [4].

There is a process called binding which takes place when a node leaves it native network and enters a foreign network. This binding ensures that the node's home agent knows where the node is in the IPv6 internet (Fig. 1). As the result of binding, which is a three way handshake process, the packets are continued to be delivered to the node. The first step is initiated by mobile node, upon sensing that network prefix is changed (node is entering into a foreign network), by sending a binding update message to its home agent. The home agent then replies with a binding update msg, which is finally ack by node as binding acknowledgement to the home agent. This completes the binding process between the node and its home agent. When we talk about a mobile node, then there comes another node or nodes to which this mobile node is talking to. In MIPv6 this node is called the correspondent node. Correspondent node may be stationary or mobile itself.

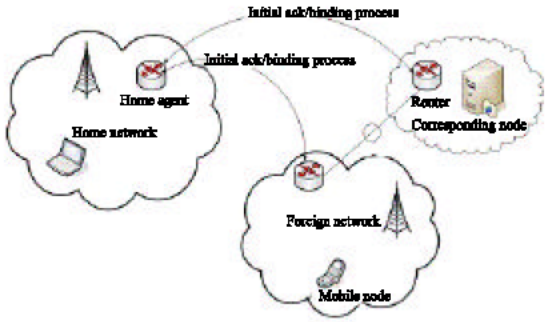


Fig. 1: Mobile Ipv6-conceptul diagram

There are two modes defined for the communication between the mobile node and the correspondent node. The first one is bi-directional tunneling. In this type of communication Packets from the correspondent node are routed to the home agent and then tunneled to the mobile node. Packets to the correspondent node are tunneled from the mobile node to the home agent (reverse tunneled) and then routed normally from the home network to the correspondent node. The other way is a direct communication between the correspondent node and mobile node, once binding is established.

BENEFITS

- A vast range of simpler and secured Internet application.
- Connectivity ranging from desktops to mobile phones, cars, and home appliances.
- Super scalar addressing schemes
- Broadband connectivity
- P2P networking
- 3G mobile networks
- Grid computing
- Car-2-Car
- IP mobility
- Neighbor discovery
- Seamless mobility
- Built-in security and QoS

THINGS TO IMPROVE

As IPv6 is being deployed, many troubles appear. Here are typical problems that were recorded:

- One day a person stayed in a hotel and plugged an Ether cable to the information socket in his room. But Windows could not gain access to any web pages. He asked the hotel and the hotel staff told him, type ipv6 uninstall. After this operation, the Windows came to be on the net. (This is probably because of a poor implemented hotel system.)

- Mozilla on Linux 2.4 takes a few seconds to gain access to web page which is provided with IPv4 but registered with IPv6 as well as IPv4. (This is due to a harmful specification called on-link assumption.)
- When an ISP installed BIND 9 to customer's network, web browsers of the customer became slow to gain access to web pages. (This is because BIND 9 can try to resolve names with IPv6 first even if it does not have IPv6 connectivity, in which case the server will endure hopeless timeouts.)

The causes of these problems include harmful specification, poor implementations, and poor-managed networks. These flaws are minor, though, they are enough to give a bad impression of IPv6 to end users[5].
The purpose of the IPv6 Fix program is to solve such problems as soon as possible. This program is operated by the WIDE project[6].

CONCLUSION

The two widely deployed mobility mechanism GPRS and WCDMA will be very nicely complemented by Mobile IPv6 to support the IP Layer mobility thru out the network. MIPv6 has the inherent feature to support mobility management in Multi Access Networks. Additionally MIPv6 has feasible method to providing IPv6 addresses to the mobile node. Implementation of application layer Mobile IPv6 in 2G and 3G mobile networks basically requires user plane IPv6 support from network, installing a home Agent and implementing IP Security.

REFERENCES

1. Deering, S. and R. Hinden, RFC 2460, Internet Protocol, Version 6 (Ipv6) Specification.
2. Charles, E., Perkins and David B. Johson, RFC 3775, Mobility Support in IPv6.
3. Yaiz, R.A. and O. Oztruk, Mobility in IPv6.
4. Introducing Mobile IPv6 in 2G and 3G Mobile Networks, Nokia.
5. IPv6 Fixes - http://v6fix.net/index.html
6. http://www.v6.wide.ad.jp/