Mobility Support in Internet Protocol Version 6 (MIPv6)

Mansoor Ramzan Baloch[1], Kamran Abid[2]

[1]MSCS Student, SZABIST
Karachi

[2]Pakistan Telecommunication Authority, PTCL
Karachi
Kamran.abid@ptcl.net.pk

Abstract: *The designated successor of IPv4, IPv6 is the next generation internet protocol. It provides a much larger address space, allows address auto-configuration, supports 'any-cast' groups and eliminates the need for triangular routing. This paper discusses IPv6 with specific focus on mobility support in IPv6 (MIPv6), while constantly comparing the IPv4 technology. Although mobile internet protocols are not widely deployed today, MIPv6 is nonetheless an advantage, which will be realized in the future when mobility of nodes becomes a norm.*

Index Terms: *Mobile nodes, internet protocol, IPv6, IPv4, network, handoffs.*

1. INTRODUCTION

When internet and network technologies were not very mature, it was safely assumed that computers would remain stationary and would remain connected to their home networks only. If however such a situation arose where a computer node is required to connect to a different network, it was required by the node to manually configure an IP address thus temporarily losing its ability to communicate.

This paper aims to investigate Mobile IPv6 [3], the protocol that allows nodes to remain mobile and connected to their respective networks.

1.1 Internet Protocol IPv4

The IPv4 [5] protocol, an inter-network layer protocol, widely deployed has been successfully providing network connectivity between various computers since its inception. IPv4 uses 32-bit addresses, a seemingly large range but which limits to only 4,294,967,296 (232) possible unique addresses, a relatively small number for the internet considering the addresses reserved for the private networks.

IPv4 was not capable of handling the mobility between different homogeneous or heterogeneous networks and the need to include the support of mobility with IPv4 arose. Since mobility support was added at a later stage in IPv4, several issues led to emergence of triangular routing [2].

In triangle routing, all packets sent to a Mobile Node must be routed first to the Mobile Node's home subnet and then forwarded to the Mobile Node at its current location by its home agent. Packets sent from a Mobile Node are not forwarded in this way (unless they are destined to another Mobile Node), leading to this triangular combination of the two routes used for all communication between these two nodes.

1.2 Why Do We Need Mobile IP

IPs work very well in their capacity when the nodes are not roaming around and there is a limited requirement for IPs. The IP based routing method is influenced by the hierarchal structure of IP addresses. The following example is used to illustrate this concept:-

A sender at location A sends a message to a receiver at location B. The sender will provide the IP address of the receiver's machine. Only part of the IP address of the receiver is read by the router depending, indicating the address of the domain and finally the machine of the receiver.

If the receiver's machine is a laptop connected to location B but then disconnects from location B and connects to location C, how will the router know where presently the receiver's machine is? Assigning a new IP address to the receiver's machine might be the immediate response, but is it feasible? How will all the IP addresses which intend to transmit to receiver's machine know about *the new IP* address? What about the packets already in transit on the internet while the node moved away? The Domain Name Services (DNS) may not be able to update its internal tables so that the receiver's machine is mapped to its new IP address in a short time period. It will not scale up to support the simultaneous mobility of hundreds of thousands of computers. The above mentioned issues cannot be solved by just IPv4, hence the need to provide mobility support in IPv4.

2. INTERNET PROTOCOL VERSION 6

Developed by Internet Engineering Task Force (IETF) [6], the principle standards development body for the internet, IPv6 is a new internet protocol which is to replace IPv4. The address space in IPv6 has been increased to 128 bit long addresses from 32 bit length in IPv4. This vast library of addresses accommodates all the current IPv4 addresses available and has some space reserved for the Link-Local Addresses. Nodes on a local network communicate with each other using link-local addresses without the usage of routers. These link-local addresses are thus unique in a local network. Neighbor Discovery Protocol, as used in IPs, helps the nodes discover each other's company and MAC addresses.

In addition to the capabilities it inherits from previous IPs, IPv6 also realizes local routers and network prefixes. IPv6 has been extended from previous IPs, by the inclusion of additional information in the headers of its packets as shown in Figure 1. The IPv6 extension headers [2] include:

Destination Options Header [3] carries the sequence of options to be processed when the packet reaches the final destination node.
Hop-to-Hop Options Header [3] carries the sequence of options to be processed by each intermediate router when the packet arrives.

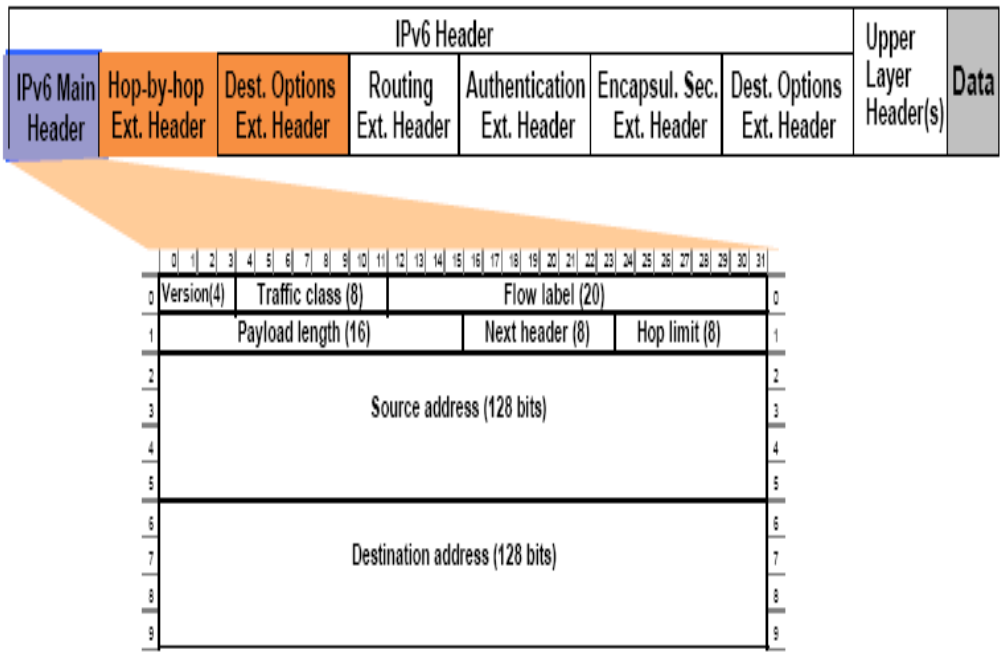

Figure 1: IPv6 Header [3]

- Routing Header [3] similar to Source Route in IPv4 is not examined/processed until it reaches the next node identified in the route. Also the destination node may not necessarily send packets through the same route from where it has received packets.
- Authentication header [3] provides optional authentication data which allows the receiver to verify the authenticity of the packet sender and protects against any modification of the packet. There exists a security association between the sender and receiver, which can be manually configured and automatically established.

2.1 Basic Overview of Mobile IPv6

The development of a completely new protocol gave the opportunity to incorporate mobility support right into the protocol. IPv6 avoids the problem of triangular routing which was a major cause of inefficiency in IPv4 mobility support.

IPv6 is derived from IPv4 and in many ways is similar to it, and mobility support of IPv4 nodes could be adapted for use in IPv6 with only the straightforward changes needed to accommodate differences between IPv4 and IPv6.

The key components of Mobile IPv6 as depicted in Figure 2 are Home Agent, Mobile Node and Correspondent Node. Each Mobile Node is assigned an IP address (permanent) in the same way as any other node, and this IP address is known as the Mobile Node's home address. A Mobile Node's home address remains unchanged regardless of where the node is attached to the internet.

The IP subnet indicated by this home address is the Mobile Node's home subnet, and standard IP routing mechanisms will deliver packets destined to a Mobile Node's home address only to the Mobile Node's home subnet. A Mobile Node is simply any node that may change its point of attachment from one IP subnet to another, while continuing to be addressed by its home address. Any node with which a Mobile Node is communicating is referred to as a correspondent node, which itself may be either mobile or stationary.

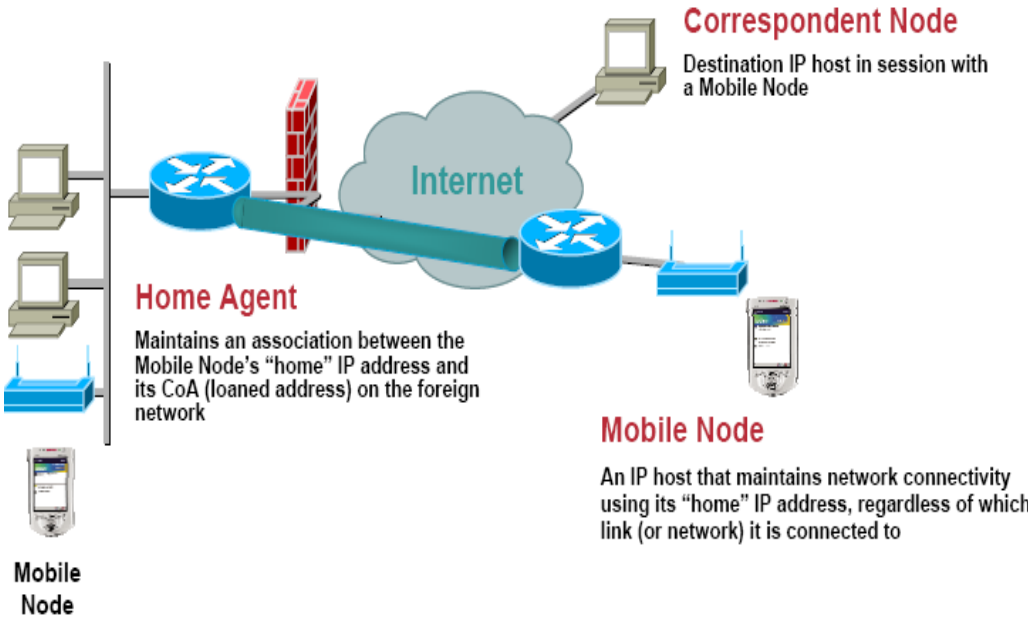

Figure 2: Key Components of Mobile IPv6 [5]

A Mobile Node's current location while away from home is known as its care-of address, which is a globally routable address acquired by the Mobile Node through IPv6 address auto-configuration in the foreign subnet being visited by it. The association of a Mobile Node's home address with a care-of address, along with the remaining lifetime of that association, is known as a binding. While away from its home subnet, a router on the Mobile Node's home subnet, known as its home agent, maintains a record of the current binding of the Mobile Node. The Home Agent then intercepts any packets on the home subnet addressed to the Mobile Node's home address and tunnels them to the Mobile Node at its current care-of address.

This tunneling uses IPv6 encapsulation and the path followed by a packet, while it is encapsulated, is known as a tunnel. Once a correspondent node has learned the Mobile Node's care-of address, it may cache it and route its own packets for the Mobile Node directly there using an IPv6 routing header, bypassing the home agent completely. The most important function needed to support mobility is the reliable and timely notification of a Mobile Node's current care-of address to those other nodes that need it, in order to

avoid the routing anomaly known as triangle routing.

Triangle routing as shown in Figure 3, because of its poor route selection, has many problems, including:

- increased impact of possible network partitions;
- increased load on the network; and,
- increased delay in delivering packets.

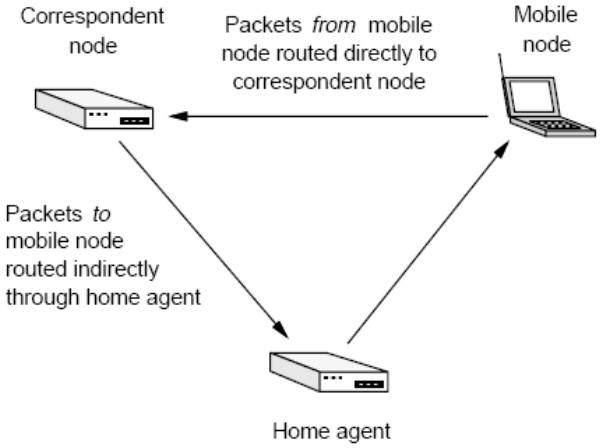

Figure 3: Triangular Routing Problem [1]

2.2 Protocol Comparison: Mobile IPv4 and Mobile IPv6

Mobile IPv6 benefits from the opportunities provided by IPv6 and from the lessons learned from Mobile IPv4. Additionally, mobility was a core factor in the design of

IPv6, whereas it was an afterthought in the design of IPv4. For these reasons, Mobile IPv6 has several core operational advantages over Mobile IPv4. The following is a list of the major differences between Mobile IPv4 and Mobile IPv6:

- IPv4 addresses are 32 bits long. IPv6 addresses are 128 bits long, which almost eliminates the possibility of using up all the addresses in IPv6.

- IPv4 uses Network Address Translation (NAT) [4] to conserve the number of public IP addresses an organization can use on networks like the internet. IPv6 eliminates the need for NAT.

- Mobile IPv4 uses tunnel routing to deliver packets to Mobile Nodes. Mobile IPv6 uses tunnel routing and source routing with IPv6 headers.

- Mobile IPv4 deploys Foreign Agents [1] for Mobile Node movement detection and to de-capsulate packets addressed to the Mobile Node's care-of address [1]. IPv6 Mobile Nodes de-capsulate messages sent to the care-of address itself, and uses IPv6 Router Advertisements for movement detection, thereby eliminating the need for Foreign Agents.

- Mobile IPv4 uses Agent Discovery for Movement Detection. Mobile IPv6 uses IPv6 Router Discovery.

- Mobile IPv4 Route Optimization is an extension to the protocol, not part of the base RFC [5]; requires preconfigured and static security associations; and, is difficult to operate with ingress-filtering routers. Mobile IPv6 Route Optimization [6] is a fundamental part included in the protocol; integrated Return Routability to dynamically secure Route Optimization; and, operates effectively with ingress-filtering routers.

- Mobile IPv4 reverse tunneling is an extension to the protocol. Mobile IPv6 bi-directional tunneling is part of the core protocol.

- Mobile IPv4 uses one home address. Mobile IPv6 uses a globally routable home address and a link local home address.

- Mobile IPv4 uses Address Resolution Protocol (ARP) [2] to determine the link-layer address of neighbors. Mobile IPv6 uses IPv6 Neighbor Discovery and is de-coupled from any given link-layer.

- Mobile IPv4 Dynamic Home Agent Address Discovery [6] uses broadcast approach and returns separate replies from each Home Agent to the Mobile Node. Mobile IPv6 Dynamic Home Agent Address Discovery uses any-cast addressing and returns a single reply to the Mobile Node.

- Mobile IPv4 Mobile Nodes can obtain care-of addresses via Agent Discovery, DHCP, and manual configuration. Mobile IPv6 Mobile Nodes can obtain care-of addresses via Stateless Address Auto-configuration [4], DHCP, and manual configuration.

- Mobile IPv4 uses Foreign Agent care-of address and a co-located care-of address. Mobile IPv6 care-of addresses are all co-located.

3. OPERATION OF MOBILITY PROTOCOL (MIPv6)

Mobile devices, just like stationary entities, have a permanently assigned home IP address corresponding to its home network and can communicate with networks it finds in its range of wired or wireless communication. It uses a second address called the Link-Local address.

When a Mobile Node moves from its home network, it enters a foreign network. Any node (mobile or stationary) trying to communicate with the Mobile Node is called the correspondent node. Mobile IPv6 adds a third address, known as the Mobile Node's care-of address, which is associated with the Mobile Node only while visiting a particular foreign subnet. The network prefix of a Mobile

Node's care-of address is equal to the network prefix of the foreign subnet being visited by the Mobile Node, and thus packets addressed to this care-of address will be routed by normal internet routing mechanisms to the Mobile Node's location away from home. Figure 4 shows a Mobile Node at its home network.

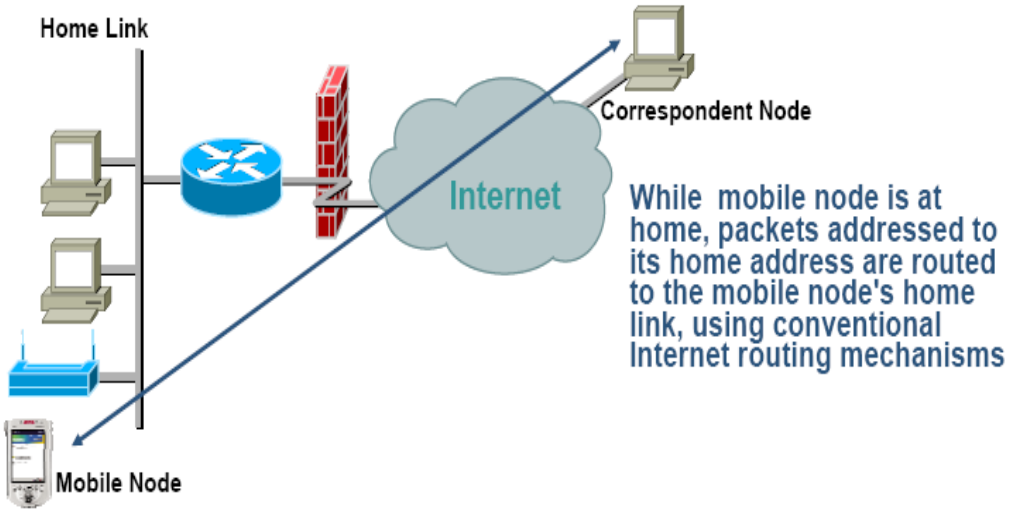

Figure 4: Mobile Node at its Home Network [5]

Each time the Mobile Node moves its point of attachment from one IP subnet to another; the Mobile Node will configure its care-of address by stateless address auto-configuration, or alternatively by some means of state-full address auto-configuration such as DHCPv6 or PPPv6.

While away from home, a Mobile Node registers one of its bindings with a router in its home subnet, requesting this router to function as the home agent for the Mobile Node. The care-of address in this binding registered with its home agent is known as the Mobile Node's primary care-of address, and the Mobile Node's home agent retains this entry in its Binding Cache, marked as a 'home registration', until its lifetime expires.

While it has a home registration entry in its Binding Cache, the home agent uses proxy Neighbor Discovery to intercept any IPv6 packets addressed to the Mobile Node's home address on the home subnet, and tunnels each intercepted packet to the Mobile Node's primary care-of address. To tunnel the packet, the home agent encapsulates it using IPv6 encapsulation. This process avoids the triangular routing problem, since the packet does not have to pass the home agent.

The detailed explanation of this process is mentioned step-by-step in the following sections:

3.1 Entering a Foreign Network

Mobile Nodes make use of the IPv6 Neighbor Discovery protocol to detect mobility. Unreachability Detection indicates when the Mobile Node has moved out of the coverage of its current router. For wireless networks, Mobile Nodes can also detect that it has moved into a new network as shown in Figure 5, when the signal strength from the current base station falls below a threshold. Router Discovery is used to find a new router in the network. This is done by listening to the periodically broadcast Router Advertisement [5] messages.

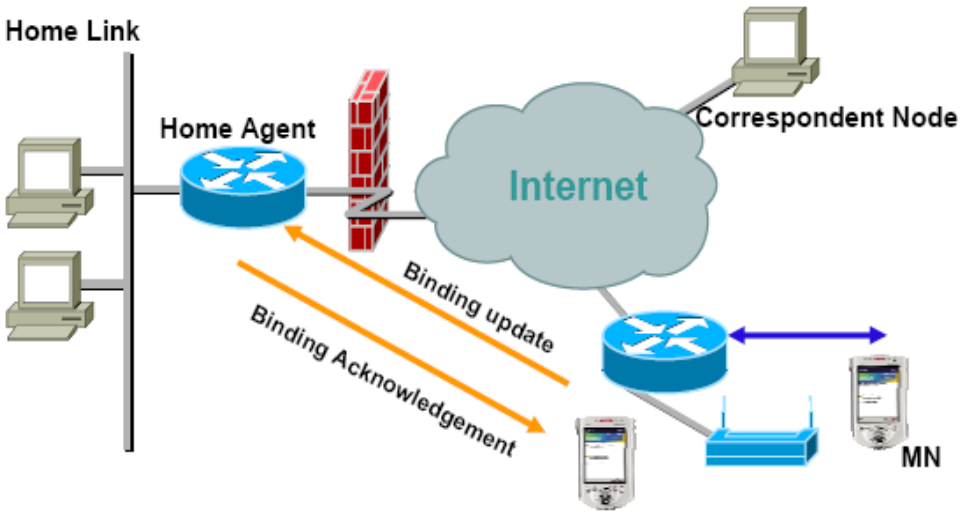

Figure 5: Mobile Node moving to a new network [5]

On the basis of the information contained in the Router advertisements, the Mobile Node configures its care-of address and sets it Default Router entry to be used to send packets while in the foreign network. In Mobile IPv4, the Router Advertisements are broadcast by the Foreign Agents and contain the care-of address to be used. In IPv6, the explicit notion of Foreign Agents has been done away with and the Mobile Node configures its care-of address. The minimum interval between two advertisements is 3 seconds. This lag of 3 seconds may work fine for wired networks. However, for wireless networks, it will be a hindrance to smooth handoffs. The Mobile Node need not always wait for a Router Advertisement as it may send Router Solicitation messages. We must keep in mind that Mobile Nodes are often constrained in processing capabilities and work on limited battery power. In such a case, continuously listening for Router Advertisements leads to the expenditure of scarce battery power.

The Mobile Node should try to remain in doze mode for as long as possible. However, the Mobile Node should also constantly monitor for unreachability of its current default router—an indication that the Mobile Node has changed location. No clear solution exists for how the Mobile Node can optimally conserve resources while listening to Router Advertisements. We must also note that sending Router Solicitations is a very costly operation and may lead to network congestion if a large number of Mobile Nodes attempt it simultaneously.

3.2 Acquiring a Care-of-Address (CoA)

A Mobile Node on entering a new network must first acquire a care-of address. Stateless auto-configuration is used by the Mobile Node for this purpose. This does away with the need for Foreign Agents or DHCP servers, which were required in Mobile IPv4.

The auto-configuration process includes creating a link-level local address for the Mobile Node in its current network and also verifying its uniqueness on the link. It also determines the information to be auto-configured like default router information and care-of addresses. This can be done in a stateless or stateful manner. The stateful approach is taken in the DHCP v6 protocol (not dealt with in this paper). Stateless auto-configuration requires no manual configuration of hosts or servers, the host generates its own address using a combination of locally available information and the information available in the Router Advertisements. The subnet prefixes are taken from the Router Advertisements while the Mobile Nodes generate unique interface identifiers. These two are combined to get the care-of address. Of course, the address generated should be verified to be unique using the Duplicate Address Detection Algorithm. The generated care-of addresses are also associated with a lifetime. Here we must also note that IPv6 provides an extremely large number of IP addresses (due to its 128 bit length). In IPv4, the luxury of assigning a unique care-of address to every roaming Mobile Node was not possible due to IP address shortage.

3.3 Registering with the Home Agent

After acquiring a Care of Address in the foreign network, the Mobile Node should register this care-of address with a machine or router in its home network known as the Home Agent. In the case of Mobile IPv4, this registration process is handled with the support of the Foreign Agent. In Mobile IPv6, there is no Foreign Agent and the Mobile Node

directly sends a Binding Update [4] to the Home Agent. The Home Agent creates an entry for the Mobile Node's care-of address in its Binding Cache and sends a binding acknowledgment back to the Mobile Node. The Home Agent also sends out IPv6 Neighbor Discovery messages for the Mobile Node in the home network. This is done so that all the packets received for the roaming Mobile Node are sent to the Home Agent, to be in turn tunneled to the Mobile Node.

3.4 Dynamically Finding a Home Agent

The Home Agent of a network may change over a period of time—the machine may have been replaced by another one. In such a scenario, a currently roaming Mobile Node belonging to a particular home network will not be aware of this change of Home Agent Address. IPv6 supports the dynamic discovery of Home Agents. The Mobile Node sends the registration Binding Update to the Home Agent IPv6 any cast address which will be invariant. Exactly one Home Agent responds, it rejects this Binding Update but sends a list of Home Agent addresses in decreasing order of preference back to the Mobile Node. Now the Mobile Node tries to register with the Home Agents in the list one by one in decreasing order of priority, till the registration succeeds.

3.5 Binding Caches and Binding Updates

The Binding Caches [6] and Binding Updates are very important to Mobile IPv6. Binding Updates are used by the Mobile Node to register with its Home Agent and also to inform Correspondent Nodes about its current location.

A binding is an association between the home address of the Mobile Node and its care-of address, along with the remaining period of association. This binding is stored in the Binding Cache of the node. Each IPv6 node has a Destination Cache into which the Binding Cache can be easily integrated. The binding is created on receiving a Binding Update message. The Binding Cache follows a cache replacement policy like LRU (Least Recently Used). IPv6 defines several extension headers—Routing, Authentication, Destination Options and Hop-by-Hop Options.

The Binding Updates are sent as part of the Destination Options Header of an IP packet. This implies that the Binding Update messages can be sent along with other data packets, thus saving network bandwidth. The current care-of address of the Mobile Node is specified inside the message. The home address of the Mobile Node is obtained from the source address in the packet header. A life time held in the Binding Update message specifies the number of seconds for this binding is to be considered valid. The binding should be refreshed before it expires.

Each Binding Update is also associated with an Id held, which ensures that the updates are applied in the correct order. The value of Id is incremented each time a node sends a Binding Update. The setting of the H bit indicates a request to the node receiving the update to serve as a Home Agent for the Mobile Node. This bit is set during the Home Agent registration.

A Binding Acknowledgment may be requested by setting the A bit of the Binding Update. If the acknowledgment is not received within a timeout period (starting at 1 second), the Mobile Node keeps retransmitting the update with an ex-potential back-off in the timeout period. The acknowledge option is used mainly in the case of Home Agent registrations and not with Correspondent Nodes. The Binding Update feature of Mobile IPv6 is the target of hacker attacks like the Remote Indirection attack.

3.6 Sending and Receiving Data

This section describes how a node receives and sends packets while it is away from its home network as shown in figure 6 and figure 7. We have already seen the process of obtaining a care-of address and registering with the Home Agent.

3.6.1 From Correspondent Node to Mobile Node

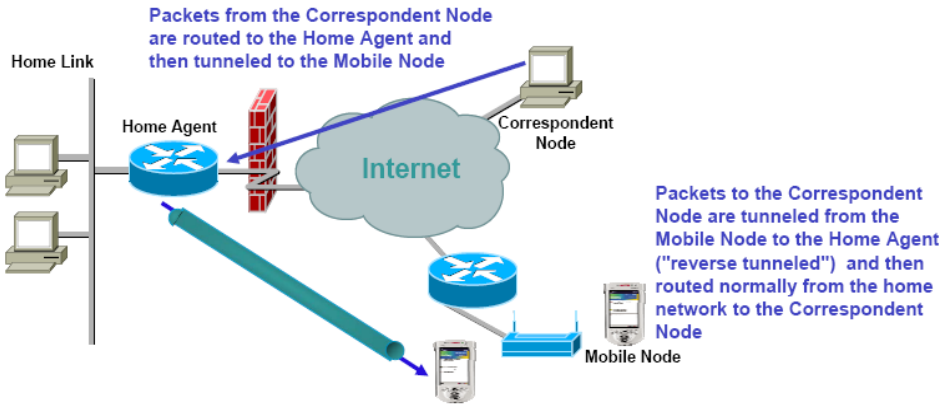

Figure 6: Packet Forwarding to a Mobile Node [5]

When a Correspondent Node wishes to send a packet to the Mobile Node, it first looks in its Binding Cache for the Mobile Node's current care-of address. If no care-of address is found, the Correspondent Node sends the packet to the Mobile Node's Home IP Address. When this packet reaches the Home Network, it is intercepted by the Home Agent. It is the responsibility of the Home Agent to correctly forward the packet to the Mobile Node at its current care-of address, looked up from its Binding Cache. The Home Agent encapsulates this packet in the payload held of another IP packet addressed to the Mobile Node's current care-of address. The source head of this outer packet is set to the Home Agent's IP address. This is called IPv6 encapsulation. This packet reaches the Mobile Node at its care-of address where it is de-capsulated and sent locally within the Mobile Node itself as packet from the Correspondent Node. Thus, the higher layers of the networking protocol stack see the packet as having directly originated from the Correspondent Node and process it appropriately.

Many fields of the original header are duplicated during IP-in-IP encapsulation. This waste of bandwidth due to redundancy may be decreased by using a form of encapsulation called minimal encapsulation. When a Mobile Node receives an encapsulated packet from the Correspondent Node via the Home Agent, it immediately sends a Binding Update to the Correspondent Node. Once the binding is created in the Correspondent Node's Binding Cache, packets may be directed to the Mobile Node without the help of the Home Agent. This avoids the problem of triangular routing. The packet is addressed to the care-of address of the Mobile Node. However, the home address of the Mobile Node is indicated as the final destination using theIPv6 Routing Headers. When this packet reaches the Mobile Node, normal IPv6 processing of the Routing Header is done and the packet gets delivered to the higher layers of the protocol stack using the Mobile Node's home address. The binding is maintained by the Mobile Node by sending more update messages before the expiry time of the binding. When the Mobile Node moves into a new network, the Mobile Node sends the Binding Update messages with the new care-of address to its Home Agent and all currently corresponding nodes.

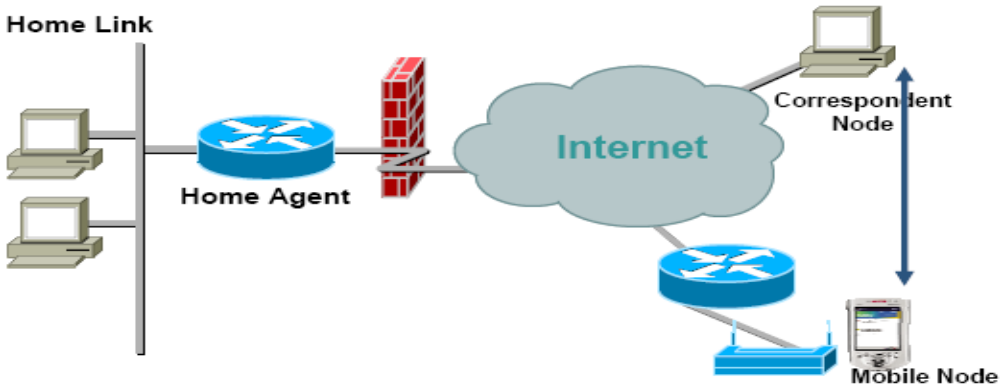

Figure 7: Communication between Correspondent and Mobile Node [5]

An expected question now is why the Home Agent uses encapsulated packets to create a tunnel to the Mobile Node rather than using Routing Headers which are more efficient. The Home Agent does not alter the Routing Header because doing so will destroy the IPv6 authentication i.e. the signature made by the Correspondent Node will not be valid when the packet is authenticated at its destination Mobile Node.

Hence, Home Agents use tunneling instead of Routing Headers. In Mobile IPv4, the Correspondent Nodes send the packets to the Home Agent which then tunnels the packet to the Mobile Node's Foreign Agent. Although extensions envisage the use of a Binding Cache, most nodes on the internet do not support it and hence it is not prevalent. All communication from the Correspondent Node to Mobile Node is only through the Home Agent. This is highly inefficient and makes the Home Agent a bottleneck.

3.6.2 From Mobile Node to Correspondent Node

When the Mobile Node wants to send a packet to the Correspondent Node, it does so directly through the foreign network router discovered when it first entered the network. The IP packet is addressed to the Correspondent Node and carries the Mobile Node's home address as the source address. This communication with the Correspondent Node does not involve the Home Agent of the Mobile Node neither in Mobile IPv6 nor in Mobile IPv4.

3.7 Solving the Triangular Routing Problem

In Mobile IPv6, every IP node has a binding cache to store the care-of address of the Mobile Node. The Binding Updates and Binding Acknowledgment messages help in maintaining the appropriate bindings in the Binding Cache. The triangular routing problem takes place only for a short initial period of the Correspondent Node's communication with the Mobile Node. This is one of the major strengths of Mobile IPv6.

3.8 Smooth Handoffs

When a Mobile Node moves from one foreign network to another, it is assigned a new care-of address, but packets in transit at that moment might be lost since they are addressed to the previous care-of address. This problem is solved because the Mobile Node, which has moved to a new network, sends a Binding Update to the router in the previous foreign network. The previous foreign network now serves as a temporary home network for the Mobile Node. When a packet arrives at the previous care of address, the router tunnels it forward to the new care-of address, the same way a home agent does for the Mobile Node. This allows the Mobile Node to move around wireless networks without having to worry about losing data being sent or received.

4. ADVANTAGES OF MIPv6

In this section, we will discuss various advantages of Mobile IPv6, some of which have already been mentioned earlier.

- One of the main problems faced by IPv4 was the shortage of IP addresses. In such a situation, it was not possible to assign separate care-of addresses (or correlated IP addresses) for each Mobile Node in a foreign network. Mobile IPv6, with 128 bit IP addresses makes it possible even to assign multiple CoAs to roaming Mobile Nodes.

- The Mobile Nodes acquire care-of address using the IPv6 stateless address auto-configuration methods and

neighbor discovery mechanisms. There is no need for a Foreign Agent as in the case of Mobile IPv4.

- Triangular routing was a major problem in Mobile IPv4. However, the Binding Cache present in all IPv6 nodes mitigates this problem to a large extent. Also, the Binding protocol is uniformly handled by all nodes—correspondent nodes, home agents and foreign routers.

- Security is an integral part of IPv6, and the IPSEC features are built into each IPv6 node. As against in Mobile IPv4, security features like authentication of registration messages, and data integrity, do not have to be handled separately.

- Mobile IPv6 offers an elegant solution for dynamically discovering Home Agents through IPv6 any-cast addresses. Such a feature was not available in Mobile IPv4.

- Mobile IPv6 allows nodes to surpass ingress filtering by using the care-of address of the Mobile Node as the source address of the packet to be sent to the Correspondent Node. The home address of the Mobile Node is specified in the home address destination option.

5. PROBLEMS OF MIPv6

Regardless of Mobile IPv6's benefits, there are few problems associated with Mobile IPv6. First of all the difficulties to Mobile IP caused by packet filtering at firewalls have not been completely solved.

Mobile IPv6 does not also deal with Home Agent failures, although it does allow dynamic Home Agent discovery. We propose a solution in which the multiple home agent capable machines present in the network balance the load of roaming Mobile Nodes among themselves.

They also monitor whether the other Home Agents are functioning properly. If one of the Home Agents is noticed to be down, then another Home Agent can automatically take over the roaming Mobile Nodes currently being served by the dead Home Agent. A message is sent to the Mobile Node informing it about the change. The bindings from the dead Home Agent should be salvaged from periodic backups to a highly reliable central storage or to all the Home Agents. If the roaming Mobile Node by itself detects that its Home Agent has gone down e.g. by long periods of silence from the Home Agent, it can send a distress signal to the anycast address. Then another Home Agent will take over. This is just a preliminary proposal. More work is required in developing the detailed protocol and its functioning is to be analyzed.

Preserving the location privacy of the Mobile Node is a matter of concern. Authentication of the node before sending a Binding Update to it and encryption of the update message can solve the problem to an extent. Now suppose the Mobile Node requires to communicate with a Correspondent Node without revealing its current location. Of course, triangular routing through the Home Agent is a solution but it is highly inefficient. The problem remains unsolved.

Mobile Nodes connected to the network via wireless links may change their locations at a very fast pace. This leads to a very large number of Binding Update messages being sent to the Home Agent and the Correspondent Nodes, which in turn causes network congestion. In the case of Mobile IPv4, solutions to avoid this problem by clustering Foreign Agents and sending location updates to the Home Agent only on changing clusters have been proposed. A similar solution can be adapted for Mobile IPv6 keeping in mind the absence of foreign agents.

6. CONCLUSION

This paper has discussed the Mobile IPv6 protocol step by step with the aid of a running example. Each step was also compared with the corresponding procedures in Mobile IPv4. With the expected large scale use of IPv6 in the future, network connectivity for Mobile Nodes is sure to become seamless and efficient. A very large number of mobile devices of all types and sizes will use this support to access the internet and to communicate with each other. There are already many implementations of Mobile IPv6 existing, both in the industry and academia. With widespread use and active research, the protocol is sure to evolve to support newer requirements and to achieve greater efficiency and efficacy in mobile communications.

REFERENCES

[1] Charles E. Perkins and David B. Johnson. 'Mobility Support in IPv6,' in Proceedings of the Second Annual International Conference on Mobile Computing and Networking, Rye, New York, 1996.

[2] Claude Castelluccia. Towards a Hierarchical Mobile IPv6, IEEE, France.

[3] Claude Castelluccia. ‘A Hierarchical Mobilility Management Scheme for IPv6’, in Proceedings of the Third IEEE Symposium on Computers and Communications, Athens, 1998.

[4] David Johnson et al.. (ed.). ‘Mobility Support in IPv6’, Request For Comment, RFC3775, 2004.

[5] Dilip A. Joseph. Mobility Support in IPv6. IEEE, IIT Madras, India.

[6] Pravin Bhagwat, Satish Tripathi and Charles Perkins. ‘Network Layer Mobility: An Architecture and Survey’, Technical Report CS-TR-3570, University of Maryland, 1995.

[7] Ramón Cáceres, Venkata N. Padmanabhan. ‘Fast and Scalable Handoffs for Wireless Internetworks’, Proceedings of the Second Annual International Conference on Mobile Computing and Networking, Rye, New York, 1996.