ISBN-978-93-5288-834-3

A Review of Mobile IP

Md Sahim Raza[1], Vinay Prakash[2]
[1] *Department , College of Computer Science And Information Technology,Teerthanker Mahaveer University Moradabad,India*
[3] *Department , College of Computer Science And Information Technology,Teerthanker Mahaveer University Moradabad,India*
[1]sahimraza123@gmail.com
[2]vinayvaish@gmail.com

Abstract— **The Mobile Internet Protocol (Mobile IP) is an extension to the Internet Protocol proposed by the Internet Engineering Task Force (IETF) that addresses the mobility issues. In order to support un-interrupted services and seamless mobility of nodes across the networks (and/or sub-networks) with permanent IP addresses, Handoff is performed in mobile IP enabled networks services. Handoff in a mechanism that initiated due to performance degradation in terms of increased latency and packet loss. The convergence of three technology paradigms, viz. light-weight portable computers, the spread of wireless networks and services, and the ubiquitous Internet, aimed at allowing users the freedom to connect to the Internet at any time and in any place, to read email, query databases, retrieve information from the web or to entertain themselves, makes mobile computing a very promising prospect as well as a very formidable challenge. This paper details the mechanism of operation of Mobile IP network protocol, designed and developed to enable efficient and effective communication between a mobile host and a remote server.**

Keywords— **Mobile IP, Routing in the Internet, Hierarchical Mobile IP, Fast Handover**.

I. INTRODUCTION

Mobile Computing is becoming increasingly important due to the rise in the number of portable computers and the desire to have continuous network connectivity to the Internet irrespective of Internet infrastructure is built on top of a collection of protocols, called the TCP/IP the physical location of the node. The protocol suite. Transmission Control Protocol (TCP) and Internet Protocol (IP) are the core protocols in this suite. IP requires the location of any host connected to the Internet to be uniquely identified by an assigned IP address. This raises one of the most important issues in mobility, because when a host moves to another physical location, it has to change its IP address. However, the higher level protocols require IP address of a host to be fixed for identifying connections. The **Mobile Internet Protocol** (Mobile IP) is an extension to the Internet Protocol proposed by the Internet Engineering Task Force (IETF) that addresses this issue. It enables mobile computers to stay connected to the Internet regardless of their location and A fully deployed wide-area Mobile IP system will allow the nomadic user to plug her palmtop computer into a network in a conference room or at a coffee house without a need for her to reconfigure her machine. She would be able to create and maintain a video-conferencing session even while moving between the building's internal wireless local area network (WLAN) and an external wide-area wireless data network. When visiting another company she would be able to plug her laptop into a "foreign" LAN and using cryptographically secure communications, mount file systems from her own company to get complete access to all her personal files, databases, email, and other similar resources. It is useful to note here that although Mobile IP has been designed with the future in mind, the scenarios just described can already be achieved today using hardware that is already commercially available. Looking towards the future, we can expect IP to be the pervasive communication protocol across a diverse set of devices, not just limited to computers. For example, a person's wristwatch could have a miniature network transceiver and an IP address so that no matter where she goes she will be able to access her email by connecting to whichever IP network exists in her vicinity. Similarly sophisticated instrumentation such as moving robots will be able to communicate wirelessly with their home networks without the need for configuration as they move to different geographic areas and between different subnets, automatically receiving software updates and command messages from their control servers. In summary, the demand for Mobile IP will be limited only by the need to support seamless mobile data communication between homogeneous and heterogeneous networks.

ISBN-978-93-5288-834-3

Fortunately, due to the medium-independent design philosophy, Mobile IP does not require specialized hardware and several software implementations are already available freely . Thus the cost of deployment is mostly from constructing the infra-structure of wireless and wired networking hardware. Anytime, anywhere, to anyone communications can be made transparent, robust and seamless with Mobile IP. IP in today's mobile world and point out reasons why other solutions such as Cellular Digital Packet Data (CDPD) are geographically constrained and do not support seamless heterogeneous mobility. We follow this with a section describing how Mobile IP works, including the entities involved, and how packets are routed to mobile nodes within the Internet. Next, we discuss some of the challenges Mobile IP has faced over its evolution and the availability of some implementations. We conclude with our perspectives on the future of Mobile IP and its relation to the next generation of IP protocols.

II. ROUTING IN THE INTERNET

To appreciate Mobile IP, we have to first consider how the Internet works normally. The Internet provides a means of letting geographically separated users exchange messages in the form of voice, data, and video packets. Occasionally, the devices ("nodes") employed by the users to communicate over the Internet are physically linked to each other and messages can be exchanged directly. However, due to serious scalability limitations arising out of directly connect ingmillions of nodes, a majority of the time there are no such direct links and packets have to traverse several intermediate nodes before reaching their final destination. These message packets are able to reach their destination because the intermediate nodes cooperate with them and with each other by "routing" the packets appropriately and towards the final destination node. These intermediate nodes are thus called routers. Since routing in the Internet is based on the address of the destination node, it is intimately influenced by how addresses are assigned to the communicating nodes. The Internet is made up of millions of subnets. A subnet is a network of nodes that may be common to an organization such as a university campus or a corporation. If there are more nodes in the organization than can be accommodated within a single subnet additional subnets can be created for the same organization. Every node on the Internet has a unique 4 byte IP address. Out of these 4 bytes, as many as 3 bytes may be used to identify the node's subnet. The node's unique address within the subnet is assigned from a pool of addresses known to the maintainer of the subnet. Address assignment and subsequent configuration within the node is done either manually or automatically. Furthermore, addresses are given out either as static IP addresses, that is, nodes are identified by the same IP address always, or dynamically via a protocol such as the Dynamic Host Configuration Protocol (DHCP), in which case the IP address is leased to the node for a finite period of time with the provision that the node can renew its lease every time it needs to. Each router on an IP network can contain three different types of routing table entries. These are described as either host-specific, network-specific, or default routing entries. Host-specific routes are typically for delivering packets to nodes that are connected to the router directly via a particular network interface. Host-specific route entries therefore provide a one-to-one mapping between the destination IP address and the specific interface used to forward the packet. Network specific route entries are used for routing packets according to the destination node's subnet location. Thus the bits in the IP destination address which represent the subnet which the destination node is on, are used to determine which network interface the packet is to be forwarded with. Default-routing table entries are for addresses whose appropriate network interface cannot be resolved either via host-specific routes or via network-specific routes. In this case the router simply forwards the packet to the "next-

ISBN-978-93-5288-834-3

hop" router with the hope that the next router will know how to further route the packet properly. Network-specific routing tables entries and the default routing table entries are the key to the scalability of the Internet. By determining the subnet address in the header field of the packet, routers between the destination and source nodes select the next node, or next-hop that should receive the packet. Thus even though intermediate nodes do not necessarily know how to get data to a particular destination node, they do know how to get data to a node that does. With only a few properly selected routers, all nodes on the Internet can reach all other nodes. In general routers are specially-constructed hardware devices dedicated to the task of routing several million packets every second, we will often use the term router to refer to any general purpose machine which can forward packets, not destined for them, across the network. Thus our definition of routers can often apply to machines which appear to be simply "hosts" or "nodes" (i.e. PCs or workstations) on the network. As mentioned earlier, the addressing described is reminiscent of the area code and prefix numbers of the public service telephone network which allow the phone company to instantly know how to route our calls. Consider a potential alternative in the case of a random address assignment to nodes. Routing in this case would require an extremely inefficient or unscalable scheme such as a few central routing hubs with full knowledge of the locations of all nodes, or alternatively all routers would require an entry in their routing tables for every node in the world they could potentially communicate with.

III. THE NEED FOR MOBILE IP

From the preceding description it should be apparent that the fundamental need for Mobile IP arises when a node connected to the Internet changes its point of attachment. This is typically due to a change in its physical location, which then necessitates a change in its IP ddress. If during the course of communication the mobile node moves to a different subnet, for example if it moves between a wired and a wireless network, other nodes will no longer able to communicate with it. Packets will arrive at the mobile node's original subnet, identified by its original IP address, but do not reach the node since it is Mobile IP is a network layer routing protocol. It makes no lower-level assumptions about the link characteristics such as bit-rates, error-rates or delay and thus is a device and communication medium independent solution. Mobile IP can be as easily used when moving between different high-speed Ethernet LANs in an office environment as it can when moving over a wide-area wireless data service in the field. It supports both homogeneous mobility, that is when moving between similar medium networks and heterogeneous mobility, that is when moving from one medium to another, as is the case when the node moves between a wired network and a wireless one.

IV. HOW MOBILE IP WORKS

Mobile IP was designed by the "IP Routing for Wireless/ Mobile Hosts" working group (mobile ip WG) of the Internet Engineering Task Force (IETF) and published as a proposed standard in November 1996. A list of publicly-available request for comments (RFCs) that define Mobile IP are described at the end of this article. Before explaining how Mobile IP works, it is useful to become familiar witthe terminology used in the rest of this article. We will use these terms extensively in our subsequent description of M h obile IP operation and in describing the exchange of messages between the mobile nodes and the other key entities within the network.

Mobile Node: A node running the Mobile IP protocol stack which moves between different IP subnets. This node is assigned a (permanent) IP address which defines where all its packets should be sent. When other nodes send packets to the mobile node, they only specify this home.

Home Network: The subnet which corresponds to the home address of the mobile node as well as

that of the hom agent. It is considered the mobile node's "home" point of attachment.

Home Agent: A router on the home network that is responsible for intercepting packets destined for the mobile node when the mobile node is attached to a foreign network. The home agent is responsible for forwarding these packets to the mobile node.

Foreign Network: A network, other than the mobile node's home network, that a mobile node attaches itself to.

Foreign Agent: A router on the foreign network configured for Mobile IP. When the mobile node has a foreign agent care-of address all packets are relayed through this node. When using a collocated care-of address, the mobile node may still use a foreign agent for its default router or for registration with the foreign network.

Care-of Address: The address that the mobile node uses for communication when it is away from its home network. This address can either be a foreign agent care-of address, when the mobile node uses the foreign agent's IP address as its care-of address or a collocated care-of address, where the network interface of the mobile node is temporarily assigned an IP number on the foreign network.

Correspondent Node: Any host which is communicating with the mobile node. This node could be located on the home network, foreign network, or any other place which is able to route packets to the mobile node's home network.

Tunneling: The process of encapsulating an IP packet within another IP packet for the purpose of routing it to a location other than the one specified in the original destination field. Specifically, when a packet is received by the home agent, it encapsulates the original packet inside a new packet, placing the mobile node's care-of address in the new destination address field before forwarding it to the appropriate router. The path that is followed by this new packet is called the tunnel. When a collocated care-of address is used by the mobile node, a foreign agent is often not even required. Home agents and foreign agents periodically broadcast their willingness to act as Mobile IP routers through agent advertisements. If a mobile node needs to immediately know the address of a potential agent without waiting for the next advertisement, it can broadcast an agent solicitation message

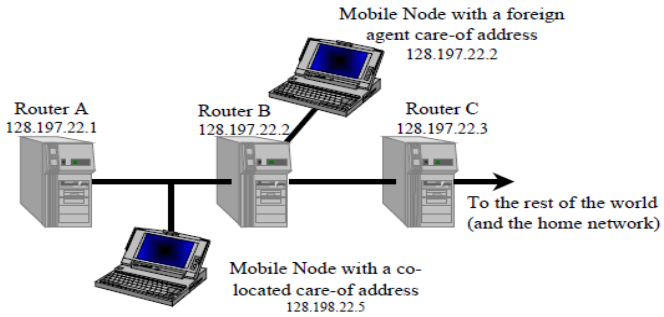

Figure 1: A mobile node with a foreign agent care-of address

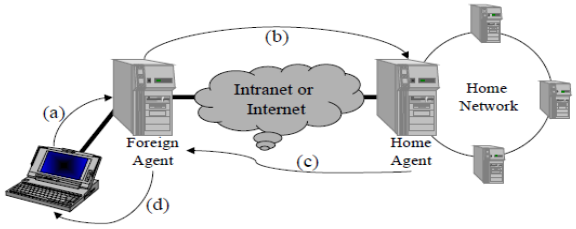

Figure 2: Flow of registration messages between a mobile node with a foreign agent care-of-address and its home agent

From the above descriptions it should be clear that only three entities have to be modified in order to support Mobile

IP over the Internet: the mobile node, the home agent, and the foreign agent. When a collocated care-of address is used by the mobile node, a foreign agent is often not even required.

Home agents and foreign agents periodically broadcast their willingness to act as Mobile IP routers through agent advertisements.If a mobile node needs to immediately know the address of a potential agent without waiting for the next advertisement, it can broadcast an agent solicitation message. The Understand that many care-of-addresses can be registered for a mobile node at once. This allows for potential situations such as a node quickly alternating between two adjacent wireless cells, and multiple points of

ISBN-978-93-5288-834-3

attachment are preferable to rapid deregistration and registration between cells. The transmission of registration messages is shown in Figure 2 for the case of a foreign agent care-of-address. The mobile node submits a registration request to the foreign agent Once a node has obtained a new care-of-address, it registers this address with its home agent. Registration with the home agent is performed for the following reasons: a node has moved to a newforeign network and therefore needs to register a new care-of-address, a node needs to deregister an old careof- address with its home agent when it returns to the home network, or when a node needs to reregister with the home agent because its previous registration is about to expire.

(a). The care-of-address which the mobile node requests will be determined by the foreign agent's agent advertisement messages.The foreign agent does some validity checks on the registration request and then relays the packet to the home agent.The foreign agent makes sure that parameters such as the registration lifetime, and the tunneling method are supported. It also verifies security authentification information. The foreign agent will maintain information such as the link-layer address and the IP source address that the mobile node is using before it resends the registration request with it's own address as the IP source address to the home agent as labeled in

(b).The home agent receives the registration request, checks the options of requested service and authentification from the foreign agent. If the request is considered to be valid and serviceable the agent updates its bindings to record the new careof-address for the mobile node. The home agent then forms an authenticated registration reply to send back to the foreign agent informing it of a successful or unsuccessful registration

(c). Finally the foreign agent receives the reply, and sends a new authenticated message back to the mobile node. If all these replies indicate a successful registration, themobile node will begin to receive its packets tunneled from the home agent through the foreign agent.

V. ROUTE OPTIMIZATION

Route optimization extensions to Mobile IP which have recently been proposed would allow a correspondent node to be informed of the mobile node's care-of address so that it can send packets directly to it. When a correspondent node sends packets to a home agent for tunneling to the mobile node, the home agent can assume that the correspondent node is unaware of the mobile node's current care-of address. After tunnelling this packet for the correspondent node, the home agent sends an authenticated Binding Update to the correspondent node, advising it to update its Binding Cache with the care-of address of the mobile node it is sending packets to. This binding cache contains mappings from home addresses to the temporary care-of addresses. Each entry is specified to be valid for an amount of time which is equal to the time the node is registered with the home agent. Once a correspondent node updates its binding cache it can tunnel packets directly to the care of address.

VI. EXAMPLE OF A COMMERCIAL APPLICATION THAT USES MOBILE IP

Today, mobile warriors can dial into their home network via the Point to Point Protocol or other similar remote access protocols.However, to be able to do this the corporation to which these mobile warriors belong has to have an infrastructure of modems, phone lines, and remote-access servers. The cost of purchasing and maintaining such equipment, along with the administrative costs can become prohibitive. Consequently,there is a strong desire within the Internet community to develop protocols that allow sharing this cost with entities external to the corporations while still providing this important capability to the workforce. Corporations which have already made the investment in building this infrastructure would be happy to share their expenses by charging the mobile warriors of other corporations to gain access to their own home networks, if the integrity of the service providers internal networks is not compromised. Similarly,

corporations that have not yet build this infrastructure would be happy to use the infrastructure of other corporation if they can feel secure in the knowledge that their data will not be compromised and that the foreign network will provide their mobile workforce with secure connectivity to their home networks. Mobile IP can provide a solution to lowering the cost of providing Internet access to mobile warriors by enabling Virtual Private Network (VPN). A Virtual Private Network is one in which the mobile node can send and receive messages exactly as if it was connected to its home network directly. The Internet can thus be used for virtual dial-up. The way this is done is to have the mobile node acquire a IP care-of-address from the local network and then have it pass this on to the home agent at its home network. This way the roaming mobile node can be contacted by any node on the Internet as easily as if it was on its home network. An example of a proposal for a protocol that uses Mobile IP to establish such virtual private networks is the Virtual Tunneling Protocol (VTP) built into the "Bay Steam Dial VPN Service" supported by Bay Networks. VTP uses Mobile IP to dynamically establish bi-directional tunnels through the Internet. Interestingly, in case of VTP, the mobile user node does not have to have Mobile IP support built within its networking stack. Examples of other similar protocols that achieve the functionality described above but without using Mobile IP are the Point-to-Point Tunneling Protocol (PPTP), Layer Two Forwarding (LTF), and the Layer Two Tunneling Protocol (L2TP). While all of these protocols provide support for nomadicity they do not provide support for mobility. In other words, the mobiles are unable to retain their IP addresses and consequently cannot move within the subnets of the foreign network and over different mediums, while continuing to stay connected to their home network.

VII. CONCLUSION

Network mobility is enabled by Mobile IP, which provides a scalable, transparent, and secure solution. It is scalable because only the participating components need to be Mobile IP aware—the Mobile Node and the endpoints of the tunnel. No other routers in the network or any hosts with which the Mobile Node is communicating need to be changed or even aware of the movement of the Mobile Node. It is transparent to any applications while providing mobility...

VIII. ACKNOWLEDGEMENT

The love that accompanies that the doing well achievement of any task would be incomplete without the talk about of people whose constant cooperation made it possible, whose regular guidance and support put the finishing touch to all efforts with success. We are obliged to our project internal guide **Mr. Vinay Prakash** motivation and supportive suggestions that helpul us in the prepration of this seminr.

REFERENCES

[1] Charles E. Perkins, Mobile IP IEEE Communications Magazine , May 1997
[2] Chen Yi-an. A Survey Paper on Mobile IP. http://www.cis.ohiostate.edu/~jain/cis788-95/mobile_ip 17
[3] Charles Perkins, IP Encapsulation within IP Internet Draft, 6 July 1995.This draft specifies a way by which an IP datagram may be encapsulated within an IP datagram
[4] David Johnson and Charles Perkins, Route Optimisation in Mobile IP, Internet Draft, 6 July 1995. This draft specifies extensions to the operations of the base Mobile IP protocol to allow for optimal routing of datagrams from a correspondent node to a mobile node.
[5] MobileIP. http://www.srvloc.org/charliep/txt/commag97/paper.ps
[6] Mobile Networking Through Mobile IP. http://computer.org/internet/v2n1/perkins.htm.
[7] Johnson D. Special Tunnels for Mobile IP. http://monarch.cs.cmu.edu/internetdrafts/draft-ietf-mobileip-spectun-00.txt.
[8] RFC 2004 - Minimal Encapsulation within IP.
[9] http://www.ietf.org/rfc/rfc2004.txt. October 1996
[10] RFC 2002 - IP Mobility Support. http://www.ietf.org/rfc/rfc2002.txt. October 1996
[11] Rivest R., RFC 1321 - The MD5 Message-Digest Algorithm. http://www.toc.lcs.mit.edu/~rivest/rfc1321.txtApri l1992.