International Journal of Mathematical Archive-3(2), 2012, Page: 694-706
Available online through www.ijma.info ISSN 2229 – 5046

UNDERSTANDING OF MOBILE IP

DEHGAN AMIR*
DEPARTMENT OF COMPUTER SCIENCE, UNIVERSITY OF PUNE, INDIA
E-MAIL: DEHGAN.AMIR@gmail.com

(Received on: 01-02-12; Accepted on: 24-02-12)

ABSTRACT

T*o accomplish this, mobile IP established the visited network as a foreign node and the home network as the home node. Mobile IP uses a tunneling protocol to allow messages from the PDN to be directed to the mobile node's IP address. This is accomplished by way of routing messages to the foreign node for delivery via tunneling the original IP address inside a packet destined for the temporary IP address assigned to the mobile node by the foreign node. The Home Agent and Foreign Agent continuously advertise their services on the network through an Agent Discovery process, enabling the Home Agent to recognize when a new Foreign Agent is acquired and allowing the Mobile Node to register a new Care of Address. This method allows for seamless communications between the mobile node and applications residing on the PDN, allowing for seamless, always-on connectivity for mobile data applications and wireless computing.*

Connectivity to the Internet while in motion is becoming an extremely important part of computing research and development. Mobile IP, created by the Internet Engineering Task Force (IETF), is a standard protocol that builds on Internet Protocol by making mobility of a user transparent to applications and higher-level protocols such as Transfer Control Protocol. Mobile IP can be seen as the least common mobility denominator – providing seamless macro mobility solutions among the diversity of access. This paper will attempt to introduce Mobile IP from a technical point of view, while taking into consideration that the reader may not know anything about Mobile IP. However, the reader should know some networking basics before reading further. Building on these concepts, this paper will then discuss effective implementations of Mobile IP, the protocols used by Mobile IP and the importance of Mobile IP. This paper will also introduce Mobile IP from a consumer perspective, i.e. electronic devices (and their Operating Systems) which allow networking mobility.

1. INTRODUCTION

The Internet is an excellent source of information which is readily accessible from almost any computer with a fixed connection to some kind of a network, however with increasing popularity of mobile devices such as PDA's, internet ready cell phones, PC Tablets, etc, there is a need to provide access to the Internet from a device that may be constantly in motion or wireless access to the Internet. Mobile IP, a standard proposed by the Internet Engineering Task Force (IETF) aims to make mobile computing a reality. The principal advantage of Mobile IP is that it frees the user from a fixed location. Mobile IP makes invisible the boundaries between attachment points, it is able to track and deliver information to mobile devices without needing to change the device's long-term Internet Protocol (IP) address (for that session) [1.CP.2002].

Before studying Mobile IP, it is important to define the concept of 'computing mobility'. Computing mobility can be defined as allowing the user some degree of freedom for his/her computing tasks. There are essentially two kinds of computing mobility – Personal mobility and Terminal mobility [2.IP.2003].

Personal mobility involves making it possible for a user to use the network's services from any terminal. When the user logs onto a terminal, he/she will get the same functionality as the user's home network, without having to go through time-consuming configuration procedures. When this user starts an IP session, an IP address will be assigned if it has not been done so already. As long as the IP session is kept alive, the IP address will serve as a destination for information delivery. An inherent problem with this approach is that once logged on, the user cannot switch to any other terminal. To use another terminal the user will have to repeat the login process on that terminal. An example of this may be an employee's laptop. At work, when the laptop is docked, the IP address will serve for communications, however, if the employee were to work from home over a high-speed connection or dial-up, the IP address of the laptop will be different, but the destination network will be the same. This approach requires technologies such as Network Access Identifier (NAI), where there is a relationship between the user's IP address and the NAI.

Corresponding author: DEHGAN AMIR*, *E-mail: dehgan.amir@GMAIL.COM

Terminal mobility means that the user and the terminal are mobile as one entity. The terminal may change its point of attachment[1] with the home network without:

- Informing the network to which it is connected to
- Having any impact on ongoing network services

Terminal mobility is tied to the Mobile IP protocol itself. Mobile IP does these two things in a seamless and lossless manner, in fact, ideally, the user should not ever be aware of the processes in the background which allow the mobility.

This mobility is handled in the network layer[2]; hence application session continuity is inherently provided for, as they will not even have to deal with mobility.

Mobile IP faces many obstacles, but ingenuity in modifying existing technology and communication protocols and adding new technologies have made Mobile IP a reality. Once the technology is perfected, users will enjoy the convenience of seamless untethered roaming and application transparency of nomadic computing[3].

Though the Internet can seem anarchic, IP routing depends on a well-ordered hierarchy. At the Internet core, routers are not concerned with individual users. They look at only the first few bits of an IP address (the prefix) and forward the packet to the correct network. Once at the network, routers within the network further look at the next few bits on the IP address, and send the packet to a subnet. At the edge, access routers look at the final parts of an address and send the packet to a specific machine [3.AD.2002].

To summarize the features of Mobile IP:

- No geographical limitations
- No physical connection required
- Modifications to other mobile devices/routers is not required
- Mobile IP leaves transport and higher-level protocols unaffected
- No modifications to the current IP address of the mobile device or the format of the IP address
- Supports security or implements some kind of authentication scheme to provide security

2. HOW MOBILE IP WORKS

IP addresses are typically associated with a fixed non-mobile location such as a router or a client computer. IP routes packets from a source to a destination by allowing routers to forward packets from incoming network interfaces to outbound interfaces according to routing tables. These routing tables typically maintain the next-hop information for each destination IP address, which is based on the number of networks to which that IP address is connected. The network number is derived from the IP address by masking off some of the low order bits. Thus, the IP address specifies the node's[4] point of attachment.

To maintain existing transport-layer connections the node must maintain a single IP address. In Transfer Control Protocol (TCP), the overwhelmingly popular protocol for Internet connections, the connections are indexed by a quadruplet that is analogous to someone's geographical home address. This set of numbers is what allows for delivery of a packet of data. If any of these numbers are changed then the connection will most likely be lost. Correct delivery of data packets to the node depends on the network number contained within the node's IP address.

If the node is mobile, packets sent to this node may never make it as, logically, mobility will force a new IP address to be associated with the node every time it changes its connection point. Constantly changing IP address of a node will make transparent mobility impossible.

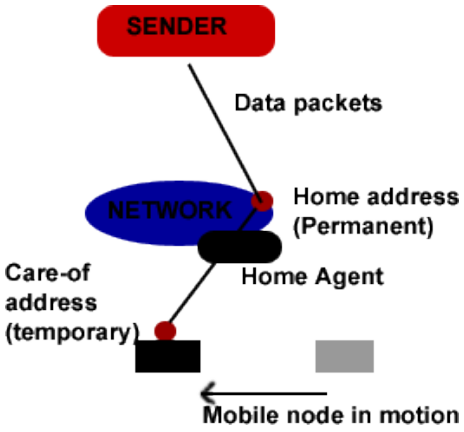
Mobile IP was designed to solve this problem by allowing the node to use two IP addresses:

- Home address
- Care-of address

[1] A Point of Attachment can be defined as the access point of an entity into a network.
[2] Discussion of Mobile IP in terms of network layers is done in section 4.
[3] Nomadic computing is analogous to Terminal Mobility.
[4] *'node', 'client computer', and 'client'* are used interchangeably to mean a computer that is the receiving station.

Figure 2.1

Simple diagram showing concept of having two IP addresses and a Home agent



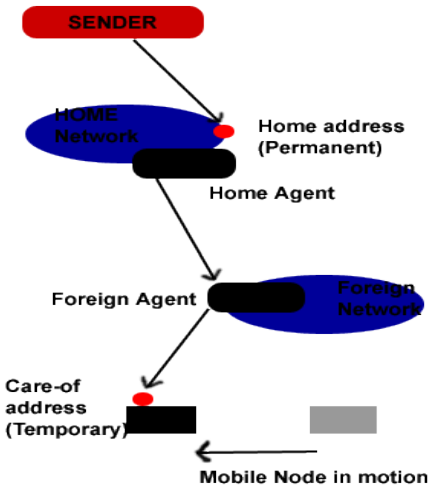
Home address is static and is used to identify TCP connections. By definition, a home address is an address that makes the mobile node appear logically connected to the home network[5]. Mobile IP enables mobile nodes to surf the Internet, but remain addressable via their home network [4.CP.1996]. The care-of address changes at each new point of attachment; it indicates the network number and thus identifies the mobile node's point of attachment with respect to the network topology.

The home address makes it appear that the mobile node is continually able to receive data on its home network where a network node known as the home agent assists in this operation. The home agent's principal job is to get data packets intended for the mobile node and deliver them transparently to the mobile node's current point of attachment. Whenever

the mobile node is in a foreign network[6], delivery of data to the mobile node is taken care of by the foreign agent.

FIGURE 2.2

Mobile node on a Foreign Network



As mentioned, the care-of address changes at every new point of attachment. Whenever the point of attachment changes, the mobile node registers its new care-of address with its home agent. To get a packet to the mobile node from its home network, the home agent delivers the packet from the home network to the care-of address. To ensure delivery, the packet's header is modified so that the destination IP address is the care-of-address. This process can be thought of as a redirection where the packet is transformed from its original state to get delivered to its destination – the mobile node. This new header then shields or encapsulates the original packet, causing the mobile node's home address

[5] A Home Network of a mobile node is the network to which the mobile node is a part of, and thus to the rest of the Internet & other services.

[6] A Foreign Network can be defined as any network that is not the home network.

to have no effect on the encapsulated packet's routing until it arrives at the care-of address. Such encapsulation is also called tunneling[7]. This allows the packet to bypass the usual effects of IP routing.

The need for the existence of the home agent, foreign agent, and two different IP addresses is because of the lack of end-to-end network layer transparency, which is sometimes referred to as "Internet fog" [2.IP.2003]. Essentially, an IP address has to find its way through the Internet in order to get to its destination with the help of routing devices on the way. For Mobile IP to work properly, functionality has to be built-in so that it can find a way through the "fog".

So, the basic entities of a network that supports Mobile IP are:

- The mobile node
- The foreign agent
- The home agent
- The sender or correspondent node

Mobile IP can be understood as the cooperation of 3 separate mechanisms [5.CP.1999]:

2.1 Discovering the care-of address
2.2 Registering the care-of address
2.3 Tunneling to the care-of address

2.1 Discovering the care-of address

The Mobile IP discovery process has been built on top of an existing standard protocol, Router Advertisement. Internet Control Message Protocol (ICMP) router discovery messages are known as Router Advertisement. Router Advertisement enables hosts attached to multicast or broadcast networks to discover the IP address of their neighboring routers. Each router periodically multicasts a Router Advertisement from each of its multicast interfaces, announcing the IP address of that interface. Hosts discover the addresses of their neighboring routers by simply listening for advertisements [6.SED.1991].

Mobile IP does not modify the original fields of existing router advertisements but simply extends them to associate mobility functions. Thus, a router advertisement can carry information about default routers, just as before, and in addition carry further information about one or more care-of addresses. When the router advertisements are extended to also contain the needed care-of address, they are known as agent advertisements. Home agents and foreign agents typically broadcast agent advertisements at regular intervals of time. If the mobile node needs to get a care-of address and does not wish to wait for the periodic advertisement, the mobile node can broadcast or multicast a solicitation that will be answered by any foreign agent or home agent that receives it. Home agents use agent advertisements to make themselves known, even if they do not offer any care-of addresses.

An agent advertisement performs the following important functions:

- Allows for detection of mobility agents.
- Lists one or more available care-of addresses.
- Informs the mobile node about special features provided by foreign agents, for example, alternative encapsulation techniques.
- Lets the mobile node determine the network number and status of their link to the Internet.
- Lets the mobile node know whether the agent is a home agent, foreign agent, or both, and therefore whether it is on its home network or a foreign network.

Mobile nodes use router advertisements as defined in [6.SED.1991] to detect any changes in the state of mobility agents available at the current point of attachment[8]. If advertisements are no longer detectable from a foreign agent that previously had offered a care-of address to the mobile node, the mobile node should presume that the foreign agent is no longer within range of the mobile node's network interface. In this situation, the mobile node should begin to hunt for a new care-of address, or possibly use a care-of address known from advertisements it is still receiving. The mobile node may choose to wait for another advertisement if it has not received any recently advertised care-of address, or it may send an agent solicitation.

Due to the unavailability of an Internet key management protocol, agent discovery messages are not required to be authenticated [7.JS.1996].

2.2 Registering the care-of address

Once a mobile node has a care-of address, its home agent must find out about it. The process begins when the mobile node, possibly with the assistance of a foreign agent, sends a registration request with the care-of address information. When the home agent receives this request, it adds the necessary information to its routing table, approves the request,

[7] The concept of IP-within-IP encapsulation and tunneling is described in detail in later sections.
[8] This is known as *agent solicitation.*

and sends a registration reply back to the mobile node. Although the home agent is not required by the Mobile IP protocol to handle registration requests by updating entries in its routing table, doing so offers a natural implementation strategy, and thus necessary.

Registration requests contains parameters and flags that characterize the tunnel[9] through which the home agent will deliver packets to the care-of address. When a home agent accepts the request, it begins to associate the home address of the mobile node with the care-of address, and maintains its association until the registration lifetime[10] expires. The triplet that contains the home address, care-of address and the registration lifetime is called a binding for the mobile node. A registration request can be considered a binding update[11] sent by the mobile node.

A binding update is an example of a remote redirect, because it is sent remotely to the home agent to affect the home agent's routing table. This makes the need for authentication very clear. The home agent must be certain that the registration was originated by the mobile node and not by some other malicious node pretending to be the mobile node. A malicious node could cause the home agent to alter its routing table with erroneous care-of address information, and the mobile node would be unreachable to all incoming communications from the Internet.

The need to authenticate registration information has played a major role in determining the acceptable design parameters for Mobile IP. A detailed discussion of authentication is beyond the scope of this paper, however it is worthwhile to briefly mention how identification fields in the registration message are modified to improve authentication.

Mobile IP includes within the registration message a special identification field that changes with every new registration; this is mandated within Mobile IP. There are two main ways to make the identification field unique. One is to use a timestamp; then each new registration will have a later timestamp and thus differ from previous registrations [7.JS.1996]. The other is to cause the identification to be a pseudorandom number. With enough bits of randomness, it is highly unlikely that two independently chosen values for the identification field will be the same [1.CP.2002].

This identification field is also used by the foreign agent to match pending registration requests to registration replies when they arrive at the home agent and to subsequently be able to relay the reply to the mobile node. The foreign agent also stores other information for pending registrations, including the mobile node's home address, the mobile node's Media Access Layer (MAC) address, the source port number for the registration request from the mobile node, the registration lifetime proposed by the mobile node, and the home agent's address. The foreign agent can limit registration lifetimes to a configurable value that it puts into its agent advertisements. The home agent can reduce the registration lifetime, which it includes as part of the registration reply, but it can never increase it [1.CP.2002].

2.3 Tunneling to the care-of address

The default encapsulation mechanism that must be supported by all mobility agents using Mobile IP is IP-within-IP (IPIP) [8.CP.1996.2]. Using IPIP, the home agent, which is the tunnel source, inserts a new IP header, or tunnel header, in front of the IP header of any datagram addressed to the mobile node's home address. The new tunnel header uses the mobile node's care-of address as the destination IP address, or tunnel destination. The tunnel source IP address is the home agent, and the tunnel header uses 4 as the higher-level protocol number, indicating that the next protocol header is again an IP header. In IPIP the entire original IP header is preserved as the first part of the payload of the tunnel header. Intermediate routers are unaware of this encapsulation.

In order to recover the original packet, the foreign agent merely has to eliminate the tunnel header and deliver the rest to the mobile node. In order to reduce header overhead, minimal encapsulation can be used instead of IPIP [9.CP.1996.3], however, this increases the complexity of processing the header as some of the information from the tunnel header is combined with information in the inner encapsulation header [10.CW, et al.2002].

3. EFFECTIVE USE OF MOBILE IP

As can be gathered from reading the previous two sections, the uses of Mobile IP are numerous. They can range from simple Internet access from handheld devices to allowing interactive sessions between employees in different locations while any one or all are on the move.

This is perhaps best demonstrated though a rudimentary example – imagine a scenario where an employee unplugs a mobile computer form its dock in the office. The computer, Mobile IP enabled, will be able to continue downloads,

[9] A Tunnel is the path taken by encapsulated packets. It is the path that leads packets from the home agent to the foreign agent. Tunnels will be explained in more detail in later sections.

[10] Registration lifetime is how long the mobility agents may use the binding.

[11] A binding update is a message that supplies a new binding to an entity that needs to know the new care-of address for a mobile node. The binding update contains the mobile node's home address, instead of being one offered by a foreign agent.

conduct Voice over IP (VoIP) sessions, and continue any other networking task without any interruptions, even while the employee is on his or her way home and finally from home (hopefully, the employee will not be working from home too much). Connectivity will first be transferred from the office Local Area Network (LAN), then to a cellular network and finally to the connection to the Internet that the employee has from home.

Another effective use of Mobile IP is the concept of Mobile Networks. According to Cisco Systems [11.CS.2001]:

> Cisco Mobile Networks enables a router and its subnets to be mobile while continuing to maintain IP connectivity transparent to the IP hosts connecting to the network through this mobile router. This solution enables the IP hosts on a LAN connected to such a mobile router to transparently connect to the parent network while the LAN is in motion. The mobile router ensures network connectivity from a mobile environment.
>
> The Mobile Networks solution enables entire networks to roam. For example, this enables a plane to fly around the world while passengers stay connected to the Internet. In this case, each passenger's IP device is a node on the mobile network connected to a router on the plane. The nodes on such a mobile network are not aware of any IP mobility at all. The Mobile Networks solution that is running on the router in the plane 'hides' the IP roaming from the local IP nodes so that the local nodes appear to be directly attached to the home network.

These are just some of the examples of the effective uses of Mobile IP. However, Mobile IP is expected to become even more important as wireless networks and IPv6[12] become popular. Cellular vendors are pushing Mobile IP hard as a way to allow seamless roaming between Third-Generation (3G) networks and higher bandwidth hot spots based on Bluetooth or Wi-Fi (802.11b).

To make clear some of the underlying technology that aid the effective use of Mobile IP, some of the concepts explained in the previous section will be reiterated with effective implementation kept in mind.

As explained, every kind of Mobile IP gives the mobile node two IP addresses, a permanent address on its home network (home address), and a care-of address (required if the mobile node is on a foreign network). The home address is the one that higher-level protocols use, while the care-of address signifies the node's actual location within a network and its subnets.

Whenever the mobile node moves to a new network, it must acquire a new care-of address on the network it is visiting. In IPv4 this means requesting one from a special mobility agent known as the foreign agent. Most likely, this agent will essentially be a Dynamic Host Configuration Protocol (DHCP) server. This server should have some Authentication, Authorization, and Accounting (AAA) functionality added on to the foreign network. AAA is basically an infrastructure, which allows "trust" in communications [12.SN, RP.2002].

Remote Authentication Dial In User Service (RADIUS) is the dominating AAA protocol in IP networks today [13.CR, et al.2000], while Diameter is the successor of this well-known protocol. Diameter is the currently standardized within the IETF AAA working group. Both RADIUS and Diameter are flexible and extensible protocols. Additionally Diameter is built to be backwards compatible with RADIUS. Both RADIUS and Diameter protocols are and will be used for roaming Mobile IP users [14.PC, et al.2002].

Back at the home network, another mobility agent, the home agent, usually an edge router with some AAA functions keeps track of all the mobile nodes with permanent addresses on that network, associating each with its care-of address. The mobile node keeps the home agent informed of its whereabouts by sending a binding update via ICMP, whenever its care-of address changes. These updates can incorporate a digital certificate, to ensure that they are actually sent by the mobile agent, rather than an attacker seeking to impersonate him or her.

When information (packets) is to be sent to the mobile node, the home agent intercepts these packets and sends them to the mobile node at its care-of address via tunneling. This allows the sender to send packets to a permanent IP address (which belongs to the home network).

In IPv4, this is the simplest way to ensure mobility, but this adds extra routing hops that tend to use more bandwidth and increase latency. The possibility of increased latency is of particular concern for wireless networks where preventing latency is paramount. In the original version of mobile IPv4, standardized in 1996, mobile nodes were supposed to send replies directly to senders, for compatibility with higher-level protocols, the "source" address field in these packets had to be the permanent address on the home network, even though routers on the Internet would see that the packets were actually coming from the care-of address on the visited network. This is a serious problem now.

To curb Denial of Service (DoS) attacks, where malicious packets often claim to be from fake IP addresses, routers on the Internet began to incorporate ingress and outgress filtering [15.PF, et al.1998]. Routers would only allow a packet

[12] There is a brief discussion of IPv6 implementations in Mobile IP in section 6 of this paper.

through if its source address field was consistent with its origin. To get around these filters, mobile IPv4 was updated in 2002 to include reverse tunneling [16.GM.2001]. Instead of taking a triangular path (Figure 3.1), all packets travel via the home network only (Figure 3.2); this is known as Reserve Tunneling. Reverse Tunneling wastes bandwidth and adds to latency.

Figure 3.1
Triangular Routing

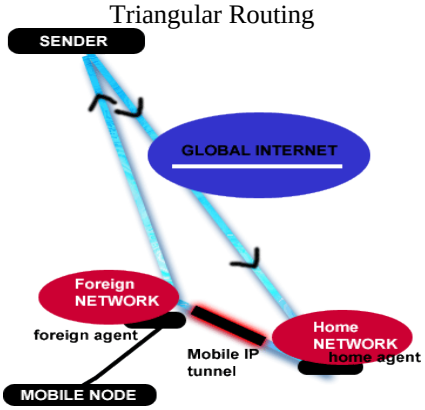
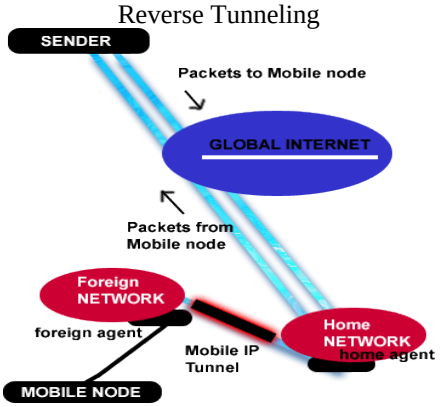


FIGURE 3.2
Reverse Tunneling



This problem is easily solved in Mobile IPv6 by avoiding tunneling as much as possible. Though the first few packets of every session are still tunneled via the home agent, the mobile node also sends binding updates to every correspondent. Future packets can be sent directly, just as if the mobile node belonged on the network it was visiting. Mobile IPv6 can accomplish this by using extensible headers – a feature allowing IPv6 packets to contain extra protocol information to deal with issues such as Quality of Service (QoS) and prioritization. The header of each packet can contain both the home and care-of address, satisfying both higher-level protocols and Internet routers. Section 6 briefly outlines these and other benefits of Mobile IPv6.

4. PROTOCOLS OF MOBILE IP

Mobile IP is a large part, but by no means the only part of mobile computing and networking. A good understanding of Mobile IP involves studying the relationships between the various layers of network protocols. Each layer should present a clear model of operation to the architect. Once the model is identified, the effects of mobility can be studied in relation to it.

The Internet networking stack showing common protocols is shown in the table below.

TABLE 4.1

Layers	Common Protocols
Application Presentation Session	HTTP, DNS, FTP, etc
Transport	TCP, UDP, RTP
Network	IP, ICMP, Mobile IP, etc
Data Link	IEEE 802.*, PPP, etc
Physical	Network Adaptor

Table 4.1 shows a simplified view of the International Standards Organization's (ISO) protocol stack as it applies to Internet networking. The major goal of Mobile IP protocol design was to handle mobility at the network layer and leave the other higher protocols unaffected. This allows for the existing routing infrastructure to be unaffected. This is also a big advantage to current applications, as they do not have to incorporate any new technologies either.

The cell[13] of a mobile node is the geographical location around the network (which supports mobile nodes). This area is defined by the propagation characteristics of the electromagnetic waves at the operating frequency. Infrared communications, for example, stop at the walls of a room, while radio frequency communications have much more complicated propagation characteristics. The ability of the hardware of the mobile host to detect signal strength and report it to the device driver will be helpful in realizing that the host is at the outer reaches of a cell and that it should try to switch to a different one. In addition, in the case of spread-spectrum of multi-channel radio communications, the ability to receive on multiple channels at once is highly desirable [17.JI, et al.1996].

The data link layer is responsible for link establishment and maintenance. Thus, physical effects from mobility are likely to require changes in this layer. Changes in position affect the Signal-to-Interference Ratio (SIR). Link layers that adapt forward error correction to SIR can exhibit variable bandwidth but far fewer lost packets. Wireless media typically introduce many other design requirements at the data link layer, such as encryption (to maintain a degree of confidentiality) and compression techniques (to fit more data in lower bandwidth) [18.TIA.1995].

An interesting problem to be dealt with in this layer is modifying the Address Resolution Protocol (ARP) to allow for mobility. In the data link layer, we either map a logical address to a physical address (non-mobile) or dynamically acquire an IP address for a moving node. ARP works by broadcasting a request on the communication network with the IP address of the target in the packet. All hosts on the network will receive this packet, but only the node with the required IP address will respond[14].

The problem with ARP and mobile nodes arises when one mobile node tries to get the address of another mobile node. If both the mobile nodes are on the same home network then ARP will work in the normal way. However, if one of the mobile nodes (MN1) is on another network, then the sending mobile node (MN2) will have to 'proxy-ARP' the request for MN1. MN2 will send all traffic intended for MN1 to its own home network, which will then encapsulate the request in an IP-within-IP datagram. The home network will then query all other networks in order to find out which one is handling MN1. This process continues until success or failure [17.JI, et al.1996]. This is also known as "Gratuitous ARP".

At the network layer, IP determines a path through a loosely confederated association of independent network links, routing from one network to another, while offering some services such as fragmentation, reassembly and checksumming. Hence, logically, changing the point of attachment (mobility) requires changing the routing of datagrams intended to and from the mobile node. This is done by encapsulation and decapsulation techniques. The standard technique for encapsulation and decapsulation is IP-within-IP (IPIP); this must be supported by default by all mobility agents.

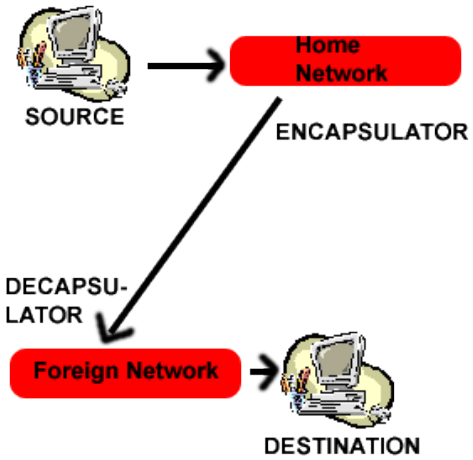
Previously in this paper, IPIP has been used repeatedly without actually defining the concept in some detail. The concept of IPIP means that the payload of an IP datagram will actually contain another IP address and a payload. This is done to allow for delivery to an intermediate destination that would otherwise not be selected by the (network part of the) IP destination address field in the original IP header [8.CP.1996.2]. Once the encapsulated datagram arrives at this intermediate destination node, it is decapsulated, yielding the original IP datagram, which is then delivered to the destination indicated by the originally encapsulated IP datagram's destination address field.

This use of encapsulation and decapsulation of a datagram is referred to as tunneling, and the encapsulator and decapsulator are considered to be the endpoints of the tunnel shown in figures 3.1 and 3.2. The working for an encapsulator and decapsulator is shown in Figure 4.1. The end-points of a tunnel can also be thought of as the route between the home agent and the care-of address, handled by the foreign agent. It should be noted that encapsulation/decapsulation is employed only if the mobile node is on a foreign network.

[13] A cell is the geographic area in which a wireless device may function as desired. A large geographical area may be divided into cells in order to provide maximum signal strength to a wireless device.

[14] This fact is debatable, there are some cases when this might fail, or some rouge node may fake the IP address and respond instead. There are ways to prevent this, but they are beyond the scope of this paper.

FIGURE 4.1
Simple diagram showing IPIP scheme



SOURCE, shown in Figure 4,1 may be an Internet host or another mobile node; DESTINATION is the mobile node for which the datagram is intended. The home agent handles the start point of the tunnel where the encapsulation is done. At the end point of the tunnel, resides the foreign agent, which decapsulates the packet and delivers the packet to the mobile node. A problem arises at the decapsulation point. When the encapsulated packet is decapsulated the foreign agent sees that the destination field of the packet actually specifies the address of the home agent (home address). To avoid sending the packet right back to the home agent, the foreign agent must be smart enough to forward the packet to the intended mobile node identified by its hardware address, rather than the destination IP address.

Some problems with this kind of source routing[15] are [8.CP1996.2]:

- Some current routers do not handle datagram modification or even source routing very well.
- There are some security issues with source routing.
- Encapsulation cannot be used if it is known that the tunnel end-point does not support it (i.e. it cannot decapsulate it).
- Firewalls may cause problems.

At the transport layer, TCP and other transport protocols attempt to offer a more convenient abstraction for data services than the characteristically chaotic stream of data emanating from IP. The vagaries and time dependencies of routers and Internet congestion often cause datagrams to be delivered out of order, duplicated or even dropped entirely before reaching their destination. TCP attempts to solve these and other problems, but offers little help in supplying a steady (constant bandwidth) stream of data.

Over time, TCP has been modified to treat dropped packets as an indication of network congestion, and therefore to throttle transmissions as soon as a lost packet is detected (by managing sequence numbers). In wireless communications, a lost or corrupted packet may be caused by noisy wireless channel, immediate retransmission is the best way to correct this, rather than delayed transmission. There is still a lot of research going on to find the best solution.

At the top layer are the application protocols. Depending on the transport model employed, application protocols are largely freed from the hassles of error correction, retransmission, flow control, and the like. However, mobility creates new needs at the application layer, which require additional protocol support: automatic configuration, service, discovery, link awareness, and environment awareness.

Essentially, these protocol support mechanisms form a set of middleware services. For example, a mobile computer might need to be configured differently at each different point of attachment. Among other things, a new DNS server, IP address, Link Minimum Transmission Unit (MTU), and default router may be required. These configuration items are usually thought of as being worked out at setup time for desktop systems, but for mobile computers no single answer can be sufficient. Recent deployment of DHCP goes some way toward resolving configuration difficulties, but is not the whole answer. Discovering services can be modeled as a requirement for automatic configuration, but is more naturally useful when services are located upon demand and according to the needs of application protocols. This need is being investigated by many means, Service Location Protocol being one of the primary ones.

[15] Source routing is a technique by which the sender can specify the route the datagram will take. Mobile IP utilizes Loose Source Record Route (LSRR), in which the sender gives one or more hops that the packet must go through. Another type, Strict source routing is not very common.

The Service Location Protocol provides a scalable framework for the discovery and selection of network services. Using this protocol, computers using the Internet no longer need so much static configuration of network services for network-based applications. This is especially important as computers become more portable, and users less tolerant or able to fulfill the demands of network system administration [19.JV, et al.1997].

One of the challenges of such architecture of middleware is that it offers applications the opportunity to detect the state of the physical link, which may change dynamically and in turn affect the application's proper operation. Mobility requires that applications adapt to changing connection parameters such as bandwidth, error rate, and Round-Trip Times (RTT).

The following table concludes this section and summarizes what we know so far of the services provided/required by Mobile IP by showing the Network Stack and its corresponding nomadic services [20.CP.1998].

TABLE 4.2

NETWORK STACK	NOMADIC SERVICES
Application Layer	• Resource Discovery • Link Adaptation Layer
Transport Layer	• Congestion Control • Flow Control • Quality of Service
Network Layer	• Addressing • Routing • Location Management • Authentication
Physical/Link Layer	• Signal Modulation • Encryption • Compression • Interference • Channel Access/Selection

5. NEED FOR MOBILE IP

A good analogy for Mobile IP is the development of Mobile Cellular phones over the past decade. A lot of customers have migrated form the traditional fixed-point telephones (phones which require a fixed phone-jack in the wall) to Cellular phones which allow the user to be in motion while talking to someone. This mobility is achieved by using technology that allows a user to maintain a constant connection to the receiver, and vice-versa.

A big difference in this analogy is the fact that it took a long time for mobile phones to become accepted in the consumer market. The prohibitive cost of cellular technology and limited areas of coverage discouraged many users from using cellular phones. Mobile computing is guaranteed to become a hot technology, as acceptance of mobile devices that can be modified to support Internet access is already popular with consumers. Some manufactures are already providing portable devices that allow wireless Internet access. Having already found user acceptance, mobile computing may become popular much faster.

As mentioned, one of the biggest advantages of Mobile IP is that the user can seamlessly move about without having to reconnect/reconfigure at every point of attachment. The main aim of Mobile IP with the aid of the protocols discussed in the previous section is to provide completely automatic, non-interactive reconnection to network activities from any point of attachment.

The important advantages of Mobile IP are:

- Location independent access to computing resources
- Wireless network access
- Ease of and comfortable operation – user can work from almost anywhere
- Economy – Mobile networking environments can save a lot of money by avoiding cabling costs and the subsequent maintenance (wear and tear) that come with wires.
- Software reusability – Existing applications do not have to be modified in order to be able to access a network over Mobile IP.
- Continuous connectivity

Some examples of Mobile IP in action have already been given in section 3 of this paper. Some more examples can be given where the use of Mobile IP can be critical to success:

- Collaborative office environments: Employees can freely move about with mobile devices and be able to interact, share and discuss data on their devices by being able to meet on a personal level. Airbus Wichita has a collaborative engineering facility that may be able to use this effectively [21.JL.2003].
- Hospitals: Doctors can get immediate information on their mobile devices on their patients without having to go to their terminals – they can the needed information in the presence of the patient. Using this kind of access will be particularly useful to Emergency Medical Services. Such services are already being tested [22.EMS].
- Battlefield Operations: Wireless voice communication has been mainstay in the military for many decades now, but with the advent of new military technology the need is there to provide devices that can receive/relay important battlefield data to/from a central computer [23.JJ.2002].
- Campus/College environments: Campus environments will benefit greatly from the implementation of Mobility within the campus environment.

Thus, once problems of mobile computing are ironed out, almost any computing environment, which needs Internetworking, can benefit greatly from the implementation of Mobile IP.

6. IMPLEMENTATIONS OF MOBILE IP

There are numerous implementations of Mobile IP. Already there are devices which support Mobile IP, and this is only furthered by technologies for Mobile IP that have been extended to different Operating systems such as Linux, and also to IPv6. This section will include:

6.1 A short discussion of Mobile IPv6
6.2 Mobile IP under Linux
6.3 Devices developed and being developed which support Mobile IP

6.1 A short discussion of Mobile IPv6

IPv6 was developed to include enhancements from IPv4 and many new technologies that are missing from IPv4. Mobile IPv6 contains many features that were sorely missed in Mobile IPv4. Principally the mobility support for Internet devices in possible and standardized for both IP protocol versions, IPv4 and IPv6, but due to the enhanced functionality and later design of IPv6 some features concerning the mobility support have been integrated more efficiently in Mobile IPv6 when compared to Mobile IPv4.

Some important advantages of Mobile IPv6 and differences from IPv4 are [24.WF, FH.2000, 25.DJ, et al.2003]:

- A mobile node requires a new care-of address every time it changes its point of attachment. There is a possibility under IPv4 that availability of these addresses becomes a problem. Due to the huge number of addresses available under IPv6, assigning addresses will never be a problem.
- Using anycast address of IPv6 enables a node to send a packet to one out of several systems having this anycast address assigned to one of their interfaces. Mobile IPv6 makes efficient use of this mechanism for the dynamic host discovery mechanism by sending a binding update to the home agent anycast address and getting a response form exactly one home agent. This is absent from IPv4.
- Employing Stateless Address Autoconfiguration and Neighbor Discovery mechanisms Mobile IPv6 neither needs DHCP nor foreign agents to configure care-of addresses. Using Neighbor Discovery, Mobile IPv6 does not need to use ARP; this improves overall robustness of the protocol.
- Mobile IPv6 can use IPsec (IP Security Protocol) for all security requirements, like authentication, data integrity protection, and replay protection. This is perhaps the biggest difference between Mobile IPv4 and Mobile IPv6.
- Route optimization is greatly improved and is a fundamental part of Mobile IPv6. 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 hosts that send data to them.
- Mobile IPv6 has no problems with ingress filtering, this improves efficiency and the wasteful technique of Reverse Tunneling is not required.
- The movement detection mechanism in Mobile IPv6 provides bidirectional confirmation of a mobile node's ability to communicate with its router from its current location.
- Packets in Mobile IPv4 require encapsulation if the mobile node is away from home, packets in Mobile IPv6 are sent using a Mobile IPv6 routing header, doing away with the need for encapsulation/ decapsulation techniques. This reduces the amount of resulting overhead compared to Mobile IPv4.
- Managing tunnel "soft state" is unnecessary in Mobile IPv6.

Conversely, Mobile IPv6 does not solve all general problems related to the use of mobility or wireless networks, some important examples [25.DJ, et al.2003]:

- Mobile IPv6 does not handle links with partial connectivity or unidirectional connectivity.
- Access control on a link being visited by another mobile node is not handled.
- Assistance for adaptive applications is absent.

- Mobile routers are not inherently supported; these have to be designed by the vendor.

A full discussion of IPv6 is worthy of a whole new paper, however, in this introductory paper it is sufficient to say that Mobile IPv4 contains many enhancements over Mobile IPv4 and is definitely the way to go for future mobile devices.

6.2 Mobile IP under Linux

There is currently a lot of research and implementations of Mobile IP under Linux, just to name a few:

- Mosquito Net - http://mosquitonet.stanford.edu/mip/
- Dynamics – HUT Mobile IP - http://www.cs.hut.fi/Research/Dynamics/
- Lancaster Mobile IPv6 Package - http://www.cs-ipv6.lancs.ac.uk/ipv6/MobileIP/
- Portland State University - http://www.cs.pdx.edu/research/SMN/

As can be seen, there are quite a few implementation of Mobile IPv6 for Linux, one common denominator is that most focus is now shifting towards Mobile IPv6 due the built-in IPv6 functionality in Linux kernels available today (Versions 2.1.x).

6.3 Devices developed and being developed which support Mobile IP

Companies which manufacture devices such as laptops, PDA's and similar devices are showing a lot of interest in Mobile IP as a way to provide reliable and "always-on" connections to services such as web browsing and e-mail.

Earthlink, Palm/Handspring, Sony, and other companies are investing heavily to get the edge in developing a device that can support seamless mobility.

Some examples of vendors developing products specifically to support Mobile IP are IPAQ 5455 from Hewlett Packard, supported by T-mobile. The IPAQ retails for about $600-$700 and has a modified version of the Windows operating system. Some new the newer models of PDA's from Palm and Sony also have nifty wireless features.

Research is underway at the labs of major vendors to produce devices which are fully capable if wireless communication, of course, the infrastructure needs to be in place for true nomadic computing. In some of the major metropolitan cities, where such infrastructure exists wireless communications have proved to be priceless.

This was best demonstrated by one of the biggest tragedies to happen to the United States. In the aftermath of the September 11th terrorist attacks, hundreds of office workers, finding themselves without an office, turned to wireless communications to carry out the most vital of business tasks. Cellular technology and mobile computing also allowed rescue and other operations to be carried out with some semblance of reliability in the midst of tremendous destruction [26.SM.2003].

7. CONCLUSION

As this introductory paper has shown, Mobile IP has great potential. Within the IETF, Mobile IP already has a large number of both RFCs and Drafts, which indicates that Mobile IP has been a well researched field and that a great deal of current research is ongoing as well (A search in IETF website, http://search.ietf.org/, revealed 12,086 documents).

Test results have given added confidence that the Mobile IP specification is sound, implement able, and of diverse interest throughout the Internet community. Mobile IP specification has also been easily interpreted by network protocol engineers and network programmers [18.TIA.1995].

It is possible that the deployment pace of Mobile IP will track that of IPv6, or that the requirements for supporting mobility in IPv6 nodes will give additional impetus to the deployment of both IPv6 and mobile networking. The increased user convenience and the reduced need for application awareness of mobility can be a major driving force for adoption. Since both IPv6 and Mobile IP have little direct effect on the protocol stack, application designers should find this to be an acceptable programming environment. Of course, everything depends heavily on the willingness of platform and router vendors to implement Mobile IP and/or IPv6. Indications are there are most major vendors are already dedicating a lot of time and money to this field which has enormous potential.

REFERENCES

[1] CP.2002] Charles E. Perkins. IP Mobility Support. http://www.ietf.org/rfc/ rfc3344.txt. August 2002

[2] IP.2003] ipUnplugged White Paper Mobility and Mobile IP, Introduction. 2003

[3]AD.2002] Andy Dornan. Mobile IP. http://www.networkmagaine.com/article/ NMG20020429S0013. June 2002.

[4] CP.1996] Charles E. Perkins. Mobile IP, Ad-Hoc Networking and Nomadicity. http://citeseer.nj.nec.com/34824. html. 1996.

[5] CP.1999] Charles Perkins. Mobile Networking Through Mobile IP. http://www.computer.org/internet/v2n1/perkins.html. 1999.

[6] SED.1991] S.E. Deering. ICMP Router Discovery Messages. http://www.ietf.org/rfc/rfc1256.txt. September 1991.

[7] JS.1996] J. Solomon, Applicability Statement for IP Mobility Support. http://www.ietf.org/rfc/rfc2005.txt. October 1996.

[8] CP.1996.2] Charles E. Perkins. IP Encapsulation within IP. http://www.ietf.org/rfc/rfc2003.txt. October 1996

[9] CP.1996.3] Charles E. Perkins. Minimal Encapsulation within IP. http://www.ietf.org/rfc/rfc2004.txt. October 1996.

[10] CW, et al.2002] Chun-Hsin Wu, AnnTzung Cheng, Shao-Ting Lee, Jan-Ming Ho, Der-Tsai Lee. Bi-directional Route Optimization in Mobile IP Over Wireless LAN. 2002.

[11] CS.2001] Cisco Systems. Cisco Mobile Networks. http://www.cisco.com/warp/public /732/Tech/mobile/networks/. 2001.

[12] SN, RP. 2002] Sanket Nesargi, Ravi Prakash. Configuration of Hosts in a Mobile Ad Hoc Network. 2002.

[13] CR, et al.2000] C. Rigney, S. Willens Livingston, A. Rubens Merit, W. Simpson Daydreamer. Remote Authentication Dial In User Service (RADIUS). http://www.ietf.org/rfc/rfc2865.txt. June 2000.

[14] PC, et al.2002] Pat R. Calhoun, John Loughney, Erik Guttman, Glen Zorn, Jari Arkko. Diameter Base Protocol. http://www.ietf.org/internet-drafts/draft-ietf- aaa-diameter-17.txt. December 2002.

[15] PF, et al.1998] P. Ferguson, D. Senie. Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing. http://www.ietf.org/rfc/ rfc2267.txt. January 1998.

[16] GM.2001] G. Montenegro. Reverse Tunneling for Mobile IP, revised. http://www.ietf.org/rfc/rfc3024.txt. January 2001.

[17] JI, et al.1996] John Ioannidis, Dan Duchamp & Gerald Q. Maguire Jr. IP-based protocols for Mobile Internetworking. 1996.

[18] TIA.1995] Telecommunications Industry Association. Mobile Station --- Base Station compatibility standard for dualmode wideband spread spectrum cellular systems. July 1995.

[19] JV, et al.1997] J. Veizades E. Guttman, C. Perkins, S. Kaplan. Service Location Protocol. http://www.ietf.org/rfc/rfc2165.txt.June 1997.

[20] CP.1998] Charles E. Perkins. Mobile Networking in the Internet. http://ntrg.cs.tcd. ie/htewari/papers/mnt071.pdf. 1998.

[21] JL.2003] John O'Leary. World Trade Council of Wichita Inc. Program Proceedings. April 2003.

[22] EMS] Emergency Medical Services: LifeLink Model Deployment Initiative System Users Manual. http://www.transguide. dot.state.tx.us/mdi/LifeLink_Systems.pdf.

[23] J J.2002] Joab Jackson. Mobile IP networks stir interest. http://www.washingtontechnology.com/ news/17_18/emergingtech/19644-1.html. December 2002.

[24] WF, FH.2000] Wolfgang Fritsche, Florian Hiessenhuber. Mobile IPv6, Mobilty Support for the Next Generation Internet. 2000.

[25] DJ, et al.2003] D. Johnson C. Perkins J. Arkko. Mobility Support in IPv6 [Work in Progress]. http://www.ietf.org/internet-drafts/draft-ietf-mobileip-ipv6-21.txt. Feb 2003.

[26] SM.2003] Sun Microsystems. All IP Wireless All the time. http://research.sun.com/features/4g_wireless/mob ileORportable.html.

****

