Mobile Devices on IP Internetworks

Ms. Susanna S Henry, Dr. V. Santhosh Kumar

Computer Science, Birla Institute of Technology & Science, Pilani
Dubai Campus,
Dubai International Academic City
P. O. Box No. 345055, Dubai, UAE

Computer Science, Birla Institute of Technology & Science, Pilani
Dubai Campus,
Dubai International Academic City
P. O. Box No. 345055, Dubai, UAE

Abstract

Due to advances in miniaturization, Mobile computing has greatly increased in popularity over the past years. Today we can get in a notebook PC or even a hand-held computer the power that once required a massive machine. Wireless LAN technologies help a device to easily move from one place to other and still retain networking connectivity at the data link layer. Unfortunately, the Internet Protocol was developed back in the era of those bulky or massive machines, thus IP is not designed to deal gracefully with computers that move around. To understand why IP doesn't work well in a mobile environment, we must take a look back at how IP addressing and routing function

Keywords: *Mobile IP, network identifier (network ID), Mobile Node, Home Agent, Foreign Agent, Care-Of Address, Quality of Service (QoS)*

1. Introduction

IP addresses are fundamentally divided into two portions: A network identifier (network ID) and a host identifier (host ID).The network ID specifies which network a host is on, and the host ID uniquely specifies hosts within a network. This structure is fundamental to datagram routing, because devices use the network ID portion of the destination address of a datagram to determine if the recipient is on a local network or a remote one, and routers use it to determine how to route the datagram. This is a great system, but it has one critical flaw: the IP address is tied tightly to the network where the device is located. Most devices never (or at least rarely) change their attachment point to the network, so this is not a problem, but it is certainly an issue for a mobile device. When the mobile device travels away from its home location, the system of routing based on IP address "breaks".

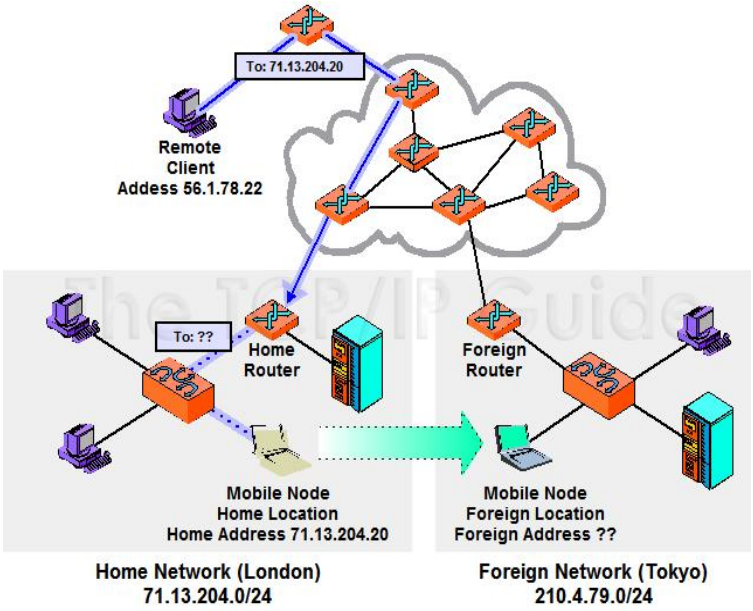

Figure 1: The Main Problem with Mobile Devices on IP Internetworks

In this example, a mobile device (the notebook PC) has been moved from its home network in London to another network in Tokyo. A remote client (upper left) decides to send a datagram to the mobile device. However, it has no idea the device has moved. Since it sends using the mobile node's home address, 71.13.204.20, its request is routed to the router responsible for that network, which is in London. Of course the mobile device isn't there, so the router can't deliver it.

Mobile IP solves this problem by giving mobile devices and routers the capability to forward datagrams from one location to another [1].

2. Difficulties with Older Mobile Node Solutions

The tight binding of network identifier and host IP address means that there are only two real options under conventional IP when a mobile device moves from one network to another:

- **Change IP Address:** We can change the IP address of the host to a new address that includes the network ID of the network to which it is moving.
- **Decouple IP Routing From Address:** We can change the way routing is done for the device, so that instead of routers sending datagrams to it based on its network ID, they route based on its entire address.

Unfortunately, The above two options are inefficient, they both seem like viable options at first glance, but they are often impractical and not ***scalable,*** meaning, they are not practical when thousands or millions of devices try them:

- Changing the IP address each time a device moves normally requires manual intervention and is time-consuming. In addition, the entire TCP/IP stack would need to be restarted, breaking any existing connections.
- If we change the mobile device's IP address, how do we communicate the change of address to other devices on the Internet? These devices will only have the mobile node's original home address, which means they won't be able to find it even if we give it a new address matching its new location.
- Routing based on the entire address of a host would mean the entire Internet would be flooded with routing information for each and every mobile computer. Considering how much trouble has gone into developing technologies like classless addressing to reduce routing table entries, it's obvious this is a Pandora's Box nobody wants to touch.

3. A Better Solution: Mobile IP

The solution to these difficulties was to define a new protocol that will support mobile devices, and which also adds up to the original Internet Protocol. The technology is commonly called *Mobile IP* .To ensure its success, Mobile IP's designers had to meet a number of important goals. The key attributes and features of the resulting protocol are as follows:

- **Seamless Device Mobility Using Existing Device Address:** While continuing to use their existing IP address mobile devices can change their physical network attachment method and location
- **No New Addressing or Routing Requirements:** The overall scheme for addressing and routing as in regular IP is maintained. IP addresses are still assigned in the conventional way, by the owner of each device. No new routing requirements are placed on the internetwork, such as host-specific routes.
- **Interoperability:** Mobile IP devices can still send to and receive from existing IP devices that do not know how Mobile IP works, and vice-versa.
- **Layer Transparency:** The changes made by Mobile IP are confined to the network layer. Transport layer and higher layer protocols and applications are able to function as in regular IP, and existing connections can even be maintained across a move.
- **Limited Hardware Changes:** Hardware devices do not need any changes; however, Changes are required to the software in the mobile device, as well as to routers used directly by the mobile device, including routers between the ones on the home and visited networks.
- **Scalability:** Mobile IP allows a device to move from any network to any other, and supports this for an arbitrary number of devices. The scope of the connection change can be global; you could detach a notebook from an office in London and move it to Australia or Brazil, for example, and it will work the same as if you took it to the office next door.
- **Security:** Mobile IP works by redirecting messages, and includes authentication procedures to prevent an unauthorized device from causing problems.

Mobile IP accomplishes these goals by implementing a *forwarding system* for mobile devices. When a mobile unit is on its "home" network, it functions normally. When it moves to a different network, datagrams are sent from its home network to its new location. This allows normal hosts and routers that don't know about Mobile IP to continue to operate as if the mobile device had not moved. Special support services are required to implement Mobile IP, to allow activities such as letting a mobile device determine where it is, telling the home network where to forward messages and more.

Mobile IP is often associated with wireless networks, since devices using WLAN technology can move so easily from one network to another. However, it wasn't designed specifically for wireless. It can be equally useful for moving from an Ethernet network in one building to a network in another building, city or country. Mobile IP can be of great benefit in numerous applications, including traveling salespeople, consultants who visit client sites, administrators that walk around a campus troubleshooting problems, and much more. Mobile IP solves the problems associated with devices that change network locations, by setting up a system where datagrams sent to the mobile node's home location are forwarded to it wherever it may be located. It is particularly useful for wireless devices but can be used for any device that moves between networks periodically [1].

4. Mobile IP Device Roles

Just as mail forwarding requires support from one or more post offices, Mobile IP requires the help of two routers. In fact, special names are given to the three main players that implement the protocol.

- **Mobile Node:** This is the mobile device, the one moving around the internetwork.
- **Home Agent:** This is a router on the home network that is responsible for catching datagrams intended for the mobile node and forwarding them to it when it is traveling. It also implements other support functions necessary to run the protocol.
- **Foreign Agent:** This is a router on the network to which the mobile node is currently attached. It serves as a "home away from home" for the mobile node, normally acting as its default router as well as implementing Mobile IP functions. Depending on the mode of operation, it may receive forwarded datagrams from the home agent and forward them to the mobile node. It also supports the sharing of mobility information to make Mobile IP operate. The foreign agent may not be required in some Mobile IP implementations but is usually considered part of how the protocol operates.

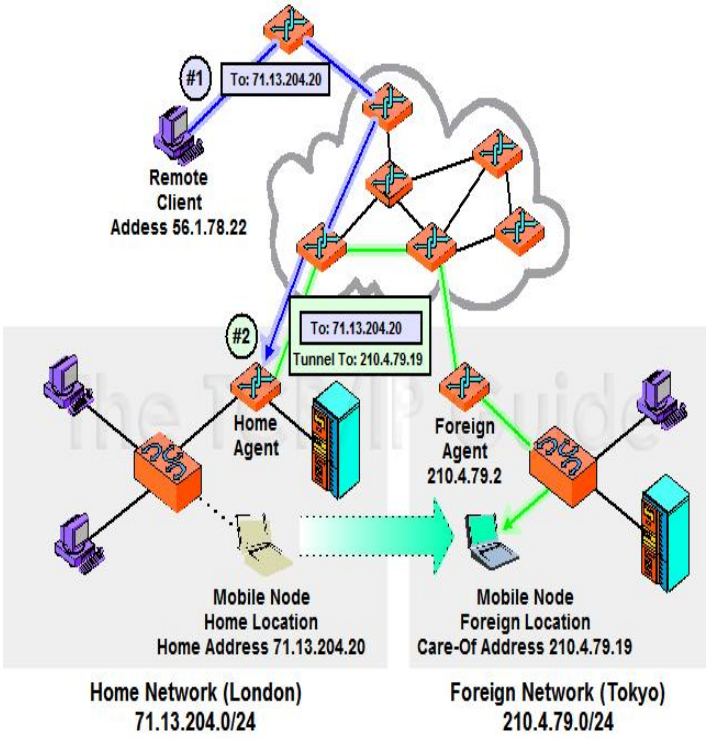

Figure 2: General Operation of the Mobile IP Protocol

5. Mobile IP Functions

Mobile IP includes a host of special functions that are used to set up and manage datagram forwarding. To see how these support functions work, we can describe the general operation of Mobile IP as a simplified series of steps:

1. **Agent Communication:** The mobile node finds an agent on its local network by engaging in the *Agent Discovery* process. It listens for *Agent Advertisement* messages sent out by agents and from this can

determine where it is located. If it doesn't hear these messages it can ask for one using an *Agent Solicitation* message.

2. **Network Location Determination:** The mobile node determines whether it is on its home network or a foreign one by looking at the information in the *Agent Advertisement* message.

If it is on its home network it functions using regular IP. To show how the rest of the process works, let's say the device sees that it just moved to a foreign network. The remaining steps are:

3. **Care-Of Address Acquisition:** The device obtains a temporary address called a *care-of address*. This comes from the *Agent Advertisement* message from the foreign agent. This address is used only as the destination point for forwarding datagrams, and for no other purpose.
4. **Agent Registration:** The mobile node informs the home agent on its home network of its presence on the foreign network and enables datagram forwarding, by *registering* with the home agent. This may be done either directly between the node and the home agent, or indirectly using the foreign agent as a conduit or a channel.
5. **Datagram Forwarding:** The home agent captures datagrams intended for the mobile node and forwards them. It may send them either directly to the node or indirectly to the foreign agent for delivery, depending on the type of care-of address in use.

Datagram forwarding continues until the current agent registration expires. The device can then renew it. If it moves again, it repeats the process to get a new care-of address and then registers its new location with the home agent. When mobile node returns back to its home network, it deregisters to cancel datagram forwarding and resumes normal IP operation.

5.1 The Mobile-IP addresses

Just as most of us have only a single address used for our mail, most IP devices have only a single address. The Mobile-IP-equipped notebook needs to have two addresses as well

- Home Address: This is the address used by the device on its home network, the "normal", permanent IP address assigned to the mobile node and the one to which datagrams intended for the mobile node are always sent.
- Care-Of Address: A secondary, temporary address used by a mobile node while it is 'traveling" away from its home network. It is a normal 32-bit IP address in most respects, but is used only by Mobile IP for forwarding IP datagrams and for administrative functions. Higher layers never use it, nor do regular IP devices when creating datagrams.

5.2 Mobile IP Care-Of Address Types

There are two different types of care-of Address, which correspond to two distinctly different methods of forwarding datagrams from the home agent router.

- Foreign Agent Care-Of Address: This is a care-of address provided by a foreign agent in its Agent Advertisement message. It is, in fact, the IP address of the foreign agent itself. When this type of care-of address is used, all datagrams captured by the home agent are not relayed directly to the mobile node, but indirectly to the foreign agent, which is responsible for final delivery.
- Co-Located Care-Of Address: This is a care-of address assigned directly to the mobile node. It may be assigned on the foreign network manually, or automatically **[1]**.

Mobile IP or Mobile IPv4 is an Internet protocol designed to support mobility in mobile devices that keep moving without physical interruption and reconnection. Operations of Mobile IPv4 include 3 main steps [6]:

Agent Discovery: In this step, Mobile Node recognizes where it is. If it is in a foreign network, it will require a new Care-of Address.

Agent Registration: Mobile Node registers its Care-of Address with Home Agent. Home Agent updates its routing table and prepares for forwarding packets addressed with Mobile Node's home address to Mobile Node.

Data Delivering: Communication Node communicates with Mobile Node via Home Agent.
Details of the Operations of Mobile IPv4 is given below

Agent Discovery: Home Agent and Foreign Agent broadcast or multicast Agent Advertisement Message constantly to monitor Mobile Node. When Mobile Node moves far from Home Network, it tries to catch the Agent Advertisement message, compares the IP inside message with its Home Address to recognize where it is now, then it sends an Agent Solicitation Message to announce to the local router about its appearance and requires a Care-of Address. If Mobile Node doesn't receive any Advertisement Message, it will broadcast Solicitation Message continuously to find out a Mobility Agent (HA or FA) and request the Agent to solicit to its advertisement message immediately [3][6].

Agent Registration: When Mobile Node receives a Care-of Address, Mobile Node must register this address to its Home Agent so that Home Agent can forward packets destined exactly to Mobile Node. This process can be described as follow: Mobile Node sends a Registration Request Message to Home Agent via Foreign Agent. If Foreign Agent does not have enough resource or this message is not suitable with the rights set up at Foreign Agent, then Foreign Agent can discard the message. If the message is accepted by Foreign Agent, it will be forwarded to Home Agent. When Home Agent receives the message, it updates the binding cache and sends a Registration Reply Message back to Mobile Node bypass Home Agent. Home Agent then forwards this message to Mobile Node and the Care-of Address registration process is completed and data transferring between Mobile Node and Communication Node can be implemented.

Data Delivering: In transferring data to Mobile Node, Communication Node just needs to know Mobile Node's Home Address such that it can communicate with Mobile Node by this address. In the case that Mobile Node is in its Home Network, Communication Node sends packets to Mobile Node's Home Address and Home Agent forwards these packets to Mobile Node directly. In other case, when Mobile Node is in Foreign Network, Communication Node still sends data destined to Mobile Node through Home Agent. Then Home Agent encapsulates each of packets with Mobile Node's Care-of Address and forwards them to Mobile Node's current address via Foreign Agent. When Mobile Node receives packets, it decapsulates them and gets the original data sent from Communication Node.

6. Security related requirements in Mobile IP

As the use of mobile nodes becomes more common, five security related requirements become vital:

6.1. Authentication and Integrity. The receiver of a message should be able to ascertain who the actual originator of the message is; thereby negating an intruder from masquerading as a legitimate source of the message in question. The majority of networks that mobile nodes visit will be wireless nets which are subject to eavesdropping and unable to control actual attachment via physical controls. Unless a wireless network provides encryption, frequency hopping or other form of link layer access controls or privacy mechanisms, a rogue or hostile Foreign Agent could transmit messages indistinguishable from legitimate Foreign Agent messages. When a Mobile Node receives an Agent Advertisement message, the Mobile Node needs to know it comes from a valid Foreign Agent. Without authentication a hostile Foreign Agent could easily masquerade as a legitimate Foreign Agent and present a denial-of-service threat (as well as other privacy and integrity threats) by:

- Issuing registration reply messages stating the Mobile Node registration request is denied
- Forwarding Mobile Node registration requests to an address other than that of the Mobile Node’s Home Agent causing the

Mobile Node to never receive a Registration reply from its Home Agent.

- Discarding Mobile Node registration requests causing the Mobile Node to never receive a registration reply from its Home Agent.

When a Mobile Node wants to attach to a foreign network, the Foreign Agent needs to know the authentic identity of the Mobile Node. The actual decision to allow the attachment falls within the area of authorization but the Foreign Agent cannot make a valid decision unless it knows, with some defined degree of assurance, that the Mobile Node is who it says it is . When a Mobile Node sends a registration message to its Home Agent, the Home Agent must be able to determine that the registration message really did originate from the Mobile Node. Should the Home Agent accept a registration message which did not originate from the real Mobile Node, a denial-of service threat exists. Any messages sent between Mobile Nodes Home Agents and Foreign Agents that affect how IP packets are routed must be received at the destination exactly as sent by the message source. Failure to validate the integrity of these types of messages allows a hostile node to modify these messages while in transit. Modification could easily result in a Mobile Node's attempt to register at a foreign network being denied or the registration occurring but packets destined for the Mobile Node being misroute/lost.

6.2. Authorization. The organization which owns/operates a network should have the ability to decide who may attach to the network and what network resources may be used by the attaching node. Access control (authorization) at a foreign network being visited by a Mobile Node is critical within a mobile node context. Networks supporting visiting Mobile Nodes need the ability to decide which Mobile Nodes are allowed visiting rights. These networks also need a mechanism by which access control information may be defined, stored, validated and applied to requested Mobile Node visits. An IP mobility protocol needs to address the mechanism(s) by which a network node obtains authorization information and guidelines to ensure interoperability between different implementations.

6.3. Nonrepudiation. The sender of a message should not be able to falsely deny that it originated a message at a later time. When a Mobile Node visits a foreign network the Mobile Node will consume network resources (i.e. number of packets sent/received, number of packets detunneled by the Foreign Agent, assigned IP address space, etc.). From the perspective of the organization responsible for the visited network, a record of what resources are consumed by the visiting Mobile Node needs to be kept for performance and accounting management purposes. The Foreign Agent must have a way of identifying which Mobile Node consumed what resources such that the owner of the Mobile Node cannot deny the visit or resources consumed. The use of digital signatures provides the organization, owning the visited network, an undeniable way to positively identify a visiting Mobile Node.

6.4. Key Management. The only method available to accurately enforce authentication, integrity and nonrepudiation is by using some form of cryptography; which requires the Distribution/exchange of encryption key information amongst message senders and receivers. Strong authentication, integrity and nonrepudiation approaches are based primarily on the use of cryptographic algorithms. If the security of a cryptographic algorithm is based on keeping the way the algorithm works a secret, then the algorithm is inadequate by today's standards. Modem algorithms base their security capabilities on the use of a key, or keys, which allows the algorithm(s) to be publicly available so long as the keying information is kept and distributed in a private manner. One method for distributing the key information is to manually load it into each node. This is fine for a small number of nodes but runs into administrative problems. If a separate key is used for each pair of nodes, the total number of keys increases rapidly as the number of user's increases. *N* users require $N(N-1)/2$ keys. Individual key pairs

amongst *1000* nodes would require 499,500 keys, where each key must be kept and distributed in a secure manner. It quickly becomes apparent that manual key distribution is not feasible for use in IP mobility except with a very small number of nodes. A truly viable solution for Mobile Nodes must scale well to large numbers of mobile nodes by providing a secure dynamic key distribution function.

6.5. Location Privacy. The sender of a message should be able to control which, if any, receivers know the location of the sender's current physical attachment to the network. Location privacy is concerned with hiding the location of a Mobile Node from Communicating Nodes. One can envision situations when the user of a Mobile Node does not want Communication Nodes to know the Mobile Node is not at its home network. However, when a Mobile Node wishes to hide its current location, Communication Nodes are forced to fall back to using the Mobile Node's permanent home address when sending packets to the Mobile Node, thereby introducing possible extra network traffic [5].

7. Mobile IP Quality of Service (QoS)

Mobility gives a significant impact to the QoS management. This is because, in a mobile environment, QoS management requires much more sophisticated techniques than those used in fixed systems. As an example, a short loss of communication during handoffs may occur, which is usually not acceptable [4]. Therefore, Quality of Service (QoS) is an important issue that should be addressed to provide acceptable and predictable level of service to the end user. In a layered protocol stack model, QoS is a guaranteed level of performance that a protocol is capable of delivering to a higher-layer protocol. It is important to note that we need to consider different QoS metrics and requirements depending on the type of application and the network environment. [2] [5] [6].

7.1 Quality of Service Parameters (QoS)

QoS between a home agent and a foreign agent of a Mobile IP network is described below. In response to a registration request message originated from a mobile node coupled to a foreign network, a registration reply message is received from a home agent of a home network. Quality of service (QoS) parameters are extracted from this registration reply message Thus, network traffics between mobile node of the foreign network and home agent of the home network associated with the mobile node are routed according to at least a portion of the QoS parameters. The QoS parameters are applied specifically to a subscriber session of a mobile node between a foreign agent and a home agent of the mobile node (e.g., per session basis). As a result, different QoS parameters may be applied based on a particular session and/or a particular foreign agent, or other circumstance factors.

The following steps provide a rough outline of operation of the Mobile IP protocol:

- Mobility agents (i.e., foreign agents and home agents) advertise their presence via Agent Advertisement messages. A mobile node may optionally solicit an Agent Advertisement message from any locally attached mobility agents through an Agent Solicitation message.

- A mobile node receives these Agent Advertisements and determines whether it is on its home network or a foreign network.

- When the mobile node detects that it is located on its home network, it operates without mobility services. If returning to its home network from being registered elsewhere, the mobile node deregisters with its home agent, through exchange of a Registration Request and Registration Reply message with it.

- When a mobile node detects that it has moved to a foreign network, it obtains a care-of address on the foreign network. The care-of address can either be determined from a foreign agent's advertisements (a foreign agent care-of address), or

by some external assignment mechanism such as DHCP [7] (a co-located care-of address).

- The mobile node operating away from home then registers its new care-of address with its home agent through exchange of a Registration Request and Registration Reply message with it, possibly via a foreign agent.

- Datagram's sent to the mobile node's home address are intercepted by its home agent, tunneled by the home agent to the mobile node's care-of address, received at the tunnel endpoint (either at a foreign agent or at the mobile node itself), and finally delivered to the mobile node.

- In the reverse direction, datagrams sent by the mobile node are generally delivered to their destination using standard IP routing mechanisms, not necessarily passing through the home agent **[3].**

8. APPLICATIONS

Mobile IP is most often found in wired and wireless environments where users need to carry their mobile devices across multiple LAN subnets with different IP addresses. It may for example be used in roaming between overlapping wireless systems, for example IP over WLAN and Wi Max. Currently, Mobile IP is not required within cellular systems such as 3G, to provide transparency when internet users migrate between cellular towers, since these systems provide their own data link layer handover and roaming mechanisms. However, it is often used in 3G systems to allow seamless IP mobility between different Packet Data Serving Node (PDSN) domains Moreover, with the arrival of IPv6; mobile IP concept can be more implemented in ISPs and mobile phone services. Since there is no concept of Private IP or Public IP in IPv6, mobile IPv6 can be a very convincing way to access seamless network along mobility.

9. BENEFITS

Mobile IP is most useful in environments where mobility is desired and the traditional land line dial in model or DHCP do not provide adequate solutions for the needs of the users. If it is necessary or desirable for a user to maintain a single address while they transition between networks and network media, Mobile IP can provide them with this ability. Generally, Mobile IP is most useful in environments where a wireless technology is being utilized. This includes cellular environments as well as wireless LAN situations that may require roaming. Mobile IP can go hand in hand with many different cellular technologies like CDMA, TDMA, GSM, AMPS, NAMPS, as well as other proprietary solutions, to provide a mobile system which will scale for many users Each mobile node is always identified by its home address, no matter what its current point of attachment to the Internet allowing for transparent mobility with respect to the network and all other devices. The only devices which need to be aware of the movement of this node are the mobile device and a router serving the user's topologically correct subnet PROSPECTS / EXTENTIONS
Enhancements to the Mobile IP technique, such as Mobile IPv6and Hierarchical Mobile IPv6 (HMIPv6), are being developed to improve mobile communications in certain circumstances by making the processes more secure and more efficient.

10. Conclusions

In this paper, we have introduced various aspects of Mobile Devices on IP Internetworks. The Difficulties faced by Older Mobile Nodes while travelling from one network to the other network, Thus Mobile IP being considered as a better solution. Mobile IP Devices with Mobile IP functions and Security related requirements are discussed. This paper also provides an insight on Quality of Service (QoS) parameters, thus concluding with the Applications and Benefits of Mobile IP.

References:

[1]. Charles M. Kozierok, The TCP/IP Guide

[2]. Fayza Nada, Performance Analysis of Mobile IPv4 and Mobile IPv6, The International Arab Journal of Information Technology, Vol 4, No. 2, 153-160, April 2007.

[3]. C. Perkins, Ed, Nokia Research Center, IP Mobility Support for IPv4, RFC 3344, August 2002.

[4]. C. Perkins, Ed, WiChorus Inc, IP Mobility Support for IPv4, Revised, RFC 3344, ISSN: 2070-1721, November 2010.

[5]. C. Perkins, P. Calhoun, J. Bharatia, Mobile IPv4 Challenge/Response Extensions (Revised), RFC 4721, January 2007.

[6]. Michal Skorepa, Mobile IPv4 – Simulation and Implementation, GACR project 102/06/1569.

[7]. Matthew G. Marsh, Policy Routing With Linux - Online Edition, Section1, Chapter 1: Basic IPv4 Routing.

[8]. Anand K.Oswal, Ramakanthan Lakshmikanthan, Quality of service (QoS) negotiation between network nodes in a Mobile IP network, Patent application number: 20080240053, February 2008.