A Survey Paper on Mobile IP

By **Yi-an Chen**

ABSTRACT

Mobile Internet Protocol (IP) is a new recommended Internet protocol designed to support the mobility of a user (host). Host mobility is becoming important because of the recent blossoming of laptop computers and the high desire to have continuous network connectivity anywhere the host happens to be. The development of Mobile IP makes this possible. This paper describes and summarizes the characteristics of the current Internet draft for Mobile IP. In addition to the current internet draft, this paper also discusses alternative Mobile IP proposals so that the reader may understand the different design issues associated with the different protocols.

Table of Contents

Introduction

Background -- The Problem with Old IPs

Current internet protocol versions do not support host mobility. These were designed such that moving hosts were not considered: a node's point of attachment to the network remains unchanged at all times, and an IP address identifies a particular network. To support a mobile host with current methods, reconfiguration is necessary any time a mobile host moves. This is an unacceptable solution as it is time consuming and error prone. Thus, the rise of Mobile IP.

What is Mobile IP?

Mobile IP is an internet protocol designed to support host mobility. Its goal is to provide the ability of a host to stay connected to the internet regardless of their location. Mobile IP is able to track a mobile host without needing to change the mobile host's long-term IP address.

Features [1,4]

Mobile IP has several features associated with it:

No geographical limitations:

A user can take a palmtop or laptop computer anywhere without losing the connection to the home network.

No physical connection required:

Mobile IP finds local IP routers and connects automatically. It is phone jack and wire free.

Modifications to other routers and hosts is not required:

Other than mobile nodes/routers, the remaining routers and hosts will still use current IP. Mobile IP leaves transport and higher protocols unaffected.

No modifications to the current IP address and IP address format:

The current IP address and address format remains the same.

Supports security:

Authentication is performed to ensure that rights are being protected.

Impact [1]

Network access is assured at all times and from all locations. Home and local resources would be accessible continuously. E- mail would never be missed, and there would no longer be an excuse for lack of productivity due to lack of connectivity.

Entities and Services

Entities [3]

Mobile IP is consisting of the following entities:

Mobile Node (MN):

A host or router that may change its point of attachment from one network or subnetwork to another through the internet. This entity is pre-assigned a fixed home address on a home network, which other correspondent hosts will use to address their packets to, regardless of its current location.

Home Agent (HA):

A router that maintains a list of registered mobile nodes in a visitor list. It is used to forward mobile node-addressed packets to the appropriate local network when the mobile nodes are away from home. After checking with the current mobility bindings for a particular mobile node, it encapsulates (see below) datagrams and sends it to the mobile host's current temporary address when the mobile node.

Foreign Agent (FA):

A router that assists a locally reachable mobile node that is away from its home network. It delivers information between the mobile node and the home agent.

Care-of-address (COA):

An address which identifies the mobile node's current location. It can be viewed as the end of a tunnel (see below) directed towards a mobile node. It can be either assigned dynamically or associated with its foreign agent.

Correspondent Node (CN):

This node sends the packets which are addressed to the mobile node.

Home Address:

A permanent IP address that is assigned to a mobile node. It remains unchanged regardless of where the mobile node is attached to the internet.

Mobility Agent:

An agent which supports mobility. It could be either a home agent or a foreign agent.

Tunnel:

The path which is taken by encapsulated (see below) packets. It is the path which leads packets from the home agent to the foreign agent.

Support Services [3]

The following services are supported in Mobile IP:

Agent Discovery:

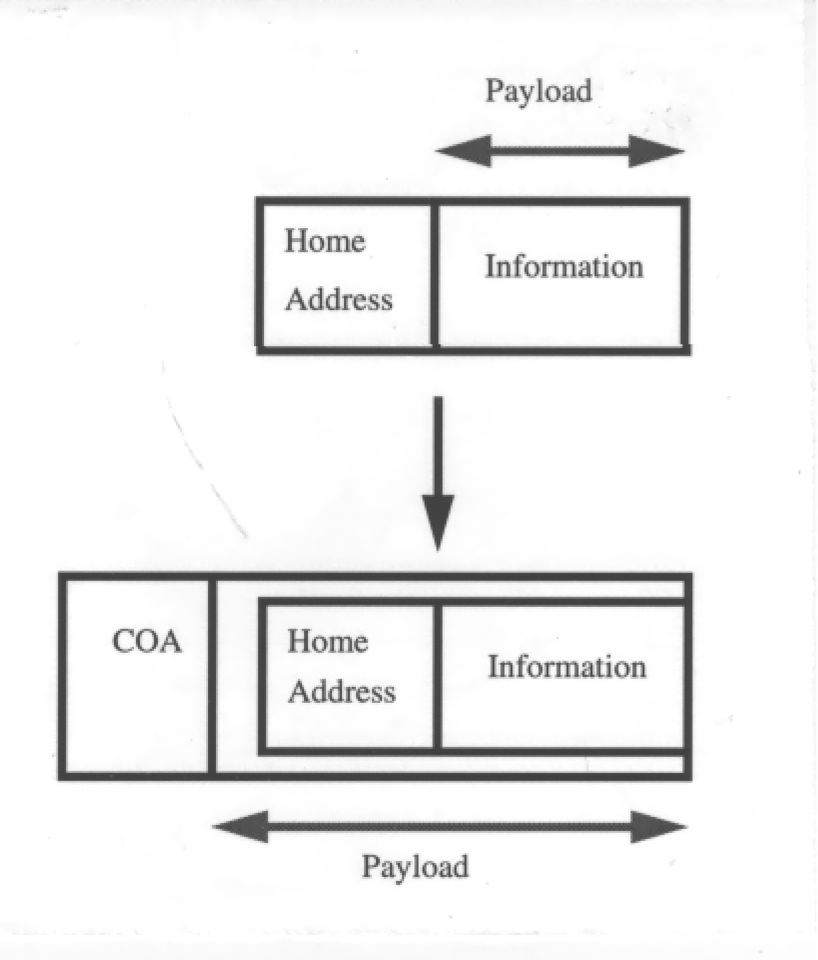
Home agents and foreign agents broadcast their availability on each link to where they can provide service. A newly arrived mobile node can send a solicitation on the link to learn if any prospective agents are present.

Registration:

When the mobile node is away from home, it registers its care-of-address with its home agent so that the home agent knows where to forward its packets. Depending on the network configuration, the mobile node could either register directly with its home agent, or indirectly via the help of its foreign agent.

***Encapsulation:*[8]**

The process of enclosing an IP datagram within another IP header which contains the care-of-address of the mobile node. The IP datagram itself remains intact and untouched throughout the enclosing process (figure 1).

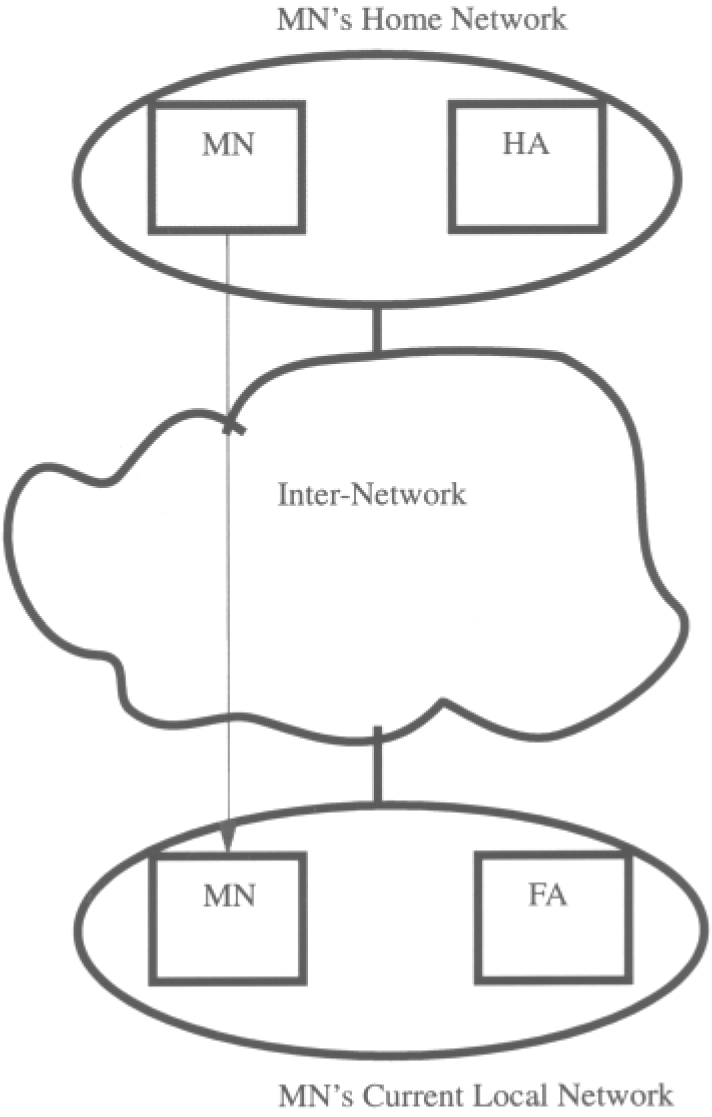


Decapsulation:

The process of stripping the outermost IP header of the incoming packets so that the enclosed datagram can be accessed and delivered to the proper destination. Decapsulation is the reverse process of encapsulation.

Operations

To best picture the relationships between MN, HA, and FA, you can think of it as that between Jeff, his permanent home post office, and his current local post office. Jeff is on vacation for a while. After moving, Jeff would write a temporary change-of-address card to his permanent home post office to inform them about his new address and how long this new address will be valid, so as to avoid missing important mail. With this notification, every time Jeff's home post office gets his mail with his home address, it would attach his new address and forward it to Jeff's current local post office. Jeff's current local post office would then deliver it to Jeff's address. The current local post office and home post office will continue to repeat this process until the end-date indicated on the change-of-address card expires. If Jeff were to later change his mind and decide to stay longer, he could send another request to his home post office to extend the forwarding of his mail. Figure 2 illustrates the relationships between the HN, HA, and FA.



Overall Processes [3]

Four different stages in chronological order:

Agent discovery:

When a mobile node is away from home, it wants to find agents so it does not lose access to the Internet. There are two ways of finding agents. The first is by selecting an agent from among those periodically advertised, and the second is by sending out a periodic solicitation until it receives a response from a mobility agent. The mobile node thus gets its care-of-address which may be dynamically assigned or associated with its foreign agent.

Registration:

The mobile node registers its care-of-address with its home agent in order to obtain service. The registration process can be performed directly from the mobile node, or relayed by the foreign agent to the home agent, depending on whether the care-of-address was dynamically assigned or associated with its foreign agent. Note that simultaneous registrations with multiple care-of-addresses is possible.

In service:

This is the period after the registration process and before the service time expiration, provided that the mobile node stays in the service area. During service time, the mobile node gets forwarded packets from its foreign agent which were originally sent from the mobile node's home agent. Tunneling is the method used to forward the message from home agent to foreign agent and finally to mobile node.

Deregistration:

After the mobile node returns home, it deregisters with its home agent to drop its registered care-of-address. In other words, it sets its care-of-address back to its home address. The mobile node achieves this by sending a registration request directly to its home agent with the lifetime set to zero. There it is no need to deregister with the foreign agent because the service expires automatically when the service time expires.

Detailed operations

Goal Summary [3]

Mobile Node's Main Goal

A mobile node's main responsibility is generally to listen for agent advertisements and initiate the registration when a change in its network connectivity is detected. When it is away from home, the mobile node will register with its home agent so its home agent will do mobility binding for it. When it returns home, it would send a register request with the proper code to tell its home agent to erase any previous mobility binding to it.

Home Agent's Main Goal

A home agent's main responsibility is generally to process and coordinate mobility services. It receives registration or responds to a registration request with a reply message, and it encapsulates the datagram addressed to its mobile client, and passes it to the FA.

Foreign Agent's Main Goal

A foreign agent's main responsibility is generally to relay a registration request and reply between the home agent and the mobile node, and decapsulates the datagram for delivery to the mobile node. So the foreign agent only functions when it is asked. Therefore, the foreign agent is passive and plays a minimal role, compared to the home agent and the mobile node.

Mobile Node and Home Agent [3]

-Establish contact between the mobile node and the home agent

If the mobile node knows a home agent's address in its home network beforehand, it could go ahead and send a registration request to the home to ask for service. Otherwise, the following technique could be used to find a home agent: the mobile node may send a registration request to the directed broadcast address of the home network, and it will get a registration reply from an arbitrary home agent in the home network. This home agent's address is also included within the reply message. Therefore, the mobile node can re-issue the registration request with the correct home agent address.

-Registration process between the mobile node and the home agent

The registration message set by the mobile node to its home agent could either be relayed by its foreign agent, or directly sent from the mobile node, depending on whether or not the mobile node is able to dynamically acquire a transient IP address, which plays a role as the care-of address. Either way would work to get the request message out to the home agent.

To complete the registration procedure between both parties, two steps should be performed: the home agent receives the registration request from the mobile node, and the mobile node receives the registration reply from the home agent.

Step 1:

The mobile node send a registration request containing the following information:

- Type: message type
- Code: information about the request
- Lifetime: desired service time; a value of zero indicates deregistration
- Home Address: the IP address of the mobile node
- Home Agent: the IP address of its home agent
- Care-of-Address: the IP address for the decapsulation end of a tunnel
- Identification: used to protect against reply attacks

Step 2:

After receiving the registration request from the mobile node, the home agent should send a reply message containing the following information:

- Type: message type
- code: status about the mobile node's request
- Lifetime: duration of the registration granted
- Home Address: the IP address of the mobile node
- Home Agent: the IP address of the home agent
- Identification: used by the mobile node in matching its reply with an outstanding request

-What happens after the completion of the registration process

After both steps are followed, the registration process between the mobile node and the home agent is complete. However, the end result could be either a successful registration or a failed registration. For a successful registration, for which service has been granted, the home agent starts to serve its client -- the registered mobile node -- by accepting the incoming datagram which is addressed to the mobile node, encapsulating the datagram, and forwarding it to the mobile node's care-of address. The mobile node's foreign agent then gets the encapsulated datagram, decapsulates it, and finally delivers it to the mobile node. For the case of the mobile node not having a foreign agent because it itself has a transient address, the datagram is directly and forwarded intact to the mobile node from the home agent without going through the intermediate step. The home agent will iterate the procedure until the service time expires for the mobile node. It is the responsibility of the mobile node to notify the home agent by issuing a new registration request if it wants to extend the service time, or to cancel the service.

Mobile Node and Foreign Agent [15]

-Establish contact between the mobile node and the foreign agent

There are two ways for the mobile node to know about a foreign agent:

1) Some foreign agents will continuously signal their existence by emitting beacon messages. When the mobile node moves, it will continuously listen to a set of channels, trying to pick out a foreign agent whose signal is the clearest and the most recognizable. A beacon message of a foreign agent contains the following information:

- Type, code, checksum
- Care-of address
- Foreign agent's address
- Foreign agent's incarnation number
- Advertisement interval
- Media address

2) Instead of waiting for periodically emitted beacons, the mobile node may send a solicitation at a regular interval until the solicitation is answered by a foreign agent. A solicitation message contains the following entries:

- Type, code, checksum
- Mobile node IP address
- Media address

After a foreign agent is chosen, through the use of either of the above methods, the next stage is for the mobile node to send a registration request to the foreign agent to ask for service, and then for the foreign node to return a reply message to confirm the status of the request.

-Registration process between the mobile node and the foreign agent

The procedures performed and message formats in this section are similar to those described in the "Registration process between the mobile node and the home agent" section. Please refer to it for information. However, unlike the home agent, if the foreign agent is able to satisfy the incoming registration request, it simply relays the request to the home agent. The registration reply is only sent by it when it rejects the request, i.e. the requested lifetime is too long.

-What happens after the completion of the registration

The foreign agent's role is very passive and minimal. After it grants service to the mobile node, it starts to relay the datagram from the home agent to the mobile node, or to relay the mobile node's registration request to the home agent. When the mobile node wants to send a datagram to some correspondent node, the mobile node forwards the datagram to the foreign agent, which then relays it to the correspondent node using normal IP routing. A home agent is not involved. Therefore, the path from the mobile node to the correspondent node is shorter than the path from the correspondent node to the mobile node.

Since the home agent encapsulates the datagram before it is sent out to the care-of address, the foreign agent needs to decapsulates it before relaying to the mobile node.

The foreign agent will repeat these processes until the granted lifetime expires. The mobile node does not need to send a deregistration message when the lifetime expires, but it does have to reissue a registration request if it wants to continue the service after expiration

Security [3]

- Authentication is performed by all home agents, mobile nodes and foreign agents, and a default algorithm is known as keyed MD5. How good the random numbers used in authentication will determine the success or failure of the authentication.

  Note that some algorithms other than keyed MD5 may be supported and could be used.

- There might be a breech of security if the registration and Address Resolution Protocol (ARP) are not authentic.

- Key management is strongly desired in order to preclude many potential attacks based on the Mobile IP registration protocol. However, this would be hard to achieve due to the lack of a network key management protocol.

- Encryption or some other mechanisms can be used to better protect important data.

Problems with base Mobile IP protocol [4,5,6,15]

1. Dogleg routing
Consider that if a mobile node happens to move to the same subnetwork as its correspondent node that wants to send it datagrams, this is what will happen in order for the datagram to be received by the mobile node, based on the base Mobile IP protocol: the correspondent node will send the datagram all the way to the mobile node's home agent, which may be a half globe away; its home agent will then forward the datagram to its care-of-address, which might just take a half second to reach if the datagram is sent directly from the correspondent node. This kind of "indirect routing" is inefficient and undesirable.

*Fix:*The effort to define extensions to the operation of the base Mobile IP to allow for the optimization of datagram routing from a correspondent node to a mobile node has been made by the Mobile IP Working Group of the Internet Engineering Task Force (IETF). The key approach to route optimization is as follows:

- Binding cache containing the mobility binding of mobile node(s) is provided for the node that looks for optimizing its own communication with mobile nodes. In this way, the correspondent node has a way to keep track of where the mobile node(s) is. So when the time comes that the correspondent node wishes to send the datagram to its mobile node, it can send the datagram directly to the destination address, eliminating the "zig-zag" routing.

- The means for the mobile node's previous foreign agent to be notified of the mobile node's new location is provided. This mechanism allows datagrams in flight to the mobile node's previous foreign agent to be re-directed to its current address.

2. Too many unwanted duplicated fields in "IP within IP"
As discussed previously, the way to encapsulate the datagram is to put the original datagram (= IP header + payload) inside another IP envelope, of which the whole packet = outer IP header (Care-of Address) + original datagram. The fields in the outer IP header add too much overhead to the final datagram -- several fields are duplicated from the inner IP header. This waste of unnecessary space is uneconomical.

*Fix:*Also coming from the IETF, a so-called Minimal Encapsulation scheme is defined, and becomes another option to encapsulate the datagram. The approach to the encapsulation method is as follows:

- Instead of inserting a new header, the original header is modified to reflect the care-of address, and in between the modified IP header and unmodified IP payload, a minimal forwarding header is inserted to store the original source address and original destination address. When the foreign agent tries to decapsulate, it will simply restore the fields in the forwarding header to the IP header, and remove the forwarding header.

There is a restriction to the use of this encapsulation method. If the original datagram is already fragmented, then minimal encapsulation must not be used since there is no room left to store fragmentation information.

3. Single home agent model -- a fragile model
Although single home agent model is simple and easy to configure, it has the disadvantage of fragility. The mobile node becomes unreachable once the home agent breaks down.

*Fix:*One possible solution is to support multiple home agents. If one conventional home agent fails, there are still other home agents who can take over the duty and route for the datagram for the mobile node.

4. Unbearable frequent report to the home agent if the mobile node moves frequently
If a person is in a moving vehicle and roaming around into neighboring communities, the mobile IP will have to constantly report to the home agent to change its address. This degrades the performance and delays the datagram transmission.

*Fix:*One possible solution is to support foreign agent clustering. The idea is that by making a cluster of foreign agents, moves only from cluster to cluster have to be notified to the home agent. This approach eliminates the number of times a highly mobile node needs to report to its home agent.

The Evolution of Mobile IP [3,7,9,10,12,13,14]

The current Mobile IP Internet draft is the culmination of a series of mobile protocol proposals suggested by various researchers over the last few years. This section examines the key features of each of these proposals, some of which have found their way into the current draft. Mobile*IP and VIP came out around the same time. For Mobile*IP, its most known features are virtual mobile subnet, and packet encapsulation; for VIP, are MH locations in special routers, and tunneling using a new IP option. Then later on, IBM MIP was introduced. It uses loose source routing to deal with the mobile node trace issue existing in mobility problem. The last two proposals are MIP, and MHRP. MHRP adopts a new type of encapsulation different than an old IP option which is defined in VIP. Each of these protocols is briefly described in chronological order below:

-Mobile*IP

This protocol uses a virtual mobile subnet which is created by placing a small number of cooperating mobile subnet routers (MSRs) wherever mobile nodes may be connected to the network.

When a mobile node moves to a new location, it first detects its movement and register with an MSR, and then informs its previous MSR about its current location. The packet for the mobile node would be delivered by the MSR. If this MSR is not the local one to this mobile node, the datagram would be encapsulated (using IPIP method), and forwarded to the local MSR that will then decapsulate it and send it to the mobile node.

The above scheme is good for narrow range mobility. But when it comes to wide range mobility, it has limitations. To overcome this problem, a "popup" operation was defined for a wide area mode. The idea is as follows: when a mobile node moves, it registers with an MSR on its home network, and also acquires a temporary address. So when the MSR receives datagrams addressed for the mobile node, it would encapsulate datagrams and tunnel them directly to MH's temporary address.

-VIP

In this protocol, when a mobile node moves to a new location, it acquires a temporary address from its local address server. And then Propagating cache Method is used to distribute the mappings, between temporary address and the identifier information, through the network. The mapping is also sent to the mobile node's home gateway.

As a datagram is passed through the network to the mobile node, the intermediate gateways uses the source and destination mappings to update their caches. Various methods are defined, i.e, cache time-outs, and management procedures, to prevent stale information from being held for extended periods.

If an intermediate node gets a packet and knows the mobile node's current location, it would directly forward it to the mobile node; otherwise, it will send the packet to the mobile node's home gateway, which always knows the location of the mobile node, and it would forward the packet to the destination.

-IBM I

This protocol uses loose source routing (LSSR) to propagate the mapping between location information and identifier information through the network so an optimal route could be taken when the packet is sent. The basic operation of the protocol is as follows: when a mobile node moves to a new location, it would detect the change in position, register with a base station, which is similar to Mobile*IP's MSR, and inform its home mobile router (MR), which is similar to VIP's home gateway. When the mobile host migrates, it notifies its previous base station and the MR of its new location. When a correspondent node sends a datagram to the mobile node through the old base station, it will be forwarded to the MR for the correct routing. LSSR in the correspondent node will be eventually updated to make sure route optimization is performed.

-IBM II

The architecture suggested in IBM II is similar to IBM I. The main difference is that IBM II allows the use of encapsulation. The use of encapsulation implies that every packet sent from the correspondent node must be routed via the RDS/LD (=MR in IBM I). Therefore, unlike IBM I, routing optimization is not used.

-MIP

When a mobile node moves to a new location, it registers with an Internet Access Point (IAP), which acts as its local agent. And then it notifies its location directory (LD), which is responsible for making bindings for its mobile nodes available to a home redirector (HR) that serves the mobile node's home network. The packet can always be forwarded to the HR which always has a binding for the mobile node when the mobile node's current location is not known by any of LAPs or correspondent node that receive the data packet.

There is another entity in this protocol called Mobile Support Router (MSR) which is similar to an IAP except that it only keeps non-local binding. It is used mainly to optimize communications between mobile nodes.

-MHRP

This protocol uses ideas similar to loose source routing. However, it uses a new encapsulation method compatible with ICMP, but has a header of 8 or 12 bytes which helps to reduce bandwidth.

Conclusion

Mobile IP is a newly defined protocol which supports mobile users but also is compatible with the current IP. It is still in the process of being standardized, and there are still many items that need to be worked on and enhanced, such as the security issue and the routing issue. The IETF has been continuously working on the problems which had been found on the base Mobile IP protocol.

References

1. Raj Jain, Networking Issues for Mobile Computing, Recent Advances in Networking and Telecommunications Seminarsin Columbus, Ohio
   This seminar describes networking issues for mobile computing.

2. Charles Perkins, The Internet Mobile Host Protocol (IMHP),Internet Draft, 6 July 1995.
   This draft specifies protocol enhancements that allow transparent routing of IP datagrams to mobile nodes in the Internet.

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. Charles Perkins, Minimal Encapsulation within IP Internet Draft, 6 July 1995.
   This draft specifies a means by which an IP datagram may be encapsulated within an IP datagram.

6. Jon Postel, Internet Protocol, RFC 791,September 1981.
   This draft specifies the Internet Protocol.

7. W. Simpson, IPng Mobility Considerations, rfc1688, August 1994.
   This RFC describes the criteria related to mobility for consideration in design and selection of IPng.

8. Charles Perkins, Andrew Myles, David Johnson, *The Internet Mobile Host Protocol*, iNET'94, Prague, Czech Republic, 13-17 June 1994. Also accepted by Computer Networks and ISDN Systems.
   This paper describes the design and implementation of a mobile host protocol known as IMHP, which is compatible with the TCP/IP protocol suite.

9. Charles Perkins, Andrew Myles, *Mobile IP*, SBT/IEEE International Telecommunications Symposium , Rio De Janeiro, Brazil, 22-25 August 1994.
   This paper describes a mobile host protocol known as MIP, which allows for suboptimal transparent routing of datagrams between mobile nodes and other nodes.

10. Andrew Myles, David Skellern, *Comparing four IP based mobile host protocols*, Computer Networks and ISDN Systems , vol. 26, pp. 349-355, 1993. Also Proceedings of 4th Joint European Networking Conference, Trondheim, Norway, pp. 191-196, 10-13 May 1993.
    This paper compares four initial proposals for mobile host protocols.

11. David B. Johnson, *Mobile Host Internetworking Using IP Loose Source Routing*, CMU Technical Report CMU-CS-93-128, Feb. 1993.
    This paper describes a protocol for allowing mobile hosts to transparently interoperate in the Internet using IP.

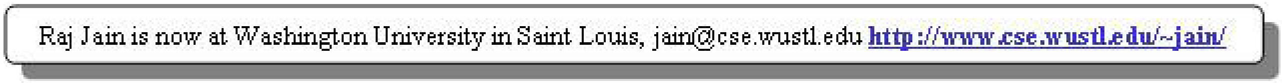
12. Fumio Terqoka, Keisuke Uehara, Hideki Sunahara, and Jun Murai, *VIP: A Protocol Providing Host Mobility*, Communications of the ACM, Aug. 1994, Vol. 37, No 8, pp. 67-75.
    This paper describes a mobile host protocol known as Virtual IP, which is based on caching a mobile host's locations in special routers and tunneling using an IP option.

13. John Ioannidis, *Protocols for Mobile Networking*, PhD dissertation, Columbia University, 1993.
    This dissertation describes one of the first mobile host protocols known as Mobile*IP, which is based on the idea of virtual mobile subnet and uses a datagram encapsulation called IPIP.

14. Christian Huitema, *ROUTING IN THE INTERNET*, Prentice Hall, 1995, 315 pp.
    This book presents and discusses various routing protocols and routing issues in the Internet, including Mobile IP

Other Reports on Recent Advances in Networking Back to Raj Jain's Home Page

Last modified: Aug. 23, 1995



Raj Jain is now at Washington University in Saint Louis, jain@cse.wustl.edu **http://www.cse.wustl.edu/~jain/**