

# **Mobile IP Resources**

Neda Document Number: 103-101-04

Last Updated: 1999/04/05 23:34:50

Doc. Revision: 1.1

**Payman Arabshahi  
Neda Communications, Inc.  
17005 SE 31st Place  
Bellevue, WA 98008**

**March 24, 2000**

# List of Tables



# Chapter 1

## IETF Mobile IP Working Group

<http://www.ietf.cnri.reston.va.us/html.charters/mobileip-charter.html>

### 1.1 About the IETF

<http://www.ietf.org>

The Internet Engineering Task Force (IETF) is the protocol engineering and development arm of the Internet. The IETF is a large open international community of network designers, operators, vendors, and researchers concerned with the evolution of the Internet architecture and the smooth operation of the Internet. It is open to any interested individual.

The actual technical work of the IETF is done in its working groups, which are organized by topic into several areas (e.g., routing, network management, security, etc.). Much of the work is handled via mailing lists, however, the IETF also holds meetings three times per year.

The internal management of the IETF is handled by the area directors. Together with the Chair of the IETF, they form the Internet Engineering Steering Group (IESG). The operational management of the Internet standards process is handled by the IESG under the auspices of the Internet Society. The Internet Architecture Board (IAB) is a body of the Internet Society responsible for overall architectural considerations in the Internet. It also serves to adjudicate disputes in the standards process.

## 1.2 Working Group on IP Routing for Wireless/Mobile Hosts (mobileip)

<http://www.ietf.cnri.reston.va.us/html.charters/mobileip-charter.html>

Basically, Mobile-IP extends the existing Internet Protocol to allow a portable computer to be moved from one network to another without changing its IP address and without losing existing connections. This is the working field of the IETF mobileip Working Group.

### 1.2.1 Chairs

- Jim Solomon, [solomon@comm.mot.com](mailto:solomon@comm.mot.com)
- Tony Li, [tli@jnx.com](mailto:tli@jnx.com)

### 1.2.2 Routing Area Director

- Joel Halpern, [jhalpern@newbridge.com](mailto:jhalpern@newbridge.com)

### 1.2.3 History

The Mobile IP Working Group of the Internet Engineering task Force (IETF) is the culmination of efforts by many individuals interested in the problem of mobile routing of hosts. The first meetings were in the form of BOF (Birds of a Feather) sessions held in Atlanta (July 1991), Santa Fe (November 1991), and San Diego (March 1992) IETF meetings. In June 1992 a proposed charter for a formal Working Group was submitted by Steve Deering (who had chaired the BOF sessions) to the IETF and at the same time a mailing list was set up for conduct of the group's business. Following a revision of the charter, the Working Group was officially formed in June 30, 1992. The group uses <ftp://software.watson.ibm.com/pub/mobile-ip> as its archive, where minutes of meetings, proposals, and a mail archive is kept.

### 1.2.4 Accomplishments

- Reviewed and approved the group charter.
- Posted and Internet-Draft documenting the Mobile Hosts protocol.
- Reviewed the charter of the Mobile IP Working Group for additional work required to facilitate non-host mobility.

## 1.2. WORKING GROUP ON IP ROUTING FOR WIRELESS/MOBILE HOSTS (MOBILEIP)5

### 1.2.5 Future Goals

- By July 1996: Submit the IPv4 Mobile Host Protocol to the IESG as a Proposed Standard.
- By December 1996: Submit the IPv6 Mobile Host Protocol to the IESG as a Proposed Standard.
- By March 1997: Review the WG charter and update as needed.

### 1.2.6 Charter

The IETF Mobile IP Working Group (mobileip WG) is chartered to develop or adopt architectures and protocols to support mobility within the Internet. In the near-term, protocols for supporting transparent host “roaming” among different subnetworks and different media (e.g., LANs, dial-up links, and wireless communication channels) shall be developed and entered into the Internet standards track. The work is expected to consist mainly of new and/or revised protocols at the (inter)network layer, but may also include proposed modifications to higher-layer protocols (e.g., transport or directory). However, it shall be a requirement that the proposed solutions allow mobile hosts to interoperate with existing Internet systems.

In the longer term, the group may address, to the extent not covered by the mobile host solutions, other types of internet mobility, such as mobile subnets (e.g., a local network within a vehicle), or mobile clusters of subnets (e.g., a collection of hosts, routers, and subnets within a large vehicle, like a ship or spacecraft, or a collection of wireless, mobile routers that provide a dynamically changing internet topology).

### 1.2.7 Mailing List Information

- General Discussion: [mobile-ip@smallworks.com](mailto:mobile-ip@smallworks.com)
- To Subscribe: [majordomo@smallworks.com](mailto:majordomo@smallworks.com)
  - In Body: `subscribe mobile-ip`
- Archive: <ftp://software.watson.ibm.com/pub/mobile-ip>
- Meeting minutes: <http://taurus.u-aizu.ac.jp/cgi-shl/BrowseDL.exe/1804X/InternetInfo-0395/ietf/mobileip/>



## Chapter 2

# Mobile IP RFCs

There are two types of Internet documents: Internet-Drafts and Request for Comments (RFCs). Internet-Drafts have absolutely no formal status and can be changed or deleted at any time. RFCs are the official document series of the IAB, and are archived permanently (i.e., they are never deleted, and once an RFC is published, it will never change); however, it is important to note that not all RFCs are standards.

### 2.1 Current Internet-Drafts

#### 2.1.1 Official IETF

- IP Mobility Support: <ftp://ftp.ietf.cnri.reston.va.us/internet-drafts/draft-ietf-mobileip-protocol-16.txt>

Editor: Charles Perkins, IBM

Date: 22 April 1996

Expires: 22 October 1996

This document specifies protocol enhancements that allow transparent routing of IP datagrams to mobile nodes in the Internet. Each mobile node is always identified by its home address, regardless of its current point of attachment to the Internet. While situated away from its home, a mobile node is also associated with a care-of address, which provides information about its current point of attachment to the Internet. The protocol provides for registering the care-of address with a home agent. The home agent sends datagrams destined for the mobile node through a tunnel to the care-of address. After

arriving at the end of the tunnel, each datagram is then delivered to the mobile node.

- IP Encapsulation within IP: <ftp://ftp.ietf.cnri.reston.va.us/internet-drafts/draft-ietf-mobileip-ip4inip4-02.txt>

Editor: Charles Perkins, IBM

Date: 10 May 1996

Expires: 10 November 1996

This document specifies a method by which an IP datagram may be encapsulated (carried as payload) within an IP datagram. Encapsulation is suggested as a means to alter the normal IP routing for datagrams, by delivering them to an intermediate destination which would not be otherwise selected by the (network part of the) IP destination field. This may be done for any of a variety of reasons, but is particularly useful for adherence to the mobile-IP specification.

- Minimal Encapsulation Within IP: <ftp://ftp.ietf.cnri.reston.va.us/internet-drafts/draft-ietf-mobileip-minenc-01.txt>

Editor: Charles Perkins, IBM

Date: 25 October 1995

Expires: 25 April 1996

This document specifies a method by which an IP datagram may be encapsulated (carried as payload) within an IP datagram, without incurring all the overhead of using a standard IP header. Encapsulation is suggested as a means to effect "re-addressing" datagrams (i.e., delivering them to an intermediate destination other than that specified in the IP destination field) for any of a variety of reasons, but particularly those useful for adherence to the mobile-IP specification.

### 2.1.2 Unofficial/Personal

- Route Optimization in Mobile IP: <ftp://ftp.ietf.cnri.reston.va.us/internet-drafts/draft-ietf-mobileip-optim-04.txt>

Authors: David B. Johnson, Carnegie Mellon University; and Charles Perkins, IBM

Date: 22 February 1996

Expires: 22 August 1996

This document defines extensions to the operation of the base Mobile IP protocol to allow for optimization of datagram routing from a correspondent node to a mobile node. Without Route Optimization, all datagrams destined to a mobile node are routed through that mobile node's home agent, which then tunnels each datagram to the mobile node's current location. The protocol extensions described here provide a means for correspondent nodes that implement them to cache the binding of a mobile node and to then tunnel their own datagrams for the mobile node directly to that location, bypassing the possibly lengthy route for each datagram to and from the mobile node's home agent. Extensions are also provided to allow datagrams in flight when a mobile node moves, and datagrams sent based on an out-of-date cached binding, to be forwarded directly to the mobile node's new binding.

- Applicability Statement for IP Mobility Support: <ftp://ftp.ietf.cnri.reston.va.us/internet-drafts/draft-ietf-mobileip-appl-02.txt>

Author: Jim Solomon, Motorola

Date: December 29 1995

Expires: June 29, 1996

As required by [RFC 1264], this draft report discusses the applicability of Mobile IP to provide host mobility in the Internet. The final form of this draft report is a prerequisite to advancing Mobile IP on the standards track. In particular, this document describes the key features of Mobile IP and shows how the requirements for advancement to Proposed Standard RFC have been satisfied.

- Mobility Support in IPv6: <ftp://ftp.ietf.cnri.reston.va.us/internet-drafts/draft-ietf-mobileip-ipv6-00.txt>

Author: Charles Perkins, IBM; and David B. Johnson, Carnegie Mellon University

Date: 26 January 1996

Expires: 26 July 1996

This document specifies mobility messages that allow transparent routing of IP datagrams to mobile nodes in the Internet. Each mobile

node is always identified by its home address, regardless of its current point of attachment to the Internet. While situated away from its home, a mobile node is also associated with a care-of address, which provides information about its current point of attachment to the Internet. The protocol provides for notifying the mobile node's home agent, and any other interested IPv6 addressable entities, about the care-of address of the mobile node. When necessary, the home agent sends packets destined for the mobile node through a tunnel to the care-of address. After arriving at the end of the tunnel, the packets are then delivered to the mobile node.

- The Definitions of Managed Objects for IP Mobility Support: <ftp://ftp.ietf.cnri.reston.va.us/in-drafts/draft-ietf-mobileip-mib-00.txt>

Authors: D. Cong and M. Hamlen, Motorola; and Charles Perkins, IBM

Date: April 1996

Expires: October 1996

This memo defines the Management Information Base (MIB) for use with network management protocols in TCP/IP-based internets. In particular, it describes managed objects used for managing the Mobile Node, Foreign Agent and Home Agent of the Mobile IP Protocol.

## 2.2 Request for Comments

- IP in IP Tunneling (RFC 1853): <ftp://ds.internic.net/rfc/rfc1853.txt>

Author: W. Simpson, Daydreamer

Date: October 1995

This document discusses implementation techniques for using IP Protocol/Payload number 4 Encapsulation for tunneling with IP Security and other protocols.

## Chapter 3

# Mobile IP Research and Technical papers

This Chapter contains abstracts of some recent papers in the area of Mobile IP.

### 3.1 Comparison of Mobile Host Protocols for IP

<ftp://ftp.mpce.mq.edu.au/pub/elec/dist/mobile/comparison/jire93/jire.a4.2col.ps.Z>

Authors: Andrew Myles and David Skellern

Date: December 1993

Host mobility is becoming an increasingly important feature with the recent arrival of notebook and palm top computers, the development of wireless network interfaces and the implementation of the global network. This paper describes and compares three proposals from Sony, IBM and Columbia University for mobile host protocols (MHP) that are compatible with the TCP/IP protocol suite. A set of basic requirements for a MHP are also suggested and it is observed that none of the three proposals entirely satisfies these requirements. Each proposal has faults in their implementation of mobile network layer functionality. Moreover, it is noted they do not address problems that must be solved in both higher and lower layers.

### **3.2 Comparing Four IP Based Mobile Host Protocols**

<ftp://ftp.mpce.mq.edu.au/pub/elec/dist/mobile/comparison/jenc93/jenc93.ps.Z>

Authors: Andrew Myles and David Skellern

Date: May 1993

Host mobility is becoming an increasingly important issue because of the arrival of notebook and palm top computers, the development of wireless network interfaces and the implementation of global networks. The paper compares four proposals for mobile host protocols (MHPs) that are compatible with the TCP/IP protocol suite. A set of requirements for an MHP is proposed and it is observed that while all proposals perform the basic task none of the proposals entirely satisfy the requirements.

### **3.3 Mobile IP**

<ftp://ftp.mpce.mq.edu.au/pub/elec/dist/mobile/mip/its92.ps.Z>

Authors: Andrew Myles and Charles Perkins

Date: August 1994

### **3.4 The Internet Mobile Host Protocol (IMHP)**

<ftp://ftp.mpce.mq.edu.au/pub/elec/dist/mobile/imhp/jenc94/inet94.ps>

Authors: Charles Perkins, Andrew Myles, and David Johnson

Date: June 1994

The paper describes the Internet Mobile Host Protocol (IMHP), which allows transparent routing of IP packets to mobile hosts in the Internet, while using only the mobile host's home IP address. No changes are required in stationary hosts that communicate with mobile hosts, and no changes are required in mobile hosts above the IP level. IMHP quickly converges to optimal routing following the movement of a mobile host, while maintaining the weak security model of today's Internet. Detailed examples of operation are presented.

### **3.5 IMHP: A Mobile Host Protocol for the Internet**

<http://www.cs.cmu.edu/afs/cs.cmu.edu/user/dbj/www/ftp/mobile/comnet94.ps>

Authors: Charles Perkins, Andrew Myles, and David Johnson

Date: December 1994

Remarks: Revised Version of INET'94 Paper (previous reference)

This paper describes a protocol that allows transparent routing of IP packets to mobile hosts in the Internet, while using only the mobile host's home IP address. The protocol, called IMHP (Internet Mobile Host Protocol), requires no changes in stationary hosts that communicate with mobile hosts, and requires no changes in mobile hosts above the IP level. IMHP quickly converges to optimal routing following the movement of a mobile host, while preserving the current level of security in the Internet. Detailed examples of operation are presented.

### **3.6 Scalable Support for Transparent Mobile Host Internetworking**

<http://www.cs.cmu.edu/afs/cs.cmu.edu/user/dbj/www/ftp/mobile/kluwer-ietf.ps>

Author: David Johnson

Date: October 1995

Considers the problem of providing transparent support for very large numbers of mobile hosts within a large internetwork such as the Internet. The availability of powerful mobile computing devices and wireless networking products and services is increasing dramatically, but internetworking protocols such as IP used in the Internet do not currently support host movement. To address this need, the Internet Engineering Task Force (IETF) is developing protocols for mobile hosts in the Internet. The paper analyzes the problem to be solved, reviews the current state of that effort, and discusses its scalability to very large numbers of mobile hosts in a large internetwork.

### **3.7 Scalable and Robust Internetwork Routing for Mobile Hosts**

<http://www.cs.cmu.edu/afs/cs.cmu.edu/user/dbj/www/ftp/mobile/icdcs94.ps>

Author: David Johnson  
Date: June 1994

This paper describes a new protocol for transparently routing packets to mobile hosts operating in a large internetwork. The protocol, called the Mobile Host Routing Protocol (MHRP), allows any host to become mobile at any time, yet there is no penalty for a host being "mobile capable", since the protocol automatically uses only the standard internetwork routing mechanisms and adds no overhead when a mobile host is currently connected to its home network. The paper concentrates on the design of MHRP as it applies to the Internet using IP. Mobile hosts use only their "home" IP addresses, regardless of their current location in the Internet. No changes are required in stationary hosts that communicate with mobile hosts, and no changes are required in mobile hosts above the IP level. MHRP introduces several new features to provide better robustness for routing to mobile hosts, and provides better scalability to very large numbers of mobile hosts than previous mobile host protocols.

### **3.8 Ubiquitous Mobile Host Internetworking**

<http://www.cs.cmu.edu/afs/cs.cmu.edu/user/dbj/www/ftp/mobile/wwos93.ps>

Author: David Johnson  
Date: October 1993

Argues that being a mobile host (or a mobile capable host) should be a standard property of all hosts in the Internet, and summarizes the design of a new protocol for transparently allowing these mobile hosts to interoperate in the Internet using IP. A mobile host may move from one network to another at any time, while always using only its "home" IP address. Any host may be configured to be a "mobile host" simply by running the appropriate software on it, and there is no penalty for this configuration, since the protocol automatically uses only the standard IP routing mechanisms, adding no overhead to IP, when a mobile host is currently connected to its home network. The protocol scales well to very large numbers of mobile hosts and adds little overhead for packets sent to a mobile host currently connected to a foreign network. The protocol is currently being implemented within the Berkeley networking code and is expected to be available shortly to interested groups outside Carnegie Mellon.

### **3.9 Dynamic Source Routing in Ad Hoc Wireless Networks**

<http://www.cs.cmu.edu/afs/cs.cmu.edu/user/dbj/www/ftp/mobile/kluwer-adhoc.ps>

Authors: David B. Johnson and David A. Maltz

Date: 1996

An ad hoc network is a collection of wireless mobile hosts forming a temporary network without the aid of any centralized administration or standard support services. In such an environment, it may be necessary for one mobile host to enlist the aid of others in forwarding a packet to its destination due to the limited propagation range of each mobile host's wireless transmissions. Some previous attempts have been made to use conventional routing protocols for routing in ad hoc networks, treating each mobile host as a router. This position paper points out a number of problems with this design and suggests a new approach based on separate route discovery and route maintenance protocols.

### **3.10 Mobile Host Internetworking Using IP Loose Source Routing**

<http://www.cs.cmu.edu/afs/cs.cmu.edu/user/dbj/www/ftp/mobile/CMU-CS-93-128.ps>

Author: David Johnson

Date: February 1993

### **3.11 A Mobile Host Protocol Supporting Route Optimization and Authentication**

<http://www.cs.cmu.edu/afs/cs.cmu.edu/user/dbj/www/ftp/mobile/jsac.ps>

Authors: Andrew Myles, David Johnson, and Charles Perkins

Date: June 1995

Host mobility is becoming an important issue due to the recent proliferation of notebook and palmtop computers, the development of wireless network interfaces, and the growth in global internetworking. This paper describes the design and implementation of a mobile host protocol,

called the Internet mobile host protocol (IMHP), that is compatible with the TCP/IP protocol suite, and allows a mobile host to move around the Internet without changing its identity. In particular, IMHP provides host mobility over both the local and wide area, while remaining transparent to the user and to other hosts communicating with the mobile host. IMHP features route optimization and integrated authentication of all management packets. Route optimization allows a node to cache the location of a mobile host and to send future packets directly to that mobile host. By authenticating all management packets, IMHP guards against possible attacks on packet routing to mobile hosts, including the interception or redirection of arbitrary packets within the network. A simple new authentication mechanism is introduced that preserves the level of security found in the Internet today, while accommodating the transition to stronger authentication based on public key cryptography or shared keys that may either be manually administered or provided by a future Internet key management protocol.

### **3.12 A Survey Paper on Mobile IP**

<http://ncrl17.seu.edu.cn/gzy/html/mobileip.html>

Author: Henry Y. Gong

Date: January 1996

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.

### **3.13 Protocols and Caching Strategies in Support of Internetwork Mobility**

<ftp://ftp.cs.wisc.edu/tech-reports/reports/94/tr1249.ps.Z>

Author: Mitchell P. Tasman

Date: 1994

We describe a new type of network layer address, the hybrid address, which contains a Partial Destination Identifier, a Unique ID, and a Location Sequence number. The Partial Destination Identifier, which changes as a mobile ES relocates between areas of an internetwork, allows for efficient

routing, while the Unique ID is used for ES identification at the lowest layers of a routing hierarchy. Finally, the Location Sequence Number, which a mobile ES increments as it relocates between areas, is used to compare the age of multiple addresses for a given mobile ES.

We present a mobility design that incorporates the hybrid address, and is based on the ISO OSI connectionless routing architecture and protocols. Each mobile ES has a home address and a current address. The home address is stored in a global database, and the ES's home area keeps track of the current address. After a mobile ES relocates to a new area, it sends Reconnect messages to the home and previous areas, each of which caches a forwarding pointer for the mobile ES. ESs that communicate with a mobile ES send datagrams directly to the mobile ES. To accomplish this, each ES maintains cache entries for its mobile correspondents. When a datagram containing an out-of-date address is forwarded by an area, a Rewrite message is sent to the source ES, which updates its cache entry for the destination. An ES also updates its cache based on the source addresses of incoming datagrams.

The mobility algorithm has been implemented and tested in a simulation environment, and performs quite well. We also present the results of a study on strategies for caching mobile ES forwarding pointers at Intermediate Systems in the interior of an internetwork, based on the type and contents of transit control messages. Caching at interior Intermediate Systems based on Reconnect messages yields the greatest benefit, for both tree-shaped and general topology internetworks, while caching based on transit Rewrite messages is not recommended.

### **3.14 Secure Short-cut Routing for Mobile IP**

<ftp://virtual.harvard.edu/pub/cs96/usenix94.ps.gz>

Authors: T. Blackwell, Chan Kee, Chang Koling, T. Charuhas, J. Gwertzman, B. Karp, H.T. Kung, W.D. Li, Lin Dong, R. Morris.

Date: June 1994

Describes the architecture and implementation of a mobile IP (Internet Protocol) system. It allows mobile hosts to roam between cells implemented with 2-Mbps radio base stations, while maintaining Internet connectivity. The system is being developed as part of a course on wireless networks at Harvard and has been operational since March 1994.

The architecture scales well, both geographically and in the number of mobile hosts supported. It supports secure short-cut routing to mobile hosts using the existing Internet routing system without change. The

implementation demonstrates a robust, low-complexity realization of the architecture, and provides trade-off opportunities between efficiency and cost.

Measured performance of the mobile system is generally excellent. The system can handle a high rate of location updates, and routes packets almost as efficiently for mobile hosts as the Internet does for stationary hosts. We observe reasonable TCP (Transmission Control Protocol) behavior during hand-offs.

### **3.15 MINT- A Mobile Internet Router**

<ftp://ftp.it.kth.se/Reports/Telecommunication-Systems/1993/930518.VTC.MINT.ps>

Authors: R. Hager, A. Klemets, G.Q. Maguire, M.T. Smith, and F. Reichert

Date: May 1993

The mobility of portable computers and workstations is not transparent to users. They adjust to reduced services as long as they have no connection to a supporting infrastructure. The goal of the Walkstation project is to realize a user transparent mobile IP router (MINT) for wireless links (infrared and radio) operating at 1-10 Mbit/sec. For the study of user behavior and system characteristics, a campuswide testbed (ERIC) with 50-100 stations is planned to demonstrate the new solutions found in the Walkstation II project.

### **3.16 MINT- A Mobile Internet Router**

<ftp://ftp.it.kth.se/Reports/Telecommunication-Systems/1993/931213.IEEE.GDN.ps>

Authors: A. Klemets, G.Q. Maguire, F. Reichert, and M.T. Smith

Date: December 1993

Today, mobility of portable computers and workstations is not transparent to users. They adjust to reduced services as long as they have no connection to a supporting infrastructure. The goal of the Walkstation project is to realize a user transparent mobile IP router (MINT) for wireless links (infrared and radio) operating at 1-10 Mbit/sec. For the study of user behavior and system characteristics a campus wide testbed (ERIC) with 50-100 stations is planned to demonstrate the new solutions found in the Walkstation II project.

### **3.17 I-TCP: Indirect TCP for Mobile Hosts**

<ftp://paul.rutgers.edu/pub/badri/itcp-tr314.ps.Z>

Authors: A. Bakre, and B.R. Badrinath

Date: June 1995

IP based solutions to accommodate mobile hosts within existing inter-networks do not address the distinctive features of wireless mobile computing. IP-based transport protocols thus suffer from poor performance when a mobile host communicates with a host on the fixed network. This is caused by frequent disruptions in network layer connectivity due to i) mobility and ii) unreliable nature of the wireless link. We describe I-TCP, which is an indirect transport layer protocol for mobile hosts. I-TCP utilizes the resources of Mobility Support Routers (MSRs) to provide transport layer communication between mobile hosts and hosts on the fixed network. With I-TCP, the problems related to mobility and unreliability of wireless link are handled entirely within the wireless link; the TCP/IP software on the fixed hosts is not modified. Using I-TCP on our testbed, the throughput between a fixed host and a mobile host improved substantially in comparison to regular TCP.

### **3.18 Mobile-IP: Supporting Transparent Host Migration on the Internet**

<http://anchor.cs.binghamton.edu/~mobileip/LJ/index.html>

Authors: Ben Lancki, Abhijit Dixit, and Vipul Gupta

Date: May 1996

A short article which motivates the need for Mobile-IP and describes its basic operation.

### **3.19 A set of Transparencies Describing Mobile-IP and Linux Mobile-IP**

<http://anchor.cs.binghamton.edu/~mobileip/mip-talk.ps>

Authors: Vipul Gupta, Abhijit Dixit, and Ben Lancki, SUNY Binghamton

Date: May 1996

Among other topics, these transparencies include a description of the ARP and nonce-related problems (w/ solutions) in Draft-15 of the IETF Mobile-IP proposal (pages 33-34). These problems have been fixed in Draft-16. Also included are route manipulations (pp. 18-19) on Linux machines required to support mobility without foreign agents.

### **3.20 Improving Reliable Transport and Handoff Performance in Cellular Wireless Networks**

<http://http.cs.berkeley.edu/~hari/papers/winet.ps>

Authors: H. Balakrishnan, S. Seshan, and R.H. Katz

Date: 1995

TCP is a reliable transport protocol tuned to perform well in traditional networks where congestion is the primary cause of packet loss. However, networks with wireless links and mobile hosts incur significant losses due to bit-errors and handoffs. This environment violates many of the assumptions made by TCP, causing degraded end-to-end performance. The authors describe the additions and modifications to the standard Internet protocol stack (TCP/IP) to improve end-to-end reliable transport performance in mobile environments. The protocol changes are made to network-layer software at the base station and mobile host, and preserve the end-to-end semantics of TCP. One part of the modifications, called the snoop module, caches packets at the base station and performs local retransmissions across the wireless link to alleviate the problems caused by high bit-error rates. The second part is a routing protocol that enables low-latency handoff to occur with negligible data loss. The authors have implemented this new protocol stack on a wireless testbed. The experiments show that this system is significantly more robust at dealing with unreliable wireless links than normal TCP; the authors have achieved throughput speedups of up to 20 times over regular TCP and handoff latencies over 10 times shorter than other mobile routing protocols.

### **3.21 Analysis of Security and Privacy in Mobile IP**

<http://www-i4.informatik.rwth-aachen.de/~andreas/PAPERS/SecurityPerformance.ps.gz>

Authors: A. Fasbender, D. Kesdogan, and O. Kubitz

Date: March 1996

### 3.22. VARIABLE AND SCALABLE SECURITY: PROTECTION OF LOCATION INFORMATION IN MOBILE IP21

In this paper we present a possible extension of the proposed Mobile IP and route optimization protocols, the Non-Disclosure Method (NDM). It prevents the tracking of user movements by third parties and gives mobile users control over the revelation of their location information, according to their personal security demands.

We give an overview on Mobile IP protocols and briefly discuss these protocols in terms of security issues. We show that confidential location management in Mobile IP is an unsolved problem. Then we propose our method for providing untraceable communications in packet-oriented mobile networks. NDM is based on the idea of mixes, which has been suggested by Chaum for hiding the originator addresses of electronic mails. Our algorithm prevents the linkability of sender and recipient addresses in Mobile IP, can be easily adopted to other mobility supporting networks as well. We conclude our paper with performance aspects, discussing the trade-off between the level of security provided and the costs of NDM in terms of increased packet transmission delays. For this purpose, we present a new modelling approach for Internet connections, which is based on empirically derived packet delay distributions and their analytical description. Our results show that the overhead for confidential location management is not as critical as might be expected, and that a considerable delay reduction compared to mixes can be achieved.

## **3.22 Variable and Scalable Security: Protection of Location Information in Mobile IP**

<http://www-i4.informatik.rwth-aachen.de/~andreas/PAPERS/SecurityArchitecture.ps.gz>

Authors: A. Fasbender, D. Kesdogan, and O. Kubitz

Date: March 1996

The amount of mobile and nomadic computing is expected to increase dramatically in the near future. Hand in hand with this ubiquitous mobile computing security and privacy problems show up, which have not been dealt with sufficiently up to now. The main problems are traffic analysis and the easy access to location information, for example in the popular Internet just by looking at the address headers of messages. In this paper the need for security and privacy supporting networks is discussed.

We present the Non-Disclosure Method (NDM) as a way to provide the user with variable and scalable security and privacy. We exemplarily demonstrate the applicability of NDM in an existing network by presenting an upward compatible protocol extension to the Internet Protocol (IP), the

Secure IP in IP Protocol. Its main design goal is the untraceability of network connections in mobile environments.

### **3.23 VIP: Virtual Internet Protocol**

<http://www.csl.sony.co.jp/project/VIP/index.html>

## Chapter 4

# Mobile IP Implementations

### 4.1 Royal Institute of Technology, Stockholm, Sweden (1)

<ftp://it.kth.se/pub/klemets/>

Author: Anders Klemets, [klemets@it.kth.se](mailto:klemets@it.kth.se)

Date: July 1995

- Based on version 11 of IP Mobility Support: draft-ietf-mobileip-protocol-11.txt.
- The minimal encapsulation protocol.
- MD5 authentication.
- Support for using authentication algorithms other than MD5.
- Mobile-Foreign and Foreign-Home authentication.
- Nonce based ID's.

There is provision for signalling between the link layer and the Mobile-IP code. This is useful if running Mobile-IP over a connection-oriented link layer protocol.

Porting friendly implementation. I have tried hard to make the Mobile-IP implementation as portable as possible. The parts of the user level code that interface to the operating system have been separated into separate files. Memory allocation, timers, network interfaces and network I/O have been abstracted. Separate files are used to implement a system independent interface to these operating system functions.

## 4.2 Royal Institute of Technology, Stockholm, Sweden (2)

<http://www.it.kth.se/d91-fta/exjobb/exjobb.html>

Authors: Fredrik Tarberg and Fredrik Broman

Date: January 1996

- Based on the implementation by Anders Klemets (see above) and draft version 14 of IP Mobility Support: draft-ietf-mobileip-protocol-14.txt (21 December 1995) and IP Encapsulation within IP Draft version 1: draft-ietf-mobileip-ip4inip4-01.txt
- Develops and implements a Management Information Base for the Mobile IP Protocol.
- Ports a Mobile IP Implementation for SunOS to MachOS and Solaris
- Tests the throughput and latency of the protocol

## 4.3 Digital Equipment Coporation

<http://www.digital.com/info/Customer-Update/940208042.txt.html>

Date: February 8 1994

RoamAbout Mobile IP mobile client/server networking software from Digital Equipment Corporation enables mobile users with portable computers to connect to their company's network wherever they are working. These portable computers keep their permanent IP network address independently of their physical location, so mobile users have the same environment and level of service both in the workplace and away from it.

When applications are permanently bound to an IP address, mobile workers can access them from their portable computers no matter where they are connected to the network – within the building or campus or at company sites reachable via a corporate network infrastructure. Moreover, they can have access to the same network services without reconfiguring their hosts. For sites with many in-building wireless networks on different subnets, RoamAbout Mobile IP lets users roam across subnets without losing ongoing network connections.

- Client/server networking software for portable computers (laptops and notebooks), allowing mobile users access to all network services in their home office regardless of physical location on the network

- Supports Internet Protocol (IP); client support for Dynamic Host Configuration Protocol (DHCP) servers

#### 4.4 FTP Software and Telxon Corporation

<http://www.telxon.com/tch1.htm>

Date: September 25 1995

Telxon Corporation today announced it has joined forces with FTP Software, Inc. and Aironet Wireless Communications Inc. to deliver the first integrated mobile Internet Protocol (IP) solution that allows mobile workers to take notebook, portable or pen-based computers anywhere they go in a corporate facility and maintain continuous wireless connections to an enterprise computing network. The initiative extends wired, in-building network environments by supporting a virtual office where mobile computer users can stay in touch with associates and manage business as if they were at their desks.

The new mobile IP solution combines FTP Software's DOS and Windows network software, Aironet's wireless LAN access points and Telxon's portable and pen-based computers to enable the TCP/IP networking protocol to better meet the full needs of mobile users. It allows users to roam across multiple segments of TCP/IP enterprise networks, without disrupting wireless network connections, and access applications and information, send and receive electronic mail, and update and query databases.

#### 4.5 Carnegie Mellon University

[http://www.ini.cmu.edu/WIRELESS/W\\_Research\\_2.html](http://www.ini.cmu.edu/WIRELESS/W_Research_2.html)

Slide Presentation is available at <http://www.ini.cmu.edu/~æ26/mip/>

Authors: John F. Drum and Adam S. Epstein

Date: December 14, 1995

- Apparently based on draft version 12 of IP Mobility Support: draft-ietf-mobileip-protocol-12.txt
- Linux Implementation

#### 4.6 National University of Singapore

<http://zaphod.ee.nus.sg/mip/mip-doc.html>

Authors: Y.Z. Li, K.C. Chua, and Y.C. Tay, National University of Singapore  
Date: December 1995

- Based on draft version 13 of IP Mobility Support: draft-ietf-mobileip-protocol-16.txt

This document describes an implementation of mobile IP within the Linux kernel. The implementation conforms to mobile IP Internet Draft 13, but leaves some modules to be implemented in the future. The system supplies an interface to user programs through the existing TCP/IP socket. Some problems are also stated. The source code with the implementation is free software and can be redistributed and modified under the terms of GNU General Public License.

## 4.7 SUNY Binghamton

<http://anchor.cs.binghamton.edu/~mobileip/>

Authors: Vipul Gupta, Abhijit Dixit, and Ben Lancki, SUNY Binghamton  
Date: May 1996

- Based on draft version 16 of IP Mobility Support: draft-ietf-mobileip-protocol-16.txt

Linux Mobile-IP is an implementation of Mobile-IP for the Linux operating system. Among other features, this release supports operation of a mobile host on a foreign network even in the absence of foreign agents, e.g. we are able to remove a portable computer from an ethernet LAN in our Lab, drive home (several miles away) and reattach to the Internet using PPP without disturbing any existing TCP connections. To the best of the authors' knowledge, it is the first IETF compliant Mobile-IP implementation for Linux with such support.

## Chapter 5

# Comparison of Mobile IP and CDPD

The Cellular Digital Packet Data (CDPD) Network is a peer multi-protocol, connectionless network, proposed by the CDPD Forum, a trade association of carriers, equipment suppliers, and application developers. It is based on early IETF Mobile-IP work so the two proposals have many similarities but also some differences. The idea behind CDPD is that it may share unused channels in existing Advanced Mobile Phone Systems (AMPS) to provide a 19.2 kbps data channel. The CDPD describes in detail the three lower network layers.

The terminologies of CDPD and Mobile-IP are different. CDPD is following the OSI model terminology. The mobile node is called a mobile end-system (M-ES), the home and foreign agents are called mobile home and mobile serving functions (MHF and MSF respectively) and reside in a mobile data intermediate system (MD-IS). A mobile data base station (MDBS) is also defined which deals with the airlink communications and acts as a data link layer relay between the M-ES and the serving MD-IS. Two protocols, the Mobile Node Registration Protocol (MNRP) and the Mobile Node Location Protocol (MNLP) are responsible for registration of the M-ES with its home MD-IS and the proper routing of packets destined for the M-ES.

How do Mobile IP and CDPD compare? We can compare these mobile data systems from a variety of perspectives including:

- Objectives, goals and design assumptions
- Technical architecture and design

- Model and terminology
- Operational assumptions
- Standardization process
- Potential

The final topic in our comparison is a prediction and a discussion of issues surrounding co-existence and convergence between these standards.

Obviously, the goal is to objectively compare Mobile IP and CDPD. In particular,

- For the most part we limit ourselves to a comparative analysis of the CDPD specifications and current Mobile IP specifications. In other words we do not compare existing or future implementations of mobile devices or networks.
- We limit the comparative analysis to the mobility dimension of CDPD. This limitation is necessary for a meaningful comparison. In addition to mobility support, the CDPD specifications cover the airlink protocols, network management, network administration, accounting and conformance testing. Thus, we limit ourselves to Part 500 (Mobility Management), Part 501 (Mobile Network Location Protocol), Part 507 (Mobile Network Registration Protocol) and Part 406 (Airlink Security) in our analysis of CDPD.

## 5.1 Objectives, Goals and Assumptions

Both CDPD and Mobile IP require mobile hosts to be able to communicate with other systems that do not implement mobility functions. No changes or enhancements are required for systems that do not support mobility, to be able to communicate with mobile hosts.

### 5.1.1 Underlying Data Link Layer

Mobile IP makes no assumption about any particular link layer technology. One of the driving requirements for design of Mobile IP was that it should be completely independent of the data link.

In the case of CDPD, there were no external requirements for support of data links other than the CDPD airlink (an overlay on AMPS). From the onset the CDPD architects recognized that mobility for CDPD could be independent of CDPD's airlink. To this end, CDPD was designed under

a self-imposed requirement for CDPD mobility to be independent of the airlink.

### 5.1.2 Link Layer Efficiency

CDPD treats the airlink as a precious resource and minimizes the number of bytes transferred over the air. Trade-offs made between layering integrity (Layer 3 vs. Layer 2) and airlink efficiency in CDPD favor airlink efficiency.

Mobile IP is contained strictly within Layer 3. Mobile IP recognizes that the link by which a mobile node is attached to the Internet may often be a precious wireless link, which should be optimized where possible by the Layer 3 protocol (in this case Mobile IP).

### 5.1.3 Network Layer Support

CDPD was designed to not only support IP, but also to be a multi-protocol mobility solution. Mobile IP is a pure IP solution. Both CDPD and Mobile IP require that mobility be supported without the mobile system needing to change its IP address. This is a departure from existing IP networks.

### 5.1.4 Network Administration and Management

CDPD assumes that the network is centrally administered, managed and operated by cooperating cellular Service Providers. Mobile IP assumes no additional constraints beyond the existing mode of operation of the Internet. This is probably the most fundamental difference between CDPD and Mobile IP and has serious ramifications on address assignment and security.

## 5.2 Technical Architecture and Design

CDPD is based on early Mobile IP work, and thus resembles but does not exactly match Mobile IP. In particular, the triangular routing mobility approach is essentially the same in both CDPD and Mobile IP.

The following enumerates major areas of design differences between the two approaches:

- The user's IP address must be assigned by the CDPD service provider. Mobile IP makes no such assumptions.

- Mobile IP allows for co-location of mobile node and the foreign agent. Combining the M-ES and the Serving MD-IS was not considered and is not practical in CDPD.
- CDPD's mobility tunnel is based on CLNP. Mobile IP's mobility tunnel is IP-based.
- Mobile IP is a pure IP design. CDPD is a multiprotocol design.
- Mobile IP operates completely above the data link layer. CDPD mobility is mostly above the data link layer.
- Since the infrastructure of the CDPD network is closed there are less security considerations for CDPD.

### 5.3 Model and Terminology

The terminologies of CDPD and Mobile IP are different. CDPD is following the OSI reference model terminology. Mobile IP adheres to conventional IP terminology with some extensions. Table 1 maps the key concepts of Mobile IP to their corresponding terms in CDPD.

### 5.4 Operational Assumptions

Mobile IP uses the Internet as an operational model. Operational assumptions for Mobile IP are the same as those for the Internet, which can best be described as "managed chaos".

On the other hand CDPD assumes a clearly defined network with well defined boundaries of authority and responsibility. The CDPD internetwork is a collection of CDPD service provider networks. Based on bilateral agreements, each Home MD-IS interoperates with various serving MD-ISs, which may be administered by various CDPD service providers.

The infrastructure of the CDPD network is a closed network. This implies that some level of trust, order and accountability can be expected. "Control and Order" expresses the general flavor of CDPD's operational assumptions.

These operational assumptions had a direct impact on many of CDPD's protocol design decisions, particularly in the areas of security, manageability and scalability.

Because the mobility tunnel begins and ends within the CDPD networks, to some extent it does not require the level of security that is necessary between the home agent and the foreign agent in Mobile IP.

Even though, securing the network layer of the CDPD network is not required in the CDPD specifications, the CDPD specification team recognized that providing data confidentiality and authentication for the mobility tunnel was important. Network Layer Security Protocol (NLSP), which can be considered an adjunct to CLNP, provides comprehensive security services. Unfortunately, it is a lot more theoretical than real.

## 5.5 Standardization Process

Mobile IP specifications are the product of one of IETF's Working Groups. The standardization process is completely open and based on volunteers' effort. This process is also complex and dynamic. "Rough Consensus and Running Code" best expresses the general flavor of Mobile IP's standardization process.

Sometimes, IETF Working Groups are highly efficient and produce high quality specifications in short time frames. That has not been the case with the Mobile IP Working Group.

The CDPD specification effort was funded by a group of cellular service providers. The specification was developed by a small team of paid consultants under the direction of cellular service provider representatives. There was significant schedule pressure in the CDPD specification development process. The CDPD Release 1.0 specification was developed in less than a year, and the following Release 1.1 was developed in about one year.

## 5.6 Potential

The value of coupling mobility with Internet access is significant. Any solution that provides mobile connectivity to the Internet is likely to be in high demand and heavily used. From this perspective, the opportunity for widespread deployment of both CDPD and Mobile IP technologies is immense.

However, in some ways these technologies are in competition with one other. Unless CDPD services are widely deployed soon and unless the subnetwork-independent characteristic of CDPD mobility is further developed and adopted by users of other than cellular-based media, it is unlikely that CDPD mobility will become the mainstream solution to Internet mobility.

The Mobile IP standardization process has been quite slow and the base specification for Mobile IP has not yet reached RFC status as of this

writing. However, Mobile IP enjoys certain characteristics which seem to ensure its survival until it becomes widely adopted. These characteristics include complete openness, subnetwork independence, user orientation, and proven correct specifications.

Another key factor in the widespread deployment of any network is the fitness of the network operators and equipment manufacturers for the job at hand. CDPD network operators are cellular service providers and CDPD equipment manufacturers are typically tele-communication equipment suppliers. Mobile IP network operators are likely to be Internet Service Providers and Mobile IP equipment manufacturers are typically data-communication equipment suppliers. We note that the entire Internet phenomenon was essentially independent of the public telecommunications providers.

It is important to recognize that even though CDPD mobility has the potential to become a generalized mobility solution and compete with Mobile IP, it was not designed as such. Since CDPD's mobility management scheme is similar to that of Mobile IP, either could be adapted to interoperate with the other. Depending on the degree of integration desired, this could be a relatively easy or a significant job.

Finally, CDPD devices are native IP hosts which can communicate with Mobile IP hosts without any modifications. The whole point of the Internet is that the local subnetwork connection is largely irrelevant to communications with the rest of the IP-based world. This is the foundation and the benefit of layered communications protocols. It is the communication itself and not the protocol used that is important.

## 5.7 Other views on comparison of CDPD and Mobile-IP

<http://www.raleigh.ibm.com/tr2/tr292003.ps>

The popularity of wireless communications has underscored the need for a standardized set of Network layer protocols that allow mobile computers to access the Internet from various points of attachment without the need for user intervention or system reconfiguration: that is, support for mobility must be provided. This paper discusses two protocols being developed to address this need:

The CDPD Forum, a trade association of carrier, equipment suppliers, and application developers, has specified a set of mobility-enabling protocols for use in the Cellular Digital Packet Data networks that are now being deployed nationwide by cellular carriers. The CDPD Forum recently pub-

## 5.7. OTHER VIEWS ON COMPARISON OF CDPD AND MOBILE-IP 33

lished their revised specification: CDPD Specification, Version 1.1; January 1, 1995.

The Mobile-IP Working Group of the Internet Engineering Task Force has also developed a set of mobility-enabling protocols. Currently, this work is at the level of an Internet Draft, with plans to have it accepted as an RFC by year end 1995. The most recent version of this specification is: IP Mobility Support; Internet Draft; January 4, 1995, C. Perkins (editor).

Mobility support is provided by new protocols that complement the existing IP protocol and its associated intra- and inter-domain routing protocols. This paper describes the constituent functions of each approach, outlining their strengths and weaknesses. It discusses basic methods, network management support, and conformance issues. It briefly touches on additional mobility support functions offered by the respective protocols. Finally, it discusses unification between the CDPD and Mobile-IP approaches.

Triangular routing is the basic approach used in both CDPD and Mobile-IP. Since this has been the subject of much discussion and debate, Appendix A presents the author's views on the topic.



## Chapter 6

# Future Directions in Mobility

The most ubiquitous internetwork is called the Internet. Routing in the Internet is based on the Internet Protocol (IP). In the late 1970s and early 1980s when the IP was developed, mobility of hosts was never considered. At that time most hosts were simply physically too large to move around.

The explosive growth of the Internet combined with the widespread availability of highly mobile small hosts in the form of laptop and palmtop computers, and personal digital assistants, has created a big demand for the concept of Mobile IP. The current trends point clearly towards further miniaturization and greater mobility. It is not unreasonable to expect many of tomorrow's hosts to be in the form of pagers, cell phones or even wrist watches. Transparent mobility is a major requirement for the next generation IP (IPv6).

For the Internet to support global transparent mobility, a new set of mobility management protocols that accommodate roaming among different subnetworks and different media types is required. None of the technologies discussed thus far completely addresses this requirement.

However, significant efforts are presently underway to develop a comprehensive solution for transparent mobility in the Internet. Here we discuss two such efforts. First, we survey the so called "Mobile IP" effort which enhances the current Internet Protocol (IPv4) to support mobility. Next, we discuss the next generation of Internet Protocol (IPv6), which is being designed to address the mobility requirement. We then compare and contrast CDPD mobility with Mobile IP. Table 1 provides a comparative glossary of CDPD and Mobile IP, which those familiar with CDPD may

choose to review first.

## 6.1 Mobility under IPv4

The Mobile IP Working Group of the Internet Engineering Task Force (IETF) is addressing the requirement of mobility in today's Internet. Mobile IP enables a mobile node to send and receive packets over the Internet using its home address regardless of its point of attachment. In essence, Mobile IP extends the existing Internet Protocol to allow a portable computer to be moved from one network to another without changing its IP address and without losing existing connections.

In this section we will discuss:

- The Mobile IP Standards Process
- A summary of the current Mobile IP specifications

The current base specification for Mobile IP is an "Internet Draft". Internet Drafts are draft documents that may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet Drafts as reference material or to cite them other than as "work in progress."

### 6.1.1 The Mobile IP Standards Process

#### Mobile IP and the IETF

The Mobile IP Working Group of the Internet Engineering Task Force (IETF) is the culmination of efforts by many individuals interested in the problem of mobile routing of hosts. The first meetings were in the form of BOF (Birds of a Feather) sessions held at the Atlanta (July, 1991), Santa Fe (November, 1991), and San Diego (March, 1992) IETF meetings. In June, 1992, a proposed charter for a formal Working Group was submitted to the IETF and at the same time a mailing list was set up for conduct of the group's business. Following a revision of the charter, the Working Group was officially formed in June 30, 1992.

#### IETF Mobile IP Working Group Charter, Goals, and Milestones

The IETF Mobile IP Working Group (mobileip WG) is chartered to develop or adopt architectures and protocols to support mobility within the Internet. In the near-term, protocols for supporting transparent host "roaming" among different subnetworks and different media (e.g., LANs, dial-up

links, and wireless communication channels) are to be developed and entered into the Internet standards track. The work is expected to consist mainly of new and/or revised protocols at the (inter)network layer, but may also include proposed modifications to higher-layer protocols (e.g., transport or directory). However, it is a requirement that the proposed solutions allow mobile hosts to interoperate with existing Internet systems.

In the longer term, the group may address, to the extent not covered by the mobile host solutions, other types of internet mobility, such as mobile subnets (e.g., a local network within a vehicle), or mobile clusters of subnets (e.g., a collection of hosts, routers, and subnets within a large vehicle, like a ship or spacecraft, or a collection of wireless, mobile routers that provide a dynamically changing internet topology).

### **6.1.2 Overview of Draft Version 16 of the IETF IP Mobility Support**

In this section we provide an overview of the current base specification for Mobile IP. The terminology is similar to CDPD and is summarized in Table 1.

The Mobile IP approach is analogous to postal service delivery: whenever you move to a new location, you ask your home post office to forward your mail to your new address via the local post office there. Thus, a mobile node first leaves its home network and connects to a foreign network. An agent on the home network then intercepts packets sent to the mobile node and forwards them to an agent on the foreign agent. This agent then delivers packets locally to the mobile node visiting that network.

#### **Mobile IP Entities and Mechanisms**

Mobile nodes are supported by two service entities.

- A home agent which is the mobile support node on the home network. It keeps track of mobile node location (mobility binding) and intercepts and tunnels packets destined for the mobile node.
- A foreign agent which is the mobile support node on the foreign network which decapsulates and delivers packets tunneled to the mobile node. Mobile nodes may act as their own foreign agent.

These entities interact in the following ways:

##### **1. Agent Discovery**

Home agents and foreign agents may advertise their availability via broadcast on each link for which they provide service. A newly arrived

mobile node can likewise broadcast a solicitation on the link to learn if any prospective agents are present. The advertisement is an extension of router advertisement (RFC 1256). It allows a mobile node to determine its point of attachment (moved to a new foreign network, or returned to its home network). Advertisements contain:

- Care-of-address (foreign agents only)
- Home agent/foreign agent status bits

### 2. Registration

When the mobile node is away from home, it registers its care-of address with its home agent. Depending on its method of attachment, the mobile node will register either directly with its home agent, or through a foreign agent which forwards the registration to the home agent. Home and foreign agents may reject registration requests; this option is necessary to combat registration attacks by the "bad guys."

Registration attacks can be of at least three types: Forgery, whereby bogus mobile node location is sent to the home agent; Modification, whereby a valid registration request is altered to send the mobile node's traffic elsewhere; and Replay which involves storing a valid registration request for later malicious diversion of mobile node traffic.

To prevent an attacker from changing a mobility binding the following precautions are taken:

- The mobile node and home agent share a security association. This may be a shared secret key or a public/private key pair, or an authentication algorithm such as MD5.
- An authenticator is sent in registration requests and replies. An example is a nonce or timestamp included for replay protection.

### 3. Tunneling/Encapsulation

Tunneling is used for transportation of mobile node packets from the home network to the foreign network. There are two endpoints: The home agent which encapsulates and transmits; and the care-of address entity which receives and decapsulates. The original packet becomes a payload in the new packet sent to the care-of address. There are various options for implementing this: IP-in-IP (draft), GRE, and Minimal Encapsulation are among the encapsulation options.

## Mobile IP Operation

The following steps outline the operation of the Mobile IP protocol:

1. 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.
2. A mobile node receives these agent advertisements and determines whether it is on its home network or a foreign network.
3. When the mobile node determines that it is located on its home network, it operates without mobility services. If it is returning to its home network after being registered elsewhere, the mobile node deregisters with its home agent, by exchanging registration request and registration reply messages.
4. 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, see section 10.1.2.2.1), or by some external assignment mechanism such as DHCP (a co-located care-of address).
5. 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 messages, possibly via a foreign agent.
6. Datagrams 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.
7. 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.

### Care-of Addresses

When away from home, Mobile IP uses protocol tunneling to hide a mobile node's home address from intervening routers between its home network and its current location. The tunnel terminates at the mobile node's care-of address. The care-of address must be an address to which datagrams can be delivered via conventional IP routing. At the care-of address, the

original datagram is removed from the tunnel and delivered to the mobile node.

Mobile IP provides two alternative modes for the acquisition of a care-of address:

- A foreign agent care-of address is a care-of address provided by a foreign agent through its agent advertisement messages. In this case, the care-of address is an IP address of the foreign agent. In this mode, the foreign agent is the endpoint of the tunnel and, upon receiving tunneled datagrams, decapsulates them and delivers the inner datagram to the mobile node. This mode of acquisition is preferred because it allows many mobile nodes to share the same care-of address and therefore does not place unnecessary demands on the already limited IPv4 address space.
- A co-located care-of address is a care-of address acquired by the mobile node as a local IP address through some external means, which the mobile node then associates with one of its own network interfaces. The address may be dynamically acquired as a temporary address by the mobile node such as through DHCP, or may be owned by the mobile node as a long-term address for its use only while visiting some foreign network. When using a co-located care-of address, the mobile node serves as the endpoint of the tunnel and itself performs decapsulation of the datagrams tunneled to it.

The mode of using a co-located care-of address has the advantage that it allows a mobile node to function without a foreign agent, for example, in networks that have not yet deployed a foreign agent. It does, however, place additional burden on the IPv4 address space because it requires a pool of addresses within the foreign network to be made available to visiting mobile nodes. It is difficult to efficiently maintain pools of addresses for each subnet that may permit mobile nodes to visit.

It is important to understand the distinction between the care-of address and the foreign agent functions. The care-of address is simply the endpoint of the tunnel. It might indeed be an address of a foreign agent (a foreign agent care-of address), but it might instead be an address temporarily acquired by the mobile node (a co-located care-of address). A foreign agent, on the other hand, is a mobility agent that provides services to mobile nodes.

### Home and Foreign Agents

A home agent must be able to attract and intercept datagrams that are destined to the home address of any of its registered mobile nodes. Using the proxy and gratuitous ARP mechanisms, this requirement can be satisfied if the home agent has a network interface on the link indicated by the mobile node's home address. Other placements of the home agent relative to the mobile node's home location may also be possible using other mechanisms for intercepting datagrams destined to the mobile node's home address.

Similarly, a mobile node and a prospective or current foreign agent must be able to exchange datagrams without relying on standard IP routing mechanisms; that is, those mechanisms which make forwarding decisions based upon the network prefix of the mobile node's destination IP address. This requirement can be satisfied if the foreign agent and the visiting mobile node have an interface on the same link.

In this case, the mobile node and foreign agent simply bypass their normal IP routing mechanism when sending datagrams to each other, addressing the underlying link layer packets to their respective link layer addresses. Other placements of the foreign agent relative to the mobile node may also be possible using other mechanisms to exchange datagrams between these nodes, but such placements are beyond the scope of our discussion.

If a mobile node is using a co-located care-of address, the mobile node must be located on the link identified by the network prefix of this care-of address. Otherwise, datagrams destined to the care-of address would be undeliverable to the mobile node.

For example, the figures below illustrates the routing of datagrams to and from a mobile mode (MN) away from home, once the mobile node has registered with its home agent (HA). In the figures below, the mobile node is using a foreign agent (FA) care-of address.

In Figure 1, a correspondent node (CN) transmits a packet destined for the mobile node. The packet is routed (1) in the conventional manner to the network specified by the mobile node's home address. At the home network the packet is intercepted by the home agent and tunneled (2) to the foreign agent, which then decapsulates it and forwards (3) the packet to the mobile node by way of a link layer address.

c../gif/fig1.gif

In Figure 2, the visiting mobile node transmits a packet to the correspondent node. Routing of this packet is done in the conventional way, with no need to involve either the home or foreign agent.

c../gif/fig2.gif

### Mobile IP Protocol Walkthrough

The Mobile IP protocol is outlined in steps below, under four basic procedural categories. In our discussions MN denotes "Mobile Node," HA denotes "Home Agent," and FA denotes "Foreign Agent".

#### 1. Network Attachment

During this phase, foreign and home agents advertise their presence via agent advertisement messages. The mobile node may also optionally solicit an agent advertisement message from them.

1. MN - attaches to a new foreign network.
2. MN - solicits an agent advertisement (if necessary).
3. FA - sends advertisement.

#### 2. Registration

Now that the mobile node is on a foreign network, it obtains a care-of address on this network, and registers its new care-of address with its home agent, possibly via the foreign agent.

4. MN - requests registration from FA.
5. FA - forwards registration request to HA.
6. HA - sends registration reply to FA.
7. FA - forwards registration reply to MN.
8. HA - proxy ARPs for MN.

#### 3. Data Transfer to the Mobile Node

Data sent to the mobile node's home address are now intercepted and tunneled by the home agent to the mobile node's care-of address. These are then received at the tunnel endpoint (foreign agent for example) and delivered to the mobile node.

9. HA - intercepts, encapsulates, and forwards packets to FA (arrow 2 in Figure 1).

10. FA - decapsulates and forwards to MN (arrow 3 in Figure 2).

#### 4. Data Transfer From the Mobile Node

Data from the mobile node are delivered to their destination using standard IP routing mechanisms, not necessarily passing through the home agent.

11. MN - Encapsulates and forwards packets to Destination (Figure 2).

## 6.2 Mobility under IPv6

A new version of the Internet Protocol, IPv6, is being developed with 128-bit addresses. IPv6 remedies perceived flaws in the existing version of IP (that is, IPv4). Mobile computers are likely to account for a substantial fraction of the population of the Internet during the lifetime of IPv6.

The development of IPv6 presents a rare opportunity, in that there is no existing installed base of IPv6 hosts or routers with which compatibility must be maintained. All IPv6 nodes may be assumed to perform the few operations needed to support Internet-wide mobility. The most important function needed to support mobility is the reliable and timely notification of a mobile node's current location to those other nodes that need it. The home agent needs this location information in order to redirect packets from the home network to the mobile node. Correspondent nodes need this information in order to send their own packets directly to the mobile node.

### 6.2.1 The IPv6 Standards Process

It is important to recognize that IPv6 is rapidly evolving. The current base specification for IPv6 is an "Internet Draft." Internet Drafts are draft documents that may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet Drafts as reference material or to cite them other than as "work in progress." Therefore, this entire section should be read with the understanding that it provides only a snapshot as of June 1996.

### 6.2.2 Overview of Mobility Support in IPv6

From the model of operation enabling mobile networking for IPv4, the authors of the Mobile IPv6 draft [PERK96] borrow the concepts of home network, home address, home agent, care-of address, and binding. Mobile computers are assigned (at least) two IPv6 addresses whenever they are roaming away from their home network. One (the home address) is permanent; the other (the IPv6 link-local address) is used temporarily. In addition, the mobile node will typically autoconfigure figure a globally-routable address at each new point of attachment. Every IPv6 router supports encapsulation, so every router is capable of serving as a home agent on the network(s) to which it is attached.

Using IPv4 terminology, the basic model of operation in IPv6 assumes that mobile node can always be reached by sending packets to its home (permanent) address. Whenever the mobile node is not present on its home network, packets arriving for it there will be intercepted by the home agent, and tunneled to a care-of address.

Care-of addresses can be constructed by the mobile node using the methods of automatic address configuration. If the mobile node receives router advertisements, it must use automatic address configuration to con-

struct a globally unique, routable address. This routable address can be used by the mobile node as its care-of address.

After determining its care-of address, a mobile node must send a binding update containing that care-of address to the home agent (and any other correspondent nodes that may have out-of-date bindings in their binding cache). By default, correspondent nodes send packets to mobile nodes by using routing headers instead of encapsulation. As detailed in the next section, correspondent nodes are usually expected to deliver packets directly to the mobile node's care-of address, so that the home agent is rarely involved with packet transmission to the mobile node.

It is essential for scalability and minimizing network load that correspondent nodes be able to learn the care-of address for a mobile node, and to be able to cache this information for use in sending future packets to the mobile node's care-of address. By caching the care-of address of a mobile node, optimal routing of packets can be achieved between the correspondent node and the mobile node. Routing packets directly to the mobile node's care-of address also eliminates congestion at the home agent and thus contributes significantly to the overall health of the Internet.

Moreover, many communication events between mobile nodes and correspondent nodes can be carried out with no assistance from the home agent. Thus, the impact of failure at the home agent can be drastically reduced; this is important because many administrative domains will have a single home agent to serve a particular home network, and thus a single point of failure for communications to nodes using that home agent.

Communications between the home agent and a mobile node may depend on a number of intervening networks. Thus, there are many more ways that packets can fail to reach a mobile node when the home agent is required as an intermediate node. This would be particularly relevant on, say, trans-oceanic links between home agent and mobile node. Caching the binding of a mobile node at the correspondent node enables communication with the mobile nodes even if the home agent fails or is difficult to contact over the Internet.

In the typical case, when a mobile node has configured its care-of address at one of its own interfaces, transferring data to the mobile node means no more work for routers on the link at its current point of attachment, than transferring data to any other node on that link. This improves performance further.