ARMY RESEARCH LABORATORY

Mobile IP LAN for ARL Mobile Communications/Networking Testbed

Brian B. Luu

ARL-TR-758

February 2001

Approved for public release; distribution unlimited.

20010330 107

The findings in this report are not to be construed as an official Department of the Army position unless so designated by other authorized documents.

Citation of manufacturer's or trade names does not constitute an official endorsement or approval of the use thereof.

Destroy this report when it is no longer needed. Do not return it to the originator.

Army Research Laboratory

Adelphi, MD 20783-1197

ARL-TR-758 February 2001

Mobile IP LAN for ARL Mobile Communications/Networking Testbed

Brian B. Luu

Computational and Information Sciences Directorate

Approved for public release; distribution unlimited.

Abstract

This report describes the protocol and implementation of a Mobile IP (Internet protocol) LAN (local area network) for the LAN of the U.S. Army Research Laboratory (ARL) Mobile Communications/Networking Testbed. Mobile IP LAN protocol is developed to allow a LAN to be mobile with IP mobility. The mobility of a LAN provides mobility for its nodes, which are fixed relative to the LAN and are not mobile IP in nature. This report includes discussions and comparisons of Mobile IP LAN versus Mobile IP for mobile nodes.

Contents

1. **Introduction** 1

2. **Mobile IP LAN** 2
   - 2.1 Overview 2
   - 2.2 Requirements 2
   - 2.3 Details 2

3. **Implementation on Linux** 4

4. **Discussion** 8

5. **Conclusion** 10

References 11

Distribution 13

Report Documentation Page 15

Figures

1. LAN when connecting normally at home network 5
2. LAN when moving and connecting at foreign network 6

1. Introduction

The U.S. Army Research Laboratory (ARL) Mobile Communications/ Networking Testbed has demonstrated the usefulness and necessity of mobility for the U.S. Army digital battlefield. However, the vast majority of software and network applications for the Army either rely on commercial off-the-shelf products or are developed and based on standard protocols that are not generally mobile. In particular, the local area network (LAN) of the ARL Testbed is Internet protocol (IP)-based and comprises wired workstations, such as Sun (Sun Microsystems, Inc.), SGI (Silicon Graphics, Inc.), Dell (Dell Computer Corporation), and wireless portable laptop personal computers.

Recently, there have been experiments and protocols that support IP mobility, especially Mobile IP (MIP) specified by the RFC (request for comment) 2002 [1]. But so far, MIP has been implemented only on individual mobile nodes, and in some implementations, it can be resource demanding. For example, Dixit and Gupta's [2] or MosquitoNet [3] implementation requires an IP tunnel for every mobile node. Moreover, the IP version 6 (IPv6) is designed to accommodate mobility. Therefore, the industry will not likely accept and adopt MIP for use in the current IPv4. As a result, most of the implementations for MIP are just experimental and available only on an open-source platform, such as Linux.

On the other hand, the mobility for the standard IP nodes, which are not mobile IP in nature, can be supported through the mobility of the LAN. The Communications and Computer Science Division of the Information Science and Technology Directorate (now called the Computational and Information Sciences Directorate) of ARL has studied, designed, implemented, and tested Mobile IP LAN protocol in the ARL Testbed. Mobile IP LAN is designed to provide mobility for IP LANs on the Internet but still support Internet connectivity for nonmobile IP nodes on LANs.

For the remainder of this report, I will discuss LANs that are IP-based. For simplicity, the aspects of registration (the "handshaking" to establish a temporary connection change of a mobile LAN at a foreign network), deregistration (the handshaking to disconnect a temporary connection change of a mobile LAN), and security are not discussed in this report. The registration and deregistration are needed to improve accountability and network security for mobile LANs.

2. Mobile IP LAN

2.1 Overview

Normally, a LAN accesses a gateway to the Internet by at least one connection through a router on the LAN. When the LAN moves to a different location with a different connection to the Internet, all the connectivity within the LAN still behaves normally, but the inbound traffic for the LAN continues to be routed on the Internet to its home network (the autonomous system where the LAN belongs). To reestablish the link, a special computer node in its home network (called home agent) accepts the traffic for the LAN and routes the inbound LAN traffic through an IP tunnel with the destination address at the new Internet connection of the LAN router. The outbound traffic of the LAN can be routed normally through the foreign network connection to the Internet. In brief, when the LAN is away from the home network, the traffic of a mobile LAN is redirected to an IP tunnel whose end nodes are the home agent and LAN router.

2.2 Requirements

Because of the complexity of LAN connections, not all LANs can adopt Mobile IP LAN implementation. Striving for simplicity and flexibility, I designed Mobile IP LAN protocol to support LANs meeting the following criteria:

- Single network address determined based on netmask.
- Ending LAN that does not route other LANs' traffic through the LAN.
- Single gateway connection that provides a single entering and exiting of traffic from the LAN. This implies a single default gateway for all nodes in the LAN.
- All LAN nodes must be moved together as a single entity.

2.3 Details

The network routing of Mobile IP LAN protocol is modeled based on the concept of network routing of MIP [1]. However, instead of considering IP mobility for individual nodes, I apply IP mobility implementation to a LAN as a whole, which, in turn, makes LAN nodes IP mobile.

Basically, Mobile IP LAN protocol requires a minimum of two nodes furnished with mobility software, a home agent, and a mobile router. The mobile router is usually the router of a mobile LAN. A foreign agent [1] can be implemented, but it just complicates the network routing and reduces the network efficiency. Generally, the mobile router should have two network interface cards (NIC): one that connects to the mobile LAN, called LAN NIC, and the other that connects to the gateway LAN (home network), called gateway NIC.

Mobile IP LAN operation happens when a LAN is moved and the gateway NIC of the LAN is connected to a new point of attachment on the Internet. Through its gateway NIC, the LAN's mobile router tries to acquire an IP address (a care-of address) at the new location through Dynamic Host Configuration Protocol (DHCP) mechanism or preassignment. The mobile router then configures the gateway NIC with all the acquired information (such as IP address, netmask, broadcast address, and default gateway for routing) to be able to communicate on the Internet. The mobile router uses the care-of address to communicate with a home agent in its home network to request the home agent to reroute all the inbound traffic of the LAN through an IP tunnel, which uses an encapsulation mechanism [4], to the care-of-address destination. The home agent should use an IP routing software, such as Routing Information Protocol (RIP) or Open Shortest Path First (OSPF), to advertise the network reachability of the LAN through it (home agent) in its home network and spread on to the Internet. Concisely, the inbound traffic for the LAN is received and tunneled by the home agent to the care-of address of the mobile router. Receiving encapsulated packets from the IP tunnel, the mobile router decapsulates ("detunnels") and routes the packets to the LAN.

On the other hand, the outbound traffic of the LAN is channeled through the mobile router and through a default gateway of the foreign network. A second IP tunnel can be created to redirect the outbound traffic of the LAN from the mobile router to the home agent and to let the home agent route all inbound and outbound traffic of the LAN. The second IP tunnel should be used if the foreign network environment blocks outbound traffic of unknown networks [5] or if the new LAN connection to the Internet is not to be disclosed.

In short, for mobility, not one of the nodes in a mobile LAN, except for the mobile router, requires mobility software or changes in the nodes' network configuration as long as the nodes have the mobile router set as the default gateway for their network configuration. Only the mobile router and home agent, which are the two end nodes of the IP tunnel(s), need to be equipped with additional software to do routing, encapsulating, and decapsulating.

3. Implementation on Linux

In this section, I describe the implementation of Mobile IP LAN on the ARL Testbed. For this demonstration (the feasibility of Mobile IP LAN), there are no registration and deregistration of Mobile IP LAN. The Linux operating system (O/S) distributed by Red Hat, Inc., version 5.2, with kernel 2.0.36 level, is chosen to implement Mobile IP LAN, since it provides all the needed software, such as IP tunneling, RIP, and OSPF. Be aware that those software features are not automatically built in the Linux kernel; a kernel rebuilt needs to be done to ensure those software modules are available for use. No additional software besides the Linux operating system is needed to implement Mobile IP LAN. All connections and configuration are done manually. I use a preassigned care-of address at a new location for the mobile LAN.

The LAN of the ARL Testbed mainly consists of an Ethernet network, with a wireless extension. The mobile router of the LAN is a laptop computer equipped with one wired Ethernet NIC and one wireless Ethernet NIC. The wireless Ethernet NIC is configured to connect to the LAN, and the wired NIC is configured as a gateway NIC for the LAN. The LAN NIC is wireless to provide flexibility in positioning the mobile router near an Internet connection point, which can be a distance away from the ARL Testbed. The home agent for the LAN is a desktop personal computer that is configured with one NIC connected to the ARL network at Adelphi Laboratory Center (ALC).

For security reasons, simulated IP addresses that conformed to the RFC 1918 [6] are used in this report instead of the actual IP addresses used in the ARL Testbed. Figure 1 depicts the normal connection of the LAN to its home network. The mobile LAN with network identification 192.168.23.0 has a gateway to the home network 172.16.0.0 through the mobile router that has an IP address 192.168.23.1 assigned to the LAN NIC and 172.16.27.211 assigned to the gateway NIC. The home agent resides on the home network with the IP address 172.16.27.215. When the LAN is at the home network, its mobile router advertises to the home network its presence and its routing path with the gateway address 172.16.27.211.

Figure 2 shows that the LAN moves and connects to a different point of attachment on the Internet. The mobile router keeps the configuration of LAN NIC intact and configures the gateway NIC with the care-of-address 172.30.250.99. Also the new default gateway is specified for the mobile router at the foreign network. The following commands are used to achieve the above setting on the mobile router:

```
ifconfig eth1 down

ifconfig eth1 172.30.250.99 netmask 255.255.255.0 broadcast\
172.30.250.255

route add default gw 172.30.250.1 dev eth1
```

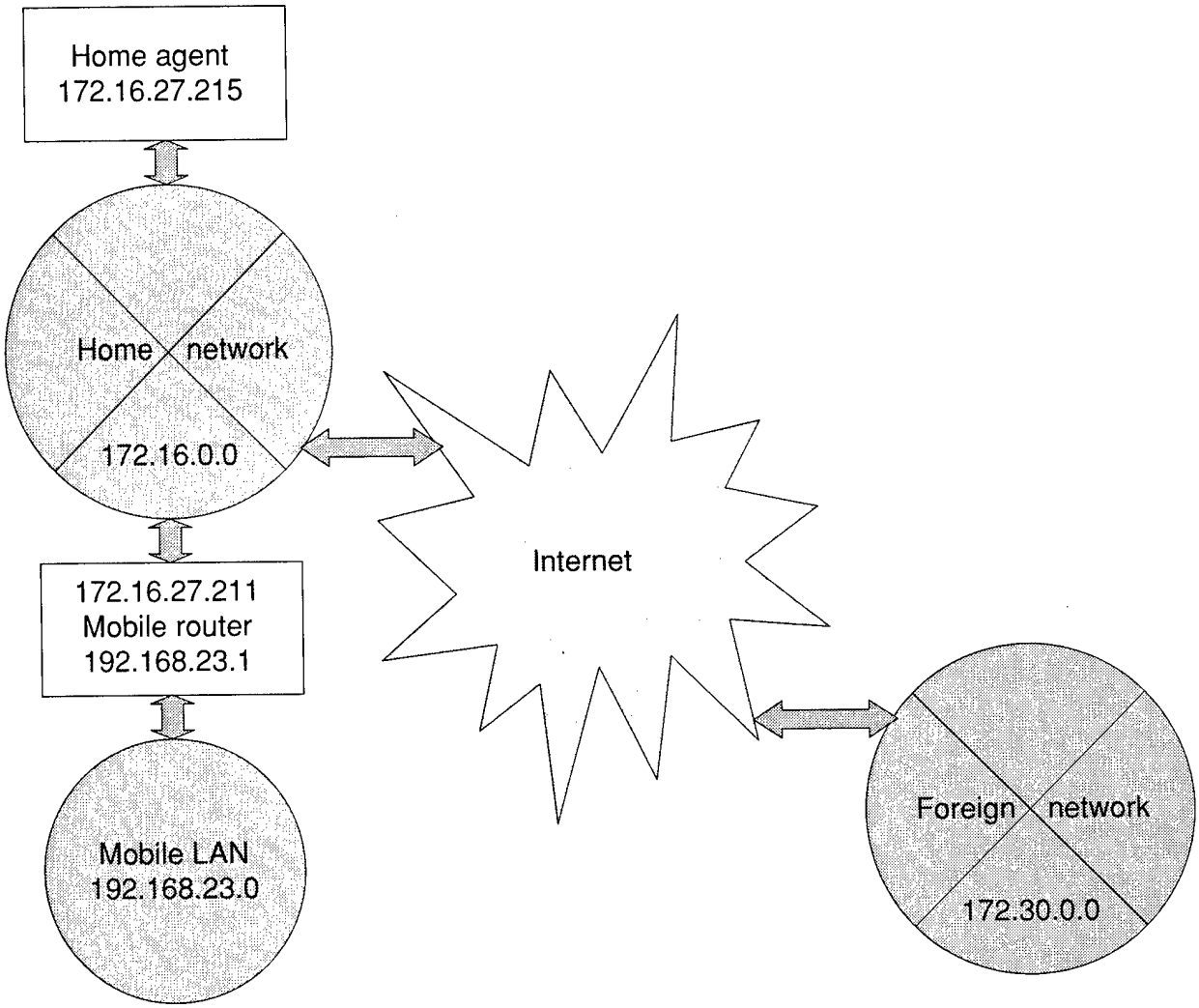

Figure 1. LAN when connecting normally at home network.

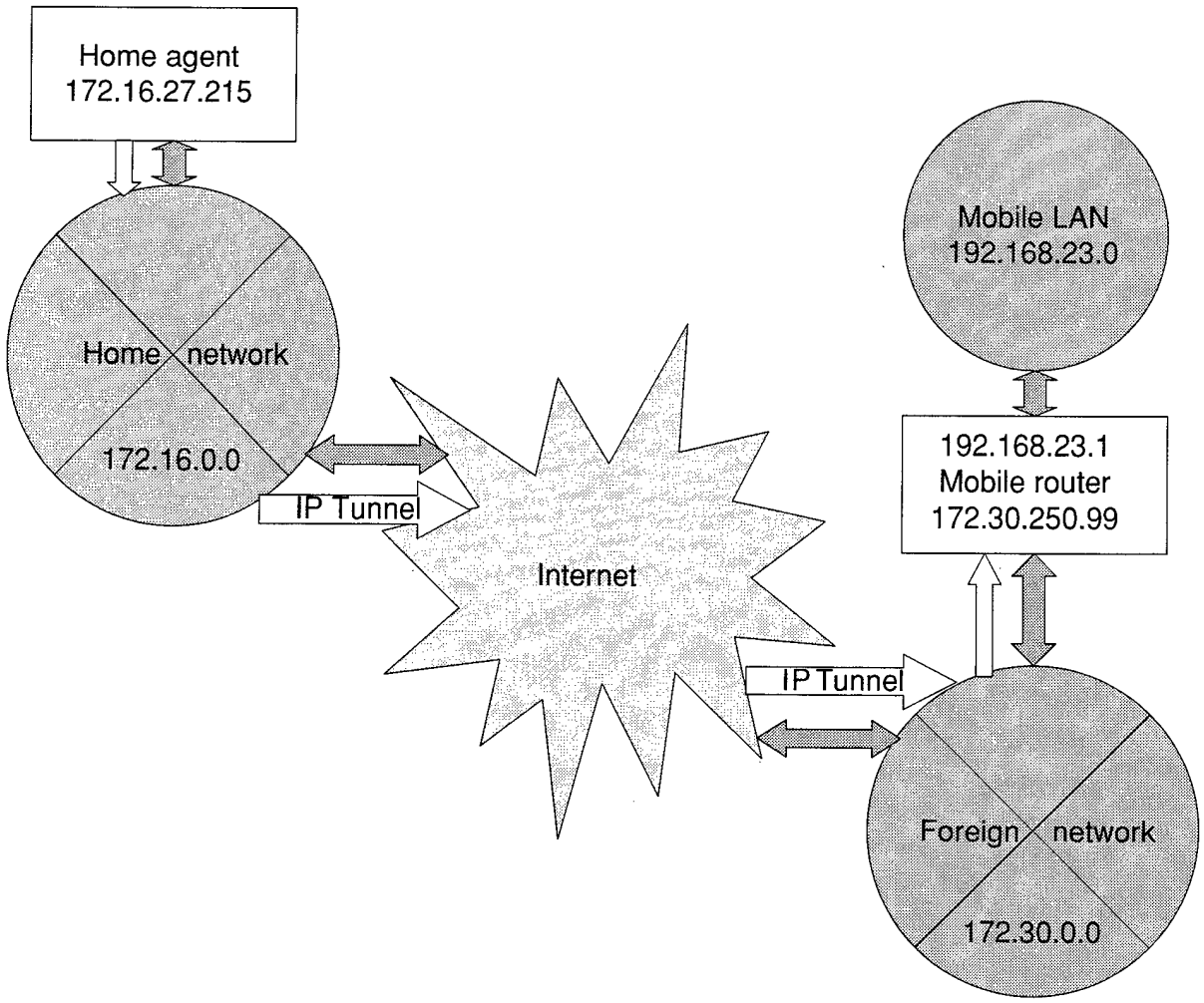

Figure 2. LAN when moving and connecting at foreign network.

At the home network, the home agent configures an IP tunnel with the destination address to the care-of-address 172.30.250.99 and routes the network traffic destined to the LAN through the tunnel. Supposedly, the routing software, such as RIP or OSPF, on the home agent should advertise the routing path of the LAN with the gateway IP address of the home agent 172.16.27.215. Unfortunately, I was unable to configure the routing software on the home agent to perform that routing advertisement. To overcome the problem, one has to create on the main gateway of the home network a static routing that points the routing path of the LAN to the home agent. The following commands are used to achieve the IP tunnel on the home agent:

```
ifconfig tunl0 172.16.27.215 netmask 255.255.0.0 point to point\
172.30.250.99

route add -net 192.168.23.0 netmask 255.255.255.0 dev tunl0
```

When the LAN returns to the original attachment point at the home network, the home agent removes the tunnel; also the static routing on the main gateway should be removed. As a consequence, the routing path to the LAN at the foreign network connection is automatically removed. The mobile router reconfigures its gateway NIC as before and readvertises the routing path of the LAN at the home network.

4. Discussion

As described in the previous section, one can implement the whole Mobile IP LAN protocol just by using two Linux computer systems with an exception of a static route on the main router of a home network. I believe that the RIP or OSPF software on the Linux is not designed to advertise the network reachability of a LAN with the routing path through an IP tunnel, which is not a true NIC device, to avoid any routing loops. To solve this problem, one should modify the routing software to allow this network advertisement, especially, since the software source code is available on the Linux platform.

In theory, a LAN can be moved on the Internet as long as routers on the Internet propagate the LAN's routing reachability advertised by the LAN's router at any new location. But for the Internet routing to be manageable, workable, and secure, all border gateway routers are configured to advertise only the network reachability of the networks, which belong to the organization or affiliated organizations of the routers. Exceptions might be made to accommodate a permanent move of a LAN but not for unpredictable moves of a LAN. For a LAN to move from one organization to another, border gateway routers and possibly some internal routers need numerous adjustments. Most likely, network administrators for those routers will adamantly oppose these requests. For example, imagine that an ARL IP LAN is connected to an Internet location in Japan; ARL would have had to request coordination of each of the network administrators from the Defense Research Engineer Network, the military domain, intermediate domains (domains that link the military domain and the Japan domain), the Japan domain, and local Japanese organizations. It would be an impractical and hardly achievable attempt. Besides, this time-consuming process must be repeated whenever the LAN is moved.

When a mobile LAN is connected to a foreign network without the second IP tunnel, a mobile LAN can improve the LAN connectivity with the nodes on the foreign network by having its mobile router advertising the routing path of the mobile LAN on the foreign network environment. As mentioned previously, filtering policies on the foreign network routers filter routing advertisement of the mobile router, but usually only the main gateway routers or the border gateway protocol (BGP) routers perform this special filtering. Moreover, any computer nodes on the foreign network equipped with routing software can receive the routing advertisement of the mobile router directly rather than from a router. As a result, nodes in the mobile LAN are just one or a few network hops away from nodes on the foreign network instead of being numerous hops away if the mobile LAN were at its home network.

At a foreign network connection, the routing path of network traffic of a mobile LAN with only one IP tunnel is asymmetric because the inbound traffic is tunneled from its home agent to its mobile router. The asymmetric

routing path causes dissimilar transmission time of inbound and outbound traffic. Because of the IP tunnel, usually the outbound traffic's transmission time is shorter than the inbound traffic's time. To have the symmetric routing path for the traffic of the mobile LAN, the second IP tunnel should be created. A similar asymmetric routing problem occurred in the implementation of MIP, but Montenegro proposed a similar resolution in RFC 2344 [7]. Unfortunately, I have not succeeded in implementing the second IP tunnel for mobile IP LAN in the Red Hat Linux-kernel 2.0.36 platform. The problem arises in directing the outbound traffic of the LAN through a tunnel.

Since all nodes of a mobile LAN are moved together, broadcast traffic within the mobile LAN should have no effect. At the time of this report, no full investigation has been done to determine any effects on multicasting in a mobile LAN. I believe that multicasting to the Internet should function properly on a mobile LAN as long as its mobile router supports multicast routing. With the use of a care-of address, a mobile router can participate to multicasting traffic at the foreign network and reroute multicast information to nodes in its mobile LAN.

Although I have not yet tested MIP for individual mobile nodes in a mobile LAN that implements Mobile IP LAN, it should function properly as long as a foreign agent or care-of addresses are available in the LAN.

In contrast to MIP, the home agent of a mobile LAN using Mobile IP LAN does not have to be a node on the same network with the gateway network of the mobile LAN at the home network. Any nodes on any LANs within the home network environment furnished with the routing, encapsulating, and decapsulating software can be the home agent of the mobile LAN.

When a mobile LAN using Mobile IP LAN is away from its home network, it still keeps its LAN traffic to itself. Therefore, two nodes in a mobile LAN still communicate normally regardless where the mobile LAN is located. Conversely, two mobile nodes using MIP from the same LAN must tunnel their traffic back and forth to their home network to communicate to each other even though they may be on the same foreign network. Furthermore, all nodes (except the mobile router) in a mobile LAN using Mobile IP LAN require no additional software and reconfiguration for IP mobility, whereas currently, MIP can work only on a Linux platform. For example, on the mobile LAN of the ARL Testbed, an SGI workstation running IRIX O/S, a Sun workstation running Solaris O/S, and Dell workstations running Window 95 or Linux O/S functioned and communicated properly without any network adjustments or reconfiguration to the workstations.

5. Conclusion

I have demonstrated the feasibility and ease of the implementation of Mobile IP LAN. In fact, the mobile LAN for the ARL Testbed was successfully tested at the Internet connection at the University of Maryland University College. I also encountered less software development, routing management, network overhead, and computer resources for the implementation of Mobile IP LAN compared to MIP. Although all the nodes of the mobile LAN have to move together to have IP mobility, I believe that by implementing network subnetting, a number of LAN nodes can be mobile together at a same foreign network without requiring the entire LAN to be mobile.

References

1. C. Perkins, "IP Mobility Support," *RFC 2002*, October 1996.
2. A. Dixit and V. Gupta, "Mobile IP for Linux (version 1.00)," May 1996.
3. Computer Science Department of Stanford University, "Stanford MosquitoNet Project Mobile IP v4 Distribution Users Manual (release 1.0.5)," April 1999.
4. C. Perkins, "IP Encapsulation within IP," *RFC 2003*, October 1996.
5. P. Ferguson and D. Senie, "Network Ingress Filtering: Defeating Denial of Service Attacks Which Employ IP Source Address Spoofing," *RFC 2267*, January 1998.
6. Y. Rekhter, B. Moskowitz, D. Karrenberg, G. J. de Groot, and E. Lear, "Address Allocation for Private Internets," *RFC 1918*, February 1996.
7. G. Montenegro, "Reverse Tunneling for Mobile IP," *RFC 2344*, May 1998.

Distribution

Admnstr
Defns Techl Info Ctr
ATTN DTIC-OCP
8725 John J Kingman Rd Ste 0944
FT Belvoir VA 22060-6218

Ofc of the Secy of Defns
ATTN ODDRE (R&AT)
The Pentagon
Washington DC 20301-3080

Ofc of the Secy of Defns
ATTN OUSD(A&T)/ODDR&E(R) R J Trew
3080 Defense Pentagon
Washington DC 20301-7100

AMCOM MRDEC
ATTN AMSMI-RD W C McCorkle
Redstone Arsenal AL 35898-5240

US Military Acdmy
Mathematical Sci Ctr of Excellence
ATTN MADN-MATH MAJ M Huber
Thayer Hall
West Point NY 10996-1786

Dir for MANPRINT
Ofc of the Deputy Chief of Staff for Prsnnl
ATTN J Hiller
The Pentagon Rm 2C733
Washington DC 20301-0300

TECOM
ATTN AMSTE-CL
Aberdeen Proving Ground MD 21005-5057

US Army ARDEC
ATTN AMSTA-AR-TD
Bldg 1
Picatinny Arsenal NJ 07806-5000

US Army Info Sys Engrg Cmnd
ATTN AMSEL-IE-TD F Jenia
FT Huachuca AZ 85613-5300

US Army Natick RDEC Acting Techl Dir
ATTN SBCN-T P Brandler
Natick MA 01760-5002

US Army Simulation Train & Instrmntn Cmnd
ATTN AMSTI-CG M Macedonia
ATTN J Stahl
12350 Research Parkway
Orlando FL 32826-3726

US Army Tank-Automtv Cmnd RDEC
ATTN AMSTA-TR J Chapin
Warren MI 48397-5000

Nav Surfc Warfare Ctr
ATTN Code B07 J Pennella
17320 Dahlgren Rd Bldg 1470 Rm 1101
Dahlgren VA 22448-5100

Hicks & Assoc Inc
ATTN G Singley III
1710 Goodrich Dr Ste 1300
McLean VA 22102

US Army Rsrch Lab
ATTN AMSRL-CI N Radhakrishnan
Aberdeen Proving Ground MD 21005-5067

Director
US Army Rsrch Lab
ATTN AMSRL-RO-D JCI Chang
ATTN AMSRL-RO-EN W D Bach
PO Box 12211
Research Triangle Park NC 27709

US Army Rsrch Lab
ATTN AMSRL-CI J D Gantt
ATTN AMSRL-CI-AI-R Mail & Records Mgmt
ATTN AMSRL-CI-AP Techl Pub (2 copies)
ATTN AMSRL-CI-C J Gowens
ATTN AMSRL-CI-CN B Luu (10 copies)
ATTN AMSRL-CI-CN G Cirincione
ATTN AMSRL-CI-CN H Harrelson
ATTN AMSRL-CI-LL Techl Lib (2 copies)
ATTN AMSRL-DD J M Miller
Adelphi MD 20783-1197

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188), Washington, DC 20503.

1. AGENCY USE ONLY *(Leave blank)*	2. REPORT DATE	3. REPORT TYPE AND DATES COVERED
	February 2001	Final, FY98

4. TITLE AND SUBTITLE Mobile IP LAN for ARL Mobile Communications/Networking Testbed

5. FUNDING NUMBERS
DA PR: AH48
PE: 611102H48

6. AUTHOR(S) Brian B. Luu

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
U.S. Army Research Laboratory
Attn: AMSRL-CI-CN email: bluu@arl.army.mil
2800 Powder Mill Road
Adelphi, MD 20783-1197

8. PERFORMING ORGANIZATION REPORT NUMBER
ARL-TR-758

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)
U.S. Army Research Laboratory
2800 Powder Mill Road
Adelphi, MD 20783-1197

10. SPONSORING/MONITORING AGENCY REPORT NUMBER

11. SUPPLEMENTARY NOTES
ARL PR: 1FEPA1
AMS code: 611102H4811

12a. DISTRIBUTION/AVAILABILITY STATEMENT Approved for public release; distribution unlimited.

12b. DISTRIBUTION CODE

13. ABSTRACT *(Maximum 200 words)*

This report describes the protocol and implementation of a Mobile IP (Internet protocol) LAN (local area network) for the LAN of the U.S. Army Research Laboratory (ARL) Mobile Communications/Networking Testbed. Mobile IP LAN protocol is developed to allow a LAN to be mobile with IP mobility. The mobility of a LAN provides mobility for its nodes, which are fixed relative to the LAN and are not mobile IP in nature. This report includes discussions and comparisons of Mobile IP LAN versus Mobile IP for mobile nodes.

14. SUBJECT TERMS MIP, tunneling, routing

15. NUMBER OF PAGES 18

16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
Unclassified	Unclassified	Unclassified	UL

NSN 7540-01-280-5500

Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. Z39-18
298-102