ARMY RESEARCH LABORATORY

Selective Routing for the Mobile IP LAN Protocol

by Brian B. Luu and Richard D. Gopaul

ARL-TR-3661 **September 2005**

NOTICES

Disclaimers

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-3661 **September 2005**

Selecting Routing for the Mobile IP LAN Protocol

Brian B. Luu and Richard D. Gopaul
Computational and Information Sciences Directorate, ARL

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	2. REPORT TYPE	3. DATES COVERED (From - To)
September 2005	Final	September 2003 to September 2004

4. TITLE AND SUBTITLE
Selective Routing for the Mobile IP LAN Protocol

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)
Brian B. Luu and Richard D. Gopaul

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
U.S. Army Research Laboratory
ATTN: AMSRD-ARL-CI-CN
2800 Powder Mill Road
Adelphi, MD 20783-1197

8. PERFORMING ORGANIZATION REPORT NUMBER
ARL-TR-3661

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

10. SPONSOR/MONITOR'S ACRONYM(S)

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

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

13. SUPPLEMENTARY NOTES

14. ABSTRACT
Mobile Internet Protocol (IP) Local Area Network (LAN) is a technique developed by the U.S. Army Research Laboratory which allows a LAN to be IP mobile when it attaches to a foreign IP-based network and uses this network as a means to retain connectivity to its home network. This technique is a form of virtual private networking which enables a LAN to roam on the Internet. In this report, we describe implementation of selective routing for the Mobile IP LAN technique in order to improve network communications for a mobile LAN. The selective routing implementation performs network address translation to route selected network application packets based on IP address (layer 3 address) or transport identifier (layer 4 port) through the foreign network. All other traffic is tunneled to the home network for routing, as in the conventional implementation of Mobile IP LAN. This improves the network latency for those applications that do not specifically require the IP and transport layers to be intact. To evaluate the performance of the Mobile IP LAN with selective routing technique, we have implemented the following three different scenarios in which we vary the Internet connection of Mobile LAN: direct LAN-to-LAN connection at the home network, connection at a foreign network using the secure mobile IP LAN technique, and connection at a foreign network using the secure Mobile IP LAN with selective routing technique. We compare the data rates of file transfers between a node on the mobile LAN and a node on the Internet in these three cases.

15. SUBJECT TERMS
Routing, mobile IP LAN, mobile IP, VPN, secure tunnel, OpenSSH

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			Brian B. Luu
Unclassified	Unclassified	Unclassified	UL	18	19b. TELEPHONE NUMBER (*Include area code*) (301) 394-3102

Standard Form 298 (Rev. 8/98)
Prescribed by ANSI Std. Z39.18

Contents

List of Figures

List of Tables

1. Introduction

The U.S. Army Research Laboratory (ARL) has developed and tested the Mobile Internet Protocol (IP) Local Area Network (LAN) protocol to support mobility for the Army digital battlefield. The Mobile IP LAN technique (*1*) allows a LAN to be IP mobile without modification of its LAN IP configuration (such as IP address, network mask, broadcast address, etc.). Only the LAN default gateway (router) needs to adjust to accommodate the change in network connection. When the mobile LAN moves to a new location, a foreign network, Mobile IP LAN requires the mobile router (mobile LAN default gateway) to acquire an IP address at the foreign network in order to retain network connectivity for the entire LAN. To protect the network traffic of the mobile LAN traversing between the foreign network and the home network of the mobile LAN, we use Open Secure Shell (OpenSSH) software, a freeware version of Secure Shell (SSH) (*2*). By taking advantage of strong encryption, authentication, and tunneling (port forwarding) of the OpenSSH software, we create a secure tunnel to channel the network traffic of the mobile LAN between the mobile router and the home agent (a special node at the home network to redirect the mobile LAN network traffic). Therefore, the Mobile IP LAN with OpenSSH technique just described is an implementation of a virtual private network (VPN) for a mobile LAN to roam the Internet.

In the Mobile IP LAN with OpenSSH technique, all mobile LAN network traffic is tunneled back to the home network where it is routed to the Internet. Since all mobile LAN network traffic still originates from the home network, the mobile LAN appears as part of the home network, although realistically, it is at a new location. Thus, the tunneling process is the main cause of delay for the network traffic of a mobile LAN using the Mobile IP LAN with OpenSSH technique. In this report, we demonstrate the use of selective routing at the mobile LAN default gateway (mobile router) to improve mobile LAN network communication. The selective routing implementation allows the mobile router to make efficient use of network resources by translating (network address and port translation) network traffic for those applications that do not specifically require the intactness of the IP and transport layers. All other traffic is tunneled to the home network for routing, as in the conventional implementation of the Mobile IP LAN technique. This technique improves network latency for the mobile LAN network traffic that is not tunneled back to the home network.

2. Background

2.1 Mobile IP LAN With OpenSSH

In general, a LAN accesses the Internet through a default gateway (router), as in a normal LAN-to-LAN connection at its home network (as shown in figure 1).

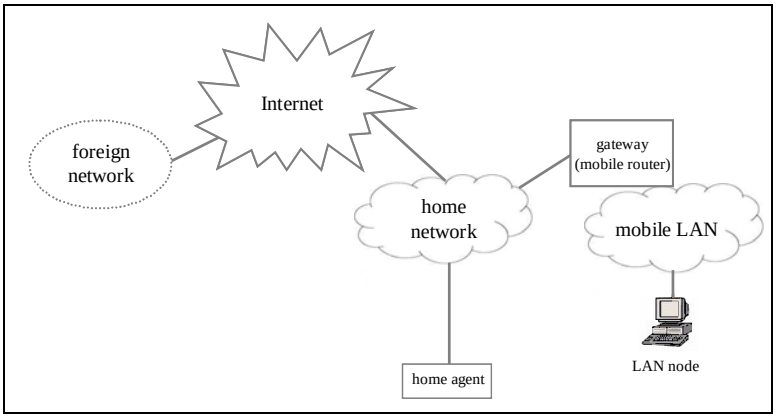

Figure 1. Mobile LAN at its home network.

When the LAN, including its default gateway, moves to a different location (termed a "foreign network") and acquires a new connection to the Internet, all intra-LAN connectivity still behaves normally. However, the in-bound traffic for the LAN continues to be routed on the Internet to its home network (the autonomous system where the LAN belongs). Normally, this change in the LAN gateway connection results in the loss of all LAN Internet traffic. To maintain Internet connectivity, the LAN gateway (termed the "mobile router") uses the new Internet connection acquired at the foreign network to establish a link to a special node at the home network (termed the "home agent") and to request that its in-bound Internet traffic be forwarded to the LAN at its new Internet connection. The home agent accepts the inbound traffic for the LAN and routes it through a network tunnel (such as a layer 3 network tunnel [IP tunnel] (*3*) or a layer 4 network tunnel) using an encapsulation mechanism, with the destination address at the new Internet connection of the mobile router. The out-bound traffic of the LAN can be routed normally through the foreign network connection to the Internet (if the foreign network allows this) or through another tunnel from the mobile router to the home agent. Figure 2 shows the network communication of the mobile LAN when it connects to a foreign network.

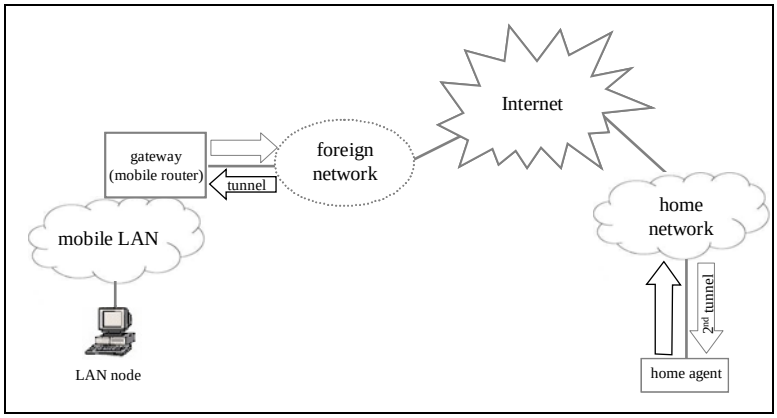

Figure 2. Mobile LAN using Mobile IP LAN at a foreign network.

In brief, to maintain Internet connectivity when the LAN is away from its home network, the network traffic of the LAN is redirected through tunnels whose end nodes are the home agent and the mobile router. The Mobile IP LAN protocol implementation is based on this concept. It requires two special nodes (a home agent and a mobile router) equipped with network routing software, tunneling software, and an IP address on the foreign network. All other LAN nodes become IP mobile without reconfiguration.

Thus, when IP mobile, a mobile LAN's tunneled network traffic must traverse one or more foreign networks that may not be trusted. This traffic could be subject to eavesdropping, interception, modification, or redirection by malicious nodes in these foreign networks. To protect network traffic passing through the tunnels, we use the port-forwarding feature provided by OpenSSH to provide a secure, bi-directional tunnel to carry the mobile LAN network traffic between the mobile router and the home agent. Port forwarding inherently takes advantage of the data encryption and data integrity features of OpenSSH to safeguard data flowing through the tunnel. OpenSSH also provides authentication that allows the mobile router and home agent to safely validate one another. Since OpenSSH software is found in the public domain, is available for most current operating systems, and is commonly used to provide secure network communications, it is the software of choice. Figure 3 depicts a general overview of the operation of a mobile LAN using the Mobile IP LAN with OpenSSH technique when at a foreign network.

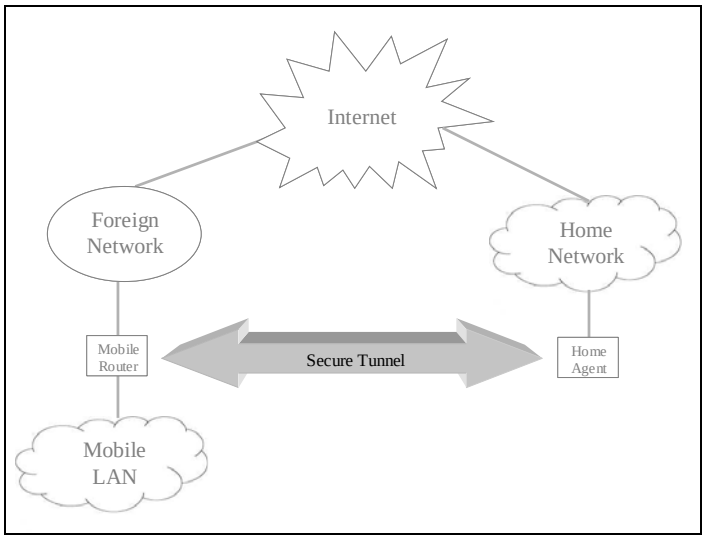

Figure 3. Mobile IP LAN with OpenSSH.

As previously described, the port-forwarding feature of OpenSSH provides a secure tunnel between the mobile router and home agent. To use this tunnel, a mechanism is necessary on both the mobile router and home agent systems that will pass all non-local mobile LAN traffic to the secure tunnel (port forwarded by OpenSSH). To implement this mechanism, we use the freeware TUN/TAP device driver (*4*), available on the Linux, FreeBSD, and Solaris platforms to create a virtual network device. The mobile LAN network traffic can then be routed to this virtual device. An in-house ARL-developed program, STIP (Secure Tunnel Interface Program), reads network packets from the virtual device and passes them to the secure tunnel (*5*). The use of the combined virtual network device and STIP program is necessary on both the mobile router and home agent systems to properly implement the Mobile IP LAN with OpenSSH technique. In the remainder of this report, we refer to the Mobile IP LAN with OpenSSH technique as the secure Mobile IP LAN technique.

2.2 IP Masquerading

IP Masquerading is a technique of mapping many IP addresses of an internal realm (usually IP addresses of one or more internal LANs) to one IP address of an external realm (usually a routable IP address of an external LAN connected to the Internet). The mapping only occurs for network traffic moving between the internal and external realms and allows internal packets to be routed on the external network. To uniquely identify packets through the many-to-one mapping, the transport identifier (i.e., TCP [transport control protocol] port numbers, UDP [user datagram protocol] port numbers, or ICMP [Internet control message protocol] identifiers) of mapped IP addresses is translated to a unique transport identifier of the mapping IP address. For the in-bound network traffic, the unique translation of the transport identifier done for the out-bound traffic helps to uniquely re-map the destination IP address of packets from a single external IP address to many internal IP addresses. Because of the address and port translation functionality, IP Masquerading is also regarded as network address port translation (NAPT),

which is a form of traditional network address translation (NAT) or out-bound NAT (*6*). Since the NAPT technique involves changing both the IP address and transport identifier of the packet, some Internet applications that require the use of the exact transport identifier or the address and port embedded in the payload of the packet will not function properly. By translating many internal IP addresses as one external IP address, NAPT not only allows Internet access sharing among many internal network nodes but also provides limited Internet protection for internal nodes. Usually, the external nodes (Internet world) cannot initiate connections to internal nodes, but the reverse is true.

3. Selective Routing Technique, Test Results, and Discussion

3.1 Technique

As previously mentioned, when a mobile LAN moves to a foreign network and acquires an Internet connection at this network, the mobile LAN can use the secure Mobile IP LAN technique to securely tunnel the mobile LAN Internet traffic between the mobile router and home agent to provide Internet access for all nodes in the mobile LAN. Thus, the secure Mobile IP LAN technique allows all nodes in the mobile LAN to access the Internet while retaining their home network IP addresses and configuration. The drawback to this technique is that the tunneling process (a VPN technique) for the mobile LAN network traffic extends the communication path of the mobile LAN traffic by at least the length of the tunneling path. Also, the encryption and decryption of tunnel traffic requires additional CPU (central processing unit) processing on the mobile router and home agent systems. Therefore, the secure tunnel employed by the secure Mobile IP LAN technique provides Internet access for all mobile LAN nodes at the cost of increased network latency. A lengthy tunneling path or just one very slow connection in the tunneling path can result in a significant Internet access delay, which can cause some Internet applications to expire.

Since many Internet applications do not require the source IP address or transport identifier to be fixed or embedded in the network traffic of the application, IP Masquerading can be used to decrease the network latency for these Internet applications. Selected network traffic can be translated and routed directly to the Internet from the mobile router, while all other network traffic will continue to pass through the secure tunnel. This will result in an overall improvement in latency of mobile LAN network traffic since the selected network traffic will not be subject to the extended communication path of the secure tunnel. Therefore, to improve the network communication of the mobile LAN when at a foreign network, the mobile router should be implemented with the selective routing technique. This technique allows the use of secure tunneling and IP Masquerading, either individually or concurrently, to route the mobile LAN network traffic.

To implement the selective routing technique, we define a combination of rules in the firewall and routing components of the Linux operating system used by the mobile router. By default, the selective routing technique on the mobile router routes all non-local (gateway) network traffic of the mobile LAN to the secure tunnel. Only selected out-bound network traffic, identified by IP addresses or transport identifiers, is translated with the IP address associated with the mobile router Internet connection at the foreign network. Figure 4 shows a diagram of out-bound network traffic at the mobile router via the selective routing technique.

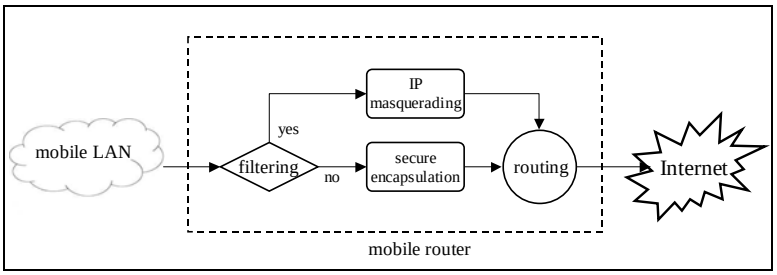

Figure 4. Mobile IP LAN with OpenSSH and selective routing.

3.2 Test Results

To measure the improvement in network performance achieved by using IP Masquerading versus tunneling alone at the mobile router, we conducted a data transfer experiment from a node on the mobile LAN to a node on the Internet during a time of low Internet usage. The Internet connection of the mobile LAN was varied as follows: direct LAN-to-LAN connection at the home network, connection at a foreign network using the secure Mobile IP LAN technique, and connection at a foreign network using the secure Mobile IP LAN with selective routing technique. The Internet node was connected via a commercial cable Internet service provider (ISP) network and therefore was limited in network bandwidth to 1.5 Mbps. All other network links were 10 Mbps or greater. We used Test TCP (TTCP), a freeware network performance evaluator (*7*), to measure the data transfer times for each of the three connection methods previously described. For each method, 10 MB of data were repeatedly transferred. The average data rates are shown in table 1.

Table 1. Average data rate for different connection types.

Mobile LAN Connection for Transferring 10 MB Data	**Average Data Rate (kbps)**
Direct LAN-to-LAN connection at the home network	1436.32
Secure Mobile IP LAN (secure tunneling)	1367.26
Secure Mobile IP LAN with selective routing (IP Masquerading)	1435.91

3.3 Discussion

The test results showed an improvement in the data rate of about 5% for the network traffic using IP Masquerading versus secure tunneling during a time of low Internet usage. The improvement would be more significant during a time of high Internet usage or if the tunnel path were bottlenecked by a very slow connection. The test also showed that the data rate of network traffic with the mobile router using IP Masquerading at a foreign network is comparable to the data rate of network traffic with the mobile router connected directly to the home network. Further, the comparison of data rates for the three methods will tend to favor the method using IP Masquerading if the destination node is on the foreign network. This is because IP Masquerading allows the mobile LAN network traffic to route directly onto the foreign network.

In fact, the selective routing technique combines two gateway techniques, secure tunneling (a VPN technique) and IP Masquerading, to route the Internet traffic of the mobile LAN at the mobile router. Secure tunneling is the default gateway technique for the mobile router so that the mobile LAN will always appear to be connected at the home network. Any network application traffic that does not require the IP and transport layers to be intact should be routed with the IP Masquerading technique to reduce network latency for those applications. This, in turn, will improve the overall network communication of the mobile LAN when at a foreign network. Each gateway technique has its advantages and disadvantages with respect to routing the gateway traffic (Internet traffic) of a LAN (*8*), and it is ultimately the choice of the operator who administers the mobile LAN connection at a foreign network to determine which techniques will be most beneficial for the mobile LAN.

Special care needs to be taken when IP Masquerading and secure tunneling are used concurrently in order to avoid network packet loss or misdirection. These situations may arise when there is a conflict in the use or purpose of the two gateway techniques. For example, assume that all telnet traffic for the mobile LAN is masqueraded by the mobile router and a telnet server exists within the mobile LAN. All client telnet traffic from the mobile LAN to the Internet will function properly through IP Masquerading. However, if a node on the Internet attempts to establish a telnet connection with the telnet server in the mobile LAN, the telnet connection request will reach the server node correctly through the secure tunnel, but, the connection acknowledgments sent by the telnet server on the mobile LAN will not return via the secure tunnel. Any out-bound mobile LAN telnet packets generated by the telnet server will be masqueraded and unresolved (un-referenced) at the end.

5. Conclusion

In summary, by combining two gateway techniques, VPN and IP Masquerading, the selective routing technique implemented on the mobile router of a mobile LAN allows the mobile LAN (including all of its nodes) to efficiently use network resources while connected to a foreign network. A simple adjustment of network filtering rules on the mobile router can alternate between the two gateway techniques for a selected network application used on the mobile LAN. Human intervention is still needed to oversee and optimize the network traffic of the mobile LAN when at a foreign network. A future development using information from a stateful firewall implementation at the mobile router can automatically adjust the selective routing technique to optimize the network traffic of the mobile LAN when it is roaming on the Internet.

6. References

1. Luu, B. A Prototype Implementation of Mobile IP LAN. *Proceedings of Advanced Telecommunications & Information Distribution Consortium of ARL Federated Laboratory 5th Annual Symposium*, pp. 211-215, March 2001.
2. Barrett, D.; Silverman, R. SSH, The Secure Shell: The Definitive Guide. O'Reilly & Associates, Inc., 2001.
3. Perkins, C. "IP Encapsulation within IP," RFC 2003, October 1996.
4. "Universal TUN/TAP Driver," <http://vtun.sourceforge.net/tun>.
5. Luu, B.; Gopaul, R. Using OpenSSH to Secure Mobile LAN Network Traffic. *Proceedings of SPIE AeroSense 2002*, Vol. 4741, pp. 54-61, April 2002.
6. Srisuresh, P.; Holdrege, M. "IP Network Address Translator (NAT) Terminology and Considerations," RFC 2663, August 1999.
7. "Test TCP (TTCP) Benchmarking Tool for Measuring TCP and UDP Performance," <http://www.pcausa.com/Utilities/pcattcp.htm>.
8. Luu, B.; Harrelson, H. R.; Gopaul, R. Mobile Gateway Techniques. *Proceedings of SPIE AeroSense 2001*, Vol. 4396, pp. 141-148, April 2002.

INTENTIONALLY LEFT BLANK.

Distribution

ADMNSTR
DEFNS TECHL INFO CTR
ATTN DTIC-OCP (ELECTRONIC COPY)
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

US ARMY ARDEC
ATTN AMSTA-AR-TD
BLDG 1
PICATINNY ARSENAL NJ 07806-5000

COMMANDING GENERAL
US ARMY AVN & MIS CMND
ATTN AMSAM-RD W C MCCORKLE
REDSTONE ARSENAL AL 35898-5000

US ARMY INFO SYS ENGRG CMND
ATTN AMSEL-IE-TD F JENIA
FT HUACHUCA AZ 85613-5300

US ARMY SIMULATION TRAIN & INSTRMNTN CMND
ATTN AMSTI-CG M MACEDONIA
12350 RESEARCH PARKWAY
ORLANDO FL 32826-3726

US ARMY RSRCH LAB
ATTN AMSRD-ARL-CI-OK-TP TECHL LIB T LANDFRIED (2 HC)
ABERDEEN PROVING GROUND MD 21005-5066

DIRECTOR
US ARMY RSRCH LAB
ATTN AMSRD-ARL-RO-EN W D BACH
PO BOX 12211
RESEARCH TRIANGLE PARK NC 27709

US ARMY RSRCH LAB
ATTN AMSRD-ARL-CI J GOWENS
ATTN AMSRD-ARL-CI-C
ATTN AMSRD-ARL-CI-CN G RACINE
ATTN AMSRD-ARL-CI-OK-T TECHL PUB (2 COPIES)
ATTN AMSRD-ARL-CI-OK-TL TECHL LIB (2 COPIES)
ATTN AMSRD-ARL-D J M MILLER
ATTN AMSRL-CI-CN B LUU (3 COPIES)
ATTN AMSRL-CI-SD R GOPAUL (2 COPIES)
ATTN IMNE-ALC-IMS MAIL & RECORDS MGMT
ADELPHI MD 20783-1197

INTENTIONALLY LEFT BLANK.