INTERNET DRAFT
Category:
Title: draft-mccann-thema-00.txt
Date: March 1999

Pete McCann
Tom Hiller
Jin Wang
Alessio Casati
Lucent Technologies
Charles E. Perkins
Pat R. Calhoun
Sun Laboratories, Inc

Transparent Hierarchical Mobility Agents (THEMA)

draft-mccann-thema-00.txt

Status of this Memo

This document is an Internet Draft and is in full compliance with all provisions of Section 10 of RFC2026.

Internet Drafts are working documents of the Internet Engineering Task Force (IETF), its Areas, and its Working Groups. Note that other groups may also distribute working documents as Internet Drafts.

Internet Drafts are draft documents valid for a maximum of six months. Internet Drafts 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".

The list of current Internet Drafts can be accessed at http://www.ietf.org/ietf/1id-abstracts.txt

The list of Internet Draft Shadow Directories can be accessed at http://www.ietf.org/shadow.html.

Abstract

For various reasons it may be desirable to separate the functionality of a mobility agent, such as the home and foreign agents in Mobile IP [Perkins96], from their link-layer presence on a given network. This draft outlines mechanisms based on the Tunnel Establishment Protocol [Calhoun98a] for accomplishing this. The tunnels so established will not be visible to a mobile node and therefore provide a transparent way to build hierarchies of mobility agents, which can lessen the frequency of Mobile IP re-registrations.

1. Introduction

The Mobile IP protocol [Perkins96] and its extensions define the notions of Home Agent (HA) and Foreign Agent (FA) and assume that the FA is deployed with link-layer connectivity to some visited network and the HA is deployed with link-layer connectivity to some home network. For various reasons, carriers who actually deploy such agents may wish to separate the agent's functionality from the link-layer presence on the proper network. This may allow the agent functionality to be shared over a wider area, which could lower the cost of deployment. Service providers may also have administrative or other reasons for centralizing mobile agent functionality.

For example, market forces may drive a carrier to buy equipment that terminates the link-layer from one vendor and hardware that implements FA functionality from another. Alternatively, a carrier may wish to deploy an FA near its controlling authentication, authorization, and accounting (AAA) server for security reasons, which could place it far from the actual links on which mobile nodes will connect. Also, by creating networks of surrogate agents in a foreign network, a carrier can form a hierarchy that lessens the frequency of Mobile IP registrations. By confining local mobility events to the local carrier network, handoff can often be completed without waiting for a round-trip through the Internet and the associated cryptographic AAA processing. Also, the computational burden on FAs and HAs will be reduced. This is possible using THEMA because after a local handoff, tunnels can often be established back to a common ancestor in the hierarchy of surrogate agents or to the original FA, obviating the need for Mobile IP re-registration.

A home network may also desire to position an HA several network hops away from a MNs home link. This may be so that the HA can be co-located with AAA functionality just behind a firewall. The actual presence on the home link can be supported by a surrogate home agent that complies exactly with basic Mobile IP [Perkins96] and need not interact with a AAA server. This option might be attractive to a private network operator with an installed base of basic Mobile IP home agents who, with the addition of a special home agent at the firewall, wishes to provide service to users roaming outside the firewall. This draft describes such a scenario and shows how an HA can interact with a surrogate agent to provide transparent access to the home link.

To accomplish separation of the link-layer termination point from mobility agent functionality, this draft draws on ideas from the

Tunnel Establishment Protocol [Calhoun98a]. It allows the link-layer termination point to play the role of a surrogate agent, which tunnels packets to the real mobility agent and de-tunnels packets that arrive from the mobility agent. To the agent software at the mobility agent itself, the tunnel endpoint should appear to be a link-layer address to which packets can be sent or from which packets may be received. The creation of the tunnel is completely

transparent to mobile nodes (MNs), which means it can be deployed without changing the Mobile IP client software to be aware of the hierarchies, as is the case in other proposals [Calhoun98b]. Also, we support the use of private, potentially overlapping addresses with an FA-located care-of address, which is not a capability of [Valko98].

THEMA can be the basis for the design of an access network between MNs and FAs. When deployed in this manner, THEMA tunnels are established immediately after the MNs link-layer connection is brought up, and before any Mobile IP registration or agent solicitation messages are sent. They provide the MN and FA with the illusion of direct, link-layer connectivity, although this connectivity is actually via one or more GRE tunnels that each potentially span several network routing hops. Because the tunnels are established using only information available at link establishment time, there is no interaction between THEMA establishment and the subsequent Mobile IP registration messages. After THEMA tunnels are established, the MN and FA may engage in Mobile IP registration as normal. Solicitations, Registrations, and Replies are carried through the GRE tunnel in the same way as any other IP packets between the MN and FA.

While THEMA tunnels do preserve link-layer information, they carry only network-layer packets, not link-layer frames. THEMA assumes that the link-layer will be terminated as early as possible in a carrier network, in order to support the tight integration needed to support quality of service guarantees over potentially complex wireless media types. THEMA provides a degree of separation between the mobility agent functionality and the specific link-layer technology used and allows packets in tunnels to be reordered by intervening routers. THEMA is therefore a more natural choice for standardization compared to proposals that tunnel link-layer frames [Valencia98].

The keywords MUST, MUST NOT, REQUIRED, SHALL, SHALL NOT, SHOULD, SHOULD NOT, RECOMMENDED, MAY, and OPTIONAL, when they appear in this document, are to be interpreted as described in RFC 2119 [Bradner97].

1.1 Terminology

Mobile Node (MN)
As in Mobile IP [Perkins96].

Correspondent Node (CN)
As in Mobile IP [Perkins96].

Home Agent (HA)
As in Mobile IP [Perkins96].

Foreign Agent (FA)
As in Mobile IP [Perkins96].

Surrogate Agent (SA)
A mobility agent that is neither a home nor a foreign agent. In this draft, SAs will be placed between the MNs link-layer termination point and the FA, and between the HA and the home link.

Authentication, Authorization, and Accounting (AAA) Server
A server implementing a protocol such as DIAMETER [Calhoun98c] which can authenticate users and serve as a repository for accounting information.

2. Architectural Assumptions

We assume that the MN has a link-layer connection to some entity in the carrier network. Also, this entity is one or more network hops away from a node that implements foreign agent functionality. This scenario is depicted in Figure 1.

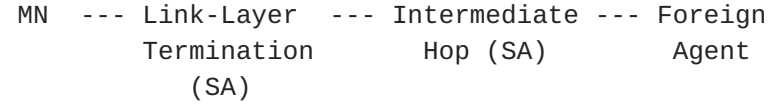


Figure 1. The MNs link-layer is terminated at a point distant from the FA.

The nodes marked SA will play the role of Surrogate Agents, a term borrowed from [Calhoun98a] which is usually applied to nodes between the FA and HA but here is applied to nodes between the MN and FA and between the HA and home link. We assume that a MN connects to the first hop SA through means specific to the given link-layer

technology used. In a cellular environment, for instance, this would mean connecting via a base-station to some Inter-Working Function; in a wireless LAN environment, it might mean simply wandering into the coverage area of some wireless LAN device.

Similarly, the home agent may be located one or more network hops away from the home link, as depicted in Figure 2.

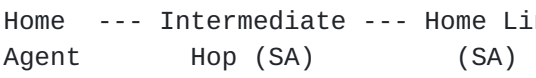


Figure 2. The MNs home link is distant from the HA functionality.

We assume that the SAs in Figure 1 belong to the same administrative domain as the FA, and that the SAs in Figure 2 belong to the same administrative domain as the HA. As we will see below, this simplifies the registration process because there may be pre-

arranged security associations between these entities. Also, authentication of the registration messages outlined in this draft may not be necessary at all because the tunnel establishment happens between entities in a mutual trust relationship. These assumptions allow us to place the burden of authentication of Mobile IP registration messages originating from the MN on the actual FA and HA. These mobility agents can offload this task to AAA servers which are suitably connected via a roaming consortium, but the SAs will not necessarily require any such AAA service and do not need any authenticated access identifiers from the MN.

3. Summary of Operation

The goal of THEMA is to provide transparent link-layer connectivity between a MN and FA and between the HA and home link. THEMA is based on Mobile IP [Perkins96] with some of the extensions from TEP [Clahoun98a].

When a MN arrives in a visited network, that network transparently establishes a tunnel from the MNs attachment point back to an FA. The first-hop SA where the link-layer is terminated begins the process by setting up a tunnel to its neighbor SA or directly to the FA, passing along any link-layer identification information. This creates a chain of tunnels, each of which carries a Tunnel Identifier that can be used to distinguish traffic from a given MN.

The use of THEMA on the home network is triggered by receipt of a successful Mobile IP Registration Request at the HA sitting at the

boundary of the home network. It establishes a tunnel back to the home link, which may be separated by several network hops. The SA sitting on the home link then forwards packets from the home network back to the HA and receives packets from the HA which it decapsulates and delivers. This gives the HA a virtual presence on the home link.

We will describe each leg of operation separately, beginning with the MN - FA connection and finishing with the HA - home link.

3.1 MN - FA

In what follows, we will use the term "upstream" to refer to nodes closer to the FA and the term "downstream" to refer to nodes closer to the MN.

First, assume the MN opens a link-layer connection to the first hop SA in Figure 1. If the link is connection oriented, the SA will have an immediate indication that the MN is present. Otherwise, the SA may need to use lower layer indications or simply wait for the first message from the MN, such as a Mobile IP Agent Solicitation. The SA should now have available some kind of link-layer address,

such as the IMSI of a mobile phone or the hardware address of an Ethernet adapter. The SA then establishes a tunnel to another SA (the Intermediate Hop in Figure 1) or to the FA itself by sending a Registration Request. The choice of intermediate node or FA may be static or dynamic. This is essentially a routing problem, where the SA must find the next hop on a path to some FA which is "good" according to some metric which may involve hop count, frequency of registration messages, and load balancing considerations. The exact mechanism for discovering or maintaining routes is outside the scope of this draft. If the FA function were available at the link-layer termination point, a simpler solution would be to use a regionalized registration approach [Calhoun98b].

Registration Request messages are sent over UDP to port 434, and formatted as in basic Mobile IP. When sent from an SA to an FA or intermediate SA, the 'S' bit MAY be set, indicating simultaneous registrations; the 'G' bit MUST be set, indicating GRE encapsulation; all other flag bits MUST be set to '0'. The Home Address field SHOULD be set to zero (0.0.0.0). This field is not needed by THEMA and should be ignored by the receiver. The Home Agent field MUST be set to the recipient's IP address, and the Care-of Address field MUST be set to the sender's IP address. In a Link-Layer Address extension to the Registration Request, the SA SHOULD

identify the link-layer address information it has for the MN. Also, the SA MUST use the Tunnel Identifier extension, setting the first 16 bits to a locally unique value. The Lifetime field SHOULD be set to an appropriate number of seconds.

Upon reception of a Registration Request, the receiving SA or FA determines if this is a new tunnel or a refresh of an old tunnel. A refresh of an old tunnel can be detected by looking for an existing tunnel with the same downstream SA address, the same 16 most significant bits in the Tunnel Identifier field, and the same Link-Layer Address extension in the Registration Request. If this is a new tunnel, the SA or FA MUST complete the Tunnel Identifier extension with a locally unique 16 bit number, and create a new tunnel endpoint. Otherwise, the SA or FA MUST continue to use the same Tunnel Identifier and tunnel endpoint. In either case the SA or FA notes the requested Lifetime, sets an expiration timer for the tunnel, and immediately sends a Registration Response to the SA that sent the Registration Request. Success or failure of the registration can be indicated as in Mobile IP [Perkins96]. The Reply MUST have its Home Agent field set to the sender's address and SHOULD have the Home Address field set to zero (0.0.0.0). Again, the Home Address field is not needed by THEMA and should be ignored.

If this is a new tunnel, an Intermediate Hop SA then immediately sends a Registration Request to the next upstream SA or FA, containing an appropriate Lifetime. Otherwise, the Intermediate Hop SHOULD merely refresh the upstream tunnel as needed while downstream tunnels are active. Tunnels are refreshed by sending a new Registration Request with an appropriate Lifetime field. By

adjusting the Lifetime fields used by each layer of a hierarchy, a carrier can adjust the frequency of re-registration. In general nodes closer to the FA should use longer Lifetimes, as these tunnels are expected to be more stable.

An SA will then have established one link in a chain of concatenated tunnels, and begins to serve as a forwarding point for traffic. Packets originating from the MN are encapsulated by the first SA in a GRE tunnel to the next hop agent using the Tunnel Identifier that was negotiated. If the next hop is also an SA, it maps the incoming Tunnel Identifier to an outgoing Tunnel Identifier and agent IP address, and re-encapsulates the packet in a GRE header containing the new tunnel identifier. Finally, if the next hop is an FA, it decapsulates the packet and processes it exactly as if it had been received on a local link.

If the 'S' bit was set in the Registration Request, a given agent

may have more than one downstream tunnel opened for a given link-layer address at a time. Any packets that arrive on either downstream tunnel should be forwarded to the same upstream tunnel, and packets that arrive on the corresponding upstream tunnel should be "forked" and a duplicate packet sent to each downstream tunnel.

If the first hop SA has an indication that the link-layer connection to the MN has been disconnected, and after waiting a sufficient amount of time for the MN to reconnect, the upstream tunnel SHOULD be torn down by sending a new Registration Request with a Lifetime of 0. As with all Registration Requests, the SA retransmits the request as necessary, waiting for a Registration Reply acknowledging the tunnel tear-down. Lack of a reply after several retransmissions may indicate that the upstream node has crashed in which case the tunnel MAY be torn down and an error MUST be logged.

If all downstream tunnels corresponding to a given link-layer address are torn down by the downstream SAs, this indicates that the MN has disconnected. The first hop SA MAY also use idle timers to detect that a MN has disconnected, which may be the only mechanism available if the MN is using a connectionless medium. In either case the upstream tunnel SHOULD be torn down as specified above.

If a downstream tunnel's lifetime expires without the receipt of any new Registration Requests, it may indicate that the downstream node has crashed. In this case the downstream tunnel MAY be torn down without notification of the downstream node and an error MUST be logged. If this is the last downstream tunnel corresponding to a given link-layer address, the corresponding upstream tunnel MUST then be torn down as specified above.

The first hop SA should monitor the Lifetime of the tunnel. When it is about to expire, but the SA has an indication that the MN is still connected, it MUST initiate a tunnel refresh operation by

sending a new Registration Request upstream with an appropriate Lifetime.

Disconnection of a link-layer tunnel at the FA MUST NOT trigger expiration of the corresponding Mobile IP binding. Expiration of this binding should occur as specified in RFC 2002 [Perkins96]. The MN may simply have left the coverage area momentarily and may reappear soon, perhaps at a different SA. The FA should be able to recognize the link-layer address as matching the existing binding and should begin forwarding datagrams along the new tunnel.

Depending on the medium type connecting the MN to the first hop SA,

link-layer specific procedures may be necessary to complete the illusion of direct connectivity to the FA. For example, an Ethernet deployment would require the SA to implement Proxy ARP on behalf of the FA.

3.2 HA - Home Link

In addition to separating the FA from the visited link, there may also be reasons to separate the HA from the home link. For instance, the HA may sit just behind a firewall, while the home link is distant by several IP routing hops. However, putting intervening tunnel endpoints between the HA and the home link, analogous to the Intermediate Hops in the foreign network case, is not likely to be useful, because the HA is not likely to change over the course of the data session. Therefore, we consider only the case of direct interaction between the HA and the SA, the latter of which is assumed to be directly connected to the MN's home link.

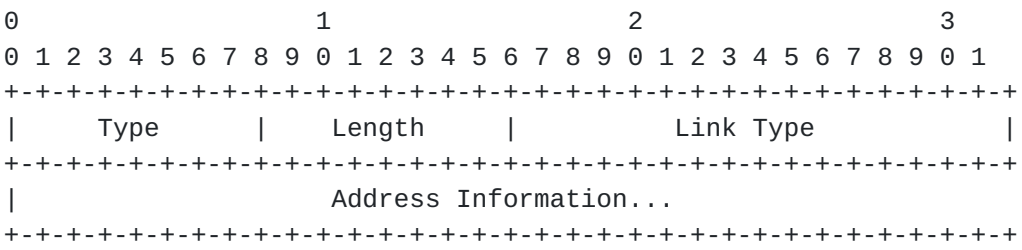
First, assume that the MN sends a Mobile IP Registration Request to the HA. Assuming that the registration is otherwise successful, the HA must arrange to intercept packets destined to the MN home address. Normally this is impossible if the HA is not co-located on the MNs home link. However, this can be accomplished with the use of an SA on the home link. The HA sends a Registration Request to the SA. The 'S' bit must be set, and the 'B' bit must be set if and only if the corresponding bit was set in the original Mobile IP Registration Request from the MN. The other flag bits may or may not be set depending on the scenario in which the HA and SA are deployed. The Home Address may be zero if the address is to be allocated by the home-link SA, but must be the home address of the MN otherwise. The Home Agent field must be set to the address of the SA. The Care-of address must be set to the internal address of the HA. Upon receipt of the request, the SA allocates an address, if necessary, sends a Registration Response, and begins to intercept packets destined for that address and forward them to the HA. The Response must have a Home Agent address set to the SA's address, and the Home Address field must be set to the address of the MN.

De-registrations, retransmissions, and time-outs should be handled as in Mobile IP [Perkins96].

4. Link-Layer Address Extension

This draft defines a new extension for use in THEMA Registration

Request messages. This extension is not intended for use in Registration Requests that originate from MNs; it should appear only in the surrogate registrations sent from SAs. Within this extension, we define two possible link-layer address formats. Additional message types may be defined in the future for other link-layer technologies.



Type

TBD - Link-Layer Address

Length

Indicates the total length (in octets) of the Link Type and Address Information fields.

Link Type

Indicates the type of address contained in the Address Information field. Allowed values are:

TBD - Ethernet address
TBD - International Mobile Station Identifier (IMSI)

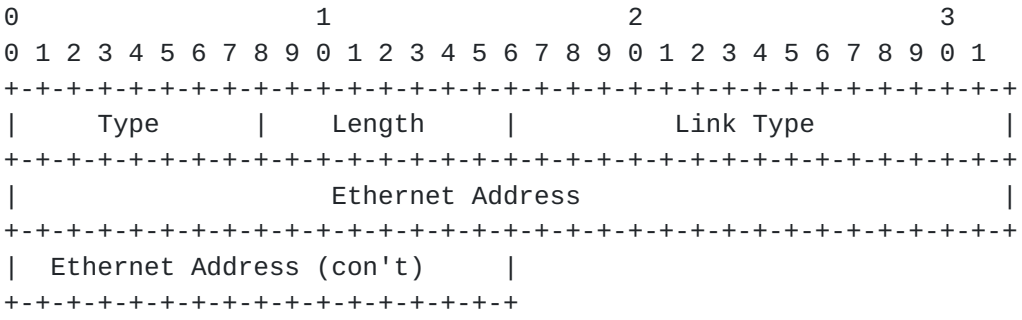
Address Information

A variable length sequence of octets representing the link-layer address of the MN on behalf of whom this tunnel is being requested.

Below we define formats for several specific instances of link-layer technologies, but it is not necessary for the FAs or SAs (except for the first hop SA that actually terminates the link-layer) to understand the semantics of a given link-layer or the encapsulation formats of that link-layer. The agent can simply use the tuple (Link Type, Address Information) as an opaque identifier that uniquely identifies a MN interface.

4.1 Ethernet Address Extension

Ethernet hardware addresses are 48-bit numbers uniquely identifying an Ethernet adapter. This extension applies to both wired and wireless Ethernet.



Type

TBD - Link-Layer Address

Length

8 (0x08)

Link Type

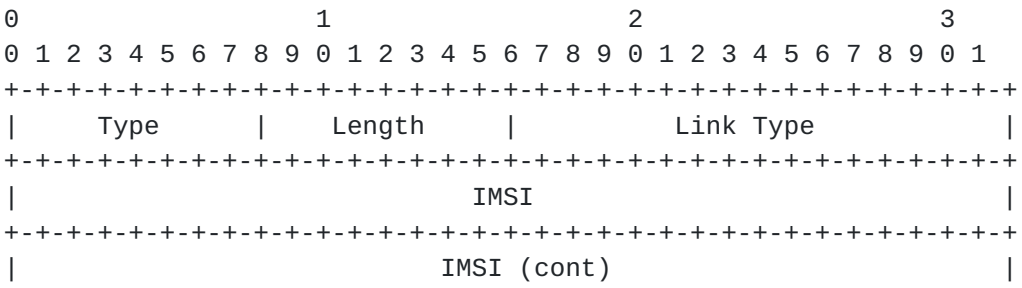
TBD - Ethernet address

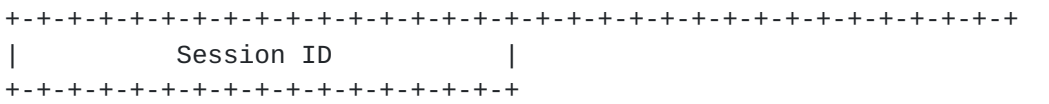
Address Information

The six octet Ethernet address being used by the MNs Ethernet adapter.

4.2 International Mobile Station Identifier (IMSI) Extension

Mobile cellular telephones and data-only devices designed to connect to the global cellular infrastructure are expected to be uniquely identified by their IMSI. This identifier may be either 40, 50, or 56 bits in length, depending on whether the underlying technology is CDMA, TDMA, or GSM.





Type

TBD - Link-Layer Address

Length

12 (0x0c)

Link Type

TBD - International Mobile Station Identifier (IMSI)

Address Information

This is the 40, 50, or 56 bit number which identifies a cellular telephony device. The IMSI field is padded with leading zeros, so the LSB of the IMSI is always the 64th bit.

Session ID

Because many cellular technologies can accommodate multiple open sessions simultaneously, this extra two bytes of information is included to distinguish them. When a MN moves to a new SA, each virtual link-layer interface on the MN should retain the same session ID. This ID may be inferred from technology-dependent procedures when the MN connects to the new SA or it may be supplied explicitly by the MN, such as during link-layer negotiation. The exact means is outside the scope of this draft.

5. Security

Mechanisms for ensuring that a given MN actually does possess a given link-layer address are particular to each technology and are outside the scope of this document. THEMA provides only the amount of security given by the underlying link-layer, and it is up to the FA to carry out network-layer authentication. If a given technology permits either "snooping" or "spoofing" of link-layer addresses, then higher security may be obtained by network-layer encryption between the MN and FA.

Throughout this document, we assume that the FA and HA will be connected to AAA servers, which will process NAI Extensions as

outlined in [Calhoun98d], but that this will not be necessary for the SAs. They may be configured with static security associations

or no security at all, provided they are in a protected part of a private network.

6. Discussion

The proposal outlined here preserves the link-layer address information through several hops all the way back to the FA. These addresses do not actually appear in tunneled packets; the Tunnel Identifier key acts as a replacement. Essentially, the MN is given a link-layer connection to the FA that is independent of any particular link-layer technology. This has advantages over other layer-2 tunneling schemes, such as L2TP [Valencia98], that are tied to PPP. Also, because the tunneled datagrams are IP packets, not layer-2 frames, we don't need to include sequence numbers. Packets can be re-ordered to support Quality of Service requirements.

No new extensions were necessary for the successful separation of the HA from the SA on the home link. This case is very similar to the base Mobile IP protocol and in fact the home link SA can comply completely with the requirements for a home agent laid out in basic Mobile IP [Perkins96].

7. References

[Calhoun98a] Calhoun, Montenegro, Perkins, "Tunnel Establishment Protocol", draft-ietf-mobileip-calhoun-tep-01.txt, March 1998. Work In Progress.

[Calhoun98b] Calhoun, Montenegro, Perkins, "Mobile IP Regionalized Tunnel Management", draft-ietf-mobileip-reg-tunnel-00.txt, November 1998. Work In Progress.

[Calhoun98c] Calhoun, Rubens, "DIAMETER Base Protocol", draft-calhoun-diameter-04.txt, July 1998. Work In Progress.

[Calhoun98d] Calhoun, Perkins, "DIAMETER Mobile IP Extensions", draft-calhoun-diameter-mobileip-01.txt, November 1998. Work In Progress.

[Perkins96] C. Perkins, Editor, "IP Mobility Support", RFC 2002, October 1996.

[Valencia98] Valencia, Hamzeh, Rubens, Kilar, Littlewood, Townsley, Taarud, Pall, Palter, Verthein, "Layer Two Tunneling Protocol (L2TP)", draft-ietf-pppext-l2tp-12.txt, October 1998. Work In Progress.

[Valko98] Valko, Campbell, Gomez, "Cellular IP", draft-valko-cellularip-00.txt, November 1998. Work In Progress.

8. Author's Addresses

Questions about this memo can be directed to:

Peter J. McCann
Lucent Technologies
Rm 2Z-305
263 Shuman Blvd
Naperville, IL 60566
USA
email: mccap@lucent.com
phone: +1 630 713 9359
fax: +1 630 713 4982

Tom Hiller
Lucent Technologies
Rm 2F-218
263 Shuman Blvd
Naperville, IL 60566
USA
email: tomhiller@lucent.com
phone: +1 630 979 7673
fax: +1 630 713 3663

Jin Wang
Lucent Technologies
Rm 1Q-305
1000 E Warrenville Rd
Naperville, IL 60566
USA
email: jinwang@lucent.com
phone: +1 630 713 5292
fax: +1 630 979 3983

Alessio Casati
Lucent Technologies
Sigma Building
Windmill Hill Business Park

Wiltshire, SN5 6P
United Kingdom
email: acasati@lucent.com
phone: +44 179388 3861

Charles E. Perkins
Sun Laboratories, Network and Security Research Center
Sun Microsystems, Inc.
15 Network Circle
Menlo Park, CA 94025
USA
email: charles.perkins@eng.sun.com
phone: +1 650 786 6464

fax: +1 650 786 6445

Pat R. Calhoun
Sun Laboratories, Network and Security Research Center
Sun Microsystems, Inc.
15 Network Circle
Menlo Park, CA 94025
USA
email: pcalhoun@eng.sun.com
phone: +1 650 786 7733
fax: +1 650 786 6445