   Mobile IP Authentication, Authorization, and Accounting Requirements

Status of this Memo

Copyright Notice

Abstract

   The Mobile IP and Authentication, Authorization, Accounting (AAA)
   working groups are currently looking at defining the requirements for
   Authentication, Authorization, and Accounting. This document
   contains the requirements which would have to be supported by a AAA
   service to aid in providing Mobile IP services.

1. Introduction

   Clients obtain Internet services by negotiating a point of attachment
   to a "home domain", generally from an ISP, or other organization from
   which service requests are made, and fulfilled. With the increasing
   popularity of mobile devices, a need has been generated to allow
   users to attach to any domain convenient to their current location.
   In this way, a client needs access to resources being provided by an
   administrative domain different than their home domain (called a
   "foreign domain"). The need for service from a foreign domain
   requires, in many models, Authorization, which leads directly to
   Authentication, and of course Accounting (whence, "AAA"). There is
   some argument which of these leads to, or is derived from the others,
   but there is common agreement that the three AAA functions are
   closely interdependent.

An agent in a foreign domain, being called on to provide access to a
resource by a mobile user, is likely to request or require the client
to provide credentials which can be authenticated before access to
resources is permitted. The resource may be as simple as a conduit
to the Internet, or may be as complex as access to specific private
resources within the foreign domain. Credentials can be exchanged in
many different ways, all of which are beyond the scope of this
document. Once authenticated, the mobile user may be authorized to
access services within the foreign domain. An accounting of the
actual resources may then be assembled.

Mobile IP is a technology that allows a network node ("mobile node")
to migrate from its "home" network to other networks, either within
the same administrative domain, or to other administrative domains.
The possibility of movement between domains which require AAA
services has created an immediate demand to design and specify AAA
protocols. Once available, the AAA protocols and infrastructure will
provide the economic incentive for a wide-ranging deployment of
Mobile IP. This document will identify, describe, and discuss the
functional and performance requirements that Mobile IP places on AAA
protocols.

The formal description of Mobile IP can be found in [13,12,14,17].

In this document, we have attempted to exhibit requirements in a
progressive fashion. After showing the basic AAA model for Mobile
IP, we derive requirements as follows:

- requirements based on the general model
- requirements based on providing IP service for mobile nodes
- requirements derived from specific Mobile IP protocol needs

Then, we exhibit some related AAA models and describe requirements
derived from the related models.

2. Terminology

This document frequently uses the following terms in addition to
those defined in RFC 2002 [13]:

   Accounting   The act of collecting information on resource usage
                for the purpose of trend analysis, auditing, billing,
                or cost allocation.

Administrative Domain
          An intranet, or a collection of networks, computers,
          and databases under a common administration.
          Computer entities operating in a common
          administration may be assumed to share
          administratively created security associations.

Attendant   A node designed to provide the service interface
             between a client and the local domain.

Authentication
          The act of verifying a claimed identity, in the form
          of a pre-existing label from a mutually known name
          space, as the originator of a message (message
          authentication) or as the end-point of a channel
          (entity authentication).

Authorization
          The act of determining if a particular right, such as
          access to some resource, can be granted to the
          presenter of a particular credential.

Billing   The act of preparing an invoice.

Broker   An intermediary agent, trusted by two other AAA
             servers, able to obtain and provide security services
             from those AAA servers. For instance, a broker may
             obtain and provide authorizations, or assurances that
             credentials are valid.

Client   A node wishing to obtain service from an attendant
             within an administrative domain.

Foreign Domain
          An administrative domain, visited by a Mobile IP
          client, and containing the AAA infrastructure needed
          to carry out the necessary operations enabling Mobile
          IP registrations. From the point of view of the
          foreign agent, the foreign domain is the local
          domain.

Inter-domain Accounting
          Inter-domain accounting is the collection of
          information on resource usage of an entity with an
          administrative domain, for use within another
          administrative domain. In inter-domain accounting,
          accounting packets and session records will typically
          cross administrative boundaries.

        Intra-domain Accounting
                     Intra-domain accounting is the collection of
                     information on resource within an administrative
                     domain, for use within that domain. In intra-domain
                     accounting, accounting packets and session records
                     typically do not cross administrative boundaries.

        Local Domain
                     An administrative domain containing the AAA
                     infrastructure of immediate interest to a Mobile IP
                     client when it is away from home.

        Real-time Accounting
                     Real-time accounting involves the processing of
                     information on resource usage within a defined time
                     window. Time constraints are typically imposed in
                     order to limit financial risk.

        Session record
                     A session record represents a summary of the resource
                     consumption of a user over the entire session.
                     Accounting gateways creating the session record may
                     do so by processing interim accounting events.

   In this document, the key words "MAY", "MUST, "MUST NOT", "optional",
   "recommended", "SHOULD", and "SHOULD NOT", are to be interpreted as
   described in [4].

3. Basic Model

   In this section, we attempt to capture the main features of a basic
   model for operation of AAA servers that seems to have good support
   within the Mobile IP working group. Within the Internet, a client
   belonging to one administrative domain (called the home domain) often
   needs to use resources provided by another administrative domain
   (called the foreign domain). An agent in the foreign domain that
   attends to the client's request (call the agent the "attendant") is
   likely to require that the client provide some credentials that can
   be authenticated before access to the resources is permitted. These
   credentials may be something the foreign domain understands, but in
   most cases they are assigned by, and understood only by the home
   domain, and may be used for setting up secure channels with the
   mobile node.

```
              Local Domain                    Home Domain
              +-------------+          +--------------------+
              |   +------+  |          |   +------+         |
              |   |      |  |          |   |      |         |
              |   | AAAL |  |          |   | AAAH |         |
              |   |      +------------------+      |        |
              |   +---+--+  |          |   +------+         |
              |       |     |          |       |           |
              |       |     |          +--------------------+
   +------+   |   +---+--+  |
   |      |   |   |      |  |          C    =  client
   |   C  |- -|- -|   A  |  |          A    =  attendant
   |      |   |   |      |  |          AAAL =  local authority
   +------+   |   +------+  |          AAAH =  home authority
              |       |     |
              +-------------+
```
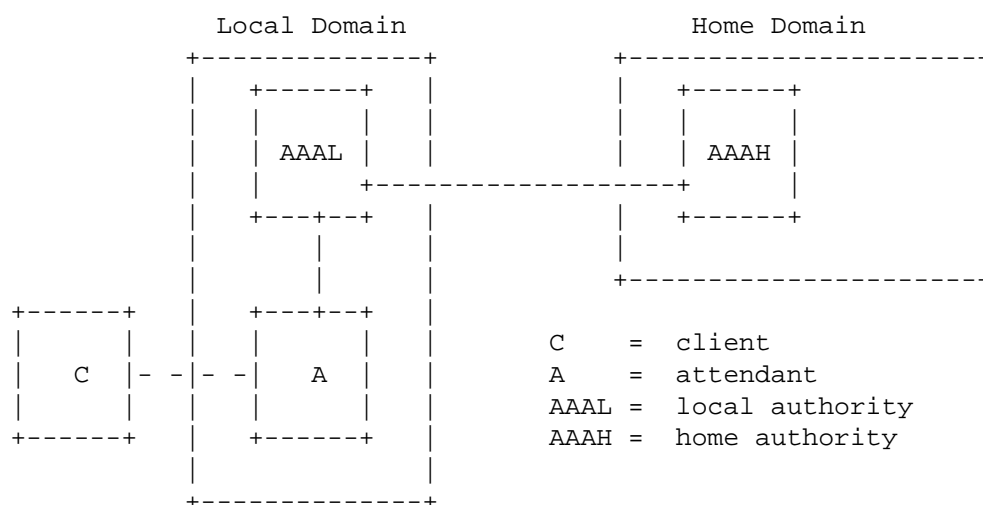
                   Figure 1: AAA Servers in Home and Local Domains

The attendant often does not have direct access to the data needed to
complete the transaction. Instead, the attendant is expected to
consult an authority (typically in the same foreign domain) in order
to request proof that the client has acceptable credentials. Since
the attendant and the local authority are part of the same
administrative domain, they are expected to have established, or be
able to establish for the necessary lifetime, a secure channel for
the purposes of exchanging sensitive (access) information, and
keeping it private from (at least) the visiting mobile node.

The local authority (AAAL) itself may not have enough information
stored locally to carry out the verification for the credentials of
the client. In contrast to the attendant, however, the AAAL is
expected to be configured with enough information to negotiate the
verification of client credentials with external authorities. The
local and the external authorities should be configured with
sufficient security relationships and access controls so that they,
possibly without the need for any other AAA agents, can negotiate the
authorization that may enable the client to have access to any/all
requested resources. In many typical cases, the authorization
depends only upon secure authentication of the client's credentials.

Once the authorization has been obtained by the local authority, and
the authority has notified the attendant about the successful
negotiation, the attendant can provide the requested resources to the
client.

In the picture, there might be many attendants for each AAAL, and
there might be many clients from many different Home Domains. Each
Home Domain provides a AAAH that can check credentials originating
from clients administered by that Home Domain.

There is a security model implicit in the above figure, and it is
crucial to identify the specific security associations assumed in the
security model.

First, it is natural to assume that the client has a security
association with the AAAH, since that is roughly what it means for
the client to belong to the home domain.

Second, from the model illustrated in figure 1 it is clear that AAAL
and AAAH have to share a security association, because otherwise they
could not rely on the authentication results, authorizations, nor
even the accounting data which might be transacted between them.
Requiring such bilateral security relationships is, however, in the
end not scalable; the AAA framework MUST provide for more scalable
mechanisms, as suggested below in section 6.

Finally, in the figure, it is clear that the attendant can naturally
share a security association with the AAAL. This is necessary in
order for the model to work because the attendant has to know that it
is permissible to allocate the local resources to the client.

As an example in today's Internet, we can cite the deployment of
RADIUS [16] to allow mobile computer clients to have access to the
Internet by way of a local ISP. The ISP wants to make sure that the
mobile client can pay for the connection. Once the client has
provided credentials (e.g., identification, unique data, and an
unforgeable signature), the ISP checks with the client's home
authority to verify the signature, and to obtain assurance that the
client will pay for the connection. Here, the attendant function can
be carried out by the NAS, and the local and home authorities can use
RADIUS servers. Credentials allowing authorization at one attendant
SHOULD be unusable in any future negotiations at the same or any
other attendant.

From the description and example above, we can identify several
requirements.

- Each local attendant has to have a security relationship with the
  local AAA server (AAAL)
- The local authority has to share, or dynamically establish,
  security relationships with external authorities that are able to
  check client credentials

- The attendant has to keep state for pending client requests while
  the local authority contacts the appropriate external authority
- Since the mobile node may not necessarily initiate network
  connectivity from within its home domain, it MUST be able to
  provide complete, yet unforgeable credentials without ever having
  been in touch with its home domain.
- Since the mobile node's credentials have to remain unforgeable,
  intervening nodes (e.g., neither the attendant or the local
  authority (AAAL) or any other intermediate nodes) MUST NOT be able
  to learn any (secret) information which may enable them to
  reconstruct and reuse the credentials.

From this last requirement, we can see the reasons for the natural
requirement that the client has to share, or dynamically establish, a
security relationship with the external authority in the Home Domain.
Otherwise, it is technically infeasible (given the implied network
topology) for the client to produce unforgeable signatures that can
be checked by the AAAH. Figure 2 illustrates the natural security
associations we understand from our proposed model. Note that,
according to the discussion in section 6, there may, by mutual
agreement between AAAL and AAAH, be a third party inserted between
AAAL and AAAH to help them arbitrate secure transactions in a more
scalable fashion.

```
                         +------+              +------+
                         |      |              |      |
                         | AAAL +--------------+ AAAH |
                         |      |              |      |
                         +---+--+              +--+---+
                             |                    |
                             |                    |
                         +---+--+              +--+---+
C    = client            |      |              |      |
A    = attendant         |  A   |              |  C   |
AAAL = local authority   |      |              |      |
AAAH = home authority    +------+              +------+
```
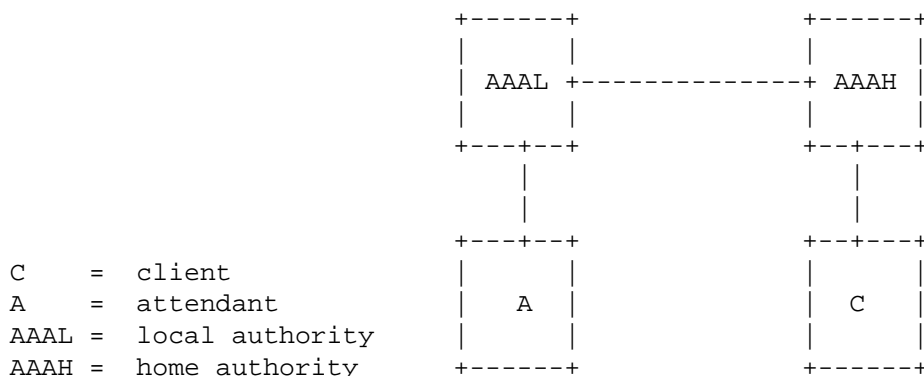
Figure 2: Security Associations

In addition to the requirements listed above, we specify the
following requirements which derive from operational experience with
today's roaming protocols.

- There are scenarios in which an attendant will have to manage
  requests for many clients at the same time.
- The attendant MUST protect against replay attacks.

- The attendant equipment should be as inexpensive as possible, since it will be replicated as many times as possible to handle as many clients as possible in the foreign domain.
- Attendants SHOULD be configured to obtain authorization, from a trusted local AAA server (AAAL) for Quality of Service requirements placed by the client.

Nodes in two separate administrative domains (for instance, AAAH and AAAL) often must take additional steps to verify the identity of their communication partners, or alternatively to guarantee the privacy of the data making up the communication. While these considerations lead to important security requirements, as mentioned above in the context of security between servers, we consider the exact choice of security associations between the AAA servers to be beyond the scope of this document. The choices are unlikely even to depend upon any specific features of the general model illustrated in figure 1. On the other hand, the security associations needed between Mobile IP entities will be of central importance in the design of a suitable AAA infrastructure for Mobile IP. The general model shown above is generally compatible with the needs of Mobile IP. However, some basic changes are needed in the security model of Mobile IP, as detailed in section 5.

Lastly, recent discussion in the mobile-ip working group has indicated that the attendant MUST be able to terminate service to the client based on policy determination by either AAAH or AAAL server.

3.1. AAA Protocol Roaming Requirements

In this section we will detail additional requirements based on issues discovered through operational experience of existing roaming RADIUS networks. The AAA protocol MUST satisfy these requirements in order for providers to offer a robust service. These requirements have been identified by TR45.6 as part of their involvement with the Mobile IP working group.

- Support a reliable AAA transport mechanism.
  * There must be an effective hop-by-hop retransmission and failover mechanism so that reliability does not solely depend on end-to-end retransmission
  * This transport mechanism will be able indicate to an AAA application that a message was delivered to the next peer AAA application or that a time out occurred.
  * Retransmission is controlled by the reliable AAA transport mechanism, and not by lower layer protocols such as TCP.

          * Even if the AAA message is to be forwarded, or the message's
             options or semantics do not conform with the AAA protocol, the
             transport mechanism will acknowledge that the peer received the
             AAA message.
          * Acknowledgements SHOULD be allowed to be piggybacked in AAA
             messages
          * AAA responses have to be delivered in a timely fashion so that
             Mobile IP does not timeout and retransmit
      - Transport a digital certificate in an AAA message, in order to
         minimize the number of round trips associated with AAA
         transactions. Note: This requirement applies to AAA applications
         and not mobile stations. The certificates could be used by
         foreign and home agents to establish an IPSec security association
         to secure the mobile node's tunneled data. In this case, the AAA
         infrastructure could assist by obtaining the revocation status of
         such a certificate (either by performing online checks or
         otherwise validating the certificate) so that home and foreign
         agents could avoid a costly online certificate status check.
      - Provide message integrity and identity authentication on a hop-
         by-hop (AAA node) basis.
      - Support replay protection and optional non-repudiation
         capabilities for all authorization and accounting messages. The
         AAA protocol must provide the capability for accounting messages
         to be matched with prior authorization messages.
      - Support accounting via both bilateral arrangements and via broker
         AAA servers providing accounting clearinghouse and reconciliation
         between serving and home networks. There is an explicit agreement
         that if the private network or home ISP authenticates the mobile
         station requesting service, then the private network or home ISP
         network also agrees to reconcile charges with the home service
         provider or broker. Real time accounting must be supported.
         Timestamps must be included in all accounting packets.

   4. Requirements related to basic IP connectivity

      The requirements listed in the previous section pertain to the
      relationships between the functional units, and don't depend on the
      underlying network addressing. On the other hand, many nodes (mobile
      or merely portable) are programmed to receive some IP-specific
      resources during the initialization phase of their attempt to connect
      to the Internet.

      We place the following additional requirements on the AAA services in
      order to satisfy such clients.

      - Either AAA server MUST be able to obtain, or to coordinate the
         allocation of, a suitable IP address for the customer, upon
         request by the customer.

      - AAA servers MUST be able to identify the client by some means
         other than its IP address.

   Policy in the home domain may dictate that the home agent instead of
   the AAAH manages the allocation of an IP address for the mobile node.
   AAA servers MUST be able to coordinate the allocation of an IP
   address for the mobile node at least in this way.

   AAA servers today identify clients by using the Network Access
   Identifier (NAI) [1]. A mobile node can identify itself by including
   the NAI along with the Mobile IP Registration Request [6]. The NAI
   is of the form "user@realm"; it is unique and well suited for use in
   the AAA model illustrated in figure 1. Using a NAI (e.g.,
   "user@realm") allows AAAL to easily determine the home domain (e.g.,
   "realm") for the client. Both the AAAL and the AAAH can use the NAI
   to keep records indexed by the client's specific identity.

5. AAA for Mobile IP

   Clients using Mobile IP require specific features from the AAA
   services, in addition to the requirements already mentioned in
   connection with the basic AAA functionality and what is needed for IP
   connectivity. To understand the application of the general model for
   Mobile IP, we consider the mobile node (MN) to be the client in
   figure 1, and the attendant to be the foreign agent (FA). If a
   situation arises that there is no foreign agent present, e.g., in the
   case of an IPv4 mobile node with a co-located care of address or an
   IPv6 mobile node, the equivalent attendant functionality is to be
   provided by the address allocation entity, e.g., a DHCP server. Such
   an attendant functionality is outside the scope of this document.
   The home agent, while important to Mobile IP, is allowed to play a
   role during the initial registration that is subordinate to the role
   played by the AAAH. For application to Mobile IP, we modify the
   general model (as illustrated in figure 3). After the initial
   registration, the mobile node is authorized to continue using Mobile
   IP at the foreign domain without requiring further involvement by the
   AAA servers. Thus, the initial registration will probably take
   longer than subsequent Mobile IP registrations.

   In order to reduce this extra time overhead as much as possible, it
   is important to reduce the time taken for communications between the
   AAA servers. A major component of this communications latency is the
   time taken to traverse the wide-area Internet that is likely to
   separate the AAAL and the AAAH. This leads to a further strong
   motivation for integration of the AAA functions themselves, as well
   as integration of AAA functions with the initial Mobile IP
   registration. In order to reduce the number of messages that
   traverse the network for initial registration of a Mobile Node, the

AAA functions in the visited network (AAAL) and the home network
(AAAH) need to interface with the foreign agent and the home agent to
handle the registration message. Latency would be reduced as a
result of initial registration being handled in conjunction with AAA
and the mobile IP mobility agents. Subsequent registrations,
however, would be handled according to RFC 2002 [13]. Another way to
reduce latency as to accounting would be the exchange of small
records.

As there are many different types of sub-services attendants may
provide to mobile clients, there MUST be extensible accounting
formats. In this way, the specific services being provided can be
identified, as well as accounting support should more services be
identified in the future.

The AAA home domain and the HA home domain of the mobile node need
not be part of the same administrative domain. Such an situation can
occur if the home address of the mobile node is provided by one
domain, e.g., an ISP that the mobile user uses while at home, and the
authorization and accounting by another (specialized) domain, e.g., a
credit card company. The foreign agent sends only the authentication
information of the mobile node to the AAAL, which interfaces to the
AAAH. After a successful authorization of the mobile node, the
foreign agent is able to continue with the mobile IP registration
procedure. Such a scheme introduces more delay if the access to the
AAA functionality and the mobile IP protocol is sequentialized.
Subsequent registrations would be handled according to RFC 2002 [13]
without further interaction with the AAA. Whether to combine or
separate the Mobile IP protocol data with/from the AAA messages is
ultimately a policy decision. A separation of the Mobile IP protocol
data and the AAA messages can be successfully accomplished only if
the IP address of the mobile node's home agent is provided to the
foreign agent performing the attendant function.

All needed AAA and Mobile IP functions SHOULD be processed during a
single Internet traversal. This MUST be done without requiring AAA
servers to process protocol messages sent to Mobile IP agents. The
AAA servers MUST identify the Mobile IP agents and security
associations necessary to process the Mobile IP registration, pass
the necessary registration data to those Mobile IP agents, and remain
uninvolved in the routing and authentication processing steps
particular to Mobile IP registration.

For Mobile IP, the AAAL and the AAAH servers have the following
additional general tasks:

- enable [re]authentication for Mobile IP registration

      - authorize the mobile node (once its identity has been established)
        to use at least the set of resources for minimal Mobile IP
        functionality, plus potentially other services requested by the
        mobile node
      - initiate accounting for service utilization
      - use AAA protocol extensions specifically for including Mobile IP
        registration messages as part of the initial registration sequence
        to be handled by the AAA servers.

   These tasks, and the resulting more specific tasks to be listed later
   in this section, are beneficially handled and expedited by the AAA
   servers shown in figure 1 because the tasks often happen together,
   and task processing needs access to the same data at the same time.

```
                  Local Domain                     Home Domain
                  +-------------+          +--------------------+
                  |  +------+   |          |  +------+          |
                  |  |      |   |          |  |      |          |
                  |  | AAAL |   |          |  | AAAH |          |
                  |  |      +------------------+      |          |
                  |  +---+--+   |          |  +--+---+          |
                  |      |      |          |     |              |
                  |      |      |          |     |              |
   +------+       |  +---+--+   |          |  +--+---+          |
   |      |       |  |      |   |          |  |      |          |
   |  MN  +- -|- -+  FA  + --  --  --  --  - +  HA  |          |
   |      |   |  |      |   |          |  |      |          |
   +------+       |  +------+   |          |  +------+          |
                  |             |          |                    |
                  +-------------+          +--------------------+
```
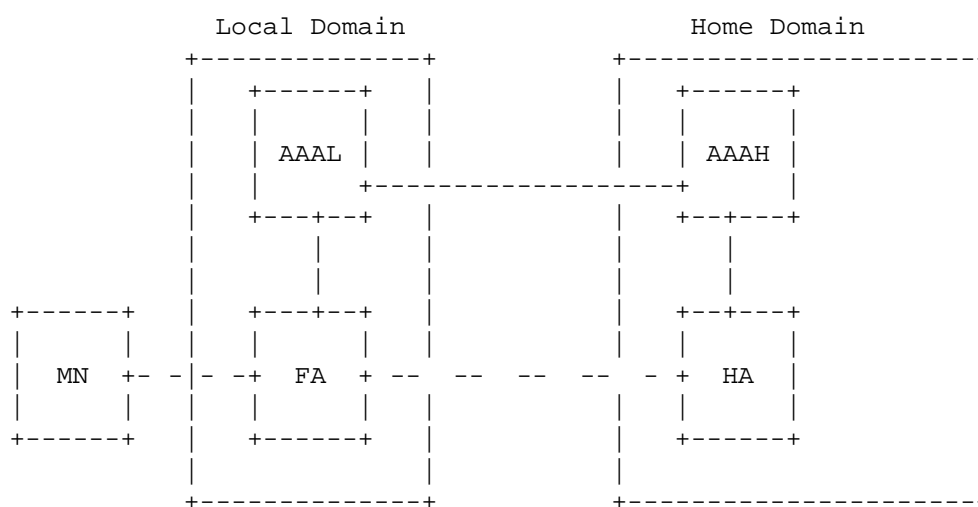
               Figure 3: AAA Servers with Mobile IP agents

   In the model in figure 1, the initial AAA transactions are handled
   without needing the home agent, but Mobile IP requires every
   registration to be handled between the home agent (HA) and the
   foreign agent (FA), as shown by the sparse dashed (lower) line in
   figure 3. This means that during the initial registration, something
   has to happen that enables the home agent and foreign agent to
   perform subsequent Mobile IP registrations. After the initial
   registration, the AAAH and AAAL in figure 3 would not be needed, and
   subsequent Mobile IP registrations would only follow the lower
   control path between the foreign agent and the home agent.

   Any Mobile IP data that is sent by FA through the AAAL to AAAH MUST
   be considered opaque to the AAA servers. Authorization data needed
   by the AAA servers then MUST be delivered to them by the foreign

agent from the data supplied by the mobile node. The foreign agent
becomes a translation agent between the Mobile IP registration
protocol and AAA.

As mentioned in section 3, nodes in two separate administrative
domains often must take additional steps to guarantee their security
and privacy,, as well as the security and privacy of the data they
are exchanging. In today's Internet, such security measures may be
provided by using several different algorithms. Some algorithms rely
on the existence of a public-key infrastructure [8]; others rely on
distribution of symmetric keys to the communicating nodes [9]. AAA
servers SHOULD be able to verify credentials using either style in
their interactions with Mobile IP entities.

In order to enable subsequent registrations, the AAA servers MUST be
able to perform some key distribution during the initial Mobile IP
registration process from any particular administrative domain.

This key distribution MUST be able to provide the following security
functions:

- identify or create a security association between MN and home
  agent (HA); this is required for the MN to produce the
  [re]authentication data for the MN--HA authentication extension,
  which is mandatory on Mobile IP registrations.
- identify or create a security association between mobile node and
  foreign agent, for use with subsequent registrations at the same
  foreign agent, so that the foreign agent can continue to obtain
  assurance that the same mobile node has requested the continued
  authorization for Mobile IP services.
- identify or create a security association between home agent and
  foreign agent, for use with subsequent registrations at the same
  foreign agent, so that the foreign agent can continue to obtain
  assurance that the same home agent has continued the authorization
  for Mobile IP services for the mobile node.
- participate in the distribution of the security association (and
  Security Parameter Index, or SPI) to the Mobile IP entities
- The AAA server MUST also be able to validate certificates provided
  by the mobile node and provide reliable indication to the foreign
  agent.
- The AAAL SHOULD accept an indication from the foreign agent about
  the acceptable lifetime for its security associations with the
  mobile node and/or the mobile node's home agent. This lifetime
  for those security associations SHOULD be an integer multiple of
  registration lifetime offered by the foreign agent to the mobile
  node. This MAY allow for Mobile IP reauthentication to take place

   without the need for reauthentication to take place on the AAA
   level, thereby shortenning the time required for mobile node
   reregistration.
- The AAA servers SHOULD be able to condition their acceptance of a
   Mobile IP registration authorization depending upon whether the
   registration requires broadcast or multicast service to the mobile
   node tunneled through the foreign agent.
- In addition, reverse tunneling may also be a necessary requirement
   for mobile node connectivity. Therefore, AAA servers SHOULD also
   be able to condition their acceptance of Mobile IP registration
   authorization depending upon whether the registration requires
   reverse tunnelling support to the home domain through the foreign
   agent.

   The lifetime of any security associations distributed by the AAA
   server for use with Mobile IP SHOULD be great enough to avoid too-
   frequent initiation of the AAA key distribution, since each
   invocation of this process is likely to cause lengthy delays between
   [re]registrations [5]. Registration delays in Mobile IP cause
   dropped packets and noticeable disruptions in service. Note that any
   key distributed by AAAH to the foreign agent and home agent MAY be
   used to initiate Internet Key Exchange (IKE) [7].

   Note further that the mobile node and home agent may well have a
   security association established that does not depend upon any action
   by the AAAH.

5.1. Mobile IP with Dynamic IP Addresses

   According to section 4, many people would like their mobile nodes to
   be identified by their NAI, and to obtain a dynamically allocated
   home address for use in the foreign domain. These people may often
   be unconcerned with details about how their computers implement
   Mobile IP, and indeed may not have any knowledge of their home agent
   or any security association except that between themselves and the
   AAAH (see figure 2). In this case the Mobile IP registration data
   has to be carried along with the AAA messages. The AAA home domain
   and the HA home domain have to be part of the same administrative
   domain.

   Mobile IP requires the home address assigned to the mobile node
   belong to the same subnet as the Home Agent providing service to the
   mobile node. For effective use of IP home addresses, the home AAA
   (AAAH) SHOULD be able to select a home agent for use with the newly
   allocated home address. In many cases, the mobile node will already
   know the address of its home agent, even if the mobile node does not
   already have an existing home address. Therefore, the home AAA
   (AAAH) MUST be able to coordinate the allocation of a home address

   with a home agent that might be designated by the mobile node.

   Allocating a home address and a home agent for the mobile would
   provide a further simplification in the configuration needs for the
   client's mobile node. Currently, in the Proposed Standard Mobile IP
   specification [13] a mobile node has to be configured with a home
   address and the address of a home agent, as well as with a security
   association with that home agent. In contrast, the proposed AAA
   features would only require the mobile node to be configured with its
   NAI and a secure shared secret for use by the AAAH. The mobile
   node's home address, the address of its home agent, the security
   association between the mobile node and the home agent, and even the
   identity (DNS name or IP address) of the AAAH can all be dynamically
   determined as part of Mobile IP initial registration with the
   mobility agent in the foreign domain (i.e., a foreign agent with AAA
   interface features). Nevertheless, the mobile node may choose to
   include the MN-HA security extension as well as AAA credentials, and
   the proposed Mobile IP and AAA server model MUST work when both are
   present.

   The reason for all this simplification is that the NAI encodes the
   client's identity as well as the name of the client's home domain;
   this follows existing industry practice for the way NAIs are used
   today (see section 4). The home domain name is then available for
   use by the local AAA (AAAL) to locate the home AAA serving the
   client's home domain. In the general model, the AAAL would also have
   to identify the appropriate security association for use with that
   AAAH. Section 6 discusses a way to reduce the number of security
   associations that have to be maintained between pairs of AAA servers
   such as the AAAL and AAAH just described.

5.2. Firewalls and AAA

   Mobile IP has encountered some deployment difficulties related to
   firewall traversal; see for instance [11]. Since the firewall and
   AAA server can be part of the same administrative domain, we propose
   that the AAA server SHOULD be able to issue control messages and keys
   to the firewall at the boundary of its administrative domain that
   will configure the firewall to be permeable to Mobile IP registration
   and data traffic from the mobile node.

5.3. Mobile IP with Local Home Agents

```
              +-------------------------+        +--------------+
              |  +------+    +------+    |        |  +------+    |
              |  |      |    |      |    |        |  |      |    |
              |  | HA   +----+ AAAL |    |        |  | AAAH |    |
              |  |      |    |      +------------------+      |    |
              |  +-+----+    +---+--+    |        |  +------+    |
              |    |             |       |        | Home Domain  |
              |    |  +- - - - - +       |        +--------------+
    +------+  |  +-+--+-+        |       |
    |      |  |  |    | |        |       |
    | MN   +------+ FA |        |       |
    |      |  |  | |   |  Local Domain   |
    +------+  |  +------+        |       |
              +-------------------------+
```
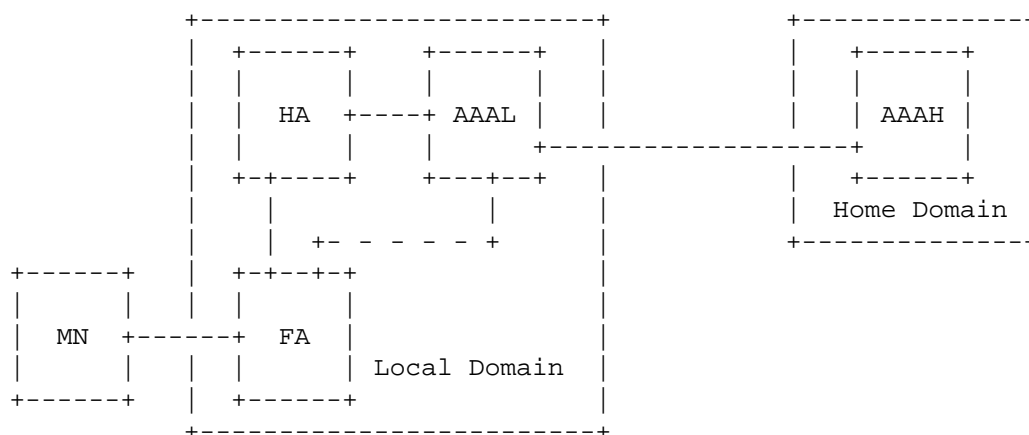
                 Figure 4: Home Agent Allocated by AAAL

   In some Mobile IP models, mobile nodes boot on subnets which are
   technically foreign subnets, but the services they need are local,
   and hence communication with the home subnet as if they were residing
   on the home is not necessary. As long as the mobile node can get an
   address routable from within the current domain (be it publicly, or
   privately addressed) it can use mobile IP to roam around that domain,
   calling the subnet on which it booted its temporary home. This
   address is likely to be dynamically allocated upon request by the
   mobile node.

   In such situations, when the client is willing to use a dynamically
   allocated IP address and does not have any preference for the
   location of the home network (either geographical or topological),
   the local AAA server (AAAL) may be able to offer this additional
   allocation service to the client. Then, the home agent will be
   located in the local domain, which is likely to be offer smaller
   delays for new Mobile IP registrations.

   In figure 4, AAAL has received a request from the mobile node to
   allocate a home agent in the local domain. The new home agent
   receives keys from AAAL to enable future Mobile IP registrations.
   From the picture, it is evident that such a configuration avoids
   problems with firewall protection at the domain boundaries, such as
   were described briefly in section 5.2. On the other hand, this
   configuration makes it difficult for the mobile node to receive data
   from any communications partners in the mobile node's home
   administrative domain. Note that, in this model, the mobile node's
   home address is affiliated with the foreign domain for routing
   purposes. Thus, any dynamic update to DNS, to associate the mobile

   node's home FQDN (Fully Qualified Domain Name [10]) with its new IP
   address, will require insertion of a foreign IP address into the home
   DNS server database.

5.4. Mobile IP with Local Payments

   Since the AAAL is expected to be enabled to allocate a local home
   agent upon demand, we can make a further simplification. In cases
   where the AAAL can manage any necessary authorization function
   locally (e.g., if the client pays with cash or a credit card), then
   there is no need for an AAA protocol or infrastructure to interact
   with the AAAH. The resulting simple configuration is illustrated in
   figure 5.

   In this simplified model, we may consider that the role of the AAAH
   is taken over either by a national government (in the case of a cash
   payment), or by a card authorization service if payment is by credit
   card, or some such authority acceptable to all parties. Then, the
   AAAL expects those external authorities to guarantee the value
   represented by the client's payment credentials (cash or credit).
   There are likely to be other cases where clients are granted access
   to local resources, or access to the Internet, without any charges at
   all. Such configurations may be found in airports and other common

```
                    +------------------------+
                    |  +------+    +------+   |
                    |  |      |    |      |   |
                    |  | HA   +----+ AAAL |   |
                    |  |      |    |      |   |
                    |  +--+---+    +----+-+   |
                    |     |             |     |
                    |     +- - - - - +  |     |
       +------+     |               +-+--+-+  |
       |      |     |               |      |  |
       |  MN  +- -|- - - - - - - +  FA   |  |
       |      |     | Local Domain |      |  |
       +------+     |               +------+  |
                    +------------------------+
```
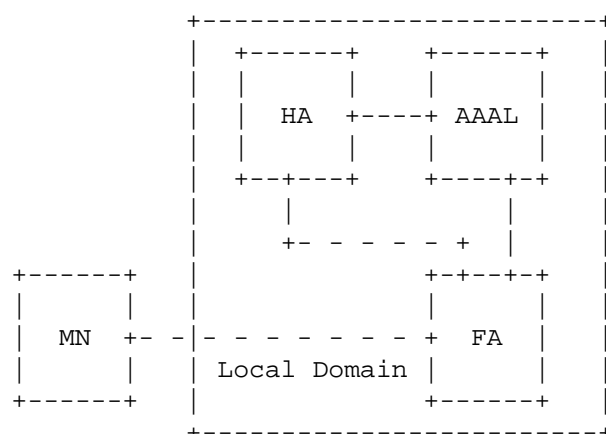
        Figure 5: Local Payment for Local Mobile IP services

   areas where business clients are likely to spend time. The service
   provider may find sufficient reward in the goodwill of the clients,
   or from advertisements displayed on Internet portals that are to be
   used by the clients. In such situations, the AAAL SHOULD still
   allocate a home agent, appropriate keys, and the mobile node's home
   address.

5.5. Fast Handover

   Since the movement from coverage area to coverage area may be
   frequent in Mobile IP networks, it is imperative that the latency
   involved in the handoff process be minimized. See, for instance, the
   Route Optimization document [15] for one way to do this using Binding
   Updates. When the mobile node enters a new visited subnet, it would
   be desirable for it to provide the previous foreign agent's NAI. The
   new FA can use this information to either contact the previous FA to
   retrieve the KDC session key information, or it can attempt to
   retrieve the keys from the AAAL. If the AAAL cannot provide the
   necessary keying information, the request will have to be sent to the
   mobile node's AAAH to retrieve new keying information. After initial
   authorization, further authorizations SHOULD be done locally within
   the Local Domain.

   When a MN moves into a new foreign subnet as a result of a handover
   and is now served by a different FA, the AAAL in this domain may
   contact the AAAL in the domain that the MN has just been handed off
   from to verify the authenticity of the MN and/or to obtain the
   session keys. The new serving AAAL may determine the address of the
   AAAL in the previously visited domain from the previous FA NAI
   information supplied by the MN.

6. Broker Model

   The picture in Figure 1 shows a configuration in which the local and
   the home authority have to share trust. Depending on the security
   model used, this configuration can cause a quadratic growth in the
   number of trust relationships, as the number of AAA authorities (AAAL
   and AAAH) increases. This has been identified as a problem by the
   roamops working group [3], and any AAA proposal MUST solve this
   problem. Using brokers solves many of the scalability problems
   associated with requiring direct business/roaming relationships
   between every two administrative domains. In order to provide
   scalable networks in highly diverse service provider networks in
   which there are many domains (e.g., many service providers and large
   numbers of private networks), multiple layers of brokers MUST be
   supported for both of the broker models described.

   Integrity or privacy of information between the home and serving
   domains may be achieved by either hop-by-hop security associations or
   end-to-end security associations established with the help of the
   broker infrastructure. A broker may play the role of a proxy between
   two administrative domains which have security associations with the
   broker, and relay AAA messages back and forth securely.

Alternatively, a broker may also enable the two domains with which it
has associations, but the domains themselves do not have a direct
association, in establishing a security association, thereby
bypassing the broker for carrying the messages between the domains.
This may be established by virtue of having the broker relay a shared
secret key to both the domains that are trying to establish secure
communication and then have the domains use the keys supplied by the
broker in setting up a security association.

Assuming that AAAB accepts responsibility for payment to the serving
domain on behalf of the home domain, the serving domain is assured of
receiving payments for services offered. However, the redirection
broker will usually require a copy of authorization messages from the
home domain and accounting messages from the serving domain, in order
for the broker to determine if it is willing to accept responsibility
for the services being authorized and utilized. If the broker does
not accept such responsibility for any reason, then it must be able
to terminate service to a mobile node in the serving network. In the
event that multiple brokers are involved, in most situations all
brokers must be so copied. This may represent an additional burden
on foreign agents and AAALs.

Though this mechanism may reduce latency in the transit of messages
between the domains after the broker has completed its involvement,
there may be many more messages involved as a result of additional
copies of authorization and accounting messages to the brokers
involved. There may also be additional latency for initial access to
the network, especially when a new security association needs to be
created between AAAL and AAAH (for example, from the use of ISAKMP).
These delays may become important factors for latency-critical
applications.

```
              Local Domain                          Home Domain
              +--------------+          +----------------------+
              |   +------+    |  +------+  |   +------+          |
              |   |      |    |  |      |  |   |      |          |
              |   | AAAL +-------+ AAAB +--------+ AAAH |        |
              |   |      |    |  |      |  |   |      |          |
              |   +------+    |  +------+  |   +------+          |
              |      |        |            |                     |
              |      |        |            +----------------------+
   +------+   |   +---+--+    |
   |      |   |   |      |    |          C   =  client
   |  C   +- -|- -+   A  |    |          A   =  attendant
   |      |   |   |      |    |          AAAL =  local authority
   +------+   |   +------+    |          AAAH =  home authority
              |              |           AAAB =  broker authority
              +--------------+
```
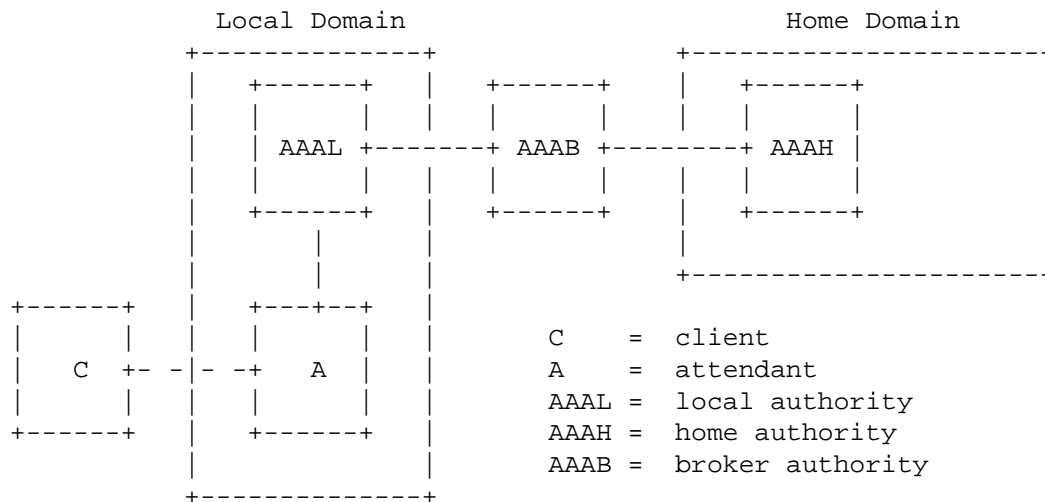
                    Figure 6: AAA Servers Using a Broker

     The AAAB in figure 6 is the broker's authority server. The broker
     acts as a settlement agent, providing security and a central point of
     contact for many service providers and enterprises.

     The AAAB enables the local and home domains to cooperate without
     requiring each of the networks to have a direct business or security
     relationship with all the other networks. Thus, brokers offer the
     needed scalability for managing trust relationships between otherwise
     independent network domains. Use of the broker does not preclude
     managing separate trust relationships between domains, but it does
     offer an alternative to doing so. Just as with the AAAH and AAAL
     (see section 5), data specific to Mobile IP control messages MUST NOT
     be processed by the AAAB. Any credentials or accounting data to be
     processed by the AAAB must be present in AAA message units, not
     extracted from Mobile IP protocol extensions.

     The following requirements come mostly from [2], which discusses use
     of brokers in the particular case of authorization for roaming dial-
     up users.

     - allowing management of trust with external domains by way of
        brokered AAA.
     - accounting reliability. Accounting data that traverses the
        Internet may suffer substantial packet loss. Since accounting
        packets may traverse one or more intermediate authorization points
        (e.g., brokers), retransmission is needed from intermediate points
        to avoid long end-to-end delays.

     - End to End security. The Local Domain and Home Domain must be
        able to verify signatures within the message, even though the
        message is passed through an intermediate authority server.
     - Since the AAAH in the home domain MAY be sending sensitive
        information, such as registration keys, the broker MUST be able to
        pass encrypted data between the AAA servers.

   The need for End-to-End security results from the following attacks
   which were identified when brokered operation uses RADIUS [16] (see
   [2] for more information on the individual attacks):

       + Message editing
       + Attribute editing
       + Theft of shared secrets
       + Theft and modification of accounting data
       + Replay attacks
       + Connection hijacking
       + Fraudulent accounting

   These are serious problems which cannot be allowed to persist in any
   acceptable AAA protocol and infrastructure.

7. Security Considerations

   This is a requirements document for AAA based on Mobile IP. Because
   AAA is security driven, most of this document addresses the security
   considerations AAA MUST make on behalf of Mobile IP. As with any
   security proposal, adding more entities that interact using security
   protocols creates new administrative requirements for maintaining the
   appropriate security associations between the entities. In the case
   of the AAA services proposed however, these administrative
   requirements are natural, and already well understood in today's
   Internet because of experience with dial up network access.

8. IPv6 Considerations

   The main difference between Mobile IP for IPv4 and Mobile IPv6 is
   that in IPv6 there is no foreign agent. The attendant function,
   therefore, has to be located elsewhere. Logical repositories for
   that function are either at the local router, for stateless address
   autoconfiguration, or else at the nearest DHCPv6 server, for stateful
   address autoconfiguration. In the latter case, it is possible that
   there would be a close relationship between the DHCPv6 server and the
   AAALv6, but we believe that the protocol functions should still be
   maintained separately.

   The MN-NAI would be equally useful for identifying the mobile node to
   the AAALv6 as is described in earlier sections of this document.

9. Acknowledgements

   Thanks to Gopal Dommety and Basavaraj Patil for participating in the
   Mobile IP subcommittee of the aaa-wg which was charged with
   formulating the requirements detailed in this document. Thanks to N.
   Asokan for perceptive comments to the mobile-ip mailing list. Some
   of the text of this document was taken from a draft co-authored by
   Pat Calhoun. Patrik Flykt suggested text about allowing AAA home
   domain functions to be separated from the domain managing the home
   address of the mobile computer.

   The requirements in section 5.5 and section 3.1 were taken from a
   draft submitted by members of the TIA's TR45.6 Working Group. We
   would like to acknowledge the work done by the authors of that draft:
   Tom Hiller, Pat Walsh, Xing Chen, Mark Munson, Gopal Dommety,
   Sanjeevan Sivalingham, Byng-Keun Lim, Pete McCann, Brent Hirschman,
   Serge Manning, Ray Hsu, Hang Koo, Mark Lipford, Pat Calhoun, Eric
   Jaques, Ed Campbell, and Yingchun Xu.

References

   [1] Aboba, B. and M. Beadles, "The Network Access Identifier", RFC
        2486, January 1999.

   [2] Aboba, B. and J. Vollbrecht, "Proxy Chaining and Policy
        Implementation in Roaming", RFC 2607, June 1999.

   [3] Aboba, B. and G. Zorn, "Criteria for Evaluating Roaming
        Protocols", RFC 2477, December 1998.

   4]   Bradner, S., "Key words for use in RFCs to Indicate Requirement
        Levels", BCP 14, RFC 2119, March 1997.

   [5] Ramon Caceres and Liviu Iftode. Improving the Performance of
        Reliable Transport Protocols in Mobile Computing Environments.
        IEEE Journal on Selected Areas in Communications, 13(5):850--
        857, June 1995.

   [6] Calhoun, P. and C. Perkins, "Mobile IP Network Address
        Identifier Extension, RFC 2794, March 2000.

   [7] Harkins, D. and D. Carrel, "The Internet Key Exchange (IKE)",
        RFC 2409, November 1998.

   [8] Housley, R., Ford, W., Polk, T. and D. Solo, "Internet X.509
        Public Key Infrastructure Certificate and CRL Profile", RFC
        2459, January 1999.

RFC 2977   Mobile IP AAA Requirements   October 2000

[9] Kohl, J. and C. Neuman, "The Kerberos Network Authentication
        Service (V5)", RFC 1510, September 1993.

   [10] Mockapetris, P., "Domain names - implementation and
        specification", STD 13, RFC 1035, November 1987.

   [11] Montenegro, G. and V. Gupta, "Sun's SKIP Firewall Traversal for
        Mobile IP", RFC 2356, June 1998.

   [12] Perkins, C., "IP Encapsulation within IP", RFC 2003, October
        1996.

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

   [14] Perkins, C., "Minimal Encapsulation within IP", RFC 2004,
        October 1996.

   [15] Perkins, C. and D. Johnson, "Route Optimization in Mobile IP",
        Work in Progress.

   [16] Rigney, C., Rubens, A., Simpson, W. and S. Willens, "Remote
        Authentication Dial In User Service (RADIUS)", RFC 2138, April
        1997.

   [17] Solomon, J. and S. Glass, "Mobile-IPv4 Configuration Option for
        PPP IPCP", RFC 2290, February 1998.

Glass, et al.   Informational   [Page 23]

Addresses

   The working group can be contacted via the current chairs:

   Basavaraj Patil
   Nokia
   6000 Connection Drive
   Irving, TX 75039
   USA

   Phone: +1 972-894-6709
   EMail: Basavaraj.Patil@nokia.com

   Phil Roberts
   Motorola
   1501 West Shure Drive
   Arlington Heights, IL 60004
   USA

   Phone: +1 847-632-3148
   EMail: QA3445@email.mot.com

Questions about this memo can be directed to:

Pat R. Calhoun
Network and Security Center
Sun Microsystems Laboratories
15 Network Circle
Menlo Park, California 94025
USA

Phone: +1 650-786-7733
Fax: +1 650-786-6445
EMail: pcalhoun@eng.sun.com

Gopal Dommety
IOS Network Protocols
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA

Phone: +1-408-525-1404
Fax: +1 408-526-4952
EMail: gdommety@cisco.com

Steven M. Glass
Sun Microsystems
1 Network Drive
Burlington, MA 01803
USA

Phone: +1-781-442-0504
EMail: steven.glass@sun.com

Stuart Jacobs
Secure Systems Department
GTE Laboratories
40 Sylvan Road
Waltham, MA 02451-1128
USA

Phone: +1 781-466-3076
Fax: +1 781-466-2838
EMail: sjacobs@gte.com

      Tom Hiller
      Lucent Technologies
      Rm 2F-218
      263 Shuman Blvd
      Naperville, IL 60566
      USA

      Phone: +1 630 979 7673
      Fax: +1 630 713 3663
      EMail: tomhiller@lucent.com

      Peter J. McCann
      Lucent Technologies
      Rm 2Z-305
      263 Shuman Blvd
      Naperville, IL 60566
      USA

      Phone: +1 630 713 9359
      Fax: +1 630 713 4982
      EMail: mccap@lucent.com

      Basavaraj Patil
      Nokia
      6000 Connection Drive
      Irving, TX 75039
      USA

      Phone: +1 972-894-6709
      Fax : +1 972-894-5349
      EMail: Basavaraj.Patil@nokia.com

      Charles E. Perkins
      Communications Systems Lab
      Nokia Research Center
      313 Fairchild Drive
      Mountain View, California 94043
      USA

      Phone: +1-650 625-2986
      Fax: +1 650 625-2502
      EMail: charliep@iprg.nokia.com

Full Copyright Statement

   Copyright (C) The Internet Society (2000). All Rights Reserved.

   This document and translations of it may be copied and furnished to
   others, and derivative works that comment on or otherwise explain it
   or assist in its implementation may be prepared, copied, published
   and distributed, in whole or in part, without restriction of any
   kind, provided that the above copyright notice and this paragraph are
   included on all such copies and derivative works. However, this
   document itself may not be modified in any way, such as by removing
   the copyright notice or references to the Internet Society or other
   Internet organizations, except as needed for the purpose of
   developing Internet standards in which case the procedures for
   copyrights defined in the Internet Standards process must be
   followed, or as required to translate it into languages other than
   English.

   The limited permissions granted above are perpetual and will not be
   revoked by the Internet Society or its successors or assigns.

   This document and the information contained herein is provided on an
   "AS IS" basis and THE INTERNET SOCIETY AND THE INTERNET ENGINEERING
   TASK FORCE DISCLAIMS ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING
   BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION
   HEREIN WILL NOT INFRINGE ANY RIGHTS OR ANY IMPLIED WARRANTIES OF
   MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Acknowledgement

   Funding for the RFC Editor function is currently provided by the
   Internet Society.