Network Working Group   B. Aboba, Microsoft
Request for Comments: 2989   P. Calhoun, S. Glass, Sun Microsystems, Inc.
Category: Informational T. Hiller, P. McCann, H. Shiino, P. Walsh, Lucent
                                  G. Zorn, G. Dommety, Cisco Systems, Inc.
                             C. Perkins, B. Patil, Nokia Telecommunications
                                   D. Mitton, S. Manning, Nortel Networks
                                             M. Beadles, SmartPipes Inc.
                                                       X. Chen, Alcatel
                          S. Sivalingham, Ericsson Wireless Communications
                                                     A. Hameed, Fujitsu
                                             M. Munson, GTE Wireless
                                             S. Jacobs, GTE Laboratories
                             B. Lim, LG Information & Communications, Ltd.
                                                 B. Hirschman, Motorola
                                                 R. Hsu, Qualcomm, Inc.
                          H. Koo, Samsung Telecommunications America, Inc.
                                                 M. Lipford, Sprint PCS
                                           E. Campbell, 3Com Corporation
                                             Y. Xu, Watercove Networks
                             S. Baba, Toshiba America Research, Inc.
                                         E. Jaques, Vodaphone Airtouch
                                                         November 2000

           Criteria for Evaluating AAA Protocols for Network Access

Abstract

   This document represents a summary of Authentication, Authorization,
   Accounting (AAA) protocol requirements for network access. In
   creating this document, inputs were taken from documents produced by
   the Network Access Server Requirements Next Generation (NASREQ),
   Roaming Operations (ROAMOPS), and MOBILEIP working groups, as well as
   from TIA 45.6.

This document summarizes the requirements collected from those
sources, separating requirements for authentication, authorization
and accounting. Details on the requirements are available in the
original documents.

1. Introduction

This document represents a summary of AAA protocol requirements for
network access. In creating this documents, inputs were taken from
documents produced by the NASREQ [3], ROAMOPS [2], and MOBILEIP [5]
working groups, as well as from TIA 45.6 [4]. This document
summarizes the requirements collected from those sources, separating
requirements for authentication, authorization and accounting.
Details on the requirements are available in the original documents.

1.1. Requirements language

In this document, the key words "MAY", "MUST, "MUST NOT", "optional",
"recommended", "SHOULD", and "SHOULD NOT", are to be interpreted as
described in [1].

Please note that the requirements specified in this document are to
be used in evaluating AAA protocol submissions. As such, the
requirements language refers to capabilities of these protocols; the
protocol documents will specify whether these features are required,
recommended, or optional. For example, requiring that a protocol
support confidentiality is NOT the same thing as requiring that all
protocol traffic be encrypted.

A protocol submission is not compliant if it fails to satisfy one or
more of the MUST or MUST NOT requirements for the capabilities that
it implements. A protocol submission that satisfies all the MUST,
MUST NOT, SHOULD and SHOULD NOT requirements for its capabilities is
said to be "unconditionally compliant"; one that satisfies all the
MUST and MUST NOT requirements but not all the SHOULD or SHOULD NOT
requirements for its protocols is said to be "conditionally
compliant."

1.2. Terminology

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

   Administrative Domain
             An internet, 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   A Broker is an entity that is in a different administrative
             domain from both the home AAA server and the local ISP, and
             which provides services, such as facilitating payments
             between the local ISP and home administrative entities.
             There are two different types of brokers; proxy and
             routing.

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

   End-to-End
             End-to-End is the security model that requires that
             security information be able to traverse, and be validated
             even when an AAA message is processed by intermediate nodes
             such as proxies, brokers, etc.

   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.

   Home Domain
            An administrative domain, containing the network whose
            prefix matches that of a mobile node's home address, and
            containing the AAA infrastructure needed to carry out the
            necessary operations enabling Mobile IP registrations.
            From the point of view of the home agent, the home domain
            is the local domain.

   Hop-by-hop
            Hop-by-hop is the security model that requires that each
            direct set of peers in a proxy network share a security
            association, and the security information does not traverse
            a AAA entity.

   Inter-domain Accounting
            Inter-domain accounting is the collection of information on
            resource usage of an entity within 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.

   Proxy   A AAA proxy is an entity that acts as both a client and a
            server. When a request is received from a client, the
            proxy acts as a AAA server. When the same request needs to
            be forwarded to another AAA entity, the proxy acts as a AAA
            client.

Local Proxy
          A Local Proxy is a AAA server that satisfies the definition
          of a Proxy, and exists within the same administrative
          domain as the network device (e.g., NAS) that issued the
          AAA request. Typically, a local proxy will enforce local
          policies prior to forwarding responses to the network
          devices, and are generally used to multiplex AAA messages
          from a large number of network devices.

Network Access Identifier
          The Network Access Identifier (NAI) is the userID submitted
          by the client during network access authentication. In
          roaming, the purpose of the NAI is to identify the user as
          well as to assist in the routing of the authentication
          request. The NAI may not necessarily be the same as the
          user's e-mail address or the user-ID submitted in an
          application layer authentication.

Routing Broker
          A Routing Broker is a AAA entity that satisfies the
          definition of a Broker, but is NOT in the transmission path
          of AAA messages between the local ISP and the home domain's
          AAA servers. When a request is received by a Routing
          Broker, information is returned to the AAA requester that
          includes the information necessary for it to be able to
          contact the Home AAA server directly. Certain
          organizations providing Routing Broker services MAY also
          act as a Certificate Authority, allowing the Routing Broker
          to return the certificates necessary for the local ISP and
          the home AAA servers to communicate securely.

Non-Proxy Broker
          A Routing Broker is occasionally referred to as a Non-Proxy
          Broker.

Proxy Broker
          A Proxy Broker is a AAA entity that satisfies the
          definition of a Broker, and acts as a Transparent Proxy by
          acting as the forwarding agent for all AAA messages between
          the local ISP and the home domain's AAA servers.

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.

Roaming Capability
        Roaming capability can be loosely defined as the ability to
        use any one of multiple Internet service providers (ISPs),
        while maintaining a formal, customer-vendor relationship
        with only one. Examples of cases where roaming capability
        might be required include ISP "confederations" and ISP-
        provided corporate network access support.

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.

Transparent Proxy
        A Transparent Proxy is a AAA server that satisfies the
        definition of a Proxy, but does not enforce any local
        policies (meaning that it does not add, delete or modify
        attributes or modify information within messages it
        forwards).

2. Requirements Summary

   The AAA protocol evaluation criteria for network access are
   summarized below. For details on the requirements, please consult
   the documents referenced in the footnotes.

2.1. General requirements

   These requirements apply to all aspects of AAA and thus are
   considered general requirements.

General Reqts.	NASREQ	ROAMOPS	MOBILE IP
Scalability a	M 12	M 3	M 30 39
Fail-over b	M 12		M 31
Mutual auth AAA client/server c	M 16		M 30
Transmission level security d		M 6	S 31 39
Data object Confidentiality e	M 26	M 6	M 40
Data object Integrity f	M 16	M 6	M 31 39
Certificate transport g	M 42		S/M 31,33/46

```
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                           |       |       |       |       |
|  Reliable AAA transport   |   M   |       |       |   M   |
|  mechanism                |   22  |       |       | 31 32 |
|         h                 |       |       |       |       |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                           |       |       |       |       |
|    Run Over IPv4          |   M   |   M   |       |   M   |
|                           |   11  |   1   |       |   33  |
|                           |       |       |       |       |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                           |       |       |       |       |
|    Run Over IPv6          |   M   |       |       |   S   |
|                           |   11  |   1   |       |   47  |
|                           |       |       |       |       |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                           |       |       |       |       |
|  Support Proxy and        |   M   |       |       |   M   |
|  Routing Brokers          |   12  |       |       | 31 39 |
|         i                 |       |       |       |       |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                           |       |       |       |       |
|  Auditability             |   S   |       |       |       |
|         j                 |   25  |       |       |       |
|                           |       |       |       |       |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                           |       |       |       |       |
|  Dual App and Transport   |       |   O   |       |   M   |
|   Security not required   |       |   6   |       |   40  |
|         k                 |       |       |       |       |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                           |       |       |       |       |
|  Ability to carry         |   M   |       |       |   S   |
|  service-specific attr.   |   43  |       |       | 31 33 |
|         l                 |       |       |       |       |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Key
M = MUST
S = SHOULD
O = MAY
N = MUST NOT
B = SHOULD NOT

Clarifications

[a]   The AAA protocol must be capable of supporting millions of users
      and tens of thousands of simultaneous requests. The AAA
      architecture and protocol MUST be capable of supporting tens of
      thousands of devices, AAA servers, proxies and brokers.

[b]   In the event of failure to communicate with a given server, the
      protocol must provide a mechanism to change service to another
      backup or secondary server.

[c]   This requirement refers to the ability to support mutual
      authentication between the AAA client and server.

[d]   The AAA protocol requires authentication, integrity protection
      and confidentiality at the transmission layer. This security
      model is also referred to as hop-by-hop security, whereas the
      security is established between two communicating peers. All of
      the security is removed when the AAA message is processed by a
      receiving AAA entity.

[e]   The AAA protocol requires confidentiality at the object level,
      where an object consists of one or more attributes. Object
      level confidentiality implies that only the target AAA entity
      for whom the data is ultimately destined may decrypt the data,
      regardless of the fact that the message may traverse one or more
      intermediate AAA entities (e.g., proxies, brokers).

[f]   The AAA protocol requires authentication and integrity
      protection at the object level, which consists of one or more
      attributes. Object level authentication must be persistent
      across one or more intermediate AAA entity (e.g., proxy, broker,
      etc), meaning that any AAA entity in a proxy chain may verify
      the authentication. This implies that data that is covered by
      object level security CANNOT be modified by intermediate
      servers.

[g]   The AAA protocol MUST be capable of transporting certificates.
      This requirement is intended as an optimization, in lieu of
      requiring that an out-of-band protocol be used to fetch
      certificates.

[h]   This requirement refers to resilience against packet loss,
      including:

      1. Hop-by-hop retransmission and fail-over so that reliability
         does not solely depend on single hop transport
         retransmission.

         2. Control of the retransmission mechanism by the AAA
            application.
         3. Acknowledgment by the transport that a message was delivered
            successfully, separate from message semantics or syntax
            evaluation.
         5. Piggy-backing of acknowledgments in AAA messages.
         6. Timely delivery of AAA responses.

   [i]   In the Mobile IP AAA architecture, brokers can be in the
         forwarding path, in which case they act as transparent proxies
         (proxy brokers). Alternatively, it is also possible to conceive
         of brokers operating as certifying authorities outside of the
         forwarding path (routing brokers).

   [j]   An auditable process is one in which it is possible to
         definitively determine what actions have been performed on AAA
         packets as they travel from the home AAA server to the network
         device and back.

   [k]   The AAA protocol MUST allow communication to be secured.
         However, the AAA protocol MUST also allow an underlying security
         service (e.g., IP Security) to be used. When the latter is
         used, the former MUST NOT be required.

   [l]   The AAA protocol MUST be extensible by third parties (e.g.,
         other IETF Working Groups), in order to define attributes that
         are specific to the service being defined. This requirement
         simply means that the AAA protocol MUST allow groups other than
         the AAA WG to define standard attributes.

2.2. Authentication Requirements

```
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                          |        |        |         |
| Authentication          | NASREQ | ROAMOPS | MOBILE  |
| Reqts.                   |        |        |   IP    |
|                          |        |        |         |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                          |        |        |         |
|    NAI Support           |    M   |    M   |   S/M   |
|        a                 |    9   |    2   |32,34,39/|
|                          |        |        |   40    |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                          |        |        |         |
|    CHAP Support          |    M   |    M   |         |
|        b                 |   10   |    3   |         |
|                          |        |        |         |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                          |        |        |         |
|    EAP Support           |    M   |    S   |         |
|        c                 |   10   |    3   |         |
|                          |        |        |         |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                          |        |        |         |
|    PAP/Clear-Text Support|    M   |    B   |         |
|        d                 |   26   |    3   |         |
|                          |        |        |         |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                          |        |        |         |
|    Re-authentication     |    M   |        |    S    |
|    on demand             |   17   |        |   33    |
|        e                 |        |        |         |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                          |        |        |         |
|    Authorization Only    |    M   |        |         |
|    without Authentication|    9   |        |         |
|        f                 |        |        |         |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Key
M = MUST
S = SHOULD
O = MAY
N = MUST NOT
B = SHOULD NOT

Clarifications

[a] The AAA protocol MUST allow the use of Network Access
     Identifiers (NAI) [8] to identify users and/or devices.

[b] The AAA protocol MUST allow CHAP [20] authentication information
     to be transported. This is commonly used by Network Access
     Servers that request authentication of a PPP user.

[c] The AAA protocol MUST allow for Extensible Authentication
     Protocol (EAP) [14] payload to be transported. Since some EAP
     authentication mechanisms require more than one round trip, the
     AAA protocol must allow for such authentication mechanisms to be
     used. The actual EAP authentication mechanism negotiated MUST
     be transparent to the AAA protocol. When EAP is used,
     authentication typically occurs between the user being
     authenticated and his/her home AAA server.

[d] While PAP is deprecated, it is still in widespread use for its
     original intended purpose, which is support of clear-text
     passwords. As a result, a AAA protocol will need to be able to
     securely transport clear-text passwords. This includes
     providing for confidentiality of clear-text passwords traveling
     over the wire, as well as protecting against disclosure of
     clear-text passwords to proxies in the forwarding path.

[e] The AAA protocol MUST allow for a user to be re-authenticated
     on-demand. The protocol MUST allow for this event to be
     triggered by either the user, access device (AAA client), or the
     home or visited AAA server.

[f] The AAA protocol MUST NOT require that credentials of the user
     be provided during authorization. The AAA protocol supports
     authorization by identification or assertion only.

2.3. Authorization Requirements

```
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                           |          |          |          |
| Authorization            | NASREQ   | ROAMOPS  | MOBILE   |
| Reqts.                    |          |          |  IP      |
|                           |          |          |          |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|  Static and Dynamic       |          |          |          |
|  IPv4/6 Address Assign.   |    M     |    M     |    M     |
|      a                    |    11    |    5     |  32 36   |
|                           |          |          |          |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                           |          |          |          |
|  RADIUS gateway           |    M     |    M     |    M     |
|  capability               |    44    |    3     |    45    |
|      b                    |          |          |          |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                           |          |          |          |
|  Reject                   |    M     |    M     |    M     |
|  capability               |    12    |    4     |    39    |
|      c                    |          |          |          |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                           |          |          |          |
|  Precludes layer 2        |    N     |    N     |          |
|  tunneling                |    11    |    5     |          |
|                           |          |          |          |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                           |          |          |          |
|  Re-Authorization on      |    M     |          |    S     |
|   demand                  |    18    |          |  30 33   |
|      d                    |          |          |          |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                           |          |          |          |
|  Support for Access Rules,|    M     |          |          |
|  Restrictions, Filters    |  11, 19  |          |          |
|      e                    |          |          |          |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                           |          |          |          |
|  State Reconciliation     |    M     |          |          |
|      f                    |    20    |          |          |
|                           |          |          |          |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                           |          |          |          |
|  Unsolicited Disconnect   |    M     |          |          |
|      g                    |    18    |          |          |
|                           |          |          |          |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Key
M = MUST
S = SHOULD
O = MAY
N = MUST NOT
B = SHOULD NOT

Clarifications

[a] The AAA protocol MUST allow a server to provide a static or
     dynamic address during the authorization phase of a user and/or
     device. The address assigned MUST be either of type IPv4 or
     IPv6. If both the client AND the server are aware of a pre-
     configured address, then it is considered static. Anything else
     is dynamic.

[b] This requirement refers to the ability of a new AAA protocol be
     sufficiently compatible with the large installed base of
     attributes for existing approaches (RADIUS), such that a server
     implementation could speak both protocols, or translate between
     them.

[c] This requirement refers to the ability of a proxy broker to deny
     access without forwarding the access request to the AAA server,
     or to deny access after receiving an access accept from the AAA
     server.

[d] This requirement refers to the ability of the AAA client or
     server to trigger re-authorization, or to the ability of the
     server to send updated authorization information to the device,
     such as "stop service." Authorization can allow for a time
     period, then additional authorization can be sought to continue.
     A server can initially authorize a user to connect and receive
     services, but later decide the user is no longer allowed use of
     the service, for example after N minutes. Authorizations can
     have a time limit. Re-authorization does not necessarily imply
     re-authentication.

[e] This requirement refers to the ability to of the protocol to
     describe access operational limitations and authorization
     restrictions to usage to the NAS which includes (but is not
     limited to):

     1. Session expirations and Idle Timeouts
     2. Packet filters
     3. Static routes
     4. QoS parameters

   [f] This requirement refers to the ability of the NAS to use the AAA
        server to manage resource allocation state. This capability can
        assist with, but it is not synonymous with, simultaneous user
        login control, port usage limitations, or IP address pooling.

        The design must provide for recovery from data loss due to a
        variety of faults, including NAS and AAA server reboots, and
        NAS/AAA server communication outages, and MUST be independent of
        the accounting stream. The granularity of the recovery of state
        information after an outage may be on the order of a fraction of
        a minute. In order to provide for state recovery, explicit
        session/resource status and update and disconnect messages will
        be required.

        Because of potential multi-domain issues, only systems that
        allocate or use a resource should track its state.

   [g] This requirement refers to the ability of the AAA server to
        request the NAS to disconnect an active session for
        authorization policy reasons.

2.4. Accounting Requirements

```
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                        |        |        |        |
| Accounting             | NASREQ | ROAMOPS| MOBILE |
| Reqts.                 |        |        | IP     |
|                        |        |        |        |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                        |        |        |        |
|   Real-time accounting |    M   |    M   |   M    |
|       a                |   14   |    7   |   31   |
|                        |        |        |        |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                        |        |        |        |
|   Mandatory Compact    |        |    M   |        |
|    Encoding            |        |    7   |        |
|       b                |        |        |        |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                        |        |        |        |
|   Accounting Record    |        |    M   |   M    |
|    Extensibility       |        |    7   |   33   |
|                        |        |        |        |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                        |        |        |        |
|   Batch Accounting     |    S   |        |        |
|       c                |   21   |        |        |
|                        |        |        |        |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                        |        |        |        |
|   Guaranteed Delivery  |    M   |        |   M    |
|       d                |   22   |        |   31   |
|                        |        |        |        |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                        |        |        |        |
|   Accounting Time Stamps|   M   |        |   M    |
|       e                |   23   |        |   40   |
|                        |        |        |        |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                        |        |        |        |
|   Dynamic Accounting   |    M   |        |        |
|       f                |   48   |        |        |
|                        |        |        |        |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Key
M = MUST
S = SHOULD
O = MAY
N = MUST NOT
B = SHOULD NOT

Clarifications

[a] This requirement may be loosely defined as reporting
     synchronously with events. Typically the time window is on the
     order of seconds, not milliseconds.

[b] The AAA protocol's Accounting data format MUST NOT be bloated,
     imposing a large overhead for one or more accounting data
     elements.

[c] This requirement refers to the ability to buffer or store
     multiple accounting records, and send them together at some
     later time.

[d] This is an application layer acknowledgment. This is sent when
     the receiving server is willing to take responsibility for the
     message data.

[e] This requirement refers to the ability to reflect the time of
     occurrence of events such as log-on, logoff, authentication,
     authorization and interim accounting. It also implies the
     ability to provide for unambiguous time-stamps.

[f] This requirement refers to the ability to account for dynamic
     authentication and authorization. To support this, there can be
     multiple accounting records for a single session.

2.5. Unique Mobile IP requirements

   In addition to the above requirements, Mobile IP also has the
   following additional requirements:

```
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                    |        |       |      |        |
|   Encoding of Mobile IP |   |       |      |   M    |
|   registration messages |   |       |      |   33   |
|                    |        |       |      |        |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                    |        |       |      |        |
|   Firewall friendly |       |       |      |   M    |
|        a           |        |       |      |   35   |
|                    |        |       |      |        |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                    |        |       |      |        |
|   Allocation of local Home |        |      |  S/M   |
|   agent            |        |       |      | 37/41  |
|                    |        |       |      |        |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Key
M = MUST
S = SHOULD
O = MAY
N = MUST NOT
B = SHOULD NOT

Clarifications

[a] A firewall friendly protocol is one which is designed to
     accommodate a firewall acting as a proxy. For example, this
     would permit a Home Agent AAA server situated behind a firewall
     to be reachable from the Internet for the purposes of providing
     AAA services to a Mobile IP Foreign Agent.

     Notes

     [1] Section 4.2.1 of [2]
     [2] Section 4.2.2 of [2]. Also see [8].
     [3] Section 4.2.3 of [2]. Also see [14].
     [4] Section 4.2.4 of [2].
     [5] Section 4.2.5 of [2].
     [6] Section 4.2.6 of [2].
     [7] Section 4.3 of [2].
     [8] Section 6 of [3]. Also see [6].
     [9] Section 8.2.2.2 of [3]. Also see [14].
     [10] Section 8.2.2.1 of [3]. Also see [14].
     [11] Section 8.3.2.2 of [3]. Also see [7].
     [12] Section 8.1.1 of [3].
     [13] Section 8.1.4.4 of [3].
     [14] Section 8.4.1.2 of [3].

          [15] Section 8.4.2 of [3].
          [16] Section 8.1.3 of [3].
          [17] Section 8.2.1.2 of [3].
          [18] Section 8.3.1.1 of [3].
          [19] Section 8.3.2.1 of [3]. Also see [7].
          [20] Section 8.3.2.3 of [3]. Also see [6], [7].
          [21] Section 8.4.1.3 of [3].
          [22] Section 8.4.1.1 of [3].
          [23] Section 8.4.1.4 of [3].
          [24] Section 8.4.3.1 of [3].
          [25] Section 8.4.3.2 of [3].
          [26] Section 8.2.3.1 of [3].
          [27] Section 8.3.3.1 of [3].
          [28] Section 8.1.4.1 of [3].
          [29] Refer [15]
          [30] Section 3 of [5]
          [31] Section 3.1 of [5]
          [32] Section 4 of [5]
          [33] Section 5 of [5]
          [34] Section 5.1 of [5]
          [35] Section 5.2 of [5]
          [36] Section 5.3 of [5]
          [37] Section 5.4 of [5]
          [38] Section 5.5 of [5]
          [39] Section 6 of [5]
          [40] Section 5.1 of [4]
          [41] Section 5.2.2 of [4]
          [42] Section 8.2.2.2 of [3]
          [43] Section 8.1.2.3 of [3]
          [44] Section 8.1.2.2 of [3]
          [45] Section 5.4 of [4]
          [46] Section 7 of [4]
          [47] Section 8 of [5]
          [48] Section 8.4.1.5 of [3]

3. References

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

   [2] Aboba, B. and G. Zorn, "Criteria for Evaluating Roaming
        Protocols", RFC 2477, January 1999.

   [3] Beadles, M. and D. Mitton, "Criteria for Evaluating Network
        Access Server Protocols", Work in Progress.

   [4] Hiller, T., et al., "Cdma2000 Wireless Data Requirements for
        AAA", Work in Progress.

[5]   Glass, S., Hiller, T., Jacobs, S. and C. Perkins, "Mobile IP
      Authentication, Authorization, and Accounting Requirements", RFC
      2977, October 2000.

[6]   Mitton, D., Beadles, M., "Network Access Server Requirements
      Next Generation (NASREQNG) NAS Model", RFC 2881, July 2000.

[7]   Mitton, D., "Network Access Server Requirements: Extended RADIUS
      Practices", RFC 2882, July 2000.

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

[9]   Rigney, C., Willens, S., Rubens, A. and W. Simpson, "Remote
      Authentication Dial In User Service (RADIUS)", RFC 2865, June
      2000.

[10] Rigney, C., "RADIUS Accounting", RFC 2866, June 2000.

[11] Simpson, W., Editor, "The Point-to-Point Protocol (PPP)", STD
      51, RFC 1661, July 1994.

[12] Sklower, K., Lloyd, B., McGregor, G., Carr, D. and T. Coradetti,
      "The PPP Multilink Protocol (MP)", RFC 1990, August 1996.

[13] Simpson, W., Editor, "PPP LCP Extensions", RFC 1570, January
      1994.

[14] Blunk, L. and J. Vollbrecht, "PPP Extensible Authentication
      Protocol (EAP)", RFC 2284, March 1998.

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

[16] Calhoun, P. and C. Perkins, "Mobile IP Network Access Identifier
      Extension for IPv4", RFC 2794, March 2000.

[17] Perkins, C., "IP Mobility Support", RFC 2002, Oct 1996.

[18] Johnson, D. and C. Perkins, "Mobility Support in IPv6", Work in
      Progress.

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

[20] Simpson, W., "PPP Challenge Handshake Authentication Protocol
      (CHAP)", RFC 1994, August 1996.

4. Security Considerations

   This document, being a requirements document, does not have any
   security concerns. The security requirements on protocols to be
   evaluated using this document are described in the referenced
   documents.

5. IANA Considerations

   This memo does not create any new number spaces for IANA
   administration.

6. Acknowledgments

   Thanks to the members of the Mobile IP, AAA, and NASREQ working
   groups who have discussed and commented on these requirements. We
   would also like to thank the members of the AAA evaluation team, Mike
   St. Johns, Barney Wolf, Mark Stevens, David Nelson, Dave Mitton,
   Basavaraj Patil and Stuart Barkley for their thorough review of this
   document.

7. Authors' Addresses

   Bernard Aboba
   Microsoft Corporation
   One Microsoft Way
   Redmond, WA 98052

   Phone: +1 425-936-6605
   Fax: +1 425-936-7329
   EMail: bernarda@microsoft.com

   Pat R. Calhoun
   Network and Security Research Center, Sun Labs
   Sun Microsystems, Inc.
   15 Network Circle
   Menlo Park, CA 94025

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

Steven M. Glass
Sun Microsystems
1 Network Drive
Burlington, MA 01845

Phone: +1 781-442-0504
Fax: +1 781-442-1677
EMail: steven.glass@sun.com

Tom Hiller
Wireless Data Standards & Architectures
Lucent Technologies
263 Shuman Drive
Room 1HP2F-218
Naperville, IL 60563

Phone: +1 630-976-7673
EMail: tom.hiller@lucent.com

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

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

Hajime Shiino
Lucent Technologies Japan Ltd.
25 Mori Bldg. 1-4-30 Roppongi,
Minato-ku Tokyo
Japan

Phone: +81-3-5561-3695
EMail: hshiino@lucent.com

Glen Zorn
Cisco Systems, Inc.
500 108th Avenue N.E., Suite 500
Bellevue, WA 98004

Phone: +1 425-468-0955
EMail: gwz@cisco.com

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

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

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

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

Basavaraj Patil
Nokia Networks
6000 Connection Dr.
Irving, TX 75039

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

David Mitton
Nortel Networks
880 Technology Park Drive
Billerica, MA 01821

Phone: +1 978-288-4570
EMail: dmitton@nortelnetworks.com

Serge Manning
Nortel Networks
2201 Lakeside Blvd
Richardson, TX 75082-4399

Phone: +1 972-684-7277
EMail: smanning@nortelnetworks.com

Mark Anthony Beadles
SmartPipes, Inc.
565 Metro Place South
Suite 300
Dublin, OH 43017

Phone: +1 614-923-5657
EMail: mbeadles@smartpipes.com

Pat Walsh
Lucent Technologies
263 Shuman Blvd.
1F-545
Naperville, IL

Phone: +1 630-713-5063
EMail: walshp@lucent.com

Xing Chen
Alcatel USA
1000 Coit Road
Plano, TX 75075

Phone: +1 972-519-4142
Fax: +1 972-519-3300
EMail: xing.chen@usa.alcatel.com

Sanjeevan Sivalingham
Ericsson Wireless Communications Inc.,
Rm Q-356C
6455 Lusk Blvd
San Diego, CA 92126

Phone: +1 858-332-5670
EMail: s.sivalingham@ericsson.com

Alan Hameed
Fujitsu
2801 Telecom Parkway
Richardson, TX 75082

Phone: +1 972-479-2089

      Mark Munson
      GTE Wireless
      One GTE Place
      Alpharetta, GA   30004

      Phone: +1 678-339-4439
      EMail: mmunson@mobilnet.gte.com

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

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

      Byung-Keun Lim
      LG Electronics, Ltd.
      533, Hogye-dong, Dongan-ku, Anyang-shi,
      Kyungki-do,431-080
      Korea

      Phone: +82-31-450-7199
      Fax: +82-31-450-7050
      EMail: bklim@lgic.co.kr

      Brent Hirschman
      1501 Shure Dr.
      Arlington Hieghts, IL 60006

      Phone: +1 847-632-1563
      EMail: qa4053@email.mot.com

      Raymond T. Hsu
      Qualcomm Inc.
      6455 Lusk Blvd.
      San Diego, CA 92121

      Phone: +1 619-651-3623
      EMail: rhsu@qualcomm.com

Haeng S. Koo
Samsung Telecommunications America, Inc.
1130 E. Arapaho Road
Richardson, TX 75081

Phone: +1 972-761-7755
EMail: hskoo@sta.samsung.com

Mark A. Lipford
Sprint PCS
8001 College Blvd.; Suite 210
Overland Park, KS 66210

Phone: +1 913-664-8335
EMail: mlipfo01@sprintspectrum.com

Ed Campbell
3Com Corporation
1800 W. Central Rd.
Mount Prospect, IL 60056

Phone: +1 847-342-6769
EMail: ed_campbell@3com.com

Name: Yingchun Xu
WaterCove Networks
One Century Centre, Suite 550
1750 E. Golf Road
Schaumburg, IL

Phone: +1 847-477-9280
EMail: yxu@watercove.com

Shinichi Baba
Toshiba America Research, Inc.
PO Box 136,
Convent Station, NJ 07961-0136

Phone: +1 973-829-4795
EMail: sbaba@tari.toshiba.com

      Eric Jaques
      Vodafone AirTouch
      2999 Oak Road, MS-750
      Walnut Creek, CA 94596

      Phone: +1 925-279-6142
      EMail: ejaques@akamail.com

8. Intellectual Property Statement

   The IETF takes no position regarding the validity or scope of any
   intellectual property or other rights that might be claimed to
   pertain to the implementation or use of the technology described in
   this document or the extent to which any license under such rights
   might or might not be available; neither does it represent that it
   has made any effort to identify any such rights. Information on the
   IETF's procedures with respect to rights in standards-track and
   standards-related documentation can be found in BCP-11. Copies of
   claims of rights made available for publication and any assurances of
   licenses to be made available, or the result of an attempt made to
   obtain a general license or permission for the use of such
   proprietary rights by implementors or users of this specification can
   be obtained from the IETF Secretariat.

   The IETF invites any interested party to bring to its attention any
   copyrights, patents or patent applications, or other proprietary
   rights which may cover technology that may be required to practice
   this standard. Please address the information to the IETF Executive
   Director.

9. Full Copyright Statement

Acknowledgement