             Network Access Server Requirements Next Generation (NASREQNG)
                              NAS Model

Status of this Memo

Copyright Notice

Abstract

   This document describes the terminology and gives a model of typical
   Network Access Server (NAS). The purpose of this effort is to set
   the reference space for describing and evaluating NAS service
   protocols, such as RADIUS (RFCs 2865, 2866) [1], [2] and follow-on
   efforts like AAA Working Group, and the Diameter protocol [3]. These
   are protocols for carrying user service information for
   authentication, authorization, accounting, and auditing, between a
   Network Access Server which desires to authenticate its incoming
   calls and a shared authentication server.

Table of Contents

1. Introduction

   A Network Access Server is the initial entry point to a network for
   the majority of users of network services. It is the first device in
   the network to provide services to an end user, and acts as a gateway
   for all further services. As such, its importance to users and
   service providers alike is paramount. However, the concept of a
   Network Access Server has grown up over the years without being
   formally defined or analyzed [4].

1.1 Scope of this Document

   There are several tradeoffs taken in this document. The purpose of
   this document is to describe a model for evaluating NAS service
   protocols. It will give examples of typical NAS hardware and
   software features, but these are not to be taken as hard limitations
   of the model, but merely illustrative of the points of discussion.
   An important goal of the model is to offer a framework that allows
   further development and expansion of capabilities in NAS
   implementation.

   As with most IETF projects, the focus is on standardizing the
   protocol interaction between the components of the system. The
   documents produced will not address the following areas:

   - AAA server back-end implementation is abstracted and not
     prescribed. The actual organization of the data in the server, its
     internal interfaces, and capabilities are left to the
     implementation.

- NAS front-end call technology is not assumed to be static.
  Alternate and new technology will be accommodated. The resultant
  protocol specifications must be flexible in design to allow for new
  technologies and services to be added with minimal impact on
  existing implementations.

1.2 Specific Terminology

   The following terms are used in this document in this manner: A
   "Call" - the initiation of a network service request to the NAS.
   This can mean the arrival of a telephone call via a dial-in or
   switched telephone network connection, or the creation of a tunnel to
   a tunnel server which becomes a virtual NAS. A "Session" - is the
   NAS provided service to a specific authorized user entity.

2. Network Access System Equipment Assumptions

   A typical hardware-based NAS is implemented in a constrained system.
   It is important that the NAS protocols don't assume unlimited
   resources on the part of the platform. The following are typical
   constraints:

   - A computer system of minimal to moderate performance
     (example processors: Intel 386 or 486, Motorola 68000)
   - A moderate amount, but not large RAM (typically varies with
     supported # of ports 1MB to 8MB)
   - Some small amount of non-volatile memory, and/or way to be
     configured out-of-band
   - No assumption of a local file system or disk storage

   A NAS system may consist of a system of interconnected specialized
   processor system units. Typically they may be circuit boards (or
   blades) that are arrayed in a card cage (or chassis) and referred to
   by their position (i.e., slot number). The bus interconnection
   methods are typically proprietary and will not be addressed here.

   A NAS is sometimes referred to as a Remote Access Server (RAS) as it
   typically allows remote access to a network. However, a more general
   picture is that of an "Edge Server", where the NAS sits on the edge
   of an IP network of some type, and allows dynamic access to it.

   Such systems typically have;

   - At least one LAN or high performance network interface (e.g.,
     Ethernet, ATM, FR)

- At least one, but typically many, serial interface ports, which
  could be;
  - serial RS232 ports direct wired or wired to a modem, or
  - have integral hardware or software modems (V.22bis,V.32, V.34,
    X2, Kflex, V.90, etc.)
  - have direct connections to telephone network digital WAN lines
    (ISDN, T1, T3, NFAS, or SS7)
  - an aggregation of xDSL connections or PPPoe sessions [5].

However, systems may perform some of the functions of a NAS, but not
have these kinds of hardware characteristics. An example would be a
industry personal computer server system, that has several modem line
connections. These lines will be managed like a dedicated NAS, but
the system itself is a general file server. Likewise, with the
development of tunneling protocols (L2F [6], ATMP [7], L2TP [8]),
tunnel server systems must behave like a "virtual" NAS, where the
calls come from the network tunneled sessions and not hardware ports
([11], [9], [10]).

3. NAS Services

The core of what a NAS provides, are dynamic network services. What
distinguishes a NAS from a typical routing system, is that these
services are provided on a per-user basis, based on an authentication
and the service is accounted for. This accounting may lead to
policies and controls to limit appropriate usage to levels based on
the availability of network bandwidth, or service agreements between
the user and the provider.

Typical services include:

- dial-up or direct access serial line access; Ability to access the
  network using a the public telephone network.
- network access (SLIP, PPP, IPX, NETBEUI, ARAP); The NAS allows the
  caller to access the network directly.
- asynchronous terminal services (Telnet, Rlogin, LAT, others); The
  NAS implements the network protocol on behalf of the caller, and
  presents a terminal interface.
- dial-out connections; Ability to cause the NAS to initiate a
  connection over the public telephone network, typically based on the
  arrival of traffic to a specific network system.
- callback (NAS generates call to caller); Ability to cause the NAS to
  reverse or initiate a network connection based on the arrival of a
  dial-in call.
- tunneling (from access connection to remote server); The NAS
  transports the callers network packets over a network to a remote
  server using an encapsulation protocol. (L2TP [8], RADIUS support
  [11])

4. Authentication, Authorization and Accounting (AAA) Servers

   Because of the need to authenticate and account, and for practical
   reasons of implementation, NAS systems have come to depend on
   external server systems to implement authentication databases and
   accounting recording.

   By separating these functions from the NAS equipment, they can be
   implemented in general purpose computer systems, that may provide
   better suited long term storage media, and more sophisticated
   database software infrastructures. Not to mention that a centralized
   server can allow the coordinated administration of many NAS systems
   as appropriate (for example a single server may service an entire POP
   consisting of multiple NAS systems).

   For ease of management, there is a strong desire to piggyback NAS
   authentication information with other authentication databases, so
   that authentication information can be managed for several services
   (such as OS shell login, or Web Server access) from the same
   provider, without creating separate passwords and accounts for the
   user.

   Session activity information is stored and processed to produce
   accounting usage records. This is typically done with a long term
   (nightly, weekly or monthly) batch type process.

   However, as network operations grow in sophistication, there are
   requirements to provide real-time monitoring of port and user status,
   so that the state information can be used to implement policy
   decisions, monitor user trends, and the ability to possibly terminate
   access for administrative reasons. Typically only the NAS knows the
   true dynamic state of a session.

5. Typical NAS Operation Sequence:

   The following details a typical NAS operational sequence:

      - Call arrival on port or network
        - Port:
          - auto-detect (or not) type of call
          - CLI/SLIP: prompt for username and password (if security
            set)
          - PPP: engage LCP, Authentication
          - Request authentication from AAA server
          - if okay, proceed to service
          - may challenge
          - may ask for password change/update

          - Network:
             - activate internal protocol server (telnet, ftp)
             - engage protocol's authentication technique
             - confirm authentication information with AAA server

       - Call Management Services
          - Information from the telephone system or gateway controller
            arrives indicating that a call has been received
          - The AAA server is consulted using the information supplied by
            the telephone system (typically Called or Calling number
            information)
          - The server indicates whether to respond to the call by
            answering it, or by returning a busy to the caller.
          - The server may also need to allocate a port to receive a
            call, and route it accordingly.

       - Dial-out
          - packet destination matches outbound route pre-configured
          - find profile information to setup call
          - Request information from AAA server for call details

       - VPN/Tunneling (compulsory)
          - authentication server identifies user as remote
          - tunnel protocol is invoked to a remote server
          - authentication information may be forwarded to remote AAA
            server
          - if successful, the local link is given a remote identity

       - Multi-link aggregation
          - after a new call is authenticated by the AAA server, if MP
            options are present, then other bundles with the same
            identifying information is searched for
          - bundle searches are performed across multiple systems
          - join calls that match authentication and originator
            identities as one network addressable data source with a
            single network IP address

       - Hardwired (non-interactive) services
          - permanent WAN connections (Frame Relay or PSVCs)
          - permanent serial connections (printers)

5.1 Characteristics of Systems and Sessions:

   Sessions must have a user identifier and authenticator to complete
   the authentication process. Accounting starts from time of call or
   service, though finer details are allowed. At the end of service, the
   call may be disconnected or allow re-authentication for additional
   services.

   Some systems allow decisions on call handling to be made based on
   telephone system information provided before the call is answered
   (e.g., caller id or destination number). In such systems, calls may
   be busied-out or non-answered if system resources are not ready or
   available.

   Authorization to run services are supplied and applied after
   authentication. A NAS may abort call if session authorization
   information disagrees with call characteristics. Some system
   resources may be controlled by server driven policies

   Accounting messages are sent to the accounting server when service
   begins, and ends, and possibly periodically during service delivery.
   Accounting is not necessarily a real-time service, the NAS may be
   queue and batch send event records.

5.2 Separation of NAS and AAA server functions

   As a distributed system, there is a separation of roles between the
   NAS and the Server:

     - Server provides authentication services; checks passwords
       (static or dynamic)
     - Server databases may be organized in any way (only protocol
       specified)
     - Server may use external systems to authenticate (including OS
       user databases, token cards, one-time-lists, proxy or other
       means)
     - Server provides authorization information to NAS
     - The process of providing a service may lead to requests for
       additional information
     - Service authorization may require real-time enforcement
       (services may be based on Time of Day, or variable cost
       debits)
     - Session accounting information is tallied by the NAS and
       reported to server

5.3 Network Management and Administrative features

   The NAS system is presumed to have a method of configuration that
   allows it to know it's identity and network parameters at boot time.
   Likewise, this configuration information is typically managed using
   the standard management protocols (e.g., SNMP). This would include
   the configuration of the parameters necessary to contact the AAA
   server itself. The purpose of the AAA server is not to provide
   network management for the NAS, but to authorize and characterize the
   individual services for the users. Therefore any feature that can be
   user specific is open to supply from the AAA server.

The system may have other operational services that are used to run
and control the NAS. Some users that have _Administrative_
privileges may have access to system configuration tools, or services
that affect the operation and configuration of the system (e.g.,
loading boot images, internal file system access, etc..) Access to
these facilities may also be authenticated by the AAA server
(provided it is configured and reachable!) and levels of access
authorization may be provided.

6. Authentication Methods

   A NAS system typically supports a number of authentication systems.
   For async terminal users, these may be a simple as a prompt and
   input. For network datalink users, such as PPP, several different
   authentication methods will be supported (PAP, CHAP [12], MS-CHAP
   [13]). Some of these may actually be protocols in and of themselves
   (EAP [14] [15], and Kerberos).

   Additionally, the content of the authentication exchanges may not be
   straightforward. Hard token cards, such as the Safeword and SecurId,
   systems may generate one-time passphrases that must be validated
   against a proprietary server. In the case of multi-link support, it
   may be necessary to remember a session token or certificate for the
   later authentication of additional links.

   In the cases of VPN and compulsory tunneling services, typically a
   Network Access Identifier (RFC 2486 [16]) is presented by the user.
   This NAI is parsed into a destination network identifier either by
   the NAS or by the AAA server. The authentication information will
   typically not be validated locally, but by a AAA service at the
   remote end of the tunnel service.

7. Session Authorization Information

   Once a user has been authenticated, there are a number of individual
   bits of information that the network management may wish to configure
   and authorize for the given user or class of users.

   Typical examples include:

        For async terminal users:

        - banners
        - custom prompts
        - menus
        - CLI macros - which could be used for: shortcuts, compound
          commands, restrictive scripts

For network users:

- addresses, and routes
- callback instructions
- packet and activity filters
- network server addresses
- host server addresses

Some services may require dynamic allocation of resources.
Information about the resources required may not be known during the
authentication phase, it may come up later. (e.g., IP Addresses for
multi-link bundles) It's also possible that the authorization will
change over the time of the session. To provide these there has to be
a division of responsibility between the NAS and the AAA server, or a
cooperation using a stateful service.

Such services include:

- IP Address management
- Concurrent login limitations
- Tunnel usage limitations
- Real-time account expirations
- Call management policies

In the process of resolving resource information, it may be required
that a certain level of service be supplied, and if not available,
the request refused, or corrective action taken.

8. IP Network Interaction

As the NAS participates in the IP network, it interacts with the
routing mechanisms of the network itself. These interactions may
also be controlled on a per-user/session basis.

For example, some input streams may be directed to specific hosts
other than the default gateway for the destination subnet. In order
to control services within the network provider's infrastructure,
some types of packets may be discarded (filtered) before entering the
network. These filters could be applied based on examination of
destination address and port number. Anti-spoofing packet controls
may be applied to disallow traffic sourced from addresses other than
what was assigned to the port.

A NAS may also be an edge router system, and apply Quality of Service
(QoS) policies to the packets. This makes it a QOS Policy
Enforcement Point [19], [17]. It may learn QOS and other network
policies for the user via the AAA service.

9. A NAS Model

   So far we have looked at examples of things that NASes do. The
   following attempts to define a NAS model that captures the
   fundamentals of NAS structure to better categorize how it interacts
   with other network components.

   A Network Access Server is a device which sits on the edge of a
   network, and provides access to services on that network in a
   controlled fashion, based on the identity of the user of the network
   services in question and on the policy of the provider of these
   services. For the purposes of this document, a Network Access Server
   is defined primarily as a device which accepts multiple point-to-
   point [18] links on one set of interfaces, providing access to a
   routed network or networks on another set of interfaces.

   Note that there are many things that a Network Access Server is not.
   A NAS is not simply a router, although it will typically include
   routing functionality in it's interface to the network. A NAS is not
   necessarily a dial access server, although dial access is one common
   means of network access, and brings its own particular set of
   requirements to NAS's.

   A NAS is the first device in the IP network to provide services to an
   end user, and acts as a gateway for all further services. It is the
   point at which users are authenticated, access policy is enforced,
   network services are authorized, network usage is audited, and
   resource consumption is tracked. That is, a NAS often acts as the
   policy enforcement point for network AAAA (authentication,
   authorization, accounting, and auditing) services. A NAS is
   typically the first place in a network where security measures and
   policy may be implemented.

9.1 A Reference Model of a NAS

   For reference in the following discussion, a diagram of a NAS, its
   dependencies, and its interfaces is given below. This diagram is
   intended as an abstraction of a NAS as a reference model, and is not
   intended to represent any particular NAS implementation.

```
                           Users
                        v v v v v v v
                        | | PSTN  | |
                        | |  or   | |
                        |encapsulated
                     +-----------------+
                     |    (Modems)     |
                     +-----------------+
                       | | | | | | |
                  +--+---------------------------+
                  |  |                           |
                  |N |      Client Interface     |
                  |  |                           |
                  |A +---------Routing ----------+
                  |  |                           |
                  |S |    Network Interface      |
                  |  |                           |
                  +--+---------------------------+
                       /       |       \
                      /        |        \
                     /         |         \
                    /          |          \
   POLICY MANAGEMENT/          |           \  DEVICE MANAGEMENT
   +---------------+           |             +------------------+
   | Authentication|         _/^\_          |Device Provisioning|
   +---------------+        _/   \_          +------------------+
   | Authorization |      _/       \_        |Device Monitoring |
   +---------------+     _/           \_      +------------------+
   | Accounting    |    /     The       \
   +---------------+    \_  Network(s)  _/
   | Auditing      |     \_           _/
   +---------------+       \_       _/
                            \_    _/
                              \_/
```

9.2 Terminology

   Following is a description of the modules and interfaces in the
   reference model for a NAS given above:

   Client Interfaces - A NAS has one or more client interfaces, which
      provide the interface to the end users who are requesting network
      access. Users may connect to these client interfaces via modems
      over a PSTN, or via tunnels over a data network. Two broad
      classes of NAS's may be defined, based on the nature of the
      incoming client interfaces, as follows. Note that a single NAS
      device may serve in both classes:

   Dial Access Servers - A Dial Access Server is a NAS whose client
      interfaces consist of modems, either local or remote, which are
      attached to a PSTN.

   Tunnel Servers - A Tunnel Server is a NAS whose client interfaces
      consists of tunneling endpoints in a protocol such as L2TP

   Network Interfaces - A NAS has one or more network interfaces, which
      connect to the networks to which access is being granted.

   Routing - If the network to which access is being granted is a routed
      network, then a NAS will typically include routing functionality.

   Policy Management Interface - A NAS provides an interface which
      allows access to network services to be managed on a per-user
      basis. This interface may be a configuration file, a graphical
      user interface, an API, or a protocol such as RADIUS, Diameter, or
      COPS [19]. This interface provides a mechanism for granular
      resource management and policy enforcement.

   Authentication - Authentication refers to the confirmation that a
      user who is requesting services is a valid user of the network
      services requested. Authentication is accomplished via the
      presentation of an identity and credentials. Examples of types of
      credentials are passwords, one-time tokens, digital certificates,
      and phone numbers (calling/called).

   Authorization - Authorization refers to the granting of specific
      types of service (including "no service") to a user, based on
      their authentication, what services they are requesting, and the
      current system state. Authorization may be based on restrictions,
      for example time-of-day restrictions, or physical location
      restrictions, or restrictions against multiple logins by the same
      user. Authorization determines the nature of the service which is
      granted to a user. Examples of types of service include, but are
      not limited to: IP address filtering, address assignment, route
      assignment, QoS/differential services, bandwidth control/traffic
      management, compulsory tunneling to a specific endpoint, and
      encryption.

   Accounting - Accounting refers to the tracking of the consumption of
      NAS resources by users. This information may be used for
      management, planning, billing, or other purposes. Real-time
      accounting refers to accounting information that is delivered
      concurrently with the consumption of the resources. Batch
      accounting refers to accounting information that is saved until it

is delivered at a later time. Typical information that is
gathered in accounting is the identity of the user, the nature of
the service delivered, when the service began, and when it ended.

Auditing - Auditing refers to the tracking of activity by users. As
opposed to accounting, where the purpose is to track consumption
of resources, the purpose of auditing is to determine the nature
of a user's network activity. Examples of auditing information
include the identity of the user, the nature of the services used,
what hosts were accessed when, what protocols were used, etc.

AAAA Server - An AAAA Server is a server or servers that provide
authentication, authorization, accounting, and auditing services.
These may be co-located with the NAS, or more typically, are
located on a separate server and communicate with the NAS's User
Management Interface via an AAAA protocol. The four AAAA
functions may be located on a single server, or may be broken up
among multiple servers.

Device Management Interface - A NAS is a network device which is
owned, operated, and managed by some entity. This interface
provides a means for this entity to operate and manage the NAS.
This interface may be a configuration file, a graphical user
interface, an API, or a protocol such as SNMP [20].

Device Monitoring - Device monitoring refers to the tracking of
status, activity, and usage of the NAS as a network device.

Device Provisioning - Device provisioning refers to the
configurations, settings, and control of the NAS as a network
device.

9.3 Analysis

Following is an analysis of the functions of a NAS using the
reference model above:

9.3.1 Authentication and Security

NAS's serve as the first point of authentication for network users,
providing security to user sessions. This security is typically
performed by checking credentials such as a PPP PAP user
name/password pair or a PPP CHAP user name and challenge/response,
but may be extended to authentication via telephone number
information, digital certificates, or biometrics. NAS's also may
authenticate themselves to users. Since a NAS may be shared among
multiple administrative entities, authentication may actually be
performed via a back-end proxy, referral, or brokering process.

   In addition to user security, NAS's may themselves be operated as
   secure devices. This may include secure methods of management and
   monitoring, use of IP Security [21] and even participation in a
   Public Key Infrastructure.

9.3.2 Authorization and Policy

   NAS's are the first point of authorization for usage of network
   resources, and NAS's serve as policy enforcement points for the
   services that they deliver to users. NAS's may provision these
   services to users in a statically or dynamically configured fashion.
   Resource management can be performed at a NAS by granting specific
   types of service based on the current network state. In the case of
   shared operation, NAS policy may be determined based on the policy of
   multiple end systems.

9.3.3 Accounting and Auditing

   Since NAS services are consumable resources, usage information must
   often be collected for the purposes of soft policy management,
   reporting, planning, and accounting. A dynamic, real-time view of
   NAS usage is often required for network auditing purposes. Since a
   NAS may be shared among multiple administrative entities, usage
   information must often be delivered to multiple endpoints.
   Accounting is performed using such protocols as RADIUS [2].

9.3.4 Resource Management

   NAS's deliver resources to users, often in a dynamic fashion.
   Examples of the types of resources doled out by NAS's are IP
   addresses, network names and name server identities, tunnels, and
   PSTN resources such as phone lines and numbers. Note that NAS's may
   be operated in a outsourcing model, where multiple entities are
   competing for the same resources.

9.3.5 Virtual Private Networks (VPN's)

   NAS's often participate in VPN's, and may serve as the means by which
   VPN's are implemented. Examples of the use of NAS's in VPN's are:
   Dial Access Servers that build compulsory tunnels, Dial Access
   Servers that provide services to voluntary tunnelers, and Tunnel
   Servers that provide tunnel termination services. NAS's may
   simultaneously provide VPN and public network services to different
   users, based on policy and user identity.

9.3.6 Service Quality

   A NAS may delivery different qualities, types, or levels of service
   to different users based on policy and identity. NAS's may perform
   bandwidth management, allow differential speeds or methods of access,
   or even participate in provisioned or signaled Quality of Service
   (QoS) networks.

9.3.7 Roaming

   NAS's are often operated in a shared or outsourced manner, or a NAS
   operator may enter into agreements with other service providers to
   grant access to users from these providers (roaming operations).
   NAS's often are operated as part of a global network. All these
   imply that a NAS often provides services to users from multiple
   administrative domains simultaneously. The features of NAS's may
   therefore be driven by requirements of roaming [22].

10. Security Considerations

   This document describes a model not a particular solution.

   As mentioned in section 9.3.1 and elsewhere, NAS'es are concerned
   about the security of several aspects of their operation, including:

      - Providing sufficiently robust authentication techniques as
        required by network policies,
      - NAS authentication of configured authentication server(s),
      - Server ability to authenticate configured clients,
      - Hiding of the authentication information from network snooping
        to protect from attacks and provide user privacy,
      - Protecting the integrity of message exchanges from attacks
        such as; replay, or man-in-the middle,
      - Inability of other hosts to interfere with services authorized
        to NAS, or gain unauthorized services,
      - Inability of other hosts to probe or guess at authentication
        information.
      - Protection of NAS system configuration and administration from
        unauthorized users
      - Protection of the network from illegal packets sourced by
        accessing connections

11. References

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

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

   [3]   Calhoun, P., "Diameter Base Protocol", Work in Progress.

   [4]   Zorn, G., "Yet Another Authentication Protocol (YAAP)", Work in
         Progress.

   [5]   Mamakos, L., Lidl, K., Evarts, K., Carrel, D., Simone, D. and R.
         Wheeler, "A Method for Transmitting PPP Over Ethernet (PPPoE)",
         RFC 2516, February 1999.

   [6]   Valencia, A., Littlewood, M. and T. Kolar, "Cisco Layer Two
         Forwarding (Protocol) L2F", RFC 2341, May 1998.

   [7]   Hamzeh, K., "Ascend Tunnel Management Protocol - ATMP", RFC
         2107, February 1997.

   [8]   Valencia, A., Townsley, W., Rubens, A., Pall, G., Zorn, G., and
         B. Palter, "Layer Two Tunneling Protocol (L2TP)", RFC 2661,
         August 1999.

   [9]   Zorn, G., Leifer, D., Rubens, A., Shriver, J. and M. Holdrege,
         "RADIUS Attributes for Tunnel Protocol Support", RFC 2868, June
         2000.

   [10] Zorn, G., Aboba, B. and D. Mitton, "RADIUS Accounting
         Modifications for Tunnel Protocol Support", RFC 2867, June 2000.

   [11] Aboba, B. and G. Zorn, "Implementation of PPTP/L2TP Compulsory
         Tunneling via RADIUS", RFC 2809, April 2000.

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

   [13] Zorn, G. and S. Cobb, "Microsoft PPP CHAP Extensions", RFC 2433,
         March 1998.

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

   [15] Calhoun, et al., "Extensible Authentication Protocol Support in
         RADIUS", Work in Progress.

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

   [17] Braden, R., Zhang, L., Berson, S., Herzog, S. and S. Jamin,
        "Resource ReSerVation Protocol (RSVP) Version 1 Functional
        Specification", RFC 2205, September 1997.

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

   [19] Boyle, J., Cohen, R., Durham, D., Herzog, S., Raja, R. and A.
        Sastry. "The COPS (Common Open Policy Service) Protocol", RFC
        2748, January 2000.

   [20] Case, J., Fedor, M., Schoffstall, M. and J. Davin. "A Simple
        Network Management Protocol (SNMP)", STD 15, RFC 1157, May 1990.

   [21] Atkinson, R. and S. Kent, "Security Architecture for the
        Internet Protocol", RFC 2401, November 1998.

   [22] Aboba, Zorn, "Dialup Roaming Requirements", Work in Progress.

12. Acknowledgments

   This document is a synthesis of my earlier draft and Mark Beadles'
   NAS Reference Model draft.

13. Authors' Addresses

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

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

   Mark Beadles
   SmartPipes Inc.
   545 Metro Place South
   Suite 100
   Dublin, OH 43017

   Phone: 614-327-8046
   EMail: mbeadles@smartpipes.com

14. Appendix - Acronyms and Glossary:

   AAA - Authentication, Authorization, Accounting, The three primary
   services required by a NAS server or protocol.

   NAS - Network Access Server, a system that provides access to a
   network. In some cases also know as a RAS, Remote Access Server.

   CLI - Command Line Interface, an interface to a command line service
   for use with an common asynchronous terminal facility.

   SLIP - Serial Line Internet Protocol, an IP-only serial datalink,
   predecessor to PPP.

   PPP - Point-to-Point Protocol; a serial datalink level protocol that
   supports IP as well as other network protocols. PPP has three major
   states of operation: LCP - Link layer Control Protocol,
   Authentication, of which there are several types (PAP, CHAP, EAP),
   and NCP - Network layer Control Protocol, which negotiates the
   network layer parameters for each of the protocols in use.

   IPX - Novell's NetWare transport protocol

   NETBEUI - A Microsoft/IBM LAN protocol used by Microsoft file
   services and the NETBIOS applications programming interface.

   ARAP - AppleTalk Remote Access Protocol

   LAT - Local Area Transport; a Digital Equipment Corp. LAN protocol
   for terminal services.

   PPPoe - PPP over Ethernet; a protocol that forwards PPP frames on an
   LAN infrastructure. Often used to aggregate PPP streams at a common
   server bank.

   VPN - Virtual Private Network; a term for networks that appear to be
   private to the user by the use of tunneling techniques.

   FR - Frame Relay, a synchronous WAN protocol and telephone network
   intraconnect service.

   PSVC - Permanent Switched Virtual Circuit - a service which delivers
   an virtual permanent circuit by a switched network.

   PSTN - Public Switched Telephone Network

   ISDN - Integrated Services Digital Network, a telephone network
   facility for transmitting digital and analog information over a
   digital network connection. A NAS may have the ability to receive
   the information from the telephone network in digital form.

   ISP - Internet Service Provider; a provider of Internet access (also
   Network Service Provider, NSP).

   BRI - Basic Rate Interface; a digital telephone interface.

   PRI - Primary Rate Interface; a digital telephone interface of 64K
   bits per second.

   T1 - A digital telephone interface which provides 24-36 channels of
   PRI data and one control channel (2.048 Mbps).

   T3 - A digital telephone interface which provides 28 T1 services.
   Signalling control for the entire connection is provided on a
   dedicated in-band channel.

   NFAS - Non-Facility Associated Signaling, a telephone network
   protocol/service for providing call information on a separate wire
   connection from the call itself. Used with multiple T1 or T3
   connections.

   SS7 - A telephone network protocol for communicating call supervision
   information on a separate data network from the voice network.

   POP - Point Of Presence; a geographic location of equipment and
   interconnection to the network. An ISP typically manages all
   equipment in a single POP in a similar manner.

   VSA - Vendor Specific Attributes; RADIUS attributes defined by
   vendors using the provision of attribute 26.

15. Full Copyright Statement

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

Acknowledgement