Internet Engineering Task Force
INTERNET-DRAFT
Category: Informational
<draft-beadles-nas-01.txt>
12 November 1998

Mark A. Beadles
MCI WorldCom Advanced Networks

The Network Access Server

1. Status of this Memo

This document is an Internet-Draft. Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as ``work in progress.''

To learn the current status of any Internet-Draft, please check the ``1id-abstracts.txt'' listing contained in the Internet-Drafts Shadow Directories on ftp.ietf.org (US East Coast), nic.nordu.net (Europe), ftp.isi.edu (US West Coast), or munnari.oz.au (Pacific Rim).

The distribution of this memo is unlimited. It is filed as <draft-beadles-nas-01.txt> and expires May 13, 1999. Please send comments to the author.

2. Abstract

The 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. This document offers a framework for the definition and analysis of a modern Network Access Server.

3. Definition of a Network Access Server

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 as a device which accepts multiple point-to-point [PPP] links on one set of interfaces, providing access to a routed network or networks on another set of interfaces. Examples of a network access server include:

> A remote access server which provides access to a private network via attached modems which are directly dialed by the user.
>
> A tunneling server which sits at the border of a protected network, and acts as a gateway for users to enter the protected network from the Internet.
>
> A shared commercial dial access server operated by a Network Service Provider, where incoming users connect via modems operated by a Telephone Service Provider, and access is provided to many dissimilar private and public networks.

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. However, the boundary between NAS and router is admittedly fuzzy. 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 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.

4. Interested parties

The following are examples of parties who are concerned with the operation of Network Access Servers. This list is by no means exhaustive.

> Network Service Providers (NSPs) who operate and manage NAS's, AAAA servers, policy servers, and networks; and who provide network services to end users.

End users who gain access to their private and public networks through NAS's.

Businesses and other entities who operate NAS's for their users' public and private network access, or who outsource the operation and management of NAS's to a NSP.

Telephone Service Providers (TSPs) who operate and manage modems and telephony networks; and who provide telephony services to end users, NSP's, and businesses.

Manufacturers of NAS's, AAAA servers, policy servers, modems, etc.

5. 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      |    \_            _/
  +---------------+      \_       _/
                           \_   _/
                             \_/
```

5.1. 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 enpoints in a protocol such as L2TP [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 [RADIUS], Diameter [DIAMETER], or COPS [COPS]. 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 wich 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 colocated with the NAS, or more typically, are located on a seperate 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 [SNMP].

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.

5.2. Analysis

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

5.2.1. 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 [IPSEC] and even participation in a Public Key Infrastcture.

5.2.2. 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.

5.2.3. Accounting and Auditing

Since NAS services are consumable resources, usage information must often be collected for 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 [RADIUS-ACCT].

5.2.4. 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.

5.2.5. 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 identity.

5.2.6. 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.

5.2.7. 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 [ROAMREQ].

6. Acknowledgements

Thanks to Dave Mitton (Nortel Networks), John Vollbrecht (Merit), and Rich Petke (MCI WorldCom) for useful discussions of this problem space.

7. References

[RADIUS] Rigney, Rubens, Simpson, Willens. "Remote Authentication Dial In User Service (RADIUS)", RFC 2138, April 1997.

[RADIUS-ACCT] Rigney, et. al. "RADIUS Accounting", RFC 2139, April 1977.

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

[DIAMETER] Calhoun, Rubens. "DIAMETER Base Protocol", draft-calhoun-diameter-06.txt, October 1998.

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

[COPS] Boyle, Cohen, Durham, Herzog, Raja, Sastry. "The COPS (Common Open Policy Service) Protocol", draft-ietf-rap-cops-02.txt, August 1998.

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

[IPSEC] Atkinson, Kent. "Security Architecture for the Internet Protocol", draft-ietf-ipsec-arch-sec-07.txt, July 1998.

[ROAMREQ] Aboba, Zorn. "Roaming Requirements", draft-ietf-roamops-romreq-10.txt, August 1998.

8. Author's Address

Mark A. Beadles
MCI WorldCom Advanced Networks
5000 Britton Rd.
Hilliard, OH 43026

Phone: 614-723-1941
EMail: mbeadles@wcom.net