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 "id-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-00.txt> and expires February 7, 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. This document offers a framework for the definition 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. Examples of a network access server include:
A text-mode terminal server.

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. A NAS is not necessarily a dial access server, although dial access is one common means of network access.

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 acts as the enforcement point for network AAAA (authentication, authorization, accounting, and auditing) services. A NAS is typically the first place in a network where security measures 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 ServiceProviders (TSPs) who operate and manage modems and telephony networks; and who provide telephony services to end users, NSPs, 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.
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, via tunnels over a data network, or by some other means.

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.

User 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 [1]. 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 colocated 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 [2].

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.

6. Security Considerations

As mentioned, a NAS is typically the first place in a network where security measures may be implemented. Also, since a NAS is often a shared device, its various interfaces (client, user management, and device management) may need to be secured by integrity and/or confidentiality measures.
7. References


8. Author’s Address

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

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