INTERNET DRAFT                                   Nancy Greene
Category: Informational             Nortel (Northern Telecom)
Title: <draft-greene-nasreq-00.txt>           Fernando Cuervo
Date: March 1998                    Nortel (Northern Telecom)
Expires: September 1998

Best Current Practice for Modem Outsourcing
<draft-greene-nasreq-00.txt>

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 view the entire list of current Internet-Drafts, please check the
"iid-abstracts.txt" listing contained in the Internet-Drafts Shadow
Directories on ftp.is.co.za (Africa), ftp.nordu.net (Northern Europe),
ftp.nis.garr.it (Southern Europe), munnari.oz.au (Pacific Rim),
ftp.iert.org (US East Coast), or ftp isi.edu (US West Coast).

Abstract

This document describes an architecture and the protocol used with
respect to a Network Access Server (NAS), when modems are outsourced
from the data network operator to the carrier network operator. At the
heart of modem outsourcing there are several key areas, namely, varied
mechanisms for authentication, authorization based on network wide state
and policy for resource sharing, accounting/auditing and other
management functions.

1.0 Introduction

Presently, dial-up connections over the public telephone network are
used for on-demand connection to the Internet or corporate networks. An
ISP may wish to outsource its modems to the telephone or carrier network
operator. In this case, the carrier network provides connections and
modems while the data network operator (e.g., an ISP or a corporate
network) is responsible for other functions such as subscriber
authentication, or accounting. Data network operators benefit by
replacing remote access hardware with a virtual modem pool service
provided by a carrier, traffic is forwarded from the resources that make
up the virtual modem pool over broadband connections to one or more ÂISP
gatewaysÂ, or Home Gateways. The virtual modem pool provides the ISP
with independence from the signaling used at the NAS (for example, PRI
or SS7).

2.0 Modem outsourcing requirements

Modem outsourcing and mass deployment of dial-up access, need
capabilities that are beyond the functionality provided by RADIUS. When
NAS boxes are placed in the carrier network operator domain many new
factors are introduced in the way NAS boxes operate:

1-Resource control is more complex since network resources can be shared
to optimize cost (e.g., modem pools may be dynamically shared between ISPs).

2-Resources such as tunnels may be authorized, set up and controlled in many ways (e.g., according to ISP, or tunnel type).

3-Access becomes a carrier’s responsibility. The carrier may need to manage resources for different access networks.

Increased flexibility is introduced when the NAS is placed in the carrier network. In the case of modem outsourcing, several distinct configurations can be defined depending on the following factors:

1-Where the point of authentication is (e.g., carrier network operator domain or ISP).

2-The level and distribution of authorization (for example, before and after end-user authentication, or just after. Note that RADIUS uses an end-user based authentication-authorization model. However, in the shared environment that results from modem outsourcing, authorization functions in the carrier network operator domain must often be based on the attributes of both the end-user and the ISP.

3-Whether signaling is physically co-located with the connection it establishes (e.g., front-end PRI signaling), or whether it is physically separate from the connection (e.g., back-end SS7 signaling).

4-Control and management relationships between carrier and ISP network elements, e.g. ISP Home Gateways, NAS Controller/AAA Servers in the carrier network, AAA Servers/Proxies.

These factors place requirements on the protocol that are above and beyond the scope of RADIUS. The protocol described in section 6.0, DSM-CC, includes functions for system configuration and resource control that provide the flexibility required to properly address these requirements.

3.0 Terminology

AAA Server function
This function provides the NAS with Authentication, Authorization, Accounting and/or other management functions. It may be located in the ISP, in the carrier network, or both.

AAA Proxy function
It is a proxy to a AAA Server.

Network Access Server (NAS) Control function
A NAS Control function allocates and deallocates resources according to some resource policy. A NAS Control function may control many NAS. It may share a server platform with AAA server functions and/or proxies to other AAA Servers. It may be located at an ISP, but is more likely found in a carrier network, for example, allowing NAS to be shared among ISPs.

NAS Controller/AAA Server/Proxy (NCAP)
This is a server platform that hosts the NAS Control function. This platform may also host AAA server functions and/or proxies to other AAA Servers. It is typically deployed in the carrier network domain, for example, allowing NAS to be shared among ISPs. In some situations it may be deployed in the data network domain. The AAA functions may be RADIUS
based or other.

End-User
The subject of the authentication/authorization.

Data Network Operator
An ISP or corporation, sometimes referred to as the wholesale-customer.

Carrier Network Operator
Provider of access and transport services between the end-user and a data network.

Network Access Server (NAS)
The Network Access Server (NAS) is the device that provides resources for users to access the data network. A NAS provides physical terminations of user access connections, and modems. A NAS includes a client that uses the functions of a NAS control server.

ISP (Home) Gateway
Network interworking platform between the Carrier Network and Data Network domains.

4.0 Modem Outsourcing Architectures

In modem outsourcing there are currently two scenarios for establishing a data session to an ISP. In the first scenario, authentication, authorization and accounting is done by the ISP (Figure 1). PPP is carried all the way to the ISP. Access to a tunnel may be subject to authorization functions exercised by the NAS itself or an authorization server (NAS Controller) in the carrier network operator domain. The client in the NAS collects the authentication information from the user. The information is then tunneled to a target network and its target RADIUS (AAA) server.
In the second scenario (Figure 2), PPP is terminated at the NAS. When this is the case, a client in the NAS must contact an appropriate server for user authentication. If necessary, (normally for scalability reasons,) a proxy may be used between the NAS and the ISP’s AAA Server. In this scenario, end-user authorization functions are more naturally integrated with the authentication steps, but it is likely that some level of authorization would be exercised by NAS Controller/AAA Server in the carrier network operator domain (e.g., based on attributes of the target ISP). Accounting is fairly independent of the setup style, the NAS collects resource and traffic information that can be relayed to the ISP according to the specific requirements (i.e. main accounting source, auditing, monitoring functions, etc.)

4.1 Properties of the NCAP-NAS architecture

Having a few NCAPs in the network for a large number of NAS boxes makes the NAS systems scaleable. Thus, instead of an ISP’s AAA server needing to be able to serve a large number of NAS, as the number of outsourced modems grows, it can deal with a lesser number of NCAPs in the network. In modern large NAS systems (e.g., many NAS boxes, several ISPs, roaming users, etc.) NAS boxes do not have the resources to store policy and configuration information (let alone the complexity of maintaining all these data). The NCAP is responsible for coordinating the administrative functions, modem pool resource allocation and configuration policies. The dependency between a NAS and a NCAP in the network varies according to the NAS box capabilities for storing and enacting policy (resource and administrative), and on the complexity of the interworking between networking domains. The NCAP is also responsible for insulating the ISP from specific aspects of NAS boxes (e.g., vintage, manufacturer, etc).

Additionally, as NAS boxes continue growing their port capacity the NCAP-NAS protocol must be able to efficiently support the configuration and control of a large number of resources and devices.

The interaction between the NAS and the NCAP uses a subset of the ISO/IEC DSM-CC User-Network protocol [DSM-CC], with extensions [DSM-CC extensions]. This is done to support the additional flexibility that modem outsourcing requires (See section 2.0.) This protocol is outlined in section 6.0. Interaction between the NCAP in the network and an AAA Server at an ISP may be based on the DSM-CC protocol with extensions, or a RADIUS proxy. Ideally, all interaction between AAA servers can be supported by the same protocol as the one between the NAS and its NCAP.

5.0 Requirements for a NAS <-> NCAP protocol

>From the discussion above, we can now determine some of the requirements for a NAS <-> NCAP protocol. It must:

- allow separation of AAA (AAA -> A/A/A)
Separating the AAA allows different configurations. For example, authorization may be handled by an NCAP in the network, while authentication is always performed by the AAA Server at the ISP. Also, accounting records may be kept by the ISP or by the network, or both.

- be a simple light-weight and symmetric protocol that allows NAS -> Server and Server -> NAS requests.

An ISP may require information about NAS usage, or resources available. This should be available on demand.

- support resource policy and configuration (e.g. tunnels).

The protocol should allow, for instance, tunneling attributes per user to be stored at an ISP or in the network, to be requested by a NAS as required for tunnel setup. NAS running independently of an NCAP is an example of policy and configuration since the NAS must have this information.

- allows sharing of NAS resources between ISPs.

This is generally accomplished by allowing control of a NAS by an intermediary such as a network operator (i.e. outsourcing).

6.0 DSM-CC Functionality

DSM-CC is a light-weight ISO standard protocol [DSM-CC]. It is a request/response protocol that is usually implemented over UDP/IP. The following NAS functionality is provided using its message set.

6.1 NAS Initialization

Used by the NAS to indicate that it is ready to respond to the NCAP, it may indicate the ÂservicesÂ that it is ready to support. Basic configuration information such as hardware and software versions may be communicated to the NCAP. The response from the NCAP indicates whether the management and control associations requested will take place. Configuration information may be supplied at this point by the NCAP to the NAS, for instance, several timers that govern the control relationship between the NAS and the NCAP may be set at this point.

DSM-CC messages:
UN-Config*, * = <Request, Confirm>

6.2 NAS failure recovery

A failed NAS will try to reestablish a control association using the NAS Initialization messages. The NCAP will launch a NAS Audit to match against the NAS state last known to the control server.

DSM-CC messages:
UN-Config*, * = <Request, Confirm>

6.3 NAS Control Server reset indication

The NCAP must reestablish the association with the NAS. Configuration information may be exchanged, including the definition of a new NCAP. This action must be followed by an update of the state changes of the NAS and its resources that occurred while running without the NCAP.
DSM-CC messages:
UN-Config*, * = <Indication, Response>

6.4 Link Failure recovery

The NCAP or the NAS may reestablish the association. This must be followed by an update of the state changes of the NAS and its resources that occurred while running without the NCAP.

DSM-CC messages:
UN-Config*, * = <Request, Confirm, Indication, Response>

6.5 Resource Allocate/Release

DSM-CC Session messages are used to allocate NAS resources to end-users. Session set-up messages may involve authentication or authorization functionality. A session identifier is used to simplify the control and management of resources used in a single association between an end-user and an ISP. Session messages may be initiated by the NAS or the NCAP, depending on the location of the native signaling and authentication client (e.g., in the NAS for PRI or in the NCAP for SS7). Authentication may be carried out in the NCAP, proxied to another server or tunneled to the ISP. Authorization functions in the NCAP determine users rights to access resources before and after authentication. Separate Add/Delete resource messages are provided by DSM-CC, however, they are not necessary for current NAS applications.

DSM-CC messages:
ClientSessionSetUp*, * = <Request, Confirm, Indication, Response>
ClientRelease*, * = <Request, Confirm, Indication, Response>

6.6 ISP Gateway (Home Gateway)

Coordinated action between the NAS, the NCAP and the ISP gateway is necessary. Depending on the mode of operation, the state of a target ISP may be known (e.g., via management) or inferred (e.g., via retries) by either the NAS or the NCAP. When the ISP Gateway is unavailable, the NAS and the NCAP must coordinate their actions for Session Set-Up and Release.

DSM-CC messages:
ClientSessionSetUp*, * = <Request, Confirm, Indication, Response>
ClientRelease*, * = <Request, Confirm, Indication, Response>

6.7 Initiate accounting (for local PPP termination)

Successful establishment of an end-to-end session is notified by the NAS to the NCAP. The NAS signals the NCAP to indicate that it has successfully connected the data session, and that it is proceeding to forward packets to the ISP. This message is used to trigger generation of accounting records and to convey additional call set-up information.

DSM-CC Messages:
ClientConnect*  * = <Request, Confirm>

6.8 NAS Audit

The NCAP requests status of a session or sessions from the NAS.

DSM-CC Messages:
ClientStatus*  * = <Request, Confirm>
7.0 Way Forward

It is proposed to use DSM-CC as a basis for a RADIUS replacement protocol for modern NAS. DSM-CC would provide secure, bi-directional functions for subscriber authentication, resource configuration, status reports and subscriber management. Since RADIUS is widely used for authentication of dial-up users, DSM-CC would be adapted for compatibility with RADIUS.

8.0 Authors

Fernando Cuervo  
Nortel  
Ottawa, ON, Canada.  
Phone: 613-763-4628  
EMail: cuervo@nortel.ca

Nancy Greene  
Nortel  
Ottawa, ON, Canada  
Phone: 613-763-9789  
Email: ngreene@nortel.ca

9.0 References
