Network Working Group
Request for Comments: 2882
Category: Informational

D. Mitton
Nortel Networks

July 2000

Network Access Servers Requirements: Extended RADIUS Practices

Status of this Memo

Copyright Notice

Abstract

This document describes current practices implemented in NAS products that go beyond the scope of the RADIUS RFCs 2138, 2139 [1,2]. The purpose of this effort is to give examples that show the need for addressing and standardizing these types of ad-hoc functions. Since many of these features require a matching server support component, the ability to deploy and manage interoperable NAS and AAA server products is severely hindered.

These practices are documented here to show functions that are obviously desired in developing future AAA protocols for NAS deployment.

Table of Contents

1. Introduction

The RADIUS Working Group was formed in 1995 to document the protocol of the same name, and was chartered to stay within a set of bounds for dial-in terminal servers. Unfortunately the real world of Network Access Servers (NASes) hasn't stayed that small and simple, and continues to evolve at an amazing rate.

This document shows some of the current implementations on the market have already outstripped the capabilities of the RADIUS protocol. A quite a few features have been developed completely outside the protocol. These features use the RADIUS protocol structure and format, but employ operations and semantics well beyond the RFC documents.

I learn of the details of these functions from reading industry manuals and often have to respond to them in competive bid specifications. As they become deployed in the field, they gather the force of de-facto standards.

Because they have been done outside scope of the RFCs, they are vendor specific, and introduce significant problems in offering an interoperable product.

1.1. Disclaimers

The data and numbers in this document have been gleaned from public sources and vendor documents along the way. Actual implementation of many these features and variation from the documentation has not been confirmed.

This document is a snapshot of known practices at the time of writing. It is not intended to standardize these practices here, or keep this document current, beyond initial publication. While some detailed information is given, it is not the purpose of this document to directly or sufficiently describe the functions mentioned to the level of a complete functional specification.

The author has not transcribed copyrighted material, and is not aware of whether any of these practices have of intellectual property restrictions.

Any numeric assignments or functional operations are subject to change by vendors without notice. I would appreciate any direct input, preferably first hand, from implementors.

1.2. Presentation

Without any easy organization for the material, information is arranged in a simple taxonomy from bottom-up complexity:

- Attribute Usage
- Attribute Data Types
- Message Codes
- New Operations

2. Attribute Usage

The RADIUS RFCs define attribute type ranges and specific attribute definitions.

- There are about 70 defined RADIUS attributes:
- Values 192-223 are reserved for experimental use
- Values 224-240 are reserved for implementation-specific use
- Values 241-255 are reserved and should not be used.

Attribute 26 was defined to be the Vendor Specific Attribute (VSA) with further internal structure to allow vendor expansion.

2.1. Attribute conflicts

In practice attributes 92-255 are in use by a vendor. And another vendor also use attributes in the 90-104 range and conflicts with this usage.

To deal with these issues, server vendors have added vendor specific parameters to their client database files. The administrator has to indicate the vendor type of NAS along with the client IP address and secret, so that the server can disambiguate the attribute usage.

One server has a single large vendors file to describe the mapping all attributes to an internal format that retains the vendor id. Another server implementation uses multiple dictionaries, each indexed to a NAS and Vendor Model definition list.

2.2. Attribute Value Conflicts

Adding additional attributes may be more trouble than necessary for simple features. Often existing RADIUS attributes could be extended with additional values (particularly attributes that are enumerated choices). But in doing such there is no way to guarantee not conflicting with other vendor's extensions.

2.2.1. Vendor Specific Enumerations proposal

One proposed solution to this problem was Vendor Specific Enumerations (VSEs). That is to imbed the vendor's management ID in the numeric value (ala VSAs) which would to divide up the attribute value space. This technique has not seen any acceptance by the working group or other vendors, however, the vendor did accomplish the goal of not conflicting with working group additions or other vendor values.

Example dictionary of VSE values:

```
VALUE   Service-Type        VSE-Authorize-Only       0x06300001

VALUE   Acct-Status-Type    VSE-User-Reject          0x06300001
VALUE   Acct-Status-Type    VSE-Call-Reject          0x06300002
VALUE   Acct-Status-Type    VSE-IPCP-Start           0x06300003
VALUE   Acct-Status-Type    VSE-IPXCP-Start          0x06300004
VALUE   Acct-Status-Type    VSE-ATCP-Start           0x06300005
VALUE   Acct-Status-Type    VSE-Accounting-Restart   0x06300006
VALUE   Acct-Status-Type    VSE-Accounting-Shutoff   0x06300007
```

```
VALUE   Acct-Status-Type    VSE-Tunnel-Start         0x06300008
VALUE   Acct-Status-Type    VSE-Tunnel-Stop          0x06300009
VALUE   Acct-Status-Type    VSE-Tunnel-Reject        0x0630000a
VALUE   Acct-Status-Type    VSE-Tunnel-Link-Start    0x0630000b
VALUE   Acct-Status-Type    VSE-Tunnel-Link-Stop     0x0630000c
VALUE   Acct-Status-Type    VSE-MP-Start             0x0630000d
VALUE   Acct-Status-Type    VSE-MP-Stop              0x0630000e
VALUE   Acct-Status-Type    VSE-Line-Seizure         0x0630000f
VALUE   Acct-Status-Type    VSE-Rlogin-Start         0x06300010
VALUE   Acct-Status-Type    VSE-Rlogin-Stop          0x06300011
```

2.3. Vendor Specific Attribute Usage

Because attribute 26 Vendor Specific Attributes (VSAs) came late in the RADIUS working group development, there were some server implementations that were late to support them. Today, there are several leading implementations of clients that make extensive use of VSAs. What's unfortunate is that there is also several different formats of VSAs implemented. This is because the RFC suggested format does not support more than 256 attributes.

2.3.1. VSAs in use by some clients:

At the time this document was written, the following had be observed:

- Microsoft: several for MS-CHAP authentication support [9]

- ACC: 42 [10]

- Nortel(Bay): about 60 VSAs and 16 VSEs

- Nortel(Aptis): about 60 VSA: 20 1-byte, ~130 4-byte header.
  Aptis VSAs have shifted from a regular format to a 4-byte header format, due to the large number of attributes implemented.

- 3Com (USR): about 130
  USR VSAs are different than the format suggested in RFC 2138.
  They have a 4 byte type field and have no internal length.

Some vendors that did not initially use VSAs, have shifted in later releases VSA usage as a configuration option.

2.3.2. Clients that support Multiple Vendor Attributes

Now that MS-CHAP RADIUS attributes have been published in RFC 2548 [9] as Microsoft VSA attributes, it will become typical that for NAS clients that support MS-CHAP authentication to process several

different vendor VSA types. This has implications for RADIUS servers that filter or "prune" return attributes based on the vendor make/model of the NAS client.

One NAS implementation can receive up to three different vendor specific attribute sets, but will only send attributes according to the "mode" that has been configured by the operator. This allows it to fit into environments where the customer has become dependent on a particular set of RADIUS attributes, and allows the NAS to "drop-in" without server attribute changes.

There is another NAS that supports 3 vendor attributes sets concurrently. That is, it will normally use a combination of different vendor VSAs in return profiles from the server. This was done to support a superset of competing vendor's extensions, as well as it's own, and include an extensions from a sister product.

3. Attribute Data Types

The base RFCs define only has 4 basic data types:

- integer, 32 bit unsigned
- string, 1-253 bytes, counted.
- ipaddr, 32 bit IPv4
- date, 32 bit Unix format.

Since then, various variations have been added:

The tunnel authentication document [6] adds an optional compound "tag" byte to tunnel attributes. These are a single byte prepended to the data field in order to support sets of attributes to be returned. The byte value must be in the range 01-3F hex or it is considered to be data.

Note that there is no native support for IPv6 addresses. In fact IPv6 support is missing in some fixed message components too.

There have been special attribute types created within servers. For packet filters, the format called "abinary" was created. The user enters an ASCII string filter description in the user profile, but the server parses it into a binary string before passing it to the NAS. This lowers the complexity of the NAS parser. Also a "phonestring" server data type allows additional data type checking at the entry application.

4. New Messages

A number of new message types have been introduced by various parties over time. The base specification has 6, vendors have added 26.

These fall into a number of categories which are described in the next section below. Some of these messages are actually used between the RADIUS server and some other resource server, using a RADIUS-like protocol to implement new functions.

6 Accounting Status
(now Interim Accounting [5])
7 Password Request
8 Password Ack
9 Password Reject
10 Accounting Message

21 Resource Free Request
22 Resource Free Response
23 Resource Query Request
24 Resource Query Response
25 Alternate Resource Reclaim Request
26 NAS Reboot Request
27 NAS Reboot Response

29 Next Passcode
30 New Pin
31 Terminate Session
32 Password Expired
33 Event Request
34 Event Response
40 Disconnect Request
41 Disconnect Ack
42 Disconnect Nak
43 Change Filters Request
44 Change Filters Ack
45 Change Filters Nak
50 IP Address Allocate
51 IP Address Release

5. Additional Functions

These are operations performed using RADIUS extensions and additional messages types.

5.1. Password Change

Remotely requested password change operations were described and proposed, but rejected by the working group. None the less, the feature is still deployed in a number of products.

Message types:

- Password Request
- Password Ack or Reject

5.2. Authentication Modes

Additional message types have been added to negotiate passcode changes for token card servers.

- Next Passcode
- New PIN
- Password Expired

They allow the NAS or RADIUS server negotiate passcode changes with an external security server.

5.3. Menus

At least two vendors have built menuing interaction systems for use with terminal dial-ins.

One implementation uses the Reply-Message string as the menu text to be displayed, and the State attribute to keep track of the place in the menu. The menu is displayed using the Access-Challenge message. The response is encoded in the User-Password field like an ordinary challenge sequence would.

Some RADIUS clients have problems with this because they cannot handle long or multiple Reply-Message attributes that may have embedded carriage returns and line-feeds. The new Echo attribute should also control echo behavior on the menu response. Use of the State attribute to keep track of a Challenge sequence is also standard behavior.

Another implementation uses two vendor attributes (VSA-Menu-Item, and VSA-Menu-Selector as well as VSA-Third-Prompt) to convey this information. This implementation is vendor specific.

5.4. Pseudo Users

One client implementation takes advantage of your vanilla RADIUS server's ability to be used as a remote database server. By using some well-known, implementation specific, strings for Username and Password attributes, the NAS can request information from the server, such as: Static IP routes, Static IPX routes, or the Message of the Day.

These are called pseudo-user requests, because they use a user entry with this manufactured name, for purposes other than authentication.

Another client also uses a pseudo-user technique for resolving unknown Filter-ID(11) values. An Access-Request message is sent to the RADIUS server with the Filter-ID as the Username value, the password is a known string, and the Service-Type is VSE-Authorization-Only. The response must also be of the same Service-Type, or the response will be ignored. The responding profile should contain the IP-Filter VSA attributes that will define the desired filter.

It should be noticed that pseudo-user profiles could be a security problem if a specific or operationally invalid Service-Type is not attached to the profile. The client should test for this returned value, to prevent normal dial-in users from gaining access via this profile.

6. Resource Management

Authorized sessions may need to be allocated additional dynamic resources in order to perform their services. The most typical is IP addresses. The allocation may want to be delayed until needed or coordinated on a scale independent of the RADIUS server. Additional messages may be used to allocate and free these resources. The RADIUS server may proxy these requests to another server.

Examples: Certain servers can allocate addresses local to the NAS or use an outboard address server. Other servers have an internal address pool capability, which will fill in the Framed-IP-Address attribute with an assigned value based on pool selected.

6.1. Managed Resources:

Resources managed include: IP Addresses, Concurrent Logins, Dial-in Port allocation policies, Tunnel limits and load distribution.

There are several different types of implementation techniques:

- Explicit request/free resource requests
- Monitor usage with deamons watching the state
- Explicit messages to a state deamon
- Monitor Accounting messages for state changes

6.2. Resource Management Messages

Messages used for resource management

- IP Address Allocate
- IP Address Release

- Resource Request
- Resource Response
- Resource Free Request
- Resource Free Response
- Resource Reclaim Request
- NAS Reboot Request/Response

These messages are used to allocate and free resources for a NAS from a centralized server. These mechanisms allows the service provider better administrative control than some automated LAN services, which don't have policy inputs or controls.

6.3. Concurrent Logins

The RADIUS protocol was designed to allow stateless servers. That is, servers that don't know the status of the active sessions. However, it is very important for many service providers to keep track of how many sessions a given user may have open, and accordingly disallow access.

There are several different techniques used to implement login limits on a RADIUS environment. Some vendors have build NAS monitoring tools either into their RADIUS servers, either directly or as auxiliary deamons, that can check the session status of the controlled NASes by SNMP or proprietary methods.

Other vendors monitor the RADIUS accesses and accounting messages and derive state information from the requests. This monitoring is not as reliable as directly auditing the NAS, but it is also less vendor specific, and can work with any RADIUS NAS, provided it sends both streams to the same server.

Some of the approaches used:

- SNMP commands
- Telnet monitor deamon
- Accounting monitor

6.4. Authorization Changes:

To implement an active changes to a running session, such as filter changes or timeout and disconnect, at least one vendor has added a RADIUS "server" to his NAS. This server accepts messages sent from an application in the network, and upon matching some session information, will perform such operations.

Messages sent from Server to NAS

- Change Filter Request
- Change Filter Ack / Nak
- Disconnect Request
- Disconnect Response

Filters are used to limit the access the user has to the network by restricting the systems and protocols he can send packets to. Upon fulfilling some registration with an authorization server, the service provider may wish to remove those restrictions, or disconnect the user.

7. Policy Services

Some vendors have implemented policy servers using RADIUS as the control protocol. Two prominent Policy Managers act as RADIUS proxy filters and use RADIUS messages to deny access to new sessions that exceed active policy limits.

One implementation behaves like a RADIUS proxy server, but with a policy process governing it’s forward decisions. Typically a pre-authentication message (like the new RADIUS draft Service-Type = CallCheck) is emitted by the NAS upon call arrival. This message will contain only the Dialed-Number information in the Username field. The server receives the Access-Request messages and processes them against it’s knowledge of the network state and the provisioned policies.

An Access-Accept will be returned to the system to accept the call, and many also contain dynamic policy information and Virtual POP specific default parameters. When the real PPP authentication is engaged, the proxy will forwards the Access-Request to a RADIUS server, if this session was approved at pre-auth. It can also process Access-Requests that were not preceded by a pre-auth exchange, and use the Username field for information about the

desired realm, in it's policy evaluation.

The other implementation performs a similar operations. It uses VSAs in the Access-Request to distinguish pre-authentication message types.

8. Accounting Extensions

Traditional Accounting only records session starts and stops which is pretty boring. Additional session information reporting can be added easily which gives a better picture of operation in use as they happen. Some event types are listed below.

8.1. Auditing/Activity

- Call or Modem Starts, Stops
- Tunnel Starts, Stops
- Tunnel Link Starts & Stops
- Admin changes

These events if monitored by a stateful server can be used to gather information about the usage of the network on a user/session basis. Information about when a particular user entered the network is more relevant to network service management than attempting track backwards from low level IP address flows. Useful information about port usage across a range of NASes allows service provider to quickly find problem areas or users.

Information about call failures, successes, and quality are also deemed important many service providers.

Extending RADIUS accounting is easy, it's surprising that more implementations have not been made in this area.

9. Conclusions

In real life RADIUS Servers are becoming rather complex software implementations. They are often brokering authentication and authorization to other authorities or repositories. Variants of RADIUS protocol is often used as glue protocol for these type of solutions.

Some of the solutions are kludges that could be cleaned up by better underlying services.

What this means to the implementor is that RADIUS as the RFCs describe it is becoming less relevant. Many additional features require matching client and server processing message processing.

Without standardization of these functions we don't have much interoperability in the field and much effort is spent in reverse engineering and reaction to unknown areas.

This memo is not a complete survey by any means. It is a representative summary of practices that I am aware of at the time of writing. I still appreciate input from vendors or users on practices and details known, and particularly any reference material you can pass me.

10. Security Considerations

This document documents known practices, and does not propose any particular new protocols. Extensions to RADIUS protocols create new security implications because of their functions go beyond those considered in the RFCs. Some of these include:

- The ability to change passwords via a RADIUS exchange was deliberately left out of the protocol by the working group, because of security concerns.
- The Pseudo-User profiles and the Call-Check operation may allow unintended access if static and well-know account names and passwords are allowed to be used by regular interactive accounts.
- Resource Management operations must be protected from denial of service attacks.
- Client side authorization change exchanges need to be secured from attacks that could disconnect or restrict user services.

11. Implementation Documents

Information about the following implementations can be obtained from the respective owners. Most listed are available from the manufacturer's web site.

11.1. Clients:

- 3Com(USR) Total Control Hub
- Ericsson(ACC) Tigris
  draft-ilgun-radius-accvsa-01.txt, Dec 1998
- Lucent(Ascend) MAX TNT
- Lucent(Livingston) Portmaster
- Nortel(Aptis) CVX 1800
- Nortel(Bay Networks) Versalar 5399/8000 Remote Access Controller
- Intel(Shiva)

11.2. Servers:

- Ericsson(ACC) Virtual Port Server Manager
- Funk Steel-Belted RADIUS
- Intel(Shiva) Access Manager
- Lucent(Ascend) Access Control
- Lucent(Ascend) NavisAccess
- Lucent(Ascend) Modified Livingston 1.16
- Lucent(Livingston) V2.01
- Lucent(Livingston) ABM
- Lucent Port Authority
- MERIT AAA Servers
- Nortel(Bay Networks) BaySecure Access Control
- Nortel Preside Radius
- Nortel CVX Policy Manager

12. References

[1] Rigney, C., Rubens, A., Simpson, W. and S. Willens, "Remote Authentication Dial In User Service (RADIUS)", RFC 2138, April 1997.

[2] Rigney, C., "RADIUS Accounting", RFC 2139, April 1997.

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

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

[5] Rigney, C., Willats, W. and P. Calhoun, "RADIUS Extensions", RFC 2869, June 2000.

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

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

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

[9] Zorn, G., "Microsoft Vendor-specific RADIUS Attributes", RFC 2548, March 1999.

[10] Ilgun, K., "RADIUS Vendor Specific Attributes for ACC/Ericsson Datacom Access", Work in Progress.

13. Author's Address

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

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

14. Full Copyright Statement

Acknowledgement

Funding for the RFC Editor function is currently provided by the Internet Society.