Status of this Memo

This document is an Internet-Draft and is in full conformance with all provisions of Section 3 of RFC3667.

By submitting this Internet-Draft, I certify that any applicable patent or other IPR claims of which I am aware have been disclosed, and any of which I become aware will be disclosed, in accordance with RFC 3668.

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."

The list of current Internet-Drafts can be accessed at http://www.ietf.org/ietf/1id-abstracts.txt The list of Internet-Draft Shadow Directories can be accessed at http://www.ietf.org/shadow.html.

This document is an individual submission to the Authentication, Authorization and Accounting (AAA) Working Group of the Internet Engineering Task Force (IETF). Comments are welcome should be submitted to the mailing list aaa-wg@merit.edu.

Copyright (C) The Internet Society 2005.
Abstract

This document describes how a Diameter protocol application would interact with a RADIUS protocol application with respect to translation of Vendor Specific Attributes and AVPs in both networks.

This interactions between Diameter applications and RADIUS specified in this document are in addition to that specified in the Diameter Base, the Diameter NAS Application and RADIUS. In this sense, this document extends the Base Diameter protocol and requests an addition to the RADIUS attribute space.
# Table of Contents

1. Introduction ........................................... 4  
2. Background ............................................. 4  
   2.1. RADIUS Vendor Specific Attributes (VSA) ............ 4  
   2.2. Diameter Vendor Specific Attribute Value Pairs ....... 5  
3. Translation ............................................ 5  
   3.1. Goals ............................................. 6  
   3.2. Issues ........................................... 6  
   3.3. Technical Differences ............................. 6  
   3.4. RADIUS VSA data in Diameter ....................... 7  
   3.5. Diameter VSA data in RADIUS ....................... 8  
4. IANA Considerations ................................. 9  
5. Security Considerations ............................ 10  
6. References ............................................ 11  
   6.1. Normative References ............................... 11  
   6.2. Informative References ............................. 11  
7. Acknowledgements .................................... 12  
8. Authors’ Addresses ................................... 12  
Intellectual Property Considerations ................. 13  
Full Copyright Statement ............................... 13
1. Introduction

This document describes how a Diameter protocol application would interact with a RADIUS protocol application with respect to translation of Vendor Specific Attributes and AVPs in both networks.

RFC 4005 [DiameterNAS] describes how RADIUS functionality should be represented within the Diameter AAA protocol. However there are issues when translating between the two different formats because of the differences in capabilities.

This draft specifies methods where RADIUS VSAs and Diameter Vendor Specific AVPs could be exchanged with minimum transformational knowledge and no loss of information.

2. Background

2.1. RADIUS Vendor Specific Attributes

RFC 2865 [RADIUS] Section 5.26 Attribute 26 describes the VSA format which includes an SMI identifier and a value string. Section 5.26 continues to describe that the string SHOULD encode a sequence of vendor type / vendor length / values fields. It gives an example format that has one octet Vendor Type field and one byte Vendor Length.

RADIUS VSA Generic:

```
  0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|   Type = 26   |    Length     |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                         Vendor-Id                             |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|    Attribute-Specific...                                    |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-
```

RFC 2865 [RADIUS] Section 5.26 Attribute 26 describes the VSA format which includes an SMI identifier and a value string. Section 5.26 continues to describe that the string SHOULD encode a sequence of vendor type / vendor length / values fields. It gives an example format that has one octet Vendor Type field and one byte Vendor Length.

```
  0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|   Type = 26   |    Length     |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                         Vendor-Id                             |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|    Attribute-Specific...                                    |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-
```
RADIUS VSA Suggested format:

```
  0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|   Type = 26   |    Length     |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                         Vendor-Id                             |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|  Vendor Type  | Vendor Length |    Attribute-Specific...|
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

2.2. Diameter Vendor Specific Attribute Value Pairs

RFC 3588 [DiameterBase] Section 4.1 defines the Vendor-Specific AVP bit flag. When the V-bit is set, it indicates that the AVP has a Vendor-Specific Type code. The Vendor Type code is not IANA assigned, though the RFC suggests that the first 255 values be reserved for RADIUS compatibility. The Vendor-ID code is the SMA Enterprise code [ASSIGNNO]. Diameter AVP values have a 24 bit length.

Diameter Vendor-Specific AVP

```
  0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                                        Vendor Type     |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|V M P r r r r r|                  AVP Length                   |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                          Vendor-ID                            |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|    Attribute-Specific...|
+-+-+-+-+-+-+-+-+-+-+-+
```

where V=1, M=x, P=x

3. Translation
3.1. Goals

One goal of Diameter was to allow Diameter systems to operate as a superset of the RADIUS functionality. Diameter should be able to accommodate RADIUS attributes with minimal per attribute knowledge (per RFC 4005 Section 9). Conversely, whenever possible, Diameter capabilities should translate into RADIUS cleanly.

In a mixed network, RADIUS and Diameter systems will not generally know which peer they will be communicating with, and while such information can be configured, it should not be necessary. Vendors are to be discouraged from creating VSAs that are substantially different in each protocol. And should consider their encodings formats carefully in coexistence situations.

The translation between RADIUS and Diameter should involve as few as possible exception cases on a per attribute basis. A Diameter/RADIUS gateway should not have to have a VSA dictionary for each vendors equipment.

3.2. Issues

At this writing RADIUS devices are the majority of AAA applications in the field. Many RADIUS devices operate well and do not justify an effort to retrofit Diameter on them.

There is a installed legacy base of RADIUS equipment that has an established base of practice that must be accomodated. Diameter practices are still in their formative stages, and attention should be paid to forward compatible operations.

RFC 4005, Diameter NAS Application, Section 9.6, describes a transformation that works only for RADIUS VSAs that meet the SHOULD format. The described transform maps one byte into the Diameter Vendor space. It cannot transparently deal with codes greater than 255. And other RADIUS formats would require special knowledge and formats.

3.3. Technical Differences

Many RADIUS vendors found the suggested one byte type code indequate and expanded their format to a two or four byte type code. Given there is no expansion technique defined, it is not possible, without Vendor Specific knowledge to recognize a such a differently formated VSA. RADIUS systems that use these attributes must be specially coded to recognize them.
Diameter Vendor Attributes use the setting of the V-flag in the header to indicate that the Base Diameter Type code is Vendor Specific and is 32 bits wide. When the V-Flag is set, a Vendor SMI code is included in the Diameter message header.

Diameter AVPs data field can be >16M bytes long (length 24 bits). RADIUS attributes can only be up to 253 bytes long, which doesn’t include the SMI value. To handle longer values, there must be a chaining and concatenation process.

3.4. RADIUS VSA data in Diameter

Because they come in various non-standard formats RADIUS VSA data should treated transparently and directly presented in a Diameter Base AVP of type 26. Header-wise this is not a Diameter VSA, but it doesn’t differ by much. It SHOULD be treated as another logical form of VSA. This requires a Diameter change, as this AVP value is currently not allowed by RFC 4005, section 9.4.

Diameter speaking applications could parse the RADIUS information with the same processing that a similar RADIUS application would use.

Diameter applications that wish to communicate directly with RADIUS applications can use this format to send responses.

When forwarding from a Diameter network to a RADIUS network. Lengths greater than 249 are NOT allowed and MUST be discarded.
Diameter AVP #26

```
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                      AVP Code = 26                             |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|V M P r r r r r|                  AVP Length                   |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                          Vendor-ID                            |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|  Attribute-Specific...                                       |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+

where V=0, M=0, P=0

Diameter AVP Type = 26 RADIUS VSA type
Diameter Length = length of VSA data
Diameter Flags: V=0, M=0, P=0
Data:
  Vendor Code (begining of RADIUS 26 data)
  Remaining data
```

Diameter AVP #26, RFC 2865 Suggested Format

```
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                      AVP Code = 26                             |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|V M P r r r r r|                  AVP Length                   |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                      Vendor-ID                            |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                      Vendor Type   | Vendor Length |    Attribute-Specific...
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+

where V=0, M=0, P=0

3.5. Diameter VSA data in RADIUS

Diameter gateways that wish to forward Diameter format VSAs to RADIUS applications should transform the data in to a RADIUS attribute format as shown below. This format is subject to review in the RADIUS Extentions Working Group.
RADIUS Diameter Vendor AVP:

```
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
| Type = TBA |    Length     |V M P r r r r r|
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                Vendor-Id (first segment only)                |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                Vendor Type (first segment only)               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                      Attribute-Specific...                   |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

where V=1 for first, 0=continuation,

Flags M & P retrain their Diameter values.

- **RADIUS Type = TBA**
- **RADIUS Length (3-255)**
- **Vendor Code = 4 bytes from the Diameter Vendor Code**
- **Vendor Type = 4 bytes from the Diameter VSA Type code**
- **Vendor data = upto 242 bytes**

For Diameter values with lengths greater than 242, the additional data would be put in consecutive attributes, in the same manner as EAP [RADIUS-EAP], [DiameterEAP].

Because there can be multiple VSAs in a message, each attribute which is NOT the beginning of a new VSA value SHALL have the V-bit of copy of the Diameter flags, set to 0. And the Vendor-Id and Vendor-Type SHALL not be repeated.

Note that RADIUS applications that do not understand the Vendor’s attributes will not honor the Diameter M and P flags. These flags have no meaning in RADIUS, but are preserved for vendor specific meaning and potential transport back to Diameter.

### 4. IANA Considerations

This document defines the use of a RADIUS type 26 attribute code in the Diameter Protocol space as defined in [DiameterBase] and [DiameterNAS]. It also calls for the assignment of a RADIUS attribute type to encapsulate Diameter Vendor Specific AVPs. The IANA references are [DiameterTypes] and [RADIUSTypes].
5. Security Considerations

This document does not contain a security protocol, it describes an addition to the existing Diameter and RADIUS protocols. All security issues of those protocols must be considered in implementing this specification. This extension does not add any unique concerns.
6. References

6.1. Normative References


[DiameterTypes]  IANA, "AAA Parameters", URL: <http://www.iana.org/assignments/aaa-parameters>


[RADIUSTypes] IANA, "RADIUS Types", URL: <http://www.iana.org/assignments/radius-types>


[IANA] IANA Assigned Numbers Database, URL: <http://www.iana.org/numbers.html>


6.2. Informative References


7. Acknowledgements

The author would like to thank Glen Zorn for looking after this issue in spite of Section 9 of RFC 4005, which I wrote. And my co-chairs Bernard Aboba and John Loughney for suggesting this document.

8. Authors’ Addresses

Questions about this memo can be directed to:

David Mitton
RSA Security, Inc.
174 Middlesex Turnpike
Bedford, MA 01730

Email: dmitton@circularnetworks.com
Intellectual Property Considerations

The IETF takes no position regarding the validity or scope of any intellectual property or other rights that might be claimed to pertain to the implementation or use of the technology described in this document or the extent to which any license under such rights might or might not be available; neither does it represent that it has made any effort to identify any such rights. Information on the IETF’s procedures with respect to rights in standards-track and standards-related documentation can be found in BCP-11. Copies of claims of rights made available for publication and any assurances of licenses to be made available, or the result of an attempt made to obtain a general license or permission for the use of such proprietary rights by implementers or users of this specification can be obtained from the IETF Secretariat.

The IETF invites any interested party to bring to its attention any copyrights, patents or patent applications, or other proprietary rights which may cover technology that may be required to practice this standard. Please address the information to the IETF Executive Director.

Full Copyright Statement

Copyright (C) The Internet Society (2005). This document is subject to the rights, licenses and restrictions contained in BCP 78, and except as set forth therein, the authors retain all their rights.

This document and the information contained herein are provided on an "AS IS" basis and THE CONTRIBUTOR, THE ORGANIZATION HE/SHE REPRESENTS OR IS SPONSORED BY (IF ANY), THE INTERNET SOCIETY AND THE INTERNET ENGINEERING TASK FORCE DISCLAIM ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION HEREIN WILL NOT INFRINGE ANY RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.