

RADIUS EXTensions Working Group
INTERNET-DRAFT
Intended Status: Standards Track
Expires: May 10, 2016

Sanal Kumar Kariyethath Sivaraman
Aravind Prasad Sridharan
DELL
November 7, 2015

RADIUS Extended Identifier Attribute
draft-aravind-radext-extended-identifier-attribute-00

Abstract

This document proposes solution to alleviate the limitation of limited size (8 bits) of RADIUS Identifier field by proposing a new Extended Identifier attribute.

Status of this Memo

This Internet-Draft is submitted to IETF in full conformance with the provisions of [BCP 78](#) and [BCP 79](#).

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/lid-abstracts.html>

The list of Internet-Draft Shadow Directories can be accessed at <http://www.ietf.org/shadow.html>

Copyright and License Notice

Copyright (c) 2015 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to [BCP 78](#) and the IETF Trust's Legal Provisions Relating to IETF Documents (<http://trustee.ietf.org/license-info>) in effect on the date of publication of this document. Please review these documents

carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

Table of Contents

1	Introduction	2
1.1	Terminology	3
2	Extended Identifier Attribute	3
3	Implementation and Usage Guidelines	3
3.1	Extended Identifier Attribute Value	3
3.2	RADIUS Client	4
3.3	RADIUS Server	4
4	Backward compatibility	4
5	Security Considerations	5
6	IANA Considerations	5
7	References	5
7.1	Normative References	5
7.2	Informative References	5
	Authors' Addresses	6

[1](#) Introduction

The Identifier field in RADIUS Message is only one octet in size. As a result, only 256 simultaneous "in flight" packets can be present at a time. This problem is also specified in [RFC 6613](#) (RADIUS over TCP) [Section 2.6.5](#) and [RFC 3539](#) (Authentication, Authorization and Accounting (AAA) Transport Profile) [Section 2.4](#).

This problem is significant in embedded systems where RADIUS clients most likely re-use the same socket due to the limitation in resources such as file descriptors.

For Example, consider the deployment of a NAS that handles thousands of 802.1x supplicants. There are many scenarios, where thousands of supplicants can request for authorization at the same time. Most of the 802.1x supplicants may not get authorized due to ID mismatch if the RADIUS client re-uses same socket for multiple requests as mentioned above.

1.1 Terminology

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [RFC 2119](#) [[RFC2119](#)].

2 Extended Identifier Attribute

```

0                               1                               2
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
|      Type      |      Length      |      Value ...
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+

```

Description

This Attribute has the same purpose as that of Identifier Field in Message Header, ie, match a request with its corresponding response and aids in detecting duplicate requests if they have the same client source IP address and source UDP port and Identifier within a short span of time.

Type

TBD

Length

6

Value

The Value field is four octets

3 Implementation and Usage Guidelines

The value of the Extended Identifier Attribute should be given more precedence than the Identifier field in Message Header.

3.1 Extended Identifier Attribute Value

The approach for generating the Extended Identifier Attribute value shall be same as followed for generation of Identifier field in

Message Header.

For example, if a Radius client uses the approach of incrementing identifier field (can support from 0 to 255) for each request, then the same approach shall be used for Extended Identifier Attribute too.

As Extended Identifier attribute length is of 4 bytes, it can support from 0 to 4294967295.

3.2 RADIUS Client

Radius client should send all the messages (say, Access-Request) with both identifier field (as part of message header) and Extended Identifier attribute.

Identifier field in the message header can get restarted from 0 after it reaches 255. But the Extended Identifier attribute needs to be restarted only after the count of 4294967295(4 bytes) is reached.

3.3 RADIUS Server

If the RADIUS Server supports Extended Identifier Attribute and the attribute is present in the message, Radius server must consider only the Extended Radius Identifier attribute value and ignore the Identifier field in the message header. In this case, Radius server should send the response (say, Access Challenge, Access Accept or Access Reject) to client with the same Extended Identifier Attribute and Identifier field in Message Header values.

If the server doesn't support Extended Identifier attribute, then Identifier field in the message header will be considered and Extended Identifier attribute must be ignored. In this case, this attribute shall not be present in the response to the client.

For the response message from Radius server, client must consider only the value of the Extended Identifier attribute value instead of Identifier field in the message header if the attribute exists in the message.

4 Backward compatibility

The proposed usage of both Identifier field and the Extended Identifier attribute ensures the backward compatibility with the servers that don't have the support for Extended Identifier

attribute.

5 Security Considerations

This document does not introduce any new security concerns to RADIUS or any other specifications referenced in this document.

6 IANA Considerations

This document requests IANA to allocate the new type code value to the proposed Extended Identifier attribute and add it to the list of RADIUS Attributes.

7 References

7.1 Normative References

- [RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", [BCP 14](#), [RFC 2119](#), March 1997.
- [RFC2865] Rigney, C., Willens, S., Rubens, A., and W. Simpson, "Remote Authentication Dial In User Service (RADIUS)", [RFC 2865](#), June 2000.
- [RFC3575] Aboba, B., "IANA Considerations for RADIUS (Remote Authentication Dial In User Service)", [RFC 3575](#), July 2003.
- [RFC5226] Narten, T. and H. Alvestrand, "Guidelines for Writing an IANA Considerations Section in RFCs", [BCP 26](#), [RFC 5226](#), May 2008.
- [RFC6158] DeKok, A. and G. Weber, "RADIUS Design Guidelines", [BCP 158](#), [RFC 6158](#), March 2011.
- [RFC6929] DeKok, A. and A. Lior, "Remote Authentication Dial In User Service (RADIUS) Protocol Extensions", [RFC 6929](#), April 2013.

7.2 Informative References

- [RFC6613] DeKok, A., "RADIUS over TCP", May 2012.
- [RFC2868] Zorn, G., Leifer, D., Rubens A., Shriver, J.,

Holdrege, M., Goyret, I, "RADIUS Attributes for Tunnel Protocol Support", June 2000

[RFC6929] DeKok, A. and Lior , A., "Remote Authentication Dial-In User Service (RADIUS) Protocol Extensions", April 2013.

[RFC5080] Nelson, D. and DeKok. A., "Common Remote Authentication Dial In User Service (RADIUS) Implementation Issues and Suggested Fixes"

[RFC2867] Zorn, G., Aboba, B. and Mitton, D., "RADIUS Accounting Modifications for Tunnel Protocol Support", June 2000.

[RFC5997] DeKok. A., "Use of Status-Server Packets in the Remote Authentication Dial In User Service (RADIUS) Protocol", August 2010.

Authors' Addresses

Sanal Kumar Kariyezhath Sivaraman
DELL
Olympia Technology Park
Guindy, Chennai 600032
India
Phone: +91 4058643
Email: Sanal_Kumar_Sivarama@dell.com

Aravind Prasad Sridharan
DELL
Olympia Technology Park
Guindy, Chennai 600032
India
Phone: +91 9884612715
Email: aravind_sridharan@dell.com

