Network Working Group
Internet Draft
Intended Status: Standards Track
Expiration Date: September 28, 2017

E. Chen
N. Shen
Cisco Systems
March 27, 2017

RADIUS Identifier Attribute
draft-chen-radext-extended-header-02.txt

Status of this Memo

Copyright Notice

Internet Draft draft-chen-radext-extended-header-02.txt March 2017

Abstract

The limitation with the one-octet "Identifier" field in the RADIUS packet is well known. In this document we propose extensions to the RADIUS protocol to address this fundamental limitation, and thus allowing for more efficient and more scalable implementations.

1. Introduction

The "Identifier" field in the RADIUS packet [RFC2865] is used to match outstanding requests and replies. As the field is one octet in size, only 256 requests can be in progress between two endpoints, which would present a significant bottleneck for performance. The workaround for this limitation is to use multiple source ports as documented and discussed in [RFC2865], [RFC3539], and [RFC6613].

Currently it is quite common to have hundreds of parallel connections between a RADIUS client and a server, especially in the deployment of controllers for wireless clients. As the scale requirement continues to increase, the number of "parallel connections" is expected to grow (perhaps reaching thousands), which will undoubtedly create a number of challenges with resource utilization, efficiency, and connection management (with RADIUS over TCP [RFC6613] in particular) on both the client and the server.

In this document we propose extensions to the RADIUS protocol to address this fundamental limitation and thus allowing for more efficient and more scalable implementations. More specifically, a new attribute ("Identifier Attribute") is defined that can be used to discover the support of this specification between a client and a server using the Status-Server message [RFC5997]. Once the support is confirmed, the attribute can then be used to carry the identifier parameter in subsequent RADIUS packets.

The attribute also provides an option for carrying the RADIUS packet type "Code" in a larger field just in case that becomes necessary in the future.

For brevity the extensions specified in this document are referred to as "the Extended Identifier feature" hereafter.

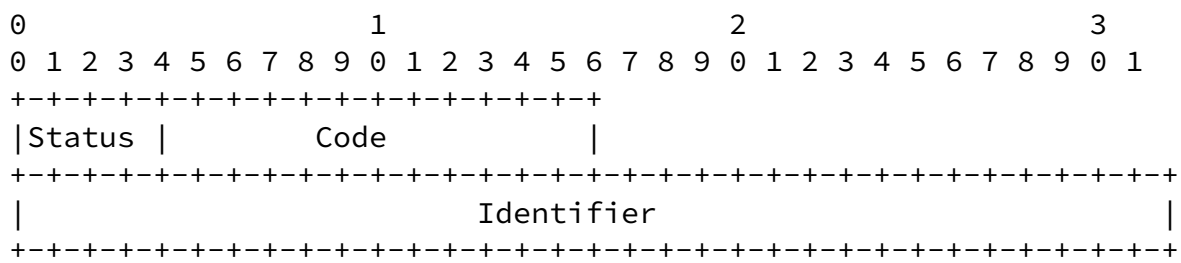
1.1. Specification of Requirements

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 [RFC2119].

2. Protocol Extensions

2.1. The Identifier Attribute

A new attribute, termed "Identifier Attribute", is specified which can be used to discover the support for the Extended Identifier feature between a client and a server. It can also be used to carry the Identifier field (and optionally the Code field) in a RADIUS packet after the support is confirmed. The attribute number is TBD. The value of the attribute has 6 octets, and consists of the following fields:



where the 4-bit Status field is to be used in a Status-Server message to discover the support for the Extended Identifier feature. The following settings are defined:

- It is set to 1 (for "request") when a client sends the Status-Server request to a server indicating its support for

the Extended Identifier feature.

- It is set to 2 (for "accept") or 3 (for "reject") by the server in its response to indicate whether it supports the Extended Identifier feature.

The 12-bit Code field, when needed, can be used in lieu of the Code field in the RADIUS packet header. The field is unused if its value is zero. The field is in use otherwise.

The Identifier field is a 4-octet unsigned integer. It is to be used in lieu of the Identifier field in the RADIUS packet header.

When the "Identifier Attribute" is used in a Status-Server request or reply, only the Status field is used. All other fields SHOULD be set to zero by the sender and MUST be ignored by the receiver.

When the "Identifier Attribute" is used in a message other than the Status-Server request or reply, the Status field is unused, and SHOULD be set to zero by the sender and MUST be ignored by the receiver.

Other than the larger sizes for the Identifier field and optionally for the Code field, these two fields remain unchanged semantically as defined in RFC 2865 [RFC2865] (and subsequent documents using the same packet format).

To simplify packet processing and for consistency, the "Identifier Attribute" MUST be encoded as the very first attribute in the attribute list of a RADIUS packet. If the attribute does not appear as the first one in the attribute list of a RADIUS packet, the RADIUS packet MUST be treated as invalid and the packet be discarded according to [RFC2865].

Due to the hop-by-hop nature of RADIUS packet transmission between RADIUS devices, a PROXY server MUST strip the "Identifier Attribute" (and reconstruct if appropriate) before sending the packet over a different session.

2.2. Status-Server Considerations

This section extends processing of Status-Server messages as described in Sections 4.1 and 4.2 of [RFC5997].

Prior to sending a RADIUS packet (other than the Status-Server request) with the "Identifier Attribute", a client implementing this specification SHOULD first send a Status-Server request with the "Identifier Attribute" to indicate its support for the Extended Identifier feature.

When a server implementing this specification receives a Status-Server request with the "Identifier Attribute", it MUST include the "Identifier Attribute" in its response to indicate whether it supports the Extended Identifier feature. If the Status-server reply from a server does not contain the "Identifier Attribute", the client MUST treat this case as "reject" by the server for the Extended Identifier feature.

Unless specified by configuration, a client MUST NOT send a RADIUS packet (other than the Status-Server request) with the "Identifier

Attribute" to a server until it has received a response from the server confirming its support for the Extended Identifier feature using the "Identifier Attribute".

When TCP is used as the transport protocol for RADIUS [RFC6613] between a client and a server, the Extended Identifier feature SHOULD be discovered each time the TCP session is established.

2.3. Co-existence of Identifier Fields

After the functionality defined in this specification is discovered between the client and the server, RADIUS packets can be exchanged using either the Identifier field in the RADIUS packet header (without the "Identifier Attribute" in the packet), or the Identifier field in the "Identifier Attribute" as the very first attribute in the attribute list.

When the "Identifier Attribute" is present in a RADIUS packet other than the Status-Server request or reply, the Identifier field in the attribute MUST be used in lieu of the Identifier field in the RADIUS packet header. Similarly the Code field in the attribute, if it is

non-zero, MUST be used in lieu of the Code field in the RADIUS packet header.

When the "Identifier Attribute" is used to carry the Identifier field, for better debugging it is RECOMMENDED that 255 be used in the Identifier field of the RADIUS packet header. Similarly it is RECOMMENDED that 255 be used in the Code field of the RADIUS packet header when the attribute is used to carry the Code field as well.

To simplify implementation, it is RECOMMENDED that the numbers 256 and larger be used as the "Identifier" in the "Identifier Attribute".

In response to a request from a client, the server SHOULD format the Identifier field in the same way as in the request, i.e., using either the Identifier field in the RADIUS packet header or the one in the "Identifier Attribute".

3. IANA Considerations

A new attribute ("Identifier Attribute") is defined for the RADIUS protocol. The type value [RFC3575] needs to be assigned using the assignment rules in section 10.3 of [RFC6929].

4. Security Considerations

This document defines a new RADIUS attribute, which does not affect the security considerations of the RADIUS protocol [RFC2865].

The new RADIUS attribute and the procedures described in this document helps eliminate the need for "parallel connections" between a RADIUS client and a server due to the limitation with the

"Identifier" field. Thus the resource utilization (such as the number of UDP/TCP ports) on a RADIUS device is expected to be reduced significantly in large scale deployment.

5. Acknowledgments

TBD

6. References

6.1. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <http://www.rfc-editor.org/info/rfc2119>.

[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.

6.2. Informative References

[RFC3539] Aboba, B. and J. Wood, "Authentication, Authorization and Accounting (AAA) Transport Profile", RFC 3539, June 2003.

[RFC6613] DeKok, A., "RADIUS over TCP", RFC 6613, May 2012.

[RFC5997] DeKok, A., "Use of Status-Server Packets in the Remote Authentication Dial In User Service (RADIUS) Protocol", RFC 5997, August 2010.

[RFC6929] DeKok, A. and A. Lior, "Remote Authentication Dial In User Service (RADIUS) Protocol Extensions", RFC 6929, April 2013.

7. Authors' Addresses

Enke Chen
Cisco Systems
560 McCarthy Blvd.
Milpitas, CA 95035
USA

Email: enkechen@cisco.com

Naiming Shen
Cisco Systems
560 McCarthy Blvd.
Milpitas, CA 95035
USA

Email: naiming@cisco.com