

Network Working Group  
Internet Draft  
Intended Status: Standards Track  
Expiration Date: October 26, 2017

E. Chen  
N. Shen  
Cisco Systems  
April 25, 2017

RADIUS Extended Identifier Attribute  
draft-chen-radext-identifier-attr-01.txt

## 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>

This Internet-Draft will expire on October 26, 2017.

## Copyright Notice

Copyright (c) 2017 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.

Internet Draft [draft-chen-radext-identifier-attr-01.txt](#)

April 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 ("Extended 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 extended identifier parameter in subsequent RADIUS packets. The extended identifier parameter can be used together with the Identifier to match outstanding requests and replies.

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].

Internet Draft [draft-chen-radext-identifier-attr-01.txt](#)

April 2017

## 2. Protocol Extensions

### 2.1. The Extended Identifier Attribute

A new attribute, termed "Extended 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 "extended identifier" parameter in a RADIUS packet after the support is confirmed. The attribute number is TBD. The value of the attribute has 4 octets, and consists of the following fields:

[illegible]

where the 2-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:

- o 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.
- o 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 30-bit "Extended Identifier" field is an unsigned integer. It is to be used together with the Identifier field to match outstanding requests and replies.

When the "Extended 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 "Extended 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.

To simplify packet processing and for consistency, the "Extended 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 "Extended 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 "Extended Identifier Attribute", a client implementing this specification SHOULD first send a Status-Server request with the "Extended Identifier Attribute" to indicate its support for the Extended Identifier feature.

When a server implementing this specification receives a Status-Server request with the "Extended Identifier Attribute", it MUST include the "Extended 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 "Extended 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 "Extended Identifier Attribute" to a server until it has received a response from the server confirming its support for the Extended Identifier feature using the "Extended 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](#). Use of the Extended Identifier Field

After the functionality defined in this specification is discovered between the client and the server, the Extended Identifier field can be carried using the "Extended Identifier Attribute" in a RADIUS packet. The Extended Identifier is to be used together with the Identifier to identify requests and replies. The assignment of these

parameters is left to implementation.

When the "Extended Identifier Attribute" is present in a RADIUS packet other than the Status-Server request or reply, the Extended Identifier field in the attribute MUST be used together with the Identifier field to identify requests and replies.

In response to a request from a client that contains the Extended Identifier field, the server MUST include the Extended Identifier field with an identical value in its reply.

### [3](#). IANA Considerations

A new attribute ("Extended 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

We would like to thank Alan DeKok for useful discussions and suggestions.

## [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](mailto:enkechen@cisco.com)

Naiming Shen  
Cisco Systems

Chen & Shen

[Page 6]

---

Internet Draft [draft-chen-radext-identifier-attr-01.txt](#)

April 2017

560 McCarthy Blvd.  
Milpitas, CA 95035  
USA

Email: [naiming@cisco.com](mailto:naiming@cisco.com)

