Extended Packet Header for RADIUS
draft-chen-radext-extended-header-00.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/1id-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 January 9, 2017.

Copyright Notice

Copyright (c) 2016 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.
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.

The protocol extensions primarily consist of the following:

- an extended packet header (with a larger "Identifier" field) is defined for the RADIUS packet.
- a RADIUS packet code is reserved for carrying RADIUS packets using the "extended packet header".
- a new attribute ("Extended Packet Header") is defined for indicating support for the "extended packet header" between a client and server using the Status-Server message.

The "code" field in the RADIUS packet is also enlarged from one-octet to two-octets.
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. Extended Packet Header Format

In this document we reserve a RADIUS packet code ("EXT-PKT-CODE") for carrying a RADIUS packet using the "extended packet header" (or just "extended header") as follows:

```
| EXT-PKT-CODE | Reserve-A |            Length             |
| Authenticator |
| Reserve-B (0x0008) | Code |
| Identifier |
| Attributes ... |
```

The value of the "EXT-PKT-CODE" is TBD.

Other than the larger sizes for the "Code" and "Identifier" fields, all the fields "Code", "Identifier", "Length", and "Attributes" remain unchanged semantically as defined in RFC 2865 (and subsequent documents using the same packet format).

The "Reserved-A" field is reserved. It SHOULD be set to zero by the sender and MUST be ignored by the receiver.

The "Reserved-B" field is reserved. It SHOULD be set to 0x0008 by the sender and MUST be ignored by the receiver.
The layout of the fields allow the packet to be parsed syntactically by an existing protocol analysis tool.

While the primary motivation is to enlarge the "Identifier" field, the "Code" field is also enlarged as part of this header definition. The larger "Code" field allows new packet types to be defined in the future. Obviously all the existing types would fit in the 2-octet field.

For the sake of brevity, the packet format specified in [RFC2865] is referred to as the "standard packet header" or "standard header".

Although the "EXT-PKT-CODE" is used in this specification as the indication that the "extended header" is in use, it is not a bonafide RADIUS packet code in the usual sense, and MUST NOT be used other than as described above. If encountered in the "Code" field of a RADIUS packet using the "extended header", it MUST be treated as invalid and the packet be discarded according to [RFC2865].

2.2. Extended Packet Header Attribute

A new attribute, "Extended Packet Header Attribute", is specified which can be used to indicate support for the "Extended Packet Header Format". The "value" of the attribute is 0-octet.

   Name: Extended Packet Header
   Attribute: TBD
   Description: 0-octet attribute indicating support for the extended packet header

The attribute MAY be included in a Status-Server message [RFC5997] to indicate that the client is prepared to receive the RADIUS packets using the "extended header" as well as the ones using the "standard header". The attribute MAY also be included in a response to a Status-Server message to indicate that the server is prepared to receive the RADIUS packets using the "extended header" as well as the ones using the "standard header".

2.3. 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 using the "extended header", a client implementing this specification SHOULD first send a Status-Server request with the "Extended Packet Header" attribute to
indicate that it is prepared to receive the RADIUS packets using the "extended header" in addition to the ones using the "standard header".

When a server implementing this specification receives a Status-Server request with the "Extended Packet Header" attribute, it MUST include the "Extended Packet Header" attribute in its response to indicate that it is prepared to receive the RADIUS packets using the "extended header" in addition to the ones using the "standard header".

Unless specified by configuration, a client MUST not send a RADIUS packet using the "extended header" to a server until it has received a response from the server containing the "Extended Packet Header" attribute.

Unless specified by configuration, a server MUST not send a RADIUS packet using the "extended header" to a client until it has received a Status-Server request from the client containing the "Extended Packet Header" attribute.

2.4. Co-existence of Packet Headers

When the functionality defined in this specification is discovered between the client and the server, RADIUS packets using either the "standard header" or the "extended header" can be exchanged.

To simplify implementation, it is RECOMMENDED that the numbers 0 - 255 be used as the "Identifier" in packets with the "standard header", and the numbers 256 and larger are used as the "Identifier" in packets with the "extended header".

The "Status-Server" message MUST be encoded using the "standard header".

In response to a request from a client, the server SHOULD use the same header format as the one in the request.
3. Backward Compatibility

This specification relies on the discovery mechanism using the the Status-Server message.

The "extended header" is compatible with the "standard header" syntactically. Thus existing protocol analysis tools can still be used.

The existing packet "Code" is to be encoded into the 2-octet field in the "extended header".

The co-existence of the "standard header" and the "extended header" would facilitate recovery in case of software downgrades and some failure scenarios.

Due to the hop-by-hop nature of RADIUS packets transmission between RADIUS devices, a PROXY server usually need to correlate between packets over separate sessions. With this specification a packet may need to be transformed to accommodate the header changes.

4. IANA Considerations

A new RADIUS packet type code is proposed in the RADIUS packet type codes registry discussed in section 2.1 of RFC 3575 [RFC3575]. The name is "Extended Packet Header" and the code is <TBD>.

The following RADIUS attribute type value [RFC3575] is proposed. The assignment rules in section 10.3 of [RFC6929] are used.

5. Security Considerations

TBD
6. Acknowledgments

TBD

7. References

7.1. Normative References


7.2. Informative References


[RFC6614] Winter, S., McCauley, M., Venaas, S., and K. Wierenga,


8. 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