RADIUS Error Messages
draft-zorn-radius-err-msg-00.txt

Status of this Memo

This document is an Internet-Draft and is in full conformance with all provisions of Section 10 of RFC2026.

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 Internet-Draft will expire on November 4, 2004.

Copyright Notice

Copyright (C) The Internet Society (2004). All Rights Reserved.

Abstract

This document describes new RADIUS protocol elements designed to allow the communication of packet and attribute errors between RADIUS servers and clients.
Table of Contents

1. Introduction .................................................. 3
2. Specification of Requirements ................................. 3
3. RADIUS Packet Format ........................................... 3
4. Packet Types .................................................... 6
4.1 Error-Notification ............................................ 6
5. Attributes ....................................................... 7
5.1 Error-Code ..................................................... 7
6. Attribute Values ................................................ 8
6.1 Acct-Error-Notification ....................................... 8
7. IANA Considerations ............................................. 9
8. Security Considerations ......................................... 9
    Normative References ......................................... 9
    Author’s Address ................................................ 9
    Intellectual Property and Copyright Statements ............... 10
1. Introduction

The RADIUS protocol [RFC2865] is defined to allow most errors to be ignored and to silently discard unrecognized or erroneous packets. In many cases, this behavior is beneficial or at least innocuous. For example, it's probably a good idea to discard messages from unknown clients and server messages having incorrect authenticators, and discarding short packets doesn’t seem to hurt anything. In some cases, however, this policy can cause interoperability problems and may result in the provision of incorrect services to users, particularly in roaming situations.

Because RADIUS packets having unknown values in the Code field of the header are silently discarded it is difficult to ascertain whether a new packet type is considered invalid by the remote client/server or if the message was simply lost. Similarly, RFC 2865 allows clients to ignore unrecognized attributes, which can lead to incorrect service provisioning.

This document defines a set of messages and attributes that can be used to notify a RADIUS client or server of various message errors.

Discussion of this draft may be directed to the author.

2. 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].

3. RADIUS Packet Format

Exactly one RADIUS packet is encapsulated in the UDP Data field [RFC0768] where the UDP Destination Port field indicates 1812 (decimal).

When a reply is generated, the source and destination ports are reversed.

A summary of the RADIUS data format is shown below. The fields are transmitted from left to right.
The Code field is one octet, and identifies the type of RADIUS packet. When a client receives a packet with an invalid Code field, it is silently discarded. If a server receives a packet with an invalid Code field from a valid client, it MUST reply with an Error-Notification packet (see below).

The RADIUS Codes (decimal) defined in this document are as follows:

<MSG1>    Error-Notification

The Identifier field is one octet, and aids in matching requests, replies and notifications. The RADIUS server can detect a duplicate request if it has the same client source IP address, source UDP port and Identifier within a short span of time.

The Length field is two octets. It indicates the length of the packet including the Code, Identifier, Length, Authenticator and Attribute fields. Octets outside the range of the Length field MUST be treated as padding and ignored on reception. If the packet is shorter than the Length field indicates, it MUST be silently discarded. The minimum length is 20 and maximum length is 4096.
Authenticator

The Authenticator field is sixteen (16) octets. The most significant octet is transmitted first. This value is used to authenticate the reply from the RADIUS server.

Notification Authenticator

The value of the Authenticator field in the Error-Notification packet is called the Notification Authenticator, and contains a one-way MD5 hash calculated over a stream of octets consisting of: the RADIUS packet, beginning with the Code field, including the Identifier, the Length, the Authenticator field from the packet to which this packet is a response, and the response Attributes, followed by the shared secret. That is,

\[
\text{Notification Auth} = \text{MD5(Code+ID+Length+RequestAuth+Attributes+Secret)}
\]

where ‘+’ denotes concatenation.

Administrative Note

The secret shared between the client and the RADIUS server SHOULD be at least as large and unguessable as a well-chosen password. It is preferred that the secret be at least 16 octets. This is to ensure a sufficiently large range for the secret to provide protection against exhaustive search attacks. The secret MUST NOT be empty (length 0) since this would allow packets to be trivially forged.

A RADIUS server MUST use the source IP address of the RADIUS UDP packet to decide which shared secret to use, so that RADIUS requests can be proxied.

When using a forwarding proxy, the proxy must be able to alter the packet as it passes through in each direction - when the proxy forwards the request, the proxy MAY add a Proxy-State Attribute, and when the proxy forwards a response, it MUST remove its Proxy-State Attribute if it added one. Proxy-State is always added or removed after any other Proxy-States, but no other assumptions regarding its location within the list of attributes can be made. Since Access-Accept and Access-Reject replies are authenticated on the entire packet contents, the stripping of the Proxy-State attribute invalidates the signature in the packet - so the proxy has to re-sign it.

Further details of RADIUS proxy implementation are outside the
4. Packet Types

The RADIUS Packet type is determined by the Code field in the first octet of the Packet.

4.1 Error-Notification

Description

Error-Notification packets are sent by a RADIUS server as an indication that a previous request contained one or more errors. A RADIUS server wishing to notify a client that one or more errors occurred MUST transmit a RADIUS packet with the Code field set to \(<MSG1>\) (Error-Notification).

Error-Notification packets MUST contain at least one Error-Code Attribute.

A summary of the Error-Notification packet format is shown below. The fields are transmitted from left to right.

\[
\begin{array}{|c|c|c|}
\hline
0 & 1 & 2 & 3 \\
\hline
\text{Code} & \text{Identifier} & \text{Length} \\
\hline
\text{Notification Authenticator} \\
\hline
\text{Attributes ...} \\
\hline
\end{array}
\]

Code

\(<MSG1>\) for Error-Notification

Identifier

The Identifier field is a copy of the Identifier field of the packet which caused this Error-Notification packet to be
created.

Notification Authenticator

The Notification Authenticator value is calculated from the Error-Notification packet, as described above.

Attributes

The Attribute field is variable in length, and contains any desired optional Attributes in addition to the required Attributes.

5. Attributes

5.1 Error-Code

Description

This attribute contains a code identifying the class of error that occurred, a code signifying the error itself and an optional text description of the error.

The Error-Code Attribute MUST be included in Error-Notification packets sent from a server.

RADIUS Accounting [RFC2866] clients MUST include this Attribute in Accounting-Request packets in which the Acct-Status-Type Attribute has a value of Acct-Error-Notification (see below).

A summary of the Error-Code Attribute format is shown below. The fields are transmitted from left to right.

```
+-----------------------------------+
<table>
<thead>
<tr>
<th>Type</th>
<th>Length</th>
<th>Class</th>
<th>Code</th>
</tr>
</thead>
<tbody>
<tr>
<td>Code (cont’d.)</td>
<td>String...</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
```

Type

<ATR> for Error-Code.
Length

>= 4

Class

The CLASS field contains a single ASCII character indicating the severity of the error. This document defines the following error classes:

F  The error was fatal and the message causing the error was discarded.

W  Warning error: the message was processed, but the result may not be as anticipated.

Code

The Code field contains an unsigned integer representing the type of error that occurred. This document defines the following decimal values for the Code field:

1  Unrecognized Packet Type

2  Unrecognized Vendor OUI

3  Unrecognized Attribute

4  Unknown Session Identifier

5  Unknown Key Identifier

String

The optional String field contains a text description of the error. When the Error-Code Attribute is used in Accounting-Request packets, the String field SHOULD contain a message describing the error.

6. Attribute Values

The following sub-sections defines a new value for the Acct-Status-Type Attribute [RFC2866].

6.1 Acct-Error-Notification
Description

When the value <VAL> is present in the Value field of an Acct-Status-Type Attribute in an Accounting-Request packet, it signifies that one or more errors have occurred on the client side.

7. IANA Considerations

The criteria to be used by the Internet Assigned Numbers Authority (IANA) for assignment of numbers within namespaces defined within this document are identical to those given in [RFC3575].

8. Security Considerations

None.

Normative References


Author’s Address

Glen Zorn
Cisco Systems
2901 Third Avenue, Suite 600
Seattle, WA  98121
US

Phone: +1 425 344 8113
EMail: gwz@cisco.com
Intellectual Property Statement

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 implementors 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 (2004). All Rights Reserved.

This document and translations of it may be copied and furnished to others, and derivative works that comment on or otherwise explain it or assist in its implementation may be prepared, copied, published and distributed, in whole or in part, without restriction of any kind, provided that the above copyright notice and this paragraph are included on all such copies and derivative works. However, this document itself may not be modified in any way, such as by removing the copyright notice or references to the Internet Society or other Internet organizations, except as needed for the purpose of developing Internet standards in which case the procedures for copyrights defined in the Internet Standards process must be followed, or as required to translate it into languages other than English.

The limited permissions granted above are perpetual and will not be revoked by the Internet Society or its successors or assignees.

This document and the information contained herein is provided on an "AS IS" basis and THE INTERNET SOCIETY AND THE INTERNET ENGINEERING TASK FORCE DISCLAIMS 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.

Acknowledgment

Funding for the RFC Editor function is currently provided by the
Internet Society.