Internet Draft
Category: Experimental
expires in six months

Pat R. Calhoun
US Robotics Access Corp.
Allan Rubens
Merit Network Inc.
June 1996

Enhanced Remote Authentication Dial In User Service (RADIUS)

<draft-calhoun-enh-radius-00.txt>

Status of this Memo

Abstract

This document describes a protocol for carrying authentication, authorization, and configuration information between a Network Access Server which desires to authenticate its links and a shared Authentication Server. This enhanced protocol is a backward compatible protocol which attempts to solve many deficiencies with the existing protocol.

1. Introduction

Enhanced RADIUS is an extension to the existing RADIUS specification [1]. This document in itself is not complete and should be used with the RADIUS Version 1 specification [1].

Since RADIUS Version 1 has a very limited number of available commands and attributes, the intent of the Enhanced RADIUS protocol is to allow for future protocol enhancements.

This document will describe the packet headers for the Enhanced RADIUS protocol as well as any commands and attributes which MUST be supported. An accompanying document will describe the documentation required in order to standardize any protocol extensions.

1.1. Specification of Requirements

In this document, several words are used to signify the requirements of the specification. These words are often capitalized.

MUST — This word, or the adjective "required", means that the definition is an absolute requirement of the specification.

MUST NOT — This phrase means that the definition is an absolute prohibition of the specification.

SHOULD — This word, or the adjective "recommended", means that there may exist valid reasons in particular circumstances to ignore this item, but the full implications must be understood and carefully weighed before choosing a different course.

MAY — This word, or the adjective "optional", means that this item is one of an allowed set of alternatives. An implementation which does not include this option MUST be prepared to interoperate with another implementation which does include the option.

1.2. Terminology

This document frequently uses the following terms:

silently discard

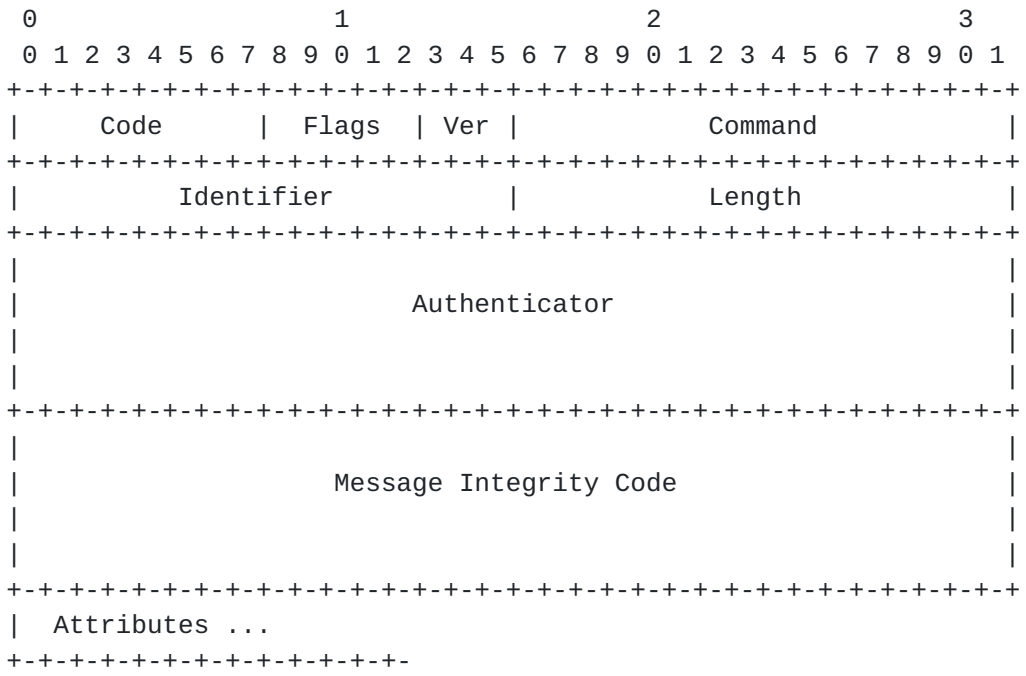
> This means the implementation discards the packet without further processing. The implementation SHOULD provide the capability of logging the error, including the contents of the silently discarded packet, and SHOULD record the event in a statistics counter.

2. Packet Format

Exactly one RADIUS packet is encapsulated in the UDP Data field [3], where the UDP Destination Port field indicates 1645.

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

A summary of the Enhanced RADIUS data format is shown below. The fields are transmitted from left to right.



Code

The Code field is one octet, and identifies the type of RADIUS packet. When a valid code is received, the packet format to use is as defined in the RADIUS V1 specification [1]. When a packet is received with an invalid Code field, it is silently discarded. When a code of 0xFE (254) is received, it identifies an Enhanced RADIUS packet as shown above, in which case the Command field is to be checked. In this case the RADIUS Codes wich follow (with the exception of 254) are passed in the Command field instead.

RADIUS Codes (decimal) are assigned as follows:

1	Access-Request
2	Access-Accept
3	Access-Reject
4	Accounting-Request
5	Accounting-Response
11	Access-Challenge
12	Status-Server (experimental)
13	Status-Client (experimental)
254	Enhanced RADIUS packet

Flags

The Flags field is five bits, and is used in order to identify any options. This field MUST be set to zero unless any options are used. The following flags are defined globally for all commands:

0x1 - (Bit 12) TimeStamp is included in the Authenticator Field.

Note that additional options in the Flag field may be defined per Command (see individual commands).

Version

The Version field is three bits, and indicates the version number which is associated with the packet received. This field MUST be set to 2.

Command

The Command field is two octet, and identifies the type of RADIUS packet. When a packet is received with an invalid Code field, a Command-Unrecognized message SHOULD be returned.

RADIUS Commands (decimal), in addition to those shown above, are assigned as follows:

256 Command-Unrecognized
267 NAS-Reboot-Indication
268 NAS-Reboot-Ack

Identifier

The Identifier field is two octets, and aids in matching requests and replies.

Length

The Length field is two octets. It indicates the length of the packet including the header fields. Octets outside the range of the Length field should be treated as padding and should be ignored on reception.

Authenticator

The Authenticator field is a random 16 octet value. This field adds randomness to the packets and makes the guessing of the shared secret much more diffcult to the malicious user.

If the Timestamp option is supported, the first four octets contains a timestamp of when the packet was sent from the peer. This allows the protocol to detect replay attacks. The Timestamp value is the current time relative to a base of 0:0:0 GMT January 1, 1900.

Message Integrity Code

This field contains an MD5 hash of the following:

MD5(packet | Shared Secret)

When creating a message, the MIC must be set to all zeros before calculating the MD5 hash. When receiving a message, the receiver must save the MIC, set the field to all zeroes and perform the hash function. The resulting value MUST be identical to the value which was in the message.

3. Command Name and Command Code

Command Name: Command-Unrecognized
Command Code: 256

Command Name: NAS-Reboot-Indicationr
Command Code: 267

Command Name: NAS-Reboot-Ack
Command Code: 268

4. Command Meanings

The Enhanced RADIUS Packet type is determined by the Command Code field in the second and third octets of the Packet. This section will not describe the RADIUS packets already defined in [1].

4.1. Command-Unrecognized

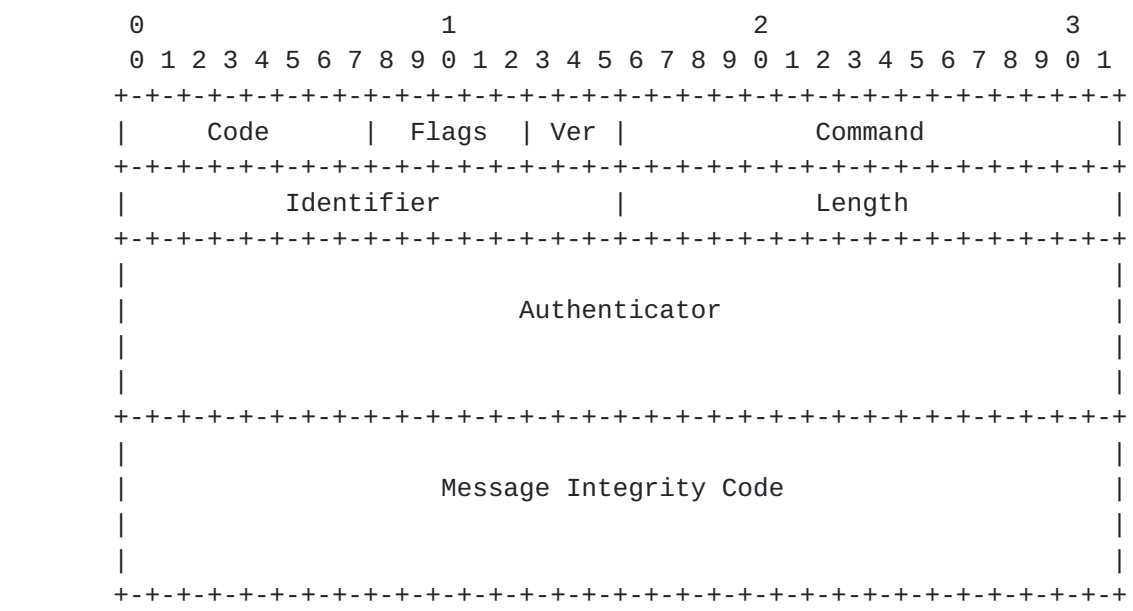
Description

Command-Unrecognized packets are sent by the NAS or the RADIUS server to inform its peer that a previous packet received is unrecognized.

Since there certainly will exist a case where an existing device does not support a new extension to the Enhanced RADIUS protocol, a device which receives a packet with an unrecognized Command code SHOULD return a Command-Unrecognized packet.

For backward compatibility with RADIUS Version 1, a device MUST support the fact that its peer may silently discard the packet.

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



Code

254 for Enhanced RADIUS.

Flags

The Flag field is used as described above.

Version

MUST be set to 2

Command

256 for Command-Unrecognized.

Identifier

The Identifier field is a copy of the Identifier field of the packet which caused this event.

Length

The total length of the message, including the this header.

Authenticator

The Authenticator field is a random 16 octet value. If the Timestamp option is supported, the first four octets contains a timestamp of when the packet was sent from the peer.

Message Integrity Code

This field contains an MD5 hash of the following:

MD5(packet | Shared Secret)

4.2. NAS-Reboot-Indication

Description

The NAS-Reboot-Indication message is sent from the NAS to the RADIUS Server in order for the NAS to inform the local server that it has rebooted. The server MUST respond to the message with a successful acknowledge, indicating its version.

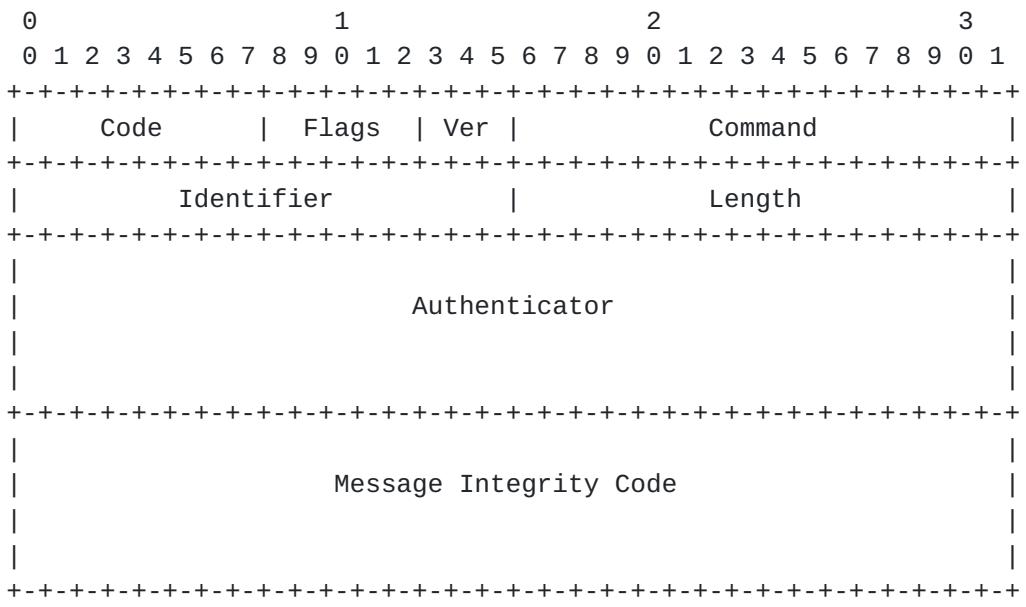
This message is used by both the NAS and the RADIUS Server in order to exchange protocol version numbers which it supports. The NAS MUST insert the highest version number which it supports. The RADIUS Server must respond with the highest version which it supports, but may not be higher than the version number requested by the NAS.

In the case of a proxy server, the proxy is responsible for inserting the highest version number which it supports in the version field before sending the proxy request to the remote RADIUS server. The proxy server may then retain the version number of the remote server as received in the response, and must insert its highest version number (with the limitations described above) in the response to the NAS.

The Server may discard this information if it wishes to do so, however it is envisioned that the Server would retain the NAS' and remote RADIUS server's version numbers to retain backward and forward protocol compatibility.

A NAS MUST support the fact that it may not receive an acknowledge to this message if the RADIUS Server does not support this version of the protocol. In this case, if no acknowledge was receive, it must default to version 1 messages as described in [1].

If a NAS is configured to communicate with more than one RADIUS server it MUST issue NAS-Reboot-Indications to each such server.



Code

254 for Enhanced RADIUS

Flags

The Flag field is used as described above.

Version

The version field is used by the NAS to indicate the highest supported version of the RADIUS protocol. This will allow the NAS and RADIUS Server to be able to negotiate a version of the protocol to use between both peers.

Command

267 for NAS-Reboot-Indication.

Identifier

The Identifier field MUST be changed whenever the content of the Attributes field changes, and whenever a valid reply has been received for a previous request. For retransmissions, the Identifier MAY remain unchanged.

Length

The total length of the message, including this header.

Authenticator

The Authenticator field is a random 16 octet value. If the Timestamp option is supported, the first four octets contain a timestamp of when the packet was sent from the peer.

Message Integrity Code

This field contains an MD5 hash of the following:

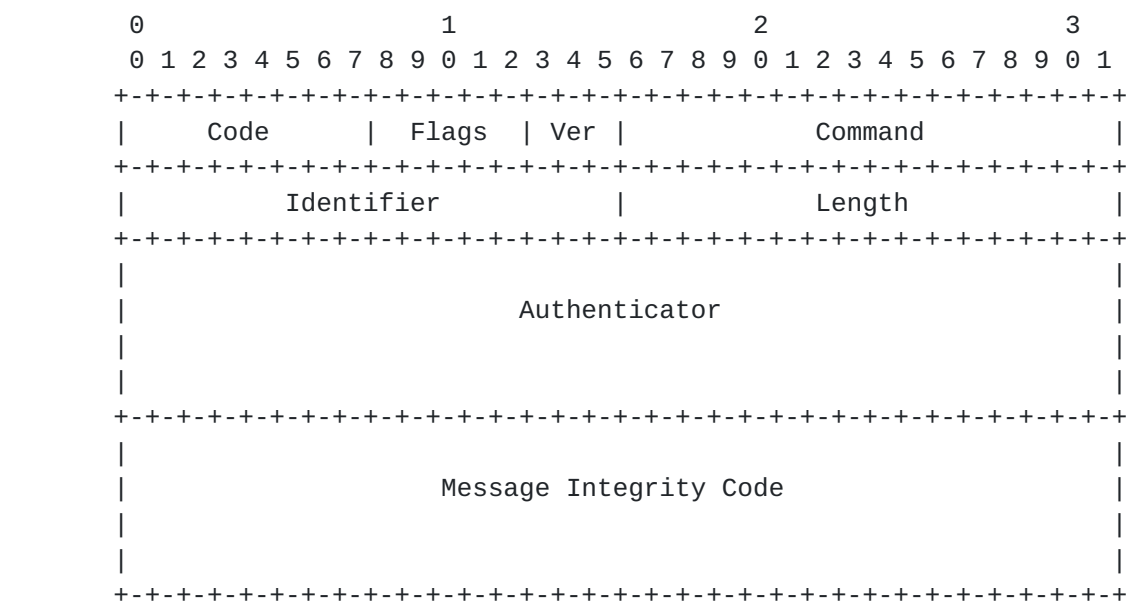
MD5(packet | Shared Secret)

5.3. NAS-Reboot-Ack

Description

The NAS-Reboot-Ack message is sent from the RADIUS Server to the NAS to acknowledge the receipt of the NAS-Reboot message. The Server MUST replace the version value in the version field with the highest version number which it supports, up to and including the version which was included in the NAS-Reboot's version field.

The NAS may wish to ignore the version number contained in the Flag field, however it is envisioned that the NAS would retain this information to remove any backward compatibility problems with any future versions of the protocol.



Code

254 for Enhanced RADIUS.

Flags

The Flag field is used as described above.

Version

The Version field is used by the RADIUS Server to inform the NAS the highest version which it supports. The Server MUST not insert a version which is higher than requested by the NAS. The client MUST use the version which is reported by the Server. If the NAS does not support the version returned by the Server, it should default to RADIUS V1.

Command

268 for NAS-Reboot-Ack.

Identifier

The Identifier field is a copy of the Identifier field of the packet which caused this event.

Length

The total length of the message, including this header.

Authenticator

The Authenticator field is a random 16 octet value. If the Timestamp option is supported, the first four octets contain a timestamp of when the packet was sent from the peer.

Message Integrity Code

This field contains an MD5 hash of the following:

MD5(packet | Shared Secret)

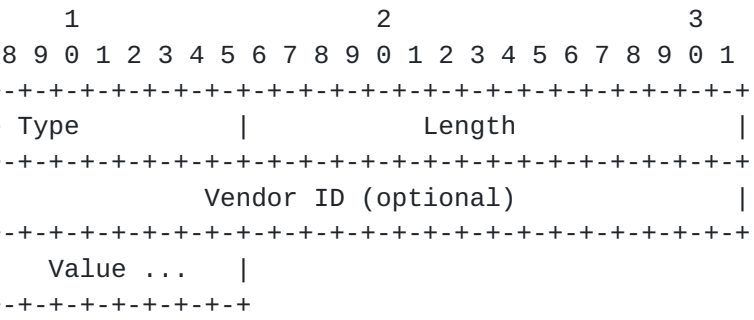
6. Attributes

RADIUS Attributes carry the specific authentication, authorization, information and configuration details for the request and reply.

Some Attributes MAY be listed more than once. The effect of this is Attribute specific, and is specified by each such Attribute description.

The end of the list of Attributes is indicated by the length of the RADIUS packet.

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



Type

The Type field is two octets. RADIUS Version 1 reserves the lowest 256 attribute numbers. Up-to-date values of the RADIUS Type field are specified in the most recent "Assigned Numbers" RFC [2].

Enhanced RADIUS Versions will use attribute numbers 257 and above. Vendor Specific attributes reside within this space when the Vendor Specific bit is set (see flags). This will allow up to 65535 trouble-free vendor specific attributes (per vendor).

Length

The Length field is two octets, and indicates the length of this Attribute including the Type, Length, Flag, Vendor ID is present and Value fields. If a packet is received with an Invalid length, the packet SHOULD be rejected.

Flags

The Flags field indicates how the NAS or RADIUS Server MUST react to the attribute. The following values are currently supported:

1 - The Device MUST support this attribute. If the attribute is NOT supported, the device MUST reject the Command. If this flag is not set, then the device MAY accept the command regardless of whether or not the particular attribute is recognized.

128 - If this bit is set, the optional Vendor ID field will be present. When set, the attribute is a vendor specific attribute

Value

The Value field is zero or more octets and contains information specific to the Attribute. The format and length of the Value field is determined by the Type and Length fields.

The format of the value field is one of five data types.

string 0-65526 octets.

address 32 bit value, most significant octet first.

extended address Address Length is determined from the Length field, most significant octet first. This is required in order to support protocols which require an address length greater than 32 bits (i.e. IPNG). Note that this type is differentiated from the previous type by the value of length.

integer 32 bit value, most significant octet first.

time 32 bit value, most significant octet first -- seconds since 00:00:00 GMT, January 1, 1970.

References

[1] Rigney, et alia, "RADIUS Authentication", Internet-Draft, Livingston, May 1995.

[2] Reynolds, J., and J. Postel, "Assigned Numbers", RFC 1700, USC/Information Sciences Institute, October 1994.

[3] Postel, J., "User Datagram Protocol", RFC 768, USC/Information Sciences Institute, August 1980.

[4] Calhoun, "Enhanced RADIUS Protocol Extension Specifications", Internet-Draft, US Robotics Access Corp., May 1996.