Network Working Group
INTERNET-DRAFT
Obsoletes: 3576
Category: Informational
<draft-ietf-radext-rfc3576bis-07.txt>
27 May 2007

Murtaza S. Chiba
Gopal Dommety
Mark Eklund
Cisco Systems, Inc.
David Mitton
RSA Security, Inc.
Bernard Aboba
Microsoft Corporation

Dynamic Authorization Extensions to Remote Authentication Dial In User Service (RADIUS)

By submitting this Internet-Draft, each author represents that any applicable patent or other IPR claims of which he or she is aware have been or will be disclosed, and any of which he or she becomes aware will be disclosed, in accordance with Section 6 of 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/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 December 25, 2007.

Copyright Notice

Copyright (C) The IETF Trust (2007). All Rights Reserved.

Abstract

This document describes a currently deployed extension to the Remote Authentication Dial In User Service (RADIUS) protocol, allowing dynamic changes to a user session, as implemented by network access server products. This includes support for disconnecting users and changing authorizations applicable to a user session.

Table of Contents

1. Introduction 3
  1.1 Applicability 3
  1.2 Requirements Language 4
  1.3 Terminology 4
2. Overview 5
  2.1 Disconnect Messages (DM) 5
  2.2 Change-of-Authorization Messages (CoA) 5
  2.3 Packet Format 6
3. Attributes 10
  3.1 Proxy State 12
  3.2 Authorize Only 12
  3.3 State 13
  3.4 Message-Authenticator 14
  3.5 Error-Cause 15
  3.6 Table of Attributes 18
4. Diameter Considerations 21
5. IANA Considerations 23
6. Security Considerations 24
  6.1 Authorization Issues 24
  6.2 Impersonation 25
  6.3 IPsec Usage Guidelines 25
  6.4 Replay Protection 28
7. Example Traces 29
8. References 29
  8.1 Normative References 29
  8.2 Informative References 30
ACKNOWLEDGMENTS 31
AUTHORS' ADDRESSES 32
Appendix A - Changes from RFC 3576 33
Full Copyright Statement 35
Intellectual Property 35

1. Introduction

The RADIUS protocol, defined in [RFC2865], does not support unsolicited messages sent from the RADIUS server to the Network Access Server (NAS).

However, there are many instances in which it is desirable for changes to be made to session characteristics, without requiring the NAS to initiate the exchange. For example, it may be desirable for administrators to be able to terminate a user session in progress. Alternatively, if the user changes authorization level, this may require that authorization attributes be added/deleted from a user session.

To overcome these limitations, several vendors have implemented additional RADIUS commands in order to be able to support unsolicited messages to be sent to the NAS. These extended commands provide support for Disconnect and Change-of-Authorization (CoA) packets. Disconnect packets cause a user session to be terminated immediately, whereas CoA packets modify session authorization attributes such as data filters.

1.1. Applicability

This protocol is being recommended for publication as an Informational RFC rather than as a standards-track RFC because of problems that cannot be fixed without creating incompatibilities with deployed implementations. This includes security vulnerabilities, as well as semantic ambiguities resulting from the design of the Change-of-Authorization (CoA) commands. While fixes are recommended, they cannot be made mandatory since this would be incompatible with existing implementations.

Existing implementations of this protocol do not support authorization checks, so that an ISP sharing a NAS with another ISP could disconnect or change authorizations for another ISP's users. In order to remedy this problem, a "Reverse Path Forwarding" check is described; see Section 6.1. for details.

Existing implementations utilize per-packet authentication and integrity protection algorithms with known weaknesses [MD5Attack]. To provide stronger per-packet authentication and integrity protection, the use of IPsec is recommended. See Section 6.3 for details.

Existing implementations lack replay protection. In order to support replay detection, it is recommended that an Event-Timestamp Attribute be added to all packets in situations where IPsec replay protection

is not employed. See Section 6.4 for details.

The approach taken with CoA commands in existing implementations results in a semantic ambiguity. Existing implementations of the CoA-Request identify the affected session, as well as supply the authorization changes. Since RADIUS Attributes included within existing implementations of the CoA-Request can be used for session identification or authorization change, it may not be clear which function a given attribute is serving.

The problem does not exist within the Diameter protocol [RFC3588], in which server-initiated authorization change is initiated using a Re-Auth-Request (RAR) command identifying the session via User-Name and Session-Id AVPs and containing a Re-Auth-Request-Type AVP with value "AUTHORIZE_ONLY". This results in initiation of a standard Request/Response sequence where authorization changes are supplied. As a result, in no command can Diameter AVPs have multiple potential meanings.

1.2. Requirements Language

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].

1.3. Terminology

This document frequently uses the following terms:

Dynamic Authorization Client (DAC)
The entity originating Change of Authorization (CoA) Requests or Disconnect-Requests. While it is possible that the DAC is co-resident with a RADIUS authentication or accounting server, this need not necessarily be the case.

Dynamic Authorization Server (DAS)
The entity receiving CoA-Request or Disconnect-Request packets. The DAS may be a NAS or a RADIUS proxy.

Network Access Server (NAS)
The device providing access to the network.

service
The NAS provides a service to the user, such as IEEE 802 or Point-to-Point Protocol (PPP).

session
Each service provided by the NAS to a user constitutes a session,

with the beginning of the session defined as the point where service is first provided and the end of the session defined as the point where service is ended. A user may have multiple sessions in parallel or series if the NAS supports that.

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. Overview

This section describes the most commonly implemented features of Disconnect and Change-of-Authorization (CoA) packets.

2.1. Disconnect Messages (DM)

A Disconnect-Request packet is sent by the Dynamic Authorization Client in order to terminate a user session on a NAS and discard all associated session context. The Disconnect-Request packet is sent to UDP port 3799, and identifies the NAS as well as the user session to be terminated by inclusion of the identification attributes described in Section 3.

```
+----------+                          +----------+
|          |   Disconnect-Request     |          |
|          |   <--------------------  |  Dynamic |
|    NAS   |                          |  Authz   |
|          |   Disconnect-Response    |  Client  |
|          |   ---------------------> |          |
+----------+                          +----------+
```

The NAS responds to a Disconnect-Request packet sent by a Dynamic Authorization Client with a Disconnect-ACK if all associated session context is discarded and the user session is no longer connected, or a Disconnect-NAK, if the NAS was unable to disconnect the session and discard all associated session context. A Disconnect-ACK MAY contain the Attribute Acct-Terminate-Cause (49) [RFC2866] with the value set to 6 for Admin-Reset.

2.2. Change-of-Authorization Messages (CoA)

CoA-Request packets contain information for dynamically changing session authorizations. Typically this is used to change data filters. The data filters can be of either the ingress or egress kind, and are sent in addition to the identification attributes as described in section 3. The port used, and packet format (described

in Section 2.3), are the same as that for Disconnect-Request packets.

The following attributes MAY be sent in a CoA-Request:

Filter-ID (11) - Indicates the name of a data filter list to be applied for the session that the identification attributes map to.

NAS-Filter-Rule (92) - Provides a filter list to be applied for the session that the identification attributes map to [RFC4849].

```
+----------+                            +----------+
|          |      CoA-Request           |          |
|          |  <--------------------     | Dynamic  |
|   NAS    |                            | Authz    |
|          |     CoA-Response           | Client   |
|          |   ---------------------> |          |
+----------+                            +----------+
```

The NAS responds to a CoA-Request sent by a Dynamic Authorization Client with a CoA-ACK if the NAS is able to successfully change the authorizations for the user session, or a CoA-NAK if the CoA-Request is unsuccessful. A NAS MUST respond to a CoA-Request including a Service-Type Attribute with an unsupported value with a CoA-NAK; an Error-Cause Attribute with value "Unsupported Service" SHOULD be included.

2.3. Packet Format

For either Disconnect-Request or CoA-Request packets UDP port 3799 is used as the destination port. For responses, the source and destination ports are reversed. Exactly one RADIUS packet is encapsulated in the UDP Data field.

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

The packet format consists of the fields: Code, Identifier, Length, Authenticator, and Attributes in Type:Length:Value (TLV) format. All fields hold the same meaning as those described in RADIUS [RFC2865]. The Authenticator field MUST be calculated in the same way as is specified for an Accounting-Request in [RFC2866].

```
    0                   1                   2                   3
    0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |     Code      |  Identifier   |            Length             |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |                                                               |
   |                         Authenticator                         |
   |                                                               |
   |                                                               |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |  Attributes ...
   +-+-+-+-+-+-+-+-+-+-+-+-+-
```

Code

The Code field is one octet, and identifies the type of RADIUS packet. Packets received with an invalid Code field MUST be silently discarded. RADIUS codes (decimal) for this extension are assigned as follows:

40 - Disconnect-Request [RFC3575]
41 - Disconnect-ACK [RFC3575]
42 - Disconnect-NAK [RFC3575]
43 - CoA-Request [RFC3575]
44 - CoA-ACK [RFC3575]
45 - CoA-NAK [RFC3575]

Identifier

The Identifier field is one octet, and aids in matching requests and replies. A Dynamic Authorization Server implementing this specification MUST be capable of detecting a duplicate request if it has the same source IP address, source UDP port and Identifier within a short span of time.

The responsibility for retransmission of Disconnect-Request and CoA-Request packets lies with the Dynamic Authorization Client. If after sending these packets, the Dynamic Authorization Client does not receive a response, it will retransmit.

The Identifier field MUST be changed whenever the content of the Attributes field changes, or whenever a valid reply has been received for a previous request. For retransmissions where the contents are identical, the Identifier MUST remain unchanged.

If the Dynamic Authorization Client is retransmitting a Disconnect-Request or CoA-Request to the same Dynamic Authorization Server as before, and the Attributes haven't

changed, the same Request Authenticator, Identifier and source port MUST be used. If any Attributes have changed, a new Authenticator and Identifier MUST be used.

If the Request to a primary Dynamic Authorization Server fails, a secondary Dynamic Authorization Server must be queried, if available; issues relating to failover algorithms are described in [RFC3539]. Since this represents a new request, a new Request Authenticator and Identifier MUST be used. However, where the Dynamic Authorization Client is sending directly to the NAS, failover typically does not make sense, since CoA-Request or Disconnect-Request packets need to be delivered to the NAS where the session resides.

Length

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 packets between the Dynamic Authorization Client and the Dynamic Authorization Server.

Request Authenticator

In Request packets, the Authenticator value is a 16 octet MD5 [RFC1321] checksum, called the Request Authenticator. The Request Authenticator is calculated the same way as for an Accounting-Request, specified in [RFC2866].

Note that the Request Authenticator of a CoA-Request or Disconnect-Request cannot be computed the same way as the Request Authenticator of a RADIUS Access-Request, because there is no User-Password Attribute in a CoA-Request or Disconnect-Request.

Response Authenticator

The Authenticator field in a Response packet (e.g. Disconnect-ACK, Disconnect-NAK, CoA-ACK, or CoA-NAK) is called the

Response Authenticator, and contains a one-way MD5 hash calculated over a stream of octets consisting of the Code, Identifier, Length, the Request Authenticator field from the packet being replied to, and the response Attributes if any, followed by the shared secret. The resulting 16 octet MD5 hash value is stored in the Authenticator field of the Response packet.

Administrative note: As noted in [RFC2865] Section 3, the secret (password shared between the Dynamic Authorization Client and the Dynamic Authorization Server) SHOULD be at least as large and unguessable as a well-chosen password. The Dynamic Authorization Server MUST use the source IP address of the RADIUS UDP packet to decide which shared secret to use, so that requests can be proxied.

Attributes

In Disconnect and CoA-Request packets, all attributes are treated as mandatory. If one or more authorization changes specified in a CoA-Request cannot be carried out, the NAS MUST send a CoA-NAK. A NAS MUST respond to a CoA-Request containing one or more unsupported Attributes or Attribute values with a CoA-NAK; an Error-Cause Attribute with value 401 (Unsupported Attribute) or 407 (Invalid Attribute Value) MAY be included. A NAS MUST respond to a Disconnect-Request containing one or more unsupported Attributes or Attribute values with a Disconnect-NAK; an Error-Cause Attribute with value 401 (Unsupported Attribute) or 407 (Invalid Attribute Value) MAY be included.

State changes resulting from a CoA-Request MUST be atomic: if the CoA-Request is successful, the Dynamic Authorization Server MUST send a CoA-ACK in reply, and all requested authorization changes MUST be made. If the CoA-Request is unsuccessful, a CoA-NAK MUST be sent in reply, and the requested authorization changes MUST NOT be made. Similarly, a state change MUST NOT occur as a result of an unsuccessful Disconnect-Request; the Dynamic Authorization Server MUST send a Disconnect-NAK in reply.

Within this specification attributes can be used for identification, authorization or other purposes. RADIUS Attribute specifications created after publication of this document SHOULD state whether an attribute can be included in CoA or Disconnect messages and if so, which messages it can be included in and whether it serves as an identification or authorization attribute.

Even if a NAS implements an attribute for use with RADIUS authentication and accounting, it is possible that it will not

support inclusion of that attribute within CoA-Request and Disconnect-Request packets, given the difference in attribute semantics. This is true even for attributes specified as allowable within Access-Accept packets (such as those defined within [RFC2865], [RFC2868], [RFC2869], [RFC3162], [RFC3579], [RFC4372], [RFC4675], [RFC4818] and [RFC4849]).

3. Attributes

In Disconnect-Request and CoA-Request packets, certain attributes are used to uniquely identify the NAS as well as a user session on the NAS. All NAS identification attributes included in a Request packet MUST match in order for a Disconnect-Request or CoA-Request to be successful; otherwise a Disconnect-NAK or CoA-NAK SHOULD be sent. For session identification attributes, the User-Name and Acct-Session-Id Attributes, if included, MUST match in order for a Disconnect-Request or CoA-Request to be successful; other session identification attributes SHOULD match. Where a mismatch of session identification attributes is detected, a Disconnect-NAK or CoA-NAK SHOULD be sent.

The ability to use NAS or session identification attributes to map to unique/multiple sessions is beyond the scope of this document. Identification attributes include NAS and session identification attributes, as described below.

NAS identification attributes

Attribute	#	Reference	Description
NAS-IP-Address	4	[RFC2865]	The IPv4 address of the NAS.
NAS-Identifier	32	[RFC2865]	String identifying the NAS.
NAS-IPv6-Address	95	[RFC3162]	The IPv6 address of the NAS.

Session identification attributes

Attribute	#	Reference	Description
User-Name	1	[RFC2865]	The name of the user associated with the session.
NAS-Port	5	[RFC2865]	The port on which the session is terminated.
Called-Station-Id	30	[RFC2865]	The link address to which the session is connected.
Calling-Station-Id	31	[RFC2865]	The link address from which the session is connected.
Acct-Session-Id	44	[RFC2866]	The identifier uniquely identifying the session

			on the NAS.
Acct-Multi-Session-Id	50	[RFC2866]	The identifier uniquely identifying related sessions.
NAS-Port-Id	87	[RFC2869]	String identifying the port where the session is.
Chargeable-User-Identity	89	[RFC4372]	The CUI associated with the session. Needed where a privacy NAI is used, because the User-Name may not be unique (e.g. "anonymous").

To address security concerns described in Section 6.1, either the User-Name or Chargeable-User-Identity attribute SHOULD be present in Disconnect-Request and CoA-Request packets.

Where a Diameter client utilizes the same Session-Id for both authorization and accounting, inclusion of an Acct-Session-Id Attribute in a Disconnect-Request or CoA-Request can assist with Diameter/RADIUS translation, since Diameter RAR and ASR commands include a Session-Id AVP. An Acct-Session-Id Attribute SHOULD be included in Disconnect-Request and CoA-Request packets.

A NAS implementing this specification SHOULD send an Acct-Session-Id or Acct-Multi-Session-Id Attribute within an Access-Request. Where an Acct-Session-Id or Acct-Multi-Session-Id Attribute is not included within an Access-Request, the Dynamic Authorizatoin Client will not know the Acct-Session-Id or Acct-Multi-Session-Id of the session it is attempting to target, unless it also has access to the accounting data for that session.

Where an Acct-Session-Id or Acct-Multi-Session-Id Attribute is not present in a CoA-Request or Disconnect-Request, it is possible that the the User-Name or Chargeable-User-Identity attributes will not be sufficient to uniquely identify the session (e.g. if the same user has multiple sessions on the NAS, or if the privacy NAI is used). In this case, session identification MAY be performed by using one or more of the Called-Station-Id, Calling-Station-Id, NAS-Port and NAS-Port-Id attributes.

To address security concerns described in Section 6.2, one or more of the NAS-IP-Address or NAS-IPv6-Address Attributes SHOULD be present in CoA-Request and Disconnect-Request packets; the NAS-Identifier Attribute MAY be present.

A Disconnect-Request MUST contain only NAS and session identification attributes. If other attributes are included in a Disconnect-Request, implementations MUST send a Disconnect-NAK; an Error-Cause Attribute with value "Unsupported Attribute" MAY be included.

3.1. Proxy State

If there are any Proxy-State attributes in a Disconnect-Request or CoA-Request received from the Dynamic Authorization Client, the Dynamic Authorization Server MUST include those Proxy-State attributes in its response to the Dynamic Authorization Client.

A forwarding proxy or NAS MUST NOT modify existing Proxy-State, State, or Class attributes present in the packet. The forwarding proxy or NAS MUST treat any Proxy-State attributes already in the packet as opaque data. Its operation MUST NOT depend on the content of Proxy-State attributes added by previous proxies. The forwarding proxy MUST NOT modify any other Proxy-State attributes that were in the packet; it may choose not to forward them, but it MUST NOT change their contents. If the forwarding proxy omits the Proxy-State attributes in the request, it MUST attach them to the response before sending it.

When the proxy forwards a Disconnect or CoA-Request, it MAY add a Proxy-State Attribute, but it MUST NOT add more than one. If a Proxy-State Attribute is added to a packet when forwarding the packet, the Proxy-State Attribute MUST be added after any existing Proxy-State attributes. The forwarding proxy MUST NOT change the order of any attributes of the same type, including Proxy-State. Other attributes can be placed before, after or even between the Proxy-State attributes.

When the proxy receives a response to a CoA-Request or Disconnect-Request, it MUST remove its own Proxy-State (the last Proxy- State in the packet) Attribute before forwarding the response. Since Disconnect and CoA responses are authenticated on the entire packet contents, the stripping of the Proxy-State Attribute invalidates the integrity check - so the proxy needs to recompute it.

3.2. Authorize Only

Support for a CoA-Request including a Service-Type Attribute with value "Authorize Only" is OPTIONAL on the NAS and Dynamic Authorization Client. A Service-Type Attribute MUST NOT be included within a Disconnect-Request.

A NAS MUST respond to a CoA-Request including a Service-Type Attribute with value "Authorize Only" with a CoA-NAK; a CoA-ACK MUST NOT be sent. If the NAS does not support a Service-Type value of "Authorize Only" then it MUST respond with a CoA-NAK; an Error-Cause value of 405 (Unsupported Service) SHOULD be included.

A CoA-Request containing a Service-Type Attribute with value

"Authorize Only" MUST in addition contain only NAS or session identification attributes, as well as a State Attribute. If other attributes are included in such a CoA-Request, a CoA-NAK MUST be sent; an Error-Cause Attribute with value 401 (Unsupported Attribute) SHOULD be included.

If a CoA-Request packet including a Service-Type value of "Authorize Only" is successfully processed, the NAS MUST respond with a CoA-NAK containing a Service-Type Attribute with value "Authorize Only", and an Error-Cause Attribute with value 507 (Request Initiated). The NAS then MUST send an Access-Request to the RADIUS server including a Service-Type Attribute with value "Authorize Only", along with a State Attribute. This Access-Request SHOULD contain the NAS identification attributes from the CoA-Request, as well as the session identification attributes from the CoA-Request permitted in an Access-Request. As noted in [RFC2869] Section 5.19, a Message-Authenticator attribute SHOULD be included in an Access-Request that does not contain a User-Password, CHAP-Password, ARAP-Password or EAP-Message Attribute. The RADIUS server then will respond to the Access-Request with an Access-Accept to (re-)authorize the session or an Access-Reject to refuse to (re-)authorize it.

3.3. State

The State Attribute is available to be sent by the Dynamic Authorization Client to the NAS in a CoA-Request packet and MUST be sent unmodified from the NAS to the Dynamic Authorization Client in a subsequent ACK or NAK packet.

[RFC2865] Section 5.44 states:

> An Access-Request MUST contain either a User-Password or a CHAP-Password or State. An Access-Request MUST NOT contain both a User-Password and a CHAP-Password. If future extensions allow other kinds of authentication information to be conveyed, the attribute for that can be used in an Access-Request instead of User-Password or CHAP-Password.

In order to satisfy the requirements of [RFC2865] Section 5.44, an Access-Request with Service-Type="Authorize-Only" MUST contain a State attribute.

In order to provide a State attribute to the NAS, a Dynamic Authorization Client sending a CoA-Request with a Service-Type value of "Authorize-Only" MUST include a State Attribute, and the NAS MUST send the State Attribute unmodified to the RADIUS server in the resulting Access-Request, if any. A NAS receiving a CoA-Request containing a Service-Type value of "Authorize-Only" but lacking a

State attribute MUST send a CoA-NAK and SHOULD include an Error-Cause attribute with value 402 (Missing Attribute).

The State Attribute is also available to be sent by the Dynamic Authorization Client to the NAS in a CoA-Request that also includes a Termination-Action Attribute with the value of RADIUS-Request. If the NAS performs the Termination-Action by sending a new Access-Request upon termination of the current session, it MUST include the State Attribute unchanged in that Access-Request. In either usage, the Dynamic Authorization Server MUST NOT interpret the Attribute locally. A CoA-Request packet MUST have only zero or one State Attribute. Usage of the State Attribute is implementation dependent.

3.4. Message-Authenticator

The Message-Authenticator Attribute MAY be used to authenticate and integrity-protect CoA-Request, CoA-ACK, CoA-NAK, Disconnect-Request, Disconnect-ACK and Disconnect-NAK packets order to prevent spoofing.

A Dynamic Authorization Server receiving a CoA-Request or Disconnect-Request with a Message-Authenticator Attribute present MUST calculate the correct value of the Message-Authenticator and silently discard the packet if it does not match the value sent. A Dynamic Authorization Client receiving a CoA/Disconnect-ACK or CoA/Disconnect-NAK with a Message-Authenticator Attribute present MUST calculate the correct value of the Message-Authenticator and silently discard the packet if it does not match the value sent.

When a Message-Authenticator Attribute is included within a CoA-Request or Disconnect-Request, it is calculated as follows:

Message-Authenticator = HMAC-MD5 (Type, Identifier, Length, Request Authenticator, Attributes)

When the HMAC-MD5 message integrity check is calculated the Request Authenticator field and Message-Authenticator Attribute should be considered to be sixteen octets of zero. The Message-Authenticator Attribute is calculated and inserted in the packet before the Request Authenticator is calculated.

When a Message-Authenticator Attribute is included within a CoA-ACK, CoA-NAK, Disconnect-ACK or Disconnect-NAK, it is calculated as follows:

Message-Authenticator = HMAC-MD5 (Type, Identifier, Length, Request Authenticator, Attributes)

When the HMAC-MD5 message integrity check is calculated the

Message-Authenticator Attribute should be considered to be sixteen octets of zero. The Request Authenticator is taken from the corresponding CoA/Disconnect-Request. The Message-Authenticator is calculated and inserted in the packet before the Response Authenticator is calculated.

3.5. Error-Cause

Description

It is possible that a Dynamic Authorization Server cannot honor Disconnect-Request or CoA-Request packets for some reason. The Error-Cause Attribute provides more detail on the cause of the problem. It MAY be included within CoA-NAK and Disconnect-NAK packets.

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

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|     Type      |    Length     |             Value
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
           Value (cont)         |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Type

101 for Error-Cause

Length

6

Value

The Value field is four octets, containing an integer specifying the cause of the error. Values 0-199 and 300-399 are reserved. Values 200-299 represent successful completion, so that these values may only be sent within CoA-ACK or Disconnect-ACK packets and MUST NOT be sent within a CoA-NAK or Disconnect-NAK packet. Values 400-499 represent fatal errors committed by the Dynamic Authorization Client, so that they MAY be sent within CoA-NAK or Disconnect-NAK packets, and MUST NOT be sent within CoA-ACK or Disconnect-ACK packets. Values 500-599 represent fatal errors occurring on a Dynamic Authorization Server, so that they MAY be sent within CoA-NAK and Disconnect-NAK packets, and MUST NOT be

sent within CoA-ACK or Disconnect-ACK packets. Error-Cause values SHOULD be logged by the Dynamic Authorization Client. Error-Code values (expressed in decimal) include:

#	Value
201	Residual Session Context Removed
202	Invalid EAP Packet (Ignored)
401	Unsupported Attribute
402	Missing Attribute
403	NAS Identification Mismatch
404	Invalid Request
405	Unsupported Service
406	Unsupported Extension
407	Invalid Attribute Value
501	Administratively Prohibited
502	Request Not Routable (Proxy)
503	Session Context Not Found
504	Session Context Not Removable
505	Other Proxy Processing Error
506	Resources Unavailable
507	Request Initiated

"Residual Session Context Removed" is sent in response to a Disconnect-Request if the user session is no longer active, but residual session context was found and successfully removed. This value is only sent within a Disconnect-ACK and MUST NOT be sent within a CoA-ACK, Disconnect-NAK or CoA-NAK.

"Invalid EAP Packet (Ignored)" is a non-fatal error that MUST NOT be sent by implementations of this specification.

"Unsupported Attribute" is a fatal error sent if a Request contains an attribute (such as a Vendor-Specific or EAP-Message Attribute) that is not supported.

"Missing Attribute" is a fatal error sent if critical attributes (such as NAS or session identification attributes) are missing from a Request.

"NAS Identification Mismatch" is a fatal error sent if one or more NAS identification attributes (see Section 3) do not match the identity of the NAS receiving the Request.

"Invalid Request" is a fatal error sent if some other aspect of the Request is invalid, such as if one or more attributes (such as EAP- Message Attribute(s)) are not formatted properly.

"Unsupported Service" is a fatal error sent if a Service-Type Attribute included with the Request is sent with an invalid or unsupported value. This error cannot be sent in response to a Disconnect-Request.

"Unsupported Extension" is a fatal error sent due to lack of support for an extension such as Disconnect and/or CoA packets. This will typically be sent by a proxy receiving an ICMP port unreachable message after attempting to forward a CoA or Disconnect-Request to the NAS.

"Invalid Attribute Value" is a fatal error sent if a CoA-Request or Disconnect-Request contains an attribute with an unsupported value.

"Administratively Prohibited" is a fatal error sent if the NAS is configured to prohibit honoring of CoA-Request or Disconnect-Request packets for the specified session.

"Request Not Routable" is a fatal error which MAY be sent by a proxy and MUST NOT be sent by a NAS. It indicates that the proxy was unable to determine how to route a CoA or Disconnect-Request to the NAS. For example, this can occur if the required entries are not present in the proxy's realm routing table.

"Session Context Not Found" is a fatal error sent if the session context identified in the CoA-Request or Disconnect-Request does not exist on the NAS.

"Session Context Not Removable" is a fatal error sent in response to a Disconnect-Request if the NAS was able to locate the session context, but could not remove it for some reason. It MUST NOT be sent within a CoA-ACK, CoA-NAK or Disconnect-ACK, only within a Disconnect-NAK.

"Other Proxy Processing Error" is a fatal error sent in response to a CoA or Disconnect-Request that could not be processed by a proxy, for reasons other than routing.

"Resources Unavailable" is a fatal error sent when a CoA or Disconnect-Request could not be honored due to lack of available NAS resources (memory, non- volatile storage, etc.).

"Request Initiated" is a fatal error sent by a NAS in response to a CoA-Request including a Service-Type Attribute with a value of "Authorize Only". It indicates that the CoA-Request has not been honored, but that the NAS is sending a RADIUS Access-Request including a Service-Type Attribute with value "Authorize Only" to

the RADIUS server.

3.6. Table of Attributes

The following table provides a guide to which attributes may be found in which packets, and in what quantity.

Change-of-Authorization Messages

Request	ACK	NAK	#	Attribute
0-1	0	0	1	User-Name [Note 1]
0-1	0	0	4	NAS-IP-Address [Note 1]
0-1	0	0	5	NAS-Port [Note 1]
0-1	0	0-1	6	Service-Type
0-1	0	0	7	Framed-Protocol [Note 3]
0-1	0	0	8	Framed-IP-Address [Note 6]
0-1	0	0	9	Framed-IP-Netmask [Note 6]
0-1	0	0	10	Framed-Routing [Note 3]
0+	0	0	11	Filter-ID [Note 3]
0-1	0	0	12	Framed-MTU [Note 3]
0+	0	0	13	Framed-Compression [Note 3]
0+	0	0	14	Login-IP-Host [Note 3]
0-1	0	0	15	Login-Service [Note 3]
0-1	0	0	16	Login-TCP-Port [Note 3]
0+	0	0	18	Reply-Message [Note 2]
0-1	0	0	19	Callback-Number [Note 3]
0-1	0	0	20	Callback-Id [Note 3]
0+	0	0	22	Framed-Route [Note 3]
0-1	0	0	23	Framed-IPX-Network [Note 6]
0-1	0-1	0-1	24	State
0+	0	0	25	Class [Note 3]
0+	0	0	26	Vendor-Specific [Note 3]
0-1	0	0	27	Session-Timeout [Note 3]
0-1	0	0	28	Idle-Timeout [Note 3]
0-1	0	0	29	Termination-Action [Note 3]
0-1	0	0	30	Called-Station-Id [Note 1]
0-1	0	0	31	Calling-Station-Id [Note 1]
0-1	0	0	32	NAS-Identifier [Note 1]
0+	0+	0+	33	Proxy-State
0-1	0	0	34	Login-LAT-Service [Note 3]
0-1	0	0	35	Login-LAT-Node [Note 3]
0-1	0	0	36	Login-LAT-Group [Note 3]
0-1	0	0	37	Framed-AppleTalk-Link [Note 3]
0+	0	0	38	Framed-AppleTalk-Network [Note 3]
0-1	0	0	39	Framed-AppleTalk-Zone [Note 3]
0-1	0	0	44	Acct-Session-Id [Note 1]
0-1	0	0	50	Acct-Multi-Session-Id [Note 1]
Request	ACK	NAK	#	Attribute

Request	ACK	NAK	#	Attribute
0-1	0-1	0-1	55	Event-Timestamp
0+	0	0	56	Egress-VLANID [Note 3]
0-1	0	0	57	Ingress-Filters [Note 3]
0+	0	0	58	Egress-VLAN-Name [Note 3]
0-1	0	0	59	User-Priority-Table [Note 3]
0-1	0	0	61	NAS-Port-Type [Note 3]
0-1	0	0	62	Port-Limit [Note 3]
0-1	0	0	63	Login-LAT-Port [Note 3]
0+	0	0	64	Tunnel-Type [Note 5]
0+	0	0	65	Tunnel-Medium-Type [Note 5]
0+	0	0	66	Tunnel-Client-Endpoint [Note 5]
0+	0	0	67	Tunnel-Server-Endpoint [Note 5]
0+	0	0	69	Tunnel-Password [Note 5]
0-1	0	0	71	ARAP-Features [Note 3]
0-1	0	0	72	ARAP-Zone-Access [Note 3]
0+	0	0	78	Configuration-Token [Note 3]
0+	0-1	0	79	EAP-Message [Note 2]
0-1	0-1	0-1	80	Message-Authenticator
0+	0	0	81	Tunnel-Private-Group-ID [Note 5]
0+	0	0	82	Tunnel-Assignment-ID [Note 5]
0+	0	0	83	Tunnel-Preference [Note 5]
0-1	0	0	85	Acct-Interim-Interval [Note 3]
0-1	0	0	87	NAS-Port-Id [Note 1]
0-1	0	0	88	Framed-Pool [Note 6]
0-1	0	0	89	Chargeable-User-Identity [Note 1]
0+	0	0	90	Tunnel-Client-Auth-ID [Note 5]
0+	0	0	91	Tunnel-Server-Auth-ID [Note 5]
0-1	0	0	92	NAS-Filter-Rule [Note 3]
0	0	0	94	Originating-Line-Info
0-1	0	0	95	NAS-IPv6-Address [Note 1]
0-1	0	0	96	Framed-Interface-Id [Note 6]
0+	0	0	97	Framed-IPv6-Prefix [Note 6]
0+	0	0	98	Login-IPv6-Host [Note 3]
0+	0	0	99	Framed-IPv6-Route [Note 3]
0-1	0	0	100	Framed-IPv6-Pool [Note 6]
0	0	0+	101	Error-Cause
0+	0	0	123	Delegated-IPv6-Prefix [Note 6]
Request	ACK	NAK	#	Attribute

Disconnect Messages

Request	ACK	NAK	#	Attribute
0-1	0	0	1	User-Name [Note 1]
0-1	0	0	4	NAS-IP-Address [Note 1]
0-1	0	0	5	NAS-Port [Note 1]
0	0	0	6	Service-Type
0	0	0	8	Framed-IP-Address [Note 6]
0+	0	0	18	Reply-Message [Note 2]
0	0	0	24	State
0+	0	0	25	Class [Note 4]
0+	0	0	26	Vendor-Specific
0-1	0	0	30	Called-Station-Id [Note 1]
0-1	0	0	31	Calling-Station-Id [Note 1]
0-1	0	0	32	NAS-Identifier [Note 1]
0+	0+	0+	33	Proxy-State
0-1	0	0	44	Acct-Session-Id [Note 1]
0-1	0-1	0	49	Acct-Terminate-Cause
0-1	0	0	50	Acct-Multi-Session-Id [Note 1]
0-1	0-1	0-1	55	Event-Timestamp
0	0	0	61	NAS-Port-Type
0+	0-1	0	79	EAP-Message [Note 2]
0-1	0-1	0-1	80	Message-Authenticator
0-1	0	0	87	NAS-Port-Id [Note 1]
0-1	0	0	89	Chargeable-User-Identity [Note 1]
0-1	0	0	95	NAS-IPv6-Address [Note 1]
0	0	0	96	Framed-Interface-Id [Note 6]
0	0	0	97	Framed-IPv6-Prefix [Note 6]
0	0	0	100	Framed-IPv6-Pool [Note 6]
0	0	0+	101	Error-Cause
Request	ACK	NAK	#	Attribute

The following table defines the meaning of the above table entries.

0	**This attribute MUST NOT be present in packet.**
0+	Zero or more instances of this attribute MAY be present in packet.
0-1	Zero or one instance of this attribute MAY be present in packet.
1	**Exactly one instance of this attribute MUST be present in packet.**

[Note 1] Where NAS or session identification attributes are included in Disconnect-Request or CoA-Request packets, they are used for identification purposes only. These attributes MUST NOT be used for purposes other than identification (e.g. within CoA-Request packets to request authorization changes).

[Note 2] The Reply-Message Attribute is used to present a displayable message to the user. The message is only displayed as a result of a successful Disconnect-Request or CoA-Request (where a Disconnect-ACK

or CoA-ACK is subsequently sent). Where EAP is used for authentication, an EAP-Message/Notification-Request Attribute is sent instead, and Disconnect-ACK or CoA-ACK packets contain an EAP-Message/Notification-Response Attribute.

[Note 3] When included within a CoA-Request, these attributes represent an authorization change request. When one of these attributes is omitted from a CoA-Request, the NAS assumes that the attribute value is to remain unchanged. Attributes included in a CoA-Request replace all existing value(s) of the same attribute(s).

[Note 4] When included within a successful Disconnect-Request (where a Disconnect-ACK is subsequently sent), the Class Attribute SHOULD be sent unmodified by the NAS to the RADIUS accounting server in the Accounting Stop packet. If the Disconnect-Request is unsuccessful, then the Class Attribute is not processed.

[Note 5] When included within a CoA-Request, these attributes represent an authorization change request. Where tunnel attribute(s) are included within a successful CoA-Request, all existing tunnel attributes are removed and replaced by the new attribute(s).

[Note 6] Where included within a CoA-Request, these attributes represent a renumbering request. Since these attributes are not used for session identification, they MUST NOT be included within a Disconnect-Request. Note that renumbering may not be possible in all situations. For example, in order to change an IP address on receipt of a changed Framed-IP-Address address, IPCP re-negotiation could be required, which is not supported by all PPP implementations.

4. Diameter Considerations

Due to differences in handling change-of-authorization requests in RADIUS and Diameter, it may be difficult or impossible for a Diameter/RADIUS gateway to successfully translate a Diameter Re-Auth-Request (RAR) to a CoA-Request and vice versa. For example, since a CoA-Request only initiates an authorization change but does not initiate re-authentication, a RAR command containing a Re-Auth-Request-Type AVP with value "AUTHORIZE_AUTHENTICATE" cannot be directly translated to a CoA-Request. A Diameter/RADIUS gateway receiving a CoA-Request containing authorization changes will need to translate this into two Diameter exchanges. First, the Diameter/RADIUS gateway will issue a RAR command including a Session-Id AVP and a Re-Auth-Request-Type AVP with value "AUTHORIZE ONLY". Then the Diameter/RADIUS gateway will respond to the ensuing access request with a response including the authorization attributes gleaned from the CoA-Request. For the translation to be possible, the CoA-Request MUST include a Acct-Session-Id Attribute. If the

Diameter client uses the same Session-Id for both authorization and accounting, then the Diameter/RADIUS gateway can copy the contents of the Acct-Session-Id Attribute into the Session-Id AVP; otherwise, it will need to map the Acct-Session-Id value to an equivalent Session-Id for use within a RAR command.

To simplify translation between RADIUS and Diameter, Dynamic Authorization Clients can include a Service-Type Attribute with value "Authorize Only" within a CoA-Request, as described in Section 3.2. A Diameter/RADIUS gateway receiving a CoA-Request containing a Service-Type with value "Authorize Only" translates this to a RAR with Re-Auth-Request-Type AVP with value "AUTHORIZE ONLY". The received RAA is then translated to a CoA-NAK with a Service-Type value of "Authorize Only". If the Result-Code AVP in the RAA has a value in the success category, then an Error-Cause Attribute with value "Request Initiated" is included in the CoA-NAK. If the Result-Code AVP in the RAA has a value indicating a Protocol Error or a Transient or Permanent Failure, then an alternate Error-Cause Attribute is returned as suggested below.

Within Diameter, a server can request that a session be aborted by sending an Abort-Session-Request (ASR), identifying the session to be terminated using Session-ID and User-Name AVPs. The ASR command is translated to a Disconnect-Request containing Acct-Session-Id and User-Name attributes. If the Diameter client utilizes the same Session-Id in both authorization and accounting, then the value of the Session-ID AVP may be placed in the Acct-Session-Id attribute; otherwise the value of the Session-ID AVP will need to be mapped to an appropriate Acct-Session-Id value. For a Disconnect-Request to be translatable to an ASR, an Acct-Session-Id attribute MUST be present. If the Diameter client utilizes the same Session-Id in both authorization and accounting, then the value of the Acct-Session-Id may be placed into the Session-ID AVP within the ASR; otherwise the value of the Acct-Session-Id will need to be mapped to an appropriate Session-ID value.

An Abort-Session-Answer (ASA) command is sent in response to an ASR in order to indicate the disposition of the request. A Diameter/RADIUS gateway receiving a Disconnect-ACK translates this to an ASA command with a Result-Code AVP of "DIAMETER_SUCCESS". A Disconnect-NAK received from the NAS is translated to an ASA command with a Result-Code AVP which depends on the value of the Error-Cause Attribute. Suggested translations between Error-Cause Attribute values and Result-Code AVP values are included below:

#	Error-Cause Attribute Value	Result-Code AVP
201	Residual Session Context Removed	DIAMETER_SUCCESS
202	Invalid EAP Packet (Ignored)	DIAMETER_LIMITED_SUCCESS
401	Unsupported Attribute	DIAMETER_AVP_UNSUPPORTED
402	Missing Attribute	DIAMETER_MISSING_AVP
403	NAS Identification Mismatch	DIAMETER_REALM_NOT_SERVED
404	Invalid Request	DIAMETER_UNABLE_TO_COMPLY
405	Unsupported Service	DIAMETER_COMMAND_UNSUPPORTED
406	Unsupported Extension	DIAMETER_APPLICATION_UNSUPPORTED
407	Invalid Attribute Value	DIAMETER_INVALID_AVP_VALUE
501	Administratively Prohibited	DIAMETER_AUTHORIZATION_REJECTED
502	Request Not Routable (Proxy)	DIAMETER_UNABLE_TO_DELIVER
503	Session Context Not Found	DIAMETER_UNKNOWN_SESSION_ID
504	Session Context Not Removable	DIAMETER_AUTHORIZATION_REJECTED
505	Other Proxy Processing Error	DIAMETER_UNABLE_TO_COMPLY
506	Resources Unavailable	DIAMETER_RESOURCES_EXCEEDED
507	Request Initiated	DIAMETER_SUCCESS

Since both the ASR/ASA and Disconnect-Request/Disconnect-NAK/Disconnect-ACK exchanges involve just a request and response, inclusion of an "Authorize Only" Service-Type within a Disconnect-Request is not needed to assist in Diameter/RADIUS translation, and may make translation more difficult. As a result, as noted in Section 3.2, the Service-Type Attribute MUST NOT be used within a Disconnect-Request.

5. IANA Considerations

This document uses the RADIUS [RFC2865] namespace, see <http://www.iana.org/assignments/radius-types>. In addition to the allocations already made in [RFC3575] and [RFC3576], this specification requests allocation of an additional value of the Error-Cause Attribute (101):

#	Value
407	Invalid Attribute Value

6. Security Considerations

6.1. Authorization Issues

Where a NAS is shared by multiple providers, it is undesirable for one provider to be able to send Disconnect-Request or CoA-Requests affecting the sessions of another provider.

A Dynamic Authorization Server MUST silently discard Disconnect-Request or CoA-Request packets from untrusted sources. In situations where the Dynamic Authorization Client is co-resident with a RADIUS authentication or accounting server, a proxy MAY perform a "reverse path forwarding" (RPF) check to verify that a Disconnect-Request or CoA-Request originates from an authorized Dynamic Authorization Client. In addition, it SHOULD be possible to explicitly authorize additional sources of Disconnect-Request or CoA-Request packets relating to certain classes of sessions. For example, a particular source can be explicitly authorized to send CoA-Request packets relating to users within a set of realms.

To perform the RPF check, the Dynamic Authorization Server uses the session identification attributes included in Disconnect-Request or CoA-Request packets, in order to determine the RADIUS server(s) to which an equivalent Access-Request could be routed. If the source address of the Disconnect-Request or CoA-Request is within this set, then the CoA-Request or Disconnect-Request is forwarded; otherwise it MUST be silently discarded.

Typically the Dynamic Authorization Server will extract the realm from the Network Access Identifier [RFC4282] included within the User-Name or Chargeble-User-Identity Attribute, and determine the corresponding RADIUS servers in the realm routing tables. If the Dynamic Authorization Server maintains long-term session state, it MAY perform the authorization check based on the session identification attributes in the CoA-Request. The session identification attributes can be used to tie a session to a particular proxy or set of proxies, as with the NAI realm.

Where no proxy is present, the RPF check can only be performed by the NAS if it maintains its own a realm routing table. If the NAS does not maintain a realm routing table (e.g. it selects forwarding proxies based on primary/secondary configuration and/or liveness checks), then an RPF check cannot be performed.

Since authorization to send a Disconnect-Request or CoA-Request is determined based on the source address and the corresponding shared secret, the Dynamic Authorization Server SHOULD configure a different shared secret for each Dynamic Authorization Client.

6.2. Impersonation

[RFC2865] Section 3 states:

> 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 RADIUS Access-Requests are forwarded by a proxy, the NAS-IP-Address or NAS-IPv6-Address Attributes will typically not match the source address observed by the RADIUS server. Since the NAS-Identifier Attribute need not contain an FQDN, this Attribute may not be resolvable to the source address observed by the RADIUS server, even when no proxy is present.

As a result, the authenticity check performed by a RADIUS server or proxy does not verify the correctness of NAS identification attributes. This makes it possible for a rogue NAS to forge NAS-IP-Address, NAS-IPv6-Address or NAS-Identifier Attributes within a RADIUS Access-Request in order to impersonate another NAS. It is also possible for a rogue NAS to forge attributes such as the Called-Station-Id, Calling-Station-Id, or Originating-Line-Info [RFC4005]. This could fool the Dynamic Authorization Client into sending CoA-Request or Disconnect-Request packets containing forged session identification attributes to a NAS targeted by an attacker.

To address these vulnerabilities RADIUS proxies one hop from the NAS SHOULD check whether NAS identification attributes (see Section 3) match the packet source address. Where one or more attributes do not match, Access-Request packets SHOULD be silently discarded.

Such a check may not always be possible. Since the NAS-Identifier Attribute need not correspond to an FQDN, it may not be resolvable to an IP address to be matched against the source address. Also, where a NAT exists between the RADIUS client and proxy, checking the NAS-IP-Address or NAS-IPv6-Address Attributes may not be feasible.

6.3. IPsec Usage Guidelines

In addition to security vulnerabilities unique to Disconnect or CoA packets, the protocol exchanges described in this document are susceptible to the same vulnerabilities as RADIUS [RFC2865]. It is RECOMMENDED that IPsec be employed to afford better security.

Implementations of this specification SHOULD support IPsec [RFC4301] along with IKEv1 [RFC2409] for key management. IPsec ESP [RFC4303] with non-null transform SHOULD be supported, and IPsec ESP with a non-null encryption transform and authentication support SHOULD be

used to provide per-packet confidentiality, authentication, integrity and replay protection. IKE SHOULD be used for key management.

Within RADIUS [RFC2865], a shared secret is used for hiding of Attributes such as User-Password, as well as in computation of the Response Authenticator. In RADIUS accounting [RFC2866], the shared secret is used in computation of both the Request Authenticator and the Response Authenticator.

Since in RADIUS a shared secret is used to provide confidentiality as well as integrity protection and authentication, only use of IPsec ESP with a non-null transform can provide security services sufficient to substitute for RADIUS application-layer security. Therefore, where IPsec AH or ESP null is used, it will typically still be necessary to configure a RADIUS shared secret.

Where RADIUS is run over IPsec ESP with a non-null transform, the secret shared between the Dynamic Authorization Server and the Dynamic Authorization Client MAY NOT be configured. In this case, a shared secret of zero length MUST be assumed. However, a Dynamic Authorization Client that cannot know whether incoming traffic is IPsec-protected MUST be configured with a non-null RADIUS shared secret.

When IPsec ESP is used with RADIUS, per-packet authentication, integrity and replay protection MUST be used. 3DES-CBC MUST be supported as an encryption transform and AES-CBC SHOULD be supported. AES-CBC SHOULD be offered as a preferred encryption transform if supported. HMAC-SHA1-96 MUST be supported as an authentication transform. DES-CBC SHOULD NOT be used as the encryption transform.

A typical IPsec policy for an IPsec-capable RADIUS client is "Initiate IPsec, from me to any destination port UDP 1812". This IPsec policy causes an IPsec SA to be set up by the RADIUS client prior to sending a RADIUS Access-Request to a RADIUS server. If some RADIUS servers contacted by the RADIUS client do not support IPsec, then a more granular policy will be required: "Initiate IPsec, from me to IPsec-Capable-RADIUS-Server, destination port UDP 1812."

For a Dynamic Authorization Server implementing this specification the policy would be "Accept IPsec, from any to me, destination port UDP 3799". This causes the Dynamic Authorization Server to accept (but not require) use of IPsec. It may not be appropriate to require IPsec for all Dynamic Authorization Clients connecting to an IPsec-enabled Dynamic Authorization Server, since some Dynamic Authorization Clients may not support IPsec.

For an IPsec-capable RADIUS server, a typical IPsec policy is "Accept

IPsec, from any to me, destination port 1812". This causes the RADIUS server to accept (but not require) use of IPsec. It may not be appropriate to require IPsec for all RADIUS clients connecting to an IPsec-enabled RADIUS server, since some RADIUS clients may not support IPsec.

For Dynamic Authorization Clients implementing this specification, the policy would be "Initiate IPsec, from me to any, destination port UDP 3799". This causes the Dynamic Authorization Client to initiate IPsec when sending Dynamic Authorization traffic to any Dynamic Authorization Server. If some Dynamic Authorization Servers contacted by the Dynamic Authorization Client do not support IPsec, then a more granular policy will be required, such as "Initiate IPsec, from me to IPsec-capable-Dynamic-Authorization-Server, destination port UDP 3799".

Where IPsec is used for security, and no RADIUS shared secret is configured, it is important that the Dynamic Authorization Server and Dynamic Authorization Client perform an authorization check. Before enabling a host to act as a Dynamic Authorization Server, the Dynamic Authorization Client SHOULD check whether the host is authorized to act in that role. Similarly, before enabling a host to act as a Dynamic Authorization Client, the Dynamic Authorization Server SHOULD check whether the host is authorized for that role.

Dynamic Authorization Clients can be configured with the IP addresses (for IKEv1 Aggressive Mode with pre-shared keys) or FQDNs (for certificate authentication) of Dynamic Authorization Servers. Alternatively, if a separate Certification Authority (CA) exists for Dynamic Authorization Servers, then the Dynamic Authorization Client can configure this CA as a trust anchor [RFC3280] for use with IKEv1.

Similarly, Dynamic Authorization Servers can be configured with the IP addresses (for IKEv1 Aggressive Mode with pre-shared keys) or FQDNs (for certificate authentication) of Dynamic Authorization Clients. Alternatively, if a separate CA exists for Dynamic Authorization Clients, then the Dynamic Authorization Server can configure this CA as a trust anchor for use with IKEv1.

Since unlike SSL/TLS, IKEv1 does not permit certificate policies to be set on a per-port basis, certificate policies need to apply to all uses of IKEv1 on Dynamic Authorization Servers and Dynamic Authorization Clients. In a deployment supporting only certificate authentication, a management station initiating an IPsec-protected telnet session to the Dynamic Authorization Client would need to obtain a certificate chaining to the Dynamic Authorization Server CA. Issuing such a certificate might not be appropriate if the management station was not authorized as a Dynamic Authorization Server.

Where Dynamic Authorization Servers obtain their IP address dynamically (such as an Access Point supporting DHCP), IKEv1 Main Mode with pre-shared keys [RFC2409] SHOULD NOT be used, since this requires use of a group pre-shared key; instead, Aggressive Mode SHOULD be used. Where Dynamic Authorization Server addresses are statically assigned either IKEv1 Aggressive Mode or Main Mode MAY be used. With certificate authentication, IKEv1 Main Mode SHOULD be used.

Care needs to be taken with IKEv1 Phase 1 Identity Payload selection in order to enable mapping of identities to pre-shared keys even with Aggressive Mode. Where the ID_IPV4_ADDR or ID_IPV6_ADDR Identity Payloads are used and addresses are dynamically assigned, mapping of identities to keys is not possible, so that group pre-shared keys are still a practical necessity. As a result, the ID_FQDN identity payload SHOULD be employed in situations where Aggressive mode is utilized along with pre-shared keys and IP addresses are dynamically assigned. This approach also has other advantages, since it allows the Dynamic Authorization Client and Dynamic Authorization Server to configure themselves based on the fully qualified domain name of their peers.

Note that with IPsec, security services are negotiated at the granularity of an IPsec SA, so that exchanges requiring a set of security services different from those negotiated with existing IPsec SAs will need to negotiate a new IPsec SA. Separate IPsec SAs are also advisable where quality of service considerations dictate different handling RADIUS conversations. Attempting to apply different quality of service to connections handled by the same IPsec SA can result in reordering, and falling outside the replay window. For a discussion of the issues, see [RFC2983].

6.4. Replay Protection

Where IPsec replay protection is not used, an Event-Timestamp (55) [RFC2869] Attribute SHOULD be included within CoA-Request and Disconnect-Request packets, and MAY be included within CoA-ACK, CoA-NAK, Disconnect-ACK and Disconnect-NAK packets.

When the Event-Timestamp attribute is present, both the Dynamic Authorization Server and the Dynamic Authorization Client MUST check that the Event-Timestamp Attribute is current within an acceptable time window. If the Event-Timestamp Attribute is not current, then the packet MUST be silently discarded. This implies the need for loose time synchronization within the network, which can be achieved by a variety of means, including SNTP, as described in [RFC4330]. Implementations SHOULD be configurable to discard CoA-Request or Disconnect-Request packets not containing an Event-Timestamp

attribute.

If the Event-Timestamp Attribute is included, it represents the time at which the original packet was sent, and therefore it SHOULD NOT be updated when the packet is retransmitted. If the Event-Timestamp attribute is not updated, this implies that the Identifier is not changed in retransmitted packets. As a result, the ability to detect replay within the time window is dependent on support for duplicate detection within that same window. As noted in Section 2.3, duplicate detection is REQUIRED for Dynamic Authorization Servers implementing this specification.

The time window used for duplicate detection MUST be the same as the window used to detect stale Event-Timestamp Attributes. Since the RADIUS Identifier cannot be repeated within the selected time window, no more than 256 Requests can be accepted within the time window. As a result, the chosen time window will depend on the expected maximum volume of CoA/Disconnect-Requests, so that unnecessary discards can be avoided. A default time window of 300 seconds should be adequate in many circumstances.

7. Example Traces

Disconnect Request with User-Name:

```
 0: xxxx xxxx xxxx xxxx xxxx 2801 001c 1b23    .B.....$.-(....#
16: 624c 3543 ceba 55f1 be55 a714 ca5e 0108    bL5C..U..U...^..
32: 6d63 6869 6261
```

Disconnect Request with Acct-Session-ID:

```
 0: xxxx xxxx xxxx xxxx xxxx 2801 001e ad0d    .B..... ~.(.....
16: 8e53 55b6 bd02 a0cb ace6 4e38 77bd 2c0a    .SU.......N8w.,.
32: 3930 3233 3435 3637                        90234567
```

Disconnect Request with Framed-IP-Address:

```
 0: xxxx xxxx xxxx xxxx xxxx 2801 001a 0bda    .B....."2.(.....
16: 33fe 765b 05f0 fd9c c32a 2f6b 5182 0806    3.v[.....*/kQ...
32: 0a00 0203
```

8. References

8.1. Normative References

[RFC1321] Rivest, R., "The MD5 Message-Digest Algorithm", RFC 1321, April 1992.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", RFC 2119, March 1997.

[RFC2409] Harkins, D. and D. Carrel, "The Internet Key Exchange (IKE)", RFC 2409, November 1998.

[RFC2865] Rigney, C., Rubens, A., Simpson, W. and S. Willens, "Remote Authentication Dial In User Service (RADIUS)", RFC 2865, June 2000.

[RFC2866] Rigney, C., "RADIUS Accounting", RFC 2866, June 2000.

[RFC2869] Rigney, C., Willats W. and P. Calhoun, "RADIUS Extensions", RFC 2869, June 2000.

[RFC3162] Aboba, B., Zorn, G. and D. Mitton, "RADIUS and IPv6", RFC 3162, August 2001.

[RFC3280] Housley, R., Polk, W., Ford, W. and D. Solo, "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile", RFC 3280, April 2002.

[RFC3575] Aboba, B., "IANA Considerations for RADIUS", RFC 3575, July 2003.

[RFC3579] Aboba, B. and P. Calhoun, "RADIUS Support for Extensible Authentication Protocol (EAP)", RFC 3579, September 2003.

[RFC4282] Aboba, B., Beadles, M., Arkko, J. and P. Eronen, "The Network Access Identifier", RFC 4282, December 2005.

[RFC4301] Kent, S. and K. Seo, "Security Architecture for the Internet Protocol", RFC 4301, December 2005.

[RFC4303] Kent, S., "IP Encapsulating Security Payload (ESP)", RFC 4303, December 2005.

8.2. Informative References

[MD5Attack]
Dobbertin, H., "The Status of MD5 After a Recent Attack", CryptoBytes Vol.2 No.2, Summer 1996.

[RFC2868] Zorn, G., Leifer, D., Rubens, A., Shriver, J., Holdrege, M. and I. Goyret, "RADIUS Attributes for Tunnel Protocol Support", RFC 2868, June 2000.

[RFC2983] Black, D. "Differentiated Services and Tunnels", RFC 2983, October 2000.

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

[RFC3588] Calhoun, P., Loughney, J., Guttman, E., Zorn, G. and J. Arkko, "Diameter Base Protocol", RFC 3588, September 2003.

[RFC3576] Chiba, M., Dommety, G., Eklund, M., Mitton, D. and B. Aboba, "Dynamic Authorization Extensions to Remote Authentication Dial In User Service (RADIUS)", RFC 3576, July 2003.

[RFC4005] Calhoun, P., Zorn, G., Spence, D. and D. Mitton, "Diameter Network Access Server Application", RFC 4005, August 2005.

[RFC4330] Mills, D., "Simple Network Time Protocol (SNTP) Version 4 for IPv4, IPv6 and OSI", RFC 4330, January 2006.

[RFC4372] Adrangi, F., Lior, A., Korhonen, J. and J. Loughney, "Chargeable User Identity", RFC 4372, January 2006.

[RFC4675] Congdon, P., Sanchez, M. and B. Aboba, "RADIUS Attributes for Virtual LAN and Priority Support", RFC 4675, September 2006.

[RFC4818] Salowey, J. and R. Droms, "RADIUS Delegated-IPv6-Prefix Attribute", RFC 4818, April 2007.

[RFC4849] Congdon, P., Sanchez, M. and B. Aboba, "RADIUS Filter Rule Attribute", RFC 4849, April 2007.

Acknowledgments

This protocol was first developed and distributed by Ascend Communications. Example code was distributed in their free server kit.

The authors would like to acknowledge valuable suggestions and feedback from Avi Lior, Randy Bush, Steve Bellovin, Glen Zorn, Mark Jones, Claudio Lapidus, Anurag Batta, Kuntal Chowdhury, Tim Moore, Russ Housley, Joe Salowey, Alan DeKok and David Nelson.

Authors' Addresses

Murtaza Chiba
Cisco Systems, Inc.
170 West Tasman Dr.
San Jose CA, 95134

EMail: mchiba@cisco.com
Phone: +1 408 525 7198

Gopal Dommety
Cisco Systems, Inc.
170 West Tasman Dr.
San Jose, CA 95134

EMail: gdommety@cisco.com
Phone: +1 408 525 1404

Mark Eklund
Cisco Systems, Inc.
170 West Tasman Dr.
San Jose, CA 95134

EMail: meklund@cisco.com
Phone: +1 865 671 6255

David Mitton
RSA Security, Inc.
174 Middlesex Turnpike
Bedford, MA 01730

EMail: dmitton@circularnetworks.com

Bernard Aboba
Microsoft Corporation
One Microsoft Way
Redmond, WA 98052

EMail: bernarda@microsoft.com
Phone: +1 425 706 6605
Fax: +1 425 936 7329

Appendix A - Changes from RFC 3576

This Appendix lists the major changes between [RFC3576] and this document. Minor changes, including style, grammar, spelling, and editorial changes are not mentioned here.

o The term "Dynamic Authorization Client" is used instead of RADIUS server where it applies to the originator of CoA and Disconnect-Request packets. Similarly, the term "Dynamic Authorizatin Server" is used instead of NAS where it applies to the receiver of CoA and Disconnect-Request packets. Definitions of these terms have been added (Section 1.3).

o Added requirement for duplicate detection on the Dynamic Authorization Server (Section 2.3).

o Added Chargeable-User-Identity as a session identification attribute. Removed Framed-IP-Address, Framed-IPv6-Prefix, Framed-Interface-Id and NAS-Port-Type attributes as session identification attributes. Recommended inclusion of Acct-Session-Id or Acct-Multi-Session-Id attributes in an Access-Request (Section 3).

o Added recommendation that an Acct-Session-Id or Acct-Mult-Session-Id Attribute be included in an Access-Request (Section 3).

o Added details relating to handling of the Proxy-State Attribute (Section 3.1).

o Added clarification that support for a Service-Type Attribute with value "Authorize Only" is optional on both the NAS and Dynamic Authorization Client (Section 3.2).

o Added requirement for inclusion of the State Attribute in CoA-Request packets including a Service-Type Attribute with a value of "Authorize Only" (Section 3.3).

o Added clarification on the calculation of the Message-Authenticator Attribute (Section 3.4).

o An additional Error-Cause Attribute value (407) is allocated for Invalid Attribute Value (Sections 3.5, 4).

o Updated the CoA-Request Attribute Table to include Filter-Rule, Delegated-IPv6-Prefix, Egress-VLANID, Ingress-Filters, Egress-VLAN-Name and User-Priority attributes (Section 3.6).

o Added the Chargeable-User-Identity Attribute to both the CoA-Request and Disconnect-Request Attribute table (Section 3.6).

- o Added note on the use of the CoA-Request for renumbering (Section 3.6).

- o Use of the Service-Type Attribute within a Disconnect-Request is prohibited (Sections 3.2, 3.6).

- o Added Diameter Considerations (Section 4).

- o Changed the text to indicate that the Event-Timestamp Attribute should not be recalculated on retransmission. The implications for replay and duplicate detection are discussed (Section 6.4).

- o Operation of the RPF check has been clarified. Use of the RPF check is optional rather than recommended by default (Section 6.1).

Full Copyright Statement

Copyright (C) The IETF Trust (2007).

This document is subject to the rights, licenses and restrictions contained in BCP 78, and except as set forth therein, the authors retain all their rights.

This document and the information contained herein are provided on an "AS IS" basis and THE CONTRIBUTOR, THE ORGANIZATION HE/SHE REPRESENTS OR IS SPONSORED BY (IF ANY), THE INTERNET SOCIETY, THE IETF TRUST AND THE INTERNET ENGINEERING TASK FORCE DISCLAIM 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.

Intellectual Property

The IETF takes no position regarding the validity or scope of any Intellectual Property Rights 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; nor does it represent that it has made any independent effort to identify any such rights. Information on the procedures with respect to rights in RFC documents can be found in BCP 78 and BCP 79.

Copies of IPR disclosures made to the IETF Secretariat 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 implementers or users of this specification can be obtained from the IETF on-line IPR repository at http://www.ietf.org/ipr.

The IETF invites any interested party to bring to its attention any copyrights, patents or patent applications, or other proprietary rights that may cover technology that may be required to implement this standard. Please address the information to the IETF at ietf-ipr@ietf.org.

Acknowledgment

Funding for the RFC Editor function is provided by the IETF Administrative Support Activity (IASA).

Open issues

Open issues relating to this specification are tracked on the following web site:

http://www.drizzle.com/~aboba/RADEXT/