Network Working Group	G. Zorn, Ed.
Internet-Draft	Network Zen
Obsoletes: RFC4005	May 23, 2010
(if approved)	
Intended status: Standards Track	
Expires: November 24, 2010	

TOC

Diameter Network Access Server Application
draft-zorn-dime-rfc4005bis-01

Abstract

This document describes the Diameter protocol application used for Authentication, Authorization, and Accounting (AAA) services in the Network Access Server (NAS) environment. When combined with the Diameter Base protocol, Transport Profile, and Extensible Authentication Protocol specifications, this application specification satisfies typical network access services requirements.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.
Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at http://datatracker.ietf.org/drafts/current/.
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.”
This Internet-Draft will expire on November 24, 2010.

Copyright Notice

Table of Contents

---

1. Introduction

TOC

This document describes the Diameter protocol application used for AAA in the Network Access Server (NAS) environment. When combined with the Diameter Base protocol [I-D.ietf-dime-rfc3588bis] (Fajardo, V., Arkko, J., Loughney, J., and G. Zorn, "Diameter Base Protocol," April 2010.),

Transport Profile [RFC3539] (Aboba, B. and J. Wood, "Authentication, Authorization and Accounting (AAA) Transport Profile," June 2003.), and EAP [RFC4072] (Eronen, P., Hiller, T., and G. Zorn, "Diameter Extensible Authentication Protocol (EAP) Application," August 2005.) specifications, this specification satisfies NAS-related requirements defined in [RFC2989] (Aboba, B., Calhoun, P., Glass, S., Hiller, T., McCann, P., Shiino, H., Zorn, G., Dommety, G., C.Perkins, B.Patil, D.Mitton, S.Manning, M.Beadles, P.Walsh, X.Chen, S.Sivalingham, A.Hameed, M.Munson, S.Jacobs, B.Lim, B.Hirschman, R.Hsu, Y.Xu, E.Campell, S.Baba, and E.Jaques, "Criteria for Evaluating AAA Protocols for Network Access," November 2000.) and [RFC3169] (Beadles, M. and D. Mitton, "Criteria for Evaluating Network Access Server Protocols," September 2001.).

First, this document describes the operation of a Diameter NAS application. Then it defines the Diameter message Command-Codes. The following sections list the AVPs used in these messages, grouped by common usage. These are session identification, authentication, authorization, tunneling, and accounting. The authorization AVPs are further broken down by service type.

1.1. Terminology

TOC

Section 1.2 of the base Diameter specification [I-D.ietf-dime-rfc3588bis] (Fajardo, V., Arkko, J., Loughney, J., and G. Zorn, "Diameter Base Protocol," April 2010.) defines most of the terminology used in this document. Additionally, the following terms and acronyms are used in this application:

NAS (Network Access Server) A device that provides an access service for a user to a network. The service may be a network connection or a value-added service such as terminal emulation [RFC2881] (Mitton, D. and M. Beadles, "Network Access Server Requirements Next Generation (NASREQNG) NAS Model," July 2000.).

PPP (Point-to-Point Protocol) A multiprotocol serial datalink. PPP is the primary IP datalink used for dial-in NAS connection service [RFC1661] (Simpson, W., "The Point-to-Point Protocol (PPP)," July 1994.).

CHAP (Challenge Handshake Authentication Protocol) An authentication process used in PPP [RFC1994] (Simpson, W., "PPP Challenge Handshake Authentication Protocol (CHAP)," August 1996.).

PAP (Password Authentication Protocol) A deprecated PPP authentication process, but often used for backward compatibility

[RFC1334] (Lloyd, B. and W. Simpson, “PPP Authentication Protocols,” October 1992.).

SLIP (Serial Line Interface Protocol) A serial datalink that only supports IP. A design prior to PPP.

ARAP (Appletalk Remote Access Protocol) A serial datalink for accessing Appletalk networks [ARAP] (Apple Computer, “Apple Remote Access Protocol (ARAP) Version 2.0 External Reference Specification,” September 1994.).

IPX (Internet Packet Exchange) The network protocol used by NetWare networks [IPX] (Novell, Inc., “NetWare System Technical Interface Overview,” June 1989.).

LAT (Local Area Transport A Digital Equipment Corp. LAN protocol for terminal services [LAT] (Digital Equipment Corp., “Local Area Transport (LAT) Specification V5.0,” June 1989.).

VPN (Virtual Private Network) In this document, this term is used to describe access services that use tunneling methods.

1.2. Requirements Language

TOC

In this document, the key words "MAY", "MUST", "MUST NOT", "OPTIONAL", "RECOMMENDED", "SHOULD", and "SHOULD NOT" are to be interpreted as described in [RFC2119] (Bradner, S., “Key words for use in RFCs to Indicate Requirement Levels,” March 1997.),

---

1.3. Advertising Application Support

TOC

Diameter applications conforming to this specification MUST advertise support by including the value of one (1) in the Auth-Application-Id of the Capabilities-Exchange-Request (CER), AA-Request (AAR), and AA-Answer (AAA) messages. All other messages are defined by RFC 3588 and use the Base application id value.

---

2. NAS Calls, Ports, and Sessions

TOC

The arrival of a new call or service connection at a port of a Network Access Server (NAS) starts a Diameter NAS message exchange. Information

about the call, the identity of the user, and the user's authentication information are packaged into a Diameter AA-Request (AAR) message and sent to a server.

The server processes the information and responds with a Diameter AA-Answer (AAA) message that contains authorization information for the NAS, or a failure code (Result-Code AVP). A value of DIAMETER_MULTI_ROUND_AUTH indicates an additional authentication exchange, and several AAR and AAA messages may be exchanged until the transaction completes.

Depending on the vale of the Auth-Request-Type AVP, the Diameter protocol allows authorization-only requests that contain no authentication information from the client. This capability goes beyond the Call Check capabilities provided by RADIUS (Section 5.6 of (Rigney, C., Willens, S., Rubens, A., and W. Simpson, "Remote Authentication Dial In User Service (RADIUS)," June 2000.) [RFC2865]) in that no access decision is requested. As a result, service cannot be started as a result of a response to an authorization-only request without introducing a significant security vulnerability.

2.1. Diameter Session Establishment

TOC

When the authentication or authorization exchange completes successfully, the NAS application SHOULD start a session context. If the Result-Code of DIAMETER_MULTI_ROUND_AUTH is returned, the exchange continues until a success or error is returned.

If accounting is active, the application MUST also send an Accounting message [I-D.ietf-dime-rfc3588bis] (Fajardo, V., Arkko, J., Loughney, J., and G. Zorn, "Diameter Base Protocol," April 2010.). An Accounting-Record-Type of START_RECORD is sent for a new session. If a session fails to start, the EVENT_RECORD message is sent with the reason for the failure described.

Note that the return of an unsupportable Accounting-Realtime-Required value [I-D.ietf-dime-rfc3588bis] (Fajardo, V., Arkko, J., Loughney, J., and G. Zorn, "Diameter Base Protocol," April 2010.) would result in a failure to establish the session.

2.2. Diameter Session Reauthentication or Reauthorization

TOC

The Diameter Base protocol allows users to be periodically reauthenticated and/or reauthorized. In such instances, the Session-Id

AVP in the AAR message MUST be the same as the one present in the original authentication/authorization message.

A Diameter server informs the NAS of the maximum time allowed before reauthentication or reauthorization via the Authorization-Lifetime AVP [I-D.ietf-dime-rfc3588bis] (Fajardo, V., Arkko, J., Loughney, J., and G. Zorn, "Diameter Base Protocol," April 2010.). A NAS MAY reauthenticate and/or reauthorize before the end, but A NAS MUST reauthenticate and/or reauthorize at the end of the period provided by the Authorization-Lifetime AVP. The failure of a reauthentication exchange will terminate the service.

Furthermore, it is possible for Diameter servers to issue an unsolicited reauthentication and/or reauthorization request (e.g., Re-Auth-Request (RAR) message [I-D.ietf-dime-rfc3588bis] (Fajardo, V., Arkko, J., Loughney, J., and G. Zorn, "Diameter Base Protocol," April 2010.)) to the NAS. Upon receipt of such a message, the NAS MUST respond to the request with a Re-Auth-Answer (RAA) message [I-D.ietf-dime-rfc3588bis] (Fajardo, V., Arkko, J., Loughney, J., and G. Zorn, "Diameter Base Protocol," April 2010.).

If the RAR properly identifies an active session, the NAS will initiate a new local reauthentication or authorization sequence as indicated by the Re-Auth-Request-Type value. This will cause the NAS to send a new AAR message using the existing Session-Id. The server will respond with an AAA message to specify the new service parameters.

If accounting is active, every change of authentication or authorization SHOULD generate an accounting message. If the NAS service is a continuation of the prior user context, then an Accounting-Record-Type of INTERIM_RECORD indicating the new session attributes and cumulative status would be appropriate. If a new user or a significant change in authorization is detected by the NAS, then the service may send two messages of the types STOP_RECORD and START_RECORD. Accounting may change the subsession identifiers (Acct-Session-ID, or Acct-Sub-Session-Id) to indicate such sub-sessions. A service may also use a different Session-Id value for accounting see Section 9.6 of (Fajardo, V., Arkko, J., Loughney, J., and G. Zorn, "Diameter Base Protocol," April 2010.) [I-D.ietf-dime-rfc3588bis].

However, the Diameter Session-ID AVP value used for the initial authorization exchange MUST be used to generate an STR message when the session context is terminated.

TOC

2.3. Diameter Session Termination

When a NAS receives an indication that a user's session is being disconnected by the client (e.g., LCP Terminate is received) or an administrative command, the NAS MUST issue a Session-Termination-Request (STR) [I-D.ietf-dime-rfc3588bis] (Fajardo, V., Arkko, J., Loughney, J., and G. Zorn, "Diameter Base Protocol," April 2010.) to its Diameter Server. This will ensure that any resources maintained on the servers are freed appropriately.

Furthermore, a NAS that receives an Abort-Session-Request (ASR) [I-D.ietf-dime-rfc3588bis] (Fajardo, V., Arkko, J., Loughney, J., and G. Zorn, "Diameter Base Protocol," April 2010.) MUST issue an ASA if the session identified is active and disconnect the PPP (or tunneling) session.

If accounting is active, an Accounting STOP_RECORD message [I-D.ietf-dime-rfc3588bis] (Fajardo, V., Arkko, J., Loughney, J., and G. Zorn, "Diameter Base Protocol," April 2010.) MUST be sent upon termination of the session context.

More information on Diameter Session Termination can be found in Sections 8.4 and 8.5 of (Fajardo, V., Arkko, J., Loughney, J., and G. Zorn, "Diameter Base Protocol," April 2010.) [I-D.ietf-dime-rfc3588bis].

---

3. Diameter NAS Application Messages

TOC

This section defines the Diameter message Command-Code [I-D.ietf-dime-rfc3588bis] (Fajardo, V., Arkko, J., Loughney, J., and G. Zorn, "Diameter Base Protocol," April 2010.) values that MUST be supported by all Diameter implementations conforming to this specification. The Command Codes are as follows:

Command Name	Abbrev.	Code	Reference
AA-Request	AAR	265	Section 3.1 (AA-Request (AAR) Command)
AA-Answer	AAA	265	Section 3.2 (AA-Answer (AAA) Command)
Re-Auth-Request	RAR	258	Section 3.3 (Re-Auth-Request (RAR) Command)

Re-Auth-Answer	RAA	258	Section 3.4 (Re-Auth-Answer (RAA) Command)
Session-Termination-Request	STR	275	Section 3.5 (Session-Termination-Request (STR) Command)
Session-Termination-Answer	STA	275	Section 3.6 (Session-Termination-Answer (STA) Command)
Abort-Session-Request	ASR	274	Section 3.7 (Abort-Session-Request (ASR) Command)
Abort-Session-Answer	ASA	274	Section 3.8 (Abort-Session-Answer (ASA) Command)
Accounting-Request	ACR	271	Section 3.9 (Accounting-Request (ACR) Command)
Accounting-Answer	ACA	271	Section 3.10 (Accounting-Answer (ACA) Command)

3.1. AA-Request (AAR) Command

TOC

The AA-Request (AAR), which is indicated by setting the Command-Code field to 265 and the 'R' bit in the Command Flags field, is used to request authentication and/or authorization for a given NAS user. The type of request is identified through the Auth-Request-Type AVP [I-D.ietf-dime-rfc3588bis] (Fajardo, V., Arkko, J., Loughney, J., and G. Zorn, “Diameter Base Protocol,” April 2010.) The recommended value for most RADIUS interoperability situations is AUTHORIZE_AUTHENTICATE.

If Authentication is requested, the User-Name attribute SHOULD be present, as well as any additional authentication AVPs that would carry the password information. A request for authorization SHOULD only include the information from which the authorization will be performed,

such as the User-Name, Called-Station-Id, or Calling-Station-Id AVPs. All requests SHOULD contain AVPs uniquely identifying the source of the call, such as Origin-Host and NAS-Port. Certain networks MAY use different AVPs for authorization purposes. A request for authorization will include some AVPs defined in Section 4.4 (NAS Authorization AVPs).

It is possible for a single session to be authorized first and then for an authentication request to follow.

This AA-Request message MAY be the result of a multi-round authentication exchange, which occurs when the AA-Answer message is received with the Result-Code AVP set to DIAMETER_MULTI_ROUND_AUTH. A subsequent AAR message SHOULD be sent, with the User-Password AVP that includes the user's response to the prompt, and MUST include any State AVPs that were present in the AAA message.

Message Format

```
   <AA-Request> ::= < Diameter Header: 265, REQ, PXY >
                    < Session-Id >
                    { Auth-Application-Id }
                    { Origin-Host }
                    { Origin-Realm }
                    { Destination-Realm }
                    { Auth-Request-Type }
                    [ Destination-Host ]
                    [ NAS-Identifier ]
                    [ NAS-IP-Address ]
                    [ NAS-IPv6-Address ]
                    [ NAS-Port ]
                    [ NAS-Port-Id ]
                    [ NAS-Port-Type ]
                    [ Origin-AAA-Protocol ]
                    [ Origin-State-Id ]
                    [ Port-Limit ]
                    [ User-Name ]
                    [ User-Password ]
                    [ Service-Type ]
                    [ State ]
                    [ Authorization-Lifetime ]
                    [ Auth-Grace-Period ]
                    [ Auth-Session-State ]
                    [ Callback-Number ]
                    [ Called-Station-Id ]
                    [ Calling-Station-Id ]
                    [ Originating-Line-Info ]
                    [ Connect-Info ]
                    [ CHAP-Auth ]
                    [ CHAP-Challenge ]
                  * [ Framed-Compression ]
                    [ Framed-Interface-Id ]
                    [ Framed-IP-Address ]
                  * [ Framed-IPv6-Prefix ]
                    [ Framed-IP-Netmask ]
                    [ Framed-MTU ]
                    [ Framed-Protocol ]
                    [ ARAP-Password ]
                    [ ARAP-Security ]
                  * [ ARAP-Security-Data ]
                  * [ Login-IP-Host ]
                  * [ Login-IPv6-Host ]
                    [ Login-LAT-Group ]
                    [ Login-LAT-Node ]
                    [ Login-LAT-Port ]
```

```
  [ Login-LAT-Service ]
* [ Tunneling ]
* [ Proxy-Info ]
* [ Route-Record ]
* [ AVP ]
```

3.2. AA-Answer (AAA) Command

TOC

The AA-Answer (AAA) message is indicated by setting the Command-Code field to 265 and clearing the 'R' bit in the Command Flags field. It is sent in response to the AA-Request (AAR) message. If authorization was requested, a successful response will include the authorization AVPs appropriate for the service being provided, as defined in Section 4.4 (NAS Authorization AVPs).

For authentication exchanges requiring more than a single round trip, the server MUST set the Result-Code AVP to DIAMETER_MULTI_ROUND_AUTH. An AAA message with this result code MAY include one Reply-Message or more and MAY include zero or one State AVPs.

If the Reply-Message AVP was present, the network access server SHOULD send the text to the user's client to display to the user, instructing the client to prompt the user for a response. For example, this capability can be achieved in PPP via PAP. If the access client is unable to prompt the user for a new response, it MUST treat the AA-Answer (AAA) with the Reply-Message AVP as an error and deny access.

Message Format

```
   <AA-Answer> ::= < Diameter Header: 265, PXY >
                   < Session-Id >
                   { Auth-Application-Id }
                   { Auth-Request-Type }
                   { Result-Code }
                   { Origin-Host }
                   { Origin-Realm }
                   [ User-Name ]
                   [ Service-Type ]
                  * [ Class ]
                  * [ Configuration-Token ]
                   [ Acct-Interim-Interval ]
                   [ Error-Message ]
                   [ Error-Reporting-Host ]
                  * [ Failed-AVP ]
                   [ Idle-Timeout ]
                   [ Authorization-Lifetime ]
                   [ Auth-Grace-Period ]
                   [ Auth-Session-State ]
                   [ Re-Auth-Request-Type ]
                   [ Multi-Round-Time-Out ]
                   [ Session-Timeout ]
                   [ State ]
                  * [ Reply-Message ]
                   [ Origin-AAA-Protocol ]
                   [ Origin-State-Id ]
                  * [ Filter-Id ]
                   [ Password-Retry ]
                   [ Port-Limit ]
                   [ Prompt ]
                   [ ARAP-Challenge-Response ]
                   [ ARAP-Features ]
                   [ ARAP-Security ]
                  * [ ARAP-Security-Data ]
                   [ ARAP-Zone-Access ]
                   [ Callback-Id ]
                   [ Callback-Number ]
                   [ Framed-Appletalk-Link ]
                  * [ Framed-Appletalk-Network ]
                   [ Framed-Appletalk-Zone ]
                  * [ Framed-Compression ]
                   [ Framed-Interface-Id ]
                   [ Framed-IP-Address ]
                  * [ Framed-IPv6-Prefix ]
                   [ Framed-IPv6-Pool ]
                  * [ Framed-IPv6-Route ]
```

```
  [ Framed-IP-Netmask ]
* [ Framed-Route ]
  [ Framed-Pool ]
  [ Framed-IPX-Network ]
  [ Framed-MTU ]
  [ Framed-Protocol ]
  [ Framed-Routing ]
* [ Login-IP-Host ]
* [ Login-IPv6-Host ]
  [ Login-LAT-Group ]
  [ Login-LAT-Node ]
  [ Login-LAT-Port ]
  [ Login-LAT-Service ]
  [ Login-Service ]
  [ Login-TCP-Port ]
* [ NAS-Filter-Rule ]
* [ QoS-Filter-Rule ]
* [ Tunneling ]
* [ Redirect-Host ]
  [ Redirect-Host-Usage ]
  [ Redirect-Max-Cache-Time ]
* [ Proxy-Info ]
* [ AVP ]
```

3.3. Re-Auth-Request (RAR) Command

TOC

A Diameter server may initiate a re-authentication and/or re-authorization service for a particular session by issuing a Re-Auth-Request (RAR) message [I-D.ietf-dime-rfc3588bis] (Fajardo, V., Arkko, J., Loughney, J., and G. Zorn, “Diameter Base Protocol,” April 2010.).

For example, for pre-paid services, the Diameter server that originally authorized a session may need some confirmation that the user is still using the services.

If a NAS receives an RAR message with Session-Id equal to a currently active session and a Re-Auth-Type that includes authentication, it MUST initiate a re-authentication toward the user, if the service supports this particular feature.

Message Format

```
   <RA-Request>  ::= < Diameter Header: 258, REQ, PXY >
                     < Session-Id >
                     { Origin-Host }
                     { Origin-Realm }
                     { Destination-Realm }
                     { Destination-Host }
                     { Auth-Application-Id }
                     { Re-Auth-Request-Type }
                     [ User-Name ]
                     [ Origin-AAA-Protocol ]
                     [ Origin-State-Id ]
                     [ NAS-Identifier ]
                     [ NAS-IP-Address ]
                     [ NAS-IPv6-Address ]
                     [ NAS-Port ]
                     [ NAS-Port-Id ]
                     [ NAS-Port-Type ]
                     [ Service-Type ]
                     [ Framed-IP-Address ]
                     [ Framed-IPv6-Prefix ]
                     [ Framed-Interface-Id ]
                     [ Called-Station-Id ]
                     [ Calling-Station-Id ]
                     [ Originating-Line-Info ]
                     [ Acct-Session-Id ]
                     [ Acct-Multi-Session-Id ]
                     [ State ]
                   * [ Class ]
                     [ Reply-Message ]
                   * [ Proxy-Info ]
                   * [ Route-Record ]
                   * [ AVP ]
```

3.4. Re-Auth-Answer (RAA) Command

TOC

The Re-Auth-Answer (RAA) message [I-D.ietf-dime-rfc3588bis] (Fajardo, V., Arkko, J., Loughney, J., and G. Zorn, “Diameter Base Protocol,” April 2010.) is sent in response to the RAR. The Result-Code AVP MUST be present and indicates the disposition of the request.

A successful RAA transaction MUST be followed by an AAR message.

Message Format

```
   <RA-Answer>  ::= < Diameter Header: 258, PXY >
                    < Session-Id >
                    { Result-Code }
                    { Origin-Host }
                    { Origin-Realm }
                    [ User-Name ]
                    [ Origin-AAA-Protocol ]
                    [ Origin-State-Id ]
                    [ Error-Message ]
                    [ Error-Reporting-Host ]
                  * [ Failed-AVP ]
                  * [ Redirected-Host ]
                    [ Redirected-Host-Usage ]
                    [ Redirected-Host-Cache-Time ]
                    [ Service-Type ]
                  * [ Configuration-Token ]
                    [ Idle-Timeout ]
                    [ Authorization-Lifetime ]
                    [ Auth-Grace-Period ]
                    [ Re-Auth-Request-Type ]
                    [ State ]
                  * [ Class ]
                  * [ Reply-Message ]
                    [ Prompt ]
                  * [ Proxy-Info ]
                  * [ AVP ]
```

3.5. Session-Termination-Request (STR) Command

TOC

The Session-Termination-Request (STR) message [I-D.ietf-dime-rfc3588bis] (Fajardo, V., Arkko, J., Loughney, J., and G. Zorn, “Diameter Base Protocol,” April 2010.) is sent by the NAS to inform the Diameter Server that an authenticated and/or authorized session is being terminated.

Message Format

```
<ST-Request> ::= < Diameter Header: 275, REQ, PXY >
                 < Session-Id >
                 { Origin-Host }
                 { Origin-Realm }
                 { Destination-Realm }
                 { Auth-Application-Id }
                 { Termination-Cause }
                 [ User-Name ]
                 [ Destination-Host ]
               * [ Class ]
                 [ Origin-AAA-Protocol ]
                 [ Origin-State-Id ]
               * [ Proxy-Info ]
               * [ Route-Record ]
               * [ AVP ]
```

3.6. Session-Termination-Answer (STA) Command

TOC

The Session-Termination-Answer (STA) message [I-D.ietf-dime-rfc3588bis] (Fajardo, V., Arkko, J., Loughney, J., and G. Zorn, “Diameter Base Protocol,” April 2010.) is sent by the Diameter Server to acknowledge the notification that the session has been terminated. The Result-Code AVP MUST be present and MAY contain an indication that an error occurred while the STR was being serviced.

Upon sending or receiving the STA, the Diameter Server MUST release all resources for the session indicated by the Session-Id AVP. Any intermediate server in the Proxy-Chain MAY also release any resources, if necessary.

Message Format

```
   <ST-Answer>  ::= < Diameter Header: 275, PXY >
                    < Session-Id >
                    { Result-Code }
                    { Origin-Host }
                    { Origin-Realm }
                    [ User-Name ]
                  * [ Class ]
                    [ Error-Message ]
                    [ Error-Reporting-Host ]
                  * [ Failed-AVP ]
                    [ Origin-AAA-Protocol ]
                    [ Origin-State-Id ]
                  * [ Redirect-Host ]
                    [ Redirect-Host-Usase ]
                    [ Redirect-Max-Cache-Time ]
                  * [ Proxy-Info ]
                  * [ AVP ]
```

3.7. Abort-Session-Request (ASR) Command

TOC

The Abort-Session-Request (ASR) message [I-D.ietf-dime-rfc3588bis] (Fajardo, V., Arkko, J., Loughney, J., and G. Zorn, “Diameter Base Protocol,” April 2010.) may be sent by any server to the NAS providing session service, to request that the session identified by the Session-Id be stopped.

Message Format

```
   <AS-Request>  ::= < Diameter Header: 274, REQ, PXY >
                     < Session-Id >
                     { Origin-Host }
                     { Origin-Realm }
                     { Destination-Realm }
                     { Destination-Host }
                     { Auth-Application-Id }
                     [ User-Name ]
                     [ Origin-AAA-Protocol ]
                     [ Origin-State-Id ]
                     [ NAS-Identifier ]
                     [ NAS-IP-Address ]
                     [ NAS-IPv6-Address ]
                     [ NAS-Port ]
                     [ NAS-Port-Id ]
                     [ NAS-Port-Type ]
                     [ Service-Type ]
                     [ Framed-IP-Address ]
                     [ Framed-IPv6-Prefix ]
                     [ Framed-Interface-Id ]
                     [ Called-Station-Id ]
                     [ Calling-Station-Id ]
                     [ Originating-Line-Info ]
                     [ Acct-Session-Id ]
                     [ Acct-Multi-Session-Id ]
                     [ State ]
                   * [ Class ]
                   * [ Reply-Message ]
                   * [ Proxy-Info ]
                   * [ Route-Record ]
                   * [ AVP ]
```

3.8. Abort-Session-Answer (ASA) Command

TOC

The ASA message [I-D.ietf-dime-rfc3588bis] (Fajardo, V., Arkko, J., Loughney, J., and G. Zorn, “Diameter Base Protocol,” April 2010.) is sent in response to the ASR. The Result-Code AVP MUST be present and indicates the disposition of the request.

If the session identified by Session-Id in the ASR was successfully terminated, Result-Code is set to DIAMETER_SUCCESS. If the session is not currently active, the Result-Code AVP is set to DIAMETER_UNKNOWN_SESSION_ID. If the access device does not stop the

session for any other reason, the Result-Code AVP is set to DIAMETER_UNABLE_TO_COMPLY.

Message Format

```
   <AS-Answer>  ::= < Diameter Header: 274, PXY >
                    < Session-Id >
                    { Result-Code }
                    { Origin-Host }
                    { Origin-Realm }
                    [ User-Name ]
                    [ Origin-AAA-Protocol ]
                    [ Origin-State-Id ]
                    [ State]
                    [ Error-Message ]
                    [ Error-Reporting-Host ]
                  * [ Failed-AVP ]
                  * [ Redirected-Host ]
                    [ Redirected-Host-Usage ]
                    [ Redirected-Max-Cache-Time ]
                  * [ Proxy-Info ]
                  * [ AVP ]
```

3.9. Accounting-Request (ACR) Command

TOC

The ACR message [I-D.ietf-dime-rfc3588bis] (Fajardo, V., Arkko, J., Loughney, J., and G. Zorn, “Diameter Base Protocol,” April 2010.) is sent by the NAS to report its session information to a target server downstream.

Either the Acct-Application-Id AVP or the Vendor-Specific-Application-Id AVP MUST be present. If the Vendor-Specific-Application-Id grouped AVP is present, it must have an Acct-Application-Id inside.

The AVPs listed in the Base protocol specification [I-D.ietf-dime-rfc3588bis] (Fajardo, V., Arkko, J., Loughney, J., and G. Zorn, “Diameter Base Protocol,” April 2010.) MUST be assumed to be present, as appropriate. NAS service-specific accounting AVPs SHOULD be present as described in Section 4.6 (NAS Accounting AVPs) and the rest of this specification.

Message Format

```
   <AC-Request> ::= < Diameter Header: 271, REQ, PXY >
                    < Session-Id >
                    { Origin-Host }
                    { Origin-Realm }
                    { Destination-Realm }
                    { Accounting-Record-Type }
                    { Accounting-Record-Number }
                    [ Acct-Application-Id ]
                    [ Vendor-Specific-Application-Id ]
                    [ User-Name ]
                    [ Accounting-Sub-Session-Id ]
                    [ Acct-Session-Id ]
                    [ Acct-Multi-Session-Id ]
                    [ Origin-AAA-Protocol ]
                    [ Origin-State-Id ]
                    [ Destination-Host ]
                    [ Event-Timestamp ]
                    [ Acct-Delay-Time ]
                    [ NAS-Identifier ]
                    [ NAS-IP-Address ]
                    [ NAS-IPv6-Address ]
                    [ NAS-Port ]
                    [ NAS-Port-Id ]
                    [ NAS-Port-Type ]
                  * [ Class ]
                    [ Service-Type ]
                    [ Termination-Cause ]
                    [ Accounting-Input-Octets ]
                    [ Accounting-Input-Packets ]
                    [ Accounting-Output-Octets ]
                    [ Accounting-Output-Packets ]
                    [ Acct-Authentic ]
                    [ Accounting-Auth-Method ]
                    [ Acct-Link-Count ]
                    [ Acct-Session-Time ]
                    [ Acct-Tunnel-Connection ]
                    [ Acct-Tunnel-Packets-Lost ]
                    [ Callback-Id ]
                    [ Callback-Number ]
                    [ Called-Station-Id ]
                    [ Calling-Station-Id ]
                  * [ Connection-Info ]
                    [ Originating-Line-Info ]
                    [ Authorization-Lifetime ]
                    [ Session-Timeout ]
                    [ Idle-Timeout ]
```

```
  [ Port-Limit ]
  [ Accounting-Realtime-Required ]
  [ Acct-Interim-Interval ]
* [ Filter-Id ]
* [ NAS-Filter-Rule ]
* [ Qos-Filter-Rule ]
  [ Framed-AppleTalk-Link ]
  [ Framed-AppleTalk-Network ]
  [ Framed-AppleTalk-Zone ]
  [ Framed-Compression ]
  [ Framed-Interface-Id ]
  [ Framed-IP-Address ]
  [ Framed-IP-Netmask ]
* [ Framed-IPv6-Prefix ]
  [ Framed-IPv6-Pool ]
* [ Framed-IPv6-Route ]
  [ Framed-IPX-Network ]
  [ Framed-MTU ]
  [ Framed-Pool ]
  [ Framed-Protocol ]
* [ Framed-Route ]
  [ Framed-Routing ]
* [ Login-IP-Host ]
* [ Login-IPv6-Host ]
  [ Login-LAT-Group ]
  [ Login-LAT-Node ]
  [ Login-LAT-Port ]
  [ Login-LAT-Service ]
  [ Login-Service ]
  [ Login-TCP-Port ]
* [ Tunneling ]
* [ Proxy-Info ]
* [ Route-Record ]
* [ AVP ]
```

3.10. Accounting-Answer (ACA) Command

TOC

The ACA message [I-D.ietf-dime-rfc3588bis] (Fajardo, V., Arkko, J., Loughney, J., and G. Zorn, “Diameter Base Protocol,” April 2010.) is used to acknowledge an Accounting-Request command. The Accounting-Answer command contains the same Session-Id as the Request. If the Accounting-Request was protected by end-to-end security, then the corresponding ACA message MUST be protected as well.

Only the target Diameter Server or home Diameter Server SHOULD respond

with the Accounting-Answer command.

Either the Acct-Application-Id AVP or the Vendor-Specific-Application-Id AVP MUST be present, as it was in the request.

The AVPs listed in the Base protocol specification [I-D.ietf-dime-rfc3588bis] (Fajardo, V., Arkko, J., Loughney, J., and G. Zorn, “Diameter Base Protocol,” April 2010.) MUST be assumed to be present, as appropriate. NAS service-specific accounting AVPs SHOULD be present as described in Section 4.6 (NAS Accounting AVPs) and the rest of this specification.

Message Format

```
   <AC-Answer> ::= < Diameter Header: 271, PXY >
                   < Session-Id >
                   { Result-Code }
                   { Origin-Host }
                   { Origin-Realm }
                   { Accounting-Record-Type }
                   { Accounting-Record-Number }
                   [ Acct-Application-Id ]
                   [ Vendor-Specific-Application-Id ]
                   [ User-Name ]
                   [ Accounting-Sub-Session-Id ]
                   [ Acct-Session-Id ]
                   [ Acct-Multi-Session-Id ]
                   [ Event-Timestamp ]
                   [ Error-Message ]
                   [ Error-Reporting-Host ]
                  * [ Failed-AVP ]
                   [ Origin-AAA-Protocol ]
                   [ Origin-State-Id ]
                   [ NAS-Identifier ]
                   [ NAS-IP-Address ]
                   [ NAS-IPv6-Address ]
                   [ NAS-Port ]
                   [ NAS-Port-Id ]
                   [ NAS-Port-Type ]
                   [ Service-Type ]
                   [ Termination-Cause ]
                   [ Accounting-Realtime-Required ]
                   [ Acct-Interim-Interval ]
                  * [ Class ]
                  * [ Proxy-Info ]
                  * [ Route-Record ]
                  * [ AVP ]
```

---

4. Diameter NAS Application AVPs

TOC

The following sections define a new derived AVP data format, a set of application-specific AVPs and describe the use of AVPs defined in other documents by the Diameter NAS Application.

TOC

4.1. Derived AVP Data Formats

4.1.1. QoSFilterRule

TOC

The QosFilterRule format is derived from the OctetString AVP Base Format. It uses the ASCII charset. Packets may be marked or metered based on the following information:

- *Direction (in or out)
- *Source and destination IP address (possibly masked)
- *Protocol
- *Source and destination port (lists or ranges)
- *DSCP values (no mask or range)

Rules for the appropriate direction are evaluated in order; the first matched rule terminates the evaluation. Each packet is evaluated once. If no rule matches, the packet is treated as best effort. An access device unable to interpret or apply a QoS rule SHOULD NOT terminate the session.

QoSFilterRule filters MUST follow the following format:

> action dir proto from src to dst [options]
>
> where
>
> **action**
>
> **tag** Mark packet with a specific DSCP [RFC2474] (Nichols, K., Blake, S., Baker, F., and D. Black, “Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers,” December 1998.)
>
> **meter** Meter traffic
>
> **dir** The format is as described under IPFilterRule [I-D.ietf-dime-rfc3588bis] (Fajardo, V., Arkko, J., Loughney, J., and G. Zorn, “Diameter Base Protocol,” April 2010.)

proto
: The format is as described under IPFilterRule [I-D.ietf-dime-rfc3588bis] (Fajardo, V., Arkko, J., Loughney, J., and G. Zorn, "Diameter Base Protocol," April 2010.)

src and dst The format is as described under IPFilterRule [I-D.ietf-dime-rfc3588bis] (Fajardo, V., Arkko, J., Loughney, J., and G. Zorn, "Diameter Base Protocol," April 2010.)

The options are described in Section 4.4.9 (QoS-Filter-Rule AVP).

The rule syntax is a modified subset of ipfw(8) from FreeBSD, and the ipfw.c code may provide a useful base for implementations.

4.2. NAS Session AVPs

TOC

Diameter reserves the AVP Codes 0 - 255 for RADIUS functions that are implemented in Diameter.

AVPs new to Diameter have code values of 256 and greater. A Diameter message that includes one of these AVPs may represent functions not present in the RADIUS environment and may cause interoperability issues, should the request traverse an AAA system that only supports the RADIUS protocol.

4.2.1. Call and Session Information

TOC

This section describes the AVPs specific to NAS Diameter applications that are needed to identify the call and session context and status information. On a request, this information allows the server to qualify the session.

These AVPs are used in addition to the following AVPs from the base protocol specification [I-D.ietf-dime-rfc3588bis] (Fajardo, V., Arkko, J., Loughney, J., and G. Zorn, "Diameter Base Protocol," April 2010.):

Session-Id

Auth-Application-Id

Origin-Host

Origin-Realm

Auth-Request-Type

Termination-Cause

The following table gives the possible flag values for the session level AVPs and specifies whether the AVP MAY be encrypted.

Attribute Name	Section Defined	AVP Flag rules				
		MUST	MAY	SHLD NOT	MUST NOT	Encr
NAS-Port	4.2.2	M	P		V	Y
NAS-Port-Id	4.2.3	M	P		V	Y
NAS-Port-Type	4.2.4	M	P		V	Y
Called-Station-Id	4.2.5	M	P		V	Y
Calling-Station-Id	4.2.6	M	P		V	Y
Connect-Info	4.2.7	M	P		V	Y
Originating-Line-Info	4.2.8		M,P		V	Y
Reply-Message	4.2.9	M	P		V	Y

4.2.2. NAS-Port AVP

TOC

The NAS-Port AVP (AVP Code 5) is of type Unsigned32 and contains the physical or virtual port number of the NAS which is authenticating the user. Note that "port" is meant in its sense as a service connection on the NAS, not as an IP protocol identifier.

Either the NAS-Port AVP or the NAS-Port-Id AVP (Section 4.2.3 (NAS-Port-Id AVP)) SHOULD be present in the AA-Request (AAR, Section 3.1 (AA-Request (AAR) Command)) command if the NAS differentiates among its ports.

4.2.3. NAS-Port-Id AVP

TOC

The NAS-Port-Id AVP (AVP Code 87) is of type UTF8String and consists of ASCII text identifying the port of the NAS authenticating the user. Note that "port" is meant in its sense as a service connection on the NAS, not as an IP protocol identifier.

Either the NAS-Port-Id or the NAS-Port (Section 4.2.2 (NAS-Port AVP)) SHOULD be present in the AA-Request (AAR, Section 3.1 (AA-Request (AAR) Command)) command if the NAS differentiates among its ports. NAS-Port-Id is intended for use by NASes that cannot conveniently number their ports.

4.2.4. NAS-Port-Type AVP

TOC

The NAS-Port-Type AVP (AVP Code 61) is of type Enumerated and contains the type of the port on which the NAS is authenticating the user. This AVP SHOULD be present if the NAS uses the same NAS-Port number ranges for different service types concurrently.

The currently supported values of the NAS-Port-Type AVP are listed in [RADIUSTypes] (IANA, "RADIUS Types," .).

4.2.5. Called-Station-Id AVP

TOC

The Called-Station-Id AVP (AVP Code 30) is of type UTF8String and allows the NAS to send the ASCII string describing the Layer 2 address the user contacted in the request. For dialup access, this can be a phone number obtained by using the Dialed Number Identification Service (DNIS) or a similar technology. Note that this may be different from the phone number the call comes in on. For use with IEEE 802 access, the Called-Station-Id MAY contain a MAC address formatted as described in [RFC3580] (Congdon, P., Aboba, B., Smith, A., Zorn, G., and J. Roese, "IEEE 802.1X Remote Authentication Dial In User Service (RADIUS) Usage Guidelines," September 2003.). It SHOULD only be present in authentication and/or authorization requests.

If the Called-Station-Id AVP is present in an AAR message, Auth-Request-Type AVP is set to AUTHORIZE_ONLY and the User-Name AVP is absent, the Diameter Server MAY perform authorization based on this AVP. This can be used by a NAS to request whether a call should be answered based on the DNIS.

The codification of this field's allowed usage range is outside the scope of this specification.

TOC

4.2.6. Calling-Station-Id AVP

The Calling-Station-Id AVP (AVP Code 31) is of type UTF8String and allows the NAS to send the ASCII string describing the Layer 2 address from which the user connected in the request. For dialup access, this is the phone number the call came from, using Automatic Number Identification (ANI) or a similar technology. For use with IEEE 802 access, the Calling-Station-Id AVP MAY contain a MAC address, formated as described in [RFC3580] (Congdon, P., Aboba, B., Smith, A., Zorn, G., and J. Roese, "IEEE 802.1X Remote Authentication Dial In User Service (RADIUS) Usage Guidelines," September 2003.). It SHOULD only be present in authentication and/or authorization requests.

If the Calling-Station-Id AVP is present in an AAR message, the Auth-Request-Type AVP is set to AUTHORIZE_ONLY and the User-Name AVP is absent, the Diameter Server MAY perform authorization based on the value of this AVP. This can be used by a NAS to request whether a call should be answered based on the Layer 2 address (ANI, MAC Address, etc.)

The codification of this field's allowed usage range is outside the scope of this specification.

4.2.7. Connect-Info AVP

TOC

The Connect-Info AVP (AVP Code 77) is of type UTF8String and is sent in the AA-Request message or an ACR message with the value of the Accounting-Record-Type AVP set to STOP. When sent in the AA-Request, it indicates the nature of the user's connection. The connection speed SHOULD be included at the beginning of the first Connect-Info AVP in the message. If the transmit and receive connection speeds differ, both may be included in the first AVP with the transmit speed listed first (the speed at which the NAS modem transmits), then a slash (/), then the receive speed, and then other optional information.

For example: "28800 V42BIS/LAPM" or "52000/31200 V90"

If sent in an ACR message with the value of the Accounting-Record-Type AVP set to STOP, this attribute may summarize statistics relating to session quality. For example, in IEEE 802.11, the Connect-Info AVP may contain information on the number of link layer retransmissions. The exact format of this attribute is implementation specific.

TOC

4.2.8. Originating-Line-Info AVP

The Originating-Line-Info AVP (AVP Code 94) is of type OctetString and is sent by the NAS system to convey information about the origin of the call from an SS7 system.

The originating line information (OLI) element indicates the nature and/or characteristics of the line from which a call originated (e.g., pay phone, hotel, cellular). Telephone companies are starting to offer OLI to their customers as an option over Primary Rate Interface (PRI). Internet Service Providers (ISPs) can use OLI in addition to Called-Station-Id and Calling-Station-Id attributes to differentiate customer calls and to define different services.

The Value field contains two octets (00 - 99). ANSI T1.113 and BELLCORE 394 can be used for additional information about these values and their use. For information on the currently assigned values, see [ANITypes] (NANPA Number Resource Info, "ANI Assignments," .).

4.2.9. Reply-Message AVP

TOC

The Reply-Message AVP (AVP Code 18) is of type UTF8String and contains text that MAY be displayed to the user. When used in an AA-Answer message with a successful Result-Code AVP, it indicates success. When found in an AAA message with a Result-Code other than DIAMETER_SUCCESS, the AVP contains a failure message.

The Reply-Message AVP MAY contain text to prompt the user before another AA-Request attempt. When used in an AA-Answer message containing a Result-Code AVP with the value DIAMETER_MULTI_ROUND_AUTH or in an Re-Auth-Request message, it MAY contain text to prompt the user for a response.

4.3. NAS Authentication AVPs

TOC

This section defines the AVPs necessary to carry the authentication information in the Diameter protocol. The functionality defined here provides a RADIUS-like AAA service over a more reliable and secure transport, as defined in the base protocol [I-D.ietf-dime-rfc3588bis] (Fajardo, V., Arkko, J., Loughney, J., and G. Zorn, "Diameter Base Protocol," April 2010.).

The following table gives the possible flag values for the session level AVPs and specifies whether the AVP MAY be encrypted.

		AVP Flag rules			
Attribute Name	Section Defined	MUST	MAY	SHLD NOT	MUST NOT	Encr
User-Password	4.3.1	M	P		V	Y
Password-Retry	4.3.2	M	P		V	Y
Prompt	4.3.3	M	P		V	Y
CHAP-Auth	4.3.4	M	P		V	Y
CHAP-Algorithm	4.3.5	M	P		V	Y
CHAP-Ident	4.3.6	M	P		V	Y
CHAP-Response	4.3.7	M	P		V	Y
CHAP-Challenge	4.3.8	M	P		V	Y
ARAP-Password	4.3.9	M	P		V	Y
ARAP-Challenge-Response	4.3.10	M	P		V	Y
ARAP-Security	4.3.11	M	P		V	Y
ARAP-Security-Data	4.3.12	M	P		V	Y

4.3.1. User-Password AVP

TOC

The User-Password AVP (AVP Code 2) is of type OctetString and contains the password of the user to be authenticated, or the user's input in a multi-round authentication exchange.

The User-Password AVP contains a user password or one-time password and therefore represents sensitive information. As required in [I-D.ietf-dime-rfc3588bis] (Fajardo, V., Arkko, J., Loughney, J., and G. Zorn, “Diameter Base Protocol,” April 2010.), Diameter messages are encrypted by using IPsec or TLS. Unless this AVP is used for one-time passwords, the User-Password AVP SHOULD NOT be used in untrusted proxy environments without encrypting it by using end-to-end security techniques.

The clear-text password (prior to encryption) MUST NOT be longer than 128 bytes in length.

4.3.2. Password-Retry AVP

TOC

The Password-Retry AVP (AVP Code 75) is of type Unsigned32 and MAY be included in the AA-Answer if the Result-Code indicates an

authentication failure. The value of this AVP indicates how many authentication attempts a user is permitted before being disconnected. This AVP is primarily intended for use when the Framed-Protocol AVP (Section 4.4.10.1 (Framed-Protocol AVP)) is set to ARAP.

4.3.3. Prompt AVP

TOC

The Prompt AVP (AVP Code 76) is of type Enumerated and MAY be present in the AA-Answer message. When present, it is used by the NAS to determine whether the user's response, when entered, should be echoed.

The supported values are listed in [RADIUSTypes] (IANA, “RADIUS Types,” .)

4.3.4. CHAP-Auth AVP

TOC

The CHAP-Auth AVP (AVP Code 402) is of type Grouped and contains the information necessary to authenticate a user using the PPP Challenge-Handshake Authentication Protocol (CHAP) [RFC1994] (Simpson, W., “PPP Challenge Handshake Authentication Protocol (CHAP),” August 1996.). If the CHAP-Auth AVP is found in a message, the CHAP-Challenge AVP Section 4.3.8 (CHAP-Challenge AVP) MUST be present as well. The optional AVPs containing the CHAP response depend upon the value of the CHAP-Algorithm AVP Section 4.3.8 (CHAP-Challenge AVP). The grouped AVP has the following ABNF grammar:

```
CHAP-Auth  ::= < AVP Header: 402 >
               { CHAP-Algorithm }
               { CHAP-Ident }
               [ CHAP-Response ]
             * [ AVP ]
```

4.3.5. CHAP-Algorithm AVP

TOC

The CHAP-Algorithm AVP (AVP Code 403) is of type Enumerated and contains the algorithm identifier used in the computation of the CHAP response [RFC1994] (Simpson, W., “PPP Challenge Handshake Authentication Protocol (CHAP),” August 1996.). The following values are currently supported:

CHAP with MD5 5

> The CHAP response is computed by using the procedure described in [RFC1994] (Simpson, W., “PPP Challenge Handshake Authentication Protocol (CHAP),” August 1996.) This algorithm requires that the CHAP-Response AVP Section 4.3.7 (CHAP-Response AVP) MUST be present in the CHAP-Auth AVP Section 4.3.4 (CHAP-Auth AVP).

4.3.6. CHAP-Ident AVP

TOC

The CHAP-Ident AVP (AVP Code 404) is of type OctetString and contains the 1 octet CHAP Identifier used in the computation of the CHAP response [RFC1994] (Simpson, W., “PPP Challenge Handshake Authentication Protocol (CHAP),” August 1996.)

4.3.7. CHAP-Response AVP

TOC

The CHAP-Response AVP (AVP Code 405) is of type OctetString and contains the 16 octet authentication data provided by the user in response to the CHAP challenge [RFC1994] (Simpson, W., “PPP Challenge Handshake Authentication Protocol (CHAP),” August 1996.).

4.3.8. CHAP-Challenge AVP

TOC

The CHAP-Challenge AVP (AVP Code 60) is of type OctetString and contains the CHAP Challenge sent by the NAS to the CHAP peer [RFC1994] (Simpson, W., “PPP Challenge Handshake Authentication Protocol (CHAP),” August 1996.).

4.3.9. ARAP-Password AVP

TOC

The ARAP-Password AVP (AVP Code 70) is of type OctetString and is only present when the Framed-Protocol AVP (Section 4.4.10.1 (Framed-Protocol AVP)) is included in the message and is set to ARAP. This AVP MUST NOT be present if either the User-Password or the CHAP-Auth AVP is present. See [RFC2869] (Rigney, C., Willats, W., and P. Calhoun, “RADIUS Extensions,” June 2000.) for more information on the contents of this AVP.

4.3.10. ARAP-Challenge-Response AVP

TOC

The ARAP-Challenge-Response AVP (AVP Code 84) is of type OctetString and is only present when the Framed-Protocol AVP (Section 4.4.10.1 (Framed-Protocol AVP)) is included in the message and is set to ARAP. This AVP contains an 8 octet response to the dial-in client's challenge. The RADIUS server calculates this value by taking the dial-in client's challenge from the high-order 8 octets of the ARAP-Password AVP and performing DES encryption on this value with the authenticating user's password as the key. If the user's password is fewer than 8 octets in length, the password is padded at the end with NULL octets to a length of 8before it is used as a key.

4.3.11. ARAP-Security AVP

TOC

The ARAP-Security AVP (AVP Code 73) is of type Unsigned32 and MAY be present in the AA-Answer message if the Framed-Protocol AVP (Section 4.4.10.1 (Framed-Protocol AVP)) is set to the value of ARAP, and the Result-Code AVP ([I-D.ietf-dime-rfc3588bis] (Fajardo, V., Arkko, J., Loughney, J., and G. Zorn, “Diameter Base Protocol,” April 2010.), Section 7.1) is set to DIAMETER_MULTI_ROUND_AUTH. See [RFC2869] (Rigney, C., Willats, W., and P. Calhoun, “RADIUS Extensions,” June 2000.) for more information on the contents of this AVP.

4.3.12. ARAP-Security-Data AVP

TOC

The ARAP-Security-Data AVP (AVP Code 74) is of type OctetString and MAY be present in the AA-Request or AA-Answer message if the Framed-Protocol AVP (Section 4.4.10.1 (Framed-Protocol AVP)) is set to the value of ARAP and the Result-Code AVP ([I-D.ietf-dime-rfc3588bis] (Fajardo, V., Arkko, J., Loughney, J., and G. Zorn, “Diameter Base Protocol,” April 2010.), Section 7.1) is set to DIAMETER_MULTI_ROUND_AUTH. This AVP contains the security module challenge or response associated with the ARAP Security Module specified in the ARAP-Security AVP (Section 4.3.11 (ARAP-Security AVP)).

TOC

4.4. NAS Authorization AVPs

This section contains the authorization AVPs supported in the NAS Application. The Service-Type AVP SHOULD be present in all messages and, based on its value, additional AVPs defined in this section and Section 4.5 (NAS Tunneling AVPs) MAY be present.

The following table gives the possible flag values for the session level AVPs and specifies whether the AVP MAY be encrypted.

		AVP Flag rules				
Attribute Name	Section Defined	MUST	MAY	SHLD NOT	MUST NOT	Encr
Service-Type	4.4.1	M	P		V	Y
Callback-Number	4.4.2	M	P		V	Y
Callback-Id	4.4.3	M	P		V	Y
Idle-Timeout	4.4.4	M	P		V	Y
Port-Limit	4.4.5	M	P		V	Y
NAS-Filter-Rule	4.4.6	M	P		V	Y
Filter-Id	4.4.7	M	P		V	Y
Configuration-Token	4.4.8	M			P,V	
QoS-Filter-Rule	4.4.9					
Framed-Protocol	4.4.10.1	M	P		V	Y
Framed-Routing	4.4.10.2	M	P		V	Y
Framed-MTU	4.4.10.3	M	P		V	Y
Framed-Compression	4.4.10.4	M	P		V	Y
Framed-IP-Address	4.4.10.5.1	M	P		V	Y
Framed-IP-Netmask	4.4.10.5.2	M	P		V	Y
Framed-Route	4.4.10.5.3	M	P		V	Y
Framed-Pool	4.4.10.5.4	M	P		V	Y
Framed-Interface-Id	4.4.10.5.5	M	P		V	Y
Framed-IPv6-Prefix	4.4.10.5.6	M	P		V	Y
Framed-IPv6-Route	4.4.10.5.7	M	P		V	Y
Framed-IPv6-Pool	4.4.10.5.8	M	P		V	Y
Framed-IPX-Network	4.4.10.6.1	M	P		V	Y
Framed-Appletalk-Link	4.4.10.7.1	M	P		V	Y
Framed-Appletalk-Network	4.4.10.7.2	M	P		V	Y
Framed-Appletalk-Zone	4.4.10.7.3	M	P		V	Y
ARAP-Features	4.4.10.8.1	M	P		V	Y
ARAP-Zone-Access	4.4.10.8.2	M	P		V	Y
Login-IP-Host	4.4.11.1	M	P		V	Y
Login-IPv6-Host	4.4.11.2	M	P		V	Y
Login-Service	4.4.11.3	M	P		V	Y
Login-TCP-Port	4.4.11.4.1	M	P		V	Y
Login-LAT-Service	4.4.11.5.1	M	P		V	Y
Login-LAT-Node	4.4.11.5.2	M	P		V	Y
Login-LAT-Group	4.4.11.5.3	M	P		V	Y
Login-LAT-Port	4.4.11.5.4	M	P		V	Y

TOC

4.4.1. Service-Type AVP

The Service-Type AVP (AVP Code 6) is of type Enumerated and contains the type of service the user has requested or the type of service to be provided. One such AVP MAY be present in an authentication and/or authorization request or response. A NAS is not required to implement all of these service types. It MUST treat unknown or unsupported Service-Types received in a response as a failure and end the session with a DIAMETER_INVALID_AVP_VALUE Result-Code.

When used in a request, the Service-Type AVP SHOULD be considered a hint to the server that the NAS believes the user would prefer the kind of service indicated. The server is not required to honor the hint. Furthermore, if the service specified by the server is supported, but not compatible with the current mode of access, the NAS MUST fail to start the session. The NAS MUST also generate the appropriate error message(s).

The complete list of defined values that the Service-Type AVP can take can be found in [RFC2865] (Rigney, C., Willens, S., Rubens, A., and W. Simpson, "Remote Authentication Dial In User Service (RADIUS)," June 2000.) and [RADIUSTypes] (IANA, "RADIUS Types," .), but the following values require further qualification here:

> **Login (1)** The user should be connected to a host. The message MAY include additional AVPs as defined in Section 4.4.11.4 (TCP Services) or Section 4.4.11.5 (LAT Services).
>
> **Framed (2)** A Framed Protocol, such as PPP or SLIP, should be started for the User. The message MAY include additional AVPs defined in Section 4.4.10 (Framed Access Authorization AVPs), or Section 4.5 (NAS Tunneling AVPs) for tunneling services.
>
> **Callback Login (3)** The user should be disconnected and called back, then connected to a host. The message MAY include additional AVPs defined in this Section.
>
> **Callback Framed (4)** The user should be disconnected and called back, and then a Framed Protocol, such as PPP or SLIP, should be started for the User. The message MAY include additional AVPs defined in Section 4.4.10 (Framed Access Authorization AVPs), or Section 4.5 (NAS Tunneling AVPs) for tunneling services.

4.4.2. Callback-Number AVP

TOC

The Callback-Number AVP (AVP Code 19) is of type UTF8String and contains a dialing string to be used for callback. It MAY be used in an authentication and/or authorization request as a hint to the server that a Callback service is desired, but the server is not required to honor the hint in the corresponding response.

The codification of this field's allowed usage range is outside the scope of this specification.

4.4.3. Callback-Id AVP

TOC

The Callback-Id AVP (AVP Code 20) is of type UTF8String and contains the name of a place to be called, to be interpreted by the NAS. This AVP MAY be present in an authentication and/or authorization response.

This AVP is not roaming-friendly as it assumes that the Callback-Id is configured on the NAS. Using the Callback-Number AVP Section 4.4.2 (Callback-Number AVP) is therefore preferable.

4.4.4. Idle-Timeout AVP

TOC

The Idle-Timeout AVP (AVP Code 28) is of type Unsigned32 and sets the maximum number of consecutive seconds of idle connection allowable to the user before termination of the session or before a prompt is issued. The default is none, or system specific.

4.4.5. Port-Limit AVP

TOC

The Port-Limit AVP (AVP Code 62) is of type Unsigned32 and sets the maximum number of ports the NAS provides to the user. It MAY be used in an authentication and/or authorization request as a hint to the server that multilink PPP [RFC1990] (Sklower, K., Lloyd, B., McGregor, G., Carr, D., and T. Coradetti, “The PPP Multilink Protocol (MP),” August 1996.) service is desired, but the server is not required to honor the hint in the corresponding response.

TOC

4.4.6. NAS-Filter-Rule AVP

The NAS-Filter-Rule AVP (AVP Code 400) is of type IPFilterRule and provides filter rules that need to be configured on the NAS for the user. One or more of these AVPs MAY be present in an authorization response.

4.4.7. Filter-Id AVP

TOC

The Filter-Id AVP (AVP Code 11) is of type UTF8String and contains the name of the filter list for this user. Zero or more Filter-Id AVPs MAY be sent in an authorization answer.

Identifying a filter list by name allows the filter to be used on different NASes without regard to filter-list implementation details. However, this AVP is not roaming-friendly, as filter naming differs from one service provider to another.

In environments where backward compatibility with RADIUS is not required, it is RECOMMENDED that the NAS-Filter-Rule AVP Section 4.4.6 (NAS-Filter-Rule AVP) be used instead.

4.4.8. Configuration-Token AVP

TOC

The Configuration-Token AVP (AVP Code 78) is of type OctetString and is sent by a Diameter Server to a Diameter Proxy Agent or Translation Agent in an AA-Answer command to indicate a type of user profile to be used. It should not be sent to a Diameter Client (NAS).

The format of the Data field of this AVP is site specific.

4.4.9. QoS-Filter-Rule AVP

TOC

The QoS-Filter-Rule AVP (AVP Code 407) is of type QoSFilterRule Section 4.1.1 (QoSFilterRule) and provides QoS filter rules that need to be configured on the NAS for the user. One or more such AVPs MAY be present in an authorization response.

> **DSCP <color>** If action is set to tag Section 4.1.1 (QoSFilterRule) this option MUST be included in the rule.
> Color values are defined in [RFC2474] (Nichols, K., Blake, S.,

Baker, F., and D. Black, “Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers,” December 1998.). Exact matching of DSCP values is required (no masks or ranges).

metering <rate> <color_under> <color_over> The metering option provides Assured Forwarding, as defined in [RFC2597] (Heinanen, J., Baker, F., Weiss, W., and J. Wroclawski, “Assured Forwarding PHB Group,” June 1999.). and MUST be present if the action is set to meter Section 4.1.1 (QoSFilterRule) The rate option is the throughput, in bits per second, used by the access device to mark packets. Traffic over the rate is marked with the color_over codepoint, and traffic under the rate is marked with the color_under codepoint. The color_under and color_over options contain the drop preferences and MUST conform to the recommended codepoint keywords described in [RFC2597] (Heinanen, J., Baker, F., Weiss, W., and J. Wroclawski, “Assured Forwarding PHB Group,” June 1999.) (e.g., AF13).
The metering option also supports the strict limit on traffic required by Expedited Forwarding, as defined in [RFC3246] (Davie, B., Charny, A., Bennet, J., Benson, K., Le Boudec, J., Courtney, W., Davari, S., Firoiu, V., and D. Stiliadis, “An Expedited Forwarding PHB (Per-Hop Behavior),” March 2002.). The color_over option may contain the keyword "drop" to prevent forwarding of traffic that exceeds the rate parameter.

4.4.10. Framed Access Authorization AVPs

TOC

This section lists the authorization AVPs necessary to support framed access, such as PPP and SLIP. AVPs defined in this section MAY be present in a message if the Service-Type AVP was set to "Framed" or "Callback Framed".

4.4.10.1. Framed-Protocol AVP

TOC

The Framed-Protocol AVP (AVP Code 7) is of type Enumerated and contains the framing to be used for framed access. This AVP MAY be present in both requests and responses. The supported values are listed in [RADIUSTypes] (IANA, “RADIUS Types,” .).

TOC

4.4.10.2. Framed-Routing AVP

The Framed-Routing AVP (AVP Code 10) is of type Enumerated and contains the routing method for the user when the user is a router to a network. This AVP SHOULD only be present in authorization responses. The supported values are listed in [RADIUSTypes] (IANA, “RADIUS Types,” .).

4.4.10.3. Framed-MTU AVP

TOC

The Framed-MTU AVP (AVP Code 12) is of type Unsigned32 and contains the Maximum Transmission Unit (MTU) to be configured for the user, when it is not negotiated by some other means (such as PPP). This AVP SHOULD only be present in authorization responses. The MTU value MUST be in the range from 64 to 65535.

4.4.10.4. Framed-Compression AVP

TOC

The Framed-Compression AVP (AVP Code 13) is of type Enumerated and contains the compression protocol to be used for the link. It MAY be used in an authorization request as a hint to the server that a specific compression type is desired, but the server is not required to honor the hint in the corresponding response.

More than one compression protocol AVP MAY be sent. The NAS is responsible for applying the proper compression protocol to the appropriate link traffic.

The supported values are listed in [RADIUSTypes] (IANA, “RADIUS Types,” .).

4.4.10.5. IP Access Authorization AVPs

TOC

The AVPs defined in this section are used when the user requests, or is being granted, access service to IP.

4.4.10.5.1. Framed-IP-Address AVP

TOC

The Framed-IP-Address AVP (AVP Code 8) [RFC2865] (Rigney, C., Willens, S., Rubens, A., and W. Simpson, “Remote Authentication Dial In User

Service (RADIUS)," June 2000.) is of type OctetString and contains an IPv4 address of the type specified in the attribute value to be configured for the user. It MAY be used in an authorization request as a hint to the server that a specific address is desired, but the server is not required to honor the hint in the corresponding response.

Two values have special significance: 0xFFFFFFFF and 0xFFFFFFFE. The value 0xFFFFFFFF indicates that the NAS should allow the user to select an address (i.e., negotiated). The value 0xFFFFFFFE indicates that the NAS should select an address for the user (e.g., assigned from a pool of addresses kept by the NAS).

4.4.10.5.2. Framed-IP-Netmask AVP

TOC

The Framed-IP-Netmask AVP (AVP Code 9) is of type OctetString and contains the four octets of the IPv4 netmask to be configured for the user when the user is a router to a network. It MAY be used in an authorization request as a hint to the server that a specific netmask is desired, but the server is not required to honor the hint in the corresponding response. This AVP MUST be present in a response if the request included this AVP with a value of 0xFFFFFFFF.

4.4.10.5.3. Framed-Route AVP

TOC

The Framed-Route AVP (AVP Code 22) is of type UTF8String and contains the ASCII routing information to be configured for the user on the NAS. Zero or more of these AVPs MAY be present in an authorization response.

The string MUST contain a destination prefix in dotted quad form optionally followed by a slash and a decimal length specifier stating how many high-order bits of the prefix should be used. This is followed by a space, a gateway address in dotted quad form, a space, and one or more metrics separated by spaces; for example,

> "192.168.1.0/24 192.168.1.1 1"

The length specifier may be omitted, in which case it should default to 8 bits for class A prefixes, to 16 bits for class B prefixes, and to 24 bits for class C prefixes; for example,

> "192.168.1.0 192.168.1.1 1"

Whenever the gateway address is specified as "0.0.0.0" the IP address of the user SHOULD be used as the gateway address.

4.4.10.5.4. Framed-Pool AVP

TOC

The Framed-Pool AVP (AVP Code 88) is of type OctetString and contains the name of an assigned address pool that SHOULD be used to assign an address for the user. If a NAS does not support multiple address pools, the NAS SHOULD ignore this AVP. Address pools are usually used for IP addresses but can be used for other protocols if the NAS supports pools for those protocols.

Although specified as type OctetString for compatibility with RADIUS [RFC2865] (Rigney, C., Willens, S., Rubens, A., and W. Simpson, “Remote Authentication Dial In User Service (RADIUS),” June 2000.), the encoding of the Data field SHOULD also conform to the rules for the UTF8String Data Format.

4.4.10.5.5. Framed-Interface-Id AVP

TOC

The Framed-Interface-Id AVP (AVP Code 96) is of type Unsigned64 and contains the IPv6 interface identifier to be configured for the user. It MAY be used in authorization requests as a hint to the server that a specific interface id is desired, but the server is not required to honor the hint in the corresponding response.

4.4.10.5.6. Framed-IPv6-Prefix AVP

TOC

The Framed-IPv6-Prefix AVP (AVP Code 97) is of type OctetString and contains the IPv6 prefix to be configured for the user. One or more AVPs MAY be used in authorization requests as a hint to the server that specific IPv6 prefixes are desired, but the server is not required to honor the hint in the corresponding response.

4.4.10.5.7. Framed-IPv6-Route AVP

TOC

The Framed-IPv6-Route AVP (AVP Code 99) is of type UTF8String and contains the ASCII routing information to be configured for the user on the NAS. Zero or more of these AVPs MAY be present in an authorization

response.

The string MUST contain an IPv6 address prefix followed by a slash and a decimal length specifier stating how many high order bits of the prefix should be used. This is followed by a space, a gateway address in hexadecimal notation, a space, and one or more metrics separated by spaces; for example,

> "2000:0:0:106::/64 2000::106:a00:20ff:fe99:a998 1"

Whenever the gateway address is the IPv6 unspecified address, the IP address of the user SHOULD be used as the gateway address, such as in:

> "2000:0:0:106::/64 :: 1"

4.4.10.5.8. Framed-IPv6-Pool AVP

TOC

The Framed-IPv6-Pool AVP (AVP Code 100) is of type OctetString and contains the name of an assigned pool that SHOULD be used to assign an IPv6 prefix for the user. If the access device does not support multiple prefix pools, it MUST ignore this AVP.

Although specified as type OctetString for compatibility with RADIUS [RFC3162] (Aboba, B., Zorn, G., and D. Mitton, “RADIUS and IPv6,” August 2001.), the encoding of the Data field SHOULD also conform to the rules for the UTF8String Data Format.

4.4.10.6. IPX Access AVPs

TOC

The AVPs defined in this section are used when the user requests, or is being granted, access to an IPX network service [IPX] (Novell, Inc., “NetWare System Technical Interface Overview,” June 1989.).

4.4.10.6.1. Framed-IPX-Network AVP

TOC

The Framed-IPX-Network AVP (AVP Code 23) is of type Unsigned32 and contains the IPX Network number to be configured for the user. It MAY be used in an authorization request as a hint to the server that a specific address is desired, but the server is not required to honor the hint in the corresponding response.

Two addresses have special significance: 0xFFFFFFFF and 0xFFFFFFFE. The value 0xFFFFFFFF indicates that the NAS should allow the user to select an address (i.e., Negotiated). The value 0xFFFFFFFE indicates that the NAS should select an address for the user (e.g., assign it from a pool of one or more IPX networks kept by the NAS).

4.4.10.7. AppleTalk Network Access AVPs

TOC

The AVPs defined in this section are used when the user requests, or is being granted, access to an AppleTalk network [AppleTalk] (Sidhu, G., Andrews, R., and A. Oppenheimer, “Inside AppleTalk,” 1990.).

4.4.10.7.1. Framed-AppleTalk-Link AVP

TOC

The Framed-AppleTalk-Link AVP (AVP Code 37) is of type Unsigned32 and contains the AppleTalk network number that should be used for the serial link to the user, which is another AppleTalk router. This AVP MUST only be present in an authorization response and is never used when the user is not another router.

Despite the size of the field, values range from 0 to 65,535. The special value of 0 indicates an unnumbered serial link. A value of 1 to 65,535 means that the serial line between the NAS and the user should be assigned that value as an AppleTalk network number.

4.4.10.7.2. Framed-AppleTalk-Network AVP

TOC

The Framed-AppleTalk-Network AVP (AVP Code 38) is of type Unsigned32 and contains the AppleTalk Network number that the NAS should probe to allocate an AppleTalk node for the user. This AVP MUST only be present in an authorization response and is never used when the user is not another router. Multiple instances of this AVP indicate that the NAS may probe, using any of the network numbers specified.

Despite the size of the field, values range from 0 to 65,535. The special value 0 indicates that the NAS should assign a network for the user, using its default cable range. A value between 1 and 65,535 (inclusive) indicates to the AppleTalk Network that the NAS should probe to find an address for the user.

4.4.10.7.3. Framed-AppleTalk-Zone AVP

TOC

The Framed-AppleTalk-Zone AVP (AVP Code 39) is of type OctetString and contains the AppleTalk Default Zone to be used for this user. This AVP MUST only be present in an authorization response. Multiple instances of this AVP in the same message are not allowed.

The codification of this field's allowed range is outside the scope of this specification.

4.4.10.8. AppleTalk Remote Access AVPs

TOC

The AVPs defined in this section are used when the user requests, or is being granted, access to the AppleTalk network via the AppleTalk Remote Access Protocol [ARAP] (Apple Computer, “Apple Remote Access Protocol (ARAP) Version 2.0 External Reference Specification,” September 1994.) They are only present if the Framed-Protocol AVP Section 4.4.10.1 (Framed-Protocol AVP) is set to ARAP. Section 2.2 of RFC 2869 [RFC2869] (Rigney, C., Willats, W., and P. Calhoun, “RADIUS Extensions,” June 2000.) describes the operational use of these attributes.

4.4.10.8.1. ARAP-Features AVP

TOC

The ARAP-Features AVP (AVP Code 71) is of type OctetString and MAY be present in the AA-Accept message if the Framed-Protocol AVP is set to the value of ARAP. See [RFC2869] (Rigney, C., Willats, W., and P. Calhoun, “RADIUS Extensions,” June 2000.) for more information about the format of this AVP.

4.4.10.8.2. ARAP-Zone-Access AVP

TOC

The ARAP-Zone-Access AVP (AVP Code 72) is of type Enumerated and MAY be present in the AA-Accept message if the Framed-Protocol AVP is set to the value of ARAP.

The supported values are listed in [RADIUSTypes] (IANA, “RADIUS Types,” .) and defined in [RFC2869] (Rigney, C., Willats, W., and P. Calhoun, “RADIUS Extensions,” June 2000.).

4.4.11. Non-Framed Access Authorization AVPs

TOC

This section contains the authorization AVPs that are needed to support terminal server functionality. AVPs defined in this section MAY be present in a message if the Service-Type AVP was set to "Login" or "Callback Login".

4.4.11.1. Login-IP-Host AVP

TOC

The Login-IP-Host AVP (AVP Code 14) [RFC2865] (Rigney, C., Willens, S., Rubens, A., and W. Simpson, “Remote Authentication Dial In User Service (RADIUS),” June 2000.) is of type OctetString and contains the IPv4 address of a host with which to connect the user when the Login-Service AVP is included. It MAY be used in an AA-Request command as a hint to the Diameter Server that a specific host is desired, but the Diameter Server is not required to honor the hint in the AA-Answer.

Two addresses have special significance: all ones and 0. The value of all ones indicates that the NAS SHOULD allow the user to select an address. The value 0 indicates that the NAS SHOULD select a host to connect the user to.

4.4.11.2. Login-IPv6-Host AVP

TOC

The Login-IPv6-Host AVP (AVP Code 98) [RFC3162] (Aboba, B., Zorn, G., and D. Mitton, “RADIUS and IPv6,” August 2001.) is of type OctetString and contains the IPv6 address of a host with which to connect the user when the Login-Service AVP is included. It MAY be used in an AA-Request command as a hint to the Diameter Server that a specific host is desired, but the Diameter Server is not required to honor the hint in the AA-Answer.

Two addresses have special significance, 0xFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF and 0. The value 0xFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF indicates that the NAS SHOULD allow the user to select an address. The value 0 indicates that the NAS SHOULD select a host to connect the user to.

TOC

4.4.11.3. Login-Service AVP

The Login-Service AVP (AVP Code 15) is of type Enumerated and contains the service that should be used to connect the user to the login host. This AVP SHOULD only be present in authorization responses. The supported values are listed in [RFC2869] (Rigney, C., Willats, W., and P. Calhoun, "RADIUS Extensions," June 2000.).

4.4.11.4. TCP Services

TOC

The AVP described in the following section MAY be present if the Login-Service AVP is set to Telnet, Rlogin, TCP Clear, or TCP Clear Quiet.

4.4.11.4.1. Login-TCP-Port AVP

TOC

The Login-TCP-Port AVP (AVP Code 16) is of type Unsigned32 and contains the TCP port with which the user is to be connected when the Login-Service AVP is also present. This AVP SHOULD only be present in authorization responses. The value MUST NOT be greater than 65,535.

4.4.11.5. LAT Services

TOC

The AVPs described in this section MAY be present if the Login-Service AVP is set to LAT [LAT] (Digital Equipment Corp., "Local Area Transport (LAT) Specification V5.0," June 1989.).

4.4.11.5.1. Login-LAT-Service AVP

TOC

The Login-LAT-Service AVP (AVP Code 34) is of type OctetString and contains the system with which the user is to be connected by LAT. It MAY be used in an authorization request as a hint to the server that a specific service is desired, but the server is not required to honor the hint in the corresponding response. This AVP MUST only be present in the response if the Login-Service AVP states that LAT is desired.

Administrators use this service attribute when dealing with clustered systems, such as a VAX or Alpha cluster. In these environments, several different time-sharing hosts share the same resources (disks, printers, etc.), and administrators often configure each host to offer access

(service) to each of the shared resources. In this case, each host in the cluster advertises its services through LAT broadcasts.

Sophisticated users often know which service providers (machines) are faster and tend to use a node name when initiating a LAT connection. Some administrators want particular users to use certain machines as a primitive form of load balancing (although LAT knows how to do load balancing itself).

The String field contains the identity of the LAT service to use. The LAT Architecture allows this string to contain $ (dollar), - (hyphen), . (period), _ (underscore), numerics, upper- and lowercase alphabetics, and the ISO Latin-1 character set extension [ISO.8859-1.1987] (International Organization for Standardization, "Information technology - 8-bit single byte coded graphic - character sets - Part 1: Latin alphabet No. 1, JTC1/SC2," 1987.). All LAT string comparisons are case insensitive.

4.4.11.5.2. Login-LAT-Node AVP

TOC

The Login-LAT-Node AVP (AVP Code 35) is of type OctetString and contains the Node with which the user is to be automatically connected by LAT. It MAY be used in an authorization request as a hint to the server that a specific LAT node is desired, but the server is not required to honor the hint in the corresponding response. This AVP MUST only be present in a response if the Login-Service-Type AVP is set to LAT.

The String field contains the identity of the LAT service to use. The LAT Architecture allows this string to contain $ (dollar), - (hyphen), . (period), _ (underscore), numerics, upper- and lowercase alphabetics, and the ISO Latin-1 character set extension [ISO.8859-1.1987] (International Organization for Standardization, "Information technology - 8-bit single byte coded graphic - character sets - Part 1: Latin alphabet No. 1, JTC1/SC2," 1987.). All LAT string comparisons are case insensitive.

4.4.11.5.3. Login-LAT-Group AVP

TOC

The Login-LAT-Group AVP (AVP Code 36) is of type OctetString and contains a string identifying the LAT group codes this user is authorized to use. It MAY be used in an authorization request as a hint to the server that a specific group is desired, but the server is not required to honor the hint in the corresponding response. This AVP MUST

only be present in a response if the Login-Service-Type AVP is set to LAT.

LAT supports 256 different group codes, which LAT uses as a form of access rights. LAT encodes the group codes as a 256-bit bitmap.

Administrators can assign one or more of the group code bits at the LAT service provider; it will only accept LAT connections that have these group codes set in the bitmap. The administrators assign a bitmap of authorized group codes to each user. LAT gets these from the operating system and uses them in its requests to the service providers.

The codification of the range of allowed usage of this field is outside the scope of this specification.

4.4.11.5.4. Login-LAT-Port AVP

TOC

The Login-LAT-Port AVP (AVP Code 63) is of type OctetString and contains the Port with which the user is to be connected by LAT. It MAY be used in an authorization request as a hint to the server that a specific port is desired, but the server is not required to honor the hint in the corresponding response. This AVP MUST only be present in a response if the Login-Service-Type AVP is set to LAT.

The String field contains the identity of the LAT service to use. The LAT Architecture allows this string to contain $ (dollar), - (hyphen), . (period), _ (underscore), numerics, upper- and lower-case alphabetics, and the ISO Latin-1 character set extension [ISO. 8859-1.1987] (International Organization for Standardization, “Information technology - 8-bit single byte coded graphic - character sets - Part 1: Latin alphabet No. 1, JTC1/SC2,” 1987.).

All LAT string comparisons are case insensitive.

4.5. NAS Tunneling AVPs

TOC

Some NASes support compulsory tunnel services in which the incoming connection data is conveyed by an encapsulation method to a gateway elsewhere in the network. This is typically transparent to the service user, and the tunnel characteristics may be described by the remote AAA server, based on the user's authorization information. Several tunnel characteristics may be returned, and the NAS implementation may choose one. See [RFC2868] (Zorn, G., Leifer, D., Rubens, A., Shriver, J., Holdrege, M., and I. Goyret, “RADIUS Attributes for Tunnel Protocol

Support," June 2000.) and [RFC2867] (Zorn, G., Aboba, B., and D. Mitton, "RADIUS Accounting Modifications for Tunnel Protocol Support," June 2000.) for further information.

The following table gives the possible flag values for the session level AVPs and specifies whether the AVP MAY be encrypted.

		AVP Flag rules				
Attribute Name	Section Defined	MUST	MAY	SHLD NOT	MUST NOT	Encr
Tunneling	4.5.1	M	P		V	N
Tunnel-Type	4.5.2	M	P		V	Y
Tunnel-Medium-Type	4.5.3	M	P		V	Y
Tunnel-Client-Endpoint	4.5.4	M	P		V	Y
Tunnel-Server-Endpoint	4.5.5	M	P		V	Y
Tunnel-Password	4.5.6	M	P		V	Y
Tunnel-Private-Group-Id	4.5.7	M	P		V	Y
Tunnel-Assignment-Id	4.5.8	M	P		V	Y
Tunnel-Preference	4.5.9	M	P		V	Y
Tunnel-Client-Auth-Id	4.5.10	M	P		V	Y
Tunnel-Server-Auth-Id	4.5.11	M	P		V	Y

4.5.1. Tunneling AVP

TOC

The Tunneling AVP (AVP Code 401) is of type Grouped and contains the following AVPs, used to describe a compulsory tunnel service ([RFC2868] (Zorn, G., Leifer, D., Rubens, A., Shriver, J., Holdrege, M., and I. Goyret, "RADIUS Attributes for Tunnel Protocol Support," June 2000.), [RFC2867] (Zorn, G., Aboba, B., and D. Mitton, "RADIUS Accounting Modifications for Tunnel Protocol Support," June 2000.)). Its data field has the following ABNF grammar:

```
Tunneling     ::= < AVP Header: 401 >
                  { Tunnel-Type }
                  { Tunnel-Medium-Type }
                  { Tunnel-Client-Endpoint }
                  { Tunnel-Server-Endpoint }
                  [ Tunnel-Preference ]
                  [ Tunnel-Client-Auth-Id ]
                  [ Tunnel-Server-Auth-Id ]
                  [ Tunnel-Assignment-Id ]
                  [ Tunnel-Password ]
                  [ Tunnel-Private-Group-Id ]
```

4.5.2. Tunnel-Type AVP

TOC

The Tunnel-Type AVP (AVP Code 64) is of type Enumerated and contains the tunneling protocol(s) to be used (in the case of a tunnel initiator) or in use (in the case of a tunnel terminator). It MAY be used in an authorization request as a hint to the server that a specific tunnel type is desired, but the server is not required to honor the hint in the corresponding response.

The Tunnel-Type AVP SHOULD also be included in ACR messages.

A tunnel initiator is not required to implement any of these tunnel types. If a tunnel initiator receives a response that contains only unknown or unsupported Tunnel-Types, the tunnel initiator MUST behave as though a response were received with the Result-Code indicating a failure.

The supported values are listed in [RADIUSTypes] (IANA, “RADIUS Types,” .).

4.5.3. Tunnel-Medium-Type AVP

TOC

The Tunnel-Medium-Type AVP (AVP Code 65) is of type Enumerated and contains the transport medium to use when creating a tunnel for protocols (such as L2TP (Townsley, W., Valencia, A., Rubens, A., Pall, G., Zorn, G., and B. Palter, “Layer Two Tunneling Protocol "L2TP",” August 1999.) [RFC2661]) that can operate over multiple transports. It MAY be used in an authorization request as a hint to the server that a specific medium is desired, but the server is not required to honor the hint in the corresponding response.

The supported values are listed in [RADIUSTypes] (IANA, “RADIUS Types,” .).

4.5.4. Tunnel-Client-Endpoint AVP

TOC

The Tunnel-Client-Endpoint AVP (AVP Code 66) is of type UTF8String and contains the address of the initiator end of the tunnel. It MAY be used in an authorization request as a hint to the server that a specific endpoint is desired, but the server is not required to honor the hint in the corresponding response. This AVP SHOULD be included in the corresponding ACR messages, in which case it indicates the address from which the tunnel was initiated. This AVP, along with the Tunnel-Server-Endpoint (Section 4.5.5 (Tunnel-Server-Endpoint AVP)) and Session-Id AVPs ([I-D.ietf-dime-rfc3588bis] (Fajardo, V., Arkko, J., Loughney, J., and G. Zorn, “Diameter Base Protocol,” April 2010.), Section 8.8), can be used to provide a globally unique means to identify a tunnel for accounting and auditingpurposes.

If the value of the Tunnel-Medium-Type AVP (Section 4.5.3 (Tunnel-Medium-Type AVP)) is IPv4 (1), then this string is either the fully qualified domain name (FQDN) of the tunnel client machine, or a "dotted-decimal" IP address. Implementations MUST support the dotted-decimal format and SHOULD support the FQDN format for IP addresses.

If Tunnel-Medium-Type is IPv6 (2), then this string is either the FQDN of the tunnel client machine, or a text representation of the address in either the preferred or alternate form [RFC3516] (Nerenberg, L., “IMAP4 Binary Content Extension,” April 2003.). Conforming implementations MUST support the preferred form and SHOULD support both the alternate text form and the FQDN format for IPv6 addresses.

If Tunnel-Medium-Type is neither IPv4 nor IPv6, then this string is a tag referring to configuration data local to the Diameter client that describes the interface or medium-specific client address to use.

4.5.5. Tunnel-Server-Endpoint AVP

TOC

The Tunnel-Server-Endpoint AVP (AVP Code 67) is of type UTF8String and contains the address of the server end of the tunnel. It MAY be used in an authorization request as a hint to the server that a specific endpoint is desired, but the server is not required to honor the hint in the corresponding response.

This AVP SHOULD be included in the corresponding ACR messages, in which case it indicates the address from which the tunnel was initiated. This AVP, along with the Tunnel-Client-Endpoint (Section 4.5.4 (Tunnel-Client-Endpoint AVP)) and Session-Id AVP ([I-D.ietf-dime-rfc3588bis] (Fajardo, V., Arkko, J., Loughney, J., and G. Zorn, "Diameter Base Protocol," April 2010.), Section 8.8), can be used to provide a globally unique means to identify a tunnel for accounting and auditing purposes.

If Tunnel-Medium-Type is IPv4 (1), then this string is either the fully qualified domain name (FQDN) of the tunnel server machine, or a "dotted-decimal" IP address. Implementations MUST support the dotted-decimal format and SHOULD support the FQDN format for IP addresses.

If Tunnel-Medium-Type is IPv6 (2), then this string is either the FQDN of the tunnel server machine, or a text representation of the address in either the preferred or alternate form [RFC3516] (Nerenberg, L., "IMAP4 Binary Content Extension," April 2003.). Implementations MUST support the preferred form and SHOULD support both the alternate text form and the FQDN format for IPv6 addresses.

If Tunnel-Medium-Type is not IPv4 or IPv6, this string is a tag referring to configuration data local to the Diameter client that describes the interface or medium-specific server address to use.

4.5.6. Tunnel-Password AVP

TOC

The Tunnel-Password AVP (AVP Code 69) is of type OctetString and may contain a password to be used to authenticate to a remote server.

The Tunnel-Password AVP contains sensitive information. This value is not protected in the same manner as RADIUS [RFC2868] (Zorn, G., Leifer, D., Rubens, A., Shriver, J., Holdrege, M., and I. Goyret, "RADIUS Attributes for Tunnel Protocol Support," June 2000.). Diameter messages are secured by using IPsec or TLS [I-D.ietf-dime-rfc3588bis] (Fajardo, V., Arkko, J., Loughney, J., and G. Zorn, "Diameter Base Protocol," April 2010.). The Tunnel-Password AVP SHOULD NOT be used in untrusted proxy environments without encrypting it by using end-to-end security techniques.

4.5.7. Tunnel-Private-Group-Id AVP

TOC

The Tunnel-Private-Group-Id AVP (AVP Code 81) is of type OctetString and contains the group Id for a particular tunneled session. The

Tunnel-Private-Group-Id AVP MAY be included in an authorization request if the tunnel initiator can predetermine the group resulting from a particular connection. It SHOULD be included in the authorization response if this tunnel session is to be treated as belonging to a particular private group. Private groups may be used to associate a tunneled session with a particular group of users. For example, it MAY be used to facilitate routing of unregistered IP addresses through a particular interface. This AVP SHOULD be included in the ACR messages that pertain to the tunneled session.

4.5.8. Tunnel-Assignment-Id AVP

TOC

The Tunnel-Assignment-Id AVP (AVP Code 82) is of type OctetString and is used to indicate to the tunnel initiator the particular tunnel to which a session is to be assigned. Some tunneling protocols, such as PPTP [RFC2637] (Hamzeh, K., Pall, G., Verthein, W., Taarud, J., Little, W., and G. Zorn, “Point-to-Point Tunneling Protocol,” July 1999.) and L2TP [RFC2661] (Townsley, W., Valencia, A., Rubens, A., Pall, G., Zorn, G., and B. Palter, “Layer Two Tunneling Protocol "L2TP",” August 1999.), allow for sessions between the same two tunnel endpoints to be multiplexed over the same tunnel and also for a given session to use its own dedicated tunnel. This attribute provides a mechanism for Diameter to inform the tunnel initiator (e.g., PAC, LAC) whether to assign the session to a multiplexed tunnel or to a separate tunnel. Furthermore, it allows for sessions sharing multiplexed tunnels to be assigned to different multiplexed tunnels.

A particular tunneling implementation may assign differing characteristics to particular tunnels. For example, different tunnels may be assigned different QoS parameters. Such tunnels may be used to carry either individual or multiple sessions. The Tunnel-Assignment-Id attribute thus allows the Diameter server to indicate that a particular session is to be assigned to a tunnel providing an appropriate level of service. It is expected that any QoS-related Diameter tunneling attributes defined in the future accompanying this one will be associated by the tunnel initiator with the Id given by this attribute. In the meantime, any semantic given to a particular Id string is a matter left to local configuration in the tunnel initiator.

The Tunnel-Assignment-Id AVP is of significance only to Diameter and the tunnel initiator. The Id it specifies is only intended to be of local use to Diameter and the tunnel initiator. The Id assigned by the tunnel initiator is not conveyed to the tunnel peer.

This attribute MAY be included in authorization responses. The tunnel initiator receiving this attribute MAY choose to ignore it and to assign the session to an arbitrary multiplexed or non-multiplexed

tunnel between the desired endpoints. This AVP SHOULD also be included in the Accounting-Request messages pertaining to the tunneled session.

If a tunnel initiator supports the Tunnel-Assignment-Id AVP, then it should assign a session to a tunnel in the following manner:

- If this AVP is present and a tunnel exists between the specified endpoints with the specified Id, then the session should be assigned to that tunnel.

- If this AVP is present and no tunnel exists between the specified endpoints with the specified Id, then a new tunnel should be established for the session and the specified Id should be associated with the new tunnel.

- If this AVP is not present, then the session is assigned to an unnamed tunnel. If an unnamed tunnel does not yet exist between the specified endpoints, then it is established and used for this session and for subsequent ones established without the Tunnel-Assignment-Id attribute. A tunnel initiator MUST NOT assign a session for which a Tunnel-Assignment-Id AVP was not specified to a named tunnel (i.e., one that was initiated by a session specifying this AVP).

Note that the same Id may be used to name different tunnels if these tunnels are between different endpoints.

4.5.9. Tunnel-Preference AVP

TOC

The Tunnel-Preference AVP (AVP Code 83) is of type Unsigned32 and is used to identify the relative preference assigned to each tunnel when more than one set of tunneling AVPs is returned within separate Grouped-AVP AVPs. It MAY be used in an authorization request as a hint to the server that a specific preference is desired, but the server is not required to honor the hint in the corresponding response.

For example, suppose that AVPs describing two tunnels are returned by the server, one with a Tunnel-Type of PPTP and the other with a Tunnel-Type of L2TP. If the tunnel initiator supports only one of the Tunnel-Types returned, it will initiate a tunnel of that type. If, however, it supports both tunnel protocols, it SHOULD use the value of the Tunnel-Preference AVP to decide which tunnel should be started. The tunnel with the lowest numerical value in the Value field of this AVP SHOULD be given the highest preference. The values assigned to two or more instances of the Tunnel-Preference AVP within a given authorization response MAY be identical. In this case, the tunnel initiator SHOULD use locally configured metrics to decidewhich set of AVPs to use.

4.5.10. Tunnel-Client-Auth-Id AVP

TOC

The Tunnel-Client-Auth-Id AVP (AVP Code 90) is of type UTF8String and specifies the name used by the tunnel initiator during the authentication phase of tunnel establishment. It MAY be used in an authorization request as a hint to the server that a specific preference is desired, but the server is not required to honor the hint in the corresponding response. This AVP MUST be present in the authorization response if an authentication name other than the default is desired. This AVP SHOULD be included in the ACR messages pertaining to the tunneled session.

4.5.11. Tunnel-Server-Auth-Id AVP

TOC

The Tunnel-Server-Auth-Id AVP (AVP Code 91) is of type UTF8String and specifies the name used by the tunnel terminator during the authentication phase of tunnel establishment. It MAY be used in an authorization request as a hint to the server that a specific preference is desired, but the server is not required to honor the hint in the corresponding response. This AVP MUST be present in the authorization response if an authentication name other than the default is desired. This AVP SHOULD be included in the ACR messages pertaining to the tunneled session.

4.6. NAS Accounting AVPs

TOC

Applications implementing this specification use Diameter Accounting (as defined in [I-D.ietf-dime-rfc3588bis] (Fajardo, V., Arkko, J., Loughney, J., and G. Zorn, “Diameter Base Protocol,” April 2010.)) and the AVPs in the following section. Service-specific AVP usage is defined in the tables in Section 5 (AVP Occurrence Tables).

If accounting is active, Accounting Request (ACR) messages SHOULD be sent after the completion of any Authentication or Authorization transaction and at the end of a Session. The value of the Accounting-Record-Type AVP [I-D.ietf-dime-rfc3588bis] (Fajardo, V., Arkko, J., Loughney, J., and G. Zorn, “Diameter Base Protocol,” April 2010.) indicates the type of event. All other AVPs identify the session and provide additional information relevant to the event.

The successful completion of the first Authentication or Authorization transaction SHOULD cause a START_RECORD to be sent. If additional Authentications or Authorizations occur in later transactions, the first exchange should generate a START_RECORD, and the later an INTERIM_RECORD. For a given session, there MUST only be one set of matching START and STOP records, with any number of INTERIM_RECORDS in between, or one EVENT_RECORD indicating the reason a session wasn't started.

The following table gives the possible flag values for the session level AVPs and specifies whether the AVP MAY be encrypted.

		AVP Flag rules				
Attribute Name	Section Defined	MUST	MAY	SHLD NOT	MUST NOT	Encr
Accounting-Input-Octets	4.6.1	M	P		V	Y
Accounting-Output-Octets	4.6.2	M	P		V	Y
Accounting-Input-Packets	4.6.3	M	P		V	Y
Accounting-Output-Packets	4.6.4	M	P		V	Y
Acct-Session-Time	4.6.5	M	P		V	Y
Acct-Authentic	4.6.6	M	P		V	Y
Accounting-Auth-Method	4.6.7	M	P		V	Y
Acct-Delay-Time	4.6.8	M	P		V	Y
Acct-Link-Count	4.6.9	M	P		V	Y
Acct-Tunnel-Connection	4.6.10	M	P		V	Y
Acct-Tunnel-Packets-Lost	4.6.11	M	P		V	Y

4.6.1. Accounting-Input-Octets AVP

TOC

The Accounting-Input-Octets AVP (AVP Code 363) is of type Unsigned64 and contains the number of octets received from the user.

For NAS usage, this AVP indicates how many octets have been received from the port in the course of this session. It can only be present in ACR messages with an Accounting-Record-Type [I-D.ietf-dime-rfc3588bis] (Fajardo, V., Arkko, J., Loughney, J., and G. Zorn, “Diameter Base Protocol,” April 2010.) of INTERIM_RECORD or STOP_RECORD.

TOC

4.6.2. Accounting-Output-Octets AVP

The Accounting-Output-Octets AVP (AVP Code 364) is of type Unsigned64 and contains the number of octets sent to the user.

For NAS usage, this AVP indicates how many octets have been sent to the port in the course of this session. It can only be present in ACR messages with an Accounting-Record-Type of INTERIM_RECORD or STOP_RECORD.

4.6.3. Accounting-Input-Packets AVP

TOC

The Accounting-Input-Packets (AVP Code 365) is of type Unsigned64 and contains the number of packets received from the user.

For NAS usage, this AVP indicates how many packets have been received from the port over the course of a session being provided to a Framed User. It can only be present in ACR messages with an Accounting-Record-Type of INTERIM_RECORD or STOP_RECORD.

4.6.4. Accounting-Output-Packets AVP

TOC

The Accounting-Output-Packets (AVP Code 366) is of type Unsigned64 and contains the number of IP packets sent to the user.

For NAS usage, this AVP indicates how many packets have been sent to the port over the course of a session being provided to a Framed User. It can only be present in ACR messages with an Accounting-Record-Type of INTERIM_RECORD or STOP_RECORD.

4.6.5. Acct-Session-Time AVP

TOC

The Acct-Session-Time AVP (AVP Code 46) is of type Unsigned32 and indicates the length of the current session in seconds. It can only be present in ACR messages with an Accounting-Record-Type of INTERIM_RECORD or STOP_RECORD.

TOC

4.6.6. Acct-Authentic AVP

The Acct-Authentic AVP (AVP Code 45) is of type Enumerated and specifies how the user was authenticated. The supported values are listed in [RADIUSTypes] (IANA, "RADIUS Types," .).

4.6.7. Accounting-Auth-Method AVP

TOC

The Accounting-Auth-Method AVP (AVP Code 406) is of type Enumerated. A NAS MAY include this AVP in an Accounting-Request message to indicate the method used to authenticate the user. (Note that this AVP is semantically equivalent, and the supported values are identical, to the Microsoft MS-Acct-Auth-Type vendor-specific RADIUS attribute [RFC2548] (Zorn, G., "Microsoft Vendor-specific RADIUS Attributes," March 1999.)).

4.6.8. Acct-Delay-Time AVP

TOC

The Acct-Delay-Time AVP (AVP Code 41) is of type Unsigned32 and indicates the number of seconds the Diameter client has been trying to send the Accounting-Request (ACR). The accounting server may subtract this value from the time when the ACR arrives at the server to calculate the approximate time of the event that caused the ACR to be generated.

This AVP is not used for retransmissions at the transport level (TCP or SCTP). Rather, it may be used when an ACR command cannot be transmitted because there is no appropriate peer to transmit it to or was rejected because it could not be delivered. In these cases, the command MAY be buffered and transmitted later, when an appropriate peer-connection is available or after sufficient time has passed that the destination-host may be reachable and operational. If the ACR is re-sent in this way, the Acct-Delay-Time AVP SHOULD be included. The value of this AVP indicates the number of seconds that elapsed between the time of the first attempt at transmission and the current attempt.

4.6.9. Acct-Link-Count AVP

TOC

The Acct-Link-Count AVP (AVP Code 51) is of type Unsigned32 and indicates the total number of links that have been active (current or closed) in a given multilink session at the time the accounting record

is generated. This AVP MAY be included in Accounting-Requests for any session that may be part of a multilink service.

The Acct-Link-Count AVP may be used to make it easier for an accounting server to know when it has all the records for a given multilink service. When the number of Accounting-Requests received with Accounting-Record-Type = STOP_RECORD and with the same Acct-Multi-Session-Id and unique Session-Ids equals the largest value of Acct-Link-Count seen in those Accounting-Requests, all STOP_RECORD Accounting-Requests for that multilink service have been received.

The following example, showing eight Accounting-Requests, illustrates how the Acct-Link-Count AVP is used. In the table below, only the relevant AVPs are shown, although additional AVPs containing accounting information will be present in the Accounting-Requests.

Acct-Multi-Session-Id	Session-Id	Accounting-Record-Type	Acct-Link-Count
"...10"	"...10"	START_RECORD	1
"...10"	"...11"	START_RECORD	2
"...10"	"...11"	STOP_RECORD	2
"...10"	"...12"	START_RECORD	3
"...10"	"...13"	START_RECORD	4
"...10"	"...12"	STOP_RECORD	4
"...10"	"...13"	STOP_RECORD	4
"...10"	"...10"	STOP_RECORD	4

4.6.10. Acct-Tunnel-Connection AVP

TOC

The Acct-Tunnel-Connection AVP (AVP Code 68) is of type OctetString and contains the identifier assigned to the tunnel session. This AVP, along with the Tunnel-Client-Endpoint (Section 4.5.4 (Tunnel-Client-Endpoint AVP)) and Tunnel-Server-Endpoint (Section 4.5.5 (Tunnel-Server-Endpoint AVP)) AVPs, may be used to provide a means to uniquely identify a tunnel session for auditing purposes.

The format of the identifier in this AVP depends upon the value of the Tunnel-Type AVP (Section 4.5.2 (Tunnel-Type AVP)). For example, to identify an L2TP tunnel connection fully, the L2TP Tunnel Id and Call Id might be encoded in this field. The exact encoding of this field is implementation dependent.

TOC

4.6.11. Acct-Tunnel-Packets-Lost AVP

The Acct-Tunnel-Packets-Lost AVP (AVP Code 86) is of type Unsigned32 and contains the number of packets lost on a given tunnel.

---

5. AVP Occurrence Tables

TOC

The following tables present the AVPs used by NAS applications in NAS messages and specify in which Diameter messages they MAY or MAY NOT be present. Messages and AVPs defined in the base Diameter protocol [I-D.ietf-dime-rfc3588bis] (Fajardo, V., Arkko, J., Loughney, J., and G. Zorn, "Diameter Base Protocol," April 2010.) are not described in this document. Note that AVPs that can only be present within a Grouped AVP are not represented in this table.

The table uses the following symbols:

> **0** The AVP MUST NOT be present in the message.
>
> **0+** Zero or more instances of the AVP MAY be present in the message.
>
> **0-1** Zero or one instance of the AVP MAY be present in the message.
>
> **1** Exactly one instance of the AVP MUST be present in the message.

5.1. AA-Request/Answer AVP Table

TOC

The table in this section is limited to the Command Codes defined in this specification.

	Command	
AVP Name	AAR	AAA
Acct-Interim-Interval	0	0-1
ARAP-Challenge-Response	0	0-1
ARAP-Features	0	0-1
ARAP-Password	0-1	0
ARAP-Security	0-1	0-1
ARAP-Security-Data	0+	0+
ARAP-Zone-Access	0	0-1
Auth-Application-Id	1	1
Auth-Grace-Period	0-1	0-1
Auth-Request-Type	1	1
Auth-Session-State	0-1	0-1
Authorization-Lifetime	0-1	0-1

	Command	
Attribute Name	AAR	AAA
Callback-Id	0	0-1
Callback-Number	0-1	0-1
Called-Station-Id	0-1	0
Calling-Station-Id	0-1	0
CHAP-Auth	0-1	0
CHAP-Challenge	0-1	0
Class	0	0+
Configuration-Token	0	0+
Connect-Info	0+	0
Destination-Host	0-1	0
Destination-Realm	1	0
Error-Message	0	0-1
Error-Reporting-Host	0	0-1
Failed-AVP	0+	0+
Filter-Id	0	0+
Framed-Appletalk-Link	0	0-1
Framed-Appletalk-Network	0	0+
Framed-Appletalk-Zone	0	0-1
Framed-Compression	0+	0+
Framed-Interface-Id	0-1	0-1
Framed-IP-Address	0-1	0-1
Framed-IP-Netmask	0-1	0-1
Framed-IPv6-Prefix	0+	0+
Framed-IPv6-Pool	0	0-1
Framed-IPv6-Route	0	0+
Framed-IPX-Network	0	0-1
Framed-MTU	0-1	0-1
Framed-Pool	0	0-1
Framed-Protocol	0-1	0-1
Framed-Route	0	0+
Framed-Routing	0	0-1
Idle-Timeout	0	0-1
Login-IP-Host	0+	0+
Login-IPv6-Host	0+	0+
Login-LAT-Group	0-1	0-1
Login-LAT-Node	0-1	0-1
Login-LAT-Port	0-1	0-1
Login-LAT-Service	0-1	0-1
Login-Service	0	0-1
Login-TCP-Port	0	0-1
Multi-Round-Time-Out	0	0-1

	Command	
Attribute Name	AAR	AAA
NAS-Filter-Rule	0	0+
NAS-Identifier	0-1	0
NAS-IP-Address	0-1	0
NAS-IPv6-Address	0-1	0
NAS-Port	0-1	0
NAS-Port-Id	0-1	0
NAS-Port-Type	0-1	0
Origin-AAA-Protocol	0-1	0-1
Origin-Host	1	1
Origin-Realm	1	1
Origin-State-Id	0-1	0-1
Originating-Line-Info	0-1	0
Password-Retry	0	0-1
Port-Limit	0-1	0-1
Prompt	0	0-1
Proxy-Info	0+	0+
QoS-Filter-Rule	0	0+
Re-Auth-Request-Type	0	0-1
Redirect-Host	0	0+
Redirect-Host-Usage	0	0-1
Redirect-Max-Cache-Time	0	0-1
Reply-Message	0	0+
Result-Code	0	1
Route-Record	0+	0+
Service-Type	0-1	0-1
Session-Id	1	1
Session-Timeout	0	0-1
State	0-1	0-1
Tunneling	0+	0+
User-Name	0-1	0-1
User-Password	0-1	0

5.2. Accounting AVP Tables

TOC

The tables in this section are used to show which AVPs defined in this document are to be present and used in NAS application Accounting messages. These AVPs are defined in this document, as well as in [I-D.ietf-dime-rfc3588bis] (Fajardo, V., Arkko, J., Loughney, J., and

G. Zorn, “Diameter Base Protocol,” April 2010.) and [RFC2866] (Rigney, C., “RADIUS Accounting,” June 2000.).

5.2.1. Framed Access Accounting AVP Table

TOC

The table in this section is used when the Service-Type AVP (Section 4.4.1 (Service-Type AVP)) specifies Framed Access.

	Command	
Attribute Name	ACR	ACA
Accounting-Auth-Method	0-1	0
Accounting-Input-Octets	1	0
Accounting-Input-Packets	1	0
Accounting-Output-Octets	1	0
Accounting-Output-Packets	1	0
Accounting-Record-Number	0-1	0-1
Accounting-Record-Type	1	1
Accounting-Realtime-Required	0-1	0-1
Accounting-Sub-Session-Id	0-1	0-1
Acct-Application-Id	0-1	0-1
Acct-Session-Id	1	0-1
Acct-Multi-Session-Id	0-1	0-1
Acct-Authentic	1	0
Acct-Delay-Time	0-1	0
Acct-Interim-Interval	0-1	0-1
Acct-Link-Count	0-1	0
Acct-Session-Time	1	0
Acct-Tunnel-Connection	0-1	0
Acct-Tunnel-Packets-Lost	0-1	0
Authorization-Lifetime	0-1	0
Callback-Id	0-1	0
Callback-Number	0-1	0
Called-Station-Id	0-1	0
Calling-Station-Id	0-1	0
Class	0+	0+
Connection-Info	0+	0
Destination-Host	0-1	0
Destination-Realm	1	0
Event-Timestamp	0-1	0-1
Error-Message	0	0-1
Error-Reporting-Host	0	0-1
Failed-AVP	0	0+

	Command	
Attribute Name	ACR	ACA
Framed-AppleTalk-Link	0-1	0
Framed-AppleTalk-Network	0-1	0
Framed-AppleTalk-Zone	0-1	0
Framed-Compression	0-1	0
Framed-IP-Address	0-1	0
Framed-IP-Netmask	0-1	0
Framed-IPv6-Prefix	0+	0
Framed-IPv6-Pool	0-1	0
Framed-IPX-Network	0-1	0
Framed-MTU	0-1	0
Framed-Pool	0-1	0
Framed-Protocol	0-1	0
Framed-Route	0-1	0
Framed-Routing	0-1	0
NAS-Filter-Rule	0+	0
NAS-Identifier	0-1	0-1
NAS-IP-Address	0-1	0-1
NAS-IPv6-Address	0-1	0-1
NAS-Port	0-1	0-1
NAS-Port-Id	0-1	0-1
NAS-Port-Type	0-1	0-1
Origin-AAA-Protocol	0-1	0-1
Origin-Host	1	1
Origin-Realm	1	1
Origin-State-Id	0-1	0-1
Originating-Line-Info	0-1	0
Proxy-Info	0+	0+
QoS-Filter-Rule	0+	0
Route-Record	0+	0+
Result-Code	0	1
Service-Type	0-1	0-1
Session-Id	1	1
Termination-Cause	0-1	0-1
Tunnel-Assignment-Id	0-1	0
Tunnel-Client-Endpoint	0-1	0
Tunnel-Medium-Type	0-1	0
Tunnel-Private-Group-Id	0-1	0
Tunnel-Server-Endpoint	0-1	0
Tunnel-Type	0-1	0
User-Name	0-1	0-1
Vendor-Specific-Application-Id	0-1	0-1

5.2.2. Non-Framed Access Accounting AVP Table

TOC

The table in this section is used when the Service-Type AVP (Section 4.4.1 (Service-Type AVP)) specifies Non-Framed Access.

	Command	
Attribute Name	ACR	ACA
Accounting-Auth-Method	0-1	0
Accounting-Input-Octets	1	0
Accounting-Output-Octets	1	0
Accounting-Record-Type	1	1
Accounting-Record-Number	0-1	0-1
Accounting-Realtime-Required	0-1	0-1
Accounting-Sub-Session-Id	0-1	0-1
Acct-Application-Id	0-1	0-1
Acct-Session-Id	1	0-1
Acct-Multi-Session-Id	0-1	0-1
Acct-Authentic	1	0
Acct-Delay-Time	0-1	0
Acct-Interim-Interval	0-1	0-1
Acct-Link-Count	0-1	0
Acct-Session-Time	1	0
Authorization-Lifetime	0-1	0
Callback-Id	0-1	0
Callback-Number	0-1	0
Called-Station-Id	0-1	0
Calling-Station-Id	0-1	0
Class	0+	0+
Connection-Info	0+	0
Destination-Host	0-1	0
Destination-Realm	1	0
Event-Timestamp	0-1	0-1
Error-Message	0	0-1
Error-Reporting-Host	0	0-1
Failed-AVP	0	0+
Login-IP-Host	0+	0
Login-IPv6-Host	0+	0
Login-LAT-Service	0-1	0
Login-LAT-Node	0-1	0
Login-LAT-Group	0-1	0
Login-LAT-Port	0-1	0
Login-Service	0-1	0
Login-TCP-Port	0-1	0

	Command	
Attribute Name	ACR	ACA
NAS-Identifier	0-1	0-1
NAS-IP-Address	0-1	0-1
NAS-IPv6-Address	0-1	0-1
NAS-Port	0-1	0-1
NAS-Port-Id	0-1	0-1
NAS-Port-Type	0-1	0-1
Origin-AAA-Protocol	0-1	0-1
Origin-Host	1	1
Origin-Realm	1	1
Origin-State-Id	0-1	0-1
Originating-Line-Info	0-1	0
Proxy-Info	0+	0+
QoS-Filter-Rule	0+	0
Route-Record	0+	0+
Result-Code	0	1
Session-Id	1	1
Service-Type	0-1	0-1
Termination-Cause	0-1	0-1
User-Name	0-1	0-1
Vendor-Specific-Application-Id	0-1	0-1

6. IANA Considerations

TOC

This section provides guidance to the Internet Assigned Numbers Authority (IANA) regarding registration of values related to the Diameter protocol, in accordance with BCP 26 [RFC5226] (Narten, T. and H. Alvestrand, “Guidelines for Writing an IANA Considerations Section in RFCs,” May 2008.).

This document defines values in the namespaces that have been created and defined in the Diameter Base [I-D.ietf-dime-rfc3588bis] (Fajardo, V., Arkko, J., Loughney, J., and G. Zorn, “Diameter Base Protocol,” April 2010.). The IANA Considerations section of that document details the assignment criteria. Values assigned in this document, or by future IANA action, must be coordinated within this shared namespace.

TOC

6.1. Command Codes

This specification assigns the value 265 from the Command Code namespace defined in [I-D.ietf-dime-rfc3588bis] (Fajardo, V., Arkko, J., Loughney, J., and G. Zorn, "Diameter Base Protocol," April 2010.). See Sections 3.1 and 3.2 for the assignment of the namespace in this specification.

6.2. AVP Codes

TOC

This specification assigns the values 363 - 366 and 400 - 408 from the AVP Code namespace defined in [I-D.ietf-dime-rfc3588bis] (Fajardo, V., Arkko, J., Loughney, J., and G. Zorn, "Diameter Base Protocol," April 2010.). See Section 4 (Diameter NAS Application AVPs) for the assignment of the namespace in this specification. Note that the values 363 - 366 are jointly, but consistently, assigned in [RFC4004] (Calhoun, P., Johansson, T., Perkins, C., Hiller, T., and P. McCann, "Diameter Mobile IPv4 Application," August 2005.). This document also creates one new namespace to be managed by IANA, as described in Section 6.5 (Accounting-Auth-Method AVP Values)

This specification also specifies the use of AVPs in the 0 - 255 range, which are listed in [RADIUSTypes] (IANA, "RADIUS Types," .) These values are assigned according to the policy stated in Section 6 of (Rigney, C., Willens, S., Rubens, A., and W. Simpson, "Remote Authentication Dial In User Service (RADIUS)," June 2000.) [RFC2865], as amended by (Aboba, B., "IANA Considerations for RADIUS (Remote Authentication Dial In User Service)," July 2003.) [RFC3575].

6.3. Application Identifier

TOC

This specification uses the value one (1) in the Application Identifier namespace as assigned in [I-D.ietf-dime-rfc3588bis] (Fajardo, V., Arkko, J., Loughney, J., and G. Zorn, "Diameter Base Protocol," April 2010.). See Section 1.3 (Advertising Application Support) above for more information.

6.4. CHAP-Algorithm AVP Values

TOC

As defined in Section 4.3.4 (CHAP-Auth AVP), the CHAP-Algorithm AVP (AVP Code 403) uses the values of the "PPP AUTHENTICATION ALGORITHMS"

namespace defined in [RFC1994] (Simpson, W., “PPP Challenge Handshake Authentication Protocol (CHAP),” August 1996.).

6.5. Accounting-Auth-Method AVP Values

TOC

As defined in Section 4.6.7 (Accounting-Auth-Method AVP) the Accounting-Auth-Method AVP (AVP Code 406) defines the values 1 - 5. All remaining values are available for assignment via the IETF Review policy [RFC5226] (Narten, T. and H. Alvestrand, “Guidelines for Writing an IANA Considerations Section in RFCs,” May 2008.).

---

7. Security Considerations

TOC

This document describes the extension of Diameter for the NAS application. The security considerations of the Diameter protocol itself have been discussed in [I-D.ietf-dime-rfc3588bis] (Fajardo, V., Arkko, J., Loughney, J., and G. Zorn, “Diameter Base Protocol,” April 2010.). Use of this application of Diameter MUST take into consideration the security issues and requirements of the Base protocol.

This document does not contain a security protocol but does discuss how PPP authentication protocols can be carried within the Diameter protocol. The PPP authentication protocols described are PAP and CHAP.

The use of PAP SHOULD be discouraged, as it exposes users' passwords to possibly non-trusted entities. However, PAP is also frequently used for use with One-Time Passwords, which do not expose a security risk.

This document also describes how CHAP can be carried within the Diameter protocol, which is required for RADIUS backward compatibility. The CHAP protocol, as used in a RADIUS environment, facilitates authentication replay attacks.

The use of the EAP authentication protocols [RFC4072] (Eronen, P., Hiller, T., and G. Zorn, “Diameter Extensible Authentication Protocol (EAP) Application,” August 2005.) can offer better security, given a method suitable for the circumstances.

---

8. References

TOC

8.1. Normative References

TOC

[ANITypes]	NANPA Number Resource Info, “ANI Assignments.”
[I-D.ietf-dime-rfc3588bis]	Fajardo, V., Arkko, J., Loughney, J., and G. Zorn, “Diameter Base Protocol,” draft-ietf-dime-rfc3588bis-20 (work in progress), April 2010 (TXT).
[RADIUSTypes]	IANA, “RADIUS Types.”
[RFC1994]	Simpson, W., “PPP Challenge Handshake Authentication Protocol (CHAP),” RFC 1994, August 1996 (TXT).
[RFC2119]	Bradner, S., “Key words for use in RFCs to Indicate Requirement Levels,” BCP 14, RFC 2119, March 1997 (TXT, HTML, XML).
[RFC2865]	Rigney, C., Willens, S., Rubens, A., and W. Simpson, “Remote Authentication Dial In User Service (RADIUS),” RFC 2865, June 2000 (TXT).
[RFC3162]	Aboba, B., Zorn, G., and D. Mitton, “RADIUS and IPv6,” RFC 3162, August 2001 (TXT).
[RFC3516]	Nerenberg, L., “IMAP4 Binary Content Extension,” RFC 3516, April 2003 (TXT).
[RFC3539]	Aboba, B. and J. Wood, “Authentication, Authorization and Accounting (AAA) Transport Profile,” RFC 3539, June 2003 (TXT).
[RFC5226]	Narten, T. and H. Alvestrand, “Guidelines for Writing an IANA Considerations Section in RFCs,” BCP 26, RFC 5226, May 2008 (TXT).

8.2. Informative References

TOC

[ARAP]	Apple Computer, “Apple Remote Access Protocol (ARAP) Version 2.0 External Reference Specification,” R0612LL/B , September 1994.
[AppleTalk]	Sidhu, G., Andrews, R., and A. Oppenheimer, “Inside AppleTalk,” Second Edition Apple Computer, 1990.
[IPX]	Novell, Inc., “NetWare System Technical Interface Overview,” #883-000780-001, June 1989.
[ISO. 8859-1.1987]	International Organization for Standardization, “Information technology - 8-bit single byte coded graphic - character sets - Part 1: Latin alphabet No. 1, JTC1/SC2,” ISO Standard 8859-1, 1987.
[LAT]	Digital Equipment Corp., “Local Area Transport (LAT) Specification V5.0,” AA-NL26A-TE, June 1989.
[RFC1334]	Lloyd, B. and W. Simpson, “PPP Authentication Protocols,” RFC 1334, October 1992 (TXT).

[RFC1661]	Simpson, W., "The Point-to-Point Protocol (PPP)," STD 51, RFC 1661, July 1994 (TXT).
[RFC1990]	Sklower, K., Lloyd, B., McGregor, G., Carr, D., and T. Coradetti, "The PPP Multilink Protocol (MP)," RFC 1990, August 1996 (TXT).
[RFC2474]	Nichols, K., Blake, S., Baker, F., and D. Black, "Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers," RFC 2474, December 1998 (TXT, HTML, XML).
[RFC2548]	Zorn, G., "Microsoft Vendor-specific RADIUS Attributes," RFC 2548, March 1999 (TXT).
[RFC2597]	Heinanen, J., Baker, F., Weiss, W., and J. Wroclawski, "Assured Forwarding PHB Group," RFC 2597, June 1999 (TXT).
[RFC2637]	Hamzeh, K., Pall, G., Verthein, W., Taarud, J., Little, W., and G. Zorn, "Point-to-Point Tunneling Protocol," RFC 2637, July 1999 (TXT).
[RFC2661]	Townsley, W., Valencia, A., Rubens, A., Pall, G., Zorn, G., and B. Palter, "Layer Two Tunneling Protocol "L2TP"," RFC 2661, August 1999 (TXT).
[RFC2866]	Rigney, C., "RADIUS Accounting," RFC 2866, June 2000 (TXT).
[RFC2867]	Zorn, G., Aboba, B., and D. Mitton, "RADIUS Accounting Modifications for Tunnel Protocol Support," RFC 2867, June 2000 (TXT).
[RFC2868]	Zorn, G., Leifer, D., Rubens, A., Shriver, J., Holdrege, M., and I. Goyret, "RADIUS Attributes for Tunnel Protocol Support," RFC 2868, June 2000 (TXT).
[RFC2869]	Rigney, C., Willats, W., and P. Calhoun, "RADIUS Extensions," RFC 2869, June 2000 (TXT).
[RFC2881]	Mitton, D. and M. Beadles, "Network Access Server Requirements Next Generation (NASREQNG) NAS Model," RFC 2881, July 2000 (TXT).
[RFC2989]	Aboba, B., Calhoun, P., Glass, S., Hiller, T., McCann, P., Shiino, H., Zorn, G., Dommety, G., C.Perkins, B.Patil, D.Mitton, S.Manning, M.Beadles, P.Walsh, X.Chen, S.Sivalingham, A.Hameed, M.Munson, S.Jacobs, B.Lim, B.Hirschman, R.Hsu, Y.Xu, E.Campell, S.Baba, and E.Jaques, "Criteria for Evaluating AAA Protocols for Network Access," RFC 2989, November 2000 (TXT).
[RFC3169]	Beadles, M. and D. Mitton, "Criteria for Evaluating Network Access Server Protocols," RFC 3169, September 2001 (TXT).
[RFC3246]	Davie, B., Charny, A., Bennet, J., Benson, K., Le Boudec, J., Courtney, W., Davari, S., Firoiu, V., and D. Stiliadis, "An Expedited Forwarding PHB (Per-Hop Behavior)," RFC 3246, March 2002 (TXT).
[RFC3575]	

	Aboba, B., "IANA Considerations for RADIUS (Remote Authentication Dial In User Service)," RFC 3575, July 2003 (TXT).
[RFC3580]	Congdon, P., Aboba, B., Smith, A., Zorn, G., and J. Roese, "IEEE 802.1X Remote Authentication Dial In User Service (RADIUS) Usage Guidelines," RFC 3580, September 2003 (TXT).
[RFC4004]	Calhoun, P., Johansson, T., Perkins, C., Hiller, T., and P. McCann, "Diameter Mobile IPv4 Application," RFC 4004, August 2005 (TXT).
[RFC4072]	Eronen, P., Hiller, T., and G. Zorn, "Diameter Extensible Authentication Protocol (EAP) Application," RFC 4072, August 2005 (TXT).

Appendix A. Acknowledgements

TOC

A.1. RFC 4005

TOC

The authors would like to thank Carl Rigney, Allan C. Rubens, William Allen Simpson, and Steve Willens for their work on the original RADIUS protocol, from which many of the concepts in this specification were derived. Thanks, also, to Carl Rigney for [RFC2866] (Rigney, C., "RADIUS Accounting," June 2000.) and [RFC2869] (Rigney, C., Willats, W., and P. Calhoun, "RADIUS Extensions," June 2000.); Ward Willats for [RFC2869] (Rigney, C., Willats, W., and P. Calhoun, "RADIUS Extensions," June 2000.); Glen Zorn, Bernard Aboba, and Dave Mitton for [RFC2867] (Zorn, G., Aboba, B., and D. Mitton, "RADIUS Accounting Modifications for Tunnel Protocol Support," June 2000.) and [RFC3162] (Aboba, B., Zorn, G., and D. Mitton, "RADIUS and IPv6," August 2001.); and Dory Leifer, John Shriver, Matt Holdrege, Allan Rubens, Glen Zorn and Ignacio Goyret for their work on [RFC2868] (Zorn, G., Leifer, D., Rubens, A., Shriver, J., Holdrege, M., and I. Goyret, "RADIUS Attributes for Tunnel Protocol Support," June 2000.). This document stole text and concepts from both [RFC2868] (Zorn, G., Leifer, D., Rubens, A., Shriver, J., Holdrege, M., and I. Goyret, "RADIUS Attributes for Tunnel Protocol Support," June 2000.) and [RFC2869] (Rigney, C., Willats, W., and P. Calhoun, "RADIUS Extensions," June 2000.). Thanks go to Carl Williams for providing IPv6-specific text.

The authors would also like to acknowledge the following people for their contributions in the development of the Diameter protocol: Bernard Aboba, Jari Arkko, William Bulley, Kuntal Chowdhury, Daniel C.

Fox, Lol Grant, Nancy Greene, Jeff Hagg, Peter Heitman, Paul Krumviede, Fergal Ladley, Ryan Moats, Victor Muslin, Kenneth Peirce, Sumit Vakil, John R. Vollbrecht, and Jeff Weisberg.

Finally, Pat Calhoun would like to thank Sun Microsystems, as most of the effort put into this document was done while he was in their employ.

A.2. RFC 4005bis

TOC

The vast majority of the text in this document was lifted directly fro RFC 4005; the editor owes a debt of gratitude to the authors thereof (especially Dave Mitton, who somehow managed to make nroff paginate the AVP Occurance Tables correctly!).

Author's Address

TOC

	Glen Zorn (editor)
	Network Zen
	1463 East Republican Street
	#358
	Seattle, Washington 98112
	USA
EMail:	gwz@net-zen.net