Network Working Group
Request for Comments: 4005
Category: Standards Track

P. Calhoun
G. Zorn
Cisco Systems Inc.
D. Spence
Consultant
D. Mitton
Circular Networks

August 2005

# Diameter Network Access Server Application

## Status of This Memo

This document specifies an Internet standards track protocol for the Internet community, and requests discussion and suggestions for improvements. Please refer to the current edition of the "Internet Official Protocol Standards" (STD 1) for the standardization state and status of this protocol. Distribution of this memo is unlimited.

## Copyright Notice

## 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.

Initial deployments of the Diameter protocol are expected to include legacy systems. Therefore, this application has been carefully designed to ease the burden of protocol conversion between RADIUS and Diameter. This is achieved by including the RADIUS attribute space to eliminate the need to perform many attribute translations.

The interactions between Diameter applications and RADIUS specified in this document are to be applied to all Diameter applications. In this sense, this document extends the Base Diameter protocol.

Table of Contents

## 1. Introduction

This document describes the Diameter protocol application used for AAA in the Network Access Server (NAS) environment. When combined with the Diameter Base protocol [BASE], Transport Profile [DiamTrans], and EAP [DiamEAP] specifications, this Diameter NAS application specification satisfies NAS-related requirements defined in RFC 2989 [AAACriteria] and RFC 3169 [NASCriteria].

Initial deployments of the Diameter protocol are expected to include legacy systems. Therefore, this application has been carefully designed to ease the burden of protocol conversion between RADIUS and Diameter. This is achieved by including the RADIUS attribute space to eliminate the need to perform many attribute translations.

The interactions specified in this document between Diameter applications and RADIUS are to be applied to all Diameter applications. In this sense, this document extends the Base Diameter protocol [BASE].

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. Interaction and backward compatibility issues with RADIUS are discussed in later sections.

### 1.1. Terminology

The base Diameter [BASE] specification section 1.4 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 [NASModel].

PPP (Point-to-Point Protocol) - A multiprotocol serial datalink. PPP is the primary IP datalink used for dial-in NAS connection service [PPP].

CHAP (Challenge Handshake Authentication Protocol) - An authentication process used in PPP [PPPCHAP].

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

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].

IPX (Internet Packet Exchange) - The network protocol used by NetWare networks [IPX].

LAT (Local Area Transport) - A Digital Equipment Corp. LAN protocol for terminal services [LAT].

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

### 1.2. Requirements Language

In this document, the key words "MAY", "MUST", "MUST NOT", "OPTIONAL", "RECOMMENDED", "SHOULD", and "SHOULD NOT" are to be interpreted as described in [Keywords].

### 1.3. Advertising Application Support

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

## 2. NAS Calls, Ports, and Sessions

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 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 described in section 5.6 of [RADIUS] 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.

Since no equivalent capability exists in RADIUS, authorization-only requests from a NAS implementing Diameter may not be easily translated to an equivalent RADIUS message by a Diameter/RADIUS gateway. For example, when a Diameter authorization-only request cannot be translated to a RADIUS Call Check, it would be necessary for the Diameter/RADIUS gateway to add authentication information to the RADIUS Access Request. On receiving the Access-Reply, the Diameter/RADIUS gateway would need to discard the access decision (Accept/Reject). It is not clear whether these translations can be accomplished without adding significant security vulnerabilities.

## 2.1. Diameter Session Establishment

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 [BASE]. 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 [BASE] would result in a failure to establish the session.

## 2.2. Diameter Session Reauthentication or Reauthorization

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 [BASE]. 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 [BASE]) to the NAS. Upon receipt of such a message, the NAS MUST respond to the request with a Re-Auth-Answer (RAA) message [BASE].

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 [BASE] section 9.6).

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.

## 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) [BASE] 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) [BASE] 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 [BASE] MUST be sent upon termination of the session context.

More information on Diameter Session Termination is included in [BASE] sections 8.4 and 8.5.

## 3. NAS Messages

This section defines the Diameter message Command-Code [BASE] 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 | 3.1 |
| AA-Answer | AAA | 265 | 3.2 |
| Re-Auth-Request | RAR | 258 | 3.3 |
| Re-Auth-Answer | RAA | 258 | 3.4 |
| Session-Termination-Request | STR | 275 | 3.5 |
| Session-Termination-Answer | STA | 275 | 3.6 |
| Abort-Session-Request | ASR | 274 | 3.7 |
| Abort-Session-Answer | ASA | 274 | 3.8 |
| Accounting-Request | ACR | 271 | 3.9 |
| Accounting-Answer | ACA | 271 | 3.10 |

### 3.1. AA-Request (AAR) Command

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 [BASE]. The recommended value for most RADIUS interoperabily 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 6.

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

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 6.

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

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 [BASE].

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

The Re-Auth-Answer (RAA) message [BASE] 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

The Session-Termination-Request (STR) message [BASE] 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

The Session-Termination-Answer (STA) message [BASE] 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

The Abort-Session-Request (ASR) message [BASE] 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

The ASA message [BASE] 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, Result-Code is set to DIAMETER_UNKNOWN_SESSION_ID. If the access device does not stop the session for any other reason, Result-Code 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

The ACR message [BASE] is sent by the NAS to report its session information to a target server downstream.

Either of Acct-Application-Id or Vendor-Specific-Application-Id AVPs 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 MUST be assumed to be present, as appropriate. NAS service-specific accounting AVPs SHOULD be present as described in section 8 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

The ACA message [BASE] 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 Acct-Application-Id or Vendor-Specific-Application-Id AVPs MUST be present, as it was in the request.

The AVPs listed in the Base MUST be assumed to be present, as appropriate. NAS service-specific accounting AVPs SHOULD be present as described in section 8 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. NAS Session AVPs

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.

Some RADIUS attributes are not allowed or supported directly in Diameter.  See section 9 for more information.

### 4.1. Call and Session Information

This section contains 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 Base AVPs of:

Session-Id
Auth-Application-Id
Origin-Host
Origin-Realm
Auth-Request-Type
Termination-Cause

The following table describes the session level AVPs; their AVP Code values, types, and possible flag values; and whether the AVP MAY be encrypted.

| | | | | AVP Flag rules | | | | |
|---|---|---|---|---|---|---|---|---|
| Attribute Name | AVP Code | Section Defined | Value Type | MUST | MAY | SHLD NOT | MUST NOT | Encr |
| NAS-Port | 5 | 4.2 | Unsigned32 | M | P | | V | Y |
| NAS-Port-Id | 87 | 4.3 | UTF8String | M | P | | V | Y |
| NAS-Port-Type | 61 | 4.4 | Enumerated | M | P | | V | Y |
| Called-Station-Id | 30 | 4.5 | UTF8String | M | P | | V | Y |
| Calling-Station-Id | 31 | 4.6 | UTF8String | M | P | | V | Y |
| Connect-Info | 77 | 4.7 | UTF8String | M | P | | V | Y |
| Originating-Line-Info | 94 | 4.8 | OctetString | | M,P | | V | Y |
| Reply-Message | 18 | 4.9 | UTF8String | M | P | | V | Y |

### 4.2. NAS-Port AVP

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 NAS-Port or NAS-Port-Id (AVP Code 87) SHOULD be present in AA-Request (AAR) commands if the NAS differentiates among its ports.

### 4.3. NAS-Port-Id AVP

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 NAS-Port or NAS-Port-Id SHOULD be present in AA-Request (AAR) commands if the NAS differentiates among its ports. NAS-Port-Id is intended for use by NASes that cannot conveniently number their ports.

### 4.4. NAS-Port-Type AVP

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 supported values are defined in [RADIUSTypes]. The following list is informational and subject to change by the IANA.

| | |
|---|---|
| 0 | Async |
| 1 | Sync |
| 2 | ISDN Sync |
| 3 | ISDN Async V.120 |
| 4 | ISDN Async V.110 |
| 5 | Virtual |
| 6 | PIAFS |
| 7 | HDLC Clear Channel |
| 8 | X.25 |
| 9 | X.75 |
| 10 | G.3 Fax |
| 11 | SDSL - Symmetric DSL |
| 12 | ADSL-CAP - Asymmetric DSL, Carrierless Amplitude Phase Modulation |
| 13 | ADSL-DMT - Asymmetric DSL, Discrete Multi-Tone |
| 14 | IDSL - ISDN Digital Subscriber Line |

| | |
|---|---|
| 15 | Ethernet |
| 16 | xDSL - Digital Subscriber Line of unknown type |
| 17 | Cable |
| 18 | Wireless - Other |
| 19 | Wireless - IEEE 802.11 |
| 20 | Token-Ring [RAD802.1X] |
| 21 | FDDI [RAD802.1X] |
| 22 | Wireless - CDMA2000 |
| 23 | Wireless - UMTS |
| 24 | Wireless - 1X-EV |
| 25 | IAPP [IEEE 802.11f] |

### 4.5. Called-Station-Id AVP

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 Dialed Number Identification (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 [RAD802.1X]. It SHOULD only be present in authentication and/or authorization requests.

If the Auth-Request-Type AVP is set to authorization-only and the User-Name AVP is absent, the Diameter Server MAY perform authorization based on this field. 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.

### 4.6. 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 [RAD802.1X]. It SHOULD only be present in authentication and/or authorization requests.

If the Auth-Request-Type AVP is set to authorization-only and the User-Name AVP is absent, the Diameter Server MAY perform authorization based on this field. 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.

## 4.7. Connect-Info AVP

The Connect-Info AVP (AVP Code 77) is of type UTF8String and is sent in the AA-Request message or ACR STOP message. When sent in the Access-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 the NAS modem transmits at), then a slash (/), then the receive speed, and then other optional information.

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

More than one Connect-Info attribute may be present in an Accounting-Request packet to accommodate expected efforts by the ITU to have modems report more connection information in a standard format that might exceed 252 octets.

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

## 4.8. 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 more information on current assignment values, see [ANITypes].

| Value | Description |
|---|---|
| 00 | Plain Old Telephone Service (POTS) |
| 01 | Multiparty Line (more than 2) |
| 02 | ANI Failure |
| 03 | ANI Observed |
| 04 | ONI Observed |
| 05 | ANI Failure Observed |
| 06 | Station Level Rating |
| 07 | Special Operator Handling Required |
| 08 | InterLATA Restricted |
| 10 | Test Call |
| 20 | Automatic Identified Outward Dialing (AIOD) |
| 23 | Coin or Non-Coin |
| 24 | Toll Free Service (Non-Pay Origination) |
| 25 | Toll Free Service (Pay Origination) |
| 27 | Toll Free Service (Coin Control Origination) |
| 29 | Prison/Inmate Service |
| 30-32 | Intercept |
| 30 | Intercept (Blank) |
| 31 | Intercept (Trouble) |
| 32 | Intercept (Regular) |
| 34 | Telco Operator Handled Call |
| 40-49 | Unrestricted Use |
| 52 | Outward Wide Area Telecommunications Service (OUTWATS) |
| 60 | Telecommunications Relay Service (TRS)(Unrestricted) |
| 61 | Cellular/Wireless PCS (Type 1) |
| 62 | Cellular/Wireless PCS (Type 2) |
| 63 | Cellular/Wireless PCS (Roaming) |
| 66 | TRS (Hotel) |
| 67 | TRS (Restricted) |
| 70 | Pay Station, No Coin Control |
| 93 | Access for Private Virtual Network Service |

### 4.9. Reply-Message AVP

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 indicate dialog text to prompt the user before another AA-Request attempt. When used in an AA-Answer with a Result-Code of DIAMETER_MULTI_ROUND_AUTH or in an Re-Auth-Request message, it MAY contain a dialog text to prompt the user for a response.

Multiple Reply-Messages MAY be included, and if any are displayed, they MUST be displayed in the same order as they appear in the Diameter message.

## 5. NAS Authentication AVPs

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 [BASE].

The following table describes the AVPs; their AVP Code values, types, and possible flag values, and whether the AVP MAY be encrypted.

| | | | | AVP Flag rules | | | | |
|---|---|---|---|---|---|---|---|---|
| Attribute Name | AVP Code | Section Defined | Value Type | MUST | MAY | SHLD NOT | MUST NOT | Encr |
| User-Password | 2 | 5.1 | OctetString | M | P | | V | Y |
| Password-Retry | 75 | 5.2 | Unsigned32 | M | P | | V | Y |
| Prompt | 76 | 5.3 | Enumerated | M | P | | V | Y |
| CHAP-Auth | 402 | 5.4 | Grouped | M | P | | V | Y |
| CHAP-Algorithm | 403 | 5.5 | Enumerated | M | P | | V | Y |
| CHAP-Ident | 404 | 5.6 | OctetString | M | P | | V | Y |
| CHAP-Response | 405 | 5.7 | OctetString | M | P | | V | Y |
| CHAP-Challenge | 60 | 5.8 | OctetString | M | P | | V | Y |
| ARAP-Password | 70 | 5.9 | OctetString | M | P | | V | Y |
| ARAP-Challenge-Response | 84 | 5.10 | OctetString | M | P | | V | Y |
| ARAP-Security | 73 | 5.11 | Unsigned32 | M | P | | V | Y |
| ARAP-Security-Data | 74 | 5.12 | OctetString | M | P | | V | Y |

### 5.1. User-Password AVP

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 [BASE], 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, such as the proposed CMS Security [DiamCMS].

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

### 5.2. Password-Retry AVP

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 (see section 6.10.1) is set to ARAP.

### 5.3. Prompt AVP

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]. The following list is informational:

| | |
|---|---|
| 0 | No Echo |
| 1 | Echo |

### 5.4. CHAP-Auth AVP

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) [PPPCHAP]. If the CHAP-Auth AVP is found in a message, the CHAP-Challenge AVP MUST be present as well. The optional AVPs containing the CHAP response depend upon the value of the CHAP-Algorithm AVP. The grouped AVP has the following ABNF grammar:

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

### 5.5. CHAP-Algorithm AVP

The CHAP-Algorithm AVP (AVP Code 403) is of type Enumerated and contains the algorithm identifier used in the computation of the CHAP response [PPPCHAP]. The following values are currently supported:

```
   CHAP with MD5       5
      The CHAP response is computed by using the procedure described
      in [PPPCHAP].  This algorithm requires that the CHAP-Response
      AVP MUST be present in the CHAP-Auth AVP.
```

### 5.6. CHAP-Ident AVP

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 [PPPCHAP].

### 5.7. CHAP-Response AVP

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 [PPPCHAP].

### 5.8. CHAP-Challenge AVP

The CHAP-Challenge AVP (AVP Code 60) is of type OctetString and contains the CHAP Challenge sent by the NAS to the CHAP peer [PPPCHAP].

### 5.9. ARAP-Password AVP

The ARAP-Password AVP (AVP Code 70) is of type OctetString and is only present when the Framed-Protocol AVP (see section 6.10.1) 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 [RADIUSExt] for more information on the contents of this AVP.

### 5.10. ARAP-Challenge-Response AVP

The ARAP-Challenge-Response AVP (AVP Code 84) is of type OctetString and is only present when the Framed-Protocol AVP (see section 6.10.1) 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 8 before it is used as a key.

### 5.11. ARAP-Security AVP

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 (see section 6.10.1) is set to the value of ARAP, and the Result-Code AVP is set to DIAMETER_MULTI_ROUND_AUTH. See [RADIUSExt] for more information on the format of this AVP.

### 5.12. ARAP-Security-Data AVP

The ARAP-Security 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 is set to the value of ARAP, and the Result-Code AVP is set to DIAMETER_MULTI_ROUND_AUTH. This AVP contains the security module challenge or response associated with the ARAP Security Module specified in ARAP-Security.

## 6. 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 in section 7 MAY be present.

Due to space constraints, the short-form IPFltrRule is used to represent IPFilterRule, and QoSFltrRule is used for QoSFilterRule.

| | | | | AVP Flag rules | | | | |
|---|---|---|---|---|---|---|---|---|
| Attribute Name | AVP Code | Section Defined | Value Type | MUST | MAY | SHLD NOT | MUST NOT | Encr |
| Service-Type | 6 | 6.1 | Enumerated | M | P | | V | Y |
| Callback-Number | 19 | 6.2 | UTF8String | M | P | | V | Y |
| Callback-Id | 20 | 6.3 | UTF8String | M | P | | V | Y |
| Idle-Timeout | 28 | 6.4 | Unsigned32 | M | P | | V | Y |
| Port-Limit | 62 | 6.5 | Unsigned32 | M | P | | V | Y |
| NAS-Filter-Rule | 400 | 6.6 | IPFltrRule | M | P | | V | Y |
| Filter-Id | 11 | 6.7 | UTF8String | M | P | | V | Y |
| Configuration-Token | 78 | 6.8 | OctetString | M | | | P,V | |
| QoS-Filter-Rule | 407 | 6.9 | QoSFltrRule | | | | | |
| Framed-Protocol | 7 | 6.10.1 | Enumerated | M | P | | V | Y |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| Framed-Routing | 10 | 6.10.2 | Enumerated | M | P | | V | Y |
| Framed-MTU | 12 | 6.10.3 | Unsigned32 | M | P | | V | Y |
| Framed-Compression | 13 | 6.10.4 | Enumerated | M | P | | V | Y |
| Framed-IP-Address | 8 | 6.11.1 | OctetString | M | P | | V | Y |
| Framed-IP-Netmask | 9 | 6.11.2 | OctetString | M | P | | V | Y |
| Framed-Route | 22 | 6.11.3 | UTF8String | M | P | | V | Y |
| Framed-Pool | 88 | 6.11.4 | OctetString | M | P | | V | Y |
| Framed-Interface-Id | 96 | 6.11.5 | Unsigned64 | M | P | | V | Y |
| Framed-IPv6-Prefix | 97 | 6.11.6 | OctetString | M | P | | V | Y |
| Framed-IPv6-Route | 99 | 6.11.7 | UTF8String | M | P | | V | Y |
| Framed-IPv6-Pool | 100 | 6.11.8 | OctetString | M | P | | V | Y |
| Framed-IPX-Network | 23 | 6.12.1 | UTF8String | M | P | | V | Y |
| Framed-Appletalk-Link | 37 | 6.13.1 | Unsigned32 | M | P | | V | Y |
| Framed-Appletalk-Network | 38 | 6.13.2 | Unsigned32 | M | P | | V | Y |
| Framed-Appletalk-Zone | 39 | 6.13.3 | OctetString | M | P | | V | Y |
| ARAP-Features | 71 | 6.14.1 | OctetString | M | P | | V | Y |
| ARAP-Zone-Access | 72 | 6.14.2 | Enumerated | M | P | | V | Y |
| Login-IP-Host | 14 | 6.15.1 | OctetString | M | P | | V | Y |
| Login-IPv6-Host | 98 | 6.15.2 | OctetString | M | P | | V | Y |
| Login-Service | 15 | 6.15.3 | Enumerated | M | P | | V | Y |
| Login-TCP-Port | 16 | 6.16.1 | Unsigned32 | M | P | | V | Y |
| Login-LAT-Service | 34 | 6.17.1 | OctetString | M | P | | V | Y |
| Login-LAT-Node | 35 | 6.17.2 | OctetString | M | P | | V | Y |
| Login-LAT-Group | 36 | 6.17.3 | OctetString | M | P | | V | Y |
| Login-LAT-Port | 63 | 6.17.4 | OctetString | M | P | | V | Y |

### 6.1. 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 following values have been defined for the Service-Type AVP. The complete list of defined values can be found in [RADIUS] and [RADIUSTypes]. The following list is informational:

| | | |
|---|---|---|
| 1 | Login | |
| 2 | Framed | |
| 3 | Callback Login | |
| 4 | Callback Framed | |
| 5 | Outbound | |
| 6 | Administrative | |
| 7 | NAS Prompt | |
| 8 | Authenticate Only | |
| 9 | Callback NAS Prompt | |
| 10 | Call Check | |
| 11 | Callback Administrative | |
| 12 | Voice | |
| 13 | Fax | |
| 14 | Modem Relay | |
| 15 | IAPP-Register | [IEEE 802.11f] |
| 16 | IAPP-AP-Check | [IEEE 802.11f] |
| 17 | Authorize Only | [RADDynAuth] |

The following values are further qualified:

Login 1
The user should be connected to a host. The message MAY include additional AVPs defined in sections 6.16 or 6.17.

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 6.10, or section 7 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 6.10, or in section 7 for tunneling services.

### 6.2. Callback-Number AVP

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.

### 6.3. Callback-Id AVP

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 therefore preferable.

### 6.4. Idle-Timeout AVP

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.

### 6.5. Port-Limit AVP

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 [PPPMP] service is desired, but the server is not required to honor the hint in the corresponding response.

### 6.6. 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.

### 6.7. Filter-Id AVP

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 non-RADIUS environments, it is RECOMMENDED that the NAS-Filter-Rule AVP be used instead.

### 6.8. Configuration-Token AVP

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.

### 6.9. QoS-Filter-Rule AVP

The QoS-Filter-Rule AVP (AVP Code 407) is of type 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.

Note: Due to an editorial mistake in [BASE], only the AVP format is discussed. The complete QoSFilterRule definition was not included. It is reprinted here for clarification.

QoSFilterRule

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]

              tag    - Mark packet with a specific DSCP
                       [DIFFSERV].  The DSCP option MUST be
                       included.
              meter  - Meter traffic.  The metering options
                       MUST be included.

dir           The format is as described under IPFilterRule.

proto         The format is as described under IPFilterRule.

src and dst   The format is as described under IPFilterRule.

      options:

      DSCP <color>
            Color values as defined in [DIFFSERV].  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 [DIFFSERVAF], and MUST be present
            if the action is set to meter.  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 [DIFFSERVAF]
            (e.g., AF13).

            The metering option also supports the strict
            limit on traffic required by Expedited
            Forwarding, as defined in [DIFFSERVEF].  The
            color_over option may contain the keyword "drop"
            to prevent forwarding of traffic that exceeds the
            rate parameter.
```

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

### 6.10. Framed Access Authorization AVPs

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".

#### 6.10.1. Framed-Protocol AVP

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]. The following list is informational:

| | |
|---|---|
| 1 | PPP |
| 2 | SLIP |
| 3 | AppleTalk Remote Access Protocol (ARAP) |
| 4 | Gandalf proprietary SingleLink/MultiLink protocol |
| 5 | Xylogics proprietary IPX/SLIP |
| 6 | X.75 Synchronous |

#### 6.10.2. 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]. The following list is informational:

| | |
|---|---|
| 0 | None |
| 1 | Send routing packets |
| 2 | Listen for routing packets |
| 3 | Send and Listen |

#### 6.10.3. Framed-MTU AVP

The Framed-MTU AVP (AVP Code 12) is of type Unsigned32 and contains the Maximum Transmission Unit 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.

### 6.10.4. Framed-Compression AVP

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]. The following list is informational:

```
   0  None
   1  VJ TCP/IP header compression
   2  IPX header compression
   3  Stac-LZS compression
```

### 6.11. IP Access Authorization AVPs

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

### 6.11.1. Framed-IP-Address AVP

The Framed-IP-Address AVP (AVP Code 8) [RADIUS] 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).

### 6.11.2. Framed-IP-Netmask AVP

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.

### 6.11.3. Framed-Route AVP

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.

### 6.11.4. Framed-Pool AVP

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 [RADIUSExt], the encoding of the Data field SHOULD also conform to the rules for the UTF8String Data Format.

### 6.11.5. Framed-Interface-Id AVP

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.

### 6.11.6. Framed-IPv6-Prefix AVP

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.

### 6.11.7. Framed-IPv6-Route AVP

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".
```

### 6.11.8. Framed-IPv6-Pool AVP

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 [RADIUSIPv6], the encoding of the Data field SHOULD also conform to the rules for the UTF8String Data Format.

### 6.12. IPX Access

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

### 6.12.1. Framed-IPX-Network AVP

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).

## 6.13. AppleTalk Network Access

The AVPs defined in this section are used when the user requests, or is being granted, access to an AppleTalk network [AppleTalk].

### 6.13.1. Framed-AppleTalk-Link AVP

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.

### 6.13.2. Framed-AppleTalk-Network AVP

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.

### 6.13.3. Framed-AppleTalk-Zone AVP

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.

### 6.14. AppleTalk Remote Access

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]. They are only present if the Framed-Protocol AVP (see section 6.10.1) is set to ARAP. Section 2.2 of RFC 2869 [RADIUSExt] describes the operational use of these attributes.

### 6.14.1. ARAP-Features AVP

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 [RADIUSExt] for more information about the format of this AVP.

### 6.14.2. ARAP-Zone-Access AVP

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] and defined in [RADIUSExt].

### 6.15. Non-Framed Access Authorization AVPs

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".

### 6.15.1. Login-IP-Host AVP

The Login-IP-Host AVP (AVP Code 14) [RADIUS] 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.

### 6.15.2. Login-IPv6-Host AVP

The Login-IPv6-Host AVP (AVP Code 98) [RADIUSIPv6] 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.

### 6.15.3. 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 [RADIUSTypes]. The following list is informational:

| | |
|---|---|
| 0 | Telnet |
| 1 | Rlogin |
| 2 | TCP Clear |
| 3 | PortMaster (proprietary) |
| 4 | LAT |
| 5 | X25-PAD |
| 6 | X25-T3POS |
| 8 | TCP Clear Quiet (suppresses any NAS-generated connect string) |

### 6.16. TCP Services

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

### 6.16.1. Login-TCP-Port AVP

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.

### 6.17. LAT Services

The AVPs described in this section MAY be present if the Login-Service AVP is set to LAT [LAT].

### 6.17.1. Login-LAT-Service AVP

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 [ISOLatin]. All LAT string comparisons are case insensitive.

### 6.17.2. Login-LAT-Node AVP

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 [ISOLatin]. All LAT string comparisons are case insensitive.

### 6.17.3. Login-LAT-Group AVP

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.

### 6.17.4. Login-LAT-Port AVP

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 [ISOLatin]. All LAT string comparisons are case insensitive.

## 7. NAS Tunneling

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 [RADTunnels], [RADTunlAcct].

| | | | | AVP Flag rules | | | | |
|---|---|---|---|---|---|---|---|---|
| Attribute Name | AVP Code | Section Defined | Value Type | MUST | MAY | SHLD NOT | MUST NOT | Encr |
| Tunneling | 401 | 7.1 | Grouped | M | P | | V | N |
| Tunnel-Type | 64 | 7.2 | Enumerated | M | P | | V | Y |
| Tunnel-Medium-Type | 65 | 7.3 | Enumerated | M | P | | V | Y |
| Tunnel-Client-Endpoint | 66 | 7.4 | UTF8String | M | P | | V | Y |
| Tunnel-Server-Endpoint | 67 | 7.5 | UTF8String | M | P | | V | Y |
| Tunnel-Password | 69 | 7.6 | OctetString | M | P | | V | Y |
| Tunnel-Private-Group-Id | 81 | 7.7 | OctetString | M | P | | V | Y |
| Tunnel-Assignment-Id | 82 | 7.8 | OctetString | M | P | | V | Y |
| Tunnel-Preference | 83 | 7.9 | Unsigned32 | M | P | | V | Y |
| Tunnel-Client-Auth-Id | 90 | 7.10 | UTF8String | M | P | | V | Y |
| Tunnel-Server-Auth-Id | 91 | 7.11 | UTF8String | M | P | | V | Y |

### 7.1. Tunneling AVP

The Tunneling AVP (AVP Code 401) is of type Grouped and contains the following AVPs, used to describe a compulsory tunnel service: [RADTunnels], [RADTunlAcct]. 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 ]
```

### 7.2. Tunnel-Type AVP

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 Accounting-Request 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]. The following list is informational:

| | |
|---|---|
| 1 | Point-to-Point Tunneling Protocol (PPTP) |
| 2 | Layer Two Forwarding (L2F) |
| 3 | Layer Two Tunneling Protocol (L2TP) |
| 4 | Ascend Tunnel Management Protocol (ATMP) |
| 5 | Virtual Tunneling Protocol (VTP) |
| 6 | IP Authentication Header in the Tunnel-mode (AH) |
| 7 | IP-in-IP Encapsulation (IP-IP) |
| 8 | Minimal IP-in-IP Encapsulation (MIN-IP-IP) |
| 9 | IP Encapsulating Security Payload in the Tunnel-mode (ESP) |
| 10 | Generic Route Encapsulation (GRE) |
| 11 | Bay Dial Virtual Services (DVS) |
| 12 | IP-in-IP Tunneling |
| 13 | Virtual LANs (VLAN) |

### 7.3. Tunnel-Medium-Type AVP

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) 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]. The following list is informational:

| | |
|---|---|
| 1 | IPv4 (IP version 4) |
| 2 | IPv6 (IP version 6) |
| 3 | NSAP |
| 4 | HDLC (8-bit multidrop) |
| 5 | BBN 1822 |
| 6 | 802 (includes all 802 media plus Ethernet "canonical format") |
| 7 | E.163 (POTS) |
| 8 | E.164 (SMDS, Frame Relay, ATM) |
| 9 | F.69 (Telex) |
| 10 | X.121 (X.25, Frame Relay) |
| 11 | IPX |
| 12 | Appletalk |
| 13 | Decnet IV |
| 14 | Banyan Vines |
| 15 | E.164 with NSAP format subaddress |

### 7.4. Tunnel-Client-Endpoint AVP

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 Accounting-Request messages, in which case it indicates the address from which the tunnel was initiated. This AVP, along with the Tunnel-Server-Endpoint and Session-Id AVP [BASE], MAY 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 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 [IPv6Addr]. 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.

## 7.5. Tunnel-Server-Endpoint AVP

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 Accounting-Request messages, in which case it indicates the address from which the tunnel was initiated. This AVP, along with the Tunnel-Client-Endpoint and Session-Id AVP [BASE], MAY 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 [IPv6Addr]. 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.

### 7.6. Tunnel-Password AVP

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 [RADTunnels].

As required in [BASE], Diameter messages are encrypted by using IPsec or TLS. The Tunnel-Password AVP SHOULD NOT be used in untrusted proxy environments without encrypting it by using end-to-end security techniques, such as CMS Security [DiamCMS].

### 7.7. Tunnel-Private-Group-Id AVP

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 Accounting-Request messages that pertain to the tunneled session.

### 7.8. Tunnel-Assignment-Id AVP

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] and [L2TP], 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.

## 7.9. Tunnel-Preference AVP

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 decide which set of AVPs to use.

### 7.10. Tunnel-Client-Auth-Id AVP

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 Accounting-Request messages pertaining to the tunneled session.

### 7.11. Tunnel-Server-Auth-Id AVP

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 Accounting-Request messages pertaining to the tunneled session.

## 8. NAS Accounting

Applications implementing this specification use Diameter Accounting, as defined in [BASE], and the AVPs in the following section. Service-specific AVP usage is defined in the tables in section 10.

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 Accounting-Record-Type value 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 describes the AVPs; their AVP Code values, types, and possible flag values; and whether the AVP MAY be encrypted.

| | | | | AVP Flag rules | | | | |
|---|---|---|---|---|---|---|---|---|
| Attribute Name | AVP Code | Section Defined | Value Type | MUST | MAY | SHLD NOT | MUST NOT | Encr |
| Accounting-Input-Octets | 363 | 8.1 | Unsigned64 | M | P | | V | Y |
| Accounting-Output-Octets | 364 | 8.2 | Unsigned64 | M | P | | V | Y |
| Accounting-Input-Packets | 365 | 8.3 | Unsigned64 | M | P | | V | Y |
| Accounting-Output-Packets | 366 | 8.4 | Unsigned64 | M | P | | V | Y |
| Acct-Session-Time | 46 | 8.5 | Unsigned32 | M | P | | V | Y |
| Acct-Authentic | 45 | 8.6 | Enumerated | M | P | | V | Y |
| Acounting-Auth-Method | 406 | 8.7 | Enumerated | M | P | | V | Y |
| Acct-Delay-Time | 41 | 8.8 | Unsigned32 | M | P | | V | Y |
| Acct-Link-Count | 51 | 8.9 | Unsigned32 | M | P | | V | Y |
| Acct-Tunnel-Connection | 68 | 8.10 | OctetString | M | P | | V | Y |
| Acct-Tunnel-Packets-Lost | 86 | 8.11 | Unsigned32 | M | P | | V | Y |

## 8.1. Accounting-Input-Octets AVP

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 of INTERIM_RECORD or STOP_RECORD.

### 8.2. 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.

### 8.3. Accounting-Input-Packets AVP

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.

### 8.4. Accounting-Output-Packets AVP

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.

### 8.5. Acct-Session-Time AVP

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.

### 8.6. 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]. The following list is informational:

1 RADIUS<br>
2 Local<br>
3 Remote<br>
4 Diameter

## 8.7. Accounting-Auth-Method AVP

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 is equivalent to the RADIUS MS-Acct-Auth-Type VSA attribute).

The following values are defined:

1 PAP<br>
2 CHAP<br>
3 MS-CHAP-1<br>
4 MS-CHAP-2<br>
5 EAP<br>
7 None

## 8.8. Acct-Delay-Time

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 resent 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.

### 8.9. Acct-Link-Count

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-<br>Session-Id | Session-Id | Accounting-<br>Record-Type | Acct-<br>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 |

### 8.10. Acct-Tunnel-Connection AVP

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 and Tunnel-Server-Endpoint 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. 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.

### 8.11. 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 link.

## 9. RADIUS/Diameter Protocol Interactions

This section describes some basic guidelines that servers acting as AAA Translation Agents may use. A complete description of all the differences between RADIUS and Diameter is beyond the scope of this section and document. Note that this document does not restrict implementations from creating additional translation methods, as long as the translation function doesn't violate the RADIUS or the Diameter protocols.

Although the Diameter protocol is in many ways a superset of RADIUS functions, a number of RADIUS representations are not allowed, so that new capabilities can be used without the old problems.

There are primarily two different situations that must be handled: one in which a RADIUS request is received that must be forwarded as a Diameter request, and another in which the inverse is true. RADIUS does not support a peer-to-peer architecture, and server-initiated operations are generally not supported. See [RADDynAuth] for an alternative.

Some RADIUS attributes are encrypted. RADIUS security and encryption techniques are applied on a hop-per-hop basis. A Diameter agent will have to decrypt RADIUS attribute data entering the Diameter system, and if that information is forwarded, the agent MUST secure it by using Diameter specific techniques.

Note that this section uses the two terms, "AVP" and "attribute", in a concise and specific manner. The former is used to signify a Diameter AVP, and the latter to signify a RADIUS attribute.

### 9.1. RADIUS Request Forwarded as Diameter Request

This section describes the actions that should be taken when a Translation Agent receives a RADIUS message to be translated to a Diameter message.

Note that RADIUS servers are assumed to be stateless. It is also quite possible for the RADIUS messages that comprise the session (i.e., authentication and accounting messages) to be handled by different Translation Agents in the proxy network. Therefore, a RADIUS/Diameter Translation Agent SHOULD NOT be assumed to have an accurate track on session-state information.

When a Translation Agent receives a RADIUS message, the following steps should be taken:

- If a Message-Authenticator attribute is present, the value MUST be checked but not included in the Diameter message. If it is incorrect, the RADIUS message should be silently discarded. The gateway system SHOULD generate and include a Message-Authenticator in returned RADIUS responses.

- The transport address of the sender MUST be checked against the NAS identifying attributes. See the description of NAS-Identifier and NAS-IP-Address below.

- The Translation Agent must maintain transaction state information relevant to the RADIUS request, such as the Identifier field in the RADIUS header, any existing RADIUS Proxy-State attribute, and the source IP address and port number of the UDP packet. These may be maintained locally in a state table or saved in a Proxy-Info AVP group. A Diameter Session-Id AVP value must be created using a session state mapping mechanism.

- If the RADIUS request contained a State attribute and the prefix of the data is "Diameter/", the data following the prefix contains the Diameter Origin-Host/Origin-Realm/Session-Id. If no such attributes are present and the RADIUS command is an Access-Request, a new Session-Id is created. The Session-Id is included in the Session-Id AVP.

- The Diameter Origin-Host and Origin-Realm AVPs MUST be created and added by using the information from an FQDN corresponding to the NAS-IP-Address attribute (preferred if available), and/or to the NAS-Identifier attribute. (Note that the RADIUS NAS-Identifier is not required to be an FQDN.)

- The response MUST have an Origin-AAA-Protocol AVP added, indicating the protocol of origin of the message.

- The Proxy-Info group SHOULD be added, with the local server’s identity specified in the Proxy-Host AVP. This should ensure that the response is returned to this system.

- The Destination-Realm AVP is created from the information found in the RADIUS User-Name attribute.

- If the RADIUS User-Password attribute is present, the password must be unencrypted by using the link's RADIUS shared secret. The unencrypted value must be forwarded in a User-Password AVP using Diameter security.

- If the RADIUS CHAP-Password attribute is present, the Ident and Data portion of the attribute are used to create the CHAP-Auth grouped AVP.

- If the RADIUS message contains an address attribute, it MUST be converted to the appropriate Diameter AVP and type.

- If the RADIUS message contains Tunnel information [RADTunnels], the attributes or tagged groups should each be converted to a Diameter Tunneling Grouped AVP set. If the tunnel information contains a Tunnel-Password attribute, the RADIUS encryption must be resolved, and the password forwarded, by using Diameter security methods.

- If the RADIUS message received is an Accounting-Request, the Acct-Status-Type attribute value must be converted to a Accounting-Record-Type AVP value. If the Acct-Status-Type attribute value is STOP, the local server MUST issue a Session-Termination-Request message once the Diameter Accounting-Answer message has been received.

- If the Accounting message contains an Acct-Termination-Cause attribute, it should be translated to the equivalent Termination-Cause AVP value. (see below)

- If the RADIUS message contains the Accounting-Input-Octets, Accounting-Input-Packets, Accounting-Output-Octets, or Accounting-Output-Packets, these attributes must be converted to the Diameter equivalents. Further, if the Acct-Input-Gigawords or Acct-Output-Gigawords attributes are present, these must be used to properly compute the Diameter accounting AVPs.

The corresponding Diameter response is always guaranteed to be received by the same Translation Agent that translated the original request, due to the contents of the Proxy-Info AVP group in the Diameter request. The following steps are applied to the response message during the Diameter-to-RADIUS translation:

- If the Diameter Command-Code is set to AA-Answer and the Result-Code AVP is set to DIAMETER_MULTI_ROUND_AUTH, the gateway must send a RADIUS Access-Challenge. This must have the Origin-Host, Origin-Realm, and Diameter Session-Id AVPs encapsulated in the RADIUS State attribute, with the prefix "Diameter/", concatenated in the above order separated with "/" characters, in UTF-8 [UTF-8]. This is necessary to ensure that the Translation Agent receiving the subsequent RADIUS Access-Request will have access to the Session Identifier and be able to set the Destination-Host to the correct value. If the Multi-Round-Time-Out AVP is present, the value of the AVP MUST be inserted in the RADIUS Session-Timeout AVP.

- If the Command-Code is set to AA-Answer, the Diameter Session-Id AVP is saved in a new RADIUS Class attribute whose format consists of the string "Diameter/" followed by the Diameter Session Identifier. This will ensure that the subsequent Accounting messages, which could be received by any Translation Agent, would have access to the original Diameter Session Identifier.
- If a Proxy-State attribute was present in the RADIUS request, the same attribute is added in the response. This information may be found in the Proxy-Info AVP group, or in a local state table.

- If state information regarding the RADIUS request was saved in a Proxy-Info AVP or local state table, the RADIUS Identifier and UDP IP Address and port number are extracted and used in issuing the RADIUS reply.

When translating a Diameter AA-Answer (with successful result code) to RADIUS Access-Accept that contains a Session-Timeout or Authorization-Lifetime AVP, take the following steps:

- If the Diameter message contains a Session-Timeout AVP but no Authorization-Lifetime AVP, translate it to a Session-Timeout attribute (not a Termination-Action).

- If the Diameter message contains an Authorization-Lifetime AVP but no Session-Timeout AVP, translate it to a Session-Timeout attribute and a Termination-Action set to AA-REQUEST. (Remove Authorization-Lifetime and Re-Auth-Request-Type.)

- If the Diameter message has both, the Session-Timeout must be greater than or equal to the Authorization-Lifetime (required by [BASE]). Translate it to a Session-Timeout value (with value from Authorization-Lifetime AVP, the smaller one) and with the Termination-Action set to AA-REQUEST. (Remove the Authorization-Lifetime and Re-Auth-Request-Type.)

### 9.1.1. RADIUS Dynamic Authorization Considerations

A Diameter/RADIUS gateway may communicate with a server that implements RADIUS Dynamic Authorization [RADDynAuth]. If the server supports these functions, it MUST be listening on the assigned port and would receive RADIUS CoA-Request and Disconnect-Request messages. These can be mapped into the Diameter Re-Auth-Request (RAR) and Abort-Session-Request (ASR) message exchanges, respectively [BASE].

If the [RADDynAuth] is not supported, the port would not be active and the RADIUS server would receive an ICMP Port Unreachable indication. Alternatively, if the messages are received but with an inappropriate Service-Type, the gateway can respond with the appropriate NAK message and an Error-Cause attribute with the value of 405, "Unsupported Service".

The RADIUS CoA-Request and Disconnect-Request messages will not contain a Diameter Session-Id. Diameter requires that this value match an active session context. The gateway MUST have a session Id cache (or other means) to identify the sessions these functions pertain to. If unable to identify the session, the gateway (or NAS) should return an Error-Cause value 503, "Session Context Not Found".

The RADIUS CoA-Request message only supports a change of authorization attributes, and the received CoA-Request SHOULD include a Service-Type of "Authorize-Only". This indicates an extended exchange request by the rules given in [RADDynAuth] section 3.2, note 6. This is the only type of exchange supported by Diameter [BASE].

For the CoA-Request, the translated RAR message will have a Re-Auth-Type of AUTHORIZE_ONLY. The returned RAA will be translated into a CoA-NAK with Error-Cause "Request Initiated". The gateway's Diameter client SHOULD also start a reauthorization sequence by sending an AAR message, which will be translated into an Access-Request message. The RADIUS server will use the Access-Accept (or Access-Reject) message to convey the new authorization attributes, which the gateway will pass back in an AAA message.

Any attributes included in the COA-Request or Access-Accept message are to be considered mandatory in Diameter. If they cannot be supported, they MUST result in an error message return to the RADIUS server, with an Error-Cause of "Unsupported Attribute". The Diameter NAS will attempt to apply all the attributes supplied in the AA message to the session.

A RADIUS Disconnect-Request message received by the gateway would be translated to a Diameter Abort-Session-Request (ASR) message [BASE]. The results will be returned by the Diameter client in an Abort-

Session-Answer (ASA) message. A success indication would translate to a RADIUS Disconnect-ACK, and a failure would generate a Disconnect-NAK.

### 9.2. Diameter Request Forwarded as RADIUS Request

When a server receives a Diameter request to be forwarded to a RADIUS entity, the following are examples of the steps that may be taken:

- The Origin-Host AVP's value is inserted into the NAS-Identifier attribute.

- The following information MUST be present in the corresponding Diameter response and therefore MUST be saved, either in a local state table or encoded in a RADIUS Proxy-State attribute:

  1. Origin-Host AVP
  2. Session-Id AVP
  3. Proxy-Info AVP
  4. Any other AVP that MUST be present in the response and has no corresponding RADIUS attribute.

- If the CHAP-Auth AVP is present, the grouped AVPs are used to create the RADIUS CHAP-Password attribute data.

- If the User-Password AVP is present, the data should be encrypted and forwarded by using RADIUS rules. The same is true for any other RADIUS-encrypted attribute values.

- AVPs of the type Address must be translated to the corresponding RADIUS attribute.

- If the Accounting-Input-Octets, Accounting-Input-Packets, Accounting-Output-Octets, or Accounting-Output-Packets AVPs are present, they must be translated to the corresponding RADIUS attributes. If the value of the Diameter AVPs do not fit within a 32-bit RADIUS attribute, the RADIUS Acct-Input-Gigawords and Acct-Output-Gigawords must be used.

- If the RADIUS link supports the Message-Authenticator attribute [RADIUSExt], it SHOULD be generated and added to the request.

When the corresponding response is received by the Translation Agent, which is guaranteed in the RADIUS protocol, the following steps may be taken:

- If the RADIUS code is set to Access-Challenge, a Diameter AA-Answer message is created with the Result-Code set to DIAMETER_MULTI_ROUND_AUTH. If the Session-Timeout AVP is present in the RADIUS message, its value is inserted into the Multi-Round-Time-Out AVP.

- If a Proxy-State attribute is present, extract the encoded information; otherwise, retrieve the original Proxy-Info AVP group information from the local state table.

- The response's Origin-Host information is created from the FQDN of the RADIUS message's source IP address. The same FQDN is also stored to a Route-Record AVP.

- The response's Destination-Host AVP is copied from the saved request's Origin-Host information.

- The Session-Id information can be recovered from local state, or from the constructed State or Proxy-State attribute, as above.

- If a Proxy-Info AVP was present in the request, the same AVP MUST be added to the response.

- If the RADIUS State attributes are present, they must be present in the Diameter response, minus those added by the gateway.

- Any other AVPs that were saved at request time, and that MUST be present in the response, are added to the message.

When translating a RADIUS Access-Accept to Diameter AA-Answer that contains a Session-Timeout attribute, do the following:

- If the RADIUS message contains a Session-Timeout attribute and a Termination-Action attribute set to DEFAULT (or no Termination-Action attribute at all), translate it to AA-Answer with a Session-Timeout AVP and remove the Termination-Action attribute.

- If the RADIUS message contains a Session-Timeout attribute and a Termination-Action attribute set to AA-REQUEST, translate it to AA-Answer with Authorization-Lifetime AVP and with Re-Auth-Request-Type set to AUTHORIZE_AUTHENTICATE and remove the Session-Timeout attribute.

### 9.2.1. RADIUS Dynamic Authorization Considerations

A RADIUS/Diameter gateway communicating with a RADIUS client that implements RADIUS Dynamic Authorization [RADDynAuth] may translate Diameter Re-Auth-Request (RAR) messages and Abort-Session-Request (ASR) messages [BASE] into RADIUS CoA-Request and Disconnect-Request messages respectively.

If the RADIUS client does not support the capability, the gateway will receive an ICMP Port Unreachable indication when it transmits the RADIUS message. Even if the NAS supports [RADDynAuth], it may not support the Service-Type in the request message. In this case it will respond with a NAK message and (optionally) an Error-Cause attribute with value 405, "Unsupported Service". If the gateway encounters these error conditions, or if it does not support [RADDynAuth], it sends a Diameter Answer message with an Result-Code AVP of "DIAMETER_COMMAND_UNSUPPORTED" to the AAA server.

When encoding the RADIUS messages, the gateway MUST include the Diameter Session-ID in the RADIUS State attribute value, as mentioned above. The RADIUS client should return it in the response.

A Diameter Re-Auth-Request (RAR) message [BASE] received by the gateway will be translated into a RADIUS CoA-Request and sent to the RADIUS client. The RADIUS client should respond with a CoA-ACK or CoA-NAK message, which the gateway should translate into a Re-Auth-Answer (RAA) message.

If the gateway receives a RADIUS CoA-NAK response containing a Service-Type Attribute with value "Authorize Only" and an Error-Cause Attribute with value "Request Initiated", this indicates an extended exchange request per [RADDynAuth] section 3.2, note 6.

The response is translated to a Diameter Re-Auth-Answer (RAA) with a Result-Code AVP of "DIAMETER_LIMITED_SUCCESS" sent to the AAA server.

Subsequently, the gateway should receive a RADIUS Access-Request from the NAS, with a Service-Type of "Authorize Only". This is translated into a Diameter AA-Request with an Auth-Request-Type AVP of AUTHORIZE_ONLY and sent to the AAA server. The AAA server will then reply with a Diameter AA-Answer, which is translated into a RADIUS Access-Accept or Access-Reject, depending on the value of the Result-Code AVP.

A Diameter Abort-Session-Request (ASR) message [BASE] received by the gateway will be translated into a RADIUS Disconnect-Request and sent to the RADIUS client. The RADIUS client should respond with a

Disconnect-ACK or Disconnect-NAK message, which the gateway should translate into an Abort-Session-Answer (ASA) message.

If the gateway receives a RADIUS Disconnect-NAK response containing a Service-Type Attribute with value "Authorize Only" and an Error-Cause Attribute with value "Request Initiated", the Disconnect-NAK response is translated into a Diameter Abort-Session-Answer (ASA) with a Result-Code AVP of "DIAMETER_LIMITED_SUCCESS" sent to the AAA server.

Subsequently, the gateway should receive a RADIUS Access-Request from the NAS, with a Service-Type of "Authorize Only". This is translated into a Diameter AA-Request with an Auth-Request-Type AVP of AUTHORIZE_ONLY and sent to the AAA server. The AAA server will then reply with a Diameter AA-Answer, which is translated into a RADIUS Access-Accept or Access-Reject, depending on the value of the Result-Code AVP.

### 9.3. AVPs Used Only for Compatibility

The AVPs defined in this section SHOULD only be used for backwards compatibility when a Diameter/RADIUS translation function is invoked and are not typically originated by Diameter systems during normal operations.

| | | | | AVP Flag rules | | | | |
|---|---|---|---|---|---|---|---|---|
| Attribute Name | AVP Code | Section Defined | Value Type | MUST | MAY | SHLD NOT | MUST NOT | Encr |
| NAS-Identifier | 32 | 9.3.1 | UTF8String | M | P | | V | Y |
| NAS-IP-Address | 4 | 9.3.2 | OctetString | M | P | | V | Y |
| NAS-IPv6-Address | 95 | 9.3.3 | OctetString | M | P | | V | Y |
| State | 24 | 9.3.4 | OctetString | M | P | | V | Y |
| Termination-Cause | 295 | 9.3.5 | Enumerated | M | P | | V | Y |
| Origin-AAA-Protocol | 408 | 9.3.6 | Enumerated | M | P | | V | Y |

#### 9.3.1. NAS-Identifier AVP

The NAS-Identifier AVP (AVP Code 32) [RADIUS] is of type UTF8String and contains the identity of the NAS providing service to the user. This AVP SHOULD only be added by a RADIUS/Diameter Translation Agent. When this AVP is present, the Origin-Host AVP identifies the NAS providing service to the user.

In RADIUS it would be possible for a rogue NAS to forge the NAS-Identifier attribute. Diameter/RADIUS translation agents SHOULD attempt to check a received NAS-Identifier attribute against the source address of the RADIUS packet, by doing an A/AAAA RR query. If the NAS-Identifier attribute contains an FQDN, then such a query would resolve to an IP address matching the source address. However, the NAS-Identifier attribute is not required to contain an FQDN, so such a query could fail. If it fails, an error should be logged, but no action should be taken, other than a reverse lookup on the source address and insert the resulting FQDN into the Route-Record AVP.

Diameter agents and servers SHOULD check whether a NAS-Identifier AVP corresponds to an entry in the Route-Record AVP. If no match is found, then an error is logged, but no other action is taken.

### 9.3.2. NAS-IP-Address AVP

The NAS-IP-Address AVP (AVP Code 4) [RADIUS] is of type OctetString and contains the IP Address of the NAS providing service to the user. This AVP SHOULD only be added by a RADIUS/Diameter Translation Agent. When this AVP is present, the Origin-Host AVP identifies the NAS providing service to the user.

In RADIUS it would be possible for a rogue NAS to forge the NAS-IP-Address attribute value. Diameter/RADIUS translation agents MUST check a received NAS-IP-Address or NAS-IPv6-Address attribute against the source address of the RADIUS packet. If they do not match and the Diameter/RADIUS translation agent does not know whether the packet was sent by a RADIUS proxy or NAS (e.g., no Proxy-State attribute), then by default it is assumed that the source address corresponds to a RADIUS proxy, and that the NAS Address is behind that proxy, potentially with some additional RADIUS proxies in between. The Diameter/RADIUS translation agent MUST insert entries in the Route-Record AVP corresponding to the apparent route. This implies doing a reverse lookup on the source address and NAS-IP-Address or NAS-IPv6-Address attributes to determine the corresponding FQDNs.

If the source address and the NAS-IP-Address or NAS-IPv6-Address do not match, and the Diameter/RADIUS translation agent knows that it is talking directly to the NAS (e.g., there are no RADIUS proxies between it and the NAS), then the error should be logged, and the packet MUST be discarded.

Diameter agents and servers MUST check whether the NAS-IP-Address AVP corresponds to an entry in the Route-Record AVP. This is done by doing a reverse lookup (PTR RR) for the NAS-IP-Address to retrieve the corresponding FQDN, and by checking for a match with the Route-

Record AVP. If no match is found, then an error is logged, but no other action is taken.

### 9.3.3. NAS-IPv6-Address AVP

The NAS-IPv6-Address AVP (AVP Code 95) [RADIUSIPv6] is of type OctetString and contains the IPv6 Address of the NAS providing service to the user. This AVP SHOULD only be added by a RADIUS/Diameter Translation Agent. When this AVP is present, the Origin-Host AVP identifies the NAS providing service to the user.

In RADIUS it would be possible for a rogue NAS to forge the NAS-IPv6-Address attribute. Diameter/RADIUS translation agents MUST check a received NAS-IPv6-Address attribute against the source address of the RADIUS packet. If they do not match and the Diameter/RADIUS translation agent does not know whether the packet was sent by a RADIUS proxy or NAS (e.g., no Proxy-State attribute), then by default it is assumed that the source address corresponds to a RADIUS proxy, and that the NAS-IPv6-Address is behind that proxy, potentially with some additional RADIUS proxies in between. The Diameter/RADIUS translation agent MUST insert entries in the Route-Record AVP corresponding to the apparent route. This implies doing a reverse lookup on the source address and NAS-IPv6-Address attributes to determine the corresponding FQDNs.

If the source address and the NAS-IPv6-Address do not match, and the Diameter/RADIUS translation agent knows that it is talking directly to the NAS (e.g., there are no RADIUS proxies between it and the NAS), then the error should be logged, and the packet MUST be discarded.

Diameter agents and servers MUST check whether the NAS-IPv6-Address AVP corresponds to an entry in the Route-Record AVP. This is done by doing a reverse lookup (PTR RR) for the NAS-IPv6-Address to retrieve the corresponding FQDN, and by checking for a match with the Record-Route AVP. If no match is found, then an error is logged, but no other action is taken.

### 9.3.4. State AVP

The State AVP (AVP Code 24) [RADIUS] is of type OctetString and has two uses in the Diameter NAS application.

The State AVP MAY be sent by a Diameter Server to a NAS in an AA-Response command that contains a Result-Code of DIAMETER_MULTI_ROUND_AUTH. If so, the NAS MUST return it unmodified in the subsequent AA-Request command.

The State AVP MAY also be sent by a Diameter Server to a NAS in an AA-Response command that also includes a Termination-Action AVP with the value of AA-REQUEST. If the NAS performs the Termination-Action by sending a new AA-Request command upon termination of the current service, it MUST return the State AVP unmodified in the new request command.

In either usage, the NAS MUST NOT interpret the AVP locally. Usage of the State AVP is implementation dependent.

### 9.3.5. Termination-Cause AVP Code Values

This section defines a mapping between Termination-Cause AVP code values and RADIUS Acct-Terminate-Cause attribute code values from RFC 2866 [RADIUSAcct] and [RADIUSTypes], thereby allowing a RADIUS/Diameter Translation Agent to convert between the attribute and AVP values. This section thus extends the definitions in the "Termination-Cause AVP" section of the Base Diameter specification.

The table in this section defines the mapping between Termination-Cause AVP and RADIUS Acct-Terminate-Cause causes.

| | Value | | |
|---|---|---|---|
| Cause Value Name | RADIUS | Diameter | |
| User Request | 1 | 11 | |
| Lost Carrier | 2 | 12 | |
| Lost Service | 3 | 13 | |
| Idle Timeout | 4 | 14 | |
| Session Timeout | 5 | 15 | |
| Admin Reset | 6 | 16 | |
| Admin Reboot | 7 | 17 | |
| Port Error | 8 | 18 | |
| NAS Error | 9 | 19 | |
| NAS Request | 10 | 20 | |
| NAS Reboot | 11 | 21 | |
| Port Unneeded | 12 | 22 | |
| Port Preempted | 13 | 23 | |
| Port Suspended | 14 | 24 | |
| Service Unavailable | 15 | 25 | |
| Callback | 16 | 26 | |
| User Error | 17 | 27 | |
| Host Request | 18 | 28 | |
| Supplicant Restart | 19 | 29 | [RAD802.1X] |
| Reauthentication Failure | 20 | 30 | [RAD802.1X] |
| Port Reinit | 21 | 31 | [RAD802.1X] |
| Port Disabled | 22 | 32 | [RAD802.1X] |

From RFC 2866, the termination causes are as follows:

User Request         User requested termination of service, for
                     example with LCP Terminate or by logging out.

Lost Carrier         DCD was dropped on the port.

Lost Service         Service can no longer be provided; for
                     example, user's connection to a host was
                     interrupted.

Idle Timeout         Idle timer expired.

Session Timeout      Maximum session length timer expired.

Admin Reset          Administrator reset the port or session.

Admin Reboot Administrator is ending service on the NAS, for example, prior to rebooting the NAS.

Port Error NAS detected an error on the port that required ending the session.

NAS Error NAS detected an error (other than on the port) that required ending the session.

NAS Request NAS ended the session for a non-error reason not otherwise listed here.

NAS Reboot NAS ended the session to reboot non-administratively ("crash").

Port Unneeded NAS ended the session because resource usage fell below a low-water mark (for example, if a bandwidth-on-demand algorithm decided that the port was no longer needed).

Port Preempted NAS ended the session to allocate the port to a higher priority use.

Port Suspended NAS ended the session to suspend a virtual session.

Service Unavailable NAS was unable to provide requested service.

Callback NAS is terminating the current session to perform callback for a new session.

User Error Input from user is in error, causing session termination.

Host Request Login Host terminated session normally.

### 9.3.6. Origin-AAA-Protocol

The Origin-AAA-Protocol AVP (AVP Code 408) is of the type Enumerated and should be inserted in a Diameter message translated by a gateway system from another AAA protocol, such as RADIUS. It identifies the source protocol of the message to the Diameter system receiving the message.

The supported values are:

1 RADIUS

## 9.4. Prohibited RADIUS Attributes

The following RADIUS attributes MUST NOT appear in a Diameter message. Instead, they are translated to other Diameter AVPs or handled in some special manner. The rules for the treatment of the attributes are discussed in sections 9.1, 9.2, and 9.6.

| Attribute Description | Defined | Nearest Diameter AVP |
|---|---|---|
| 3 CHAP-Password | RFC 2865 | CHAP-Auth Group |
| 26 Vendor-Specific | RFC 2865 | Vendor Specific AVP |
| 29 Termination-Action | RFC 2865 | Authorization-Lifetime |
| 40 Acct-Status-Type | RFC 2866 | Accounting-Record-Type |
| 42 Acct-Input-Octets | RFC 2866 | Accounting-Input-Octets |
| 43 Acct-Output-Octets | RFC 2866 | Accounting-Output-Octets |
| 47 Acct-Input-Packets | RFC 2866 | Accounting-Input-Packets |
| 48 Acct-Output-Packets | RFC 2866 | Accounting-Output-Packets |
| 49 Acct-Terminate-Cause | RFC 2866 | Termination-Cause |
| 52 Acct-Input-Gigawords | RFC 2869 | Accounting-Input-Octets |
| 53 Acct-Output-Gigawords | RFC 2869 | Accounting-Output-Octets |
| 80 Message-Authenticator | RFC 2869 | none - check and discard |

## 9.5. Translatable Diameter AVPs

In general, Diameter AVPs that are not RADIUS compatible have code values greater than 255. The table in the section above shows the AVPs that can be converted into RADIUS attributes.

Another problem may occur with Diameter AVP values that may be more than 253 octets in length. Some RADIUS attributes (including but not limited to (8)Reply-Message, (79)EAP-Message, and (77)Connect-Info) allow concatenation of multiple instances to overcome this limitation. If this is not possible, a Result-Code of DIAMETER_INVALID_AVP_LENGTH should be returned.

## 9.6. RADIUS Vendor Specific Attributes

RADIUS supports the inclusion of Vendor Specific Attributes (VSAs) through the use of attribute 26. The recommended format [RADIUS] of the attribute data field includes a 4 octet vendor code followed by a one octet vendor type field and a one octet length field. The last two fields MAY be repeated.

A system communicating between Diameter and RADIUS MAY have specific knowledge of vendor formats, and MAY be able to translate between the two formats. However, given the deployment of many RADIUS vendor formats that do not follow the example format in RFC 2865 [RADIUS], (e.g., those that use a longer vendor type code) the translations in the next two sections will not work in general for those VSAs. RFC 2865 states that a robust implementation SHOULD support the field as undistinguished octets.

Systems that don’t have vendor format knowledge MAY discard such attributes without knowing a suitable translation. An alternative format is under consideration [VSA], which proposes encodings that would preserve the native information and not require vendor knowledge in the gateway system.

The following sections are an example for translating RADIUS VSAs that use the example RADIUS format, and Diameter VSAs that have type codes less than 255, and value field lengths less than 252.

### 9.6.1. Forwarding a Diameter Vendor Specific AVP as a RADIUS VSA

For Type codes less than 255, the value field length MUST be less than 252 or the AVP will be discarded. The RADIUS VSA attribute should consist of the following fields;

```
RADIUS Type = 26, Vendor Specific Attribute
RADIUS Length = total length of attribute (header + data)
RADIUS Vendor code = Diameter Vendor code
RADIUS Vendor type code = low order byte of Diameter AVP code
RADIUS Vendor data length = length of Diameter data
```

If the Diameter AVP code is greater than 255, then the RADIUS speaking code may use a Vendor specific field coding, if it knows one for that vendor. Otherwise, the AVP will be ignored. If it is flagged as Mandatory, a "DIAMETER_AVP_UNSUPPORTED" Result-Code will be returned, and the RADIUS message will not be sent.

### 9.6.2. Forwarding a RADIUS VSA as a Diameter Vendor Specific AVP

The Diameter AVP will consist of the following fields:

```
Diameter Flags: V=1, M=0, P=0
Diameter Vendor code = RADIUS VSA Vendor code
Diameter AVP code = RADIUS VSA Vendor type code
Diameter AVP length = length of AVP (header + data)
Diameter Data = RADIUS VSA vendor data
```

Note that the VSAs are considered optional by RADIUS rules, and this specification does not set the Mandatory flag. If an implementor desires a VSA be made mandatory because it represents a required service policy, the RADIUS gateway should have a process to set the bit on the Diameter side.

If the RADIUS receiving code knows of vendor specific field interpretations for the specific vendor, it may employ them to parse an extended AVP code or data length. Otherwise the recommended standard fields will be used.

Nested Multiple vendor data fields MUST be expanded into multiple Diameter AVPs.

## 10. AVP Occurrence Tables

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. [BASE] messages and AVPs 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 | One instance of the AVP MUST be present in the message. |

### 10.1. AA-Request/Answer AVP Table

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

| | Command | |
|---|---|---|
| Attribute 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 |

## 10.2. Accounting AVP Tables

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 [BASE] and [RADIUSAcct].

### 10.2.1. Accounting Framed Access AVP Table

The table in this section is used when the Service-Type 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 |

### 10.2.2. Accounting Non-Framed Access AVP Table

The table in this section is used when the Service-Type 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 |

## 11. IANA Considerations

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 [IANAConsid].

This document defines values in the namespaces that have been created and defined in the Diameter Base [BASE]. 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.

### 11.1. Command Codes

This specification assigns the value 265 from the Command Code namespace defined in [BASE]. See sections 3.1 and 3.2 for the assignment of the namespace in this specification.

## 11.2. AVP Codes

This specification assigns the values 363 - 366 and 400 - 408 from the AVP Code namespace defined in [BASE]. See sections 4 and 5 for the assignment of the namespace in this specification. Note that the values 363 - 366 are jointly, but consistently, assigned in [DiamMIP]. This document also creates one new namespace to be managed by IANA, as described in section 11.5.

This specification also specifies the use of AVPs in the 0 - 255 range, which are defined in [RADIUSTypes]. These values are assigned by the policy in RFC 2865 section 6 [RADIUS] and are amended by RFC 3575 [RADIUSIANA].

## 11.3. Application Identifier

This specification uses the value one (1) in the Application Identifier namespace as assigned in [BASE]. See section 1.2 above for more information.

## 11.4. CHAP-Algorithm AVP Values

As defined in section 5.5, the CHAP-Algorithm AVP (AVP Code 403) uses the values of the "PPP AUTHENTICATION ALGORITHMS" namespace defined in [PPPCHAP].

## 11.5. Accounting-Auth-Method AVP Values

As defined in section 8.6, the Accounting-Auth-Method AVP (AVP Code 406) defines the values 1 - 5. All remaining values are available for assignment via IETF Consensus [IANA].

## 11.6. Origin-AAA-Protocol AVP Values

As defined in section 9.3.6, the Origin-AAA-Protocol AVP (AVP Code 408) defines the value 1. All remaining values are available for assignment with a "Specification Required" policy [IANAConsid].

## 12. Security Considerations

This document describes the extension of Diameter for the NAS application. The security considerations of the Diameter protocol itself have been discussed in [BASE]. 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 described in [DiamEAP] can offer better security, given a method suitable for the circumstances.

## 13. References

### 13.1. Normative References

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

[DiamTrans] Aboba, B. and J. Wood, "Authentication, Authorization and Accounting (AAA) Transport Profile", RFC 3539, June 2003.

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

[RADIUSTypes] IANA, "RADIUS Types", URL: <http://www.iana.org/assignments/radius-types>

[RADIUSIPv6] Aboba, B., Zorn, G., and D. Mitton, "RADIUS and IPv6", RFC 3162, August 2001.

[IPv6Addr] Nerenberg, L., "IMAP4 Binary Content Extension", RFC 3516, April 2003.

[PPPCHAP] Simpson, W., "PPP Challenge Handshake Authentication Protocol (CHAP)", RFC 1994, August 1996.

[IANAConsid] Narten, T. and H. Alvestrand, "Guidelines for Writing an IANA Considerations Section in RFCs", BCP 26, RFC 2434, October 1998.

[IANA] IANA Assigned Numbers Database, URL: <http://www.iana.org/numbers.html>

[Keywords] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[ANITypes] NANPA Number Resource Info, ANI Assignments, URL: <http://www.nanpa.com/number_resource_info/ani_ii_assignments.html>

### 13.2. Informative References

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

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

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

[RADTunlAcct] Zorn, G., Aboba, B., and D. Mitton, "RADIUS Accounting Modifications for Tunnel Protocol Support", RFC 2867, June 2000.

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

[RADIUSIANA] Aboba, B., "IANA Considerations for RADIUS (Remote Authentication Dial In User Service)", RFC 3575, July 2003.

[NASModel] Mitton, D. and M. Beadles, "Network Access Server Requirements Next Generation (NASREQNG) NAS Model", RFC 2881, July 2000.

[NASCriteria] Beadles, M. and D. Mitton, "Criteria for Evaluating Network Access Server Protocols", RFC 3169, September 2001.

[AAACriteria] Aboba, B., Calhoun, P., Glass, S., Hiller, T., McCann, P., Shiino, H., Zorn, G., Dommety, G., Perkins, C., Patil, B., Mitton, D., Manning, S., Beadles, M., Walsh, P., Chen, X., Sivalingham, S., Hameed, A., Munson, M., Jacobs, S., Lim, B., Hirschman, B., Hsu, R., Xu, Y., Campbell, E., Baba, S., and E. Jaques, "Criteria for Evaluating AAA Protocols for Network Access", RFC 2989, November 2000.

[DiamEAP] Eronen, P., "Diameter EAP Application", Work in Progress, May 2004.

[DiamCMS] Calhoun, P., Bulley, W., and S. Farrell, "Diameter CMS Security Application", Work in Progress, March 2002.

[DiamMIP] Calhoun, P., Johansson, T., Perkins, C., Hiller, T., and P. McCann "Diameter Mobile IPv4 Application", RFC 4004, August 2005.

[VSA] Mitton, D., "Diameter/RADIUS Vendor Specific AVP Translation", Work in Progress, April 2005.

[RAD802.1X] 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.

[CDMA2000] 3GPP2 "P.S0001-B", Wireless IP Network Standard, October 2002. http://www.3gpp2.com/Public_html/specs/P.S0001-B_v1.0.pdf

[AppleTalk] Sidhu, Gursharan; Andrews, Richard F. & Oppenheimer, Alan B. "Inside AppleTalk", Second Edition, Apple Computer., 1990

[ARAP] Apple Remote Access Protocol (ARAP) Version 2.0 External Reference Specification", Apple Computer, September 1994, R0612LL/B

[IPX] Novell, Inc., "NetWare System Technical Interface Overview", June 1989, # 883-000780-001

[LAT] Local Area Transport (LAT) Specification V5.0, Digital Equipment Corp., AA-NL26A-TE, June 1989

[DIFFSERV] 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.

[DIFFSERVAF] Heinanen, J., Baker, F., Weiss, W., and J. Wroclawski, "Assured Forwarding PHB Group", RFC 2597, June 1999.

[DIFFSERVEF] Davie, B., Charny, A., Bennet, J.C., 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.

[UTF-8] Yergeau, F., "UTF-8, a transformation format of ISO 10646", STD 63, RFC 3629, November 2003.

[ISOLatin] ISO 8859. International Standard -- Information Processing -- 8-bit Single-Byte Coded Graphic Character Sets -- Part 1: Latin Alphabet No. 1, ISO 8859-1:1987. URL: <http://www.iso.ch/cate/d16338.html>

[PPP] Simpson, W., "The Point-to-Point Protocol (PPP)", STD 51, RFC 1661, July 1994.

[PAP] Lloyd, B. and W. Simpson, "PPP Authentication Protocols", RFC 1334, October 1992.

[L2TP] Townsley, W., Valencia, A., Rubens, A., Pall, G., Zorn, G., and B. Palter, "Layer Two Tunneling Protocol "L2TP"", RFC 2661, August 1999.

[PPPMP] Sklower, K., Lloyd, B., McGregor, G., Carr, D., and T. Coradetti, "The PPP Multilink Protocol (MP)", RFC 1990, August 1996.

[PPTP] Hamzeh, K., Pall, G., Verthein, W., Taarud, J., Little, W., and G. Zorn, "Point-to-Point Tunneling Protocol", RFC 2637, July 1999.

[IEEE 802.11F] IEEE, "Trial-Use Recommended Practice for Multi-Vendor Access Point Interoperability via an Inter-Access Point Protocol Across Distribution Systems Supporting IEEE 802.11 Operation", IEEE 802.11F-2003, June 2003.

## 14. Acknowledgements

The authors would like to thank Carl Rigney, Allan C. Rubens, William Allen Simpson, and Steve Willens for their work on the original RADIUS [RADIUS], from which many of the concepts in this specification were derived. Thanks, also, to Carl Rigney for [RADIUSAcct] and [RADIUSExt]; Ward Willats for [RADIUSExt]; Glen Zorn, Bernard Aboba, and Dave Mitton for [RADTunlAcct] and [RADIUSIPv6]; and Dory Leifer, John Shriver, Matt Holdrege, and Ignacio Goyret for their work on [RADTunnels]. This document stole text and concepts from both [RADTunnels] and [RADIUSExt]. 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.

## Authors' Addresses

Pat Calhoun
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134
USA

Phone: +1 408-853-5269
EMail: pcalhoun@cisco.com

Glen Zorn
Cisco Systems, Inc.
500 108th Avenue N.E., Suite 500
Bellevue, WA 98004
USA

Phone:  1 425-471-4861
EMail: gwz@cisco.com

David Spence
3259 Bluett Rd.
Ann Arbor, MI  48105
USA

Phone: +1 734 834 6481
EMail: dspence@computer.org

David Mitton
Circular Networks
733 Turnpike St #154
North Andover, MA 01845

EMail: dmitton@circularnetworks.com

## Full Copyright Statement

## Intellectual Property

## Acknowledgement

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