INTERNET DRAFT
Category: Standards Track
Title: draft-calhoun-diameter-authent-08.txt
Date: October 1999

Pat R. Calhoun
Sun Microsystems, Inc.
William Bulley
Merit Network, Inc.

DIAMETER
Dial-Up (ROAMOPS) Extensions

Status of this Memo

This document is an individual contribution for consideration by the AAA Working Group of the Internet Engineering Task Force. Comments should be submitted to the diameter@ipass.com mailing list.

Distribution of this memo is unlimited.

This document is an Internet-Draft and is in full conformance with all provisions of Section 10 of RFC2026. Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

The list of current Internet-Drafts can be accessed at:

http://www.ietf.org/ietf/1id-abstracts.txt

The list of Internet-Draft Shadow Directories can be accessed at:

http://www.ietf.org/shadow.html.

Abstract

This document describes the DIAMETER Dial-up User Authentication Extension that is used for ROAMOPS [4] purposes. This specification was carefully designed to ease the burden of servers that must act as RADIUS/DIAMETER gateways, by re-using the same address space that RADIUS has defined [1]. Further, by re-using the same address space, it allows a single server to read the same dictiionary for both

DIAMETER and RADIUS. This backward compatibility will hopefully facilitate deployment of DIAMETER.

Table of Contents

1.0 Introduction

This document describes the DIAMETER Dial-up User Authentication Extension that is used for ROAMOPS [4] purposes. This specification was carefully designed to ease the burden of servers that must act as RADIUS/DIAMETER gateways, by re-using the same address space that RADIUS has defined [1]. Further, by re-using the same address space, it allows a single server to read the same dictiionary for both DIAMETER and RADIUS. This backward compatibility will hopefully facilitate deployment of DIAMETER.

The Extension number for this draft is one (1). This value is used in the Extension-Id AVP as defined in [2].

1.1 Copyright Statement

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 [12].

1.3 Changes in version -06

The following changes have been made to version 06:

- Changes to AVP Header Flags

- Change to the document title

- Changed the Command-Specific AVP Flags in all command codes defined.

- Added a reference to RFC 1994 (CHAP)

1.4 Changes in version -07

The following changes have been made to version 07:

- Changed the Filter-Rule AVP from 280 to 300

- Changed the Framed-Password-Policy AVP from 280 to 301

1.5 Changes in version -08

The following changes have been mde to version 08:

- Removed the Framed-Password-Policy AVP since it is no longer needed with the removal of the DDR/DDA commands.

- Fixed up the text in most of all AVPs where the statement introducing the AVP format was present prior to the header.

- Added the various AVPs necessary to support Tunneling.

2.0 Command Codes

This document defines the following DIAMETER Commands. All DIAMETER implementations supporting this extension MUST support all of the following commands:

Command Name	Command Code
AA-Request	263
AA-Answer	264
AA-Challenge-Ind	265

2.1 AA-Request (AAR)

Description

The AA-Request message is used in order to request authentication and authorization for a given user.

If Authentication is requested the User-Name attribute MUST be present. If only Authorization is required it is possible to authorize based on DNIS and ANI instead. However, it is not possible to authenticate using a User-Name AVP and later requesting authorization based on DNIS using the same Session-Id (although the inverse is legal).

Note that the flag field MAY be used in this command in order to indicate that either Authentication-Only or Authorization-Only is required for the request. If the Authentication-Only bit is set the response MUST NOT include any authorization information. Both the Authenticate and Authorize bits MUST NOT be set at the same time. To ensure that a user is both authenticated and authorized, neither flag is set.

The AA-Request message MUST include a unique Session-Id AVP. If The AA-Request is a result of a successful AA-Challenge-Ind the Session-Id MUST be identical to the one provided in the initial AA-Request.

Message Format

Section 3.46 contains a complete list of all valid AVPs for this message.

```
<AA-Request> ::= <DIAMETER Header>
                 <AA-Request Command AVP>
                 <Session-Id AVP>
                 <Host-IP-Address AVP>
                 [<Host-Name AVP>]
                 [<Proxy-State AVP>]
                 [<Class AVP>]
                 [<State AVP>]
                 {<User-Name AVP> ||
                  <Called-Station-Id AVP }
                 <Miscellaneous AVPs>
                 <Timestamp AVP>
                 <Nonce AVP>
                 {<Integrity-Check-Vector AVP> ||
                  <Digital-Signature AVP }
```

The length of the DIAMETER Command AVP must be 12 when the Command Code is set to 263 (AA-Request).

The following Command-specific bits may be set in the AA-Request's Command Flag field of the AVP Header:

The 'C' (Authentication-only) bit may be set to indicate that only authentication of the user is required, and that no authorization should be performed. Additionally, no authorization information is expected in the AA-Response command.

The 'Z' (Authorization-Only) bit may be set to indicate that only authorization of the user is requested and that no authentication is required. When this bit is set, no user authentication AVPs (i.e. User-Password, etc.) will be present in the request.

2.2 AA-Answer (AAA)

Description

The AA-Answer message is used in order to indicate that Authentication and/or authorization was successful. If authorization was requested a list of AVPs with the authorization information MUST be attached to the message (see section 3.36).

The AA-Answer message MUST include the Session-Id AVP that was present in the AA-Request. The AA-Answer MUST also include the Host-Name AVP and the Result-Code AVP to indicate the status of the session. The following error codes are defined for this message:

DIAMETER_ERROR_UNKNOWN_DOMAIN 1
This error code is used to indicate to the initiator of the request that the requested domain is unknown and cannot be resolved.

DIAMETER_ERROR_USER_UNKNOWN 2
This error code is used to indicate to the initiator that the username request is not valid.

DIAMETER_ERROR_BAD_PASSWORD 3
This error code indicates that the password provided is invalid.

DIAMETER_ERROR_CANNOT_AUTHORIZE 4
This error code is used to indicate that the user cannot be authorized due to the fact that the user has expended the servers local resources. This could be a result that the server believes that the user already has an active session, or that the user has already spent the number of credits in

his/her account, etc.

Note that the flag field MUST be set to the same value that was found in the AA-Request message.

Message Format

Section 3.46 contains a complete list of all valid AVPs for this message.

```
<AA-Answer> ::= <DIAMETER Header>
                <AA-Answer Command AVP>
                <Session-Id AVP>
                <Result-Code AVP>
                [<Error-Code AVP>]
                <Host-IP-Address AVP>
                [<Host-Name AVP>]
                [<Session-Timeout AVP>]
                [<Proxy-State AVP>]
                [<Class AVP>]
                [<State AVP>]
                <Miscellaneous AVPs>
                <Timestamp AVP>
                <Nonce AVP>
                {<Integrity-Check-Vector AVP> ||
                 <Digital-Signature AVP }
```

The length of the DIAMETER Command AVP must be 12 when the Command Code is set to 264 (AA-Answer).

The following Command-specific bits may be set in the AA-Request's Command Flag field of the AVP Header:

The 'C' (Authentication-only) bit may be set to indicate that only authentication of the user is required, and that no authorization should be performed. Additionally, no authorization information is expected in the AA-Response command.

The 'Z' (Authorization-Only) bit may be set to indicate that only authorization of the user is requested and that no authentication is required. When this bit is set, no user authentication AVPs (i.e. User-Password, etc.) will be present in the request.

2.3 AA-Challenge-Ind (AACI)

Description

If the DIAMETER server desires to send the user a challenge requiring a response, then the DIAMETER server MUST respond to the AA-Request by transmitting a message with the Code field set to 265 (AA-Challenge-Ind).

The message MAY have one or more Reply-Message AVP, and MAY have a single State AVP, or none. No other AVPs are permitted in an AA-Challenge-Ind other than the Integrity-Check-Vector or Digital-Signature AVP as defined in [2].

On receipt of an AA-Challenge-Ind, the Identifier field is matched with a pending AA-Request. Invalid messages are silently discarded.

The receipt of a valid AA-Challenge-Ind indicates that a new AA-Request SHOULD be sent. The NAS MAY display the text message, if any, to the user, and then prompt the user for a response. It then sends its original Acess-Request with a new request ID, with the User-Password AVP replaced by the user's response (encrypted), and including the State AVP from the AA-Challenge-Ind, if any. Only zero or one instances of the State Attribute can be present in an AA-Request.

A NAS which supports PAP MAY forward the Reply-Message to the dialin client and accept a PAP response which it can use as though the user had entered the response. If the NAS cannot do so, it should treat the AA-Challenge-Ind as though it had received an AA-Answer with a Result-Code AVP set to a value other than DIAMETER_SUCCESS instead.

It is preferable to use EAP [5] instead of the AA-Challenge-Ind, yet it has been maintained for backward compatibility.

The AA-Challenge-Ind message MUST include the Session-Id AVP that was present in the AA-Request and MUST include the same flag value that was found in the AA-Request.

Section 3.46 contains a complete list of all valid AVPs for this message.

```
AA-Challenge-Ind ::= <DIAMETER Header>
                     <AA-Challenge-Ind Command AVP>
                     <Session-Id AVP>
                     <Result-Code AVP>
                     [<Error-Code AVP>]
                     <Host-IP-Address AVP>
                     [<Host-Name AVP>]
                     [<Proxy-State AVP>]
                     [<Class AVP>]
                     [<State AVP>]
                     <Reply-Message AVPs>
                     <Timestamp AVP>
                     <Nonce AVP>
                     {<Integrity-Check-Vector AVP> ||
                      <Digital-Signature AVP }
```

The length of the DIAMETER Command AVP must be 12 when the Command Code is set to 265 (AA-Challenge-Ind).

The following Command-specific bits may be set in the AA-Request's Command Flag field of the AVP Header:

The 'C' (Authentication-only) bit may be set to indicate that only authentication of the user is required, and that no authorization should be performed. Additionally, no authorization information is expected in the AA-Response command.

The 'Z' (Authorization-Only) bit may be set to indicate that only authorization of the user is requested and that no authentication is required. When this bit is set, no user authentication AVPs (i.e. User-Password, etc.) will be present in the request.

3.0 DIAMETER AVPs

This section will define the mandatory AVPs which MUST be supported by all DIAMETER implementations supporting this extension. The following AVPs are defined in this document:

Attribute Name	Attribute Code	Definition in Section
User-Name	1	3.1
User-Password	2	3.2
CHAP-Password	3	3.3
NAS-Port	5	3.4
Service-Type	6	3.5
Framed-Protocol	7	3.6
Framed-IP-Address	8	3.7

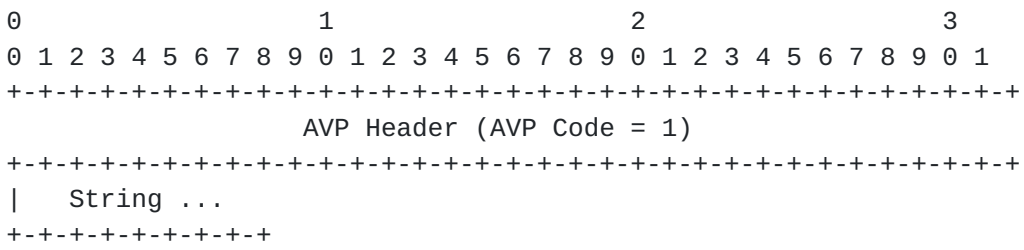
Framed-IP-Netmask	9	3.8
Framed-Routing	10	3.9
Filter-Id	11	3.10
Framed-MTU	12	3.11
Framed-Compression	13	3.12
Login-IP-Host	14	3.13
Login-Service	15	3.14
Login-TCP-Port	16	3.15
Reply-Message	18	3.16
Callback-Number	19	3.17
Callback-Id	20	3.18
Framed-Route	22	3.19
Framed-IPX-Network	23	3.20
Idle-Timeout	28	3.21
Called-Station-Id	30	3.22
Calling-Station-Id	31	3.23
Login-LAT-Service	34	3.24
Login-LAT-Node	35	3.25
Login-LAT-Group	36	3.26
Framed-AppleTalk-Link	37	3.27
Framed-AppleTalk-Network	38	3.28
Framed-AppleTalk-Zone	39	3.29
CHAP-Challenge	60	3.30
NAS-Port-Type	61	3.31
Port-Limit	62	3.32
Login-LAT-Port	63	3.33
Tunnel-Type	64	3.34
Tunnel-Medium-Type	65	3.35
Tunnel-Client-Endpoint	66	3.36
Tunnel-Server-Endpoint	67	3.37
Tunnel-Password	69	3.38
Tunnel-Private-Group-ID	81	3.39
Tunnel-Assignment-ID	82	3.40
Tunnel-Preference	83	3.41
Tunnel-Client-Auth-ID	90	3.42
Tunnel-Server-Auth-ID	91	3.43
Filter-Rule	300	3.44

3.1 User-Name

Description

This AVP indicates the name of the user to be authenticated. It is normally used in AA-Request messages, but MAY be present in the AA-Answer message.

AVP Format



AVP Flags

The 'M' bit MUST be set. The 'H' MAY be set, but the 'E' bit MUST NOT be set since proxy servers would have no knowledge of the user's domain. The 'V', 'T' and the 'P' bits MUST NOT be set.

String

The String field is one or more octets. All DIAMETER systems SHOULD support User-Name lengths of at least 63 octets. The format of the User-Name SHOULD follow the format defined in [3].

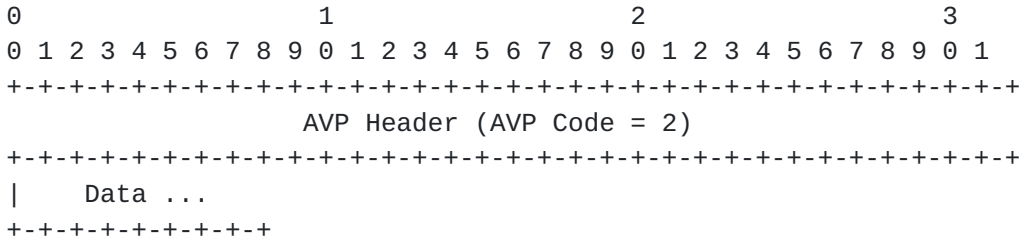
3.2 User-Password

Description

This AVP indicates the password of the user to be authenticated, or the user's input following an AA-Challenge. It is only used in AA-Request messages.

This AVP MUST be encrypted using one of the methods described in [2]. The use of this AVP with shared secret encryption is strongly discouraged by the author due to the security implications in a proxy environment, yet the support of this attribute has been retained for RADIUS backward compability.

AVP Format



AVP Length

The length of this attribute MUST be at least 24 and MUST be no larger than 136.

AVP Flags

The 'M' bit MUST be set. Either the 'H' or the 'E' bit MUST be set depending upon the security model used. The 'V', 'T' and the 'P' bits MUST NOT be set.

The AVP Flags field MUST have bit one (Mandatory Support) set. One of the AVP Encryption bits MUST be set.

Data

The Data field is between 16 and 128 octets long, inclusive.

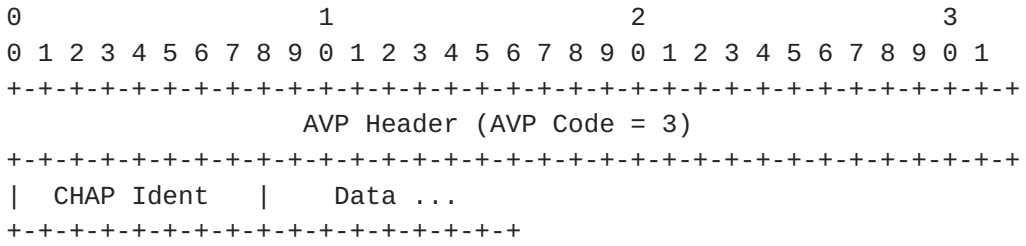
3.3 CHAP-Password

Description

This AVP indicates the response value provided by a PPP Challenge-Handshake Authentication Protocol (CHAP) user in response to the challenge. It is only used in AA-Request messages.

If the CHAP-Password AVP is found in a message, the CHAP-Challenge AVP (60) MUST be present as well.

AVP Format



AVP Length

The length of this attribute MUST be 25.

AVP Flags

The 'M' bit MUST be set. The 'H' and 'E' MAY be set depending upon the security model used. The 'V', 'T' and the 'P' bits MUST NOT be set.

CHAP Ident

This field is one octet, and contains the CHAP Identifier from the user's CHAP Response.

Data

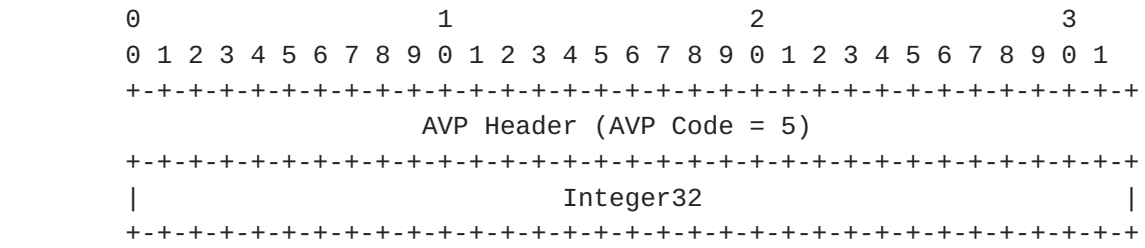
The Data field is 16 octets, and contains the CHAP Response from the user. The actual computation of the CHAP challenge can be found in [6].

3.4 NAS-Port

Description

This AVP indicates the physical port number of the NAS which is authenticating the user. It is normally only used in AA-Request messages (see section 2.2 for more info). Note that this is using "port" in its sense of a physical connection on the NAS, not in the sense of a TCP or UDP port number. Either NAS-Port or NAS-Port-Type (61) or both SHOULD be present in an AA-Request message, if the NAS differentiates among its ports.

AVP Format



AVP Flags

The 'M' bit MUST be set. The 'H' and 'E' MAY be set depending upon the security model used. The 'V', 'T' and the 'P' bits MUST NOT be set.

Integer32

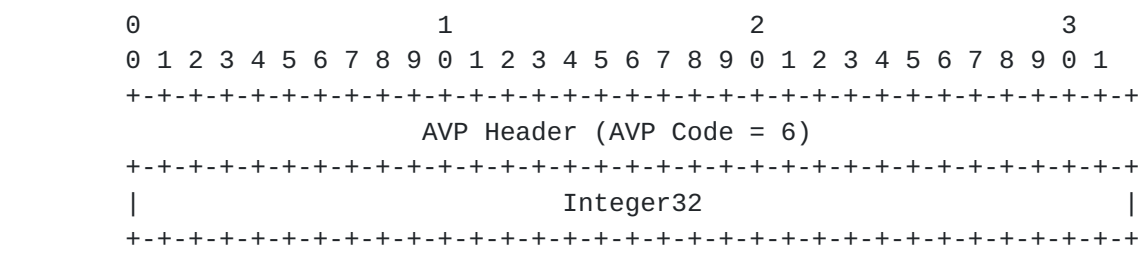
The Integer32 field is four octets.

3.5 Service-Type

Description

This AVP indicates the type of service the user has requested, or the type of service to be provided. It MAY be used in both AA-Request and AA-Answer messages. A NAS is not required to implement all of these service types, and MUST treat unknown or unsupported Service-Types as though an AA-Answer with a Result-Code other than DIAMETER-SUCCESS had been received instead.

AVP Format



AVP Flags

The 'M' bit MUST be set. The 'H' and 'E' MAY be set depending upon the security model used. The 'V', 'T' and the 'P' bits MUST NOT be set.

Integer32

The Integer32 field is four octets.

1	Login
2	Framed
3	Callback Login
4	Callback Framed
5	Outbound
6	Administrative
7	NAS Prompt
8	Authenticate Only
9	Callback NAS Prompt

The service types are defined as follows when used in an AA-Answer. When used in an AA-Request, they should be considered to be a hint to the DIAMETER server that the NAS has reason to believe the user would prefer the kind of service indicated, but the server is not required to honor the hint.

Login	The user should be connected to a host.
Framed	A Framed Protocol should be started for the User, such as PPP or SLIP.

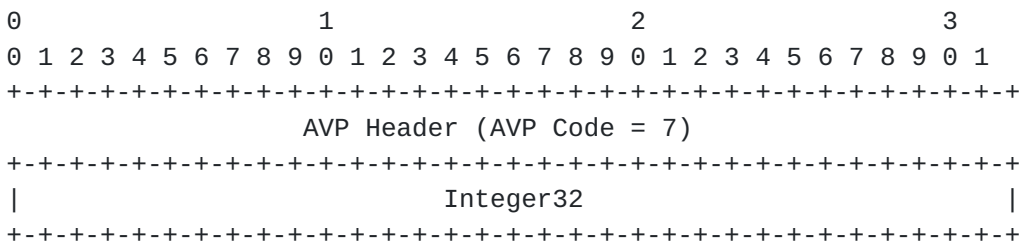
Callback Login	The user should be disconnected and calledback, then connected to a host.
Callback Framed	The user should be disconnected and called back, then a Framed Protocol should be started for the User, such as PPP or SLIP.
Outbound	The user should be granted access to outgoing devices.
Administrative	The user should be granted access to the administrative interface to the NAS from which privileged commands can be executed.
NAS Prompt	The user should be provided a command prompt on the NAS from which non-privileged commands can be executed.
Authenticate Only	Only Authentication is requested, and no authorization information needs to be returned in the AA-Answer (typically used by proxy servers rather than the NAS itself).This SHOULD NOT be used in DIAMETER, yet it is maintained for backward compatibility.
Callback NAS Prompt	The user should be disconnected and called back, then provided a command prompt on the NAS from which non-privileged commands can be executed.

3.6 Framed-Protocol

Description

This AVP indicates the framing to be used for framed access. It MAY be used in both AA-Request and AA-Answer messages.

AVP Format



AVP Flags

The 'M' bit MUST be set. The 'H' and 'E' MAY be set depending upon the security model used. The 'V', 'T' and the 'P' bits MUST NOT be set.

Integer32

The Integer32 field is four octets.

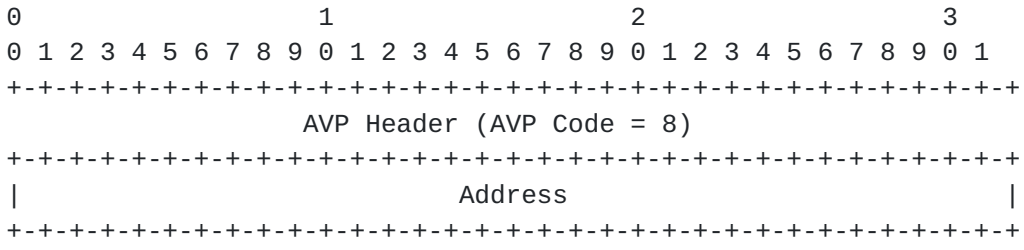
1	PPP
2	SLIP
3	AppleTalk Remote Access Protocol (ARAP)
4	Gandalf proprietary SingleLink/MultiLink protocol
5	Xylogics proprietary IPX/SLIP

3.7 Framed-IP-Address

Description

This AVP indicates the address to be configured for the user. It MAY be used in AA-Request messages as a hint by the NAS to the server that it would prefer that address, but the server is not required to honor the hint.

AVP Format



AVP Flags

The 'M' bit MUST be set. The 'H' and 'E' MAY be set depending upon the security model used. The 'V', 'T' and the 'P' bits

MUST NOT be set.

Address

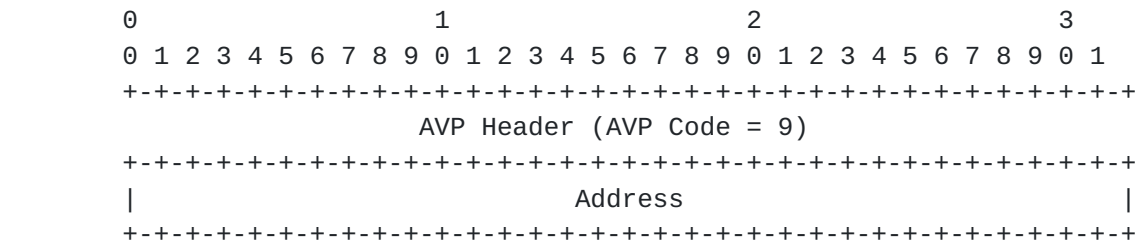
The Address field is four octets. The value 0xFFFFFFFF indicates that the NAS should allow the user to select an address (e.g. Negotiated). The value 0xFFFFFFFE indicates that the NAS should select an address for the user (e.g. Assigned from a pool of addresses kept by the NAS). Other valid values indicate that the NAS should use that value as the user's IP address.

3.8 Framed-IP-Netmask

Description

This AVP indicates the IP netmask to be configured for the user when the user is a router to a network. It MUST be used in AA-Answer messages if the Framed-IP-Address AVP was returned with a value other than 0xFFFFFFFF. It MAY be used in an AA-Request message as a hint by the NAS to the server that it would prefer that netmask, but the server is not required to honor the hint.

AVP Format



AVP Flags

The 'M' bit MUST be set. The 'H' and 'E' MAY be set depending upon the security model used. The 'V', 'T' and the 'P' bits MUST NOT be set.

Address

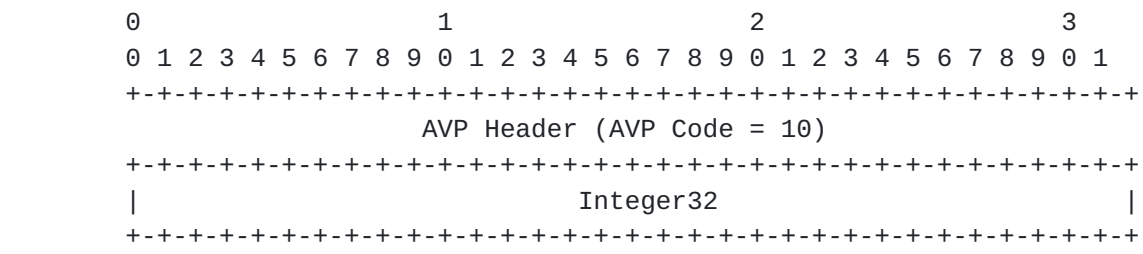
The Address field is four octets specifying the IP netmask of the user.

3.9 Framed-Routing

Description

This AVP indicates the routing method for the user, when the user is a router to a network. It is only used in AA-Answer messages.

AVP Format



AVP Flags

The 'M' bit MUST be set. The 'H' and 'E' MAY be set depending upon the security model used. The 'V', 'T' and the 'P' bits MUST NOT be set.

Integer32

The Integer32 field is four octets.

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

3.10 Filter-Id

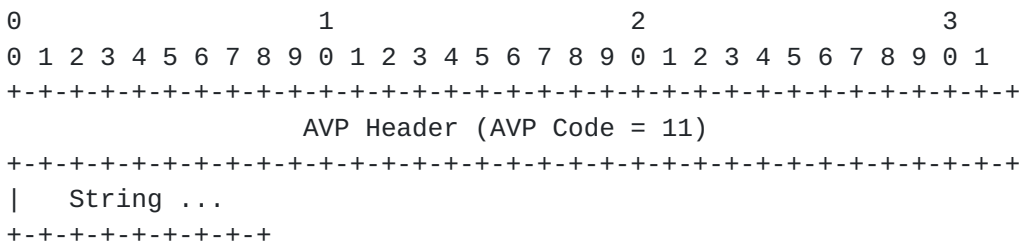
Description

This AVP indicates the name of the filter list for this user. Zero or more Filter-Id attributes MAY be sent in an AA-Answer message.

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 since filter naming differs from one service provider to another.

It is strongly encouraged to support the Filter-Rule AVP instead.

AVP Format



AVP Flags

The 'M' bit MUST be set. The 'H' and 'E' MAY be set depending upon the security model used. The 'V', 'T' and the 'P' bits MUST NOT be set.

String

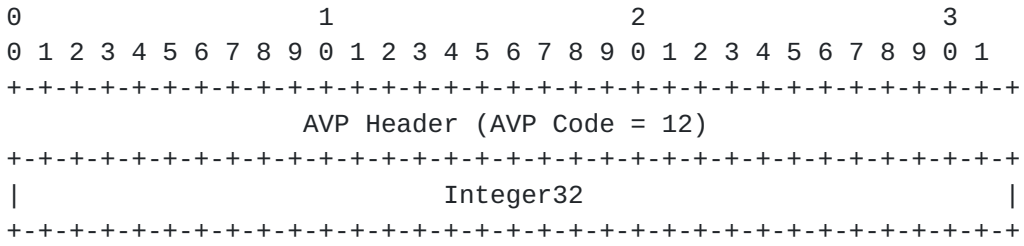
The String field is one or more octets, and its contents are implementation dependent. It is intended to be human readable and MUST NOT affect operation of the protocol. It is recommended that the message contain displayable ASCII characters from the range 32 through 126 decimal.

3.11 Framed-MTU

Description

This AVP indicates the Maximum Transmission Unit to be configured for the user, when it is not negotiated by some other means (such as PPP). It is only used in AA-Answer messages.

AVP Format



AVP Flags

The 'M' bit MUST be set. The 'H' and 'E' MAY be set depending upon the security model used. The 'V', 'T' and the 'P' bits MUST NOT be set.

Integer32

The Integer32 field is four octets. Despite the size of the field, values range from 64 to 65535.

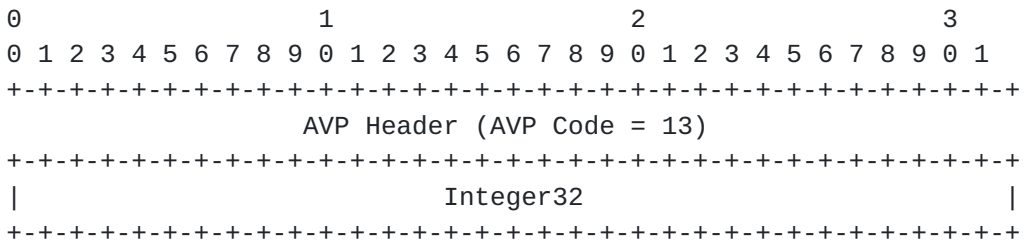
3.12 Framed-Compression

Description

This AVP indicates a compression protocol to be used for the link. It MAY be used in AA-Answer messages. It MAY be used in an AA-Request message as a hint to the server that the NAS would prefer to use that compression, but the server is not required to honor the hint.

More than one compression protocol AVP MAY be sent. It is the responsibility of the NAS to apply the proper compression protocol to appropriate link traffic.

AVP Format



AVP Flags

The 'M' bit MUST be set. The 'H' and 'E' MAY be set depending upon the security model used. The 'V', 'T' and the 'P' bits MUST NOT be set.

Integer32

The Integer32 field is four octets.

0	None
1	VJ TCP/IP header compression [7]
2	IPX header compression

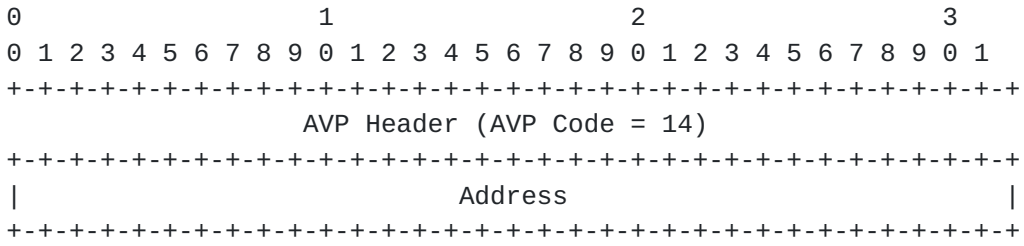
3.13 Login-IP-Host

Description

This AVP indicates the system with which to connect the user, when

the Login-Service AVP is included. It MAY be used in AA-Answer messages. It MAY be used in an AA-Request message as a hint to the server that the NAS would prefer to use that host, but the server is not required to honor the hint.

AVP Format



AVP Flags

The 'M' bit MUST be set. The 'H' and 'E' MAY be set depending upon the security model used. The 'V', 'T' and the 'P' bits MUST NOT be set.

Address

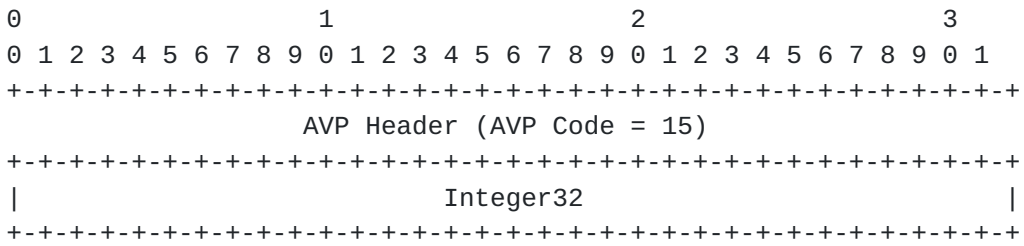
The Address field is four octets. The value 0xFFFFFFFF indicates that the NAS SHOULD allow the user to select an address. The value zero indicates that the NAS SHOULD select a host to connect the user to. Other values indicate the address the NAS SHOULD connect the user to.

3.14 Login-Service

Description

This AVP indicates the service which should be used to connect the user to the login host. It is only used in AA-Answer messages.

AVP Format



AVP Flags

The 'M' bit MUST be set. The 'H' and 'E' MAY be set depending upon the security model used. The 'V', 'T' and the 'P' bits MUST NOT be set.

Integer32

The Integer32 field is four octets.

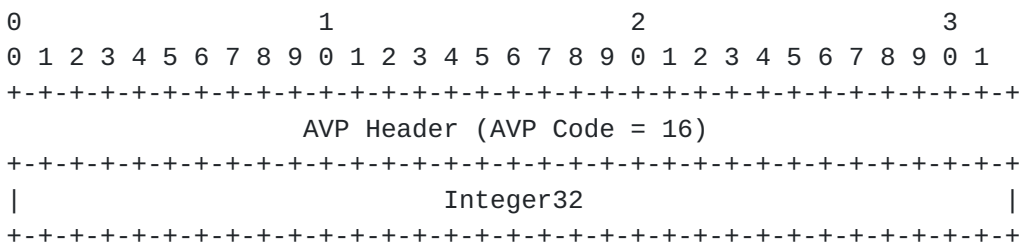
0	Telnet
1	Rlogin
2	TCP Clear
3	PortMaster (proprietary)
4	LAT

3.15 Login-TCP-Port

Description

This AVP indicates the TCP port with which the user is to be connected, when the Login-Service AVP is also present. It is only used in AA-Answer messages.

AVP Format



AVP Flags

The 'M' bit MUST be set. The 'H' and 'E' MAY be set depending upon the security model used. The 'V', 'T' and the 'P' bits MUST NOT be set.

Integer32

The Integer32 field is four octets. Despite the size of the field, values range from zero to 65535.

3.16 Reply-Message

Description

This AVP indicates text which MAY be displayed to the user.

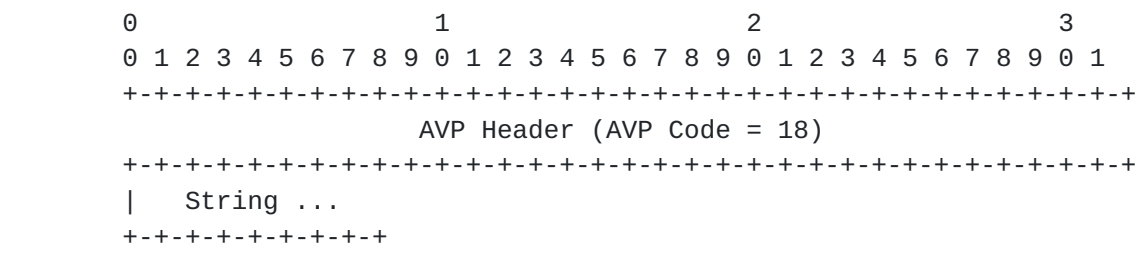
When used in an AA-Answer message with a successful Result-Code AVP it indicates the success message. When found in the same message with a Result-Code other than DIAMETER-SUCCESS it contains the failure message.

It MAY indicate a dialog message to prompt the user before another AA-Request attempt.

When used in an AA-Challenge, it MAY indicate a dialog message to prompt the user for a response.

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

AVP Format



AVP Flags

The 'M' bit MUST be set. The 'H' and 'E' MAY be set depending upon the security model used. The 'V', 'T' and the 'P' bits MUST NOT be set.

String

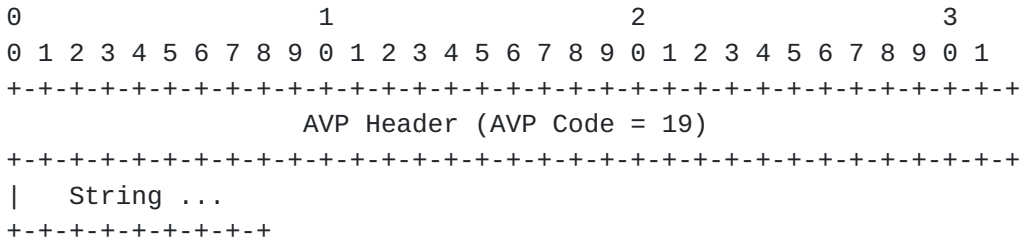
The String field is one or more octets, and its contents are implementation dependent. It is intended to be human readable, and MUST NOT affect operation of the protocol. It is recommended that the message contain displayable ASCII characters from the range 10, 13, and 32 through 126 decimal. Mechanisms for extension to other character sets are beyond the scope of this specification.

3.17 Callback-Number

Description

This AVP indicates a dialing string to be used for callback. It MAY be used in AA-Answer messages. It MAY be used in an AA-Request message as a hint to the server that a Callback service is desired, but the server is not required to honor the hint.

AVP Format



AVP Flags

The 'M' bit MUST be set. The 'H' and 'E' MAY be set depending upon the security model used. The 'V', 'T' and the 'P' bits MUST NOT be set.

String

The String field is one or more octets. The actual format of the information is site or application specific, and a robust implementation SHOULD support the field as undistinguished octets.

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

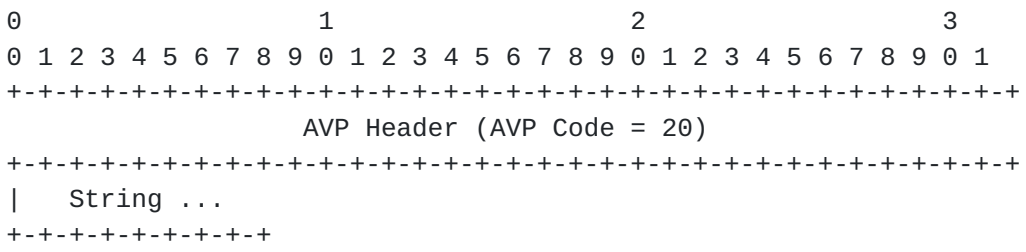
3.18 Callback-Id

Description

This AVP indicates the name of a place to be called, to be interpreted by the NAS. It MAY be used in AA-Answer messages.

This AVP is not roaming friendly since it assumes that the Callback-Id is configured on the NAS. It is therefore preferable to use the Callback-Number AVP instead.

AVP Format



AVP Flags

The 'M' bit MUST be set. The 'H' and 'E' MAY be set depending upon the security model used. The 'V', 'T' and the 'P' bits MUST NOT be set.

String

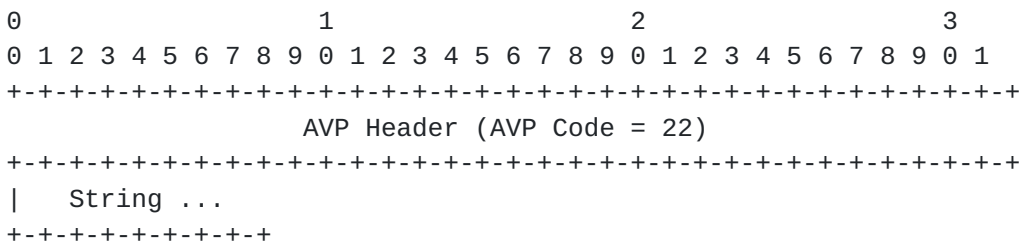
The String field is one or more octets. The actual format of the information is site or application specific, and a robust implementation SHOULD support the field as undistinguished octets. The codification of the range of allowed usage of this field is outside the scope of this specification.

3.19 Framed-IP-Route

Description

This AVP provides routing information to be configured for the user on the NAS. It is used in the AA-Answer message and can appear multiple times.

AVP Format



AVP Flags

The 'M' bit MUST be set. The 'H' and 'E' MAY be set depending upon the security model used. The 'V', 'T' and the 'P' bits MUST NOT be set.

String

It 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. That 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, 16 bits for class B prefixes, and 24 bits for class C prefixes. For example, "192.168.1.0 192.168.1.1 1".

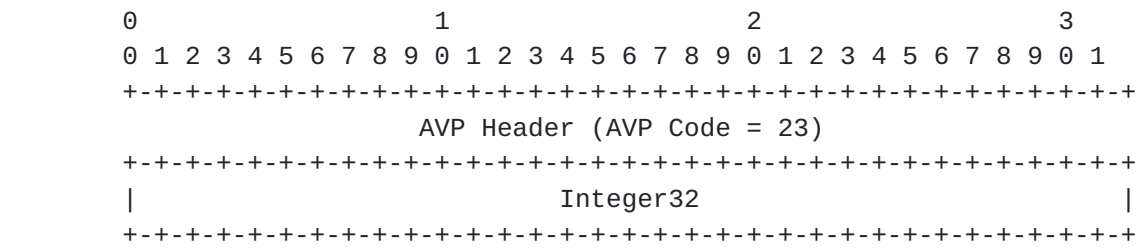
Whenever the gateway address is specified as "0.0.0.0" the IP address of the user SHOULD be used as the gateway address.

3.20 Framed-IPX-Network

Description

This AVP indicates the IPX Network number to be configured for the user. It is used in AA-Answer messages.

AVP Format



AVP Flags

The 'M' bit MUST be set. The 'H' and 'E' MAY be set depending upon the security model used. The 'V', 'T' and the 'P' bits MUST NOT be set.

Integer32

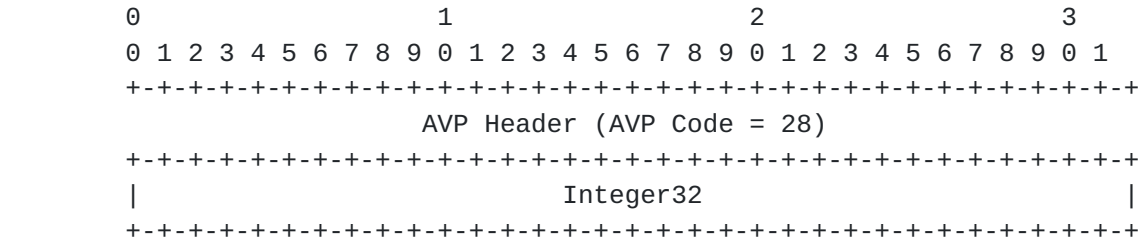
The Integer32 field is four octets. The value 0xFFFFFFFF indicates that the NAS should allow the user to select an address (e.g. Negotiated). The value 0xFFFFFFFE indicates that the NAS should select an address for the user (e.g. assigned from a pool of one or more IPX networks kept by the NAS). Other values should be used as the IPX network for the link to the user.

3.21 Idle-Timeout

Description

This AVP sets the maximum number of consecutive seconds of idle connection allowed to the user before termination of the session or prompt. This AVP is available to be sent by the server to the client in an AA-Answer or AA-Challenge.

AVP Format



AVP Flags

The 'M' bit MUST be set. The 'H' and 'E' MAY be set depending upon the security model used. The 'V', 'T' and the 'P' bits MUST NOT be set.

Integer32

The Integer32 field is 4 octets, containing a 32-bit unsigned integer with the maximum number of consecutive seconds of idle time this user should be permitted before being disconnected by the NAS.

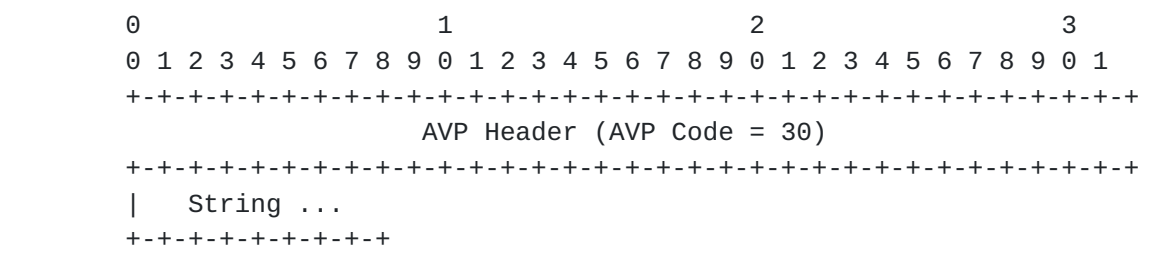
3.22 Called-Station-Id

Description

This AVP allows the NAS to send in the AA-Request message the phone number that the user called, using Dialed Number Identification (DNIS) or similar technology. Note that this may be different from the phone number the call comes in on. It is only used in AA-Request messages.

If the Authorization-Only flag is set in the message and the User-Name AVP is absent, the DIAMETER Server MUST 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.

AVP Format



AVP Flags

The 'M' bit MUST be set. The 'H' and 'E' MAY be set depending upon the security model used. The 'V', 'T' and the 'P' bits MUST NOT be set.

String

The String field is one or more octets, containing the phone number that the user's call came in on.

The actual format of the information is site or application specific. Printable ASCII is recommended, but a robust implementation SHOULD support the field as undistinguished octets.

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

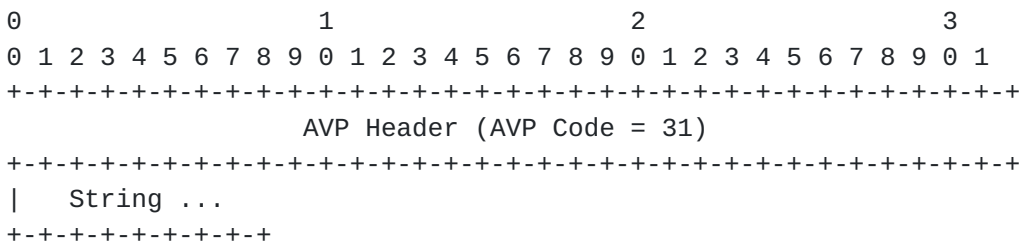
3.23 Calling-Station-Id

Description

This AVP allows the NAS to send in the AA-Request message the phone number that the call came from, using Automatic Number Identification (ANI) or similar technology. It is only used in AA-Request messages.

If the Authorization-Only flag is set in the message and the User-Name AVP is absent, the DIAMETER Server must perform authorization based on this field. This can be used by a NAS to request whether a call should be answered based on the ANI.

AVP Format



AVP Flags

The 'M' bit MUST be set. The 'H' and 'E' MAY be set depending upon the security model used. The 'V', 'T' and the 'P' bits MUST NOT be set.

String

The String field is one or more octets, containing the phone number that the user placed the call from.

The actual format of the information is site or application specific. Printable ASCII is recommended, but a robust implementation SHOULD support the field as undistinguished octets.

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

3.24 Login-LAT-Service

Description

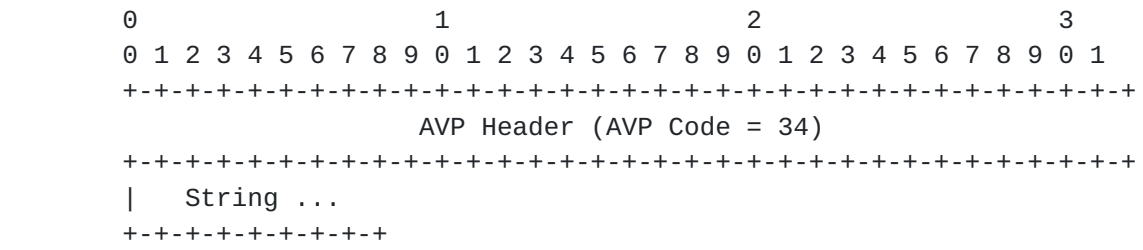
This AVP indicates the system with which the user is to be connected by LAT. It MAY be used in AA-Answer messages, but only when LAT is specified as the Login-Service. It MAY be used in an AA-Request message as a hint to the server, but the server is not required to honor the hint.

Administrators use the service attribute when dealing with clustered systems, such as a VAX or Alpha cluster. In such an environment several different time sharing hosts share the same resources (disks, printers, etc.), and administrators often configure each 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. Alternately, 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).

AVP Format



AVP Flags

The 'M' bit MUST be set. The 'H' and 'E' MAY be set depending upon the security model used. The 'V', 'T' and the 'P' bits MUST NOT be set.

String

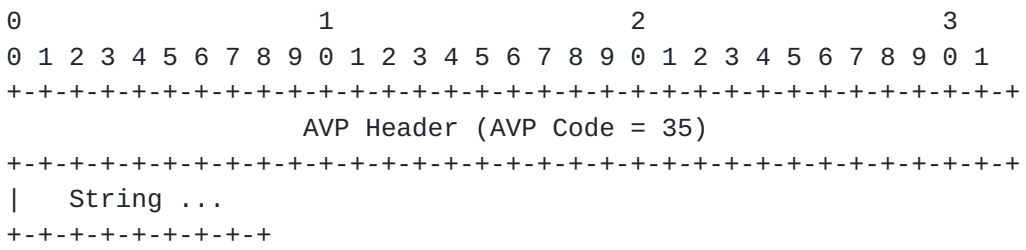
The String field is one or more octets, and contains the identity of the LAT service to use. The LAT Architecture allows this string to contain $ (dollar), - (hyphen), . (period), _ (underscore), numerics, upper and lower case alphabetics, and the ISO Latin-1 character set extension [8]. All LAT string comparisons are case insensitive.

3.25 Login-LAT-Node

Description

This AVP indicates the Node with which the user is to be automatically connected by LAT. It MAY be used in AA-Answer messages, but only when LAT is specified as the Login-Service. It MAY be used in an AA-Request message as a hint to the server, but the server is not required to honor the hint.

AVP Format



AVP Flags

The 'M' bit MUST be set. The 'H' and 'E' MAY be set depending upon the security model used. The 'V', 'T' and the 'P' bits MUST NOT be set.

String

The String field is one or more octets, and contains the identity of the LAT Node to connect the user to. 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. All LAT string comparisons are case insensitive.

3.26 Login-LAT-Group

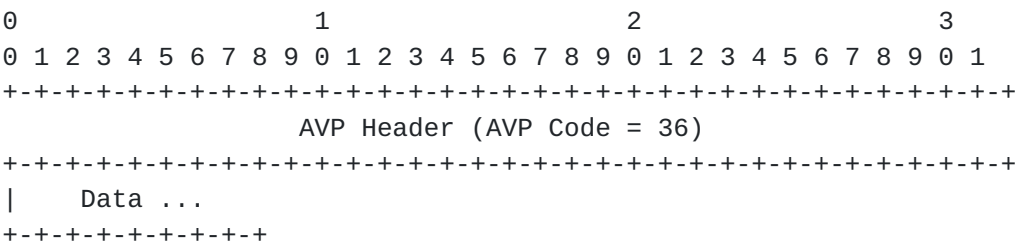
Description

This AVP contains a string identifying the LAT group codes which this user is authorized to use. It MAY be used in AA-Answer messages, but only when LAT is specified as the Login-Service. It MAY be used in an AA-Request message as a hint to the server, but the server is not required to honor the hint.

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 bit map. The administrators assign a bitmap of authorized group codes to each user; LAT gets these from the operating system, and uses these in its requests to the service providers.

AVP Format



AVP Length

The length of this attribute MUST be 40.

AVP Flags

The 'M' bit MUST be set. The 'H' and 'E' MAY be set depending upon the security model used. The 'V', 'T' and the 'P' bits MUST NOT be set.

Data

The Data field is a 32 octet bit map, most significant octet first. A robust implementation SHOULD support the field as undistinguished octets.

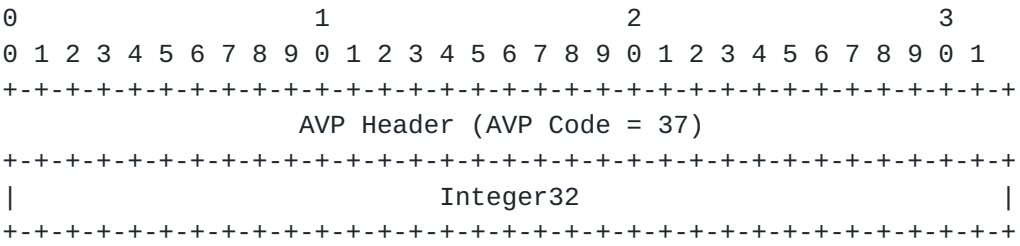
The codification of the range of allowed usage of this field is outside the scope of this specification.

3.27 Framed-AppleTalk-Link

Description

This AVP indicates the AppleTalk network number which should be used for the serial link to the user, which is another AppleTalk router. It is only used in AA-Answer messages. It is never used when the user is not another router.

AVP Format



AVP Flags

The 'M' bit MUST be set. The 'H' and 'E' MAY be set depending upon the security model used. The 'V', 'T' and the 'P' bits MUST NOT be set.

Integer32

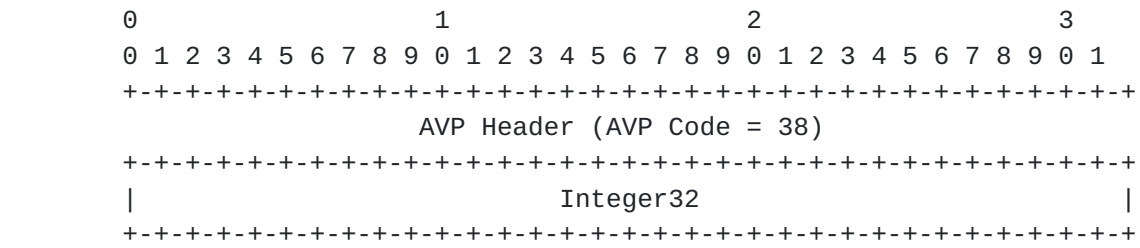
The Integer32 field is four octets. Despite the size of the field, values range from zero to 65535. The special value of zero indicates that this is an unnumbered serial link. A value of one to 65535 means that the serial line between the NAS and the user should be assigned that value as an AppleTalk network number.

3.28 Framed-AppleTalk-Network

Description

This AVP indicates the AppleTalk Network number which the NAS should probe to allocate an AppleTalk node for the user. It is only used in AA-Answer messages. It is never used when the user is another router. Multiple instances of this AVP indicate that the NAS may probe using any of the network numbers specified.

AVP Format



AVP Flags

The 'M' bit MUST be set. The 'H' and 'E' MAY be set depending upon the security model used. The 'V', 'T' and the 'P' bits MUST NOT be set.

Integer32

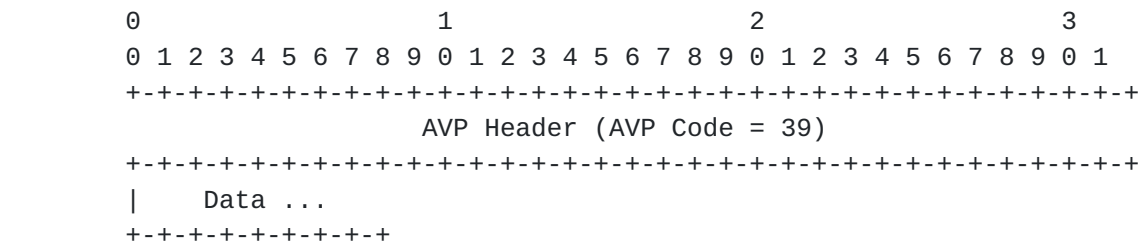
The Integer32 field is four octets. Despite the size of the field, values range from zero to 65535. The special value zero indicates that the NAS should assign a network for the user, using its default cable range. A value between one and 65535 (inclusive) indicates the AppleTalk Network the NAS should probe to find an address for the user.

3.29 Framed-AppleTalk-Zone

Description

This AVP indicates the AppleTalk Default Zone to be used for this user. It is only used in AA-Answer messages. Multiple instances of this attribute in the same message are not allowed.

AVP Format



AVP Flags

The 'M' bit MUST be set. The 'H' and 'E' MAY be set depending upon the security model used. The 'V', 'T' and the 'P' bits MUST NOT be set.

String

The name of the Default AppleTalk Zone to be used for this user. A robust implementation SHOULD support the field as undistinguished octets.

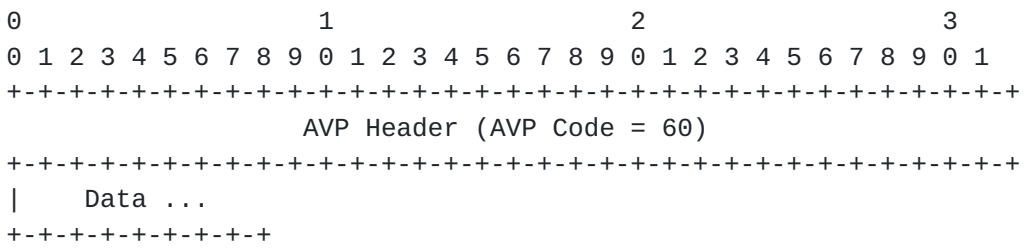
The codification of the range of allowed usage of this field is outside the scope of this specification.

3.30 CHAP-Challenge

Description

This AVP contains the CHAP Challenge sent by the NAS to a PPP Challenge-Handshake Authentication Protocol (CHAP) user. It is only used in AA-Request messages.

AVP Format



AVP Length

The length of this attribute MUST be at least 24.

AVP Flags

The 'M' bit MUST be set. The 'H' and 'E' MAY be set depending upon the security model used. The 'V', 'T' and the 'P' bits MUST NOT be set.

Data

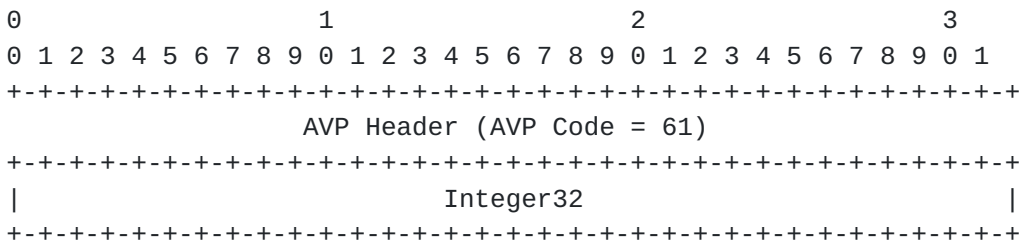
The Data field contains the CHAP Challenge.

3.31 NAS-Port-Type

Description

This AVP indicates the type of the physical port of the NAS which is authenticating the user. It can be used instead of or in addition to the NAS-Port (5) attribute. It is only used in AA-Request messages. Either NAS-Port (5) or NAS-Port-Type or both SHOULD be present in an AA-Request message, if the NAS differentiates among its ports.

AVP Format



AVP Flags

The 'M' bit MUST be set. The 'H' and 'E' MAY be set depending upon the security model used. The 'V', 'T' and the 'P' bits

MUST NOT be set.

Integer32

The Integer32 field is four octets. "Virtual" refers to a connection to the NAS via some transport protocol, instead of through a physical port. For example, if a user telnetted into a NAS to authenticate himself as an Outbound-User, the AA-Request might include NAS-Port-Type = Virtual as a hint to the DIAMETER server that the user was not on a physical port.

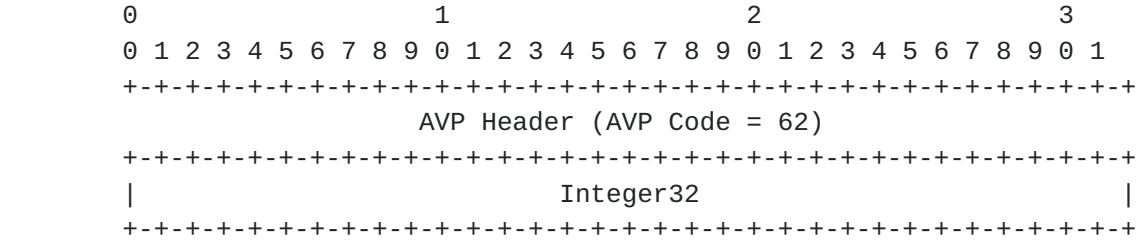
0	Async
1	Sync
2	ISDN Sync
3	ISDN Async V.120
4	ISDN Async V.110
5	Virtual

3.32 Port-Limit

Description

This AVP sets the maximum number of ports to be provided to the user by the NAS. This AVP MAY be sent by the server to the client in an AA-Answer message. It is intended for use in conjunction with Multilink PPP [9] or similar uses. It MAY also be sent by the NAS to the server as a hint that that many ports are desired for use, but the server is not required to honor the hint.

AVP Format



Type

AVP Flags

The 'M' bit MUST be set. The 'H' and 'E' MAY be set depending upon the security model used. The 'V', 'T' and the 'P' bits MUST NOT be set.

Integer32

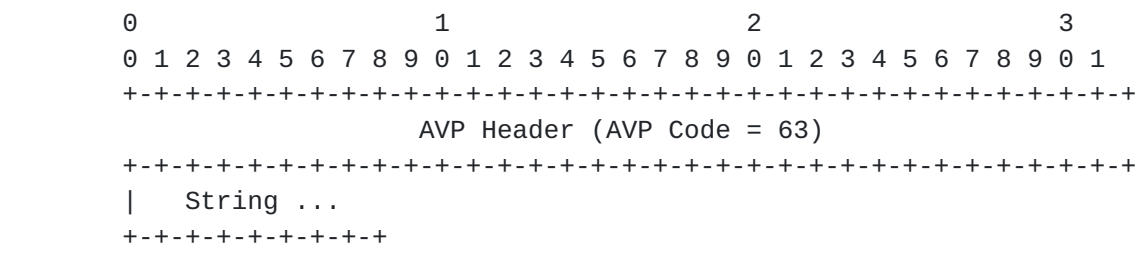
The Integer32 field is four octets, containing a 32-bit unsigned integer with the maximum number of ports this user should be allowed to connect to on the NAS.

3.33 Login-LAT-Port

Description

This AVP indicates the Port with which the user is to be connected by LAT. It MAY be used in AA-Answer messages, but only when LAT is specified as the Login-Service. It MAY be used in an AA-Request message as a hint to the server, but the server is not required to honor the hint.

AVP Format



AVP Flags

The 'M' bit MUST be set. The 'H' and 'E' MAY be set depending upon the security model used. The 'V', 'T' and the 'P' bits MUST NOT be set.

String

The String field is one or more octets, and contains the identity of the LAT port 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. All LAT string comparisons are case insensitive.

3.34 Tunnel-Type

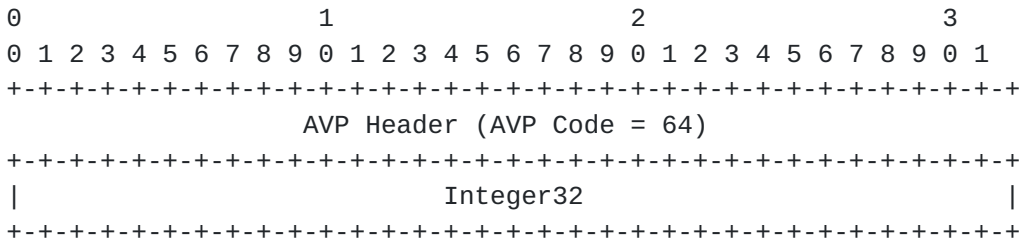
Description

This AVP indicates the tunneling protocol(s) to be used (in the case

of a tunnel initiator) or the the tunneling protocol in use (in the case of a tunnel terminator). It MAY be included in both AA-Request and AA-Answer. The Tunnel-Type SHOULD also be present in the corresponding ADIF Record within the Accounting-Request. If the Tunnel-Type AVP is present in an AA-Request message sent from a tunnel initiator, it SHOULD be taken as a hint to the DIAMETER server as to the tunnelling protocols supported by the tunnel end-point; the DIAMETER server MAY ignore the hint, however. A tunnel initiator is not required to implement any of these tunnel types; if a tunnel initiator receives an AA-Answer message which contains only unknown or unsupported Tunnel-Types, the tunnel initiator MUST behave as though an AA-Answer with a failure Result-Code had been received instead.

If the Tunnel-Type AVP is present in an AA-Request message sent from a tunnel terminator, it SHOULD be taken to signify the tunnelling protocol in use. In this case, if the DIAMETER server determines that the use of the communicated protocol is not authorized, it MAY return an AA-Answer with a failure Result-Code message. If a tunnel terminator receives an AA-Answer message which contains one or more Tunnel-Type AVPs, none of which represent the tunneling protocol in use, the tunnel terminator SHOULD behave as though an AA-Answer with a failure Result-Code had been received instead.

AVP Format



AVP Flags

The 'M' and 'T' bits MUST be set. The 'H' and 'E' MAY be set depending upon the security model used. The 'V', and 'P' bits MUST NOT be set.

Integer32

The Value field is three octets and contains one of the following values, indicating the type of tunnel to be started.

1 Point-to-Point Tunneling Protocol (PPTP) [14] 2 Layer Two Forwarding (L2F) [15] 3 Layer Two Tunneling Protocol (L2TP) [16] 4 Ascend Tunnel Management

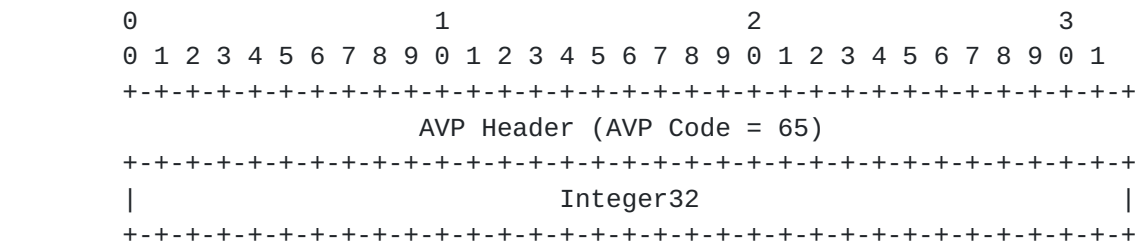
Protocol (ATMP) [17] 5 Virtual Tunneling Protocol (VTP) 6 IP Authentication Header in the Tunnel-mode (AH) [18] 7 IP-in-IP Encapsulation (IP-IP) [19] 8 Minimal IP-in-IP Encapsulation (MIN-IP-IP) [20] 9 IP Encapsulating Security Payload in the Tunnel-mode (ESP) [21] 10 Generic Route Encapsulation (GRE) [22] 11 Bay Dial Virtual Services (DVS) 12 IP-in-IP Tunneling [23]

3.35 Tunnel-Medium-Type

Description

The Tunnel-Medium-Type AVP indicates which transport medium to use when creating a tunnel for those protocols (such as L2TP) that can operate over multiple transports. It MAY be included in both AA-Request and AA-Answer messages; if it is present in an AA-Request message, it SHOULD be taken as a hint to the DIAMETER server as to the tunnel media supported by the tunnel end- point. The DIAMETER server MAY ignore the hint, however.

AVP Format



AVP Flags

The 'M' and 'T' bits MUST be set. The 'H' and 'E' MAY be set depending upon the security model used. The 'V', and 'P' bits MUST NOT be set.

Integer32

The Value field is three octets and contains one of the values listed under "Address Family Numbers" in [24]. For the sake of convenience, a relevant excerpt of this list is reproduced below.

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

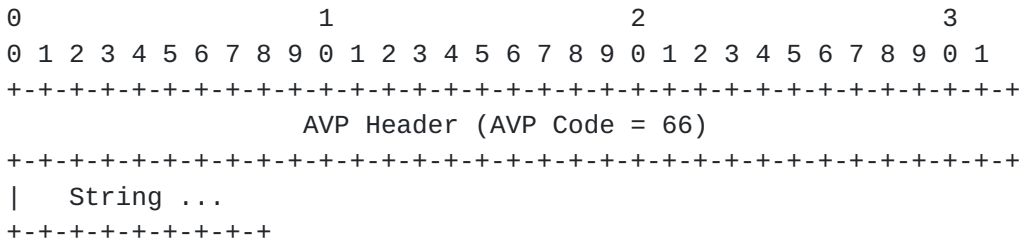
Relay, ATM) 9 F.69 (Telex) 10 X.121 (X.25, Frame Relay) 11 IPX 12 Appletalk 13 Decnet IV 14 Banyan Vines 15 E.164 with NSAP format subaddress

3.36 Tunnel-Client-Endpoint

Description

This AVP contains the address of the initiator end of the tunnel. It MAY be included in both AA-Request and AA-Answer messages to indicate the address from which a new tunnel is to be initiated. If the Tunnel-Client-Endpoint AVP is included in an AA-Request message, the DIAMETER server should take the value as a hint; the server is not obligated to honor the hint, however. This AVP SHOULD be included in the ADIF Record of 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 Acct-Tunnel-Connection-ID AVP, may be used to provide a globally unique means to identify a tunnel for accounting and auditing purposes.

AVP Format



AVP Flags

The 'M' and 'T' bits MUST be set. The 'H' and 'E' MAY be set depending upon the security model used. The 'V' and 'P' bits MUST NOT be set.

String

The format of the address represented by the String field depends upon the value of the Tunnel-Medium-Type attribute.

If Tunnel-Medium-Type is IPv4 (1), then this string is either the fully qualified domain name (FQDN) of the tunnel client machine, or it is a "dotted-decimal" IP address. Conformant 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 it is a text representation of the address in either the preferred or alternate form [25]. Conformant implementations MUST support the preferred form and SHOULD support both the alternate text form and the FQDN format for IPv6 addresses.

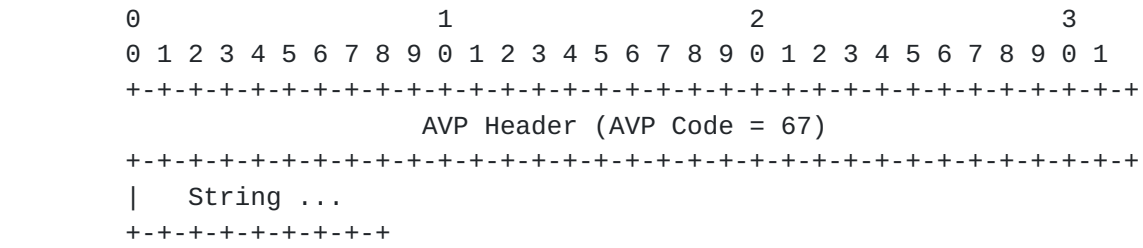
If Tunnel-Medium-Type is neither IPv4 nor IPv6, this string is a tag referring to configuration data local to the DIAMETER client that describes the interface and medium-specific address to use.

3.37 Tunnel-Server-Endpoint

Description

This AVP indicates the address of the server end of the tunnel. The Tunnel-Server-Endpoint AVP MAY be included (as a hint to the DIAMETER server) in the AA-Request message and MUST be included in the successful AA-Response message if the initiation of a tunnel is desired. It SHOULD be included in the corresponding ADIF-Record in the subsequent Accounting-Request messages. This AVP, along with the Tunnel-Client-Endpoint and Session-Id AVP [2], may be used to provide a globally unique means to identify a tunnel for accounting and auditing purposes.

AVP Format



AVP Flags

The 'M' and 'T' bits MUST be set. The 'H' and 'E' MAY be set depending upon the security model used. The 'V' and 'P' bits MUST NOT be set.

String

The format of the address represented by the String field depends upon the value of the Tunnel-Medium-Type attribute.

If Tunnel-Medium-Type is IPv4 (1), then this string is either the fully qualified domain name (FQDN) of the tunnel client machine, or it is a "dotted-decimal" IP address. Conformant 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 it is a text representation of the address in either the preferred or alternate form [25]. Conformant implementations MUST support the preferred form and SHOULD support both the alternate text form and the FQDN format for IPv6 addresses.

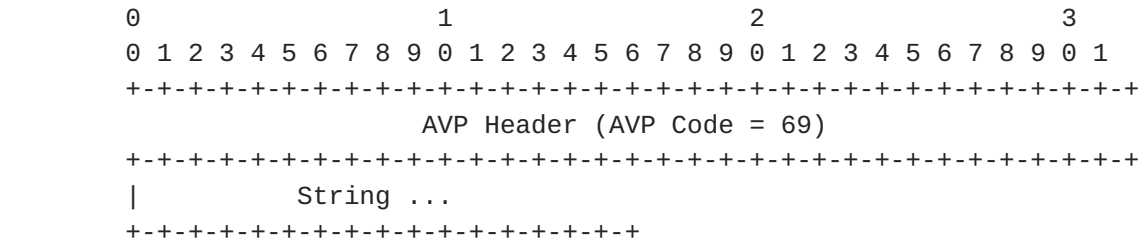
If Tunnel-Medium-Type is not IPv4 or IPv6, this string is a tag referring to configuration data local to the DIAMETER client that describes the interface and medium-specific address to use.

3.38 Tunnel-Password

Description

This AVP may contain a password to be used to authenticate to a remote server. It may only be included in an AA-Answer message.

AVP Format



AVP Flags

The 'M' and 'T' bits MUST be set. Either the 'H' and 'E' MUST be set depending upon the security model used. The 'V' and 'P' bits MUST NOT be set.

String

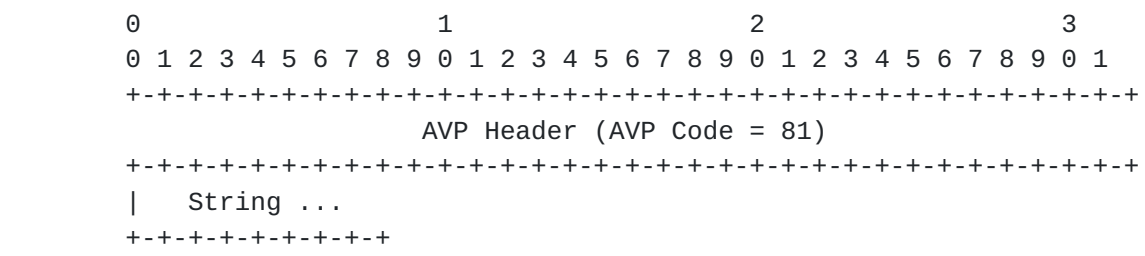
The String field contains the encrypted version of the Tunnel Password.

3.39 Tunnel-Private-Group-ID

Description

This AVP indicates the group ID for a particular tunneled session. The Tunnel-Private-Group-ID AVP MAY be included in the AA-Request message if the tunnel initiator can pre- determine the group resulting from a particular connection and SHOULD be included in the AA-Answer message 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 value SHOULD be included the corresponding ADIF-Record in the Accounting-Request which pertain to a tunneled session.

AVP Format



AVP Flags

The 'M' and 'T' bits MUST be set. The 'H' and 'E' MAY be set depending upon the security model used. The 'V' and 'P' bits MUST NOT be set.

String

This field must be present. The group is represented by the String field. There is no restriction on the format of group IDs.

3.40 Tunnel-Assignment-ID

Description

This AVP 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 utilize its own

dedicated tunnel. This attribute provides a mechanism for DIAMETER to be used 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 that provides an appropriate level of service. It is expected that any QOS-related DIAMETER tunneling attributes defined in the future that accompany this attribute 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 intended to be of only 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 the AA-Answer. The tunnel initiator receiving this attribute MAY choose to ignore it and assign the session to an arbitrary multiplexed or non-multiplexed tunnel between the desired endpoints. This attribute SHOULD also be included in the corresponding ADIF-Record in the Accounting-Request messages which pertain to a 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.

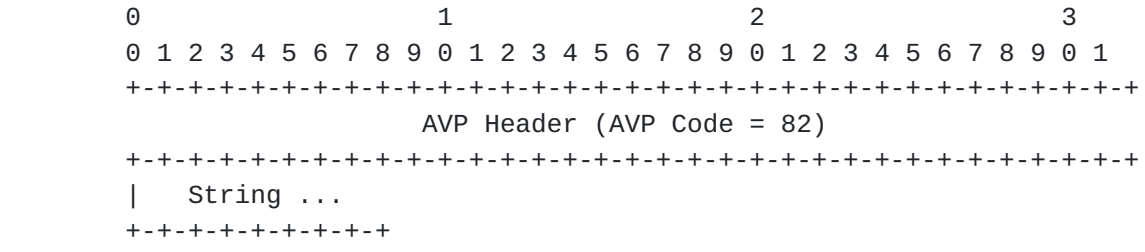
- If this AVP is present and no tunnel exists between the specified endpoints with the specified ID, then a new tunnel should be established for the session and the specified ID should be associated with the new tunnel.

- 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 and subsequent sessions 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 such tunnels are between different endpoints.

AVP Format



AVP Flags

The 'M' and 'T' bits MUST be set. The 'H' and 'E' MAY be set depending upon the security model used. The 'V' and 'P' bits MUST NOT be set.

String

This field must be present. The tunnel ID is represented by the String field. There is no restriction on the format of the ID.

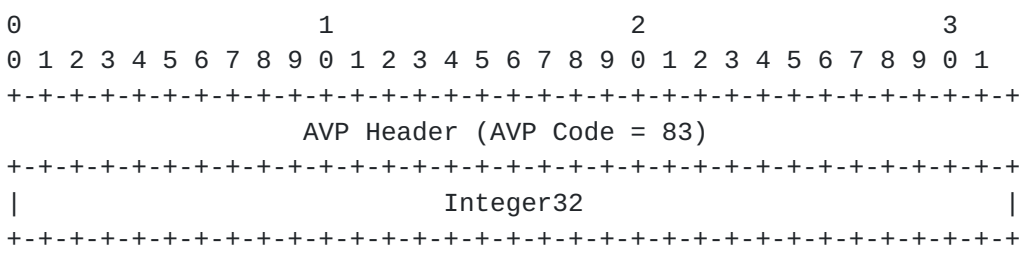
3.41 Tunnel-Preference

Description

If more than one set of tunneling attributes is returned by the DIAMETER server to the tunnel initiator, this AVP SHOULD be included in each set to indicate the relative preference assigned to each tunnel. 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 having the numerically lowest 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 AA-Answer message MAY be identical. In this case, the tunnel initiator SHOULD use locally configured metrics to decide which set of AVPs to use. This AVP MAY be included (as a hint to the server) in AA-Request messages, but the DIAMETER server is not required to honor this hint.

AVP Format



AVP Flags

The 'M' and 'T' bits MUST be set. The 'H' and 'E' MAY be set depending upon the security model used. The 'V', and 'P' bits MUST NOT be set.

Integer32

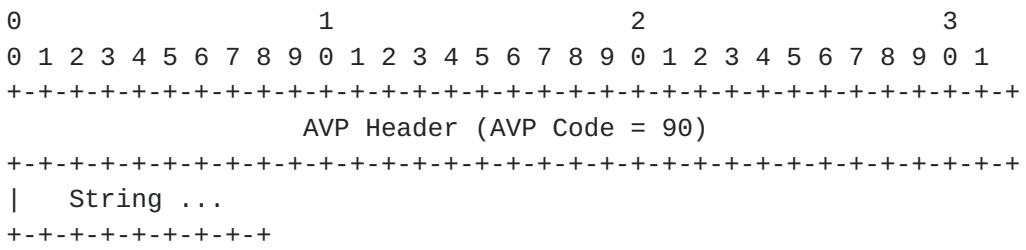
The Value field is three octets in length and indicates the preference to be given to the tunnel to which it refers; higher preference is given to lower values, with 0x000000 being most preferred and 0xFFFFFF least preferred.

3.42 Tunnel-Client-Auth-ID

Description

This AVP specifies the name used by the tunnel initiator during the authentication phase of tunnel establishment. The Tunnel-Client-Auth-ID AVP MAY be included (as a hint to the DIAMETER server) in the AA-Request message, and MUST be included in the AA-Request message if an authentication name other than the default is desired. This AVP SHOULD be included in the corresponding ADIF-Record of the Accounting-Request messages which pertain to a tunneled session.

AVP Format



AVP Flags

The 'M' and 'T' bits MUST be set. The 'H' and 'E' MAY be set depending upon the security model used. The 'V' and 'P' bits MUST NOT be set.

String

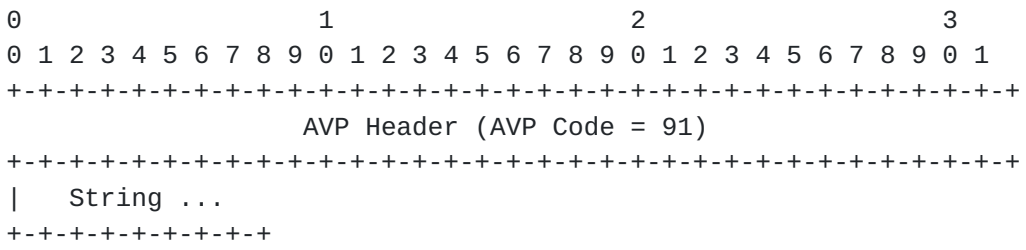
This field must be present. The String field contains the authentication name of the tunnel initiator. The authentication name SHOULD be represented in the UTF-8 charset.

3.43 Tunnel-Server-Auth-ID

Description

This AVP specifies the name used by the tunnel terminator during the authentication phase of tunnel establishment. The Tunnel-Client-Auth-ID AVP MAY be included (as a hint to the DIAMETER server) in the AA-Request message, and MUST be included in the AA-Request message if an authentication name other than the default is desired. This AVP SHOULD be included in the corresponding ADIF-Record of the Accounting-Request messages which pertain to a tunneled session.

AVP Format



AVP Flags

The 'M' and 'T' bits MUST be set. The 'H' and 'E' MAY be set depending upon the security model used. The 'V' and 'P' bits

MUST NOT be set.

String

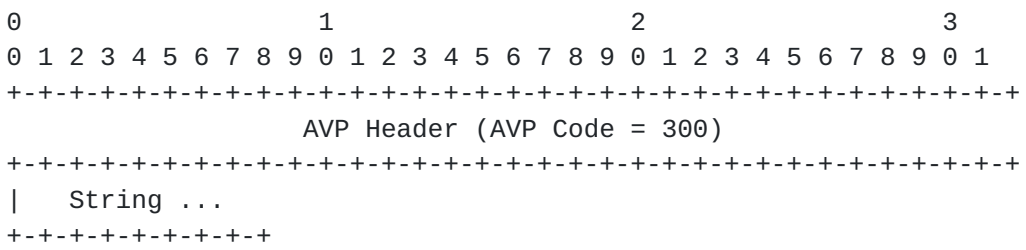
This field must be present. The String field contains the authentication name of the tunnel terminator. The authentication name SHOULD be represented in the UTF-8 charset.

3.44 Filter-Rule

Description

This AVP provides filter rules that need to be configured on the NAS for the user. It is used in the AA-Answer message and can appear multiple times.

AVP Format



AVP Flags

The 'M' bit MUST be set. The 'H' and 'E' MAY be set depending upon the security model used. The 'V', 'T' and the 'P' bits MUST NOT be set.

String

The String field MUST contain a filter rule in the following format: "permit (offset=value AND offset=value) OR offset=value" or "deny (offset=value AND offset=value) OR offset=value". The keyword "permit" means that the filter will allow any traffic that matches the rule, while deny will not allow the traffic to be routed. The filter rules can also use the keywords "AND" and "OR", for which no additional explanation is necessary. The braces "(" and ")" can be used to setup grouping of expressions.

3.45 Table of AVPs

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

AA-Req	Success AA-Answ	Failed AA-Answ	AA-Chal Req	#	AVP
0-1	0-1	0	0	1	User-Name
0-1	0	0	0	2	User-Password [*1]
0-1	0	0	0	3	CHAP-Password [*1]
0-1	0	0	0	5	NAS-Port
0-1	0-1	0	0	6	Service-Type
0-1	0-1	0	0	7	Framed-Protocol
0-1	0-1	0	0	8	Framed-IP-Address
0-1	0-1	0	0	9	Framed-IP-Netmask
0	0-1	0	0	10	Framed-Routing
0	0+	0	0	11	Filter-Id
0	0-1	0	0	12	Framed-MTU
0+	0+	0	0	13	Framed-Compression
0+	0+	0	0	14	Login-IP-Host
0	0-1	0	0	15	Login-Service
0	0-1	0	0	16	Login-TCP-Port
0	0+	0+	0+	18	Reply-Message
0-1	0-1	0	0	19	Callback-Number
0	0-1	0	0	20	Callback-Id
0	0+	0	0	22	Framed-Route
0	0-1	0	0	23	Framed-IPX-Network
0	0-1	0	0-1	28	Idle-Timeout
0-1	0	0	0	30	Called-Station-Id
0-1	0	0	0	31	Calling-Station-Id
0-1	0-1	0	0	34	Login-LAT-Service
0-1	0-1	0	0	35	Login-LAT-Node
0-1	0-1	0	0	36	Login-LAT-Group
0	0-1	0	0	37	Framed-AppleTalk-Link
0	0+	0	0	38	Framed-AppleTalk-Net.
0	0-1	0	0	39	Framed-AppleTalk-Zone
0-1	0	0	0	60	CHAP-Challenge
0-1	0	0	0	61	NAS-Port-Type
0-1	0-1	0	0	62	Port-Limit
0-1	0-1	0	0	63	Login-LAT-Port
0+	0+	0	0	64	Tunnel-Type
0+	0+	0	0	65	Tunnel-Medium-Type
0+	0+	0	0	66	Tunnel-Client-Endpoint
0+	0+	0	0	67	Tunnel-Server-Endpoint
0+	0+	0	0	69	Tunnel-Password
0+	0+	0	0	81	Tunnel-Private-Group-ID
0+	0+	0	0	82	Tunnel-Assignment-ID
0+	0+	0	0	83	Tunnel-Preference
0+	0+	0	0	90	Tunnel-Client-Auth-ID
0+	0+	0	0	91	Tunnel-Server-Auth-ID

AA-Req	Success AA-Answ	Failed AA-Answ	AA-Chal Req	#	Filter-Rule AVP
0	0+	0	0	280	

[*1] An AA-Request MUST NOT contain both a User-Password and a CHAP-Password AVP.

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

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

4.0 Protocol Definition

This section will outline how the DIAMETER Authentication Extension can be used.

4.1 Feature Advertisement/Discovery

As defined in [2], the Reboot-Ind and Device-Feature-Query messages can be used to inform a peer about locally supported DIAMETER Extensions. In order to advertise support of this extension, the Extension-Id AVP must be transmitted with a value of one (1).

4.2 Authorization Procedure

This specification allows two different types of Authorization procedures. The first method is identical to the way RADIUS works today and requires the AA-Request to contain the UserName as well as either the Password or the CHAP-Password AVPs.

The second method is used by NASes that send AA-Request whenever they receive an incoming call and want to get authorization from the DIAMETER Server to answer the call. In this case the AA-Request contains the NAS-IP-Address, the Calling-Station-Id and the Called-Station-Id AVPs.

In this case the DIAMETER Server can lookup the combination of the

Calling-Station-Id and the Called-Station-Id in order to ensure that the pair are authorized as per the local policy.

4.3 Integration with Resource-Management

Document [10] specifies the Resource-Token AVP that is used to carry information required for a DIAMETER server to rebuild its state information in the event of a crash or some other event that would cause the server to loose its state information.

When creating the Resource-Token AVP, the following AVPs MUST be present, in addition to the AVPs listed in [10]; the UserName AVP, the NAS-IP- Address, the NAS-Port. Any additional AVP MAY be included if the AVP is a resource that is being managed (i.e. Framed-IP-Address in the case where the DIAMETER Server is allocating IP Addresses out of a centrally managed address pool).

5.0 References

[1] Rigney, et alia, "RADIUS", RFC-2138, Livingston, April 1997
[2] Calhoun, Rubens, "DIAMETER Base Protocol", draft-calhoun-diameter-08.txt, Work in Progress, August 1999.
[3] Aboba, Beadles "The Network Access Identifier." RFC 2486. January 1999.
[4] Aboba, Zorn, "Criteria for Evaluating Roaming Protocols", RFC 2477, January 1999.
[5] Calhoun, Rubens, Aboba, "DIAMETER Extensible Authentication Protocol Extensions", draft-calhoun-diameter-eap-03.txt, Work in Progress, August 1999.
[6] W. Simpson, "PPP Challenge Handshake Authentication Protocol (CHAP)", RFC 1994, August 1996.
[7] Jacobson, "Compressing TCP/IP headers for low-speed serial links", RFC 1144, February 1990.
[8] 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>
[9] Sklower, Lloyd, McGregor, Carr, "The PPP Multilink Protocol (MP)", RFC 1717, November 1994.
[10] Calhoun, Greene, "DIAMETER Resource Management Extension", draft-calhoun-diameter-res-mgmt-02.txt, Work in Progress, February 1999.
[11] Calhoun, Zorn, Pan, "DIAMETER Framework", draft-calhoun-diameter-framework-02.txt, Work in Progress, December 1998.

[12] S. Bradner, "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.
[13] P. Calhoun, W. Bulley, "DIAMETER Proxy Server Extensions", draft-calhoun-diameter-proxy-02.txt, Work in Progress, August 1999.
[14] Hamzeh, K., Pall, G., Verthein, W., Taarud, J., Little, W., Zorn, G., "Point-to-Point Tunneling Protocol (PPTP)", RFC 2637, July 1999
[15] Valencia, A., Littlewood, M., Kolar, T., "Cisco Layer Two Forwarding (Protocol) 'L2F'", RFC 2341, May 1998
[16] Townsley, W. M., Valencia, A., Rubens, A., Pall, G. S., Zorn, G., Palter, B., "Layer Two Tunnelling Protocol (L2TP)", RFC 2661, August 1999
[17] Hamzeh, K., "Ascend Tunnel Management Protocol - ATMP", RFC 2107, February 1997
[18] Kent, S., Atkinson, R., "Security Architecture for the Internet Protocol", RFC 2401, November 1998
[19] Perkins, C., "IP Encapsulation within IP", RFC 2003, October 1996
[20] Perkins, C., "Minimal Encapsulation within IP", RFC 2004, October 1996
[21] Atkinson, R., "IP Encapsulating Security Payload (ESP)", RFC 1827, August 1995
[22] Hanks, S., Li, T., Farinacci, D., Traina, P., "Generic Routing Encapsulation (GRE)", RFC 1701, October 1994
[23] Simpson, W., "IP in IP Tunneling", RFC 1853, October 1995
[24] Reynolds, J., Postel, J., "Assigned Numbers", STD 2, RFC 1700, October 1994
[17] Hinden, R., Deering, S., "IP Version 6 Addressing Architecture", RFC 2373, July 1998

6.0 Acknowledgements

The Author wishes to thank Carl Rigney since much of the text in the document was shamefully copied from [1] as well as the following people for their help in the development of this protocol:

Nancy Greene, Ryan Moats

7.0 Authors' Addresses

Questions about this memo can be directed to:

Pat R. Calhoun
Network and Security Research Center, Sun Labs
Sun Microsystems, Inc.
15 Network Circle

Menlo Park, California, 94025
USA

Phone: 1-650-786-7733
Fax: 1-650-786-6445
E-mail: pcalhoun@eng.sun.com

William Bulley
Merit Network, Inc.
4251 Plymouth Road, Suite C
Ann Arbor, Michigan, 48105-2785
USA

Phone: 1-734-764-9993
Fax: 1-734-647-3185
E-mail: web@merit.edu

8.0 Full Copyright Statement