TECHNICAL REPORT

TR-341
Radius Attributes Catalog

Issue: 1
Date: July 2016

Notice

The Broadband Forum is a non-profit corporation organized to create guidelines for broadband network system development and deployment. This Technical Report has been approved by members of the Forum. This Technical Report is subject to change. This Technical Report is copyrighted by the Broadband Forum, and all rights are reserved. Portions of this Technical Report may be copyrighted by Broadband Forum members.

Intellectual Property

Recipients of this Technical Report are requested to submit, with their comments, notification of any relevant patent claims or other intellectual property rights of which they may be aware that might be infringed by any implementation of this Technical Report, or use of any software code normatively referenced in this Technical Report, and to provide supporting documentation.

Terms of Use

1. License

Broadband Forum hereby grants you the right, without charge, on a perpetual, non-exclusive and worldwide basis, to utilize the Technical Report for the purpose of developing, making, having made, using, marketing, importing, offering to sell or license, and selling or licensing, and to otherwise distribute, products complying with the Technical Report, in all cases subject to the conditions set forth in this notice and any relevant patent and other intellectual property rights of third parties (which may include members of Broadband Forum). This license grant does not include the right to sublicense, modify or create derivative works based upon the Technical Report except to the extent this Technical Report includes text implementable in computer code, in which case your right under this License to create and modify derivative works is limited to modifying and creating derivative works of such code. For the avoidance of doubt, except as qualified by the preceding sentence, products implementing this Technical Report are not deemed to be derivative works of the Technical Report.

2. NO WARRANTIES

THIS TECHNICAL REPORT IS BEING OFFERED WITHOUT ANY WARRANTY WHATSOEVER, AND IN PARTICULAR, ANY WARRANTY OF NONINFRINGEMENT IS EXPRESSLY DISCLAIMED. ANY USE OF THIS TECHNICAL REPORT SHALL BE MADE ENTIRELY AT THE IMPLEMENTER'S OWN RISK, AND NEITHER THE BROADBAND FORUM, NOR ANY OF ITS MEMBERS OR SUBMITTERS, SHALL HAVE ANY LIABILITY WHATSOEVER TO ANY IMPLEMENTER OR THIRD PARTY FOR ANY DAMAGES OF ANY NATURE WHATSOEVER, DIRECTLY OR INDIRECTLY, ARISING FROM THE USE OF THIS TECHNICAL REPORT.

3. THIRD PARTY RIGHTS

Without limiting the generality of Section 2 above, BROADBAND FORUM ASSUMES NO RESPONSIBILITY TO COMPILE, CONFIRM, UPDATE OR MAKE PUBLIC ANY THIRD PARTY ASSERTIONS OF PATENT OR OTHER INTELLECTUAL PROPERTY RIGHTS THAT MIGHT NOW OR IN THE FUTURE BE INFRINGED BY AN IMPLEMENTATION OF THE TECHNICAL REPORT IN ITS CURRENT, OR IN ANY FUTURE FORM. IF ANY SUCH

RIGHTS ARE DESCRIBED ON THE TECHNICAL REPORT, BROADBAND FORUM TAKES NO POSITION AS TO THE VALIDITY OR INVALIDITY OF SUCH ASSERTIONS, OR THAT ALL SUCH ASSERTIONS THAT HAVE OR MAY BE MADE ARE SO LISTED.

The text of this notice must be included in all copies of this Technical Report.

Issue History

Issue Number	Approval Date	Publication Date	Issue Editor	Changes
1	18 July 2016	5 August 2016	Frederic Klamm, Orange	Original

Editors	Devasena Morrissette	Verizon	
	Frederic Klamm	Orange	frederic.klamm@orange.com
Wireline-Wireless Convergence WA Directors	David Allan	Ericsson	david.i.allan@ericsson.com
	Hongyu Li	Huawei	hongyu.li@huawei.com

TABLE OF CONTENTS

EXECUTIVE SUMMARY 6

1 PURPOSE AND SCOPE 7

1.1 PURPOSE 7
1.2 SCOPE 7

2 REFERENCES AND TERMINOLOGY 8

2.1 REFERENCES 8
2.2 DEFINITIONS 9
2.3 ABBREVIATIONS 10

3 TECHNICAL REPORT IMPACT 12

3.1 ENERGY EFFICIENCY 12
3.2 IPV6 12
3.3 SECURITY 12
3.4 PRIVACY 12

4 STANDARD ATTRIBUTES 13

4.1 DESCRIPTION 13
4.2 APPLICABILITY IN AUTHENTICATION AND DYNAMIC AUTHORIZATION MESSAGES 18
4.3 APPLICABILITY IN ACCOUNTING MESSAGES 21

5 BBF SPECIFIC ATTRIBUTES 24

5.1 DESCRIPTION 24
5.2 APPLICABILITY IN AUTHENTICATION AND DYNAMIC AUTHORIZATION MESSAGES 27
5.3 APPLICABILITY IN ACCOUNTING MESSAGES 28

6 OTHER RADIUS VENDOR SPECIFIC ATTRIBUTES 29

List of Tables

Table 1: Description of standard attributes 18
Table 2: Standard attributes in authentication and dynamic authorization messages 21
Table 3: Standard attributes in accounting messages 23
Table 4: Description of BBF-specific attributes 26
Table 5: BBF-specific attributes in authentication and dynamic authorization messages 28
Table 6: BBF-specific attributes in accounting messages 29
Table 7: Description of other useful vendor-specific attributes 32

Executive Summary

This document, called BBF RADIUS Catalog, is a registry of the RADIUS AVPs commonly used in the context of the BBF. This includes general purpose attributes which are standardized at the IETF, attributes which have been specified specifically for the Broadband Forum, and attributes which are not yet standardized, but of very common use in the Broadband Forum context.

For each of the registered attribute, the catalog provides a description, contextual information if needed, the messages they may be in, the BBF Technical Report evoking them, and, when appropriate, identifies the IETF RFC that defines them.

1 Purpose and Scope

1.1 Purpose

RADIUS messages, together with associated attributes are identified in TR-58, TR-102, and TR-144 as well as in other technical reports such as TR-101, TR-134, TR-146 and TR-178. The purpose of this Working Text is to consolidate BBF AAA work into a single concise catalog for authentication, authorization and accounting functions.

This Working Text may facilitate the standardization of common vendor specific attributes.

1.2 Scope

This Working Text focuses on the consolidation of the existing BBF AAA work found in various BBF TRs into a concise catalog. This includes IETF standard attributes, BBF-specific attributes, and vendor specific attributes when they are widely used in the MSBN context.
In future versions of this catalog, there may be an opportunity to standardize vendor-specific extensions to lower the interop and deployment burden on operators.

This catalog can be seen as a basis for an information model for authentication, authorization and accounting functions within a BBF network.

Only the RADIUS AAA protocol is considered in this issue.

2 References and Terminology

2.1 References

The following references are of relevance to this Technical Report. At the time of publication, the editions indicated were valid. All references are subject to revision; users of this Technical Report are therefore encouraged to investigate the possibility of applying the most recent edition of the references listed below.
A list of currently valid Broadband Forum Technical Reports is published at www.broadband-forum.org.

Document		Title	Source	Year
[1]	TR-059	*DSL Evolution – Architecture Requirements for the Support of QoS-Enabled IP Services*	BBF	2003
[2]	TR-092	*Broadband Remote Access Server Requirements Document*	BBF	2004
[3]	TR-101 Issue 2	*Migration to Ethernet-Based Broadband Aggregation*	BBF	2011
[4]	TR-134 Corrigendum 1	*Broadband Policy Control Framework (BPCF)*	BBF	2013
[5]	TR-146	*Subscriber Sessions*	BBF	2013
[6]	TR-147	*Layer 2 Control Mechanism For Broadband Multi-Service Architectures*	BBF	2008
[7]	TR-177	*IPv6 in the context of TR-101*	BBF	2010
[8]	TR-178	*Multi-service Broadband Network Architecture and Nodal Requirements*	BBF	2014
[9]	TR-187 Issue 2	*IPv6 for PPP Broadband Access*	BBF	2013
[10]	TR-242 Issue 1	*IPv6 Transition Mechanisms for Broadband Networks*	BBF	2012
[11]	TR-317	*Network Enhanced Residential Gateway*	BBF	2016
[12]	TR-321	*Public Wi-Fi Access*	BBF	2015
[13]	RFC 2119	*Key words for use in RFCs to Indicate Requirement Levels*	IETF	1997
[14]	RFC 2865	*Remote Authentication Dial In User Service (RADIUS)*	IETF	2000
[15]	RFC 2866	*RADIUS Accounting*	IETF	2000
[16]	RFC 2867	*RADIUS Tunnel Accounting Support*	IETF	2000
[17]	RFC 2868	*RADIUS Attributes for Tunnel Protocol Support*	IETF	2000

[18]	RFC 2869	*RADIUS Extensions*	IETF	2000
[19]	RFC 3004	*The User Class Option for DHCP*	IETF	2000
[20]	RFC 3118	*Authentication for DHCP messages*	IETF	2001
[21]	RFC 3162	*RADIUS and Ipv6*	IETF	2001
[22]	RFC 3315	*Dynamic Host Configuration Protocol for IPv6 (DHCPv6)*	IETF	2003
[23]	RFC 3579	*RADIUS (Remote Authentication Dial In User Service) Support For Extensible Authentication Protocol (EAP)*	IETF	2003
[24]	RFC 3580	*IEEE 802.1X Remote Authentication Dial In User Service (RADIUS) Usage Guidelines*	IETF	2003
[25]	RFC 4679	*DSL Forum Vendor-Specific RADIUS Attributes*	IETF	2006
[26]	RFC 4818	*RADIUS Delegated-IPv6-Prefix Attribute*	IETF	2007
[27]	RFC 5176	*Dynamic Authorization Extensions to Remote Authentication Dial In User Service(RADIUS)*	IETF	2008
[28]	RFC 5580	*Carrying Location Objects in RADIUS and Diameter*	IETF	2009
[29]	RFC 6911	*RADIUS IPv6 Access*	IETF	2013

2.2 Definitions

The following terminology is used throughout this Technical Report.

Standard Attribute	Attribute defined and numbered in IETF RFCs as part of the RADIUS protocol.
Vendor-specific Attribute	Attribute defined by particular vendors for their specific context. It is part of a RADIUS dictionary identified by an IANA enterprise number allocated to the vendor.
BBF-specific Attributes	Attribute defined by the Broadband Forum for its specific context. They are initially described in RFC 4679[25] as “DSL Forum Attributes” and will be extended by this document. They are registered under the IANA assigned vendor ID 3561.
Authentication Attribute	Attribute carrying either authentication associated authorization or configuration information; between a Network Access Server and a shared Authentication Server in order to authenticate the subscribers (see RFC 2865[14]).

Accounting Attribute	Attribute carrying accounting information between a Network Access Server and a shared Accounting Server (see RFC 2866[15]).
Dynamic Authorization Attribute	Attribute sent in RADIUS messages allowing dynamic changes to a user session, as implemented by network access server products. This includes support for disconnecting users and changing authorizations applicable to a user session (see RFC 5176[27]).

2.3 Abbreviations

This Technical Report uses the following abbreviations:

ACK, NAK	ACKnowledged, Non AcKnowledged
ANCP	Access Node Control Protocol
AVP	Attribute Value Pair
CHAP	(PPP) Challenge Handshake Authentication Protocol
CoA	Change of Authorization
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name Service
DSLAM	Digital Subscriber Line Access Multiplexer
EAP	Extensible Authorization Protocol
HTTP	HyperText Transfer Protocol
IANA	Internet Assigned Numbers Authority
IGMP	Internet Group Management Protocol
IPCP	Internet Protocol Control Protocol
IWF	InterWorking Function
MAC	Media Access Control
MLD	Multicast Listener Discovery (protocol)
NAS	Network Access Server
PPP	Point-to-point protocol
PPPoA/oE	PPP over ATM/over Ethernet
QoS	Quality of Service
RADIUS	Remote Authentication Dial In User Service (RFC2865)
TLV	Type-Length-Value (encoding)
TR	Technical Report
URI	Uniform Resource Identifier
VPN	Virtual Private Network

VSA	Vendor Specific Attribute
WA	Working Area

3 Technical Report Impact

3.1 Energy Efficiency

TR-341 has no impact on energy efficiency.

3.2 IPv6

TR-341 has no impact on IPv6.

3.3 Security

TR-341 contains information usable by certain security mechanism, especially for authentication. But it has no impact on security in a given architecture.

3.4 Privacy

Any issues regarding privacy are not affected by TR-341.

4 Standard attributes

This section describes the RADIUS attributes that are commonly used in BBF networks, and specified in IETF RFCs.

4.1 Description

Each description below is provided for convenience. It is a simplification of the description that can be found in the reference RFC, together with more semantic and syntax information.

AVP ID	AVP Name	Description	Reference(s)
1	User-Name	The name of the user to be authenticated	RFC2865 [14]
2	Password	The password of the user to be authenticated.	RFC2865 [14]
3	CHAP-Password	The response value provided by a PPP CHAP user in response to the challenge.	RFC2865 [14]
4	NAS-IP-Address	The identifying IP address of the NAS which is requesting authentication of the user.	RFC2865 [14]
5	NAS-Port	The physical port number of the NAS which is authenticating the user.	RFC2865 [14]
6	Service-Type	The type of service the user has requested or the type of service to be provided.	RFC2865 [14]
7	Framed-Protocol	The framing to be used for framed access (e.g. 'PPP')	RFC2865 [14]
8	Framed-IP-Address	The IPv4 address to be configured for the user.	RFC2865 [14]
9	Framed-IP-Netmask	Indicates the IP netmask to be configured for the user when the user is a router.	RFC2865 [14]
18	Reply-Message	Normalized error cause. WRIX-i proxy normalizes the error code to a given list.	RFC2865 [14]
22	Framed-Route	Provides routing information to be configured for the user on the NAS. It can appear multiple times.	RFC2865 [14]
24	State	This attribute is available to be sent by the server to the client in an Access-Challenge and must be sent unmodified from the client to the server in	RFC2865 [14]

		the new Access-Request reply to that challenge	
25	Class	Generic, available to be sent by the server to the client and to be sent unmodified by the client to the accounting server as part of the Accounting-Request packet if accounting is supported.	RFC2865 [14]
27	Session-Time-Out	Sets the maximum number of seconds of service to be provided to the user before termination of the session or prompt.	RFC2865 [14]
28	Idle-Timeout	Sets the maximum number of consecutive seconds of idle connection allowed to the user before termination of the session.	RFC2865 [14]
30	Called-Station-Id	Allows the NAS to send in the Access-Request packet the phone number that the user called, using DNIS or similar technology. This may be different from the phone number the call comes in on. This attribute may also be used for other purposes in broadband networks (e.g. indicating SSID in Wi-Fi scenarios)	RFC2865 [14]
31	Calling-Station-Id	Id of the entity from which the call came from.	RFC2865 [14]
32	NAS Identifier	A string identifying the NAS originating the Access-Request.	RFC2865 [14]
33	Proxy-State	This Attribute is available to be sent by a proxy server to another server when forwarding an Access-Request. It must be returned unmodified in the Access-Accept, Access-Reject or Access-Challenge.	RFC2865 [14]
40	Acct-Status-Type	Indicates whether this Accounting-request marks the beginning of the user service (Start) or the end (Stop).	RFC2866 [15]
41	Acct-Delay-Time	Indicates how many seconds the client has been trying to send this record for, and can be subtracted from the time of arrival on the server to find the approximate time of the event generating this Accounting-Request.	RFC2866 [15]
42	Acct-Input-Octets	Indicates how many octets have been received	RFC2866 [15]

		from the port over the course of delivering this service being provided.	
43	Acct-Output-Octets	Indicates how many octets have been sent to the port over the course of delivering this service.	RFC2866 [15]
44	Acct-Session-Id	A unique Accounting ID to make it easy to match Request and stop records in a log file.	RFC2866 [15]
46	Acct-Session-Time	Indicates how many seconds the user has received service for, and can only be present.	RFC2866 [15]
47	Acct-Input-Packets	Indicates how many octets have been received from the port over the course of delivering this service.	RFC2866 [15]
48	Acct-Output-Packets	Indicates how many octets have been sent to the port over the course of delivering this service.	RFC2866 [15]
49	Acct-Terminate-Cause	Indicates how the session was terminated.	RFC2866 [15]
50	Acct-Multi-Session--Id	Unique Accounting ID to link together multiple related sessions in log file. Each session would have a unique Acct-Session-Id but the same Acct-Multi-Session-Id.	RFC2866 [15]
52	Acct-Input-Gigawords	indicates how many times the Acct-Input-Octets counter has wrapped around 2^32 over the course of this service being provided.	RFC2869 [18]
53	Acct-Output-Gigawords	Indicates how many times the Acct-Output-Octets counter has wrapped around 2^32 in the course of delivering this service.	RFC2869 [18]
55	Event-Time-Stamp	Included to record the time at which that this event occurred on the NAS, in seconds since January 1, 1970 00:00 UTC.	RFC2869 [18]
60	CHAP- Challenge	The CHAP Challenge sent by the NAS to a PPP Challenge - Handshake Authentication Protocol (CHAP) user.	RFC2865 [14]
61	NAS-Port-Type	The type of the physical port of the NAS which is authenticating the user (e.g. xDSL, PPPoEoE).	RFC2865 [14]
64	Tunnel-Type	Indicates the tunneling protocol(s) to be used (in the case of a tunnel initiator) or the tunneling protocol in use (in the case of a tunnel	RFC2868 [17]

		terminator).	
65	Tunnel-Medium-Type	Indicates which transport medium to use when creating a tunnel for those protocols (such as L2TP) that can operate over multiple transports.	RFC2868 [17]
66	Tunnel-Client-Endpoint	Contains the address of the initiator end of the tunnel.	RFC2868 [17]
67	Tunnel-Server-Endpoint	Contains the address of the initiator end of the tunnel.	RFC2868 [17]
68	Acct-Tunnel-Connection	Indicates the identifier assigned to the tunnel session.	RFC2867 [16]
69	Tunnel-Password	May contain a password to be used to authenticate to a remote server.	RFC2868 [17]
79	EAP-Message	Encapsulates EAP packets so as to allow the NAS to authenticate peers via EAP without having to understand the EAP method it is passing through. If EAP authentication is used, this attribute is mandatory.	RFC3579 [23]
80	Message-Authenticator	May be used to authenticate and integrity-protect Access-Requests in order to prevent spoofing.	RFC3579 [23]
81	Tunnel-Private-Group-ID	Indicates the group ID for a particular tunneled session. Private groups may be used to associate a tunneled session with a particular group of users (e.g. to facilitate routing of unregistered IP addresses through a particular interface.	RFC2868 [17]
82	Tunnel-Assignment-ID	Indicate to the tunnel initiator the particular tunnel to which a session is to be assigned. It provides a mechanism for RADIUS to be used to inform the tunnel initiator whether to assign the session to a multiplexed or a separate tunnel.	RFC2868 [17]
83	Tunnel-Preference	If more than one set of tunneling attributes is returned by the RADIUS server to the tunnel initiator, this attribute should be included in each set to indicate the relative preference assigned to	RFC2868 [17]

		each tunnel.	
85	Acct-Interim-Interval	Indicates the number of seconds between each interim update in seconds for this specific session.	RFC2869 [18]
87	NAS-Port-Id	A text string which identifies the port of the NAS which is authenticating the user. Intended for use by NASes which cannot conveniently number their ports.	RFC2869 [18]
88	Framed-Pool	Contains the name of an assigned address pool that should be used to assign an address for the user.	RFC2869 [18]
89	Chargeable-User-Identity	Support for this AVP is highly recommended. However, if the billable user's identity is masked through encryption or other means, then it is mandatory in Access-Accept.	RFC4372
90	Tunnel-Client-Auth-ID	Specifies the name used by the tunnel initiator during the authentication phase of tunnel establishment.	RFC2868 [17]
91	Tunnel-Server-Auth-ID	Specifies the name used by the tunnel terminator during the authentication phase of tunnel establishment.	RFC2868 [17]
95	NAS-IPv6-Address	Indicates the identifying IPv6 Address of the NAS which is requesting authentication of the user, and should be unique to the NAS within the scope of the RADIUS server.	RFC3162 [21]
97	Framed-IPv6-Prefix	Indicates an IPv6 prefix (and corresponding route) to be configured for the user.	RFC3162 [21]
99	Framed-IPv6-Route	Provides routing information to be configured for the user on the NAS.	RFC3162 [21]
100	Framed-IPv6-Pool	Contains the name of an assigned pool that should be used to assign an IPv6 prefix for the user.	RFC3162 [21]
123	Delegated-IPv6-Prefix	An IPv6 prefix that is to be delegated to the user, for use in the user's network.	RFC4818 [26]

126	Operator-Name	Carries the operator namespace identifier and the operator name. The operator name is combined with the namespace identifier to uniquely identify the owner of an access network.	RFC5580 [28]
127	Location-Information	Provides meta-data about the location information, such as sighting time, time-to-live, location-determination method, etc. It will be only provided in those cases when the Hotspot can be located.	RFC5580 [28]
128	Location-Data	Describe the location of an entity using the civil location profile or the geospatial profile as described in RFC5580, §4.3.	RFC5580 [28]
129	Basic-Location-Policy-Rules	Contains flags indicating privacy settings. Used to control the distribution of location information.	RFC5580 [28]
130	Extended-Location-Policy-Rules	Contains a Ruleset Reference, i.e. a URI that indicates where the richer ruleset can be found.	RFC5580 [28]
131	Location-Capable	Allows an NAS (or client function of a proxy server) to indicate support for carrying location objects in RADIUS.	RFC5580 [28]
132	Requested-Location-Info	Allows the RADIUS server to indicate which location information about which entity it wants to receive.	RFC5580 [28]
169	DNS-Server-IPv6-Address	The IPv6 address of a DNS server. It may be included multiple times in Access-Accept packets.	RFC6911 [29]

Table 1: Description of standard attributes

4.2 Applicability in authentication and dynamic authorization messages

Table 2 indicates the number of times an individual AVP will appear in each of the listed authentication and dynamic authorization message types.

AVP ID	AVP Name	Access Request	Access Accept	CoA Request

1	User-Name	1	0-1	0-1
2	Password	0-1	0	0
3	CHAP-Password	0-1	0	0
4	NAS-IP-Address	0-1	0	0
5	NAS-Port	0-1	0	0
6	Service-Type	0-1	0-1	0-1
7	Framed-Protocol	0-1	0-1	0-1
8	Framed-IP-Address	0	0-1	0-1
9	Framed-IP-Netmask	0	0-1	0
18	Reply-Message	0	0-1	0
22	Framed-Route	0	0+	0
24	State	0-1	0-1	0-1
25	Class	0	0+	0+
27	Session-Time-Out	0	0-1	0-1
28	Idle-Timeout	0	0-1	0-1
30	Called-Station-Id	0-1	0	0-1
31	Calling-Station-Id	0-1	0-1	0-1
32	NAS-Identifier	0-1	0	0
33	Proxy-State	0+	0+	0+
44	Acct-Session-Id	0-1	0	0-1
55	Event-Time-Stamp	0	0	0-1
60	CHAP-Challenge	0-1	0	0
61	NAS-Port-Type	0-1	0	0-1
64	Tunnel-Type	0-1	1	0

65	Tunnel-Medium-Type	0-1	1	0
66	Tunnel-Client-Endpoint	0-1	0-1	0
67	Tunnel-Server-Endpoint	0-1	1	0
69	Tunnel-Password	0	0-1	0
79	EAP-Message	0+	0+	0
80	Message-Authenticator	0-1	0-1	0
81	Tunnel-Private-Group-Id	0-1	0-1	0
82	Tunnel-Assignment-Id	0	0-1	0
83	Tunnel-Preference	0	0-1	0
85	Acct-Interim-Interval	0	0-1	0-1
87	NAS-Port-Id	0-1	0	0-1
88	Framed-Pool	0	0-1	0
89	Chargeable-User-Identity	0-1	0-1	0-1
90	Tunnel-Client-Auth-Id	0-1	0-1	0
91	Tunnel-Server-Auth-Id	0-1	0-1	0
95	NAS-IPv6-Address	0-1	0	0
97	Framed-IPv6-Prefix	0	0-1	0-1
99	Framed-IPv6-Route	0	0+	0
100	Framed-IPv6-Pool	0	0-1	0
123	Delegated-IPv6-Prefix	0	0-1	0+
126	Operator-Name	0-1	0-1	0
127	Location-Information	0+	0	0
128	Location-Data	0+	0	0
129	Basic-Location-Policy-Rules	0-1	0-1	0-1

130	Extended-Location-Policy-Rules	0-1	0-1	0-1
131	Location-Capable	0-1	0	0
132	Requested-Location-Info	0	0-1	0-1
169	DNS-Server-IPv6-Address	0	0-1	0-1

Table 2: Standard attributes in authentication and dynamic authorization messages

4.3 Applicability in accounting messages

Table 3 indicates the number of times an individual AVP will appear in each of the listed accounting message types.

AVP ID	AVP Name	Acct Start	Acct Stop	Acct Interim Update	Acct On	Acct Off
1	User-Name	1	0-1	0-1	0	0
4	NAS-IP-Address	0-1	0	0	0-1	0-1
5	NAS-Port	0-1	0-1	0-1	0	0
6	Service-Type	1	1	1	0	0
7	Framed-Protocol	1	1	1	0	0
8	Framed-IP-Address	0-1	0-1	0-1	0	0
9	Framed-IP-Netmask	0-1	0-1	0-1	0	0
22	Framed-Route	0+	0+	0+	0	0
25	Class	0+	0+	0+	0	0
30	Called-Station-Id	0-1	0-1	0-1	0	0
31	Calling-Station-Id	0-1	0-1	0-1	0	0
32	NAS-Identifier	0-1	0-1	0-1	0	0
33	Proxy-State	0+	0+	0+	0	0
40	Acct-Status-Type	1	1	1	1	1

41	Acct-Delay-Time	0-1	0-1	0-1	0-1	0-1
42	Acct-Input-Octets	0	0-1	0-1	0	0
43	Acct-Output-Octets	0	0-1	0-1	0	0
44	Acct-Session-Id	1	1	1	1	1
46	Acct-Session-Time	0	0-1	0-1	0	0
47	Acct-Input-Packets	0	0-1	0-1	0	0
48	Acct-Output-Packets	0	0-1	0-1	0	0
49	Acct-Terminate-Cause	0	1	0	0	1
50	Acct-Multi-Session-Id	0-1	0-1	0-1	0	0
52	Acct-Input-Gigawords	0	0-1	0-1	0	0
53	Acct-Output-Gigawords	0	0-1	0-1	0	0
55	Event-Time-Stamp	1	1	1	1	1
61	NAS-Port-Type	0-1	0-1	0-1	0	0
64	Tunnel-Type	0-1	0-1	0-1	0	0
65	Tunnel-Medium-Type	0-1	0-1	0-1	0	0
66	Tunnel-Client-Endpoint	0-1	0-1	0-1	0	0
67	Tunnel-Server-Endpoint	0-1	0-1	0-1	0	0
68	Acct-Tunnel-Connection	0-1	0-1	0-1	0	0
87	NAS-Port-Id	0-1	0-1	0-1	0	0
90	Tunnel-Client-Auth-ID	0-1	0-1	0-1	0	0
91	Tunnel-Server-Auth-ID	0-1	0-1	0-1	0	0
95	NAS-IPv6-Address	0-1	0-1	0-1	0-1	0-1
96	Framed-Interface-Id	0-1	0-1	0-1	0	0
97	Framed-IPv6-Prefix	0-1	0-1	0-1	0	0

99	Framed-IPv6-Route	0+	0+	0+	0	0
123	Delegated-IPv6-Prefix	0-1	0-1	0-1	0	0
89	Chargeable-User-Identity	0-1	0-1	0-1	0	0
126	Operator-Name	0+	0+	0+	0	0
127	Location-Information	0+	0+	0+	0	0
128	Location-Data	0+	0+	0+	0	0
129	Basic-Location-Policy-Rules	0-1	0-1	0-1	0	0
130	Extended-Location-Policy-Rules	0-1	0-1	0-1	0	0

Table 3: Standard attributes in accounting messages

5 BBF Specific Attributes

This section describes the RADIUS vendor specific attributes defined by the Broadband Forum (IANA enterprise number 3561).

5.1 Description

In the table below, descriptions of AVPs 26-3561-3 to 26-3561-10 can be used as definitions together with section 7.1.3 of TR-317. The other BBF AVPs described here are also defined in RFC4679.

AVP ID	AVP Name	Description	Reference(s)
26-3561-1	Agent-Circuit-Id	Information about the Access-Node to which the subscriber is attached, along with an identifier for the subscriber's DSL port on that Access-Node.	RFC4679 [25]
26-3561-2	Agent-Remote-Id	An operator-specific, statically configured string that uniquely identifies the subscriber on the associated access loop of the Access Node/DSLAM.	RFC4679 [25]
26-3561-3	BBF-LSL-Tunnel-Type	The tunnel type to be used for the LSL. Values: 0: SoftGRE (Ethernet over GRE) 1: VxLAN (defined TR-317, but its use is still undescribed) 2: L2TPv3 (defined TR-317, but its use is still undescribed) 3: FLAT When < 3, this attribute is mapped onto sub-option 21 of DHCPv4 option 125, or DHCPv6 option 17, with the IANA enterprise number set to “BBF” (i.e. 3561).	TR-341 TR-317 [25]
26-3561-4	BBF-LSL-Server-Endpoint-v4	The IPv4 address identifying the Ethernet over GRE tunnel end-point at the vG_MUX side. When BBF-LSL-Tunnel-Type < 3, this attribute is mapped onto DHCPv4 option 125, sub-option 22, with the IANA enterprise number 3561.	TR-341 TR-317 [25]

26-3561-5	BBF-LSL-Server-Endpoint-v6	The IPv6 address identifying the Ethernet over GRE tunnel end-point at the vG_MUX side. When BBF-LSL-Tunnel-Type < 3, this attribute is mapped onto DHCPv6 option 17, sub-option 22, with the IANA enterprise number 3561.	TR-341 TR-317 [25]
26-3561-6	BBF-LSL-Server-Endpoint-FQDN	The FQDN identifying the Ethernet over GRE tunnel end-point at the vG_MUX side. When BBF-LSL-Tunnel-Type < 3, the FQDN is resolved by the DHCP server.	TR-341 TR-317 [25]
26-3561-7	BBF-LSL-Client-Endpoint-v4	The IPv4 address that the BRG has to use for setting up its tunnel. When BBF-LSL-Tunnel-Type < 3, this attribute is mapped onto DHCPv4 option 125, sub-option 23, with the IANA enterprise number 3561.	TR-341 TR-317 [25]
26-3561-8	BBF-LSL-Client-Endpoint-v6	The IPv6 address that the BRG has to use for setting up its tunnel. When BBF-LSL-Tunnel-Type < 3, this attribute is mapped onto DHCPv6 option 17, sub-option 23, with the IANA enterprise number 3561.	TR-341 TR-317 [25]
26-3561-9	BBF-LSL-Client-Endpoint-FQDN	the FQDN pointing to the IPv4 or IPv6 address that the BRG has to use for setting up its tunnel. When BBF-LSL-Tunnel-Type < 3, the FQDN is resolved by the DHCP server.	TR-341 TR-317 [25]
26-3561-10	BBF-LSL-Tunnel-Private-Group-ID	ID of the network resource to use at vG_MUX to extend the LSL to the vG. Value: string encoding the ID of the network resource (VLAN ID, VNI, Label, etc)	TR-341 TR-317 [25]
26-3561-129	Actual-Data-Rate-Upstream	Actual upstream train rate of a subscriber's synchronized DSL link, in kbps.	RFC4679 [25]
26-3561-130	Actual-Data-Rate-Downstream	Actual downstream rate of a subscriber's synchronized DSL link, in kbps.	RFC4679 [25]
26-3561-131	Minimum-Data	Subscriber's operator-configured minimum	RFC4679 [25]

	Rate-Upstream	upstream data rate, in kbps.	
26-3561-132	Minimum-Data Rate-Downstream	Subscriber's operator-configured minimum downstream data rate, in kbps.	RFC4679 [25]
26-3561-133	Attainable Data Rate Upstream	Subscriber's attainable upstream data rate, in kbps	RFC4679 [25]
26-3561-134	Attainable Data Rate Downstream	Subscriber's attainable downstream data rate, in kbps	RFC4679 [25]
26-3561-135	Maximum-Data Rate-Upstream	Subscriber's maximum upstream data rate, as configured by the operator, in kbps.	RFC4679 [25]
26-3561-136	Maximum-Data Rate-Downstream	Subscriber's maximum downstream data rate, as configured by the operator, in kbps.	RFC4679 [25]
26-3561-137	Minimum-Data-Rate-Upstream-Low-Power	Subscriber's minimum upstream data rate in low power state, as configured by the operator, in kbps.	RFC4679 [25]
26-3561-138	Minimum-Data-Rate-Downstream-Low-Power	Subscriber's minimum upstream data rate in low power state, as configured by the operator, in kbps.	RFC4679 [25]
26-3561-139	Maximum-Interleaving-Delay-Upstream	Subscriber's maximum one-way upstream interleaving delay, as configured by the operator, in milliseconds.	RFC4679 [25]
26-3561-140	Actual-Interleaving-Delay-Upstream	Subscriber's actual one-way upstream interleaving delay, as configured by the operator, in milliseconds.	RFC4679 [25]
26-3561-141	Maximum-Interleaving-Delay-Downstream	Subscriber's maximum one-way downstream interleaving delay, as configured by the operator, in milliseconds.	RFC4679 [25]
26-3561-142	Actual-Interleaving-Delay-Downstream	Subscriber's actual one-way downstream interleaving delay, as configured by the operator, in milliseconds.	RFC4679 [25]
26-3561-144	Access-Loop Encapsulation	The encapsulation (s) used by the subscriber on the DSL access loop.	RFC4679 [25]
26-3561-254	IWF-Session	Presence of this PPPoA/oE IWF session flag indicates that the IWF has been performed with respect to the subscriber's session.	RFC4679 [25]

Table 4: Description of BBF-specific attributes

5.2 Applicability in authentication and dynamic authorization messages

Table 5 indicates the number of times an individual AVP will appear in each of the listed authentication and dynamic authorization message types.

AVP ID	AVP Name	Access Request	Access Accept	CoA Request
26-3561-1	Agent-Circuit-Id	0-1	0	0
26-3561-2	Agent-Remote-Id	0-1	0	0
26-3561-3	BBF-LSL-Tunnel-Type	0	0-1	0
26-3561-4	BBF-LSL-Server-Endpoint-v4	0	0-1	0
26-3561-5	BBF-LSL-Server-Endpoint-v6	0	0-1	0
26-3561-6	BBF-LSL-Server-Endpoint-FQDN	0	0-1	0
26-3561-7	BBF-LSL-Client-Endpoint-v4	0	0-1	0
26-3561-8	BBF-LSL-Client-Endpoint-v6	0	0-1	0
26-3561-9	BBF-LSL-Client-Endpoint-FQDN	0	0-1	0
26-3561-10	BBF-LSL-Tunnel-Private-Group-ID	0	0-1	0
26-3561-129	Actual-Data-Rate-Upstream	0-1	0	0
26-3561-130	Actual-Data-Rate-Downstream	0-1	0	0
26-3561-131	Minimum-Data Rate-Upstream	0-1	0	0
26-3561-132	Minimum-Data Rate-Downstream	0-1	0	0
26-3561-133	Attainable Data Rate Upstream	0-1	0	0
26-3561-134	Attainable Data Rate Downstream	0-1	0	0
26-3561-135	Maximum-Data Rate-Upstream	0-1	0	0
26-3561-136	Maximum-Data Rate-Downstream	0-1	0	0
26-3561-137	Minimum-Data-Rate-Upstream- Low-Power	0-1	0	0
26-3561-138	Minimum-Data-Rate-Downstream-	0-1	0	0

	Low-Power			
26-3561-139	Maximum-Interleaving-Delay-Upstream	0-1	0	0
26-3561-140	Actual-Interleaving-Delay-Upstream	0-1	0	0
26-3561-141	Maximum-Interleaving-Delay-Downstream	0-1	0	0
26-3561-142	Actual-Interleaving-Delay-Downstream	0-1	0	0
26-3561-144	Access-Loop Encapsulation	0-1	0	0
26-3561-254	IWF-Session	0-1	0-1	0

Table 5: BBF-specific attributes in authentication and dynamic authorization messages

5.3 Applicability in accounting messages

Table 6 indicates the number of times an individual AVP will appear in each of the listed accounting message types.

AVP ID	AVP Name	Acct Start	Acct Stop	Acct Interim Update	Acct On	Acct Off
26-3561-1	Agent-Circuit-Id	0-1	0-1	0-1	0	0
26-3561-2	Agent-Remote-Id	0-1	0-1	0-1	0	0
26-3561-3	BBF-LSL-Tunnel-Type	0-1	0-1	0-1	0	0
26-3561-4	BBF-LSL-Server-Endpoint-v4	0-1	0-1	0-1	0	0
26-3561-5	BBF-LSL-Server-Endpoint-v6	0-1	0-1	0-1	0	0
26-3561-6	BBF-LSL-Server-Endpoint-FQDN	0-1	0-1	0-1	0	0
26-3561-7	BBF-LSL-Client-Endpoint-v4	0-1	0-1	0-1	0	0
26-3561-8	BBF-LSL-Client-Endpoint-v6	0-1	0-1	0-1	0	0

26-3561-9	BBF-LSL-Client-Endpoint-FQDN	0-1	0-1	0-1	0	0
26-3561-129	Actual-Data-Rate-Upstream	0-1	0-1	0-1	0	0
26-3561-130	Actual-Data-Rate-Downstream	0-1	0-1	0-1	0	0
26-3561-131	Minimum-Data Rate-Upstream	0-1	0-1	0-1	0	0
26-3561-132	Minimum-Data Rate-Downstream	0-1	0-1	0-1	0	0
26-3561-133	Attainable Data Rate Upstream	0-1	0-1	0-1	0	0
26-3561-134	Attainable Data Rate Downstream	0-1	0-1	0-1	0	0
26-3561-135	Maximum-Data Rate-Upstream	0-1	0-1	0-1	0	0
26-3561-136	Maximum-Data Rate-Downstream	0-1	0-1	0-1	0	0
26-3561-137	Minimum-Data-Rate-Upstream- Low-Power	0-1	0-1	0-1	0	0
26-3561-138	Minimum-Data-Rate-Downstream- Low-Power	0-1	0-1	0-1	0	0
26-3561-139	Maximum-Interleaving-Delay-Upstream	0-1	0-1	0-1	0	0
26-3561-140	Actual-Interleaving-Delay-Upstream	0-1	0-1	0-1	0	0
26-3561-141	Maximum-Interleaving-Delay-Downstream	0-1	0-1	0-1	0	0
26-3561-142	Actual-Interleaving-Delay-Downstream	0-1	0-1	0-1	0	0
26-3561-144	Access-Loop Encapsulation	0-1	0-1	0-1	0	0
26-3561-254	IWF-Session	0-1	0-1	0-1	0	0

Table 6: BBF-specific attributes in accounting messages

6 Other RADIUS vendor specific Attributes

This section contains RADIUS Attributes that are found in multiple vendor dictionaries and are of common used in the MSBN context.We believe there are common semantics but cannot verify a common syntax for the duplicate instances.

AVP	**Description**
ANCP-DSL-Type	Defines the transmission system in use (e.g. ADSL, ADSL2, ADSL2+, VDSL2). This AVP is useful to fulfill requirement 71 of TR-147 [6].
Virtual-Router-Id	Contains an identifier that identifies exactly one virtual router when multiple, independent virtual routers co-exist on the same physical routing platform.
Policy-Name	Contains a name that identifies the policy to apply on the user session for the egress or ingress direction. The policy definition itself resides locally in the NAS.
HTTP-Redirect-URI	Contains an HTTP uniform resource identifiers (URI) to which user originating HTTP requests are redirected by the NAS.
HTTP-Redirect-Profile-Name	Contains the name of a HTTP redirect profile to apply on the user session.
Primary-DNS-Server-Address	Contains the IPv4 address (in network byte order) of the primary DNS server negotiated during IPCP.
Secondary-DNS-Server-Address	Contains the IPv4 address (in network byte order) of the secondary DNS server negotiated during IPCP.
QoS-Profile-Name	Contains a name that identify the QoS profile to apply on the user session. The QoS profile definition itself resides locally in the NAS.
IGMP-Enable	Contains an enumerated value that indicates whether the MLD protocol is enabled or disabled on the user interface upon connection establishment.
IGMP-Profile-Name	Contains the name of the IGMP service profile configured on the NAS and to apply on the user session.
MLD-Enable	Contains an enumerated value that indicates whether the MLD protocol is enabled or disabled on the user interface upon connection establishment.
	Contains the identifier of the IGMP service profile configured on

MLD-Profile-Name	the NAS and applied to the user session. If the value of the IGMP Profile in the RADIUS message sent by the RADIUS server does not exist, the NAS may assign a default IGMP Profile the user if one exists on the NAS itself.
Tunnel-Virtual-Router	Identifies the virtual router name such as the VPN instance of the tunnel context. When returned in the RADIUS Access-Accept, this attribute defines the virtual routing context to which a tunnel is assigned.
Tunnel-Max-Sessions	Specifies the maximum number of sessions that are allowed in a given tunnel. A session must be denied once the value tied to this attribute is exceeded.
Tunnel-Profile-Name	Contains a name that identifies the profile that defines the tunnel to which the subscriber session is tied. The Tunnel profile definition itself that comprises various tunnel specific parameters resides locally in the NAS. If the value of the tunnel profile name provided in the RADIUS message does not exist, the (NAS) may apply a default Tunnel profile to the subscriber session if one exists on the NAS itself.
Service-Name	Specifies the name of the service to be activated for a given subscriber session. The Service-Name attribute may be tagged supporting multiple tags.
Deactivate-Service-Name	Specifies the name of the service to be de-activated for a given subscriber session.
Ipv4-Authentication	Matches the “Algorithm” field of the DHCPv4 authentication option (90), which is the object of RFC3118 [20]. Through this option, authorization tickets can be easily generated and newly attached hosts with authorization can be configured from an authenticated DHCP server. This attribute is useful at session creation or at reconfiguration under the operator’s control (c.f. DHCPFORCERENEW_ NONCE_CAPABLE in TR-146 [5], § 6.3)
Ipv6-Authentication	RADIUS attribute, matching the DHCPv6 authentication option (11), defined in RFC3315 [22]. This attribute is useful at session creation or at reconfiguration

	under the operator's control (c.f. DHCP RECONFIGURE KEY in TR-146 [5], § 6.3).
Ipv4-User-Class	Matches the DHCPv4 User-Class-Information option (77), defined in RFC3004 [19]. Attribute used by a client to identify the type or category of user or applications it represents.
Ipv6-User-Class	Matches the DHCPv6 User-Class option (15), defined in RFC3315 [22]. Attribute used by a client to identify the type or category of user or applications it represents.
DHCP Req. option set	Concatenated DHCPv4 options received in a DHCPv4 Message triggering authentication.
Subscriber profile(s)	A handful of attributes allowing binding policies to a (set of) subscriber session(s).
Client-MAC-Addr	Users MAC address.
Vendor-Class-Id	DHCPv4 DHCPDISCOVER Option 60 or DHCPv6 SOLICIT Option 16.
Tunnel-Terminate-Cause	Specifies the disconnect cause when a tunneled subscriber is disconnected, for example when the termination is initiated by the L2TP layer in the case of LNS.

Table 7: Description of other useful vendor-specific attributes

End of Broadband Forum Technical Report TR-341