

RADEXT WG
Internet-Draft
Intended status: Standards Track
Expires: January 7, 2016

D. Morrisette
Verizon
F. Kamm
L. Morand
Orange
July 6, 2015

RADIUS attributes commonly used in fixed networks
draft-kammorrisette-radext-very-common-vsas-00

Abstract

There is a set of Remote Authentication Dial-In User Service attributes which have been widely used in different types of fixed networks though they don't appear as standard attributes. Each of these attributes has for long been part of many vendor dictionaries, thus presented in different approaches and different syntaxes. This document try to solve this in an effort to present them in a standard, common way, based on approaches found in multiple dictionaries.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of [BCP 78](#) and [BCP 79](#).

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at <http://datatracker.ietf.org/drafts/current/>.

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

This Internet-Draft will expire on January 7, 2016.

Copyright Notice

Copyright (c) 2015 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to [BCP 78](#) and the IETF Trust's Legal Provisions Relating to IETF Documents (<http://trustee.ietf.org/license-info>) in effect on the date of publication of this document. Please review these documents

carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

Table of Contents

1.	Introduction	3
2.	Conventions and Terminology	3
2.1.	Conventions	3
2.2.	Terminology	3
3.	Deployment Scenarios	3
4.	RADIUS attributes	4
4.1.	Attributes for Routing Context	4
4.1.1.	Virtual-Router-Id	4
4.2.	Policies and QoS Attributes	5
4.2.1.	Policy-Name	5
4.2.2.	QoS-Profile-Name	6
4.3.	Attributes for walled garden services	6
4.3.1.	HTTP-Redirect-URI	7
4.3.2.	HTTP-Redirect-Profile-Name	7
4.4.	DNS	8
4.4.1.	Primary-DNS-Server-Address	8
4.4.2.	Secondary-DNS-Server-Address	8
4.5.	Multicast attributes	9
4.5.1.	IGMP-Enable	9
4.5.2.	IGMP-Profile-Name	10
4.5.3.	MLD-Enable	10
4.5.4.	MLD-Profile-Name	11
4.6.	Tunnel attributes	11
4.6.1.	Tunnel-Virtual-Router	12
4.6.2.	Tunnel-Max-Sessions	12
4.6.3.	Tunnel-Profile-Name	13
4.6.4.	Tunnel-Terminate-Cause	13
4.7.	Service attributes	14
4.7.1.	Service-Name	14
4.7.2.	Deactivat-Service-Name	15
4.7.3.	Service-Accounting	15
5.	Table of Attributes	16
6.	IANA Considerations	17
7.	Security Considerations	18
8.	Acknowledgements	18

9.	References	18
9.1.	Normative References	18
9.2.	Informative References	19
	Authors' Addresses	19

[1.](#) Introduction

This document describes a set of Remote Authentication Dial-In User Service (RADIUS) [[RFC2865](#)] attributes which have been widely used in different fixed network contexts (residential access, business services...). Since those attributes have been for long part of many vendor dictionaries, they were presented in different syntax and semantic approaches. This document is as far as possible an effort to present them in a common way.

[2.](#) Conventions and Terminology

[2.1.](#) Conventions

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [[RFC2119](#)].

[2.2.](#) Terminology

xxx

[3.](#) Deployment Scenarios

To be added. Example below:

deployment scenarios is intended to cover a wide range of access networks The main purpose is to standardise common vendor specific attributes. The extensions in this document are intended to be applicable across a wide variety of network access scenarios in which RADIUS is involved. The involved protocols include but are not limited to DHCP, PPP, L2TP and protocols related to multicast or QoS.

One such typical network scenario is illustrated in Figure 1. It is composed of an IP Routing Residential Gateway (RG) or host; a Layer 2 Access Node (AN), e.g., a Digital Subscriber Line Access Multiplexer

(DSLAM); an IP Network Access Server (NAS) (incorporating an Authentication, Authorization, and Accounting (AAA) client); and a AAA server.

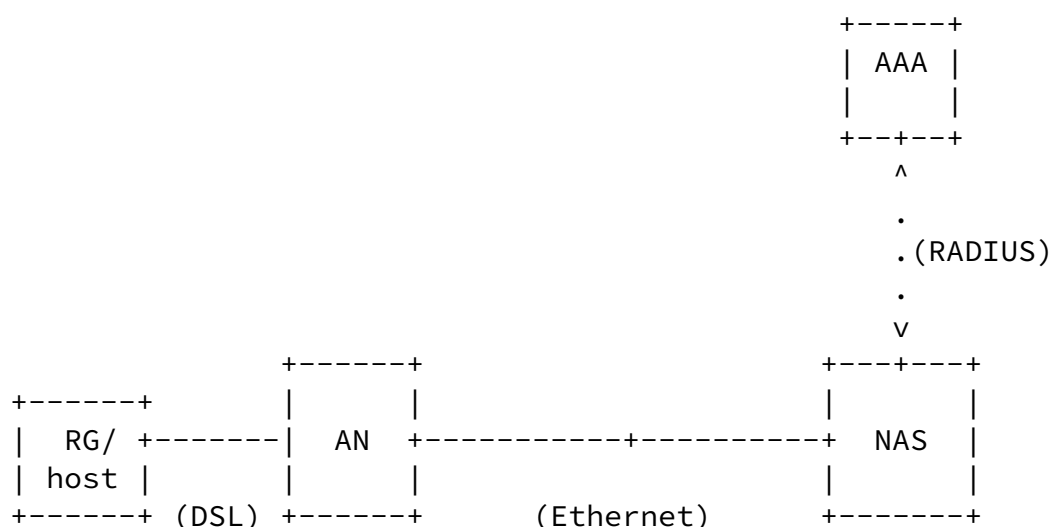


Figure 1

In the depicted scenario, the NAS may utilize an IP address configuration protocol (e.g., DHCPv6) to handle address assignment to RGs/hosts. The RADIUS server authenticates each RG/host and returns the Attributes used for authorization and accounting. These Attributes can include attributes related to routing context, policies and QoS, walled garden services, DNS servers, multicast service, PPP and L2TP configurations. The following sections defines these specific attributes.

4. RADIUS attributes

The new attributes described in this section are defined as short

extended attributes, as defined in [[RFC6929](#)].

Each attribute is described following the suggestions given in section 4 of [[draft-dekok-radext-datatypes](#)]. Please refer to this specification to find further details on the data types used for the different attributes.

[4.1.](#) Attributes for Routing Context

[To Be Completed]

[4.1.1.](#) Virtual-Router-Id

Description

The Virtual-Router-Id attribute contains an identifier that identifies exactly one virtual router when multiple, independent virtual routers co-exist on the same physical routing platform. This attribute MAY be included in Access-Accept or Change of

Authorization (CoA) Request. When returned in the RADIUS Access-Accept, this attribute defines the virtual router to which a user session is assigned. If the Virtual Router ID returned by the RADIUS server does not exist, the Network Access Server (NAS) MUST NOT permit the user to access the network. If the RADIUS server does not return any Virtual Router Id, the user session MAY be assigned to a default routing context or to any available virtual router.

Type

241.x01

Length

>= 4

Ext-Data

string

Value

The "Value" field is one or more octets and contains the virtual router ID that the user is assigned. A robust implementation SHOULD support the field as undistinguished octets.

[4.2.](#) Policies and QoS Attributes

[To Be Completed]

[4.2.1.](#) Policy-Name

Description

The Policy-Name attribute 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. This attribute MAY be included in Access-Accept and CoA-Request. If the policy name provided in the RADIUS message does not exist, the Network Access Server (NAS) MAY assign a default policy the user if one exists on the NAS itself.

Type

241.x03

Length

Morrisette, et al.

Expires January 7, 2016

[Page 5]

Internet-Draft

Common RADIUS attributes

July 2015

>=4

Ext-Data

string

Value

The "Value" field is one or more octets, specifying the name of the policy to apply on the user session in the ingress or egress direction. A robust implementation SHOULD support the field as undistinguished octets.

[4.2.2.](#) QoS-Profile-Name

Description

The QoS-Profile-Name attribute contains a name that identify the QoS profile to apply on the user session. The QoS profile definition itself resides locally in the NAS. This attribute MAY be included in Access-Accept and CoA-Request. If the value of the QoS profile name provided in the RADIUS message does not exist, the Network Access Server (NAS) MAY apply a default QoS profile to the user session if one exists on the NAS itself.

Type

241.x04

Length

>=4

Ext-Data

string

Value

The "Value" field is one or more octets, specifying the QoS profile name to apply on the user session. A robust implementation SHOULD support the field as undistinguished octets.

[4.3.](#) Attributes for walled garden services

[To Be Completed]

[4.3.1.](#) HTTP-Redirect-URI

Description

The HTTP-Redirect-URI attribute contains an HTTP uniform resource Identifier (URI) to which user originating HTTP requests are redirected by the NAS. This attribute MAY be included in Access-Accept, CoA Request and Accounting-Request.

Type

241.x05

Length

>=4

Ext-Data

string

Value

The "Value" field is one or more octets, containing an HTTP URI as specified in [[RFC7230](#)]. A robust implementation SHOULD support the field as undistinguished octets.

[4.3.2.](#) HTTP-Redirect-Profile-Name

Description

The HTTP-Redirect-Profile-Name attribute contains the name of an HTTP redirect profile to apply on the user session. This attribute MAY be included in Access-Accept, in CoA-Request and Accounting-Request.

Type

241.x06

Length

>=4

Ext-Data

sext

Value

The "Value" is one or more octets, containing the name of an HTTP redirect profile to apply on the user's originating HTTP traffic. A robust implementation SHOULD support the field as undistinguished octets.

[4.4.](#) DNS

This section only defines DNS server for IPv4. DNS servers for IPv6 can be found in [[RFC6911](#)].

[4.4.1.](#) Primary-DNS-Server-Address

Description

The Primary-DNS-Server-Address attribute contains the IPv4 address (in network byte order) of the primary DNS server negotiated during IPCP. This attribute MAY be included in Access-Accept and Accounting-Request.

Type

241.x07

Length

6

Ext-Data

ipv4addr

Value

The "Value" field contains the IPv4 address (in network byte order) of the primary DNS server.

[4.4.2.](#) Secondary-DNS-Server-Address

Description

The Secondary-DNS-Server attribute contains the IPv4 address (in network byte order) of the secondary DNS server if negotiated during IPCP. This attribute MAY be included in Access-Accept and Accounting-Request.

Type

241.x08

Length

6

Ext-Data

ipv4addr

Value

The "Value" field contains the IPv4 address (in network byte order) of the secondary DNS server.

[4.5.](#) Multicast attributes

[To Be Completed]

[4.5.1.](#) IGMP-Enable

Description

The IGMP-Enable contains an enumerated value that indicates whether the MLD protocol is enabled or disabled on the user interface upon connection establishment. This attribute MAY be included in Access-Accept and CoA-Request.

Type

241.x09

Length

6

Ext-Data

enum

Value

The "Value" field is an enumerated value that indicates whether IGMP is enabled or disabled. The valid set of enumerated values are:

0 = Disable

Internet-Draft

Common RADIUS attributes

July 2015

1 = Enable

[4.5.2.](#) IGMP-Profile-Name

Description

The IGMP-Profile-Name attribute contains the name of the IGMP service profile configured on the NAS and to apply on the user session. This attribute MAY be included in Access-Accept, CoA-Request and Accounting-Request.

Type

241.x10

Length

>=4

Ext-Data

sext

Value

The "Value" field contains the IGMP profile name that is assigned to the user session. A robust implementation SHOULD support the field as undistinguished octets.

[4.5.3.](#) MLD-Enable

Description

The MLD-Enable attribute contains an enumerated value that indicates whether the MLD protocol is enabled or disabled on the user interface upon connection establishment. This attribute MAY be included in Access-Accept and CoA-Request.

Type

241.x11

Length

6

Ext-Data

Morrisette, et al.

Expires January 7, 2016

[Page 10]

Internet-Draft

Common RADIUS attributes

July 2015

enum

Value

The "Value" field is an enumerated value that indicates whether the MLD protocol is enabled or disabled on the user interface upon connection establishment. The valid set of enumerated values are:

0 = Disable

1 = Enable

[4.5.4.](#) MLD-Profile-Name

Description

The MLD-Profile-Name attribute contains the identifier of the IGMP service profile configured on the NAS and applied to the user session. This attribute MAY be included in Access-Accept, CoA-Request and Accounting-Request. If the value of the IGMP Profile in the RADIUS message sent by the RADIUS server does not exist, the Network Access Server (NAS) MAY assign a default IGMP Profile the user if one exists on the NAS itself.

Type

241.x12

Length

>=4

Ext-Data

String

Value

The "Value" field is one or more octets, specifying the MLD profile name that is assigned to the subscriber session. A robust implementation SHOULD support the field as undistinguished octets.

[4.6.](#) Tunnel attributes

[To Be Completed]

Morrisette, et al.

Expires January 7, 2016

[Page 11]

Internet-Draft

Common RADIUS attributes

July 2015

[4.6.1.](#) Tunnel-Virtual-Router

Description

The Tunnel-Virtual-Router attribute 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.

Type

241.x13

Length

>=4

Ext-Data

sext

Value

The "Value" field is one or more octets, specifying the Tunnel

virtual router name that is assigned to the tunnel. A robust implementation SHOULD support the field as undistinguished octets.

[4.6.2.](#) Tunnel-Max-Sessions

Description

The Tunnel-Max-Sessions attribute 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.

The Tunnel-Max-Sessions attribute may be returned in Access-Accept.

Type

241.x14

Length

6

Ext-Data

Morrisette, et al.

Expires January 7, 2016

[Page 12]

Internet-Draft

Common RADIUS attributes

July 2015

enum

Value

The "Value" field is an enumerated value that indicates the maximum number of sessions that can be brought up in a tunnel.

[4.6.3.](#) Tunnel-Profile-Name

Description

The Tunnel-Profile-Name attribute 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.

This attribute MAY be included in Access-Accept. If the value of

the tunnel profile name provided in the RADIUS message does not exist, the Network Access Server (NAS) MAY apply a default Tunnel profile to the subscriber session if one exists on the NAS itself.

Type

241.x15

Length

>=1

Ext-Data

string

Value

The "Value" field is one or more octets, specifying the Tunnel profile name to apply on the user session. A robust implementation SHOULD support the field as undistinguished octets.

[4.6.4.](#) Tunnel-Terminate-Cause

Description

The Tunnel-Terminate-Cause attribute 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.

The Tunnel-Terminate-Cause attribute may be included in Accounting-Stop message.

Type

241.x16

Length

>=4

Ext-Data

enum

Value

The "Value" field is an enumerated value containing an integer specifying the cause of session termination

[4.7.](#) Service attributes

[To Be Completed]

[4.7.1.](#) Service-Name

Description

The Service-Name attribute specifies the name of the service to be activated for a given subscriber session. The Service-Name attribute may be present in Access-Accept, CoA request and CoA response RADIUS messages. The Service-Name attribute may be tagged supporting multiple tags.

Type

241.x17

Length

>=4

Ext-Data

sext

Value

The "Value" field contains the Service name that is assigned to the subscriber session. A robust implementation SHOULD support the field as undistinguished octets.

[4.7.2.](#) Deactivat-Service-Name

Description

The Deactivate-Service-Name attribute specifies the name of the service to be de-activated for a given subscriber session.

The Decativate-Service-Name attribute may be present in Access-Accept and CoA request RADIUS messages.

Type

241.x18

Length

6

Ext-Data

enum

Value

The "Value" field contains the Service name that is to be de-activated for a given subscriber session. A robust implementation SHOULD support the field as undistinguished octets.

[4.7.3.](#) Service-Accounting

Description

The Service-Accounting attribute specifies whether accounting for a given service tied to a subscriber session is enabled or disabled.

This attribute MAY be included in Access-Accept and CoA Request. Implementations may support sub-options for Service-Accounting such as time and/or volume based accounting statistics collection. The Service-Accounting attribute may support tags.

Type

241.x19

Length

>=1

Ext-Data

string

Value

The "Value" field is an enumerated value that indicates whether the Service-Accounting is enabled or disabled for the service tied to a subscriber session. The valid set of enumerated values are:

0 = Disable

1 = Enable

5. Table of Attributes

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

Access-Request	Access-Accept	Access-Reject	Access-Chall	#	Attribute
0	0-1	0	0	241.x01	Virtual-Router-Id
0	0-1	0	0	241.x02	Redirect-Virtual-Router-Id
0	0-1	0	0	241.x03	Policy-Name
0	0-1	0	0	241.x04	QoS-Policy-Name
0	0-1	0	0	241.x05	HTTP-Redirect-URI
0	0-1	0	0	241.x06	HTTP-Redirect-Profile-Name
0	0-1	0	0	241.x07	Primary-DNS-Server-Address
0	0-1	0	0	241.x08	Secondary-DNS-Server-Address
0	0-1	0	0	241.x09	IGMP-Enable
0	0-1	0	0	241.x10	IGMP-profile-Name
0	0-1	0	0	241.x11	MLD-Enable
0	0-1	0	0	241.x12	MLD-Profile-Name
0	0-1	0	0	241.x13	Tunnel-Virtual-Router
0	0-1	0	0	241.x14	Tunnel-Max-Session
0	0-1	0	0	241.x15	Tunnel-Profile-Name
0	0	0	0	241.x16	Tunnel-Terminate-Cause
0	0-1	0	0	241.x17	Service-Name
0	0-1	0	0	241.x18	Service-Deactivate
0	0-1	0	0	241.x19	Service-Accounting

Internet-Draft

Common RADIUS attributes

July 2015

CoA-Request	Dis-Request	Acct-Request	#	Attribute
0-1	0	0	241.x01	Virtual-Router-Id
0-1	0	0	241.x02	Redirect-Virtual-Router-Id
0-1	0	0	241.x03	Policy-Name
0-1	0	0	241.x04	QoS-Policy-Name
0-1	0	0-1	241.x05	HTTP-Redirect-URI
0-1	0	0-1	241.x06	HTTP-Redirect-Profile-Name
0-1	0	0-1	241.x07	Primary-DNS-Server-Address
0-1	0	0-1	241.x08	Secondary-DNS-Server-Address
0-1	0	0	241.x09	IGMP-Enable
0-1	0	0-1	241.x10	IGMP-profile-Name
0-1	0	0	241.x11	MLD-Enable
0-1	0	0-1	241.x12	MLD-Profile-Name
0-1	0	0	241.x13	Tunnel-Virtual-Router
0-1	0	0	241.x14	Tunnel-Max-Session
0-1	0	0	241.x15	Tunnel-Profile-Name
0	0	0-1	241.x16	Tunnel-Terminate-Cause
0-1	0	0	241.x17	Service-Name
0-1	0	0	241.x18	Service-Deactivate
0-1	0	0	241.x19	Service-Accounting

The following table defines the above table entries.

0 This attribute MUST NOT be present in packet.

0+ Zero or more instances of this attribute MAY be present in the packet.

0-1 Zero or one instance of this attribute MAY be present in the packet.

[6.](#) IANA Considerations

This document requires the following IANA action:

Attribute	Type
=====	=====
Virtual-Router-Id	241.x01
Redirect-Virtual-Router-Id	241.x02
Policy-Name	241.x03
QoS-Policy-Name	241.x04
HTTP-Redirect-URI	241.x05
HTTP-Redirect-Profile-Name	241.x06
Primary-DNS-Server-Address	241.x07
Secondary-DNS-Server-Address	241.x08
IGMP-Enable	241.x09
IGMP-profile-Name	241.x10
MLD-Enable	241.x11
MLD-Profile-Name	241.x12
Tunnel-Virtual-Router	241.x13
Tunnel-Max-Session	241.x14
Tunnel-Profile-Name	241.x15
Tunnel-Terminate-Cause	241.x16
Service-Name	241.x17
Service-Deactivate	241.x18
Service-Accounting	241.x19

7. Security Considerations

This document specifies additional RADIUS Attributes useful in residential broadband network deployments. In such networks, the RADIUS protocol may run either over IPv4 or over IPv6, and known security vulnerabilities of the RADIUS protocol apply to the Attributes defined in this document. A trust relationship between a NAS and RADIUS server is expected to be in place, with communication optionally secured by IPsec [[RFC4301](#)] or Transport Layer Security (TLS) [[RFC5246](#)]. This document does not introduce any new security issue compared to those identified in [[RFC2865](#)].

[8.](#) Acknowledgements

The author would like to thank Sri Gundavelli and Gaetan Feige for having shared thoughts on concepts exposed in this document.

[9.](#) References

[9.1.](#) Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", [BCP 14](#), [RFC 2119](#), March 1997.

[RFC2865] "Remote Authentication Dial In User Service (RADIUS)".

Morrisette, et al. Expires January 7, 2016 [Page 18]

Internet-Draft Common RADIUS attributes July 2015

[RFC6911] Dec, W., Sarikaya, B., Zorn, G., Miles, D., and B. Lourdelet, "RADIUS Attributes for IPv6 Access Networks", [RFC 6911](#), April 2013.

[RFC6929] DeKok, A. and A. Lior, "Remote Authentication Dial In User Service (RADIUS) Protocol Extensions", [RFC 6929](#), April 2013.

[RFC7230] "Hypertext Transfer Protocol (HTTP/1.1): Message Syntax and Routing".

[9.2.](#) Informative References

[\[draft-dekok-radext-datatypes\]](#)

"Data Types in the Remote Authentication Dial-In User Service Protocol (RADIUS)".

[RFC4301] "Security Architecture for the Internet Protocol".

[RFC5246] "The Transport Layer Security (TLS) Protocol".

Authors' Addresses

Devasena Morrisette
Verizon
555 Elm St, Manchester, NH ,

Manchester 03101
USA

Email: devasena.morrisette@verizon.com

Frederic Klamm
Orange
4, rue du Clos Courtel, BP 91226
Cesson-Sevigne 35512
France

Email: frederic.klamm@orange.com

Lionel Morand
Orange
38-40 rue du General Leclerc
Issy-Les-Moulineaux 92130
France

Email: lionel.morand@orange.com