

# IPWorks AAA Server-AAA Clients Gi Interface

---

## INTERWORK DESCRIPTION

**Copyright**

© Ericsson AB 2014. All rights reserved. No part of this document may be reproduced in any form without the written permission of the copyright owner.

**Disclaimer**

The contents of this document are subject to revision without notice due to continued progress in methodology, design and manufacturing. Ericsson shall have no liability for any error or damage of any kind resulting from the use of this document.

**Trademark List**

All trademarks mentioned herein are the property of their respective owners. These are shown in the document Trademark Information.



# Contents

<b>1</b>	<b>Introduction</b>	<b>1</b>
1.1	Prerequisites	1
1.2	Related Information	1
<b>2</b>	<b>Interface Overview</b>	<b>3</b>
2.1	Interface Role	3
2.2	Services	3
2.3	Encapsulation and Addressing	4
<b>3</b>	<b>Procedures</b>	<b>5</b>
3.1	Authentication/Authorization	5
3.2	Accounting	6
3.3	Disconnect	7
3.4	Change-of-Authorization	8
3.5	Proxy	8
<b>4</b>	<b>Information Model</b>	<b>11</b>
4.1	Authentication/Authorization	11
4.2	Accounting Messages	13
4.3	Dynamic Authorization Extension Messages	17
<b>5</b>	<b>Information Elements</b>	<b>19</b>
5.1	3GPP Vendor Specific Sub Attributes	19
5.2	Access-Control-Group Sub Attributes	21
5.3	Radius-Supported-VSA Related Messages	21
5.4	Suggested-Rule-Space Sub Attributes	45
<b>6</b>	<b>Error Handling</b>	<b>47</b>
<b>7</b>	<b>Formal Syntax</b>	<b>49</b>
<b>8</b>	<b>Related Standards</b>	<b>51</b>
	<b>Reference List</b>	<b>53</b>





# 1 Introduction

This document describes the (GGSN-to-PDN) Gi interface between the IPWorks AAA Server and the AAA Clients.

## Scope

- Interface Overview
- Procedures
- Information Model
- Information Elements
- Error Handling
- Formal Syntax
- Related Standards

## Target Groups

This document is intended for personnel needing to understand the logical entity, including interfaces and protocols, of the IPWorks.

## 1.1 Prerequisites

Not Applicable

## 1.2 Related Information

Trademark information, typographic conventions, definition and explanation of acronyms and terminology can be found in the following documents:

- *Trademark Information*, Reference [1]
- *Glossary of Terms and Acronyms*, Reference [2]
- *Typographic Conventions*, Reference [3]



## 2 Interface Overview

This section describes the interface between the IPWorks AAA Server and the AAA Clients, as shown in Figure 1.

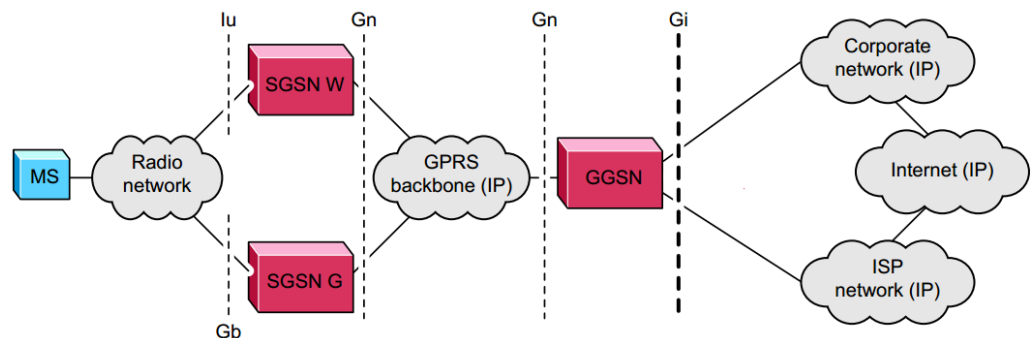


Figure 1 Gi Interface Overview

### 2.1 Interface Role

This section describes the role of the Gi interface in the GPRS network.

### 2.2 Services

This section describes the services the Gi interface offers.

The services offered by the Gi interface are shown in Table 1.

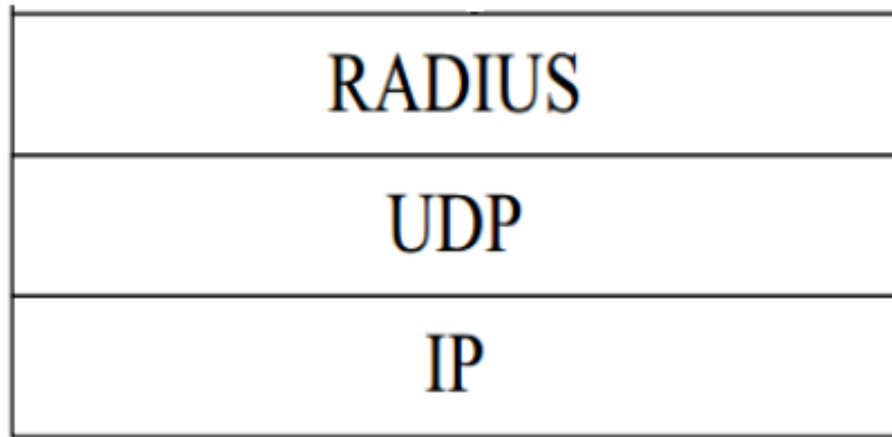
Table 1 Offered Services

Offered Service	Description
Authentication, Authorization, and Accounting	<ul style="list-style-type: none"> <li>IPWorks AAA Server uses the RADIUS protocol to realize the authentication, authorization, and accounting functionalities. These functionalities are widely used in the fixed, mobile access networks, and some other scenarios.</li> <li>IPWorks AAA Server uses the RADIUS protocol to communicate with the Network Access Server (NAS), which is based on the IETF and 3GPP Standard, see the references from Reference [5] to Reference [13] and it supports the Ericsson GGSN 2009A Gi interface as well, see Reference [4].</li> </ul>



## 2.3 Encapsulation and Addressing

This section describes what lower level protocol this Gi interface uses as described in Figure 2.



*Figure 2 Protocol Stack*





## 3 Procedures

This section describes the procedures used in connection with the offered and used interfaces of IPWorks.

### 3.1 Authentication/Authorization

IPWorks AAA server Authentication/Authorization interface is based on RFC 2865, which is carried over UDP/IP.

The IPWorks AAA Server listens on port 1812 by default, and it can be configured when necessary.

Figure 3 describes the authentication and authorization procedure:



Figure 3 IPWorks AAA Server Authentication and Authorization

The detailed procedure is listed as follows:

1. The RADIUS client (NAS) creates an `Access-Request` and sends to the AAA Server.

The `Access-Request` includes the following attributes:

- User Name
- Password
- Client Identity
- Other Attributes

2. The AAA server receives `Access-Request` from NAS and replies NAS with `Access-Accept` or `Access-Reject` according to the validation result.

## 3.2 Accounting

The AAA Accounting is known as RADIUS Accounting specified in RFC 2866, UDP/IP is used as the transport layer protocol.

The AAA Accounting listens on port 1813 by default, and it can be configured when necessary.

Figure 4 describes the accounting procedure:

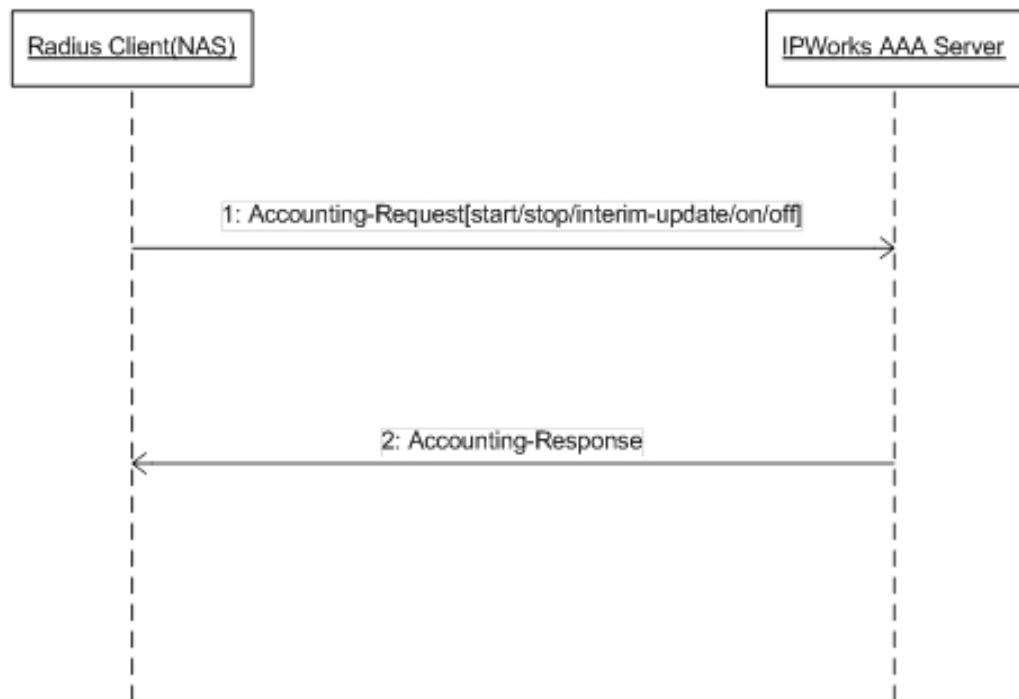


Figure 4 IPWorks AAA Server Accounting Procedure

The detailed procedure is listed as follows:

1. The RADIUS Client (NAS) sends `Accounting-Request` to the IPWorks AAA server.
  - NAS generates an `Accounting Start` packet **in the beginning of the service delivery**.
  - NAS sends an `Accounting Stop` packet to the AAA server **at the end of the service delivery**.



- NAS continually sends an Accounting `interim-update` packet to the AAA Server to update the accounting information **during the service delivery period**.
  - When a startup/shutdown happens in the NAS, it triggers an Accounting on/off packet to the AAA Server and the AAA Server releases the relevant resources.
2. Upon successfully recording/processing the Accounting Request from NAS client, the AAA Server sends the Accounting-Response ACK to the client, otherwise, it does not send back ACK to the client.

### 3.3 Disconnect

The DAS is the entity receiving CoA-Request or Disconnect-Request packets, which is a NAS or a RADIUS proxy.

The protocol used between DAS and IPWorks AAA is based on RFC 5176, which is over UDP/IP. The default destination UDP port of DAS to listen for either Disconnect Request or CoA Request is 3799, and it can be configured when necessary.

Figure 5 describes the disconnect procedure:

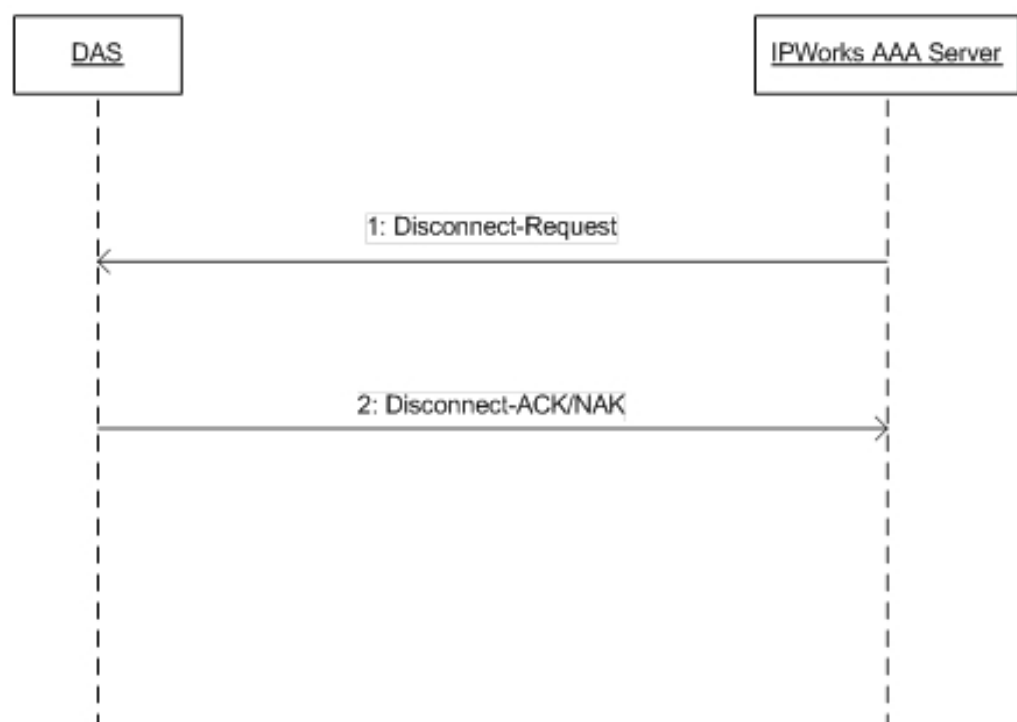


Figure 5 IPWorks AAA Server Disconnect Procedure

1. IPWorks AAA Server sends a `Disconnect-Request` to DAS/NAS to terminate the user sessions on a NAS.

2. The DAS/NAS responds to the `Disconnect-Request` sent by the AAA Server with a `Disconnect-ACK/NAK` if DAS/NAS is able/unable to terminate all the related sessions.

## 3.4 Change-of-Authorization

The protocol of Change-of-Authorization (CoA) is the same as Disconnect, see Section 3.2 on page 6.

Figure 6 describes the Change-of-Authorization procedure:

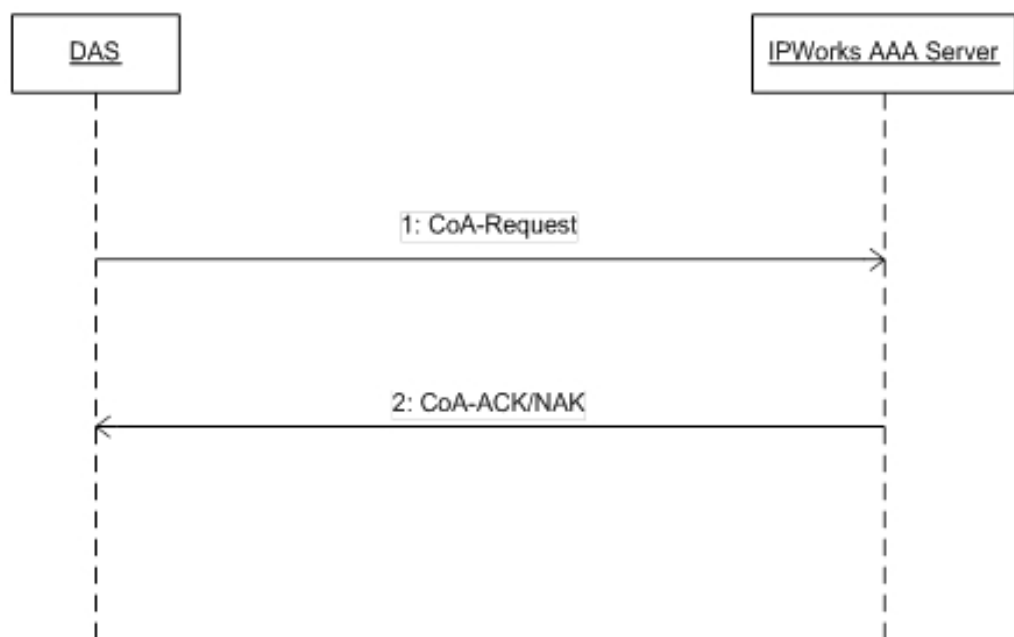


Figure 6 IPWorks AAA Server CoA Procedure

1. IPWorks AAA Server sends `CoA-Request` to DAS/NAS, which contains information for dynamically changing session authorizations.
2. The DAS/NAS replies the AAA server with a `COA-ACK/NAK` if DAS/NAS is able/unable to change the authorization for the related user sessions.

## 3.5 Proxy

As a Proxy Server, IPWorks AAA Server acts as both RADIUS Server and Client, except the interface with RADIUS Client (NAS), it's able to forward these messages (as specified above) to remote AAA Home Server as well.

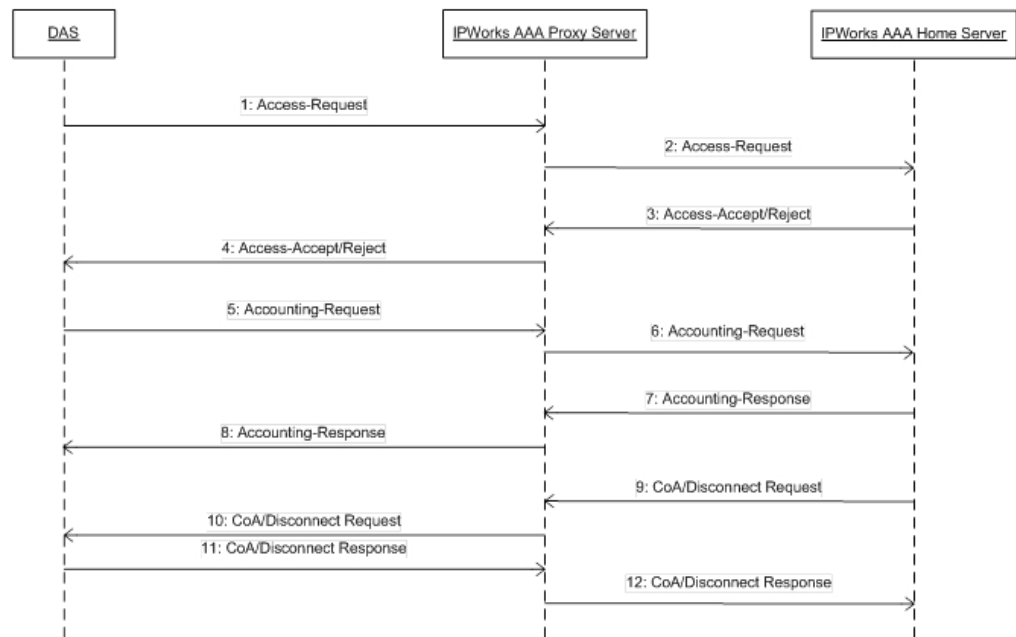


Figure 7 IPWorks AAA Proxy Server Procedure





## 4 Information Model

This section describes the information model, including mandatory and optional parameters of each service operation.

The presence of an information element is defined in the P column as follows:

- M Mandatory
- C Conditional
- O Optional

### 4.1 Authentication/Authorization

This section describes the content of messages (Access-Request, Access-Accept, Access-Reject) involved in the Authentication/Authorization procedure.

The procedure follows the basic RADIUS Message format as specified in RFC 2865. The attributes that IPWorks AAA supports in this message are specified in RFC 2865, RFC 2868, RFC 3162 and 3GPP TS 29.061 as well as in the Ericsson GGSN 2009A Gi Interface.

#### 4.1.1 Access-Request Message

The Access-Request message is sent from RADIUS Client (NAS) to IPWorks AAA Server.

Table 2 describes the significant attributes for the Access-Request Message:

*Table 2 Access-Request Message*

Attr #	Element	Type	P	Description
1	Username	String	M	It indicates the name of the user to be authenticated.
2	User-Password	String	C	Users must provide the user password if PAP is used. <sup>(1)</sup>
3	CHAP-Password	String	C	Users must provide the user password if CHAP is used. <sup>(1)</sup>
4	NAS-IP-Address	Address(IPv4)	M	It is the IP address of the NAS for communication with the
5	NAS-Port	String	O	It is a configurable value for Access-Request.
32	NAS-Identifier	String	M	It is the hostname of the NAS for communication with the F
6	Service-Type	Integer	M	It indicates the type of service for this user.
7	Framed-Protocol	Integer	M	It indicates the type of protocol for this user.
8	Framed-IP-Address	Address(IPv4)	C	It is the IP address allocated for this user. <sup>(2)</sup>
97	Framed-IPv6-Prefix	Address(IPv6)	C	It is the IPv6 address prefix allocated for this user. <sup>(3)</sup>

**Table 2 Access-Request Message**

Attr #	Element	Type	P	Description
30	Called-Station-Id	String	O	It is the phone number the user called or the identifier for the target network.
31	Calling-Station-Id	String	O	It is the phone number where the call came from.
44	Acct-Session-Id	String	O	It is the user session identifier.
60	CHAP-Challenge	String	C	CHAP-Challenge is mandatory if CHAP is used. <sup>(4)</sup>
61	NAS-Port-Type	Integer	M	It is the type of physical port used by NAS.
26/10415	3GPP Vendor-Specific	See Reference [11]	O	See Reference [11] for the sub attributes description.

(1) User Password is present when PAP is used.

(2) IPWorks AAA considers it as a hint address when allocating an IP address.

(3) IPWorks AAA considers it as a hint IPv6 prefix when allocating an IPv6 prefix.

(4) Challenge is present when CHAP is used.

#### 4.1.2 Access-Accept Message

The Access-Accept message is sent to RADIUS Client (NAS) from IPWorks AAA Server.

Table 3 describes only the significant attributes for the Access-Accept Message:

**Table 3 Access-Accept Message**

Attr #	Element	Type	P	Description
6	Service-Type	Integer	O	It indicates the type of service for this user.
7	Framed-Protocol	Integer	O	It indicates the type of protocol for this user.
8	Framed-IP-Address	Address(IPv4)	O	It is the IP address allocated for this user, if the RADIUS server is used to allocate an IP address.
9	Framed-IP-Netmask	Address(IPv4)	O	It is the netmask for the user IP address, if the RADIUS server is used to allocate IP netmask.
25	Class	String	O	It is the identifier to be used in all subsequent accounting messages.
27	Session-Timeout	Integer	O	It is the timeout value for the session
28	Idle-Timeout	Integer	O	It is the timeout value for idle session
30	Called-Station-Id	String	O	It is the phone number the user called or the identifier for target network.
88	Framed-Pool	String	O	It is the name of a local pool to be used for address allocation.
97	Framed-IPv6-Prefix	Address(IPv6)	O	It might contain IPv6 address prefixes.
100	Framed-IPv6-Pool	String	O	It is the name of a local pool to be used for address allocation.
26/311	MS-Primary-DNS-server	Address(IPv4)	O	It contains the primary DNS server address





**Table 3** Access-Accept Message

Attr #	Element	Type	P	Description
26/311	MS-Secondary-DNS-Server	Address(IPv4)	O	It contains the secondary DNS server address
26/311	MS-Primary-NBNS-Server	Address(IPv4)	O	It contains the primary NetBios name server address
26/311	MS-Secondary-NBNS-Server	Address(IPv4)	O	It contains the secondary NetBios server address
26/10923	Suggested-Rule-Space	See Table 15	O	See Table 15 for the sub attributes description.
26/10923	Access-control-group	See Table 13	O	See Table 13 for the sub attributes description.
26/10415	3GPP Vendor-Specific	See Table 12	O	See Table 12 for the sub attributes description.

### 4.1.3 Access-Reject Message

The Access-Reject message is sent to RADIUS Client (NAS) from IPWorks AAA Server.

Table 4 describes the significant attributes for the Access-Reject Messages:

**Table 4** Access-Reject Message

Attr #	Element	Type	P	Description
18	Reply-Message	Text	O	The text is displayed to the user.

## 4.2 Accounting Messages

This section describes the content of IPWorks AAA Accounting Messages.

The message format follows the standard RADIUS protocol as specified in Reference [6], and the attributes supported by these messages are specified in Reference [6] , Reference [7], Reference [10] and Reference [13].

### 4.2.1 Accounting-Request (Start) Message

The Accounting-Request (Start) message is sent from RADIUS Client (NAS) to IPWorks AAA Server.

Table 5 describes the significant attributes for the Accounting-Request (Start) Message:

**Table 5 Accounting-Request (Start) Message**

Attr #	Element	Type	P	Description
1	User-Name	String	C	It indicates the name of the user to be authenticated.
4	NAS-IP-Address	Address(IPv4)	M	It is the NAS IP Address for communication with the server.
5	NAS-Port	String	O	It is A configurable value for Accounting-Request.
32	NAS-Identifier	String	M	It is the hostname of the NAS for communication with the server.
6	Service-Type	Integer	M	It indicates the type of service for this user.
7	Framed-Protocol	Integer	M	It indicates the type of protocol for this user.
8	Framed-IP-Address	Address(IPv4)	C	It is the User IP Address. <sup>(1)</sup>
97	Framed-IPv6-Prefix	Address(IPv6)	C	It is the User IPv6 prefix <sup>(1)</sup> .
25	Class	String	C	Received in the access accept. <sup>(2)</sup>
30	Called-Station-Id	String	O	It is the phone number the user called or the identifier of the network.
31	Calling-Station-Id	String	O	It is the phone number that the call came from.
40	Acct-Status-Type	Integer	M	It is the type of accounting message, in this message it is 1 (Start).
41	Acct-Delay-Time	Integer	M	It indicates how long the NAS has been trying to find the user, for, and can be subtracted from the time of arrival at the server to find the approximate time in seconds of generating this Accounting-Request.
44	Acct-Session-Id	String	M	It is the user session identifier.
45	Acct-Authentic	Integer	M	It is the authentication method, 1(RADIUS) or 2(RADIUS).
46	Acct-Session-Time	Integer	O	It is the number of seconds that the user has received service.
61	NAS-Port-Type	Integer	M	It is the type of physical port used by NAS.
26/10415	3GPP Vendor-Specific	See Table 12	O	See Table 12 for the sub attributes description.

(1) Either IPv4 address or IPv6 prefix is present.

(2) The presence of this attribute is conditional upon it being received in the Access-Accept message.

## 4.2.2 Accounting-Request (Stop) Message

The Accounting-Request (Stop) message is sent from RADIUS Client (NAS) to IPWorks AAA Server.

Table 6 describes the significant attributes for the Accounting-Request (Stop) Message:

**Table 6 Accounting-Request (Stop) Message**

Attr #	Element	Type	P	Description
1	User-Name	String	C	It indicates the name of the user to be authenticated.
4	NAS-IP-Address	Address(IPv4)	M	The NAS IP Address for communication with AAA Server.
5	NAS-Port	String	O	It is a configurable value for Accounting-Request.



**Table 6 Accounting-Request (Stop) Message**

Attr #	Element	Type	P	Description
32	NAS-Identifier	String	M	It is the hostname of the NAS for communication with the server
6	Service-Type	Integer	M	It indicates the type of service for this user.
7	Framed-Protocol	Integer	M	It indicates the type of protocol for this user.
8	Framed-IP-Address	Address(IPv4)	C	It is the User IP Address. <sup>(1)</sup>
97	Framed-IPv6-Prefix	Address(IPv6)	C	User IPv6 prefix. <sup>(1)</sup>
25	Class	String	C	It is received in the access accept. <sup>(2)</sup>
30	Called-Station-Id	String	O	It is the phone number the user called or the network.
31	Calling-Station-Id	String	O	It is the phone number where the call came from.
40	Acct-Status-Type	Integer	M	It is the type of accounting message, in this case it is 2 (Stop).
41	Acct-Delay-Time	Integer	M	It indicates how long the NAS has been trying to find the server for, and can be subtracted from the time of a successful connection to find the approximate time in seconds spent generating this Accounting-Request.
42	Acct-Input-Octets	Integer	O	It indicates how many octets have been received by the server of this service being provided.
43	Acct-Output-Octets	Integer	O	It indicates how many octets have been sent by the server delivering this service.
44	Acct-Session-Id	String	M	It is the User session identifier.
45	Acct-Authentic	Integer	M	It is the authentication method, 1(RADIUS) or 2(Chap).
46	Acct-Session-Time	Integer	O	It is the number of seconds that the user has been connected to the server.
47	Acct-Input-Packets	Integer	O	This attribute indicates how many packets have been received by the server over the course of this service being provided.
48	Acct-Output-Packets	Integer	O	It indicates how many packets have been sent by the server delivering this service to a user.
49	Acct-Terminate-Cause	Integer	M	It indicates how the session was terminated.
61	NAS-Port-Type	Integer	M	It is the type of physical port used by NAS.
26/10415	3GPP Vendor-Specific	See Table 12	O	See Table 12 for the sub attributes description. bbf

(1) Either IPv4 address or IPv6 prefix is present.

(2) The presence of this attribute is conditional upon it being received in the Access-Accept message.

### 4.2.3 Accounting-Request (On) Message

The Accounting-Request (On) message is sent from RADIUS Client (NAS) to IPWorks AAA Server.

Table 7 describes the significant attributes for the Accounting-Request (On) Message:

**Table 7 Accounting-Request (On) Message**

Attr #	Element	Type	P	Description
4	NAS-IP-Address	Address(IPv4)	M	It is the NAS IP Address for communication with
30	Called-Station-Id	String	C	It is the phone number the user called or the identifier for the target network.
32	NAS-Identifier	String	M	It is the hostname of the NAS for communication with the AAA server
40	Acct-Status-Type	Integer	M	It is the type of accounting message, in this message, the content is 7 (Accounting-On).
44	Acct-Session-Id	String	M	It is the user session identifier.

#### 4.2.4 Accounting-Request (Off) Message

The Accounting-Request (Off) message is sent from RADIUS Client (NAS) to IPWorks AAA Server.

Table 8 describes the significant attributes for the Accounting-Request (Off) Message:

**Table 8 Accounting-Request (Off) Message**

Attr #	Element	Type	P	Description
4	NAS-IP-Address	Address(IPv4)	M	It is the NAS IP Address for communication with AAA Server
30	Called-Station-Id	String	C	It is the phone number the user called or the identifier for the target network.
32	NAS-Identifier	String	M	It is the hostname of the NAS for communication with the AAA server
40	Acct-Status-Type	Integer	M	It is the type of accounting message, in this message, the content is 8 (Accounting-Off).
44	Acct-Session-Id	String	M	It is the user session identifier.

#### 4.2.5 Accounting-Request (Interim-Update) Message

The Accounting-Request (Interim-Update) message is sent from RADIUS Client (NAS) to IPWorks AAA Server.

Table 9 describes the significant attributes for the Accounting-Request (Interim-Update) Message:

**Table 9 Accounting-Request (Interim-Update) Message**

Attr #	Element	Type	P	Description
1	User-Name	String	C	It indicates the name of the user to be authenticated.
4	NAS-IP-Address	Address(IPv4)	M	It is the NAS IP Address for communication with AAA Server
5	NAS-Port	String	O	It is a configurable value for Accounting-Requests



**Table 9 Accounting-Request (Interim-Update) Message**

Attr #	Element	Type	P	Description
32	NAS-Identifier	String	M	It is the hostname of the NAS for communication with the AAA server
6	Service-Type	Integer	M	It indicates the type of service for this user.
7	Framed-Protocol	Integer	M	It indicates the type of protocol for this user.
8	Framed-IP-Address	Address(IPv4)	C	It is the User IP Address.
97	Framed-IPv6-Prefix	Address(IPv6)	C	It is the User IPv6 prefix.
25	Class	String	C	It is received in the access accept.
30	Called-Station-Id	String	O	It is the phone number the user called or the identifier for the target network.
31	Calling-Station-Id	String	O	It is the phone number where the call came from.
40	Acct-Status-Type	Integer	M	It is the type of accounting message, in this message, the code is 3 (Interim-Update).
41	Acct-Delay-Time	Integer	M	It indicates how long the NAS has been trying to send this record, for, and can be subtracted from the time of arrival on the AAA server to find the approximate time in seconds of the event generating this Accounting-Request.
42	Acct-Input-Octets	Integer	O	It indicates how many octets have been received over the course of this service being provided.
43	Acct-Output-Octets	Integer	O	It indicates how many octets have been sent in the course of delivering this service.
44	Acct-Session-Id	String	M	It is the user session identifier.
45	Acct-Authentic	Integer	M	It is the authentication method, 1(RADIUS) or 2(LOCAL)
46	Acct-Session-Time	Integer	O	It is the number of seconds that the user has received service.
47	Acct-Input-Packets	Integer	O	It indicates how many packets have been received over the course of this service being provided to a user.
48	Acct-Output-Packets	Integer	O	It indicates how many packets have been sent in the course of delivering this service to a user.
61	NAS-Port-Type	Integer	M	It is the type of physical port used by NAS.
26/10415	3GPP Vendor-Specific	See Table 12	O	See Table 12 for the sub attributes description.

#### 4.2.6 Accounting-Response Message

The Accounting-Response message is sent to RADIUS Client (NAS) from the IPWorks AAA Server.

Accounting-Response Message is not required to have any attributes in it.

### 4.3 Dynamic Authorization Extension Messages

The section describes the messages used for dynamic authorization extension to RADIUS, which is defined in Reference [12].



### 4.3.1 Disconnect-Request Message

The Disconnect-Request message is sent to Dynamic Authorization Server (that is, NAS) from IPWorks AAA Server.

The IPWorks AAA supported attributes for this message is specified in RFC 2865, RFC 3162, RFC 5176, and 3GPP TS 29.061.

Table 10 describes the significant attributes for the Disconnect-Request Message:

Table 10 Disconnect-Request Message

Attr #	Element	Type	P	Description
8	Framed-IP-Address	Address(IPv4)	C	It is the user IP address <sup>(1)</sup>
97	Framed-IPv6-Prefix	String	C	It is the user IPv6 prefix <sup>(1)</sup>
44	Acct-Session-Id	String	M	It is the user session identifier
26/10415	3GPP Vendor-Specific	See Table 12	O	See Table 12 for the sub attributes description.

(1) Either an IPv4 or an IPv6 address or prefix is present. If no such address is available to the RADIUS-server, the value 0.0.0.0 is used.

### 4.3.2 Disconnect-ACK/NAK

The Disconnect-ACK/NAK message is sent from Dynamic Authorization Server (that is, NAS) to IPWorks AAA Server.

As there are not any specific requirement for these messages, the content of these messages follows the message content and format specified in RFC 5176.

### 4.3.3 Change-Of-Authorization (CoA) Request

The Change-Of-Request message is sent to Dynamic Authorization Server (that is, NAS) by IPWorks AAA Server.

The IPWorks AAA supported attributes for this message is specified in RFC 5176 and Ericsson GGSN 2009A Gi interface.

Table 11 describes the significant attributes for CoA Request:

Table 11 Change-Of-Authorization Message

Attr #	Element	Type	P	Description
44	Acct-Session-Id	String	M	User session identifier
26/10923	Access-control-group	String	M	Sub attributes according to Table 13



## 5 Information Elements

### 5.1 3GPP Vendor Specific Sub Attributes

Table 12 describes the sub attributes of the 3GPP Vendor-Specific attribute of the Access-Request, Accounting-Request (Start), Accounting-Request (Stop), Accounting-Request (Interim-Update), and Disconnect Request messages.

The definition of these attributes can be found in 3GPP TS 29.061.

*Table 12 3GPP Vendor Specific Sub Attributes*

Sub Attr #	Sub Attribute Name	Description	Presence	Associated Attribute (Location of Sub Attr)
1	3GPP-IMSI	IMSI for this user	Optional-Configurable	Access-Request, Accounting-Request (Start), Accounting-Request (Stop), Accounting-Request (Interim-Update)
2	3GPP-Charging-Id	The charging ID for this PDP Context (along with the GGSN-Address, constitutes a unique identifier for the PDP context)	Optional-Configurable	Accounting-Request (Start), Accounting-Request (Stop), Accounting-Request (Interim-Update)
3	3GPP-PDP Type	Type of PDP context, such as IP or PPP	Optional-Configurable	Access-Request, Accounting-Request (Start), Accounting-Request (Stop), Accounting-Request (Interim-Update)
4	3GPP-CG-Address	Charging Gateway IP address	Optional-Configurable	Access-Request, Accounting-Request (Start), Accounting-Request (Stop), Accounting-Request (Interim-Update)
5	3GPP-GPRS-QoS-Negotiated-Profile	QoS profile applied by the GGSN	Optional-Configurable	Access-Request, Accounting-Request (Start), Accounting-Request (Stop), Accounting-Request (Interim-Update)
6	3GPP-SGSN-Address	The SGSN IP address that is used by the GTP control plane for the handling of control messages. It is used to identify the PLMN to which the user is attached.	Optional-Configurable	Access-Request, Accounting-Request (Start), Accounting-Request (Stop), Accounting-Request (Interim-Update)
7	3GPP-GGSN-Address	The GGSN IP address that is used by the GTP control plane for the context establishment. It is the same as the GGSN IP address used in the G-CDRs	Optional-Configurable	Access-Request, Accounting-Request (Start), Accounting-Request (Stop), Accounting-Request (Interim-Update)
8	3GPP-IMSI-MCC-MNC	The MCC and MNC extracted from the IMSI of the user (first five or six digits, as applicable from the presented IMSI)	Optional-Configurable	Access-Request, Accounting-Request (Start), Accounting-Request (Stop), Accounting-Request (Interim-Update)
9	3GPP-GGSN-MCC-MNC	The MCC-MNC of the network to which the GGSN belongs to	Optional-Configurable	Access-Request, Accounting-Request (Start), Accounting-Request (Interim-Update)
10	3GPP-NSAPI	Identifies a particular PDP context for the associated PDN and MSISDN or IMSI from creation to deletion	Optional-Configurable	Access-Request, Accounting-Request (Start), Accounting-Request (Stop), Accounting-Request (Interim-Update)
11	3GPP-Session-Stop-Indicator	Indicates to the RADIUS server that the last PDP context of a session is released and that the PDP session has been terminated	Optional-Configurable	Accounting-Request (Stop)



Table 12 3GPP Vendor Specific Sub Attributes

Sub Attr #	Sub Attribute Name	Description	Presence	Associated Attribute (Location of Sub Attr)
12	3GPP- Selection-Mode	Contains the Selection mode for this PDP Context received in the Create PDP Context Request Message	Optional-Configurable	Access-Request, Accounting-Request (Start), Accounting-Request (Stop), Accounting-Request (Interim-Update)
13	3GPP-Charging-Characteristics	Contains the charging characteristics for this PDP Context.  This is either received from the SGSN in the Create PDP Context Request Message (only available in R99 and later releases) or from the RADIUS server in the Access-Accept message.	Optional-Configurable	Access-Accept, Access-Request, Accounting-Request (Start), Accounting-Request (Stop), Accounting-Request (Interim-Update)
17	3GPP-IPv6-DNS-Servers	A list of IPv6 addresses of DNS servers	Optional	Access-Accept
18	3GPP-SGSN-MCC-MNC	Specifies the Mobile Country Code (MCC) and Mobile Network Code (MNC), that is PLMN ID, of the SGSN. PLMN ID information is available in the following prioritized order: <ul style="list-style-type: none"> <li>• If a PLMN ID is received from the SGSN, this value is used.</li> <li>• If a PLMN ID has been configured for the SGSN, this value is used.</li> <li>• If a PLMN ID has been provided from a RADIUS server, this value is used.</li> <li>• If a PLMN ID has been provided from a RADIUS server with RADIUS Assisted Selection of APN (RAAS), this value is used.</li> </ul> If no information on PLMN ID is available, this AVP is omitted.	Optional-Configurable	Access-Request, Access-Accept, Accounting-Request (Start), Accounting-Request (Stop), Accounting-Request (Interim-Update)
19	3GPP-Teardown-Indicator	Indicates to the GGSN that all PDP contexts for this particular user and sharing user sessions need to be deleted.	Optional	Disconnect Request
20	3GPP-IMEISV	International Mobile Equipment Id and its Software Version	Optional-Configurable	Access-Request, Accounting-Request (Start)
21	3GPP-RAT-Type	Indicates which radio access technology is serving the UE. If a RAT type is received from the SGSN, this value is used. Otherwise, RAT type information is taken from a preconfigured table in the GGSN and then this value is used. If no information on RAT type is available, this AVP is omitted.	Optional-Configurable	Access-Request, Accounting-Request (Start), Accounting-Request (Stop), Accounting-Request (Interim-Update)
22	3GPP-User-Location-Info	Indicate details of where the UE is located (for example, SAI or CGI)	Optional-Configurable	Access-Request, Accounting-Request (Start), Accounting-Request (Stop), Accounting-Request (Interim-Update)
23	3GPP-MS-TimeZone	Indicate the offset between universal time and local time in steps of 15 minutes of where the MS currently resides.	Optional-Configurable	Access-Request, Accounting-Request (Start), Accounting-Request (Stop), Accounting-Request (Interim-Update)





**Table 12** 3GPP Vendor Specific Sub Attributes

Sub Attr #	Sub Attribute Name	Description	Presence	Associated Attribute (Location of Sub Attr)
25	3GPP-Packet-Filter	Exactly one packet filter used for this PDP context. If more than one filter is to be sent, one VSA per filter must be used.	Optional-Configurable	Accounting-Request (Start), Accounting-Request (Stop), Accounting-Request (Interim-Update)
26	3GPP-Negotiated-DSCP	DSCP used to mark the IP packets of this PDP context on the Gi interface	Optional-Configurable	Accounting-Request (Start), Accounting-Request (Stop), Accounting-Request (Interim-Update)

## 5.2 Access-Control-Group Sub Attributes

Table 13 describes the sub attributes of the Access-control-group attribute in the Access-Accept and Change-of-Authorization messages.

**Table 13** Access-Control-Group Subattributes

Sub Attr #	Subattribute Name	Description	Presence	Content	Associated Attribute (Location of Subattr)
33	Access-control-group-id	Gx Access-control-group ID (4 Octets)	Mandatory	OctetString(4)	Access-Accept, Change-of-Authorization
34	Authorization-code	Ericsson proprietary Gx+ cause code.	Optional	OctetString(4)	Access-Accept, Change-of-Authorization

## 5.3 Radius-Supported-VSA Related Messages

This section describes the Vendor Specific AVPs(VSAs) related messages supported by IPWorks AAA Radius Server when communicating with Ericsson Network Gateway by using Redback (RB) VSAs and Broadband Forum (BBF) VSAs.

**Note:** The RB Vendor-Id=2352. BBF Vendor-Id=3561. More BBF related information can be found in RFC 4679.

### 5.3.1 Access-Request Radius Message

#### 5.3.1.1 PPP Circuit Type

The format of Point to Point Protocol (PPP) Access-Request packet is listed as follows:

```
Access-Request ::= <RADIUS Header>
{
  User-Name
  User-Password | CHAP-Password
  [ Called-Station-Id ]
  [ Calling-Station-Id ]
  Framed-Protocol
  NAS-Identifier
  NAS-IP-Address
}
```



```

{ NAS-Port }
{ NAS-Port-Id }
{ NAS-Port-Type }
{ RB-Medium-Type }
{ RB-MAC-Address }
{ RB-NAS-Real-Port }
{ RB-OS-Version }
{ RB-Platform-Type }
{ Service-Type }
[ State ]
* [AVP]

```

**Note:** PPP Access-Request packets are used by the following access methods:

- PPP over Ethernet (PPPoE)

### 5.3.1.2 DHCP Circuit Type

The format of Dynamic Host Configuration Protocol (DHCP) Access-Request packet is listed as followings:

```

Access-Request ::= <RADIUS Header>
{ User-Name }
[ Called-Station-Id ]
[ Calling-Station-Id ]
{ Framed-Protocol }
{ NAS-Identifier }
{ NAS-IP-Address }
{ NAS-Port }
{ NAS-Port-Id }
{ NAS-Port-Type }
{ RB-Agent-Circuit-Id }
{ RB-Agent-Remote-Id }
{ RB-Medium-Type }
{ RB-MAC-Address }
{ RB-NAS-Real-Port }
{ RB-OS-Version }
{ RB-Platform-Type }
{ Service-Type }
[ State ]
* [AVP]

```

**Note:** DHCP Access-Request packets are used by the following access methods:

- IP over Ethernet (IPoE)
- WiFi

### 5.3.1.3 EAP Authentication

The format of Extensible Authentication Protocol (EAP) is listed as follows:



```

Access-Request ::= <RADIUS Header>
    { User-Name }
    [ Called-Station-Id ]
    [ Calling-Station-Id ]
    { Framed-Protocol }
    { NAS-Identifier }
    { NAS-IP-Address }
    { NAS-Port }
    { NAS-Port-Id }
    { NAS-Port-Type }
    { Service-Type }
    { EAP-Message }
    { Message-Authenticator }
    [ Chargeable-User-Identity ]
    [ State ]
    { RB-Medium-Type }
    { RB-MAC-Address }
    { RB-NAS-Real-Port }
    { RB-OS-Version }
    { RB-Platform-Type }
    * [AVP]

```

#### Where:

- Calling-Station-Id: User's MAC address
- User-Name: User's IMSI in full format: MCC+MNC+MSIN@realm
- Chargeable-User-Identity: Not sent from Ericsson Broadband Network Gateway (BNG) to the Service-Aware Policy Controller (SAPC).

The SAPC adds Chargeable-User-Identity (containing the null character, that is '\0') when proxying Access-Request to the AAA server.

## 5.3.2 Access-Accept Radius Message

Any RADIUS attribute returned by an external AAA RADIUS server which is not listed in the subsections must be configured within a default profile so that the SAPC can generate the correct CoA-Request for the user session.

### 5.3.2.1 PPP Circuit Type

The format of PPP Access-Accept packet is listed as follows:

```

Access-Accept ::= <RADIUS Header>
    [ Class ]
    { Framed-IP-Address | Framed-IPv6-Prefix }
    [ Framed-IP-Netmask ]
    * [ Framed-Route | Framed-IPv6-Route ]
    [ Port-Limit ]
    { RB-Context-Name }

```



\* [AVP]

### 5.3.2.2 DHCP Circuit Type

The format of DHCP Access-Accept packet is listed as follows:

```
Access-Accept ::= <RADIUS Header>
[ Framed-IP-Address ]
[ Framed-IPv6-Prefix ]
[ Framed-IP-Netmask ]
* [ Framed-Route ]
[ Port-Limit ]
[ Filter-Id ]
[ Idle-Timeout ]
{ RB-Context-Name }
[ RB-ATM-Profile-Name ]
[ RB-Deactivate-Service-Name ]
*[ RB-Dynamic-Qos-Param ]
[ RB-Forward-Policy ]
[ RB-HTTP-Redirect-Profile-Name | RB-HTTP-Redirect
[ RB-IGMP-Service-Profile-Name ]
[ RB-Mcast-MaxGroups ]
[ RB-Mcast-Receive ]
[ RB-Mcast-Send ]
[ RB-NAT-Profile-Name ]
[ RB-Qos-Metering-Profile-Name ]
[ RB-Qos-Policing-Profile-Name ]
[ RB-Qos-Queuing-Profile-Name ]
[ RB-Qos-Rate-Inbound ]
[ RB-Qos-Rate-Outbound ]
[ RB-Service-Name ]
[ RB-Service-Options ]
[ RB-Service-Parameter ]
{ RB-Context-Name }
{ RB-DHCP-Max-Leases }
[ Session-Timeout ]
* [AVP]
```

### 5.3.2.3 EAP Authentication

The format of EAP Access-Accept packet is listed as follows:

```
Access-Accept ::= <RADIUS Header>
[ EAP-Message ]
[ Message-Authenticator ]
[ Framed-IP-Netmask ]
* [ Framed-Route ]
[ Port-Limit ]
[ Chargeable-User-Identity ]
* [ Vendor-Specific ]
[ State ]
* [AVP]
```



### Where:

Chargeable-User-Identity is sent from AAA server to the SAPC, and proxied back from the SAPC to Ericsson BNG and it contains the user's MSISDN.

### 5.3.3 Accounting-Request Radius Message

The format of Accounting-Request packet is listed as follows:

```
Accounting-Request ::= <RADIUS Header>
                        <Standard Accounting Attributes>
                        [ RB-Acct-Input-Octets-64 ]
                        [ RB-Acct-Output-Octets-64 ]
                        [ RB-Acct-Reason ]
                        [ RB-Agent-Circuit-Id ]
                        [ RB-Agent-Remote-Id ]
                        [ RB-Assigned-IP-Address ]
                        [ RB-ATM-Profile-Name ]
                        { RB-Context-Name }
                        * [ RB-Dynamic-Qos-Param ]
                        [ RB-Forward-Policy ]
                        [ RB-HTTP-Redirect-Profile-Name |
                          RB-HTTP-Redirect-URL ]
                        [ RB-IGMP-Service-Profile-Name ]
                        * [ RB-IPv6-DNS ]
                        * [ RB-IPv6-Profile ]
                        { RB-MAC-Address }
                        [ RB-Mcast-MaxGroups ]
                        [ RB-Mcast-Receive ]
                        [ RB-Mcast-Send ]
                        [ RB-Medium-Type ]
                        { RB-NAS-Real-Port }
                        [ RB-NAT-Profile-Name ]
                        { RB-OS-Version }
                        { RB-Platform-Type }
                        [ RB-Qos-Metering-Profile-Name ]
                        [ RB-Qos-Policing-Profile-Name ]
                        [ RB-Qos-Queuing-Profile-Name ]
                        [ RB-Qos-Rate-Inbound ]
                        [ RB-Qos-Rate-Outbound ]
                        [ RB-Service-Name ]
                        [ RB-Service-Options ]
                        [ RB-Service-Parameter ]
                        * [ RB-Session-Traffic-Limit ]
                        [ RB-vCPE-Device-Policy ]
                        [ RB-vCPE-Id ]
                        [ RB-vCPE-MAC-IP-Pairs ]
                        [ RB-vCPE-Profile ]
                        [ RB-vCPE-Transport-Policy ]
                        * [AVP]
```



### 5.3.4 Radius Supported RB and BBF Attributes

Table 14 shows the Radius supported RB and BBF attributes:

*Table 14 Radius Supported RB and BBF Attributes*

#	VSA Name	Sent in Access-Request	Sent in Acct-Request	Received in Access-Response	Description
1	Client-DNS-Pri	No	Yes	Yes	IP address of the primary D subscriber's connection.
2	Client-DNS-Sec	No	Yes	Yes	IP address of the secondary subscriber's connection.
3	DHCP-Max-Leases	No	Yes	Yes	Integer. The maximum num this subscriber can allocate t is from 1 to 255.
4	Context-Name	No	Yes	Yes	It binds the subscriber sessi overriding the structured use only interpreted when global
5	Bridge-Group	No	No	Yes	String. Bridge group name; the named bridge group.
6	BG-Aging-Time	No	No	Yes	String. bg-name:val; It config for the subscriber attached t
7	BG-Path-Cost	No	No	Yes	String. bg-name:val; It config for the subscriber attached t
8	BG-Span-Dis	No	No	Yes	String. bg-name:val; It disab subscriber attaching to the n val argument can be either 1=TRUE 0=FALSE
9	BG-Trans-BPDU	No	No	Yes	String. bg-name:val; It sends bridge protocol data units (B attached to the named bridge can be either of the following 1=TRUE 0=FALSE
14	Source-Validation	No	Yes	Yes	Integer. It enables the sourc according to one of the follow 1=TRUE 0=FALSE
15	Tunnel-Domain	No	No	Yes	Integer. It binds the subscrib the domain name portion of one of the following values: 1=TRUE 0=FALSE



Table 14 Radius Supported RB and BBF Attributes

#	VSA Name	Sent in Access-Request	Sent in Acct-Request	Received in Access-Response	Description
16	Tunnel-Local-Name	No	No	Yes	String. It defines the local name of the remote peer during the tunnel establishment.
17	Tunnel-Remote-Name	No	No	Yes	String. It defines an alias for the remote peer.
18	Tunnel-Function	No	Yes	Yes	Integer. It determines this is a LAC-only endpoint or an LNS. One of the following values: 1=LAC only 2=LNS only
19	Tunnel_Flow_Control	Yes	Yes	No	Integer. It specifies using flow control for the L2TP peer (LAC or LNS) channel.
20	Tunnel_Static	Yes	Yes	No	Integer. It specifies the static tunnel given tunnel.
21	Tunnel-Max-Sessions	No	Yes	Yes	Integer. It limits the number of sessions using this tunnel configuration.
22	Tunnel-Max-Tunnels	No	Yes	Yes	Integer. It limits the number of tunnels initiated using this tunnel configuration.
23	Tunnel-Session-Auth	No	No	Yes	Integer. It specifies the authentication method during PPP authentication. One of the following values: 1=CHAP 2=PAP 3=CHAP-PAP
24	Tunnel-Window	No	No	Yes	Integer. It configures the receive window for incoming L2TP messages.
25	Tunnel-Retransmit	No	No	Yes	Integer. It specifies the number of times it retransmits a control message.
26	Tunnel-Cmd-Timeout	No	No	Yes	Integer. It specifies the timeout interval between retransmissions.
27	PPPOE-URL	No	Yes	Yes	String in PPPoE URL format. The URL that is sent to the remote peer in the PADM packet.
28	PPPOE-MOTM	No	Yes	Yes	String. It defines the PPPoE MOTM sent to the remote PPPoE peer.



Table 14 Radius Supported RB and BBF Attributes

#	VSA Name	Sent in Access-Request	Sent in Acct-Request	Received in Access-Response	Description
29	Tunnel-Group	No	Yes	Yes	Integer. It indicates whether the peer is a group with a list of member peers. 1=TRUE 0=FALSE
30	Tunnel-Context	No	Yes	Yes	String. Context name. It is used to identify the peer and this attribute specifies the peer should be found.
31	Tunnel-Algorithm	No	No	Yes	Integer. It specifies the session algorithm used to choose between the peers in the RADIUS response. This attribute is based on how to interpret standard Tunnel-Preference, according to the following values: 1=Priority 2=Load-Balance 3=Weighted round-robin
32	Tunnel-Deadtime	No	No	Yes	Integer. It specifies the number of seconds no sessions are attempted to be established if the peer is down.
33	Mcast-Send	No	Yes	Yes	Integer. It defines whether the peer sends multicast packets, according to the following values: 1=NO SEND 2=SEND 3=UNSOLICITED SEND
34	Mcast-Receive	No	Yes	Yes	Integer. It defines whether the peer receives multicast packets, according to the following values: 1=NO RECEIVE 2=RECEIVE
35	Mcast-MaxGroups	No	Yes	Yes	Integer. It specifies the maximum number of groups of which the subscriber can be a member.
36	Ip-Address-Pool-Name	No	Yes	Yes	String. Name of the interface or pool to assign an IP pool address to the subscriber.
37	Tunnel-DNIS	No	Yes	Yes	Integer. L2TP peer parameter indicating if sessions from this peer are terminated by the incoming DNIS AVP if present. 1 = DNIS 2 = DNIS ONLY





Table 14 Radius Supported RB and BBF Attributes

#	VSA Name	Sent in Access-Request	Sent in Acct-Request	Received in Access-Response	Description
38	Medium-Type	Yes	Yes	No	Integer. It contains the medium type. The system sets this value to the medium type of subscribers.
39	PVC-Encapsulation-Type	No	No	Yes	Integer. Encapsulation type. 2 = Routed 1483 4 = ATM multi 5 = Bridged 1483 6 = ATM PPP 7 = ATM PPP serial 8 = ATM PPP NLPID 9 = ATM PPP auto 10 = ATM PPPoE 12 = ATM PPP LLC 22 = Ethernet IPoE 23 = Ethernet PPPoE 24 = Ethernet dot1q 26 = Ethernet dot1q pppoe 31 = Ethernet dot1q tunnel 32 = Ethernet dot1q multi 33 = Ethernet dot1q tunnel
40	PVC-Profile-Name	No	No	Yes	String. Name of the ATM profile to be assigned to the subscriber record, or the default profile, using the subscriber configuration name.
42	Bind-Type	No	No	Yes	Integer. Binding type to be used. 1 = authentication 3 = interface 4 = subscriber 14 = autosubscriber CCO circuits support only subscribers
43	Bind-Auth-Protocol	No	No	Yes	Integer. Authentication protocol. 1 = PAP 2 = CHAP 4 = CHAP PAP 5 = AAA-PPP-CHAP-WA 7 = PAP CHAP
44	Bind-Auth-Max-Sessions	No	No	Yes	Integer. It is the maximum number of sessions allowed to be created for the same subscriber for PPPoE sessions using encapsulation over L2TP.
45	Bind-Bypass-Bypass	No	No	Yes	String. Name of the bypass profile.



Table 14 Radius Supported RB and BBF Attributes

#	VSA Name	Sent in Access-Request	Sent in Acct-Request	Received in Access-Response	Description
46	Bind-Auth-Context	No	No	Yes	String. It is the bind authenticator context. It also specifies the same for PPTP with Ethernet encapsulation
47	Bind-Auth-Service-Group	No	No	Yes	String. It is the bind authenticator service group. It also specifies the same for PPTP with Ethernet encapsulation
48	Bind-Bypass-Context	No	No	Yes	String. Bind bypass context
49	Bind-Int-Context	No	No	Yes	String. It is the bind interface context. It specifies the same for IP bridging with Ethernet encapsulation
50	Bind-Tun-Context	No	No	Yes	String. Bind tunnel context
51	Bind-Ses-Context	No	No	Yes	String. Bind session context
52	Bind-Dot1q-Slot	No	No	Yes	Integer. Bind 802.1Q slot number
53	Bind-Dot1q-Port	No	No	Yes	Integer. Bind 802.1Q port number
54	Bind-Dot1q-Vlan-Tag-Id	No	No	Yes	Integer. Bind 802.1Q VLAN ID
55	Bind-Int-Interface-Name	No	No	Yes	String. It is the bind interface name. It is the same for IP bridging session with Ethernet encapsulation over L2TP over IP
56	Bind-L2TP-Tunnel-Name	No	No	Yes	String. Bind L2TP tunnel name
57	Bind-L2TP-Flow-Control	No	No	Yes	Integer. Bind L2TP flow control
58	Bind-Sub-User-At-Context	No	No	Yes	String. Bind subscriber context
59	Bind-Sub-Password	No	No	Yes	String. Bind subscriber password
60	Ip-Host-Addr	No	No	Yes	String in the form A.B.C.D.E.F.G.H.I.J.K.L.M.N.O.P. host address and MAC address. Separate the IP address from the MAC address with a colon



Table 14 Radius Supported RB and BBF Attributes

#	VSA Name	Sent in Access-Request	Sent in Acct-Request	Received in Access-Response	Description
61	Ip_Tos_Field	No	No	Yes	<p>Integer. It specifies the value for soft QoS:</p> <p>0 = normal            1 = min-cost only            2 = max-reliability only            3 = max-reliability plus min-cost            4 = max-throughput only            5 = max-throughput plus min-cost            6 = max-throughput plus max-reliability            7 = max-throughput plus max-reliability plus min-cost            8 = min-delay only            9 = min-delay plus min-cost            10 = min-delay plus max-throughput            11 = min-delay plus max-throughput plus min-cost            12 = min-delay plus max-throughput plus max-reliability            13 = min-delay plus max-throughput plus max-reliability plus min-cost            14 = min-delay plus max-throughput plus max-reliability plus min-cost plus max-throughput            15 = min-delay plus max-throughput plus max-reliability plus min-cost plus max-throughput plus min-cost</p>
62	NAS-Real-Port	Yes	Yes	No	<p>Integer. It indicates the port number of the circuit on which the session is established (in bits) is: SSSSPPPPCC</p> <p><b>Where:</b>            S = Slot            P = Port            C = Circuit (for ATM, 8-bit)</p>
63	Tunnel-Session-Auth-Ctx	No	Yes	Yes	String. It is the L2TP peer name of the context in which L2TP sessions should be established in the domain specified in the peer name.
64	Tunnel-Session-Auth-Service-Grp	No	Yes	Yes	String. It is the L2TP peer service group (service access group) used for all incoming PPP sessions.
67	Tunnel-Police-Rate	No	Yes	Yes	4-byte integer. It is the L2TP peer policing rate that specifies the policing rate. The valid value range is from 0 to 4294967295. If the parameter is configured, the policing rate also be configured.



Table 14 Radius Supported RB and BBF Attributes

#	VSA Name	Sent in Access-Request	Sent in Acct-Request	Received in Access-Response	Description
68	Tunnel-Police-Burst	No	Yes	Yes	4-byte integer. It is the L2TP attribute that specifies the policing burst size. The valid value range is from 0 to 4096. If this parameter is configured, the Tunnel-Police-Burst must also be configured.
69	Tunnel-L2F-Second-Password	No	Yes	Yes	String. It is L2F peer parameter password string used to authenticate peer.
70	ACL-Definition	No	Yes	Yes	String. It is used to define the ACL in the RADIUS database. The ACL definition contains username and the Service-Type, and the Access-Control-List. The data format is similar to the configuration interface (CLI).
71	PPPoE-IP-Route-Add	No	Yes	Yes	String. It allows the PPPoE attribute to be populated in terms of v if multiple PPPoE sessions are active. A set of routes can be achieved if multiple sessions are active to the client. The format is g.g.g.g.m. <b>Where:</b> h.h.h.h=IP address of destination nn=optional netmask size in bits (0 to 32). g.g.g.g=IP address of gateway for this route. If the first byte of VSA 71 is 1, this VSA is used to handle the
72	TTY-Level-Start	No	No	Yes	Integer. It indicates the start level of the administrator. The value range is from 0 to 255. The value must be less than TTY-Level-Max.
73	TTY-Level-Max	No	No	Yes	Integer. It indicates the maximum level of the administrator. The value range is from 0 to 255. The value must be greater than or equal to TTY-Level-Start.
74	Tunnel-Checksum	No	Yes	Yes	Integer. It enables GRE checksum. If the checksum is computed for each packet, this allows the remote system to verify each packet. Incoming packets with incorrect checksum are discarded. A value of 1 enables the checksum. A value for this attribute equals



Table 14 Radius Supported RB and BBF Attributes

#	VSA Name	Sent in Access-Request	Sent in Acct-Request	Received in Access-Response	Description
75	Tunnel-Profile	No	No	Yes	String. It attaches a profile when configuring a tunnel. A Tunnel-Profile attribute is ignored.
78	Tunnel-Client-VPN	No	Yes	Yes	String. Name of the target network [VPN] on the client side required for GRE. If omitted, sets the value equal to the Tunnel-Server-VPN attribute.
79	Tunnel-Server-VPN	No	Yes	Yes	String. Name of the target network [VPN] on the server side of the tunnel.
85	Tunnel-Hello-Timer	No	No	Yes	Integer. Hello timer (in seconds) before the tunnel is silent before it is configured using the peer configuration mode).
86	Redback-Reason	No	Yes	No	Integer. If the NetOp Policy router (through SNMP) is trying to clear (bounce) the clear reason value is sent in RADIUS accounting Stop.
87	Qos_Policing	No	Yes	Yes	String. It attaches a QoS subscriber session.
88	Qos_Metering	No	Yes	Yes	String. It attaches a QoS subscriber session.
89	Qos_Queueing	No	Yes	Yes	String. It attaches a QoS supported by the circuit to the subscriber session.
90	Igmp_Svc_Prof_Id	No	Yes	Yes	String. Name of the IGMP to the subscriber session.
91	Sub_Profile_Name	No	Yes	Yes	Name of the subscriber profile to the subscriber session.
92	Forward-Policy	No	Yes	Yes	String. It attaches an in to the subscriber session. The following format: in:forward-policy-name



Table 14 Radius Supported RB and BBF Attributes

#	VSA Name	Sent in Access-Request	Sent in Acct-Request	Received in Access-Response	Description
94	Reauth-String	No	No	Yes	<p>String. The format is: ID-type;subID;attr-num; attr-num;attr-value; .</p> <ul style="list-style-type: none"> <li>When the ID-type is 1, the accounting session ID. When subID is read as a name.</li> <li>The semicolon ( ; ) acts as a separator.</li> <li>Attr-num is an integer that identifies the attribute. For example, start (Filter-Id) for an access control VSA 87 (Qos_Policing) for (vendor VSAs include the filter-id).</li> <li>Attr-value is the value specified by attr-num.</li> </ul>
95	Reauth-More	No	No	Yes	Integer. 0 or 1 (False or True)
96	Agent-Remote-Id	Yes	Yes	No	<p>String. It is used for two types of sessions:</p> <ul style="list-style-type: none"> <li>Incoming CLIPS sessions to relay network. This is subcode 82 packet.</li> <li>PPPoE sessions. Sent by the agent.</li> </ul> <p>This attribute can also be sent in attribute calling-station-id nas-port-id commands in mode.</p>
97	Agent-Circuit-Id	Yes	Yes	No	<p>String. It is used for two types of sessions:</p> <ul style="list-style-type: none"> <li>CLIPS sessions coming into DHCP relay network. This is option 82 packet</li> <li>PPPoE sessions. It is sent in PADR.</li> </ul> <p>This attribute can also be sent in attribute calling-station-id nas-port-id commands in mode.</p>



Table 14 Radius Supported RB and BBF Attributes

#	VSA Name	Sent in Access-Request	Sent in Acct-Request	Received in Access-Response	Description
98	Platform-Type	Yes	Yes	No	Integer. It indicates the E which the RADIUS access supported values are listed 2=PLATFORM_TYPE_SE 3=PLATFORM_TYPE_SE
99	Client_NBNS_Pri	No	Yes	Yes	IP address. It configures NetBios Name Server (NB use.
100	Client_NBNS_Sec	No	Yes	Yes	IP address. It configures NBNS that the subscriber
101	Shaping-Profile-Name	No	Yes	Yes	String. Name of the ATM
104	IP-Interface-Name	No	Yes	Yes	String. Interface name. I specified interface. This V with VSA 3, DHCP-Max-L  This attribute can also be name command (in subsc
105	NAT-Policy-Name	No	Yes	Yes	String. NAT policy name. policy to a subscriber.
107	HTTP-Redirect-Profile-Name	No	Yes (alive/ and stop records only)	Yes	String of up to 32 character name.
108	Bind-Auto-Sub-User	No	No	Yes	String. Subscriber name bind auto-subscriber com PVC, or dot1q PVC config is included in the automa name. For more informat the format for the automa name, see Configuring B
109	Bind-Auto-Sub-Context	No	No	Yes	String. Name of context i bound with the bind auto- ATM PVC, CLIPS PVC, c mode). For more informat Configuring Bindings.



Table 14 Radius Supported RB and BBF Attributes

#	VSA Name	Sent in Access-Request	Sent in Acct-Request	Received in Access-Response	Description
110	Bind-Auto-Sub-Password	No	No	Yes	String. Password prefix as s auto-subscriber command (i or dot1q PVC configuration included in the automatically password. For more informa and the format for the auton subscriber password, see C
111	Circuit-Protocol-Encap	No	Yes	Yes	Integer. Circuit encapsulation The supported values are lis 27 = PPPoE encapsulation 34 = PPPoE multiencapsula 35 = PPPoE tunnel multienc
112	OS-Version	Yes	Yes	No	String. Software version num
113	Session-Traffic-Limit	No	Yes	Yes	<p>String.</p> <ul style="list-style-type: none"> <li>It specifies that inbound or limited. Use the in: lin format where limits are ind The limit values set for inb are independent of each o</li> <li>It specifies that inbound, o traffic to be limited. Use th limit or aggregate: limits are in Kilobytes (KB) The limit value set for aggre of both inbound and outbo</li> </ul> <p>When configuring Session-T configure the limit for <b>either</b></p> <ul style="list-style-type: none"> <li>Inbound traffic</li> <li>outbound traffic</li> <li>Both Aggregate traffic</li> </ul> <p>Users cannot configure the l <b>and</b> for inbound or outbound</p>
114	QoS-Reference	No	Yes	Yes	String. It specifies the node index, the group name, and A colon (:) separates the no group name.
125	DHCP-Vendor-Class-Id	Yes	Yes	No	String. DHCP option 60 valu





Table 14 Radius Supported RB and BBF Attributes

#	VSA Name	Sent in Access-Request	Sent in Acct-Request	Received in Access-Response	Description
127	DHCP-Vendor-Encap-Options	No	Yes	Yes	<p>String. DHCP option 43 code:value:code:value</p> <p><b>Where:</b> code = DHCP vendor-encap value = option data in one</p> <ul style="list-style-type: none"> <li>• IP address type = dot n</li> <li>• Number = decimal integ</li> <li>• string = ASCII character</li> <li>• Binary string = Hex valu commas (",")</li> </ul> <p>For descriptions of the ve found in RFC 2132, DHCP Extension, see the tables</p>
128	Acct-Input-Octets-64	No	Yes	No	Integer. 64-bit value for th attribute per RFC 2139.
129	Acct-Output-Octets-64	No	Yes	No	Integer. 64-bit value for t standard attribute per RF
130	Acct-Input-Packets-64	No	Yes	No	Integer. 64-bit value for t standard attribute per RF
131	Acct-Output-Packets-64	No	Yes	No	Integer. 64-bit value for A per RFC 2139.
133	Acct-Mcast-In-Octets-64	No	Yes	No	Integer. 64-bit value for t attribute.
134	Acct-Mcast-Out-Octets-64	No	Yes	No	Integer. 64-bit value for t attribute.
135	Acct-Mcast-In-Packets-64	No	Yes	No	Integer. 64-bit value for t attribute.
136	Acct-Mcast-Out-Packets-64	No	Yes	No	Integer. 64-bit value for t attribute.
137	LAC-Port	Yes	Yes	No	Integer. It contains the cir session on an L2TP LAC present for a subscriber c or LNS only. The circuit c session.



Table 14 Radius Supported RB and BBF Attributes

#	VSA Name	Sent in Access-Request	Sent in Acct-Request	Received in Access-Response	Description
138	LAC-Real-Port	Yes	Yes	No	Integer. It contains the circuit ID of an incoming PPPoE session. This attribute should be present for tunnel switch or LNS only.
139	LAC-Port-Type	Yes	Yes	No	<p>Integer. It contains the port ID of a session on an L2TP LAC. This attribute should be present for a subscriber on a LNS only. The port can be virtual or physical.</p> <p>The values for port types are:</p> <ul style="list-style-type: none"> <li>40 = NAS_PORT_TYPE_10G</li> <li>41 = NAS_PORT_TYPE_10G</li> <li>42 = NAS_PORT_TYPE_DS</li> <li>43 = NAS_PORT_TYPE_DS</li> <li>44 = NAS_PORT_TYPE_OC</li> <li>45 = NAS_PORT_TYPE_HS</li> <li>46 = NAS_PORT_TYPE_EI</li> <li>47 = NAS_PORT_TYPE_T1</li> <li>48 = NAS_PORT_TYPE_CH</li> <li>49 = NAS_PORT_TYPE_DS</li> <li>50 = NAS_PORT_TYPE_E3</li> <li>51 = NAS_PORT_TYPE_IM</li> <li>52 = NAS_PORT_TYPE_DS</li> <li>53 = NAS_PORT_TYPE_OC</li> <li>54 = NAS_PORT_TYPE_10</li> <li>55 = NAS_PORT_TYPE_E1</li> <li>56 = NAS_PORT_TYPE_E1</li> <li>57 = NAS_PORT_TYPE_E3</li> <li>58 = NAS_PORT_TYPE_OC</li> <li>59 = NAS_PORT_TYPE_OC</li> <li>60 = NAS_PORT_TYPE_PP</li> </ul>
140	LAC-Real-Port-Type	Yes	Yes	No	Integer. It contains the port ID of an incoming PPPoE session. This attribute should be present for tunnel switch or LNS only. See values.
142	Session-Error-Code	No	Yes	No	Integer. 32 bits. Stop recording the specific error code information for devices.
143	Session-Error-Msg	No	Yes	No	String. Stop record only. It is terminated.



Table 14 Radius Supported RB and BBF Attributes

#	VSA Name	Sent in Access-Request	Sent in Acct-Request	Received in Access-Response	Description
144	Acct_Reason	No	Yes	No	<p>Integer. It is the reason code that the router generates an account for the subscriber to RADIUS.</p> <p>The reason code values are:</p> <ul style="list-style-type: none"> <li>1 = AAA_LOAD_ACCT_SESSION_EXPIRED</li> <li>2 = AAA_LOAD_ACCT_SESSION_EXPIRED</li> <li>3 = AAA_LOAD_ACCT_SESSION_EXPIRED</li> <li>7 = AAA_ACCT_RC_SESSION_EXPIRED</li> <li>16 = AAA_LOAD_ACCT_SESSION_EXPIRED</li> <li>EXCEEDED</li> <li>17 = AAA_LOAD_ACCT_SESSION_EXPIRED</li> <li>EXCEEDED</li> <li>18 = AAA_LOAD_ACCT_SESSION_EXPIRED</li> <li>19 = AAA_LOAD_ACCT_SESSION_EXPIRED</li> <li>28 = AAA_LOAD_ACCT_SESSION_EXPIRED</li> <li>XCEEDED</li> <li>34 = AAA_ACCT_RC_SESSION_EXPIRED</li> <li>35 = AAA_ACCT_RC_SESSION_EXPIRED</li> <li>36 = AAA_ACCT_RC_SESSION_EXPIRED</li> <li>37 = AAA_ACCT_RC_SESSION_EXPIRED</li> <li>38 = AAA_ACCT_RC_SESSION_EXPIRED</li> <li>NTED</li> <li>39 = AAA_ACCT_RC_SESSION_EXPIRED</li> <li>ASED</li> </ul>
145	Mac-Addr	Yes	Yes	No	String. MAC address. The MAC address is sent in the sessions. The supported 802.1Q PVCs (tagged or untagged) on Ethernet ports.
147	Acct-Mcast-In-Octets	No	Yes	No	Integer. Number of inbound multicast octets.
148	Acct-Mcast-Out-Octets	No	Yes	No	Integer. Number of outbound multicast octets.
149	Acct-Mcast-In-Packets	No	Yes	No	Integer. Number of inbound multicast packets.
150	Acct-Mcast-Out-Packets	No	Yes	No	Integer. Number of outbound multicast packets.
151	Reauth-Session-Id	No	No	Yes	String. It identifies the reauthentication session. The value in this attribute is the session ID for the identified session.



Table 14 Radius Supported RB and BBF Attributes

#	VSA Name	Sent in Access-Request	Sent in Acct-Request	Received in Access-Response	Description
156	Qos-Rate-Inbound	No	Yes	Yes	String. It changes the inbound rate: <code>burst:excess-burst</code> and <code>excess-burst</code> values is optional.
157	Qos-Rate-Outbound	No	Yes	Yes	String. It changes the outbound rate: <code>burst:excess-burst</code> and <code>excess-burst</code> values is optional.
158	Route-Tag	No	Yes	Yes	Integer. It assigns a route tag address (Framed-IP-Route), route statements (Framed-IP-Route).
164	Dynamic-Policy-Filter	No	Yes	Yes	String. The string consists of tokens separated by one or more spaces. Tokens are allowed. The tokens are defined in statement in Section 3.5 section of the keywords and arguments.
165	HTTP-Redirect-URL	No	Yes	Yes	String. URL to which the requests are redirected.
166	DSL-Actual-Rate-Up	Yes	Yes	No	Integer 32-bit value. The actual upstream direction.
167	DSL-Actual-Rate-Down	Yes	Yes	No	Integer 32-bit value. The actual downstream direction.
168	DSL-Min-Rate-Up	Yes	Yes	No	Integer 32-bit value. The minimum upstream direction.
169	DSL-Min-Rate-Down	Yes	Yes	No	Integer 32-bit value. The minimum downstream direction.
170	DSL-Attainable-Rate-Up	Yes	Yes	No	Integer 32-bit value. The attainable upstream direction.
171	DSL-Attainable-Rate-Down	Yes	Yes	No	Integer 32-bit value. The attainable downstream direction.
172	DSL-Max-Rate-Up	Yes	Yes	No	Integer 32-bit value. The maximum upstream direction.
173	DSL-Max-Rate-Down	Yes	Yes	No	Integer 32-bit value. The maximum downstream direction.
174	DSL-Min-Low-Power-Rate-Up	Yes	Yes	No	Integer 32-bit value. The DSL minimum in the upstream direction.
175	DSL-Min-Low-Power-Rate-Down	Yes	Yes	No	Integer 32-bit value. The DSL minimum in the downstream direction.
176	DSL-Max-Inter-Delay-Up	Yes	Yes	No	Integer 32-bit value. The maximum delay in the upstream direction.



Table 14 Radius Supported RB and BBF Attributes

#	VSA Name	Sent in Access-Request	Sent in Acct-Request	Received in Access-Response	Description
177	DSL-Actual-Inter-Delay-Up	Yes	Yes	No	Integer 32-bit value. The delay in the upstream direction.
178	DSL-Max-Inter-Delay-Down	Yes	Yes	No	Integer 32-bit value. The delay in the downstream direction.
179	DSL-Actual-Inter-Delay-Down	Yes	Yes	No	Integer 32-bit value. The delay in the downstream direction.
180	DSL-Line-State	Yes	Yes	No	Integer 32-bit value. The line state. SHOWTIME 2 = IDLE 3 = BUSY
181	DSL-L2-Encapsulation	Yes	Yes	No	Integer 32-bit value. The data link encapsulation: 0 = ATM AAL5 1 = ETHERNET Encapsulation 2 = Ethernet Encapsulation LLC 2 = PPPoA NULL 3 = IPoA LLC 4 = IPoA NULL 5 = Ethernet over AAL5 LLC 6 = Ethernet over AAL5 NULL 7 = Ethernet over AAL5 NULL 8 = Ethernet over AAL5 NULL
182	DSL-Transmission-System	Yes	Yes	No	Integer 32-bit value. The transmission system are: 1 = ADSL1 2 = ADSL2 3 = ADSL2+ 4 = VDSL1 5 = VDSL2 6 = SDSL 7 = UNKNOWN
183	DSL-PPPOA-PPPOE-Inter-Work-Flag	Yes	Yes	No	Integer. PPPoA-to-PPPoE
184	DSL-combined-Line-Info	Yes	Yes	No	String. The value of the Extensions for Layer 2 Configuration Discovery and Line Configuration, "Topology Discovery."
185	DSL-Actual-Rate-Down-Factor	Yes	Yes	No	Integer. The rate that can be achieved from a PPPoE or DHCP configuration of the access subscriber configuration



Table 14 Radius Supported RB and BBF Attributes

#	VSA Name	Sent in Access-Request	Sent in Acct-Request	Received in Access-Response	Description
189	Flow_FAC_Profile	No	Yes	No	String. IT specifies the name of the Admission-Control profile. To apply the flow on the circuit of a subscriber. The Flow_FAC_Profile can only be configured under the
190	Service-Name	No	Yes	Yes	<p>String. The name of the service together with the following options:</p> <ul style="list-style-type: none"><li>• <code>service id</code>: Used when multiple instances of the same service are present.</li><li>• <code>service-parameter</code>: Zero or more parameters formatted as name-value pairs. Pairs are separated by an equals sign and spaces around it. Pairs are separated by a space.</li></ul> <p>Users can also specify service options. See VSA 192 for formatting.</p>
191	Service-Options	No	No	Yes	Integer. It specifies whether service management is enabled: ACCT-DISABLED = 0x00
192	Service-Parameter	No	Yes	Yes	<p>String. Service parameters formatted as name-value pairs in VSA 190, formatted as name-value pairs. Names and values are separated by an equals sign and spaces around it. Pairs are separated by a space.</p> <p>If a parameter needs an array, the array elements are separated by commas (,), and the value and the comma.</p> <p>If the value is a string that contains commas, enclose the string in quotes.</p>



Table 14 Radius Supported RB and BBF Attributes

#	VSA Name	Sent in Access-Request	Sent in Acct-Request	Received in Access-Response	Description
193	Service-Error-Cause	No	Yes	No	Integer. It specifies a service error cause according to one of the following values: 0 = Service success 401 = Unsupported attribute 402 = Missing attribute 404 = Invalid request 506 = Resource unavailable 550 = Generic service error 551 = Service not found 552 = Service already active 553 = Service accounting error 554 = Service duplicate profile If the RADIUS server does not support these values, they are mapped to the standard RADIUS error codes (other proxy processing error).
194	Deactivate-Service-Name	No	No	No	String. The service profile is deactivated together with the service. <ul style="list-style-type: none"> <li>• service id: Used when multiple instances of the same service are active.</li> <li>• service-parameter: Parameters are formatted as name-value pairs and are separated by an equals sign around it. Pairs are separated by a space.</li> </ul>
195	QoS-Overhead	No	Yes	Yes	String. It attaches a QoS profile to a subscriber session. If the RADIUS record of the session has the specified overhead, the session comes up.
196	Dynamic-QoS-Parameter	No	No	Yes	String. The format varies depending on the service. For more information, see Section 4.3.1. Dynamic-QoS-Parameter VSAs are used in Access-Accept or CoA-Request messages.
199	Double_Authentication	No	No	Yes	Integer. The integer value indicates the number of authentication sessions needed one more if it is received from a global session.



Table 14 Radius Supported RB and BBF Attributes

#	VSA Name	Sent in Access-Request	Sent in Acct-Request	Received in Access-Response	Description
201	DHCP-Field	Yes	Yes	No	Binary. It identifies a standard generic VSA is used to identify fields that must be sent in RADIUS accounting requests. To distinguish DHCP client field, a unique value is used within this VSA to indicate which corresponds to a specific DHCP field. Currently, this VSA supports only dhcp-client-id, 1, the giaddr or gateway address. The server uses the gateway address to route to clients based on the
202	DHCP-Option	Yes	Yes	No	Binary. It identifies a DHCP option. It is a generic VSA, which is used to support supported DHCP client options. RADIUS authentication or accounting to distinguish each supported DHCP option. A unique dhcp-sub-type field is used to indicate a specific value that corresponds to a specific DHCP option. Currently, this VSA supports options 12 (hostname), 61 (user class).
203	Security-Service	No	Yes	Yes	String configured in RADIUS security profile. Optionally it can be used using the following format:  Security-Service="ike hex-value   ASCII-value"  The IKE preshared key is obtained from the Acct-Response message or Access-Request or Acct-Request.  The ASE DPI traffic management is received in the Access-Request or Acct-Request in the format:  Security-Service="dpi policy policy-name".  To enable DPI security service, either through COA or reauthentication, configure RADIUS to send the message at initial subscriber logon with the following format:  Security-Service="dpi enable-coa".





## 5.4 Suggested-Rule-Space Sub Attributes

Table 15 describes the sub attributes of the Suggested-Rule-Space attribute in the Access-Accept message.

*Table 15 Suggested-Rule-Space Subattributes*

Sub Attr #	Subattribute Name	Description	Presence	Content	Associated Attribute (Location of Subattr)
30	Suggested-Primary-Rulespace	Suggested Primary Rule Space	Optional	UTF-8 String	Access-Accept
31	Suggested-Secondary-Rulespace	Suggested Secondary Rule Space	Optional	UTF-8 String	Access-Accept





## 6 Error Handling

Table 16 describes the behaviors of different error scenarios:

*Table 16 Error Handling*

Scenario	Return Code
ACCOUNTING_REQUEST and ACCOUNTING_REQUEST Duplicated	discard
ACCOUNTING_REQUEST failed to check the accounting request authenticator	discard
PROXY_RESPONSE failed to check the reply authenticator	discard
PROXY_RESPONSE failed to get the proxy message record	discard
DA_RESPONSE failed to get the DA message record	discard
DA_RESPONSE failed to check the reply authenticator for DA message	discard
Failed to validate Message-Authenticator	discard
ACCESS_REQUEST The number of attributes is wrong	ACCESS_REJECT
DM_REQUEST and COA_REQUEST The number of attributes is wrong	ACCESS_REJECT
The number of attributes is wrong for other messages	discard
Access-Request message contains both CHAP-Password and User-Password	discard
Access-Request message contains both ARAP-Password and User-Password	discard
Access-Request message contains both ARAP-Password and CHAP-Password	discard
Access-Request message does not contain a User-Name or a Calling-Station-ID or a Called-station-ID	discard
Access-Request User-Password or CHAP-Password or State is not contained in the message	discard
Access-Request a NAS-IP-Address or a NAS-Identifier or a NAS-IPv6-Address (or all) is not contained in the message	discard
Access-Request EAP-Message existed with no Message-Authenticator contained in the message	discard
Accounting-Request a NAS-IP-Address or a NAS-Identifier (or both) is not contained in the message	discard
an Acct-Status-Type is not contained in the Accounting-Request message	discard
Accounting-Request message does not include Acct-Session-Id	discard
Acct-Status-Type is not set to stop in the Accounting -Request message	discard
Acct-Status-Type is not set to start in the Accounting -Request message	discard
Attribute with wrong length <sup>(1)</sup>	ACCESS_REJECT/discard
unsupported attribute <sup>(1)</sup>	ACCESS_REJECT/discard
Attribute of string type value error <sup>(1)</sup>	ACCESS_REJECT/discard
Attribute of integer value error <sup>(1)</sup>	ACCESS_REJECT/discard

**Table 16 Error Handling**

Scenario	Return Code
AVP SERVICE_TYPE with wrong attribute <sup>(1)</sup>	ACCESS_REJECT/discard
Attribute of IPv4 type value error <sup>(1)</sup>	ACCESS_REJECT/discard

*(1) This ACCESS\_REJECT scenario is only for the ACCESS\_REQUEST, COA\_REQUEST and DM\_REQUEST messages. The AAA server discards the other types of messages.*



# 7 Formal Syntax

Not Applicable.





## 8 Related Standards

This section states the related standards and explains any deviations from them.

For details, refer to **Standards**.







# Reference List

## IPWorks Library Documents

- [1] *Trademark Information*
- [2] *Glossary of Terms and Acronyms*
- [3] *Typographic Conventions*

## PCAT and Other Ericsson Documents

- [4] *Gi Interface Description, 1/1551-AXB 250 10/4*

## Standards

- [5] [Remote Authentication Dial In User Service \(RADIUS\) - RFC 2865](#)
- [6] [RADIUS Accounting - RFC 2866](#)
- [7] [RADIUS Accounting Modifications for Tunnel Protocol Support - RFC 2867](#)
- [8] [RADIUS Attributes for Tunnel Protocol Support - RFC 2868](#)
- [9] [RADIUS Extensions - RFC 2869](#)
- [10] [RADIUS and IPv6 - RFC 3162](#)
- [11] [Microsoft Vendor-specific RADIUS Attributes - RFC 2548](#)
- [12] [Dynamic Authorization Extensions to Remote Authentication Dial In User Service \(Radius\) - RFC 5176](#)
- [13] [Interworking between the Public Land Mobile Network \(PLMN\) supporting packet based services and Packet Data Networks \(PDN\) - 3GPP TS 29.061 V8.2.0](#)