3GPP2 X.S0011-005-E

Version: 1.0

Version Date: November 2009

cdma2000 Wireless IP Network Standard:

Accounting Services and 3GPP2 Radius VSAs

This page is left blank intentionally.

cdma2000 Wireless IP Network Standard: Chapter 5

CONTENTS

LIST OF FIGURES

LIST OF TABLES

This page is left blank intentionally.

1 Glossary and Definitions

See [Chapter 1].

2 References

See [Chapter 1].

3 Accounting

In this revision of the standards the following are not supported:

- Per-flow based prepaid; and
- Active session hot-lining of prepaid users.

3.1 General

For the main service connection (SO33 or SO59) or the auxiliary service connection of SO60 and SO61 accounting is performed on a per service connection basis. For other auxiliary service connections (such as SO64, SO66, etc), based on local policy, accounting is performed either on a per IP flow basis or a per service connection basis for all flows that are mapped onto that service connection. If an IP flow is mapped onto the main service connection but with QoS treatment, per IP flow basis accounting can also be performed.

3.1.1 Usage Data Records

Packet Data Accounting parameters are divided into radio specific parameters collected by the RAN, and IP network specific parameters collected by the Serving PDSN. The Serving PDSN shall merge radio specific parameters contained in A11 and P-P interface messages called Airlink Records with IP network specific parameters to form one or more Usage Data Records (UDR). After merging, the Serving PDSN shall use RADIUS accounting messages to send UDR information to the Visited RADIUS Server. This is outlined as below in Figure 1 , and further detailed in the subsequent sections. The Serving PDSN shall maintain UDR information until it receives positive acknowledgment from the RADIUS server that the RADIUS server has correctly received the RADIUS message. Likewise, the RADIUS server shall maintain the UDR until the record is delivered to a Home RADIUS server, or removed by the operator billing system. The method by which information is moved from a RADIUS server to a billing system is beyond the scope of this document as is the summary, reconciliation, and billing process used by the operators.

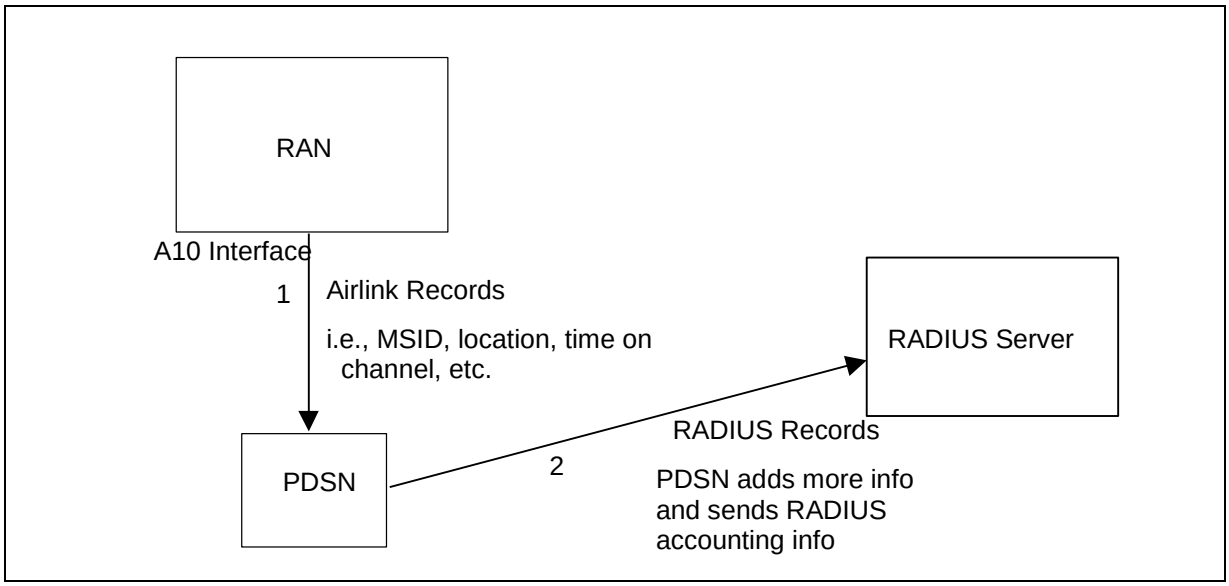


Figure 1 **Accounting Architecture**

3.1.2 Remote Address Accounting

The PDSN shall support remote address based accounting by counting the number of octets exchanged between the MS and a remote IP address during a packet data session. The PDSN shall allow for enabling of this accounting functionality on a per user (i.e., NAI) basis, as specified in the User Profile information received from the Home RADIUS server during authentication procedures.

The PDSN shall support the Remote IPv4/IPv6 Address attribute and Remote Address Table Index attributes as defined in Section 4. The Home RADIUS server may use multiple instances of the Remote IPv4/IPv6 Address and Remote Address Table Index attributes in the RADIUS Access-Accept message to authorize remote address accounting for the user for specific remote addresses. A Remote IPv4/IPv6 Address attribute shall contain an address mask/prefix-length, so that a given address and mask/prefix-length can indicate multiple addresses to be used for remote address accounting for the user[1]. The table indices specified by the Home RADIUS server index into tables of addresses stored at the PDSN. The method of provisioning the tables at the PDSN and the corresponding table indices at the Home RADIUS server is outside the scope of this document.

The PDSN shall support the Remote IPv4/IPv6 Address Octet Count attribute to count the number of octets sent/received to/from a given remote address or set of remote addresses. The attribute contains a counter for forward traffic, a counter for reverse traffic, and either the table index, remote IP address or a set of remote addresses with the same mask or prefix length (if present), as specified in section 4. The PDSN shall generate a single Remote IPv4/IPv6 Address Count attribute for all matching entries in a table when directed by the Remote Address Table Index attribute to "summarize." Otherwise, when not directed to summarize or for remote addresses or subnets identified explicitly via Remote IPv4/IPv6 Address attributes, the PDSN shall generate a Remote IPv4/IPv6 Address Octet Count attribute for each remote address or set of remote addresses as represented by a mask or prefix length used during a packet data session and authorized for the user by the RADIUS server. Hence, a UDR may contain multiple instances of the Remote IPv4/IPv6 Address Octet Count attribute. Therefore, the PDSN and the RADIUS server shall be capable of supporting multiple instances of the Remote IPv4/IPv6 Address Octet Count attribute in the RADIUS Accounting-Request (Stop) record and Interim-Update messages. A remote address mask or prefix-length shall be used to indicate a range of addresses for remote address accounting. The PDSN shall aggregate the octet counts for all the remote IP addresses of that mask or prefix and generate one Remote IPv4/IPv6 Address Octet Count attribute.

If the Remote Address Table Index is used for remote address based accounting, the current method is not easily scalable to multi-domain support, due to issues with table provisioning and synchronization between realms. In this case, the remote address functionality shall be limited to a single realm support from an access provider network point of view. All PDSNs in a single realm shall have the same set of tables. There is no explicit support in this document for coordinating table indices across realms. The Home RADIUS server shall be of the same realm as the PDSN or it shall have coordinated its indices with the realm that owns the PDSN.

It is the responsibility of the Visited RADIUS server to ensure the remote address table indices returned in a RADIUS Access-Accept message are consistent with the tables stored in the PDSN. For example, the Visited RADIUS server may filter out the Remote Address Table Index attributes contained in the RADIUS Access-Accept messages received from uncoordinated realms.

When a packet is received in the forward direction, the PDSN shall examine the source IPv4 address of the packet or the source prefix of the IPv6 address (as indicated by the prefix-

[1] An address mask of all ones means that all bits of the address shall be matched.

length Sub-Type). If the source IPv4 address matches a remote IPv4 address for the user or the source prefix of the IPv6 address matches a remote IPv6 prefix for the user, the PDSN shall create a Remote IPv4/IPv6 Address Octet Count attribute as part of the UDR if it does not exist and shall increment the octet counts.

When a packet is received in the reverse direction, the PDSN shall examine the destination IP address of the packet. If the destination IP address matches a remote address for the user, the PDSN shall create an instance of the Remote IPv4/IPv6 Address Octet Count attribute if it does not exist and shall increment octet counts.

Both IPv4 and IPv6 remote addresses are supported in remote address accounting. The structure of remote address tables and the method of communicating such information to the PDSN are outside the scope of this document.

3.1.3 Accounting and Fast Handoff

If a P-P session exists, the Target PDSN shall forward the airlink records received from the Target RAN to the Serving PDSN over the P-P interface. The Target PDSN shall not alter the airlink records. The Serving PDSN shall perform accounting functions for the data exchanged over the P-P connection per Section 3.5.1, treating the Target PDSN as if it were a PCF. Once the Serving PDSN combines these with IP network specific parameters, the UDR is sent to the RADIUS server as a RADIUS Accounting-Request record. This is outlined as below in Figure 2 , and detailed in the subsequent sections.

Upon fast handoff, the Target PDSN shall store a copy of the airlink records received at pre-setup of the A10 session for each A10 connection or for each IP flow. The Target PDSN shall update the copy of the Airlink Record received upon pre-setup of an A10 connection due to inter-PCF continuation of fast handoff on the Target PDSN (Figure 3, [Chapter 3]).

Also, the Serving PDSN copies some of the data from the current UDR or UDRs to the new UDR or UDRs while fast handoff is in progress. The PDSN accounting procedures ensure that no double counting of usage occurs.

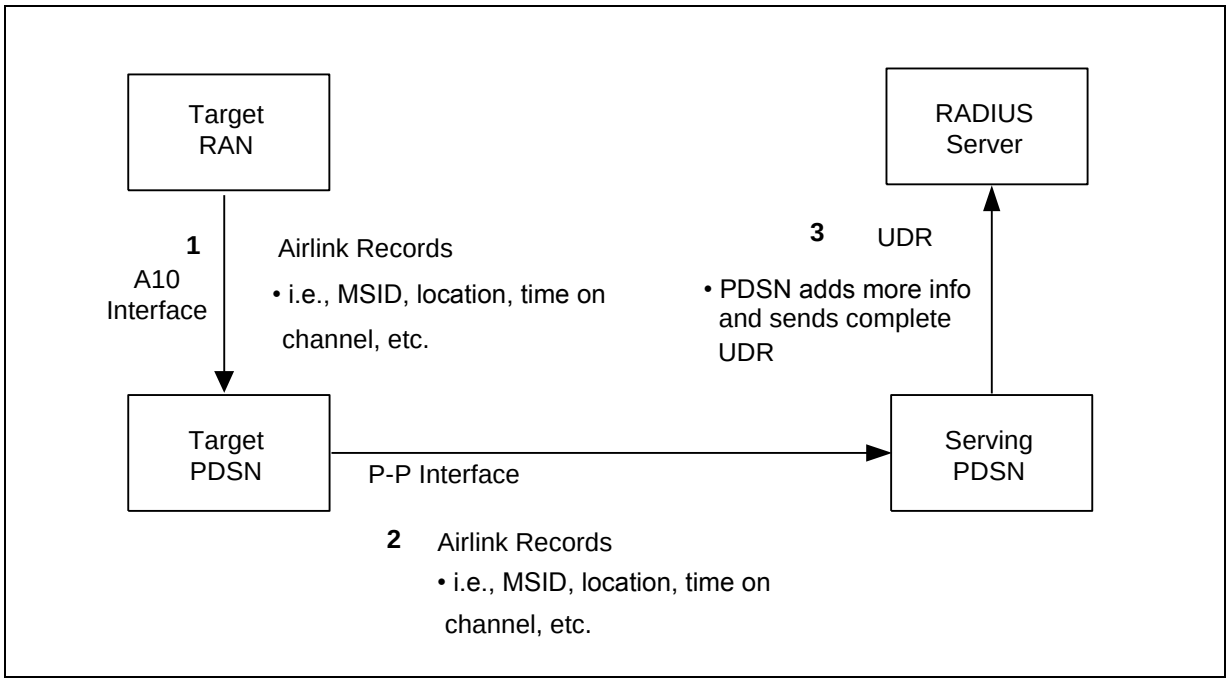


Figure 2 **Accounting Architecture with Fast Handoff**

3.1.4 Accounting Attribute Notation

A lower case letter implies an accounting attribute in an airlink record whereas a capital letter implies an accounting attribute in a UDR. Thus attributes in Table 1- Table 4 that apply to airlink records use lower case letters, and attributes in Table 5 and Table 6 that apply to UDRs use upper case letters.

3.2 Airlink Records

The RAN generates one of four types of airlink records over the A11 signaling:

- An A10 Connection Setup Airlink Record when the RAN establishes an A10 connection.
- An Active Start Airlink Record when the MS has connected the associated over-the air resources (HRPD over the air connection, 1X service connection) if FLOW_ID is not available or FLOW_ID is set to 0xff, or when the flow identified by a non 0xff FLOW_ID is opened (if FLOW_ID is available).
- An Active Stop Airlink Record when the MS has released the associated over-the-air resources if FLOW_ID is not available or FLOW_ID is set to 0xff, or when the flow identified by a non 0xff FLOW_ID is closed (if FLOW_ID is used).
- A Short Data Burst (SDB) Airlink Record when a forward or reverse short data burst is exchanged with the MS (cdma2000 1x only).

The A10 Connection ID is defined to be the PCF GRE Key for the A10 connection.

All the airlink records over an A10 connection shall include a sequence number initialized to zero at A10 connection setup. The sequence number is unique for a single identification tuple (A10 Connection ID, PCF ID, SR_ID, and MSID). Upon receiving the A10 connection setup airlink record, the Serving PDSN generates an UDR for the A10 connection (if it is the main service connection, or it is an auxiliary A10 connection and the Serving PDSN operates in connection-based accounting mode with the airlink record information and stores the sequence number. If the Serving PDSN operates in FLOW_ID-based accounting mode, it shall generate an UDR for a FLOW_ID upon receipt of the first Active Start Airlink Record over the A10 connection that includes the respective FLOW_ID information in the Granted QoS Parameters attribute. If the RN remaps an existing flow to a different A10, the PDSN shall use the current sequence number for the new A10 for processing airlink records for the flow.

The PCF shall increment the sequence number modulo 256 in the subsequent airlink record transmitted over the corresponding A10 connection. The Serving PDSN shall compare the received sequence number with the previously stored sequence number (N) for the A10 connection. If the received sequence number is in the range from (N+1) modulo 256 to (N+127) modulo 256, inclusive, the PDSN shall act accordingly based on the information contained in the airlink record, and shall update its stored sequence number for the A10 connection. If the received sequence number is in the range from (N-128) modulo 256 to N modulo 256, inclusive, the Serving PDSN shall ignore the respective airlink record. The same procedure continues for all the subsequent airlink records, until the closing of the A10 connection.

In the event of retransmission, the PCF shall retransmit with the same sequence number, and the Serving PDSN shall not update the UDR if the same sequence number corresponding to a single identification tuple is received.

When an A10 Connection Setup Airlink Record is received with a new A10 connection ID over an existing P-P connection, the serving PDSN shall start a new UDR for the new A10 connection as specified in section 3.5.1.

All Airlink attributes come from the RAN encoded as specified in this specification.

Additional information regarding airlink records can be found in [4].

3.2.1 A10 Connection Setup Airlink Record

Either a2 or a3, or both may be included. If neither a2 nor a3 is available in the RAN/AN when an Airlink Record is sent, or a2 or a3 have been sent in a previous airlink record and its value is unchanged, then a2/a3 may be absent from the current airlink record. It is possible that the Connection Setup Airlink Record omits a2/a3 because the pseudo-ESN/MEID may not be available in the AN at the time of A10 connection establishment. If the PDSN sends an Accounting-Start at the time of UDR creation and no value for a2/a3 has been received, the PDSN shall set A3 to NULL[2].

Table 1 contains fields present in the A10 Connection Setup airlink records.

Table 1 **A10 Connection Setup Airlink Fields**

Item	Parameter	Max Payload Length (Octets)	Format
y1	Airlink Record Type = 1 (Connection Setup)	4	integer
y2	A10 Connection ID	4	integer
y3	Airlink Sequence Number	4	integer
a1	MSID	15	string
a2	ESN	15	string
a3	MEID	14	string
d3	Serving PCF	4	ip-addr
d4	BSID	12	string
d7	Subnet[3]	37	string

Each A10 connection is indexed via the A10 Connection ID.

3.2.2 Active Start Airlink Record

Table 2 contains fields that should be present in Active Start airlink records.

[2] A NULL VSA is one where the value field is missing, i.e. has a length equal to 2.
[3] Either d4 and/or d7 shall be included.

Table 2 **Active Start Airlink Fields**

Item	Parameter	Max Payload Length (Octets)	Format
y1	Airlink Record Type = 2 (Active Start)	4	integer
y2	A10 Connection ID	4	integer
y3	Airlink Sequence Number	4	integer
a3	MEID[4]	14	string
d4	BSID (SID+NID+Cell Identifier)	12	string
d7	Subnet[5]	37	string
e1	User Zone	4	integer
f1	Forward FCH Mux Option[6]	4	integer
f2	Reverse FCH Mux Option	4	integer
f5	Service Option	4	integer
f6	Forward Traffic Type (Primary, Secondary)	4	integer
f7	Reverse Traffic Type (Primary, Secondary)	4	integer
f8	FCH Frame Size (0/5/20 ms)	4	integer
f9	Forward FCH RC	4	integer
f10	Reverse FCH RC	4	integer
f14	DCCH Frame Size (0/5/20ms)	4	integer
f16	Forward PDCH RC	4	integer
f17	Forward DCCH Mux Option	4	integer
f18	Reverse DCCH Mux Option	4	integer
f19	Forward DCCH RC	4	integer
f20	Reverse DCCH RC	4	integer
f22	Reverse PDCH RC	4	integer
i4	Airlink Priority	4	integer
i5	Granted QoS Parameters	Variable	string

If the e1, f1, f2, f5, f16, f17, f18, i4 and/or i5 parameters in Table 2 change during the active session, the RAN sends an Active Stop Airlink Record followed by an Active Start Airlink Record with the new parameters.

f1 to f10, f14, f16, f17 to f20 and f22 are fields from the cdma2000®[7] Service Configuration Record in [5-9].

[4] MEID (a3) may be omitted if it was previously sent. The PDSN should be prepared to receive the MEID value in zero, one or more Active Start airlink records received from the RAN for a given A10 connection and its associated flows.
[5] Either d4 and/or d7 shall be included.
[6] Forward/Reverse FCH Mux Option parameters correspond to the Forward/Reverse Mux Option parameters defined in the previous version of this document.
[7] cdma2000® is the trademark for the technical nomenclature for certain specifications and standards of the Organizational Partners (OPs) of 3GPP2. Geographically (and as of the date of publication),

Note: Active Start Airlink Record for FLOW_ID 0xff doesn't include Granted QoS Parameters i5.

3.2.3 Active Stop Airlink Record

Table 3 contains fields that should be present in Active Stop Airlink Records.

Table 3 **Active Stop Airlink Fields**

Item	Parameter	Max Payload Length (Octets)	Format
y1	Airlink Record Type = 3 (Active Stop)	4	integer
y2	A10 Connection ID	4	integer
y3	Airlink Sequence Number	4	integer
a3	MEID[8]	14	string
g8	Active Connection Time or Flow Activated Time in Seconds	4	integer
c6	FLOW_ID Parameter	2	string
f24	Flow Status	4	integer

3.2.4 SDB Airlink Record

Table 4 contains fields present in SDB Airlink Records.

Table 4 **SDB Airlink Fields**

Item	Parameter	Max Payload Length (Octets)	Format
y1	Airlink Record Type = 4 (SDB)	4	integer
y2	A10 Connection ID	4	integer
y3	Airlink Sequence Number	4	integer
y4	Mobile Originated/Mobile Terminated Indicator	4	integer
g10	SDB Octet Count	4	integer

3.3 PDSN Usage Data Record (UDR)

Table 5 contains the complete UDR and the description of each field.

---

[8] MEID (a3) may be omitted if it was previously sent. The PDSN should be prepared to receive the MEID value in zero, one or more Active Stop airlink records received from the RAN for a given A10 connection and its associated flows.

Table 5 **Complete UDR**

Item	Parameter	Description
A. Mobile Identifiers		
A1	MSID	MS ID (e.g., IMSI, MIN, IRM)
A2	ESN	Electronic Serial Number
A3	MEID	Mobile Equipment Identifier
B. User Identifiers		
B1	Source IP Address	IPv4 address of the MS.
B2	Network Access Identifier (NAI)	user@domain construct which identifies the user and home network of the MS.
B3	Framed-IPv6-Prefix	MS IPv6 prefix.
B4	IPv6 Interface ID	MS IPv6 interface identifier.
C. Session Identifiers		
C1	Account Session ID	The Account Session ID is a unique accounting ID created by the Serving PDSN that allows start and stop RADIUS records from a single A10 connection or P-P connection (if FLOW_ID Parameter is not used) or from a single FLOW_ID (if FLOW_ID Parameter is used) to be matched
C2	Correlation ID	The Correlation ID is a unique accounting ID created by the Serving PDSN for each packet data session that allows multiple accounting events for each associated A10 connection or P-P connection (if FLOW_ID Parameter is not used) or for each FLOW_ID (if FLOW_ID Parameter is used) to be correlated.
C3	Session Continue	This attribute when set to ‘true’ means it is not the end of a Session and an Accounting Stop is immediately followed by an Account Start Record. ‘False’ means end of a session.
C4	Beginning Session	The attribute when set to ‘true’ means new packet data session is established; ‘false’ means continuation of previous packet data session. This attribute is contained in a RADIUS Accounting-Request (Start) record.
C5	Service Reference ID	This is the service instance reference ID received from the RAN in an A11 Registration-Request message.
C6	FLOW_ID Parameter	This attribute identifies the IP flow.
D. Infrastructure Identifiers		
D1	Home Agent	The IPv4 address of the HA.
D2	PDSN Address	The IPv4 address of the PDSN
D3	Serving PCF	The IP address of the serving PCF, i.e., the PCF in the serving RAN.
D4	BSID	SID + NID + Cell Identifier type 2.
D5	IPv6 PDSN Address	The IPv6 address of the PDSN.
D6	Foreign Agent Address	The IPv4 address of the FA-CoA.
D7	Subnet	The subnet information for HRPD.
D8	Carrier-ID	A string that uniquely identifies the carrier that generated this UDR.
D9	IPv6 Home Agent	The IPv6 address of the HA.
E. Zone Identifiers		
E1	User Zone	Tiered Services user zone.

Item	Parameter	Description
E2	GMT- Time-Zone-Offset	A four octet string interpreted as a signed integer that indicates the offset in seconds from GMT time.
F. Session Status		
F1	Forward FCH Mux Option	Forward Fundamental Channel multiplex option.
F2	Reverse FCH Mux Option	Reverse Fundamental Channel multiplex option.
F5	Service Option	CDMA service option as received from the RAN.
F6	Forward Traffic Type	Forward direction traffic type – either Primary or Secondary.
F7	Reverse Traffic Type	Reverse direction traffic type – either Primary or Secondary.
F8	FCH Frame Size	Specifies the FCH Frame Size.
F9	Forward FCH RC	The format and structure of the radio channel in the forward Fundamental Channel. A set of forward transmission formats that are characterized by data rates, modulation characterized, and spreading rates [6].
F10	Reverse FCH RC	The format and structure of the radio channel in the reverse Fundamental Channel. A set of reverse transmission formats that are characterized by data rates, modulation characterized, and spreading rates [6].
F11	IP Technology	Identifies the IP technology to use for this call: Simple IP or MIP.
F12	Compulsory Tunnel Indicator	Indicator of invocation of compulsory tunnel established on behalf of MS for providing private network and/or ISP access during a single packet data connection.
F13	Release Indicator	Specifies reason for sending a stop record.
F14	DCCH Frame Size	Specifies Dedicated Control Channel (DCCH) frame size.
F15	Always On	Specifies the status of Always On service.
F16	Forward PDCH RC	The Radio Configuration of the Forward Packet Data Channel. (This parameter can be used as an indication that the MS is 1xEV DV capable.).
F17	Forward DCCH Mux Option	Forward Dedicated Control Channel multiplex option.
F18	Reverse DCCH Mux Option	Reverse Dedicated Control Channel multiplex option.
F19	Forward DCCH RC	The format and structure of the radio channel in the forward Dedicated Control Channel. A set of forward transmission formats that are characterized by data rates, modulation characteristics, and spreading rates [6].
F20	Reverse DCCH RC	The format and structure of the radio channel in the reverse Dedicated Control Channel. A set of reverse transmission formats that are characterized by data rates, modulation characteristics, and spreading rates [6].
F22	Reverse PDCH RC	The Radio Configuration of the Reverse Packet Data Channel. (This parameter can be used as an indication that the MS is capable of 1xEV DV enhanced reverse packet data rates.).
F23	Hot-Line Accounting Indication	Indicates if the user session is being Hot-Lined.
F24	Flow Status	Indicates the IP flow status.

Item	Parameter	Description
G. Session Activity		
G1	Data Octet Count (Terminating)	The total number of octets in IP packets sent to the user, as received at the PDSN from the IP network (i.e. prior to any compression and/or fragmentation).
G2	Data Octet Count (Originating)	The total number of octets in IP packets sent by the user.
G3	Bad PPP frame count	The total number of PPP frames from the MS dropped by the PDSN due to uncorrectable errors.
G4	Event Time	This is an event timestamp which indicates one of the following: The start of an accounting session if it is part of a RADIUS start message The end of an accounting session if it is part of a RADIUS stop message An Interim-Update accounting event if it is part of a RADIUS Interim-Update message.
G5	Remote IPv4 Address Octet Count	Contains the octet count associated with one or more remote IPv4 address; used for source/destination accounting.
G6	Remote IPv6 Address Octet Count	Contains the octet count associated with one or more remote IPv6 address; used for source/destination accounting.
G8	Active Time	The total active connection time on traffic channel in seconds. When FLOW_ID is not present, the attribute represents total active connection time on traffic channel in seconds; when FLOW_ID is present, the attribute represent the total active connection time on traffic channel in seconds for that flow.
G9	Number of Active Transitions	The total number of non-active to Active transitions by the user.
G10	SDB Octet Count (Terminating)	The total number of octets sent to the MS via Short Data Bursts.
G11	SDB Octet Count (Originating)	The total number of octets sent by the MS via Short Data Bursts.
G12	Number of SDBs (Terminating)	The total number of Short Data Burst transactions with the MS.
G13	Number of SDBs (Originating)	The total number of Short Data Burst transactions with the MS.
G14	Number of HDLC layer octets received	The count of all octets received in the reverse direction by the HDLC layer in the PDSN.
G15	Inbound MIP Signaling Octet Count	This is the total number of octets in registration requests and solicitations sent by the MS.
G16	Outbound MIP Signaling Octet Count	This is the total number of octets in registration replies and agent advertisements sent to the MS prior to any compression and/or fragmentation.
G17	Last User Activity Time	This is a Timestamp (in number of seconds from Jan 1 1970 UTC) of the last known activity of the user.
G20	Filtered Octet Count (Terminating)	The total number of octets in IP packets received by the PDSN from the IP Networks that were prevented from being sent to the user due to the filtering or redirection (IP Redirection or HTTP Redirection) action of the PDSN as instructed by Filter ID, IP Filter Rule, HTPP Redirection Rule, and IP Redirection Rule received from RADIUS in Access-Accept and COA packets.

Item	Parameter	Description
G21	Filtered Octet Count (Originating)	The total number of octets in IP packets that were received from the MS by the PDSN and were blocked from reaching the internet by the PDSN or redirected by the PDSN as instructed by Filter ID, IP Filter Rule, HTPP Redirection Rule, IP Redirection Rule received from RADIUS in Access-Accept and COA packets.
G22	3GPP2_RSVP_Signaling_Inbound_Count	RSVP signaling octets sent by the MS.
G23	3GPP2_RSVP_Signaling_Outbound_Count	RSVP signaling octets sent to the MS.
G24	3GPP2_RSVP_Signaling_In_Pkts	Number of RSVP signaling packets send by the MS.
G25	3GPP2_RSVP_Signaling_Out_Pkts	Number of RSVP signaling packets send to the MS.
I. Quality of Service		
I1	IP Quality of Service (QoS)	This attribute is deprecated.
I3	Airlink Priority	Identifies Airlink Priority associated with the user. This is the user's priority associated with the packet data service.
I5	Granted QoS Parameters	The granted QoS parameters for the IP flow.
Y. Airlink Record Specific Parameters[9]		
Y1	Airlink Record Type	3GPP2 Airlink Record Type, see [4]
Y2	A10 Connection ID	Identifier for the A10 Connection. This is the PCF GRE key that uniquely identifies an A10 connection between the PCF and the PDSN.
Y3	Airlink Sequence Number	Sequence number for Airlink records. Indicates the sequence of airlink records for an A10 connection.
Y4	Mobile Originated / Mobile Terminated Indicator	Used only in SDB airlink records. Indicates whether the SDB is Mobile Originated or Mobile Terminated.(0=Mobile Originated and 1=Mobile Terminated)
Z. Container		
Z1	Container	3GPP2 Accounting Container attribute. This attribute is used to embed 3GPP2 VSAs and/or RADIUS accounting attributes. This attribute is further described in section 3.5.

3.4 Accounting Formats

The RADIUS server shall support RADIUS attribute formats as defined in [RFC 2865] and [RFC 2866]. The RAN airlink records transmitted across the A10 interface and the P-P interface shall follow the RADIUS format encapsulated in a MIP vendor specific attribute (attribute type 38). Table 6 lists each accounting parameter and its associated RADIUS attribute.

Note: Attributes of type "26" defined in [RFC 2865] and [RFC 2866] are vendor specific, and are used to transport 3GPP2 specific parameters. Attribute value types 26/60 to 26/69 within the 3GPP2 vendor specific space are reserved. The default Vendor ID value in Vendor

[9] The Airlink Record Specific Parameters (Y1-Y4) are not included in the RADIUS Accounting records.

Specific attributes shall be 5535 defined in IANA in order for cdma2000 packet data service to support global roaming. 3GPP2 attribute formats not defined in section 3.5 are included in Table 6.

Table 6 **Accounting Parameter Attribute RADIUS Definitions**

		RADIUS Attribute Definitions				
Item	**Parameter**	**Type/ Vendor Type**	**Maximum Payload Length (in octets)**	**Format**	**Field**	**Special Values**
A.	**Mobile Identifieres**					
A1	MSID	31	15	string	Calling-Station-Id	See [4].
A2	ESN	26/52	15	string	3GPP2_ESN	ASCII string of ESN. See [4].
A3	MEID	26/116	14	string	3GPP2_MEID	ASCII string of MEID. See [4].
B.	**User Identifieres**					
B1	Source IP Address	8	4	ip-addr	Framed-IP-Address	See [RFC 2865].
B2	Network Access Identifier (NAI)	1	72	string	User-Name	See [RFC 2865].
B3	Framed-IPv6-Prefix	97	4-20	IPv6-prefix	Framed-IPv6-Prefix	See [RFC 3162].
B4	IPv6 Interface ID	96	10	string	Framed-Interface-ID	See [RFC 3162].
C.	**Session Identfiers**					
C1	Account Session ID	44	8	string	Acct-Session-Id	ASCII string of session ID
C2	Correlation ID	26/44	8	string	Correlation ID	ASCII string of Correlation ID
C3	Session Continue	26/48	4	integer	3GPP2_Session_cont	0=False, 1=True
C4	Beginning Session	26/51	4	integer	3GPP2_Begin_Session	0=False, 1=True
C5	Service Reference ID	26/94	variable	integer	3GPP2_SR_ID	See Section 3.5
C6	FLOW_ID Parameter	26/144	2	Integer	3GPP2_FLOW_ID parameter	See Section 3.5
D.	**Infrastracture Identifiers**					
D1	Home Agent	26/7	4	ip-addr	3GPP2_HA_IP_Addr	A HA IP address used during a MIP session by the user as defined in [RFC 2002].
D2	PDSN Address	4	4	ip-addr	NAS-IP-Address	IPv4 address of the RADIUS client in the PDSN.
D3	Serving PCF	26/9	4	ip-addr	3GPP2_PCF IP_Addr	The serving PCF is the PCF in the serving RAN.
D4	BSID	26/10	12	string	3GPP2_BSID	A number formed from the concatenation of SID (4 octets)+ NID (4 octets)+ Cell Identifier (type 2) (4 octets). In the Cell Identifier the 12 upper bits are the Cell Id and the lower 4 bits are the Sector. Each item is encoded using hexadecimal

						uppercase ASCII characters.
D5	IPv6 PDSN Address	95	16	Ipv6-addr	NAS-IPv6-Address	See [RFC 3162].
D6	Foreign Agent Address	26/79	4	ip-addr	3GPP2_FA_CoA	The IPv4 address of the FA-CoA.
D7	Subnet	26/108	37	string	3GPP2_Subnet	The subnet for HRPD system.
D8	Carrier-ID	26/142	4	string	3GPP2_Carrier-ID	A string that uniquely identifies the carrier that generated this UDR.
D9	IPv6 Home Agent	26/140	18	ipv6-addr	MIP6-Home Agent (Attribute B)	The IPv6 address of the Home Agent.

E. Zone Identifiers

E1	User Zone	26/11	4	integer	3GPP2_User_ID	Least significant 16 bits hold user zone ID (UZ_ID) next significant 15 bits hold user zone system ID (UZ_SID) and most significant bit always zero. UZ_ID and UZ_SID are defined in [10].
E2	GMT- Time-Zone-Offset	26/143	4	string	3GPP2_GMT_Offset	A signed integer that indicates the offset in seconds from GMT time.

F. Session Status

F1	Forward FCH Mux Option	26/12	4	integer	3GPP2_F_FCH_MUX	See [6]
F2	Reverse FCH Mux Option	26/13	4	integer	3GPP2_R_FCH_MUX	See [6]
F5	Service Option	26/16	4	integer	3GPP2_SO	See [6]
F6	Forward Traffic Type	26/17	4	integer	3GPP2_FTYPE	0=Primary, 1=Secondary
F7	Reverse Traffic Type (Primary, Secondary)	26/18	4	integer	3GPP2_RTYPE	0=Primary, 1=Secondary
F8	FCH Frame Size	26/19	4	integer	3GPP2_FFSIZE	0=no fundamental, 1=5ms and 20ms mixed frame, 2=20ms frame
F9	Forward FCH RC	26/20	4	integer	3GPP2_FRC	See [6]
F10	Reverse FCH RC	26/21	4	integer	3GPP2_RRC	See [6]
F11	IP Technology	26/22	4	integer	3GPP2_IP_Tech	1=Simple IP, 2=MIP
F12	Compulsory Tunnel Indicator	26/23	4	integer	3GPP2_Comp_Flag	0=no tunnel 1=non-secure tunnel 2=secure tunnel
F13	Release Indicator	26/24	4	integer	3GPP2_Reason_Ind	Reasons for stop record: 0=unknown

						1=PPP/Service timeout 2=Handoff 3=PPP termination 4=MIP registration failure 5= Abnormal Terminations 6=Termination due to Resource management 7=Service connection released 8=VolumeQuota reached, Service connection released (use for PrePaid packet data service) 9=DurationQuota reached, Service connection released (use for PrePaid packet data service) 10=Incompatible PrePaid accounting information (use for PrePaid packet data service) 11=Airlink Parameter Change (e1,f1,f2,i4 etc) 12=Time of Day Timer expiration 13 = Dormant by Accounting-Stop-triggered-by-Active-Stop 14 = Hot-Line Status Changed 15 = Flow is deactivated
F14	DCCH Frame Size (0/5/20ms)	26/50	4	integer	3GPP2_DFSIZE	0=no DCCH, 1=5ms and 20ms mixed frame, 2=20ms frame, 3=5ms frame
F15	Always On	26/78	4	integer	3GPP2_Always_ON	Always On 0=no 1=yes
F16	Forward PDCH RC	26/83	4	integer	3GPP2_F_PDCH_RC	See [6]
F17	Forward DCCH Mux Option	26/84	4	integer	3GPP2_F_DCCH_MUX	See [6]
F18	Reverse DCCH Mux Option	26/85	4	integer	3GPP2_R_DCCH_MUX	See [6]
F19	Forward DCCH RC	26/86	4	integer	3GPP2_FDRC	See [6]
F20	Reverse DCCH RC	26/87	4	integer	3GPP2_RDRC	See [6]
F22	Reverse PDCH RC	26/114	4	integer	3GPP2_R_PDCH_RC	See [6]
F23	Hot-Line Accounting Indication	26/122	4	integer	3GPP2_Hot-Line	0= no Hot-Line 1= Hot-Line

F24	Flow Status	26/145	4	integer	3GPP2_Flow_status	0 = active 1 = inactive

G. Session Activity

G1	Data Octet Count (Terminating)	43	4	integer	Acct-Output-Octets	See [RFC 2865].
G2	Data Octet Count (Originating)	42	4	integer	Acct-Input-Octets	See [RFC 2865].
G3	Bad PPP frame count	26/25	4	integer	3GPP2_Bad_Frame_Count	
G4	Event Time	55	4	time	Event-Timestamp	See [RFC 2869].
G5	Remote IPv4 Address Octet Count	26/72	variable	octet string		See Section 3.5
G6	Remote IPv6 Address Octet Count	26/97	variable	octet string		See Section 3.5
G8	Active Time	26/49	4	integer	3GPP2_Active_Time	This is the active time reported by the RAN in the Active Stop Airlink Record, see [4].
G9	Number of Active Transitions	26/30	4	integer	3GPP2_Num_Active	
G10	SDB Octet Count (Terminating)	26/31	4	integer	3GPP2_SDB_Input_Octets	This is the SDB octet count reported by the RAN in the SDB Airlink Record, see [4].
G11	SDB Octet Count (Originating)	26/32	4	integer	3GPP2_SDB_Output_Octets	This is the SDB octet count reported by the RAN in the SDB Airlink Record, see [4].
G12	Number of SDBs (Terminating)	26/33	4	integer	3GPP2_NumSDB_Input	
G13	Number of SDBs (Originating)	26/34	4	integer	3GPP2_NumSDB_Output	
G14	Number of HDLC layer octets received	26/43	4	integer	3GPP2_Num_Bytes_Received_Total	The count of all octets received in the reverse direction by the HDLC layer in the PDSN.
G15	Inbound MIP Signaling Octet Count	26/46	4	integer	3GPP2_Mobile_IP_Signaling_Inbound_Count	This is the total number of octets in registration requests and solicitations sent by the MS.
G16	Outbound MIP Signaling Octet Count	26/47	4	integer	3GPP2_Mobile_IP_Signaling_Outbound_Count	This is the total number of octets in registration replies and agent advertisements, sent to the MS.
G17	Last User Activity Time	26/80	4	integer	3GPP2_Last User Activity Time	Timestamp (in number of seconds from Jan 1 1970 UTC) of the last known activity of the user.
G20	Filtered Octet Count (Terminating)	26/146	4	integer	3GPP2_Filtered_Count_Input	The total number of octets in IP packets received by the PDSN from the IP Networks that were prevented from being sent to the user due to the filtering or redirection (IP Redirection or HTTP Redirection) action of the PDSN as instructed by Filter ID, IP Filter Rule, HTPP Redirection Rule, and IP Redirection

						Rule received from RADIUS in Access-Accept and COA packets
G21	Filtered Octet Count (Originating)	26/147	4	integer	3GPP2_Filtered_Count_Output	The total number of octets in IP packets that were received from the MS by the PDSN and were blocked from reaching the internet by the PDSN or redirected by the PDSN as instructed by Filter ID, IP Filter Rule, HTPP Redirection Rule, IP Redirection Rule received from RADIUS in Access-Accept and COA packets.
G22	3GPP2_RSVP_Signaling_Inbound_Count	26/162	4	integer	3GPP2_ RSVP_Signaling_Inbound_Count	RSVP signaling octets sent by the MS
G23	3GPP2_RSVP_Signaling_Outbound_Count	26/163	4	integer	3GPP2_RSVP_Signalling_Outbound_Count	RSVP signaling octets sent to the MS
G24	3GPP2_RSVP_Signaling_In_Pkts	26/164	4	integer	3GPP2_RSVP_Signaling_In_Pkts	Number of RSVP signaling packets sent by the MS
G25	3GPP2_RSVP_Signaling_Out_Pkts	26/165	4	integer	3GPP2_RSVP_Signaling_Out_Pkts	Number of RSVP signaling packets sent to the MS

I. Quality of Service

I1	IP Quality of Service	26/36	4	integer	3GPP2_IP_QOS	This attribute is deprecated.
I4	Airlink Priority	26/39	4	integer	3GPP2_Air_Priority	Least significant 4 bits hold the priority associated with the packet data service.
I5	Granted QoS Parameters	26/132	Variable	integer	3GPP2_Granted_QoS	The granted QoS for the IP flow.

Z. Container

Z1	Container	26/6	Variable	string	3GPP2_Container	See section 3.5.

3.5 PDSN Procedures

If A10 connection is the main A10 (such as SO33 or SO59) or if the auxiliary A10 connection does not include FLOW_ID (such as SO60/SO61), the PDSN shall create a UDR for each A10 connection; otherwise (such as SO64, SO66), the PDSN shall perform one of the following based on local policy or Accounting-Mode[19] if received from the access authentication phase:

- If the Accounting-Mode attribute is set to '1' (Per Reservation/IP-session Accounting Mode), the PDSN shall create a UDR for each FLOW_ID Parameter (include FLOW_ID and direction); or
- If the Accounting-Mode attribute is set to ''2' (Per IP Session Accounting Mode), the PDSN shall create a UDR for each auxiliary A10 and use the aggregated counter for all IP flows that are mapped into this A10. The PDSN shall include multiple I5 attributes in the UDR. In this case, the PDSN shall not copy the previous UDR(s) to new UDR(s) and shall not use the Container specified in this document since the mapping between IP flows and A10 connection can be potentially changed due to radio resource changes or inter PCF handoffs.

The following events cause the PDSN to take accounting action. Details are given in subsequent sections.

- Reception of A10 Connection Setup Airlink Record over A10 or P-P interface.
- A10 or P-P connection termination at the PDSN.
- Data service establishment or PPP renegotiation on the PDSN. This includes a PPP session and packet service session (Simple IP or MIP).
- Data service termination on the PDSN. This includes releasing the PPP session, or release of a packet service session (Simple IP or MIP).
- Arrival of forward direction or reverse direction user data.
- Reception of Active Start Airlink Record.
- Reception of Active Stop Airlink Record.
- Reception of SDB Airlink Record.
- Interim-Update record trigger.
- Stop record trigger.
- Time of day timer expiry.
- Hot-Lining.
- IP Flow is activated or deactivated.
- The granted QoS is updated for an activated IP flow.

Each packet data session (i.e., Simple IP and/or MIP4 session) is identified with a Correlation ID provided to the HAAA at the time authentication/authorization is performed. Individual Simple IPv4, MIP4, Simple IPv6 and MIP6 session shall be accounted for independently. All UDR information is stored and transmitted per tuple of {assigned IPv4 address or IPv6 prefix, NAI, A10 connection ID, SR_ID or FLOW_ID Parameter}. However, simultaneous Simple

IPv4 and Simple IPv6 shall use a common Correlation ID because they use a common authentication/authorization procedure. During the lifetime of the Simple IP and/or MIP session, UDRs are created, modified, maintained, copied, and released for each individual A10 connection (if FLOW_ID Parameter is not used) or for each IP flow (if FLOW_ID Parameter is used). The Serving PDSN shall create one UDR per A10 connection ID (if FLOW_ID Parameter is not used) or per FLOW_ID Parameter (if FLOW_ID Parameter is used). An A10 connection may be directly connected to the serving PDSN or indirectly connected via a P-P connection.

The PDSN closes the corresponding UDR(s) when any of the following events occur:

- An existing A10 or P-P connection is closed.
- An IP flow is removed from the corresponding A10.
- The PDSN determines the packet data session associated with the Correlation ID has ended.

At an initial A10 connection establishment (if FLOW_ID Parameter is not used) or a flow is mapped to an A10 connection (if FLOW_ID Parameter is used), a UDR is created and initialized from relevant airlink records. When there is a new A10 or P-P connection or a new mapping between an IP flow to A10 connection due to a handoff for an existing packet data session, or when a new packet data session for an existing A10 or P-P connection or for an existing IP flow identified by FLOW_ID Parameter is created, a UDR is created by copying data from a previous UDR. For example, during a fast handoff, the PDSN copies packet data session information (e.g., IP address and NAI) from the previous UDR associated with the source RAN to the new UDR associated with the new RAN. Similarly, if the MS sends an LCP Configure-Request message over the main service instance to restart the PPP session, the PDSN copies A10 or P-P connection data (e.g., F1-F20) or IP flow QoS data (e.g., i5) from all current UDRs of the entire packet data session to new UDRs for the new packet data session. The Serving PDSN closes the previous UDRs and sends accounting records to the RADIUS server.

Furthermore, during a fast handoff, either two A10 connections, or an A10 and P-P connection, or two P-P connections with the same FLOW_ID Parameter (if used) or SR_ID (if FLOW_ID Parameter is not used) and MSID may exist momentarily due to the PDSN bicasting[10]. Since the MS can connect to only one RAN for a given service instance, the PDSN accounting procedures ensure that double counting between the current and new (copy) never occurs despite the PDSN bicasting of data to both service instances.

RADIUS accounting messages are generated from the information in the UDR. The Correlation ID is used to match different accounting records (Account Session IDs) across all A10 connections or P-P connections, or across all FLOW_ID Parameters for a single packet data session. One Correlation ID for all A10 and P-P connections or all FLOW_ID Parameters is maintained for a packet data session for each NAI and IP pair within the same Serving PDSN. The Account Session ID[11] is used to match a single RADIUS Start and Stop pair. A different Account Session ID is used for each A10 connection, P-P connection, and/or FLOW_ID Parameter. A new A10 connection due to intra-PDSN handoff between PCFs shall result in a new A10 Connection ID and Account Session ID. A new P-P connection due to fast handoff between the PDSNs shall result in a new A10 Connection ID and Account Session ID. An intra-PDSN handoff at the Target PDSN, while in fast handoff (Figure 3, [Chapter 3]), shall result in a new A10 connection ID and Account Session ID at the Serving

[10] Bicasting occurs when the A11-Registration Request or P-P-Registration Request has the ‘S’ bit set to 1.
[11] The use of the Account session ID as described in this section does not apply to the container accounting procedures.

PDSN. The MSID and FLOW_ID Parameter (if used) SR_ID (if FLOW_ID Parameter is not used) are used to select the proper UDR after an intra-PDSN handoff. One A10 Connection ID may be associated with multiple simultaneous NAI, IP pairs in the Serving PDSN (i.e., multiple packet data sessions).

An Airlink record is associated with an FLOW_ID Parameter (if used) or an A10 connection ID (if FLOW_ID Parameter is not used). The Serving PDSN matches FLOW_ID Parameter (if used) or the A10 Connection ID (if FLOW_ID Parameter is not used) in the airlink record to the FLOW_ID Parameter (if used) or A10 Connection ID (if FLOW_ID Parameter is not used) in the appropriate UDR(s). If more than one UDR matches, the actions are applied to all UDRs.

Some events cause certain UDR fields to change in the middle of a session. These events are typically associated with Active Stop and Active Start Airlink Records sent from the RAN. The relevant Airlink Record field changes are listed in 3.2.2. When this happens, one of two approaches shall be taken:

(1) a container attribute as specified in Section 4.6 is created and the changed fields are embedded in that container attribute. This allows the UDR to continue to accumulate accounting information after an event without transmitting a RADIUS Accounting message.

(2) the PDSN may send a RADIUS Accounting Stop record to capture accounting data before the event, followed by a RADIUS Accounting Start record with the new field values. In fact, a PDSN may send a RADIUS Stop and RADIUS Start anytime during a single session as long as no accounting data is lost. In these cases, the PDSN shall send the same Correlation ID in both the RADIUS Start and RADIUS Stop records.

The subsequent sections specify the actions to take for each event.

3.5.1 A10 Connection Setup Airlink Record Arrives

If the Serving PDSN initially receives an A10 Connection Setup Airlink Record with a new A10 connection ID (if FLOW_ID Parameter is not used) or receives one or more new FLOW_ID Parameter(s) to be mapped in an A10 connection (if FLOW_ID Parameter is used), the serving PDSN shall generate new UDR for each A10 (if FLOW_ID Parameter is not used) or for each IP flow (if FLOW_ID Parameter is used) using information received from A10 Connection Setup Airlink Record to fill the following fields of the new UDR:

- A1, A2, A3, D3, and D4/D7. Note that A2 and or A3 (MEID) may not be present in the Connection Setup airlink record. If the PDSN sends an Accounting Start when no value for a2 or a3 has been received from the AN, the PDSN shall set A2 and or A3 to NULL.

- Zero fields G1-G17 and G20-G25

The Serving PDSN shall populate the remaining fields of the UDR as specified in sections 3.5.2 and 3.5.5.

If the Serving PDSN receives an A10 Connection Setup Airlink Record with a new A10 connection ID over an A10 or P-P connection (if FLOW_ID Parameter is not used) or receives an existing FLOW_ID Parameter to be mapped in a new A10 connection (if FLOW_ID Parameter is used) as a result of an Intra PDSN handoff or Inter PDSN fast

handoff, then the serving PDSN shall use the MSID and FLOW_ID Parameter (if is used) or SR_ID (if FLOW_ID Parameter is not used) to find the correct UDR, and, either:

- Create a new Container attribute in the UDR with Container-Reason ← Handoff, Event-timestamp ← current time and attributes D2 (in case of an IPv6 PDSN, D5), D3, D4/D7, G1, G2, G3, and G8-17, G20-G25, and all instances of G5/G6.
- Use information received from the RAN to fill in the following fields: D3 and D4/D7. The PDSN fills in D2 (in case of an IPv6 PDSN, D5).
- Zero fields G1, G2, G3, G8-17 and G20-25; all instances of G5/G6 in the newly created accounting container are eliminated.
- Mark the UDR as pending[12] if the "S" bit in the A11 Registration-Request message or P-P Registration-Request message that carries the A10 Connection Setup Airlink Record is set to '1'.
- When the Active Stop Airlink Record for the previous A10 or P-P connection arrives, update the accounting fields inside the newly created accounting container. (See section 3.5.6 for further processing of the Airlink Stop Record).

Or,

- Create a copy of the current UDR.
- Use information received from the RAN to fill the following fields in the copy UDR: D3, D4 and D7. The PDSN fills in D2 (in case of an IPv6 PDSN, D5).
- Zero fields G1, G2, G3, and G8-17 and G20-25 in the copy UDR; all instances of G5/G6 in the copy UDR are eliminated.
- Send a RADIUS Accounting-Request (Start) record containing a new Account Session ID and the same Correlation ID if the corresponding UDR is the URD for the main A10 connection.
- Mark the new UDR as pending if the "S" bit in the A11 Registration-Request message or P-P Registration-Request message that carries the A10 Connection Setup Airlink Record is set to '1'.
- When the Active Stop Airlink Record for the previous A10 or P-P connection, or flows arrives, update the current UDR and send a RADIUS Accounting-Request (Stop) record based on the current UDR. The RADIUS Accounting-Request (Stop) record contains a Session Continue attribute with the value set to 1 (True), the same Correlation ID, and the original session ID. (See section 3.5.6 for further processing of the Airlink Stop Record).

3.5.2 Packet Data Session Establishment

After the PDSN establishes a packet data session (i.e., Simple IP or MIP) on the main service connection, the Serving PDSN shall:

- Fill the following fields: B1, (in case of IPv6 MS, B3), B2, C1, C2, C4, D1(in case of IPv6 HA, D9), D2 (in case of IPv6 PDSN, D5), F11, F12, and I5.

[12] A "pending" UDR is one for which usage data is not accumulated because another UDR is accumulating usage data, e.g., because of bicasting.

- Send a RADIUS Accounting-Request (Start) record based on the current UDR.

3.5.3 Packet Data Session Termination

After the Serving PDSN terminates a packet data session to the MS for every UDR that the PDSN has not sent Accounting-Request (Stop) to the HAAA, the Serving PDSN shall:

- Add a Session Continue attribute in the UDR with the value set to 0 (False).
- Send a RADIUS Accounting-Request (Stop) record based on the current UDR.
- Delete the UDR after receiving acknowledgment from the RADIUS server that it has successfully received the UDR.

If an A11 Registration-Request message is received with lifetime 0 for the main service connection and the Accounting-Stop- triggered-by-Active-Stop-Indication is set to 1 for the user, the PDSN shall perform the following:

- If the PDSN hasn't received any SDB Airlink Record (see section 3.5.7) since the last RADIUS Accounting-Request (Stop) is sent for the corresponding UDR, the PDSN shall not[13] trigger a RADIUS Accounting-Request (stop) record merely based on this indication.
- Otherwise, the PDSN shall send RADIUS Accounting-Request (Start) with Session Continue attribute set to 0 (False) immediately followed by RADIUS Accounting-Request (Stop). The PDSN shall delete the UDR after receiving acknowledgment from the RADIUS server that it has successfully received the UDR.

If the reason for the packet data session termination is due to the MS sending an LCP Configure-Request message, and if the MS is not in a fast handoff state, then for every UDR, the Serving PDSN shall:

- Create a copy of the current UDR using A1, A2, A3, D3, D4/D7, F1-F20, F22-F23, I4 and I5 from the current UDR in the new UDR.
- Zero fields G1, G2, G3, and G8-13 and G20-25 in the new UDR.
- Add a Session Continue attribute in the current UDR with the value set to 0 (False).
- Send a RADIUS Accounting-Request (Stop) record for every UDR that the PDSN has not sent Accounting-Request (Stop) to the HAAA based on the current UDR.
- Delete the current UDR after receiving acknowledgment from the RADIUS server that it has successfully received the UDR.
- Follow Packet Data Session Establishment accounting procedures for each new UDR immediately after packet data session establishment.

[13] To prevent from sending two consecutive RADIUS Accounting-Request (stop) records at packet data session termination.

3.5.4 User Data Through PDSN

For any user data processed by the Serving PDSN in the forward direction, the Serving PDSN shall use the MS IP address and FLOW_ID Parameter (if used) or SR_ID (if FLOW_ID Parameter is not used) to find the correct UDR. If the UDR is not pending and

1. a) the PDSN supports A10 flow control and the A10 connection to which the user data being mapped has the GRE flow control turned off , or

2. b) the PDSN does not support A10 flow control,

then the PDSN shall:

- Increment G1 before compression by the number of octets in IP packets[14] sent to the user.
- Increment G22, if the data is RSVP control message, with the byte count before compression. Increment G24 by 1.
- Increment G16 before compression by the number of octets in MIP signaling packets[15] sent to the user.
- Increment G20 if the packet is being blocked or redirected away from the MS by an Filtering, Redirection rules or Filter-Ids received in the RADIUS packets (access-Accept or COA packets).
- If the source IP address of the user packet is one of the remote addresses authorized for the user for destination based accounting, a G5/G6 instance is created in the UDR for this address (if one does not exist already and no applicable summarized instance exists already), and the Forward Octet Count field in this G5/G6 instance is incremented before compression as necessary.

For any user data processed by the Serving PDSN in the reverse direction, the Serving PDSN shall use the MS IP address and FLOW_ID Parameter (if used) or SR_ID (if FLOW_ID Parameter is not used) to find the correct UDR. If the UDR is not pending then the PDSN shall:

- Increment G2 after decompression by the number of octets in IP packets[16] sent by the user.
- Increment G23, if the data is RSVP control message, with the byte count after decompression from the mobile. Increment G25 by 1.
- Increment G14 by the number of octets received at the HDLC layer.
- Increment G21 if the packet is being blocked or redirected by any filtering, redirection rule or filter ids received in the RADIUS packets (access-Accept or COA packets).
- Increment G15 after decompression by the number of octets in MIP signaling packets sent by the user.

[14] This includes MIP signaling octets.
[15] This means IP, UDP, and the MIP message payload above UDP.
[16] This includes MIP signaling octets.

- If the destination IP address of the user packet is one of the remote addresses authorized for the user for destination based accounting, a G5/G6 is created in the UDR for this address (if one does not exist already and no applicable summarized instance exists already), and the Reverse Octet Count field in this G5/G6 instance is incremented after decompression as necessary.

If the UDR is pending or the PDSN supports A10 flow control and the A10 connection to which the user data being mapped has GRE flow control turned on, then the PDSN shall not modify the accounting usage data of the corresponding UDR(s).

3.5.5 Active Start Airlink Record Arrives

When the Serving PDSN receives an Active Start Airlink record from the RAN or Target PDSN, the Serving PDSN performs the following.

If the UDR is new (some fields are blank) and UDR is associated with the main A10 connection, the Serving PDSN shall:

- Set UDR fields according to the Active Start record: D4 ← d4, E1 ← e1, F1-F10 ← f1-f10, F14 ← f14, F16 ← f16, F17-F20 ← f17-f20, F22 ← f22, I4 ← i4 and I5 ← i5.
- Set A2/A3 using the ESN/MEID received previously, if available. Otherwise if a2/a3(MEID) is present in the Active Start Airlink Record, then A2←a2/A3 ← a3. Otherwise set A2/A3 to NULL.
- If the UDR is pending, mark it as not pending.

Else, if the the Active Start record indicates parameters E1, F1, F2, F5, F16, F17, F18, I4 or I5 have changed (the PDSN receives Active Stop Airlink Record previously, see section 3.5.6), and not as a result of a handoff, the Serving PDSN shall either:

- Create a new Container attribute in the UDR with Container-Reason ← Parameter change, Event-timestamp ← current time and attributes D4/D7, E1, F1, F2, F16, F17, F18, G1, G2, G3, G8-G17, G20-25, I4, I5 and all instances of G5/G6.
- Set UDR fields according to the airlink record. D4 ← d4, E1 ← e1, F1 ← f1, F2 ← f2, F5 ← f5, F16 ← f16, F17 ← f17, F18 ← f18, I4 ← i4, I5 ← i5 and zero fields G1, G2, G3, and G8-17 and G20-21. All current instances of G5/G6 in the UDR are eliminated.
- Set A3 using the MEID received previously, if available. Otherwise if a3 (MEID) is present in the Active Start Airlink record , then A3 ← a3.

Or:

- Set UDR fields according to airlink record. D4 ← d4, E1 ← e1, F1 ← f1, F2 ← f2, F5 ← f5, F16 ← f16, F17 ← f17, F18 ← f18, I4 ← i4, I5 ← i5 and zero fields G1, G2, G3, G8-17 and G20-25. All current instances of G5/G6 in the UDR are eliminated.
- Set A3 using the MEID received previously, if available. Otherwise if a3 (MEID) is present in the Active Start Airlink record , then A3 ← a3.

- Send a RADIUS Accounting-Request (Start) record based on UDR containing a new Account Session ID and same Correlation ID.

Else, if the UDR is new (some fields are blank) and UDR is associated with an auxiliary A10 (if FLOW_ID Parameter is not used) or IP flow ((if FLOW_ID Parameter is used), the Serving PDSN shall:

- Set UDR fields according to airlink record: D4 ← d4, E1 ← e1, F1-F10 ← f1-f10, F14←f14, F16 ← f16, F17-F20 ← f17-f20, F22 ← f22, I4 ← i4 and I5 ← i5.
- Send a RADIUS Accounting-Request (Start) record based on UDR containing a new Account Session ID and same Correlation ID.
- Set A3 using the MEID received previously, if available. Otherwise if a3 (MEID) is present in the Active Start Airlink, A3 ← a3. Otherwise set A3 to NULL.

Else, if the UDR does not exist for IP flow identified by FLOW_ID Parameter, the Serving PDSN shall:

- Generate UDR and use information received from Active Start Airlink Record to fill D3, and D4/D7; and zero fields G1-G17 and G20-25. Any information other than a3 that is not available in the active start should be taken from the associated A10 connection setup Airlink Record.
- Set A3 using the MEID received previously, if available or if a3 (MEID) is present in the Active Start Airlink record , then A3<-a3. Otherwise set A3 to NULL.
- Set UDR fields according to airlink record: D4 ← d4, E1 ← e1, F1-F10 ← f1-f10, F14 ← f14, F16 ← f16, F17-F20 ← f17-f20, F22 ← f22, I4 ← i4 and I5 ← i5.
- Send a RADIUS Accounting-Request (Start) record based on UDR containing a new Account Session ID and same Correlation ID.

Else,

- If the Accounting-Stop- triggered-by-Active-Stop-Indication is set for the user, the PDSN shall send a RADIUS Accounting-Request (Start) message to the HAAA with a new Account Session ID is sent for main service instance based on the current UDR if the PDSN has not sent Accounting-Request (Start) to the HAAA. The PDSN shall increment G9 by one.

3.5.6 Active Stop Airlink Record Arrives

When the Serving PDSN receives an Active Stop Airlink record from the RAN, the PDSN shall:

- Increment G8 by the value of g8.
- Set G17 [17] with the current time if Active Stop is used to indicate last activity.

[17] If Active Stop alone is used to set G17, it may not reflect the most recent activity of the user by the time the Accounting record is sent to the Home RADIUS server. If Active Stop is not used to set the G17, the PDSN may use implementation specific methods to populate G17.

- If a3 (MEID) is present in the Active Stop Airlink record and A3 is currently NULL, then.

If the Serving PDSN receives an A11 Registration-Request for the main A10 connection containing a non-zero lifetime and an Active Stop Airlink record, and if the Accounting-Stop-triggered-by-Active-Stop-Indication is set to 1 for the user, the PDSN shall:

- If a3 (MEID) is present in the Active Stop Airlink record and A3 is currently NULL, then A3 ← a3.
- send a RADIUS Accounting-Request (Stop) record based on the current UDR including a Session Continue attribute with the value set to 1 (True) . The PDSN shall zero fields G1, G2, G3, G8-16, G20-25 and all current instances of G5/G6, D4/D7, E1, F1-F10, F14, I4 and I5 in the UDR are eliminated.

If the Serving PDSN receives Active Stop Airlink Record for the IP flow that was in active and now becomes inactive, the PDSN shall:

- If a3 (MEID) is present in the Active Stop Airlink record and A3 is currently NULL, then A3 ← a3.
- send a RADIUS Accounting-Request (Stop) record based on the current UDR including a Session Continue attribute with the value set to 1 (True). The PDSN shall zero fields G1, G2, G3, G8-16, G20-25 and all current instances of G5/G6, D4/D7, E1, F1-F10, F14, I4 and I5 in the UDR are eliminated.

If the Serving PDSN receives Active Stop Airlink Record for the auxiliary A10 connection on which the over the air service instance was in connection and now is disconnected, the PDSN shall:

- If a3 (MEID) is present in the Active Stop Airlink record and A3 is currently NULL, then A3 ← a3.
- send a RADIUS Accounting-Request (Stop) record based on the current UDR including a Session Continue attribute with the value set to 1 (True). The PDSN shall zero fields G1, G2, G3, G8-16, G20-25 and all current instances of G5/G6, D4/D7, E1, F1-F10, F14, I4 and I5 in the UDR are eliminated.

If the Serving PDSN receives Active Stop Airlink Record because any parameters E1, F1, F2, F5, F16, F17, F18, I4 or I5 have changed, and not as a result of a handoff, the Serving PDSN shall:

- If a3 (MEID) is present in the Active Stop Airlink record and A3 is currently NULL, then A3 ← a3.
- send a RADIUS Accounting-Request (Stop) record based on the current UDR including a Session Continue attribute with the value set to 1 (True). The PDSN shall then send a RADIUS Accounting-Request (Start) record based on UDR containing a new Account Session ID and same Correlation ID (see section 3.5.5).

3.5.7 SDB Airlink Record Arrives

This section only applies per A10 based accounting for cdma2000 1x. If doing flow based accounting, upon receiving an SDB Airlink Record, the PDSN shall ignore it. Note, the octets sent over SDB have already been accounted for in G1/G2.

When the Serving PDSN receives an SDB airlink record from the RAN or the Target PDSN, the Serving PDSN shall use the MS IP address and SR_ID to find the correct UDR or UDRs in the event of multiple packet data sessions.

If the mobile originated / mobile terminated indicator is equal to one (mobile terminated SDB), the Serving PDSN shall:

- Increment G10 by the value of g10.
- Increment G12 by one.

If the mobile originated / mobile terminated indicator is equal to zero (mobile originated SDB), the Serving PDSN shall use the MS IP address and SR_ID to find the correct UDR. The PDSN shall:

- Increment G11 by the value of g10.
- Increment G13 by one.

3.5.8 Interim-Update Record Trigger

When the Interim-Update Record Trigger initiates, the Serving PDSN shall send a RADIUS Accounting-Request Interim-Update record based on the current UDR. The Interim-Update Record Trigger is an operator configurable time interval since the last RADIUS accounting record was sent for a UDR. The Interim-Update Record Trigger may not be applied to dormant sessions as per the local PDSN policy.

3.5.9 Stop Record Trigger

Additional conditions may trigger a RADIUS Accounting-Request (Stop) record to be sent by the PDSN such as:

- When the size of the RADIUS accounting record to be sent for the UDR exceeds an operator configurable threshold.
- Any time during a session as an implementation dictates.

When the Stop Record Trigger initiates, the PDSN shall add a Session Continue attribute in the UDR with the value set to 1 (True). The PDSN shall send a RADIUS Accounting-Request (Stop) record based on the current UDR and fields G1, G2, G3, G8-17 and G20-25 are zeroed and all current instances of G5/G6 in the UDR are eliminated. Immediately afterwards, the PDSN shall send a RADIUS Accounting-Request (Start) record based on the current UDR containing a new Account Session ID and the same Correlation ID.

3.5.10 Time of Day Timer Expires

The time of day timer(s) shall be a set of operator configurable parameters for certain time(s) of day. These timers may be used, for example, to delineate peak and off-peak billing hour boundaries.

When an accounting time of day timer expires, the Serving PDSN shall either:

- Create a new Container attribute in the UDR with Container-Reason ← Tariff Boundary, Event-timestamp ← current time and attributes G1, G2, G3, G8-G16 and G20-25. Instances of G5/G6 are copied to the container.
- Zero fields G1, G2, G3, G8-16 and G20-25. All current instances of G5/G6 in the UDR are eliminated.

Or,

- Add a Session Continue attribute in the UDR with the value set to 1 (True).
- Send a RADIUS Accounting-Request (Stop) record based on the current UDR.
- Zero fields G1, G2, G3, G8-16 and G20-25. All current instances of G5/G6 in the UDR are eliminated.
- Send a RADIUS Accounting-Request (Start) record based on current UDR containing a new Account Session ID and the same Correlation ID.

3.5.11 Hot-Lining

When the PDSN has received the Hot-Line Accounting Indication VSA from the RADIUS Server in an Access-Accept or COA message, the PDSN shall include the Hot-Line Accounting Indication VSA in all subsequent accounting messages.

During the New Session Hot-Line procedure the PDSN shall generate a RADUS Accounting-Request (Start) message indicate the start of the packet data session as usual. If the PDSN receives the Hot-Lining Accounting Indication VSA in a RADIUS Access-Accept message, the PDSN shall include the Hot-Lining Accounting Indication VSA in the RADIUS Accounting-Request (Start) message and any subsequent RADIUS Accounting-Request (Interim) if enabled; and in the RADIUS Accounting-Request (Stop) message.

For Active Session Hot-Lining, upon receiving a COA message with a Hot-lining attributes, the PDSN shall terminate the current accounting session by generating a RADIUS Accounting-Request (Stop) message. This Accounting-Request (Stop) message includes a previously received Hot-Line Accounting Indication(if any). The PDSN then indicates the start of a new (Hot-Line) accounting session by generating a RADIUS Accounting-Request (Start) message. This Accounting-Request (Start) message includes the newly received Hot-Line Accounting Indication (if any). In this way the PDSN demarcates the start and end of the Hot-Line session in the accounting record.

Octets that have been affected by hot-lining (Filtered or Redirected) are account for by G20 and G21.

4 3GPP2 RADIUS Attributes

Figure 3 shows the general Vendor Specific Format for all 3GPP2 RADIUS attributes. The type and vendor ID are the same for every attribute. The vendor ID of 5535 is used to indicate 3GPP2. Note: All integers are in network byte order.

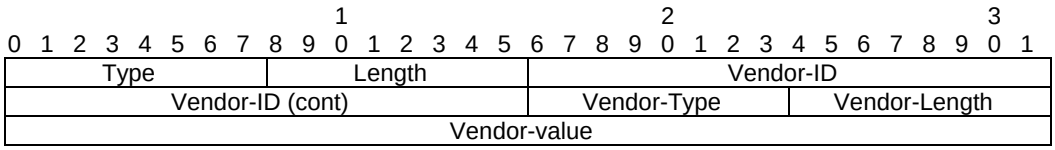


Figure 3 **3GPP2 RADIUS Attribute Format**

4.1 IKE Pre-shared Secret Request

Indicates that the PDSN needs a pre-shared secret for Phase 1 IKE negotiation with the HA. This may appear in a RADIUS Access-Request message for MIP, but not for Simple IP.

Type: 26

Length = 12

Vendor ID: 5535

Vendor-Type = 1

Vendor-Length = 6

Vendor-Value:

1 - The PDSN requests a pre-shared secret for IKE

4.2 Security Level

Indicates the type of security that the home network mandates on the visited network; this attribute optionally appears in the RADIUS Access-Accept message.

Type: 26

Length = 12

Vendor ID: 5535

Vendor-Type = 2

Vendor-Length = 6

Vendor-Value:

1 - IPsec for registration messages (deprecated)

2 - IPsec for tunnels (deprecated)

3 - IPsec for tunnels and registration messages

4 - No IPsec security

4.3 Pre-Shared Secret

A pre-shared secret for IKE that, may appear in a RADIUS Access-Accept message.

Type: 26

Length = 24

Vendor ID: 5535

Vendor-Type = 3

Vendor-Length = 18

Vendor-Value:

Binary value of the pre-shared secret

4.4 Reverse Tunnel Specification

Indicates the style of reverse tunneling that is required, and optionally appears in a RADIUS Access-Accept message.

Type: 26

Length = 12

Vendor ID: 5535

Vendor-Type = 4

Vendor-Length = 6

Vendor-Value:

0 - Reverse tunneling is not required.

1 - Reverse tunneling is required.

4.5 Differentiated Services Class Option

This attribute is deprecated and is replaced by the Allowed Differentiated Services Marking attribute. The Home RADIUS server authorizes differentiated services via the Differentiated Services Class Options attribute, and optionally appears in a RADIUS Access-Accept message.

Type: 26

Length = 12

Vendor ID: 5535

Vendor-Type = 5

Vendor-Length = 6

Vendor-Value:

0 - Best Effort

10 - AF11

12 - AF12

14 - AF13

18 - AF21

20 - AF22

22 - AF23

26 - AF31

28 - AF32

30 - AF33

34 - AF41

36 - AF42

38 - AF43

46 - EF

The above values are taken from [RFC 2597] and [RFC 2598]. There is no intention to convey the actual traffic specification parameters of the differentiated services service.

4.6 Accounting Container

Contains embedded 3GPP2 VSAs and/or RADIUS accounting attributes.

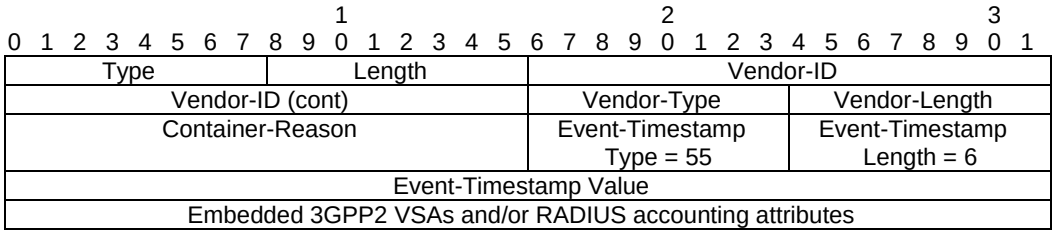


Figure 4 **Accounting Container VSA Format**

Type: 26

Length ≥ 22

Vendor-ID: 5535

Vendor-Type: 6

Vendor-Length ≥ 16

Container-Reason:

1. Tariff Boundary

2. Parameter Change

3. Handoff

Event-Timestamp: Value = The Value field is four octets encoding an unsigned integer with the number of seconds since January 1, 1970 00:00 UTC.

Embedded 3GPP2 VSAs and/or RADIUS accounting attributes: One or more parameters relating to Container-Reason above.

4.7 Home Agent

The address of the HA that appears in a RADIUS Access-Request message, RADIUS Access-Accept message, and accounting messages.

Type: 26

Length = 12

Vendor ID: 5535

Vendor-Type = 7

Vendor-Length = 6

Vendor-Value:

4 octet IP address of the HA.

4.8 KeyID

Contains the KeyID parameter used during IKE exchange between the PDSN and the HA. This VSA may be returned from the Home RADIUS server to the PDSN in the RADIUS Access-Accept message.

Type: 26

Length = 28

Vendor ID: 5535

Vendor-Type = 8

Vendor-Length = 22

Vendor-Value:

A number formed from the concatenation of the Home RADIUS IP Address, and the FA IP address, and a 32-bit timestamp, where each address is encoded using eight hexadecimal ASCII characters. The timestamp contains the number of seconds since January 1, 1970 00:00 UTC.

4.9 ‘S’ Key

Contains the ‘S’ secret parameter used to make Pre-shared secret. This parameter is returned by the Home RADIUS to the HA in the RADIUS Access-Accept message.

Type: 26

Length: greater than 9

Vendor ID: 5535

Vendor-Type = 54

Vendor-Length = 3 or greater

Vendor-Value:

Binary value of the secret.

4.10 'S' Request

Indicates whether the HA requests a shared secret "S". This appears in a RADIUS Access-Request message to the Home RADIUS server:

Type: 26

Length = 12

Vendor ID: 5535

Vendor-Type = 55

Vendor-Length = 6

Vendor-Value:

1. The HA requests a 'S' secret for IKE

4.11 'S' lifetime

Contains the lifetime of 'S' secret parameter used to make Pre-shared secret. This parameter is returned by the Home RADIUS to the HA in the RADIUS Access-Accept message.

Type: 26

Length = 12

Vendor ID: 5535

Vendor-Type = 56

Vendor-Length = 6

Vendor-Value:

Number of seconds since January 1, 1970 00:00 UTC.

4.12 MN-HA SPI

The SPI for the MN-HA shared key that optionally appears in a RADIUS Access-Request message. It is used to request an MN-HA shared key.

Type: 26

Length = 12

Vendor ID: 5535

Vendor-Type = 57

Vendor-Length = 6

Vendor-Value:

Binary value of the MN-HA SPI.

4.13 MN-HA shared key

A shared key for MN-HA that, may appear in a RADIUS Access-Accept message. The MN-HA shared key is encrypted using a method based on the RSA Message Digest Algorithm MD5 [RFC 1321] as described in Section 3.5 of [RFC 2868].

Type: 26

Length: 26 or greater

Vendor ID: 5535

Vendor-Type = 58

Vendor-Length = 20 or greater

Vendor-Value:

Two octets for the salt field as defined in [RFC 2868] followed by at least 16 octets containing the binary value of the encrypted MN-HA shared secret.

4.14 Remote IPv4 Address

Allows the PDSN to identify an IP address to be used for remote address based accounting for the user. It is only used in RADIUS Access-Accept messages. Up to ten instances of the attribute shall be supported in one RADIUS Access-Accept message.

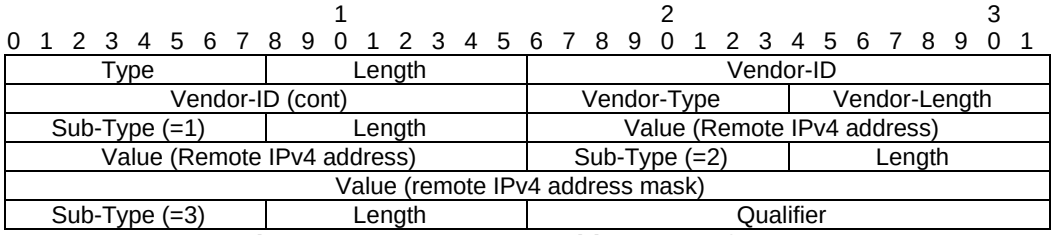


Figure 5 **Remote IPv4 Address VSA format**

Type: 26

Length ≥ 20

Vendor ID: 5535

Vendor-Type: 59

Vendor-Length ≥ 14

Sub-Type (=1): Sub-Type for remote IPv4 address attribute.

Length: length of remote IPv4 address attribute (=6 octets)

Remote IPv4 Address:

The Remote IPv4 Address Sub-Type contains an IPv4 address to be used for remote address based accounting for the user. The address is used in conjunction

with the Remote Address Mask (below), to define the range of address to be monitored.

Sub-Type (=2): Sub-Type for remote IPv4 address mask.

Length: length of remote IPv4 address mask attribute (=6 octets)

Remote Address Mask:

The Remote Address Mask Sub-Type contains an IPv4 address mask that defines a set of remote addresses to be used for remote address based accounting.

Sub-Type (=3): this Sub-Type indicates the characteristics of the IPv4 address with respect to PrePaid Packet Data Service.

Length: length of the Qualifier (=4 octets).

Qualifier bitmap where bit 0 is LSB:

Bit0=1 – Exempt from PrePaid accounting.

All other values reserved for future use.

4.15 Remote IPv6 Address

Allows the PDSN to identify an IP address to be used for remote address based accounting for the user. It is only used in RADIUS Access-Accept messages. Up to ten instances of the attribute shall be supported in one RADIUS Access-Accept message.

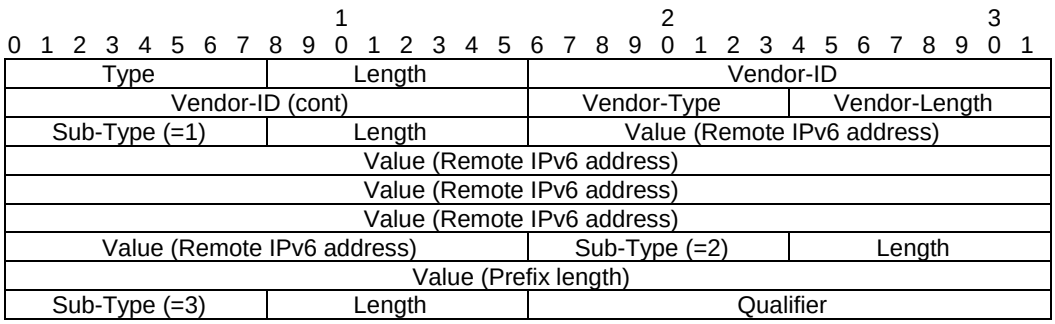


Figure 6 **Remote IPv6 Address VSA Format**

Type: 26

Length ≥ 32

Vendor ID: 5535

Vendor-Type: 70

Vendor-Length ≥26

Sub-Type (=1): type for remote IPv6 address attribute.

Length: length of remote IPv6 address attribute (=18 octets).

Remote IPv6 Address:

The Remote IPv6 Address field contains a corresponding IPv6 address to be used for remote address based accounting for the user.

Sub-Type (=2): Sub-Type for prefix length.

Length: length of prefix length attribute (=6 octets).

Prefix Length:

The prefix length specifies the number of leading bits that shall be matched. The prefix length is less than or equal to 128.

Sub-Type (=3): this Sub-Type indicates the characteristics of the IPv6 address with respect to PrePaid Packet Data Service.

Length: length of the Qualifier (=4 octets).

Qualifier bitmap where bit 0 is LSB:

Bit0=1 – Exempt from PrePaid accounting.

All other values reserved for future use.

4.16 Remote Address Table Index

Contains the index to remote addresses used to generate remote address accounting records. The Home RADIUS server returns this parameter to the PDSN in the RADIUS Access-Accept message.

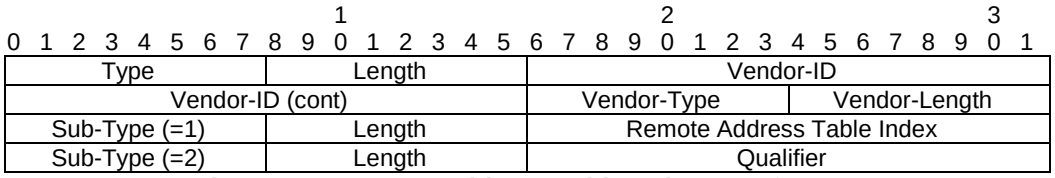


Figure 7 **Remote Address Table Index VSA format**

Type: 26

Length ≥12

Vendor ID: 5535

Vendor-Type: 71

Vendor-Length ≥ 6

Sub-Type (=1): Table Index

Length: length of the Table index value (=4 octets).

Remote Address Table Index:

The Table Index is an identifier to a table of remote addresses, available at the PDSN, used for remote-based accounting for the user.

Sub-Type (=2): this Sub-Type indicates the characteristics of the content of the table Index with respect to PrePaid Packet Data Service.

Length: length of the Qualifier (=4 octets).

Qualifier bitmap where bit 0 is LSB:

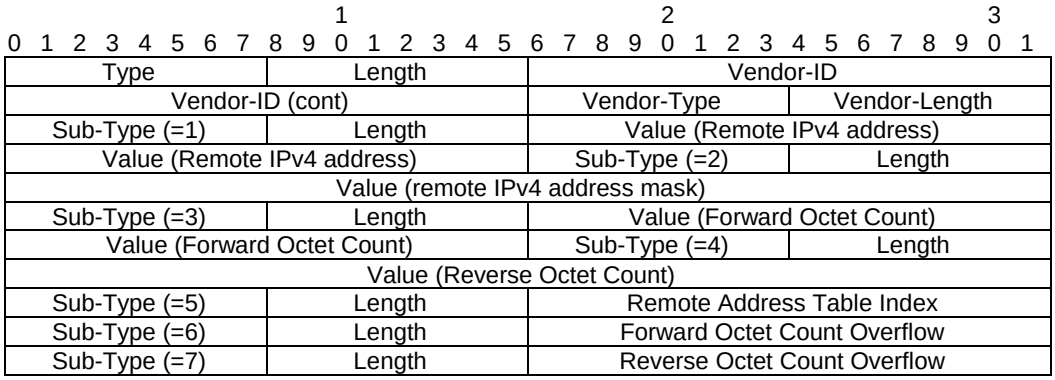
Bit0=1 – Exempt from PrePaid accounting.

Bit1=1 –Summarize Remote Address IPv4/IPv6 Octet Count

All other values reserved for future use.

4.17 Remote IPv4 Address Octet Count

This attribute indicates an IPv4 address and how many octets have been received from and sent to this address over the course of the service being provided to the user. It is only present in RADIUS Accounting-Records where the Acct-Status-Type is set to Stop or Interim-Update.



0 1 2 3 4 5 6 7	8 9 0 1 2 3 4 5	6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
Type	Length	Vendor-ID
Vendor-ID (cont)		Vendor-Type / Vendor-Length
Sub-Type (=1)	Length	Value (Remote IPv4 address)
Value (Remote IPv4 address)		Sub-Type (=2) / Length
Value (remote IPv4 address mask)		
Sub-Type (=3)	Length	Value (Forward Octet Count)
Value (Forward Octet Count)		Sub-Type (=4) / Length
Value (Reverse Octet Count)		
Sub-Type (=5)	Length	Remote Address Table Index
Sub-Type (=6)	Length	Forward Octet Count Overflow
Sub-Type (=7)	Length	Reverse Octet Count Overflow

Figure 8 **Remote IPv4 Address Octet Count format**

Type: 26

Length ≥24

Vendor ID: 5535

Vendor-Type: 72

Vendor-Length ≥18

Sub-Type (=1): Sub-Type for remote IPv4 address attribute. If present, Sub-Type 5 shall not be present.

Length: length of remote IPv4 address attribute (6 octets))

Remote Address:

The Remote Address Field contains an IPv4 address used for destination-based remote IPv4 address based accounting by the user.

Sub-Type (=2): Sub-Type for remote IPv4 address mask. If present, Sub-Type 5 shall not be present.

Length: length of remote IP address mask attribute (=6 octets)

Remote Address Mask:

The Remote Address Mask Sub-Type contains an IPv4 address mask that defines a set of remote addresses to be used for remote address based accounting.

Sub-Type (=3): Sub-Type for Forward Octet Count attribute.

Length: length of Forward Octet Count attribute (6 octets)

Forward Octet Count:

The Forward Octet Count Field indicates how many octets have been received from the Remote Address.

Sub-Type (=4): Sub-Type for Reverse Octet Count attribute.

Length: length of Reverse Octet Count attribute (6 octets)

Reverse Octet Count:

The Reverse Octet Count Field indicates how many octets have been sent to the Remote Address.

Sub-Type (=5): Table Index for summarized Remote IPv4 Address Octet Count, if present Sub-Type 1 and Sub-Type 2 shall not be present.

Length: length of table index (4 bytes)

Table Index:

The table index from the associated Remote Address Table Index attribute.

Sub-Type (=6): Sub-Type for Forward Octet Count Overflow.

Length: length of Forward Octet Count Overflow attribute (= 4 octets)

Forward Octet Count Overflow:

The optional Forward Octet Count Overflow Sub-Type is used to indicate how many times the Forward Octet Count counter has wrapped around 2^32 over the course of the service being provided.

Sub-Type (=7): Sub-Type for Reverse Octet Count Overflow.

Length: length of Reverse Octet Count Overflow attribute (= 4 octets)

Reverse Octet Count Overflow:

The optional Reverse Octet Count Overflow Sub-Type is used to indicate how many times the Reverse Octet Count counter has wrapped around 2^32 over the course of the service being provided.

4.18 Allowed Differentiated Services Marking

Specifies if the user is able to mark packets with AF (A), EF (E). The Max Class (i.e., Max Selector Class), specifies that the user may mark packets with a Class Selector Code Point that is less than or equal to Max Class. This attribute may appear in a RADIUS Access-Accept message.

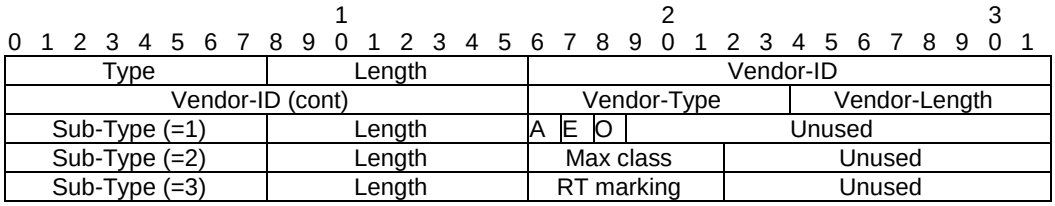


Figure 9 **Allowed Differentiated Service Marking VSA format**

Type: 26

Length = 20

Vendor ID: 5535

Vendor-Type: 73

Vendor-Length = 14

Sub-Type (=1): flags for Allowed Diffserv class

Length: 3 flags (= 4 octets)

"A" bit set means the user can send packets with AF DSCPs.

"E" bit set means the user can send packets with EF DSCP.

"O" bit set means the use can mark packets for experimental or local use.

Sub-Type (=2): Max class selection marking

Length: (=4 octets)

Value: See Reverse tunnel marking.

Sub-Type (=3): Reverse tunnel marking

Length: (= 4 octets)

RT-Marking:

'000000' = Default or Best Effort Forwarding, also Selector Class 0

'001010' = AF11

'001100' = AF12

'001110' = AF13

'010010' = AF21

'010100' = AF22

'010110' = AF23

'011010' = AF31

'011100' = AF32

'011110' = AF33

'100010' = AF41

'100100' = AF42

'100110' = AF43

'101110' = EF

'001000' = Selector Class 1

'010000' = Selector Class 2

'011000' = Selector Class 3

'100000' = Selector Class 4

'101000' = Selector Class 5

'110000' = Selector Class 6

'111000' = Selector Class 7

Other six bit long patterns are legal for this attribute, but are not standardized and therefore may have unpredictable behavior in public networks and other networks not configured to accept non-standard markings.

4.19 Service Option Profile

This attribute specifies the authorized packet data service options and the maximum number of simultaneous service connections (for cdma2000 1x) or the total maximum number of simultaneous link flows (for HRPD). For cdma2000 1x, it also specifies the authorized maximum number of simultaneous service connections of the given service option number (n). This attribute may appear in a RADIUS Access-Accept message.

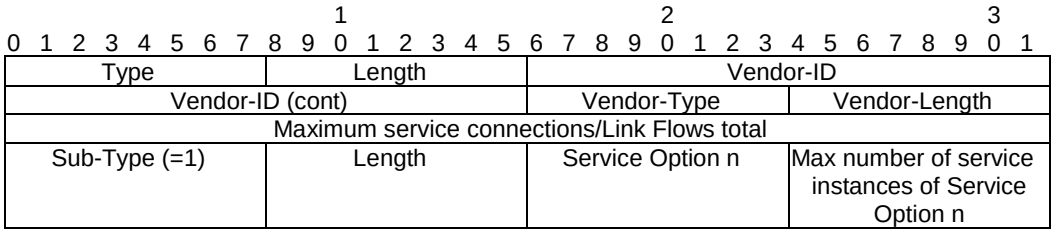


Figure 10 **Service Option Profile VSA format**

Type: 26

Length ≥16

Vendor ID: 5535

Vendor-Type: 74

Vendor-Length ≥10

Maximum Service Connections / Link Flows total:

For cdma2000 1x, the maximum number of service connections the user is allowed to establish regardless of the service option numbers. '1' represents one service connection, i.e., the main service connection. '0' is not an allowed value. For HRPD, it indicates the maximum number of link flows the user is allowed to establish over HRPD.

Sub-Type (=1): Sub-Type for service option

Length: length for service option attribute in octets (4 octets)

Service Option n: Allowed Service Option number n

Maximum Number of Service connections of service option n (only for cdma2000 1x). For HRPD this field shall be set to zero and ignored by the receiver. Sub-Type 1 may be repeated, once for each authorized service option.

4.20 DNS Update Required

Indicates whether the HA is required to send DNS Update to the DNS server for a user. This VSA optionally appears in a RADIUS Access-Accept message from the Home RADIUS server in response to a RADIUS Access-Request message from the HA that contains the DNS-Update-Capability VSA. This VSA is included in a RADIUS Access-Accept message from the Home RADIUS server to the HA only when the DNS update is enabled through the subscriber's profile.

Type: 26

Length = 12

Vendor ID: 5535

Vendor-Type = 75

Vendor-Length = 6

Vendor-Value:

1 - HA performs DNS Update.

All other values reserved for future use. If used, the HA shall discard the VSA and shall not perform DNS Update.

4.21 Always On

A VSA used to indicate if the user has the "Always On" service or not.

Type: 26

Length = 12

Vendor ID: 5535

Vendor-Type = 78

Vendor-Length = 6

Vendor-Value:

0 - Inactive

1 - Active

4.22 Foreign Agent Address

The IPv4 address of the PDSN CoA contained in RRQ.

Type: 26

Length =12

Vendor ID: 5535

Vendor-Type = 79

Vendor-Length = 6

Vendor-Value:

FA IPv4 Address

4.23 MN-AAA Removal Indication

When received in a RADIUS Access-Accept message, the PDSN shall not include the MN-AAA Authentication and MN-FA challenge extensions when relaying the RRQ to the HA.

Type: 26

Length = 12

Vendor ID: 5535

Vendor-Type = 81

Vendor-Length = 6

Vendor-Value:

1 - MN-AAA not required

4.24 RAN Packet Data Inactivity Timer

This is the value of the RAN packet data inactivity timer available for use in the radio network for a packet data session. This attribute optionally appears in the RADIUS Access-Accept message.

Type: 26

Length: = 12

Vendor ID: 5535

Vendor-Type = 82

Vendor-Length = 6

Vendor-Value:

The value of the RAN Packet Data Inactivity Timer specified as an integer according to [4].

4.25 Session Termination Capability (STC)

The value shall be bitmap encoded rather than a raw integer. This attribute shall be included in a RADIUS Access-Request message to the Home RADIUS server and shall contain the value 3 to indicate that the PDSN and HA support both Dynamic authorization with RADIUS and Registration Revocation for MIP4. The attribute shall also be included in the RADIUS Access-Accept message and shall contain the preferred resource management mechanism by the home network, which shall be used for the session and may include values 1 to 3.

Type: 26

Length = 12

Vendor ID: 5535

Vendor-Type = 88

Vendor-Length = 6

Vendor-Value:

0x00000001	Only Dynamic Authorization Extensions to RADIUS is use.
0x00000002 Note 1	Only Registration Revocation in MIP4 is used.
0x00000003	Both Dynamic Authorization Extensions to RADIUS and Registration Revocation in MIP4 are used.

Note 1: For PrePaid service, value 2 is not allowed.

4.26 Allowed Persistent TFTs

This attribute specifies the number of simultaneous persistent TFTs that may be established by the user. Persistent TFTs are those that exist at the PDSN regardless of the state of the corresponding service connection. The user shall also be authorized for the same number of persistent header generation contexts and Header compression context associated with the persistent TFT. This attribute may appear in a RADIUS Access-Accept message.

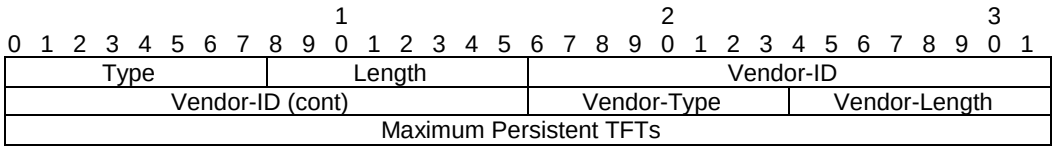


Figure 11 **Allowed Persistent TFTs VSA format**

Type: 26

Length = 12

Vendor ID: 5535

Vendor-Type: 89

Vendor-Length = 6

Maximum Persistent TFTs:

The maximum number of Persistent TFTs, Header Removal and Header Compression Contexts the user is allowed to create.

4.27 PrePaidAccountingQuota (PPAQ)

This attribute specifies the characteristics for PrePaid accounting of the volume and/or duration of a packet data session. It shall be present in all on-line RADIUS Access-Request and on-line RADIUS Access-Accept messages and may be included in other RADIUS Access-Accept messages. Non-used Sub-Types by the PPC and PPS shall be omitted.

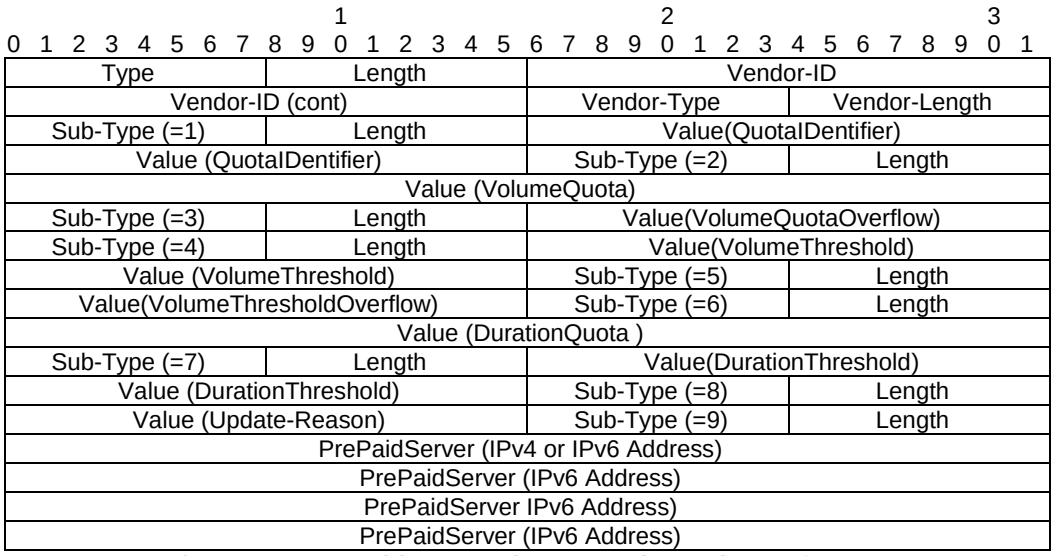


Figure 12 **PrePaidAccountingQuota (PPAQ) VSA format**

Type: 26

Length: variable, greater than 8

Vendor-ID: 5535

Vendor-Type: 90

Vendor-Length: variable, greater than 2

Sub-Type (=1): Sub-Type for QuotaIDentifier attribute

Length: length of QuotaIDentifier attribute (= 6 octets)

QuotaIDentifier (QID):

The QuotaIDentifier Sub-Type is generated by the PrePaid server at allocation of a Volume and/or Duration Quota. The on-line quota update RADIUS Access-Request message sent from the PPC to the PPS shall include a previously received QuotaIDentifier.

Sub-Type (=2): Sub-Type for VolumeQuota attribute

Length: length of VolumeQuota attribute (= 6 octets)

VolumeQuota (VQ):

The optional VolumeQuota Sub-Type is only present if Volume Based charging is used. In RADIUS Access-Accept message (PPS to PPC direction), it indicates the Volume (in octets) allocated for the session by the PrePaid server. In on-line RADIUS Access-Request message (PPC to PPS direction), it indicates the total used volume (in octets) for both forward and reverse traffic applicable to PrePaid accounting[18]. If a Tariff Switch condition was reached during the session, this Sub-Type contains the complete (before and after) volume used, while the VolumeUsedAfterTariffSwitch attribute contains the volume used after the tariff switch condition.

[18] Remote Address identified as exempt from PrePaid accounting shall not be accounted for in the volume used returned in the VolumeQuota.

Sub-Type (=3): Sub-Type for VolumeQuotaOverflow

Length: length of VolumeQuotaOverflow attribute (= 4 octets)

VolumeQuotaOverflow (VQO):

The optional VolumeQuotaOverflow Sub-Type is used to indicate how many times the VolumeQuota counter has wrapped around 2^32 over the course of the service being provided.

Sub-Type (=4): Sub-Type for VolumeThreshold attribute

Length: length of VolumeThreshold attribute (= 6 octets)

VolumeThreshold (VT):

The VolumeThreshold Sub-Type shall always be present if VolumeQuota is present in a RADIUS Access-Accept message (PPS to PPC direction). It is generated by the PrePaid server and indicates the volume (in octets) that shall be used before requesting quota update. This threshold should not be larger than the VolumeQuota.

Sub-Type (=5): Sub-Type for VolumeThresholdOverflow

Length: length of VolumeThresholdOverflow attribute (= 4 octets)

VolumeThresholdOverflow (VTO):

The optional VolumeThresholdOverflow Sub-Type is used to indicate how many times the VolumeThreshold counter has wrapped around 2^32 over the course of the service being provided.

Sub-Type (=6): Sub-Type for DurationQuota attribute

Length: length of DurationQuota attribute (= 6 octets)

DurationQuota (DQ):

The optional DurationQuota Sub-Type is only present if Duration Based charging is used. In RADIUS Access-Accept message (PPS to PPC direction), it indicates the Duration (in seconds) allocated for the session by the PrePaid server. In on-line RADIUS Access-Accept message (PPC to PPS direction), it indicates the total Duration (in seconds) since the start of the accounting session related to the QuotaID.

Sub-Type (=7): Sub-Type for DurationThreshold attribute

Length: length of DurationThreshold attribute (= 6 octets)

DurationThreshold (DT):

The DurationThreshold Sub-Type shall always be present if DurationQuota is present in a RADIUS Access-Accept message (PPS to PPC direction). It represents the duration (in seconds) that shall be used by the session before requesting quota update. This threshold should not be larger than the DurationQuota and shall always be sent with the DurationQuota.

Sub-Type (=8): Sub-Type for Update-Reason attribute

Length: length of Update-Reason attribute (= 4 octets)

Update-Reason attribute (UR):

The Update-Reason Sub-Type shall be present in the on-line RADIUS Access-Request message (PPC to PPS direction). It indicates the reason for initiating the on-line quota update operation. Update reasons 4, 5, 6, 7 and 8 indicate that the associated resources are released at the client side, and therefore the PPS shall not allocate a new quota in the RADIUS Access-Accept message.

1. Pre-initialization
2. Initial request
3. Threshold reached
4. Quota reached
5. Remote Forced disconnect
6. Client Service termination
7. Main SC released
8. Service Connection not established
9. Tariff Switch Update
10. Incorrect Quota Type Received
11. Poorly Formed Quota Attribute

Sub-Type (=9): Sub-Type for PrePaidServer attribute

Length: Length of PrePaidServer (IPv4 = 6 octets, IPv6= 18 octets

PrePaidServer:

The optional, multi-value PrePaidServer indicates the address of the serving PrePaid System. If present, the Home RADIUS server uses this address to route the message to the serving PrePaid Server. The attribute may be sent by the Home RADIUS server. If present in the incoming RADIUS Access-Accept message, the PDSN shall send this attribute back without modifying it in the subsequent RADIUS Access-Request message, except for the first one. If multiple values are present, the PDSN shall not change the order of the attributes.

4.28 PrePaidAccountingCapability (PPAC)

This attribute specifies the capability for PrePaid accounting for a packet data session. It contains the possible capabilities of the PrePaid client and the selected (by the PrePaid server) capability for the session. The absence of this VSA indicates that the client is not capable of PrePaid Accounting and the session shall not use PrePaid accounting.

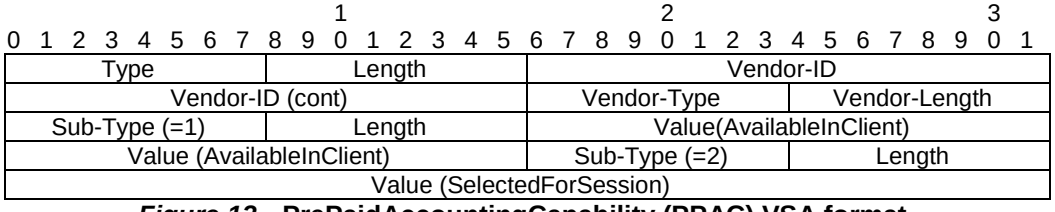


Figure 13 **PrePaidAccountingCapability (PPAC) VSA format**

Type: 26

Length: variable, greater than 8

Vendor-ID: 5535

Vendor-Type: 91

Vendor-Length: variable, greater than 2

Sub-Type (=1): Sub-Type for AvailableInClient attribute

Length: length of AvailableInClient attribute (= 6 octets)

AvailableInClient (AiC):

The optional AvailableInClient Sub-Type, generated by the PrePaid client, indicates the PrePaid Accounting capabilities of the client in the PDSN or HA and shall be bitmap encoded. The possible values are:

0x00000001	PrePaid Accounting for Volume supported
0x00000002	PrePaid Accounting for Duration supported
0x00000003	PrePaid Accounting for Volume and Duration supported (non concurrently)
Others	Reserved, treat like Not Capable of PrePaid Accounting (=0).

Sub-Type (=2): Sub-Type for SelectedForSession attribute

Length: length of SelectedForSession attribute (= 6 octets)

SelectedForSession (SfS):

The optional SelectedForSession Sub-Type, generated by the PrePaid server, indicates the PrePaid Accounting capability to be used for a given session.

The possible values are:

0x00000000	PrePaid Accounting not used
0x00000001	Usage of PrePaid Accounting for Volume. (only possible if the AvailableInClient supports PrePaid Accounting for Volume)
0x00000002	Usage of PrePaid Accounting for Duration. (only possible if the AvailableInClient supports PrePaid Accounting for Duration)
0x00000003	Usage of PrePaid Accounting for Volume and Duration (non concurrent) (only possible if the AvailableInClient supports PrePaid Accounting for Volume and duration)
Others	Reserved, treat like PrePaid Accounting not used (=0).

4.29 MIP Lifetime

This VSA shall be included in the RADIUS Access-Request message from the HA to the Home RADIUS/PPS if the HA is PrePaid capable. It may be included in the RADIUS Access-Accept message from the Home RADIUS/PPS to HA, in which case, the HA shall include the received value in the MIP RRP sent to the PDSN.

1 2 3

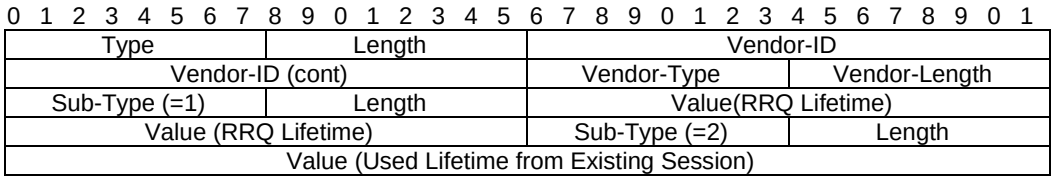


Figure 14 **MIP Lifetime VSA format**

Type: 26

Length: variable, greater than 8

Vendor-ID: 5535

Vendor-Type: 92

Vendor-Length: variable, greater than 2

Sub-Type (=1): Sub-Type for RRQ Lifetime attribute

Length: length of RRQ Lifetime attribute (= 6 octets)

RRQ Lifetime:

Shall be included in the initial RADIUS Access-Request message and subsequent on-line RADIUS Access-Request if duration based PrePaid is provided for the session. It contains the MIP RRQ integer value lifetime received in the MIP RRQ message. In the RADIUS Access-Accept message, it contains the MIP RRQ integer value lifetime that shall be used in the MIP RRP.

Sub-Type (=2): Sub-Type for Used Lifetime from Existing Session attribute

Length: length of Used Lifetime from Existing Session attribute (= 6 octets)

Used Lifetime from Existing Session:

Shall be included in the RADIUS Access-Request message at re-registration and updated RRQ (new CoA) if duration based PrePaid is provided for the session, it contains the used MIP RRQ lifetime value from an existing MIP session with the same NAI and Home Address.

4.30 Accounting-Stop-triggered-by-Active-Stop-Indication

When received in a RADIUS Access-Accept message, the PDSN shall trigger Accounting-Request (Stop) and (Start) for the main service connection at transition between dormant and active states.

Type: 26

Length = 12

Vendor ID: 5535

Vendor-Type = 93

Vendor-Length = 6

Vendor-Value =

1 – Accounting report at active/dormant transitions

4.31 Service Reference ID

Specifies the reference ID of the service instance for cdma2000 1x as received in the A11 Registration Request.

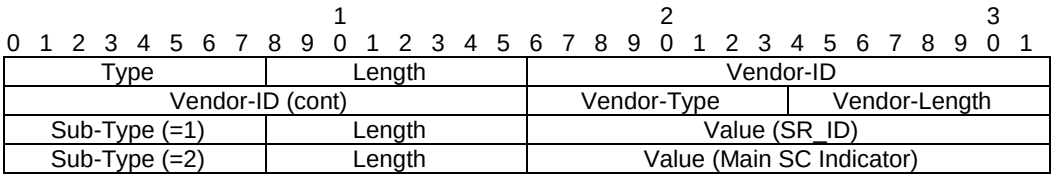


Figure 15 **Service Reference ID format**

Type: 26

Length ≥ 12

Vendor ID: 5535

Vendor-Type: 94

Vendor-Length ≥ 6

Sub-Type (=1): SR_ID

Length: (= 4 octets)

Contains the SR_ID value received in the A11 Registration-Request message.

Sub-Type (=2): Main SC Indicator

Length: (= 4 octets)

Only included for the main service connection.

1: main SI.

4.32 DNS-Update-Capability

Indicates whether the HA is capable of performing dynamic DNS update. This VSA is included in a RADIUS Access-Request message from the HA to the Home RADIUS server only when the HA is configured to do DNS update.

Type: 26

Length = 12

Vendor ID: 5535

Vendor-Type = 95

Vendor-Length = 6

Vendor-Value:

1 – HA is capable of dynamic DNS Update.

All other values reserved for future use.

4.33 DisconnectReason

Indicates the reason for disconnecting the user. This attribute may be included in a RADIUS Disconnect-Request message from Home RADIUS server to the PDSN.

Type: 26

Length = 12

Vendor ID: 5535

Vendor-Type = 96

Vendor-Length = 6

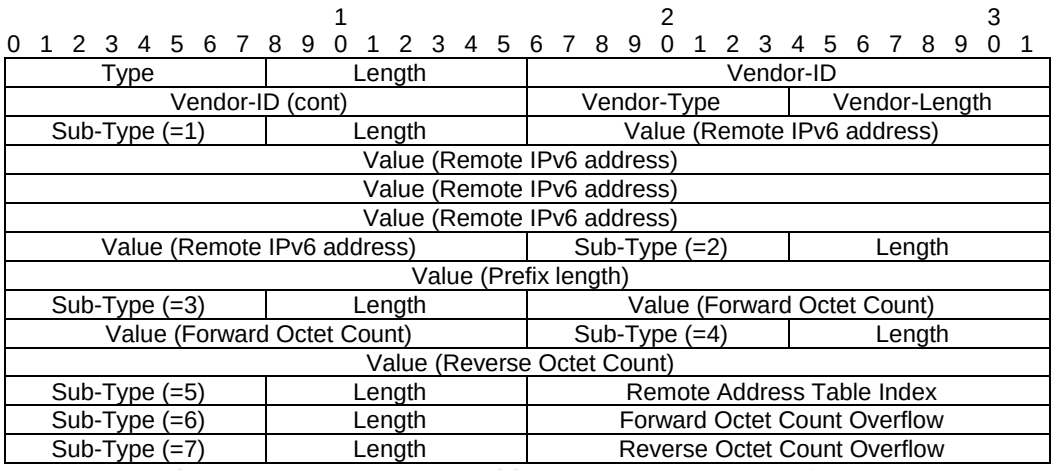
Vendor-Value:

1-MS Mobility Detection

All other values are reserved

4.34 Remote IPv6 Address Octet Count

This attribute indicates an IPv6 address and how many octets have been received from and sent to this address over the course of the service being provided to the user. It is only present in RADIUS Accounting-Records where the Acct-Status-Type is set to Stop or Interim-Update.



0 1 2 3 4 5 6 7	8 9 0 1 2 3 4 5	6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
Type	Length	Vendor-ID
Vendor-ID (cont)		Vendor-Type / Vendor-Length
Sub-Type (=1)	Length	Value (Remote IPv6 address)
Value (Remote IPv6 address)		
Value (Remote IPv6 address)		
Value (Remote IPv6 address)		
Value (Remote IPv6 address)	Sub-Type (=2)	Length
Value (Prefix length)		
Sub-Type (=3)	Length	Value (Forward Octet Count)
Value (Forward Octet Count)	Sub-Type (=4)	Length
Value (Reverse Octet Count)		
Sub-Type (=5)	Length	Remote Address Table Index
Sub-Type (=6)	Length	Forward Octet Count Overflow
Sub-Type (=7)	Length	Reverse Octet Count Overflow

Figure 16 **Remote IPv6 Address Octet Count VSA format**

Type: 26

Length ≥24

Vendor ID: 5535

Vendor-Type23: 97

Vendor-Length ≥18

Sub-Type (=1): Sub-Type for remote IPv6 address attribute. If present, Sub-Type 5 shall not be present.

Length: length of remote address attribute (18 octets)

Remote Address:

The Remote Address Field contains an IPv6 address used for destination-based remote IPv6 address based accounting by the user.

Sub-Type (=2): Sub-Type for prefix length. If present, Sub-Type 5 shall not be present.

Length: length of prefix length attribute (=4)

Prefix Length:

The prefix length specifies the number of leading bits that shall be matched. The prefix length is less than or equal to 128.

Sub-Type (=3): Sub-Type for Forward Octet Count attribute.

Length: length of Forward Octet Count attribute (6 octets)

Forward Octet Count:

The Forward Octet Count Field indicates how many octets have been received from the Remote Address.

Sub-Type (=4): Sub-Type for Reverse Octet Count attribute.

Length: length of Reverse Octet Count attribute (6 octets)

Reverse Octet Count:

The Reverse Octet Count Field indicates how many octets have been sent to the Remote Address.

Sub-Type (=5): Table Index for summarized Remote IPv6 Address Octet Count, if present Sub-Type 1 and Sub-Type 2 shall not be present.

Length: length of table index (4 bytes)

Table Index:

The table index from the associated Remote Address Table Index attribute.

Sub-Type (=6): Sub-Type for Forward octet count Overflow.

Length: length of Forward octet count Overflow attribute (= 4 octets)

Forward Octet Count Overflow:

The optional Forward Octet Count Overflow Sub-Type is used to indicate how many times the Forward Octet Count counter has wrapped around 2^32 over the course of the service being provided.

Sub-Type (=7): Sub-Type for Reverse Octet Count Overflow.

Length: length of Reverse Octet Count Overflow attribute (= 4 octets)

Reverse Octet Count Overflow:

The optional Reverse Octet Count Overflow Sub-Type is used to indicate how many times the Reverse Octet Count counter has wrapped around 2^32 over the course of the service being provided.

4.35 PrePaidTariffSwitching (PTS)

This VSA specifies the characteristics for PrePaid accounting When Tariff Switching is used. If the PTS VSA is included in the on-line RADIUS Access-Request/Accept messages or RADIUS Access-Accept message, the PPAQ VSA shall also be included. It may be present in on-line RADIUS Access-Request and on-line RADIUS Access-Accept messages and may be included in other RADIUS Access-Accept messages. Non-used Sub-Types by the PPS shall be omitted.

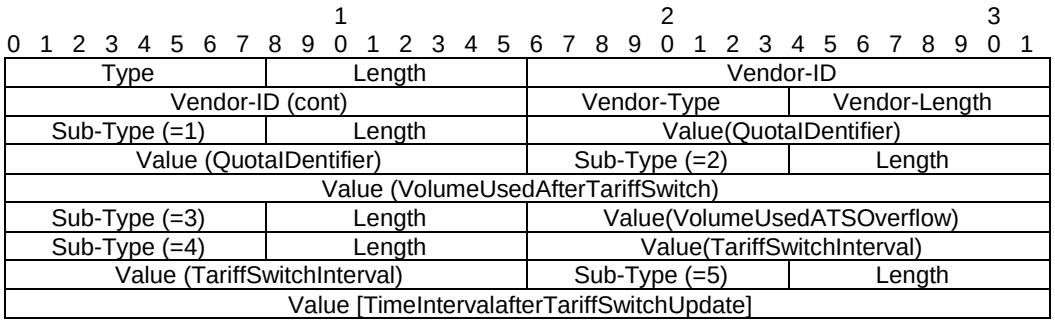


Figure 17 **PrePaidTariffSwitch (PTS) VSA format**

Type: 26

Length: variable, greater than 8

Vendor-ID: 5535

Vendor-Type: 98

Vendor-Length: variable, greater than 2

Sub-Type (=1): Sub-Type for QuotaIDentifier attribute

Length: length of QuotaIDentifier attribute (= 6 octets)

QuotaIDentifier (QID):

The QuotaIDentifier Sub-Type is generated by the PrePaid server at allocation of a Volume Quota. The on-line quota update RADIUS Access-Request message sent from the PPC to the PPS shall include a previously received QuotaIDentifier. The QuotaIDentifier value used in the PTS VSA shall be the same to the one included in the PPAQ VSA.

Sub-Type (=2): Sub-Type for VolumeUsedAfterTariffSwitch attribute

Length: length of VolumeUsedAfterTariffSwitch attribute (= 6 octets)

VolumeUsedAfterTariffSwitch (VUATS):

The VolumeUsedAfterTariffSwitch Sub-Type is only present if Volume Based charging is used and the RADIUS message is an on-line RADIUS Access-Request message (PPC to PPS direction). It indicates the total used volume (in octets) for both forward and reverse traffic applicable to PrePaid accounting after a Tariff Switch condition was reached during the session. If no Tariff Switch condition was reached, the PTS VSA shall not be present in the on-line RADIUS Access-Request message. The total volume used before and after the Tariff Switch is reported in the VolumeQuota Sub-Type in the associated PPAQ VSA.

Sub-Type (=3): Sub-Type for VolumeUsedATSOverflow

Length: length of VolumeUsedATSOverflow attribute (= 4 octets)

VolumeUsedATSOverflow (VUATSO):

The optional VolumeUsedAfterTariffSwitchOverflow Sub-Type is used to indicate how many times the VolumeUsedAfterTariffSwitch counter has wrapped around 2^32 over the course of the service being provided.

Sub-Type (=4): Sub-Type for TariffSwitchInterval attribute

Length: length of TariffSwitchInterval attribute (= 6 octets)

TariffSwitchInterval (TSI):

The TariffSwitchInterval Sub-Type is present if Volume Based charging is used and the RADIUS message is a RADIUS Access-Accept (PPS to PPC direction). It indicates the interval (in seconds) between the time stamp (G4) of the corresponding on-line RADIUS Access-Request and the next tariff switch condition. If no Tariff Switch condition is required, the PTS VSA shall not be present. The total volume used before and after the Tariff Switch is reported in the VolumeQuota Sub-Type in the PPAQ VSA, and the volume used after the Tariff Switch is reported in the VolumeUsedAfterTariffSwitch Sub-Type in the PTS VSA.

Sub-Type (=5): Sub-Type for TimeIntervalafterTariffSwitchUpdate attribute

Length: Length of TimeIntervalafterTariffSwitchUpdate (=6 octets)

TimeIntervalafterTariffSwitchUpdate (TITSU):

The TimeIntervalafterTariffSwitchUpdate Sub-Type may be present when Volume Based tariff switching is used. The Home RADIUS/PPS may send it to the PPC in the RADIUS Access-Accept message only if the TSI Sub-Type is also present. It corresponds to the duration after TSI where an on-line RADIUS Access-Request message may be sent by the PrePaid capable PDSN to report VUATS before the next tariff switch condition is triggered in the Home RADIUS/PPS.

4.36 Subnet

This attribute specifies the Subnet and Sector ID information of the HRPD RAN. One attribute may be present in the RADIUS Accounting Messages sent from the PDSN to the HAAA.

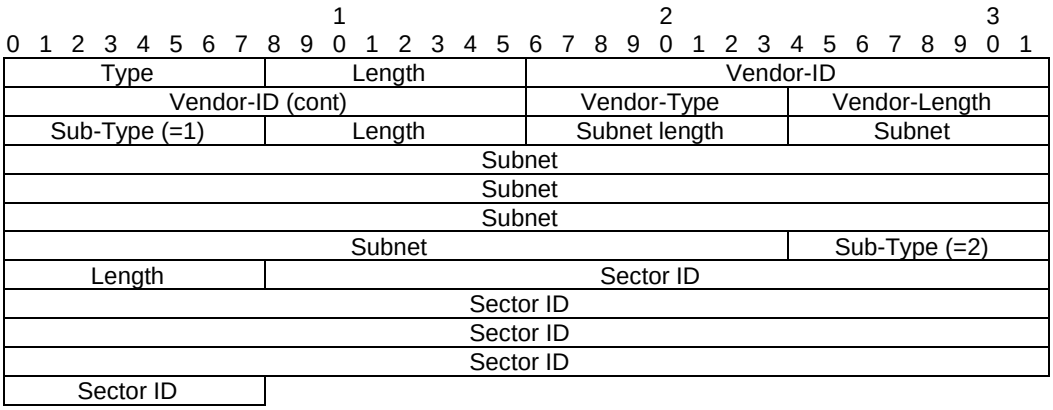


Figure 18 **Subnet VSA format**

Type: 26

Length: variable, greater than 8

Vendor-ID: 5535

Vendor-Type: 108

Vendor-Length: variable >= 6

Sub-Type (=1): Sub-Type for Subnet attribute

Length: length of the Subnet attribute (19 octets).

Subnet Length:

> The element shall contain the number of bits in the subnet identifier. These bits shall form the most significant bits of any sector identifier within the subnet. This field shall be encoded as a positive integer from 1 to 128.

Subnet:

> The element shall contain a binary representation of the subnet value for the subnet. This field is 128 bits long. If the Subnet length (L) is less than 128 bits, then the 128-L least significant bits shall be filled with all 0s.

Sub-Type (=2): Sub-Type for Sector ID attribute

Length: length of the Sector ID attribute (= 18 octets)

Sector ID:

> The element shall contain a binary representation of the Sector ID value.

Both Sub-Type (1) and Sub-Type (2) shall be present.

4.37 DNS Server IP Address

This VSA may be present in a RADIUS Access-Accept message. It includes a Primary and a Secondary DNS server IP addresses.

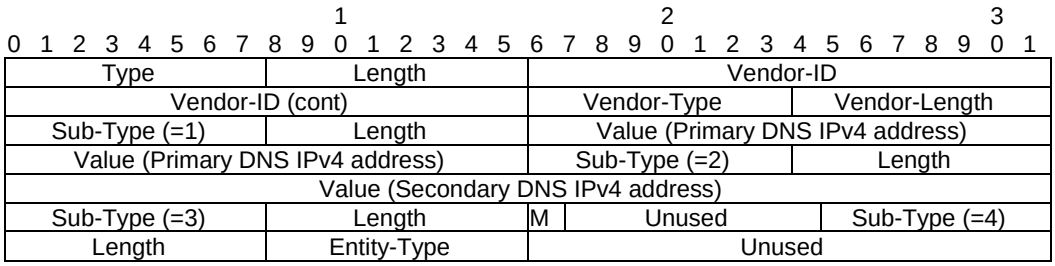


Figure 19 **DNS Server IP Address VSA**

Type: 26

Length: 28

Vendor ID: 5535

Vendor-Type: 117

Vendor-Length: 22

Sub-Type (=1):

Length: (=6 octets)

Vendor-Value:

Primary DNS server IP Address.

Sub-Type (=2):

Length: (= 6 octets)

Vendor-Value:

Secondary DNS server IP Address.

Sub-Type (=3): Flag

Length: (=3 octet)

Vendor-Value:

"M" bit set to 1 indicates to the PDSN that the Primary and Secondary DNS IP addresses provided by the Home RADIUS server shall override the Primary and Secondary DNS addresses if provided also by the Visited RADIUS server.

Sub-Type (=4):

Length: (=3 octet)

Vendor-Value:

"Entity-Type" The network entity that inserted in the DNS server IP address. Currently the following types are defined:

HAAA = 1

VAAA = 2

4.38 MIP6-Home Agent (received from BU)

This VSA carries the IPv6 Home Agent Address extracted from the Binding Update message. This VSA may be present in the RADIUS Access-Request Message sent from the HA to the Home RADIUS Server.

Type: 26

Length = 24

Vendor ID: 5535

Vendor-Type = 118

Vendor-Length = 18

Vendor-Value:

IPv6 Home Agent Address

4.39 MIP6-CoA

This VSA carries the Care-of Address extracted from the Binding Update message. This VSA may be present in the RADIUS Access-Request Message sent from the HA to the Home RADIUS Server and in the RADIUS Access-Accept Message sent from the Home RADIUS Server to the HA.

Type: 26

Length = 24

Vendor ID: 5535

Vendor-Type = 119

Vendor-Length = 18

Vendor-Value:

IPv6 Care-of Address

4.40 MIP6 HoA-Not-Authorized

This VSA carries an integer value of 1 to indicate to the HA that the HoA in the Binding Update is not authorized for use by the corresponding NAI in the Binding Update. This VSA may be present in the RADIUS Access-Accept Message sent from the Home RADIUS Server to the HA.

Type: 26

Length = 12

Vendor ID: 5535

Vendor-Type = 120

Vendor-Length = 6

Vendor-Value:

1- The HoA is not authorized.

Other values reserved.

4.41 MIP6-Session Key

This VSA carries the Integrity Key(IK) in its encrypted form, from the Home RADIUS server to the HA. The IK is encrypted using the procedures described in section 3.5 of [RFC 2868].

Type: 26

Length => 26

Vendor ID: 5535

Vendor-Type = 121

Vendor-Length => 20

Vendor-Value:

Two octets for the salt field as defined in [RFC 2868] followed by 16 octets containing the binary value of the encrypted Integrity Key (IK).

4.42 Hot-Line Accounting Indication

This attribute in a RADIUS Accounting-Request message indicates to back-office systems (billing audit systems) that the session has been Hot-Lined.

Exactly one Hot-Line Accounting Indication VSA may appear in a RADIUS Access-Accept message or RADIUS COA message. If the Hot-lining Device (PDSN, HA) received this attribute in a RADIUS Access-Accept or COA message, then it shall include the attribute in any subsequent RADIUS Accounting messages for that session.

Type: 26

Length => 9

Vendor ID: 5535

Vendor-Type = 122

Vendor-Length => 3

Vendor-Value = String

The value of this string is opaque to the Hot-Lining Device.

4.43 Filter Rule

Filter Rule is used to setup packet filter rules that block or permit traffic flows.

One or more Filter Rule attributes may be present in a RADIUS Access-Accept or RADIUS COA message.

Filter Rule VSAs are processed in the order that they were received starting with the first rule received until a rule is matched. Since the Hot-Lining Device matches the rules in the order that they were received, the order in which the attributes appear in the packet relative to each other is significant.

Type: 26

Length => 9

Vendor ID: 5535

Vendor-Type = 124

Vendor-Length => 3

Vendor-Value = Text

Filter Rule VSAs follow the format and specification of the IPFilterRule attribute defined in [RFC 3588]:

action dir proto from src to dst [options]

action

permit - Allow packets that match the rule.

deny - Drop packets that match the rule.

flush - has no other elements in the string. The PDSN and or HA shall remove all filter rules received from the HAAA for this session.

dir

"in" is from the terminal, "out" is to the terminal.

proto

An IP protocol specified by number. The "ip" keyword means any protocol will match.

src and dst <address/mask> [ports]

The <address/mask> may be specified as:

ipno

An IPv4 or IPv6 number in dotted - quad or canonical IPv6 form. Only this exact IP number will match the rule.

ipno/bits

An IP number as above with a mask width of the form 1.2.3.4/24. In this case, all IP numbers from 1.2.3.0 to 1.2.3.255 will match. The bit width shall be valid for the IP version and the IP number shall NOT have bits set beyond the mask. For a match to occur, the same IP version shall be present in the packet that was used in describing the IP address. To test for a particular IP version, the bits part can be set to zero. The keyword "any" is 0.0.0.0/0 or the IPv6 equivalent. The keyword "assigned" is the address or set of addresses assigned to the terminal. For IPv4, a typical first rule is often "deny in ip! assigned".

The sense of the match can be inverted by preceding an address with the not modifier (!), causing all other addresses to be matched instead. This does not affect the selection of port numbers.

With the TCP, UDP and SCTP protocols, optional ports may be specified as:

{port/port-port}[,ports[,...]]

The '-' notation specifies a range of ports (including boundaries).

Fragmented packets that have a non-zero offset (i.e., not the first fragment) will never match a rule that has one or more port specifications. See the frag option for details on matching fragmented packets.

options:

frag

Match if the packet is a fragment and this is not the first fragment of the datagram. frag may not be used in conjunction with either tcpflags or TCP/UDP port specifications.

ipoptions spec

Match if the IP header contains the comma separated list of options specified in spec. The supported IP options are:

ssrr (strict source route), lsrr (loose source route), rr (record packet route) and ts (timestamp). The absence of a particular optionmay be denoted with a '!'.

tcpoptions spec

Match if the TCP header contains the comma separated list of options specified in spec. The supported TCP options are:

mss (maximum segment size), window (tcp window advertisement), sack (selective ack), ts ([RFC 1323] timestamp) and cc ([RFC 1644] t/tcp connection count). The absence of a particular option may be denoted with a '!'.

established

TCP packets only. Match packets that have the RST or ACK bits set.

setup

TCP packets only. Match packets that have the SYN bit set but no ACK bit.

tcpflags spec

TCP packets only. Match if the TCP header contains the comma separated list of flags specified in spec. The supported TCP flags are:

fin, syn, rst, psh, ack and urg. The absence of a particular flag may be denoted with a '!'. A rule that contains a

tcpflags specification can never match a fragmented packet that has a non-zero offset. See the frag option for details on matching fragmented packets.

icmptypes types

ICMP packets only. Match if the ICMP type is in the list types. The list may be specified as any combination of ranges or individual types separated by commas. Both the numeric values and the symbolic values listed below can be used. The supported ICMP types are:

echo reply (0), destination unreachable (3), source quench (4), redirect (5), echo request (8), router advertisement (9), router solicitation (10), time-to-live exceeded (11), IP header bad (12), timestamp request (13), timestamp reply (14), information request (15), information reply (16), address mask request (17) and address mask reply (18).

The access device shall always discard a packet that has an IP fragment with a fragment offset of one. Although this is a valid packet, its only use is to try to circumvent firewalls.

A PDSN or HA that is unable to interpret or apply a deny rule shall terminate the session. A PDSN or HA that is unable to interpret or apply a permit rule may apply a more restrictive rule. A PDSN or HA may apply deny rules of its own before the supplied rules, for example to protect the access device owner's infrastructure.

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

4.44 HTTP Redirection Rule

HTTP Redirection Rule instructs the Hot-Lining Device where to redirect HTTP flows.

One or more HTTP Redirection-Rules attributes may be present in a RADIUS Access-Accept or RADIUS COA message.

Rule matching starts at the first rule that was received. If a rule does not match then the next rule is tried. Therefore the order that the HTTP-Rules appear in the RADIUS Access-Accept or COA message is significant.

If the source address of the request matches the source address contained in the rule and the destination address of the request matches the destination address contained in the rule, then the rule is matched and the device will respond back with either an HTTP Redirect if the action is “redirect” or pass the request through if the action is “pass”. No other HTTP Redirection rules will be processed.

Redirection is achieved by the Hot-Lining Device responding with an HTTP Redirect Response as per [RFC 2616] specifying the URL.

Type: 26

Length => 9

Vendor ID: 5535

Vendor-Type = 125

Vendor-Length => 3

Vendor-Value = Text

The text conforms to the following specification:

HTTP-Redirect-Rule shall follow the format:

action url from src to dst

action:

redirect

redirect packets that match the rule to the specified URL encoded as per [RFC 2396].

pass

if the rule is matched then the HTTP request is allowed to continue through.

If the action is pass then url is not specified.

flush

has no other elements in the string. The PDSN and/or the HA shall flush all HTTP-Redirection rules received from the HAAA

src and dst <address/mask> [ports]

The <address/mask> may be specified as:

ipno

An IPv4 or IPv6 number in dotted - quad or canonical IPv6 form. Only this exact IP number will match the rule.

ipno/bits

An IP number as above with a mask width of the form 1.2.3.4/24. In this case, all IP numbers from 1.2.3.0 to 1.2.3.255 will match. The bit width shall be valid for the IP version and the IP number shall not have bits set beyond the mask. For a match to occur, the same IP version shall be present in the packet that was used in describing the IP address. To test for a particular IP version, the bits part can be set to zero. The keyword "any" is 0.0.0.0/0 or the IPv6 equivalent. The keyword "assigned" is the address or set of addresses assigned to the terminal. For IPv4, a typical first rule is often "deny in ip! assigned"

The sense of the match can be inverted by preceding an address with the not modifier (!), causing all other addresses to be matched instead. This does not affect the selection of port numbers.

Optional ports may be specified as:

{port/port-port}[,ports[,...]]

The '-' notation specifies a range of ports (including boundaries).

Fragmented packets that have a non-zero offset (i.e., not the first fragment) will never match a rule that has one or more port specifications. See the frag option for details on matching fragmented packets.

A PDSN or HA that is unable to parse an HTTP Redirection Rule received in a RADIUS Access-Accept message shall terminate the session or shall respond with a COA NAK message if it was received in a COA message. A PDSN or HA that is unable to interpret or apply a redirect rule may apply a more restrictive rule. A PDSN or HA may apply redirect rules of its own before the supplied rules, for example to protect the access device owner's infrastructure.

4.45 IP Redirection Rule

IP Redirection Rule is used to specify which packet flow to redirect and where to redirect it.

One or more IP Redirection-Rule attributes may be present in a RADIUS Access-Accept or RADIUS COA message.

IP Redirection Rules are processed in the order that they were received starting with the first rule received until a rule is matched. Since the Hot-Lining Device matches the rules in the order that they were received, the order in which the attributes appear in the packet relative to each other is significant.

Type: 26

Length => 9

Vendor ID: 5535

Vendor-Type = 126

Vendor-Length => 3

Vendor-Value = Text

The text conforms to the following specification:

IP Redirect-Filter-Rule shall follow the format:

action redirip [port] | dir proto from src to dst [options]

action:

redirect

redirect packets that match the rule to the specified redir ip address and optional port.

flush

has no other elements in the string. The PDSN and/or the HA shall flush all redirection rules received from the HAAA.

redirip [port]

indicates the redirection ip address and optionally port.

proto

An IP protocol specified by number. The "ip" keyword means any protocol will match.

src and dst <address/mask> [ports]

The <address/mask> may be specified as:

ipno

An IPv4 or IPv6 number in dotted - quad or canonical IPv6 form. Only this exact IP number will match the rule.

ipno/bits

An IP number as above with a mask width of the form 1.2.3.4/24. In this case, all IP numbers from 1.2.3.0 to 1.2.3.255 will match. The bit width shall be valid for the IP version and the IP number shall NOT have bits set beyond the mask. For a match to occur, the same IP version shall be present in the packet that was used in describing the IP address. To test for a particular IP version, the bits part can be set to zero. The keyword "any" is 0.0.0.0/0 or the IPv6 equivalent. The keyword "assigned" is the address or set of addresses assigned to the terminal. For IPv4, a typical first rule is often "deny in ip! assigned"

The sense of the match can be inverted by preceding an address with the not modifier (!), causing all other addresses to be matched instead. This does not affect the selection of port numbers.

With the TCP, UDP and SCTP protocols, optional ports may be specified as:

{port/port-port}[,ports[,...]]

The '-' notation specifies a range of ports (including boundaries).

Fragmented packets that have a non-zero offset (i.e., not the first fragment) will never match a rule that has one or more port specifications. See the frag option for details on matching fragmented packets.

options:

frag

Match if the packet is a fragment and this is not the first fragment of the datagram. frag may not be used in conjunction with either tcpflags or TCP/UDP port specifications.

ipoptions spec

Match if the IP header contains the comma separated list of options specified in spec. The supported IP options are:

ssrr (strict source route), lsrr (loose source route), rr (record packet route) and ts (timestamp). The absence of a particular optionmay be denoted with a '!'.

tcpoptions spec

Match if the TCP header contains the comma separated list of options specified in spec. The supported TCP options are:

mss (maximum segment size), window (tcp window advertisement), sack (selective ack), ts ([RFC1323] timestamp) and cc ([RFC 1644] t/tcp connection count). The absence of a particular option may be denoted with a '!'.

established

TCP packets only. Match packets that have the RST or ACK bits set.

setup

TCP packets only. Match packets that have the SYN

bit set but no ACK bit.

tcpflags spec

TCP packets only. Match if the TCP header contains the comma separated list of flags specified in spec. The supported TCP flags are:

fin, syn, rst, psh, ack and urg. The absence of a particular flag may be denoted with a '!'. A rule that contains a tcpflags specification can never match a fragmented packet that has a non-zero offset. See the frag option for details on matching fragmented packets.

icmptypes types

ICMP packets only. Match if the ICMP type is in the list types. The list may be specified as any combination of ranges or individual types separated by commas. Both the numeric values and the symbolic values listed below can be used. The supported ICMP types are:

echo reply (0), destination unreachable (3), source quench (4), redirect (5), echo request (8), router advertisement (9), router solicitation (10), time-to-live exceeded (11), IP header bad (12), timestamp request (13), timestamp reply (14), information request (15), information reply (16), address mask request (17) and address mask reply (18).

A PDSN or HA that is unable to interpret or apply an IP Redirection Rule shall terminate the session. A PDSN or HA that is unable to interpret or apply an IP Redirection Rule may apply a more restrictive rule. A PDSN or HA may apply IP Redirection Rule of its own before the supplied rules, for example to protect the access device owner's infrastructure.

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

4.46 Hot-Line Capability

This attribute is a bit mask that specifies the capabilities of a Hot-Lining Device. The Hot-Lining Device includes this attribute in a RADIUS Access-Request message to specify its Hot-Lining capabilities. Should the packet data session require Hot-Lining, the HAAA uses the content of this attribute to ascertain how it will Hot-Line the user's packet data session. If this attribute is included, at least one hot-lining method shall be selected.

Type: 26

Length => 12

Vendor ID: 5535

Vendor-Type = 127

Vendor-Length = 6

Vendor Value: Integer

A bit mask of the supported methods for Hot-Lining a packet data session.

0x00000001	Profile-based Hot-Lining is supported (Using RADIUS Filter-Id attributes)
0x00000002	Rule-based Hot-Lining is supported using Filter Rule
0x00000003	Rule-based Hot-Lining is supported using HTTP Redirection Rule.
Others	Rule-based Hot-Lining is supported using IP Redirection Rule.

4.47 MIP6-Home Link Prefix (Attribute A)

This VSA carries the assigned Home Link Prefix during MIP6 bootstrapping. The VSA is included in a RADIUS Access-Accept message from the Home RADIUS server to the PDSN.

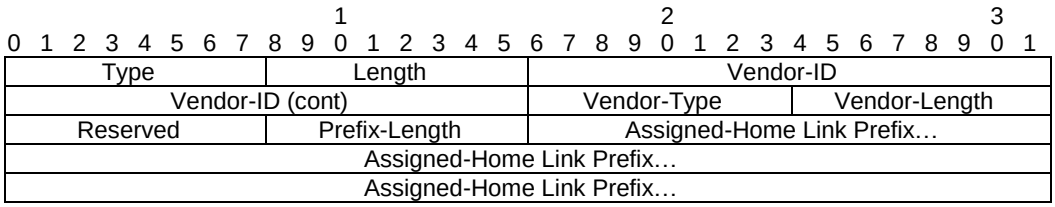


Figure 20 **MIP6 Home Link Prefix (Attribute A) VSA**

Type: 26

Length > 10

Vendor ID: 5535

Vendor-Type = 128

Vendor-Length > 4

Reserved = All bits set to 0.

Prefix-Length =

This field indicates the prefix length of the Home Link.

Assigned Home Link Prefix:

Home Link Prefix (upper order bits) that is assigned to the MN. If the Home Link Prefix length is not an integral multiple of 8, additional lower order bits of zeros are appended by the sender to make this field octet-aligned. The actual number of bits in the Home Link Prefix is indicated by the Prefix-Length field.

4.48 Maximum Authorized Aggregate Bandwidth for Best-Effort Traffic

Indicates the maximum bandwidth that may be allocated to a user for best-effort traffic. This VSA may be included in a RADIUS Access-Accept message:

Type: 26

Length = 12

Vendor ID: 5535

Vendor-Type = 130

Vendor-Length = 6

Vendor-Value:

1 – 2**32 (binary value of the maximum allowed aggregate bandwidth for the user, in bits per second)

4.49 Authorized Flow Profile IDs for the User

This is a list of Flow Profile IDs that the user is allowed to specify/request in a QoS Sub Blob. This VSA may be included in a RADIUS Access-Accept message:

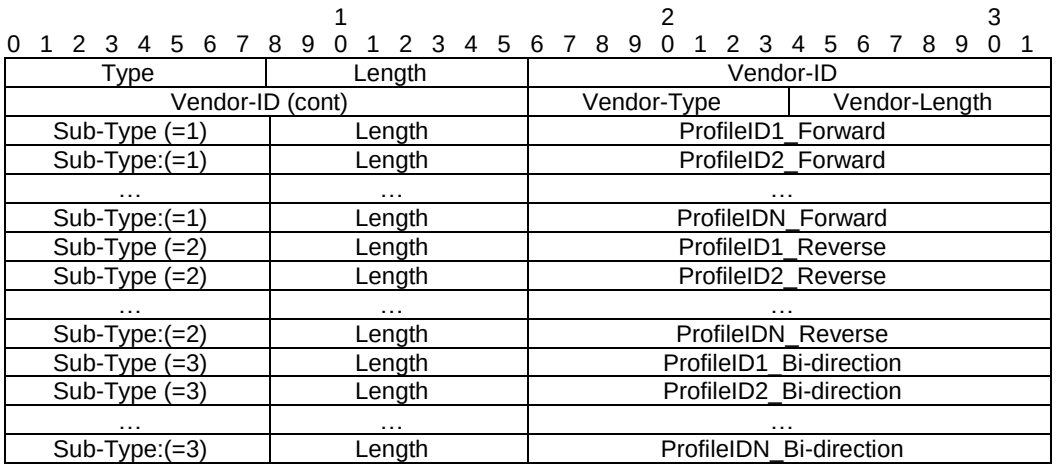


Figure 21 **Authorized Flow Profile IDs for the User VSA**

Type: 26

Length >= 12

Vendor ID: 5535

Vendor-Type = 131

Vendor-Length >= 6

Sub-Type (=1):

Repeats 0 or more times. Each instance contains a QoS profile id that the user is allowed to request in the forward direction.

Length: 4

Vendor-Value:

Represents the QoS profile_id for the QoS Profiles the user is allowed to request in the forward direction.

Sub-Type (=2):

Repeats 0 or more times. Each instance contains a QoS profile id that the user is allowed to request in the reverse direction.

Length: 4

Vendor-Value:

Represents the QoS profile_id for the QoS Profiles the user is allowed to request in the reverse direction.

Sub-Type (=3):

Repeats 0 or more times. Each instance contains a QoS profile id that the user is allowed to request in the reverse direction.

Length: 4

Vendor-Value:

Represents the QoS profile_id for the QoS Profiles the user is allowed to request in bi-directionally.

4.50 Granted QoS Parameters

Granted QoS Parameters received from the RAN for the flow identified by FLOW_ID and direction. May be included in RADIUS Accounting messages.

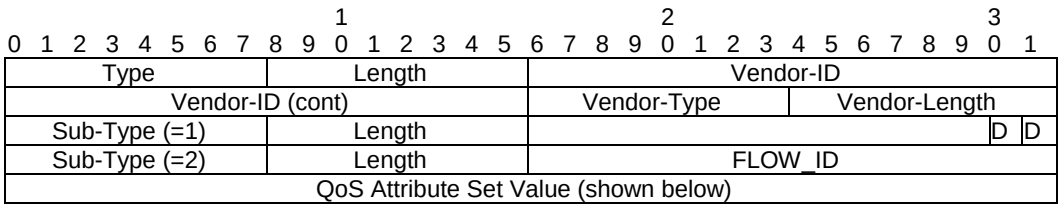


Figure 22 **Granted QoS Parameters VSA**

Granted QoS_Attribute _Set Value:

QoS_Attribute_Set for a flow given by attribute i5 of the same UDR. The value can be either verbose or non-verbose. For detail of individual field, see QOS_ATTRIBUTE_SET in Chapter 4, Annex E.

Non-verbose Value:

Sub-Type (=3)	Length	QoS_ATTRIBUTE_SET_ID
Sub-Type (=4)	Length	FlowProfileID

Verbose Value:

Sub-Type (=3)	Length	QoS_ATTRIBUTE_SET_ID
Sub-Type (=5)	Length	Traffic_Class
Sub-Type (=6)	Length	Peak_Rate
Sub-Type (=7)	Length	Bucket_Size
Sub-Type (=8)	Length	Token_Rate
Sub-Type (=9)	Length	Max_Latency
Sub-Type (=10)	Length	Max_IP_Packet_Loss_Rate
Sub-Type (=11)	Length	Packet_Size
Sub-Type (=12)	Length	Delay_Var_Sensitive

Type: 26

Length: 22 or 50

Vendor ID: 5535

Vendor-Type = 132

Vendor-Length: 16 or 44

Sub-Type (=1): Direction

Length: 4

Vendor-Value:

This field shall be set to follows:

‘00’ if this TFT is sent for Forward Direction

‘01’ if this TFT is sent for Reverse Direction.

‘10’ if this TFT is sent for both Forward and Reverse Direction.

‘11’ Reserved.

Sub-Type (=2): FLOW_ID

Length: 4

Vendor-Value:

This field shall be set to a unsigned short value (16-bit) that identifies an IP flow.

Sub-Type (=3): QoS_ATTRIBUTE_SET_ID

Length: 4

Vendor-Value:

This field shall be set to the identifier for the QoS_ATTRIBUTE_SET.

Sub-Type (=4): FlowProfileID

Length: 4

Vendor-Value:

This field shall be set to the FlowProfileID that represents the application using the IP flow.

Sub-Type (=5): Traffic_Class

Length: 4

Vendor-Value:

This field shall be set to indicate the traffic class as specified in chapter 4 Annex E.

Sub-Type (=6): Peak_Rate

Length: 4

Vendor-Value: unsigned (0 to 65535)

This field shall be set to indicate the peak rate, in units of 256 bytes per second.

Sub-Type (=7): Bucket_Size

Length: 4

Vendor-Value: unsigned (0 to 65535)

This field shall be set to indicate the token bucket size, in units of 256 bytes.

Sub-Type (=8): Token_Rate

Length: 4

Vendor-Value: unsigned (0 to 65535)

This field shall be set to indicate the token rate, in units of 256 bytes per second.

Sub-Type (=9): Max_Latency

Length: 4

Vendor-Value: unsigned (0 to 255)

This field shall be set to indicate the maximum latency, in units of 10 milliseconds.

Sub-Type (=10): Max_IP_Packet_Loss_Rate

Length: 4

Vendor-Value: unsigned (0 to 31)

This field shall be set to indicate the maximum IP packet loss rate.

Sub-Type (=11): Packet_Size

Length: 4

Vendor-Value: unsigned (0 to 255)

This field shall be set to indicate the median packet size, in units of 8 bytes.

Sub-Type (=12): Delay_Var_Sensitive

Length: 4

Vendor-Value: unsigned (0 or 1)

This field shall be set to 1 if traffic flow is sensitive to variation in delay. Or set to 0 to indicate the traffic flow sensitivity to variation in delay is not specified.

4.51 Maximum Per Flow Priority for the User

Indicates the maximum priority that may be assigned to a user's packet flow.

Type: 26

Length = 12

Vendor ID: 5535

Vendor-Type = 133

Vendor-Length = 6

Vendor-Value:

Integer - low order 4 bits indicate the maximum priority that the user can specify for a packet data flow. Priority 15 is the highest and 0 is the lowest. Specifically:

- 0000-0111: Priority 0 to 7 for regular users.
- 1000-1111: Priority 8 to 15 for Reserved Class.

4.52 MIP6-Authenticator

This VSA carries the MN-AAA authenticator obtained from the MN-AAA authentication mobility option in the BU. This VSA appears in the RADIUS Access-Request message from the HA to the Home RADIUS server.

Type: 26

Length > 8

Vendor ID: 5535

Vendor-Type = 134

Vendor-Length > 2

Vendor-Value:

The MN-AAA authenticator

4.53 MIP6-MAC-Mobility-Data

This VSA carries the hashed Mobility Data from the HA to the Home RADIUS server so that the Home RADIUS server can validate the MN-AAA authenticator. It may be included in a RADIUS Access-Request message from the HA to the Home RADIUS server.

Type: 26

Length > 8

Vendor ID: 5535

Vendor-Type = 138

Vendor-Length > 2

Vendor-Value:

SHA-1 (care-of address | home address | MH Data) followed by the Identification field in the identification mobility option.

4.54 Inter-User Priority

Indicates the inter-user priority that may be assigned to a user's packet flow on the main service connection/main link flow.

Type: 26

Length = 12

Vendor ID: 5535

Vendor-Type = 139

Vendor-Length = 6

Vendor-Value:

Integer - low order 3 bits indicate the inter-user priority used for scheduling packets for data flow on the main service instance/main link flow. Priority 7 is the highest and 0 is the lowest. Specifically:

- 000-011: Priority 0 to 3 for regular users.
- 100-111: Priority 4 to 7 for Reserved Class.

4.55 MIP6-Home Agent (Attribute B)

This VSA carries the assigned Home Agent's IPv6 address during MIP6 bootstrapping. The VSA is included in a RADIUS Access-Accept message from the Home RADIUS server to the PDSN.

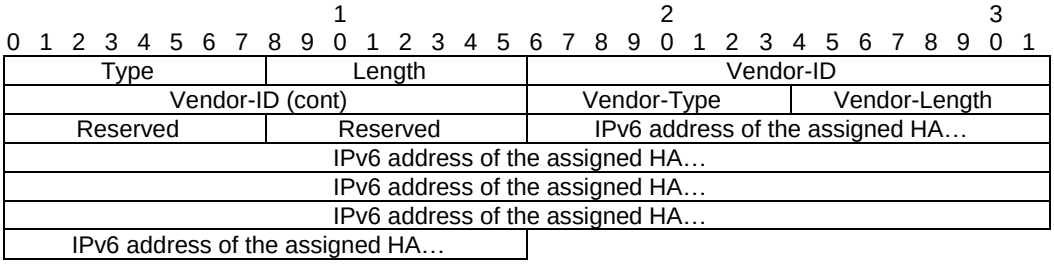


Figure 23 **MIP6 Home Agent (Attribute B) VSA**

Type: 26

Length = 26

Vendor ID: 5535

Vendor-Type = 140

Vendor-Length = 20

Reserved = All bits set to 0.

IPv6 address of the assigned HA:

128-bit IPv6 address of the assigned Home Agent.

4.56 MIP6-HoA (received from BU)

This VSA carries the IPv6 HoA extracted from the Binding Update message. The VSA is included in a RADIUS Access-Request message from the HA to the Home RADIUS Server.

Type: 26

Length = 24

Vendor ID: 5535

Vendor-Type = 141

Vendor-Length = 18

Vendor-Value:

IPv6 Home Address.

4.57 FLOW_ID Parameter

Identifies IP flow. This VSA may appear in a RADIUS Accounting message (stop).

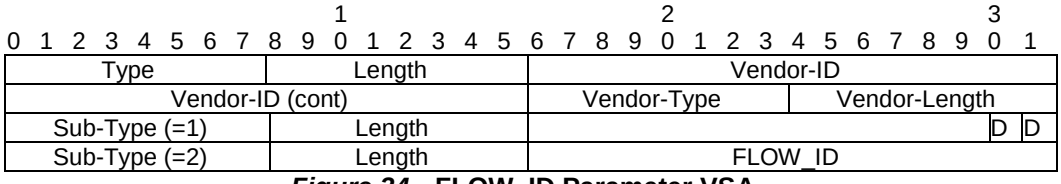


Figure 24 **FLOW_ID Parameter VSA**

Type: 26

Length = 16

Vendor ID: 5535

Vendor-Type = 144

Vendor-Length = 10

Sub-Type (=1): D

Length: 4

Vendor-Value:

This field shall be set to follows:

‘00’ if this attribute is sent for Forward Direction

‘01’ if this attribute is sent for Reverse Direction.

‘10’ if this attribute is sent for both Forward and Reverse Direction.

‘11’ Reserved.

Sub-Type (=2): FLOW_ID

Length: 4

Vendor-Value:

This field shall be set to a unsigned short value (16-bit) that identifies an IP flow.

4.58 Flow Status

Identifies IP flow status. This VSA may appear in a RADIUS Accounting message (stop).

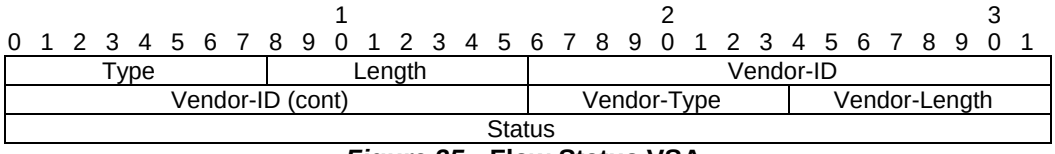


Figure 25 **Flow Status VSA**

Type: 26

Length = 12

Vendor ID: 5535

Vendor-Type = 145

Vendor-Length = 6

Status:

This field shall be set to ‘0’ if the IP flow continues to remain active; otherwise, this field shall be set to ‘1’.

4.59 Filtered Octet Count (Terminating)

Appear in accounting interim and stops to report that number of octets that are being affected are being blocked or redirected away from the mobile due to Filtering and blocking rules and profiles received in AAA.

Type: 26

Length = 12

Vendor ID: 5535

Vendor-Type = 146

Vendor-Length = 6

Vendor-Value:

Unsigned integer indicating the number of octets that were filtered from the Mobile or redirected away from the mobile due to any filtering or redirection rules or profiles received from RADIUS in Access-Request and COA packets.

4.60 Filtered Octet Count (Originating)

Appear in accounting interim and stops to report that number of octets originating at the mobile that are being affected are being blocked or redirected due to Filtering and blocking rules and profiles received in AAA.

Type: 26

Length = 12

Vendor ID: 5535

Vendor-Type = 147

Vendor-Length = 6

Vendor-Value:

Unsigned integer indicating the number of octets that were filtered from the Mobile or redirected away from the mobile due to any filtering or redirection rules or profiles received from the RADIUS in Access-Request and COA packets.

4.61 GMT- Time-Zone-Offset

This VSA contains the time offset at the PDSN from GMT time.

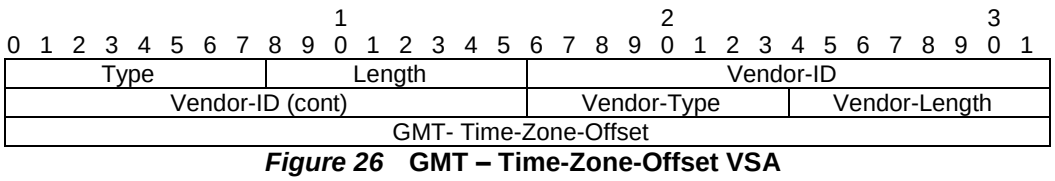


Figure 26 **GMT – Time-Zone-Offset VSA**

Type: 26

Length: 12

Vendor ID: 5535

Vendor-Type: 143

Vendor-Length: 6

Value:

GMT- Time-Zone-Offset is 4-octet string that is interpreted as a 4-byte signed integer that indicates the current offset in seconds from GMT at the visited carrier's PDSN. The offset shall be adjusted to reflect standard-time or day light saving time.

4.62 Carrier-ID

This VSA identifies the visited operator that generated the UDR.

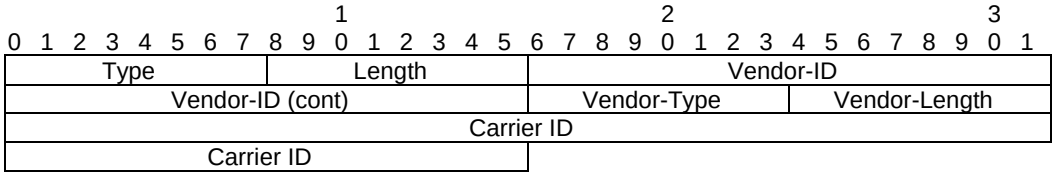


Figure 27 **Carrier-ID VSA**

Type: 26

Length: 13 or 14

Vendor ID: 5535

Vendor-Type: 142

Vendor-Length: 7 or 8

Visited Carrier ID:

A 5 or 6-byte Identifier of the visited PDSN comprising of a 3 byte Mobile Country Code (MCC) followed by a 2 or 3 byte Mobile Network Code (MNC) of the visited carrier. This value is configured locally in the visited carrier's PDSN.

4.63 MIP6-Mesg-ID

Appears in an Access-Request message. The value which this attribute contains comes from the Mobility message replay protection option and is used by the RADIUS server to compute the value of MIP6-Session Key

Type: 26

Length = 16

Vendor ID: 5535

Vendor-Type: 123

Vendor-Length = 10

Vendor-Value:

This octet-string field carries the 64 bit timestamp found in the Mobility message replay protection option with option type set to MESG-ID-OPTION-TYPE.

4.64 RSVP Inbound Octet Count

Appear in accounting interim and stop records to report that number of octets originating at the mobile that are associated with RSVP signaling.

Type: 26

Length = 12

Vendor ID: 5535

Vendor-Type = 162

Vendor-Length = 6

Vendor-Value:

Unsigned integer indicating the number of octets that were sent by the mobile as part of RSVP signaling

4.65 RSVP Outbound Octet Count

Appear in accounting interim and stop record to report that number of octets sent to the mobile that are associated with RSVP signaling.

Type: 26

Length = 12

Vendor ID: 5535

Vendor-Type = 163

Vendor-Length = 6

Vendor-Value:

Unsigned integer indicating the number of octets associated with RSVP signaling that were sent to the Mobile.

4.66 RSVP Inbound Packet Count

Appear in accounting interim and stop record to report that number of packets originating at the mobile that are associated with RSVP signaling.

Type: 26

Length = 12

Vendor ID: 5535

Vendor-Type = 164

Vendor-Length = 6

Vendor-Value:

Unsigned integer indicating the number of packets that were sent by the mobile as part of RSVP signaling.

4.67 RSVP Outbound Packet Count

Appear in accounting interim and stop record to report that number of packets sent to the mobile that are associated with RSVP signaling.

Type: 26

Length = 12

Vendor ID: 5535

Vendor-Type = 165

Vendor-Length = 6

Vendor-Value:

Unsigned integer indicating the number of packets that were sent to the mobile as part of RSVP signaling.

4.68 MIP6-HA-Local-Assignment-Capability

This VSA indicates that the PDSN supports local HA assignment function, and requests the authorization to assign a HA for the MS in the visited domain. The PDSN may include this VSA in the RADIUS Access-Request message during Access Authentication procedure for the MS.

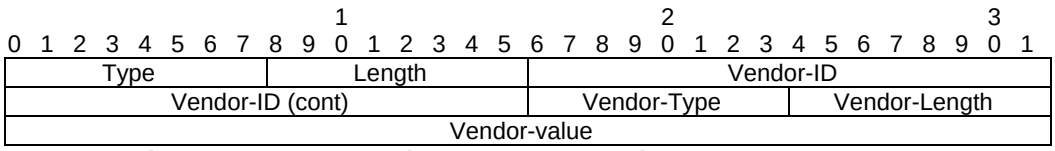


Figure 28 **MIP6-Local-Home-Agent-Assignment-Request VSA**

Type: 26

Length = 12

Vendor ID: 5535

Vendor-Type = 179

Vendor-Length = 6

Vendor-Value:

1: The PDSN indicates its ability to assign a HA in the visited network for the MS

Other values are reserved

4.69 HAAA-MIP6-HA-Protocol-Capability-Indication

This 3GPP2-specific VSA indicates the protocol supported by the HA for MIP6 signaling security. The HAAA may include this VSA in RADIUS Access-Accept message during Access Authentication procedure for the MS.

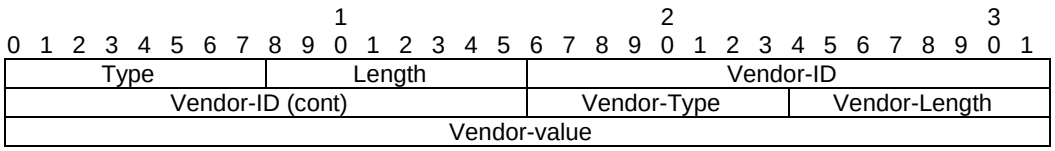


Figure 29 **HAAA-MIP6-HA-Protocol-Capability-Indication VSA**

Type: 26

Length = 12

Vendor ID: 5535

Vendor-Type = 203

Vendor-Length = 6

Vendor-Value:

1: MIP6 HA supports Authentication protocol specified by RFC 4285 for MIP6 signaling security

Other values are reserved

4.70 VAAA-Assigned-MIP6-HA

This 3GPP2-specific VSA conveys an HA address selected by the VAAA. This VSA may be included in the RADIUS Access-Accept message sent from the VAAA to the PDSN. This attribute is not allowed to be sent from the HAAA to the VAAA.

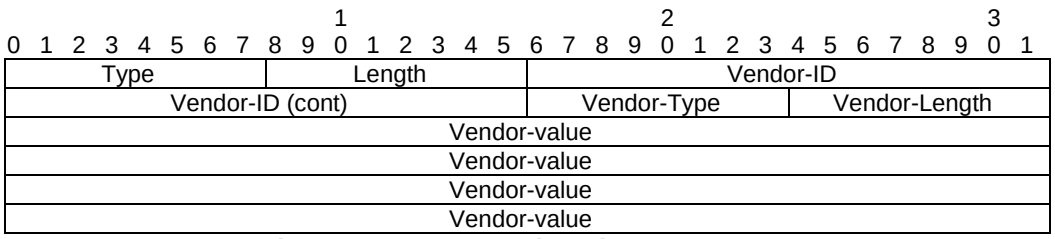


Figure 30 **VAAA-Assigned-MIP6-HA VSA**

Type: 26

Length = 24

Vendor ID: 5535

Vendor-Type = 205

Vendor-Length = 18

Vendor-Value:

128-bit HA address

4.71 VAAA-Assigned-MIP6-HL

This VSA carries the assigned Home Link Prefix during MIP6 bootstrapping. The VSA is included in a RADIUS Access-Accept message from the Visited RADIUS server to the PDSN. This attribute is not allowed to be sent from the HAAA to the VAAA.

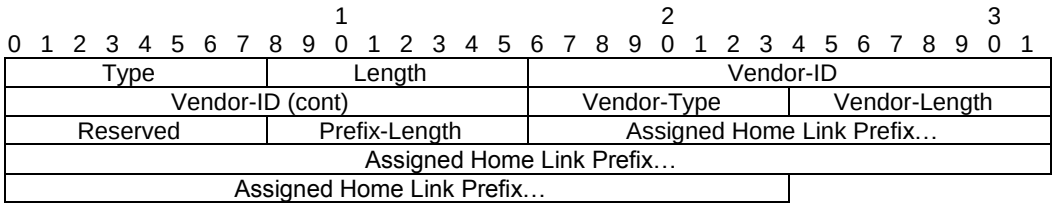


Figure 31 **VAAA-Assigned-MIP6-HA VSA**

Type: 26

Length > 10

Vendor ID: 5535

Vendor-Type = 206

Vendor-Length > 4

Reserved = All bits set to 0.

Prefix-Length =

This field indicates the prefix length of the Home Link.

Assigned Home Link Prefix:

> Home Link Prefix (upper order bits) that is assigned to the MN. If the Home Link Prefix length is not an integral multiple of 8, additional lower order bits of zeros are appended by the sender to make this field octet-aligned. The actual number of bits in the Home Link Prefix is indicated by the Prefix-Length field.

4.72 VAAA-MIP6-HA-Protocol-Capability-Indication

This 3GPP2-specific VSA indicates the protocol supported by the HA for MIP6 signaling security. The VAAA may include this VSA in RADIUS Access-Accept message sent to the PDSN during Access Authentication procedure for the MS. This attribute is not allowed to be sent from the HAAA to the VAAA.

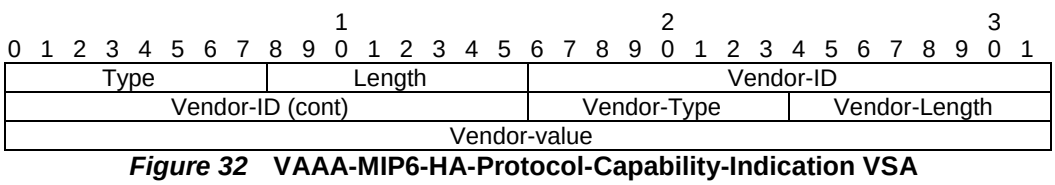


Figure 32 **VAAA-MIP6-HA-Protocol-Capability-Indication VSA**

Type: 26

Length = 12

Vendor ID: 5535

Vendor-Type = 207

Vendor-Length = 6

Vendor-Value:

1: MIP6 HA supports Authentication protocol specified by RFC 4285 for MIP6 signaling security

Other values are reserved

4.73 DNS-Server-IPv6-Address

This VSA may be present in a RADIUS Access-Accept message. It includes a Primary and a Secondary DNS Server IPv6 Addresses.

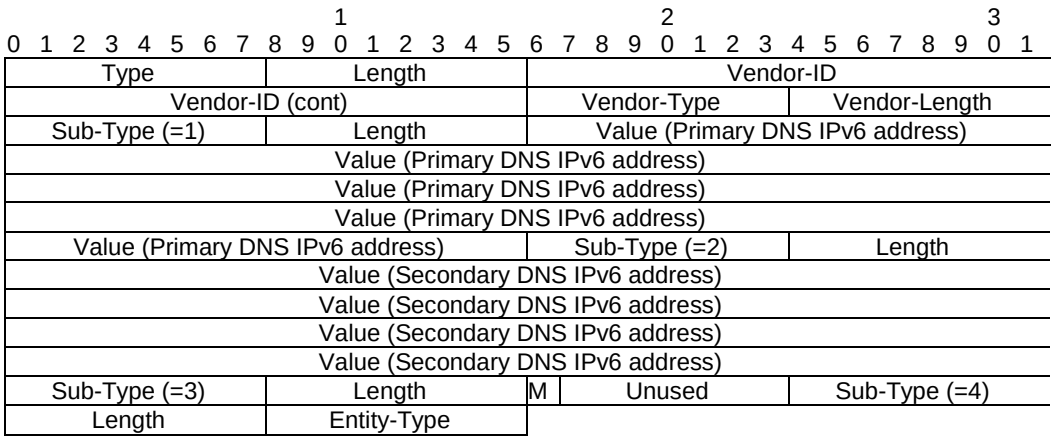


Figure 33 **DNS-Server-IPv6-Address VSA**

Type: 26

Length: 50

Vendor ID: 5535

Vendor-Type: 214

Vendor-Length: 44

Sub-Type (=1):

Length: (=18 octets)

Vendor-Value:

Primary DNS Server IPv6 Address.

Sub-Type (=2):

Length: (= 18 octets)

Vendor-Value:

Secondary DNS Server IPv6 Address.

Sub-Type (=3): Flag

Length: (=3 octet)

Vendor-Value:

M" bit set to 1 indicates to the HA that the Primary and Secondary DNS IPv6 addresses provided by the Home RADIUS server shall override the Primary and Secondary DNS addresses if provided also by the Visited RADIUS server.

Sub-Type (=4):

Length: (=3 octet)

Vendor-Value:

Entity-Type" The network entity that inserted in the DNS Server IPv6 Address. Currently the following types are defined:

HAAA = 1

VAAA = 2

5 RADIUS Attributes Table

The following table [19] provides a guide to the IETF RADIUS attributes and 3GPP2 vendor specific attributes that may be found in the RADIUS Access-Request, RADIUS Access-Accept messages and RADIUS Accounting-Request messages (following the RADIUS standard approach). The VSA types with vendor ID 5535 are reserved and shall only be allocated by published 3GPP2 specifications. The entries in the table are defined as follows:

0	This attribute shall not be present.
0+	Zero or more instances of this attribute may be present.
0-1	Zero or one instance of this attribute may be present.
1	Exactly one instance of this attribute shall be present.

Table 7 **List of used RADIUS Attributes**

Attribute	Type	Access-Request	Access-Accept	Accounting-Start	Accounting-Stop	Accounting-Interim-Update
User-Name	1	1	0-1	1	1	1
User-Password	2	0-1	0	0	0	0
HAP-Password	3	0-1	0	0	0	0
NAS-IP Address	4	0-1	0	0-1	0-1	0-1
Service-Type	6	0-1	0	0	0	0
Framed-IP-Address	8	0-1	0-1	1	1	1
Class	25	0	0-1	0-1	0-1	0-1
Session-Timeout	27	0	0-1	0	0	0
Idle-Timeout	28	0	0-1	0	0	0
Calling-Station-ID	31	1	0	1	1	1
NAS-Identifier	32	0-1	0	0-1	0-1	0-1
Acct-Delay-Time	41	0	0	1	1	1
Acct-Input-Octets	42	0	0	0	1	1
Acct-Output-Octets	43	0	0	0	1	1
Account-Session-ID	44	0	0	1	1	1
Event-Timestamp	55	0	0	1	1	1
CHAP Challenge	60	0-1	0	0	0	0
NAS-Port-Type	61	0-1	0	0-1	0-1	0-1
Message-Authenticator	80	0-1	0-1	0	0	0
Acct-Interim-Interval	85	0	0-1	0	0	0
NAS-IPv6 address	95	0-1	0	0-1	0-1	0-1
Framed-Interface-ID	96	0-1	0-1	0-1	0-1	0-1
Framed-IPv6-Prefix	97	0-1	0-1	0-1	0-1	0-1

[19] See [Chapter 6] for attributes of PrePaid Accounting.

Attribute	Type	Access-Request	Access-Accept	Accounting-Start	Accounting-Stop	Accounting-Interim-Update
IKE Pre-shared Secret Request	26/01	0-1	0	0	0	0
Security Level	26/02	0	0-1	0	0	0
Pre-shared Secret	26/03	0	0-1	0	0	0
Reverse Tunnel Specification	26/04	0	0-1	0	0	0
Differentiated Services Class Option	26/05	0	0-1	0	0	0
Container	26/06	0	0	0	0+	0+
Home Agent	26/07	0-1	0-1	0-1	0-1	0-1
KeyID	26/08	0	0-1	0	0	0
Serving PCF	26/09	0	0	1	1	1
BSID	26/10	0	0	1	1	1
User Zone	26/11	0	0	0-1	0-1	0-1
Forward Mux Option	26/12	0	0	0-1	0-1	0-1
Reverse Mux Option	26/13	0	0	0-1	0-1	0-1
Service Option	26/16	0-1	0	1	1	1
Forward Traffic Type	26/17	0	0	0-1	0-1	0-1
Reverse Traffic Type	26/18	0	0	0-1	0-1	0-1
Fundamental Frame Size	26/19	0	0	0-1	0-1	0-1
Forward Fundamental RC	26/20	0	0	0-1	0-1	0-1
Reverse Fundamental RC	26/21	0	0	0-1	0-1	0-1
IP Technology	26/22	0-1	0	1	1	1
Compulsory Tunnel Indicator	26/23	0	0-1	0-1	0-1	0-1
Release Indicator	26/24	0	0	0	1	0
Bad PPP Frame Count	26/25	0	0	0	0-1	0-1
Number of Active Transitions	26/30	0	0	0	1	1
SDB Octet Count (Terminating)	26/31	0	0	0	0-1	0-1
SDB Octet Count (Originating)	26/32	0	0	0	0-1	0-1
Number of SDBs (Terminating)	26/33	0	0	0	0-1	0-1
Number of SDBs (Originating)	26/34	0	0	0	0-1	0-1
IP Quality of Service	26/36	0	0	0-1	0-1	0-1
Airlink Priority[20]	26/39	0	0	0	0	0
Airlink Record Type[21]	26/40	0	0	0	0	0
Airlink Sequence Number[21]	26/42	0	0	0	0	0
Number of HDLC layer bytes received	26/43	0	0	0	0-1	0-1
Correlation ID	26/44	1	0-1	1	1	1

[20] The attribute is used over the A10 interface in Airlink Records, they are not sent to the Home RADIUS server in Accounting Records.

Attribute	Type	Access-Request	Access-Accept	Accounting-Start	Accounting-Stop	Accounting-Interim-Update
Mobile Originated / Mobile Terminated Indicator[21]	26/45	0	0	0	0	0
Inbound MIP Signaling Octet Count	26/46	0	0	0	0-1	0-1
Outbound MIP Signaling Octet Count	26/47	0	0	0	0-1	0-1
Session Continue	26/48	0	0	0	1	0-1
Active Time	26/49	0	0	0	0-1	0-1
DCCH Frame Format	26/50	0	0	0-1	0-1	0-1
Beginning Session	26/51	0	0	0-1	0	0
ESN	26/52	0	0	0-1	0-1	0-1
'S' Key	26/54	0	0-1	0	0	0
'S' Request	26/55	0-1	0	0	0	0
'S' Lifetime	26/56	0	0-1	0	0	0
MN-HA SPI	26/57	0-1	0	0	0	0
MN-HA Shared Key	26/58	0	0-1	0	0	0
Remote Ipv4 Address	26/59	0	0+	0	0	0
Reserved[21]	26/60-69	-	-	-	-	-
Remote Ipv6 Address	26/70	0	0+	0	0	0
Remote Address Table Index	26/71	0	0+	0	0	0
Remote IPv4 Address Octet Count	26/72	0	0	0	0+	0+
Allowed Differentiated Services Marking	26/73	0	0-1	0	0	0
Service Option Profile	26/74	0	0-1	0	0	0
DNS-Update- Required	26/75	0	0-1	0	0	0
Always On	26/78	0	0-1	0-1	0-1	0-1
Foreign Agent Address	26/79	0-1	0	0	0	0
Last User Activity Time	26/80	0	0	0	0-1	0-1
MN-AAA Removal Indication	26/81	0	0-1	0	0	0
RAN Packet Data Inactivity Timer	26/82	0	0-1	0	0	0
Forward PDCH RC	26/83	0	0	0-1	0-1	0-1
Forward DCCH Mux Option	26/84	0	0	0-1	0-1	0-1
Reverse DCCH Mux Option	26/85	0	0	0-1	0-1	0-1
Forward DCCH RC	26/86	0	0	0-1	0-1	0-1
Reverse DCCH RC	26/87	0	0	0-1	0-1	0-1
Session Termination Capability	26/88	1	1	0	0	0
Allowed Persistent TFTs	26/89	0	0-1	0	0	0

[21] Reserved for RAN usage.

Attribute	Type	Access-Request	Access-Accept	Accounting-Start	Accounting-Stop	Accounting-Interim-Update
PrePaidAccounting Quota (PPAQ)	26/90	0	0-1	0	0	0
PrePaidAccounting Capability (PPAC)	26/91	0-1	0-1	0	0	0
MIP Lifetime	26/92	0-1	0-1	0	0	0
Accounting-Stop-triggered-by-Active-Stop-Indication	26/93	0	0-1	0	0	0
Service Reference ID	26/94	0-1	0	1	1	1
DNS-Update-Capability	26/95	0-1	0	0	0	0
Remote IPv6 Address Octet Count[22]	26/97	0	0	0	0+	0+
PrePaidTariffSwitch (PTS)	26/98	0	0-1	0	0	0
Reverse PDCH_RC	26/114	0	0	0-1	0-1	0-1
MEID	26/116	0	0	0-1	0-1	0-1
DNS Server IP Address	26/117	0	0+	0	0	0
MIP6-Home Agent (received from BU)	26/118	0-1	0	0	0	0
MIP6-CoA	26/119	0-1	0	0-1	0	0-1
MIP6-HoA-Not-Authorized	26/120	0	0-1	0	0	0
MIP6-Session Key	26/121	0	0+	0	0	0
MIP6-Home Link Prefix (Attribute A)	26/128	0	0-1	0	0	0
Maximum Authorized Aggregate Bandwidth for Best-Effort Traffic	26/130	0	0-1	0	0	0
Authorized Flow Profile IDs for the User	26/131	0	0-1	0	0	0
Granted QoS Parameters	26/132	0	0	0+	0+	0+
Maximum Per Flow Priority for the User	26/133	0	0-1	0	0	0
MIP6-Authenticator	26/134	0-1	0	0	0	0
MIP6-MAC-Mobility-Data	26/138	0-1	0	0	0	0
Inter-User Priority	26/139	0	0-1	0	0	0
MIP6-Home Agent (Attribute B)	26/140	0	0-1	0	0	0
MIP6-HoA (received from BU)	26/141	0-1	0	0-1	0	0-1
FLOW_ID Parameter	26/144	0	0	0	0-1	0
Flow Status	26/145	0	0	0	0-1	0
Filtered Octet Count (Originating)	26/147	0	0	0	0-1	0-1

[22] Previous version of this document used 26/80 as a value type for the Remote IPv6 Address Count VSA. This version of the standard changed the VSA type to 26/97, because 26/80 has been assigned to G17 (Last User Activity Time) currently deployed by the cdma2000 wireless industry.

Attribute	Type	Access-Request	Access-Accept	Accounting-Start	Accounting-Stop	Accounting-Interim-Update
Filtered Octet Count (Terminating)	26/146	0	0	0	0-1	0-1
Carrier-ID	26/142	0-1	0	0-1	0-1	0-1
GMT-Time-Zone- Offset	26/143	0-1	0	0-1	0-1	0-1
MIP6-Mesg-ID	26/123	0-1	0	0	0	0
RSVP Inbound Octet Count	26/162	0	0	0	0-1	0-1
RSVP Outbound Octet Count	26/163	0	0	0	0-1	0-1
RSVP Inbound Packet Count	26/164	0	0	0	0-1	0-1
RSVP Outbound Packet Count	26/165	0	0	0	0-1	0-1
Accounting-Mode	26/198	0	0-1	0	0	0
MIP6-HA-Local-Assignment-Capability	26/179	0-1	0	0	0	0
IP-Services-Authorized	26/185	0	0-1	0	0	0
HAAA-MIP6-HA-Protocol-Capability-Indication	26/203	0	0-1	0	0	0
VAAA-Assigned-MIP6-HA	26/205	0	0-1	0	0	0
VAAA-Assigned-MIP6-HL	26/206	0	0-1	0	0	0
VAAA-MIP6-HA-Protocol-Capability-Indication	26/207	0	0-1	0	0	0
DNS-Server-IPv6-Address	26/214	0	0+	0	0	0

6 RADIUS Disconnect Attributes Table

The following table provides a guide to the RADIUS attributes found in the RADIUS Disconnect-Request, RADIUS Disconnect-ACK and RADIUS Disconnect-NAK messages. The entries in the table are defined as follows:

0	This attribute shall not be present.
0+	Zero or more instances of this attribute may be present.
0-1	Zero or one instance of this attribute may be present.
1	Exactly one instance of this attribute shall be present.

Table 8 **Attributes of RADIUS Disconnect messages**

Attribute	Type	Disconnect-Request	Disconnect-Ack
Correlation ID	26/44	0-1	0
User-Name	1	1	0
Framed-IP address	8	0-1	0
Calling-Station ID	31	0-1	0
DisconnectReason	26/96	0-1	0
NAS-Identifier	32	1	0
MIP6-CoA (Note 1)	26/119	0-1	0
Framed-IPv6-Prefix	97	0-1	0
Framed-Interface-ID	96	0-1	0

Note 1: Required for MIP6

7 Hot-Line RADIUS Attributes

The following table provides a guide to the additional RADIUS attributes that are needed to support Hot-Lining. The entries in the table are defined as follows:

0	This attribute shall not be present.
0+	Zero or more instances of this attribute may be present.
0-1	Zero or one instance of this attribute may be present.
1	Exactly one instance of this attribute shall be present.

Table 9 **Hot-Line Attributes**

Attribute	Type	Access-Request	Access-Accept	Change of Authorization	Accounting messages
FIlter-Id	11	0	0+	0+	0
Hot-Line Accounting Indication (Note 1) (Note 2)	26/122	0	0-1	0-1	0-1
Filter-Rule (Note 2)	26/124	0	0+	0+	0
HTTP-Redirection-Rule (Note 2)	26/125	0	0+	0+	0
IP Redirection Rule (Note 2)	26/126	0	0+	0+	0
Hot-Line Capability	26/127	0-1	0	0	0
Session-Timeout	27	0	0-1	0-1	0

Note 1: When the Hot-Line Accounting Indication appears in a RADIUS Access Accept or COA message then it shall also appear in subsequent Accounting Request (Start, Interim, and Stop) messages.

Note 2: When these attributes appear in a COA message they overwrite any previously received attributes of the same kind received in Access Accept or COA messages.

A Annex (Normative): Interim-Update RADIUS Accounting

A RADIUS Interim-Update Accounting record (with Acct-Status-Type = Interim-Update (3)) shall contain all of the attributes found in a RADIUS Accounting-Request (Stop) message with the exception of the Acct-Term-Cause and Release-Indicator attributes. The Session Continue attribute, if included, shall be set to 1. The values of the attributes in the RADIUS Interim-Update Accounting record shall be cumulative since the RADIUS Accounting-Request (Start) record.

Since the accounting information is cumulative, the PDSN shall ensure that only a single generation of an Interim-Update Accounting message for a given NAI and IP address is present in retransmission queues at any given time.

The PDSN may add a random delay between RADIUS Interim-Update Accounting messages for separate sessions. This will ensure that a cycle where all messages are sent at once is prevented.