3GPP2 X.S0011-005-C
Version: 1.0.0
Date: August 2003

3RD GENERATION PARTNERSHIP PROJECT 2 "3GPP2"

cdma2000 Wireless IP Network Standard: Accounting Services and 3GPP2 RADIUS VSAs

COPYRIGHT

3GPP2 and its Organizational Partners claim copyright in this document and individual Organizational Partners may copyright and issue documents or standards publications in individual Organizational Partner's name based on this document. Requests for reproduction of this document should be directed to the 3GPP2 Secretariat at secretariat@3gpp2.org. Requests to reproduce individual Organizational Partner's documents should be directed to that Organizational Partner. See www.3gpp2.org for more information.

Content

1 GLOSSARY AND DEFINITIONS 1

2 REFERENCES 2

3 ACCOUNTING 3

3.1 GENERAL 3
3.1.1 USAGE DATA RECORDS 3
3.1.2 REMOTE ADDRESS ACCOUNTING 3
3.1.3 ACCOUNTING AND FAST HANDOFF 5
3.1.4 ACCOUNTING ATTRIBUTE NOTATION 5
3.2 AIRLINK RECORDS 5
3.2.1 R-P CONNECTION SETUP AIRLINK RECORD 6
3.2.2 ACTIVE START AIRLINK RECORD 7
3.2.3 ACTIVE STOP AIRLINK RECORD 7
3.2.4 SDB AIRLINK RECORD 8
3.3 PDSN USAGE DATA RECORD (UDR) 8
3.4 ACCOUNTING FORMATS 10
3.5 PDSN PROCEDURES 14
3.5.1 R-P CONNECTION SETUP AIRLINK RECORD ARRIVES 15
3.5.2 PACKET DATA SESSION ESTABLISHMENT 16
3.5.3 PACKET DATA SESSION TERMINATION 16
3.5.4 USER DATA THROUGH PDSN 17
3.5.5 ACTIVE START AIRLINK RECORD ARRIVES 17
3.5.6 ACTIVE STOP AIRLINK RECORD ARRIVES 18
3.5.7 SDB AIRLINK RECORD ARRIVES 18
3.5.8 INTERIM-UPDATE RECORD TRIGGER 19
3.5.9 STOP RECORD TRIGGER 19
3.5.10 TIME OF DAY TIMER EXPIRES 19

4 3GPP2 RADIUS ATTRIBUTES 20

5 3GPP2 VSA TABLE 39

6 RADIUS DISCONNECT ATTRIBUTE TABLE 41

ANNEX A: INTERIM-UPDATE RADIUS ACCOUNTING 43

Figures

Figure 1. Accounting Architecture 3
Figure 2. Accounting Architecture With Fast Handoff 5
Figure 3. 3GPP2 RADIUS Attribute Format 20
Figure 4. Accounting Container VSA format 21
Figure 5. Remote IPv4 Address VSA format 23
Figure 6. Remote IPv6 Address VSA format 24
Figure 7. Remote Address Table Index VSA format 25
Figure 8. Remote IPv4 Address Octet Count format 26
Figure 9. Allowed Differentiated Services Marking VSA format 27
Figure 10. Service Option Profile VSA format 28
Figure 11. Allowed Persistent TFTs VSA format 30
Figure 12. PrePaidAccountingQuota (PPAQ) VSA format 30
Figure 13. PrePaidAccountingCapability (PPAC) VSA format 33
Figure 14. MIP Lifetime VSA format 33
Figure 15. Service Reference ID format 34
Figure 16. Remote IPv6 Address Octet Count VSA format 35
Figure 17. PrePaidTariffSwitch (PTS) VSA format 37

Tables

Table 1. R-P Connection Setup Airlink Fields 6
Table 2. Active Start Airlink Fields 7
Table 3. Active Stop Airlink Fields 8
Table 4. SDB Airlink Fields 8
Table 5. Complete UDR 10
Table 6. Accounting Parameter Attribute RADIUS Definitions 13
Table 7. Complete list of 3GPP2 VSAs 41
Table 8. Attributes of RADIUS Disconnect messages 42

General Description

This Chapter describes the off-line accounting procedures and the Usage Data Records. It describes all the 3GPP2 VSAs used to support the capabilities described in this series of specifications X.S0011-001-C to X.S0011-006-C.

1 Glossary and Definitions

See X.S0011-001-C.

2 References

See X.S0011-001-C.

3 Accounting

3.1 *General*

3.1.1 Usage Data Records

Packet Accounting parameters are divided into radio specific parameters collected by the RN, and IP network specific parameters collected by the Serving PDSN. The Serving PDSN shall merge radio specific parameters contained in R-P and P-P interface messages called Airlink Records with IP network specific ones 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 specification as is the summary, reconciliation, and billing process used by the carriers.

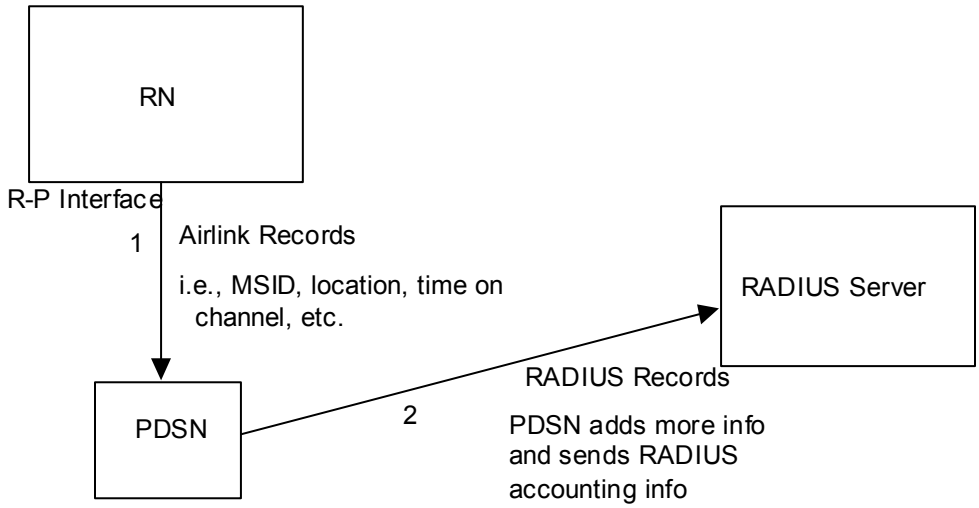


Figure 1. Accounting Architecture

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 access procedures.

The PDSN shall support the Remote IPv4/IPv6 Address 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 indicates multiple addresses to be used for

remote address accounting for the user[1]. The table indices specified by the Home RADIUS server point to 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 specification.

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 specification 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-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 specification.

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

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 RN 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 R-P session for each R-P connection. The Target PDSN shall update the copy of the Airlink Record received upon pre-setup of an R-P connection due to inter-PCF continuation of fast handoff on the Target PDSN (Figure 3, X.S0011-003-C).

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.

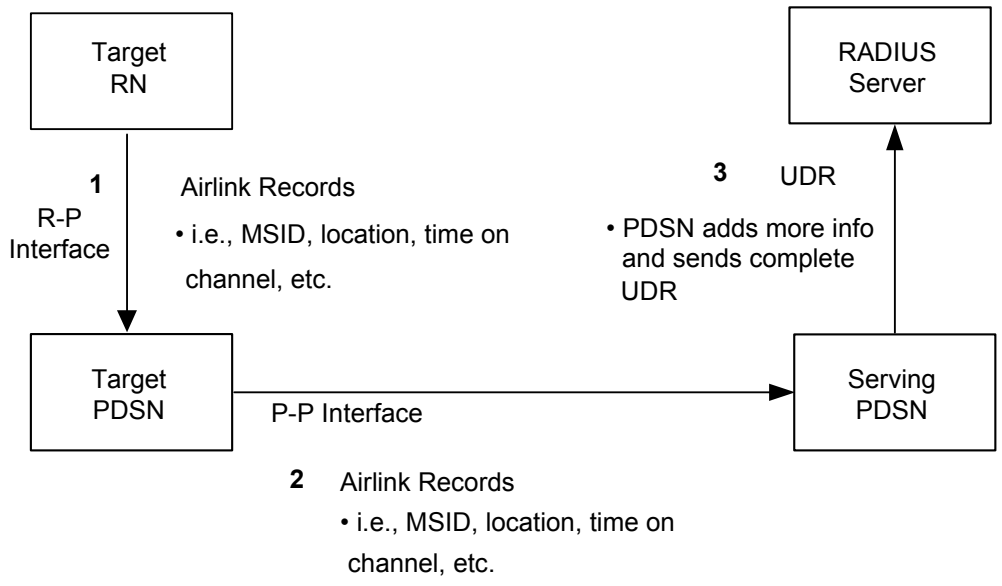


Figure 2. Accounting Architecture With Fast Handoff

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 RN generates one of four types of airlink records over the R-P interface:

- An R-P Connection Setup Airlink Record when the RN establishes an R-P connection.
- An Active Start Airlink Record when the MS has connected the associated over-the air service instance.

- An Active Stop Airlink Record when the MS has released the associated over-the-air service instance.
- A Short Data Burst (SDB) Airlink Record when a forward or reverse short data burst is exchanged with the MS.

The PCF uses the R-P Connection ID as the PCF Session Identifier Key in R-P setup messages.

All the airlink records shall include a sequence number initialized to zero at R-P connection setup. The sequence number is unique for a single identification triplet (R-P Connection ID, PCF ID, and MSID). Upon receiving the R-P connection setup airlink record, the Serving PDSN updates the UDR with the airlink record information and stores the sequence number. The PCF shall increment the sequence number modulo 256 in the subsequent airlink record transmitted over the corresponding R-P connection. The Serving PDSN shall compare the received sequence number with the previously stored sequence number (N). 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. If the received sequence number is in the range from (N-128) modulo 256 to (N-1) modulo 256, inclusive, the Serving PDSN shall ignore the message. The same procedure continues for all the subsequent airlink records, until the closing of the R-P 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 triplet is received. There should be only one outstanding unacknowledged airlink record at any given time.
When an R-P Connection Setup Airlink Record is received with a new R-P connection ID over an existing P-P connection, the serving PDSN shall start a new UDR for the new R-P connection as specified in section 3.5.1.

Detailed specifications of airlink records are in [4].

3.2.1 R-P Connection Setup Airlink Record

Table 1 contains fields present in the R-P Connection Setup airlink records.

Item	Parameter	Max Payload Length (octets)	Format
y1	Airlink Record Type = 1 (Connection Setup)	4	integer
y2	R-P Connection ID	4	integer
y3	Airlink Sequence Number	4	integer
a1	MSID	15	string
a2	ESN	15	string
d3	Serving PCF	4	ip-addr
d4	BSID	12	string

Table 1. R-P Connection Setup Airlink Fields

Each R-P connection and each airlink record is indexed via the R-P Connection ID.

3.2.2 Active Start Airlink Record

Table 2 contains fields present in Active Start airlink records.

Item	Parameter	Max Payload Length (octets)	Format
y1	Airlink Record Type = 2 (Active Start)	4	integer
y2	R-P Connection ID	4	integer
y3	Airlink Sequence Number	4	integer
e1	User Zone	4	integer
f1	Forward FCH Mux Option[2]	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
i4	Airlink Priority	4	integer

Table 2. Active Start Airlink Fields

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

f1 to f10, f14, f16 and f17 to f20 are fields from the cdma2000®[3] Service Configuration Record in [5-9].

3.2.3 Active Stop Airlink Record

Table 3 contains fields present in Active Stop Airlink Records.

Item	Parameter	Max Payload Length (octets)	Format
y1	Airlink Record Type = 3 (Active Stop)	4	integer
y2	R-P Connection ID	4	integer
y3	Airlink Sequence Number	4	integer
g8	Active Connection Time in Seconds	4	integer

[2] Forward/Reverse FCH Mux Option parameters correspond to the Forward/Reverse Mux Option parameters defined in the previous version of this specification.

[3] 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), cdma2000® is a registered trademark of the Telecommunications Industry Association (TIA-USA) in the United States.

Table 3. Active Stop Airlink Fields

3.2.4 SDB Airlink Record

Table 4 contains fields present in SDB Airlink Records.

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

Table 4. SDB Airlink Fields

3.3 *PDSN Usage Data Record (UDR)*

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

Item	Parameter	Description
A. Mobile Identifiers		
A1	MSID	MS ID (e.g., IMSI, MIN, IRM)
A2	ESN	Electronic Serial Number
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 R-P connection or P-P connection 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 R-P connection or P-P connection 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 RN in an A11 Registration-Request message.
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 RN.
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
E. Zone Identifiers		
E1	User Zone	Tiered Services user zone.
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 RN
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 Mobile IP.
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 characterized, 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 characterized, and spreading rates. [6]
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.
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 Mobile IP Signaling Octet Count	This is the total number of octets in registration requests and solicitations sent by the MS.
G16	Outbound Mobile IP 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.
I. Quality of Service		
I1	IP Quality of Service (QoS)	This attribute is deprecated.
I4	Airlink Priority	Identifies Airlink Priority associated with the user. This is the user's priority associated with the packet data service.
Y. Airlink Record Specific Parameters[4]		
Y1	Airlink Record Type	3GPP2 Airlink Record Type, see [4]
Y2	R-P Connection ID	Identifier for the R-P Connection. This is the GRE key that uniquely identifies an R-P connection (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 R-P 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 AVPs. This attribute is further described in section 4.

Table 5. Complete UDR

3.4 *Accounting Formats*

The RADIUS server shall support RADIUS attribute formats as defined in RFC 2865 and RFC 2866. The RN airlink records transmitted across the R-P 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 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 4 are included in Table 6.

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

		RADIUS Attribute Definitions				
Item	**Parameter**	**Type/ Vendor Type**	**Maximum Payload Length (in octets)**	**Format**	**Field**	**Special Values**
A. Mobile Identifiers						
A1	MSID	31	15	string	Calling-Station-Id	See [4].
A2	ESN	26/52	15	string	3GPP2_ESN	ASCII string of ESN. See [4].
B. User Identifiers						
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	Source 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 Identifiers						
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 4
D. Infrastructure 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 RN.
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
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].
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=Mobile IP
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=Mobile IP registration failure 5= Abnormal Terminations 6=Termination due to Resource management 7=Service instance released 8=VolumeQuota reached, Service instance released (use for PrePaid packet data service) 9=DurationQuota reached, Service instance 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
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]

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 4
G6	Remote IPv6 Address Octet Count	26/97	variable	octet string		See Section 4
G8	Active Time	26/49	4	integer	3GPP2_Active_Time	This is the active time reported by the RN 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 RN 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 RN 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 Mobile IP 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 Mobile IP 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.
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_Prioirty	Least significant 4 bits hold the priority associated with the packet data service.
Z. Container						
Z1	Container	26/6	Variable	string	3GPP2_Container	See Section 4

Table 6. Accounting Parameter Attribute RADIUS Definitions

3.5 *PDSN Procedures*

The following events cause the PDSN to take accounting action:

- Reception of R-P Connection Setup Airlink Record over R-P or P-P interface.
- R-P 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 Mobile IP).
- Data service termination on the PDSN. This includes releasing the PPP session, or release of a packet service session (Simple IP or Mobile IP).
- 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.

Each packet data session (i.e., Simple IP and/or Mobile IPv4 session) is identified with a Correlation ID provided to the HAAA at the time authentication/authorization is performed. Each individual Simple IPv4, Mobile IPv4, and Simple IPv6 session shall be accounted for independently. All UDR information is stored and transmitted per tuple of {assigned IPv4 address or IPv6 prefix, NAI, R-P connection ID}. 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 Mobile IP session, UDRs are created, modified, maintained, copied, and released for each individual connection. The Serving PDSN shall create one UDR per R-P connection ID. An R-P connection may be directly connected to the serving PDSN or indirectly connected via a P-P connection.

The PDSN closes a UDR when any of the following events occur:

- An existing R-P or P-P connection is closed.
- The PDSN determines the packet data session associated with the Correlation ID has ended.

At an initial R-P connection establishment, a UDR is created and initialized from relevant airlink records. When there is a new R-P or P-P connection due to a handoff for an existing packet data session, or when a new packet data session for an existing R-P or P-P connection is created, or when there is a new R-P connection for an existing packet data session, 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 RN to the new UDR associated with the new RN. Similarly, if the MS sends an LCP Configure-Request message over the main service instance to restart the PPP session, the PDSN copies R-P or P-P connection data (e.g., F1-F20) 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 R-P connections, or an R-P and P-P connection, or two P-P connections with the same SR_ID and MSID may exist momentarily due to the PDSN bicasting[5]. Since the MS can connect to only one RN 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 R-P connections

[5] Bicasting occurs when the A11-Registration Request or P-P-Registration Request has the ‘S’ bit set to 1.

or P-P connections for a single packet data session. One Correlation ID for all R-P and P-P connections is maintained for a packet data session for each NAI and IP pair within the same Serving PDSN. The Account Session ID [6]is used to match a single RADIUS Start and Stop pair. A different Account Session ID is used for each R-P connection and/or P-P connection. A new R-P connection due to intra-PDSN handoff between PCFs shall result in a new R-P Connection ID and Account Session ID. A new P-P connection due to fast handoff between the PDSNs shall result in a new R-P Connection ID and Account Session ID. An intra-PDSN handoff at the Target PDSN, while in fast handoff (Figure 3, X.S0011-003-C), shall result in a new R-P connection ID and Account Session ID at the Serving PDSN. The MSID and SR_ID are used to select the proper UDR after an intra-PDSN handoff. One R-P Connection ID may be associated with multiple simultaneous NAI, IP pairs in the Serving PDSN (i.e., multiple packet data sessions).

Airlink records are only associated with an R-P connection ID. The Serving PDSN matches the R-P Connection ID in the airlink record to the R-P Connection ID 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. When this happens, one of two approaches shall be taken: (1) a container attribute as specified in Section 4 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 message. Alternatively (2), the PDSN may send a RADIUS Stop record to capture accounting data before the event, followed by a RADIUS 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 R-P Connection Setup Airlink Record Arrives

If the Serving PDSN receives an R-P Connection Setup Airlink Record with a new R-P connection ID over an R-P or P-P connection as a result of an Intra PDSN handoff or Inter PDSN fast handoff, then the serving PDSN shall use the MSID and SR_ID 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, G1, G2, G3, and G8-17, and all instances of G5/G6.
- Use information received from the RN to fill in the following fields: D3 and D4. The PDSN fills in D2 (in case of an IPv6 PDSN, D5).
- Zero fields G1, G2, G3, G8-17; all instances of G5/G6 in the newly created accounting container are eliminated.
- Mark the UDR as pending[7] if the “S” bit in the A11 Registration-Request message or P-P Registration-Request message that carries the Session Setup Airlink Record is set to '1'.
- When the Active Stop Airlink Record for the previous R-P 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.

[6] The use of the Account session ID as described in this section does not apply to the container accounting procedures.

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

- Use information received from the RN to fill the following fields in the copy UDR: D3 and D4. The PDSN fills in D2 (in case of an IPv6 PDSN, D5).
- Zero fields G1, G2, G3, and G8-17 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.
- 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 Session Setup Airlink Record is set to '1'.
- When the Active Stop Airlink Record for the previous R-P or P-P connection 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).

Otherwise, the Serving PDSN shall use the R-P Connection Setup Airlink record (from the current RN) to fill the following fields of the new UDR:

- A1, A2, D3, and D4.
- Zero fields G1-G17.

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

3.5.2 Packet Data Session Establishment

After the PDSN establishes a packet data session (i.e., Simple IP or Mobile IP) on the main service instance, or a new R-P connection setup associated with an auxiliary service instance occurs with an existing packet data session, the Serving PDSN shall:

- Fill the following fields: B1, (in case of IPv6 MS, B3), B2, C1, C2, C4, D1, D2 (in case of IPv6 PDSN, D5), F11, F12, and I1.
- 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, 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 instance and the Accounting-Stop- triggered-by-Active-Stop-Indication is set to 1 for the user, the PDSN shall not[8] trigger a RADIUS Accounting-Request (stop) record merely based on this indication.

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, D3, D4, F1-F20 and I4 from the current UDR in the new UDR.
- Zero fields G1, G2, G3, and G8-13 in the new UDR.
- Add a Session Continue attribute in the current UDR with the value set to 0 (False).

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

- Send a RADIUS Accounting-Request (Stop) record 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.

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 SR_ID to find the correct UDR. If the UDR is not pending then the PDSN shall:

- Increment G1 before compression by the number of octets in IP packets[9] sent to the user.
- Increment G16 before compression by the number of octets in Mobile IP signaling packets[10] sent to the user.
- 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 SR_ID 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[11] sent by the user.
- Increment G14 by the number of octets received at the HDLC layer.
- Increment G15 after decompression by the number of octets in Mobile IP signaling packets sent by the user.
- 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, the PDSN shall not modify the accounting usage data of the UDR.

3.5.5 Active Start Airlink Record Arrives

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

If the UDR is new (some fields are blank), the Serving PDSN shall:

- Set UDR fields according to airlink record: E1 ← e1, F1-F10 ← f1-f10, F14←f14, F16<-f16, F17-F20←f17-f20, and I4 ← i4
- If the UDR is pending, mark it as not pending.

Else, if the airlink record indicates parameters E1, F1, F2, F5, F16, F17, F18 or I4 have changed, 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 E1, F1, F2, F16, F17, F18, G1, G2, G3, G8-G17, I4, and all instances of G5/G6.

[9] This includes Mobile IP signaling octets.
[10] This means IP, UDP, and the MIP message payload above UDP.
[11] This includes Mobile IP signaling octets.

- Set UDR fields according to the airlink record. E1 ← e1, F1 <- f1, F2 <- f2, F5 <- f5, F16 <- f16, F17 <- f17, F18 <- f18, I4 ← i4, and zero fields G1, G2, G3, and G8-17. All current instances of G5/G6 in the UDR are eliminated.

Or:

- Add a Session Continue attribute in the current UDR with the value set to 1 (True).
- Send a RADIUS Accounting-Request (Stop) record based on the current UDR.
- Set UDR fields according to airlink record. E1 ← e1, F1 <- f1, F2 <- f2, F5 <- f5, F16 <- f16, F17 <- f17, F18 <- f18, I4 ← i4 and zero fields G1, G2, G3, and G8-17. All current instances of G5/G6 in the UDR are eliminated.
- 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 and Active Start Airlink for the main service instance is received by PDSN, a RADIUS Accounting-Request (Start) message with a new Account Session ID is sent for main service instance based on the current UDR.

Finally, 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 RN, the PDSN shall:

- Increment G8 by the value of g8.
- Set G17[12] with the current time if Active Stop is used to indicate last activity.

If the Serving PDSN receives an A11 Registration-Request for the main service instance 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 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 and all current instances of G5/G6, D4, E1, F1-F10, F14 and I4 in the UDR are eliminated.

3.5.7 SDB Airlink Record Arrives

The PDSN shall increment G1/G2 for all forward/reverse user data corresponding to the MS IP address. When the Serving PDSN receives an SDB airlink record from the RN 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.

[12] 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.

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 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, and G8-G16. Instances of G5/G6 are copied to the container.
- Zero fields G1, G2, G3, and G8-16. 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, and G8-16. 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.

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.

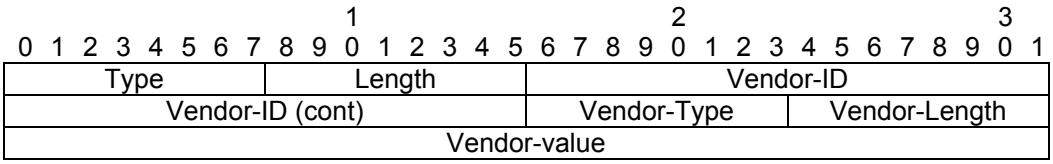


Figure 3. 3GPP2 RADIUS Attribute Format

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

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

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

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.

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.

Accounting Container:

Contains embedded 3GPP2 accounting attributes.

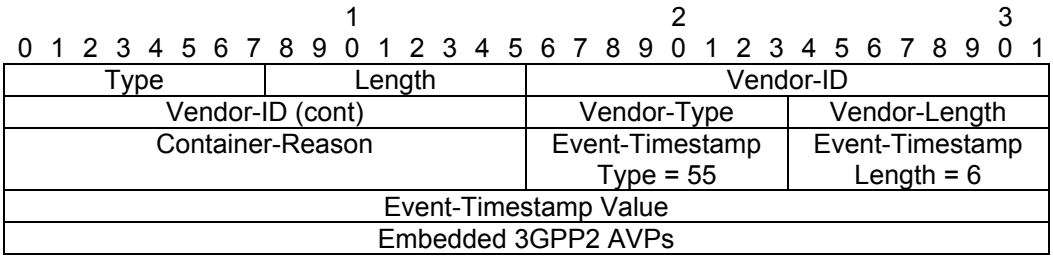


Figure 4. Accounting Container VSA format

Type: 26
Length ≥ 24
Vendor-ID: 5535
Vendor-Type: 6
Vendor-Length ≥ 18
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 AVPs: One or more parameters relating to Container-Reason above.

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.

KeyID:

Contains the KeyID parameter used during IKE exchange between the PDSN and the HA. This VSAmay 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.

‘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.

'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

‘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.

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.

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.

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.

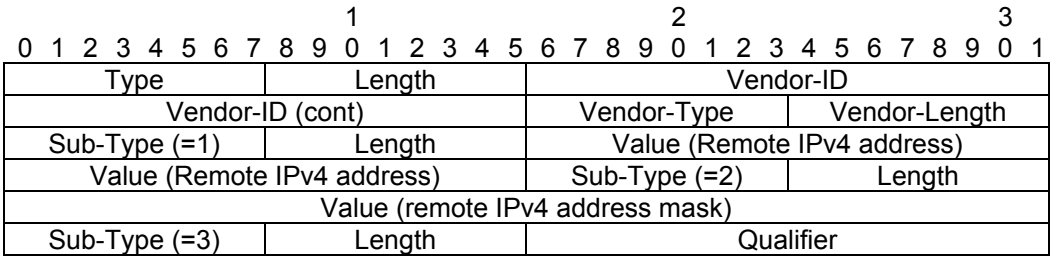


Figure 5. Remote IPv4 Address VSA format

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.

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.

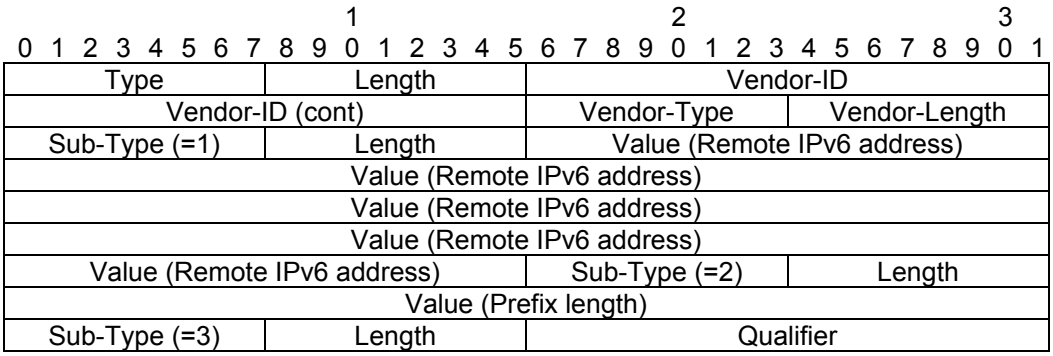


Figure 6. Remote IPv6 Address VSA format

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.

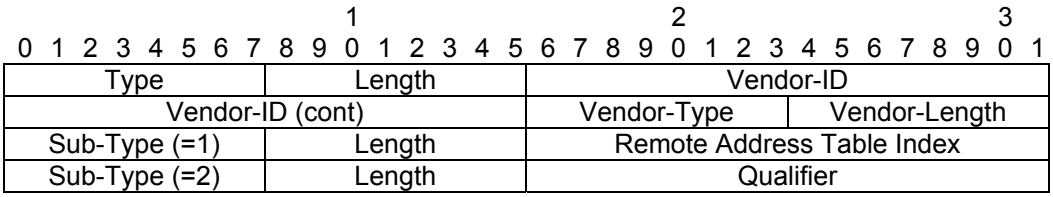
Sub-Type (=2): Sub-Type for prefix length.
Length: length of prefix length attribute (=6 octets).
Prefix Length:
The prefix length specifies the number of leading bits that must be matched. The prefix length is less than or equal to 128.

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.

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.



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	Remote Address Table Index
Sub-Type (=2)	Length	Qualifier

Figure 7. Remote Address Table Index VSA format

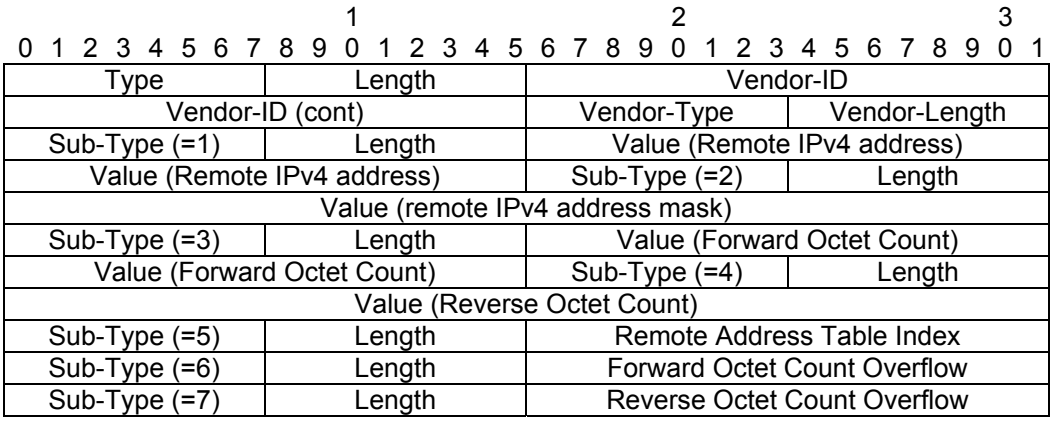
Type: 26
Length ≥12
Vendor ID: 5535
Vendor-Type: 71
Vendor-Length ≥ 6

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.

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.

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.

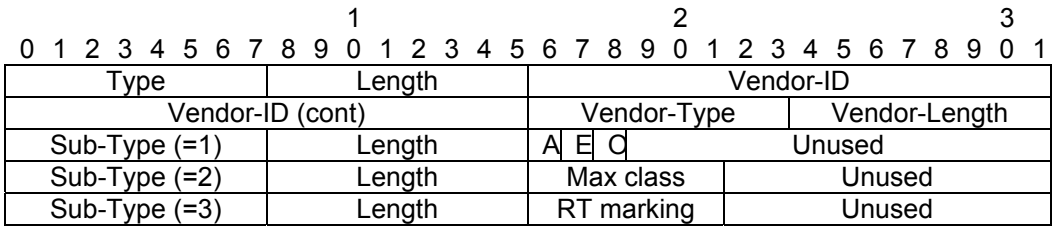


Figure 9. Allowed Differentiated Services Marking VSA format

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.

Service Option Profile:

This attribute specifies the authorized packet data service options, the maximum number of simultaneous service instances of the given service option number (n), and the total maximum number of simultaneous service instances. This attribute may appear in a RADIUS Access-Accept message.

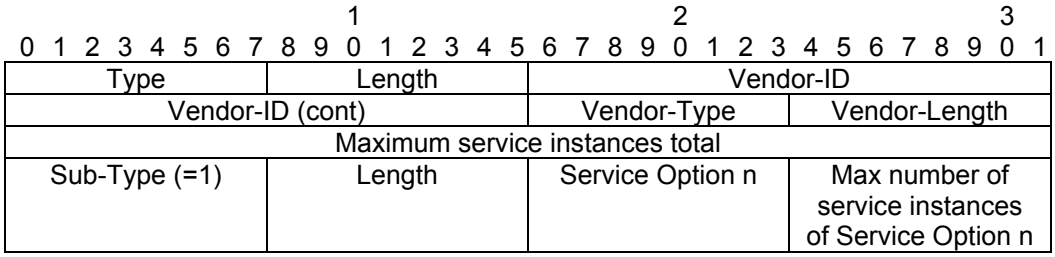


Figure 10. Service Option Profile VSA format

Type: 26
Length ≥16
Vendor ID: 5535
Vendor-Type: 74
Vendor-Length ≥10
Maximum Service Instances total:
The maximum number of service instances the user is allowed to establish regardless of the service option numbers. '1' represents one service instance, i.e., the main service instance. '0' is not an allowed value.
Sub-Type (=1): Sub-Type for service option
Length: length for service option attribute in octets (4 octets)
Service Option n: Service Option number:
Maximum Number of Service instances of service option n
Sub-Type 1 may be repeated, once for each authorized service option.

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.

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

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

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

RN Packet Data Inactivity Timer:

This is the value of the RN 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 RN Packet Data Inactivity Timer specified as an integer according to [4].

Session Termination Capability (STC):

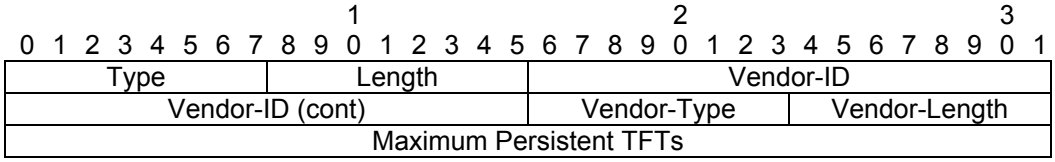
The value shall be bitmap encoded rather than a raw integer. This attribute shall be included in a RADIUS Access-Request message to the Home RADIUS server and shall contain the value 3 to indicate that the PDSN and HA support both Dynamic authorization with RADIUS and Registration Revocation for Mobile IPv4. 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.
0x00000010 Note 1	Only Registration Revocation in Mobile IPv4 is used.
0x00000011	Both Dynamic Authorization Extensions to RADIUS and Registration Revocation in Mobile IPv4 are used.

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

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 instance. 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.



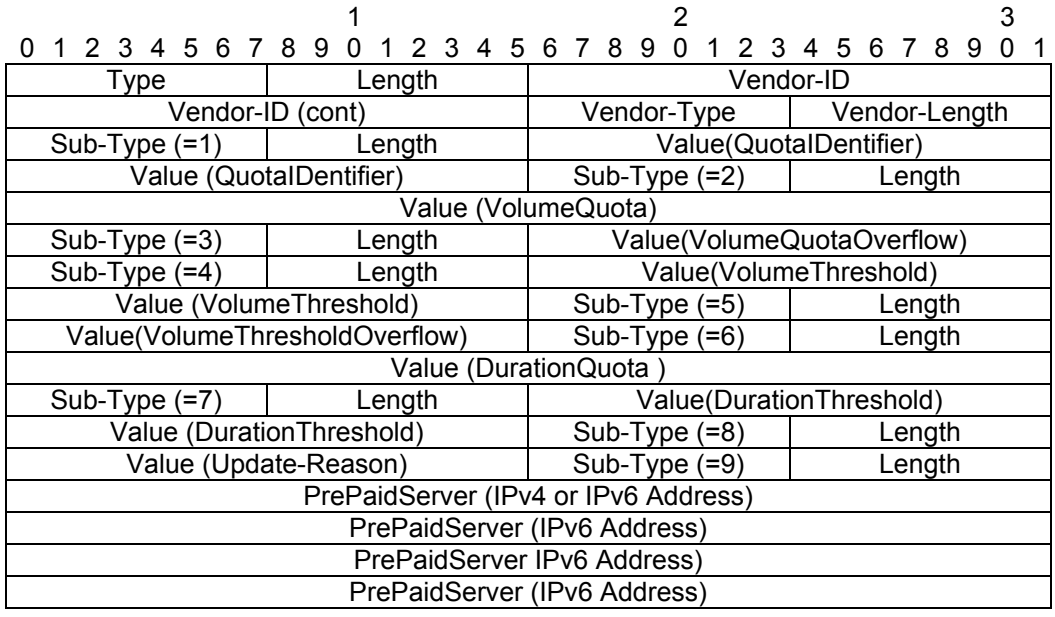
0 1 2 3 4 5 6 7	8 9 0 1 2 3 4 5	6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
Type	Length	Vendor-ID
Vendor-ID (cont)		Vendor-Type / Vendor-Length
Maximum Persistent TFTs		

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.

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.



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(QuotaIDentifier)
Value (QuotaIDentifier)		Sub-Type (=2) / Length
Value (VolumeQuota)		
Sub-Type (=3)	Length	Value(VolumeQuotaOverflow)
Sub-Type (=4)	Length	Value(VolumeThreshold)
Value (VolumeThreshold)		Sub-Type (=5) / Length
Value(VolumeThresholdOverflow)		Sub-Type (=6) / Length
Value (DurationQuota)		
Sub-Type (=7)	Length	Value(DurationThreshold)
Value (DurationThreshold)		Sub-Type (=8) / Length
Value (Update-Reason)		Sub-Type (=9) / Length
PrePaidServer (IPv4 or IPv6 Address)		
PrePaidServer (IPv6 Address)		
PrePaidServer IPv6 Address)		
PrePaidServer (IPv6 Address)		

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[13]. 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.

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

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

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 SI released
8. Service Instance not established
9. Tariff Switch Update

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.

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.

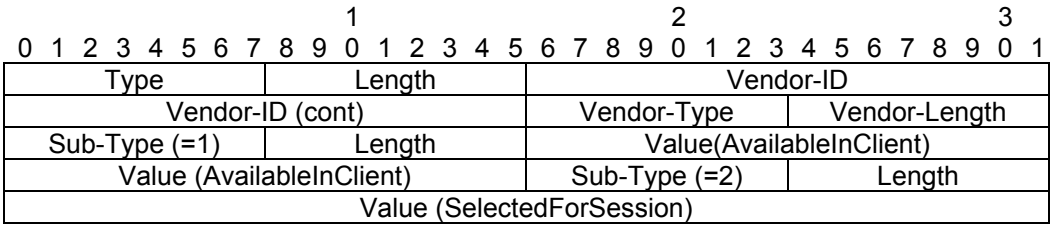


Figure 13. PrePaidAccountingCapability (PPAC) VSA format

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
0x00000010	PrePaid Accounting for Duration supported
0x00000011	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)
0x00000010	Usage of PrePaid Accounting for Duration. (only possible if the AvailableInClient supports PrePaid Accounting for Duration)
0x00000011	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).

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.

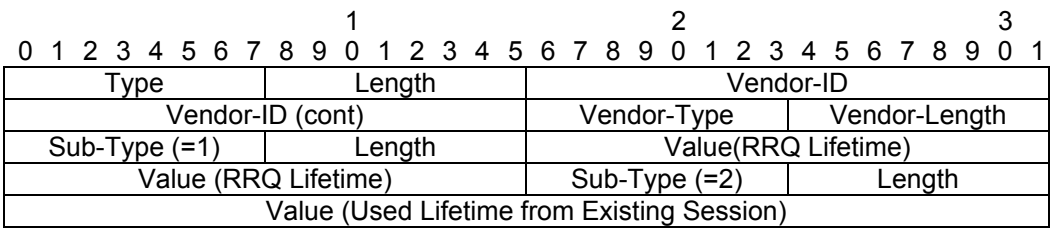


Figure 14. MIP Lifetime VSA format

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.

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 instance 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

Service Reference ID:

Specifies the reference ID of the service instance as received in the A11 Registration Request. If the service instance is the main service instance, the main SI Indicator Sub-Type shall be included.

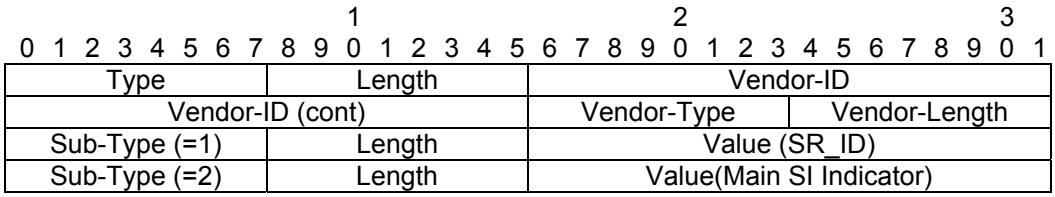


Figure 15. Service Reference ID format

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 SI Indicator
Length: (=4 octets)
Only included for the main Service instance.
1: main SI.

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.

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

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.

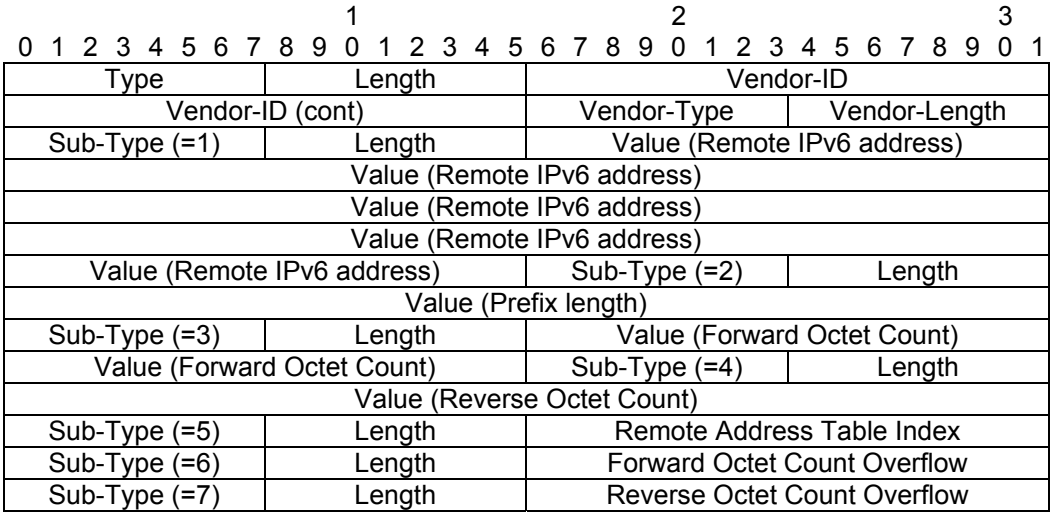


Figure 16. Remote IPv6 Address Octet Count VSA format

Type: 26
Length ≥24

Vendor ID: 5535
Vendor-Type[17]: 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 must 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.

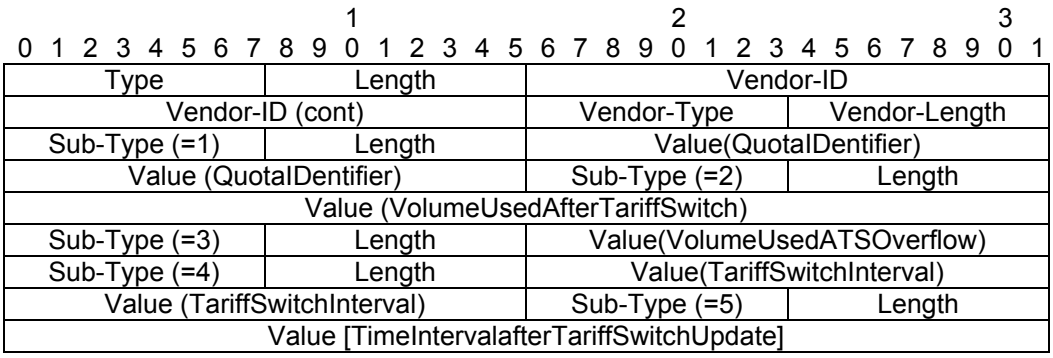
Sub-Type (=5): Table Index for summarized Remote IPv6 Address Octet Count, if present Sub-Type 1 and Sub-Type 2 shall not be present.
Length: length of table index (4 bytes)
Table Index:
The table index from the associated Remote Address Table Index attribute.

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.

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.



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(QuotaIDentifier)
Value (QuotaIDentifier)	Sub-Type (=2) / Length
Value (VolumeUsedAfterTariffSwitch)	
Sub-Type (=3)	Length / Value(VolumeUsedATSOverflow)
Sub-Type (=4)	Length / Value(TariffSwitchInterval)
Value (TariffSwitchInterval)	Sub-Type (=5) / Length
Value [TimeIntervalafterTariffSwitchUpdate]	

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.

5 3GPP2 VSA Table

The following table[14] provides a guide to the 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.

VSA	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	1	1	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	26/31	0	0	0	0-1	0-1

[14] See X.S0011-006-C for attributes of PrePaid Accounting.

(Terminating)						
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[15]	26/39	0	0	0-1	0-1	0-1
Airlink Record Type[15]	26/40	0	0	0	0	0
Airlink Sequence Number[15]	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
Mobile Originated / Mobile Terminated Indicator[15]	26/45	0	0	0	0	0
Inbound Mobile IP Signaling Octet Count	26/46	0	0	0	0-1	0-1
Outbound Mobile IP 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	1	1	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[16]	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	26/80	0	0	0	0-1	0-1

[15] The attribute is used over the R-P interface in Airlink Records, they are not sent to the Home RADIUS server in Accounting Records.
[16] Reserved for RN usage.

Time						
MN-AAA Removal Indication	26/81	0	0-1	0	0	0
RN 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
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[17]	26/97	0	0	0	0+	0+
PrePaidTariffSwitch (PTS)	26/98	0	0-1	0	0	0

Table 7. Complete list of 3GPP2 VSAs

6 RADIUS Disconnect Attribute 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.

Attribute	Type	Disconnect-Request	Disconnect-ACK
Correlation ID	26/44	0-1	0
User-Name	1	1	0

[17] Previous version of this specification used 26/80 as a value type for the Remote IPv6 Address Count VSA. This version of the specification 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.

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
Framed-IPv6-Prefix	97	0-1	0
Framed-Interface-ID	96	0-1	0

1 **Table 8. Attributes of RADIUS Disconnect messages**

2

Annex A: 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 an Accounting (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.