Cisco ASR 5000 Series AAA and GTPP Interface Administration and Reference

Version 12.0

Last Updated January 31, 2013

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

Text Part Number: OL-24895-04

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Cisco and the Cisco Logo are trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and other countries. A listing of Cisco's trademarks can be found at www.cisco.com/go/trademarks. Third party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

Cisco ASR 5000 Series AAA and GTPP Interface Administration and Reference

© 2013 Cisco Systems, Inc. All rights reserved.

CONTENTS

About this Guide ix
Conventions Used x
Contacting Customer Support xii
Additional Information xiii
AAA Introduction and Overview 15
Overview 16
Platform Requirements 18
License Requirements 18
Diameter Proxy 19
Supported Features 20
Diameter Server Selection for Load-balancing 20
Fire-and-Forget Feature 20
Realm-based Routing 21
Dynamic Route Addition 21
Dynamic Route Deletion 21
AAA Interface Configuration 23
Configuring RADIUS AAA Functionality 24
Configuring RADIUS AAA Functionality at Context Level 24
Verifying Your Configuration 26
Configuring Diameter AAA Functionality 27
Configuring Diameter Endpoint 27
Configuring Diameter AAA Functionality at Context Level 29
Verifying Your Configuration 30
Configuring Diameter Authentication Failure Handling 30
Configuring at Context Level 30
Configuring at AAA Group Level 31
Configuring System-Level AAA Functionality 32
Verifying your configuration 32
Configuring AAA Server Group for AAA Functionality 33
AAA Server Group Configuration 34
Verifying Your Configuration 34
Applying a AAA Server Group to a Subscriber 35
Verifying Subscriber Configuration 35
Applying a AAA Server Group to an APN 35
Verifying APN Configuration 36
Configuring the Destination Context Attribute 37
Verifying Your Configuration 38
Managing and Monitoring the AAA Servers 39
Managing the AAA Servers 40
Using the RADIUS Testing Tools 40
Testing a RADIUS Authentication Server 40
Testing a RADIUS Accounting Server 41
Monitoring AAA Status and Performance 42

Clearing Statistics and Counters 43
Session Recovery and AAA Statistics Behavior 43
Diameter Dictionaries and Attribute Definitions 45
Diameter Attributes 46
AVP Header 46
Basic AVP Data Formats 47
Derived AVP Data Formats 48
Address 48
Time 48
UTF8String 49
DiameterIdentity 49
DiameterURI 49
Enumerated 50
IPFilterRule 50
QoSFilterRule 52
Grouped AVP Values 53
Diameter AVP Definitions 55
RADIUS Dictionaries and Attribute Definitions 309
RADIUS Dictionaries 310
Dictionary Types 310
RADIUS Attribute Definitions 312
Attribute Notes 749
RFC 2868 Tunneling Attributes 749
GTPP Accounting Overview 751
GTPP Interface Overview 752
CDR Transport by GTPP 753
Path Protocol 754
GTPP Message Types 755
Usage of GTPP Header in Charging 756
Information Elements 757
GTPP Messages 758
Node Alive Request 758
Node Alive Response 758
Redirection Request 759
Redirection Response 760
Data Record Transfer Request 761
Information Elements in Data Record Transfer Request 761
Packet Transfer Command IE 761
Data Record Packet IE 762
Sequence Numbers of Released Packets IE 762
Sequence Numbers of Canceled Packets IE 763
Private Extension IE 763
Data Record Transfer Response 763
Handling Error Response Cause 764
Charging Characteristics 765
Charging Records 767
File Format for CDRs 767
Standard G-CDRs 769
G-CDR Format 769
Enhanced G-CDRs 769
eG-CDR Format 770
PDN Gateway Call Detail Records (PGW-CDRs) 770

PGW-CDR Format 770
Serving Gateway Call Detail Records (SGW-CDRs) 770
SGW-CDR Format 770
Standard SGSN CDRs 770
S-CDR Format 770
Wireless LAN Call Detail Records (WLAN-CDRs) 770
WLAN-CDR Format 771
Triggers for Generation of Charging Records 772
GGSN CDR Triggers 772
G-CDR Triggers 772
eG-CDR Triggers 772
PGW-CDR Triggers 774
PGW-CDR Charging Information Addition 775
SGW-CDR Triggers 776
SGW-CDR Charging Information Addition 777
WLAN-CDR Triggers 778
WLAN-CDR Charging Information Addition 778
GGSN CDR Field Reference 781
CDR Fields Supported in G-CDRs 782
custom1 – custom4 Dictionaries 782
custom5 – custom7, custom9, custom12, custom14, custom15, custom17, custom19, custom20, and custom22 Dictionaries 783
standard, custom8, custom10, custom11, custom13, custom18, custom21, custom23 – custom29 Dictionaries 785
custom16 Dictionary 786
custom30 Dictionary 791
CDR Fields Supported in eG-CDRs 797
custom1 Dictionary 797
custom2 Dictionary 798
custom3 Dictionary 799
custom4 Dictionary 801
custom5 and custom9 Dictionaries 802
custom6 – custom8, custom14, custom15, custom17, custom20 Dictionaries 804
List of Traffic Data Volumes 806
List of Service Data Volumes 807
standard and custom10 Dictionaries 808
custom12 and custom19 Dictionaries 809
List of Traffic Data Volumes 810
List of Service Data Volumes 811
custom21 Dictionary 812
custom27 Dictionary 813
custom30 Dictionary 815
custom33 Dictionary 816
List of Service Data Volumes 818
GGSN CDR Field Descriptions 821
CDR Fields 822
P-GW CDR Field Reference 835
CDR Fields Supported in PGW-CDRs 836
custom24, custom40, and custom42 Dictionary 836
Data Service Volume Block 838
P-GW CDR Field Descriptions 839
CDR Fields 840

SGSN CDR Field Reference 861
CDR Fields Supported in S-CDRs 862
standard, custom1, custom2, custom4, custom5, custom7, custom9, custom12, custom13, custom15, custom16, custom19, custom20, custom21, custom22, custom24, custom25, custom26, custom28, custom30 Dictionaries 862
custom3 Dictionary 863
custom6 Dictionary 865
custom8 Dictionary 867
custom10 and custom11 Dictionaries 868
custom13 Dictionary 870
custom14 Dictionary 872
custom17 Dictionary 874
custom18 Dictionary 877
custom27 dictionary 878
custom29 Dictionary 880
custom31 Dictionary 882
custom33 Dictionary 884
CDR Fields Supported in S-SMO-CDRs 887
standard, custom1 – custom30 Dictionaries 887
CDR Fields Supported in S-SMT-CDRs 889
standard, custom1 – custom30 Dictionaries 889
CDR Fields Supported in M-CDR 890
standard, custom1 – custom5, custom7, custom9 – 12, and custom14 – custom30 Dictionaries 890
custom6 and custom13 Dictionaries 891
custom8 Dictionary 892
SGSN CDR Field Descriptions 895
CDR Fields 896
S-GW CDR Field Reference 911
CDR Fields Supported in SGW-CDRs 912
custom6, and custom11 Dictionaries 912
List of Traffic Data Volumes 914
custom24 Dictionary 914
custom34 Dictionary 918
List of Traffic Data Volumes 920
S-GW CDR Field Descriptions 921
CDR Fields 922
WLAN CDR Field Reference 941
CDR Fields Supported in WLAN-CDRs 942
standard, and custom1 - custom6 Dictionaries 942
WLAN CDR Field Descriptions 947
CDR Fields 948
HDD Storage 959
Overview 960
Benefits 960
Supported Records on HDD 961
Accounting Request Records (ACR) 961
Charging Data Records (CDR) 961
Event Data Records (EDR) 961
Event Records 962
Reporting Event Data Records (REDR) 962

Usage Data Records (UDR) 962
Hardware Overview 964
How HDD Works 965
Deployment Scenarios 966
HDD Configuration 967
Configuring HDD 967
Configuring EDR/UDR Parameters 967
Viewing Statistics 968
Pushing EDR/UDR Files Manually 968
Retrieving EDR and UDR Files 969
AAA Engineering Rules 971
AAA Interface Rules 972
RADIUS Server State Behavior 973
Understanding RADIUS Server States and Commands 974
Server States 974
RADIUS Server Commands 974
Server State Triggers 976
Switching CDRs 977
Switching CDRs from HDD to GSS 978
LRSN Enabled 978
LRSN Disabled 979
Switching CDRs from GSS to HDD 982
LRSN Enabled 982
LRSN Disabled 983
Diameter Attribute Quick Reference 987
RADIUS Attribute Quick Reference 989

About this Guide

This document pertains to the features and functionality that run on and/or that are related to the Cisco® ASR 5000 Chassis.

This preface includes the following sections:

- Conventions Used
- Contacting Customer Support
- Additional Information

Conventions Used

The following tables describe the conventions used throughout this documentation.

Icon	Notice Type	Description
	Information Note	Provides information about important features or instructions.
	Caution	Alerts you of potential damage to a program, device, or system.
	Warning	Alerts you of potential personal injury or fatality. May also alert you of potential electrical hazards.
	Electrostatic Discharge (ESD)	Warns you to take proper grounding precautions before handling ESD sensitive components or devices.

Typeface Conventions	Description
Text represented as a `screen display`	This typeface represents text that appears on your terminal screen, for example: `Login:`
Text represented as **`commands`**	This typeface represents commands that you enter at the CLI, for example: **`show ip access-list`** This document always gives the full form of a command in lowercase letters. Commands are not case sensitive.
Text represented as a **`command`** *`variable`*	This typeface represents a variable that is part of a command, for example: **`show card`** *`slot_number`* *`slot_number`* is a variable representing the desired chassis slot number.
Text represented as menu or sub-menu names	This typeface represents menus and sub-menus that you access within a software application, for example: Click the **File** menu, then click **New**.

Command Syntax Conventions	Description
{ **`keyword`** or *`variable`* }	Required keywords and variables are surrounded by braces. They must be entered as part of the command syntax.
[**`keyword`** or *`variable`*]	Optional keywords or variables that may or may not be used are surrounded by brackets.

Command Syntax Conventions	Description
|	Some commands support alternative variables. These "options" are documented within braces or brackets by separating each variable with a vertical bar. These variables can be used in conjunction with required or optional keywords or variables. For example: **{ nonce | timestamp }** OR [**count** *number_of_packets* | **size** *number_of_bytes*]

Contacting Customer Support

Go to http://www.cisco.com/cisco/web/support/ to submit a service request. A valid Cisco account (username and password) is required to access this site. Please contact your Cisco account representative for additional information.

Additional Information

Refer to the following guides for supplemental information about the system:

- *Cisco ASR 5000 Installation Guide*
- *Cisco ASR 5000 System Administration Guide*
- *Cisco ASR 5x00 CDMA Command Line Interface Reference*
- *Cisco ASR 5x00 eHRPD / LTE Command Line Interface Reference*
- *Cisco ASR 5x00 GPRS / UMTS Command Line Interface Reference*
- *Cisco ASR 5x00 Thresholding Configuration Guide*
- *Cisco ASR 5x00 SNMP MIB Reference*
- *Web Element Manager Installation and Administration Guide*
- *Cisco ASR 5x00 AAA Interface Administration and Reference*
- *Cisco ASR 5x00 GTPP Interface Administration and Reference*
- *Cisco ASR 5x00 Release Change Reference*
- *Cisco ASR 5x00 Statistics and Counters Reference*
- *Cisco ASR 5x00 Gateway GPRS Support Node Administration Guide*
- *Cisco ASR 5x00 HRPD Serving Gateway Administration Guide*
- *Cisco ASR 5000 IP Services Gateway Administration Guide*
- *Cisco ASR 5x00 Mobility Management Entity Administration Guide*
- *Cisco ASR 5x00 Packet Data Network Gateway Administration Guide*
- *Cisco ASR 5x00 Packet Data Serving Node Administration Guide*
- *Cisco ASR 5x00 System Architecture Evolution Gateway Administration Guide*
- *Cisco ASR 5x00 Serving GPRS Support Node Administration Guide*
- *Cisco ASR 5x00 Serving Gateway Administration Guide*
- *Cisco ASR 5000 Session Control Manager Administration Guide*
- *Cisco ASR 5000 Packet Data Gateway/Tunnel Termination Gateway Administration Guide*
- Release notes that accompany updates and upgrades to the StarOS for your service and platform

Chapter 1
AAA Introduction and Overview

This chapter provides the information on how to configure the AAA interface to enable authentication, authorization, and accounting (AAA) functionality for your core network service subscribers in a wireless carrier network.

This chapter provides information on basic AAA features. For information on product-specific AAA features and product-specific AAA interface configurations, refer to the administration guide for the product that you are deploying.

Overview

The Authentication, authorization, and accounting (AAA) subsystem on the chassis provides the basic framework to configure access control on your network. The AAA subsystem in core network supports Remote Authentication Dial-In User Service (RADIUS) and Diameter protocol based AAA interface support. The AAA subsystem also provides a wide range of configurations for AAA servers in groups, which in effect contain a series of RADIUS/Diameter parameters for each application. This allows a single group to define a mix of Diameter and RADIUS servers for the various application functions.

Although AAA functionality is available through AAA subsystem, the chassis provides onboard access control functionality for simple access control through subscriber/APN authentication methods.

AAA functionality provides capabilities to operator to enable authentication and authorization for a subscriber or a group of subscriber through domain or APN configuration. The AAA interface provides the following AAA support to a network service:

- **Authentication**: It is the method of identifying users, including login and password, challenge and response, messaging support, and encryption. Authentication is the way to identify a subscriber prior to being allowed access to the network and network services. An operator can configure AAA authentication by defining a list of authentication methods, and then applying that list to various interfaces.

  All authentication methods, except for chassis-level authentication, must be defined through AAA configuration.

- **Authorization**: It is the method to provide access control, including authorization for a subscriber or domain profile. AAA authorization sends a set of attributes to the service describing the services that the user can access. These attributes determine the user's actual capabilities and restrictions.

- **Accounting**: Collects and sends subscriber usage and access information used for billing, auditing, and reporting, such as user identities, start and stop times, performed actions, number of packets, and number of bytes.

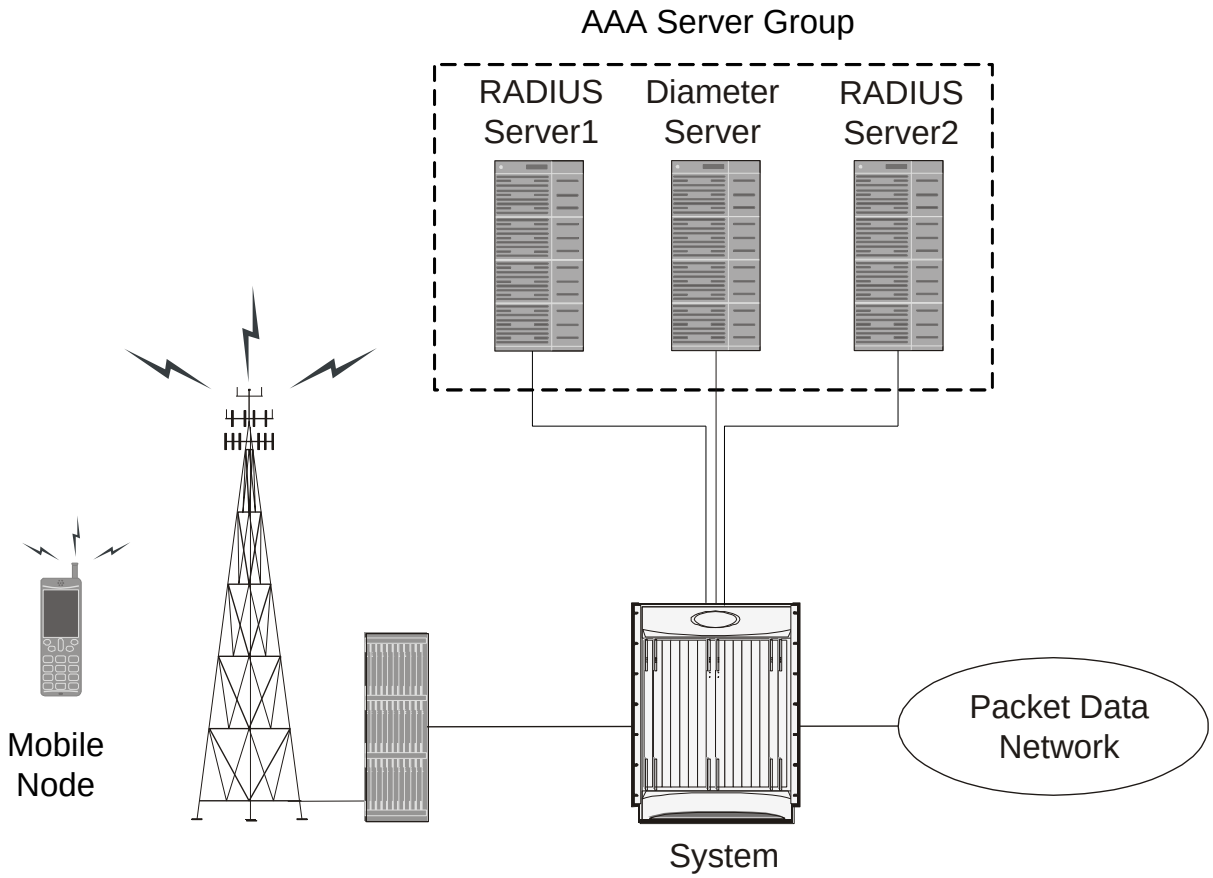
  Accounting enables operator to analyze the services users are accessing as well as the amount of network resources they are consuming. Accounting records are comprised of accounting AVPs and are stored on the accounting server. This accounting information can then be analyzed for network management, client billing, and/or auditing.

Advantages of using AAA are:

- Higher flexibility for subscriber access control configuration
- Better accounting, charging, and reporting options
- Industry standard RADIUS and Diameter authentication

The following figure shows a typical AAA server group configuration that includes three AAA servers (RADIUS and Diameter).

Figure 1. AAA Server Group Configuration in a Core Network



Product Support Matrix for AAA

The following table provides the information on AAA (RADIUS and Diameter) support with our series of core multimedia gateway products. The symbol (X) indicates that the support for the identified AAA function exists for that particular product.

Product Name	Diameter Accounting	Diameter Authentication	RADIUS
Access Service Network Gateway (ASN-GW)	X	X (EAP)	X
Femto Network Gateway (FN-GW)	N/A	N/A	X
Gateway GPRS Support Node (GGSN)	X	X (S6b)	X
Home Agent (HA)	N/A	N/A	X
Home NodeB Gateway (HNB-GW)	N/A	N/A	X
HRPD Serving Gateway (HS-GW)	X	X (STa)	N/A
IP Services Gateway (IPSG)	N/A	N/A	X
Mobility Management Entity (MME)	N/A	X (S6a/S13)	N/A
Packet Data Gateway/Tunnel Termination Gateway (PDG/TTG)	N/A	X (SWm)	X

Product Name	Diameter Accounting	Diameter Authentication	RADIUS
Packet Data Interworking Function (PDIF)	N/A	X (EAP)	X
Packet Data Support Node (PDSN)	N/A	N/A	X
Packet Data Network (PDN) Gateway (P-GW)	X	X (S6b)	X
Session Control Manager (SCM)	X	X (Cx)	X
Serving GPRS Support Node (SGSN)	N/A	X (S6d)	N/A
Serving Gateway (S-GW)	X	N/A	X

Platform Requirements

AAA runs on a Cisco® ASR 5x00 Series chassis running StarOS. The chassis can be configured with a variety of components to meet specific network deployment requirements. For additional information, refer to the Installation Guide for the chassis and/or contact your Cisco account representative.

License Requirements

AAA is a licensed Cisco feature. Separate feature licenses may be required. Contact your Cisco account representative for detailed information on specific licensing requirements. For information on installing and verifying licenses, refer to the *Managing License Keys* section of the *Software Management Operations* chapter in the *System Administration Guide*.

Diameter Proxy

The proxy acts as an application gateway for Diameter. It gets the configuration information at process startup and decides which Diameter peer has to be contacted for each application. It establishes the peer connection if no peer connection already exists. Upon receiving the answer, it uses the Diameter session ID to identify to which application the message is intended.

Each PSC has a Diameter proxy identified by the IPv6 origin host address. If the number of configured origin hosts is lesser than the number of active PSCs, some (i.e. those number where no origin hosts associated with) PSCs will not activate Diameter processing at all, and instead notify administrators of the erroneous configuration with syslog/traps.

If the number of configured origin hosts is greater than the number of active PSCs, the application will automatically select which configured host is to be used per PSC.

Supported Features

This section provides the list of features that are supported by RADIUS and Diameter.

Diameter Server Selection for Load-balancing

Diameter load balancing implementation maintains a fixed number of servers active at all times for load balancing in case of failures. This can be done by selecting a server with lower weight and adding it to the set of active servers.

Consider the following requirements in the Diameter Endpoint configuration for load balancing:

- Endpoint configuration is needed to specify the minimum number of servers that needs to be active for the service.
- If any one of the servers in the current active group fails, one of the idle servers needs to be selected for servicing the new requests.
- New sessions should be assigned to idle servers with higher weight.
- New session should be assigned to idle servers with lower weight only if
    - The number of active servers are less than the minimum number of servers required for the service
    - Idle servers with higher priority are not available

For information on the commands used for configuring the load-balancing feature, refer to the *Command Line Interface Reference*.

Fire-and-Forget Feature

The current release supports configuring secondary AAA accounting group for the APN. This supports the RADIUS Fire-and-Forget feature in conjunction with GGSN for secondary accounting (with different RADIUS accounting group configuration) to the RADIUS servers without expecting acknowledgement from the server, in addition to standard RADIUS accounting. This secondary accounting will be an exact copy of all the standard RADIUS accounting message (RADIUS Start / Interim / Stop) sent to the standard AAA RADIUS server.

This feature also supports configuring secondary AAA accounting group for the subscriber template. This supports the No-ACK RADIUS Targets feature in conjunction with PDSN and HA for secondary accounting (with different RADIUS accounting group configuration) to the RADIUS servers without expecting the acknowledgement from the server, in addition to standard RADIUS accounting. This secondary accounting will be an exact copy of all the standard RADIUS accounting message (RADIUS Start / Interim / Stop) sent to the standard AAA RADIUS server.

Typically, the request sent to the Radius Accounting Server configured under the AAA group with the CLI **`radius accounting fire-and-forget`** configured will not expect a response from the server. If there is a need to send the request to multiple servers, the accounting algorithm first-n will be used in the AAA group.

If the server is down, the request is sent to the next server in the group. If all the servers in the group are down, then the request is deleted.

Important: Please note that on-the-fly change in the configuration is not permitted. Any change in the configuration will have effect only for the new calls.

For information on the commands used for configuring this feature, refer to the *Command Line Interface Reference*.

Realm-based Routing

In StarOS 12.0 and later releases, the Diameter routing logic has been modified to enable routing to destination hosts that are not directly connected to the Diameter clients like GGSN, MME, PGW, and that does not have a route entry configured. Message routing to the host is based on the realm of the host.

For a given session towards a Destination Host, all the messages belonging to the session will be routed through the same peer until the peer is down. If the peer goes down, for the subsequent messages failure handling mechanism will be triggered and the message will be sent using other available peers connected to the destination host.

Dynamic Route Addition

Dynamic routes are added when a response to a Diameter request message arrives with Origin-Host AVP. If there is no route entry corresponding to the Origin-Host, realm and peer, a new dynamic route entry is created and added to the table. This route entry will be flagged as Dynamic and a Path Cache entry. The following entries will be added to the dynamic route entry.

- Flag (Dynamic and Path-Cache)
- Host name (Corresponding to the Origin-Host from the response)
- Realm (Obtained from the session)
- Application id (Obtained from the session)
- Peer (From which the response was received)
- Weight (Inherit the weight of the realm-based route entry based on which the request was routed)

Dynamic Route Deletion

The dynamic route will be deleted from the routing table in the following conditions:

- The peer associated with the route-entry is deleted.
- When the route is not used by any of the sessions for a given period of time.
- When the realm based route from which the dynamic route is derived, is deleted.

The route deletion can be accomplished by introducing a new CLI in the Diameter Endpoint configuration mode. This CLI allows configuring an expiry timeout based on which the route entry will be deleted.

For information on the commands used for configuring the realm-based routing feature, refer to the *Command Line Interface Reference*.

Chapter 2
AAA Interface Configuration

This chapter describes how to configure access control to network services, and the type of services available to subscribers once they have access. The authentication, authorization, and accounting (AAA) configuration described in this chapter provides the primary framework through which you can set up AAA functionality in your network for a service subscriber.

Procedures to configure and administer core network services are described in detail in the administration guide for the product that you are deploying. System-related configuration procedures are described in detail in the *System Administration Guide*. Before using the procedures in this chapter, it is recommended to refer the respective product administration guide and the *System Administration Guide*.

This chapter includes the following information:

- Configuring RADIUS AAA Functionality
- Configuring Diameter AAA Functionality
- Configuring System-Level AAA Functionality
- Configuring AAA Server Group for AAA Functionality
- Configuring the Destination Context Attribute

Configuring RADIUS AAA Functionality

RADIUS-based AAA functionality must be configured at the context and system levels. This section describes how to configure the RADIUS-based AAA parameters at the context and system levels.

To configure RADIUS AAA functionality:

Step 1 Configure RADIUS AAA functionality at context level as described in the Configuring RADIUS AAA Functionality section.

Step 2 Configure system-level AAA parameters as described in the Configuring System-Level AAA Functionality section.

Step 3 Save your configuration to flash memory, an external memory device, and/or a network location using the Exec mode command **save configuration**. For additional information on how to verify and save configuration files, refer to the *System Administration Guide* and the *Command Line Interface Reference*.

Important: Commands used in the configuration examples in this section provide base functionality to the extent that the most common or likely commands and/or keyword options are presented. In many cases, other optional commands and/or keyword options are available. Refer to the *Command Line Interface Reference* for complete information regarding all commands.

Configuring RADIUS AAA Functionality at Context Level

This section describes how to configure context-level RADIUS parameters for subscriber authentication and accounting (optional). As noted in this reference, RADIUS-based AAA functionality can be configured within any context, even its own.

Important: This section provides minimum instructions to configure context-level AAA functionality that allows the system to process data sessions. Commands that configure additional context-level AAA properties are described in the *Understanding the System Operation and Configuration* chapter of the *System Administration Guide*.

Important: Commands except **change-authorize-nas-ip**, **accounting prepaid**, **accounting prepaid custom**, and **accounting unestablished-sessions** used in this section, or in the *Understanding the System Operation and Configuration* chapter, are also applicable to support AAA server group for AAA functionality. For details on AAA server group functionality, see the Configuring AAA Server Group for AAA Functionality section.

To configure RADIUS AAA functionality at the context level use the following configuration:

```
configure

   context <context_name>

      radius server <ipv4/ipv6_address> key <shared_secret> [ max <value> ] [
oldports | port <tcp_port> ] [ priority <priority> ]

      radius [ mediation-device ] accounting server <ipv4/ipv6_address> key
<shared_secret> [ acct-on { enable | disable } ] [ acct-off { enable | disable }
```

```
] [ max <msgs> ] [ oldports ] [ port <port_number> ] [ priority <priority> ] [
type standard ]

      radius attribute nas-identifier <identifier>

      radius attribute nas-ip-address address <primary_ipv4/ipv6_address> [
backup <secondary_ipv4/ipv6_address> ]

      radius strip-domain [ authentication-only | accounting-only ]

      end
```

Notes:

- *Optional.* If you want to support more than 320 server configurations system-wide, in the Global Configuration Mode, use the following command:

  aaa large-configuration

- *<context_name>* must be the system context designated for AAA configuration.
- For information on GGSN-specific additional configurations using RADIUS accounting see the *Creating and Configuring APNs* section of the *GGSN Administration Guide*.
- In this release, the configuration of NAS IP address with IPv6 prefix is currently not supported.
- *<identifier>* must be the name designated to identify the system in the Access Request message(s) it sends to the RADIUS server.
- *Optional.* Multiple RADIUS attribute dictionaries have been created for the system. Each dictionary consists of a set of attributes that can be used in conjunction with the system. As a result, users could take advantage of all of the supported attributes or only a subset. To specify the RADIUS attribute dictionary that you want to implement, in the Context Configuration Mode, use the following command:

  radius dictionary { 3gpp | 3gpp2 | 3gpp2-835 | custom*XX* **| standard | starent | starent-835 | starent-vsa1 | starent-vsa1-835 }**

- *Optional.* Configure the system to support NAI-based authentication in the event that the system cannot authenticate the subscriber using a supported authentication protocol. To enable NAI-construction, in the Context Configuration Mode, use the following command:

  aaa constructed-nai authentication [encrypted] password *<password>*

- *Optional.* If RADIUS is configured for GGSN service, the system can be configured to support NAI-based authentication to use RADIUS shared secret as password. To enable, in the Context Configuration Mode, use the following command:

  aaa constructed-nai authentication use-shared-secret-password

  If authentication type is set to allow-noauth or msid-auth and aaa constructed-nai authentication use-shared-secret-password is issued then the system will use RADIUS shared secret as password. In case the authentication type is msid-auth it will always send RADIUS shared secret as password by default in ACCESS-REQUEST.

- *Optional.* To configure the system to allow a user session even when all authentication servers are unreachable, in the Context Configuration Mode, use the following command. When enabled, the session is allowed without authentication. However, the accounting information is still sent to the RADIUS accounting server, if it is reachable.

  radius allow authentication-down

- *Optional.* To configure the maximum number of times RADIUS authentication requests must be re-transmitted, in the Context Configuration Mode, use the following command:

  radius max-transmissions *<transmissions>*

- *Optional.* If RADIUS is configured for PDSN service, to configure the accounting trigger options for R-P originated calls to generate STOP immediately or to wait for active-stop from old PCF on handoff, in the Context Configuration Mode, use the following command:

  radius accounting rp handoff-stop { immediate | wait-active-stop }

  For more information on configuring additional accounting trigger options for R-P generated calls for a PDSN service, refer to the **radius accounting rp** command in the *Command Line Interface Reference*.

- *Optional.* To configure the system to check for failed RADIUS AAA servers, in the Context Configuration Mode, use the following command:

  radius detect-dead-server { consecutive-failures *<count>* **| keepalive | response-timeout** *<seconds>* **}**

  After a server's state is changed to "Down", the deadtime timer is started. When the timer expires, the server's state is returned to "Active". If both **consecutive-failures** and **response-timeout** are configured, then both parameters have to be met before a server's state is changed to "Down". For a complete explanation of RADIUS server states, refer to *RADIUS Server State Behavior* appendix.

- *Optional.* To configure the system to check for failed RADIUS accounting servers, in the Context Configuration Mode, use the following command:

  radius accounting detect-dead-server { consecutive-failures *<count>* **| response-timeout** *<seconds>* **}**

  After a server's state is changed to "Down", the deadtime timer is started. When the timer expires, the server's state is returned to "Active". If both **consecutive-failures** and **response-timeout** are configured, then both parameters have to be met before a server's state is changed to "Down". For a complete explanation of RADIUS server states, refer to *RADIUS Server State Behavior*.

- *Optional.* If required, users can configure the dynamic redundancy for HA as described in the *HA Redundancy for Dynamic Home Agent Assignment* chapter of the *Home Agent Administration Guide*.

Verifying Your Configuration

To verify your configurations:

In the Exec mode, enter the following command:

show configuration context *<aaa_context_name>*

The output displays a concise list of settings that you have configured for the context.

Configuring Diameter AAA Functionality

This section describes how to configure the Diameter endpoints and system to use the Diameter servers for subscriber authentication and accounting (optional).

To configure Diameter AAA functionality:

Step 1 Configure Diameter endpoint as described in the Configuring Diameter Endpoint section.

Step 2 Configure Diameter context-level AAA parameters as described in the Configuring Diameter AAA Functionality at Context Level section.

Step 3 Configure system-level AAA parameters as described in the Configuring System-Level AAA Functionality section.

Step 4 Save your configuration to flash memory, an external memory device, and/or a network location using the Exec mode command **save configuration**. For additional information on how to verify and save configuration files, refer to the *System Administration Guide* and the *Command Line Interface Reference*.

Important: Commands used in the configuration examples in this section provide base functionality to the extent that the most common or likely commands and/or keyword options are presented. In many cases, other optional commands and/or keyword options are available. Refer to the *Command Line Interface Reference* for complete information regarding all commands.

Important: In releases prior to 12.0, the configuration of Diameter nodes and host strings like endpoint name, peer name, host name, realm name, and fqdn were case-sensitive. In 12.0 and later releases, all the Diameter related node IDs are considered case insensitive. This change applies to both the local configuration and communication with external nodes.

Configuring Diameter Endpoint

Before configuring the Diameter AAA functionality you must configure the Diameter endpoint.

Use the following configuration example to configure Diameter endpoint:

```
configure

   context <context_name>

      diameter endpoint <endpoint_name>

         origin host <host_name> address <ipv4/ipv6_address> [ port <port_number>
] [ accept-incoming-connections ] [ address <ipv4/ipv6_address_secondary> ]

         peer <peer_name> [ realm <realm_name> ] address <ipv4/ipv6_address> [ [
port <port_number> ] [ connect-on-application-access ] [ send-dpr-before-
disconnect [ disconnect-cause <disconnect_cause> ] ] [ sctp ] ]+

         end
```

Notes:

- *Optional.* To support Diameter proxy server on per-PAC/PSC or per-system basis, in the Global Configuration Mode, use the following command:

  require diameter-proxy { master-slave | multiple | single }

- *<context_name>* must be the name of the system context designated for AAA configuration.
- *Optional.* To enable Diameter proxy for the endpoint, in the Diameter Endpoint Configuration Mode, use the following command:

  use-proxy

- *Optional.* To set the realm for the Diameter endpoint, in the Diameter Endpoint Configuration Mode, use the following command:

  origin realm *<realm_name>*

- *<realm_name>* is typically a company or service name. The realm is the Diameter identity and will be present in all Diameter messages.
- *Optional.* To create an entry in the route table for the Diameter peer, in the Diameter Endpoint Configuration Mode, use the following command:

  route-entry { [host *<host_name>* **] [peer** *<peer_id>* **] [realm** *<realm_name>* **] } [application credit-control] [weight** *<value>* **]**

- *Optional.* To specify the port for the Diameter endpoint, in the Diameter Endpoint Configuration Mode, use the following command:

  origin host *host_name* **address** *ipv4/ipv6_address* **[port** *port_number* **] [accept-incoming-connections] [address** *ipv4/ipv6_address_secondary* **]**

  Port number in the origin host should be configured only when the chassis is running in server mode, i.e. when **accept-incoming-connections** is configured.

  In this case it will open a listening socket on the specified port. For configurations where chassis is operating as a client, port number should not be included. In this case, a random source port will be chosen for outgoing connections. This is applicable for both with or without multi-homing.

  > ***Important:*** Currently if multi-homing is configured, then the specified port is used instead of randomly chosen port. This is done so that application knows which port is used by the kernel as it will have to use the same port while adding/removing IP address from the association. Nevertheless, configuring port number in origin host for client mode is not supported.

- *Optional.* To set how the action after failure, or recovery after failure is performed for the route table, in the Diameter Endpoint Configuration Mode, use the following command:

  route-failure { deadtime *<seconds>* **| recovery-threshold percent** *<percent>* **| result-code** *<result_code>* **| threshold** *<counter>* **}**

- *Optional.* To enable/disable the Transport Layer Security (TLS) support between Diameter client and Diameter server node, in the Diameter Endpoint Configuration Mode, use the following command:

  tls { certificate *<cert_string>* **| password** *<password>* **| privatekey** *<private_key>* **}**

- *Optional.* To set the connection timeout, in seconds, in the Diameter Endpoint Configuration Mode, use the following command:

  connection timeout *<timeout>*

- *Optional.* To set the connection retry timeout, in seconds, in the Diameter Endpoint Configuration Mode, use the following command:

```
connection retry-timeout <retry_timeout>
```

- *Optional.* To set the number of Device Watchdog Requests (DWRs) to be sent before the connection with a Diameter endpoint is closed, in the Diameter Endpoint Configuration Mode, use the following command:

  ```
  device-watchdog-request max-retries <retry_count>
  ```

- *Optional.* To set the maximum number of Diameter messages that any ACS Manager (ACSMgr)/Session Manager (SessMgr) may send to any one peer awaiting responses, in the Context Configuration Mode, use the following command:

  ```
  max-outstanding <msgs>
  ```

- *Optional.* To set the response timeout for the Diameter endpoint, in seconds, in the Diameter Endpoint Configuration Mode, use the following command:

  ```
  response-timeout <duration>
  ```

- *Optional.* To set the watchdog timeout for the Diameter endpoint, in seconds, in the Diameter Endpoint Configuration Mode, use the following command:

  ```
  watchdog-timeout <duration>
  ```

Configuring Diameter AAA Functionality at Context Level

There are context-level Diameter parameters that must be configured to provide AAA functionality for subscriber sessions. As noted in *Understanding the System Operation and Configuration* chapter of the *System Administration Guide*, AAA functionality can be configured within any context, even its own.

This section describes how to configure the Diameter-based AAA parameters at the context level. To configure Diameter-based AAA parameters at the system level, see the Configuring System-Level AAA Functionality section.

> ***Important:*** This section provides the minimum instruction set to configure context-level Diameter AAA functionality that allows the system to process data sessions. Commands that configure additional context-level AAA properties are provided in *Understanding the System Operation and Configuration* chapter of the *System Administration Guide*.

To configure Diameter AAA functionality at the context level use the following configuration:

```
configure
  context <context_name>
     diameter authentication endpoint <endpoint_name>
     diameter authentication server <host_name> priority <priority>
     diameter authentication dictionary <dictionary>
     diameter accounting endpoint <endpoint_name>
     diameter accounting server <host_name> priority <priority>
     diameter accounting dictionary <dictionary>
     end
```

Notes:

- *<context_name>* must be the name of the system context designated for AAA configuration.
- *<endpoint_name>* must be the same Diameter endpoint name configured in the Configuring Diameter Endpoint section.
- *Optional.* To configure the number of retry attempts for a Diameter authentication request with the same server, if the server fails to respond to a request, in the Context Configuration Mode, use the following command:

  diameter authentication max-retries *<tries>*
- *Optional.* To configure the maximum number of transmission attempts for a Diameter authentication request, in the Context Configuration Mode, use the following command. Use this in conjunction with the **max-retries** *<tries>* option to control how many servers will be attempted to communicate with.

  diameter authentication max-transmissions *<transmissions>*
- *Optional.* To configure how long the system must wait for a response from a Diameter server before re-transmitting the authentication request, in the Context Configuration Mode, use the following command:

  diameter authentication request-timeout *<duration>*
- *Optional.* To configure how many times a Diameter accounting request must be retried with the same server, if the server fails to respond to a request, in the Context Configuration Mode, use the following command:

  diameter accounting max-retries *<tries>*
- *Optional.* To configure the maximum number of transmission attempts for a Diameter accounting request, in the Context Configuration Mode, use the following command. You can use this in conjunction with the **max-retries tries** option to control how many servers will be attempted to communicate with.

  diameter accounting max-transmissions *<transmissions>*
- *Optional.* To configure how long the system will wait for a response from a Diameter server before re-transmitting the accounting request, in the Context Configuration Mode, use the following command:

  diameter accounting request-timeout *<duration>*

Verifying Your Configuration

To verify your configurations:

In the Exec mode, enter the following command:

show configuration context *<aaa_context_name>*

The output displays a concise list of settings that you have configured for the context.

Configuring Diameter Authentication Failure Handling

This section describes how to configure Diameter Authentication Failure Handling at the context level and the AAA group level.

Configuring at Context Level

This section describes how to configure context-level error handling for EAP requests / EAP termination requests. Specific actions (continue, retry-and-terminate, or terminate) can be associated with each possible result-code. Ranges of result codes can be defined with the same action, or actions can be specific on a per-result code basis.

To configure Diameter Authentication Failure Handling at the context level use the following configuration:

```
configure

   context <context_name>

      diameter authentication failure-handling { authorization-request | eap-
request | eap-termination-request } { request-timeout action { continue | retry-
and-terminate | terminate } | result-code <result_code> { [ to <result_code> ]
action { continue | retry-and-terminate | terminate } } }

      end
```

Notes:

- *<context_name>* must be the name of the system source context designated for subscriber configuration.

Configuring at AAA Group Level

This section describes how to configure error handling for EAP requests / EAP termination requests at the AAA group level. Specific actions (continue, retry-and-terminate, or terminate) can be associated with each possible result-code. Ranges of result codes can be defined with the same action, or actions can be specific on a per-result code basis.

To configure Diameter Authentication Failure Handling at the AAA group level use the following configuration example:

```
configure

   context <context_name>

      aaa group <group_name>

         diameter authentication failure-handling { authorization-request | eap-
request | eap-termination-request } { request-timeout action { continue | retry-
and-terminate | terminate } | result-code <result_code> { [ to <result_code> ]
action { continue | retry-and-terminate | terminate } } }

         end
```

Notes:

- *<context_name>* must be the name of the system source context designated for subscriber configuration.
- *<group_name>* must be the name of the AAA group designated for AAA functionality within the specific context.

Configuring System-Level AAA Functionality

There are system-level AAA parameters that must be configured in order to provide AAA functionality for subscriber and context-level administrative user sessions. As noted in *Understanding the System Operation and Configuration* chapter of the *System Administration Guide*, AAA functionality can be configured within any context, even its own.

Important: Commands used in the configuration examples in this section provide base functionality to the extent that the most common or likely commands and/or keyword options are presented. In many cases, other optional commands and/or keyword options are available. Refer to the *Command Line Interface Reference* for complete information regarding all commands.

This procedure applies to both RADIUS and Diameter.

To configure system-level AAA functionality use the following configuration:

```
configure

   aaa default-domain subscriber <domain_name>

   aaa default-domain administrator <domain_name>

   aaa last-resort context subscriber <context_name>

   aaa last-resort context administrator <context_name>

   aaa username-format { domain | username } { @ | % | - | \ | # | / }

   end
```

Notes:

- *<domain_name>* is the name of the domain, or context, to use for performing AAA functions in the subscriber session. For information on the role of the default domain in the context selection process can be found in the *Understanding the System Operation and Configuration* chapter of the *System Administration Guide*.
- *<context_name>* must be the name of the context to use for performing AAA functions in the subscriber session. Additional information on the role of the last-resort context in the context selection process can be found in the *Understanding the System Operation and Configuration* chapter of the *System Administration Guide*.
- Up to six user name formats can be configured. The default format is username@domain.

Verifying your configuration

To verify your configuration:

In the Exec mode, enter the following command:

show configuration context *<context_name>*

In the output, verify the AAA settings that you have configured in this user session.

Configuring AAA Server Group for AAA Functionality

In addition to the AAA configurations, a AAA server group feature can be configured at the context-level to manage subscriber authentication and accounting through configuring AAA servers into groups.

In general, 128 AAA Server IP address/port per context can be configured on the system and the system selects servers from this list depending on the server selection algorithm (round robin, first server). Instead of having a single list of servers per context, this feature provides the ability to configure multiple server groups. Each server group, in turn, consists of a list of servers.

This feature works in the following way:

- All authentication/accounting servers configured at the context-level are treated as part of a server group named "default". This default server group is available to all subscribers in that context through the realm (domain)/APN without any additional configuration.
- It provides a facility to create "user defined" AAA server groups, as many as 799 (excluding "default" server group), within a context. Any of the user-defined AAA server groups are available for assignment to a subscriber through the realm (domain)/APN configuration within that context.
- Subscribers/services/APNs/etc. are bound to a AAA group, which serves to define what Diameter/RADIUS server will be used for each AAA function (authentication, accounting, charging, and so on). Based on the request type the RADIUS or Diameter protocol type is selected to handle the AAA requests to be sent to the respective server.

AAA server group configuration is performed at the context-level. Different subscribers may use the same AAA context, but different AAA server groups only. Server configuration defined in the subscriber profile/APN template supersedes the servers or server groups configuration defined in context mode.

AAA server groups are assigned to the subscriber through realm (domain) configuration for all services. For GGSN service AAA server groups can be assigned to the subscriber through APN configuration also.

To configure AAA Server Group for AAA functionality:

Step 1 Configure the AAA Server Group as described in the AAA Server Group Configuration section.

- Apply the AAA Server Group to subscriber as described in the Applying a AAA Server Group to a Subscriber section.

  –or–

- Apply the AAA server-group to an APN as described in the Applying a AAA Server Group to an APN section.

Step 2 Save your configuration to flash memory, an external memory device, and/or a network location using the Exec mode command **`save configuration`**. For additional information on how to verify and save configuration files, refer to the *System Administration Guide* and the *Command Line Interface Reference*.

Important: Commands used in the configuration examples in this section provide base functionality to the extent that the most common or likely commands and/or keyword options are presented. In many cases, other optional commands and/or keyword options are available. Refer to the *Command Line Interface Reference* for complete information regarding all commands.

AAA Server Group Configuration

This section describes how to configure the context to use a group of AAA servers for subscriber authentication and accounting through subscriber/realm (domain)/APN configuration.

There are context-level AAA parameters that must be configured in order to provide AAA server group functionality for subscriber sessions.

Important: This section provides the minimum instruction set for configuring a AAA server group for AAA functionality. Commands that configure other properties of this functionality are provided in the *Command Line Interface Reference*.

To configure a AAA server group use the following configuration:

```
configure
   context <context_name>
      aaa group <group_name>
      end
```

Notes:

- Up to 128 authentication and/or accounting servers can be configured per AAA server group. A maximum of 1600 servers can be configured system-wide regardless of the number of groups unless **aaa large-configuration** is enabled.
- *Optional.* If you want to support more than 64 server groups system-wide, in the Global Configuration Mode, use the following command:

  aaa large-configuration
- *<context_name>* must be the name of the system context designated for AAA functionality configuration.
- *<group_name>* must be the name of the AAA group designated for AAA functionality within the specific context. A total of 800 server groups can be configured system-wide including default server-group unless **aaa large-configuration** is enabled.
- The same AAA server with IP address and port number can be configured with multiple AAA server groups within a context.
- To configure and verify RADIUS authentication and accounting servers and parameters within the AAA server group, refer to the Configuring RADIUS AAA Functionality section.
- To configure and verify Diameter authentication and accounting servers and parameters within the AAA server group, refer to the Configuring Diameter AAA Functionality section.

Verifying Your Configuration

To verify your configuration:

Step 1 Change to the context in which the AAA server group was configured by entering the following command:

context *<context_name>*

Step 2 Display the context's configuration by entering the following command:

```
show configuration context <context_name>
```

Step 3 In the output verify the server group's configuration.

> ***Important:*** The "default" server group in a context is applicable to all subscribers/APNs within that context by default.

Applying a AAA Server Group to a Subscriber

The following procedure assumes that a domain alias was previously configured as described in *Creating Contexts* section of the *System Administration Guide*.

To apply AAA server group to a subscriber use the following configuration example:

```
configure
   context <context_name>
      subscriber name <subscriber_name>
         aaa group <group_name>
         end
```

Notes:

- *<context_name>* must be the name of the system source context designated for subscriber configuration.
- *<sub_name>* must be the name of the subscriber template configured as the default template for the domain. For more information on creating contexts, refer to the *Creating Contexts* section of the *System Element Configuration Procedures* chapter in the *System Administration Guide*.
- *<group_name>* must be the name of the AAA server group designated for AAA functionality within the context as described in the AAA Server Group Configuration section.

Verifying Subscriber Configuration

Step 1 Change to the context in which the AAA server group was configured by entering the following command:

```
context <context_name>
```

Step 2 Display the subscriber's configuration by entering the following command:

```
show subscribers configuration username <subscriber_name>
```

Step 3 In the output verify the subscriber's configuration.

Applying a AAA Server Group to an APN

After configuring a AAA server group at context-level, an APN within the same context can be configured to use the user-defined server group.

Use the following configuration example to apply a user-defined AAA server group functionality to a previously configured APN within the same context.

```
configure
  context <context_name>
      apn <apn_name>
         aaa group <group_name>
         end
```

Notes:

- *<group_name>* must be the name of the AAA server group previously configured for AAA functionality in a specific context as described in the AAA Server Group Configuration section.

Verifying APN Configuration

Step 1 Change to the context in which the AAA server group was configured by entering the following command:

context *<context_name>*

Step 2 Display the APN's configuration by entering the following command:

show apn name *<apn_name>*

Step 3 In the output verify the APN's configuration.

Configuring the Destination Context Attribute

Once a user has been authenticated, a AAA attribute is returned in the access-accept message that contains the name of the destination context where the subscriber will egress from. For RADIUS-based subscribers, this is the SN-VPN-NAME attribute, or SN1-VPN-NAME attribute in some RADIUS dictionaries.

Note that when performing RADIUS authentication and authorization, RADIUS attributes returned by the RADIUS server always take precedence over the default subscriber configuration.

The system supports configuring subscriber profiles locally within a context though subscriber templates or on a RADIUS server. Subscribers configured on the system are configured within the contexts they were created. In the *Understanding the System Operation and Configuration* chapter of the *System Administration Guide*, the role of subscriber default, which is automatically configured for each context, and realm-based subscriber templates, which serves as a default subscriber template for users whose domain portion of their user name matches a domain alias within a context, was discussed. The role of these special subscriber templates is to provide a set of default attributes that may be used to populate any missing values for an authenticated RADIUS-based subscriber. The parameter that would contain this attribute value is called the IP context-name.

Further, it was explained that these attributes must be configured manually for both the subscriber default and any realm-based subscriber template created.

One of the rules that must be configured is a parameter that allows subscriber data traffic to be routed between source and destination contexts. Use the following example configuration to configure that rule.

Important: Commands used in the configuration example in this section provide base functionality to the extent that the most common or likely commands and/or keyword options are presented. In many cases, other optional commands and/or keyword options are available. Refer to the *Command Line Interface Reference* for complete information regarding all commands.

```
configure
   context <context_name>
      subscriber name default
         ip context-name <destination_context_name>
         end
```

Notes:

- *<context_name>* must be the name of the system source context designated for Default subscriber configuration.
- *<destination_context_name>* must be the name of the destination context configured on the system containing the interfaces through which session traffic is routed.
- The “ip context-name” parameter in the subscriber profiles configured on the system corresponds to the SN-VPN-NAME and SN1-VPN-NAME RADIUS attributes.
- Configure the default subscriber in any other configured source contexts.

Verifying Your Configuration

To verify your global AAA configurations:

In the Exec mode, use the following command:

`show configuration`

The output displays all the settings that you have configured in this user session. Verify the default-domain, last-resort, and username-format settings.

Chapter 3
Managing and Monitoring the AAA Servers

This chapter provides information for managing and monitoring the AAA server status and performance using the commands found in the Command Line Interface (CLI). These command have many related keywords that allow them to provide useful information on all aspects of the AAA interface activity and status.

The selection of keywords described in this chapter is intended to provided the most useful and in-depth information for monitoring AAA managers, interface, and servers on the system. For additional information on these command keywords, refer to the *Command Line Interface Reference*.

In addition to the CLI, the system supports the sending of Simple Network Management Protocol (SNMP) traps that indicate status and alarm conditions. Refer to the *SNMP MIB Reference* for a detailed listing of these traps.

This chapter includes the following sections:

- Managing the AAA Servers
- Monitoring AAA Status and Performance
- Clearing Statistics and Counters

Managing the AAA Servers

This section provides information and instructions for using the system Command Line Interface (CLI) for troubleshooting the network reachability issues for AAA servers that may arise during system operation.

The following topics are discussed in this section:

- Using the RADIUS Testing Tools

Using the RADIUS Testing Tools

The CLI provides a mechanism for testing network connectivity with and configuration of RADIUS authentication and accounting servers. This functionality can be extremely useful in determining the accuracy of the system's RADIUS configuration, the configuration of the subscriber profile on the RADIUS server, and troubleshooting the server's response time.

Testing a RADIUS Authentication Server

When used to test a RADIUS authentication server, the tool generates an authentication request message for a specific user name.

Important: The user name must already be configured on the RADIUS authentication server prior to executing the test.

To execute the RADIUS authentication test tool, in the Exec mode, use the following command:

```
radius test authentication { all | radius group <group_name> | server
<server_name> port <server_port> } <user_name> <password>
```

Notes:

- **all** specifies that all configured RADIUS authentication servers be tested.
- **radius group** *<group_name>* specifies the configured RADIUS authentication servers in a RADIUS server group named *<group_name>* for server group functionality.
- *<server_name>* specifies the IP address of a specific RADIUS authentication server to test.
- *<server_port>* specifies the TCP port over that the system should use when communicating with the RADIUS authentication server to test.
- *<user_name>* specifies a username that is supplied to the RADIUS server for authentication.
- *<password>* specifies the password associated with the username that is supplied to the RADIUS server for authentication.

The following is a sample of this command's output for a successful response when testing a RADIUS authentication server with an IP address of 192.168.250.150 on port 1812.

```
Authentication from authentication server 192.168.250.150, port 1812

Authentication Success: Access-Accept received
```

```
Round-trip time for response was 8.8 ms
```

Testing a RADIUS Accounting Server

When used to test a RADIUS accounting server, the tool generates an accounting start/stop pair for a specific username.

Important: The user name must already be configured on the RADIUS authentication server prior to executing the test.

To execute the RADIUS authentication test tool, enter the following command:

radius test accounting { all | radius group *<group_name>* **| server** *<server_name>* **port** *<server_port>* **}** *<user_name>*

Notes:

- **all** specifies that all configured RADIUS accounting servers be tested.
- **radius group** *<group_name>* specifies the configured RADIUS authentication servers in a RADIUS server group named *<group_name>* for server group functionality.
- *<server_name>* specifies the IP address of a specific RADIUS accounting server to test.
- *<server_port>* specifies the TCP port over that the system should use when communicating with the RADIUS accounting server to test.
- *<user_name>* specifies a username that is supplied to the RADIUS server for accounting.

The following is a sample of this command's output for a successful response when testing a RADIUS accounting server with an IP address of 192.168.1.102 on port 1813.

```
RADIUS Start to accounting server 192.168.1.102, port 1813

Accounting Success: response received

Round-trip time for response was 554.6 ms

RADIUS Stop to accounting server 192.168.1.102, port 1813

Accounting Success: response received

Round-trip time for response was 85.5 ms
```

Monitoring AAA Status and Performance

This section describes the commands used to monitor the status of AAA servers in the service. Output descriptions for most of the commands are available in the *Statistics and Counters Reference*.

To do this:	Enter this command:
View AAA Manager statistics	**show session subsystem facility aaamgr all**
View AAA and RADIUS Counters	
Display Local AAA Counters	
View Local AAA counters for the current context	**show aaa local counters**
Display RADIUS Server States ***Important:*** These commands can display 10 state transition histories of RADIUS accounting and authentication servers (Active/Not responding/Down States). For explanation of RADIUS server states, refer to the *RADIUS Server State Behavior* Appendix.	
View RADIUS accounting server states	**show radius accounting servers detail**
View RADIUS authentication server states	**show radius authentication servers detail**
Display RADIUS Server Group Server States ***Important:*** RADIUS Server Group functionality is a license controlled feature. A valid feature license must be installed prior to configuring RADIUS group for AAA functionality. If you have not previously purchased this enhanced feature, contact your sales representative for more information. For explanation of RADIUS server states, refer to the *RADIUS Server State Behavior* Appendix.	
View RADIUS authentication server group server states for a specific group	**show radius authentication servers radius group** *<group_name>* **detail**
View RADIUS accounting server group server states for a specific group	**show radius accounting servers radius group** *<group_name>* **detail**
Display RADIUS Protocol Counters	
View cumulative RADIUS protocol counters	**show radius counters all**
View RADIUS protocol counter summary of RADIUS authentication and accounting	**show radius counters summary**

Clearing Statistics and Counters

It may be necessary to periodically clear statistics and counters in order to gather new information. The system provides the ability to clear statistics and counters based on their grouping (PPP, MIPHA, MIPFA, etc.).

Statistics and counters can be cleared using the CLI **clear** commands. For detailed information on using this command, refer to the *Command Line Interface Reference*.

Session Recovery and AAA Statistics Behavior

After a Session Recovery operation, some statistics/counters, such as those collected and maintained on a per manager basis (AAA Manager, Session Manager, etc.) are in general not recovered, only accounting/billing related information is checkpointed/recovered.

For more information, refer to the *System Administration Guide*.

Chapter 4
Diameter Dictionaries and Attribute Definitions

This chapter presents information on Diameter dictionary types and attribute definitions.

Diameter Attributes

Diameter Attribute Value Pairs (AVPs) carry specific authentication, accounting, authorization, routing and security information as well as configuration details for the request and reply.

Some AVPs may be listed more than once. The effect of such an AVP is specific, and is specified in each case by the AVP description.

Each AVP of type OctetString must be padded to align on a 32-bit boundary, while other AVP types align naturally. A number of zero-valued bytes are added to the end of the AVP Data field till a word boundary is reached. The length of the padding is not reflected in the AVP Length field.

AVP Header

The AVP header contains three fields that requires IANA namespace management

- AVP Code
- Vendor-ID
- Flags

The fields in the AVP header MUST be sent in network byte order. The format of the header is:

Figure 2. AVP Header

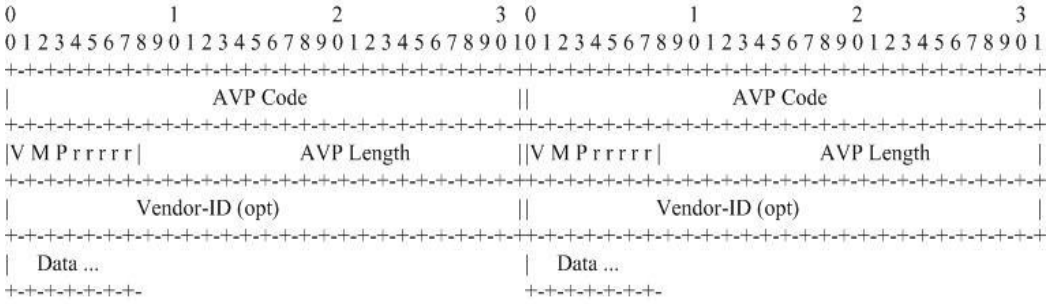


Table 1. AVP Header Details

Field	Description
AVP Code	The AVP Code, combined with the Vendor-ID field, identifies the attribute uniquely. AVP numbers 1 through 255 are reserved for backward compatibility with RADIUS, without setting the Vendor-ID field. AVP numbers 256 and above are used for Diameter, which are allocated by IANA.

Field	Description
AVP Flags	The AVP Flags field informs the receiver how each attribute must be handled. The 'r' (reserved) bits are unused and SHOULD be set to 0. Note that subsequent Diameter applications may define additional bits within the AVP Header, and an unrecognized bit SHOULD be considered an error. The 'P' bit indicates the need for encryption for end-to-end security. The 'M' Bit, known as the Mandatory bit, indicates whether support of the AVP is required. If an AVP with the 'M' bit set is received by a Diameter client, server, proxy, or translation agent and either the AVP or its value is unrecognized, the message MUST be rejected. Diameter Relay and redirect agents MUST NOT reject messages with unrecognized AVPs. The 'M' bit MUST be set according to the rules defined for the AVP containing it. In order to preserve interoperability, a Diameter implementation MUST be able to exclude from a Diameter message any Mandatory AVP which is neither defined in the base Diameter protocol nor in any of the Diameter Application specifications governing the message in which it appears. It may do this in one of the following ways: • If a message is rejected because it contains a Mandatory AVP which is neither defined in the base Diameter standard nor in any of the Diameter Application specifications governing the message in which it appears, the implementation may resend the message without the AVP, possibly inserting additional standard AVPs instead. • A configuration option may be provided on a system wide, per peer, or per realm basis that would allow/prevent particular Mandatory AVPs to be sent. Thus an administrator could change the configuration to avoid interoperability problems. Diameter implementations are required to support all Mandatory AVPs which are allowed by the message's formal syntax and defined either in the base Diameter standard or in one of the Diameter Application specifications governing the message. AVPs with the 'M' bit cleared are informational only and a receiver that receives a message with such an AVP that is not supported, or whose value is not supported, MAY simply ignore the AVP. The 'V' bit, known as the Vendor-Specific bit, indicates whether the optional Vendor-ID field is present in the AVP header. When set the AVP Code belongs to the specific vendor code address space. Unless otherwise noted, AVPs will have the following default AVP Flags field settings: The 'M' bit MUST be set. The 'V' bit MUST NOT be set.
AVP Length	The AVP Length field is three octets, and indicates the number of octets in this AVP including the AVP Code, AVP Length, AVP Flags, Vendor-ID field (if present) and the AVP data. If a message is received with an invalid attribute length, the message SHOULD be rejected.
Vendor-ID	This field is optional. The Vendor-ID field is present if the 'V' bit is set in the AVP Flags field. The optional four-octet Vendor-ID field contains the IANA assigned "SMI Network Management Private Enterprise Codes" value, encoded in network byte order. Any vendor wishing to implement a vendor-specific Diameter AVP MUST use their own Vendor-ID along with their privately managed AVP address space, guaranteeing that they will not collide with any other vendor's vendor-specific AVP(s), nor with future IETF applications. A vendor ID value of zero (0) corresponds to the IETF adopted AVP values, as managed by the IANA. Since the absence of the vendor ID field implies that the AVP in question is not vendor specific, implementations MUST NOT use the zero (0) vendor ID.

Basic AVP Data Formats

The Data field is zero or more octets and contains information specific to the attribute. The format and length of the Data field is determined by the AVP Code and AVP Length fields. The format of the Data field MUST be one of the following base data types or a data type derived from the base data types.

Table 2. Basic AVP Formats

AVP Data Format	Meaning
OctetString	The data contains arbitrary data of variable length. Unless otherwise noted, the AVP Length field MUST be set to at least 8 (12 if the 'V' bit is enabled). AVP Values of this type that are not a multiple of four-octets in length is followed by the necessary padding so that the next AVP (if any) will start on a 32-bit boundary.
Integer32	32 bit signed value, in network byte order. The AVP Length field MUST be set to 12 (16 if the 'V' bit is enabled).
Integer64	64 bit signed value, in network byte order. The AVP Length field MUST be set to 16 (20 if the 'V' bit is enabled).
Unsigned32	32 bit unsigned value, in network byte order. The AVP Length field MUST be set to 12 (16 if the 'V' bit is enabled).
Unsigned64	64 bit unsigned value, in network byte order. The AVP Length field MUST be set to 16 (20 if the 'V' bit is enabled).
Float32	This represents floating point values of single precision. The 32-bit value is transmitted in network byte order. The AVP Length field MUST be set to 12 (16 if the 'V' bit is enabled).
Float64	This represents floating point values of double precision. The 64-bit value is transmitted in network byte order. The AVP Length field MUST be set to 16 (20 if the 'V' bit is enabled).
Grouped	The Data field is specified as a sequence of AVPs. Each of these AVPs follows - in the order in which they are specified - including their headers and padding. The AVP Length field is set to 8 (12 if the 'V' bit is enabled) plus the total length of all included AVPs, including their headers and padding. Thus the AVP length field of an AVP of type Grouped is always a multiple of 4.

Derived AVP Data Formats

In addition to using the Basic AVP Data Formats, applications may define data formats derived from the Basic AVP Data Formats. An application that defines new AVP Derived Data Formats MUST include them in a section entitled "AVP Derived Data Formats", using the same format as the definitions below. Each new definition must be either defined or listed with a reference to the RFC that defines the format.

The below AVP Derived Data Formats are commonly used by applications.

Address

The Address format is derived from the OctetString AVP Base Format. It is a discriminated union, representing, for example a 32-bit (IPv4) or 128-bit (IPv6) address, most significant octet first. The first two octets of the Address

AVP represents the AddressType, which contains an Address Family defined in IANAADFAM. The AddressType is used to discriminate the content and format of the remaining octets.

Time

The Time format is derived from the OctetString AVP Base Format. The string MUST contain four octets, in the same format as the first four bytes are in the NTP timestamp format.

This represents the number of seconds since 0h on 1 January 1900 with respect to the Coordinated Universal Time (UTC).

On 6h 28m 16s UTC, 7 February 2036 the time value will overflow. SNTP describes a procedure to extend the time to 2104. This procedure MUST be supported by all DIAMETER nodes.

UTF8String

The UTF8String format is derived from the OctetString AVP Base Format. This is a human readable string represented using the ISO/IEC IS 10646-1 character set, encoded as an OctetString using the UTF-8 [UFT8] transformation format described in RFC 2279.

Since additional code points are added by amendments to the 10646 standard from time to time, implementations MUST be prepared to encounter any code point from 0x00000001 to 0x7fffffff. Byte sequences that do not correspond to the valid encoding of a code point into UTF-8 charset or are outside this range are prohibited.

The use of control codes SHOULD be avoided. When it is necessary to represent a new line, the control code sequence CR LF SHOULD be used.

The use of leading or trailing white space SHOULD be avoided.

For code points not directly supported by user interface hardware or software, an alternative means of entry and display, such as hexadecimal, MAY be provided.

For information encoded in 7-bit US-ASCII, the UTF-8 charset is identical to the US-ASCII charset.

UTF-8 may require multiple bytes to represent a single character / code point; thus the length of an UTF8String in octets may be different from the number of characters encoded.

Note that the AVP Length field of an UTF8String is measured in octets, not characters.

DiameterIdentity

The DiameterIdentity (DIAMIDENT) format is derived from the OctetString AVP Base Format.

DiameterIdentity = FQDN

DiameterIdentity value is used to uniquely identify a Diameter node for purposes of duplicate connection and routing loop detection.

The contents of the string MUST be the FQDN of the Diameter node. If multiple Diameter nodes run on the same host, each Diameter node MUST be assigned a unique DiameterIdentity. If a Diameter node can be identified by several FQDNs, a single FQDN should be picked at startup, and used as the only DiameterIdentity for that node, whatever the connection it is sent on.

DiameterURI

The DiameterURI (DIAMURI) MUST follow the Uniform Resource Identifiers (URI) syntax [URI] rules specified below:

```
"aaa://" FQDN [ port ] [ transport ] [ protocol ]
```

– or –

```
"aaas://" FQDN [ port ] [ transport ] [ protocol ]
```

Table 3. DiameterURI Field Description

Field	Description
FQDN	Fully Qualified Host Name
port	One of the ports used to listen for incoming connections. If absent, the default Diameter port (3868) is assumed.
transport	One of the transport protocols used to listen for incoming connections. If absent, the default SCTP protocol is assumed. UDP MUST NOT be used when the aaa-protocol field is set to diameter. The transport protocol could be tcp, sctp, or udp.
protocol	This field denotes AAA protocol. If absent, the default AAA protocol is diameter. The AAA protocol could be diameter, radius, or tacacs+.

The following are examples of valid Diameter host identities:

```
aaa://host.example.com;transport=tcp

aaa://host.example.com:6666;transport=tcp

aaa://host.example.com;protocol=diameter

aaa://host.example.com:6666;protocol=diameter

aaa://host.example.com:6666;transport=tcp;protocol=diameter

aaa://host.example.com:1813;transport=udp;protocol=radius
```

Enumerated

Enumerated is derived from the Integer32 AVP Base Format. The definition contains a list of valid values and their interpretation and is described in the Diameter application introducing the AVP.

IPFilterRule

The IPFilterRule format is derived from the OctetString AVP Base Format. It uses the ASCII charset. Packets may be filtered based on the following information that is associated with it:

- Direction (in or out)
- Source and destination IP address (possibly masked)
- Protocol
- Source and destination port (lists or ranges)
- TCP flags
- IP fragment flag
- IP options
- ICMP types

Rules for the appropriate direction are evaluated in order, with the first matched rule terminating the evaluation. Each packet is evaluated once. If no rule matches, the packet is dropped if the last rule evaluated was a permit, and passed if the last rule was a deny.

IPFilterRule filters MUST follow the format:

```
action dir proto from src to dst [options]
```

Table 4. IPFilterRule Field Description

Field	Description
action	This field can be set to one of the following: • permit – Allow packets that match the rule. • deny – Drop packets that match the rule.
dir	"in" is from the terminal and "out" is to the terminal.
proto	An IP protocol specified by number. The "ip" keyword means any protocol will match.
src and dst	<address/mask> [ports] The <address/mask> may be specified as: ipno — An IPv4 or IPv6 number in dotted-quad or canonical IPv6 form. Only this exact IP number will match the rule. ipno/bits — An IP number as above with a mask width of the form 1.2.3.4/24. In this case, all IP numbers from 1.2.3.0 to 1.2.3.255 will match. The bit width MUST be valid for the IP version and the IP number MUST NOT have bits set beyond the mask. For a match to occur, the same IP version must be present in the packet that was used in describing the IP address. To test for a particular IP version, the bits part can be set to zero. The keyword "any" is 0.0.0.0/0 or the IPv6 equivalent. The keyword "assigned" is the address or set of addresses assigned to the terminal. For IPv4, a typical first rule is often "deny in ip! assigned" The sense of the match can be inverted by preceding an address with the not modifier (!), causing all other addresses to be matched instead. This does not affect the selection of port numbers. With the TCP, UDP and SCTP protocols, optional ports may be specified as: `{port/port-port}[,ports[,...]]` The '-' notation specifies a range of ports (including boundaries). Fragmented packets that have a non-zero offset (i.e., not the first fragment) will never match a rule that has one or more port specifications. See the frag option for details on matching fragmented packets.

Field	Description
options	The different options are as follows: • frag — Match if the packet is a fragment and this is not the first fragment of the datagram. frag may not be used in conjunction with either tcpflags or TCP/UDP port specifications. • ipoptions spec — Match if the IP header contains the comma separated list of options specified in spec. The supported IP options are: ssrr (strict source route), lsrr (loose source route), rr (record packet route) and ts (timestamp). The absence of a particular option may be denoted with a '!'. • tcpoptions spec — Match if the TCP header contains the comma separated list of options specified in spec. The supported TCP options are: mss (maximum segment size), window (tcp window advertisement), sack (selective ack), ts (rfc1323 timestamp) and cc (rfc1644 t/tcp connection count). The absence of a particular option may be denoted with a '!'. • established — TCP packets only. Match packets that have the RST or ACK bits set. • setup — TCP packets only. Match packets that have the SYN bit set but no ACK bit. • tcpflags spec — TCP packets only. Match if the TCP header contains the comma separated list of flags specified in spec. The supported TCP flags are: fin, syn, rst, psh, ack and urg. The absence of a particular flag may be denoted with a '!'. A rule that contains a tcpflags specification can never match a fragmented packet that has a non-zero offset. See the frag option for details on matching fragmented packets. • icmptypes types — ICMP packets only. Match if the ICMP type is in the list types. The list may be specified as any combination of ranges or individual types separated by commas. Both the numeric values and the symbolic values listed below can be used. The supported ICMP types are: echo reply (0), destination unreachable (3), source quench (4), redirect (5), echo request (8), router advertisement (9), router solicitation (10), time-to-live exceeded (11), IP header bad (12), timestamp request (13), timestamp reply (14), information request (15), information reply (16), address mask request (17) and address mask reply (18).

QoSFilterRule

The QosFilterRule format is derived from the OctetString AVP Base Format. It uses the ASCII charset. Packets may be marked or metered based on the following information that is associated with it:

- Direction (in or out)
- Source and destination IP address (possibly masked)
- Protocol
- Source and destination port (lists or ranges)
- DSCP values (no mask or range)

Rules for the appropriate direction are evaluated in order, with the first matched rule terminating the evaluation. Each packet is evaluated once. If no rule matches, the packet is treated as best effort. An access device that is unable to interpret or apply a QoS rule SHOULD NOT terminate the session

QoSFilterRule filters MUST follow the format:

```
action dir proto from src to dst [options]
```

Table 5. QoSFilterRule Field Description

Field	Description
action	This field can be set to one of the following: • tag — Mark packet with a specific DSCP [DIFFSERV]. The DSCP option MUST be included. • meter — Meter traffic. The metering options MUST be included.
dir	The format is as described under IPFilterRule.
proto	The format is as described under IPFilterRule.
src and dst	The format is as described under IPFilterRule.
options	The following options are available in addition to the ones described under IPFilterRule: • DSCP <*color*> — Color values as defined in [DIFFSERV]. Exact matching of DSCP values is required (no masks or ranges). • metering <*rate*> <*color_under*> <*color_over*> — The metering option provides Assured Forwarding, as defined in [DIFFSERVAF], and MUST be present if the action is set to meter. The rate option is the throughput, in bits per second, which is used by the access device to mark packets. Traffic above the rate is marked with the color_over codepoint, while traffic under the rate is marked with the *color_under* codepoint. The *color_under* and *color_over* options contain the drop preferences, and MUST conform to the recommended codepoint keywords described in [DIFFSERVAF] (e.g. AF13). The metering option also supports the strict limit on traffic required by Expedited Forwarding, as defined in [DIFFSERVEF]. The *color_over* option may contain the keyword "drop" to prevent forwarding of traffic that exceeds the rate parameter.

Grouped AVP Values

The Diameter protocol allows AVP values of type 'Grouped.' This implies that the Data field is actually a sequence of AVPs. It is possible to include an AVP with a Grouped type within a Grouped type, that is, to nest them. AVPs within an AVP of type Grouped have the same padding requirements as non-Grouped AVPs.

The AVP Code numbering space of all AVPs included in a Grouped AVP is the same as for non-grouped AVPs. Further, if any of the AVPs encapsulated within a Grouped AVP has the 'M' (mandatory) bit set, the Grouped AVP itself MUST also include the 'M' bit set.

Every Grouped AVP defined MUST include a corresponding grammar, using ABNF (with modifications), as defined below.

```
grouped-avp-def = name "::=" avp

name-fmt = ALPHA *(ALPHA / DIGIT / "-")

name = name-fmt

avp = header [ *fixed] [ *required] [ *optional] [ *fixed]

header = "<" "AVP-Header:" avpcode [vendor] ">"
```

```
avpcode = 1*DIGIT

vendor = 1*DIGIT
```

Where, name = the name of an AVP, defined in the base or extended Diameter specifications.

avp code = The AVP Code assigned to the Grouped AVP.

vendor = The Vendor-ID assigned to the Grouped AVP. If absent, the default value of zero is used.

The Example-AVP (AVP Code 999999) is of type Grouped and is used to clarify how Grouped AVP values work. The Grouped Data field has the following ABNF grammar:

```
Example-AVP ::= < AVP Header: 999999 >

 { Origin-Host }

 1*{ Session-Id }

 *[ AVP ]
```

An Example-AVP with Grouped Data follows. The Origin-Host AVP is required.

In this case, Origin-Host = "example.com".

One or more Session-IDs must follow. Here there are two:

```
Session-Id = "grump.example.com:33041;23432;893;0AF3B81"

Session-Id = "grump.example.com:33054;23561;2358;0AF3B82"
```

Optional AVPs included are:

```
Recovery-Policy = <binary>
2163bc1d0ad82371f6bc09484133c3f09ad74a0dd5346d54195a7cf0b35
2cabc881839a4fdcfbc1769e2677a4c1fb499284c5f70b48f58503a45c5
c2d6943f82d5930f2b7c1da640f476f0e9c9572a50db8ea6e51e1c2c7bd
f8bb43dc995144b8dbe297ac739493946803e1cee3e15d9b765008a1b2a
cf4ac777c80041d72c01e691cf751dbf86e85f509f3988e5875dc905119
26841f00f0e29a6d1ddc1a842289d440268681e052b30fb638045f7779c
1d873c784f054f688f5001559ecff64865ef975f3e60d2fd7966b8c7f92

Futuristic-Acct-Record = <binary>
fe19da5802acd98b07a5b86cb4d5d03f0314ab9ef1ad0b67111ff3b90a0
57fe29620bf3585fd2dd9fcc38ce62f6cc208c6163c008f4258d1bc88b8
17694a74ccad3ec69269461b14b2e7a4c111fb239e33714da207983f58c
41d018d56fe938f3cbf089aac12a912a2f0d1923a9390e5f789cb2e5067 d3427475e49968f841
```

The data for the optional AVPs is represented in hexadecimal since the format of these AVPs is neither known at the time of definition of the Example-AVP group, nor (likely) at the time when the example instance of this AVP is interpreted - except by Diameter implementations which support the same set of AVPs. Also note that AVPs may be present in the Grouped AVP value which the receiver cannot interpret (here, the Recover-Policy and Futuristic-Acct-Record AVPs).

Diameter AVP Definitions

This section presents Diameter attribute definitions.

3GPP-CAMEL-Charging-Info

This AVP contains the Customized Application for Mobile Enhanced Logic (CAMEL) charging information.

Vendor ID
10415

VSA Type
24

AVP Type
UTF8STRING

AVP Flag
N/A

3GPP-CF-IPv6-Address

3GPP-CF-IPv6-Address

Vendor ID
10415

VSA Type
14

AVP Type
OCTETSTRING

AVP Flag
M

3GPP-CG-Address

This AVP contains address of the Charging Gateway.

Vendor ID
10415

VSA Type
4

AVP Type
OCTETSTRING

AVP Flag
M

3GPP-Called-Station-Id

This AVP contains the Layer 2 addresses that the user contacted in the request.

Vendor ID
10415

VSA Type
30

AVP Type
OCTETSTRING

AVP Flag
N/A

3GPP-Charging-Characteristics

This AVP contains the charging characteristics for this PDP context received in the Create PDP Context Request Message.

Vendor ID
10415

VSA Type
13

AVP Type
UTF8STRING

AVP Flag
M

3GPP-Charging-Id

This AVP contains the Charging ID for this PDP context (this together with the GGSN-Address constitutes a unique identifier for the PDP context).

Vendor ID
10415

VSA Type
2

AVP Type
UINT32

AVP Flag
M

3GPP-GGSN-Address

This AVP contains the IP address of the GGSN used by the GTP control plane for context establishment. It is the same as the GGSN IP address used in the G-CDRs.

Vendor ID
10415

VSA Type
7

AVP Type
OCTETSTRING

AVP Flag
M

3GPP-GGSN-MCC-MNC

This AVP contains MCC-MNC of the network that the GGSN belongs to.

Vendor ID
10415

VSA Type
9

AVP Type
UTF8STRING

AVP Flag
M

3GPP-GPRS-QoS-Negotiated-Profile

This AVP contains QoS profile applied by GGSN.

Vendor ID
10415

VSA Type
5

AVP Type
UTF8STRING

AVP Flag
M

3GPP-IMEISV

This AVP contains International Mobile Equipment ID (IMEI) and its Software Version (SV).

Vendor ID
10415

VSA Type
20

AVP Type
OCTETSTRING

AVP Flag
M

3GPP-IMSI

This AVP contains an IMSI of the user.

Vendor ID
10415

VSA Type
1

AVP Type
UTF8STRING

AVP Flag
M

3GPP-IMSI-MCC-MNC

This AVP contains MCC and MNC extracted from the user's IMSI (first 5 or 6 digits, as applicable from the presented IMSI).

Vendor ID
10415

VSA Type
8

AVP Type
UTF8STRING

AVP Flag
M

3GPP-MS-TimeZone

This AVP contains the Mobile Station Time Zone.

Vendor ID
10415

VSA Type
23

AVP Type
OCTETSTRING

AVP Flag
M

3GPP-NSAPI

This AVP contains a particular PDP context for the associated PDN and MSISDN/IMSI from creation to deletion.

Vendor ID
10415

VSA Type
10

AVP Type
UTF8STRING

AVP Flag
M

3GPP-PDP-Type

This AVP contains type of the PDP context.

Vendor ID
10415

VSA Type
3

AVP Type
ENUM

Supported enumerated value(s):

0 IPv4

1 PPP

2 IPv6

3 IPv4v6

AVP Flag
M

3GPP-Quota-Consumption-Time

This AVP contains the idle traffic threshold time, in seconds.

Vendor ID
10415

VSA Type
881

AVP Type
UINT32

AVP Flag
M

3GPP-Quota-Holding-Time

This AVP contains the quota holding time, in seconds. The client starts the quota holding timer when quota consumption ceases. This is always when traffic ceases, i.e. the timer is re-started at the end of each packet. The Credit Control Client deems a quota to have expired when no traffic associated with the quota is observed for the value indicated by this AVP.

Vendor ID
10415

VSA Type
871

AVP Type
UINT32

AVP Flag
M

3GPP-RAT-Type

This AVP indicates which Radio Access Technology (RAT) is currently serving the UE.

Vendor ID
10415

VSA Type
21

AVP Type
OCTETSTRING

AVP Flag
M

3GPP-RAT-Type-Enum

This AVP contains type of Radio Access Technology (RAT).

Vendor ID
10415

VSA Type
21

AVP Type
ENUM

Supported enumerated value(s):

1 UTRAN

2 GERAN

3 WLAN

4 GAN

5 HSPA

6 EUTRAN

102 3GPP2_eHRPD

AVP Flag
M

3GPP-Reporting-Reason

This AVP contains the reason for usage reporting for one or more types of quota for a particular category.

Vendor ID
10415

VSA Type
872

AVP Type
ENUM

Supported enumerated value(s):

0 THRESHOLD

1 QHT

2 FINAL

3 QUOTA_EXHAUSTED

4 VALIDITY_TIME

5 OTHER_QUOTA_TYPE

6 RATING_CONDITION_CHANGE

7 FORCED_REAUTHORIZATION

AVP Flag
M

3GPP-SGSN-Address

This AVP contains the address of the SGSN used by the GTP control plane for the handling of control messages. It may be used to identify the PLMN to which the user is attached.

Vendor ID
10415

VSA Type
6

AVP Type
OCTETSTRING

AVP Flag
M

3GPP-SGSN-IPv6-Address

This AVP contains the IPv6 address of the SGSN used by the GTP control plane for the handling of control messages. It may be used to identify the PLMN to which the user is attached.

Vendor ID
10415

VSA Type
15

AVP Type
OCTETSTRING

AVP Flag
M

3GPP-SGSN-MCC-MNC

This AVP contains the MCC-MNC of the network the SGSN belongs to.

Vendor ID
10415

VSA Type
18

AVP Type
UTF8STRING

AVP Flag
M

3GPP-Selection-Mode

This AVP contains the selection mode for this PDP context received in the Create PDP Context Request Message.

Vendor ID
10415

VSA Type
12

AVP Type
UTF8STRING

AVP Flag
M

3GPP-Session-Stop-Indicator

This AVP indicates to the AAA server that the last PDP context of a session is released and that the PDP session has been terminated.

Vendor ID

10415

VSA Type
11

AVP Type
OCTETSTRING

AVP Flag
M

3GPP-Time-Quota-Threshold

This AVP contains the time quota threshold value, in seconds.

Vendor ID
10415

VSA Type
868

AVP Type
UINT32

AVP Flag
M

3GPP-Trigger-Type

This AVP contains information about type of trigger, for example, CHANGE_IN_SGSN_IP_ADDRESS, CHANGE_IN_QOS, etc. for activation of the associated action.

Vendor ID
10415

VSA Type
870

AVP Type
ENUM

Supported enumerated value(s):

1 CHANGE_IN_SGSN_IP_ADDRESS

2 CHANGEINQOS_ANY

3 CHANGEINLOCATION_ANY

4 CHANGEINRAT

10 CHANGEINQOS_TRAFFIC_CLASS

11 CHANGEINQOS_RELIABILITY_CLASS

12 CHANGEINQOS_DELAY_CLASS

13 CHANGEINQOS_PEAK_THROUGHPUT

14 CHANGEINQOS_PRECEDENCE_CLASS

15 CHANGEINQOS_MEAN_THROUGHPUT

16 CHANGEINQOS_MAXIMUM_BIT_RATE_FOR_UPLINK

17 CHANGEINQOS_MAXIMUM_BIT_RATE_FOR_DOWNLINK

18 CHANGEINQOS_RESIDUAL_BER

19 CHANGEINQOS_SDU_ERROR_RATIO

20 CHANGEINQOS_TRANSFER_DELAY

21 CHANGEINQOS_TRAFFIC_HANDLING_PRIORITY

22 CHANGEINQOS_GUARANTEED_BIT_RATE_FOR_UPLINK

23 CHANGEINQOS_GUARANTEED_BIT_RATE_FOR_DOWNLINK

30 CHANGEINLOCATION_MCC

31 CHANGEINLOCATION_MNC

32 CHANGEINLOCATION_RAC

33 CHANGEINLOCATION_LAC

34 CHANGEINLOCATION_CellId

61 CHANGE_IN_SERVING_NODE

AVP Flag
M

3GPP-Unit-Quota-Threshold

This AVP contains the unit quota threshold value, in service specific units.

Vendor ID
10415

VSA Type
1226

AVP Type
UINT32

AVP Flag
M

3GPP-User-Data

This AVP contains the user data required to give service to a user.

Vendor ID
10415

VSA Type
606

AVP Type
OCTETSTRING

AVP Flag
M

3GPP-User-Location-Info

This AVP contains information about the user's current geographical location.

Vendor ID
10415

VSA Type
22

AVP Type
UTF8STRING

AVP Flag
M

3GPP-Volume-Quota-Threshold

This AVP contains the volume quota threshold value, in octets.

Vendor ID
10415

VSA Type
869

AVP Type
UINT32

AVP Flag
M

3GPP-WLAN-APN-Id

This AVP contains the W-APN for which the user will have services available.

Vendor ID
10415

VSA Type
11003

AVP Type
OCTETSTRING

AVP Flag
M

3GPP2-Allowed-Persistent-TFTS

Maximum allowed persistent TFTs.

Vendor ID
5535

VSA Type

6083

AVP Type
UINT32

AVP Flag
M

3GPP2-BSID

This AVP indicates the BSID of where the UE is currently located (for example, Cell-Id, SID, NID).

Vendor ID
5535

VSA Type
9010

AVP Type
OCTETSTRING

AVP Flag
M

3GPP2-Correlation-Id

This AVP contains correlation ID in 3GPP2 networks.

Vendor ID
5535

VSA Type
6071

AVP Type
OCTETSTRING

AVP Flag
M

3GPP2-Information

3GPP2-Information

Vendor ID
5535

VSA Type
6077

AVP Type
GROUPED

Supported group value(s):

[SUBSCRIBER_PRIORITY]

[AUTH_PROFILE_ID_FORWARD]

[AUTH_PROFILE_ID_REVERSE]

[AUTH_PROFILE_ID_BI_DIRECTION]

AVP Flag
M

3GPP2-Inter-User-Priority

3GPP2-Inter-User-Priority

Vendor ID
5535

VSA Type
139

AVP Type
UINT32

AVP Flag
M

3GPP2-MEID

This AVP contains the International Mobile Equipment Identity.

Vendor ID
10415

VSA Type
1471

AVP Type
OCTETSTRING

AVP Flag
M

3GPP2-Max-Auth-Aggr-BW-BET

This AVP contains the maximum allowed bandwidth for best effort link.

Vendor ID
5535

VSA Type
130

AVP Type
UINT32

AVP Flag
M

3GPP2-Max-Inst-Per-Service-Option

This AVP indicates the maximum service option instances.

Vendor ID
5535

VSA Type
6082

AVP Type
UINT32

AVP Flag
M

3GPP2-Max-Per-Flow-Priority-User

This AVP contains the per flow priority for the user.

Vendor ID
5535

VSA Type
6088

AVP Type
UINT32

AVP Flag
M

3GPP2-Max-Svc-Inst-Link-Flow-Total

This AVP contains the maximum allowed link flows per service instance.

Vendor ID
5535

VSA Type
6084

AVP Type
UINT32

AVP Flag
M

3GPP2-RAT-Type

3GPP2-RAT-Type

Vendor ID
5535

VSA Type

1001

AVP Type
ENUM

Supported enumerated value(s):

0 3G1X

1 HRPD

2 WLAN

AVP Flag
M

3GPP2-RP-Session-ID

3GPP2-RP-Session-ID

Vendor ID
5535

VSA Type
6074

AVP Type
OCTETSTRING

AVP Flag
M

3GPP2-Service-Option

3GPP2-Service-Option

Vendor ID
5535

VSA Type
16

AVP Type
UINT32

AVP Flag
M

3GPP2-Service-Option-Profile

3GPP2-Service-Option-Profile

Vendor ID
5535

VSA Type
74

AVP Type
GROUPED

Supported group value(s):

[3GPP2_SERVICE_OPTION]

[3GPP2_MAX_INST_PER_SERVICE_OPTION]

AVP Flag
M

3GPP2-Serving-PCF

3GPP2 Serving PCF Address

Vendor ID
5535

VSA Type
6073

AVP Type
ADDRESS

AVP Flag
M

3GPP2-User-Zone

3GPP2-User-Zone

Vendor ID
5535

VSA Type
6075

AVP Type
OCTETSTRING

AVP Flag
M

AF-Application-Identifier

This AVP contains information that identifies particular service that the Application Function (AF) service session belongs to.

Vendor ID
10415

VSA Type
504

AVP Type
OCTETSTRING

AVP Flag
M

AF-Charging-Identifier

This AVP contains the Application Function (AF) charging identifier that may be used in charging correlation.

Vendor ID
10415

VSA Type
505

AVP Type
OCTETSTRING

AVP Flag
M

AF-Correlation-Information

This grouped AVP contains the AF Charging Identifier (ICID for IMS) and associated flow identifiers generated by the AF and received by GGSN over Rx/Gx.

Vendor ID
10415

VSA Type
1276

AVP Type
GROUPED

Supported group value(s):

[AF_CHARGING_IDENTIFIER]

[FLOWS]

AVP Flag
M

AGW-IP-Address

This AVP contains the IPv4 address of the Access Gateway (AGW) in IPv4 decimal notation format.

Vendor ID
5535

VSA Type
1003

AVP Type
OCTETSTRING

AVP Flag
M

AGW-IPv6-Address

This AVP contains the IPv6 address of the Access Gateway (AGW) in IPv6 colon notation format.

Vendor ID
5535

VSA Type
1004

AVP Type
OCTETSTRING

AVP Flag
M

AGW-MCC-MNC

This AVP contains the Mobile Country Code (MCC) and Mobile Network Code (MNC) of the AGW.

Vendor ID
5535

VSA Type
1002

AVP Type
OCTETSTRING

AVP Flag
M

AMBR

This AVP contains the UE Aggregate Maximum Bit Rate (AMBR) of the user. This will be present only if the non-3GPP access network is trusted.The Rf interface supports AMBR reporting for non-guaranteed bit rate (non-GBR) bearers in the Traffic-Data-Volumes (TDV) Grouped AVP.

Vendor ID
10415

VSA Type
1435

AVP Type
GROUPED

Supported group value(s):

[MAX_REQUESTED_BANDWIDTH_UL]

[MAX_REQUESTED_BANDWIDTH_DL]

AVP Flag
M

AN-GW-Address

This AVP contains address of the Access Network Gateway.

Vendor ID
10415

VSA Type
1050

AVP Type
ADDRESS

AVP Flag
M

AN-Trusted

This AVP contains the 3GPP AAA Server's decision on handling the non-3GPP access network trusted or non-trusted.

Vendor ID
10415

VSA Type
1503

AVP Type
ENUM

Supported enumerated value(s):

0 TRUSTED

1 UNTRUSTED

AVP Flag
M

ANID

This AVP contains the Access Network Identifier (ANID) used for key derivation at the HSS.

Vendor ID
10415

VSA Type
1504

AVP Type
UTF8STRING

AVP Flag
M

APN-Aggregate-Max-Bitrate-DL

This AVP contains the maximum aggregate bit rate in bits per seconds for the downlink direction across all non-GBR bearers related with the same APN.

Vendor ID
10415

VSA Type
1040

AVP Type
UINT32

AVP Flag
M

APN-Aggregate-Max-Bitrate-UL

This AVP contains the maximum aggregate bit rate in bits per seconds for the uplink direction across all non-GBR bearers related with the same APN.

Vendor ID
10415

VSA Type
1041

AVP Type
UINT32

AVP Flag
M

APN-Authorized

APN-Authorized

Vendor ID
10415

VSA Type
6090

AVP Type
GROUPED

Supported group value(s):

[CONTEXT_IDENTIFIER]

[CALLED_STATION_ID]

[APN_BARRING_TYPE]

[FRAMED_IP_ADDRESS]

[FRAMED_IPV6_PREFIX]

[MIP6_AGENT_INFO]

[PDN_GW_ALLOCATION_TYPE]

[VPLMN_DYNAMIC_ADDRESS_ALLOWED]

[EPS_SUBSCRIBED_QOS_PROFILE]

AVP Flag
M

APN-Barring-Type

Allows operator to disable all APNs for a subscriber at one time.

Vendor ID
10415

VSA Type
6091

AVP Type
ENUM

Supported enumerated value(s):

0 NON_3GPP_APNS_ENABLE

1 NON_3GPP_APNS_DISABLE

AVP Flag
M

APN-Configuration

This AVP contains information related to the user's subscribed APN configurations.

Vendor ID
10415

VSA Type
1430

AVP Type
GROUPED

Supported group value(s):

[CONTEXT_IDENTIFIER]

[PDN_TYPE]

[SERVICE_SELECTION]

[EPS_SUBSCRIBED_QOS_PROFILE]

[VPLMN_DYNAMIC_ADDRESS_ALLOWED]

[MIP6_AGENT_INFO]

[VISITED_NETWORK_IDENTIFIER]

[PDN_GW_ALLOCATION_TYPE]

[3GPP_CHARGING_CHARACTERISTICS]

[AMBR]

[SERVED_PARTY_IP_ADDRESS]

[SPECIFIC_APN_INFO]

[APN_OI_REPLACEMENT]

AVP Flag
M

APN-Configuration-Profile

This AVP contains information related to the user's subscribed APN configurations for EPS.

Vendor ID
10415

VSA Type
1429

AVP Type
GROUPED

Supported group value(s):

[CONTEXT_IDENTIFIER]

[ALL_APN_CONFIGURATIONS_INCLUDED_INDICATOR]

[APN_CONFIGURATION]

AVP Flag
M

APN-OI-Replacement

This AVP contains the domain name to replace the APN OI when constructing the PDN GW FQDN upon which to perform a DNS resolution.

Vendor ID
10415

VSA Type
1427

AVP Type
UTF8STRING

AVP Flag
M

ARP

This AVP contains Allocation and Retention Priority (ARP) for the corresponding APN configuration.

Vendor ID
10415

VSA Type
6039

AVP Type
UINT32

AVP Flag
M

AUTN

This AVP contains the Authentication Token AUTN (EAP Authentication Vector).

Vendor ID
10415

VSA Type
1449

AVP Type
OCTETSTRING

AVP Flag
M

Abort-Cause

This AVP contains the cause of a session abort request, or of an RAR indicating a PDP context release.

Vendor ID
10415

VSA Type
500

AVP Type
ENUM

Supported enumerated value(s):

0 BEARER_RELEASED

1 INSUFFICIENT_SERVER_RESOURCES

2 INSUFFICIENT_BEARER_RESOURCES

AVP Flag
M

Acceptable-Service-Info

This AVP contains the maximum bandwidth for an AF session and/or for specific media components that will be authorized by the PCRF.

Vendor ID
10415

VSA Type

526

AVP Type
GROUPED

Supported group value(s):

[MEDIA_COMPONENT_DESCRIPTION]

[MAX_REQUESTED_BANDWIDTH_DL]

[MAX_REQUESTED_BANDWIDTH_UL]

AVP Flag
M

Access-Network-Charging-Address

This AVP contains the IP address of the network entity within the access network performing charging (for example, the GGSN IP address).

Vendor ID
10415

VSA Type
501

AVP Type
ADDRESS

AVP Flag
M

Access-Network-Charging-Identifier

This AVP contains a charging identifier (for example, GCID) within the "Access-Network-Charging-Identifier-Value" AVP along with information about the flows transported within the corresponding bearer within the Flows AVP.

Vendor ID
10415

VSA Type
502

AVP Type
GROUPED

Supported group value(s):

[ACCESS_NETWORK_CHARGING_IDENTIFIER_VALUE]

[FLOWS]

AVP Flag
M

Access-Network-Charging-Identifier-Gx

The PCRF may use this information for charging correlation towards the AF.

Vendor ID
10415

VSA Type
1022

AVP Type
GROUPED

Supported group value(s):

[ACCESS_NETWORK_CHARGING_IDENTIFIER_VALUE]

[CHARGING_RULE_BASE_NAME]

[CHARGING_RULE_NAME]

AVP Flag
M

Access-Network-Charging-Identifier-Ty

This AVP contains a charging identifier generated by the AGW within the "Access-Network-Charging-Identifier-Value" AVP and the related PCC rule name(s) within the "Charging-Rule-Name" AVP(s). The PCRF may use this information for charging correlation towards the AF.

Vendor ID
10415

VSA Type
1022

AVP Type
GROUPED

Supported group value(s):

[ACCESS_NETWORK_CHARGING_IDENTIFIER_VALUE]

[CHARGING_RULE_BASE_NAME]

[CHARGING_RULE_NAME]

AVP Flag
M

Access-Network-Charging-Identifier-Value

This AVP contains a charging identifier. For example, GCID.

Vendor ID
10415

VSA Type
503

AVP Type
OCTETSTRING

AVP Flag
M

Access-Network-Charging-Physical-Access-Id

This AVP contains the identifier for the physical device the user is connected for charging.

Vendor ID
10415

VSA Type
1472

AVP Type
GROUPED

Supported group value(s):

[ACCESS_NETWORK_CHARGING_PHYSICAL_ACCESS_ID_VALUE]

[ACCESS_NETWORK_CHARGING_PHYSICAL_ACCESS_ID_REALM]

AVP Flag
M

Access-Network-Charging-Physical-Access-Id-Realm

This AVP contains the domain of the physical device the user is connected for charging.

Vendor ID
10415

VSA Type
1474

AVP Type
OCTETSTRING

AVP Flag
M

Access-Network-Charging-Physical-Access-Id-Value

This AVP contains the identifier of the physical device the user is connected for charging.

Vendor ID
10415

VSA Type
1473

AVP Type
OCTETSTRING

AVP Flag

M

Access-Network-Information

This AVP contains access network information, such as the information included in the SIP "P-header P-Access-Network-Information".

Vendor ID
0

VSA Type
1263

AVP Type
OCTETSTRING

AVP Flag
M

Access-Network-Physical-Access-Id

This AVP contains an identifier that represents the topological segment hosting the AT within the serving IP-CAN.

Vendor ID
5535

VSA Type
1472

AVP Type
GROUPED

Supported group value(s):

[ACCESS_NETWORK_PHYSICAL_ACCESS_ID_VALUE]

[ACCESS_NETWORK_PHYSICAL_ACCESS_ID_REALM]

AVP Flag
M

Access-Network-Physical-Access-Id-Realm

Access-Network-Physical-Access-Id-Realm

Vendor ID
5535

VSA Type
1474

AVP Type
OCTETSTRING

AVP Flag
M

Access-Network-Physical-Access-Id-Value

Access-Network-Physical-Access-Id-Value

Vendor ID
5535

VSA Type
1473

AVP Type
OCTETSTRING

AVP Flag
M

Access-Network-Type

This AVP contains the type of access network over which IP connectivity is provided to the user equipment.

Vendor ID
0

VSA Type
306

AVP Type
GROUPED

Supported group value(s): none

AVP Flag
M

Access-Restriction-Data

This AVP contains a bit mask indicating the services of a subscriber, that are barred by the operator.

Vendor ID
10415

VSA Type
1426

AVP Type
UINT32

AVP Flag
M

Accounting-EAP-Auth-Method

This AVP indicates the EAP method(s) used to authenticate the user.

Vendor ID
0

VSA Type
465

AVP Type
UINT64

AVP Flag
N/A

Accounting-Input-Octets

This AVP contains the number of octets in IP packets received from the user.

Vendor ID
0

VSA Type
363

AVP Type
UINT64

AVP Flag
M

Accounting-Input-Packets

This AVP contains the number of IP packets received from the user.

Vendor ID
0

VSA Type
365

AVP Type
UINT64

AVP Flag
M

Accounting-Output-Octets

This AVP contains the number of octets in IP packets sent to the user.

Vendor ID
0

VSA Type
364

AVP Type
UINT64

AVP Flag
M

Accounting-Output-Packets

This AVP contains the number of IP packets sent to the user.

Vendor ID
0

VSA Type
366

AVP Type
UINT64

AVP Flag
M

Accounting-PCC-R3-P-Capability

This AVP indicates the accounting capabilities in a CCR that are supported by the sender. CCA will not include this AVP.

Vendor ID
24757

VSA Type
403

AVP Type
ENUM

Supported enumerated value(s):

0 Online

1 Offline

2 Online_and_Offline

AVP Flag
M

Accounting-Record-Number

This AVP contains this record within one session.

Vendor ID
0

VSA Type
485

AVP Type
UINT32

AVP Flag
M

Accounting-Record-Type

This AVP contains the type of accounting record being sent.

Vendor ID
0

VSA Type
480

AVP Type
ENUM

Supported enumerated value(s):

1 EVENT_RECORD

2 START_RECORD

3 INTERIM_RECORD

4 STOP_RECORD

AVP Flag
M

Accounting-Sub-Session-Id

This AVP contains the accounting sub-session identifier.

Vendor ID
0

VSA Type
287

AVP Type
UINT64

AVP Flag
M

Acct-Application-Id

Advertise support of the Accounting portion of an application.

Vendor ID
0

VSA Type
259

AVP Type
UINT32

AVP Flag
M

Acct-Interim-Interval

This AVP is sent from the Diameter Home Authorization Server to the Diameter client.

Vendor ID
0

VSA Type
85

AVP Type
UINT32

AVP Flag
M

Acct-Multi-Session-Id

Link multiple related accounting sessions.

Vendor ID
0

VSA Type
50

AVP Type
UTF8STRING

AVP Flag
M

Acct-Realtime-Required

This AVP is used to decide the action to be performed when sending of accounting records to the accounting server has been temporarily prevented due to network problem.

Vendor ID
0

VSA Type
483

AVP Type
ENUM

Supported enumerated value(s):

1 DELIVER_AND_GRANT

2 GRANT_AND_STORE

3 GRANT_AND_LOSE

AVP Flag
M

Acct-Session-Id

This AVP is only used when RADIUS/Diameter translation occurs. This AVP contains the contents of the RADIUS "Acct-Session-Id" attribute.

Vendor ID
0

VSA Type
44

AVP Type
OCTETSTRING

AVP Flag
M

Acct-Session-Time

This AVP indicates the length of the current session, in seconds. This AVP MUST be included in all Accounting-Request messages and MAY be present in the corresponding Accounting-Answer messages as well.

Vendor ID
10415

VSA Type
46

AVP Type
UINT32

AVP Flag
M

Additional-MBMS-Trace-Info

This AVP contains additional information such as Trace-Reference, Triggering Events in BMSC, List of Interfaces in BMSC, Trace Activity Control, etc.

Vendor ID
10415

VSA Type
910

AVP Type
OCTETSTRING

AVP Flag
M

Address-Realm

This AVP contains the realm that the user belongs to.

Vendor ID
0

VSA Type
1005

AVP Type
OCTETSTRING

AVP Flag
M

Alert-Reason

This AVP indicates that the mobile subscriber is present or the MS has available memory.

Vendor ID
10415

VSA Type
1434

AVP Type
ENUM

Supported enumerated value(s):

0 UE_PRESENT

1 UE_MEMORY_AVAILABLE

AVP Flag
M

All-APN-Configurations-Included-Indicator

This AVP indicates addition/modification/deletion of APN configuration for MME/SGSN service.

Vendor ID
10415

VSA Type
1428

AVP Type
ENUM

Supported enumerated value(s):

0 ALL_APN_CONFIGURATIONS_INCLUDED

1 MODIFIED_ADDED_APN_CONFIGURATIONS_INCLUDED

AVP Flag
M

Allocation-Retention-Priority

Allocation-Retention-Priority

Vendor ID
10415

VSA Type
1034

AVP Type
GROUPED

Supported group value(s):

[PRIORITY_LEVEL]

[PRE_EMPTION_CAPABILITY]

[PRE_EMPTION_VULNERABILITY]

AVP Flag
M

Alternative-APN

This AVP contains the value of a new APN. BM-SC only includes it if the UE must use a different APN for the MBMS PDP Context from the one used in the Join message.

Vendor ID
10415

VSA Type
905

AVP Type
UTF8STRING

AVP Flag
M

Anchor-Data-Path-Address

This AVP contains the IP address of the serving SFA and is included in the CCR message.

Vendor ID
24757

VSA Type
401

AVP Type
OCTETSTRING

AVP Flag
M

Application-Provided-Called-Party-Address

This AVP holds the called party number (SIP URL, E.164), if it is determined by an application server.

Vendor ID
10415

VSA Type
837

AVP Type
UTF8STRING

AVP Flag
M

Application-Server

This AVP contains the SIP URL(s) of the AS(s) addressed during the session.

Vendor ID
10415

VSA Type
836

AVP Type
UTF8STRING

AVP Flag
M

Application-Server-Information

This AVP contains the list of application servers visited on the ISC interface.

Vendor ID
10415

VSA Type
850

AVP Type
GROUPED

Supported group value(s):

[APPLICATION_SERVER]

[APPLICATION_PROVIDED_CALLED_PARTY_ADDRESS]

AVP Flag
M

Associated-Identities

This AVP contains the private user identities associated to an IMS subscription.

Vendor ID
10415

VSA Type
632

AVP Type
GROUPED

Supported group value(s):

[USER_NAME]

AVP Flag
M

Associated-Registered-Identities

This AVP contains the Private User Identities registered with the Public User Identity received in the request command.

Vendor ID
10415

VSA Type
647

AVP Type
GROUPED

Supported group value(s):

[USER_NAME]

AVP Flag
N/A

Associated-URI

This AVP contains a non-barred public user identity (SIP URI or TEL URI) associated to the the public user identity under registration.

Vendor ID
10415

VSA Type
856

AVP Type
UTF8STRING

AVP Flag
M

Auth-Application-Id

This AVP contains the Diameter supported authorization application ID.

Vendor ID
0

VSA Type
258

AVP Type
UINT32

AVP Flag
M

Auth-Grace-Period

This AVP contains the number of seconds the Diameter server will wait following the expiration of the Authorization-Lifetime AVP before cleaning up resources for the session.

Vendor ID
0

VSA Type
276

AVP Type
UINT32

AVP Flag
M

Auth-Profile-Id-Bi-Direction

3GPP2 Auth-Profile-Id-Bi-Direction

Vendor ID
5535

VSA Type
6081

AVP Type
UINT32

AVP Flag
M

Auth-Profile-Id-Forward

3GPP2 Auth-Profile-Id-Forward

Vendor ID
5535

VSA Type
6079

AVP Type
UINT32

AVP Flag
M

Auth-Profile-Id-Reverse

3GPP2 Auth-Profile-Id-Reverse

Vendor ID
5535

VSA Type
6080

AVP Type
UINT32

AVP Flag
M

Auth-Request-Type

This AVP contains the authorization request type to inform the peers whether a user is to be authenticated only, authorized only, or both.

Vendor ID
0

VSA Type
274

AVP Type
ENUM

Supported enumerated value(s):

1 AUTHENTICATE_ONLY

2 AUTHORIZE_ONLY

3 AUTHORIZE_AUTHENTICATE

AVP Flag
M

Auth-Session-State

This AVP indicates whether state is maintained for a particular session.

Vendor ID
0

VSA Type

277

AVP Type
ENUM

Supported enumerated value(s):

0 STATE_MAINTAINED

1 NO_STATE_MAINTAINED

AVP Flag
M

Authentication-Info

This AVP contains the Authentication Vectors.

Vendor ID
10415

VSA Type
6016

AVP Type
GROUPED

Supported group value(s):

[EPS_VECTOR]

[UMTS_VECTOR]

[GERAN_VECTOR]

AVP Flag
M

Authorised-QoS

This AVP contains the authorized QoS.

Vendor ID
0

VSA Type
849

AVP Type
UTF8STRING

AVP Flag
M

Authorization-Lifetime

This AVP contains the maximum number of seconds of service to be provided to the user before the user is to be re-authenticated and/or re- authorized.

Vendor ID
0

VSA Type
291

AVP Type
UINT32

AVP Flag
M

Authorization-Token

This AVP contains the authorization token defined in RFC 3520.

Vendor ID
10415

VSA Type
506

AVP Type
OCTETSTRING

AVP Flag
M

Authorized-QoS

This AVP carries the authorized QoS from the E-PDF to the IPC/GGSN.

Vendor ID
10415

VSA Type
1016

AVP Type
GROUPED

Supported group value(s):

[QOS_CLASS]

[MAX_REQUESTED_BANDWIDTH_UL]

[MAX_REQUESTED_BANDWIDTH_DL]

AVP Flag
M

BCID

This AVP contains the PacketCable 1.5 Billing Correlation ID as generated for a SIP session. This value is copied from the BCID field in the P-DCS-LAES header.

Vendor ID

4491

VSA Type
200

AVP Type
UTF8STRING

AVP Flag
M

BSID

BSID

Vendor ID
0

VSA Type
10003

AVP Type
OCTETSTRING

AVP Flag
M

Bearer-Control-Mode

This AVP indicates the preferred Bearer Control Mode.

Vendor ID
10415

VSA Type
1023

AVP Type
ENUM

Supported enumerated value(s):

0 UE_ONLY

1 RESERVED

2 UE_NW

AVP Flag
M

Bearer-Identifier

This AVP indicates the bearer to which the information belongs.

Vendor ID
10415

VSA Type
1020

AVP Type
OCTETSTRING

AVP Flag
M

Bearer-Operation

This AVP indicates the bearer event that causes the request for PCC rules.

Vendor ID
10415

VSA Type
1021

AVP Type
ENUM

Supported enumerated value(s):

0 TERMINATION

1 ESTABLISHMENT

2 MODIFICATION

AVP Flag
M

Bearer-Service

This AVP holds the used bearer service for the application, for example, PSTN leg in the case of voice.

Vendor ID
10415

VSA Type
854

AVP Type
OCTETSTRING

AVP Flag
M

Bearer-Usage

This AVP indicates how the bearer is being used, for example, whether it is used as a dedicated IMS signaling context or not.

Vendor ID
10415

VSA Type

1000

AVP Type
ENUM

Supported enumerated value(s):

0 GENERAL

1 IMS_SIGNALLING

2 DEDICATED

AVP Flag
M

Binding-Information

This AVP contains binding information required for NA(P)T, hosted NA(P)T, and NA(P)T-PT control.

Vendor ID
13019

VSA Type
450

AVP Type
GROUPED

Supported group value(s):

[BINDING_INPUT_LIST]

[BINDING_OUTPUT_LIST]

AVP Flag
N/A

Binding-Input-List

This AVP contains a list of transport addresses for which a binding is requested.

Vendor ID
13019

VSA Type
451

AVP Type
GROUPED

Supported group value(s):

[V6_TRANSPORT_ADDRESS]

[V4_TRANSPORT_ADDRESS]

AVP Flag
N/A

Binding-Output-List

This AVP contains a list of transport addresses which is the result of the binding operation performed by the transport plane functions.

Vendor ID
13019

VSA Type
452

AVP Type
GROUPED

Supported group value(s):

[V6_TRANSPORT_ADDRESS]

[V4_TRANSPORT_ADDRESS]

AVP Flag
N/A

CC-Correlation-Id

Correlates credit control requests generated for different components of the service.

Vendor ID
0

VSA Type
411

AVP Type
OCTETSTRING

AVP Flag
M

CC-Input-Octets

This AVP contains the number of requested, granted, or used octets that can be/have been received from the end user.

Vendor ID
0

VSA Type
412

AVP Type
UINT64

AVP Flag
M

CC-Money

This AVP indicates the monetary amount in the given currency.

Vendor ID
0

VSA Type
413

AVP Type
GROUPED

Supported group value(s): none

AVP Flag
M

CC-Output-Octets

This AVP contains the number of requested, granted, or used octets that can be/have been sent to the end user.

Vendor ID
0

VSA Type
414

AVP Type
UINT64

AVP Flag
M

CC-Request-Number

This AVP contains the number of Credit Control request for mapping requests and answers.

Vendor ID
0

VSA Type
415

AVP Type
UINT32

AVP Flag
M

CC-Request-Type

This AVP contains the type of credit-control Request/Answer message.

Vendor ID
0

VSA Type
416

AVP Type
ENUM

Supported enumerated value(s):

1 INITIAL_REQUEST

2 UPDATE_REQUEST

3 TERMINATION_REQUEST

4 EVENT_REQUEST

AVP Flag
M

CC-Service-Specific-Units

This AVP contains the number of service-specific units (for example, number of events, points) given in a selected service.

Vendor ID
0

VSA Type
417

AVP Type
UINT64

AVP Flag
M

CC-Session-Failover

This AVP contains information as to whether moving the credit-control message stream to a backup server during an ongoing credit-control session is supported.

Vendor ID
0

VSA Type
418

AVP Type
ENUM

Supported enumerated value(s):

0 FAILOVER_NOT_SUPPORTED

1 FAILOVER_SUPPORTED

AVP Flag
M

CC-Sub-Session-Id

This AVP contains the credit-control sub-session identifier.

Vendor ID
0

VSA Type
419

AVP Type
UINT64

AVP Flag
M

CC-Time

This AVP contains the length of the requested, granted, or used time, in seconds.

Vendor ID
0

VSA Type
420

AVP Type
UINT32

Supported group value(s):

[UNIT_VALUE]

[CURRENCY_CODE]

AVP Flag
M

CC-Total-Octets

This AVP contains the total number of requested, granted, or used octets regardless of the direction.

Vendor ID
0

VSA Type
421

AVP Type
UINT64

AVP Flag
M

CC-Unit-Type

This AVP contains the type of units.

Vendor ID
0

VSA Type
454

AVP Type
ENUM

Supported enumerated value(s): none

AVP Flag
M

CG-Address

This AVP contains IP address of the Charging Gateway.

Vendor ID
10415

VSA Type
846

AVP Type
ADDRESS

AVP Flag
M

CHAP-Auth

CHAP-Authentication

Vendor ID
10415

VSA Type
402

AVP Type
GROUPED

Supported group value(s):

[CHAP_IDENT]

[CHAP_RESPONSE]

AVP Flag
M

CHAP-Challenge

CHAP-Challenge

Vendor ID
10415

VSA Type
60

AVP Type
OCTETSTRING

AVP Flag
M

CHAP-Ident

CHAP-Identifier

Vendor ID
10415

VSA Type
404

AVP Type
OCTETSTRING

AVP Flag
M

CHAP-Response

CHAP-Response

Vendor ID
10415

VSA Type
405

AVP Type
OCTETSTRING

AVP Flag
M

CSG-Id

This AVP contains Closed Subscriber Group Identity used to identify Closed Subscriber Group within a PLMN.

Vendor ID
10415

VSA Type

1437

AVP Type
UINT32

AVP Flag
M

CSG-Subscription-Data

This AVP contains the CSG-Id and optionally an associated expiration date.

Vendor ID
10415

VSA Type
1436

AVP Type
GROUPED

Supported group value(s):

[CSG_ID]

[EXPIRATION_DATE]

AVP Flag
M

Call-Barring-Info-List

This AVP contains the service codes for the short message related call barring services for a subscriber.

Vendor ID
10415

VSA Type
1488

AVP Type
GROUPED

Supported group value(s):

[SS_CODE]

AVP Flag
M

Call-ID-SIP-Header

This AVP contains the information in the Call-ID header.

Vendor ID
10415

VSA Type

643

AVP Type
OCTETSTRING

AVP Flag
N/A

Callback-Id

This AVP contains the name of a place to be called, to be interpreted by the NAS.

Vendor ID
0

VSA Type
20

AVP Type
UTF8STRING

AVP Flag
M

Callback-Number

This AVP contains a dialing string to be used for callback.

Vendor ID
0

VSA Type
19

AVP Type
UTF8STRING

AVP Flag
M

Called-Asserted-Identity

This AVP contains the address (Public User ID: SIP URI, E.164, etc.) of the finally asserted called party.

Vendor ID
10415

VSA Type
1250

AVP Type
UTF8STRING

AVP Flag
M

Called-Party-Address

This AVP contains the address of the party to whom a session is established.

Vendor ID
0

VSA Type
832

AVP Type
UTF8STRING

AVP Flag
M

Called-Station-Id

This AVP contains the Layer 2 addresses the user contacted in the request.

Vendor ID
0

VSA Type
30

AVP Type
OCTETSTRING

AVP Flag
M

Calling-Party-Address

This AVP contains the address of the party initiating a session.

Vendor ID
10415

VSA Type
831

AVP Type
UTF8STRING

AVP Flag
M

Calling-Station-Id

This AVP enables the NAS to send the ASCII string describing the Layer 2 address from which the user connected in the request.

Vendor ID
0

VSA Type
31

AVP Type
UTF8STRING

AVP Flag
M

Cancellation-Type

This AVP indicates the type of cancellation.

Vendor ID
10415

VSA Type
1420

AVP Type
ENUM

Supported enumerated value(s):

0 MME_UPDATE_PROCEDURE

1 SGSN_UPDATE_PROCEDURE

2 SUBSCRIPTION_WITHDRAWAL

3 UPDATE_PROCEDURE_IWF

AVP Flag
M

Carrier-Select-Routing-Information

This AVP contains information on carrier selection performed by S-CSCF/AS.

Vendor ID
10415

VSA Type
2023

AVP Type
UTF8STRING

AVP Flag
M

Cause-Code

This AVP contains the cause code value from IMS node. It is used in Accounting-Request[stop] and/or Accounting-Request[event] messages.

Vendor ID
0

VSA Type
861

AVP Type
INT32

AVP Flag
M

Change-Condition

This AVP indicates the change in charging condition.

Vendor ID
10415

VSA Type
2037

AVP Type
INT32

Supported enumerated value(s):

0 NORMAL_RELEASE

1 ABNORMAL_RELEASE

2 QOS_CHANGE

3 VOLUME_LIMIT

4 TIME_LIMIT

5 SERVING_NODE_CHANGE

6 SERVING_NODE_PLMN_CHANGE

7 USER_LOCATION_CHANGE

8 RAT_CHANGE

9 UE_TIME_ZONE_CHANGE

10 TARIFF_TIME_CHANGE

11 SERVICE_IDLED_OUT

12 SERVICE_SPECIFIC_UNIT_LIMIT

13 MAX_NUMBER_OF_CHARGING_CONDITIONS

14 MANAGEMENT_INTERVENTION

AVP Flag
M

Change-Time

This AVP contains the time in UTC format when the volume counts associated to the service data container is closed and reported due to Charging condition change.

Vendor ID

10415

VSA Type
2038

AVP Type
TIME

AVP Flag
M

Charging-Characteristics

This AVP contains the charging mode to be applied.

Vendor ID
10415

VSA Type
11006

AVP Type
UINT32

AVP Flag
M

Charging-Data

This AVP contains addresses of the charging functions.

Vendor ID
10415

VSA Type
11005

AVP Type
GROUPED

Supported group value(s):

[CHARGING_CHARACTERISTICS]

AVP Flag
M

Charging-Information

This AVP contains the addresses of the charging functions in the grouped AVPs.

Vendor ID
10415

VSA Type
618

AVP Type

GROUPED

Supported group value(s):

[PRIMARY_EVENT_CHARGING_FUNCTION_NAME]

[SECONDARY_EVENT_CHARGING_FUNCTION_NAME]

[PRIMARY_CHARGING_COLLECTION_FUNCTION_NAME]

[SECONDARY_CHARGING_COLLECTION_FUNCTION_NAME]

AVP Flag
M

Charging-Rule-Base-Name

This AVP indicates the name of a pre-defined group of charging rules residing at the TPF.

Vendor ID
10415

VSA Type
1004

AVP Type
UTF8STRING

AVP Flag
M

Charging-Rule-Definition

This AVP contains the charging rule for a service flow sent by the CRF to the TPF.

Vendor ID
10415

VSA Type
1003

AVP Type
GROUPED

Supported group value(s):

[CHARGING_RULE_NAME]

[SERVICE_IDENTIFIER]

[RATING_GROUP]

[FLOW_DESCRIPTION]

[REPORTING_LEVEL]

[ONLINE]

[OFFLINE]

[FLOW_STATUS]

[QOS_INFORMATION]

[METERING_METHOD]

[PRECEDENCE]

[AF_CHARGING_IDENTIFIER]

[FLOWS]

AVP Flag
M

Charging-Rule-Install

Used to activate, install, or modify Charging/Firewall rules from the Policy server. Charging/Firewall ruledefs for a subscriber can be dynamically activated from gx server. If the incoming rule fails to match in the charging ruledefs of a rulebase, then there will be a lookup with the Firewall ruledefs of the rulebase.

Vendor ID
10415

VSA Type
1001

AVP Type
GROUPED

Supported group value(s):

[CHARGING_RULE_DEFINITION]

[CHARGING_RULE_NAME]

[CHARGING_RULE_BASE_NAME]

[BEARER_IDENTIFIER]

[RULE_ACTIVATION_TIME]

[RULE_DEACTIVATION_TIME]

[RESOURCE_ALLOCATION_NOTIFICATION]

AVP Flag
M

Charging-Rule-Name

This AVP contains the charging rule name provided by the CRF. It uniquely identifies a charging rule for a bearer.

Vendor ID
10415

VSA Type
1005

AVP Type
OCTETSTRING

AVP Flag
M

Charging-Rule-Name-LI

Charging rule name for LI-Indicator-Gx.

Vendor ID
10415

VSA Type
1005

AVP Type
OCTETSTRING

AVP Flag
M

Charging-Rule-Remove

This AVP contains the deactivated or removed Charging/Firewall rules from the Policy server. Charging/Firewall ruledefs for a subscriber can be dynamically deactivated from gx server. If the incoming rule fails to match in the charging ruledefs of a rulebase, then there will be a lookup with the Firewall ruledefs of the rulebase.

Vendor ID
10415

VSA Type
1002

AVP Type
GROUPED

Supported group value(s):

[CHARGING_RULE_NAME]

[CHARGING_RULE_BASE_NAME]

AVP Flag
M

Charging-Rule-Report

This AVP is used to report the status of a Policy and Charging Control (PCC) rule for installation successful/removal. It is a reference for a specific PCC rule at the AGW that has been successfully installed, modified or removed because of trigger from the MS. The PCC-Rule-Status AVP indicates the action being performed on the PCC rule. Multiple instances of Charging-Rule-Report AVPs shall be used in the case it is required to report different PCCRule-Status values for different groups of rules within the same Diameter command.

Vendor ID
10415

VSA Type
1018

AVP Type
GROUPED

Supported group value(s):

[CHARGING_RULE_NAME]

[CHARGING_RULE_BASE_NAME]

[PCC_RULE_STATUS]

[RULE_FAILURE_CODE]

[FINAL_UNIT_INDICATION]

AVP Flag
M

Check-Balance-Result

This AVP contains the result of the balance check. Applicable only when requested-Action AVP indicates CHECK_BALANCE.

Vendor ID
0

VSA Type
422

AVP Type
ENUM

Supported enumerated value(s):

0 ENOUGH_CREDIT

1 NO_CREDIT

AVP Flag
M

Civic-Location

This AVP contains location information.

Vendor ID
13019

VSA Type
355

AVP Type
OCTETSTRING

AVP Flag
M

Class

This AVP is used by Diameter servers to return state information to the access device.

Vendor ID
0

VSA Type
25

AVP Type
OCTETSTRING

AVP Flag
M

Client-Identity

This AVP contains the ISDN number of the external client.

Vendor ID
10415

VSA Type
1480

AVP Type
OCTETSTRING

AVP Flag
M

CoA-IP-Address

This AVP contains care-of-address for DSMIP6 access.

Vendor ID
10415

VSA Type
1035

AVP Type
ADDRESS

AVP Flag
M

CoA-Information

This AVP contains care-of-address and the tunnel information related to the care of address.

Vendor ID
10415

VSA Type
1039

AVP Type
GROUPED

Supported group value(s):

[TUNNEL_INFORMATION]

[COA_IP_ADDRESS]

AVP Flag
M

Codec-Data

This AVP contains CODEC-related information known at the AF.

Vendor ID
10415

VSA Type
524

AVP Type
OCTETSTRING

AVP Flag
M

Complete-Data-List-Included-Indicator

This AVP indicates addition/modification/deletion of PDP-Contexts at MME/SGSN.

Vendor ID
10415

VSA Type
1468

AVP Type
ENUM

Supported enumerated value(s):

0 ALL_PDP_CONTEXTS_INCLUDED

1 MODIFIED_ADDED_PDP_CONTEXTS_INCLUDED

AVP Flag
M

Confidentiality-Key

This AVP contains the Confidentiality Key (CK).

Vendor ID
10415

VSA Type
625

AVP Type
OCTETSTRING

AVP Flag
M

Configuration-Token

This AVP is sent by a Diameter Server to a Diameter Proxy Agent or Translation Agent in an AA-Answer command to indicate a type of user profile to be used.

Vendor ID
0

VSA Type
78

AVP Type
OCTETSTRING

AVP Flag
N/A

Connect-Info

This AVP is sent in the AA-Request message or ACR STOP message.

Vendor ID
0

VSA Type
77

AVP Type
UTF8STRING

AVP Flag
M

Contact

This AVP contains the contact addresses and parameters in the Contact header.

Vendor ID
10415

VSA Type
641

AVP Type
OCTETSTRING

AVP Flag
N/A

Content-Disposition

This AVP indicates how the message body or a message body part is to be interpreted (for example, session, render).

Vendor ID
10415

VSA Type
828

AVP Type
UTF8STRING

AVP Flag
M

Content-Length

This AVP contains the size of the message body.

Vendor ID
10415

VSA Type
827

AVP Type
UINT32

AVP Flag
M

Content-Type

This AVP contains the media type (for example, application/sdp, text/html) of the message-body.

Vendor ID
10415

VSA Type
826

AVP Type
UTF8STRING

AVP Flag
M

Context-Identifier

Context-Identifier

Vendor ID
10415

VSA Type
1423

AVP Type
UINT32

AVP Flag
M

Correlate-Reason

This AVP contains the reason the Correlate message was sent.

Vendor ID
4491

VSA Type
202

AVP Type
ENUM

Supported enumerated value(s):

0 UNKNOWN

1 B2BUA

2 INITIAL_SIP_MESSAGE

3 ADDITIONAL_TARGET_ENCOUNTERED

4 HAND_OFF_OCCURED

5 ORIGINATION_FROM_APP_SERVER

6 BCID

AVP Flag
M

Cost-Information

This AVP contains cost information of service transferred by the credit-control client to the end user.

Vendor ID
0

VSA Type
423

AVP Type
GROUPED

Supported group value(s):

[UNIT_VALUE]

[CURRENCY_CODE]

[COST_UNIT]

AVP Flag
M

Cost-Unit

This AVP contains the applicable unit to the Cost-Information when the service cost is a cost per unit, can be minutes, hours, days and kilobytes.

Vendor ID
0

VSA Type
424

AVP Type
UTF8STRING

AVP Flag
M

Credit-Control

This AVP is included in AA requests when the service element has credit-control application.

Vendor ID
0

VSA Type
426

AVP Type
ENUM

Supported enumerated value(s):

0 CREDIT_AUTHORIZATION

1 RE_AUTHORIZATION

AVP Flag
M

Credit-Control-Failure-Handling

The credit-control client uses this information to handle the credit control server failure.

Vendor ID
0

VSA Type
427

AVP Type
ENUM

Supported enumerated value(s):

0 TERMINATE

1 CONTINUE

2 RETRY_AND_TERMINATE

AVP Flag
M

Currency-Code

This AVP contains currency in which the values of AVPs containing monetary units were given.

Vendor ID
0

VSA Type
425

AVP Type
UINT32

AVP Flag
M

Current-Location

This AVP indicates whether an active location retrieval has to be initiated or not.

Vendor ID
0

VSA Type
707

AVP Type
ENUM

Supported enumerated value(s): none

AVP Flag
M

Customer-Id

This AVP contains customer identifier; used in header enrichment scenarios.

Vendor ID
8164

VSA Type
1146

AVP Type
UTF8STRING

AVP Flag
M

DIR

DIR

Vendor ID
0

VSA Type
11000

AVP Type
OCTETSTRING

AVP Flag
M

DSA-Flags

This AVP contains a bit mask.

Vendor ID
10415

VSA Type
1422

AVP Type
UINT32

AVP Flag
M

DSR-Flags

This AVP contains a bit mask.

Vendor ID
10415

VSA Type
1421

AVP Type
UINT32

AVP Flag
M

Data-Reference

This AVP contains the type of the requested used data in the operation UDR and SNR.

Vendor ID
0

VSA Type
703

AVP Type
ENUM

Supported enumerated value(s): none

AVP Flag

M

Default-EPS-Bearer-QoS

This AVP contains the QoS information for the EPS default bearer.

Vendor ID
10415

VSA Type
1049

AVP Type
GROUPED

Supported group value(s):

[QOS_CLASS_IDENTIFIER]

[ALLOCATION_RETENTION_PRIORITY]

AVP Flag
M

Deregistration-Reason

This AVP contains the reason for a de-registration operation.

Vendor ID
10415

VSA Type
615

AVP Type
GROUPED

Supported group value(s):

[REASON_CODE]

[REASON_INFO]

AVP Flag
M

Destination-Host

This AVP contains the destination endpoint of the message. This AVP is present in all request messages.

Vendor ID
0

VSA Type
293

AVP Type
DIAMIDENT

AVP Flag
M

Destination-Realm

This AVP contains the realm the message is to be routed to. It is present in all request messages sent from DCCA.

Vendor ID
0

VSA Type
283

AVP Type
DIAMIDENT

AVP Flag
M

Diagnostics

This AVP contains a more detailed cause value for sending Accounting-Request from PCN node.

Vendor ID
10415

VSA Type
2039

AVP Type
INT32

Supported enumerated value(s):

0 UNSPECIFIED

1 SESSION_TIMEOUT

2 RESOURCE_LIMITATION

3 ADMIN_DISCONNECT

4 IDLE_TIMEOUT

5 PCRF_UNREACHABLE

6 AAA_UNREACHABLE

7 AAA_INITIATED_SESSION_TERMINATION

8 REAUTHENTICATION_FAILED

9 PCRF_INITIATED_SESSION_TERMINATION

10 PCRF_INITIATED_FLOW_TERMINATION

11 PCRF_ACCOUNTING_PARAMETERS_CHANGED

12 PMIP_INITIATED_SESSION_TERMINATION

13 PPP_INITIATED_SESSION_TERMINATION

14 GTP_INITIATED_SESSION_TERMINATION

15 PMIP_REVOCATION

16 HANDOVER_ERROR

17 PMIP_LIFETIME_EXPIRED

AVP Flag
M

Dialog-Id

This AVP contains the SIP dialog identifier in the form: Call-ID=x;FTag=y;TTag=z, where x is the value of the SIP Call-ID header, y is the contents of the From header tag, and z is the contents of the To header tag. If the To header tag value is not present in the SIP message then TTag field MUST not be present in the AVP.

Vendor ID
4491

VSA Type
203

AVP Type
UTF8STRING

AVP Flag
M

Digest-Algorithm

This AVP contains the algorithm parameter that influences the HTTP Digest calculation.

Vendor ID
0

VSA Type
111

AVP Type
OCTETSTRING

AVP Flag
M

Digest-Auth-Param

This AVP is a placeholder for future extensions and corresponds to the "auth-param" parameter defined in section 3.2.1 of [RFC2617].

Vendor ID
0

VSA Type
117

AVP Type
OCTETSTRING

AVP Flag
M

Digest-Domain

This AVP contains a single URI that defines a protection space component.

Vendor ID
0

VSA Type
119

AVP Type
OCTETSTRING

AVP Flag
M

Digest-HA1

This AVP contains the hexadecimal representation of H(A1) as described in RFC2617.

Vendor ID
0

VSA Type
121

AVP Type
OCTETSTRING

AVP Flag
M

Digest-QoP

This AVP contains the Quality of Protection (QoP) parameter that influences the HTTP Digest calculation.

Vendor ID
0

VSA Type
110

AVP Type
OCTETSTRING

AVP Flag
M

Digest-Realm

This AVP describes a protection space component of the RADIUS server.

Vendor ID
0

VSA Type
104

AVP Type
OCTETSTRING

AVP Flag
M

Direct-Debiting-Failure-Handling

This AVP contains the action to handle the failure of request message to the credit control server with DIRECT_DEBITING attribute.

Vendor ID
0

VSA Type
428

AVP Type
ENUM

Supported enumerated value(s):

0 TERMINATE_OR_BUFFER

1 CONTINUE

AVP Flag
M

Direct-Message

This AVP indicates if the reported message is exchanged directly between the IAP and the intercept target.

Vendor ID
4491

VSA Type
211

AVP Type
ENUM

Supported enumerated value(s):

0 FALSE

1 TRUE

AVP Flag
M

Direction

This AVP indicates whether the reported message was sent "to" or "from" the intercept target.

Vendor ID
4491

VSA Type
210

AVP Type
ENUM

Supported enumerated value(s):

0 UNDEFINED

1 TO_TARGET

2 FROM_TARGET

AVP Flag
M

Disconnect-Cause

This AVP contains the cause of disconnection with peer.

Vendor ID
0

VSA Type
273

AVP Type
ENUM

Supported enumerated value(s):

0 REBOOTING

1 BUSY

2 DO_NOT_WANT_TO_TALK_TO_YOU

AVP Flag
M

Dynamic-Address-Flag

This AVP indicates whether the PDP context/PDN address is statically or dynamically allocated. If not present, then it is statically allocated.

Vendor ID
10415

VSA Type
2051

AVP Type

ENUM

Supported enumerated value(s):

0 STATIC

1 DYNAMIC

AVP Flag
M

EAP-Key-Name

This AVP contains an opaque key identifier (name) generated by the EAP method.

Vendor ID
0

VSA Type
102

AVP Type
OCTETSTRING

AVP Flag
M

EAP-Master-Session-Key

This AVP contains keying material for protecting the communications between the user and the NAS.

Vendor ID
0

VSA Type
464

AVP Type
OCTETSTRING

AVP Flag
N/A

EAP-Payload

This AVP is used to encapsulate the actual EAP packet that is being exchanged between the EAP client and the home Diameter server.

Vendor ID
0

VSA Type
462

AVP Type
OCTETSTRING

AVP Flag

M

EAP-Reissued-Payload

Sent in DEA for a non-fatal error, and encapsulates the previous EAP Request sent by the server.

Vendor ID
0

VSA Type
463

AVP Type
OCTETSTRING

AVP Flag
M

EPS-Subscribed-QoS-Profile

This AVP contains the bearer-level QoS parameters associated to the default bearer for an APN.

Vendor ID
10415

VSA Type
1431

AVP Type
GROUPED

Supported group value(s):

[QOS_CLASS_IDENTIFIER]

[ALLOCATION_RETENTION_PRIORITY]

AVP Flag
M

EPS-Vector

This AVP contains Authentication Information for EPS.

Vendor ID
10415

VSA Type
6017

AVP Type
GROUPED

Supported group value(s):

[ITEM_NUMBER]

[RAND]

[XRES]

[AUTN]

[KASME]

AVP Flag
M

ESN

ESN

Vendor ID
10415

VSA Type
6109

AVP Type
OCTETSTRING

AVP Flag
M

EUTRAN-Vector

EUTRAN-Vector

Vendor ID
10415

VSA Type
1414

AVP Type
GROUPED

Supported group value(s):

[ITEM_NUMBER]

[RAND]

[XRES]

[AUTN]

[KASME]

AVP Flag
M

Early-Media-Description

This AVP contains the SDP session, media parameters, and timestamps related to media components set to active according to SDP signalling exchanged during a SIP session establishment before the final successful or unsuccessful SIP answer to the initial SIP INVITE message is received.

Vendor ID
10415

VSA Type
1272

AVP Type
GROUPED

Supported group value(s):

[SDP_TIMESTAMPS]

[SDP_MEDIA_COMPONENT]

[SDP_SESSION_DESCRIPTION]

AVP Flag
M

Element-ID

This AVP contains the PacketCable IAP sending an intercept message to the DF.

Vendor ID
4491

VSA Type
212

AVP Type
UTF8STRING

AVP Flag
M

Element-Type

This AVP contains the type of node where the intercept message was generated.

Vendor ID
4491

VSA Type
213

AVP Type
ENUM

Supported enumerated value(s):

0 S_CSCF

1 P_CSCF

2 I_CSCF

3 MRFC

4 MGCF

5 BGCF

6 AS

7 UE

AVP Flag
M

Equipment-Status

This AVP contains the status of the mobile equipment.

Vendor ID
10415

VSA Type
1445

AVP Type
ENUM

Supported enumerated value(s):

0 WHITELISTED

1 BLACKLISTED

2 GREYLISTED

AVP Flag
M

Error-Message

Human Readable Error Message.

Vendor ID
0

VSA Type
281

AVP Type
UTF8STRING

AVP Flag
N/A

Error-Reporting-Host

This AVP contains the identity of the Diameter host that sent the Result Code AVP to a value other than 2001.

Vendor ID
0

VSA Type
294

AVP Type

DIAMIDENT

AVP Flag
M

Event

This AVP contains the content of the "Event" header used in SUBSCRIBE and NOTIFY messages.

Vendor ID
10415

VSA Type
825

AVP Type
UTF8STRING

AVP Flag
M

Event-Message-Type

This AVP contains the type of surveillance message.

Vendor ID
4491

VSA Type
214

AVP Type
ENUM

Supported enumerated value(s):

0 REPORT

1 CORRELATE

2 CARRIER_INFO

AVP Flag
M

Event-Report-Indication

This AVP specifies which type of changes will trigger an event report from the PCRF. This AVP is used to report an event coming from BBERF/PCEF and also to provide information about some event-triggers to the PCRF.

Vendor ID
10415

VSA Type
1033

AVP Type
GROUPED

Supported group value(s):

[EVENT_TRIGGER]

[RAT_TYPE]

[QOS_INFORMATION]

[RAI]

[3GPP_USER_LOCATION_INFO]

[TRACE_DATA]

[TRACE_REFERENCE]

[3GPP2_BSID]

[3GPP_MS_TIMEZONE]

[3GPP_SGSN_ADDRESS]

[3GPP_SGSN_IPV6_ADDRESS]

AVP Flag
M

Event-Timestamp

This AVP contains the time the event was reported.

Vendor ID
0

VSA Type
55

AVP Type
TIME

AVP Flag
M

Event-Trigger

This AVP indicates an event that shall cause a re-request of charging rules.

Vendor ID
10415

VSA Type
1006

AVP Type
ENUM

Supported enumerated value(s):

0 SGSN_CHANGE

1 QOS_CHANGE

2 RAT_CHANGE

3 TFT_CHANGE

4 PLMN_CHANGE

5 LOSS_OF_FLOW

6 RECOVERY_OF_FLOW

7 IP_CAN_CHANGE

8 GW_PCEF_MALFUNCTION

9 RESOURCES_LIMITATION

10 MAX_NR_BEARERS_REACHED

11 QOS_CHANGE_EXCEEDING_AUTHORIZATION

12 RAI_CHANGE

13 USER_LOCATION_CHANGE

14 NO_EVENT_TRIGGERS

15 OUT_OF_CREDIT

16 REALLOCATION_OF_CREDIT

17 REVALIDATION_TIMEOUT

18 UE_IP_ADDRESS_ALLOCATE

19 UE_IP_ADDRESS_RELEASE

20 DEFAULT_EPS_BEARER_QOS_CHANGE

21 AN_GW_CHANGE

22 SUCCESSFUL_RESOURCE_ALLOCATION

23 RESOURCE_MODIFICATION_REQUEST

24 PGW_TRACE_CONTROL

25 UE_TIME_ZONE_CHANGE

26 USAGE_REPORT

33 USAGE_THRESHOLD_REACHED

34 SERVICE_FLOW_DETECTION

2000 PRESERVATION_CHANGED

2001 REACTIVATION_CHANGED

1000 TFT_DELETED

1001 LOSS_OF_BEARER

1002 RECOVERY_OF_BEARER

1003 POLICY_ENFORCEMENT_FAILED

AVP Flag

M

Event-Type

This AVP contains information about the type of chargeable telecommunication service/event for which the accounting-request message is generated.

Vendor ID
10415

VSA Type
823

AVP Type
GROUPED

Supported group value(s):

[SIP_METHOD]

[EVENT]

[EXPIRES]

AVP Flag
M

Experimental-Result

This AVP contains the Result code of SUCCESS or FAILURE. The exact value is specific to Vendor-Id.

Vendor ID
0

VSA Type
297

AVP Type
GROUPED

Supported group value(s):

[VENDOR_ID]

[EXPERIMENTAL_RESULT_CODE]

AVP Flag
M

Experimental-Result-Code

This AVP contains vendor-specific result codes to indicate temporary or permanent failures.

Vendor ID
0

VSA Type
298

AVP Type
ENUM

Supported enumerated value(s):

1001 DIAMETER_MULTI_ROUND_AUTH

2001 DIAMETER_SUCCESS

2002 DIAMETER_LIMITED_SUCCESS

2021 DIAMETER_PDP_CONTEXT_DELETION_INDICATION

3001 DIAMETER_COMMAND_UNSUPPORTED

3002 DIAMETER_UNABLE_TO_DELIVER

3003 DIAMETER_REALM_NOT_SERVED

3004 DIAMETER_TOO_BUSY

3005 DIAMETER_LOOP_DETECTED

3006 DIAMETER_REDIRECT_INDICATION

3007 DIAMETER_APPLICATION_UNSUPPORTED

3008 DIAMETER_INVALID_HDR_BITS

3009 DIAMETER_INVALID_AVP_BITS

3010 DIAMETER_UNKNOWN_PEER

4001 DIAMETER_AUTHENTICATION_REJECTED

4002 DIAMETER_OUT_OF_SPACE

4003 ELECTION_LOST

4010 DIAMETER_END_USER_SERVICE_DENIED

4011 DIAMETER_CREDIT_CONTROL_NOT_APPLICABLE

4012 DIAMETER_CREDIT_LIMIT_REACHED

4041 INSUFFICIENT-RESOURCES

4043 COMMIT-FAILURE

4044 REFRESH-FAILURE

4045 QOS-PROFILE-FAILURE

4046 ACCESS-PROFILE-FAILURE

4047 PRIORITY-NOT-GRANTED

4121 DIAMETER_ERROR_OUT_OF_RESOURCES

4141 DIAMETER_PCC_BEARER_EVENT

4142 DIAMETER_BEARER_EVENT

4181 AUTHENTICATION_DATA_UNAVAILABLE

5001 DIAMETER_AVP_UNSUPPORTED

5002 DIAMETER_UNKNOWN_SESSION_ID

5003 DIAMETER_AUTHORIZATION_REJECTED

5004 DIAMETER_INVALID_AVP_VALUE

5005 DIAMETER_MISSING_AVP

5006 DIAMETER_RESOURCES_EXCEEDED

5007 DIAMETER_CONTRADICTING_AVPS

5008 DIAMETER_AVP_NOT_ALLOWED

5009 DIAMETER_AVP_OCCURS_TOO_MANY_TIMES

5010 DIAMETER_NO_COMMON_APPLICATION

5011 DIAMETER_UNSUPPORTED_VERSION

5012 DIAMETER_UNABLE_TO_COMPLY

5013 DIAMETER_INVALID_BIT_IN_HEADER

5014 DIAMETER_INVALID_AVP_LENGTH

5015 DIAMETER_INVALID_MESSAGE_LENGTH

5016 DIAMETER_INVALID_AVP_BIT_COMBO

5017 DIAMETER_NO_COMMON_SECURITY

5021 BINDING-FAILURE

5030 DIAMETER_USER_UNKNOWN

5031 DIAMETER_RATING_FAILED

5041 MODIFICATION-FAILURE

5061 INVALID_SERVICE_INFORMATION

5062 FILTER_RESTRICTIONS

5063 REQUESTED_SERVICE_NOT_AUTHORIZED

5064 DUPLICATED_AF_SESSION

5065 IP_CAN_SESSION_NOT_AVAILABLE

5120 DIAMETER_ERROR_START_INDICATION

5121 DIAMETER_ERROR_STOP_INDICATION

5122 DIAMETER_ERROR_UNKNOWN_MBMS_BEARER_SERVICE

5123 DIAMETER_ERROR_SERVICE_AREA

5140 DIAMETER_ERROR_INITIAL_PARAMETERS

5141 DIAMETER_ERROR_TRIGGER_EVENT

5142 DIAMETER_PCC_RULE_EVENT

5143 DIAMETER_ERROR_BEARER_NOT_AUTHORIZED

5144 DIAMETER_ERROR_TRAFFIC_MAPPING_INFO_REJECTED

5145 DIAMETER_QOS_RULE_EVENT

5147 DIAMETER_ERROR_CONFLICTING_REQUEST

5420 ERROR_UNKNOWN_EPS_SUBSCRIPTION

5421 ERROR_RAT_NOT_ALLOWED

5402 ERROR_ROAMING_NOT_ALLOWED

5422 ERROR_EQUIPMENT_UNKNOWN

AVP Flag

M

Expiration-Date

This AVP contains information on when the subscription to the CSG-Id expires.

Vendor ID
10415

VSA Type
1439

AVP Type
TIME

AVP Flag
M

Expires

This AVP contains the content of the "Expires" header.

Vendor ID
10415

VSA Type
888

AVP Type
UINT32

AVP Flag
M

Exponent

This AVP contains the exponent value to be applied for the Value-Digit AVP within the Unit-Value AVP.

Vendor ID
0

VSA Type
429

AVP Type
INT32

AVP Flag
M

Extended-QoS-Filter-Rule

This AVP identifies one or more traffic flows together with a set of QoS parameters that should be applied to the flow(s) by the Resource Management Function.

Vendor ID
0

VSA Type
6066

AVP Type
UINT32

AVP Flag
M

External-Client

This AVP contains the identities of the external clients that are allowed to locate a target UE for a MT-LR.

Vendor ID
10415

VSA Type
1479

AVP Type
GROUPED

Supported group value(s):

[CLIENT_IDENTITY]

[GMLC_RESTRICTION]

[NOTIFICATION_TO_UE_USER]

AVP Flag
M

FID

This AVP contains the Flow Correlation ID.

Vendor ID
10415

VSA Type
7003

AVP Type
OCTETSTRING

AVP Flag
M

Failed-AVP

This AVP contains the missing and/or unsupported AVPs that caused the failure.

Vendor ID
0

VSA Type
279

AVP Type
GROUPED

Supported group value(s): none

AVP Flag
M

Feature-List

This AVP contains a bit mask indicating the supported features of an application.

Vendor ID
10415

VSA Type
630

AVP Type
UINT32

AVP Flag
M

Feature-List-ID

This AVP contains the identity of the featured list.

Vendor ID
10415

VSA Type
629

AVP Type
UINT32

AVP Flag
M

Feature-List-ID-Resp

This AVP contains the identity of the featured list.

Vendor ID
10415

VSA Type
629

AVP Type
UINT32

AVP Flag
N/A

Feature-List-Resp

This AVP contains a bit mask indicating the supported features of an application.

Vendor ID
10415

VSA Type
630

AVP Type
UINT32

AVP Flag
N/A

Filter-Id

This AVP contains the name of the filter list for the user.

Vendor ID
0

VSA Type
11

AVP Type
UTF8STRING

AVP Flag
M

Final-Unit-Action

This AVP defines the behavior of the service element when the user's account cannot cover the cost of the service.

Vendor ID
0

VSA Type
449

AVP Type
ENUM

Supported enumerated value(s):

0 TERMINATE

1 REDIRECT

2 RESTRICT_ACCESS

AVP Flag
M

Final-Unit-Indication

This AVP indicates that the Granted-Service-Unit AVP in the Credit-Control-Answer, or in the AA answer, contains the final units for the service.

Vendor ID
0

VSA Type
430

AVP Type
GROUPED

Supported group value(s):

[FINAL_UNIT_ACTION]

[RESTRICTION_FILTER_RULE]

[FILTER_ID]

[REDIRECT_SERVER]

AVP Flag
M

Firmware-Revision

Support for Vendor Specific Applications.

Vendor ID
0

VSA Type
267

AVP Type
UINT32

AVP Flag
N/A

Flow-Description

This AVP contains the service flow filter parameters for a charging rule.

Vendor ID
10415

VSA Type
507

AVP Type
IPFILTERRULE

AVP Flag
M

Flow-Description-Info

This grouped AVP is used within the Flow-Info AVP to identify a flow and associated precedence value from the AGW to the PCRF.

Vendor ID
5535

VSA Type
1022

AVP Type
GROUPED

Supported group value(s):

[FLOW_DESCRIPTION]

[PRECEDENCE]

AVP Flag
M

Flow-Grouping

This AVP indicates that no other IP Flows shall be transported together with the listed IP Flows in the same PDP context(s).

Vendor ID
10415

VSA Type
508

AVP Type
GROUPED

Supported group value(s):

[FLOWS]

AVP Flag
M

Flow-Identifier

This AVP contains the identifier of the IP flow(s) of a given Flow-Info to which specific information refers.

Vendor ID
5535

VSA Type
1008

AVP Type
OCTETSTRING

AVP Flag
M

Flow-Info

This AVP contains the customized information of the IP flow(s). This is a unique identifier within the context of an IP-CAN session for the IP flow(s) given within the same Flow-Info AVP. The flow identifier is selected by AGW. The Flow-Description AVP(s) describe the flow using an IPFilterRule. If two Flow-Description AVPs are included, one shall represent the uplink and the other the downlink.

Vendor ID
5535

VSA Type
1007

AVP Type
GROUPED

Supported group value(s):

[FLOW_IDENTIFIER]

[FLOW_DESCRIPTION_INFO]

[REQUESTED_QOS]

[GRANTED_QOS]

[FLOW_STATUS]

AVP Flag
M

Flow-Information

This AVP contains the information from a single IP flow packet filter including the flow description.

Vendor ID
10415

VSA Type
1058

AVP Type
GROUPED

Supported group value(s):

[FLOW_DESCRIPTION]

[PACKET_FILTER_IDENTIFIER]

[TOS_TRAFFIC_CLASS]

[SECURITY_PARAMETER_INDEX]

[FLOW_LABEL]

AVP Flag
M

Flow-Label

This AVP contains the IPv6 flow label header field.

Vendor ID
10415

VSA Type
1057

AVP Type
OCTETSTRING

AVP Flag
M

Flow-Number

This AVP contains the ordinal number of the IP flow(s).

Vendor ID
10415

VSA Type
509

AVP Type
UINT32

AVP Flag
M

Flow-Operation

This AVP indicates the IP-CAN flow event that causes a request for PCC rules.

Vendor ID
5535

VSA Type
1006

AVP Type
ENUM

Supported enumerated value(s):

0 TERMINATION

1 ESTABLISHMENT

2 MODIFICATION

AVP Flag
M

Flow-Status

This AVP indicates whether the IP flow(s) are enabled or disabled.

Vendor ID
10415

VSA Type
511

AVP Type
ENUM

Supported enumerated value(s):

0 ENABLED-UPLINK

1 ENABLED-DOWNLINK

2 ENABLED

3 DISABLED

4 REMOVED

5 TERMINATE

AVP Flag
M

Flow-Usage

This AVP contains information about the usage of IP Flows.

Vendor ID
10415

VSA Type
512

AVP Type
ENUM

Supported enumerated value(s):

0 NO_INFORMATION

1 RTCP

2 AF_SIGNALLING

AVP Flag
M

Flows

This AVP contains the flow identifiers of the IP flows related to a charging rule as provided by the Application Function (AF).

Vendor ID
10415

VSA Type
510

AVP Type
GROUPED

Supported group value(s):

[MEDIA_COMPONENT_NUMBER]

[FLOW_NUMBER]

AVP Flag
M

Framed-Appletalk-Link

This AVP contains the AppleTalk network number that should be used for the serial link to the user, which is another AppleTalk router.

Vendor ID
0

VSA Type
37

AVP Type
UINT32

AVP Flag
M

Framed-Appletalk-Network

This AVP contains the AppleTalk Network number that the NAS should probe to allocate an AppleTalk node for the user.

Vendor ID
0

VSA Type
38

AVP Type
UINT32

AVP Flag
M

Framed-Appletalk-Zone

This AVP contains the AppleTalk Default Zone to be used for the user.

Vendor ID
0

VSA Type
39

AVP Type
OCTETSTRING

AVP Flag
M

Framed-Compression

This AVP contains the compression protocol to be used for the link.

Vendor ID
0

VSA Type
13

AVP Type
ENUM

Supported enumerated value(s):

0 None

1 VJ_TCP-IP_header_compression

2 IPX-header-compression

3 Stac-LZS-compression

AVP Flag
M

Framed-IP-Address

This AVP contains an IPv4 address of the type specified in the attribute value to be configured for the user.

Vendor ID
0

VSA Type
8

AVP Type
OCTETSTRING

AVP Flag
M

Framed-IP-Netmask

This AVP contains the four octets of the IPv4 netmask to be configured for the user when the user is a router to a network.

Vendor ID
0

VSA Type
9

AVP Type
OCTETSTRING

AVP Flag
M

Framed-IPX-Network

This AVP contains the IPX network number to be configured for the user.

Vendor ID
0

VSA Type
23

AVP Type
UINT32

AVP Flag
M

Framed-IPv6-Pool

This AVP contains the name of an assigned pool that must be used to assign an IPv6 prefix for the user.

Vendor ID
0

VSA Type
100

AVP Type
OCTETSTRING

AVP Flag
M

Framed-IPv6-Prefix

This AVP contains the IPv6 prefix to be configured for the user. One or more AVPs MAY be used in authorization requests as a hint to the server that a specific IPv6 prefixes are desired.

Vendor ID
0

VSA Type
97

AVP Type
OCTETSTRING

AVP Flag
M

Framed-IPv6-Route

This AVP contains the ASCII routing information to be configured for the user on the NAS.

Vendor ID
0

VSA Type
99

AVP Type
UTF8STRING

AVP Flag
N/A

Framed-Interface-Id

This AVP contains the IPv6 interface identifier to be configured for the user.

Vendor ID
0

VSA Type
96

AVP Type
UINT64

AVP Flag
M

Framed-MTU

This AVP contains the Maximum Transmission Unit (MTU) to be configured for the user, when it is not negotiated by some other means (such as PPP).

Vendor ID
0

VSA Type
12

AVP Type
UINT32

AVP Flag
M

Framed-Pool

This AVP contains the name of an assigned address pool that should be used to assign an address for the user.

Vendor ID
0

VSA Type
88

AVP Type
OCTETSTRING

AVP Flag
M

Framed-Protocol

This AVP contains the framing to be used for framed access.

Vendor ID
0

VSA Type
7

AVP Type
ENUM

Supported enumerated value(s):

1 PPP

2 SLIP

3 AppleTalk-Remote-Access-Protocol_ARAP

4 Gandalf-proprietary-SingleLink_MultiLink-protocol

5 Xylogics-proprietary_IPX-SLIP

6 X75-Synchronous

AVP Flag
M

Framed-Route

This AVP contains the ASCII routing information to be configured for the user on the NAS.

Vendor ID
0

VSA Type
22

AVP Type
UTF8STRING

AVP Flag
M

Framed-Routing

This AVP contains the routing method for the user when the user is a router to a network.

Vendor ID
0

VSA Type
10

AVP Type
ENUM

Supported enumerated value(s):

0 None

1 Send-routing-packets

2 Listen-for-routing-packets

3 Send-and-Listen

AVP Flag
M

From-SIP-Header

This AVP contains the information in the "From" header

Vendor ID
10415

VSA Type
644

AVP Type
OCTETSTRING

AVP Flag
N/A

G-S-U-Pool-Identifier

Specifies the credit pool from which credit is drawn for this unit type.

Vendor ID
0

VSA Type
453

AVP Type
UINT32

AVP Flag
M

G-S-U-Pool-Reference

This AVP contains a reference to a credit pool, a unit-type and a multiplier (using the Unit-Value AVP). It is used within Granted-Service-Units AVP to indicate that credit Service-Units AVP to indicate that credit of a particular type is pooled.

Vendor ID
0

VSA Type
457

AVP Type
GROUPED

Supported group value(s):

[G_S_U_POOL_IDENTIFIER]

[CC_UNIT_TYPE]

[UNIT_VALUE]

AVP Flag
M

GERAN-Vector

This AVP contains Authentication Information for GERAN.

Vendor ID
10415

VSA Type
6019

AVP Type
GROUPED

Supported group value(s):

[ITEM_NUMBER]

[RAND]

[SRES]

[KC_KEY]

AVP Flag
M

GGSN-Address

This AVP contains IP address of the GGSN used by the GTP control plane for context establishment. It is the same as the IP-address of the GGSN that generated the GPRS Charging ID used in the GCDRs.

Vendor ID
10415

VSA Type
847

AVP Type
ADDRESS

AVP Flag

M

GMLC-Address

This AVP contains the IPv4 or IPv6 address of the V-GMLC associated with the serving node.

Vendor ID
10415

VSA Type
1474

AVP Type
OCTETSTRING

AVP Flag
M

GMLC-Number

This AVP contains the ISDN number of the GMLC.

Vendor ID
10415

VSA Type
1474

AVP Type
OCTETSTRING

AVP Flag
M

GMLC-Restriction

This attritbue contains GMLC Restriction List.

Vendor ID
10415

VSA Type
1481

AVP Type
ENUM

Supported enumerated value(s):

0 GMLC_LIST

1 HOME_COUNTRY

AVP Flag
M

GPRS-Subscription-Data

This AVP contains the information related to the user profile relevant for GPRS.

Vendor ID
10415

VSA Type
1467

AVP Type
GROUPED

Supported group value(s):

[COMPLETE_DATA_LIST_INCLUDED_INDICATOR]

[PDP_CONTEXT]

AVP Flag
M

Geospatial-Location

This AVP contains location information using the Location Configuration Information (LCI) format.

Vendor ID
13019

VSA Type
356

AVP Type
OCTETSTRING

AVP Flag
M

Globally-Unique-Address

This AVP contains the UE's address.

Vendor ID
13019

VSA Type
300

AVP Type
GROUPED

Supported group value(s):

[FRAMED_IP_ADDRESS]

[ADDRESS_REALM]

AVP Flag
M

Granted-QoS

It is used within the Flow-Info AVP to indicate the QoS granted to the UE for a particular IP flow in the high rate packet data radio access network.

Vendor ID
5535

VSA Type
1011

AVP Type
GROUPED

Supported group value(s):

[QOS_CLASS]

[MIN_BANDWIDTH_UL]

[MIN_BANDWIDTH_DL]

AVP Flag
M

Granted-Service-Unit

This AVP contains the amount of units that the Diameter credit-control client can provide to the end user until the service must be released or the new Credit-Control-Request must be sent.

Vendor ID
0

VSA Type
431

AVP Type
GROUPED

Supported group value(s):

[TARIFF_TIME_CHANGE]

[TARIFF_CHANGE_USAGE]

[CC_TIME]

[CC_MONEY]

[CC_TOTAL_OCTETS]

[CC_INPUT_OCTETS]

[CC_OUTPUT_OCTETS]

[CC_SERVICE_SPECIFIC_UNITS]

AVP Flag
M

Guaranteed-Bitrate-DL

This AVP contains the guaranteed bit rate allowed for the downlink direction.

Vendor ID
10415

VSA Type
1025

AVP Type
UINT32

AVP Flag
M

Guaranteed-Bitrate-UL

This AVP contains the guaranteed bit rate allowed for the uplink direction.

Vendor ID
10415

VSA Type
1026

AVP Type
UINT32

AVP Flag
M

HPLMN-ODB

This AVP contains a bit mask indicating the HPLMN specific services of a subscriber that are barred by the operator.

Vendor ID
10415

VSA Type
1418

AVP Type
UINT32

AVP Flag
M

Home-Agent

This AVP contains the HA IPv4 address that the MS requests or the HA IPv4 address that the H-AAA assigns.

Vendor ID
5535

VSA Type

3

AVP Type
ADDRESS

AVP Flag
M

Host-IP-Address

This AVP contains IP address of the mobile station.

Vendor ID
0

VSA Type
257

AVP Type
ADDRESS

AVP Flag
M

IDA-Flags

The IDA-Flags AVP contains a bit mask.

Vendor ID
10415

VSA Type
1441

AVP Type
UINT32

AVP Flag
M

IDR-Flags

This AVP contains a bit mask.

Vendor ID
10415

VSA Type
1490

AVP Type
UINT32

AVP Flag
M

IMEI

This AVP contains the International Mobile Equipment Identity (IMEI).

Vendor ID
10415

VSA Type
6003

AVP Type
UTF8STRING

AVP Flag
M

IMS-Charging-Identifier

This AVP contains the IMS Charging Identifier (ICID) as generated by an IMS node for a SIP session.

Vendor ID
10415

VSA Type
841

AVP Type
UTF8STRING

AVP Flag
M

IMS-Communication-Service-Identifier

This AVP contains the IMS Communication Service Identifier (ICSI) as contained in the P-Asserted-Service header of a SIP request to identify an IMS Communication Service as defined in TS 24.229.

Vendor ID
10415

VSA Type
1281

AVP Type
UTF8STRING

AVP Flag
M

IMS-Information

This grouped AVP allows the transmission of additional IMS service specific information elements.

Vendor ID
10415

VSA Type
876

AVP Type
GROUPED

Supported group value(s):

[EVENT_TYPE]

[ROLE_OF_NODE]

[NODE_FUNCTIONALITY]

[USER_SESSION_ID]

[CALLING_PARTY_ADDRESS]

[CALLED_PARTY_ADDRESS]

[CALLED_ASSERTED_IDENTITY]

[ASSOCIATED_URI]

[TIME_STAMPS]

[APPLICATION_SERVER_INFORMATION]

[INTER_OPERATOR_IDENTIFIER]

[IMS_CHARGING_IDENTIFIER]

[IMS_COMMUNICATION_SERVICE_IDENTIFIER]

[SDP_SESSION_DESCRIPTION]

[SDP_MEDIA_COMPONENT]

[MESSAGE_BODY]

[CAUSE_CODE]

[ACCESS_NETWORK_INFORMATION]

[EARLY_MEDIA_DESCRIPTION]

AVP Flag
M

IMSI-Unauthenticated-Flag

This AVP indicates whether or not the served IMSI is authenticated.

Vendor ID
10415

VSA Type
2308

AVP Type
ENUM

Supported enumerated value(s):

0 AUTHENTICATED

1 UNAUTHENTICATED

AVP Flag
M

IP-CAN-Type

This AVP indicate the type of Connectivity Access Network in which the user is connected.

Vendor ID
10415

VSA Type
1027

AVP Type
ENUM

Supported enumerated value(s):

0 3GPP-GPRS

1 DOCSIS

2 xDSL

3 WiMAX

4 3GPP2

5 3GPP-EPS

6 NON-3GPP-EPS

AVP Flag
M

IP-MMS

IP mobility selector.

Vendor ID
10415

VSA Type
6076

AVP Type
UINT32

AVP Flag
M

IP-Version-Authorized

This AVP indicates whether the MS is authorized for using IPv4 and/or IPv6.

Vendor ID
5535

VSA Type

11

AVP Type
ENUM

Supported enumerated value(s):

0 IPv4_or_IPv6

1 IPv4_ONLY

2 IPv6_ONLY

AVP Flag
M

Identity-Set

This AVP contains the requested set of IMS Public identities.

Vendor ID
0

VSA Type
708

AVP Type
ENUM

Supported enumerated value(s): none

AVP Flag
N/A

Idle-Timeout

Sets the maximum number of consecutive seconds of idle connection allowable to the user before termination of the session or before a prompt is issued.

Vendor ID
0

VSA Type
28

AVP Type
UINT32

AVP Flag
M

Immediate-Response-Preferred

This AVP indicates which type of AV is requested for immediate use in the MME/SGSN.

Vendor ID
10415

VSA Type
6015

AVP Type
UINT32

AVP Flag
M

Inband-Security-Id

Advertise support of the Security portion of the application.

Vendor ID
0

VSA Type
299

AVP Type
ENUM

Supported enumerated value(s):

0 NO_INBAND_SECURITY

1 TLS

AVP Flag
M

Incoming-Trunk-Group-ID

This AVP contains the incoming PSTN leg.

Vendor ID
0

VSA Type
852

AVP Type
UTF8STRING

AVP Flag
M

Integrity-Key

This AVP contains the Integrity Key (IK).

Vendor ID
10415

VSA Type
626

AVP Type

OCTETSTRING

AVP Flag
M

Inter-Operator-Identifier

This AVP contains the identification of the network neighbors (originating and terminating) as exchanged via SIP signalling. The Inter-Operator-Identifier AVP contains the CIC code present in the Carrier-info message.

Vendor ID
10415

VSA Type
838

AVP Type
GROUPED

Supported group value(s):

[ORIGINATING_IOI]

[TERMINATING_IOI]

AVP Flag
M

Item-Number

If more than one EPS Vector is included within one Authentication-Info AVP, the Item-Number AVP is present within each EPS Vector.

Vendor ID
10415

VSA Type
1419

AVP Type
UINT32

AVP Flag
M

KASME

This AVP contains the KASME (EAP Authentication Vector).

Vendor ID
10415

VSA Type
1450

AVP Type
OCTETSTRING

AVP Flag
M

KC-Key

This AVP contains the Ciphering Key.

Vendor ID
10415

VSA Type
1453

AVP Type
OCTETSTRING

AVP Flag
M

LCS-Info

This AVP contains LCS related information for a subscriber.

Vendor ID
10415

VSA Type
1473

AVP Type
GROUPED

Supported group value(s):

[GMLC_ADDRESS]

[LCS_PRIVACYEXCEPTION]

[MO_LR]

AVP Flag
M

LCS-PrivacyException

This AVP contains the classes of LCS Client that are allowed to locate any target UE.

Vendor ID
10415

VSA Type
1475

AVP Type
GROUPED

Supported group value(s):

[SS_CODE]

[SS_STATUS]

[NOTIFICATION_TO_UE_USER]

[EXTERNAL_CLIENT]

[PLMN_CLIENT]

[SERVICE_TYPE]

AVP Flag
M

LI-Information

This AVP holds all the other surveillance AVPs.

Vendor ID
4491

VSA Type
218

AVP Type
GROUPED

Supported group value(s):

[EVENT_MESSAGE_TYPE]

[ELEMENT_TYPE]

[ELEMENT_ID]

[TAP_ID]

[SIP_MESSAGE]

[DIRECT_MESSAGE]

[DIRECTION]

[DIALOG_ID]

[NEW_DIALOG_ID]

[CORRELATE_REASON]

[BCID]

AVP Flag
M

Last-CellSector-Location

This AVP indicates subscriber last cell/sector location.

Vendor ID
10415

VSA Type

536

AVP Type
UTF8STRING

AVP Flag
M

Latching-Indication

This AVP contains the latching indication.

Vendor ID
13019

VSA Type
457

AVP Type
ENUM

Supported enumerated value(s):

0 LATCH

1 RELATCH

AVP Flag
N/A

Line-Identifier

This AVP contains a fixed broadband access line identifier associated with the user.

Vendor ID
13019

VSA Type
500

AVP Type
OCTETSTRING

AVP Flag
M

Local-Sequence-Number

This AVP contains the service data container sequence number; incremented by 1 for each service data container closed.

Vendor ID
10415

VSA Type
2063

AVP Type
UINT32

AVP Flag
M

Location-Information

This AVP contains the location information (or a pointer to such information) in a form that is suitable for the requesting application.

Vendor ID
13019

VSA Type
350

AVP Type
GROUPED

Supported group value(s):

[LINE_IDENTIFIER]

[CIVIC_LOCATION]

[GEOSPATIAL_LOCATION]

AVP Flag
M

Logical-Access-Id

This AVP contains the identity of the logical access where the user equipment is connected.

Vendor ID
0

VSA Type
302

AVP Type
OCTETSTRING

AVP Flag
M

Loose-Route-Indication

This AVP indicates to the S-CSCF whether or not the loose route mechanism is required to serve the registered Public User Identities.

Vendor ID
10415

VSA Type
638

AVP Type
ENUM

Supported enumerated value(s):

0 LOOSE_ROUTE_NOT_REQUIRED

1 LOOSE_ROUTE_REQUIRED

AVP Flag
N/A

MBMS-2G-3G-Indicator

This AVP indicates whether the MBMS bearer service will be delivered in 2G only, 3G only of both coverage areas.

Vendor ID
10415

VSA Type
907

AVP Type
ENUM

Supported enumerated value(s):

0 2G

1 3G

2 2G_AND_3G

AVP Flag
M

MBMS-BMSC-SSM-IP-Address

This AVP contains the IPv4 address of BMSC for Source Specific Multicasting.

Vendor ID
10415

VSA Type
918

AVP Type
UTF8STRING

AVP Flag
M

MBMS-BMSC-SSM-IPv6-Address

This AVP contains the IPv6 address of BMSC for Source Specific Multicasting.

Vendor ID
10415

VSA Type
919

AVP Type
UTF8STRING

AVP Flag
M

MBMS-Counting-Information

This AVP contains explicit information about whether the MBMS Counting procedures are applicable for the MBMS Service that is about to start.

Vendor ID
10415

VSA Type
914

AVP Type
ENUM

Supported enumerated value(s):

0 COUNTING_NOT_APPLICABLE

1 COUNTING_APPLICABLE

AVP Flag
M

MBMS-GGSN-Address

This AVP contains the IPv4 address of GGSN for user plane data.

Vendor ID
10415

VSA Type
916

AVP Type
UTF8STRING

AVP Flag
M

MBMS-GGSN-IPv6-Address

This AVP contains the IPv6 address of GGSN for user plane data.

Vendor ID
10415

VSA Type
917

AVP Type
UTF8STRING

AVP Flag
M

MBMS-Required-QoS

This AVP indicates the Quality of Service required for the MBMS bearer service.

Vendor ID
10415

VSA Type
913

AVP Type
UTF8STRING

AVP Flag
M

MBMS-Service-Area

This AVP indicates the area over which the MBMS bearer service has to be distributed.

Vendor ID
10415

VSA Type
903

AVP Type
OCTETSTRING

AVP Flag
M

MBMS-Service-Type

This AVP contains explicit information about the type of service that the BM-SC Start Procedure is about to start.

Vendor ID
10415

VSA Type
906

AVP Type
ENUM

Supported enumerated value(s):

0 MULTICAST

1 BROADCAST

AVP Flag
M

MBMS-Session-Duration

This AVP indicates the estimated session duration, if available.

Vendor ID
10415

VSA Type
904

AVP Type
OCTETSTRING

AVP Flag
M

MBMS-Session-Identity

This AVP identifies a transmission of a specific MBMS session along with TMGI.

Vendor ID
10415

VSA Type
908

AVP Type
OCTETSTRING

AVP Flag
M

MBMS-Session-Repetition-number

This AVP contains the session identity repetition number of the MBMS transmission session on the Gmb interface.

Vendor ID
10415

VSA Type
912

AVP Type
OCTETSTRING

AVP Flag
M

MBMS-StartStop-Indication

This AVP indicates whether it is session start or stop procedure.

Vendor ID
10415

VSA Type

902

AVP Type
ENUM

Supported enumerated value(s):

0 START

1 STOP

2 UPDATE

AVP Flag
M

MBMS-Time-To-Data-Transfer

This AVP indicates the expected time between reception of the MBMS Session Start and the commencement of the MBMS Data flow.

Vendor ID
10415

VSA Type
911

AVP Type
OCTETSTRING

AVP Flag
M

MBMS-User-Data-Mode-Indication

This AVP indicates whether the sending entity supports unicast or multicast mode of operation.

Vendor ID
10415

VSA Type
915

AVP Type
ENUM

Supported enumerated value(s):

0 UNICAST

1 MULTICAST_AND_UNICAST

AVP Flag
M

MEID

This AVP contains the International Mobile Equipment Identity.

Vendor ID
10415

VSA Type
6110

AVP Type
OCTETSTRING

AVP Flag
M

MIP-Feature-Vector

Is added with flag values set by the Foreign Agent or by the AAAF owned by the same administrative domain as the Foreign Agent. The Foreign Agent should include MIP-Feature-Vector AVP within the AMR message it sends to the AAAF.

Vendor ID
10415

VSA Type
337

AVP Type
UINT32

AVP Flag
M

MIP-Home-Agent-Address-IETF

This AVP contains the IPv6 or IPv4 address of the MIPv6 HA.

Vendor ID
0

VSA Type
334

AVP Type
ADDRESS

AVP Flag
M

MIP-Home-Agent-Host

This AVP contains the identity of the assigned MIPv6 HA.

Vendor ID
0

VSA Type
348

AVP Type

GROUPED

Supported group value(s):

[DESTINATION_REALM]

[DESTINATION_HOST]

AVP Flag
M

MIP-Mobile-Node-Address

This AVP contains the HA assigned IPv6 or IPv4 home address of the mobile node.

Vendor ID
10415

VSA Type
333

AVP Type
ADDRESS

AVP Flag
M

MIP6-Agent-Info

This AVP contains necessary information to assign a HA to the MN. It can be an IP address or Fully Qualified Domain Name (FQDN).

Vendor ID
0

VSA Type
486

AVP Type
GROUPED

Supported group value(s):

[MIP_HOME_AGENT_ADDRESS_IETF]

[MIP_HOME_AGENT_HOST]

[MIP6_HOME_LINK_PREFIX]

AVP Flag
M

MIP6-Feature-Vector

This AVP contains the subset of the MIPv6 features supported.

Vendor ID
0

VSA Type
6062

AVP Type
UINT64

AVP Flag
M

MIP6-Home-Link-Prefix

This AVP contains the Mobile IPv6 home network prefix information in a network byte order.

Vendor ID
0

VSA Type
125

AVP Type
OCTETSTRING

AVP Flag
M

MME-Service-Type

MME-Service-Type

Vendor ID
10415

VSA Type
1483

AVP Type
GROUPED

Supported group value(s):

[SERVICETYPEIDENTITY]

[GMLC_RESTRICTION]

[NOTIFICATION_TO_UE_USER]

AVP Flag
M

MO-LR

This AVP contains the classes of Mobile Originating Location Request (MO-LR) for which a subscription exists for a particular MS.

Vendor ID
10415

VSA Type

1485

AVP Type
GROUPED

Supported group value(s):

[SS_CODE]

[SS_STATUS]

AVP Flag
M

MSISDN

This AVP contains an MSISDN, in international number format as described in ITU-T.

Vendor ID
0

VSA Type
701

AVP Type
OCTETSTRING

AVP Flag
M

Mandatory-Capability

This AVP contains single determined mandatory capability of an S-CSCF.

Vendor ID
10415

VSA Type
604

AVP Type
UINT32

AVP Flag
M

Max-Requested-Bandwidth

This AVP contains the maximum subscriber requested bandwidth.

Vendor ID
10415

VSA Type
313

AVP Type
OCTETSTRING

AVP Flag
M

Max-Requested-Bandwidth-DL

This AVP indicates the maximum requested bandwidth in bits per second for a downlink IP flow.

Vendor ID
10415

VSA Type
515

AVP Type
UINT32

AVP Flag
M

Max-Requested-Bandwidth-UL

This AVP indicates the maximum requested bandwidth in bits per second for an uplink IP flow.

Vendor ID
10415

VSA Type
516

AVP Type
UINT32

AVP Flag
M

Media-Component-Description

This AVP contains service information for a single media component within an Application Function (AF) session.

Vendor ID
10415

VSA Type
517

AVP Type
GROUPED

Supported group value(s):

[MEDIA_COMPONENT_NUMBER]

[MEDIA_SUB_COMPONENT]

[AF_APPLICATION_IDENTIFIER]

[MEDIA_TYPE]

[MAX_REQUESTED_BANDWIDTH_UL]

[MAX_REQUESTED_BANDWIDTH_DL]

[FLOW_STATUS]

[RS_BANDWIDTH]

[RR_BANDWIDTH]

AVP Flag
M

Media-Component-Number

This AVP contains the ordinal number of the media component.

Vendor ID
10415

VSA Type
518

AVP Type
UINT32

AVP Flag
M

Media-Initiator-Flag

This AVP indicates which party has requested the session modification.

Vendor ID
10415

VSA Type
882

AVP Type
ENUM

Supported enumerated value(s): none

AVP Flag
M

Media-Initiator-Party

This AVP enumerated in IMS charging, holds the address (SIP URI or TEL URI) of the party (Public User ID or Public Service ID) who initiates the media action, like adding/removing, connecting/disconnecting the media.

Vendor ID
10415

VSA Type
1288

AVP Type
UTF8STRING

AVP Flag
M

Media-Sub-Component

The requested QoS and filters for the set of IP flows identified by their common Flow-Identifier.

Vendor ID
10415

VSA Type
519

AVP Type
GROUPED

Supported group value(s):

[FLOW_NUMBER]

[FLOW_DESCRIPTION]

[FLOW_STATUS]

[FLOW_USAGE]

[MAX_REQUESTED_BANDWIDTH_UL]

[MAX_REQUESTED_BANDWIDTH_DL]

AVP Flag
M

Media-Type

This AVP indicates the type of media in the same way as the SDP media types with the same names like AUDIO, VIDEO.

Vendor ID
10415

VSA Type
520

AVP Type
ENUM

Supported enumerated value(s):

0 AUDIO

1 VIDEO

2 DATA

3 APPLICATION

4 CONTROL

5 TEXT

6 MESSAGE

7 OTHER

AVP Flag
M

Message-Body

This grouped AVP contains information about the message bodies including user-to-user data.

Vendor ID
10415

VSA Type
889

AVP Type
GROUPED

Supported group value(s):

[CONTENT_TYPE]

[CONTENT_LENGTH]

[CONTENT_DISPOSITION]

[ORIGINATOR]

AVP Flag
M

Metering-Method

This AVP indicates what parameters will be metered for offline charging.

Vendor ID
10415

VSA Type
1007

AVP Type
ENUM

Supported enumerated value(s):

0 DURATION

1 VOLUME

2 DURATION_VOLUME

AVP Flag
M

Min-Bandwidth-DL

This AVP contains the requested/granted data rate information, in bits per second, for the mobile in the downlink direction for the associated IP flow.

Vendor ID
5535

VSA Type
1012

AVP Type
UINT32

AVP Flag
M

Min-Bandwidth-UL

This AVP contains the requested/granted data rate information, in bits per second, for the mobile in the uplink direction for the associated IP flow.

Vendor ID
5535

VSA Type
1013

AVP Type
UINT32

AVP Flag
M

Mobile-Node-Identifier

This AVP contains MN-NAI identifying the user in EPS network.

Vendor ID
0

VSA Type
89

AVP Type
OCTETSTRING

AVP Flag
M

Monitoring-Key

This AVP serves as an identifier to a usage monitoring control instance. This AVP is used for usage monitoring control purposes.

Vendor ID
10415

VSA Type
1066

AVP Type
OCTETSTRING

AVP Flag
N/A

Multi-Round-Time-Out

Present in application-specific authorization answer messages whose Result-Code AVP is set to "DIAMETER_MULTI_ROUND_AUTH".

Vendor ID
0

VSA Type
272

AVP Type
UINT32

AVP Flag
N/A

Multiple-Auth-Profile

This AVP indicates Multiple Authentication requirements for a particular user.

Vendor ID
5535

VSA Type
30

AVP Type
ENUM

Supported enumerated value(s): none

AVP Flag
M

Multiple-Auth-Support

This AVP indicates the support of the Multiple Authentication at the SRNC and AGW.

Vendor ID
5535

VSA Type
29

AVP Type
ENUM

Supported enumerated value(s): none

AVP Flag
M

Multiple-Registration-Indication

This AVP indicates to the HSS whether or not the request is related to a multiple registration.

Vendor ID
10415

VSA Type
648

AVP Type
ENUM

Supported enumerated value(s):

0 NOT_MULTIPLE_REGISTRATION

1 MULTIPLE_REGISTRATION

AVP Flag
N/A

Multiple-Services-Credit-Control

This grouped AVP contains the AVPs related to the independent credit-control of multiple services feature.

Vendor ID
0

VSA Type
456

AVP Type
GROUPED

Supported group value(s):

[REQUESTED_SERVICE_UNIT]

[GRANTED_SERVICE_UNIT]

[USED_SERVICE_UNIT]

[TARIFF_CHANGE_USAGE]

[SERVICE_IDENTIFIER]

[RATING_GROUP]

[G_S_U_POOL_REFERENCE]

[VALIDITY_TIME]

[RESULT_CODE]

[FINAL_UNIT_INDICATION]

AVP Flag
M

Multiple-Services-Indicator

This AVP indicates support for independent credit-control of multiple services within the session.

Vendor ID
0

VSA Type
455

AVP Type
ENUM

Supported enumerated value(s):

0 MULTIPLE_SERVICES_NOT_SUPPORTED

1 MULTIPLE_SERVICES_SUPPORTED

AVP Flag
M

NAS-Filter-Rule

This AVP contains filter rules that need to be configured on the NAS for the user.

Vendor ID
0

VSA Type
400

AVP Type
IPFILTERRULE

AVP Flag
M

NAS-IP-Address

This AVP contains the IP address of the NAS providing service to the user.

Vendor ID
0

VSA Type
4

AVP Type
OCTETSTRING

AVP Flag
M

NAS-IPv6-Address

This AVP contains the IPv6 address of the NAS providing service to the user.

Vendor ID
0

VSA Type
95

AVP Type
OCTETSTRING

AVP Flag
M

NAS-Identifier

This AVP contains identity of the NAS providing service to the user.

Vendor ID
0

VSA Type
32

AVP Type
UTF8STRING

AVP Flag
M

NAS-Port

This AVP contains the physical or virtual port number of the NAS which is authenticating the user.

Vendor ID
0

VSA Type
5

AVP Type
UINT32

AVP Flag
M

NAS-Port-Id

This AVP contains ASCII text identifying the port of the NAS authenticating the user.

Vendor ID
0

VSA Type

87

AVP Type
UTF8STRING

AVP Flag
M

NAS-Port-Type

This AVP contains the type of the port on which the NAS is authenticating the user.

Vendor ID
0

VSA Type
61

AVP Type
ENUM

Supported enumerated value(s):

0 Async

1 Sync

2 ISDN_Sync

3 ISDN_Async_V120

4 ISDN_Async_V110

5 Virtual

6 PIAFS

7 HDLC_Clear_Channel

8 X25

9 X75

10 G3_Fax

12 ADSL-CAP-AsymmetricDSL_Carrierless-Amplitude-Phase-Modulation

13 ADSL-DMT-AsymmetricDSL-Discrete-Multi-Tone

14 IDSL-ISDN-Digital-Subscriber-Line

15 Ethernet

16 xDSL-Digital-Subscriber-Line-of-unknown-type

17 Cable

18 Wireless-Other

19 Wireless-IEEE802_11

20 Token-Ring_RAD802_1X

21 FDDI_RAD802_1X

22 Wireless-CDMA2000

23 Wireless-UMTS

24 Wireless-1X-EV

25 IAPP_IEEE-802_11f

AVP Flag
M

NOR-Flags

The NOR-Flags AVP contains a bit mask.

Vendor ID
10415

VSA Type
1443

AVP Type
UINT32

AVP Flag
M

Network-Access-Mode

This AVP indicates whether the subscriber is registered to get access to the CS, PS network, or to both networks.

Vendor ID
10415

VSA Type
1417

AVP Type
ENUM

Supported enumerated value(s):

0 PACKET_AND_CIRCUIT

1 ONLY_CIRCUIT

2 ONLY_PACKET

AVP Flag
M

Network-Element-Type

Network-Element-Type

Vendor ID
10415

VSA Type
1461

AVP Type

ENUM

Supported enumerated value(s):

0 MME

1 SGSN

2 Serving-GW

3 PDN-GW

4 eNodeB

5 RNC

AVP Flag

M

Network-Request-Support

This AVP indicates the UE and network support of the network requested bearer control mode.

Vendor ID

10415

VSA Type

1024

AVP Type

ENUM

Supported enumerated value(s):

0 NETWORK_REQUEST_NOT_SUPPORTED

1 NETWORK_REQUEST_SUPPORTED

AVP Flag

M

New-Dialog-Id

This AVP contains the SIP dialog identifier in the form: Call-ID=x;FTag=y;TTag=z, where x is the value of the SIP Call-ID header, y is the contents of the From header tag, and z is the contents of the To header tag. If the To header tag value is not present in the SIP message then TTag field MUST not be present in the AVP.

Vendor ID

4491

VSA Type

219

AVP Type

UTF8STRING

AVP Flag

M

Node-Functionality

This AVP includes the functionality identifier of the node where the cause code was generated.

Vendor ID
0

VSA Type
862

AVP Type
ENUM

Supported enumerated value(s):

0 S-CSCF

1 P-CSCF

2 I-CSCF

AVP Flag
M

Node-Id

This AVP contains the operator configurable identifier string for the node that had generated the ACR.

Vendor ID
10415

VSA Type
2064

AVP Type
UTF8STRING

AVP Flag
M

Nortel-Data-Reference

This AVP indicates the type of the Nortel-specific user data requested or updated in the UDR and PUR operation.

Vendor ID
0

VSA Type
301

AVP Type
ENUM

Supported enumerated value(s): none

AVP Flag
M

Notification-To-UE-User

Notification-To-UE-User

Vendor ID
10415

VSA Type
1478

AVP Type
ENUM

Supported enumerated value(s):

0 NOTIFY_LOCATION_ALLOWED

1 NOTIFYANDVERIFY_ALLOWED_IF_NO_RESPONSE

2 NOTIFYANDVERIFY_NOT_ALLOWED_IF_NO_RESPONSE

3 LOCATION_NOT_ALLOWED

AVP Flag
M

Number-Of-Requested-Vectors

This AVP contains the number of AVs the MME is prepared to receive.

Vendor ID
10415

VSA Type
6013

AVP Type
UINT32

AVP Flag
M

Number-Portability-Routing-Information

This AVP contains information on routing number received by S-CSCF during number portability look-up (ENUM/DNS).

Vendor ID
10415

VSA Type
2024

AVP Type
UTF8STRING

AVP Flag
M

OMC-Id

OMC-Id

Vendor ID
10415

VSA Type
1466

AVP Type
OCTETSTRING

AVP Flag
M

Offline

Defines whether the offline charging interface from the TPF for the associated charging rule shall be enabled.

Vendor ID
10415

VSA Type
1008

AVP Type
ENUM

Supported enumerated value(s):

0 DISABLE_OFFLINE

1 ENABLE_OFFLINE

AVP Flag
M

Online

Defines whether the online charging interface from the TPF for the associated charging rule shall be enabled.

Vendor ID
10415

VSA Type
1009

AVP Type
ENUM

Supported enumerated value(s):

0 DISABLE_ONLINE

1 ENABLE_ONLINE

AVP Flag
M

Operator-Determined-Barring

This AVP contains a bit mask indicating the services of a subscriber that are barred by the operator.

Vendor ID
10415

VSA Type
1425

AVP Type
UINT32

AVP Flag
M

Optional-Capability

This AVP contains single determined optional capability of an S-CSCF.

Vendor ID
10415

VSA Type
605

AVP Type
UINT32

AVP Flag
M

Origin-Host

This AVP indicates the endpoint that originated the Diameter message.

Vendor ID
0

VSA Type
264

AVP Type
DIAMIDENT

AVP Flag
M

Origin-Realm

This AVP indicates the realm of the originator of any Diameter message, and is present in all messages.

Vendor ID
0

VSA Type

296

AVP Type
DIAMIDENT

AVP Flag
M

Origin-State-Id

The Origin-State-Id AVP is a monotonically increasing value that is advanced whenever a Diameter entity restarts with loss of previous state, for example upon reboot. Origin-State-Id MAY be included in any Diameter message, including CER.

Vendor ID
0

VSA Type
278

AVP Type
UINT32

AVP Flag
M

Originating-IOI

This AVP holds the Inter Operator Identifier (IOI) for the originating network as generated by the S-CSCF in the home network of the originating end user.

Vendor ID
0

VSA Type
839

AVP Type
UTF8STRING

AVP Flag
M

Originating-Line-Info

Sent by the NAS system to convey information about the origin of the call from an SS7 system.

Vendor ID
0

VSA Type
94

AVP Type
OCTETSTRING

AVP Flag

N/A

Originating-Request

This AVP indicates that the request is related to an AS originating SIP request in the Location-Information-Request operation.

Vendor ID
10415

VSA Type
633

AVP Type
ENUM

Supported enumerated value(s):

0 ORIGINATING

AVP Flag
M

Originator

This AVP indicates the originating party of the message body.

Vendor ID
10415

VSA Type
864

AVP Type
ENUM

Supported enumerated value(s): none

AVP Flag
M

Outgoing-Trunk-Group-ID

This AVP identifies the outgoing PSTN leg.

Vendor ID
0

VSA Type
853

AVP Type
UTF8STRING

AVP Flag
M

PC-Digest-Algorithm

PC-Digest-Algorithm

Vendor ID
4491

VSA Type
204

AVP Type
OCTETSTRING

AVP Flag
M

PC-Digest-Auth-Param

PC-Digest-Auth-Param

Vendor ID
4491

VSA Type
205

AVP Type
OCTETSTRING

AVP Flag
M

PC-Digest-Domain

PC-Digest-Domain

Vendor ID
4491

VSA Type
206

AVP Type
OCTETSTRING

AVP Flag
M

PC-Digest-HA1

PC-Digest-HA1

Vendor ID
4491

VSA Type

207

AVP Type
OCTETSTRING

AVP Flag
M

PC-Digest-QoP

PC-Digest-QoP

Vendor ID
4491

VSA Type
208

AVP Type
OCTETSTRING

AVP Flag
M

PC-Digest-Realm

PC-Digest-Realm

Vendor ID
4491

VSA Type
209

AVP Type
OCTETSTRING

AVP Flag
M

PC-SIP-Digest-Authenticate

PC-SIP-Digest-Authenticate

Vendor ID
4491

VSA Type
228

AVP Type
GROUPED

Supported group value(s):

[PC_DIGEST_REALM]

[PC_DIGEST_DOMAIN]

[PC_DIGEST_ALGORITHM]

[PC_DIGEST_QOP]

[PC_DIGEST_HA1]

[PC_DIGEST_AUTH_PARAM]

AVP Flag
M

PCC-Rule-Status

This AVP contains the status of a Policy and Charging Control (PCC) Rule.

Vendor ID
10415

VSA Type
1019

AVP Type
ENUM

Supported enumerated value(s):

0 ACTIVE

1 INACTIVE

2 TEMPORARY_INACTIVE

AVP Flag
M

PDFID

This value matches all records from the same packet data flow.

Vendor ID
24757

VSA Type
26

AVP Type
OCTETSTRING

AVP Flag
M

PDG-Address

This AVP contains IP address of the PDG.

Vendor ID
10415

VSA Type

895

AVP Type
ADDRESS

AVP Flag
M

PDG-Charging-Id

This AVP contains the charging identifier generated by the PDG for the tunnel. Charging identifier is generated at tunnel establishment and transferred to 3GPP AAA Server.

Vendor ID
10415

VSA Type
896

AVP Type
UINT32

AVP Flag
M

PDN-Connection-ID

This AVP contains the charging identifier to identify different records belonging to same PDN connection.

Vendor ID
10415

VSA Type
2050

AVP Type
UINT32

AVP Flag
M

PDN-GW-Address

IP address of the PDN GW and this IP address shall be used as the PDN GW IP address.

Vendor ID
10415

VSA Type
6041

AVP Type
ADDRESS

AVP Flag
M

PDN-GW-Allocation-Type

PDN-GW-Allocation-Type

Vendor ID
10415

VSA Type
1438

AVP Type
ENUM

Supported enumerated value(s):

0 STATIC

1 DYNAMIC

AVP Flag
M

PDN-GW-Identity

PDN-GW-Identity

Vendor ID
10415

VSA Type
6044

AVP Type
GROUPED

Supported group value(s):

[PDN_GW_ADDRESS]

[PDN_GW_NAME]

AVP Flag
M

PDN-GW-Name

FQDN which is used to derive the PDN GW IP address using Domain Name Service function.

Vendor ID
10415

VSA Type
6042

AVP Type
UTF8STRING

AVP Flag
M

PDN-Type

This AVP indicates the address type of PDN. It can be IPv4,IPV6 or both.

Vendor ID
10415

VSA Type
1456

AVP Type
ENUM

Supported enumerated value(s):

0 IPv4

1 IPv6

2 IPv4v6

AVP Flag
M

PDP-Address

This AVP contains IP address associated with the IP CAN bearer session (PDP context / PDN connection).

Vendor ID
10415

VSA Type
1227

AVP Type
ADDRESS

AVP Flag
M

PDP-Context

This AVP contains the list of PDP contexts to which a user has subscribed.

Vendor ID
10415

VSA Type
1469

AVP Type
GROUPED

Supported group value(s):

[CONTEXT_IDENTIFIER]

[PDP_TYPE]

[QOS_SUBSCRIBED]

[VPLMN_DYNAMIC_ADDRESS_ALLOWED]

[SERVICE_SELECTION]

[3GPP_CHARGING_CHARACTERISTICS]

AVP Flag
M

PDP-Context-Type

This AVP contains the type of a PDP Context.

Vendor ID
10415

VSA Type
1247

AVP Type
ENUM

Supported enumerated value(s):

0 PRIMARY

1 SECONDARY

AVP Flag
M

PDP-Session-Operation

This value is used to report in an indication of bearer termination that this indication refers to the last PDP context within a PDP session. It is only applicable for GPRS.

Vendor ID
10415

VSA Type
1015

AVP Type
ENUM

Supported enumerated value(s):

0 PDP-SESSION-TERMINATION

AVP Flag
M

PDP-Type

This AVP indicates the type of protocol that is used by MS.

Vendor ID
10415

VSA Type
1470

AVP Type
OCTETSTRING

AVP Flag
M

PGW-Type

Type of P-GW of current flow.

Vendor ID
10415

VSA Type
7002

AVP Type
UINT32

AVP Flag
M

PLMN-Client

PLMN-Client

Vendor ID
10415

VSA Type
1482

AVP Type
ENUM

Supported enumerated value(s):

0 BROADCAST_SERVICE

1 O_AND_M_HPLMN

2 O_AND_M_VPLMN

3 ANONYMOUS_LOCATION

4 TARGET_UE_SUBSCRIBED_SERVICE

AVP Flag
M

PMIP6-MAG-Address

This AVP contains IP address of MAG.

Vendor ID

10415

VSA Type
6070

AVP Type
ADDRESS

AVP Flag
M

PS-Append-Free-Format-Data

This AVP indicates if the information sent in the PS-Free-Format-Data AVP must be appended to the PS-free-format-data stored for the online-session.

Vendor ID
10415

VSA Type
867

AVP Type
ENUM

Supported enumerated value(s):

0 APPEND

1 OVERWRITE

AVP Flag
M

PS-Free-Format-Data

This AVP holds online charging session specific data.

Vendor ID
10415

VSA Type
866

AVP Type
OCTETSTRING

AVP Flag
M

PS-Furnish-Charging-Information

This grouped AVP contains online charging session specific information.

Vendor ID
10415

VSA Type

865

AVP Type
GROUPED

Supported group value(s):

[3GPP_CHARGING_ID]

[PS_FREE_FORMAT_DATA]

[PS_APPEND_FREE_FORMAT_DATA]

AVP Flag
M

PS-Information

This AVP enables the transmission of additional PS service specific information elements.

Vendor ID
10415

VSA Type
874

AVP Type
GROUPED

Supported group value(s):

[3GPP_CHARGING_ID]

[3GPP_PDP_TYPE]

[PDP_ADDRESS]

[3GPP_GPRS_QOS_NEGOTIATED_PROFILE]

[3GPP_SGSN_ADDRESS]

[3GPP_GGSN_ADDRESS]

[3GPP_CG_ADDRESS]

[3GPP_IMSI_MCC_MNC]

[3GPP_GGSN_MCC_MNC]

[3GPP_NSAPI]

[CALLED_STATION_ID]

[3GPP_SESSION_STOP_INDICATOR]

[3GPP_SELECTION_MODE]

[3GPP_CHARGING_CHARACTERISTICS]

[3GPP_SGSN_MCC_MNC]

[3GPP_RAT_TYPE]

[PDP_CONTEXT_TYPE]

AVP Flag
M

PSCID

This AVP contains the P-GW Session Correlation ID.

Vendor ID
10415

VSA Type
1450

AVP Type
OCTETSTRING

AVP Flag
M

PUA-Flags

The PUA-Flags AVP contains a bit mask.

Vendor ID
10415

VSA Type
1442

AVP Type
UINT32

AVP Flag
M

Packet-Data-Flow-Info

This AVP is unique within the context of an IP-CAN session for the IP flow(s) given within the same Packet-Data-Flow-Info AVP.

Vendor ID
24757

VSA Type
405

AVP Type
GROUPED

Supported group value(s):

[PDFID]

[PRECEDENCE]

[FLOW_DESCRIPTION]

[WIMAX_QOS_INFORMATION]

AVP Flag
M

Packet-Filter-Content

This AVP contains the content of the packet filter as requested by the UE and required by the PCRF to create the PCC rules.

Vendor ID
10415

VSA Type
1059

AVP Type
IPFILTERRULE

AVP Flag
M

Packet-Filter-Identifier

This AVP indicates identity of the packet filter. The packet filter identifier is assigned by the PCRF and within the scope of the PCRF is unique per UE.

Vendor ID
10415

VSA Type
1060

AVP Type
OCTETSTRING

AVP Flag
M

Packet-Filter-Information

This AVP contains the information from a single packet filter sent from the PCEF to the PCRF.

Vendor ID
10415

VSA Type
1061

AVP Type
GROUPED

Supported group value(s):

[PACKET_FILTER_IDENTIFIER]

[PRECEDENCE]

[PACKET_FILTER_CONTENT]

[TOS_TRAFFIC_CLASS]

[SECURITY_PARAMETER_INDEX]

[FLOW_LABEL]

AVP Flag
M

Packet-Filter-Operation

This AVP indicates a UE initiated resource operation that causes a request for PCC rules.

Vendor ID
10415

VSA Type
1062

AVP Type
ENUM

Supported enumerated value(s):

0 DELETION

1 ADDITION

2 MODIFICATION

AVP Flag
M

Packet-Interval

This AVP indicates the packetization time in millisecond which should be used to calculate the polling or grant interval.

Vendor ID
24757

VSA Type
414

AVP Type
UINT32

AVP Flag
M

Packet-Size

This AVP indicates the length in bytes of the IP Packet including the IP-header in case of IP-flows where packets have a fixed size.

Vendor ID
24757

VSA Type
415

AVP Type
UINT32

AVP Flag

M

Paging-Group-Id

Paging-Group-Id

Vendor ID
0

VSA Type
10001

AVP Type
UINT32

AVP Flag
M

Path

This AVP contains a comma separated list of SIP proxies in the Path header.

Vendor ID
10415

VSA Type
640

AVP Type
OCTETSTRING

AVP Flag
N/A

Physical-Access-Id

This AVP contains the identity of the physical access where the user equipment is connected.

Vendor ID
0

VSA Type
313

AVP Type
UTF8STRING

AVP Flag
M

Port-Limit

Sets the maximum number of ports the NAS provides to the user.

Vendor ID
0

VSA Type
62

AVP Type
UINT32

AVP Flag
M

Port-Number

Port-Number

Vendor ID
13091

VSA Type
455

AVP Type
UINT32

AVP Flag
N/A

Pre-emption-Capability

This AVP indicates whether a service data flow can get resources that were already assigned to another service data flow with a lower priority level.

Vendor ID
10415

VSA Type
1047

AVP Type
ENUM

Supported enumerated value(s):

0 PRE-EMPTION_CAPABILITY_ENABLED

1 PRE-EMPTION_CAPABILITY_DISABLED

AVP Flag
M

Pre-emption-Vulnerability

This AVP indicates whether a service data flow can loose the resources assigned to it in order to admit a service data flow with higher priority level.

Vendor ID

10415

VSA Type
1048

AVP Type
ENUM

Supported enumerated value(s):

0 PRE-EMPTION_VULNERABILITY_ENABLED

1 PRE-EMPTION_VULNERABILITY_DISABLED

AVP Flag
M

Precedence

Defines the precedence of a charging rule in case of overlapping charging rules.

Vendor ID
10415

VSA Type
1010

AVP Type
UINT32

AVP Flag
M

Primary-Charging-Collection-Function-Name

Defines the address of the primary offline charging system for the bearer.

Vendor ID
10415

VSA Type
621

AVP Type
DIAMURI

AVP Flag
M

Primary-Event-Charging-Function-Name

This AVP specifies the address or name of the primary online charging system server for the bearer.

Vendor ID
10415

VSA Type
619

AVP Type
DIAMURI

AVP Flag
M

Priority-Level

This AVP is used to decide whether a bearer establishment or modification request can be accepted or needs to be rejected in case of resource limitations.

Vendor ID
10415

VSA Type
1046

AVP Type
UINT32

AVP Flag
M

Product-Name

This AVP contains the vendor assigned name for the product.

Vendor ID
0

VSA Type
269

AVP Type
UTF8STRING

AVP Flag
N/A

Proxy-Host

This AVP contains the identity of the host that added the Proxy-Info AVP.

Vendor ID
0

VSA Type
280

AVP Type
DIAMIDENT

AVP Flag
M

Proxy-Info

The Proxy-Info AVP allows stateless agents to add local state to a Diameter request.

Vendor ID
0

VSA Type
284

AVP Type
GROUPED

Supported group value(s):

[PROXY_HOST]

[PROXY_STATE]

AVP Flag
M

Proxy-State

The Proxy-State AVP contains state local information, and MUST be treated as opaque data.

Vendor ID
0

VSA Type
33

AVP Type
OCTETSTRING

AVP Flag
M

Public-Identity

This AVP contains the public identity of a user in the IMS.

Vendor ID
10415

VSA Type
601

AVP Type
UTF8STRING

AVP Flag
M

QoS-Capability

QoS-Capability

Vendor ID
0

VSA Type
6063

AVP Type
GROUPED

Supported group value(s):

[QOS_PROFILE_TEMPLATE]

[VENDOR_SPECIFIC_QOS_PROFILE_TEMPLATE]

AVP Flag
M

QoS-Class

This AVP contains the authorized traffic class for the PDP context.

Vendor ID
10415

VSA Type
1017

AVP Type
ENUM

Supported enumerated value(s):

0 Traffic_Class_A

1 Traffic_Class_B

2 Traffic_Class_C

3 Traffic_Class_D

4 Traffic_Class_E

5 Traffic_Class_F

AVP Flag
M

QoS-Class-Identifier

Identifies a set of IP-CAN specific QoS parameters that define the authorized QoS.

Vendor ID
10415

VSA Type
1028

AVP Type
ENUM

Supported enumerated value(s):

1 TRAFFIC_CLASS_A

2 TRAFFIC_CLASS_B

3 TRAFFIC_CLASS_C

4 TRAFFIC_CLASS_D

5 TRAFFIC_CLASS_E

6 TRAFFIC_CLASS_F

7 TRAFFIC_CLASS_G

8 TRAFFIC_CLASS_H

9 TRAFFIC_CLASS_I

AVP Flag
M

QoS-Information

This AVP contains the QoS information for an IP-CAN bearer or PCC rule.

Vendor ID
10415

VSA Type
1016

AVP Type
GROUPED

Supported group value(s):

[QOS_CLASS_IDENTIFIER]

[MAX_REQUESTED_BANDWIDTH_UL]

[MAX_REQUESTED_BANDWIDTH_DL]

[GUARANTEED_BITRATE_UL]

[GUARANTEED_BITRATE_DL]

[BEARER_IDENTIFIER]

[ALLOCATION_RETENTION_PRIORITY]

[APN_AGGREGATE_MAX_BITRATE_UL]

[APN_AGGREGATE_MAX_BITRATE_DL]

AVP Flag
M

QoS-Negotiation

This AVP indicates QoS negotiation capability. I.e., if the PCRF is allowed to negotiate the QoS.

Vendor ID
10415

VSA Type
1029

AVP Type
ENUM

Supported enumerated value(s):

0 NO_QoS_NEGOTIATION

1 QoS_NEGOTIATION_SUPPORTED

AVP Flag
M

QoS-Profile-Template

This AVP contains the list of supported Quality of Service profile templates.

Vendor ID
0

VSA Type
6067

AVP Type
UINT32

AVP Flag
M

QoS-Resource-Request

Resource requested by UE to PCRF.

Vendor ID
10415

VSA Type
6106

AVP Type
GROUPED

Supported group value(s):

[QOS_RESOURCE_IDENTIFIER]

[QOS_RESOURCE_OPERATION]

[TFT_PACKET_FILTER_INFORMATION]

[QOS_INFORMATION]

AVP Flag
M

QoS-Resources

This AVP provides the description of the Quality of Service resources for policing traffic flows.

Vendor ID
0

VSA Type
6065

AVP Type
GROUPED

Supported group value(s):

[EXTENDED_QOS_FILTER_RULE]

AVP Flag
M

QoS-Rule-Definition

This AVP contains the QoS rule for a service flow sent by PCRF to the BBERF.

Vendor ID
10415

VSA Type
1053

AVP Type
GROUPED

Supported group value(s):

[QOS_RULE_NAME]

[FLOW_DESCRIPTION]

[QOS_INFORMATION]

[PRECEDENCE]

AVP Flag
M

QoS-Rule-Install

This AVP contains the QoS rules that need to be installed.

Vendor ID
10415

VSA Type
1051

AVP Type
GROUPED

Supported group value(s):

[QOS_RULE_DEFINITION]

[TUNNEL_INFORMATION]

[RESOURCE_ALLOCATION_NOTIFICATION]

AVP Flag
M

QoS-Rule-Name

For QoS rules provided by the CRF it uniquely identifies a charging rule for a bearer.

Vendor ID
10415

VSA Type
1054

AVP Type
OCTETSTRING

AVP Flag
M

QoS-Rule-Remove

Used to remove QoS rules from a Gateway Control Session.

Vendor ID
10415

VSA Type
1052

AVP Type
GROUPED

Supported group value(s):

[QOS_RULE_NAME]

AVP Flag
M

QoS-Rule-Report

Report the status of QoS rules.

Vendor ID
10415

VSA Type

1055

AVP Type
GROUPED

Supported group value(s):

[QOS_RULE_NAME]

[PCC_RULE_STATUS]

[RULE_FAILURE_CODE]

AVP Flag
M

QoS-Subscribed

This AVP indicates the quality of service subscribed for a certain service.

Vendor ID
10415

VSA Type
1404

AVP Type
OCTETSTRING

AVP Flag
M

QoS-Upgrade

This AVP indicates whether SGSN supports upgrade of QoS by GGSN.

Vendor ID
10415

VSA Type
1030

AVP Type
ENUM

Supported enumerated value(s):

0 QoS_UPGRADE_NOT_SUPPORTED

1 QoS_UPGRADE_SUPPORTED

AVP Flag
M

RACS-Contact-Point

Identifies the RACS element to which resource reservation requests should be sent.

Vendor ID

0

VSA Type
351

AVP Type
DIAMIDENT

AVP Flag
M

RAI

This AVP contains the Routing Area Identity of the SGSN where the UE is registered.

Vendor ID
10415

VSA Type
909

AVP Type
UTF8STRING

AVP Flag
M

RAND

This AVP contains the RAND (EAP Authentication Vector).

Vendor ID
10415

VSA Type
1447

AVP Type
OCTETSTRING

AVP Flag
M

RAS-Id

This AVP contains the RAS identifier.

Vendor ID
0

VSA Type
10000

AVP Type
UINT32

AVP Flag

M

RAT-Frequency-Selection-Priority

This AVP contains the RAT frequency selection priority.

Vendor ID
10415

VSA Type
1440

AVP Type
UINT32

AVP Flag
M

RAT-Type

This AVP contains value of the Radio Access Technology which is currently serving the UE.

Vendor ID
10415

VSA Type
1032

AVP Type
ENUM

Supported enumerated value(s):

0 WLAN

1000 UTRAN

1001 GERAN

1002 GAN

1003 HSPA_EVOLUTION

1004 EUTRAN

2000 CDMA2000_1X

2001 HRPD

2002 UMB

AVP Flag
M

RR-Bandwidth

This AVP indicates the maximum required bandwidth in bits per second for RTCP receiver reports within the session component.

Vendor ID
10415

VSA Type
521

AVP Type
UINT32

AVP Flag
M

RS-Bandwidth

This AVP indicates the maximum required bandwidth in bits per second for RTCP sender reports within the session component.

Vendor ID
10415

VSA Type
522

AVP Type
UINT32

AVP Flag
M

Rating-Group

Identifier of a rating group for service. It contains the charging key (defined in 3GPP TS 23.125). Each quota allocated to a Diameter CC session has a unique Rating Group value as specified in RFC 4006.

Vendor ID
0

VSA Type
432

AVP Type
UINT32

AVP Flag
M

Re-Auth-Request-Type

Specifies the re-authorization request type and included in application-specific authorization answers to inform the client of the action expected upon expiration of the Authorization-Lifetime.

Vendor ID
0

VSA Type
285

AVP Type
ENUM

Supported enumerated value(s):

0 AUTHORIZE_ONLY

1 AUTHORIZE_AUTHENTICATE

AVP Flag
M

Re-Synchronization-Info

This AVP contains the concatenation of RAND and AUTS.

Vendor ID
10415

VSA Type
6014

AVP Type
UINT32

AVP Flag
M

Reason-Code

This AVP contains the reason for the network initiated de-registration.

Vendor ID
10415

VSA Type
616

AVP Type
ENUM

Supported enumerated value(s):

0 PERMANENT_TERMINATION

1 NEW_SERVER_ASSIGNED

2 SERVER_CHANGE

3 REMOVE_S-CSCF

AVP Flag
M

Reason-Info

This AVP contains textual information to inform the user about the reason for a de-registration.

Vendor ID

10415

VSA Type
617

AVP Type
UTF8STRING

AVP Flag
M

Record-Route

This AVP contains a comma separated list of Record Route header(s).

Vendor ID
10415

VSA Type
646

AVP Type
OCTETSTRING

AVP Flag
N/A

Redirect-Address-Type

This AVP contains the address type of the address given in the Redirect-Server-Address AVP.

Vendor ID
0

VSA Type
433

AVP Type
ENUM

Supported enumerated value(s):

0 IPv4-Address

1 IPv6-Address

2 URL

3 SIP-URI

AVP Flag
M

Redirect-Host

This AVP contains the alternate routing details to which the request need to be redirected to.

Vendor ID

0

VSA Type
292

AVP Type
OCTETSTRING

AVP Flag
M

Redirect-Host-Usage

This AVP contains information on how the routing entry resulting from the Redirect-Host is to be used.

Vendor ID
0

VSA Type
261

AVP Type
ENUM

Supported enumerated value(s):

0 DONT_CACHE

1 ALL_SESSION

2 ALL_REALM

3 REALM_AND_APPLICATION

4 ALL_APPLICATION

5 ALL_HOST

6 ALL_USER

AVP Flag
M

Redirect-Max-Cache-Time

This AVP indicates the maximum duration in seconds the peer and route table entries, created as a result of the Redirect-Host, will be cached.

Vendor ID
0

VSA Type
262

AVP Type
UINT32

AVP Flag
M

Redirect-Server

This AVP contains the address information of the redirect server (for example,, HTTP redirect server, SIP Server) with which the end user is to be connected when redirected as account cannot cover the service cost.

Vendor ID
0

VSA Type
434

AVP Type
GROUPED

Supported group value(s):

[REDIRECT_ADDRESS_TYPE]

[REDIRECT_SERVER_ADDRESS]

AVP Flag
M

Redirect-Server-Address

This AVP contains address of the redirect server.

Vendor ID
0

VSA Type
435

AVP Type
UTF8STRING

AVP Flag
M

Regional-Subscription-Zone-Code

Regional-Subscription-Zone-Code. Up to 10 zone codes are used to define the tracking areas into which the subscriber is allowed or not allowed to roam.

Vendor ID
10415

VSA Type
1446

AVP Type
OCTETSTRING

AVP Flag
M

Reply-Message

This AVP contains text that may be displayed to the user.

Vendor ID
0

VSA Type
18

AVP Type
UTF8STRING

AVP Flag
M

Reporting-Level

Defines on what level the TPF reports the usage for the related charging rule.

Vendor ID
10415

VSA Type
1011

AVP Type
ENUM

Supported enumerated value(s):

0 SERVICE_IDENTIFIER_LEVEL

1 RATING_GROUP_LEVEL

AVP Flag
M

Requested-Action

The action requested when the CC_Request_Type is EVENT_REQUEST.

Vendor ID
0

VSA Type
436

AVP Type
ENUM

Supported enumerated value(s):

0 DIRECT_DEBITING

1 REFUND_ACCOUNT

2 CHECK_BALANCE

3 PRICE_ENQUIRY

AVP Flag
M

Requested-Domain

This AVP indicates the access domain for which certain data are requested.

Vendor ID
0

VSA Type
706

AVP Type
ENUM

Supported enumerated value(s): none

AVP Flag
M

Requested-EUTRAN-Authentication-Info

This AVP contains the EU Tran authentication information.

Vendor ID
10415

VSA Type
6010

AVP Type
GROUPED

Supported group value(s):

[NUMBER_OF_REQUESTED_VECTORS]

[IMMEDIATE_RESPONSE_PREFERRED]

[RE_SYNCHRONIZATION_INFO]

AVP Flag
M

Requested-GERAN-Authentication-Info

This AVP contains GE RAN authentication information.

Vendor ID
10415

VSA Type
6012

AVP Type
GROUPED

Supported group value(s):

[NUMBER_OF_REQUESTED_VECTORS]

[IMMEDIATE_RESPONSE_PREFERRED]

[RE_SYNCHRONIZATION_INFO]

AVP Flag
M

Requested-Information

This AVP provides the list of items requested by the AF.

Vendor ID
13019

VSA Type
353

AVP Type
ENUM

Supported enumerated value(s):

0 NASS-USER-ID

1 LOCATION-INFORMATION

2 RACS-CONTACT-POINT

3 ACCESS-NETWORK-TYPE

4 TERMINAL-TYPE

5 LOGICAL-ACCESS-ID

6 PHYSICAL-ACCESS-ID

7 ACCESS-NETWORK-TYPE-RESERVED

8 INITIAL-GATE-SETTING-RESERVED

9 QOS-PROFILE-RESERVED

10 IP-CONNECTIVITY-STATUS-RESERVED

AVP Flag
M

Requested-Party-Address

In IMS it holds the address (SIP URI or TEL URI) of the party (Public User ID or Public Service ID) to whom the SIP transaction was originally posted.

Vendor ID
10415

VSA Type
1251

AVP Type

UTF8STRING

AVP Flag
M

Requested-QoS

It is used within the Flow-Info AVP to indicate the QoS requested by the UE for a particular IP flow in the high rate packet data radio access network.

Vendor ID
5535

VSA Type
1010

AVP Type
GROUPED

Supported group value(s):

[QOS_CLASS]

[MIN_BANDWIDTH_UL]

[MIN_BANDWIDTH_DL]

AVP Flag
M

Requested-Service-Unit

Amount of requested units specified by the Diameter credit-control client.

Vendor ID
0

VSA Type
437

AVP Type
GROUPED

Supported group value(s):

[TARIFF_TIME_CHANGE]

[TARIFF_CHANGE_USAGE]

[CC_TIME]

[CC_MONEY]

[CC_TOTAL_OCTETS]

[CC_INPUT_OCTETS]

[CC_OUTPUT_OCTETS]

[CC_SERVICE_SPECIFIC_UNITS]

AVP Flag

M

Requested-UTRAN-Authentication-Info

This AVP contains the UTRAN authentication information.

Vendor ID
10415

VSA Type
6011

AVP Type
GROUPED

Supported group value(s):

[NUMBER_OF_REQUESTED_VECTORS]

[IMMEDIATE_RESPONSE_PREFERRED]

[RE_SYNCHRONIZATION_INFO]

AVP Flag
M

Requested-UTRAN-GERAN-Authentication-Info

This AVP contains the information related to the authentication requests for UTRAN or GERAN.

Vendor ID
10415

VSA Type
1409

AVP Type
GROUPED

Supported group value(s):

[NUMBER_OF_REQUESTED_VECTORS]

[IMMEDIATE_RESPONSE_PREFERRED]

[RE_SYNCHRONIZATION_INFO]

AVP Flag
M

Requesting-Node-Type

Requesting-Node-Type

Vendor ID
10415

VSA Type
1455

AVP Type
ENUM

Supported enumerated value(s):

0 MME

1 SGSN

2 MME_SGSN

AVP Flag
M

Required-MBMS-Bearer-Capabilities

This AVP contains the minimum bearer capabilities the UE needs to support.

Vendor ID
10415

VSA Type
901

AVP Type
UTF8STRING

AVP Flag
M

Reservation-Class

This AVP contains an integer used as an index pointing to the traffic characteristic of the flow.

Vendor ID
13019

VSA Type
456

AVP Type
UINT32

AVP Flag
N/A

Reservation-Priority

Used by the PCRF to guarantee service for an application session of a higher relative priority.

Vendor ID
13019

VSA Type
458

AVP Type
ENUM

Supported enumerated value(s):

0 DEFAULT

1 PRIORITY-ONE

2 PRIORITY-TWO

3 PRIORITY-THREE

4 PRIORITY-FOUR

5 PRIORITY-FIVE

6 PRIORITY-SIX

7 PRIORITY-SEVEN

AVP Flag
N/A

Resource-Allocation-Notification

Defines whether the rules included within the Charging-Rule-Install/QoS-Rule-Install AVP need be notified.

Vendor ID
10415

VSA Type
1063

AVP Type
ENUM

Supported enumerated value(s):

0 ENABLE_NOTIFICATION

AVP Flag
M

Restoration-Info

This AVP contains the information related to a specific registration.

Vendor ID
10415

VSA Type
649

AVP Type
GROUPED

Supported group value(s):

[PATH]

[CONTACT]

[SUBSCRIPTION_INFO]

AVP Flag

N/A

Restriction-Filter-Rule

Provides filter rules for services that are to remain accessible even if there are no more service units granted.

Vendor ID
0

VSA Type
438

AVP Type
IPFILTERRULE

AVP Flag
M

Result-Code

This AVP indicates whether a particular request was completed successfully or whether an error occurred.

Vendor ID
0

VSA Type
268

AVP Type
ENUM

Supported enumerated value(s):

1001 DIAMETER_MULTI_ROUND_AUTH

2001 DIAMETER_SUCCESS

2002 DIAMETER_LIMITED_SUCCESS

3001 DIAMETER_COMMAND_UNSUPPORTED

3002 DIAMETER_UNABLE_TO_DELIVER

3003 DIAMETER_REALM_NOT_SERVED

3004 DIAMETER_TOO_BUSY

3005 DIAMETER_LOOP_DETECTED

3006 DIAMETER_REDIRECT_INDICATION

3007 DIAMETER_APPLICATION_UNSUPPORTED

3008 DIAMETER_INVALID_HDR_BITS

3009 DIAMETER_INVALID_AVP_BITS

3010 DIAMETER_UNKNOWN_PEER

4001 DIAMETER_AUTHENTICATION_REJECTED

4002 DIAMETER_OUT_OF_SPACE

4003 ELECTION_LOST

4010 DIAMETER_END_USER_SERVICE_DENIED

4011 DIAMETER_CREDIT_CONTROL_NOT_APPLICABLE

4012 DIAMETER_CREDIT_LIMIT_REACHED

4212 DIAMETER_BALANCE_IS_ZERO

5001 DIAMETER_AVP_UNSUPPORTED

5002 DIAMETER_UNKNOWN_SESSION_ID

5003 DIAMETER_AUTHORIZATION_REJECTED

5004 DIAMETER_INVALID_AVP_VALUE

5005 DIAMETER_MISSING_AVP

5006 DIAMETER_RESOURCES_EXCEEDED

5007 DIAMETER_CONTRADICTING_AVPS

5008 DIAMETER_AVP_NOT_ALLOWED

5009 DIAMETER_AVP_OCCURS_TOO_MANY_TIMES

5010 DIAMETER_NO_COMMON_APPLICATION

5011 DIAMETER_UNSUPPORTED_VERSION

5012 DIAMETER_UNABLE_TO_COMPLY

5013 DIAMETER_INVALID_BIT_IN_HEADER

5014 DIAMETER_INVALID_AVP_LENGTH

5015 DIAMETER_INVALID_MESSAGE_LENGTH

5016 DIAMETER_INVALID_AVP_BIT_COMBO

5017 DIAMETER_NO_COMMON_SECURITY

5030 DIAMETER_USER_UNKNOWN

5031 DIAMETER_RATING_FAILED

AVP Flag
M

Revalidation-Time

This AVP contains the value indicating the NTP time before which the PCEF will have to re-request PCC rules.

Vendor ID
10415

VSA Type
1042

AVP Type
TIME

AVP Flag
M

Roaming-Restricted-Due-To-Unsupported-Feature

This AVP indicates that roaming is restricted due to unsupported feature.

Vendor ID
10415

VSA Type
1457

AVP Type
ENUM

Supported enumerated value(s):

0 ROAMING_RESTRICTED_DUE_TO_UNSUPPORTED_FEATURE

AVP Flag
M

Role-Of-Node

This AVP specifies the role of the AS/CSCF.

Vendor ID
10415

VSA Type
829

AVP Type
ENUM

Supported enumerated value(s): none

AVP Flag
M

Route-Record

The value added to this AVP same as the one received in the Origin-Host of the Capabilities Exchange message.

Vendor ID
0

VSA Type
282

AVP Type
DIAMIDENT

AVP Flag
M

Routing-Policy

This AVP is used to describe a single IP flow.

Vendor ID
10415

VSA Type
312

AVP Type
IPFILTERRULE

AVP Flag
M

Rule-Activation-Time

This AVP contains the value indicating the NTP time at which the PCC rule has to be enforced.

Vendor ID
10415

VSA Type
1043

AVP Type
TIME

AVP Flag
M

Rule-Deactivation-Time

This AVP contains the value indicating the NTP time at which the PCEF has to stop enforcing the PCC rule.

Vendor ID
10415

VSA Type
1044

AVP Type
TIME

AVP Flag
M

Rule-Failure-Code

This AVP contains the rule failure code.

Vendor ID
10415

VSA Type

1031

AVP Type
ENUM

Supported enumerated value(s):

1 UNKNOWN_RULE_NAME

2 RATING_GROUP_ERROR

3 SERVICE_IDENTIFIER_ERROR

4 GW_PCEF_MALFUNCTION

5 RESOURCES_LIMITATION

6 MAX_NR_BEARERS_REACHED

7 UNKNOWN_BEARER_ID

8 MISSING_BEARER_ID

9 MISSING_FLOW_DESCRIPTION

10 RESOURCE_ALLOCATION_FAILURE

11 UNSUCCESSFUL_QOS_VALIDATION

AVP Flag
M

Rule-Reason-Code

This AVP contains the rule reason code.

Vendor ID
5535

VSA Type
814

AVP Type
ENUM

Supported enumerated value(s):

0 UNKNOWN_FLOW_IDENTIFIER

1 UNKNOWN_RULE_NAME

2 RATING_GROUP_ERROR

3 SERVICE_IDENTIFIER_ERROR

4 AGW_MALFUNCTION

5 RESOURCES_LIMITATION

AVP Flag
M

SCSCF-Restoration-Info

This AVP contains the information required for an S-CSCF to handle the requests for a user.

Vendor ID
10415

VSA Type
639

AVP Type
GROUPED

Supported group value(s):

[USER_NAME]

[RESTORATION_INFO]

[SIP_AUTHENTICATION_SCHEME]

AVP Flag
N/A

SDP-Answer-Timestamp

This AVP specifies the time in UTC format of the response to the SDP offer.

Vendor ID
0

VSA Type
1275

AVP Type
TIME

AVP Flag
M

SDP-Media-Component

This AVP contains the interface representing the SDP-Media-Component grouped AVP type.

Vendor ID
10415

VSA Type
843

AVP Type
GROUPED

Supported group value(s):

[SDP_MEDIA_NAME]

[SDP_MEDIA_DESCRIPTION]

[MEDIA_INITIATOR_FLAG]

[AUTHORISED_QOS]

[3GPP_CHARGING_ID]

AVP Flag
M

SDP-Media-Description

This AVP contains the content of an attribute-line" (i=, c=, b=, k=, a=) related to a media component. The attributes are specifying the media described in the SDP-Media-Name AVP.

Vendor ID
10415

VSA Type
845

AVP Type
UTF8STRING

AVP Flag
M

SDP-Media-Name

This AVP holds the content of a "m=" line in the SDP data.

Vendor ID
10415

VSA Type
844

AVP Type
UTF8STRING

AVP Flag
M

SDP-Offer-Timestamp

This AVP specifies the time in UTC format of the SDP offer.

Vendor ID
0

VSA Type
1274

AVP Type
TIME

AVP Flag
M

SDP-Session-Description

This AVP holds the content of an "attribute-line" (i=, c=, b=, k=, a=) related to a session.

Vendor ID
10415

VSA Type
842

AVP Type
UTF8STRING

AVP Flag
M

SDP-TimeStamps

This AVP specifies the time of the SDP offer and the SDP answer.

Vendor ID
0

VSA Type
1273

AVP Type
GROUPED

Supported group value(s):

[SDP_OFFER_TIMESTAMP]

[SDP_ANSWER_TIMESTAMP]

AVP Flag
M

SDP-Type

This AVP indicates whether the SDP media component is of type SDP offer or SDP answer.

Vendor ID
10415

VSA Type
2036

AVP Type
ENUM

Supported enumerated value(s):

0 SDP_OFFER

1 SDP_ANSWER

AVP Flag
M

SGSN-Address

This AVP contains the IP address of the SGSN that was used during a report.

Vendor ID
10415

VSA Type
1228

AVP Type
ADDRESS

AVP Flag
M

SGSN-Number

This AVP contains the ISDN number of the SGSN.

Vendor ID
10415

VSA Type
1489

AVP Type
OCTETSTRING

AVP Flag
M

SGW-Change

This AVP indicates that this is the first Accounting Request (ACR) due to S-GW change.

Vendor ID
10415

VSA Type
2065

AVP Type
ENUM

Supported enumerated value(s):

0 ACR_START_NOT_DUE_TO_SGW_CHANGE

1 ACR_START_DUE_TO_SGW_CHANGE

AVP Flag
M

SGW-Type

This AVP specifies the type of SGW of current flow.

Vendor ID
10415

VSA Type
7001

AVP Type
UINT32

AVP Flag
M

SIP-Auth-Data-Item

This AVP contains the authentication and/or authorization information for the Diameter client.

Vendor ID
10415

VSA Type
612

AVP Type
GROUPED

Supported group value(s):

[SIP_ITEM_NUMBER]

[SIP_AUTHENTICATION_SCHEME]

[SIP_AUTHENTICATE]

[SIP_DIGEST_AUTHENTICATE]

[SIP_AUTHORIZATION]

[SIP_AUTHENTICATION_CONTEXT]

[CONFIDENTIALITY_KEY]

[INTEGRITY_KEY]

[LINE_IDENTIFIER]

AVP Flag
M

SIP-Authenticate

This AVP contains specific parts of the data portion of the WWW-Authenticate or Proxy-Authenticate SIP headers that are to be present in a SIP response.

Vendor ID
10415

VSA Type

609

AVP Type
OCTETSTRING

AVP Flag
M

SIP-Authentication-Context

This AVP contains authentication-related information relevant for performing the authentication but that is not part of the SIP authentication headers.

Vendor ID
10415

VSA Type
611

AVP Type
OCTETSTRING

AVP Flag
M

SIP-Authentication-Scheme

This AVP contains the authentication scheme used in the authentication of SIP messages.

Vendor ID
10415

VSA Type
608

AVP Type
UTF8STRING

AVP Flag
M

SIP-Authorization

This AVP contains specific parts of the data portion of the Authorization or Proxy-Authorization SIP headers suitable for inclusion in a SIP request.

Vendor ID
10415

VSA Type
610

AVP Type
OCTETSTRING

AVP Flag
M

SIP-Digest-Authenticate

This AVP contains a reconstruction of either the SIP WWW-Authenticate or Proxy-Authentication header fields specified in IETF RFC 2617.

Vendor ID
10415

VSA Type
635

AVP Type
GROUPED

Supported group value(s):

[DIGEST_REALM]

[DIGEST_DOMAIN]

[DIGEST_ALGORITHM]

[DIGEST_QOP]

[DIGEST_HA1]

[DIGEST_AUTH_PARAM]

AVP Flag
M

SIP-Forking-Indication

This AVP indicates if several SIP dialogues are related to one Diameter session.

Vendor ID
10415

VSA Type
523

AVP Type
ENUM

Supported enumerated value(s):

0 SINGLE_DIALOGUE

1 SEVERAL_DIALOGUES

AVP Flag
M

SIP-Item-Number

This AVP contains the order number of the SIP-Auth-Data-Item AVP.

Vendor ID
10415

VSA Type

613

AVP Type
UINT32

AVP Flag
M

SIP-Message

This AVP hold the entire SIP message or messages received by the IAP.

Vendor ID
4491

VSA Type
229

AVP Type
OCTETSTRING

AVP Flag
M

SIP-Method

This AVP holds the name of the SIP Method (INVITE, UPDATE, etc.) causing an accounting request to be sent to the AAA.

Vendor ID
10415

VSA Type
824

AVP Type
UTF8STRING

AVP Flag
M

SIP-Number-Auth-Items

This AVP contains the number of authentication vectors asked/provided.

Vendor ID
10415

VSA Type
607

AVP Type
UINT32

AVP Flag
M

SIP-Request-Timestamp

This AVP holds the time in UTC format of the initial SIP request (for example, Invite).

Vendor ID
0

VSA Type
834

AVP Type
TIME

AVP Flag
M

SIP-Response-Timestamp

This AVP holds the time in UTC format of the response to the initial SIP request (for example, 200 OK).

Vendor ID
0

VSA Type
835

AVP Type
TIME

AVP Flag
M

SN-Absolute-Validity-Time

This AVP contains the validity time of the granted service units.

Vendor ID
8164

VSA Type
505

AVP Type
TIME

AVP Flag
N/A

SN-Bandwidth-Control

This AVP contains the value to control bandwidth usage.

Vendor ID
8164

VSA Type

512

AVP Type
ENUM

Supported enumerated value(s):

0 HIGH

1 LOW

AVP Flag
M

SN-Charging-Id

This AVP contains the charging identifier.

Vendor ID
8164

VSA Type
525

AVP Type
OCTETSTRING

AVP Flag
N/A

SN-Fast-Reauth-Username

This AVP is used for fast re-authentication of subscriber.

Vendor ID
8164

VSA Type
11010

AVP Type
OCTETSTRING

AVP Flag
M

SN-Firewall-Policy

This AVP contains the name of the Firewall policy to be enabled.

Vendor ID
8164

VSA Type
515

AVP Type
UTF8STRING

AVP Flag
N/A

SN-Monitoring-Key

It is an identifier to a usage monitoring control instance.

Vendor ID
8164

VSA Type
518

AVP Type
UINT32

AVP Flag
N/A

SN-Phase0-PSAPName

This AVP contains name of the County to be used for a subscriber.

Vendor ID
8164

VSA Type
523

AVP Type
UTF8STRING

AVP Flag
N/A

SN-Pseudonym-Username

This AVP is used for reauthentication of subscriber.

Vendor ID
8164

VSA Type
11011

AVP Type
OCTETSTRING

AVP Flag
M

SN-Service-Flow-Detection

This AVP defines whether the PCEF should notify the PCRF when it detects traffic matching rules included within Charging-Rule-Install AVP.

Vendor ID
8164

VSA Type
520

AVP Type
ENUM

Supported enumerated value(s):

0 ENABLE_DETECTION

AVP Flag
N/A

SN-Time-Quota-Threshold

This AVP contains a quota threshold for time in percent value. This is vendor specific AVP.

Vendor ID
8164

VSA Type
503

AVP Type
UINT32

AVP Flag
M

SN-Total-Used-Service-Unit

This is a vendor-specific AVP. This AVP contains the total consumed service units.

Vendor ID
8164

VSA Type
504

AVP Type
GROUPED

Supported group value(s):

[TARIFF_CHANGE_USAGE]

[CC_TIME]

[CC_TOTAL_OCTETS]

[CC_INPUT_OCTETS]

[CC_OUTPUT_OCTETS]

[CC_SERVICE_SPECIFIC_UNITS]

[3GPP_REPORTING_REASON]

AVP Flag
N/A

SN-Traffic-Policy

This AVP contains name of the Traffic Policing Policy.

Vendor ID
8164

VSA Type
514

AVP Type
UTF8STRING

AVP Flag
N/A

SN-Transparent-Data

This is a vendor-specific AVP. This AVP contains current PDP session information. This AVP provides information obtained from the RADIUS server during Access-Accept that can be put into vendor-specific extension towards the CGF and Prepaid server for billing purposes. This AVP is optional in the Access-Accept message.

Vendor ID
8164

VSA Type
513

AVP Type
OCTETSTRING

AVP Flag
N/A

SN-Unit-Quota-Threshold

This is a vendor-specific AVP. This AVP contains quota threshold for service specific units of quota in the CLCI-C in percent value.

Vendor ID
8164

VSA Type
502

AVP Type
UINT32

AVP Flag
M

SN-Usage-Monitoring

This AVP is used by PCRF to indicate if usage-monitoring and reporting is enabled or disabled.

Vendor ID
8164

VSA Type
521

AVP Type
ENUM

Supported enumerated value(s):

0 USAGE_MONITORING_DISABLED

1 USAGE_MONITORING_ENABLED

AVP Flag
N/A

SN-Usage-Monitoring-Control

This AVP is used for provisioning and reporting of usage information.

Vendor ID
8164

VSA Type
517

AVP Type
GROUPED

Supported group value(s):

[SN_MONITORING_KEY]

[SN_USAGE_MONITORING]

[SN_USAGE_VOLUME]

AVP Flag
N/A

SN-Usage-Volume

This AVP indicates total uplink and downlink usage volume in octets.

Vendor ID
8164

VSA Type
519

AVP Type
UINT64

AVP Flag
N/A

SN-Volume-Quota-Threshold

This AVP contains a volume threshold value in percentage value.

Vendor ID
8164

VSA Type
501

AVP Type
UINT32

AVP Flag
M

SRES

This AVP contains the SRES.

Vendor ID
10415

VSA Type
1454

AVP Type
OCTETSTRING

AVP Flag
M

SS-Code

This AVP contains the supplementary service codes that are to be deleted from the subscription.

Vendor ID
10415

VSA Type
1476

AVP Type
OCTETSTRING

AVP Flag
M

SS-Status

This AVP refers to the state information of individual supplementary services as defined in 3GPP TS 23.011.

Vendor ID
10415

VSA Type
1477

AVP Type
OCTETSTRING

AVP Flag
M

STN-SR

This AVP contains the session transfer number for SRVCC.

Vendor ID
10415

VSA Type
1433

AVP Type
UTF8STRING

AVP Flag
M

Secondary-Charging-Collection-Function-Name

Defines the address of the secondary offline charging system for the bearer.

Vendor ID
10415

VSA Type
622

AVP Type
DIAMURI

AVP Flag
M

Secondary-Event-Charging-Function-Name

Defines the address of the secondary online charging system for the bearer.

Vendor ID
10415

VSA Type

620

AVP Type
DIAMURI

AVP Flag
M

Sector-Id

The identifier of sector that MS exists.

Vendor ID
0

VSA Type
10002

AVP Type
UINT32

AVP Flag
M

Security-Parameter-Index

This AVP contains the security parameter index of the IPSec packet.

Vendor ID
10415

VSA Type
1056

AVP Type
OCTETSTRING

AVP Flag
M

Send-Data-Indication

This AVP indicates that sender requests user data in SNR.

Vendor ID
0

VSA Type
710

AVP Type
ENUM

Supported enumerated value(s): none

AVP Flag
M

Served-Party-IP-Address

This AVP holds the IP address of either the calling or called party, depending on whether the P-CSCF is in touch with the calling or the called party. This AVP is only provided by the P-CSCF and S-CSCF.

Vendor ID
10415

VSA Type
848

AVP Type
ADDRESS

AVP Flag
M

Server-Assignment-Type

This AVP contains the type of server update being performed in a Server-Assignment-Request operation.

Vendor ID
10415

VSA Type
614

AVP Type
ENUM

Supported enumerated value(s):

0 NO_ASSIGNMENT

1 REGISTRATION

2 RE_REGISTRATION

3 UNREGISTERED_USER

4 TIMEOUT_DEREGISTRATION

5 USER_DEREGISTRATION

6 TIMEOUT_DEREGISTRATION_STORE_SERVER_NAME

7 USER_DEREGISTRATION_STORE_SERVER_NAME

8 ADMINISTRATIVE_DEREGISTRATION

9 AUTHENTICATION_FAILURE

10 AUTHENTICATION_TIMEOUT

11 DEREGISTRATION_TOO_MUCH_DATA

AVP Flag
M

Server-Capabilities

This grouped AVP contains information/capabilities of an S-CSCF server.

Vendor ID
10415

VSA Type
603

AVP Type
GROUPED

Supported group value(s):

[MANDATORY_CAPABILITY]

[OPTIONAL_CAPABILITY]

[SERVER_NAME]

AVP Flag
M

Server-Name

This AVP contains a SIP-URL used to identify a SIP server.

Vendor ID
10415

VSA Type
602

AVP Type
UTF8STRING

AVP Flag
M

Service-Class

This AVP contains the service class requested by the AF.

Vendor ID
13019

VSA Type
459

AVP Type
UTF8STRING

AVP Flag
N/A

Service-Context-Id

This AVP contains a unique identifier of the Diameter Credit Control service specific document that applies to the request. This is an identifier allocated by the service provider/operator, by the service element manufacturer or by a standardization body and MUST uniquely identify a given Diameter Credit Control service specific document. For offline charging, this identifies the service specific document ('middle tier' TS) on which associated CDRs should based. The format of the Service-Context-Id is: "extensions".MNC.MCC."Release"."service-context" "@" "domain"

Vendor ID
0

VSA Type
461

AVP Type
UTF8STRING

AVP Flag
M

Service-Data-Container

This AVP enables the transmission of the container to be reported for Flow-based Charging. On encountering change on charging condition, this container identifies the volume count (separated for uplink and downlink), elapsed time or number of events, per service data flow identified per rating group or combination of the rating group and service id within an IP-CAN bearer.

Vendor ID
10415

VSA Type
2040

AVP Type
GROUPED

Supported group value(s):

[AF_CORRELATION_INFORMATION]

[CHARGING_RULE_BASE_NAME]

[ACCOUNTING_INPUT_OCTETS]

[ACCOUNTING_OUTPUT_OCTETS]

[ACCOUNTING_INPUT_PACKETS]

[ACCOUNTING_OUTPUT_PACKETS]

[LOCAL_SEQUENCE_NUMBER]

[QOS_INFORMATION]

[RATING_GROUP]

[CHANGE_TIME]

[SERVICE_IDENTIFIER]

[SERVICE_SPECIFIC_INFO]

[SGSN_ADDRESS]

[TIME_FIRST_USAGE]

[TIME_LAST_USAGE]

[TIME_USAGE]

[CHANGE_CONDITION]

[3GPP_USER_LOCATION_INFO]

[FLOW_DESCRIPTION]

[CHARGING_RULE_NAME]

[FIRST_PACKET_DIRECTION]

[3GPP2_BSID]

AVP Flag
M

Service-Identifier

Specifies the identity of the service or service component the service data flow in a charging rule relates to.

Vendor ID
0

VSA Type
439

AVP Type
UINT32

AVP Flag
M

Service-Indication

This AVP contains the Service Indication that identifies a service in AS.

Vendor ID
0

VSA Type
704

AVP Type
OCTETSTRING

AVP Flag
M

Service-Info-Status

This AVP indicates the status of the service information that the AF is providing to the PCRF.

Vendor ID
10415

VSA Type
527

AVP Type
ENUM

Supported enumerated value(s):

0 FINAL_SERVICE_INFORMATION

1 PRELIMINARY_SERVICE_INFORMATION

AVP Flag
M

Service-Information

The purpose of this AVP is to allow the transmission of additional 3GPP service-specific information elements.

Vendor ID
10415

VSA Type
873

AVP Type
GROUPED

Supported group value(s):

[IMS_INFORMATION]

AVP Flag
M

Service-Parameter-Info

Service-specific information used for rating.

Vendor ID
0

VSA Type
440

AVP Type
GROUPED

Supported group value(s): none

AVP Flag
M

Service-Parameter-Type

Service event specific parameter (for example, end-user location or service name.

Vendor ID

0

VSA Type
441

AVP Type
UINT32

AVP Flag
M

Service-Parameter-Value

Value of the service parameter type.

Vendor ID
0

VSA Type
442

AVP Type
OCTETSTRING

AVP Flag
M

Service-Selection

This AVP contains the name of the service or the external network with which the mobility service should be associated.

Vendor ID
0

VSA Type
493

AVP Type
OCTETSTRING

AVP Flag
M

Service-Specific-Data

This AVP holds service specific data if and as provided by an Application Server.

Vendor ID
0

VSA Type
1249

AVP Type
GROUPED

Supported group value(s):

[SERVICE_SPECIFIC_TYPE]

[SERVICE_SPECIFIC_VALUE]

AVP Flag
M

Service-Specific-Info

This AVP holds service specific data if and as provided by an Application Server or a PCEF only for pre-defined PCC rules.

Vendor ID
10415

VSA Type
1249

AVP Type
GROUPED

Supported group value(s):

[SERVICE_SPECIFIC_DATA]

[SERVICE_SPECIFIC_TYPE]

AVP Flag
M

Service-Specific-Type

This AVP holds the type of the Service-Specific-Data.

Vendor ID
0

VSA Type
1248

AVP Type
UINT32

AVP Flag
M

Service-Specific-Value

This AVP holds service specific value.

Vendor ID
0

VSA Type
863

AVP Type
UTF8STRING

AVP Flag
M

Service-Type

This AVP contains the type of service the user has requested or the type of service to be provided.

Vendor ID
0

VSA Type
6

AVP Type
ENUM

Supported enumerated value(s):

1 Login

2 Framed

3 Callback-Login

4 Callback-Framed

5 Outbound

6 Administrative

7 NAS-Prompt

8 Authenticate-Only

9 Callback-NAS-Prompt

10 Call-Check

11 Callback-Administrative

12 Voice

13 Fax

14 Modem-Relay

15 IAPP-Register_IEEE-802_11f

16 IAPP-AP-Check_IEEE-802_11f

17 Authorize-Only-RADDynAuth

AVP Flag
M

Service-URN

This AVP indicates that an AF session is used for emergency traffic. It contains values of the service URN including sub-services, as registered at IANA.

Vendor ID
10415

VSA Type
525

AVP Type
OCTETSTRING

AVP Flag
M

ServiceTypeIdentity

This AVP contains the LCS service type identity.

Vendor ID
10415

VSA Type
1484

AVP Type
UINT32

AVP Flag
M

Serving-Node-Type

This AVP contains type of the Serving Node.

Vendor ID
10415

VSA Type
2047

AVP Type
ENUM

Supported enumerated value(s):

0 SGSN

1 PMIPSGW

2 GTPSGW

3 ePDG

4 hSGW

5 MME

AVP Flag
M

Session-Bundle-Id

Used to identify the group of sessions to which session of the AA-Answer belongs.

Vendor ID
13019

VSA Type
400

AVP Type
UINT32

AVP Flag
M

Session-Id

Specifies the specific session with an identifier.

Vendor ID
0

VSA Type
263

AVP Type
UTF8STRING

AVP Flag
M

Session-Linking-Indicator

This AVP indicates whether the session linking between the Gateway Control Session and the Gx session must be deferred.

Vendor ID
10415

VSA Type
1064

AVP Type
ENUM

Supported enumerated value(s):

0 SESSION_LINKING_IMMEDIATE

1 SESSION_LINKING_DEFERRED

AVP Flag
M

Session-Priority

This AVP indicates to the HSS or accounting server the session's priority. PRIORITY-0 is the highest priority.

Vendor ID
10415

VSA Type
650

AVP Type
ENUM

Supported enumerated value(s):

0 PRIORITY-0

1 PRIORITY-1

2 PRIORITY-2

3 PRIORITY-3

4 PRIORITY-4

AVP Flag
N/A

Session-Release-Cause

This AVP contains the release cause of the IP-CAN session.

Vendor ID
10415

VSA Type
1045

AVP Type
ENUM

Supported enumerated value(s):

0 UNSPECIFIED_REASON

1 UE_SUBSCRIPTION_REASON

2 INSUFFICIENT_SERVER_RESOURCES

AVP Flag
M

Session-Request-Type

This AVP indicates the action that the PDG is asking to the 3GPP AAA server to perform.

Vendor ID
10415

VSA Type
311

AVP Type
ENUM

Supported enumerated value(s): none

AVP Flag
M

Session-Start-Indicator

This AVP contains the SFR Session Start Indication. Flags Primary PDP Context. Value is always 0xFF".

Vendor ID
8164

VSA Type
522

AVP Type
OCTETSTRING

AVP Flag
M

Session-Timeout

This AVP contains the maximum number of seconds of service to be provided to the user before termination of the session.

Vendor ID
0

VSA Type
27

AVP Type
UINT32

AVP Flag
M

Software-Version

This AVP contains the Software Version of the International Mobile Equipment Identity.

Vendor ID
10415

VSA Type
6004

AVP Type
UTF8STRING

AVP Flag
M

Specific-APN-Info

This AVP contains the APN which is not present in the subscription context but the UE is authorized to connect to and the identity of the registered PDN-GW.

Vendor ID

10415

VSA Type
1472

AVP Type
GROUPED

Supported group value(s):

[SERVICE_SELECTION]

[MIP6_AGENT_INFO]

AVP Flag
M

Specific-Action

Within an E-PDF initiated Re-Authorization Request; the Specific-Action AVP determines the type of the action.

Vendor ID
10415

VSA Type
513

AVP Type
ENUM

Supported enumerated value(s):

1 CHARGING_CORRELATION_EXCHANGE

2 INDICATION_OF_LOSS_OF_BEARER

3 INDICATION_OF_RECOVERY_OF_BEARER

4 INDICATION_OF_RELEASE_OF_BEARER

5 INDICATION_OF_ESTABLISHMENT_OF_BEARER

6 IP_CAN_CHANGE

AVP Flag
M

Starent-Subscriber-Permission

This AVP is used to control the Network Mobility (NEMO) permission on a per Enterprise/PDN connection basis.

Vendor ID
8164

VSA Type
20

AVP Type
ENUM

Supported enumerated value(s):

0 None

1 Simple-IP

2 Mobile-IP

3 Simple-IP-Mobile-IP

4 HA-Mobile-IP

5 Simple-IP-HA-Mobile-IP

6 Mobile-IP-HA-Mobile-IP

7 SIP-MIP-HA-MIP

8 GGSN-PDP-TYPE-IP

16 GGSN-PDP-TYPE-PPP

32 Network-Mobility

38 FA-HA-NEMO

63 All

AVP Flag
M

Start-Time

This AVP contains a time-stamp (in UTC format) which represents the start of a service flow at the BM.

Vendor ID
10415

VSA Type
2041

AVP Type
TIME

AVP Flag
M

State

Sent by Diameter server to the NAS in an AA Response command that contains either a Result-Code of "DIAMETER_MULTI_ROUND_AUTH" or a "Termination-Action" AVP with the value of "AA-REQUEST".

Vendor ID
0

VSA Type
24

AVP Type
OCTETSTRING

AVP Flag
M

Stop-Time

This AVP contains a time-stamp (in UTC format) which represents the termination of a service flow at the BM. This AVP is only included in an accounting request with Accounting-Record-Type indicating STOP_RECORD.

Vendor ID
10415

VSA Type
2042

AVP Type
TIME

AVP Flag
M

Subs-Req-Type

This AVP indicates the type of subscription to notifications request in SNR.Subs-Req-Type.

Vendor ID
0

VSA Type
705

AVP Type
ENUM

Supported enumerated value(s): none

AVP Flag
M

Subscriber-Priority

Subscriber-Priority

Vendor ID
5535

VSA Type
6078

AVP Type
GROUPED

Supported group value(s):

[3GPP2_MAX_AUTH_AGGR_BW_BET]

[3GPP2_MAX_PER_FLOW_PRIORITY_USER]

[3GPP2_INTER_USER_PRIORITY]

[3GPP2_ALLOWED_PERSISTENT_TFTS]

[3GPP2_MAX_SVC_INST_LINK_FLOW_TOTAL]

[3GPP2_SERVICE_OPTION_PROFILE]

AVP Flag
M

Subscriber-Status

This AVP indicates if the service is barred or granted.

Vendor ID
10415

VSA Type
1424

AVP Type
ENUM

Supported enumerated value(s):

0 SERVICEGRANTED

1 OPERATORDETERMINEDBARRING

AVP Flag
M

Subscription-Data

This AVP contains the information related to the user profile relevant for EPS and GERAN/UTRAN.

Vendor ID
10415

VSA Type
6001

AVP Type
GROUPED

Supported group value(s):

[SUBSCRIBER_STATUS]

[MSISDN]

[STN_SR]

[NETWORK_ACCESS_MODE]

[OPERATOR_DETERMINED_BARRING]

[HPLMN_ODB]

[REGIONAL_SUBSCRIPTION_ZONE_CODE]

[ACCESS_RESTRICTION_DATA]

[APN_OI_REPLACEMENT]

[3GPP_CHARGING_CHARACTERISTICS]

[AMBR]

[APN_CONFIGURATION_PROFILE]

[RAT_FREQUENCY_SELECTION_PRIORITY]

AVP Flag
M

Subscription-Id

Identifier for the end-users subscription (IMSI, MSISDN, etc.).

Vendor ID
0

VSA Type
443

AVP Type
GROUPED

Supported group value(s):

[SUBSCRIPTION_ID_TYPE]

[SUBSCRIPTION_ID_DATA]

AVP Flag
M

Subscription-Id-Data

Used to identify the end user information.

Vendor ID
0

VSA Type
444

AVP Type
UTF8STRING

AVP Flag
M

Subscription-Id-Type

Determines the type of identifier carried by the Subscription-Id AVP.

Vendor ID
0

VSA Type
450

AVP Type
ENUM

Supported enumerated value(s):

0 END_USER_E164

1 END_USER_IMSI

2 END_USER_SIP_URI

3 END_USER_NAI

4 END_USER_PRIVATE

AVP Flag
M

Subscription-Info

This AVP contains the UE's subscription information.

Vendor ID
10415

VSA Type
642

AVP Type
GROUPED

Supported group value(s):

[CALL_ID_SIP_HEADER]

[FROM_SIP_HEADER]

[TO_SIP_HEADER]

[RECORD_ROUTE]

[CONTACT]

AVP Flag
N/A

Supported-Applications

This AVP contains supported application identifiers of a Diameter node.

Vendor ID
10415

VSA Type
631

AVP Type
GROUPED

Supported group value(s):

[AUTH_APPLICATION_ID]

[ACCT_APPLICATION_ID]

[VENDOR_SPECIFIC_APPLICATION_ID]

AVP Flag
M

Supported-Features

This AVP informs the destination host about the features supported by the origin host.

Vendor ID
10415

VSA Type
628

AVP Type
GROUPED

Supported group value(s):

[VENDOR_ID]

[FEATURE_LIST_ID]

[FEATURE_LIST]

AVP Flag
M

Supported-Features-Resp

This AVP contains a list of supported features of the origin host (Answer message without M bit set).

Vendor ID
10415

VSA Type
628

AVP Type
GROUPED

Supported group value(s):

[VENDOR_ID_RESP]

[FEATURE_LIST_ID_RESP]

[FEATURE_LIST_RESP]

AVP Flag
N/A

Supported-RAT-Type

This AVP contains one of E-UTRAN, UTRAN, GERAN, GAN, I-HSPA-EVOLUTION.

Vendor ID
10415

VSA Type

6005

AVP Type
UTF8STRING

AVP Flag
M

Supported-Vendor-Id

Specifies the vendor ID other than the device vendor.

Vendor ID
0

VSA Type
265

AVP Type
UINT32

AVP Flag
M

TFT-Filter

This AVP contains the flow filter for one Traffic Flow Template (TFT) packet filter.

Vendor ID
10415

VSA Type
1012

AVP Type
IPFILTERRULE

AVP Flag
M

TFT-Packet-Filter-Information

This AVP contains the information from a single TFT packet filter including the evaluation precedence, the filter and the Type-of-Service/Traffic Class sent from the TPF to the CRF.

Vendor ID
10415

VSA Type
1013

AVP Type
GROUPED

Supported group value(s):

[PRECEDENCE]

[TFT_FILTER]

[TOS_TRAFFIC_CLASS]

AVP Flag
M

TMGI

This AVP contains the Temporary Mobile Group Identity (TMGI) allocated to a particular MBMS bearer service.

Vendor ID
10415

VSA Type
900

AVP Type
OCTETSTRING

AVP Flag
M

TS-Code

This AVP contains the code identifying a single teleservice, a group of teleservices, or all teleservices.

Vendor ID
10415

VSA Type
1487

AVP Type
OCTETSTRING

AVP Flag
M

Tap-Id

This AVP holds the Tap ID as provisioned by the DF.

Vendor ID
4491

VSA Type
231

AVP Type
UTF8STRING

AVP Flag
M

Tariff-Change-Usage

Defines whether units are used before or after a tariff change.

Vendor ID
0

VSA Type
452

AVP Type
ENUM

Supported enumerated value(s):

0 UNIT_BEFORE_TARIFF_CHANGE

1 UNIT_AFTER_TARIFF_CHANGE

2 UNIT_INDETERMINATE

AVP Flag
M

Tariff-Time-Change

It is sent from the server to the client and includes the time in seconds since January 1, 1900, 00:00 UTC, when the tariff of the service is changed.

Vendor ID
0

VSA Type
451

AVP Type
TIME

AVP Flag
M

Teleservice-List

This AVP contains the service codes for the short message related teleservice for a subscriber.

Vendor ID
10415

VSA Type
1486

AVP Type
GROUPED

Supported group value(s):

[TS_CODE]

AVP Flag
M

Terminal-Information

This AVP contains the information about the user's mobile equipment.

Vendor ID
10415

VSA Type
6002

AVP Type
GROUPED

Supported group value(s):

[ESN]

[MEID]

[IMEI]

[SOFTWARE_VERSION]

AVP Flag
M

Terminal-Type

This AVP contains a value of the User Class DHCP Option.

Vendor ID
13019

VSA Type
352

AVP Type
OCTETSTRING

AVP Flag
M

Terminating-IOI

This AVP holds the Inter Operator Identifier for the originating network as generated by the S-CSCF in the home network of the terminating end user.

Vendor ID
0

VSA Type
840

AVP Type
UTF8STRING

AVP Flag
M

Termination-Cause

This AVP indicates the reason why a session was terminated on the access device.

Vendor ID
0

VSA Type
295

AVP Type
ENUM

Supported enumerated value(s):

1 DIAMETER_LOGOUT

2 DIAMETER_SERVICE_NOT_PROVIDED

3 DIAMETER_BAD_ANSWER

4 DIAMETER_ADMINISTRATIVE

5 DIAMETER_LINK_BROKEN

6 DIAMETER_AUTH_EXPIRED

7 DIAMETER_USER_MOVED

8 DIAMETER_SESSION_TIMEOUT

AVP Flag
M

Time-First-Usage

This AVP specifies the time in UTC format for the first IP packet to be transmitted and mapped to the current service data container.

Vendor ID
10415

VSA Type
2043

AVP Type
TIME

AVP Flag
M

Time-Last-Usage

This AVP specifies the time in UTC format for the last IP packet to be transmitted and mapped to the current service data container.

Vendor ID
10415

VSA Type

2044

AVP Type
TIME

AVP Flag
M

Time-Stamps

This grouped AVP holds the time of the initial SIP request and the time of the response to the initial SIP Request.

Vendor ID
0

VSA Type
833

AVP Type
GROUPED

Supported group value(s):

[SIP_REQUEST_TIMESTAMP]

[SIP_RESPONSE_TIMESTAMP]

AVP Flag
M

Time-Usage

This AVP indicates the length of the current flow in seconds.

Vendor ID
10415

VSA Type
2045

AVP Type
UINT32

AVP Flag
M

To-SIP-Header

This AVP contains the information in the To header.

Vendor ID
10415

VSA Type
645

AVP Type
OCTETSTRING

AVP Flag
N/A

ToS-Traffic-Class

This AVP contains the Type-of-Service/Traffic-Class of a TFT packet filter.

Vendor ID
10415

VSA Type
1014

AVP Type
OCTETSTRING

AVP Flag
M

Trace-Collection-Entity

This AVP contains the IPv4 or IPv6 address of the Trace Collection Entity.

Vendor ID
10415

VSA Type
1452

AVP Type
ADDRESS

AVP Flag
M

Trace-Data

This AVP contains the information related to trace function.

Vendor ID
10415

VSA Type
1458

AVP Type
GROUPED

Supported group value(s):

[TRACE_REFERENCE]

[TRACE_DEPTH_LIST]

[TRACE_NE_TYPE_LIST]

[TRACE_INTERFACE_LIST]

[TRACE_EVENT_LIST]

[OMC_ID]

[TRACE_COLLECTION_ENTITY]

AVP Flag
M

Trace-Depth

This AVP indicates whether entire signaling messages or just some IEs need to be recorded.

Vendor ID
10415

VSA Type
1462

AVP Type
ENUM

Supported enumerated value(s):

0 Minimum

1 Medium

2 Maximum

3 MinimumWithoutVendorSpecificExtension

4 MediumWithoutVendorSpecificExtension

5 MaximumWithoutVendorSpecificExtension

AVP Flag
M

Trace-Depth-List

This AVP contains the list of Trade Depths per NE Type.

Vendor ID
10415

VSA Type
1460

AVP Type
GROUPED

Supported group value(s):

[TRACE_DEPTH_PER_NE_TYPE]

AVP Flag
M

Trace-Depth-Per-NE-Type

This AVP contains the Network-Element-Type that is involved in a session trace, and the corresponding depth of trace for the specified Network-Element-Type.

Vendor ID
10415

VSA Type
1451

AVP Type
GROUPED

Supported group value(s):

[NETWORK_ELEMENT_TYPE]

[TRACE_DEPTH]

AVP Flag
M

Trace-Event-List

Trace-Event-List

Vendor ID
10415

VSA Type
1465

AVP Type
OCTETSTRING

AVP Flag
M

Trace-Interface-List

Trace-Interface-List

Vendor ID
10415

VSA Type
1464

AVP Type
OCTETSTRING

AVP Flag
M

Trace-NE-Type-List

This AVP contains the concatenation of MCC MNC.

Vendor ID
10415

VSA Type
1463

AVP Type
OCTETSTRING

AVP Flag
M

Trace-Reference

This AVP contains the concatenation of MCC MNC.

Vendor ID
10415

VSA Type
1459

AVP Type
OCTETSTRING

AVP Flag
M

Traffic-Data-Volumes

This AVP is used to allow the transmission of the IPCAN bearer container on encountering change on charging condition for this IP-CAN bearer.The Rf interface supports AMBR reporting for non-guaranteed bit rate (non-GBR) bearers in a TDV AVP group.

Vendor ID
10415

VSA Type
2046

AVP Type
GROUPED

Supported group value(s):

[QOS_INFORMATION]

[ACCOUNTING_INPUT_OCTETS]

[ACCOUNTING_INPUT_PACKETS]

[ACCOUNTING_OUTPUT_OCTETS]

[ACCOUNTING_OUTPUT_PACKETS]

[CHANGE_CONDITION]

[CHANGE_TIME]

[3GPP_USER_LOCATION_INFO]

AVP Flag
M

Transport-Class

This AVP contains an integer used as an index pointing to a class of transport services to be applied.

Vendor ID
13019

VSA Type
311

AVP Type
UINT32

AVP Flag
N/A

Trunk-Group-ID

This grouped AVP identifies the incoming and outgoing PSTN legs.

Vendor ID
10415

VSA Type
851

AVP Type
GROUPED

Supported group value(s):

[INCOMING_TRUNK_GROUP_ID]

[OUTGOING_TRUNK_GROUP_ID]

AVP Flag
M

Tunnel-Assignment-Id

Used to indicate to the tunnel initiator the particular tunnel to which a session is to be assigned.

Vendor ID
0

VSA Type
82

AVP Type
OCTETSTRING

AVP Flag
M

Tunnel-Client-Auth-Id

Specifies the name used by the tunnel initiator during the authentication phase of tunnel establishment.

Vendor ID
0

VSA Type
90

AVP Type
UTF8STRING

AVP Flag
M

Tunnel-Client-Endpoint

This AVP contains the address of the initiator end of the tunnel.

Vendor ID
0

VSA Type
66

AVP Type
UTF8STRING

AVP Flag
M

Tunnel-Header-Filter

Tunnel-Header-Filter

Vendor ID
10415

VSA Type
1036

AVP Type
IPFILTERRULE

AVP Flag
M

Tunnel-Header-Length

This AVP indicates the length of the tunnel header in octets.

Vendor ID
10415

VSA Type
1037

AVP Type
UINT32

AVP Flag
M

Tunnel-Information

This AVP contains the tunnel (outer) header information from a single IP flow.

Vendor ID
10415

VSA Type
1038

AVP Type
GROUPED

Supported group value(s):

[TUNNEL_HEADER_LENGTH]

[TUNNEL_HEADER_FILTER]

AVP Flag
M

Tunnel-Medium-Type

This AVP contains the transport medium to use when creating a tunnel for protocols (such as L2TP) that can operate over multiple transports.

Vendor ID
0

VSA Type
65

AVP Type
ENUM

Supported enumerated value(s):

1 IPv4_IPversion4

2 IPv6_IPversion6

3 NSAP

4 HDLC-8-bit_multidrop

5 BBN-1822

6 802-includes-all-802-media-plus-Ethernet-canonical_format

7 E163_POTS

8 E164_SMDS_Frame-Relay_ATM

9 F69_Telex

10 X121_X25_Frame-Relay

11 IPX

12 Appletalk

13 Decnet_IV

14 Banyan_Vines

15 E164-with-NSAP-format-subaddress

AVP Flag
M

Tunnel-Password

This AVP contains a password to be used to authenticate to a remote server.

Vendor ID
0

VSA Type
69

AVP Type
OCTETSTRING

AVP Flag
M

Tunnel-Preference

Used to identify the relative preference assigned to each tunnel when more than one set of tunneling AVPs is returned within separate Grouped-AVPs.

Vendor ID
0

VSA Type
83

AVP Type
UINT32

AVP Flag
M

Tunnel-Private-Group-Id

This AVP contains the group ID for a particular tunneled session.

Vendor ID

0

VSA Type
81

AVP Type
OCTETSTRING

AVP Flag
M

Tunnel-Server-Auth-Id

This AVP contains the name used by the tunnel terminator during the authentication phase of tunnel establishment.

Vendor ID
0

VSA Type
91

AVP Type
UTF8STRING

AVP Flag
M

Tunnel-Server-Endpoint

This AVP contains the address of the server end of the tunnel.

Vendor ID
0

VSA Type
67

AVP Type
UTF8STRING

AVP Flag
M

Tunnel-Type

This AVP contains the tunneling protocol(s) to be used (in the case of a tunnel initiator) or in use (in the case of a tunnel terminator).

Vendor ID
0

VSA Type
64

AVP Type
ENUM

Supported enumerated value(s):

1 Point-to-Point_Tunneling_Protocol-PPTP

2 Layer-Two-Forwarding_L2F

3 Layer-Two-Tunneling_Protocol-L2TP

4 Ascend-Tunnel-Management-Protocol-ATMP

5 Virtual-Tunneling-Protocol-VTP

6 IP-Authentication-Header-in-the-Tunnel-mode_AH

7 IP-in-IP_Encapsulation_IP-IP

8 Minimal_IP-in-IP_Encapsulation_MIN-IP-IP

9 IP_Encapsulating_Security_Payload_in_the_Tunnel-mode_ESP

10 Generic_Route_Encapsulation_GRE

11 Bay_Dial_Virtual_Services-DVS

12 IP-in-IP-Tunneling

13 Virtual-LANs-VLAN

AVP Flag

M

Tunneling

Used to describe a compulsory tunnel service.

Vendor ID

0

VSA Type

401

AVP Type

GROUPED

Supported group value(s):

[TUNNEL_TYPE]

[TUNNEL_MEDIUM_TYPE]

[TUNNEL_CLIENT_ENDPOINT]

[TUNNEL_SERVER_ENDPOINT]

[TUNNEL_PREFERENCE]

[TUNNEL_CLIENT_AUTH_ID]

[TUNNEL_SERVER_AUTH_ID]

[TUNNEL_ASSIGNMENT_ID]

[TUNNEL_PASSWORD]

[TUNNEL_PRIVATE_GROUP_ID]

AVP Flag

M

UAR-Flags

This AVP contains a bit mask, if the bit 0 is set, it indicates that the request corresponds to an IMS Emergency Registration.

Vendor ID
0

VSA Type
637

AVP Type
UINT32

AVP Flag
M

ULA-Flags

The ULR-Flags AVP is of type Unsigned32 and it contains a bit mask.

Vendor ID
10415

VSA Type
6007

AVP Type
UINT32

AVP Flag
M

ULR-Flags

The ULR-Flags AVP is of type Unsigned32 and it contains a bit mask.

Vendor ID
10415

VSA Type
6006

AVP Type
UINT32

AVP Flag
M

UMTS-Vector

This AVP contains Authentication Information for UMTS.

Vendor ID
10415

VSA Type
6018

AVP Type
GROUPED

Supported group value(s):

[ITEM_NUMBER]

[RAND]

[XRES]

[AUTN]

[CONFIDENTIALITY_KEY]

[INTEGRITY_KEY]

AVP Flag
M

UTRAN-Vector

This AVP contains Authentication Information for UTRAN.

Vendor ID
10415

VSA Type
1415

AVP Type
GROUPED

Supported group value(s):

[ITEM_NUMBER]

[RAND]

[XRES]

[AUTN]

[CONFIDENTIALITY_KEY]

[INTEGRITY_KEY]

AVP Flag
M

Unit-Value

This AVP contains cost estimate (type of money) of the service.

Vendor ID
0

VSA Type
445

AVP Type
GROUPED

Supported group value(s):

[VALUE_DIGITS]

[EXPONENT]

AVP Flag
M

Usage-Monitoring-Information

This AVP contains the usage monitoring control information.

Vendor ID
10415

VSA Type
1067

AVP Type
GROUPED

Supported group value(s):

[MONITORING_KEY]

[GRANTED_SERVICE_UNIT]

[USED_SERVICE_UNIT]

[USAGE_MONITORING_LEVEL]

[USAGE_MONITORING_REPORT]

[USAGE_MONITORING_SUPPORT]

AVP Flag
N/A

Usage-Monitoring-Level

This AVP is used by the PCRF to indicate whether the usage monitoring instance applies to the IP-CAN session or to one or more PCC rules.

Vendor ID
10415

VSA Type
1068

AVP Type
ENUM

Supported enumerated value(s):

0 SESSION_LEVEL

1 PCC_RULE_LEVEL

AVP Flag
N/A

Usage-Monitoring-Report

This AVP is used by the PCRF to indicate that accumulated usage is to be reported by the PCEF regardless of whether a usage threshold is reached for certain usage monitoring key.

Vendor ID
10415

VSA Type
1069

AVP Type
ENUM

Supported enumerated value(s):

0 USAGE_MONITORING_REPORT_REQUIRED

AVP Flag
N/A

Usage-Monitoring-Support

This AVP is used by the PCRF to indicate whether usage monitoring should be disabled for certain Monitoring Key.

Vendor ID
10415

VSA Type
1070

AVP Type
ENUM

Supported enumerated value(s):

0 USAGE_MONITORING_DISABLED

AVP Flag
N/A

Used-Service-Unit

The used service unit measured from the point when service is active.

Vendor ID
0

VSA Type
446

AVP Type
GROUPED

Supported group value(s):

[TARIFF_TIME_CHANGE]

[TARIFF_CHANGE_USAGE]

[CC_TIME]

[CC_MONEY]

[CC_TOTAL_OCTETS]

[CC_INPUT_OCTETS]

[CC_OUTPUT_OCTETS]

[CC_SERVICE_SPECIFIC_UNITS]

AVP Flag
M

User-Authorization-Type

This AVP contains the type of user authorization being performed in a User Authorization operation.

Vendor ID
10415

VSA Type
623

AVP Type
ENUM

Supported enumerated value(s):

0 REGISTRATION

1 DE_REGISTRATION

2 REGISTRATION_AND_CAPABILITIES

AVP Flag
M

User-Data

This AVP contains the user data requested in the PUR and SNR operations and the data to be modified in the UPR operations.

Vendor ID
0

VSA Type
702

AVP Type
OCTETSTRING

AVP Flag
M

User-Data-Already-Available

This AVP indicates whether S-CSCF is already storing the user data or not.

Vendor ID
10415

VSA Type
624

AVP Type
ENUM

Supported enumerated value(s):

0 USER_DATA_NOT_AVAILABLE

1 USER_DATA_ALREADY_AVAILABLE

AVP Flag
M

User-Equipment-Info

This AVP indicates the identification and capabilities of the terminal.

Vendor ID
0

VSA Type
458

AVP Type
GROUPED

Supported group value(s):

[USER_EQUIPMENT_INFO_TYPE]

[USER_EQUIPMENT_INFO_VALUE]

AVP Flag
M

User-Equipment-Info-Type

Defines the type of information present in User-Equipment-Info-Value AVP.

Vendor ID
0

VSA Type
459

AVP Type
ENUM

Supported enumerated value(s):

0 IMEISV

1 MAC

2 EUI64

3 MODIFIED_EUI64

4 ESN

5 MEID

AVP Flag
M

User-Equipment-Info-Value

Defines the type of identifier used.

Vendor ID
0

VSA Type
460

AVP Type
OCTETSTRING

AVP Flag
M

User-Id

User-Id

Vendor ID
10415

VSA Type
1444

AVP Type
UTF8STRING

AVP Flag
M

User-Identity

This grouped AVP contains either a Public-Identity AVP or an MSISDN AVP.

Vendor ID
10415

VSA Type
700

AVP Type
GROUPED

Supported group value(s):

[PUBLIC_IDENTITY]

[MSISDN]

AVP Flag
M

User-Name

This AVP contains identification of the service user in a format consistent with the Network Access Identifier (NAI) specification.

Vendor ID
0

VSA Type
1

AVP Type
UTF8STRING

AVP Flag
M

User-Password

This AVP indicates PAP for multiauth in PDG.

Vendor ID
0

VSA Type
2

AVP Type
OCTETSTRING

AVP Flag
M

User-Session-Id

This AVP holds the session identifier.

Vendor ID
10415

VSA Type
830

AVP Type
UTF8STRING

AVP Flag
M

V4-Transport-Address

This AVP contains a single IPv4 address and a single port number.

Vendor ID
13019

VSA Type
454

AVP Type
GROUPED

Supported group value(s):

[FRAMED_IP_ADDRESS]

[PORT_NUMBER]

AVP Flag
N/A

V6-Transport-Address

This AVP contains a single IPv6 address and a single port number.

Vendor ID
13019

VSA Type
453

AVP Type
GROUPED

Supported group value(s):

[FRAMED_IPV6_PREFIX]

[PORT_NUMBER]

AVP Flag
N/A

VPLMN-Dynamic-Address-Allowed

This AVP indicates whether for this APN, the UE is allowed to use the PDN GW in the domain of the HPLMN only, or additionally, the PDN GW in the domain of the VPLMN.

Vendor ID
10415

VSA Type
1432

AVP Type
ENUM

Supported enumerated value(s):

0 NOTALLOWED

1 ALLOWED

AVP Flag
M

Validity-Time

Validity time of the granted service units. Measurement starts upon receipt of the Credit-Control-Answer Message containing this AVP.

Vendor ID
0

VSA Type
448

AVP Type
UINT32

AVP Flag
M

Value-Digits

This AVP contains the significant digits of the number. If decimal values are needed to present the units, the scaling MUST be indicated with the related Exponent AVP.

Vendor ID
0

VSA Type
447

AVP Type
INT64

AVP Flag
M

Vendor-Id

Unique Identifier of the Vendor and contains the IANA "SMI Network Management Private Enterprise Codes" value assigned to the vendor of the Diameter application.

Vendor ID
0

VSA Type
266

AVP Type
UINT32

AVP Flag

M

Vendor-Id-Resp

Unique identifier of the vendor.

Vendor ID
10415

VSA Type
266

AVP Type
UINT32

AVP Flag
N/A

Vendor-Specific-Application-Id

Specifies the Vendor Specific Application ID and is used to advertise support of a vendor-specific Diameter Application.

Vendor ID
0

VSA Type
260

AVP Type
GROUPED

Supported group value(s):

[VENDOR_ID]

[AUTH_APPLICATION_ID]

[ACCT_APPLICATION_ID]

AVP Flag
M

Vendor-Specific-QoS-Profile-Template

This AVP defines the namespace of the QoS profile (indicated in the Vendor-ID AVP) followed by the specific value for the profile.

Vendor ID
0

VSA Type
6064

AVP Type
GROUPED

Supported group value(s):

[VENDOR_ID]

[QOS_PROFILE_TEMPLATE]

AVP Flag
M

Visited-Network-Identifier

This AVP contains an identifier that helps the home network to identify the visited network (for example, the visited network domain name).

Vendor ID
10415

VSA Type
600

AVP Type
OCTETSTRING

AVP Flag
M

Visited-PLMN-Id

This AVP contains the concatenation of MCC and MNC.

Vendor ID
10415

VSA Type
6008

AVP Type
UTF8STRING

AVP Flag
M

WLAN-Session-Id

This AVP contains the WLAN Session ID that is used to correlate PDG and WLAN AN charging data.

Vendor ID
0

VSA Type
11009

AVP Type
UINT32

AVP Flag
M

WiMAX-A-PCEF-Address

This AVP indicates the IP address of the A-PCEF to the PDF.

Vendor ID
24757

VSA Type
411

AVP Type
ADDRESS

AVP Flag
M

WiMAX-PCC-R3-P-Capability

This AVP contains in a CCR message the WiMAX capabilities supported by the ASN. In a CCA it identifies the options selected by the PCRF.

Vendor ID
24757

VSA Type
404

AVP Type
GROUPED

Supported group value(s):

[WIMAX_RELEASE]

[ACCOUNTING_PCC_R3_P_CAPABILITY]

AVP Flag
M

WiMAX-QoS-Information

This AVP contains the WiMAX QoS information for ASN GW.

Vendor ID
24757

VSA Type
407

AVP Type
GROUPED

Supported group value(s):

[QOS_CLASS_IDENTIFIER]

[MAX_REQUESTED_BANDWIDTH_UL]

[MAX_REQUESTED_BANDWIDTH_DL]

[GUARANTEED_BITRATE_UL]

[GUARANTEED_BITRATE_DL]

[PACKET_INTERVAL]

[PACKET_SIZE]

AVP Flag
M

WiMAX-Release

This AVP indicates a WiMAX release formatted as major/minor.

Vendor ID
24757

VSA Type
301

AVP Type
OCTETSTRING

AVP Flag
M

Wildcarded-IMPU

This AVP contains a wild-carded Public User Identity stored in the HSS.

Vendor ID
10415

VSA Type
636

AVP Type
UTF8STRING

AVP Flag
N/A

Wildcarded-PSI

This AVP contains a wild-carded PSI stored in the HSS.

Vendor ID
10415

VSA Type
634

AVP Type
UTF8STRING

AVP Flag
M

Wildcarded-Public-Identity

This AVP contains a Wildcarded PSI or Wildcarded Public User Identity stored in the HSS.

Vendor ID
10415

VSA Type
634

AVP Type
UTF8STRING

AVP Flag
N/A

XRES

This AVP contains the XRES (Expected Response USIM).

Vendor ID
10415

VSA Type
1448

AVP Type
OCTETSTRING

AVP Flag
M

Chapter 5
RADIUS Dictionaries and Attribute Definitions

This chapter presents information on RADIUS dictionary types and attribute definitions.

For the quick reference table, see the *RADIUS Attribute Quick Reference* appendix.

RADIUS Dictionaries

This section presents information on RADIUS dictionary types.

Dictionary Types

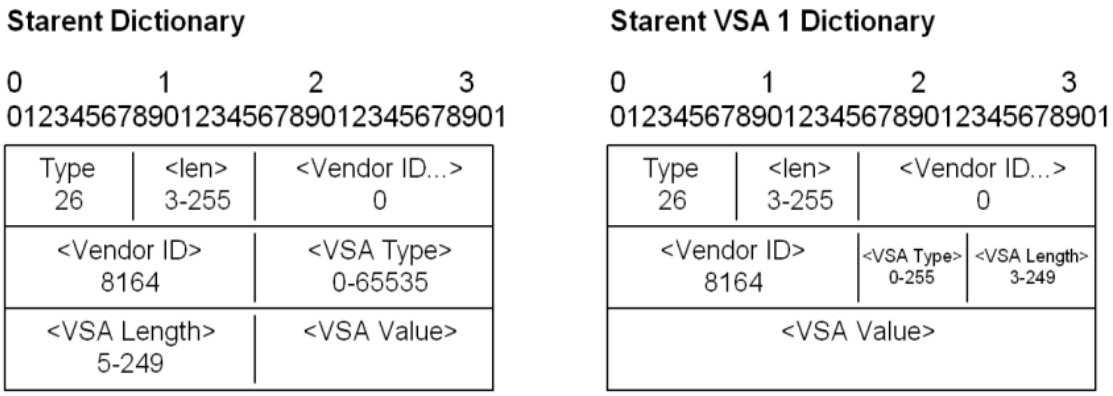
The CLI command to specify the RADIUS dictionary is:

radius dictionary [3gpp | 3gpp2 | 3gpp2-835 | custom *XX* **| standard | starent | starent-835 | starent-vsa1 | starent-vsa1-835]**

Keyword	Description
custom*XX*	These dictionaries can be customized. Customization information can be obtained by contacting your local service representative. *XX* is the integer value of the custom dictionary. ***Important:*** RADIUS dictionary custom23 should be used in conjunction with Enhanced Charging Service (ECS).
standard	This dictionary consists only of the attributes specified in RFC 2865, RFC 2866, and RFC 2869. It also supports 3GPP release 4 and 3GPP Release 5 - extended QoS format.
3gpp	This dictionary consists not only of all of the attributes in the standard dictionary, but also all of the attributes specified in 3GPP 32.015.
3gpp2	This dictionary consists of all of the attributes in the standard dictionary, and all of the attributes specified in IS-835-A.
3gpp2-835	This dictionary consists of all of the attributes in the standard dictionary, and all of the attributes specified in IS-835.
starent-vsa1	This dictionary consists of the 3GPP2 dictionary, and includes the vendor-specific attributes (VSAs) as well. The VSAs in this dictionary support a one-byte wide VSA Type field in order to support certain RADIUS applications. The one-byte limit allows support for only 256 VSAs (0 - 255) as shown in the following figure. This is the default dictionary. ***Important:*** In 12.0 and later releases, no new RADIUS/Diameter attributes can be added to the **starent-vsa1** dictionary. If there are any new attributes to be added, these can be added to the **starent** dictionary.
starent-vsa1-835	This dictionary consists of the 3GPP2-835 dictionary, and includes the vendor-specific attributes (VSAs) as well. The VSAs in this dictionary support a one-byte wide VSA Type field in order to support certain RADIUS applications. The one-byte limit allows support for only 256 VSAs (0 - 255) as shown in the following figure.
starent	This dictionary consists of all of the attributes in the starent-vsa1 dictionary and incorporates additional VSAs by using a two-byte VSA Type field as shown in the following figure. This dictionary is the master-set of all of the attributes in all of the dictionaries supported by the system.

Keyword	Description
`starent-835`	This dictionary consists of all of the attributes in the starent-vsa1-835 dictionary and incorporates additional VSAs by using a two-byte VSA Type field. This dictionary is the master-set of all of the attributes in all of the -835 dictionaries supported by the system.

Figure 3. Difference in VSA Value Lengths per Dictionary



Important: Customer-specific attributes are not documented in this reference. For information on customer-specific attributes, contact your Cisco account representative.

Important: The length documented for each attribute is the length of the attribute's Value field (data portion) and not length of the attribute (Type + Length + Value fields).

RADIUS Attribute Definitions

This section presents RADIUS attribute definitions.

Important: RADIUS attributes received by the system from the RADIUS server always take precedence over local-subscriber attributes and parameters configured on the system.

3GPP-Allocate-IPType

This attribute indicates whether the Access-Request is sent for user authentication only and/or for allocation of IPv4 and/or IPv6 address.

Type
26

Vendor ID
10415

VSA Type
27

Length
4

Value
Enumerated integer. Supported values are:

- none = 0
- ipv4 = 1
- ipv6 = 2
- ipv4-or-ipv6 = 3

3GPP-CAMEL-Charging-Info

This attribute contains the received CAMEL charging information. CAMEL charging information is applicable to GGSN.

Type
26

Vendor ID
10415

VSA Type
24

Length
1–255

Value
String

3GPP-CG-Address

This attribute identifies the charging gateway address.

Type
26

Vendor ID
10415

VSA Type
4

Length
4

Value
IPv4 address

3GPP-Charging-ID

This attribute contains the charging ID for the PDP Context. This together with the GGSN-Address constitutes a unique identifier for the PDP context.

Type
26

Vendor ID
10415

VSA Type
2

Length
4

Value
Unsigned integer

3GPP-Chrg-Char

This attribute contains the charging characteristics for this PDP Context received in the Create PDP Context Request Message (only available in R99 and later releases).

This attribute is also accepted in CoA request message to be used in a currently active subscriber session.

If this AVP is present in Access Accept message the locally configured APN value will be overridden.

Type
26

Vendor ID
10415

VSA Type
13

Length
4

Value
Opaque value

3GPP-GGSN-Address

This attribute contains IPv4 address of the GGSN.

Type
26

Vendor ID
10415

VSA Type
7

Length
4

Value
IPv4 address

3GPP-GGSN-IPv6-Address

For GGSN, it represents the GGSN IPv6 address that is used by the GTP control plane for thecontext establishment. For P-GW, it represents the P-GW IPv6 address that is used on S5/S8, S2a, S2b, or S2c control plane for the IP-CAN session establishment.

Type
26

Vendor ID
10415

VSA Type
16

Length
16

Value
Opaque value

3GPP-GGSN-Mcc-Mnc

This attribute contains the MCC-MNC of the network the GGSN belongs to.

Type
26

Vendor ID
10415

VSA Type
9

Length
1–6

Value
Opaque value

3GPP-IMEISV

This attribute identifies the International Mobile Equipment Identity and Software Version (IMEISV) number received from the mobile node (MN). It is sent in RADIUS authentication and accounting messages by GGSN.

Type
26

Vendor ID
10415

VSA Type
20

Length
16

Value
Opaque value

3GPP-IMSI

This attribute contains the IMSI identifying the mobile unit.

This attribute is also accepted in CoA request message to be used in a currently active subscriber session.

Type
26

Vendor ID
10415

VSA Type
1

Length
1–15

Value
Opaque value

3GPP-IMSI-Mcc-Mnc

This attribute contains the MCC and MNC extracted from the user's IMSI (first 5 or 6 digits, as applicable from the presented IMSI).

Type
26

Vendor ID
10415

VSA Type
8

Length
1–6

Value
Opaque value

3GPP-IPv6-DNS-Servers

This attribute contains list of IPv6 DNS server addresses.

Type
26

Vendor ID
10415

VSA Type
17

Length
16–240

Value
Opaque value

3GPP-MS-TimeZone

This attribute indicates the offset between universal time and local time in steps of 15 minutes of where the MS currently resides.

Type
26

Vendor ID
10415

VSA Type
23

Length
2

Value
Opaque value

3GPP-Negotiated-DSCP

This attribute is used to mark IP packets of PDP context on the Gi interface.

Type
26

Vendor ID
10415

VSA Type
26

Length
1

Value
Unsigned integer

3GPP-Negotiated-QoS-Profile

This attribute specifies the QoS profile to be used for the subscriber.

This attribute is also accepted in CoA request message to be used in a currently active subscriber session.

Type
26

Vendor ID
10415

VSA Type
5

Length
In 10.2 and earlier releases: 1–35

In 11.0 and later releases: 1–39

Value
Opaque value

3GPP-NSAPI

This attribute specifies the value of the NSAPI of the PDP context that the RADIUS message is related to. It is encoded as its hexadecimal representation, using 1 UTF-8 encoded digit.

This attribute is also accepted in CoA request message to be used in a currently active subscriber session.

Type
26

Vendor ID
10415

VSA Type
10

Length
1

Value
Opaque value

3GPP-Packet-Filter

This compound attribute specifies the Packet Filter used for the PDP context.

Type
26

Vendor ID
10415

VSA Type
25

Length
65

Value
Contains the following subattributes:

Identifier

Identifier of the packet filter.

Type
1

Length
1

Value
Unsigned integer

Eval-Precedence

Evaluation precedence of the packet filter.

Type
2

Length
1

Value
Unsigned integer

Length

Length of the packet filter.

Type

3

Length

1

Value

Unsigned integer

Direction

Direction of the packet filter.

Type

4

Length

1

Value

Unsigned integer

IPv4-Address-Type

This is a compound attribute specifying the IPv4 source address and netmask if the direction is downlink, or destination address and netmask if the direction is downlink, or destination address and netmask if the direction is uplink.

Type

5

Length

8

Value

Contains the following two subattributes:

Address

This attribute contains source address if direction value is set to Downlink, and destination address if direction value is set to Uplink.

Type

1

Length

4

Value

IPv4 address

Netmask

This attribute contains netmask of the IPv4 address.

Type

2

Length

4

Value

IPv4 address

IPv6-Address-Type

This is a compound attribute specifying the IPv6 source address and netmask if the direction is Downlink, or Destination Address and Netmask if the direction is Downlink, or Destination Address and Netmask if the direction is Uplink.

Type

6

Length

32

Value

Contains the following two subattributes:

Address

This attribute contains source address if direction value is set to Downlink, and destination address if direction value is set to Uplink.

Type

1

Length

16

Value

Opaque value

Netmask

This attribute contains the Netmask of the IPv6 address.

Type

2

Length

16

Value

Opaque value

Protocol-Identifier-Or-Next-Header

Specifies the IPv4 Protocol Identifier or IPv6 Next Header.

Type

7

Length

1

Value

Unsigned integer

Destination-Port

Specifies the Destination Port number of the packet filter.

Type

8

Length

2

Value

An integer in network byte order

Destination-Port-Range

This is a compound attribute and specifies the destination port range.

Type

9

Length

4

Value

Contains the following two subattributes:

Lower

Specifies the lower range of the destination port of the packet filter.

Type

1

Length

2

Value

Unsigned integer

Higher

Specifies the higher range of the destination port of the packet filter.

Type

2

Length

2

Value

Unsigned integer

Source-Port

Specifies the source port number of the packet filter.

Type
10

Length
2

Value
Unsigned integer

Source-Port-Range

Specifies the source port range.

Type
11

Length
4

Value
Contains the following two subattributes:

Lower

Specifies lower range of the source port of the packet filter.

Type
1

Length
2

Value
Unsigned integer

Higher

Specifies higher range of the source port of the packet filter.

Type
2

Length
2

Value
Unsigned integer

Security-Parameter-Index

Specifies the IPSec Security Parameter Index(IPv6).

Type
12

Length
4

Value

Unsigned integer

Type-Of-Service

This is a compound attribute and specifies the Type of Service/ Traffic Class.

Type

13

Length

2

Value

Contains the following two subattributes:

Value

Specifies the Type of Service/Traffic Class Value.

Type

1

Length

1

Value

Unsigned integer

Mask

Specifies the Type of Service/Traffic Class Mask.

Type

2

Length

1

Value

Unsigned integer

Flow-Label

Specifies the IPv6 Flow Label.

Type

14

Length

3

Value

Opaque value

3GPP-PDP-Type

This attribute identifies the PDP Context type.

Type
26

Vendor ID
10415

VSA Type
3

Length
4

Value
Enumerated integer. Supported values are:

- ipv4 = 0
- ppp = 1
- ipv6 = 2
- ipv4-or-ipv6 = 3

3GPP-RAT-Type

This attribute indicates which Radio Access Technology is currently serving the UE.

Type
26

Vendor ID
10415

VSA Type
21

Length
1

Value
Opaque value

3GPP-Selection-Mode

This attribute contains the selection mode for this PDP Context received in the Create PDP Context Request message as an UTF-8 encoded character.

Type
26

Vendor ID
10415

VSA Type

12

Length
1

Value
Opaque value

3GPP-Session-Stop-Ind

The presence of this attribute indicates to the AAA server that the last PDP context of a session is released and that the PDP session has been terminated.

Type
26

Vendor ID
10415

VSA Type
11

Length
1

Value
Opaque value

3GPP-SGSN-Address

This attribute contains IPv4 address of the SGSN.

Type
26

Vendor ID
10415

VSA Type
6

Length
4

Value
IPv4 address

3GPP-SGSN-IPv6-Address

For GGSN, it represents the SGSN IPv6 address that is used by the GTP control plane for the handling of control messages. For P-GW, it represents the IPv6 address of the S-GW, trusted non-3GPP IP access or ePDG that is used on S5/S8, S2a, or S2b for the handling of control messages. The address may beused to identify the PLMN to which the user is attached.

Type
26

Vendor ID
10415

VSA Type
15

Length
16

Value
Opaque value

3GPP-SGSN-Mcc-Mnc

For GPRS the MCC and the MNC of the SGSN.

Type
26

Vendor ID
10415

VSA Type
18

Length
1–6

Value
String

3GPP-Teardown-Indicator

If this value is set to 1 in disconnect-request, the whole correlated sessions would be disconnected.

This attribute is also accepted in CoA request message to be used in a currently active subscriber session.

Type
16

Vendor ID
10415

VSA Type
19

Length
1

Value
Opaque value

3GPP-User-Location-Info

GTP user location information attribute for the subscriber session.

Type
26

Vendor ID
10415

VSA Type
22

Length
In 10.2 and earlier releases: 8

In 11.0, 12.0 and 12.1 releases: 37

Value
Opaque value

3GPP2-835-Release-Indicator

3GPP2-895- Standard Release-Indicator, reason/cause for session release.

Type
26

Vendor ID
5535

VSA Type
24

Length
4

Value
Enumerated integer. Supported values are:

- Unknown = 0
- PPP-Timeout = 1
- Handoff = 2
- PPP-Termination = 3
- Mobile-IP-Registration-Failure = 4
- Active-To-Dormant = 5

3GPP2-Acct-Session-Time

The total amount of time spent in the Active state, in seconds. This attribute has the same type as Acct-Session-Time, and thus conforms to IS-835.

Type
46

Vendor ID
N/A

VSA Type

N/A

Length

4

Value

Unsigned integer

3GPP2-Active-Time

The total period of time spent in the Active state, in seconds.

Type

26

Vendor ID

5535

VSA Type

49

Length

4

Value

Unsigned integer

3GPP2-Active-Time-Corrected

3GPP2 Active session time value.

Type

26

Vendor ID

5535

VSA Type

49

Length

4

Value

Unsigned integer

3GPP2-Airlink-Record-Type

This attribute indicates the most recent type of Airlink Record to be received for this subscriber's connection.

Type

26

Vendor ID

5535

VSA Type
40

Length
4

Value
Enumerated integer. Supported values are:

- Connection-Setup = 1
- Active-Start = 2
- Active-Stop = 3
- SDB = 4
- BCMCS-Connection-Setup = 5
- BCMCS-Active-Start = 6
- BCMCS-Active-Stop = 7

3GPP2-Airlink-Sequence-Number

This represents the sequence number of an Airlink Record and is incremented (modulo 256) by the PCF for each Airlink Record. The sequence number is unique for a given RP Session ID, PCF ID, and MSID.

Type
26

Vendor ID
5535

VSA Type
42

Length
4

Value
Unsigned integer

3GPP2-Air-QOS

This attribute identifies airlink QOS associated with the user data. The least significant 4 bits hold the QOS priority as defined in C.S0001-A in the subscriber profile.

Type
26

Vendor ID
5535

VSA Type
39

Length
4

Value
Unsigned integer

3GPP2-Allowed-Diffserv

This attribute specifies if the user is able to mark packets with AF and/or EF. The Max Class specifies that the user may mark packets with a Class Selector Code Point that is less then or equal to Max Class.

Type
26

Vendor ID
5535

VSA Type
73

Length
24

Value
Contains the following three subattributes:

Flags

Allowed DSCP flag.

Type
1

Length
2

Value
Enumerated integer. Supported values are:

- Allow_AF_EF_Exp = 0xE000
- Allow_AF_EF = 0xC000
- Allow_AF_Exp = 0xA000
- Allow_EF_Exp = 0x6000
- Allow_AF = 0x8000
- Allow_EF = 0x4000
- Allow_Exp = 0x2000
- Allow_None = 0x0

Max-Class

Allowed max dscp.

Type
2

Length

2

Value

Enumerated integer. Supported values are:

- Best-Effort = 0x0
- AF11 = 0x2800
- AF12 = 0x3000
- AF13 = 0x3800
- AF21 = 0x4800
- AF22 = 0x5000
- AF23 = 0x5800
- AF31 = 0x6800
- AF32 = 0x7000
- AF33 = 0x7800
- AF41 = 0x8800
- AF42 = 0x9000
- AF43 = 0x9800
- EF = 0xb800
- Class1 = 0x2000
- Class2 = 0x4000
- Class3 = 0x6000
- Class4 = 0x8000
- Class5 = 0xa000
- Class6 = 0xc000
- Class7 = 0xe000

RT-Marking

Allowed max dscp rev. tun.

Type

3

Length

2

Value

Enumerated integer. Supported values are:

- Best-Effort = 0x0
- AF11 = 0x2800
- AF12 = 0x3000
- AF13 = 0x3800
- AF21 = 0x4800

- AF22 = 0x5000
- AF23 = 0x5800
- AF31 = 0x6800
- AF32 = 0x7000
- AF33 = 0x7800
- AF41 = 0x8800
- AF42 = 0x9000
- AF43 = 0x9800
- EF = 0xb800
- Class1 = 0x2000
- Class2 = 0x4000
- Class3 = 0x6000
- Class4 = 0x8000
- Class5 = 0xa000
- Class6 = 0xc000
- Class7 = 0xe000

3GPP2-Allowed-Persistent-TFTs

This attribute displays the 3GPP2 Allowed Persistent Traffic Flow Templates.

Type
26

Vendor ID
5535

VSA Type
89

Length
4

Value
Unsigned integer

3GPP2-Alternate-Billing-ID

This attribute is currently not supported.

3GPP2-Always-On

This attribute, when set to Active, indicates that the subscriber's session should be kept up regardless of the idle time as long as the subscriber is reachable. Reachability is ascertained using LCP keepalive messages.

Type
26

Vendor ID
5535

VSA Type
78

Length
4

Value
Enumerated integer. Supported values are:

- Inactive = 0
- Active = 1

3GPP2-Auth-Flow-Profile-Id

This compound attribute is a list of flow profile IDs.

Type
26

Vendor ID
5535

VSA Type
131

Length
6

Value
Contains the following three subattributes:

Profile-Id-Forward

This attribute specifies a list of Forward Flow Profile IDs that the user is allowed to specify/request in a QoS Sub Blob.

Type
1

Length
2

Value
Unsigned integer

Profile-Id-Reverse

This attribute specifies a list of Reverse Flow Profile IDs that the user is allowed to specify/request in a QoS Sub Blob.

Type

2

Length

2

Value

Unsigned integer

Profile-Id-Bi-Direction

This attribute specifies the list of Bi-Direction Flow Profile IDs that the user is allowed to specify/request in a QoS Sub Blob.

Type

3

Length

2

Value

Unsigned integer

3GPP2-Auth-QoS-Profile-Id

This attribute specifies the authorized QOS profile ID.

Type

26

Vendor ID

5535

VSA Type

131

Length

1

Value

1

3GPP2-Bad-PPP-Frame-Count

The total number of PPP frames from the MS dropped by the PDSN due to uncorrectable errors.

Type

26

Vendor ID

5535

VSA Type

25

Length

4

Value
Unsigned integer

3GPP2-BCMCS-Auth-Parameters

This is a grouped AVP with Authentication signature, Sequence number, and timestamp required to validate each flow in a BCMCS flow registration request. Each flow is validated using the procedure described in 3GPP2 standard C.S0054-0_v1.0. This information is configured on a per subscriber basis.

Type
26

Vendor ID
5535

VSA Type
99

Length
38

Value
Contains the following three subattributes:

BAK-Sequence-Number

Type
1

Length
1

Value
Opaque value

Timestamp

Type
2

Length
33

Value
Opaque value

Auth-Signature

Type
3

Length
4

Value

Unsigned integer

3GPP2-BCMCS-BSN-Session-Info

This is a grouped AVP containing information about the established flows. This includes the multicast address, port, compression status of the flow, and the content server address.

Type
26

Vendor ID
5535

VSA Type
103

Length
46

Value
Contains the following 11 subattributes:

Flow-ID

Type
1

Length
2-4

Value
Opaque value

Mcast-IP-Addr

Type
2

Length
4

Value
IPv4 address

Mcast-Port

Type
3

Length
2

Value
Unsigned integer

Header-Compression-Algorithm

Type

4

Length

4

Value

Enumerated integer. Supported values are:

- No_header_compression = 0
- ROHC_U_Mode = 1

CID-Type-Attribute

Type

5

Length

4

Value

Enumerated integer. Supported values are:

- Small_CID = 0
- Large_CID = 1

MAX-CID

Type

6

Length

2

Value

Unsigned integer

Compression-Profile

Type

7

Length

2

Value

Unsigned integer

MAX-Header-Size

Type

8

Length
2

Value
Unsigned integer

MRRU

Type
9

Length
2

Value
Unsigned integer

Content-Server-Source-IP-Address

Type
10

Length
4

Value
IPv4 address

Content-Server-Source-IPv6-Address

Type
11

Length
16

Value
Opaque value

3GPP2-BCMCS-Capability

This AVP defines the specific BCMCS protocol revision the PDSN supports.

Type
26

Vendor ID
5535

VSA Type
101

Length
4

Value

Contains the following subattribute:

BCMCS-Protocol-Revision

Type
1

Length
2

Value
Enumerated integer. Supported value is:

- Release_0 = 1

3GPP2-BCMCS-Common-Session-Info

This is a grouped AVP which specifies the program start time, end time and the allowed registration time on a per flow basis.

Type
26

Vendor ID
5535

VSA Type
102

Length
18

Value
Contains the following five subattributes:

Flow-ID

Type
1

Length
2–4

Value
Opaque value

Program-Start-Time

Type
2

Length
4

Value
Unsigned integer

Program-End-Time

Type
3

Length
4

Value
Unsigned integer

Program-Allowed-Registration-Time

Type
4

Length
4

Value
Unsigned integer

Auth-Required-Flag

Type
5

Length
2

Value
Enumerated integer. Supported values are:

- Authorization_not_required = 0
- Authorization_required = 1

3GPP2-BCMCS-Flow-ID

This attribute specifies the BCMCS_FLOW_ID.

Type
26

Vendor ID
5535

VSA Type
100

Length
2–4

Value
String

3GPP2-BCMCS-Flow-Transmit-Time

The total BCMCS flow transmission time in seconds.

Type
26

Vendor ID
5535

VSA Type
107

Length
4

Value
Unsigned integer

3GPP2-BCMCS-Mcast-IP-Addr

This attribute contains the multicast IP address of the BCMCS flow as it would appear in the source or destination field of an IP header.

Type
26

Vendor ID
5535

VSA Type
109

Length
4

Value
IPv4 address

3GPP2-BCMCS-Mcast-Port

The multicast port for the BCMCS flow.

Type
26

Vendor ID
5535

VSA Type
110

Length
2

Value
Unsigned integer

3GPP2-BCMCS-Reason-Code

This attribute specifies the reason to send the RADIUS Access-Accept message.

Type
26

Vendor ID
5535

VSA Type
105

Length
1

Value
Opaque value

3GPP2-BCMCS-RN-Session-Info

This is a grouped AVP which contains the encryption mechanism, BAK (Broadcast access key), BAK_ID, BAK expire time and authorization required flag. This attribute specifies the session information that needs to be known only by the RN.

Type
26

Vendor ID
5535

VSA Type
104

Length
31

Value
Contains the following six subattributes:

Flow-ID

Type
1

Length
2-4

Value
Opaque value

BCMCS-Encryption-Mechanism-Attribute

Type
2

Length

2

Value

Enumerated integer. Supported values are:

- High_layer_encryption_in_CS = 0
- Link_layer_encryption_in_RN = 1

BCMCS-BAK-ID-Attribute

Type

3

Length

1

Value

Unsigned integer

BCMCS-BAK

Type

4

Length

16

Value

Opaque value

BCMCS-BAK-Expire-Time

Type

5

Length

4

Value

Unsigned integer

BCMCS-Session-Bandwidth-attribute

Type

6

Length

2

Value

Unsigned integer

3GPP2-BCMCS-Subnet-VSA-Format

This attribute is deprecated.

3GPP2-Beginning-Session

3GPP2 Beginning Session will be TRUE or FALSE depending on if this is a new session.

Type
26

Vendor ID
5535

VSA Type
51

Length
4

Value
Enumerated integer. Supported values:

- False = 0
- True = 1

3GPP2-BSID

The base station ID.

Type
26

Vendor ID
5535

VSA Type
10

Length
6–12

Value
Opaque value

3GPP2-Carrier-ID

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

Type
26

Vendor ID

5535

VSA Type
142

Length
5–6

Value
Opaque value

3GPP2-Comp-Tunnel-Indicator

This attribute indicates the invocation of a compulsory tunnel established on behalf of the MS for providing private network and/or ISP access during a single packet data connection. Normal PPP sessions will show No Tunnel. L2TP, IPinIP, and IP-GRE tunnels will show Non-Secure-Tunnel. IPSEC support will show Secure-Tunnel.

Type
26

Vendor ID
5535

VSA Type
23

Length
4

Value
Enumerated integer. Supported values are:

- No Tunnel = 0
- Non-Secure-Tunnel = 1
- Secure-Tunnel = 2

3GPP2-Container

A compound attribute that encapsulates the User Data Record for an Airlink Event.

Type
26

Vendor ID
5535

VSA Type
6

Length
Varies

Value
Embedded attributes as defined in “Wireless IP Network Standard – 3GPP2.P.S0001-A-1” [6].

Format of the 3GPP2-Container attribute:

Embedded attributes will contain 0 or 1 of the following attributes:

- 3GPP2-User-Zone
- 3GPP2-Air-QOS
- NAS-IP-Address
- 3GPP2-Serving-PCF
- 3GPP2-BSID
- Acct-Output-Octets
- Acct-Output-Gigawords
- Acct-Input-Octets
- Acct-Input-Gigawords
- SNA1-PPP-Unfr-data-In-Oct
- SNA1-PPP-Unfr-data-Out-Oct
- 3GPP2-Bad-PPP-Frame-Count
- 3GPP2-Active-Time
- 3GPP2-Number-Active-Transitions
- 3GPP2-SDB-Input-Octets
- 3GPP2-SDB-Output-Octets
- 3GPP2-Num-SDB-Input
- 3GPP2-Num-SDB-Output
- 3GPP2-Num-Bytes-Received-Total
- 3GPP2-MIP-Sig-Octet-Count-In
- 3GPP2-MIP-Sig-Octet-Count-Out

Embedded attributes inside the 3GPP2-Container attribute have the same format as those outside the 3GPP2-Container attribute.

3GPP2-Correlation-Id

This attribute contains an ID that correlates all accounting sessions authorized for this NAI by this access request.

This attribute is also accepted in CoA request and response messages to be used in a currently active subscriber session.

Type

26

Vendor ID

5535

VSA Type

44

Length

1–253

Value

String

3GPP2-Correlation-Id-Old

Custom-11 style correlation ID.

Type
26

Vendor ID
5535

VSA Type
40

Length
1–251

Value
Opaque value

3GPP2-DCCH-Frame-Size

Specifies the DCCH frame size.

Type
26

Vendor ID
5535

VSA Type
50

Length
4

Value
Enumerated integer. Supported values are:

- None = 0
- 5s = 1
- 20ms = 2

3GPP2-Diff-Service-Class-Option

This is the DSCP (Differentiated Service Code Point) value as defined in the 3GPP2 standard. The DSCP values are assigned for different classes of traffic so that each traffic class can be given different priorities (QoS).

Type
26

Vendor ID
5535

VSA Type
5

Length
4

Value
Unsigned integer

3GPP2-Disconnect-Reason

This attribute indicates the reason for disconnecting the user. This attribute may be present in the RADIUS Disconnect-request Message from Home RADIUS server to the PDSN.

This attribute is also accepted in CoA request message to be used in a currently active subscriber session.

Type
26

Vendor ID
5535

VSA Type
96

Length
4

Value
Enumerated integer. Supported values are:

- MS_Mobility_Detection = 1
- All other values are reserved.

3GPP2-DNS-Server-IP-Address

DNS server IP address. Used in custom dictionary.

Type
26

Vendor ID
5535

VSA Type
117

Value
Contains the following four subattributes:

Primary-DNS-Server-IP

Primary DNS Server IP address.

Type
1

Length
4

Value
IPv4 address

Secondary-DNS-Server-IP

Secondary DNS Server IP address.

Type
2

Length
4

Value
IPv4 address

Flag

M bit set to 1 indicates to the PDSN that primary and secondary IP addresses provided by the Home RADIUS server should override the primary and secondary IP addresses provided also by the visited RADIUS server.

Type
3

Length
1

Value
Unsigned integer

Entity-Type

Network Entity that inserted in the DNS server ID address. Currently the following types are defined. HAAA = 1, VAAA = 1.

Type
4

Length
1

Value
Unsigned integer

3GPP2-DNS-Server-IPV6-Addr

DNS server IPv6 address.

Type
26

Vendor ID

5535

VSA Type
214

Length
0–50

Value
Contains the following four subattributes:

Primary-DNS-Server-IPV6

Primary DNS server IPv6 address.

Type
1

Length
2

Value
Opaque value

Secondary-DNS-Server-IPV6

Secondary IPv6 DNS server IP address.

Type
2

Length
2

Value
Opaque value

Flag-IPV6

M bit set to 1 indicates to the PDSN that Primary and Secondary IPv6 addresses provided by the Home RADIUS server should override the Primary and Secondary IPv6 addresses provided also by the visited RADIUS server.

Type
3

Length
1

Value
Unsigned integer

Entity-Type-IPV6

Network Entity that inserted in the DNS server ID address. Either HAAA = 1, VAAA = 1.

Type

4

Length
1

Value
Unsigned integer

3GPP2-DNS-Update-Required

This attribute indicates whether the HA needs to send the DNS update to the DNS server.

Type
26

Vendor ID
5535

VSA Type
75

Length
4

Value
Enumerated integer. Supported values are:

- No = 0 — HA does not need to send DNS update
- Yes = 1 — HA needs to send DNS update

3GPP2-ESN

This attribute contains the Electronic Serial Number (ESN) of the Mobile Station.

Type
26

Vendor ID
5535

VSA Type
52

Length
1–15

Value
Opaque value

3GPP2-FA-Address

This attribute indicates if compulsory tunneling is to be employed on behalf of a subscriber. Usually compulsory tunneling is employed when a subscriber cannot initiate a tunnel itself, usually because the subscriber's device does not support tunneling. Contains an IP address as it would appear in the IP header.

Type
26

Vendor ID
5535

VSA Type
79

Length
4

Value
IPv4 address

3GPP2-FEID

This attribute specifies the FEID value.

Type
26

Vendor ID
5535

VSA Type
216

Length
0–16

Value
Opaque value

3GPP2-Flow-Id

This attribute displays the 3GPP2-Flow-Id-parameter.

Type
26

Vendor ID
5535

VSA Type
144

Value
Contains the following two subattributes:

Direction

This attribute identifies the IP flow id direction.

Type
1

Length
2

Value
Enumerated integer. Supported values are:

- Forward = 0
- Reverse = 1
- Both = 2

Flow-Id

This attribute identifies the IP flow.

Type
2

Length
2

Value
Unsigned integer

3GPP2-Flow-Status

This attribute displays the 3GPP2 Flow Status.

Type
26

Vendor ID
5535

VSA Type
145

Length
4

Value
Enumerated integer. Supported values are:

- Active = 0
- Inactive = 1

3GPP2-Forward-Fundamental-Rate

As defined in “Wireless IP Network Standard – 3GPP2.P.S0001-A-1”.

Type
26

Vendor ID
5535

VSA Type
14

Length
4

Value
Unsigned integer

3GPP2-Forward-Fundamental-RC

The format and structure of the RADIUS channel in the forward direction. A set of forward transmission formats that are characterized by data rates, modulation characterized, and spreading rates.

Type
26

Vendor ID
5535

VSA Type
20

Length
4

Value
Unsigned integer

3GPP2-Forward-Mux-Option

Forward direction multiplexer option.

Type
26

Vendor ID
5535

VSA Type
12

Length
4

Value
Unsigned integer

3GPP2-Forward-Traffic-Type

Specifies the forward traffic type.

Type
26

Vendor ID
5535

VSA Type
17

Length
4

Value
Enumerated integer. Supported values are:

- Primary = 0
- Secondary = 1

3GPP2-Fundamental-Frame-Size

This attribute indicates the fundamental frame size. The fundamental channel has the choice of 5 or 20 ms size. The 5 ms frame size allows fast response for short signaling messages (short frame can be decoded quickly). However, depending on configuration, the fundamental may not be present.

Type
26

Vendor ID
5535

VSA Type
19

Length
4

Value
Enumerated integer. Supported values are:

- None = 0
- 5ms = 1
- 20ms = 2

3GPP2-Fwd-Dcch-Mux-Option

This attribute specifies Forward DCCH Mux option.

Type
26

Vendor ID
5535

VSA Type
84

Length
4

Value
Unsigned integer

3GPP2-Fwd-Dcch-Rc

This attribute specifies Radio Configuration of the Forward Packet Data Channel.

Type
26

Vendor ID
5535

VSA Type
86

Length
4

Value
Unsigned integer

3GPP2-Fwd-Pdch-Rc

This attribute specifies Radio Configuration of the Forward Packet Data Channel.

Type
26

Vendor ID
5535

VSA Type
83

Length
4

Value
Unsigned integer

3GPP2-GMT-Timezone-Offset

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

Type
26

Vendor ID
5535

VSA Type
143

Length
4

Value
Integer

3GPP2-Granted-QoS

This attribute displays the 3GPP2-Granted-QoS-Parameter.

Type
26

Vendor ID
5535

VSA Type
132

Value
Contains the following subattributes:

Direction

This attribute specifies the Granted QoS parameters received from the RAN for the flow identified by direction.

Type
1

Length
2

Value
Enumerated integer. Supported values are:

- Forward = 0
- Reverse = 1
- Both = 2

Flow-Id

This attribute specifies the Granted QoS parameters received from the RAN for the flow identified by FLOW_ID.

Type
2

Length
2

Value
Unsigned integer

Attribute-Set-Id

This attribute specifies the Granted QoS parameters received from the RAN for flow verbose or non-verbose.

Type

3

Length

2

Value

Unsigned integer

Flow-Profile-Id

This attribute specifies the Granted QoS parameters received from the RAN for the flow profile ID.

Type

4

Length

2

Value

Unsigned integer

Traffic-Class

This attribute specifies the Granted QoS parameters received from the RAN for the flow traffic class.

Type

5

Length

2

Value

Enumerated integer. Supported values are:

- Unknown = 0
- Conversational = 1
- Streaming = 2
- Interactive = 3
- Background = 4

Peak-Rate

This attribute specifies the Granted QoS parameters received from the RAN for the flow Peak Rate.

Type

6

Length

2

Value
Unsigned integer

Bucket-Rate

This attribute specifies the Granted QoS parameters received from the RAN for the flow Bucket Rate.

Type
7

Length
2

Value
Unsigned integer

Token-Rate

This attribute specifies the Granted QoS parameters received from the RAN for the flow Token Rate.

Type
8

Length
2

Value
Unsigned integer

Max-Latency

This attribute specifies the Granted QoS parameters received from the RAN for the flow Max Latency.

Type
9

Length
2

Value
Unsigned integer

Max-IP-Packet-Loss-Rate

This attribute specifies the Granted QoS parameters received from the RAN for the flow Packet Loss Rate.

Type
10

Length
2

Value
Unsigned integer

Packet-Size

This attribute specifies the Granted QoS parameters received from the RAN for the flow Packet Size.

Type
11

Length
2

Value
Unsigned integer

Delay-Var-Sensitive

This attribute specifies the Granted QoS parameters received from the RAN for the flow Delay Var Sensitive.

Type
12

Length
2

Value
Enumerated integer. Supported values are:

- Not-Specified = 0
- Sensitive = 1

3GPP2-IKE-Secret

This attribute contains the FA/HA shared secret for the IKE protocol. This attribute is salt-encrypted.

Type
26

Vendor ID
5535

VSA Type
3

Length
1-247

Value
Opaque value

3GPP2-IKE-Secret-Request

This attribute indicates if the IKE secret for the FA/HA pair is to be returned for the subscriber.

Type
26

Vendor ID
5535

VSA Type
1

Length
4

Value
Enumerated integer. Supported values are:

- No = 0
- Yes = 1

3GPP2-IKE-Secret-Unencrypted

IKE Secret key from RADIUS server in Access Accept message

Type
26

Vendor ID
5535

VSA Type
3

Length
1–247

Value
Opaque value

3GPP2-IMSI

This is the calling Station-ID attribute. IMSI value of the mobile is being filled in. This is sent when Custom11 dictionary is selected.

Type
26

Vendor ID
5535

VSA Type
1

Length
1–253

Value
Opaque value

3GPP2-Interconnect-IP

This attribute is currently not supported.

3GPP2-Interconnect-QOS

This attribute is currently not supported.

3GPP2-Inter-User-Priority

This attribute displays the 3GPP2-Inter-User-Priority.

This attribute is also accepted in CoA request message to be used in a currently active subscriber session.

Type

26

Vendor ID

5535

VSA Type

139

Length

4

Value

Unsigned integer

3GPP2-IP-QOS

This attribute defines the differentiated Services code points associated with the user data.

Type

26

Vendor ID

5535

VSA Type

36

Length

4

Value

Enumerated integer. Supported values are:

- Best-Effort = 0
- CS1 = 8
- AF11 = 10
- AF12 = 12

- AF13 = 14
- CS2 = 16
- AF21 = 18
- AF22 = 20
- AF23 = 22
- CS3 = 24
- AF31 = 26
- AF32 = 28
- AF33 = 30
- CS4 = 32
- AF41 = 34
- AF42 = 36
- AF43 = 38
- CS5 = 40
- EF = 46
- CS6 = 48
- CS7 = 56

3GPP2-IP-Services-Authorized

This attribute specifies the type of IP services (IPv4/CMIPv4/IPv6/CMIPv6/PMIPv4/PMIPv6, etc.) authorized.

Type

26

Vendor ID

5535

VSA Type

185

Length

4

Value

In 11.0 and earlier releases: Unsigned integer

In 12.0 and later releases: Enumerated integer. Supported values are:

- SIP4 = 1
- SIP6 = 2
- MIP4 = 4
- MIP6 = 8
- IP4_PMIP4 = 16
- IP6_PMIP4 = 32

- IP4_PMIP6 = 64
- IP6_PMIP6= 128

3GPP2-IP-Technology

This attribute identifies whether we are using Simple IP, Mobile IP, or another technology.

Type
26

Vendor ID
5535

VSA Type
22

Length
4

Value
Enumerated integer. Supported values are:

- Simple IP = 1
- Mobile IP = 2

3GPP2-IP-Services-Authorized

This attribute specifies the type of IP services (IPv4/CMIPv4/IPv6/CMIPv6/PMIPv4/PMIPv6..etc) authorized.

Type
26

Vendor ID
5535

VSA Type
185

Length
4

Value
Unsigned integer

3GPP2-KeyID

This attribute contains the opaque IKE Key Identifier for the FA/HA shared IKE secret. The first eight bytes is the network-order FA IP address in hexadecimal characters. The next eight bytes is the network-order HA IP address in hexadecimal characters. The final four bytes is a timestamp in network order, indicating when the key was created, and is the number of seconds since January 1, 1970, UTC.

Type
26

Vendor ID
5535

VSA Type
8

Length
20

Value
Opaque value

3GPP2-Last-Activity

This attribute contains timestamp of the last user activity. This attribute is same as the **3GPP2-Last-User-Activity-Time** standard attribute.

Type
26

Vendor ID
5535

VSA Type
80

Length
4

Value
Unsigned integer

3GPP2-Max-Auth-Aggr-Bw-BET

This attribute contains the maximum authorized aggregate bandwidth for Best Effort Traffic.

This attribute is also accepted in CoA request message to be used in a currently active subscriber session.

Type
26

Vendor ID
5535

VSA Type
130

Length
4

Value
Unsigned integer

3GPP2-Max-Per-Fl-Pri-ForTheUser

The maximum per flow priority for the user.

Type
26

Vendor ID
5535

VSA Type
133

Length
4

Value
Unsigned integer

3GPP2-MEID

Mobile Equipment Identifier (MEID) uniquely identifies the mobile equipment.

Type
26

Vendor ID
5535

VSA Type
116

Length
0–14

Value
Opaque value

3GPP2-MIP-HA-Address

The IP address of the MIP Home Agent.

Type
26

Vendor ID
5535

VSA Type
7

Length
4

Value
IPv4 address

3GPP2-MIP-Lifetime

This VSA should 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 should include the received value in the MIP RRP sent to the PDSN.

Type
26

Vendor ID
5535

VSA Type
92

Length
Variable, greater than 8

Value
Contains the following two subattributes:

RRQ-Lifetime

Should 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 should be used in the MIP RRP.

Type
1

Length
4

Value
Unsigned integer

Used-Lifetime

Should 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.

Type
1

Length
4

Value
Unsigned integer

3GPP2-MIP-Rev-Tunnel-Required

Indicates to the PDSN if MIP Reverse Tunneling is required.

Type
26

Vendor ID
5535

VSA Type
4

Length
4

Value
Enumerated integer. Supported values are:

- NotRequired = 0
- Required = 1

3GPP2-MIP-Sig-Octet-Count-In

The total number of octets in registration requests and solicitations sent by the mobile.

Type
26

Vendor ID
5535

VSA Type
46

Length
4

Value
Unsigned integer

3GPP2-MIP-Sig-Octet-Count-Out

The total number of octets in registration replies and agent advertisements, sent to the mobile.

Type
26

Vendor ID
5535

VSA Type
47

Length
4

Value
Unsigned integer

3GPP2-MIP6-Authenticator

The MN-AAA authenticator obtained from the MN-AAA authentication mobility option in the BU.

Type
26

Vendor ID
5535

VSA Type
134

Length
12

Value
Opaque value

3GPP2-MIP6-CoA

MIPv6 CoA received in binding update.

This attribute is also accepted in CoA request message to be used in a currently active subscriber session.

Type
26

Vendor ID
5535

VSA Type
119

Length
16

Value
Opaque value

3GPP2-MIP6-HA

MIPv6 Home Agent address received in binding update.

Type
26

Vendor ID
5535

VSA Type
118

Length
16

Value

Opaque value

3GPP2-MIP6-HoA

MIPv6 HoA received in binding update.

Type
26

Vendor ID
5535

VSA Type
141

Length
16

Value
Opaque value

3GPP2-MIP6-HoA-Not-Authorized

Value of 1 indicates to the HA that the HoA is not authorized to be used by HA.

Type
26

Vendor ID
5535

VSA Type
120

Length
4

Value
Enumerated integer. Supported value is:

- UnAuthorized = 1

3GPP2-MIP6-Home-Address

Carries the assigned Home Address during MIP6 bootstrapping.

Type
26

Vendor ID
5535

VSA Type
129

Length

18

Value
Opaque value

3GPP2-MIP6-Home-Agent

Carries the assigned MIPv6 Home Agent address received during MIPv6 bootstrapping.

Type
26

Vendor ID
5535

VSA Type
140

Length
18

Value
Opaque value

3GPP2-MIP6-Home-Link-Prefix

Carries the assigned Home Link Prefix during MIP6 bootstrapping.

Type
26

Vendor ID
5535

VSA Type
128

Length
2–18

Value
Opaque value

3GPP2-MIP6-MAC-Mobility-Data

The hashed Mobility Data from the HA to the Home RADIUS server so that the Home RADIUS server can validate the MN-AAA authenticator.

Type
26

Vendor ID
5535

VSA Type

138

Length
20

Value
Opaque value

3GPP2-MIP6-Mesg-ID

Value of Message ID from Mobility message replay protection option in Binding Update.

Type
26

Vendor ID
5535

VSA Type
123

Length
8

Value
Opaque value

3GPP2-MIP6-Session-Key

This VSA carries the Integrity Key (IK) in its encrypted form, from the Home RADIUS server to the HA.

Type
26

Vendor ID
5535

VSA Type
121

Length
16–64

Value
Opaque value

3GPP2-MN-AAA-Removal-Indication

This attribute, when set to “Not Required”, indicates that the system, when acting as a Mobile-IP Foreign Agent, should remove the MN-FA challenge and the MN-AAA Authentication Extensions, when present, from the RRQ before relaying the RRQ to the Mobile-IP Home Agent.

Vendor ID
26

VSA Type
5535

Length
4

Value
Enumerated integer. Supported values are:

- Allowed = 0
- Not-Required = 1

3GPP2-MN-HA-Shared-Key

A shared key for MN-HA authentication. The MN-HA shared key is encrypted using a method based on MD5.

Type
26

Vendor ID
5535

VSA Type
58

Length
1–251

Value
Opaque value

3GPP2-MN-HA-Shared-Key-No-Enc

This attribute contains the MN-HA shared key in plain format.

Type
26

Vendor ID
5535

VSA Type
58

Length
1–251

Value
Opaque value

3GPP2-MN-HA-SPI

The SPI for the MN-HA authentication shared key.

Type

26

Vendor ID
5535

VSA Type
57

Length
4

Value
Unsigned integer

3GPP2-Mobile-Term-Orig-Ind

Tells whether the call is mobile originated (Call initiated from mobile side) or mobile terminated (Call initiated from external towards mobile).

Type
26

Vendor ID
5535

VSA Type
45

Length
1

Value
Enumerated integer. Supported values are:

- Mobile-Originated = 0
- Mobile-Terminated = 1

3GPP2-Number-Active-Transitions

This attribute counts the total number of non-active to active transitions by the user.

Type
26

Vendor ID
5535

VSA Type
30

Length
4

Value
Unsigned integer

3GPP2-Num-Bytes-Received-Total

This attribute counts all bytes received in the reverse direction by the HDLC layer in the PDSN.

Type
26

Vendor ID
5535

VSA Type
43

Length
4

Value
Unsigned integer

3GPP2-Num-SDB-Input

This attribute counts the total number of Short Data Burst transactions to the user.

Type
26

Vendor ID
5535

VSA Type
33

Length
4

Value
Unsigned integer

3GPP2-Num-SDB-Output

This attribute counts the total number of Short Data Burst transactions from the user.

Type
26

Vendor ID
5535

VSA Type
34

Length
4

Value
Unsigned integer

3GPP2-PMIP-Capability

This attribute specifies the AGW's PMIP capability.

Type
26

Vendor ID
5535

VSA Type
193

Length
4

Value
Enumerated integer. Supported values are:

- PMIPv4_ONLY = 1
- PMIPv6_ONLY = 2
- PMIPv4_PMIPv6 = 3

3GPP2-PMIP-NAI

This attribute specifies the PMIP NAI provided by AAA.

Type
26

Vendor ID
5535

VSA Type
192

Length
1–128

Value
Opaque value

3GPP2-PMIP-IPv4Session-Info

This attribute specifies PMIP information for IPv4 session.

Type
26

Vendor ID
5535

VSA Type
194

Length

0–160

Value

Contains the following subattributes:

VAAA-IPv4Session-HA-Addr

An IPv4 address or IPv6 Address of the local HA assigned by the AGW/VAAA for AT's IPv4 Address assignment.

Type

1

Length

0–16

Value

Opaque value

HAAA-IPv4Session-HA-Addr

An IPv4 address or IPv6 Address of the home or local HA assigned by the HAAA for AT's IPv4 Address assignment.

Type

2

Length

0–16

Value

Opaque value

PMN-HA-KEY

256 bits value of network PMIP MN-HA key.

Type

3

Length

0–32

Value

Opaque value

PMN-HA-SPI

32 bits value of network PMIP MN-HA SPI value.

Type

4

Length

4

Value

Unsigned integer

VAAA-IPv4Session-LMA-Addr

An IPv4 address or IPv6 Address of the local LMA assigned by the AGW/VAAA for AT's IPv4 Address assignment

Type
5

Length
0–16

Value
Opaque value

HAAA-IPv4Session-LMA-Addr

An IPv4 address or IPv6 Address of the home or local LMA assigned by the HAAA for AT's IPv4 Address assignment.

Type
6

Length
0–16

Value
Opaque value

3GPP2-PMIP-IPv6Session-Info

This attribute specifies the PMIP information for IPv6 session.

Type
26

Vendor ID
5535

VSA Type
195

Length
0–160

Value
Contains the following subattributes:

VAAA-IPv6Session-HA-Addr

Type
1

Length
0–16

Value
Opaque value

HAAA-IPv6Session-HA-Addr

Type
2

Length
0–16

Value
Opaque value

PMN-HA-KEY

Type
3

Length
0–32

Value
Opaque value

PMN-HA-SPI

Type
4

Length
4

Value
Unsigned integer

VAAA-IPv6Session-LMA-Addr

An IPv4 address or IPv6 Address of the local LMA assigned by the AGW/VAAA for AT's IPv6 Address assignment.

Type
5

Length
0–16

Value
Opaque value

HAAA-IPv6Session-LMA-Addr

An IPv4 address or IPv6 Address of the home or local LMA assigned by the HAAA for AT's IPv6 Address assignment.

Type
6

Length
0–16

Value
Opaque value

3GPP2-Pre-Paid-Accounting-Quota

This attribute specifies the characteristics for PrePaid accounting of the volume and/or duration of a packet data session. It should 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 should be omitted.

Type
26

Vendor ID
5535

VSA Type
90

Length
Variable, greater than 8.

Value
Contains the following nine subattributes:

Quota-Identifier

The Quota-IDentifier 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 should include a previously received Quota-Identifier.

Type
1

Length
8

Value
Unsigned integer

Volume-Quota

The optional Volume-Quota 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 accounting13. 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.

Type

2

Length

4

Value

Unsigned integer

Volume-Quota-Overflow

The optional Volume-Quota-Overflow 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.

Type

3

Length

2

Value

Unsigned integer

Volume-Threshold

The Volume-Threshold Sub-Type should 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 should be used before requesting quota update. This threshold should not be larger than the VolumeQuota.

Type

4

Length

4

Value

Unsigned integer

Volume-Threshold-Overflow

The optional Volume-Threshold-Overflow 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.

Type

5

Length

2

Value

Unsigned integer

Duration-Quota

The optional Duration-Quota Sub-Type is only present if Duration Based charging is used. In RADIUS Access-Accept message (PPS to PPC direction), it indicates the Duration (in seconds) allocated for the

session by the PrePaid server. In on-line RADIUS Access-Accept message (PPC to PPS direction), it indicates the total Duration (in seconds) since the start of the accounting session related to the QuotaID.

Type

6

Length

4

Value

Unsigned integer

Duration-Threshold

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

Type

7

Length

4

Value

Unsigned integer

Update-Reason

The Update-Reason Sub-Type should 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 should not allocate a new quota in the RADIUS Access-Accept message.

Type

8

Length

2

Value

Enumerated integer. Supported values are:

- Pre-Initialization = 1
- Initial-Request = 2
- Threshold-Reached = 3
- Quota-Reached = 4
- Remote-Forced-Disconnect = 5
- Client-Service-Termination = 6
- Main-SI-Released = 7
- Service-Instance-Not-Established = 8
- Tariff-Switch-Update = 9

- Incorrect-Quota-Type-Received = 10
- Poorly-Formed-Quota-Attribute = 11

Pre-Paid-Server

The optional, multi-value Pre-Paid-Server 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 should 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 should not change the order of the attributes.

Type
9

Length
4

Value
IPv4 address

3GPP2-Pre-Paid-Acct-Capability

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 should not use PrePaid accounting.

Type
26

Vendor ID
5535

VSA Type
91

Length
Variable, greater than 8

Value
Contains the following two subattributes:

Available-In-Client

The optional Available-In-Client Sub-Type, generated by the PrePaid client, indicates the PrePaid Accounting capabilities of the client in the PDSN or HA and should be bitmap encoded.

Type
1

Length
4

Value
Enumerated integer. Supported values are:

- Supported_None = 0
- Supported_Volume = 1 — PrePaid Accounting for Volume supported
- Supported_Duration = 2 — PrePaid Accounting for Duration supported
- Supported_Volume_And_Duration = 3 — PrePaid Accounting for Volume and Duration supported (non concurrently)

Selected-For-Session

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

Type
2

Length
4

Value
Enumerated integer. Supported values are:

- Usage_None = 0 — PrePaid Accounting not used
- Usage_Volume = 1 — Usage of PrePaid Accounting for Volume (only possible if the AvailableInClient supports PrePaid Accounting for Volume).
- Usage_Duration = 2 — Usage of PrePaid Accounting for Duration (only possible if the AvailableInClient supports PrePaid Accounting for Duration).
- Usage_Volume_And_Duration = 3 — Usage of PrePaid Accounting for Volume and Duration (non concurrent) (only possible if the AvailableInClient supports PrePaid Accounting for Volume and duration).

3GPP2-Pre-Paid-TariffSwitch

Type
26

Vendor ID
5535

VSA Type
98

Length
Compound

Value
Contains the following subattributes:

Quota-Identifier

Quota-Identifier

Type
1

Length
4

Value
Unsigned integer

Volume-Used-After-Tariff-Switch

Volume Quota used after Tariff Switch happened.

Type
2

Length
4

Value
Unsigned integer

Volume-Used-ATS-Overflow

Indicates how many times the VUATS counter has wrapped around 2^32 over the course of the service being provided.

Type
3

Length
2

Value
Unsigned integer

Tariff-Switch-Interval

Indicates Tariff Switch Interval in seconds.

Type
4

Length
4

Value
Unsigned integer

Time-Interval-After-Tariff-Switch-Update

Duration after TSI where an on-line RADIUS Access-Request is sent by PrePaid client to report VUATS before the next TS condition is triggered.

Type
5

Length
4

Value
Unsigned integer

3GPP2-QoS-Service-Opt-Profile

The attribute specifies the unauthorized packet data service options, the maximum number of simultaneous service instances of the given service option number and the total maximum number of simultaneous service instances.

Type
26

Vendor ID
5535

VSA Type
74

Length
8-247

Value
Opaque value

3GPP2-Release-Indicator

This attribute specifies reasons for sending a stop record. The enumeration of this attribute conforms to IS-835-1.

Type
26

Vendor ID
5535

VSA Type
24

Length
4

Value
Enumerated integer. Supported values are:

- Unknown = 0
- PPP-Timeout = 1
- Handoff = 2
- PPP-Termination = 3
- Mobile-IP-Registration-Failure = 4
- Abnormal-Terminations = 5
- Termation-Dueto-Resource-Mgmt = 6
- Service-Instance-Released = 7
- VolumeQuota-Reached = 8

- DurationQuota-Reached = 9
- Incompatible-Prepaid = 10
- Airlink-Parameter-Change = 11
- TOD-Timer-Expiry = 12
- Active-To-Dormant = 13
- Flow-Deactivated = 15
- PPP-Renegotiation = 1001
- MIP-Lifetime-Expired = 1002
- A11-Lifetime-Expired = 1003
- MIP-Remote-Dereg = 1004
- Tarrif-Boundary = 1006
- PPP-Renegotiation-Handoff = 1007
- MIP-Registration-Revocation = 1008

3GPP2-Release-Indicator-custom9

3GPP2 Release Indicator for custom9, reason/cause for session release.

Type

26

Vendor ID

5535

VSA Type

24

Length

4

Value

Enumerated integer. Supported values are:

- Unknown = 0
- PPP-Timeout = 1
- Handoff = 2
- PPP-Termination = 3
- Mobile-IP-Registration-Failure = 4
- PPP-Renegotiation = 5
- MIP-Registration-Revocation = 6
- VolumeQuota-Reached = 8
- DurationQuota-Reached = 9
- Incompatible-Prepaid = 10

3GPP2-Release-Indicator-Old

3GPP2 old Standard Release Indicator, reason/cause for session release.

Type
26

Vendor ID
5535

VSA Type
24

Length
4

Value
Enumerated integer. Supported values are:

- Unknown = 0
- PPP-Timeout = 1
- Handoff = 2
- PPP-Protocol-Failure = 3
- PPP-Abnormal-Release = 4
- PPP-Termination = 5
- Mobile-IP-Registration-Failure = 6
- Active-To-Dormant = 7

3GPP2-Remote-Addr-Table-Index

This attribute contains the Remote Address Table Index used to generate remote address accounting records. Supported range is 1–65535. Only one 3GPP2-Remote-Addr-Table-Index can be associated with a session.

Type
26

Vendor ID
5535

VSA Type
71

Length
4

Value
Contains the following two subattributes:

Table-Index

Table-Index

Type

1

Length

2

Value

Unsigned integer

Qualifier

Qualifier

Type

2

Length

2

Value

Enumerated integer. Supported values are:

- Exempt-From-Prepaid = 1
- Summarize-Octet-Count = 2
- Both = 3

3GPP2-Remote-IPv4-Address

This attribute allows the HA or PDSN to identify any IP address to be used for remote address-based accounting for the user. Up to 20 instances of the attribute are supported in the access response.

Type

26

Vendor ID

5535

VSA Type

59

Length

12

Value

Contains the following three subattributes:

Address

This attribute 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** subattribute to define the range of addresses to be monitored.

Type

1

Length

4

Value
IPv4 address

Netmask

This attribute contains an IPv4 address mask that defines the set of remote addresses to be used for remote address based accounting.

Type
2

Length
4

Value
IPv4 address

Qualifier

Qualifier

Type
3

Length
2

Value
Enumerated integer. Supported values are:

- Exempt-From-Prepaid = 1
- Summarize-Octet-Count = 2
- Both = 3

3GPP2-Remote-IPv4-Addr-Octets

This attribute allows the HA or PDSN to identify any IP address to be used for remote address based accounting for the user. Up to 10 instances of the attribute are supported.

Type
26

Vendor ID
5535

VSA Type
72

Length
26

Value
Contains the following subattributes:

Address

This attribute contains an IPv4 address to be used for remote address based accounting for the user. The address is used in conjunction with the Netmask subattribute to define the range of addresses to be monitored.

Type

1

Length

4

Value

IPv4 address

Netmask

This attribute contains an IPv4 address mask that defines the set of remote addresses to be used for remote address based accounting.

Type

2

Length

4

Value

An IP Netmask specified in IP address format.

Octets-Out

Indicates how many bytes have been sent to the remote address specification (corresponds to forward traffic direction).

Type

3

Length

4

Value

Unsigned integer

Octets-In

Indicates how many bytes have been received from the remote address specification (corresponds to reverse traffic direction).

Type

4

Length

4

Value

Unsigned integer

Table-Index

Table-Index

Type
5

Length
2

Value
Unsigned integer

Octets-Overflow-Out

Indicates how many times the forward octet overflow counter has wrapped around 2^32 over the course of the service being provided.

Type
6

Length
2

Value
Unsigned integer

Octets-Overflow-In

Indicates how many times the reverse octets overflow counter has wrapped around 2^32 over the course of the service being provided.

Type
7

Length
2

Value
Unsigned integer

3GPP2-Rev-Dcch-Mux-Option

This attribute specifies Reverse DCCH Mux option.

Type
26

Vendor ID
5535

VSA Type
85

Length
4

Value
Unsigned integer

3GPP2-Rev-Dcch-Rc

This attribute specifies the Radio Configuration of the Reverse Packet Data Channel.

Type
26

Vendor ID
5535

VSA Type
87

Length
4

Value
Unsigned integer

3GPP2-Reverse-Fundamental-Rate

As defined in "Wireless IP Network Standard - 3GPP2.P.S0001-A-1[4]".

Type
26

Vendor ID
5535

VSA Type
15

Length
4

Value
Unsigned integer

3GPP2-Reverse-Fundamental-RC

The format and structure of the RADIUS channel in the reverse direction. A set of forward transmission formats that are characterized by data rates, modulation characterized, and spreading rates.

Type
26

Vendor ID
5535

VSA Type
21

Length
4

Value
Unsigned integer

3GPP2-Reverse-Mux-Option

Forward direction multiplexer option.

Type
26

Vendor ID
5535

VSA Type
13

Length
4

Value
Unsigned integer

3GPP2-Reverse-Traffic-Type

Specifies the reverse traffic type.

Type
26

Vendor ID
5535

VSA Type
18

Length
4

Value
Enumerated integer. Supported values are:

- Primary = 0
- Secondary = 1

3GPP2-Rev-Pdch-Rc

This attribute displays the 3GPP2-Rev-Pdch-Rc.

Type
26

Vendor ID

5535

VSA Type
114

Length
4

Value
Unsigned integer

3GPP2-RP-Session-ID

This represents the GRE key selected by the PCF that identifies the A10 traffic for a user session.

Type
26

Vendor ID
5535

VSA Type
41

Length
4

Value
Unsigned integer

3GPP2-Rsvp-Signal-In-Count

This attribute specifies the RSVP signaling octets sent by the MS.

Type
26

Vendor ID
5535

VSA Type
162

Length
4

Value
Unsigned integer

3GPP2-Rsvp-Signal-In-Packets

This attribute specifies the Number of RSVP signaling packets sent by the MS.

Type
26

Vendor ID
5535

VSA Type
164

Length
4

Value
Unsigned integer

3GPP2-Rsvp-Signal-Out-Count

This attribute specifies the RSVP signaling octets sent to the MS.

Type
26

Vendor ID
5535

VSA Type
163

Length
4

Value
Unsigned integer

3GPP2-Rsvp-Signal-Out-Packets

This attribute specifies the Number of RSVP signaling packets sent to the MS.

Type
26

Vendor ID
5535

VSA Type
165

Length
4

Value
Unsigned integer

3GPP2-S

This attribute contains the 'S' secret parameter used to make the IKE pre-shared secret.

Type

26

Vendor ID
5535

VSA Type
54

Length
1–247

Value
A binary string of the value of 'S'.

3GPP2-SDB-Input-Octets

This attribute counts the total number of octets sent to the user via Short Data Bursts.

Type
26

Vendor ID
5535

VSA Type
31

Length
4

Value
Unsigned integer

3GPP2-SDB-Output-Octets

This attribute counts the total number of octets sent by the user via Short Data Bursts.

Type
26

Vendor ID
5535

VSA Type
32

Length
4

Value
Unsigned integer

3GPP2-Security-Level

This attribute indicates the type of security that the home network mandates on the visited network.

Type
26

Vendor ID
5535

VSA Type
2

Length
4

Value
Enumerated integer. Supported values are:

- IPSec = 3—IPSec for tunnels and registration messages
- None = 4

3GPP2-Service-Option

This attribute indicates the service option used for CDMA air interface.

Type
26

Vendor ID
5535

VSA Type
16

Length
4

Value
Enumerated integer. Supported values are:

- HSPD = 0x21
- HRPD = 0x3b
- LLAROHC = 0x3d
- HRPD-AUX = 0x40
- HRPD-AUX-IP = 0x43
- eHRPD = 0x252
- LTE = 0x253
- UTRAN = 0x254
- GERAN = 0x255
- WIFI = 0x806c

3GPP2-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.

Type
26

Vendor ID
5535

VSA Type
74

Length
4

Value
Unsigned integer Supported values are:

- 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 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.

3GPP2-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 should be included.

Type
26

Vendor ID
5535

VSA Type
94

Length
4

Value
Contains two subattributes:

SR-ID

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

Type
1

Length

2

Value

Unsigned integer

Main-SI-Indicator

Only included for the main service instance.

Type

2

Length

2

Value

Enumerated integer. Supported value is:

- Main-SI = 1

3GPP2-Serving-PCF

IP address of the serving PCF.

Type

26

Vendor ID

5535

VSA Type

9

Length

4

Value

IPv4 address

3GPP2-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.

Type

26

Vendor ID

5535

VSA Type

48

Length

4

Value

Enumerated integer. Supported values are:

- False = 0
- True = 1

3GPP2-Session-Term-Capability

This attribute should be included in a RADIUS Access-request message to the Home RADIUS server and should 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 should also be included in the RADIUS Access-Accept message and should contain the preferred resource management mechanism by the home network, which should be used for the session and may include values 1 to 3.

Type

26

Vendor ID

5535

VSA Type

88

Length

4

Value

Enumerated integer. Supported values are:

- Only_Dynamic_Auth_Extn_to_Radius = 0x00000001 = 1
- Only_Reg_Revocation_in_MIP = 0x00000002 = 2
- Both_Dynamic_Auth_And_Reg_Revocation_in_MIP = 0x00000003 = 3

3GPP2-S-Key

This attribute contains the HA IKE key in encrypted format.

Type

26

Vendor ID

5535

VSA Type

54

Length

1–247

Value

Opaque value

3GPP2-S-Lifetime

This attribute contains the lifetime of the 'S' secret parameter used to make the IKE pre-shared secret. indicating the time in seconds since January 1, 1970 00:00 UTC. Note that this is equivalent to the UNIX operating system expression of time.

Type
26

Vendor ID
5535

VSA Type
55

Length
4

Value
Unsigned integer

3GPP2-S-Request

This attribute indicates whether the HA requests a shared secret 'S'.

Type
26

Vendor ID
5535

VSA Type
55

Length
4

Value
Enumerated integer. Supported values are:

- No = 0
- Yes = 1 — 'S' secret requested for IKE

3GPP2-Subnet

This attribute specifies the Subnet information of the HRPD RAN.

Type
26

Vendor ID
5535

VSA Type
108

Value

Contains the following subattributes:

Rev-A-Subnet

This attribute specifies the Subnet information of the HRPD RAN.

Type
1

Length
In StarOS 8.1 and earlier: 1-18; In StarOS 9.0 and later: 1-19

Value
Opaque value

Rev-A-Sector-Id

This attribute specifies the Sector ID information of the HRPD RAN.

Type
2

Length
In StarOS 8.1 and earlier: 1-19; In StarOS 9.0 and later: 1-18

Value
Opaque value

3GPP2-S-Unencrypted

This attribute contains the HA IKE key in plain format.

Type
26

Vendor ID
5535

VSA Type
54

Length
1–247

Value
Opaque value

3GPP2-User-Zone

This attribute describes the Tiered Services user zone. The least significant 16 bits are the user zone ID, the next significant 15 bits are the user zone system ID, and the most significant bit is zero.

Type
26

Vendor ID
5535

VSA Type
11

Length
4

Value
Unsigned integer

AAA-Session-ID

A unique per realm identifier assigned to WiMAX session by the Home network during network entry.

This attribute is also accepted in CoA request message to be used in a currently active subscriber session.

Type
26

Vendor ID
24757

VSA Type
4

Length
1–246

Value
Opaque value

Access-In-Subs

This attribute is used in a custom dictionary, and the VSA type is not standard. Opaque 1 byte value received in Access Accept. This will be included in accounting messages for this session.

Type
136

Vendor ID
5535 (Reusing the 3GPP2 VID in a non-standard way.)

VSA Type
224

Length
1

Value
Opaque value

Acct-Authentic

This attribute is included in Accounting-Request packets to indicate how the session was authenticated (RADIUS or locally).

Type

45

Vendor ID

N/A

VSA Type

N/A

Length

4

Value

Enumerated integer. Supported values are:

- None = 0 — Authentication was not required for the session
- RADIUS = 1 — The session was authenticated via RADIUS
- Local = 2 — The session was authenticated locally
- Remote = 3
- Diameter = 4

Acct-Delay-Time

This attribute indicates how many seconds the chassis has been trying to send this record for. The standard behavior is that this AVP will be visible in the Accounting Request message only if it has a non-zero value.

Type

41

Vendor ID

N/A

VSA Type

N/A

Length

4

Value

Unsigned integer

Acct-Input-Gigawords

This attribute indicates how many times the Acct-Input-Octets attribute has wrapped within its 32-bit field length. In effect, the number of octets received is a 64-bit integer, with this attribute representing the high 32 bits, and the Acct-Input-Octets attribute representing the low 32 bits. This attribute is not included unless it has a non-zero value.

Type

52

Vendor ID
N/A

VSA Type
N/A

Length
4

Value
Unsigned integer

Acct-Input-Octets

This attribute indicates how many octets have been received in the PPP session. Since the value field is 32 bits, it is possible that the number of octets will exceed the 32-bit field length. If this happens, this attribute will "wrap" back to 0. Each time the "wrap" occurs, the **Acct-Input-Gigawords** attribute will be incremented. In effect, the number of octets received is a 64-bit integer, with the **Acct-Input-Gigawords** attribute representing the high 32 bits, and this attribute representing the low 32 bits.

Important: RADIUS reports what is going through the air interface. For uplink traffic, it reports all packets including those dropped/filtered by ACS. For downlink traffic, it reports what is going to the MS after ACS filtering. When DCCA is enabled, packets may be dropped due to unavailability of quota. Therefore, for pre-paid calls, accounting attributes "Acct-Input-Octets" and "Acct-Output-Octets" will not match totals of "dataVolumeGPRSUplink" and "dataVolumeGPRSDownlink" respectively from generated eG-CDRs.

Type
42

Vendor ID
N/A

VSA Type
N/A

Length
4

Value
Unsigned integer

Acct-Input-Packets

This attribute indicates how many PPP packets have been received during the session.

Type
47

Vendor ID
N/A

VSA Type
N/A

Length

4

Value

Unsigned integer

Acct-Interim-Interval

This attribute indicates the time (in seconds) between updates to session counters (log file on RADIUS or AAA event log) during the session. Note that the setting for this attribute always takes precedence over interim interval settings configured on the system.

Caution: To avoid increasing network traffic unnecessarily and potentially reducing network and system performance, do not set this parameter to a value less than 50.

If this AVP is present in Access Accept message, the locally configured RADIUS accounting interim interval value in AAA group will be overriden. If there are no values configured in the RADIUS and AAA group the accounting interim is disabled.

Type

85

Vendor ID

N/A

VSA Type

N/A

Length

4

Value

Unsigned integer

Acct-Multi-Session-Id

This attribute is a unique Accounting ID to make it easy to link together multiple related sessions in a log file. Each session linked together would have a unique **Acct-Session-Id** but the same **Acct-Multi-Session-Id**. It is strongly recommended that the **Acct-Multi-Session-Id** contain UTF-8 encoded characters.

Type

50

Vendor ID

N/A

VSA Type

N/A

Length

1–253

Value

String

Acct-Output-Gigawords

This attribute indicates how many times the **Acct-Output-Octets** attribute has wrapped within its 32-bit field length. In effect, the number of octets received is a 64-bit integer, with this attribute representing the high 32 bits, and the **Acct-Output-Octets** attribute representing the low 32 bits. This attribute is not included unless it has a non-zero value.

Type
53

Vendor ID
N/A

VSA Type
N/A

Length
4

Value
Unsigned integer

Acct-Output-Octets

This attribute indicates how many octets have been sent in the PPP session. Since the value field is 32 bits, it is possible that the number of octets will exceed the 32-bit field length. If this happens, this attribute will "wrap" back to 0. Each time the "wrap" occurs, the **Acct-Output-Gigawords** attribute will be incremented. In effect, the number of octets received is a 64-bit integer, with the **Acct-Output-Gigawords** attribute representing the high 32 bits, and this attribute representing the low 32 bits.

Important: RADIUS reports what is going through the air interface. For uplink traffic, it reports all packets including those dropped/filtered by ACS. For downlink traffic, it reports what is going to the MS after ACS filtering. When DCCA is enabled, packets may be dropped due to unavailability of quota. Therefore, for pre-paid calls, accounting attributes "Acct-Input-Octets" and "Acct-Output-Octets" will not match totals of "dataVolumeGPRSUplink" and "dataVolumeGPRSDownlink" respectively from generated eG-CDRs.

Type
43

Vendor ID
N/A

VSA Type
N/A

Length
4

Value
Unsigned integer

Acct-Output-Packets

This attribute indicates how many PPP packets have been sent during the session.

Type
48

Vendor ID
N/A

VSA Type
N/A

Length
4

Value
Unsigned integer

Acct-Session-Id

This attribute is a session ID. Combined with the identification of the chassis (NAS-IP-Address or NAS-Identifier), this uniquely describes a session. For a given chassis, there will never be another session (even across boots) with this same session ID. The **Acct-Session-ID** AVP is sent on both Gx and Gy messages.

This attribute is also accepted in CoA request and response messages to be used in a currently active subscriber session.

Type
44

Vendor ID
N/A

VSA Type
N/A

Length
1–253

Value
String

Acct-Session-Id-Long

This attribute contains long format account session ID. This is supported only for custom2 dictionary.

Type
44

Vendor ID
N/A

VSA Type
N/A

Length
1–253

Value
String

Acct-Session-Time

This attribute indicates the duration of the session in seconds.

Type
46

Vendor ID
N/A

VSA Type
N/A

Length
4

Value
Integer

Acct-Status-Type

This attribute indicates the event for the session.

Type
40

Vendor ID
N/A

VSA Type
N/A

Length
4

Value
Enumerated integer. Supported values are:

- Start = 1 — The session has started, or the service has been delivered
- Stop = 2 — The session has completed, or the user has released service
- Interim-Update = 3 — The session or service is still ongoing. Usage details are given in other RADIUS attributes.
- Accounting-On = 7 — The chassis sends this message to the RADIUS server upon boot.
- Accounting-Off = 8 — The chassis sends this message to the RADIUS server when it shuts down in a normal fashion.
- Tunnel-Start = 9
- Tunnel-Stop = 10
- Tunnel-Reject = 11
- Tunnel-Link-Start = 12
- Tunnel-Link-Stop = 13
- Tunnel-Link-Reject = 14

- Failed = 15

Acct-Termination-Cause

This attribute indicates why the session was terminated.

This attribute is also accepted in CoA response message to be used in a currently active subscriber session.

Type

49

Vendor ID

N/A

VSA Type

N/A

Length

4

Value

Enumerated integer. Supported values are:

- User_Request = 1 — The user requested termination
- Lost_Carrier = 2
- Lost_Service = 3 — The chassis session terminated abnormally
- Idle_Timeout = 4 — The session idle timeout expired
- Session_Timeout = 5 — The session timeout expired
- Admin_Reset = 6 — The Service Provisioning system terminated the session
- Admin_Reboot = 7 — The Service Provisioning system rebooted the chassis
- Port_Error = 8 — PAC error, requiring the session to be terminated
- NAS_Error = 9 — Error other than PAC error, requiring session to be terminated
- NAS_Request = 10 — Session terminated for any other non error reason by PDSN
- NAS_Reboot = 11 — The chassis rebooted abnormally.
- Port_Unneeded = 12
- Port_Preempted = 13 — Duplicate Home Address Requested. Call aborted.
- Port_Suspended = 14 — PPP restart or RP-A11 disconnect without active Stop conditions
- Service_Unavailable = 15 — The chassis could not provide the service requested
- Callback = 16
- User_Error = 17 — A non-compliant PPP client required the chassis to terminate the session
- Host_Request = 18 — Inter-PDSN handoff, Active->Dormant transition, PPP re-nego-tiation, Active Start Parameter change, Accounting Tariff Boundary
- Supplicant_Restart = 19
- Reauthentication_Failure = 20
- Port_Reinitialized = 21
- Port_Administratively_Disabled = 22

- Inter-PDSN-Handoff = 99 — Customer-specific implementation
- Long-Duration-Timeout = 1001
- Invalid-Source-Address = 1002
- Duplicate-IMSI = 1003
- Interim-Update = 1004
- Hotlining-Status-Change=1005

BU-CoA-Ipv6

The IPv6 address extracted from the Careof Address field in the BU and sent in Access Request from HA for WiMAX call.

Type
26

Vendor ID
24757

VSA Type
51

Length
16

Value
Opaque value

Callback-Id

This attribute contains the name of the place to be called, to be interpreted by NAS.

Type
20

Length
1-253

Value
Opaque value

Called-Station-ID

For PDSN, the value of this attribute is a single zero byte for custom6/7/8 dictionaries. For other dictionaries, this attribute will not be present for PDSN calls.

Type
30

Vendor ID
N/A

VSA Type
N/A

Length
1–253

Value
For GGSN, a UTF-8 encoded string identifying the target network. For PDSN, a single zero byte.

Calling-Station-Id

This attribute indicates the Mobile Station Identifier in PDSN, and MSISDN in GGSN.

This attribute is also accepted in CoA request message to be used in a currently active subscriber session.

Type
31

Vendor ID
N/A

VSA Type
N/A

Length
1–15

Value
ASCII string

Calling-Subscriber-Type

Opaque one byte value received from customer RADIUS server in access request. We need to retain this value and return it back in all future accounting messages. Used in custom dictionary.

Type
136

Vendor ID
5535 (Reusing the 3GPP2 VID in a non-standard way.)

VSA Type
218

Length
1

Value
The system does not interpret this value, it is only copied in accounting messages.

CHAP-Challenge

This attribute contains the CHAP Challenge that was sent by the chassis to the other end of the PPP link, when CHAP authentication is being used.

Type
60

Vendor ID
N/A

VSA Type
N/A

Length
1-253

Value
Opaque value

CHAP-Password

This attribute contains the CHAP ID and the CHAP Response when CHAP authentication is used.

Type
3

Vendor ID
N/A

VSA Type
N/A

Length
17

Value
Bit string. First byte is the CHAP ID. Next 16 bytes is the CHAP Response.

Charging-Id

Same as **3GPP-Charging-ID** standard attribute; non-standard behavior for use in custom dictionary.

Type
225

Vendor ID
N/A

VSA Type
N/A

Length
4

Value
Unsigned integer

Class

This attribute may be sent by the RADIUS server to the chassis in an Access-Accept packet. The chassis will include this attribute in all subsequent Accounting-Request messages sent to the RADIUS Accounting server for this user's session. This attribute is included to support the RADIUS protocol and should not be human-interpreted.

Type
25

Vendor ID
N/A

VSA Type
N/A

Length
1–253

Value
The format of the value is server-dependent. The chassis will interpret it as simply a bit string to be reflected in Accounting-Request messages.

CUI

Chargeable User Identity is a unique temporary handle to the user responsible for paying bill. Set to NULL in Initial Access request and set to value sent by AAA in subsequent messages.

Type
89

Vendor ID
N/A

VSA Type
N/A

Length
1–253

Value
Opaque value

DHCP-RK

DHCP-RK is a 160-bit randomly generated for every DHCP server, the DHCP Key is derived from this.

Type
26

Vendor ID
24757

VSA Type
40

Length
1–250

Value
Opaque value

DHCP-RK-Key-ID

An integer uniquely identifying the DHCP-RK within the scope of a single DHCP server.

Type
26

Vendor ID
24757

VSA Type
41

Length
4

Value
Unsigned Integer

DHCP-RK-Lifetime

Lifetime of the DHCP-RK and derived keys.

Type
26

Vendor ID
24757

VSA Type
42

Length
4

Value
Unsigned Integer

DHCPMSG-Server-IP

The IPv4 address of the DHCP server.

Type
26

Vendor ID
24757

VSA Type
43

Length
4

Value
IPv4 address

Digest-AKA-Auts

This attribute holds the auts parameter that is used in the Digest AKA calculation.

Type
118

Vendor ID
N/A

VSA Type
N/A

Length
0-253

Value
ASCII string

Digest-Algorithm

This parameter holds the algorithm parameter that influences the HTTP Digest calculation.

Type
111

Vendor ID
N/A

VSA Type
N/A

Length
0–253

Value
Opaque value

Digest-Auth-Param

This attribute is a placeholder for future extensions.

Type
117

Vendor ID
N/A

VSA Type
N/A

Length
0–253

Value
Opaque value

Digest-CNonce

This attribute holds the client nonce that is used in the digest calculation.

Type
113

Vendor ID
N/A

VSA Type
N/A

Length
0–253

Value
Opaque value

Digest-Domain

This attribute consists of single URI that defines a protection space component.

Type
119

Vendor ID
N/A

VSA Type
N/A

Length
0-256

Value
Opaque value

Digest-Entity-Body-Hash

This attribute holds the hexadecimal representation of H(entity-body). This hash is required when quality of protection is set to “auth-int”.

Type
112

Vendor ID
N/A

VSA Type
N/A

Length
0-253

Value
Hexadecimal string

Digest-HA1

This attribute contains the hexadecimal representation on H(A1) as described in RFC 2617.

Type
121

Vendor ID
N/A

VSA Type
N/A

Length
0-253

Value
ASCII string

Digest-Method

This attribute holds the method value to be used in the HTTP digest calculation.

Type
108

Vendor ID
N/A

VSA Type
N/A

Length
0-253

Value
ASCII string

Digest-Nextnonce

This attribute holds a nonce to be used in the HTTP digest calculation.

Type
107

Vendor ID
N/A

VSA Type
N/A

Length
0-253

Value
Hexadecimal string

Digest-Nonce-Count

This attribute holds the nonce count parameter that is used to detect replay attacks.

Type
114

Vendor ID
N/A

VSA Type
N/A

Length
0-253

Value
ASCII string

Digest-Opaque

This attribute holds the opaque parameter that is passed to the SIP client.

Type
116

Vendor ID
N/A

VSA Type
N/A

Length
0-253

Value
ASCII string

Digest-Qop

This attribute holds the quality of protection parameter that influences the HTTP digest calculation.

Type
110

Vendor ID
N/A

VSA Type
N/A

Length
0-253

Value
ASCII string

Digest-Realm

This attribute describes a protection space component of the RADIUS server.

Type
104

Vendor ID
N/A

VSA Type
N/A

Length
0-253

Value
ASCII string

Digest-Response-Auth

This enables the RADIUS server to prove possession of the password.

Type
106

Vendor ID
N/A

VSA Type
N/A

Length
0-253

Value
Hexadecimal string

Digest-Stale

This attribute is sent by RADIUS server in order to notify the RADIUS client whether it has accepted a nonce.

Type
120

Vendor ID
N/A

VSA Type
N/A

Length
0-253

Value
ASCII string. The following are the valid values for this attribute:

- False = 0
- True = 1

Digest-URI

This attribute is used to transport the contents of the URI of the SIP request.

Type
109

Vendor ID
N/A

VSA Type
N/A

Length
0-253

Value
ASCII string

Digest-Username

This attribute holds the user name used in the HTTP Digest calculation.

Type
115

Vendor ID
N/A

VSA Type
N/A

Length
0-253

Value
ASCII string

DNS

IPv4/IPv6 address of the DNS server to be conveyed to the MS via DHCP.

Type
26

Vendor ID
24757

VSA Type
52

Length

4–16

Value

Opaque value

EAP-Message

The EAP exchanged transported over RADIUS.

Type

79

Vendor ID

N/A

VSA Type

N/A

Length

0-253

Value

Opaque value

Error-Cause

It is possible that the NAS cannot honor Disconnect-Request or CoA-Request messages for some reason. The Error-Cause Attribute provides more detail on the cause of the problem. It may be included within Disconnect-ACK, Disconnect-NAK, and CoA-NAK messages.

This attribute is also accepted in CoA response message to be used in a currently active subscriber session.

Type

101

Vendor ID

N/A

VSA Type

N/A

Length

4

Value

Enumerated integer. Supported values are:

- Residual-Session-Context-Remove = 201
- Invalid-EAP-Packet = 202
- Unsupported-Attribute = 401
- Missing-Attribute = 402
- NAS-Identification-Mismatch = 403
- Invalid-Request = 404
- Unsupported-Service = 405

- Unsupported-Extension = 406
- Administratively-Prohibited = 501
- Request-Not-Routable = 502
- Session-Context-Not-Found = 503
- Session-Context-Not-Removable = 504
- Other-Proxy-Processing-Error = 505
- Resources-Unavailable = 506
- Request-Initiated = 507
- Session-Context-Not-Removable-Dormant = 599

Event-Timestamp

This attribute is a timestamp of when the event being logged occurred, indicating the time in seconds since January 1, 1970 00:00 UTC. Note that this is equivalent to the UNIX operating system expression of time.

This attribute is also accepted in CoA request and response messages to be used in a currently active subscriber session.

Type
55

Vendor ID
N/A

VSA Type
N/A

Length
4

Value
Unsigned integer

FA-RK-KEY

This attribute contains the encrypted FA-RK-KEY. The FA-RK determined during EAP authentication by the RADIUS server and passed on to the NAS upon successful EAP authentication. It is used by the NAS to generate MN-FA keys.

Type
26

Vendor ID
24757

VSA Type
14

Length
1–244

Value
Opaque value

FA-RK-SPI

SPI used for the FA-RK associated with FA-RK Key for generating MN-FA key for WiMAX call

Type
26

Vendor ID
24757

VSA Type
61

Length
4

Value
Unsigned integer

Filter-Id

This attribute identifies the IP access-list/filter by name.

This attribute is also accepted in CoA request message to be used in a currently active subscriber session.

By default, a Filter-Id is applied in both directions. To apply a filter in a single direction, add the prefix “in:” or “out:” to the access-list name in the Filter-Id. Syntax:

in:<filter_name>

This assigns an input filter identified by filter_name

out:<filter_name>

This assigns an output filter identified by filter_name <filter_name>

If the Filter-Id value in the Access Accept message is invalid this value will not be applied to the session.

If this AVP is missing in the Access Accept message the value configured in the APN / subscriber template, if any, will be taken.

Type
11

Vendor ID
N/A

VSA Type
N/A

Length
1–253

Value
ASCII string

Framed-Compression

This attribute indicates the compression protocol to be used.

Type
13

Vendor ID
N/A

VSA Type
N/A

Length
4

Value
Enumerated integer. Supported values are:

- None = 0 — Do not use compression
- VJ_TCP_IP_header_compression = 1 — Use VJ TCP/IP header compression
- IPX_header_compression = 2
- Stac_LZS_compressions = 3 — Use Stac-LZS compression

Framed-Interface-Id

This attribute contains the value of IPv6 Interface ID.

This attribute is also accepted in CoA request message to be used in a currently active subscriber session.

Type
96

Vendor ID
N/A

VSA Type
N/A

Length
8

Value
Opaque value

Framed-IP-Address

This attribute indicates the IP address to be configured for the user.

This attribute is also accepted in CoA request and response messages to be used in a currently active subscriber session.

Type
8

Vendor ID
N/A

VSA Type
N/A

Length
4

Value
An IP address as it would appear in the source or destination field of an IP header. Special values are:

- 255.255.255.255 — User selected address
- 255.255.255.254 — Assign address from a pool (see Framed-Pool and SN-IP-Pool-Name)

Framed-IP-Netmask

This attribute indicates the IP netmask to be configured for the session when the PPP connection is to a router servicing a network.

Type
9

Vendor ID
N/A

VSA Type
N/A

Length
4

Value
An IP netmask specified in IPv4 address format.

Framed-IPv6-Pool

This attribute contains the IPv6 pool name.

Type
100

Vendor ID
N/A

VSA Type
N/A

Length
1–253

Value
String

Framed-IPv6-Prefix

This attribute contains IPv6 prefix.

This attribute is also accepted in CoA request message to be used in a currently active subscriber session.

Type

97

Vendor ID
N/A

VSA Type
N/A

Length
2–18

Value
Opaque value

Framed-MTU

This attribute indicates the Maximum Transmission Unit that was configured for the PPP session.

Type
12

Vendor ID
N/A

VSA Type
N/A

Length
4

Value
Integer. Supported values are from 64 through 4096.

Framed-Pool

This standard attribute indicates the name of the IP pool from which an IP address should be allocated to the subscriber. Also, see **SN-IP-Pool-Name**, which is a vendor-specific attribute accomplishing the same.

Type
88

Vendor ID
N/A

VSA Type
N/A

Length
1–253

Value
String

Framed-Protocol

This attribute describes the framed protocol that the user is granted to use (Access-Accept), when Service-Type = Framed. Note that PPP is the only framed protocol supported.

Type

7

Vendor ID

N/A

VSA Type

N/A

Length

4

Value

Enumerated integer. Supported values are:

- PPP = 1
- SLIP = 2
- ARAP = 3
- Gandalf_proprietary___ = 4
- Xylogics_proprietary_IPX_SLIP = 5
- X_75_Synchronous = 6
- GPRS_PDP_Context = 7

Framed-Route

This attribute specifies the subnet route to be installed in GGSN for the mobile router.

If the GGSN receives a packet with a destination address matching the Framed-Route, the packet is forwarded to the mobile router through the associated PDP context.

This attribute is accepted in the Access-Accept message and can appear multiple times. The format of value to be assigned to the Framed-Route attribute should be as follows:

<dest-ip>/<net-mask> <gateway-ip> hops

- or -

<dest-ip> <subnet-mask> <gateway-ip> hops

For example, Framed-Route = 40.40.41.0/24

Important: Note that the *<gateway-ip>* and *hops* are optional.

If the *gateway_ip* is 0.0.0.0 then the mobile node's (user's) IP is considered as the Gateway IP.

Important: The maximum number of framed routes allowed per subscriber is 10.

These framed routes are established at the time of call setup and deleted when the call is terminated.

Type
61

Vendor ID
N/A

VSA Type
N/A

Length
In StarOS 8.x and earlier: 16; in StarOS 9.0 and later: 1–64

Value
Opaque value

Geographical-Location

This attribute contains the information of geographical location as reported by HNB.

Type
26

Vendor ID
9

VSA Type
114

Length
10

Value
Opaque value

GGSN-GTP-IP-Address

Same as **3GPP-GGSN-Address** standard attribute; non-standard behavior for use in custom dictionary.

Type
230

Vendor ID
N/A

VSA Type
N/A

Length
4

Value
IPv4 address

HA-IP-MIP4

IPv4 address of the HA.

Type
26

Vendor ID
24757

VSA Type
6

Length
4

Value
IPv4 address

HA-IP-MIP6

IPv6 address of the HA for CMIP4.

Type
26

Vendor ID
24757

VSA Type
7

Length
4–16

Value
Opaque value

HA-RK-KEY

The HA-RK-KEY determined during EAP authentication by the RADIUS server and passed to the NAS upon successful EAP authentication. It is used by the NAS to generate FA-HA keys.

Type
26

Vendor ID
24757

VSA Type
15

Length
1–244

Value
Opaque value

HA-RK-Lifetime

Lifetime of the HA-RK and derived keys.

Type
26

Vendor ID
24757

VSA Type
17

Length
4

Value
Unsigned integer

HA-RK-SPI

The SPI associated with the HA-RK for generating MN-HA key for WiMAX call.

Type
26

Vendor ID
24757

VSA Type
16

Length
4

Value
Unsigned integer

hLMA-IPv6-PMIP6

MIPv6 Home Agent address received in binding update.

Type
26

Vendor ID
24757

VSA Type
127

Length
2

Value
Opaque value

HNB-Internet-Information

This attribute contains public IP address (either IPv4 or IPv6 address) of HNB assigned through the broadband connection.

Type
26

Vendor ID
9

VSA Type
115

Length
4–16

Value
Opaque value

HNB-Parameters

This attribute contains PLMN ID, LAC, RAC, SAC, and Cell ID of the HNB as reported to HNB-GW in RADIUS Access-Request during authentication.

Type
26

Vendor ID
9

VSA Type
112

Length
12

Value
Opaque value

Hotline-Indicator

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

This attribute is also accepted in CoA request message to be used in a currently active subscriber session.

Type
26

Vendor ID
24757

VSA Type
24

Length
In 10.2 and earlier releases: 1–246

In 11.0 and later releases: 1–54

Value

In 10.2 and earlier releases: Opaque value

In 11.0 and later releases: String

Hotline-Profile-ID

A unique identifier of a hotline profile to be applied to the session.

This attribute is also accepted in CoA request message to be used in a currently active subscriber session.

Type

26

Vendor ID

24757

VSA Type

53

Length

In 10.2 and earlier releases: 1–246

In 11.0 and later releases: 1–64

Value

In 10.2 and earlier releases: Opaque value

In 11.0 and later releases: String

Hotline-Session-Timer

The time period, in seconds, the session can remain hotlined.

This attribute is also accepted in CoA request message to be used in a currently active subscriber session.

Type

26

Vendor ID

24757

VSA Type

56

Length

4

Value

Unsigned Integer

HTTP-Redirection-Rule

An HTTP redirection rule.

This attribute is also accepted in CoA request message to be used in a currently active subscriber session.

Type
26

Vendor ID
24757

VSA Type
54

Length
1–246

Value
Opaque value

Idle-Timeout

This attribute sets the maximum idle session time, in seconds. A session is idle when there is no IP traffic on the link. After the connection has been idle for the indicated amount of time, the chassis will tear down the session.

Type
28

Vendor ID
N/A

VSA Type
N/A

Length
4

Value
Integer

IMSI

Same as **3GPP-IMSI** standard attribute; non-standard behavior for use in custom dictionary.

Type
224

Vendor ID
N/A

VSA Type
N/A

Length
1–6

Value
ASCII string

IMSI-MCC-MNC

Same as **3GPP-IMSI-Mcc-Mnc** standard attribute; non-standard behavior for use in custom dictionary.

Type
226

Vendor ID
N/A

VSA Type
N/A

Length
1–6

Value
String

In-Packet-Period

Opaque 4 byte value received in Access Accept. This will be included in accounting messages for the session. Used in custom dictionary.

Type
136

Vendor ID
5535 (Reusing the 3GPP2 VID in a non-standard way.)

VSA Type
247

Length
Unsigned integer

IP-Redirection-Rule

This attribute is used to specify which packet flow to redirect and where to redirect it.

Type
26

Vendor ID
24757

VSA Type
55

Length
1–246

Value
Opaque value

Macro-Coverage-Information

This attribute contains the marco coverage information as reported by HNB which could be a GERAN or UTRAN cell information.

Type
26

Vendor ID
9

VSA Type
113

Length
8–11

Value
Opaque value

MN-HA-MIP4-KEY

MN-HA key for SPI value in the Access request if present.

Type
26

Vendor ID
24757

VSA Type
10

Length
1–244

Value
Opaque value

MN-HA-MIP4-SPI

SPI associated with the MN-HA-MIP4 key. This attribute needs to be sent in the Access Request to fetch the corresponding MN-HA keys.

Type
26

Vendor ID
24757

VSA Type
11

Length
4

Value

Unsigned integer

MN-HA-MIP6-KEY

Used to calculate AUTH for MIP6 BU during PMIP6 on ASN and to validate and compute AUTH for MIP6 Binding Answer on HA.

Type
26

Vendor ID
24757

VSA Type
12

Length
1–244

Value
Opaque value

MN-HA-MIP6-SPI

SPI associated with the MN-HA-MIP6-KEY.

Type
26

Vendor ID
24757

VSA Type
12

Length
4

Value
Unsigned integer

MSISDN

MSIDSN of the call. Used in custom dictionary.

Type
136

Vendor ID
5535 (Reusing the 3GPP2 VID in a non-standard way.)

VSA Type
222

Length

1-256

Value

String

MSK

The Master Session Key determined during EAP authentication by the RADIUS server and passed to the NAS upon successful EAP authentication.

Type

26

Vendor ID

24757

VSA Type

5

Length

1–246

Value

Opaque value

NAS-Filter-Rule

Indicates filter rules to be applied for the user.

Type

92

Vendor ID

N/A

VSA Type

N/A

Length

1–246

Value

Opaque value

NAS-Identifier

This attribute identifies the NAS generating the record.

This attribute is also accepted in CoA request message to be used in a currently active subscriber session.

Type

32

Vendor ID

N/A

VSA Type
N/A

Length
1–253

Value
ASCII string

NAS-IP-Address

This attribute identifies the serving NAS.

This attribute is also accepted in CoA request message to be used in a currently active subscriber session.

Type
4

Vendor ID
N/A

VSA Type
N/A

Length
4

Value
An IP address as it would appear in the source or destination field of an IP header.

NAS-Port

This attribute describes the assigned resource number to the user session. It is guaranteed to be unique at a particular instance in time for a particular chassis.

Type
5

Vendor ID
N/A

VSA Type
N/A

Length
4

Value
Unsigned integer

NAS-Port-Type

This attribute indicates the physical layer that the session is using.

Type

61

Vendor ID

N/A

VSA Type

N/A

Length

4

Value

Enumerated integer. Supported values are:

- Async = 0
- Sync = 1
- ISDN_Sync = 2
- ISDN_Async_V_120 = 3
- ISDN_Async_V_110 = 4
- Virtual = 5 – MGMT
- PIAFS = 6
- HDLC_Clear_Channel = 7
- X_25 = 8
- X_75 = 9
- G_3_Fax = 10
- SDSL_Symmetric_DSL = 11
- ADSL_CAP = 12
- ADSL_DMT = 13
- IDSL = 14
- Ethernet = 15
- xDSL = 16
- Cable = 17
- Wireless_Other = 18 – Other wireless
- Wireless_IEEE_802_11 = 19 – Wireless IEEE 802.11
- Token_Ring = 20
- FDDI = 21
- Wireless_CDMA2000 = 22
- Wireless_UMTS = 23
- HRPD = 24 — High Rate Packet Data. HRPD is only available if included in the custom dictionary. None of the standard dictionaries include it.
- IAPP = 25
- FTTP = 26
- Wireless_IEEE_802_16 = 27

- Wireless_IEEE_802_20 = 28
- Wireless_IEEE_802_22 = 29
- Wireless_XGP=36

PMIP-Authenticated-Nwk-Id

The real user identifier returned by hAAA after successful authentication.

Type
26

Vendor ID
24757

VSA Type
In 10.2 and earlier releases: 58

In 11.0 and later releases: 78

Length
1–246

Value
Opaque value

PMIP6-RK-KEY

The PMIP6-RK-KEY sent by the RADIUS Server to the ASN and hCSN LMA for PMIP6. It is used to calculate the individual LMA-MAG key being the base for PBU and PBA messages protection through mobility authentication options.

Type
26

Vendor ID
24757

VSA Type
131

Length
1–251

Value
Opaque value

PMIP6-RK-SPI

The SPI associated with the PMIP6-RK-KEY.

Type
26

Vendor ID
24757

VSA Type
132

Length
1–251

Value
Opaque value

PMIP6-Service-Info

Indicates which PMIPv6 features are supported and enabled on ASN/LMA.

Type
26

Vendor ID
24757

VSA Type
126

Length
2

Value
Unsigned Integer

Price-Plan

Opaque 1 byte value received from customer RADIUS server in access request. We need to retain this value and return it back in all future accounting messages. Used in custom dictionary.

Type
136

Vendor ID
5535 (Reusing the 3GPP2 VID in a non-standard way.)

VSA Type
196

Length
1

Value
The system does not interpret this value, but it is copied in accounting messages.

Primary-DNS-Server

Same as **SN1-Primary-DNS-Server** standard attribute; non-standard behavior for use in custom dictionary.

Type
135

Vendor ID
N/A

VSA Type
N/A

Length
4

Value
IPv4 address

Prohibit-Payload-Compression

Flag to prohibit SGSN from compressing user data on per APN basis.

Type
26

Vendor ID
8164

VSA Type
237

Length
2

Value
Enumerated integer. Supported values are:

- Allowed = 0
- Prohibited = 1

Prohibit-Payload-Compression1

Flag to prohibit SGSN from compressing user data on per APN basis.

Type
26

Vendor ID
8164

VSA Type
237

Length
2

Value
Enumerated integer. Supported values are:

- Allowed = 0
- Prohibited = 1

Reject-Cause

This attribute indicates the cause for sending Access-Reject.

Type
26

Vendor ID
9

VSA Type
116

Length
1

Value
Opaque value

Reply-Message

This attribute indicates the text to be displayed to a user upon completion of authentication, whether successful or not.

Type
18

Vendor ID
N/A

VSA Type
N/A

Length
1–2048

Value
An ASCII string to be displayed to the user. This attribute may appear more than once, in which case the string displayed to the user is a concatenation of the Reply-Message attributes in the order in which they appear in the RADIUS response message.

RRQ-MN-HA-KEY

MN-HA key computed using RRQ-HA-IP if sent in Access request.

Type
26

Vendor ID
24757

VSA Type
19

Length
1–244

Value

Opaque value

Secondary-DNS-Server

Same as **SN1-Secondary-DNS-Server** standard attribute; non-standard behavior for use in custom dictionary.

Type
136

Vendor ID
N/A

VSA Type
N/A

Length
4

Value
IPv4 address

Selection-Mode

Same as **3GPP-Selection-Mode** standard attribute; non-standard behavior for use in custom dictionary.

Type
229

Vendor ID
N/A

VSA Type
N/A

Length
1

Value
Opaque value

Service-Type

This attribute identifies the service that the user is attempting to use (Access-Request), or is granted to use (Access-Accept).

This attribute is also accepted in CoA request message to be used in a currently active subscriber session.

Type
6

Vendor ID
N/A

VSA Type
N/A

Length

4

Value

Enumerated integer. Supported values are:

- Framed = 2—PPP or HA session
- Administrative = 6—Configuration administration CLI session
- Authenticate_Only = 8
- Inspector = 19650516—Configuration/statistics read-only CLI session
- Security_Admin = 19660618—Security administration CLI session

The following values are not supported, used only for display/decoding purposes:

- Login = 1
- Callback_Login = 3
- Callback_Framed = 4
- Outbound = 5
- NAS_Prompt = 7—CLI session
- Callback_NAS_Prompt = 9
- Call_Check = 10
- Callback_Administrative = 11
- Voice = 12
- Fax = 13
- Modem_Relay = 14
- IAPP_Register = 15
- IAPP_AP_Check = 16
- Authorize_Only = 17—RADIUS Change of Authorize/Disconnect/Prepaid Access Requests

Session-Timeout

This attribute sets the maximum session time in seconds. After this session time expires the chassis will tear down the session.

Type

27

Vendor ID

N/A

VSA Type

N/A

Length

4

Value

Unsigned integer

SGSN-IP-Address

Same as **3GPP-SGSN-Address** standard attribute; non-standard behavior for use in custom dictionary.

Type
228

Vendor ID
N/A

VSA Type
N/A

Length
4

Value
IPv4 address

SIP-AOR

This attribute identifies the URI, the use of which must be authenticated and authorized.

Type
122

Vendor ID
N/A

VSA Type
N/A

Length
0–253

Value
ASCII string

SN-Access-link-IP-Frag

This attribute specifies what to do when data received for the subscriber on the Access link that needs to be fragmented and the DF bit is either set or unset. The default is Normal.

Type
26

Vendor ID
8164

VSA Type
63

Length
4

Value
Enumerated integer. Supported values are:

- Normal = 0 — Data to be fragmented is not fragmented if the DF bit is set
- DF-Ignore = 1 — Fragment regardless
- DF-Fragment-ICMP-Notify = 2 — Fragment regardless, and ICMP Notify if DF bit is set

SN-Acct-Input-Giga-Dropped

This attribute contains the number of input gigawords dropped if the number of input bytes is greater than 2^32 - 1.

Type
26

Vendor ID
8164

VSA Type
230

Length
4

Value
Unsigned integer

SN-Acct-Input-Octets-Dropped

This attribute indicates how many octets received have been dropped in the PPP session. Since the value field is 32 bits, it is possible that the number of octets will exceed the 32-bit field length. If this happens, this attribute will "wrap" back to 0. Each time the "wrap" occurs, the SN-Acct-Input-Giga-Dropped attribute will be incremented.

Type
26

Vendor ID
8164

VSA Type
228

Length
8

Value
Unsigned integer

SN-Acct-Input-Packets-Dropped

This attribute indicates how many PPP packets received have been dropped during the session.

Type
26

Vendor ID
8164

VSA Type
226

Length
4

Value
Unsigned integer

SN-Acct-Output-Giga-Dropped

This attribute contains the number of output gigawords dropped if the number of output bytes is greater than 2^32 - 1.

Type
26

Vendor ID
8164

VSA Type
231

Length
4

Value
Unsigned integer

SN-Acct-Output-Octets-Dropped

This attribute indicates how many octets have been dropped in the PPP session. Since the value field is 32 bits, it is possible that the number of octets will exceed the 32-bit field length. If this happens, this attribute will "wrap" back to 0. Each time the "wrap" occurs, the SN-Acct-Output-Giga-Dropped attribute will be incremented.

Type
26

Vendor ID
8164

VSA Type
229

Length
8

Value
Unsigned integer

SN-Acct-Output-Packets-Dropped

This attribute indicates how many output PPP packets have been dropped during the session.

Type
26

Vendor ID
8164

VSA Type
227

Length
4

Value
Unsigned integer

SN-Acs-Credit-Control-Group

This attribute contains the Diameter Credit Control Group name. It is used to send the Credit Control Group name from APN config to the ACS module.

Type
26

Vendor ID
8164

VSA Type
301

Length
1–63

Value
String

SN-Admin-Expiry

This attribute contains the date/time the administrative user account expires. It is an integer value specifying the number of seconds since the UNIX epoch at which time the account will expire.

Type
26

Vendor ID
8164

VSA Type
204

Length
4

Value
Integer

SN-Admin-Permission

This attribute indicates the services allowed to be delivered to the administrative user. The attribute value is a bit field, and many algorithms can be specified to indicate that one of these may be chosen by the user.

Type
26

Vendor ID
8164

VSA Type
21

Length
4

Value
Enumerated integer. Supported values are:

- None = 0
- CLI = 1
- FTP = 2
- CLI-FTP = 3
- Intercept = 4
- CLI-Intercept = 5
- CLI-Intercept-FTP = 7
- ECS = 8
- CLI-ECS = 9
- CLI-FTP-ECS = 11
- CLI-Intercept-ECS = 13
- CLI-Intercept-FTP-ECS = 15

SN-ANID

This attribute contains the Access Network ID.

Type
26

Vendor ID
5535

VSA Type
178

Length
10

Value
Opaque value

SN-Assigned-VLAN-ID

This attribute contains the Assigned VLAN ID.

Type
26

Vendor ID
8164

VSA Type
152

Length
2

Value
Unsigned integer

SN-Authorised-Qos

This attribute contains the authorized QoS.

Type
26

Vendor ID
8164

VSA Type
266

Length
4

Value
ASCII string

SN-Bandwidth-Policy

This attribute contains the Traffic Policy value.

This attribute is also accepted in CoA request message to be used in a currently active subscriber session.

If this AVP is present in Access Accept message the locally configured APN value will be overridden. If there is no value configured in the APN this policy will not be applied.

Type
26

Vendor ID
8164

VSA Type
300

Length

1–63

Value

String

SN-Call-Id

This attribute contains the Call ID.

Type

26

Vendor ID

8164

VSA Type

251

Length

4

Value

Unsigned integer

SN-Cause-Code

This attribute includes the termination cause code value from IMS node.

Type

26

Vendor ID

8164

VSA Type

267

Length

4

Value

Enumerated integer. Supported values are:

- Normal_End_Of_Session = 0
- Successful_Transaction = 1
- End_Of_Subscriber_Dialog = 2
- 3XX_Redirection = 3
- 4XX_Request_Failure = 4
- 5XX_Server_Failure = 5
- 6XX_Global_Failure = 6
- Unspecified_Error = 7
- Unsuccessful_Session_Setup = 8

- Internal_Error = 9

SN-Cause-For-Rec-Closing

This attribute contains the GGSN Specific Record Closing Reason Value.

Type
26

Vendor ID
8164

VSA Type
139

Length
4

Value
Unsigned integer

SN-CBB-Policy

This attribute contains the CBB policy name.

This attribute is also accepted in CoA request message to be used in a currently active subscriber session.

If this AVP is present in Access Accept message the locally configured APN value will be overridden. If there is no value configured in the APN this policy will not be applied.

Type
26

Vendor ID
8164

VSA Type
302

Length
1–63

Value
String

SN-CF-Call-International

This attribute contains enable/disable config for CF call restriction and dialing permission for international calls.

Type
26

Vendor ID
8164

VSA Type

293

Length
4

Value
Enumerated integer. Supported values are:

- Disable = 0
- Enable = 1

SN-CF-Call-Local

This attribute contains enable/disable config for CF call restriction and dialing permission for local calls.

Type
26

Vendor ID
8164

VSA Type
291

Length
4

Value
Enumerated integer. Supported values are:

- Disable = 0
- Enable = 1

SN-CF-Call-LongDistance

This attribute contains enable/disable config for CF call restriction and dialing permission for long distance calls.

Type
26

Vendor ID
8164

VSA Type
292

Length
4

Value
Enumerated integer. Supported values are:

- Disable = 0
- Enable = 1

SN-CF-Call-Premium

This attribute contains enable/disable config for CF call restriction and dialing permission for premium calls.

Type
26

Vendor ID
8164

VSA Type
294

Length
4

Value
Enumerated integer. Supported values are:

- Disable = 0
- Enable = 1

SN-CF-Call-RoamingInternatnl

This attribute contains enable/disable config for CSCF call restriction and dialing permission - Roaming International call.

Type
26

Vendor ID
8164

VSA Type
298

Length
4

Value
Enumerated integer. Supported values are:

- Disable = 0
- Enable = 1

SN-CF-Call-Transfer

This attribute contains enable/disable config for CSCF call feature - call transfer.

Type
26

Vendor ID
8164

VSA Type
285

Length
4

Value
Enumerated integer. Supported values are:

- Disable = 0
- Enable = 1

SN-CF-Call-Waiting

This attribute contains enable/disable config for CSCF call feature - call waiting.

Type
26

Vendor ID
8164

VSA Type
284

Length
4

Value
Enumerated integer. Supported values are:

- Disable = 0
- Enable = 1

SN-CF-Cld-Display

This attribute contains enable/disable config for CSCF call feature — caller ID display.

Type
26

Vendor ID
8164

VSA Type
282

Length
4

Value
Enumerated integer. Supported values are:

- Disable = 0
- Enable = 1

SN-CF-Cld-Display-Blocked

This attribute contains enable/disable config for CSCF call feature — caller ID display blocked.

Type
26

Vendor ID
8164

VSA Type
283

Length
4

Value
Enumerated integer. Supported values are:

- Disable = 0
- Enable = 1

SN-CF-Follow-Me

This attribute contains URIs for CSCF call feature — follow me.

Type
26

Vendor ID
8164

VSA Type
281

Length
0–255

Value
ASCII string

SN-CF-Forward-Busy-Line

This attribute contains URI for CSCF call feature — forward busy line.

Type
26

Vendor ID
8164

VSA Type
279

Length
0–255

Value
ASCII string

SN-CF-Forward-No-Answer

This attribute contains URI for CSCF call feature — forward no answer.

Type
26

Vendor ID
8164

VSA Type
278

Length
0–255

Value
ASCII string

SN-CF-Forward-Not-Regd

This attribute contains URI for CSCF call feature — forward not registered.

Type
26

Vendor ID
8164

VSA Type
280

Length
0–255

Value
ASCII string

SN-CF-Forward-Unconditional

This attribute contains URI for CSCF call feature — forward unconditional.

Type
26

Vendor ID
8164

VSA Type
277

Length

0–255

Value

ASCII string

SN-CFPolicy-ID

This attribute contains the Content Filtering policy ID.

This attribute is also accepted in CoA request message to be used in a currently active subscriber session.

Type

26

Vendor ID

8164

VSA Type

220

Length

4

Value

Unsigned integer

SN-Change-Condition

The change condition that triggered this record for a GGSN session.

Type

26

Vendor ID

8164

VSA Type

140

Length

4

Value

Enumerated integer. Supported values are:

- QOSCHANGE = 0
- TARIFFTIMECHANGE = 1
- SGSNCHANGE = 500

SN-Charging-VPN-Name

The Charging Context Name for GGSN sessions.

Type

26

Vendor ID
8164

VSA Type
137

Length
1–252

Value
ASCII string

SN-Chrg-Char-Selection-Mode

SN-Chrg-Char-Selection-Mode

Type
26

Vendor ID
8164

VSA Type
138

Length
4

Value
Unsigned integer

SN-Content-Disposition

This attribute indicates how the SIP message body or a message body part is to be interpreted.

Type
26

Vendor ID
8164

VSA Type
272

Length
4

Value
ASCII string

SN-Content-Length

This attribute contains size of the SIP message body.

Type
26

Vendor ID
8164

VSA Type
271

Length
4

Value
ASCII string

SN-Content-Type

This attribute contains the media type of the SIP message body.

Type
26

Vendor ID
8164

VSA Type
270

Length
4

Value
ASCII string

SN-CR-International-Cid

Carrier ID for routing international calls.

Type
26

Vendor ID
8164

VSA Type
295

Length
4

Value
Unsigned integer

SN-CR-LongDistance-Cid

Carrier ID for routing long distance calls.

Type
26

Vendor ID
8164

VSA Type
296

Length
4

Value
Unsigned integer

SN-CSCF-App-Server-Info

This is a compound attribute and contains information about application servers.

Type
26

Vendor ID
8164

VSA Type
275

Length
4

Value
Contains the following two subattributes:

App-Server

Holds URL of the application server.

Type
1

Length
4

Value
ASCII string

AS-Called-Party-Address

Holds the called party addresses determined by the application server.

Type

2

Length
4

Value
ASCII string

SN-CSCF-Rf-SDP-Media-Components

This is a compound attribute for IMS SDP media components.

Type
26

Vendor ID
8164

VSA Type
273

Value
Contains the following subattributes:

Media-Name

Name of the media as available in the SDP data.

Type
1

Length
0–128

Value
String

Media-Description

Holds the attributes of the media as available in the SDP data.

Type
2

Length
0–128

Value
String

Authorised-QoS

Holds the 3GPP Authorised QoS string.

Type
3

Length
0–128

Value
String

3GPP-Charging-Id

Holds the 3GPP charging ID.

Type
4

Length
0–253

Value
String

Access-Network-Charging-Identifier-Value

Holds the access network charging identifier value.

Type
5

Length
1–256

Value
Opaque value

SN-Cscf-Subscriber-Ip-Address

This attribute contains the IP address of subscriber, used for early IMS authentication procedures.

Type
26

Vendor ID
8164

VSA Type
287

Length
4

Value
IPv4 address

SN-Data-Tunnel-Ignore-DF-Bit

This attribute specifies if the PDSN/FA or HA should ignore the DF bit in the IPv4 header when encapsulating the IPv4 packet in MIP, and therefore fragmenting the resulting tunneled packet if necessary. The default is not to ignore the DF bit.

Type
26

Vendor ID
8164

VSA Type
49

Length
4

Value
Enumerated integer. Supported values are:

- Disabled = 0 — Do not ignore DF bit
- Enabled = 1 — Ignore DF bit

SN-DHCP-Lease-Expiry-Policy

This attribute specifies whether to renew or disconnect on expiry of IP address lease time.

Type
26

Vendor ID
8164

VSA Type
157

Length
4

Value
Enumerated integer. Supported values are:

- auto-renew = 0
- disconnect = 1

SN-DHCP-Options

Specific information to be sent from the DHCP server to the client.

Type
26

Vendor ID
8164

VSA Type
309

Length
1–245

Value

Opaque value

SN-Direction

ROHC protocol control that specifies in which direction to enable Robust Header Compression (ROHC).

Type
26

Vendor ID
8164

VSA Type
153

Length
4

Value
Enumerated integer. Supported values are:

- Any = 0
- Uplink = 1
- Downlink = 2

SN-Disconnect-Reason

This attribute indicates the reason the user was disconnected from service.

This attribute is also accepted in CoA request message to be used in a currently active subscriber session.

Type
26

Vendor ID
8164

VSA Type
3

Length
4

Value
Enumerated integer. Supported values are:

- Not-Defined = 0
- Admin-Disconnect = 1
- Remote-Disconnect = 2
- Local-Disconnect = 3
- Disc-No-Resource = 4
- Disc-Excd-Service-Limit = 5
- PPP-LCP-Neg-Failed = 6

- PPP-LCP-No-Response = 7
- PPP-LCP-Loopback = 8
- PPP-LCP-Max-Retry = 9
- PPP-Echo-Failed = 10
- PPP-Auth-Failed = 11
- PPP-Auth-Failed-No-AAA-Resp = 12
- PPP-Auth-No-Response = 13
- PPP-Auth-Max-Retry = 14
- Invalid-AAA-Attr = 15
- Failed-User-Filter = 16
- Failed-Provide-Service = 17
- Invalid-IP-Address-AAA = 18
- Invalid-IP-Pool-AAA = 19
- PPP-IPCP-Neg-Failed = 20
- PPP-IPCP-No-Response = 21
- PPP-IPCP-Max-Retry = 22
- PPP-No-Rem-IP-Address = 23
- Inactivity-Timeout = 24
- Session-Timeout = 25
- Max-Data-Excd = 26
- Invalid-IP-Source-Address = 27
- MSID-Auth-Failed = 28
- MSID-Auth-Failed-No-AAA-Resp = 29
- A11-Max-Retry = 30
- A11-Lifetime-Expired = 31
- A11-Message-Integrity-Failure = 32
- PPP-lcp-remote-disc = 33
- Session-setup-timeout = 34
- PPP-keepalive-failure = 35
- Flow-add-failed = 36
- Call-type-detection-failed = 37
- Wrong-ipcp-params = 38
- MIP-remote-dereg = 39
- MIP-lifetime-expiry = 40
- MIP-proto-error = 41
- MIP-auth-failure = 42
- MIP-reg-timeout = 43

- Invalid-dest-context = 44
- Source-context-removed = 45
- Destination-context-removed = 46
- Req-service-addr-unavailable = 47
- Demux-mgr-failed = 48
- Internal-error = 49
- AAA-context-removed = 50
- invalid-service-type = 51
- mip-relay-req-failed = 52
- mip-rcvd-relay-failure = 53
- ppp-restart-inter-pdsn-handoff = 54
- gre-key-mismatch = 55
- invalid_tunnel_context = 56
- no_peer_lns_address = 57
- failed_tunnel_connect = 58
- l2tp-tunnel-disconnect-remote = 59
- l2tp-tunnel-timeout = 60
- l2tp-protocol-error-remote = 61
- l2tp-protocol-error-local = 62
- l2tp-auth-failed-remote = 63
- l2tp-auth-failed-local = 64
- l2tp-try-another-lns-from-remote = 65
- l2tp-no-resource-local = 66
- l2tp-no-resource-remote = 67
- l2tp-tunnel-disconnect-local = 68
- l2tp-admin-disconnect_remote = 69
- l2tpmgr-reached-max-capacity = 70
- MIP-reg-revocation = 71
- path-failure = 72
- dhcp-relay-ip-validation-failed = 73
- gtp-unknown-pdp-addr-or-pdp-type = 74
- gtp-all-dynamic-pdp-addr-occupied = 75
- gtp-no-memory-is-available = 76
- dhcp-relay-static-ip-addr-not-allowed = 77
- dhcp-no-ip-addr-allocated = 78
- dhcp-ip-addr-allocation-tmr-exp = 79
- dhcp-ip-validation-failed = 80

- dhcp-static-addr-not-allowed = 81
- dhcp-ip-addr-not-available-at-present = 82
- dhcp-lease-expired = 83
- lpool-ip-validation-failed = 84
- lpool-static-ip-addr-not-allowed = 85
- static-ip-validation-failed = 86
- static-ip-addr-not-present = 87
- static-ip-addr-not-allowed = 88
- radius-ip-validation-failed = 89
- radius-ip-addr-not-provided = 90
- invalid-ip-addr-from-sgsn = 91
- no-more-sessions-in-aaa = 92
- ggsn-aaa-auth-req-failed = 93
- conflict-in-ip-addr-assignment = 94
- apn-removed = 95
- credits-used-bytes-in = 96
- credits-used-bytes-out = 97
- credits-used-bytes-total = 98
- prepaid-failed = 99
- l2tp-ipsec-tunnel-failure = 100
- l2tp-ipsec-tunnel-disconnected = 101
- mip-ipsec-sa-inactive = 102
- Long-Duration-Timeout = 103
- proxy-mip-registration-failure = 104
- proxy-mip-binding-update = 105
- proxy-mip-inter-pdsn-handoff-require-ip-address = 106
- proxy-mip-inter-pdsn-handoff-mismatched-address = 107
- Local-purge = 108
- failed-update-handoff = 109
- closed_rp-handoff-complete = 110
- closed_rp-duplicate-session = 111
- closed_rp-handoff-session-not-found = 112
- closed_rp-handoff-failed = 113
- pcf-monitor-keep-alive-failed = 114
- call-internal-reject = 115
- call-restarted = 116
- a11-mn-ha-auth-failure = 117

- a11-badly-formed = 118
- a11-t-bit-not-set = 119
- a11-unsupported-vendor-id = 120
- a11-mismatched-id = 121
- mipha-dup-home-addr-req = 122
- mipha-dup-imsi-session = 123
- ha-unreachable = 124
- IPSP-addr-in-use = 125
- mipfa-dup-home-addr-req = 126
- mipha-ip-pool-busyout = 127
- inter-pdsn-handoff = 128
- active-to-dormant = 129
- ppp-renegotiation = 130
- active-start-param-change = 131
- tarrif-boundary = 132
- a11-disconnect-no-active-stop = 133
- nw-reachability-failed-reject = 134
- nw-reachability-failed-redirect = 135
- container-max-exceeded = 136
- static-addr-not-allowed-in-apn = 137
- static-addr-required-by-radius = 138
- static-addr-not-allowed-by-radius = 139
- mip-registration-dropped = 140
- counter-rollover = 141
- constructed-nai-auth-fail = 142
- inter-pdsn-service-optimize-handoff-disabled = 143
- gre-key-collision = 144
- inter-pdsn-service-optimize-handoff-triggered = 145
- intra-pdsn-handoff-triggered = 146
- delayed-abort-timer-expired = 147
- Admin-AAA-disconnect = 148
- Admin-AAA-disconnect-handoff = 149
- PPP-IPV6CP-Neg-Failed = 150
- PPP-IPV6CP-No-Response = 151
- PPP-IPV6CP-Max-Retry = 152
- PPP-Restart-Invalid-source-IPV4-address = 153
- a11-disconnect-handoff-no-active-stop = 154

- call-restarted-inter-pdsn-handoff = 155
- call-restarted-ppp-termination = 156
- mipfa-resource-conflict = 157
- failed-auth-with-charging-svc = 158
- mipha-dup-imsi-session-purge = 159
- mipha-rev-pending-newcall = 160
- volume-quota-reached = 161
- duration-quota-reached = 162
- gtp-user-authentication-failed = 163
- MIP-reg-revocation-no-lcp-term = 164
- MIP-private-ip-no-rev-tunnel = 165
- Invalid-Prepaid-AAA-attr-in-auth-response = 166
- mipha-prepaid-reset-dynamic-newcall = 167
- gre-flow-control-timeout = 168
- mip-paaa-bc-query-not-found = 169
- mipha-dynamic-ip-addr-not-available = 170
- a11-mismatched-id-on-handoff = 171
- a11-badly-formed-on-handoff = 172
- a11-unsupported-vendor-id-on-handoff = 173
- a11-t-bit-not-set-on-handoff = 174
- MIP-reg-revocation-i-bit-on = 175
- A11-RRQ-Deny-Max-Count = 176
- Dormant-Transition-During-Session-Setup = 177
- PPP-Rem-Reneg-Disc-Always-Cfg = 178
- PPP-Rem-Reneg-Disc-NAI-MSID-Mismatch = 179
- mipha-subscriber-ipsec-tunnel-down = 180
- mipha-subscriber-ipsec-tunnel-failed = 181
- mipha-subscriber-ipsecmgr-death = 182
- flow-is-deactivated = 183
- ecsv2-license-exceeded = 184
- IPSG-Auth-Failed = 185
- driver-initiated = 186
- ims-authorization-failed = 187
- service-instance-released = 188
- flow-released = 189
- ppp-renego-no-ha-addr = 190
- intra-pdsn-handoff = 191

- overload-disconnect = 192
- css-service-not-found = 193
- Auth-Failed = 194
- dhcp-client-sent-release = 195
- dhcp-client-sent-nak = 196
- msid-dhcp-chaddr-mismatch = 197
- link-broken = 198
- prog-end-timeout = 199
- qos-update-wait-timeout = 200
- css-synch-cause = 201
- Gtp-context-replacement = 202
- PDIF-Auth-failed = 203
- l2tp-unknown-apn = 204
- ms-unexpected-network-reentry = 205
- r6-invalid-nai = 206
- eap-max-retry-reached = 207
- vbm-hoa-session-disconnected = 208
- vbm-voa-session-disconnected = 209
- in-acl-disconnect-on-violation = 210
- eap-msk-lifetime-expiry = 211
- eap-msk-lifetime-too-low = 212
- mipfa-inter-tech-handoff = 213
- r6-max-retry-reached = 214
- r6-nwexit-recd = 215
- r6-dereg-req-recd = 216
- r6-remote-failure = 217
- r6r4-protocol-errors = 218
- wimax-qos-invalid-aaa-attr = 219
- npu-gre-flows-not-available = 220
- r4-max-retry-reached = 221
- r4-nwexit-recd = 222
- r4-dereg-req-recd = 223
- r4-remote-failure = 224
- ims-authorization-revoked = 225
- ims-authorization-released = 226
- ims-auth-decision-invalid = 227
- mac-addr-validation-failed = 228

- excessive-wimax-pd-flows-cfgd = 229
- sgsn-canc-loc-sub = 230
- sgsn-canc-loc-upd = 231
- sgsn-mnr-exp = 232
- sgsn-ident-fail = 233
- sgsn-sec-fail = 234
- sgsn-auth-fail = 235
- sgsn-glu-fail = 236
- sgsn-imp-det = 237
- sgsn-smgr-purge = 238
- sgsn-subs-handed-to-peer = 239
- sgsn-dns-fail-inter-rau = 240
- sgsn-cont-rsp-fail = 241
- sgsn-hlr-not-found-for-imsi = 242
- sgsn-ms-init-det = 243
- sgsn-opr-policy-fail = 244
- sgsn-duplicate-context = 245
- hss-profile-update-failed = 246
- sgsn-no-pdp-activated = 247
- asnpc-idle-mode-timeout = 248
- asnpc-idle-mode-exit = 249
- asnpc-idle-mode-auth-failed = 250
- asngw-invalid-qos-configuration = 251
- sgsn-dsd-allgprswithdrawn = 252
- r6-pmk-key-change-failure = 253
- sgsn-illegal-me = 254
- sess-termination-timeout = 255
- sgsn-sai-fail = 256
- sgsn-rnc-removal = 257
- sgsn-rai-removal = 258
- sgsn-init-deact = 259
- ggsn-init-deact = 260
- hlr-init-deact = 261
- ms-init-deact = 262
- sgsn-detach-init-deact = 263
- sgsn-rab-rel-init-deact = 264
- sgsn-iu-rel-init-deact = 265

- sgsn-gtpu-path-failure = 266
- sgsn-gtpc-path-failure = 267
- sgsn-local-handoff-init-deact = 268
- sgsn-remote-handoff-init-deact = 269
- sgsn-gtp-no-resource = 270
- sgsn-rnc-no-resource = 271
- sgsn-odb-init-deact = 272
- sgsn-invalid-ti = 273
- sgsn-ggsn-ctxt-non-existent = 274
- sgsn-apn-restrict-vio = 275
- sgsn-regular-deact = 276
- sgsn-abnormal-deact = 277
- sgsn-actv-rejected-by-peer = 278
- sgsn-err-ind = 279
- asngw-non-anchor-prohibited = 280
- asngw-im-entry-prohibited = 281
- session-idle-mode-entry-timeout = 282
- session-idle-mode-exit-timeout = 283
- asnpc-ms-power-down-nwexit = 284
- asnpc-r4-nwexit-recd = 285
- sgsn-iu-rel-before-call-est = 286
- ikev2-subscriber-ipsecmgr-death = 287
- All-dynamic-pool-addr-occupied = 288
- mip6ha-ip-addr-not-available = 289
- bs-monitor-keep-alive-failed = 290
- sgsn-att-in-reg-state = 291
- sgsn-inbound-srns-in-reg-state = 292
- dt-ggsn-tun-reestablish-failed = 293
- sgsn-unknown-pdp = 294
- sgsn-pdp-auth-failure = 295
- sgsn-duplicate-pdp-context = 296
- sgsn-no-rsp-from-ggsn = 297
- sgsn-failure-rsp-from-ggsn = 298
- sgsn-apn-unknown = 299
- sgsn-serv-req-init-deact = 300
- sgsn-attach-on-attch-init-abort = 301
- sgsn-iu-rel-in-israu-init-abort = 302

- sgsn-smgr-init-abort = 303
- sgsn-mm-ctx-cleanup-init-abort = 304
- sgsn-unknown-abort = 305
- sgsn-guard-timeout-abort = 306
- vpn-bounce-dhcpip-validate-req = 307
- mipv6-id-mismatch = 308
- aaa-session-id-not-found = 309
- x1-max-retry-reached = 310
- x1-nwexit-recd = 311
- x1-dereg-req-recd = 312
- x1-remote-failure = 313
- x1x2-protocol-errors = 314
- x2-max-retry-reached = 315
- x2-nwexit-recd = 316
- x2-dereg-req-recd = 317
- x2-remote-failure = 318
- x1-pmk-key-change-failure = 319
- sa-rekeying-failure = 320
- sess-sleep-mode-entry-timeout = 321
- phsgw-non-anchor-prohibited = 322
- asnpc-pc-relocation-failed = 323
- asnpc-pc-relocation = 324
- auth_policy_mismatch = 325
- sa-lifetime-expiry = 326
- asnpc-del-ms-entry-recd = 327
- phspc-sleep-mode-timeout = 328
- phspc-sleep-mode-exit = 329
- phspc-sleep-mode-auth-failed = 330
- phspc-ms-power-down-nwexit = 331
- phspc-x2-nwexit-recd = 332
- invalid-nat-config = 333
- asngw-tid-entry-not-found = 334
- No-NAT-IP-Address = 335
- excessive-phs-pd-flows-cfgd = 336
- phsgw-invalid-qos-configuration = 337
- Interim-Update = 338
- sgsn-attach-abrt-rad-lost = 339

- sgsn-inbnd-irau-abrt-rad-lost = 340
- ike-keepalive-failed = 341
- sgsn-attach-abrt-ms-suspend = 342
- sgsn-inbnd-irau-abrt-ms-suspend = 343
- duplicate-session-detected = 344
- sgsn-xid-response-failure = 345
- sgsn-nse-cleanup = 346
- sgsn-gtp-req-failure = 347
- sgsn-imsi-mismatch = 348
- sgsn-bvc-blocked = 349
- sgsn-attach-on-inbound-irau = 350
- sgsn-attach-on-outbound-irau = 351
- sgsn-incorrect-state = 352
- sgsn-t3350-expiry = 353
- sgsn-page-timer-expiry = 354
- phsgw-tid-entry-not-found = 355
- phspc-del-ms-entry-recd = 356
- sgsn-pdp-local-purge = 357
- phs-invalid-nai = 358
- session-sleep-mode-exit-timeout = 359
- sgsn-offload-phase2 = 360
- phs-thirdparty-auth-fail = 361
- remote-error-notify = 362
- no-response = 363
- PDG-Auth-failed = 364
- mme-s1AP-send-failed=365
- mme-egtpc-connection-failed=366
- mme-egtpc-create-session-failed=367
- mme-authentication-failure=368
- mme-ue-detach=369
- mme-mme-detach=370
- mme-hss-detach=371
- mme-pgw-detach=372
- mme-sub-validation-failure=373
- mme-hss-connection-failure=374
- mme-hss-user-unknown=375
- dhcp-lease-mismatch-detected=376

- nemo-link-layer-down=377
- eapol-max-retry-reached = 378
- sgsn-offload-phase3 = 379
- mbms-bearer-service-disconnect = 380
- disconnect-on-violation-odb = 381
- disconn-on-violation-focs-odb = 382
- CSCF-REG-Admin-disconnect = 383
- CSCF-REG-User-disconnect = 384
- CSCF-REG-Inactivity-timeout = 385
- CSCF-REG-Network-disconnect = 386
- CSCF-Call-Admin-disconnect = 387
- CSCF-CAll-User-disconnect = 388
- CSCF-CALL-Local-disconnect = 389
- CSCF-CALL-No-Resource = 390
- CSCF-CALL-No-Respone = 391
- CSCF-CALL-Inactivity-timeout = 392
- CSCF-CALL-Media-Auth-Failure = 393
- CSCF-REG-No-Resource = 394
- ms-unexpected-idle-mode-entry = 395
- re-auth-failed = 396
- sgsn-pdp-nse-cleanup = 397
- sgsn-mm-ctxt-gtp-no-resource = 398
- unknown-apn = 399
- gtpc-path-failure = 400
- gtpu-path-failure = 401
- actv-rejected-by-sgsn = 402
- sgsn-pdp-gprs-camel-release = 403
- sgsn-check-imei-failure = 404
- sgsn-sndcp-init-deact = 405
- sgsn-pdp-inactivity-timeout = 406
- fw-and-nat-policy-removed = 407
- FNG-Auth-failed = 408
- ha-stale-key-disconnect = 409
- No-IPV6-address-for-subscriber = 410
- prefix-registration-failure = 411
- disconnect-from-policy-server = 412
- s6b-auth-failed = 413

- gtpc-err-ind = 414
- gtpu-err-ind = 415
- invalid-pdn-type = 416
- aaa-auth-req-failed = 417
- apn-denied-no-subscription = 418
- Sgw-context-replacement = 419
- dup-static-ip-addr-req = 420
- apn-restrict-violation = 421
- invalid-wapn = 422
- ttg-nsapi-allocation-failed = 423
- mandatory-gtp-ie-missing = 424
- aaa-unreachable = 425
- asngw-service-flow-deletion = 426
- CT-PMIP-RRQ-NVSE-Value-Change = 427
- tcp-read-failed = 428
- tcp-write-failed = 429
- ssl-handshake-failed = 430
- ssl-renegotiate-failed = 431
- ssl-bad-message = 432
- ssl-alert-received = 433
- ssl-disconnect = 434
- ssl-migration = 435
- sgsn-ard-failure = 436
- sgsn-camel-release = 437
- Hotlining-Status-Change=447
- ggsn-no-rsp-from-sgsn = 448
- diameter-protocol-error=449
- diameter-request-timeout=450
- operator-policy=451
- spr-connection-timeout=452
- mipha-dup-wimax-session = 453
- invalid-version-attr = 454
- sgsn-zone-code-failure = 455
- invalid-qci = 456
- no_rules = 457
- mme-init-ctxt-setup-failure = 459
- mme-driver-initiated = 460

- mme-s1ap-connection-down = 461
- mme-s1ap-reset-recd = 462
- mme-s6a-response-timeout = 463
- mme-s13-response-timeout = 464
- mme-Illegal-equipment = 465
- mme-unexpected-attach = 466
- mme-sgw-selection-failure = 467
- mme-pgw-selection-failure = 468
- mme-reselection-to-sgsn = 469
- mme-relocation-to-sgsn = 470
- mme-reselection-to-mme = 471
- mme-relocation-to-mme = 472
- mme-tau-attach-collision = 473
- mme-old-sgsn-resolution-failure = 474
- mme-old-mme-resolution-failure = 475
- mme-reloc-ho-notify-timeout = 476
- mme-reloc-ho-req-ack-timeout = 477
- mme-create-session-timeout = 478
- mme-create-session-failure = 479
- mme-s11-path-failure = 480
- mme-policy-no-ue-irat = 481
- mme-x2-handover-failed = 482
- mme-attach-restrict = 483
- mme-regional-zone-code = 484
- mme-no-response-from-ue = 485
- mme-sgw-relocation-failed = 486
- mme-implicit-detach = 487
- sgsn-detach-notify = 488
- emergency-inactivity-timeout = 489
- policy-initiated-release = 490
- gy-result-code-system-failure = 491
- mme-zone-code-validation-failed = 492
- sgsn-pgw-init-deact = 493
- s6b-ip-validation-failed = 494
- sgsn-failure-rsp-from-sgw = 495
- tcp-remote-close = 496
- tcp-reset-received = 497

- tcp-socket-error = 498
- ptmsi-signature-mismatch = 499

SN-DNS-Proxy-Intercept-List

This attribute is used to specify the list name which contains the rules to intercept and redirect DNS requires received from mobile. This attribute can be configured using either local subscriber template or returned from Access-Accept.

Type
26

Vendor ID
8164

VSA Type
214

Length
1–253

Value
ASCII string

SN-DNS-Proxy-Use-Subscr-Addr

This attribute is used to convey whether to use the subscriber's address as the source address for DNS Proxy.

Type
26

Vendor ID
8164

VSA Type
25

Length
4

Value
Enumerated integer. Supported values are:

- Disable = 0
- Enable = 1

SN-Dynamic-Addr-Alloc-Ind-Flag

This attribute indicates whether the IP address is allocated statically or dynamically from SGW perspective.

Type
26

Vendor ID
8164

VSA Type
141

Length
1

Value
Opaque value

SN-Ecs-Data-Volume

Compound attribute indicating downlink and uplink octet usage for a PDP context per rating group.

Type
26

Vendor ID
8164

VSA Type
176

Length
12

Value
Contains the following subattributes:

Rating-Group-Id

Rating Group Id in a PDP context.

Type
1

Length
4

Value
Unsigned integer

GPRS-Uplink

Uplink octet usage for a PDP context per rating group.

Type
2

Length
4

Value
Unsigned integer

GPRS-Downlink

Downlink octet usage for a PDP context per rating group.

Type
3

Length
4

Value
Unsigned integer

SN-Enable-QoS-Renegotiation

This attribute configures the enabling of dynamic QoS renegotiation.

Type
26

Vendor ID
8164

VSA Type
144

Length
4

Value
Enumerated integer. Supported values are:

- No = 0
- Yes = 1

SN-Event

This attribute contains the type of SIP event for which the accounting-request message is generated.

Type
26

Vendor ID
8164

VSA Type
255

Length
4

Value
ASCII string

SN-Ext-Inline-Srvr-Context

This attribute configures the context name in which the External In-line server resides.

Type
26

Vendor ID
8164

VSA Type
41

Length
1–247

Value
String

Important: This attribute is used in conjunction with the External In-line Server feature, which is not supported in StarOS 9.0 and later releases.

SN-Ext-Inline-Srvr-Down-Addr

This attribute configures the IP address of the Downstream External In-line server to forward VLAN-tagged packets to. It can be tagged, in which case it is treated as part of an external in-line server group.

Type
26

Vendor ID
8164

VSA Type
56

Length
4

Value
IPv4 address

Important: This attribute is used in conjunction with the External In-line Server feature, which is not supported in StarOS 9.0 and later releases.

SN-Ext-Inline-Srvr-Down-VLAN

This attribute configures the IP address of the Downstream External In-line server to forward VLAN-tagged packets to. It can be tagged, in which case it is treated as part of an external in-line server group.

Type
26

Vendor ID
8164

VSA Type
59

Length
4

Value
The VLAN tag to apply.

Important: This attribute is used in conjunction with the External In-line Server feature, which is not supported in StarOS 9.0 and later releases.

SN-Ext-Inline-Srvr-Preference

This attribute configures the preference for the tagged group of External In-line Servers. This attribute is required, although it doesn't actually assign a preference right now. It can be tagged, in which case it is treated as part of an external in-line server group.

Type
26

Vendor ID
8164

VSA Type
57

Length
4

Value
Unsigned integer

Important: This attribute is used in conjunction with the External In-line Server feature, which is not supported in StarOS 9.0 and later releases.

SN-Ext-Inline-Srvr-Up-Addr

This attribute configures the IP address of the Upstream External In-line server to forward VLAN-tagged packets to. It can be tagged, in which case it is treated as part of an external in-line server group

Type
26

Vendor ID
8164

VSA Type
55

Length

4

Value

IPv4 address

Important: This attribute is used in conjunction with the External In-line Server feature, which is not supported in StarOS 9.0 and later releases.

SN-Ext-Inline-Srvr-Up-VLAN

This attribute configures the VLAN tag to be applied to Upstream packets and forwarded to the External In-line server. It can be tagged, in which case it is treated as part of an external in-line server group.

Type

26

Vendor ID

8164

VSA Type

58

Length

4

Value

The VLAN tag to apply.

Important: This attribute is used in conjunction with the External In-line Server feature, which is not supported in StarOS 9.0 and later releases.

SN-Fast-Reauth-Username

Fast re-authentication user name.

Type

26

Vendor ID

8164

VSA Type

304

Length

1–128

Value

Opaque value

SN-Firewall-Enabled

Firewall for subscriber enabled.

Type

26

Vendor ID

8164

VSA Type

198

Length

4

Value

Enumerated integer. Supported values are:

- False = 0
- True = 1

SN-Firewall-Policy

This attribute contains the firewall policy name.

Important: This AVP was deprecated in StarOS 8.0, and was later reintroduced in StarOS 8.1.

This attribute is also accepted in CoA request message to be used in a currently active subscriber session.

If this AVP is present in Access Accept message the locally configured APN value will be overridden. If there is no value configured in the APN this policy will not be applied.

Type

26

Vendor ID

8164

VSA Type

239

Length

1–63

Value

String

SN-FMC-Location

MAC address and CDMA location information.

Type

26

Vendor ID
8164

VSA Type
171

Length
1–247

Value
String

SN-GGSN-Address

The control plane IP address of the GGSN that handles one or more media component(s) of an IMS session.

Type
26

Vendor ID
8164

VSA Type
264

Length
4

Value
IPv4 address

SN-GGSN-MIP-Required

This attribute specifies if MIP is required for the GGSN subscriber.

Type
26

Vendor ID
8164

VSA Type
68

Length
4

Value
Enumerated integer. Supported values are:

- Disabled = 0
- Enabled = 1

SN-Gratuitous-ARP-Aggressive

This attribute specifies whether to generate a gratuitous ARP message whenever a MIP handoff or re-registration occurs. A non-zero of this attribute also configures the mode of operation when sending the gratuitous ARP, although only one mode (Aggressive) is supported at this time.

Type
26

Vendor ID
8164

VSA Type
54

Length
4

Value
Enumerated integer. Supported values are:

- Disabled = 0 — Do not send Gratuitous ARP
- Enabled = 1 — Send Gratuitous ARP in Aggressive mode

SN-GTP-Version

This attribute indicates the version of GTP the subscriber is using.

Type
26

Vendor ID
8164

VSA Type
62

Length
4

Value
Enumerated integer. Supported values are:

- GTP_VERSION_0 = 0
- GTP_VERSION_1 = 1
- GTP_VERSION_2 = 2

SN-HA-Send-DNS-ADDRESS

This attribute specifies if the HA should send the DNS address in the Mobile IP RRP message. The default is not to send the DNS address.

Type
26

Vendor ID
8164

VSA Type
47

Length
4

Value
Enumerated integer. Supported values are:

- Disabled = 0 — Do not send
- Enabled = 1 — Send

SN-Handoff-Indicator

This attribute indicates whether the Accounting Interim is sent because of the interim or not.

Type
26

Vendor ID
8164

VSA Type
310

Length
1

Value
Enumerated integer. Supported values are:

- Active-Handoff = 0
- Location-Update = 1

SN-Home-Behavior

This attribute specifies the configuration for the behavior bits settings for a home subscriber in an APN.

When GGSN is configured to reject the charging characteristics sent by the SGSN for "home" subscribers, it uses the profile index specified by **`cc-home behavior <bits> profile <index>`** command to determine the appropriate CCs to use.

Multiple behavior bits can be configured for a single profile index by "Or"ing the bit strings together and convert the result to hexadecimal. The properties of the actual CC profile index are configured as part of the GGSN service using the cc profile command.

If this AVP is present in Access Accept message the locally configured APN value will be overridden.

Type
26

Vendor ID
8164

VSA Type
119

Length
4

Value
Unsigned integer

SN-Home-Profile

This attribute specifies the configuration for the profile bits settings for a home subscriber in an APN.

If this AVP is present in Access Accept message the locally configured APN value will be overridden.

Type
26

Vendor ID
8164

VSA Type
109

Length
4

Value
Unsigned integer

SN-Home-Sub-Use-GGSN

This attribute configures GGSN to accept GGSN's charging characteristics for home subscribers defined for the APN.

If this AVP is present in Access Accept message the locally configured APN value will be overridden.

Type
26

Vendor ID
8164

VSA Type
106

Length
4

Value
Enumerated integer. Supported values are:

- Deny = 0
- Accept = 1

SN-IMS-AM-Address

IMS application manager address.

Type
26

Vendor ID
8164

VSA Type
167

Length
4

Value
IPv4 address

SN-IMS-AM-Domain-Name

IMS application manager domain name.

Type
26

Vendor ID
8164

VSA Type
168

Length
1–64

Value
String

SN-IMS-Charging-Identifier

This attribute holds the IMS Charging Identifier (ICID) as generated by an IMS node for a SIP session.

Type
26

Vendor ID
8164

VSA Type
260

Length
4

Value
ASCII string

SN-IMSI

SN-IMSI

Type
26

Vendor ID
8164

VSA Type
252

Length
1–8

Value
Opaque value

SN-Inactivity-Time

This attribute contains the inactivity time duration for a subscriber session under long time duration timer configuration.

Type
26

Vendor ID
8164

VSA Type
232

Length
4

Value
Integer

SN-Internal-SM-Index

SN-Internal-SM-Index

Type
26

Vendor ID
8164

VSA Type
122

Length
4

Value
Unsigned integer

SN-IP-Alloc-Method

This attribute specifies the method for allocating an IP address. This feature only applies to the GGSN service.

Type
26

Vendor ID
8164

VSA Type
53

Length
4

Value
Enumerated integer. Supported values are:

- Alloc_Local_Pool = 0
- Alloc_Dhcp_Client = 1
- Alloc_Radius = 2
- Alloc_No_Alloc = 3
- Alloc_Static_Alloc = 4
- Alloc_Dhcp_Relay = 5

SN-IP-Filter-In

This attribute specifies the IP input filter rules to determine whether the traffic should undergo DPI processing.

If this AVP is present in Access Accept message the locally configured APN value will be overridden. If there is no value configured in the APN this value will not be applied to the session.

Type
26

Vendor ID
8164

VSA Type
10

Length
1–253

Value
String

SN-IP-Filter-Out

This attribute specifies the IP output filter rules to determine whether the traffic should undergo DPI processing.

If this AVP is present in Access Accept message the locally configured APN value will be overridden. If there is no value configured in the APN this value will not be applied to the session.

Type
26

Vendor ID
8164

VSA Type
11

Length
1–253

Value
String

SN-IP-Header-Compression

Specifies the IP header compression method to use.

Type
Type 26

Vendor ID
8164

VSA Type
150

Length
4

Value
Enumerated integer. Supported values are:

- None = 0
- VJ = 1
- ROHC = 2
- VJ_ROHC = 3

SN-IP-Hide-Service-Address

This attribute prevents subscribers from using traceroute to discover the public domain network addresses configured on HA and other services on the system.

Type
26

Vendor ID
8164

VSA Type
60

Length
4

Value

Enumerated integer. Supported values are:

- No = 0 — Disabled
- Yes = 1 — Enabled

SN-IP-In-ACL

This attribute contains a definition for one Input IP Access Control List, which is used to filter the IP packets coming from the user. Note that more than one of these attributes can be included, in which case they are processed in the order in which they appear in the RADIUS Access-Accept.

Type

26

Vendor ID

8164

VSA Type

17

Length

1–253

Value

ASCII string

SN-IP-In-Plcy-Grp

This attribute specifies the name of the policy group configuration applied in the uplink direction.

Type

26

Vendor ID

8164

VSA Type

193

Length

1–15

Value

String

SN-IP-Out-ACL

This attribute contains a definition for one Output IP Access Control List, which is used to filter the IP packets sent to the user. Note that more than one of these attributes can be included, in which case they are processed in the order in which they appear in the RADIUS Access-Accept.

Type

26

Vendor ID
8164

VSA Type
18

Length
1–253

Value
ASCII string

SN-IP-Out-Plcy-Grp

This attribute specifies the name of the policy group configuration applied in the downlink direction.

Type
26

Vendor ID
8164

VSA Type
194

Length
1–15

Value
String

SN-IP-Pool-Name

This vendor-specific attribute indicates the name of the IP pool from which an IP address should be allocated to the subscriber. Also, see **Framed-Pool**, which is the standard attribute accomplishing the same.

Type
26

Vendor ID
8164

VSA Type
8

Length
1–253

Value
ASCII string

SN-IP-Source-Validation

This attribute indicates if the source IP address should be validated before forwarding the IP packet.

Type
26

Vendor ID
8164

VSA Type
14

Length
4

Value
Enumerated integer. Supported values are:

- No = 0 — No Validation
- Yes = 1 — Validated

SN-IP-Source-Violate-No-Acct

This attribute excludes the Source Violated IP packets and byte counts when reporting the Octet and Packet count in an accounting message.

If this AVP is present in Access Accept message the locally configured APN value will be overridden. If there is no value configured in the APN this value will not be applied to the session.

Type
26

Vendor ID
8164

VSA Type
196

Length
4

Value
Enumerated integer. Supported values are:

- Disabled = 0
- Enabled = 1

SN-IP-Src-Validation-Drop-Limit

Maximum number of packet drops entertained before disconnecting the session for source violated packets for the session.

Type
26

Vendor ID
8164

VSA Type
110

Length
4

Value
Unsigned integer

SN-IPv6-DNS-Proxy

IPV6 DNS proxy enabled or disabled setting for the session.

Type
26

Vendor ID
8164

VSA Type
126

Length
4

Value
Enumerated integer. Supported values are:

- Disabled = 0
- Enabled = 1

SN-IPv6-Egress-Filtering

This attribute enables egress filtering to make sure that packets being sent to the mobile device have an interface ID that matches that of the mobile device. This feature is meant to protect the Mobile from receiving unwanted packets from the Internet.

Type
26

Vendor ID
8164

VSA Type
103

Length
4

Value
Enumerated integer. Supported values are:

- Disabled = 0
- Enabled = 1

SN-IPv6-Min-Link-MTU

IPV6 MTU size.

Type
26

Vendor ID
8164

VSA Type
136

Length
4

Value
Unsigned integer

SN-IPv6-num-rtr-advt

This attribute indicates the IPv6 number of Initial Router Advertisements. The default value is 3.

Type
26

Vendor ID
8164

VSA Type
97

Length
4

Value
Unsigned integer

SN-IPv6-Primary-DNS

This attribute specifies a Primary DNS server address that the Router Advertisement message sent by the PDSN will include.

Type
26

Vendor ID
8164

VSA Type
101

Length
2

Value
IPv6 address

SN-IPv6-rtr-advt-interval

This attribute indicates the IPv6 Initial Router Advertisement Interval specified in milliseconds. The default value is 3000.

Type
26

Vendor ID
8164

VSA Type
96

Length
4

Value
Unsigned integer

SN-IPv6-Secondary-DNS

This attribute specifies a Secondary DNS server address that the Router Advertisement message sent by the PDSN will include.

Type
26

Vendor ID
8164

VSA Type
102

Length
16

Value
Opaque value

SN-IPv6-Sec-Pool

IPv6 secondary pool names.

Type
26

Vendor ID
8164

VSA Type
124

Length
1–253

Value
String

SN-IPv6-Sec-Prefix

IPv6 Secondary Pool name prefix.

Type
26

Vendor ID
8164

VSA Type
125

Length
2–18

Value
Opaque value

SN-ISC-Template-Name

This attribute contains name of the CSCF ISC template to be used for a subscriber.

Type
26

Vendor ID
8164

VSA Type
276

Length
0-255

Value
ASCII string

SN-Is-Unregistered-Subscriber

This attribute specifies if a subscriber is registered or not.

Type
26

Vendor ID
8164

VSA Type
269

Length
4

Value
ASCII string

SN-L3-to-L2-Tun-Addr-Policy

This attribute specifies the address allocation policy.

Type
26

Vendor ID
8164

VSA Type
43

Length
4

Value
Enumerated integer. Supported values are:

- no-local-alloc-validate = 0 — Do not locally allocate, do not validate
- local-alloc = 1 — Locally allocate
- local-alloc-validate = 2 — Locally allocate and validate

SN-Local-IP-Address

This attribute indicates the IP address of the local interface on the chassis for the user's session.

Type
26

Vendor ID
8164

VSA Type
13

Length
4

Value
IPv4 address

SN-Long-Duration-Action

This attribute specifies the action to take place when the long duration timeout expires for a subscriber session.

Type
26

Vendor ID
8164

VSA Type
45

Length

4

Value

Enumerated integer. Supported values are:

- Detection = 1 — Detect the session and alert the administrator
- Disconnection = 2 — Disconnect the session
- Dormant-Only-Disconnection = 3
- Dormant-Only-Detection = 4

SN-Long-Duration-Notification

SN-Long-Duration-Notification.

Type

26

Vendor ID

8164

VSA Type

253

Length

4

Value

Enumerated integer. Supported values are:

- Suppress = 0
- Send = 1

SN-Long-Duration-Timeout

This attribute is used to detect and if necessary disconnect sessions connected to the PDSN. This attribute configures the time period, in seconds, before either alerting the administrator or disconnecting the subscriber.

Type

26

Vendor ID

8164

VSA Type

44

Length

4

Value

Integer

SN-Max-Sec-Contexts-Per-Subs

Maximum secondary PDP contexts per subscriber.

Type
26

Vendor ID
8164

VSA Type
290

Length
2

Value
Unsigned integer

SN-Mediation-Acct-Rsp-Action

When this attribute is set to **None**, there is no action taken while waiting for a response for the accounting start message from the Mediation Accounting server. When this attribute is set to **No-Early-PDUs** the system buffers all packets from the user (uplink) until a response for the accounting start message is received from the Mediation Accounting server. When set to **Delay_GTP_Response**, the system does not send a GTP create PDP response to the GGSN until a response for the accounting start message is received from the Mediation Accounting server. If the AVP is not present in Access Accept message or if the AVP value is invalid, the value "**None**" is assumed.

Type
26

Vendor ID
8164

VSA Type
105

Length
4

Value
Enumerated integer. Supported values are:

- None = 0
- No_Early_PDUs = 1
- Delay_GTP_Response = 2

SN-Mediation-Enabled

This attribute indicates whether the Mediation Accounting configuration is enabled or disabled for GGSN.

If this AVP is not present in Access Accept message or if the AVP value is invalid, the locally configured APN value will be used.

Type

26

Vendor ID
8164

VSA Type
123

Length
4

Value
Enumerated integer. Supported values are:

- Disabled = 0
- Enabled = 1

SN-Mediation-No-Interims

This attribute is used to disable or enable Mediation Interim Accounting Records for the session.

If this AVP is not present in Access Accept message or if the AVP value is invalid, the locally configured APN value will be used.

Type
26

Vendor ID
8164

VSA Type
146

Length
4

Value
Enumerated integer. Supported values are:

- Disabled = 0
- Enabled = 1

SN-Mediation-VPN-Name

This attribute specifies the Mediation Context name for the session.

If this AVP is not received in the Access Accept message or if the AVP value is invalid, the locally configured APN value will be used.

Type
26

Vendor ID
8164

VSA Type
104

Length
1–128

Value
String

SN-Min-Compress-Size

This attribute specifies the minimum size (in octets) a data packet can have in order to be compressed.

Type
26

Vendor ID
8164

VSA Type
23

Length
4

Value
Unsigned integer

SN-MIP-AAA-Assign-Addr

This attribute specifies if the PDSN/FA will allow AAA to assign the home address. The default is to not allow AAA to assign the home address.

Type
26

Vendor ID
8164

VSA Type
50

Length
4

Value
Enumerated integer. Supported values are:

- Disabled = 0 — Do not allow AAA to assign home address
- Enabled = 1 — Allow AAA to assign home address

SN-MIP-ANCID

Accounting correlation ID created by IPGW, received by VBM and HBM.

Type
26

Vendor ID
8164

VSA Type
166

Length
12

Value
Opaque value

SN-MIP-Dual-Anchor

Enable/disable dual-anchor service for a subscriber.

Type
26

Vendor ID
8164

VSA Type
165

Length
4

Value
Enumerated integer. Supported values are:

- Disabled = 0
- Enabled = 1

SN-MIP-HA-Assignment-Table

MIP-HA Assignment Table name. When this is received in an Access Accept message, the system uses this local table to get the HA Address.

Type
26

Vendor ID
8164

VSA Type
154

Length
1–253

Value
ASCII string

SN-MIP-Match-AAA-Assign-Addr

This attribute specifies if the PDSN/FA will enforce that a non-zero AAA-specified home address must match the home address present in the MIP RRQ from the mobile node, and disconnect the subscriber session if a match is not present. The default is not to force the addresses to match.

Type
26

Vendor ID
8164

VSA Type
51

Length
4

Value
Enumerated integer. Supported values are:

- Disabled = 0 — Do not force the AAA-specified home address to match RRQ
- Enabled = 1 — Force the AAA-specified home address to match RRQ

SN-MIP-Reg-Lifetime-Realm

Configure the maximum MIP registration lifetime for a subscriber/realm.

Type
26

Vendor ID
8164

VSA Type
175

Length
2

Value
Unsigned integer

SN-MIP-Send-Ancid

This attribute enables/disables sending ANCID from FA to HA in MIP RRQ.

Type
26

Vendor ID
8164

VSA Type
163

Length
4

Value
Enumerated integer. Supported values are:

- Disabled = 0
- Enabled = 1

SN-MIP-Send-Correlation-Info

This attribute enables/disables sending of correlation-id from FA to HA in MIP RRQ.

Type
26

Vendor ID
8164

VSA Type
188

Length
4

Value
Enumerated integer. In StarOS 8.1 and earlier, supported values are:

- Disabled = 0
- Enabled = 1

In StarOS 8.3 and later, supported values are:

- Disabled = 0
- NVSE_Starent = 1
- NVSE_CUstom1 = 2
- NVSE_Custom2 = 3

SN-MIP-Send-Host-Config

This attribute is used to enable/disable Host Config Extension in MIP RRQ.

Type
26

Vendor ID
8164

VSA Type
311

Length
1

Value

Enumerated integer. Supported values are:

- Disabled = 0
- Enabled = 1

SN-MIP-Send-Imsi

AAA attribute to enable/disable sending IMSI from FA to HA in MIP RRQ.

Type

26

Vendor ID

8164

VSA Type

164

Length

4

Value

Enumerated integer. In StarOS and 8.1 and earlier, supported values are:

- None = 0
- Starent_NVSE = 1
- Custom1_NVSE = 2

In StarOS 8.3 and later, supported values are:

- Disabled = 0
- NVSE_Starent = 1
- NVSE_Custom1 = 2
- NVSE_Custom2 = 3

SN-MIP-Send-Term-Verification

This attribute specifies whether the PDSN/FA should send the Terminal Verification Normal Vendor/Organization Specific Extension (NVSE) in the Mobile IP RRQ message to the HA. The default is not to send the Terminal Verification NVSE.

Type

26

Vendor ID

8164

VSA Type

48

Length

4

Value

Enumerated integer. In StarOS 8.1 and earlier, supported values are:

- Disabled = 0 — Do not send
- Enabled = 1 — Send

In StarOS 8.3 and later, supported values are:

- Disabled = 0
- NVSE_Custom1 = 1 — Send custom NVSE
- NVSE_Custom2 = 2 — Send custom NVSE
- NVSE_Starent = 3 — Send custom NVSE

SN-MN-HA-Hash-Algorithm

This attribute contains the hash algorithm to use for MN-HA authentication.

Type
26

Vendor ID
8164

VSA Type
99

Length
4

Value
Enumerated integer. Supported values are:

- MD5 = 1
- MD5-RFC2002 = 2
- HMAC-MD5 = 3

SN-MN-HA-Timestamp-Tolerance

This attribute indicates the duration of timestamp tolerance, in seconds, to use for MN-HA authentication.

Type
26

Vendor ID
8164

VSA Type
30

Length
4

Value
Unsigned integer

SN-Mode

Robust Header Compression (ROHC) Mode. Reliable mode means each ROHC control needs to be Acknowledged. Optimistic mode is a modified version to reduce the number of control messages and bandwidth consumption. Unidirectional assumes a one way link without any Feedback from the decompressor.

Type
26

Vendor ID
8164

VSA Type
151

Length
4

Value
Enumerated integer. Supported values are:

- Reliable = 0
- Optimistic = 1
- Unidirectional = 2

SN-MS-ISDN

SN-MS-ISDN.

Type
26

Vendor ID
8164

VSA Type
248

Length
1–9

Value
Opaque value

SN-MSK-Lifetime

This attribute is currently not supported.

SN-NAI-Construction-Domain

This attribute specifies the domain name to use when constructing the NAI.

Type

26

Vendor ID
8164

VSA Type
37

Length
1–247

Value
String

SN-NAT-IP-Address

This attribute includes the NAT (public) IP address used for the call.

This attribute is also accepted in CoA request and response messages to be used in a currently active subscriber session.

Type
26

Vendor ID
8164

VSA Type
297

Length
4

Value
IPv4 address

SN-Node-Functionality

This attribute includes the functionality identifier of the IMS node where the cause code was generated.

Type
26

Vendor ID
8164

VSA Type
268

Length
4

Value
Enumerated integer. Supported values are:

- S-CSCF = 0
- P-CSCF = 1

- I-CSCF = 2

SN-NPU-Qos-Priority

This attribute configures Inter-Subscriber priority Queueing based on class of service offered. Gold has highest priority and Best_effort lowest priority. From DSCP, means the priority queueing will be done based on the DSCP marking the incoming subscriber packet carries.

Type
26

Vendor ID
8164

VSA Type
98

Length
4

Value
Enumerated integer. Supported values are:

- Best_Effort = 0
- Bronze = 1
- Silver = 2
- Gold = 3
- From_DSCP = 4

SN-Ntk-Initiated-Ctx-Ind-Flag

Indicates whether the GGSN call is a network initiated PDP Context.

Type
26

Vendor ID
8164

VSA Type
142

Length
1

Value
Opaque value

SN-Ntk-Session-Disconnect-Flag

SN-Ntk-Session-Disconnect-Flag.

Type

26

Vendor ID
8164

VSA Type
143

Length
4

Value
Enumerated integer. Supported value is:

- Session-Disconnect = 1

SN-Nw-Reachability-Server-Name

This attribute specifies the name of the Network Reachability Detection Server.

Type
26

Vendor ID
8164

VSA Type
65

Length
1–16

Value
String

SN-Originating-IOI

This attribute holds the Inter Operator Identifier for the originating network in the home network of the originating end user.

Type
26

Vendor ID
8164

VSA Type
261

Length
1–253

Value
ASCII string

SN-Overload-Disc-Connect-Time

This attribute provides inactivity time for session to become candidate for disconnection during overload.

Type
26

Vendor ID
8164

VSA Type
233

Length
4

Value
Unsigned integer

SN-Overload-Disc-Inact-Time

This attribute provides inactivity time for session to become candidate for disconnection during overload.

Type
26

Vendor ID
8164

VSA Type
234

Length
4

Value
Unsigned integer

SN-Overload-Disconnect

This attribute enables (if one) and disables the overload-disconnect feature for a subscriber.

Type
26

Vendor ID
8164

VSA Type
235

Length
4

Value
Unsigned integer

SN-PDG-TTG-Required

TTG mode of operation Required for PDG.

Type
26

Vendor ID
8164

VSA Type
299

Length
1

Value
Enumerated integer. Supported values are:

- No = 0
- Yes = 1

SN-PDIF-MIP-Release-TIA

PDIF mobile IP release TIA.

Type
26

Vendor ID
8164

VSA Type
172

Length
4

Value
Enumerated integer. Supported values are:

- No = 0
- Yes = 1

SN-PDIF-MIP-Required

PDIF mobile IP required.

Type
26

Vendor ID
8164

VSA Type
170

Length
4

Value
Enumerated integer. Supported values are:

- No = 0
- Yes = 1

SN-PDIF-MIP-Simple-IP-Fallback

PDIF mobile IP simple IP fallback.

Type
26

Vendor ID
8164

VSA Type
173

Length
4

Value
Enumerated integer. Supported values are:

- No = 0
- Yes = 1

SN-PDSN-Correlation-Id

Correlation ID received from PDSN to HA.

Type
26

Vendor ID
8164

VSA Type
189

Length
8

Value
Opaque value

SN-PDSN-Handoff-Req-IP-Addr

This attribute specifies if the PDSN should reject and terminate the subscriber session when the proposed address in IPCP by the mobile does not match the existing address in the PDSN. The default (Disabled) is not to reject these sessions.

Type
26

Vendor ID
8164

VSA Type
46

Length
4

Value
Enumerated integer. Supported values are:

- Disabled = 0 — Do not reject
- Enabled = 1 — Reject

SN-PDSN-NAS-Id

NAS Identifier received from PDSN to HA

Type
26

Vendor ID
8164

VSA Type
190

Length
1–253

Value
String

SN-PDSN-NAS-IP-Address

NAS IP address received from PDSN to HA.

Type
26

Vendor ID
8164

VSA Type
191

Length
4

Value
IPv4 address

SN-Permit-User-Mcast-PDUs

Specifies whether or not to let the subscriber discard multicast PDUs.

Type
26

Vendor ID
8164

VSA Type
134

Length
2

Value
Enumerated integer. Supported values are:

- disabled = 0
- enabled = 1

SN-PPP-Accept-Peer-v6Ifid

This attribute indicates the acceptance of the interface ID provided by peer during PPP IPv6CP if the ID is valid. The default is disabled.

Type
26

Vendor ID
8164

VSA Type
95

Length
4

Value
Enumerated integer. Supported values are:

- Disabled = 0 — Do not accept interface ID
- Enabled = 1 — Accept interface ID

SN-PPP-Always-On-Vse

SN-PPP-Always-On-Vse.

Type
26

Vendor ID
8164

VSA Type

130

Length

4

Value

Enumerated integer. Supported values are:

- Disabled = 0
- Enabled = 1

SN-PPP-Data-Compression

This attribute indicates the PPP data compression algorithm to use for the PPP session. The attribute value is a bit field, and many algorithms can be specified to indicate that one of these may be chosen by the user.

Type

26

Vendor ID

8164

VSA Type

9

Length

4

Value

Enumerated integer. Supported values are:

- None = 0
- Stac-LZS = 1
- MPPC = 2
- Deflate = 4

SN-PPP-Data-Compression-Mode

This attribute indicates the PPP data compression mode to use for the PPP session when PPP data compression is used.

Type

26

Vendor ID

8164

VSA Type

19

Length

4

Value

Enumerated integer. Supported values are:

- Normal = 0

- Stateless = 1

SN-PPP-Keepalive

This attribute indicates the interval for the PPP keepalive, in seconds.

Type
26

Vendor ID
8164

VSA Type
16

Length
4

Value
Unsigned integer

SN-PPP-NW-Layer-IPv4

This attribute indicates the PPP IPCP negotiation for IPv4. The default is enabled.

Type
26

Vendor ID
8164

VSA Type
92

Length
4

Value
Enumerated integer. Supported values are:

- Disabled = 0 — IPCP negotiation for IPv4 is disabled.
- Enabled = 1 — IPCP negotiation for IPv4 is enabled.
- Passive = 2 — Start the negotiation only if peer initiates it.

SN-PPP-NW-Layer-IPv6

This attribute indicates the PPP IPv6CP negotiation for IPv6. The default is enabled.

Type
26

Vendor ID
8164

VSA Type
93

Length
4

Value
Enumerated integer. Supported values are:

- Disabled = 0 — IPCP negotiation for IPv6 is disabled.
- Enabled = 1 — IPCP negotiation for IPv6 is enabled.
- Passive = 2 — Start the negotiation only if peer initiates it.

SN-PPP-Outbound-Password

This attribute indicates the password to be used when the user side of the PPP connection requires authentication.

Type
26

Vendor ID
8164

VSA Type
15

Length
1–247

Value
ASCII string

SN-PPP-Outbound-Username

This attribute indicates the username to be used when the user side of the PPP connection requires authentication.

Type
26

Vendor ID
8164

VSA Type
61

Length
1–247

Value
ASCII string

SN-PPP-Progress-Code

This attribute provides information about the “state” of the PPP connection, when the connection was terminated.

Type
26

Vendor ID
8164

VSA Type
4

Length
4

Value
Enumerated integer. Supported values are:

- Not-Defined = 0
- Call-Lcp-Down = 10
- Call-Disconnecting = 20
- Call-Ppp-Renegotiating = 30
- Call-Arrived = 40
- Call-Pdg-Tcp-Connecting = 45
- Call-Pdg-Ssl-Connecting = 46
- Call-Lcp-Up = 50
- Call-Authenticating = 60
- Call-Bcmcs-Authenticating = 70
- Call-Authenticated = 80
- Call-Tunnel-Connecting = 85
- Call-Ipcp-Up = 90
- Call-Imsa-Authorizing = 95
- Call-Imsa-Authorized = 97
- Call-MBMS-UE-Authorizing = 98
- Call-MBMS-Bearer-Authorizing = 99
- Call-Simple-IP-Connected = 100
- Call-Mobile-IP-Connected = 110
- Call-Tunnel-Connected = 115
- Call-Pdp-Type-IP-Connected = 120
- Call-Pdp-Type-IPv6-Connected = 125
- Call-Pdp-Type-PPP-Connected = 130
- Call-Proxy-Mobile-IP-Connected = 140
- Call-Pdg-Connected = 142
- Call-Pdg-Ssl-Connected = 141
- Call-Pdg-Connected = 142
- Call-Pdg-Connected = 142

- Call-Ipsg-Connected = 145
- Call-Bcmcs-Connected = 150
- Call-MBMS-UE-Connected = 155
- Call-MBMS-Bearer-Connected = 156
- Call-Pending-Addr-From-DHCP = 160
- Call-Got-Addr-From-DHCP = 170
- Call-HA-IPSEC-Tunnel-Connecting = 180
- Call-HA-IPSEC-Connected = 190
- Call-ASN-Non-Anchor-Connected = 200
- Call-ASNPC-Connected = 210
- Call-Mobile-IPv6-Connected = 220
- Call-PMIPv6-Connected = 221
- Call-PHSPC-Connected = 230
- Call-GTP-IPv4-Connected = 235
- Call-GTP-IPv6-Connected = 236
- Call-GTP-IPv4-IPv6-Connected = 237
- Call-SGW-Connected = 245
- Call-MME-Attached = 246
- Call-Auth-Only-Connected = 247

SN-PPP-Reneg-Disc

PPP remote reneg disconnect policy

Type
26

Vendor ID
8164

VSA Type
187

Length
4

Value
Enumerated integer. Supported values are:

- Never = 0
- Always = 1
- NAI_Prefix_MSID_Mismatch = 2

SN-Prepaid

Prepaid

Type
26

Vendor ID
8164

VSA Type
128

Length
4

Value
Enumerated integer. Supported values are:

- no_prepaid = 0
- custom_prepaid = 1
- standard_prepaid = 2
- wimax_prepaid = 4

SN-Prepaid-Compressed-Count

This attribute indicates if a Pre-paid subscriber's byte usage should be counted on the basis of compressed or uncompressed byte data over the subscriber's PPP connection to the system. If not present, the default is to count uncompressed byte data.

Type
26

Vendor ID
8164

VSA Type
31

Length
4

Value
Enumerated integer. Supported values are:

- Uncompressed = 0
- Compressed = 1

SN-Prepaid-Final-Duration-Alg

For prepaid, final duration is calculated based on the algorithm specified by the value of this attribute.

If this AVP is not received in the Access Accept message or if the AVP value is invalid, the locally configured APN value will be used.

Type

26

Vendor ID
8164

VSA Type
135

Length
4

Value
Enumerated integer. Supported values are:

- current_time = 0
- last-user-layer3-activity-time = 1
- last-airlink-activity-time = 2
- last-airlink-activity-time-last-reported = 3

SN-Prepaid-Inbound-Octets

In an Access-Accept, this indicates how many additional inbound (bytes delivered to the subscriber) byte credits should be granted to the subscriber. In an Accounting- Request, this indicates how many total inbound byte credits have been granted to the subscriber. When this attribute is not present in the Access-Accept, then pre-paid usage checking is disabled on an inbound octet basis.

Type
26

Vendor ID
8164

VSA Type
32

Length
4

Value
Unsigned integer

SN-Prepaid-Outbound-Octets

Type
26

Vendor ID
8164

VSA Type
33

Length
4

Value

Unsigned integer

SN-Prepaid-Preference

This attribute specifies whether prepaid is volume based or duration based.

Type
26

Vendor ID
8164

VSA Type
129

Length
4

Value
Enumerated integer. Supported values are:

- prepaid_duration = 0
- prepaid_volume = 1

SN-Prepaid-Timeout

This attribute indicates how much time may elapse before a new request for more pre-paid credits is issued. If the specified time has elapsed since the prior grant of credits was received from the RADIUS server, then a new request for credits is issued. This attribute is primarily used to periodically update the subscriber of new credits issued since the subscriber was connected. Note that credit requests will still be made on behalf of the subscriber when the subscriber drops down to the low watermark of credits (or zero if there is no low watermark). The presence or absence of this attribute does not affect that mechanism in any way. However, this timer is re-set whenever any grant of credits is received on behalf of the subscriber, regardless of why the grant of credits was requested.

Type
26

Vendor ID
8164

VSA Type
35

Length
4

SN-Prepaid-Total-Octets

In an Access-Accept, this attribute indicates how many additional byte credits (combining both inbound and outbound counts) should be granted to the subscriber. In an Accounting- Request, this indicates how many total bytes credits (combined inbound and outbound) have been granted to the subscriber. When this attribute is not present in the Access-Accept, then pre-paid usage checking is disabled on a combined inbound and outbound octet-count basis.

Type
26

Vendor ID
8164

VSA Type
34

Length
4

Value
Unsigned integer

SN-Prepaid-Watermark

This attribute Indicates the percentage of remaining granted credits that will trigger a new request to grant credits from the RADIUS server. For example, if 1GB of credits was granted to a user, and the value of SN-Prepaid-Watermark was 10, then when 100 MB of credits are remaining (900 MB have been used) to the subscriber, a new request for any new byte credits is issued on behalf of the subscriber. Note that when calculating the pre-paid low watermark, the total credits granted for the subscriber's entire session is used.

Type
26

Vendor ID
8164

VSA Type
36

Length
4

Value
Unsigned integer

SN-Primary-DCCA-Peer

This attribute indicates the name of the primary DCCA peer and primary DCCA realm.

If this AVP is received in Access Accept message, the primary DCCA peer is used for Gy functionality. If not present in the Access Accept message or if the AVP value is invalid, the locally configured APN value will be used.

Type
26

Vendor ID
8164

VSA Type
223

Length
1-192

Value
A colon separated string, like “primary_peer : primary_realm”

SN-Primary-DNS-Server

This attribute indicates the IP address of the primary DNS server that should be used for the session.

Type
26

Vendor ID
8164

VSA Type
5

Length
4

Value
IPv4 address

SN-Primary-NBNS-Server

Primary NBNS Server IP address.

Type
26

Vendor ID
8164

VSA Type
148

Length
4

Value
IPv4 address

SN-Proxy-MIP

This attribute specifies if the PDSN/FA will perform compulsory Proxy-MIP tunneling for a Simple-IP PDSN subscriber. This feature is licensed. The default is not to perform compulsory Proxy-MIP.

Type
26

Vendor ID
8164

VSA Type
52

Length
4

Value
Enumerated integer. Supported values are:

- Disabled = 0 — Do not perform compulsory Proxy-MIP
- Enabled = 1 — Perform compulsory Proxy-MIP

SN-Proxy-MIPV6

Enable/disable PMIPv6 for a subscriber.

Type
26

Vendor ID
8164

VSA Type
65530

Length
8

Value
Enumerated integer. Supported values are:

- Disabled = 0
- Enabled = 1

SN-Pseudonym-Username

This attribute contains the pseudonym user name generated by AAA server.

Type
26

Vendor ID
8164

VSA Type
305

Length
1-256

Value
Opaque value

SN-QoS-Background-Class

This attribute defines the QOS Background Traffic Class.

Type

26

Vendor ID
8164

VSA Type
91

Length
28 bytes

Value
Opaque value encoded in the following format:

- Byte 16 Bit 1 - Uplink Traffic Policing Enable/Disable
- Byte 16 Bit 2 - Downlink Traffic Policing Enable/Disable
- Byte 16 Bits 3,4 - Uplink Exceed Action
- Byte 16 Bits 5,6 - Downlink Exceed Action
- Byte 16 Bits 7,8 - Uplink Violate Action
- Byte 15 Bits 1,2 - Downlink Violate Action
- Byte 15 Bit 3 - Downlink Ext Peak Data Rate
- Byte 15 Bit 4 - Downlink Ext Committed Data Rate
- Byte 14 - Uplink Peak Data Rate
- Byte 13 - Downlink Peak Data Rate
- Byte 12 - Uplink Committed Data Rate
- Byte 11 - Downlink Committed Data Rate
- Byte 5-8 - Uplink Burst Size (in Network Byte Order)
- Byte 1-4 - Downlink Burst Size (in Network Byte Order)

SN-QoS-Class-Background-PHB

Quality of Service DSCP classification value.

Type
26

Vendor ID
8164

VSA Type
113

Length
4

Value
Enumerated integer. Supported values are:

- Best-Effort = 0
- Pass-Through = 1

- AF11 = 10
- AF12 = 12
- AF13 = 14
- AF21 = 18
- AF22 = 20
- AF23 = 22
- AF31 = 26
- AF32 = 28
- AF33 = 30
- AF41 = 34
- AF42 = 36
- AF43 = 38
- EF = 46

SN-QoS-Class-Conversational-PHB

Quality of Service DSCP classification value.

Type

26

Vendor ID

8164

VSA Type

111

Length

4

Value

Enumerated integer. Supported values are:

- Best-Effort = 0
- Pass-Through = 1
- AF11 = 10
- AF12 = 12
- AF13 = 14
- AF21 = 18
- AF22 = 20
- AF23 = 22
- AF31 = 26
- AF32 = 28
- AF33 = 30

- AF41 = 34
- AF42 = 36
- AF43 = 38
- EF = 46

SN-QoS-Class-Interactive-1-PHB

Interactive-1 class PHB value.

Type
26

Vendor ID
8164

VSA Type
114

Length
4

Value
Enumerated integer. Supported values are:

- Best-Effort = 0
- Pass-Through = 1
- AF11 = 10
- AF12 = 12
- AF13 = 14
- AF21 = 18
- AF22 = 20
- AF23 = 22
- AF31 = 26
- AF32 = 28
- AF33 = 30
- AF41 = 34
- AF42 = 36
- AF43 = 38
- EF = 46

SN-QoS-Class-Interactive-2-PHB

Interactive-2 class PHB.

Type
26

Vendor ID
8164

VSA Type
115

Length
4

Value
Enumerated integer. Supported values are:

- Best-Effort = 0
- Pass-Through = 1
- AF11 = 10
- AF12 = 12
- AF13 = 14
- AF21 = 18
- AF22 = 20
- AF23 = 22
- AF31 = 26
- AF32 = 28
- AF33 = 30
- AF41 = 34
- AF42 = 36
- AF43 = 38
- EF = 46

SN-QoS-Class-Interactive-3-PHB

Interactive-3 class PHB.

Type
26

Vendor ID
8164

VSA Type
115

Length
4

Value
Enumerated integer. Supported values are:

- Best-Effort = 0
- Pass-Through = 1

- AF11 = 10
- AF12 = 12
- AF13 = 14
- AF21 = 18
- AF22 = 20
- AF23 = 22
- AF31 = 26
- AF32 = 28
- AF33 = 30
- AF41 = 34
- AF42 = 36
- AF43 = 38
- EF = 46

SN-QoS-Class-Streaming-PHB

Quality of Service DSCP classification value.

Type
26

Vendor ID
8164

VSA Type
112

Length
4

Value
Enumerated integer. Supported values are:

- Best-Effort = 0
- Pass-Through = 1
- AF11 = 10
- AF12 = 12
- AF13 = 14
- AF21 = 18
- AF22 = 20
- AF23 = 22
- AF31 = 26
- AF32 = 28
- AF33 = 30

- AF41 = 34
- AF42 = 36
- AF43 = 38
- EF = 46

SN-QoS-Conversation-Class

This attribute defines the QOS Conversation Traffic Class.

Type

26

Vendor ID

8164

VSA Type

86

Length

28 bytes

Value

Opaque value encoded in the following format:

- Byte 16 Bit 1 - Uplink Traffic Policing Enable/Disable
- Byte 16 Bit 2 - Downlink Traffic Policing Enable/Disable
- Byte 16 Bits 3,4 - Uplink Exceed Action
- Byte 16 Bits 5,6 - Downlink Exceed Action
- Byte 16 Bits 7,8 - Uplink Violate Action
- Byte 15 Bits 1,2 - Downlink Violate Action
- Byte 15 Bit 3 - Downlink Ext Peak Data Rate
- Byte 15 Bit 4 - Downlink Ext Committed Data Rate
- Byte 14 - Uplink Peak Data Rate
- Byte 13 - Downlink Peak Data Rate
- Byte 12 - Uplink Committed Data Rate
- Byte 11 - Downlink Committed Data Rate
- Byte 5-8 - Uplink Burst Size (in Network Byte Order)
- Byte 1-4 - Downlink Burst Size (in Network Byte Order)

SN-QOS-HLR-Profile

QoS with Allocation Retention bit. QoS structured as per 29.002.

This attribute is also accepted in CoA request message to be used in a currently active subscriber session.

Type

26

Vendor ID
8164

VSA Type
303

Length
1–35

Value
Opaque value

SN-QoS-Interactive1-Class

This attribute defines the QOS Interactive TrafficClass.

Type
26

Vendor ID
8164

VSA Type
88

Length
28 bytes

Value
Opaque value encoded in the following format:

- Byte 16 Bit 1 - Uplink Traffic Policing Enable/Disable
- Byte 16 Bit 2 - Downlink Traffic Policing Enable/Disable
- Byte 16 Bits 3,4 - Uplink Exceed Action
- Byte 16 Bits 5,6 - Downlink Exceed Action
- Byte 16 Bits 7,8 - Uplink Violate Action
- Byte 15 Bits 1,2 - Downlink Violate Action
- Byte 15 Bit 3 - Downlink Ext Peak Data Rate
- Byte 15 Bit 4 - Downlink Ext Committed Data Rate
- Byte 14 - Uplink Peak Data Rate
- Byte 13 - Downlink Peak Data Rate
- Byte 12 - Uplink Committed Data Rate
- Byte 11 - Downlink Committed Data Rate
- Byte 5-8 - Uplink Burst Size (in Network Byte Order)
- Byte 1-4 - Downlink Burst Size (in Network Byte Order)

SN-QoS-Interactive2-Class

This attribute defines the QOS Interactive2 Traffic Class.

Type
26

Vendor ID
8164

VSA Type
89

Length
28 bytes

Value
Opaque value encoded in the following format:

- Byte 16 Bit 1 - Uplink Traffic Policing Enable/Disable
- Byte 16 Bit 2 - Downlink Traffic Policing Enable/Disable
- Byte 16 Bits 3,4 - Uplink Exceed Action
- Byte 16 Bits 5,6 - Downlink Exceed Action
- Byte 16 Bits 7,8 - Uplink Violate Action
- Byte 15 Bits 1,2 - Downlink Violate Action
- Byte 15 Bit 3 - Downlink Ext Peak Data Rate
- Byte 15 Bit 4 - Downlink Ext Committed Data Rate
- Byte 14 - Uplink Peak Data Rate
- Byte 13 - Downlink Peak Data Rate
- Byte 12 - Uplink Committed Data Rate
- Byte 11 - Downlink Committed Data Rate
- Byte 5-8 - Uplink Burst Size (in Network Byte Order)
- Byte 1-4 - Downlink Burst Size (in Network Byte Order)

SN-QoS-Interactive3-Class

This attribute defines the QOS Interactive3 Traffic Class.

Type
26

Vendor ID
8164

VSA Type
90

Length
28 bytes

Value
Opaque value encoded in the following format:

- Byte 16 Bit 1 - Uplink Traffic Policing Enable/Disable
- Byte 16 Bit 2 - Downlink Traffic Policing Enable/Disable

- Byte 16 Bits 3,4 - Uplink Exceed Action
- Byte 16 Bits 5,6 - Downlink Exceed Action
- Byte 16 Bits 7,8 - Uplink Violate Action
- Byte 15 Bits 1,2 - Downlink Violate Action
- Byte 15 Bit 3 - Downlink Ext Peak Data Rate
- Byte 15 Bit 4 - Downlink Ext Committed Data Rate
- Byte 14 - Uplink Peak Data Rate
- Byte 13 - Downlink Peak Data Rate
- Byte 12 - Uplink Committed Data Rate
- Byte 11 - Downlink Committed Data Rate
- Byte 5-8 - Uplink Burst Size (in Network Byte Order)
- Byte 1-4 - Downlink Burst Size (in Network Byte Order)

SN-QoS-Negotiated

Negotiated QoS for GGSN sessions.

Type
26

Vendor ID
8164

VSA Type
147

Length
In 10.2 and earlier releases: 4–17

In 11.0 and later releases: 4–20

Value
ASCII string

SN-QoS-Renegotiation-Timeout

This attribute configures the timeout duration of dampening time for dynamic QoS renegotiation.

Type
26

Vendor ID
8164

VSA Type
145

Length
4

Value

Unsigned integer

SN-QoS-Streaming-Class

This attribute defines the QOS Streaming Traffic Class.

Type
26

Vendor ID
8164

VSA Type
87

Length
28 bytes

Value
Opaque value encoded in the following format:

- Byte 16 Bit 1 - Uplink Traffic Policing Enable/Disable
- Byte 16 Bit 2 - Downlink Traffic Policing Enable/Disable
- Byte 16 Bits 3,4 - Uplink Exceed Action
- Byte 16 Bits 5,6 - Downlink Exceed Action
- Byte 16 Bits 7,8 - Uplink Violate Action
- Byte 15 Bits 1,2 - Downlink Violate Action
- Byte 15 Bit 3 - Downlink Ext Peak Data Rate
- Byte 15 Bit 4 - Downlink Ext Committed Data Rate
- Byte 14 - Uplink Peak Data Rate
- Byte 13 - Downlink Peak Data Rate
- Byte 12 - Uplink Committed Data Rate
- Byte 11 - Downlink Committed Data Rate
- Byte 5-8 - Uplink Burst Size (in Network Byte Order)
- Byte 1-4 - Downlink Burst Size (in Network Byte Order)

SN-QoS-Tp-Dnlk

This attribute enables/disables Traffic Policing/Shaping in downlink direction.

This attribute is also accepted in CoA request message to be used in a currently active subscriber session.

Type
26

Vendor ID
8164

VSA Type

73

Length

4

Value

Enumerated integer. Supported values are:

- Disabled = 0
- Policing = 1
- Shaping = 2

SN-QoS-Tp-Uplk

This attribute enables/disables Traffic Policing/Shaping in uplink direction.

This attribute is also accepted in CoA request message to be used in a currently active subscriber session.

Type

26

Vendor ID

8164

VSA Type

79

Length

4

Value

Enumerated integer. Supported values are:

- Disabled = 0
- Policing = 1
- Shaping = 2

SN-QoS-Traffic-Policy

This compound attribute simplifies sending QoS values for Traffic Class, Direction, Burst-Size, Committed-Data-Rate, Peak-Data-Rate, Exceed-Action, and Violate-Action from the RADIUS server. When the SN-QoS-Traffic-Policy attribute is sent along with Acct-Session-ID attribute, the system matches the particular PDP context, and applies the new policy and retains the policy with the subscriber profile for future use. The next time the system sends a CoA request with a new policy and a different Acct-Session-ID for the same subscriber, the previously received policy is also applied to the matching PDP context along with the new policy.

Important: This attribute is specific to the GGSN service.

This attribute is also accepted in CoA request message to be used in a currently active subscriber session.

Type

26

Vendor ID
8164

VSA Type
177

Value
Contains the following subattributes:

Direction

Direction of traffic.

This attribute is also accepted in CoA request message to be used in a currently active subscriber session.

Type
1

Length
1

Value
Unsigned integer. Supported values are:

- Downlink = 0
- Uplink = 1

Class

Traffic class.

Type
2

Length
1

Value
Unsigned integer. Supported values are:

- Undefined = 0
- Conversational = 1
- Streaming = 2
- Interactive TP 1 = 4
- Interactive TP 2 = 5
- Interactive TP 3 = 6
- Background = 7

Burst-Size

Peak burst size.

This attribute is also accepted in CoA request message to be used in a currently active subscriber session.

Type

3

Length

4

Value

Unsigned integer

Committed-Data-Rate

Committed data rate.

This attribute is also accepted in CoA request message to be used in a currently active subscriber session.

Type

4

Length

4

Value

Unsigned integer

Peak-Data-Rate

Peak data rate.

This attribute is also accepted in CoA request message to be used in a currently active subscriber session.

Type

5

Length

4

Value

Unsigned integer

Exceed-Action

Action to take on packets that exceed the Committed-Data-Rate but do not violate the Peak-Data-Rate.

This attribute is also accepted in CoA request message to be used in a currently active subscriber session.

Type

6

Length

1

Value

Unsigned integer. Supported values are:

- Transmit = 0
- Drop = 1
- Lower IP Precedence = 2

Violate-Action

Violate action.

This attribute is also accepted in CoA request message to be used in a currently active subscriber session.

Type

7

Length

1

Value

Unsigned integer. Supported values are:

- Transmit = 0
- Drop = 1
- Lower IP Precedence = 2
- Buffer = 3
- Buffer-Transmit-On-Full = 4

Auto-Readjust-Enabled

Available only in StarOS 8.1 and later. Auto-readjust enabled.

This attribute is also accepted in CoA request message to be used in a currently active subscriber session.

Type

8

Length

1

Value

Unsigned integer

Auto-Readjust-Duration

Available only in StarOS 8.1 and later. Auto-readjust duration.

This attribute is also accepted in CoA request message to be used in a currently active subscriber session.

Type

9

Length

4

Value
Unsigned integer

Qci

Available only in 11.0 and later releases. QOS QCI accepted values are 1 (qci 1), 2 (qci 2), 3 (qci 3), 4 (qci 4), 5 (qci 5), 6 (qci 6), 7 (qci 7), 8 (qci 8), 9 (qci 9).

Type
10

Length
1

Value
Unsigned integer

SN-Rad-APN-Name

This attributes specifies the RADIUS returned APN name.

If this AVP is not present in the Access Accept message or if the AVP value is invalid, the SGSN supplied APN value in create PDP context will be used for the session.

Type
26

Vendor ID
8164

VSA Type
162

Length
1–64

Value
Opaque value

SN-Radius-Returned-Username

This attribute is used to prefer RADIUS returned user name over constructed user name in the accounting messages.

Type
26

Vendor ID
8164

VSA Type
236

Length
4

Value

Enumerated integer. Supported values are:

- No = 0
- Yes = 1

SN-Re-CHAP-Interval

The Periodic CHAP authentication interval for PPP, in seconds.

Type
26

Vendor ID
8164

VSA Type
7

Length
4

Value
Unsigned integer

SN-Roaming-Behavior

This attribute specifies the configuration for the behavior bits settings for a roaming subscriber in an APN.

When GGSN is configured to reject the charging characteristics sent by the SGSN for "roaming" subscribers, it uses the profile index specified by **`cc-home behavior <bits> profile <index>`** command to determine the appropriate CCs to use.

Multiple behavior bits can be configured for a single profile index by "Or"ing the bit strings together and convert the result to hexadecimal. The properties of the actual CC profile index are configured as part of the GGSN service using the cc profile command.

If this AVP is present in Access Accept message the locally configured APN value will be overridden.

Type
26

Vendor ID
8164

VSA Type
121

Length
4

Value
Unsigned integer

SN-Roaming-Profile

This attribute specifies the configuration for the profile bits settings for a roaming subscriber in an APN.

If this AVP is present in Access Accept message the locally configured APN value will be overridden.

Type

26

Vendor ID

8164

VSA Type

118

Length

4

Value

Unsigned integer

SN-Roaming-Sub-Use-GGSN

This attribute configures GGSN to accept GGSN's charging characteristics for roaming subscribers defined for the APN.

If this AVP is present in Access Accept message the locally configured APN value will be overridden.

Type

26

Vendor ID

8164

VSA Type

108

Length

4

Value

Enumerated integer. Supported values are:

- Deny = 0
- Accept = 1

SN-ROHC-Flow-Marking-Mode

Configure ROHC compression for marked flows only.

Type

26

Vendor ID

8164

VSA Type

274

Length
4

Value
Enumerated integer. Supported values are:

- False = 0
- True = 1

SN-ROHC-Mode

ROHC Mode.

Type
26

Vendor ID
8164

VSA Type
151

Length
4

Value
An integer in network order. Supported values are:

- Reliable = 0
- Optimistic = 1
- Unidirectional = 2

SN-ROHC-Profile-Name

Specifies the ROHC profile to use for the subscriber.

Type
26

Vendor ID
8164

VSA Type
238

Length
1–64

Value
ASCII string

SN-Role-Of-Node

This attribute denotes the role of the CSCF.

Type
26

Vendor ID
8164

VSA Type
256

Length
4

Value
Enumerated integer. Supported values are:

- ORIGINATING_ROLE = 0
- TERMINATING_ROLE = 1

SN-Routing-Area-Id

For GGSN calls this indicates the Routing Area ID of the subscriber.

Type
26

Vendor ID
8164

VSA Type
249

Length
3

Value
String

SN-Rulebase

When the session is active charging enabled, Rulebase name will specify one of the pre-configured ECSv2 rulebases in active charging subsystem.

This attribute is also accepted in CoA request message to be used in a currently active subscriber session.

If this AVP is present in Access Accept message the locally configured APN value will be overridden. If there is no value configured in the APN, this value will not be applied to the session.

Type
26

Vendor ID
8164

VSA Type
250

Length
1–64

Value
String

SN-SDP-Media-Components

This attribute is currently not supported. See *SN-CSCF-Rf-SDP-Media-Components*.

SN-SDP-Session-Description

This attribute contains the Session portion of the SDP data exchanged between the User Agents in the SIP transaction.

Type
26

Vendor ID
8164

VSA Type
263

Length
4

Value
ASCII string

SN-Sec-IP-Pool-Name

Available only in StarOS 8.1 and later. This attribute contains the secondary IP pool name.

Type
26

Vendor ID
8164

VSA Type
265

Length
1–253

Value
String

SN-Secondary-DCCA-Peer

This attribute indicates the name of the Secondary DCCA peer and Secondary DCCA realm.

If this AVP is received in Access Accept message the secondary DCCA peer is used for Gy functionality. If not present in the Access Accept message or if the AVP value is invalid, the locally configured APN value will be used.

Type

26

Vendor ID
8164

VSA Type
224

Length
1–192

Value
A colon separated string, like “secondary_peer : secondary_realm”.

SN-Secondary-DNS-Server

This attribute indicates the IP address of the secondary DNS server that should be used for the session.

Type
26

Vendor ID
8164

VSA Type
6

Length
4

Value
IPv4 address

SN-Secondary-NBNS-Server

Secondary NBNS server IP address.

Type
26

Vendor ID
8164

VSA Type
149

Length
4

Value
IPv4 address

SN-Served-Party-Address

This attribute is currently not supported.

SN-Service-Address

Used to send bind IP address of the service in RADIUS messages.

Type
26

Vendor ID
8164

VSA Type
169

Length
4

Value
IPv4 address

SN-Service-Type

This attribute indicates the service type that the user is accessing.

Type
26

Vendor ID
8164

VSA Type
24

Length
4

Value
Enumerated integer. Supported values are:

- None = 0
- PDSN = 1
- Management = 2
- HA = 3
- GGSN = 4
- LNS = 5
- IPSG = 6
- CSCF = 7
- ASNGW = 8
- PDIF = 9
- STANDALONE_FA = 10
- SGSN = 11
- PHSGW = 12

- PDG = 13
- MIPV6HA = 14
- PGW = 15
- SGW = 16
- FNG = 17
- OGW = 18 — NOTE: Applicable only in release 12.0.
- HNBGW = 19
- BNG = 20

SN-Session-Id

This attribute contains Call-ID of the SIP session.

Type
26

Vendor ID
8164

VSA Type
257

Length
4

Value
ASCII string

SN-Simultaneous-SIP-MIP

This attribute indicates if a PDSN Subscriber can simultaneously be given Simple IP and Mobile IP service.

Type
26

Vendor ID
8164

VSA Type
22

Length
4

Value
Enumerated integer. Supported values are:

- Disabled = 0
- Enabled = 1

SN-SIP-Method

This attribute identifies the SIP-method for which acct request is sent.

Type
26

Vendor ID
8164

VSA Type
254

Length
4

Value
ASCII string

SN-SIP-Request-Time-Stamp

This attribute specifies the time of initial SIP request.

Type
26

Vendor ID
8164

VSA Type
258

Length
4

Value
ASCII string

SN-SIP-Response-Time-Stamp

This attribute specifies the time of response to initial SIP request.

Type
26

Vendor ID
8164

VSA Type
259

Length
4

Value
ASCII string

SN-Software-Version

Provides the Software version. This contains the major version number, minor version number and build number.

Type
26

Vendor ID
8164

VSA Type
288

Length
1–32

Value
ASCII string

SN-Subs-Acc-Flow-Traffic-Valid

This attribute indicates the subscriber account flow traffic is valid.

Type
26

Vendor ID
8164

VSA Type
225

Length
4

Value
Enumerated integer. Supported values are:

- Disable = 0
- Enable = 1

SN-Subscriber-Accounting

This attribute specifically enables or disables subscriber accounting. Note that if enabled, subscriber accounting still needs to be enabled in the subscriber's AAA context for accounting to be performed.

The AVP value 0 means no accounting; 1 indicates RADIUS accounting; and 2 indicates GTPP accounting. If an invalid value is received or if the AVP is not present in the Access Accept message, the locally configured APN value will be used.

Type
26

Vendor ID
8164

VSA Type
64

Length
4

Value
Enumerated integer. Supported values are:

- None = 0
- Radius = 1
- GTPP = 2

SN-Subscriber-Acct-Interim

This attribute specifies if accounting INTERIM messages are enabled for the subscriber. Note that accounting must also be globally enabled for the subscriber (SN-Subscriber-Accounting), and enabled for the subscriber's AAA context (along with a specific INTERIM interval), if accounting INTERIM messages are to be sent.

The AVP value 0 represents normal or enabled for generating accounting START messages. The value 1 represents enabled for suppressing RADIUS accounting START messages.

If the AVP is not present in the Access Accept message or if the AVP value is invalid, the value 0 is assumed.

Type
26

Vendor ID
8164

VSA Type
70

Length
4

Value
Enumerated integer. Supported values are:

- Normal = 0
- Suppress = 1

SN-Subscriber-Acct-Mode

This attribute contains the subscriber accounting mode.

Type
26

Vendor ID
8164

VSA Type
192

Length

4

Value

Enumerated integer. Supported values are:

- flow-based-auxilliary = 0
- flow-based-all = 1
- flow-based-none = 2
- session-based = 3
- main-a10-only = 4

SN-Subscriber-Acct-Rsp-Action

When this attribute is set to None, there is no action taken while waiting for a response for the accounting start message from the RADIUS server. When this attribute is set to No-Early-PDUs the system buffers all packets from the user (uplink) until a response for the accounting start message is received from the RADIUS server. When set to Delay_GTP_Response, the system does not send a GTP create response to the GGSN until a response for the accounting start message is received from the RADIUS server.

Type

26

Vendor ID

8164

VSA Type

100

Length

4

Value

Enumerated integer. Supported values are:

- None = 0
- No_Early_PDUs = 1
- Delay_GTP_Response = 2

SN-Subscriber-Acct-Start

This attribute specifies if accounting START messages are enabled for the subscriber. Note that accounting must also be globally enabled for the subscriber (SN-Subscriber-Accounting), and enabled for the subscriber's AAA context, if accounting START messages are to be sent.

The AVP value 0 represents normal or enabled for generating accounting START messages. The value 1 represents enabled for suppressing RADIUS accounting START messages.

If the AVP is not present in the Access Accept message or if the AVP value is invalid, the value 0 is assumed.

Type

26

Vendor ID

8164

VSA Type
69

Length
4

Value
Enumerated integer. Supported values are:

- Normal = 0
- Suppress = 1

SN-Subscriber-Acct-Stop

This attribute specifies if accounting STOP messages are enabled for the subscriber. Note that accounting must also be globally enabled for the subscriber (**SN-Subscriber-Accounting**), and enabled for the subscriber's AAA context, if accounting STOP messages are to be sent.

The AVP value 0 represents normal or enabled for generating accounting STOP messages. The value 1 represents enabled for suppressing RADIUS accounting STOP messages.

If the AVP is not present in the Access Accept message or if the AVP value is invalid, the value 0 is assumed.

Type
26

Vendor ID
8164

VSA Type
71

Length
4

Value
Enumerated integer. Supported values are:

- Normal = 0
- Suppress = 1

SN-Subscriber-Class

Customer-specific attribute to support specific subscriber billing behavior.

Type
26

Vendor ID
8164

VSA Type
219

Length

4

Value

Enumerated integer. Supported values are:

- Normal_Subscriber = 0
- Ting_100 = 1
- Ting_500 = 2
- Ting_Buddy = 3
- Ting_Star = 4
- Ting_Nolimit_SMS = 5
- Kids_Locator = 6
- Ting_2000 = 7
- Handicapped_Welfare = 8
- Reserved = 9

SN-Subscriber-Dormant-Activity

This attribute specifies whether to treat dormant packets routed to the mobile as activity for idle timeout purposes. The default is Enabled. Disabled means dormant packets routed to the mobile is not treated as activity for idle timeout purposes.

Type

26

Vendor ID

8164

Length

4

Value

Enumerated integer. Supported values are:

- Disabled = 0
- Enabled = 1

SN-Subscriber-IP-Hdr-Neg-Mode

This attribute specifies whether to wait (detect) for IP header compression to be requested by the mobile before responding, or not to wait (force). Force is the default.

Type

26

Vendor ID

8164

VSA Type

67

Length

4

Value

Enumerated integer. Supported values are:

- Force = 0
- Detect = 1

SN-Subscriber-IP-TOS-Copy

This attribute controls the copying of the IP TOS octet value from IPv4 datagrams to the IP header in tunnel encapsulation.

Type

26

Vendor ID

8164

VSA Type

85

Length

4

Value

Enumerated integer. Supported values are:

- None = 0
- Access-Tunnel = 1
- Data-Tunnel = 2
- Both = 3

SN-Subscriber-Nexthop-Address

This attribute specifies the nexthop gateway address to be returned by AAA on a per subscriber basis.

Type

26

Vendor ID

8164

VSA Type

127

Length

4

Value

IPv4 address

SN-Subscriber-No-Interims

This is a GGSN specific attribute. When set to 0 (disabled) interim accounting is generated. When set to 1 (enabled) interim accounting generation is disabled.

If the AVP is not present in the Access Accept message or if the AVP value is invalid, the value 0 is assumed.

Type

26

Vendor ID

8164

VSA Type

133

Length

4

Value

Enumerated integer. Supported values are:

- Enabled = 0
- Disabled = 1

SN-Subscriber-Permission

This attribute indicates the services allowed to be delivered to the subscriber. The attribute value is a bit field, and many algorithms can be specified to indicate that one of these may be chosen by the user.

Type

26

Vendor ID

8164

VSA Type

20

Length

4

Value

Enumerated integer. In StarOS 8.1 and earlier, supported values are:

- None = 0
- Simple-IP = 1
- Mobile-IP = 2
- Simple-IP-Mobile-IP = 3
- HA-Mobile-IP = 4
- Simple-IP-HA-Mobile-IP = 5
- Mobile-IP-HA-Mobile-IP = 6
- All = 7

In StarOS 8.3 and later, supported values are:

- None = 0
- Simple-IP = 1
- Mobile-IP = 2
- Simple-IP-Mobile-IP = 3
- HA-Mobile-IP = 4
- Simple-IP-HA-Mobile-IP = 5
- Mobile-IP-HA-Mobile-IP = 6
- SIP-MIP-HA-MIP = 7
- GGSN-PDP-TYPE-IP = 0x08, # see SessSubscriberPermission in sess_common.x
- GGSN-PDP-TYPE-PPP = 0x10, # see SessSubscriberPermission in sess_common.x
- Network-Mobility = 0x20
- FA-HA-NEMO = 0x26
- All = 0x3F

SN-Subscriber-Template-Name

RADIUS returned subscriber template.

Type
26

Vendor ID
8164

VSA Type
158

Length
1–127

Value
String

SN-Subs-IMSA-Service-Name

IMS authorization service name.

Type
26

Vendor ID
8164

VSA Type
159

Length
1–128

Value
String

SN-Subs-VJ-Slotid-Cmp-Neg-Mode

Enable/Disable slot ID compression in either direction when using VJ compression.

Type
26

Vendor ID
8164

VSA Type
221

Length
4

Value
Enumerated integer. Supported values are:

- None = 0
- Receive = 1
- Transmit = 2
- Both = 3

SN-Transparent-Data

This AVP is used by RADIUS to provide Global Title information for the GGSN to use in CDRs and Quota Auth.

Type
26

Vendor ID
8164

VSA Type
247

Length
In StarOS 8.1 and later: 1–247

In StarOS 8.0: 1–237

Value
Opaque value

SN-Terminating-IOI

This attribute holds the Inter Operator Identifier for the originating network in the home network of the terminating end user.

Type
26

Vendor ID
8164

VSA Type
262

Length
4

Value
ASCII string

SN-Tp-Dnlk-Burst-Size

This attribute specifies the Traffic Policing downlink burst size in bytes.

This attribute is also accepted in CoA request message to be used in a currently active subscriber session.

Type
26

Vendor ID
8164

VSA Type
76

Length
4

Value
Unsigned integer

SN-Tp-Dnlk-Committed-Data-Rate

This attribute specifies the Traffic Policing downlink committed data rate in bps.

This attribute is also accepted in CoA request message to be used in a currently active subscriber session.

Type
26

Vendor ID
8164

VSA Type
74

Length
4

Value
Unsigned integer

SN-Tp-Dnlk-Exceed-Action

This attribute specifies the action to take on Traffic Policing downlink packets that exceed the committed-data-rate but do not violate the peak-data-rate.

This attribute is also accepted in CoA request message to be used in a currently active subscriber session.

Type

26

Vendor ID

8164

VSA Type

77

Length

4

Value

Enumerated integer. Supported values are:

- Transmit = 0
- Drop = 1
- Lower-IP-Precedence = 2
- Buffer = 3
- Transmit-On-Buffer-Full = 4

SN-Tp-Dnlk-Peak-Data-Rate

This attribute specifies the Traffic Policing downlink peak data rate in bps.

This attribute is also accepted in CoA request message to be used in a currently active subscriber session.

Type

26

Vendor ID

8164

VSA Type

75

Length

4

Value

Unsigned integer

SN-Tp-Dnlk-Violate-Action

This attribute specifies the action to take on Traffic Policing downlink packets that exceed both the committed-data-rate and the peak-data-rate.

This attribute is also accepted in CoA request message to be used in a currently active subscriber session.

Type
26

Vendor ID
8164

VSA Type
78

Length
4

Value
Enumerated integer. Supported values are:

- Transmit = 0
- Drop = 1
- Lower-IP-Precedence = 2
- Buffer = 3
- Transmit-On-Buffer-Full = 4

SN-Tp-Uplk-Burst-Size

This attribute specifies the Traffic Policing uplink burst size in bytes.

This attribute is also accepted in CoA request message to be used in a currently active subscriber session.

Type
26

Vendor ID
8164

VSA Type
82

Length
4

Value
Unsigned integer

SN-Tp-Uplk-Committed-Data-Rate

This attribute specifies the Traffic Policing uplink committed data rate in bps.

This attribute is also accepted in CoA request message to be used in a currently active subscriber session.

Type
26

Vendor ID
8164

VSA Type
80

Length
4

Value
Unsigned integer

SN-Tp-Uplk-Exceed-Action

This attribute specifies the action to take on Traffic Policing uplink packets that exceed the committed-data-rate but do not violate the peak-data-rate.

This attribute is also accepted in CoA request message to be used in a currently active subscriber session.

Type
26

Vendor ID
8164

VSA Type
83

Length
4

Value
Enumerated integer. Supported values are:

- Transmit = 0
- Drop = 1
- Lower-IP-Precedence = 2
- Buffer = 3
- Transmit-On-Buffer-Full = 4

SN-Tp-Uplk-Peak-Data-Rate

This attribute specifies the Traffic Policing Uplink Peak Data Rate in bps.

This attribute is also accepted in CoA request message to be used in a currently active subscriber session.

Type
26

Vendor ID
8164

VSA Type
81

Length
4

Value
Unsigned integer

SN-Tp-Uplk-Violate-Action

This attribute specifies the action to take on Traffic Policing uplink packets that exceed both the committed-data-rate and the peak-data-rate.

This attribute is also accepted in CoA request message to be used in a currently active subscriber session.

Type

26

Vendor ID

8164

VSA Type

84

Length

4

Value

Enumerated integer. Supported values are:

- Transmit = 0
- Drop = 1
- Lower-IP-Precedence = 2
- Buffer = 3
- Transmit-On-Buffer-Full = 4

SN-TPO-Policy

This attribute contains the TPO policy name.

Type

26

Vendor ID

8164

VSA Type

308

Length

1–63

Value

String

SN-Traffic-Group

This attribute is used to assign a tag to an FA or a group of FAs, so that traffic policy can be enforced based on the tag value.

Type

26

Vendor ID
8164

VSA Type
161

Length
2

Value
Unsigned integer

SN-TrafficSelector-Class

The ipsec traffic selector class.

Type
26

Vendor ID
8164

VSA Type
307

Length
4

Value
Unsigned integer

SN-Tun-Addr-Policy

Describes IP address validation policy for non L2TP tunneled calls.

Type
26

Vendor ID
8164

VSA Type
156

Length
4

Value
Enumerated integer. Supported values are:

- no-local-alloc-validate = 0
- local-alloc = 1
- local-alloc-validate = 2

SN-Tunnel-Gn

Used to enable/disable Gn interface from PDG/TTG to GGSN.

Type
26

Vendor ID
8164

VSA Type
174

Length
4

Value
Enumerated integer. Supported values are:

- Disabled = 0
- Enabled = 1

SN-Tunnel-ISAKMP-Crypto-Map

This attribute specifies the system-defined crypto map to use for the subscriber's Mobile-IP connection, when IPSec is used to protect the Mobile-IP connection. This attribute is salt-encrypted.

Type
26

Vendor ID
8164

VSA Type
38

Length
1–128

Value
String

SN-Tunnel-ISAKMP-Secret

This attribute specifies the secret to use for IKE.

Type
26

Vendor ID
8164

VSA Type
39

Length

1–128

Value

String

SN-Tunnel-Load-Balancing

This attribute specifies the load-balancing algorithm to use when tunneling is employed.

Type

26

Vendor ID

8164

VSA Type

27

Length

4

Value

Enumerated integer. Supported values are:

- random = 1
- balanced = 2
- prioritized = 3

SN-Tunnel-Password

This attribute contains a secret for tunneling usage. Currently this is only used for L2TP. It is recommended that you use the Tunnel-Password attribute if your RADIUS server supports salt-encryption of attributes.

Type

26

Vendor ID

8164

VSA Type

26

Length

1–240

Value

Opaque value

SN-Unclassify-List-Name

Unclassify List Name.

Type

26

Vendor ID
8164

VSA Type
132

Length
1–32

Value
An ASCII string

SN-Virtual-APN-Name

This attribute contains the virtual APN name.

Type
26

Vendor ID
8164

VSA Type
94

Length
1–64

Value
ASCII string

SN-Visiting-Behavior

This attribute specifies the configuration for the behavior bits settings for a visiting subscriber in an APN.

When GGSN is configured to reject the charging characteristics sent by the SGSN for "home" subscribers, it uses the profile index specified by **cc-home behavior <bits> profile <index>** command to determine the appropriate CCs to use.

Multiple behavior bits can be configured for a single profile index by "Or"ing the bit strings together and convert the result to hexadecimal. The properties of the actual CC profile index are configured as part of the GGSN service using the cc profile command.

If this AVP is present in Access Accept message the locally configured APN value will be overridden.

Type
26

Vendor ID
8164

VSA Type
120

Length
4

Value

Unsigned integer

SN-Visiting-Profile

This attribute specifies the configuration for the profile bits settings for a visiting subscriber in an APN.

If this AVP is present in Access Accept message the locally configured APN value will be overridden.

Type

26

Vendor ID

8164

VSA Type

117

Length

4

Value

Unsigned integer

SN-Visiting-Sub-Use-GGSN

This attribute configures GGSN to accept GGSN's charging characteristics for visiting subscribers defined for the APN.

If this AVP is present in Access Accept message the locally configured APN value will be overridden.

Type

26

Vendor ID

8164

VSA Type

107

Length

4

Value

Enumerated integer. Supported values are:

- Deny = 0
- Accept = 1

SN-Voice-Push-List-Name

SN-Voice-Push-List-Name.

Type

26

Vendor ID

8164

VSA Type
131

Length
1–32

Value
ASCII string

SN-VPN-ID

This attribute contains the Destination VPN of the user, specified by a 32-bit identifier.

Type
26

Vendor ID
8164

VSA Type
1

Length
4

Value
Unsigned integer

SN-VPN-Name

This attribute contains the name of the user's Destination VPN.

Type
26

Vendor ID
8164

VSA Type
2

Length
1–253

Value
ASCII string

SN-WiMAX-Auth-Only

Specifies whether the call is established for Authentication Mode Only.

Type
26

Vendor ID
8164

VSA Type
306

Length
1

Value
Enumerated integer. Supported values are:

- Disabled = 0
- Enabled = 1

SN1-Access-link-IP-Frag

This attribute specifies what to do when data received for the subscriber on the Access link that needs to be fragmented and the DF bit is either set or unset. The default is Normal.

Type
26

Vendor ID
8164

VSA Type
63

Length
4

Value
Enumerated integer. Supported values are:

- Normal = 0 — Data to be fragmented is not fragmented if the DF bit is set
- DF-Ignore = 1 — Fragment regardless
- DF-Fragment-ICMP-Notify = 2 — Fragment regardless, and ICMP Notify if DF bit is set

SN1-Acct-Input-Giga-Dropped

This attribute contains the number of input gigawords dropped if the number of input bytes is greater than 2^32 - 1

Type
26

Vendor ID
8164

VSA Type
230

Length
4

Value

Unsigned integer

SN1-Acct-Input-Octets-Dropped

This attribute contains the number of input bytes dropped.

Type
26

Vendor ID
8164

VSA Type
228

Length
4

Value
Unsigned integer

SN1-Acct-Input-Packets-Dropped

This attribute contains the number of input packets dropped.

Type
26

Vendor ID
8164

VSA Type
226

Length
4

Value
Unsigned integer

SN1-Acct-Output-Giga-Dropped

This attribute contains the number of output gigawords dropped if the number of output bytes is greater than 2^32 - 1.

Type
26

Vendor ID
8164

VSA Type
231

Length
4

Value
integer

SN1-Acct-Output-Octets-Dropped

This attribute contains the number of output bytes dropped.

Type
26

Vendor ID
8164

VSA Type
229

Length
4

Value
Integer

SN1-Acct-Output-Packets-Dropped

This attribute contains the number of output packets dropped.

Type
26

Vendor ID
8164

VSA Type
227

Length
4

Value
Integer

SN1-Admin-Expiry

This attribute contains the date/time the administrative user account expires. It is an integer value specifying the number of seconds since the UNIX epoch at which time the account will expire.

Type
26

Vendor ID
8164

VSA Type
72

Length
4

Value
Integer

SN1-Admin-Permission

This attribute indicates the services allowed to be delivered to the administrative user. The attribute value is a bit field, and many algorithms can be specified to indicate that one of these may be chosen by the user.

Type
26

Vendor ID
8164

VSA Type
21

Length
4

Value
Enumerated integer. Supported values are:

- None = 0
- CLI = 1
- FTP = 2
- CLI-FTP = 3
- Intercept = 4
- CLI-Intercept = 5
- CLI-Intercept-FTP = 7
- ECS = 8
- CLI-ECS = 9
- CLI-FTP-ECS = 11
- CLI-Intercept-ECS = 13
- CLI-Intercept-FTP-ECS = 15

SN1-Assigned-VLAN-ID

The VLAN ID assigned to the subscriber.

Type
26

Vendor ID
8164

VSA Type

152

Length
4

Value
Unsigned integer

SN1-Call-Id

Internal system generated call ID number for the session.

Type
26

Vendor ID
8164

VSA Type
251

Length
4

Value
Unsigned integer

SN1-Cause-For-Rec-Closing

This attribute contains a reason for the release of the CDR.

Type
26

Vendor ID
8164

VSA Type
139

Length
4

Value
Enumerated integer. Supported values are:

- normalRelease = 0
- abnormalRelease = 4
- volumeLimit = 16
- timeLimit = 17
- SGSNChange = 18
- maxChangeCond = 19
- managementIntervention = 20

SN1-CFPolicy-ID

This attribute contains the Content Filtering policy ID.

This attribute is also accepted in CoA request message to be used in a currently active subscriber session.

Type
26

Vendor ID
8164

VSA Type
220

Length
4

Value
Unsigned integer

SN1-Change-Condition

This attribute defines the reason for closing the container.

Type
26

Vendor ID
8164

VSA Type
140

Length
4

Value
Enumerated integer. Supported values are:

- QOSCHANGE = 0
- TARIFFTIMECHANGE = 1
- SGSNCHANGE = 500

SN1-Charging-VPN-Name

Charging VPN Name.

Type
26

Vendor ID
8164

VSA Type
137

Length
1–252

Value
String

SN1-Chrg-Char-Selection-Mode

This attribute contains the charging characteristics type that the GSNs applied to the CDR.

Type
26

Vendor ID
8164

VSA Type
138

Length
4

Value
Integer. Supported values are:

- SGSN = 0
- HOME = 3
- ROAMING = 4
- VISITING = 5

SN1-Data-Tunnel-Ignore-DF-Bit

This attribute specifies if the PDSN/FA or HA should ignore the DF bit in the IPv4 header when encapsulating the IPv4 packet in MIP, and therefore fragmenting the resulting tunneled packet if necessary. The default is not to ignore the DF bit.

Type
26

Vendor ID
8164

VSA Type
49

Length
4

Value
Enumerated integer. Supported values are:

- Disabled = 0 — Do not ignore DF bit
- Enabled = 1 — Ignore DF bit

SN1-DHCP-Lease-Expiry-Policy

This attribute specifies whether to renew or disconnect on expiry of IP address lease time.

Type
26

Vendor ID
8164

VSA Type
157

Length
4

Value
Enumerated integer. Supported values are:

- auto-renew = 0
- disconnect = 1

SN1-Disconnect-Reason

This attribute contains the reason the user was disconnected from service.

This attribute is also accepted in CoA request message to be used in a currently active subscriber session.

Type
26

Vendor ID
8164

VSA Type
3

Length
4

Value
Enumerated integer. Supported values are:

- Not-Defined = 0
- Admin-Disconnect = 1
- Remote-Disconnect = 2
- Local-Disconnect = 3
- Disc-No-Resource = 4
- Disc-Excd-Service-Limit = 5
- PPP-LCP-Neg-Failed = 6
- PPP-LCP-No-Response = 7
- PPP-LCP-Loopback = 8
- PPP-LCP-Max-Retry = 9

- PPP-Echo-Failed = 10
- PPP-Auth-Failed = 11
- PPP-Auth-Failed-No-AAA-Resp = 12
- PPP-Auth-No-Response = 13
- PPP-Auth-Max-Retry = 14
- Invalid-AAA-Attr = 15
- Failed-User-Filter = 16
- Failed-Provide-Service = 17
- Invalid-IP-Address-AAA = 18
- Invalid-IP-Pool-AAA = 19
- PPP-IPCP-Neg-Failed = 20
- PPP-IPCP-No-Response = 21
- PPP-IPCP-Max-Retry = 22
- PPP-No-Rem-IP-Address = 23
- Inactivity-Timeout = 24
- Session-Timeout = 25
- Max-Data-Excd = 26
- Invalid-IP-Source-Address = 27
- MSID-Auth-Failed = 28
- MSID-Auth-Failed-No-AAA-Resp = 29
- A11-Max-Retry = 30
- A11-Lifetime-Expired = 31
- A11-Message-Integrity-Failure = 32
- PPP-lcp-remote-disc = 33
- Session-setup-timeout = 34
- PPP-keepalive-failure = 35
- Flow-add-failed = 36
- Call-type-detection-failed = 37
- Wrong-ipcp-params = 38
- MIP-remote-dereg = 39
- MIP-lifetime-expiry = 40
- MIP-proto-error = 41
- MIP-auth-failure = 42
- MIP-reg-timeout = 43
- Invalid-dest-context = 44
- Source-context-removed = 45
- Destination-context-removed = 46

- Req-service-addr-unavailable = 47
- Demux-mgr-failed = 48
- Internal-error = 49
- AAA-context-removed = 50
- invalid-service-type = 51
- mip-relay-req-failed = 52
- mip-rcvd-relay-failure = 53
- ppp-restart-inter-pdsn-handoff = 54
- gre-key-mismatch = 55
- invalid_tunnel_context = 56
- no_peer_lns_address = 57
- failed_tunnel_connect = 58
- l2tp-tunnel-disconnect-remote = 59
- l2tp-tunnel-timeout = 60
- l2tp-protocol-error-remote = 61
- l2tp-protocol-error-local = 62
- l2tp-auth-failed-remote = 63
- l2tp-auth-failed-local = 64
- l2tp-try-another-lns-from-remote = 65
- l2tp-no-resource-local = 66
- l2tp-no-resource-remote = 67
- l2tp-tunnel-disconnect-local = 68
- l2tp-admin-disconnect_remote = 69
- l2tpmgr-reached-max-capacity = 70
- MIP-reg-revocation = 71
- path-failure = 72
- dhcp-relay-ip-validation-failed = 73
- gtp-unknown-pdp-addr-or-pdp-type = 74
- gtp-all-dynamic-pdp-addr-occupied = 75
- gtp-no-memory-is-available = 76
- dhcp-relay-static-ip-addr-not-allowed = 77
- dhcp-no-ip-addr-allocated = 78
- dhcp-ip-addr-allocation-tmr-exp = 79
- dhcp-ip-validation-failed = 80
- dhcp-static-addr-not-allowed = 81
- dhcp-ip-addr-not-available-at-present = 82
- dhcp-lease-expired = 83

- lpool-ip-validation-failed = 84
- lpool-static-ip-addr-not-allowed = 85
- static-ip-validation-failed = 86
- static-ip-addr-not-present = 87
- static-ip-addr-not-allowed = 88
- radius-ip-validation-failed = 89
- radius-ip-addr-not-provided = 90
- invalid-ip-addr-from-sgsn = 91
- no-more-sessions-in-aaa = 92
- ggsn-aaa-auth-req-failed = 93
- conflict-in-ip-addr-assignment = 94
- apn-removed = 95
- credits-used-bytes-in = 96
- credits-used-bytes-out = 97
- credits-used-bytes-total = 98
- prepaid-failed = 99
- l2tp-ipsec-tunnel-failure = 100
- l2tp-ipsec-tunnel-disconnected = 101
- mip-ipsec-sa-inactive = 102
- Long-Duration-Timeout = 103
- proxy-mip-registration-failure = 104
- proxy-mip-binding-update = 105
- proxy-mip-inter-pdsn-handoff-require-ip-address = 106
- proxy-mip-inter-pdsn-handoff-mismatched-address = 107
- Local-purge = 108
- failed-update-handoff = 109
- closed_rp-handoff-complete = 110
- closed_rp-duplicate-session = 111
- closed_rp-handoff-session-not-found = 112
- closed_rp-handoff-failed = 113
- pcf-monitor-keep-alive-failed = 114
- call-internal-reject = 115
- call-restarted = 116
- a11-mn-ha-auth-failure = 117
- a11-badly-formed = 118
- a11-t-bit-not-set = 119
- a11-unsupported-vendor-id = 120

- a11-mismatched-id = 121
- mipha-dup-home-addr-req = 122
- mipha-dup-imsi-session = 123
- ha-unreachable = 124
- IPSP-addr-in-use = 125
- mipfa-dup-home-addr-req = 126
- mipha-ip-pool-busyout = 127
- inter-pdsn-handoff = 128
- active-to-dormant = 129
- ppp-renegotiation = 130
- active-start-param-change = 131
- tarrif-boundary = 132
- a11-disconnect-no-active-stop = 133
- nw-reachability-failed-reject = 134
- nw-reachability-failed-redirect = 135
- container-max-exceeded = 136
- static-addr-not-allowed-in-apn = 137
- static-addr-required-by-radius = 138
- static-addr-not-allowed-by-radius = 139
- mip-registration-dropped = 140
- counter-rollover = 141
- constructed-nai-auth-fail = 142
- inter-pdsn-service-optimize-handoff-disabled = 143
- gre-key-collision = 144
- inter-pdsn-service-optimize-handoff-triggered = 145
- intra-pdsn-handoff-triggered = 146
- delayed-abort-timer-expired = 147
- Admin-AAA-disconnect = 148
- Admin-AAA-disconnect-handoff = 149
- PPP-IPV6CP-Neg-Failed = 150
- PPP-IPV6CP-No-Response = 151
- PPP-IPV6CP-Max-Retry = 152
- PPP-Restart-Invalid-source-IPV4-address = 153
- a11-disconnect-handoff-no-active-stop = 154
- call-restarted-inter-pdsn-handoff = 155
- call-restarted-ppp-termination = 156
- mipfa-resource-conflict = 157

- failed-auth-with-charging-svc = 158
- mipha-dup-imsi-session-purge = 159
- mipha-rev-pending-newcall = 160
- volume-quota-reached = 161
- duration-quota-reached = 162
- gtp-user-authentication-failed = 163
- MIP-reg-revocation-no-lcp-term = 164
- MIP-private-ip-no-rev-tunnel = 165
- Invalid-Prepaid-AAA-attr-in-auth-response = 166
- mipha-prepaid-reset-dynamic-newcall = 167
- gre-flow-control-timeout = 168
- mip-paaa-bc-query-not-found = 169
- mipha-dynamic-ip-addr-not-available = 170
- a11-mismatched-id-on-handoff = 171
- a11-badly-formed-on-handoff = 172
- a11-unsupported-vendor-id-on-handoff = 173
- a11-t-bit-not-set-on-handoff = 174
- MIP-reg-revocation-i-bit-on = 175
- A11-RRQ-Deny-Max-Count = 176
- Dormant-Transition-During-Session-Setup = 177
- PPP-Rem-Reneg-Disc-Always-Cfg = 178
- PPP-Rem-Reneg-Disc-NAI-MSID-Mismatch = 179
- mipha-subscriber-ipsec-tunnel-down = 180
- mipha-subscriber-ipsec-tunnel-failed = 181
- mipha-subscriber-ipsecmgr-death = 182
- flow-is-deactivated = 183
- ecsv2-license-exceeded = 184
- IPSG-Auth-Failed = 185
- driver-initiated = 186
- ims-authorization-failed = 187
- service-instance-released = 188
- flow-released = 189
- ppp-renego-no-ha-addr = 190
- intra-pdsn-handoff = 191
- overload-disconnect = 192
- css-service-not-found = 193
- Auth-Failed = 194

- dhcp-client-sent-release = 195
- dhcp-client-sent-nak = 196
- msid-dhcp-chaddr-mismatch = 197
- link-broken = 198
- prog-end-timeout = 199
- qos-update-wait-timeout = 200
- css-synch-cause = 201
- Gtp-context-replacement = 202
- PDIF-Auth-failed = 203
- l2tp-unknown-apn = 204
- ms-unexpected-network-reentry = 205
- r6-invalid-nai = 206
- eap-max-retry-reached = 207
- vbm-hoa-session-disconnected = 208
- vbm-voa-session-disconnected = 209
- in-acl-disconnect-on-violation = 210
- eap-msk-lifetime-expiry = 211
- eap-msk-lifetime-too-low = 212
- mipfa-inter-tech-handoff = 213
- r6-max-retry-reached = 214
- r6-nwexit-recd = 215
- r6-dereg-req-recd = 216
- r6-remote-failure = 217
- r6r4-protocol-errors = 218
- wimax-qos-invalid-aaa-attr = 219
- npu-gre-flows-not-available = 220
- r4-max-retry-reached = 221
- r4-nwexit-recd = 222
- r4-dereg-req-recd = 223
- r4-remote-failure = 224
- ims-authorization-revoked = 225
- ims-authorization-released = 226
- ims-auth-decision-invalid = 227
- mac-addr-validation-failed = 228
- excessive-wimax-pd-flows-cfgd = 229
- sgsn-canc-loc-sub = 230
- sgsn-canc-loc-upd = 231

- sgsn-mnr-exp = 232
- sgsn-ident-fail = 233
- sgsn-sec-fail = 234
- sgsn-auth-fail = 235
- sgsn-glu-fail = 236
- sgsn-imp-det = 237
- sgsn-smgr-purge = 238
- sgsn-subs-handed-to-peer = 239
- sgsn-dns-fail-inter-rau = 240
- sgsn-cont-rsp-fail = 241
- sgsn-hlr-not-found-for-imsi = 242
- sgsn-ms-init-det = 243
- sgsn-opr-policy-fail = 244
- sgsn-duplicate-context = 245
- hss-profile-update-failed = 246
- sgsn-no-pdp-activated = 247
- asnpc-idle-mode-timeout = 248
- asnpc-idle-mode-exit = 249
- asnpc-idle-mode-auth-failed = 250
- asngw-invalid-qos-configuration = 251
- sgsn-dsd-allgprswithdrawn = 252
- r6-pmk-key-change-failure = 253
- sgsn-illegal-me = 254
- sess-termination-timeout = 255
- sgsn-sai-fail = 256
- sgsn-rnc-removal = 257
- sgsn-rai-removal = 258
- sgsn-init-deact = 259
- ggsn-init-deact = 260
- hlr-init-deact = 261
- ms-init-deact = 262
- sgsn-detach-init-deact = 263
- sgsn-rab-rel-init-deact = 264
- sgsn-iu-rel-init-deact = 265
- sgsn-gtpu-path-failure = 266
- sgsn-gtpc-path-failure = 267
- sgsn-local-handoff-init-deact = 268

- sgsn-remote-handoff-init-deact = 269
- sgsn-gtp-no-resource = 270
- sgsn-rnc-no-resource = 271
- sgsn-odb-init-deact = 272
- sgsn-invalid-ti = 273
- sgsn-ggsn-ctxt-non-existent = 274
- sgsn-apn-restrict-vio = 275
- sgsn-regular-deact = 276
- sgsn-abnormal-deact = 277
- sgsn-actv-rejected-by-peer = 278
- sgsn-err-ind = 279
- asngw-non-anchor-prohibited = 280
- asngw-im-entry-prohibited = 281
- session-idle-mode-entry-timeout = 282
- session-idle-mode-exit-timeout = 283
- asnpc-ms-power-down-nwexit = 284
- asnpc-r4-nwexit-recd = 285
- sgsn-iu-rel-before-call-est = 286
- ikev2-subscriber-ipsecmgr-death = 287
- All-dynamic-pool-addr-occupied = 288
- mip6ha-ip-addr-not-available = 289
- bs-monitor-keep-alive-failed = 290
- sgsn-att-in-reg-state = 291
- sgsn-inbound-srns-in-reg-state = 292
- dt-ggsn-tun-reestablish-failed = 293
- sgsn-unknown-pdp = 294
- sgsn-pdp-auth-failure = 295
- sgsn-duplicate-pdp-context = 296
- sgsn-no-rsp-from-ggsn = 297
- sgsn-failure-rsp-from-ggsn = 298
- sgsn-apn-unknown = 299
- sgsn-serv-req-init-deact = 300
- sgsn-attach-on-attch-init-abort = 301
- sgsn-iu-rel-in-israu-init-abort = 302
- sgsn-smgr-init-abort = 303
- sgsn-mm-ctx-cleanup-init-abort = 304
- sgsn-unknown-abort = 305

- sgsn-guard-timeout-abort = 306
- vpn-bounce-dhcpip-validate-req = 307
- mipv6-id-mismatch = 308
- aaa-session-id-not-found = 309
- x1-max-retry-reached = 310
- x1-nwexit-recd = 311
- x1-dereg-req-recd = 312
- x1-remote-failure = 313
- x1x2-protocol-errors = 314
- x2-max-retry-reached = 315
- x2-nwexit-recd = 316
- x2-dereg-req-recd = 317
- x2-remote-failure = 318
- x1-pmk-key-change-failure = 319
- sa-rekeying-failure = 320
- sess-sleep-mode-entry-timeout = 321
- phsgw-non-anchor-prohibited = 322
- asnpc-pc-relocation-failed = 323
- asnpc-pc-relocation = 324
- auth_policy_mismatch = 325
- sa-lifetime-expiry = 326
- asnpc-del-ms-entry-recd = 327
- phspc-sleep-mode-timeout = 328
- phspc-sleep-mode-exit = 329
- phspc-sleep-mode-auth-failed = 330
- phspc-ms-power-down-nwexit = 331
- phspc-x2-nwexit-recd = 332
- invalid-nat-config = 333
- asngw-tid-entry-not-found = 334
- No-NAT-IP-Address = 335
- excessive-phs-pd-flows-cfgd = 336
- phsgw-invalid-qos-configuration = 337
- Interim-Update = 338
- sgsn-attach-abrt-rad-lost = 339
- sgsn-inbnd-irau-abrt-rad-lost = 340
- ike-keepalive-failed = 341
- sgsn-attach-abrt-ms-suspend = 342

- sgsn-inbnd-irau-abrt-ms-suspend = 343
- duplicate-session-detected = 344
- sgsn-xid-response-failure = 345
- sgsn-nse-cleanup = 346
- sgsn-gtp-req-failure = 347
- sgsn-imsi-mismatch = 348
- sgsn-bvc-blocked = 349
- sgsn-attach-on-inbound-irau = 350
- sgsn-attach-on-outbound-irau = 351
- sgsn-incorrect-state = 352
- sgsn-t3350-expiry = 353
- sgsn-page-timer-expiry = 354
- phsgw-tid-entry-not-found = 355
- phspc-del-ms-entry-recd = 356
- sgsn-pdp-local-purge = 357
- phs-invalid-nai = 358
- session-sleep-mode-exit-timeout = 359
- sgsn-offload-phase2 = 360
- phs-thirdparty-auth-fail = 361
- remote-error-notify = 362
- no-response = 363
- PDG-Auth-failed = 364
- mme-s1AP-send-failed=365
- mme-egtpc-connection-failed=366
- mme-egtpc-create-session-failed=367
- mme-authentication-failure=368
- mme-ue-detach=369
- mme-mme-detach=370
- mme-hss-detach=371
- mme-pgw-detach=372
- mme-sub-validation-failure=373
- mme-hss-connection-failure=374
- mme-hss-user-unknown=375
- dhcp-lease-mismatch-detected=376
- nemo-link-layer-down=377
- eapol-max-retry-reached = 378
- sgsn-offload-phase3 = 379

- mbms-bearer-service-disconnect = 380
- disconnect-on-violation-odb = 381
- disconn-on-violation-focs-odb = 382
- CSCF-REG-Admin-disconnect = 383
- CSCF-REG-User-disconnect = 384
- CSCF-REG-Inactivity-timeout = 385
- CSCF-REG-Network-disconnect = 386
- CSCF-Call-Admin-disconnect = 387
- CSCF-CAll-User-disconnect = 388
- CSCF-CALL-Local-disconnect = 389
- CSCF-CALL-No-Resource = 390
- CSCF-CALL-No-Respone = 391
- CSCF-CALL-Inactivity-timeout = 392
- CSCF-CALL-Media-Auth-Failure = 393
- CSCF-REG-No-Resource = 394
- ms-unexpected-idle-mode-entry = 395
- re-auth-failed = 396
- sgsn-pdp-nse-cleanup = 397
- sgsn-mm-ctxt-gtp-no-resource = 398
- unknown-apn = 399
- gtpc-path-failure = 400
- gtpu-path-failure = 401
- actv-rejected-by-sgsn = 402
- sgsn-pdp-gprs-camel-release = 403
- sgsn-check-imei-failure = 404
- sgsn-sndcp-init-deact = 405
- sgsn-pdp-inactivity-timeout = 406
- fw-and-nat-policy-removed = 407
- FNG-Auth-failed = 408
- ha-stale-key-disconnect = 409
- No-IPV6-address-for-subscriber = 410
- prefix-registration-failure = 411
- disconnect-from-policy-server = 412
- s6b-auth-failed = 413
- gtpc-err-ind = 414
- gtpu-err-ind = 415
- invalid-pdn-type = 416

- aaa-auth-req-failed = 417
- apn-denied-no-subscription = 418
- Sgw-context-replacement = 419
- dup-static-ip-addr-req = 420
- apn-restrict-violation = 421
- invalid-wapn = 422
- ttg-nsapi-allocation-failed = 423
- mandatory-gtp-ie-missing = 424
- aaa-unreachable = 425
- asngw-service-flow-deletion = 426
- CT-PMIP-RRQ-NVSE-Value-Change = 427
- tcp-read-failed = 428
- tcp-write-failed = 429
- ssl-handshake-failed = 430
- ssl-renegotiate-failed = 431
- ssl-bad-message = 432
- ssl-alert-received = 433
- ssl-disconnect = 434
- ssl-migration = 435
- sgsn-ard-failure = 436
- sgsn-camel-release = 437
- Hotlining-Status-Change=447
- ggsn-no-rsp-from-sgsn = 448
- diameter-protocol-error=449
- diameter-request-timeout=450
- operator-policy=451
- spr-connection-timeout=452
- mipha-dup-wimax-session = 453
- invalid-version-attr = 454
- sgsn-zone-code-failure = 455
- invalid-qci = 456
- no_rules = 457
- mme-init-ctxt-setup-failure = 459
- mme-driver-initiated = 460
- mme-s1ap-connection-down = 461
- mme-s1ap-reset-recd = 462
- mme-s6a-response-timeout = 463

- mme-s13-response-timeout = 464
- mme-Illegal-equipment = 465
- mme-unexpected-attach = 466
- mme-sgw-selection-failure = 467
- mme-pgw-selection-failure = 468
- mme-reselection-to-sgsn = 469
- mme-relocation-to-sgsn = 470
- mme-reselection-to-mme = 471
- mme-relocation-to-mme = 472
- mme-tau-attach-collision = 473
- mme-old-sgsn-resolution-failure = 474
- mme-old-mme-resolution-failure = 475
- mme-reloc-ho-notify-timeout = 476
- mme-reloc-ho-req-ack-timeout = 477
- mme-create-session-timeout = 478
- mme-create-session-failure = 479
- mme-s11-path-failure = 480
- mme-policy-no-ue-irat = 481
- mme-x2-handover-failed = 482
- mme-attach-restrict = 483
- mme-regional-zone-code = 484
- mme-no-response-from-ue = 485
- mme-sgw-relocation-failed = 486
- mme-implicit-detach = 487
- sgsn-detach-notify = 488
- emergency-inactivity-timeout = 489
- policy-initiated-release = 490
- gy-result-code-system-failure = 491
- mme-zone-code-validation-failed = 492
- sgsn-pgw-init-deact = 493
- s6b-ip-validation-failed = 494
- sgsn-failure-rsp-from-sgw = 495
- tcp-remote-close = 496
- tcp-reset-received = 497
- tcp-socket-error = 498

SN1-DNS-Proxy-Intercept-List

DNS proxy list.

Type
26

Vendor ID
8164

VSA Type
214

Length
1–253

Value
String

SN1-DNS-Proxy-Use-Subscr-Addr

This attribute is used to convey whether to use the subscriber's address as the source address for DNS Proxy.

Type
26

Vendor ID
8164

VSA Type
25

Length
4

Value
Enumerated integer. Supported values are:

- Disable = 0
- Enable = 1

SN1-Dynamic-Addr-Alloc-Ind-Flag

This attribute indicates that the PDP address has been dramatically allocated for that particular PDP context. This field is missing if the address is static (e.g., part of the PDP context subscription). Dynamic address allocation might be relevant for charging (e.g., the duration of PDP context as one resource offered and possibly owned by the network operator).

Type
26

Vendor ID
8164

VSA Type
141

Length
1

Value
Integer. Supported value is:

- Dynamic address allocation = 1

SN1-Ecs-Data-Volume

Compound attribute indicating downlink and uplink octet usage for a PDP context per rating group.

Type
26

Vendor ID
8164

VSA Type
176

Length
12

Value
Contains the following subattributes:

Rating-Group-Id

Rating Group Id in a PDP context.

Type
1

Length
4

Value
Unsigned integer

GPRS-Uplink

Uplink octet usage for a PDP context per rating group.

Type
2

Length
4

Value
Unsigned integer

GPRS-Downlink

Downlink octet usage for a PDP context per rating group.

Type
3

Length
4

Value
Unsigned integer

SN1-Enable-QoS-Renegotiation

This attribute configures the enabling of dynamic QoS renegotiation.

Type
26

Vendor ID
8164

VSA Type
144

Length
1

Value
Enumerated integer. Supported values are:

- No = 0
- Yes = 1

SN1-Ext-Inline-Srvr-Context

This attribute configures the context name in which the External In-line server resides. The value is an ASCII string naming the In-line Server Context.

Type
26

Vendor ID
8164

VSA Type
41

Length
1–247

Value
ASCII string

SN1-Ext-Inline-Srvr-Down-Addr

This attribute configures the IP address of the Downstream External In-line server to forward VLAN-tagged packets to. It can be tagged, in which case it is treated as part of an external in-line server group.

Type
26

Vendor ID
8164

VSA Type
56

Length
4

Value
IPv4 address

SN1-Ext-Inline-Srvr-Down-VLAN

This attribute configures the IP address of the downstream external in-line server to forward VLAN-tagged packets to. It can be tagged, in which case it is treated as part of an external in-line server group.

Type
26

Vendor ID
8164

VSA Type
59

Length
4

Value
Unsigned integer

SN1-Ext-Inline-Srvr-Preference

This attribute configures the preference for the tagged group of External In-line Servers. This attribute is required, although it doesn't actually assign a preference right now. It can be tagged, in which case it is treated as part of an external in-line server group.

Type
26

Vendor ID
8164

VSA Type
57

Length
4

Value
Unsigned integer

SN1-Ext-Inline-Srvr-Up-Addr

This attribute configures the IP address of the Upstream External In-line server to forward VLAN-tagged packets to. It can be tagged, in which case it is treated as part of an external in-line server group.

Type
26

Vendor ID
8164

VSA Type
55

Length
4

Value
IPv4 address

SN1-Ext-Inline-Srvr-Up-VLAN

This attribute configures the VLAN tag to be applied to Upstream packets and forwarded to the External In-line server. It can be tagged, in which case it is treated as part of an external in-line server group.

Type
26

Vendor ID
8164

VSA Type
58

Length
4

Value
The VLAN tag to apply.

SN1-Firewall-Enabled

Firewall for subscriber enabled.

Type
26

Vendor ID
8164

VSA Type
198

Length
4

Value

Enumerated integer. Supported values are:

- False = 0
- True = 1

SN1-Firewall-Policy

This attribute is obsoleted.

SN1-FMC-Location

MAC address and CDMA location information.

Type
26

Vendor ID
8164

VSA Type
171

Length
1–247

Value
String

SN1-GGSN-MIP-Required

This attribute specifies if MIP is required for the GGSN subscriber.

Type
26

Vendor ID
8164

VSA Type
68

Length
4

Value
Enumerated integer. Supported values are:

- Disabled = 0
- Enabled = 1

SN1-Gratuitous-ARP-Aggressive

This attribute specifies whether to generate a gratuitous ARP message whenever a MIP handoff or re-registration occurs. A non-zero of this attribute also configures the mode of operation when sending the gratuitous ARP, although only one mode (Aggressive) is supported at this time.

Type

26

Vendor ID

8164

VSA Type

54

Length

4

Value

Enumerated integer. Supported values are:

- Disabled = 0
- Enabled = 1

SN1-Gratuitous-ARP-Mode

This attribute specifies whether to generate a gratuitous ARP message whenever a MIP handoff or re-registration occurs. A non-zero of this attribute also configures the mode of operation when sending the gratuitous ARP, although only one mode (Aggressive) is supported at this time.

Type

26

Vendor ID

8164

VSA Type

54

Length

4

Value

An integer in network order. Supported values are:

- Disabled = 0 — Do not send Gratuitous ARP
- Aggressive = 1 — Send Gratuitous ARP in Aggressive mode

SN1-GTP-Version

This attribute contains the version of GTP the subscriber is using.

Type

26

Vendor ID
8164

VSA Type
62

Length
4

Value
Enumerated integer. Supported values are:

- GTP_VERSION_0 = 0
- GTP_VERSION_1 = 1
- GTP_VERSION_2 = 2

SN1-HA-Send-DNS-Address

This attribute specifies if the HA should send the DNS address in the Mobile IP RRP message. The default is not to send the DSN Address.

Type
26

Vendor ID
8164

VSA Type
47

Length
4

Value
Enumerated integer. Supported values are:

- Disabled = 0 — Do not send
- Enabled = 1 — Send

SN-Home-Behavior

This attribute specifies the configuration for the behavior bits settings for a home subscriber in an APN.

When GGSN is configured to reject the charging characteristics sent by the SGSN for "home" subscribers, it uses the profile index specified by **cc-home behavior <bits> profile <index>** command to determine the appropriate CCs to use.

Multiple behavior bits can be configured for a single profile index by "Or"ing the bit strings together and convert the result to hexadecimal. The properties of the actual CC profile index are configured as part of the GGSN service using the cc profile command.

If this AVP is present in Access Accept message the locally configured APN value will be overridden.

Type
26

Vendor ID
8164

VSA Type
119

Length
4

Value
Unsigned integer

SN1-Home-Behavior

This attribute specifies the configuration for the behavior bits settings for a home subscriber in an APN.

When GGSN is configured to reject the charging characteristics sent by the SGSN for "home" subscribers, it uses the profile index specified by **cc-home behavior <bits> profile <index>** command to determine the appropriate CCs to use.

Multiple behavior bits can be configured for a single profile index by "Or"ing the bit strings together and convert the result to hexadecimal. The properties of the actual CC profile index are configured as part of the GGSN service using the cc profile command.

If this AVP is present in Access Accept message the locally configured APN value will be overridden.

Type
26

Vendor ID
8164

VSA Type
119

Length
4

Value
Unsigned integer

SN1-Home-Profile

This attribute specifies the configuration for the profile bits settings for a home subscriber in an APN.

If this AVP is present in Access Accept message the locally configured APN value will be overridden.

Type
26

Vendor ID
8164

VSA Type
109

Length
4

Value
Unsigned integer

SN1-Home-Sub-Use-GGSN

This attribute configures GGSN to accept GGSN's charging characteristics for home subscribers defined for the APN.

If this AVP is present in Access Accept message the locally configured APN value will be overridden.

Type
26

Vendor ID
8164

VSA Type
106

Length
4

Value
Enumerated integer. Supported values are:

- Deny = 0
- Accept = 1

SN1-Ignore-Unknown-HA-Addr-Err

Value of 1 enables HA to ignore unknown HA address error for incoming RRQ.

Type
26

Vendor ID
8164

VSA Type
160

Length
1

Value
Unsigned integer

SN1-IMSI

This is the IMSI that identifies the mobile subscriber.

Type
26

Vendor ID
8164

VSA Type
252

Length
1–8

Value
ASCII string

SN1-IMS-AM-Address

IMS application manager address.

Type
26

Vendor ID
8164

VSA Type
167

Length
4

Value
IPv4 address

SN1-IMS-AM-Domain-Name

IMS application manager domain name.

Type
26

Vendor ID
8164

VSA Type
168

Length
1 - 64

Value
String

SN1-Internal-SM-Index

GGSN charging service, internally used.

Type
26

Vendor ID

8164

VSA Type
122

Length
4

Value
Unsigned integer

SN1-Inactivity-Time

This attribute contains the inactivity time duration for a subscriber session under long time duration timer configuration.

Type
26

Vendor ID
8164

VSA Type
232

Length
1

Value
1

SN1-IP-Alloc-Method

This attribute specifies the method for allocating an IP address. This feature only applies to the GGSN Service.

Type
26

Vendor ID
8164

VSA Type
53

Length
4

Value
Enumerated integer. Supported values are:

- Alloc_Local_Pool = 0
- Alloc_Dhcp_Client = 1
- Alloc_Radius = 2
- Alloc_No_Alloc = 3
- Alloc_Static_Alloc = 4
- Alloc_Dhcp_Relay = 5

SN1-IP-Filter-In

This attribute is deprecated. To select an IP access list that is already defined in the destination context, use the IETF standard **Filter-Id** attribute. The filter ID is used to identify the IP access list by name.

SN1-IP-Filter-Out

This attribute is deprecated. To select an IP access list that is already defined in the destination context, use the IETF standard **Filter-Id** attribute. The filter ID is used to identify the IP access list by name.

SN1-IP-Header-Compression

Specifies the IP header compression method to use.

Type
Type 26

Vendor ID
8164

VSA Type
150

Length
2

Value
Enumerated integer. Supported values are:

- None = 0
- VJ = 1
- ROHC = 2
- VJ_ROHC = 3

SN1-IP-Hide-Service-Address

This attribute prevents the IP address bound to a call service from responding to ping and IMCP error packets.

Type
26

Vendor ID
8164

VSA Type
60

Length
4

Value
Enumerated integer. Supported values are:

- No = 0
- Yes = 1

SN1-IP-In-ACL

This attribute contains a definition for one Input IP Access Control List, which is used to filter the IP packets coming from the user. Note that more than one of these attributes can be included, in which case they are processed in the order in which they appear in the RADIUS Access-Accept.

Type
26

Vendor ID
8164

VSA Type
17

Length
1–253

Value
ASCII string

SN1-IP-In-Plcy-Grp

This attribute specifies the name of the policy group config applied in the uplink direction.

Type
26

Vendor ID
8164

VSA Type
193

Length
1–16

Value
String

SN1-IP-Out-ACL

This attribute contains a definition for one Output IP Access Control List, which is used to filter the IP packets sent to the user. Note that more than one of these attributes can be included, in which case they are processed in the order in which they appear in the RADIUS Access-Accept.

Type
26

Vendor ID
8164

VSA Type
18

Length
1–253

Value
ASCII string

SN1-IP-Out-Plcy-Grp

This attribute specifies the name of the policy group config applied in the downlink direction.

Type
26

Vendor ID
8164

VSA Type
194

Length
1–16

Value
String

SN1-IP-Pool-Name

This attribute contains the name of the IP pool, configured on the chassis, from which an IP address should be chosen for the user.

Type
26

Vendor ID
8164

VSA Type
8

Length
1–253

Value
ASCII string

SN1-IP-Source-Validation

This attribute indicates if the source IP address should be validated before forwarding the IP packet.

Type
26

Vendor ID
8164

VSA Type
14

Length
4

Value
Enumerated integer. Supported values are:

- No = 0 — No Validation
- Yes = 1 — Validated
- VSA1 vendor specific.

SN1-IP-Source-Violate-No-Acct

This attribute excludes the Source Violated IP packets and byte counts when reporting the Octet and Packet count in an accounting message.

If this AVP is present in Access Accept message the locally configured APN value will be overridden. If there is no value configured in the APN this value will not be applied to the session.

Type
26

Vendor ID
8164

VSA Type
196

Length
4

Value
Enumerated integer. Supported values are:

- Disabled = 0
- Enabled = 1

SN1-IP-Src-Valid-Drop-Limit

Maximum number of packet drops entertained before disconnecting the session for source violated packets for the session

Type
26

Vendor ID
8164

VSA Type
110

Length

1

Value

Unsigned integer

SN1-IPv6-DNS-Proxy

IPV6 DNS Proxy Enabled or Disabled Setting for the session.

Type

26

Vendor ID

8164

VSA Type

126

Length

2

Value

Enumerated integer. Supported values are:

- Disabled = 0
- Enabled = 1

SN1-IPv6-Egress-Filtering

This attribute enables egress filtering to make sure that packets being sent to the mobile device have an interface ID that matches that of the mobile device. This feature is meant to protect the Mobile from receiving unwanted packets from the Internet.

Type

26

Vendor ID

8164

VSA Type

103

Length

1

Value

Enumerated integer. Supported values are:

- Disabled = 0
- Enabled = 1

SN1-IPv6-Min-Link-MTU

SN1-IPv6-Min-Link-MTU

Type
26

Vendor ID
8164

VSA Type
136

Length
2

Value
Unsigned integer

SN1-IPv6-num-rtr-advt

This attribute contains the IPv6 number of Initial Router Advertisements. Default value is 3.

Type
26

Vendor ID
8164

VSA Type
97

Length
4

Value
Unsigned integer

SN1-IPv6-Primary-DNS

This attribute specifies a Primary DNS server address that the Router Advertisement message sent by the PDSN will include.

Type
26

Vendor ID
8164

VSA Type
101

Length
4

Value
IPv6 address

SN1-IPv6-rtr-advt-interval

This attribute contains the IPv6 Initial Router Advertisement Interval, specified in milliseconds. The default value is 3000.

Type
26

Vendor ID
8164

VSA Type
96

Length
4

Value
Unsigned integer

SN1-IPv6-Sec-Pool

This attribute contains the IPv6 secondary pool name.

Type
26

Vendor ID
8164

VSA Type
124

Length
1–253

Value
String

SN1-IPv6-Sec-Prefix

IPv6 Secondary Pool name prefix.

Type
26

Vendor ID
8164

VSA Type
125

Length
2–18

Value
Opaque value

SN1-IPv6-Secondary-DNS

This attribute specifies a Secondary DNS server address that the Router Advertisement message sent by the PDSN will include.

Type
26

Vendor ID
8164

VSA Type
102

Length
4

Value
IPv6 address

SN1-L3-to-L2-Tun-Addr-Policy

This attribute specifies the address allocation policy.

Type
26

Vendor ID
8164

VSA Type
43

Length
4

Value
Enumerated integer. Supported values are:

- no-local-alloc-validate = 0 — Do not locally allocate, do not validate
- local-alloc = 1 — Locally allocate
- local-alloc-validate = 2 — Locally allocate and validate

SN1-Local-IP-Address

This attribute contains the IP address of the local interface on the chassis for the user's session.

Type
26

Vendor ID
8164

VSA Type
13

Length
4

Value
IPv4 address

SN1-Long-Duration-Action

This attribute specifies the action to take place when the long duration timeout expires for a subscriber session.

Type
26

Vendor ID
8164

VSA Type
45

Length
4

Value
Enumerated integer. Supported values are:

- Detection = 1 — Detect the session and alert the administrator
- Disconnection = 2 — Disconnect the session
- Dormant-Only-Disconnection = 3
- Dormant-Only-Detection = 4

SN1-Long-Duration-Notification

Long Duration Notification.

Type
26

Vendor ID
8164

VSA Type
253

Length
4

Value
Enumerated integer. Supported values are:

- Suppress = 0
- Send = 1

SN1-Long-Duration-Timeout

This attribute is used to detect and if necessary disconnect sessions connected to the PDSN. This attribute configures the time period before either alerting the administrator or disconnecting the subscriber.

Type
26

Vendor ID
8164

VSA Type
44

Length
4

Value
An integer in network order which is the number of seconds for the long duration timer.

SN1-Mediation-Acct-Rsp-Action

When this attribute is set to **None**, there is no action taken while waiting for a response for the accounting start message from the Mediation Accounting server. When this attribute is set to **No-Early-PDUs** the system buffers all packets from the user (uplink) until a response for the accounting start message is received from the Mediation Accounting server. When set to **Delay_GTP_Response**, the system does not send a GTP create PDP response to the GGSN until a response for the accounting start message is received from the Mediation Accounting server. If the AVP is not present in Access Accept message or if the AVP value is invalid, the value "**None**" is assumed.

Type
26

Vendor ID
8164

VSA Type
105

Length
4

Value
Enumerated integer. Supported values are:

- None = 0
- No_Early_PDUs = 1
- Delay_GTP_Response = 2

SN1-Mediation-Enabled

This attribute indicates whether the Mediation Accounting configuration is enabled or disabled for GGSN.

If the AVP is not present in Access Accept message or if the AVP value is invalid, the locally configured APN value will be used.

Type
26

Vendor ID
8164

VSA Type
123

Length
4

Value
Enumerated integer. Supported values are:

- Disabled = 0
- Enabled = 1

SN1-Mediation-No-Interims

This attribute is used to disable or enable Mediation Interim Accounting Records for the session.

If this AVP is not present in Access Accept message or if the AVP value is invalid, the locally configured APN value will be used.

Type
26

Vendor ID
8164

VSA Type
146

Length
4

Value
Enumerated integer. Supported values are:

- Disabled = 0
- Enabled = 1

SN1-Mediation-VPN-Name

This attribute specifies the Mediation Context name for the session.

If this AVP is not received in the Access Accept message or if the AVP value is invalid, the locally configured APN value will be used.

Type
26

Vendor ID
8164

VSA Type

104

Length
1–128

Value
String

SN1-Min-Compress-Size

This attribute contains the minimum size (in octets) a data packet can have in order to be compressed.

Type
26

Vendor ID
8164

VSA Type
23

Length
4

Value
Unsigned integer

SN1-MIP-AAA-Assign-Addr

This attribute specifies if the PDSN/FA will allow AAA to assign the home address. The default is to not allow AAA to assign the home address.

Type
26

Vendor ID
8164

VSA Type
50

Length
4

Value
Enumerated integer. Supported values are:

- Disabled = 0 — Do not allow AAA to assign home address
- Enabled = 1 — Allow AAA to assign home address

SN1-MIP-ANCID

Accounting correlation ID created by IPGW, received by VBM and HBM.

Type

26

Vendor ID
8164

VSA Type
166

Length
12

Value
Opaque value

SN1-MIP-Dual-Anchor

Enable/disable dual-anchor service for a subscriber.

Type
26

Vendor ID
8164

VSA Type
165

Length
4

Value
Enumerated integer. Supported values are:

- Disabled = 0
- Enabled = 1

SN1-MIP-HA-Assignment-Table

MIP-HA Assignment Table name. When this is received in an Access Accept message, the system uses this local table to get the HA Address.

Type
26

Vendor ID
8164

VSA Type
154

Length
1–253

Value
ASCII string

SN1-MIP-Match-AAA-Assign-Addr

This attribute specifies if the PDSN/FA will enforce that a non-zero AAA-specified home address must match the home address present in the MIP RRQ from the mobile node, and disconnect the subscriber session if a match is not present. The default is not to force the addresses to match.

Type
26

Vendor ID
8164

VSA Type
51

Length
4

Value
Enumerated integer. Supported values are:

- Disabled = 0 — Do not force the AAA-specified home address to match RRQ
- Enabled = 1 — Force the AAA-specified home address to match RRQ

SN1-MIP-Reg-Lifetime-Realm

Configure the maximum MIP registration lifetime for a subscriber/realm.

Type
26

Vendor ID
8164

VSA Type
175

Length
2

Value
Unsigned integer

SN1-MIP-Send-Ancid

AAA attribute to enable/disable sending ANCID from FA to HA in MIP RRQ.

Type
26

Vendor ID
8164

VSA Type
163

Length
4

Value
Enumerated integer. Supported values are:

- Disabled = 0
- Enabled = 1

SN1-MIP-Send-Correlation-Info

This attribute enables/disables sending of correlation-id from FA to HA in MIP RRQ.

Type
26

Vendor ID
8164

VSA Type
188

Length
4

Value
Enumerated integer. In StarOS 8.1 and earlier, supported values are:

- Disabled = 0
- Enabled = 1

In StarOS 8.3 and later, supported values are:

- Disabled = 0
- NVSE_Starent = 1
- NVSE_CUstom1 = 2
- NVSE_Custom2 = 3

SN1-MIP-Send-Imsi

Attribute to enable/disable sending IMSI from FA to HA in MIP RRQ.

Type
26

Vendor ID
8164

VSA Type
164

Length
4

Value

Enumerated integer. In StarOS 8.1 and earlier, supported values are:

- None = 0
- Starent_NVSE = 1
- Custom1_NVSE = 2

In StarOS 8.3 and later, supported values are:

- Disabled = 0,
- NVSE_Starent = 1,
- NVSE_Custom1 = 2,
- NVSE_Custom2 = 3

SN1-MIP-Send-Term-Verification

This attribute specifies whether the PDSN/FA should send the Terminal Verification Normal Vendor/Organization Specific Extension (NVSE) in the Mobile IP RRQ message to the HA. The default is not to send the Terminal Verification NVSE.

Type

26

Vendor ID

8164

VSA Type

48

Length

4

Value

Enumerated integer. In StarOS 8.1 and earlier, supported values are:

- Disabled = 0 — Do not send
- Enabled = 1 — Send

In StarOS 8.3 and later, supported values are:

- Disabled = 0
- NVSE_Custom1 = 1 — Send custom NVSE
- NVSE_Custom2 = 2 — Send custom NVSE
- NVSE_Starent = 3 — Send custom NVSE

SN1-MN-HA-Hash-Algorithm

This attribute contains the hash algorithm to use for MN-HA authentication.

Type

26

Vendor ID

8164

VSA Type
28

Length
4

Value
Enumerated integer. Supported values are:

- MD5 = 1
- MD5-RFC2002 = 2
- HMAC-MD5 = 3

SN1-MN-HA-Timestamp-Tolerance

This attribute contains the duration of timestamp tolerance, in seconds, to use for MN-HA authentication.

Type
26

Vendor ID
8164

VSA Type
30

Length
4

Value
Unsigned integer

SN1-MS-ISDN

SN1-MS-ISDN.

Type
26

Vendor ID
8164

VSA Type
248

Length
1–9

Value
Opaque value

SN1-MSK-Lifetime

This attribute is currently not supported.

SN1-NAI-Construction-Domain

This attribute specifies the domain name to use when constructing the NAI.

Type
26

Vendor ID
8164

VSA Type
37

Length
1–247

Value
An ASCII string specifying the domain to use when constructed NAI is used.

SN1-NAT-Bind-Record

This attribute contains the NAT Binding Record.

Type
26

Vendor ID
8164

VSA Type
216

Length
Compound

Value
Contains the following subattributes:

NAT-IP-Address

NAT IP Address.

Type
1

Length
4

Value
IPv4 address

NAT-Port-Block-Start

Start port of the port chunk.

Type

2

Length

2

Value

Unsigned integer

NAT-Port-Block-End

End port of the port chunk.

Type

3

Length

2

Value

Unsigned integer

Alloc-Flag

Port chunk status. Accepted Values are 0(De-Allocated) and 1(Allocated).

Type

4

Length

1

Value

Unsigned integer

Correlation-Id

Correlation ID.

Type

5

Length

1–253

Value

String

Loading-Factor

Indicates maximum number of users per NAT IP address.

Type

6

Length

2

Value

Unsigned integer

Binding-Timer

Port chunk hold timer.

Type
7

Length
4

Value
Unsigned integer

SN1-NAT-Info-Record

NAT-Record-Info.

This attribute is also accepted in CoA response message to be used in a currently active subscriber session.

Type
26

Vendor ID
8164

VSA Type
246

Length
Compound

Value
Contains the following subattributes:

Framed-IP-Address

Framed IP address.

This attribute is also accepted in CoA response message to be used in a currently active subscriber session.

Type
1

Length
4

Value
IPv4 address

NAT-IP-Address

NAT IP address.

This attribute is also accepted in CoA response message to be used in a currently active subscriber session.

Type

2

Length

4

Value

IPv4 address

NAT-Port-Block-Start

Start port of the port chunk

This attribute is also accepted in CoA response message to be used in a currently active subscriber session.

Type

3

Length

2

Value

Unsigned integer

NAT-Port-Block-End

End port of the port chunk.

This attribute is also accepted in CoA response message to be used in a currently active subscriber session.

Type

4

Length

2

Value

Unsigned integer

Acct-Session-Id

Accounting Session ID.

This attribute is also accepted in CoA response message to be used in a currently active subscriber session.

Type

5

Length

1–17

Value

String

User-Name

User name.

This attribute is also accepted in CoA response message to be used in a currently active subscriber session.

Type
6

Length
1–128

Value
String

Correlation-Id

Correlation ID.

This attribute is also accepted in CoA response message to be used in a currently active subscriber session.

Type
7

Length
1–17

Value
String

SN1-NAT-IP-Address

This attribute includes the NAT (public) IP address used for the call.

This attribute is also accepted in CoA request and response messages to be used in a currently active subscriber session.

Type
26

Vendor ID
8164

VSA Type
217

Length
4

Value
IPv4 address

SN1-NAT-IP-Address-Old

Public IP address used for the call

This attribute is also accepted in CoA request message to be used in a currently active subscriber session.

Type

26

Vendor ID

8164

VSA Type

0

Length

4

Value

IPv4 address

SN1-NPU-Qos-Priority

This attribute configures Inter-Subscriber priority Queueing based on class of service offered. Gold has highest priority and Best_effort lowest priority. From DSCP, means the priority queueing will be done based on the DSCP marking the incoming subscriber packet carries.

Type

26

Vendor ID

8164

VSA Type

98

Length

4

Value

Enumerated integer. Supported values are:

- Best_Effort = 0
- Bronze = 1
- Silver = 2
- Gold = 3
- From_DSCP = 4

SN1-Ntk-Initiated-Ctx-Ind-Flag

This attribute indicates that the PDP context is network initiated. The attribute is missing for a mobile activated PDP context.

Type

26

Vendor ID
8164

VSA Type
142

Length
1

Value
Opaque value

SN1-Ntk-Session-Disconnect-Flag

SN1-Ntk-Session-Disconnect-Flag.

Type
26

Vendor ID
8164

VSA Type
143

Length
4

Value
Enumerated integer. Supported value is:

- Session-Disconnect = 1

SN1-Ntk-Session-Disconnect-Reason

SN1-Ntk-Session-Disconnect-Reason.

Type
26

Vendor ID
8164

VSA Type
143

Length
4

Value
Enumerated integer. Supported value is:

- Session-Disconnect = 1

SN1-Nw-Reachability-Server-Name

This attribute specifies the name of a network reachability server (defined in the destination context of the subscriber) that must respond as reachable, or the user is be redirected.

Type
26

Vendor ID
8164

VSA Type
65

Length
1–247

Value
An ASCII string representing the name of the Network Reachability Detection Server.

SN1-Overload-Disconnect

Enables/disables the overload-disconnect feature (if 1) and disables if 0

Type
26

Vendor ID
8164

VSA Type
235

Length
4

Value
Unsigned Integer

SN1-Overload-Disc-Connect-Time

Provides the connect time for a session. When this time expires, the session may become a candidate for disconnection.

Type
26

Vendor ID
8164

VSA Type
233

Length
1

Value
Integer

SN1-Overload-Disc-Inact-Time

Provides inactivity time for a session after which it may become candidate for disconnection.

Type
26

Vendor ID
8164

VSA Type
234

Length
1

Value
Integer

SN1-PDIF-MIP-Release-TIA

PDIF mobile IP release TIA.

Type
26

Vendor ID
8164

VSA Type
172

Length
4

Value
Enumerated integer. Supported values are:

- No = 0
- Yes = 1

SN1-PDIF-MIP-Required

PDIF mobile IP required.

Type
26

Vendor ID
8164

VSA Type
170

Length
4

Value

Enumerated Integer. Supported values are:

- No = 0
- Yes = 1

SN1-PDIF-MIP-Simple-IP-Fallback

PDIF mobile IP simple IP fallback.

Type

26

Vendor ID

8164

VSA Type

173

Length

4

Value

Enumerated integer. Supported values are:

- No = 0
- Yes = 1

SN1-PDSN-Correlation-Id

Correlation ID received from PDSN to HA.

Type

26

Vendor ID

8164

VSA Type

189

Length

8

Value

Opaque value

SN1-PDSN-Handoff-Req-IP-Addr

This attribute specifies if the PDSN should reject and terminate the subscriber session when the proposed address in IPCP by the mobile does not match the existing address in the PDSN. The default (Disabled) is not to reject these sessions.

Type

26

Vendor ID
8164

VSA Type
46

Length
4

Value
Enumerated integer. Supported values are:

- Disabled = 0 — Do not reject
- Enabled = 1 — Reject

SN1-PDSN-NAS-Id

NAS Identifier received from PDSN to HA.

Type
26

Vendor ID
8164

VSA Type
190

Length
1–253

Value
String

SN1-PDSN-NAS-IP-Address

NAS IP address received from PDSN to HA.

Type
26

Vendor ID
8164

VSA Type
191

Length
4

Value
IPv4 address

SN1-Permit-User-Mcast-PDUs

Specifies whether or not to let the subscriber discard multicast PDUs.

Type
26

Vendor ID
8164

VSA Type
134

Length
2

Value
Enumerated integer. Supported values are:

- Disabled = 0
- Enabled = 1

SN1-PPP-Accept-Peer-v6Ifid

This attribute indicates the acceptance of the interface ID provided by peer during PPP IPv6CP if the ID is valid. The default is disabled.

Type
26

Vendor ID
8164

VSA Type
95

Length
4

Value
Enumerated integer. Supported values are:

- Disabled = 0 — Do not accept interface ID
- Enabled = 1 — Accept interface ID

SN1-PPP-Always-On-Vse

SN1-PPP-Always-On-Vse.

Type
26

Vendor ID
8164

VSA Type

130

Length

4

Value

Enumerated integer. Supported values are:

- Disabled = 0
- Enabled = 1

SN1-PPP-Data-Compression

This attribute indicates the PPP data compression algorithm to use for the PPP session. The attribute value is a bit field, and many algorithms can be specified to indicate that one of these may be chosen by the user.

Type

26

Vendor ID

8164

VSA Type

9

Length

4

Value

Enumerated integer. Supported values are:

- None = 0
- Stac-LZS = 1
- MPPC = 2
- Deflate = 4

SN1-PPP-Data-Compression-Mode

This attribute indicates the PPP data compression mode to use for the PPP session when PPP data compression is used.

Type

26

Vendor ID

8164

VSA Type

19

Length

4

Value

Enumerated integer. Supported values are:

- Normal = 0

- Stateless = 1

SN1-PPP-Keepalive

This attribute indicates the interval for the PPP keepalive, in seconds.

Type
26

Vendor ID
8164

VSA Type
16

Length
4

Value
Unsigned integer

SN1-PPP-NW-Layer-IPv4

This attribute indicates the PPP IPCP negotiation for IPv4. The default is enabled.

Type
26

Vendor ID
8164

VSA Type
92

Length
4

Value
Enumerated integer. Supported values are:

- Disabled = 0 — IPCP negotiation for IPv4 is disabled.
- Enabled = 1 — IPCP negotiation for IPv4 is enabled.
- Passive = 2 — Start the negotiation only if peer initiates it.

SN1-PPP-NW-Layer-IPv6

This attribute indicates the PPP IPv6CP negotiation for IPv6. The default is enabled.

Type
26

Vendor ID
8164

VSA Type
93

Length
4

Value
Enumerated integer. Supported values are:

- Disabled = 0 — IPCP negotiation for IPv6 is disabled.
- Enabled = 1 — IPCP negotiation for IPv6 is enabled.
- Passive = 2 — Start the negotiation only if peer initiates it.

SN1-PPP-Outbound-Password

This attribute indicates the password to be used when the user side of the PPP connection requires authentication.

Type
26

Vendor ID
8164

VSA Type
15

Length
1–253

Value
ASCII string

SN1-PPP-Outbound-Username

This attribute indicates the username to be used when the user side of the PPP connection requires authentication.

Type
26

Vendor ID
8164

VSA Type
61

Length
1–253

Value
ASCII string

SN1-PPP-Progress-Code

This attribute provides information about the “state” of the PPP connection, when the connection was terminated.

Type
26

Vendor ID
8164

VSA Type
4

Length
4

Value
Enumerated integer. Supported values are:

- Not-Defined = 0
- Call-Lcp-Down = 10
- Call-Disconnecting = 20
- Call-Ppp-Renegotiating = 30
- Call-Arrived = 40
- Call-Pdg-Tcp-Connecting = 45
- Call-Pdg-Ssl-Connecting = 46
- Call-Lcp-Up = 50
- Call-Authenticating = 60
- Call-Bcmcs-Authenticating = 70
- Call-Authenticated = 80
- Call-Tunnel-Connecting = 85
- Call-Ipcp-Up = 90
- Call-Imsa-Authorizing = 95
- Call-Imsa-Authorized = 97
- Call-MBMS-UE-Authorizing = 98
- Call-MBMS-Bearer-Authorizing = 99
- Call-Simple-IP-Connected = 100
- Call-Mobile-IP-Connected = 110
- Call-Tunnel-Connected = 115
- Call-Pdp-Type-IP-Connected = 120
- Call-Pdp-Type-IPv6-Connected = 125
- Call-Pdp-Type-PPP-Connected = 130
- Call-Proxy-Mobile-IP-Connected = 140
- Call-Pdg-Connected = 142
- Call-Pdg-Ssl-Connected = 141
- Call-Pdg-Connected = 142
- Call-Pdg-Connected = 142

- Call-Ipsg-Connected = 145
- Call-Bcmcs-Connected = 150
- Call-MBMS-UE-Connected = 155
- Call-MBMS-Bearer-Connected = 156
- Call-Pending-Addr-From-DHCP = 160
- Call-Got-Addr-From-DHCP = 170
- Call-HA-IPSEC-Tunnel-Connecting = 180
- Call-HA-IPSEC-Connected = 190
- Call-ASN-Non-Anchor-Connected = 200
- Call-ASNPC-Connected = 210
- Call-Mobile-IPv6-Connected = 220
- Call-PMIPv6-Connected = 221
- Call-PHSPC-Connected = 230
- Call-GTP-IPv4-Connected = 235
- Call-GTP-IPv6-Connected = 236
- Call-GTP-IPv4-IPv6-Connected = 237
- Call-SGW-Connected = 245
- Call-MME-Attached = 246
- Call-Auth-Only-Connected = 247

SN1-PPP-Reneg-Disc

PPP remote reneg disconnect policy.

Type
26

Vendor ID
8164

VSA Type
187

Length
1

Value
Enumerated integer. Supported values are:

- Disc_no = 0
- Always = 1
- NAI_Prefix_MSID_Mismatch = 2

SN1-Prepaid

Prepaid.

Type
26

Vendor ID
8164

VSA Type
128

Length
1

Value
Enumerated integer. Supported values are:

- no_prepaid = 0
- custom_prepaid = 1
- standard_prepaid = 2
- wimax_prepaid = 4

SN1-Prepaid-Compressed-Count

This attribute indicates if a Pre-paid subscriber's byte usage should be counted on the basis of compressed or uncompressed byte data over the subscriber's PPP connection to the system. If not present, the default is to count uncompressed byte data.

Type
26

Vendor ID
8164

VSA Type
31

Length
4

Value
Enumerated integer. Supported values are:

- Uncompressed = 0
- Compressed = 1

SN1-Prepaid-Final-Duration-Alg

For prepaid, final duration is calculated based on the algorithm specified by the value of this attribute.

If this AVP is not received in the Access Accept message or if the AVP value is invalid, the locally configured APN value will be used.

Type

26

Vendor ID
8164

VSA Type
135

Length
4

Value
Enumerated integer. Supported values are:

- current_time = 0
- last-user-layer3-activity-time = 1
- last-airlink-activity-time = 2
- last-airlink-activity-time-last-reported = 3

SN1-Prepaid-Inbound-Octets

In an Access-Accept, this indicates how many additional inbound (bytes delivered to the subscriber) byte credits should be granted to the subscriber. In an Accounting- Request, this indicates how many total inbound byte credits have been granted to the subscriber. When this attribute is not present in the Access-Accept, then pre-paid usage checking is disabled on an inbound octet basis.

Type
26

Vendor ID
8164

VSA Type
32

Length
4

Value
Unsigned integer

SN1-Prepaid-Outbound-Octets

SN1-Prepaid-Outbound-Octets.

Type
26

Vendor ID
8164

VSA Type
33

Length

4

Value

Unsigned integer

SN1-Prepaid-Preference

This attribute specifies whether prepaid is volume based or duration based.

Type

26

Vendor ID

8164

VSA Type

129

Length

1

Value

Enumerated integer. Supported values are:

- prepaid_duration = 0
- prepaid_volume = 1

SN1-Prepaid-Profile

Do not do prepaid, regardless of the Rulebase configuration.

Type

26

Vendor ID

8164

VSA Type

155

Length

4

Value

Enumerated integer. Supported values are:

- Use-Rulebase-Config = 0
- Prohibit = 1

SN1-Prepaid-Total-Octets

In an Access-Accept, this attribute indicates how many additional byte credits (combining both inbound and outbound counts) should be granted to the subscriber. In an Accounting- Request, this indicates how many total bytes credits (combined

inbound and outbound) have been granted to the subscriber. When this attribute is not present in the Access-Accept, then pre-paid usage checking is disabled on a combined inbound and outbound octet-count basis.

Type
26

Vendor ID
8164

VSA Type
34

Length
4

Value
Unsigned integer

SN1-Prepaid-Timeout

This attribute indicates how much time may elapse before a new request for more pre-paid credits is issued. If the specified time has elapsed since the prior grant of credits was received from the RADIUS server, then a new request for credits is issued. This attribute is primarily used to periodically update the subscriber of new credits issued since the subscriber was connected. Note that credit requests will still be made on behalf of the subscriber when the subscriber drops down to the low watermark of credits (or zero if there is no low watermark). The presence or absence of this attribute does not affect that mechanism in any way. However, this timer is re-set whenever any grant of credits is received on behalf of the subscriber, regardless of why the grant of credits was requested.

Type
26

Vendor ID
8164

VSA Type
35

Length
4

Value
Unsigned integer

SN1-Prepaid-Watermark

This attribute Indicates the percentage of remaining granted credits that will trigger a new request to grant credits from the RADIUS server. For example, if 1GB of credits was granted to a user, and the value of SN-Prepaid-Watermark was 10, then when 100 MB of credits are remaining (900 MB have been used) to the subscriber, a new request for any new byte credits is issued on behalf of the subscriber. Note that when calculating the pre-paid low watermark, the total credits granted for the subscriber's entire session is used.

Type
26

Vendor ID
8164

VSA Type
36

Length
4

Value
Unsigned integer

SN1-Primary-DCCA-Peer

This attribute indicates the name of the primary DCCA peer and primary DCCA realm.

If the AVP is received in Access Accept message, the primary DCCA peer is used for Gy functionality. If not present in the Access Accept message or if the AVP value is invalid, the locally configured APN value will be used.

Type
26

Vendor ID
8164

VSA Type
223

Length
1-192

Value
A colon separated string, like “primary_peer : primary_realm”

SN1-Primary-DNS-Server

This attribute indicates the IP address of the primary DNS server that should be used for the session.

Type
26

Vendor ID
8164

VSA Type
5

Length
4

Value
IPv4 address

SN1-Primary-NBNS-Server

Primary NBNS Server IP address.

Type

26

Vendor ID
8164

VSA Type
148

Length
4

Value
IPv4 address

SN1-Proxy-MIP

This attribute specifies if the PDSN/FA will perform compulsory Proxy-MIP tunneling for a Simple-IP PDSN subscriber. This feature is licensed. The default is not to perform compulsory Proxy-MIP.

Type
26

Vendor ID
8164

VSA Type
52

Length
4

Value
Enumerated integer. Supported values are:

- Disabled = 0 — Do not perform compulsory Proxy-MIP
- Enabled = 1 — Perform compulsory Proxy-MIP

SN1-QoS-Background-Class

This attribute defines the QOS Background Traffic Class.

Type
26

Vendor ID
8164

VSA Type
91

Length
28 bytes

Value
Opaque value encoded in the following format:

- Byte 16 Bit 1 - Uplink Traffic Policing Enable/Disable

- Byte 16 Bit 2 - Downlink Traffic Policing Enable/Disable
- Byte 16 Bits 3,4 - Uplink Exceed Action
- Byte 16 Bits 5,6 - Downlink Exceed Action
- Byte 16 Bits 7,8 - Uplink Violate Action
- Byte 15 Bits 1,2 - Downlink Violate Action
- Byte 15 Bit 3 - Downlink Ext Peak Data Rate
- Byte 15 Bit 4 - Downlink Ext Committed Data Rate
- Byte 14 - Uplink Peak Data Rate
- Byte 13 - Downlink Peak Data Rate
- Byte 12 - Uplink Committed Data Rate
- Byte 11 - Downlink Committed Data Rate
- Byte 5-8 - Uplink Burst Size (in Network Byte Order)
- Byte 1-4 - Downlink Burst Size (in Network Byte Order)

SN1-QoS-Class-Background-PHB

SN1-QoS-Class-Background-PHB

Type

26

Vendor ID

10415

VSA Type

113

Length

4

Value

Enumerated integer. Supported values are:

- Best-Effort = 0
- Pass-Through = 1
- AF11 = 10
- AF12 = 12
- AF13 = 14
- AF21 = 18
- AF22 = 20
- AF23 = 22
- AF31 = 26
- AF32 = 28
- AF33 = 30

- AF41 = 34
- AF42 = 36
- AF43 = 38
- EF = 46

SN1-QoS-Class-Converstional-PHB

SN1-QoS-Class-Converstional-PHB.

Type
26

Vendor ID
10415

VSA Type
111

Length
4

Value
Enumerated integer. Supported values are:

- Best-Effort = 0
- Pass-Through = 1
- AF11 = 10
- AF12 = 12
- AF13 = 14
- AF21 = 18
- AF22 = 20
- AF23 = 22
- AF31 = 26
- AF32 = 28
- AF33 = 30
- AF41 = 34
- AF42 = 36
- AF43 = 38
- EF = 46

SN1-QoS-Class-Interactive-1-PHB

SN1-QoS-Class-Interactive-1-PHB

Type
26

Vendor ID
10415

VSA Type
114

Length
4

Value
Enumerated integer. Supported values are:

- Best-Effort = 0
- Pass-Through = 1
- AF11 = 10
- AF12 = 12
- AF13 = 14
- AF21 = 18
- AF22 = 20
- AF23 = 22
- AF31 = 26
- AF32 = 28
- AF33 = 30
- AF41 = 34
- AF42 = 36
- AF43 = 38
- EF = 46

SN1-QoS-Class-Interactive-2-PHB

SN1-QoS-Class-Interactive-2-PHB

Type
26

Vendor ID
10415

VSA Type
115

Length
4

Value
Enumerated integer. Supported values are:

- Best-Effort = 0
- Pass-Through = 1

- AF11 = 10
- AF12 = 12
- AF13 = 14
- AF21 = 18
- AF22 = 20
- AF23 = 22
- AF31 = 26
- AF32 = 28
- AF33 = 30
- AF41 = 34
- AF42 = 36
- AF43 = 38
- EF = 46

SN1-QoS-Class-Interactive-3-PHB

SN1-QoS-Class-Interactive-3-PHB

Type

26

Vendor ID

10415

VSA Type

116

Length

4

Value

Enumerated integer. Supported values are:

- Best-Effort = 0
- Pass-Through = 1
- AF11 = 10
- AF12 = 12
- AF13 = 14
- AF21 = 18
- AF22 = 20
- AF23 = 22
- AF31 = 26
- AF32 = 28
- AF33 = 30

- AF41 = 34
- AF42 = 36
- AF43 = 38
- EF = 46

SN1-QoS-Class-Streaming-PHB

SN1-QoS-Class-Streaming-PHB

Type

26

Vendor ID

10415

VSA Type

112

Length

4

Value

Enumerated integer. Supported values are:

- Best-Effort = 0
- Pass-Through = 1
- AF11 = 10
- AF12 = 12
- AF13 = 14
- AF21 = 18
- AF22 = 20
- AF23 = 22
- AF31 = 26
- AF32 = 28
- AF33 = 30
- AF41 = 34
- AF42 = 36
- AF43 = 38
- EF = 46

SN1-QoS-Conversation-Class

This attribute defines the QOS Conversation Traffic Class.

Type

26

Vendor ID
8164

VSA Type
86

Length
28 bytes

Value
Opaque value encoded in the following format:

- Byte 16 Bit 1 - Uplink Traffic Policing Enable/Disable
- Byte 16 Bit 2 - Downlink Traffic Policing Enable/Disable
- Byte 16 Bits 3,4 - Uplink Exceed Action
- Byte 16 Bits 5,6 - Downlink Exceed Action
- Byte 16 Bits 7,8 - Uplink Violate Action
- Byte 15 Bits 1,2 - Downlink Violate Action
- Byte 15 Bit 3 - Downlink Ext Peak Data Rate
- Byte 15 Bit 4 - Downlink Ext Committed Data Rate
- Byte 14 - Uplink Peak Data Rate
- Byte 13 - Downlink Peak Data Rate
- Byte 12 - Uplink Committed Data Rate
- Byte 11 - Downlink Committed Data Rate
- Byte 5-8 - Uplink Burst Size (in Network Byte Order)
- Byte 1-4 - Downlink Burst Size (in Network Byte Order)

SN1-QoS-Interactive1-Class

This attribute defines the QOS Interactive Traffic Class.

Type
26

Vendor ID
8164

VSA Type
88

Length
28 bytes

Value
Opaque value encoded in the following format:

- Byte 16 Bit 1 - Uplink Traffic Policing Enable/Disable
- Byte 16 Bit 2 - Downlink Traffic Policing Enable/Disable
- Byte 16 Bits 3,4 - Uplink Exceed Action

- Byte 16 Bits 5,6 - Downlink Exceed Action
- Byte 16 Bits 7,8 - Uplink Violate Action
- Byte 15 Bits 1,2 - Downlink Violate Action
- Byte 15 Bit 3 - Downlink Ext Peak Data Rate
- Byte 15 Bit 4 - Downlink Ext Committed Data Rate
- Byte 14 - Uplink Peak Data Rate
- Byte 13 - Downlink Peak Data Rate
- Byte 12 - Uplink Committed Data Rate
- Byte 11 - Downlink Committed Data Rate
- Byte 5-8 - Uplink Burst Size (in Network Byte Order)
- Byte 1-4 - Downlink Burst Size (in Network Byte Order)

SN1-QoS-Interactive2-Class

This attribute defines the QOS Interactive2 Traffic Class.

Type

26

Vendor ID

8164

VSA Type

89

Length

28 bytes

Value

Opaque value encoded in the following format:

- Byte 16 Bit 1 - Uplink Traffic Policing Enable/Disable
- Byte 16 Bit 2 - Downlink Traffic Policing Enable/Disable
- Byte 16 Bits 3,4 - Uplink Exceed Action
- Byte 16 Bits 5,6 - Downlink Exceed Action
- Byte 16 Bits 7,8 - Uplink Violate Action
- Byte 15 Bits 1,2 - Downlink Violate Action
- Byte 15 Bit 3 - Downlink Ext Peak Data Rate
- Byte 15 Bit 4 - Downlink Ext Committed Data Rate
- Byte 14 - Uplink Peak Data Rate
- Byte 13 - Downlink Peak Data Rate
- Byte 12 - Uplink Committed Data Rate
- Byte 11 - Downlink Committed Data Rate
- Byte 5-8 - Uplink Burst Size (in Network Byte Order)

- Byte 1-4 - Downlink Burst Size (in Network Byte Order)

SN1-QoS-Interactive3-Class

This attribute defines the QOS Interactive3 Traffic Class.

Type
26

Vendor ID
8164

VSA Type
90

Length
28 bytes

Value
Opaque value encoded in the following format:

- Byte 16 Bit 1 - Uplink Traffic Policing Enable/Disable
- Byte 16 Bit 2 - Downlink Traffic Policing Enable/Disable
- Byte 16 Bits 3,4 - Uplink Exceed Action
- Byte 16 Bits 5,6 - Downlink Exceed Action
- Byte 16 Bits 7,8 - Uplink Violate Action
- Byte 15 Bits 1,2 - Downlink Violate Action
- Byte 15 Bit 3 - Downlink Ext Peak Data Rate
- Byte 15 Bit 4 - Downlink Ext Committed Data Rate
- Byte 14 - Uplink Peak Data Rate
- Byte 13 - Downlink Peak Data Rate
- Byte 12 - Uplink Committed Data Rate
- Byte 11 - Downlink Committed Data Rate
- Byte 5-8 - Uplink Burst Size (in Network Byte Order)
- Byte 1-4 - Downlink Burst Size (in Network Byte Order)

SN1-QoS-Negotiated

Negotiated QoS for GGSN sessions.

Type
26

Vendor ID
8164

VSA Type
147

Length

In 10.2 and earlier releases: 4–17

In 11.0 and later releases: 4–20

Value

String

SN1-QoS-Renegotiation-Timeout

This attribute configures the timeout duration of dampening time for dynamic QoS renegotiation.

Type

26

Vendor ID

8164

VSA Type

145

Length

1

Value

1

SN1-QoS-Streaming-Class

This attribute defines the QOS Streaming Traffic Class.

Type

26

Vendor ID

8164

VSA Type

87

Length

28 byte

Value

Opaque value encoded in the following format:

- Byte 16 Bit 1 - Uplink Traffic Policing Enable/Disable
- Byte 16 Bit 2 - Downlink Traffic Policing Enable/Disable
- Byte 16 Bits 3,4 - Uplink Exceed Action
- Byte 16 Bits 5,6 - Downlink Exceed Action
- Byte 16 Bits 7,8 - Uplink Violate Action
- Byte 15 Bits 1,2 - Downlink Violate Action
- Byte 15 Bit 3 - Downlink Ext Peak Data Rate

- Byte 15 Bit 4 - Downlink Ext Committed Data Rate
- Byte 14 - Uplink Peak Data Rate
- Byte 13 - Downlink Peak Data Rate
- Byte 12 - Uplink Committed Data Rate
- Byte 11 - Downlink Committed Data Rate
- Byte 5-8 - Uplink Burst Size (in Network Byte Order)
- Byte 1-4 - Downlink Burst Size (in Network Byte Order)

SN1-QoS-Tp-Dnlk

This attribute enables/disables Traffic Policing/Shaping in downlink direction.

This attribute is also accepted in CoA request message to be used in a currently active subscriber session.

Type

26

Vendor ID

8164

VSA Type

73

Length

4

Value

Enumerated integer. Supported values are:

- Disabled = 0
- Policing = 1
- Shaping = 2

SN1-QoS-Tp-Uplk

This attribute enables/disables Traffic Policing/Shaping in uplink direction.

This attribute is also accepted in CoA request message to be used in a currently active subscriber session.

Type

26

Vendor ID

8164

VSA Type

79

Length

4

Value

Enumerated integer. Supported values are:

- Disabled = 0
- Policing = 1
- Shaping = 2

SN1-QoS-Traffic-Policy

This compound attribute simplifies sending QoS values for Traffic Class, Direction, Burst-Size, Committed-Data-Rate, Peak-Data-Rate, Exceed-Action, and Violate-Action from the RADIUS server. When the SN1-QoS-Traffic-Policy attribute is sent along with the Acct-Session-ID attribute, the system matches the particular PtDP context, and applies the new policy and retains the policy with the subscriber profile for future use. The next time the system sends a CoA request with a new policy and a different Acct-Session-ID for the same subscriber, the previously received policy is also applied to the matching PDP context along with the new policy.

Important: This attribute is specific to the GGSN service.

This attribute is also accepted in CoA request message to be used in a currently active subscriber session.

Type
26

Vendor ID
8164

VSA Type
177

Value
Contains the following subattributes:

Direction

Direction of traffic.

Type
1

Length
1

Value
Unsigned integer. Supported values are:

- Downlink = 0
- Uplink = 1

Class

Traffic class.

Type
2

Length

1

Value

Unsigned integer. Supported values are:

- Undefined = 0
- Conversational = 1
- Streaming = 2
- Interactive TP 1 = 4
- Interactive TP 2 = 5
- Interactive TP 3 = 6
- Background = 7

Burst-Size

Peak burst size.

Type

3

Length

4

Value

Unsigned integer

Committed-Data-Rate

Committed data rate.

Type

4

Length

4

Value

Unsigned integer

Peak-Data-Rate

Peak data rate.

Type

5

Length

4

Value

Unsigned integer

Exceed-Action

Action to take on packets that exceed the Committed-Data-Rate but do not violate the Peak-Data-Rate.

Type

6

Length

1

Value

Unsigned integer. Supported values are:

- Transmit = 0
- Drop = 1
- Lower IP Precedence = 2

Violate-Action

Violate action.

Type

7

Length

1

Value

Unsigned integer. Supported values are:

- Transmit = 0
- Drop = 1
- Lower IP Precedence = 2
- Buffer = 3
- Buffer-Transmit-On-Full = 4

Auto-Readjust-Enabled

Available only in StarOS 8.1 and later. Auto-readjust enabled.

Type

8

Length

1

Value

Unsigned integer

Auto-Readjust-Duration

Available only in StarOS 8.1 and later. Auto-readjust duration.

Type

9

Length
4

Value
Unsigned integer

Qci

Available only in 11.0 and later releases. QOS QCI accepted values are 1 (qci 1), 2 (qci 2), 3 (qci 3), 4 (qci 4), 5 (qci 5), 6 (qci 6), 7 (qci 7), 8 (qci 8), 9 (qci 9).

Type
10

Length
1

Value
Unsigned integer

SN1-Rad-APN-Name

This attributes specifies the RADIUS returned APN name.

If this AVP is not present in the Access Accept message or if the AVP value is invalid, the SGSN supplied APN value in create PDP context will be used for the session.

Type
26

Vendor ID
8164

VSA Type
162

Length
1–64

Value
Opaque value

SN1-Radius-Returned-Username

This attribute is used to prefer RADIUS returned user name over constructed username in the accounting messages.

Type
26

Vendor ID
8164

VSA Type
236

Length

4

Value

Enumerated integer. Supported values are:

- No = 0
- Yes = 1

SN1-Re-CHAP-Interval

The Periodic CHAP authentication interval for PPP, in seconds.

Type

26

Vendor ID

8164

VSA Type

7

Length

4

Value

Integer

SN1-Roaming-Behavior

This attribute specifies the configuration for the behavior bits settings for a roaming subscriber in an APN.

When GGSN is configured to reject the charging characteristics sent by the SGSN for "roaming" subscribers, it uses the profile index specified by **`cc-home behavior <bits> profile <index>`** command to determine the appropriate CCs to use.

Multiple behavior bits can be configured for a single profile index by "Or"ing the bit strings together and convert the result to hexadecimal. The properties of the actual CC profile index are configured as part of the GGSN service using the cc profile command.

If this AVP is present in Access Accept message the locally configured APN value will be overridden.

Type

26

Vendor ID

8164

VSA Type

121

Length

4

Value

Unsigned integer

SN1-Roaming-Profile

This attribute specifies the configuration for the profile bits settings for a roaming subscriber in an APN.

If this AVP is present in Access Accept message the locally configured APN value will be overridden.

Type

26

Vendor ID

8164

VSA Type

118

Length

4

Value

Unsigned integer

SN1-Roaming-Sub-Use-GGSN

This attribute configures GGSN to accept GGSN's charging characteristics for roaming subscribers defined for the APN.

If this AVP is present in Access Accept message the locally configured APN value will be overridden.

Type

26

Vendor ID

8164

VSA Type

108

Length

4

Value

Enumerated integer. Supported values are:

- Deny = 0
- Accept = 1

SN1-ROHC-Direction

Specifies in which direction to apply Robust Header Compression (ROHC).

Type

Type 26

Vendor ID

Vendor-ID 8164

VSA Type

VSA-Type 153

Length
4

Value
Enumerated integer. Supported values are:

- Any = 0
- Uplink = 1
- Downlink = 2

SN1-ROHC-Flow-Marking-Mode

Configure ROHC compression for marked flows only.

Type
26

Vendor ID
8164

VSA Type
216

Length
4

Value
Enumerated integer. Supported values are:

- False = 0
- True = 1

SN1-ROHC-Mode

Sets the mode of operation for Robust Header Compression for IP.

Type
26

Vendor ID
8164

VSA Type
151

Length
4

Value
Enumerated integer. Supported values are:

- Reliable = 0
- Optimistic = 1
- Unidirectional = 2

SN1-ROHC-Profile-Name

Specifies the ROHC profile name to use for the subscriber.

Type
26

Vendor ID
8164

VSA Type
238

Length
1–64

Value
ASCII string

SN1-Routing-Area-Id

For GGSN calls this indicates the Routing Area ID of the subscriber.

Type
26

Vendor ID
8164

VSA Type
249

Length
3

Value
Opaque value

SN1-Rulebase

When the session is active charging enabled, Rulebase name will specify one of the pre configured ECSv2 rulebases in active charging subsystem.

This attribute is also accepted in CoA request message to be used in a currently active subscriber session.

If this AVP is present in Access Accept message the locally configured APN value will be overridden. If there is no value configured in the APN, this value will not be applied to the session.

Type
26

Vendor ID
8164

VSA Type
250

Length
1–64

Value
String

SN1-Secondary-DCCA-Peer

This attribute indicates the name of the Secondary DCCA peer and Secondary DCCA realm.

If this AVP is received in Access Accept message the secondary DCCA peer is used for Gy functionality. If not present in the Access Accept message or if the AVP value is invalid, the locally configured APN value will be used.

Type
26

Vendor ID
8164

VSA Type
224

Length
1–192

Value
A colon separated string, like “secondary_peer : secondary_realm”.

SN1-Secondary-DNS-Server

This attribute indicates the IP address of the secondary DNS server that should be used for the session.

Type
26

Vendor ID
8164

VSA Type
6

Length
4

Value
IPv4 address

SN1-Secondary-NBNS-Server

Secondary NBNS Server IP Address.

Type
26

Vendor ID

8164

VSA Type
149

Length
4

Value
IPv4 address

SN1-Service-Address

Used to send the bind IP address of the service in RADIUS messages.

Type
26

Vendor ID
8164

VSA Type
169

Length
4

Value
IPv4 address

SN1-Service-Type

This attribute signifies the type that the user is accessing.

Type
26

Vendor ID
8164

VSA Type
24

Length
4

Value
Enumerated integer. Supported values are:

- None = 0
- PDSN = 1
- Management = 2
- HA = 3
- GGSN = 4
- LNS = 5

- IPSG = 6
- CSCF = 7
- ASNGW = 8
- PDIF = 9
- STANDALONE_FA = 10
- SGSN = 11
- PHSGW = 12
- PDG = 13
- MIPV6HA = 14
- PGW = 15
- SGW = 16
- FNG = 17
- OGW = 18 — NOTE: Applicable only in release 12.0.
- HNBGW = 19

SN1-Simultaneous-SIP-MIP

This attribute indicates if a PDSN Subscriber can simultaneously be given Simple IP and Mobile IP service.

Type
26

Vendor ID
8164

VSA Type
22

Length
4

Value
Enumerated integer. Supported values are:

- Disabled = 0
- Enabled = 1

SN1-Subscriber-Acct-Mode

SN1-Subscriber-Acct-Mode

Type
26

Vendor ID
8164

VSA Type

192

Length

4

Value

Enumerated integer. Supported values are:

- flow-based-auxilliary = 0
- flow-based-all = 1
- flow-based-none = 2
- session-based = 3
- main-a10-only = 4

SN1-Subscriber-Accounting

This attribute specifically enables or disables subscriber accounting. Note that if enabled, subscriber accounting still needs to be enabled in the subscriber's AAA context for accounting to be performed.

The AVP value 0 means no accounting; 1 indicates RADIUS accounting; and 2 indicates GTPP accounting. If an invalid value is received or if the AVP is not present in the Access Accept message, then the locally configured APN value will be used.

Type

26

Vendor ID

8164

VSA Type

64

Length

4

Value

Enumerated integer. Supported values are:

- None = 0
- Radius = 1
- GTPP = 2

SN1-Subscriber-Acct-Interim

This attribute specifies if accounting INTERIM messages are enabled for the subscriber. Note that accounting must also be globally enabled for the subscriber (SN-Subscriber-Accounting), and enabled for the subscriber's AAA context (along with a specific INTERIM interval), if accounting INTERIM messages are to be sent.

The AVP value 0 represents normal or enabled for generating accounting INTERIM messages. The value 1 represents enabled for suppressing RADIUS accounting INTERIM messages.

If the AVP is not present in the Access Accept message or if the AVP value is invalid, the value 0 is assumed.

Type

26

Vendor ID
8164

VSA Type
70

Length
4

Value
Enumerated integer. Supported values are:

- Normal = 0
- Suppress = 1

SN1-Subscriber-Acct-Rsp-Action

When this attribute is set to None, there is no action taken while waiting for a response for the accounting start message from the RADIUS server. When this attribute is set to No-Early-PDUs the system buffers all packets from the user (uplink) until a response for the accounting start message is received from the RADIUS server. When set to Delay_GTP_Response, the system does not send a GTP create response to the GGSN until a response for the accounting start message is received from the RADIUS server.

Type
26

Vendor ID
8164

VSA Type
100

Length
4

Value
Enumerated integer. Supported values are:

- None = 0
- No_Early_PDUs = 1
- Delay_GTP_Response = 2

SN1-Subscriber-Acct-Start

This attribute specifies if accounting START messages are enabled for the subscriber. Note that accounting must also be globally enabled for the subscriber (**SN-Subscriber-Accounting**), and enabled for the subscriber's AAA context, if accounting START messages are to be sent.

The AVP value 0 represents normal or enabled for generating accounting START messages. The value 1 represents enabled for suppressing RADIUS accounting START messages.

If the AVP is not present in the Access Accept message or if the AVP value is invalid, the value 0 is assumed.

Type

26

Vendor ID
8164

VSA Type
69

Length
4

Value
Enumerated integer. Supported values are:

- Normal = 0
- Suppress = 1

SN1-Subscriber-Acct-Stop

This attribute specifies if accounting STOP messages are enabled for the subscriber. Note that accounting must also be globally enabled for the subscriber (**SN-Subscriber-Accounting**), and enabled for the subscriber's AAA context, if accounting STOP messages are to be sent.

The AVP value 0 represents normal or enabled for generating accounting STOP messages. The value 1 represents enabled for suppressing RADIUS accounting STOP messages.

If the AVP is not present in the Access Accept message or if the AVP value is invalid, the value 0 is assumed.

Type
26

Vendor ID
8164

VSA Type
71

Length
4

Value
Enumerated integer. Supported values are:

- Normal = 0
- Suppress = 1

SN1-Subscriber-Class

Customer-requested attribute for supporting specific behavior for their subscriber billing.

Type
26

Vendor ID
8164

VSA Type

219

Length

4

Value

Enumerated integer. Supported values are:

- Normal_Subscriber = 0
- Ting_100 = 1
- Ting_500 = 2
- Ting_Buddy = 3
- Ting_Star = 4
- Ting_Nolimit_SMS = 5
- Kids_Locator = 6
- Ting_2000 = 7
- Handicapped_Welfare = 8
- Reserved = 9

SN1-Subscriber-Dormant-Activity

This attribute specifies whether to treat dormant packets routed to the mobile as activity for idle timeout purposes. The default is Enabled. Disabled means dormant packets routed to the mobile are not treated as activity for idle timeout purposes.

Type

26

Vendor ID

8164

Length

4

Value

Enumerated integer. Supported values are:

- Disabled = 0
- Enabled = 1

SN1-Subscriber-IP-Hdr-Neg-Mode

This attribute specifies whether to wait for (detect) IP header compression to be requested by the mobile before responding, or not to wait (force). Force is the default.

Type

26

Vendor ID

8164

VSA Type

67

Length
4

Value
Enumerated integer. Supported values are:

- Force = 0
- Detect = 1

SN1-Subscriber-IP-TOS-Copy

This attribute enables copying of TOS bits from outer IP headers into inner tunneled IP headers. The default is Both.

Type
26

Vendor ID
8164

VSA Type
85

Length
4

Value
Enumerated integer. Supported values are:

- None = 0
- Access-Tunnel = 1
- Data-Tunnel = 2
- Both = 3

SN1-Subscriber-Nexthop-Address

This attribute specifies the nexthop gateway address to be returned by AAA on a per subscriber basis.

Type
26

Vendor ID
8164

VSA Type
127

Length
6

Value
IPv4 address

SN1-Subscriber-No-Interims

This is a GGSN specific attribute. When set to 0 (disabled) interim accounting is generated. When set to 1 (enabled) interim accounting generation is disabled.

If the AVP is not present in the Access Accept message or if the AVP value is invalid, the value 0 is assumed.

Type

26

Vendor ID

8164

VSA Type

133

Length

4

Value

Enumerated integer. Supported values are:

- Enabled = 0
- Disabled = 1

SN1-Subscriber-Permission

This attribute indicates the services allowed to be delivered to the subscriber. The attribute value is a bit field, and many algorithms can be specified to indicate that one of these may be chosen by the user.

Type

26

Vendor ID

8164

VSA Type

20

Length

4

Value

Enumerated integer. Supported values are:

- None = 0
- Simple-IP = 1
- Mobile-IP = 2
- Simple-IP-Mobile-IP = 3
- HA-Mobile-IP = 4
- Simple-IP-HA-Mobile-IP = 5
- Mobile-IP-HA-Mobile-IP = 6
- All = 7

In StarOS 8.3 and later, supported values are:

- None = 0
- Simple-IP = 1
- Mobile-IP = 2
- Simple-IP-Mobile-IP = 3
- HA-Mobile-IP = 4
- Simple-IP-HA-Mobile-IP = 5
- Mobile-IP-HA-Mobile-IP = 6
- SIP-MIP-HA-MIP = 7
- GGSN-PDP-TYPE-IP = 0x08, # see SessSubscriberPermission in sess_common.x
- GGSN-PDP-TYPE-PPP = 0x10, # see SessSubscriberPermission in sess_common.x
- Network-Mobility = 0x20
- FA-HA-NEMO = 0x26
- All = 0x3F

SN1-Subscriber-Template-Name

RADIUS returned subscriber template.

Type
26

Vendor ID
8164

VSA Type
158

Length
1–127

Value
String

SN1-Subs-Acc-Flow-Traffic-Valid

This attribute indicates the subscriber account flow traffic is valid.

Type
26

Vendor ID
8164

VSA Type
225

Length
4

Value

Enumerated integer. Supported values are:

- Disable = 0
- Enable = 1

SN1-Subs-IMSA-Service-Name

IMS Authorization Service name.

Type

26

Vendor ID

8164

VSA Type

159

Length

1–128

Value

ASCII string

SN1-Subs-VJ-Slotid-Cmp-Neg-Mode

Enable/Disable slotid compression in either direction when using VJ compression.

Type

26

Vendor ID

8164

VSA Type

221

Length

4

Value

Enumerated integer. Supported values are:

- None = 0
- Receive = 1
- Transmit = 2
- Both = 3

SN1-Tp-Dnlk-Burst-Size

This attribute specifies the Traffic Policing downlink burst size in bytes.

This attribute is also accepted in CoA request message to be used in a currently active subscriber session.

Type
26

Vendor ID
8164

VSA Type
76

Length
4

Value
Unsigned integer

SN1-Tp-Dnlk-Committed-Data-Rate

This attribute specifies the Traffic Policing downlink committed data rate in bps.

This attribute is also accepted in CoA request message to be used in a currently active subscriber session.

Type
26

Vendor ID
8164

VSA Type
74

Length
4

Value
Unsigned integer

SN1-Tp-Dnlk-Exceed-Action

This attribute specifies the action to take on Traffic Policing downlink packets that exceed the committed-data-rate but do not violate the peak-data-rate.

This attribute is also accepted in CoA request message to be used in a currently active subscriber session.

Type
26

Vendor ID
8164

VSA Type
77

Length
4

Value

Enumerated integer. Supported values are:

- Transmit = 0
- Drop = 1
- Lower-IP-Precedence = 2
- Buffer = 3
- Transmit-On-Buffer-Full = 4

SN1-Tp-Dnlk-Peak-Data-Rate

This attribute specifies the Traffic Policing downlink peak data rate in bps.

This attribute is also accepted in CoA request message to be used in a currently active subscriber session.

Type

26

Vendor ID

8164

VSA Type

75

Length

4

Value

Unsigned integer

SN1-Tp-Dnlk-Violate-Action

This attribute specifies the action to take on Traffic Policing downlink packets that exceed both the committed-data-rate and the peak-data-rate.

This attribute is also accepted in CoA request message to be used in a currently active subscriber session.

Type

26

Vendor ID

8164

VSA Type

78

Length

4

Value

Enumerated integer. Supported values are:

- Transmit = 0
- Drop = 1
- Lower-IP-Precedence = 2

- Buffer = 3
- Transmit-On-Buffer-Full = 4

SN1-Tp-Uplk-Burst-Size

This attribute specifies the Traffic Policing uplink burst size in bytes.

This attribute is also accepted in CoA request message to be used in a currently active subscriber session.

Type
26

Vendor ID
8164

VSA Type
82

Length
4

Value
Unsigned integer

SN1-Tp-Uplk-Committed-Data-Rate

This attribute specifies the Traffic Policing uplink committed data rate in bps.

This attribute is also accepted in CoA request message to be used in a currently active subscriber session.

Type
26

Vendor ID
8164

VSA Type
80

Length
4

Value
Unsigned integer

SN1-Tp-Uplk-Exceed-Action

This attribute specifies the action to take on Traffic Policing uplink packets that exceed the committed-data-rate but do not violate the peak-data-rate.

This attribute is also accepted in CoA request message to be used in a currently active subscriber session.

Type
26

Vendor ID
8164

VSA Type
83

Length
4

Value
Enumerated integer. Supported values are:

- Transmit = 0
- Drop = 1
- Lower-IP-Precedence = 2
- Buffer = 3
- Transmit-On-Buffer-Full = 4

SN1-Tp-Uplk-Peak-Data-Rate

This attribute specifies the Traffic Policing uplink peak data rate in bps.

This attribute is also accepted in CoA request message to be used in a currently active subscriber session.

Type
26

Vendor ID
8164

VSA Type
81

Length
4

Value
Unsigned integer

SN1-Tp-Uplk-Violate-Action

This attribute specifies the action to take on Traffic Policing uplink packets that exceed both the committed-data-rate and the peak-data-rate.

This attribute is also accepted in CoA request message to be used in a currently active subscriber session.

Type
26

Vendor ID
8164

VSA Type
84

Length

4

Value

Enumerated integer. Supported values are:

- Transmit = 0
- Drop = 1
- Lower-IP-Precedence = 2
- Buffer = 3
- Transmit-On-Buffer-Full = 4

SN1-Traffic-Group

This attribute is used to assign a tag to a FA or a group of FAs, so that traffic policy can be enforced based on the tag value.

Type

26

Vendor ID

8164

VSA Type

161

Length

2

Value

Unsigned integer

SN1-Transparent-Data

This AVP is used by RADIUS to provide Global Title information for the GGSN to use in CDRs and Quota Auth.

Type

26

Vendor ID

8164

VSA Type

247

Length

In StarOS 8.1 and later: 1–247 In StarOS 8.0: 1–237

Value

Opaque value

SN1-Tun-Addr-Policy

Describes IP address validation policy for non L2TP tunneled calls.

Type
26

Vendor ID
8164

VSA Type
156

Length
4

Value
Enumerated integer. Supported values are:

- no-local-alloc-validate = 0
- local-alloc = 1
- local-alloc-validate = 2

SN1-Tunnel-Gn

Used to enable/disable Gn interface from PDG/TTG to GGSN.

Type
26

Vendor ID
8164

VSA Type
174

Length
4

Value
Enumerated integer. Supported values are:

- Disabled = 0
- Enabled = 1

SN1-Tunnel-ISAKMP-Crypto-Map

This attribute specifies the system-defined crypto map to use for the subscriber's Mobile-IP connection, when IPSec is used to protect the Mobile-IP connection. This attribute is salt-encrypted.

Type
26

Vendor ID
8164

VSA Type
38

Length

1–128

Value

String

SN1-Tunnel-ISAKMP-Secret

This attribute specifies the secret to use for IKE.

Type

26

Vendor ID

8164

VSA Type

39

Length

1–128

Value

String

SN1-Tunnel-Load-Balancing

Specifies the load-balancing algorithm to use when tunneling is employed.

Type

26

Vendor ID

8164

VSA Type

27

Length

4

Value

Enumerated integer. Supported values are:

- random = 1
- balanced = 2
- prioritized = 3

SN1-Tunnel-Password

This attribute contains a secret for tunneling usage. Currently this is only used for L2TP. It is recommended that if your RADIUS server supports salt-encryption of attributes, that you use the Tunnel-Password attribute instead.

Type

26

Vendor ID
8164

VSA Type
26

Length
1–247

Value
A bitstring which is the tunnel secret.

SN1-Unclassify-List-Name

SN1-Unclassify-List-Name.

Type
26

Vendor ID
8164

VSA Type
132

Length
1–132

Value
String

SN1-Virtual-APN-Name

This attribute indicates the virtual APN name.

Type
26

Vendor ID
8164

VSA Type
94

Length
1–64

Value
Opaque value

SN1-Visiting-Behavior

This attribute specifies the configuration for the behavior bits settings for a visiting subscriber in an APN.

When GGSN is configured to reject the charging characteristics sent by the SGSN for "home" subscribers, it uses the profile index specified by **cc-home behavior <bits> profile <index>** command to determine the appropriate CCs to use.

Multiple behavior bits can be configured for a single profile index by "Or"ing the bit strings together and convert the result to hexadecimal. The properties of the actual CC profile index are configured as part of the GGSN service using the cc profile command.

If this AVP is present in Access Accept message the locally configured APN value will be overridden.

Type
26

Vendor ID
8164

VSA Type
120

Length
4

Value
Unsigned integer

SN1-Visiting-Profile

This attribute specifies the configuration for the profile bits settings for a visiting subscriber in an APN.

If this AVP is present in Access Accept message the locally configured APN value will be overridden.

Type
26

Vendor ID
8164

VSA Type
117

Length
4

Value
Unsigned integer

SN1-Visiting-Sub-Use-GGSN

This attribute configures GGSN to accept GGSN's charging characteristics for visiting subscribers defined for the APN.

If this AVP is present in Access Accept message the locally configured APN value will be overridden.

Type
26

Vendor ID
8164

VSA Type
107

Length
4

Value
Enumerated integer. Supported values are:

- Deny = 0
- Accept = 1

SN1-Voice-Push-List-Name

SN1-Voice-Push-List-Name.

Type
26

Vendor ID
8164

VSA Type
131

Length
1–32

Value
String

SN1-VPN-ID

This attribute indicates the Destination VPN of the user, specified by a 32-bit identifier.

Type
26

Vendor ID
8164

VSA Type
1

Length
4

Value
Unsigned integer

SN1-VPN-Name

This attribute indicates the name of the user's destination VPN.

Type

26

Vendor ID
8164

VSA Type
2

Length
1–253

Value
ASCII string

SNA-Input-Gigawords

This attribute contains the total number of input gigawords.

Type
26

Vendor ID
8164

VSA Type
206

Length
4

Value
Unsigned integer

SNA-Output-Gigawords

This attribute contains the total number of output gigawords.

Type
26

Vendor ID
8164

VSA Type
207

Length
4

Value
Unsigned integer

SNA-PPP-Bad-Addr

This attribute contains the total number of frames received with bad address field in the HDLC header field, for the user's PPP session.

Type
26

Vendor ID
8164

VSA Type
1011

Length
4

Value
Unsigned integer

SNA-PPP-Bad-Ctrl

This attribute contains the total number of frames received with bad control field in the HDLC header field, for the user's PPP session.

Type
26

Vendor ID
8164

VSA Type
1012

Length
4

Value
Unsigned integer

SNA-PPP-Bad-FCS

This attribute contains the number of frames received, for the user's PPP session, with bad FCS.

Type
26

Vendor ID
8164

VSA Type
1014

Length
4

Value

Unsigned integer

SNA-PPP-Ctrl-Input-Octets

This attribute contains the number of PPP Control Octets received for the user's PPP session.

Type
26

Vendor ID
8164

VSA Type
1001

Length
4

Value
Unsigned integer

SNA-PPP-Ctrl-Input-Packets

This attribute contains the number of PPP Control packets received for the user's PPP session.

Type
26

Vendor ID
8164

VSA Type
1003

Length
4

Value
Unsigned integer

SNA-PPP-Ctrl-Output-Octets

This attribute contains the number of PPP Control Octets sent to the user during the user's PPP session.

Type
26

Vendor ID
8164

VSA Type
1002

Length
4

Value
Unsigned integer

SNA-PPP-Ctrl-Output-Packets

This attribute contains the number of PPP Control packets sent to the user during the user's PPP session.

Type
26

Vendor ID
8164

VSA Type
1004

Length
4

Value
Unsigned integer

SNA-PPP-Discards-Input

This attribute contains the number of PPP input frames that were discarded during the user's PPP session.

Type
26

Vendor ID
8164

VSA Type
1007

Length
4

Value
Unsigned integer

SNA-PPP-Discards-Output

This attribute contains the number of PPP output frames that were discarded during the user's PPP session.

Type
26

Vendor ID
8164

VSA Type
1008

Length

4

Value
Unsigned integer

SNA-PPP-Echo-Req-Input

This attribute contains the number of LCP echo packets received, for the user's PPP session.

Type
26

Vendor ID
8164

VSA Type
1015

Length
4

Value
Unsigned integer

SNA-PPP-Echo-Req-Output

This attribute contains the number of LCP echo packets sent, for the user's PPP session.

Type
26

Vendor ID
8164

VSA Type
1016

Length
4

Value
Unsigned integer

SNA-PPP-Echo-Rsp-Input

This attribute contains the number of LCP echo response packets received, for the user's PPP session.

Type
26

Vendor ID
8164

VSA Type
1017

Length
4

Value
Unsigned integer

SNA-PPP-Echo-Rsp-Output

This attribute contains the number of LCP echo response packets sent, for the user's PPP session.

Type
26

Vendor ID
8164

VSA Type
1018

Length
4

Value
Unsigned integer

SNA-PPP-Errors-Input

This attribute contains the number of PPP input de-framing errors for the user's PPP session.

Type
26

Vendor ID
8164

VSA Type
1009

Length
4

Value
Unsigned integer

SNA-PPP-Errors-Output

This attribute contains the number of PPP output framing errors for the user's PPP session.

Type
26

Vendor ID
8164

VSA Type

1010

Length
4

Value
Unsigned integer

SNA-PPP-Framed-Input-Octets

This attribute contains the number of PPP octets received (without framing overhead) for the user's PPP session.

Type
26

Vendor ID
8164

VSA Type
1005

Length
4

Value
Unsigned integer

SNA-PPP-Framed-Output-Octets

This attribute contains the number of PPP octets sent (without framing overhead) to the user during the user's PPP session.

Type
26

Vendor ID
8164

VSA Type
1006

Length
4

Value
Unsigned integer

SNA-PPP-Packet-Too-Long

This attribute contains the total number of frames received, for the user's PPP session, that exceeds the MTU of the interface.

Type
26

Vendor ID
8164

VSA Type
1013

Length
4

Value
Unsigned integer

SNA-PPP-Unfr-Data-In-Gig

This attribute contains the total number of PPP gigawords without framing sent for the subscriber's session. When combined with the attribute SNA-PPP-Unfr-data-In-Oct, a 64-bit value can be formed which is the total number of PPP octets without framing send for the subscriber's session.

Type
26

Vendor ID
8164

VSA Type
202

Length
4

Value
Unsigned integer

SNA-PPP-Unfr-Data-Out-Gig

This attribute contains the total number of PPP octets without framing received for the user's session. When combined with the attribute SNA-PPP-Unfr-data-In-Oct, a 64-bit value can be formed which is the total number of PPP octets without framing received for the subscriber's session.

Type
26

Vendor ID
8164

VSA Type
203

Length
4

Value
Unsigned integer

SNA-PPP-Unfr-data-In-Oct

This attribute contains the total number of PPP octets without framing sent for the user’s session.

Type
26

Vendor ID
8164

VSA Type
200

Length
4

Value
Unsigned integer

SNA-PPP-Unfr-data-Out-Oct

This attribute contains the total number of PPP octets without framing received for the user's session.

Type
26

Vendor ID
8164

VSA Type
201

Length
4

Value
Unsigned integer

SNA-RPRAK-Rcvd-Acc-Ack

This attribute contains the total number of A11 registration ACK accepted for the user's session.

Type
26

Vendor ID
8164

VSA Type
1028

Length
4

Value
Unsigned integer

SNA-RPRAK-Rcvd-Mis-ID

This attribute contains the total number of A11 registration ACK messages received with ID-mismatch for the user's session.

Type
26

Vendor ID
8164

VSA Type
1030

Length
4

Value
Unsigned integer

SNA-RPRAK-Rcvd-Msg-Auth-Fail

This attribute contains the total number of message auth failures for A11 registration ACK messages for the user's session.

Type
26

Vendor ID
8164

VSA Type
1029

Length
4

Value
Unsigned integer

SNA-RPRAK-Rcvd-Total

This attribute contains the total number of A11 registration ACK received for the user's session.

Type
26

Vendor ID
8164

VSA Type
1027

Length
4

Value
Unsigned integer

SNA-RP-Reg-Reply-Sent-Acc-Dereg

This attribute contains the number of Accept A11 registration reply sent for the user's session.

Type
26

Vendor ID
8164

VSA Type
1033

Length
4

Value
Unsigned integer

SNA-RP-Reg-Reply-Sent-Acc-Reg

This attribute contains the number of Accept A11 registration reply sent for the user's session.

Type
26

Vendor ID
8164

VSA Type
1032

Length
4

Value
Unsigned integer

SNA-RP-Reg-Reply-Sent-Bad-Req

This attribute contains the number of A11 registration reply sent for bad requests for the user's session.

Type
26

Vendor ID
8164

VSA Type
1034

Length
4

Value
Unsigned integer

SNA-RP-Reg-Reply-Sent-Denied

This attribute contains the number of denied A11 registration reply sent for the user's session.

Type
26

Vendor ID
8164

VSA Type
1035

Length
4

Value
Unsigned integer

SNA-RP-Reg-Reply-Sent-Mis-ID

This attribute contains the number of A11 registration reply sent for mismatched ID for the user's session.

Type
26

Vendor ID
8164

VSA Type
1036

Length
4

Value
Unsigned integer

SNA-RP-Reg-Reply-Sent-Send-Err

This attribute contains the number of A11 registration reply sent with send errors for the user's session.

Type
26

Vendor ID
8164

VSA Type
1037

Length
4

Value
Unsigned integer

SNA-RP-Reg-Reply-Sent-Total

This attribute contains the total number A11 registration reply sent for the user's session.

Type
26

Vendor ID
8164

VSA Type
1031

Length
4

Value
Unsigned integer

SNA-RP-Reg-Upd-Re-Sent

This attribute contains the total number of A11 registration update re-sent for the user's session.

Type
26

Vendor ID
8164

VSA Type
1039

Length
4

Value
Unsigned integer

SNA-RP-Reg-Upd-Send-Err

This attribute contains the total number of A11 registration update send errors for the user's session.

Type
26

Vendor ID
8164

VSA Type
1040

Length
4

Value
Unsigned integer

SNA-RP-Reg-Upd-Sent

This attribute contains the total number of A11 registration update sent for the user's session.

Type
26

Vendor ID
8164

VSA Type
1038

Length
4

Value
Unsigned integer

SNA-RPRRQ-Rcvd-Acc-Dereg

This attribute contains the number of A11 De-registration Requests accepted for the user's session.

Type
26

Vendor ID
8164

VSA Type
1021

Length
4

Value
Unsigned integer

SNA-RPRRQ-Rcvd-Acc-Reg

This attribute contains the number of A11 Registration Requests accepted for the user's session.

Type
26

Vendor ID
8164

VSA Type
1020

Length
4

Value
Unsigned integer

SNA-RPRRQ-Rcvd-Badly-Formed

This attribute contains the number of badly formed A11 registration requests received for the user's session.

Type
26

Vendor ID
8164

VSA Type
1024

Length
4

Value
Unsigned integer

SNA-RPRRQ-Rcvd-Mis-ID

This attribute contains the number of A11 registration requests received with ID-mismatch for the user's session.

Type
26

Vendor ID
8164

VSA Type
1023

Length
4

Value
Unsigned integer

SNA-RPRRQ-Rcvd-Msg-Auth-Fail

This attribute contains the number of message authentication failures for A11 registration requests for the user's session.

Type
26

Vendor ID
8164

VSA Type
1022

Length
4

Value
Unsigned integer

SNA-RPRRQ-Rcvd-T-Bit-Not-Set

This attribute contains the number of A11 registration requests received with T-Bit not set for the user's session.

Type
26

Vendor ID
8164

VSA Type
1026

Length
4

Value
Unsigned integer

SNA-RPRRQ-Rcvd-Total

This attribute contains the number of A11 Registration Requests received for the user's session.

Type
26

Vendor ID
8164

VSA Type
1019

Length
4

Value
Unsigned integer

SNA-RPRRQ-Rcvd-VID-Unsupported

This attribute contains the number of A11 registration requests received with an unsupported Vendor ID for the user's session.

Type
26

Vendor ID
8164

VSA Type
1025

Length
4

Value
Unsigned integer

SNA1-PPP-Unfr-data-In-Gig

This attribute contains the total number of PPP gigawords without framing sent for the subscriber's session. When combined with the attribute SNA-PPP-Unfr-data-In-Oct, a 64-bit value can be formed which is the total number of PPP octets without framing send for the subscriber's session.

Type
26

Vendor ID
8164

VSA Type
202

Length
4

Value
Unsigned integer

SNA1-PPP-Unfr-data-Out-Gig

This attribute contains the total number of PPP octets without framing received for the user's session. When combined with the attribute SNA-PPP-Unfr-data-In-Oct, a 64-bit value can be formed which is the total number of PPP octets without framing received for the subscriber's session.

Type
26

Vendor ID
8164

VSA Type
203

Length
4

Value
Unsigned integer

SNA1-PPP-Unfr-data-In-Oct

This attribute contains the total number of PPP octets without framing sent for the user’s session.

Type
26

Vendor ID
8164

VSA Type
200

Length

4

Value

Unsigned integer

SNA1-PPP-Unfr-data-Out-Oct

This attribute contains the total number of PPP octets without framing received for the user's session.

Type

26

Vendor ID

8164

VSA Type

201

Length

4

Value

Unsigned integer

Terminal-Capability

Opaque one byte value received from customer RADIUS server in access request. We need to retain this value and return it back in all future accounting messages. Used in custom dictionary.

Type

136

Vendor ID

5535 (Reusing the 3GPP2 VID in a non-standard way.)

VSA Type

219

Length

1

Value

The system does not interpret this value, but it is copied in accounting messages.

Termination-Action

Indicates what action the NAS should take when the service is completed. AAAmgr passes this attribute to Sessmgr only for ASN-GW calls. The combination of **Session-Timeout** and **Termination-Action** attributes received in Access-Accept or Access-Challenge determines how NAS should interpret it.

Type

29

Vendor ID

N/A

VSA Type
N/A

Length
6

Value
Enumerated integer. Supported values are:

- Default = 0 — Indicates that the session should terminate.
- RADIUS-Request = 1 — Indicates that re-authentication should occur on expiration of the Session-Time. Upon termination of the specified service the NAS may send a new Access-Request to the RADIUS server, including the State attribute if any.

Tunnel-Assignment-ID

This attribute indicates the tunnel to which the session is to be assigned.

Type
82

Vendor ID
N/A

VSA Type
N/A

Length
1–247

Value
ASCII string. It can be tagged.

Tunnel-Client-Auth-ID

This attribute contains the name of the client for the purposes of tunnel authentication.

Type
90

Vendor ID
N/A

VSA Type
N/A

Length
1–247

Value
ASCII string. It can be tagged.

Tunnel-Client-Endpoint

This attribute is an identifier of the Tunnel client. When Tunnel-Medium-Type = IPv4, then this attribute is in the form of an IP address string in “dotted-decimal” notation.

Type

66

Vendor ID

N/A

VSA Type

N/A

Length

1–250

Value

Opaque value. It can be tagged.

Tunnel-Medium-Type

This attribute indicates the protocol medium over which the tunneling protocol runs. It is used to describe the format of the attributes **Tunnel-Client-Endpoint** and **Tunnel-Server-Endpoint**.

Type

65

Vendor ID

N/A

VSA Type

N/A

Length

4

Value

Enumerated integer. It can be tagged. Supported values are:

- IPv4 = 1
- IPv6 = 2
- NSAP = 3
- HDLC = 4
- BBN-1822 = 5
- IEEE-802 = 6
- E-163 = 7
- E-164 = 8
- F-69 = 9
- X-121 = 10
- IPX = 11

- Appletalk = 12
- Decnet-IV = 13
- Banyan-Vines = 14
- E-164-NSAP-Subaddress = 15

Tunnel-Password

This attribute contains a shared secret for the Tunnel connection. It is salt-encrypted.

Type
69

Vendor ID
N/A

VSA Type
N/A

Length
1–240

Value
Opaque value

Tunnel-Preference

This attribute indicates the priority given to the tunnel group. The tunnel group is defined as those tunnel attributes that have the same tag.

Type
82

Vendor ID
N/A

VSA Type
N/A

Length
4

Value
Unsigned integer

Tunnel-Private-Group-ID

This attribute contains the context of the tunnel.

Type
81

Vendor ID
N/A

VSA Type
N/A

Length
1–252

Value
ASCII string. It can be tagged.

Tunnel-Server-Auth-ID

This attribute contains the name of the server for the purposes of tunnel authentication.

Type
91

Vendor ID
N/A

VSA Type
N/A

Length
1–252

Value
Opaque value

Tunnel-Server-Endpoint

This attribute is an identifier of the Tunnel server. When Tunnel-Medium-Type = IPv4, then this attribute is in the form of an IP address string in “dotted-decimal” notation.

Type
67

Vendor ID
N/A

VSA Type
N/A

Length
1–250

Value
A string identifying the Tunnel server. It can be tagged.

Important: This attribute is used in conjunction with L2TP functionality. Refer to the RFC 2868 Tunneling Attributes section for additional information on this and other attributes added in support of this functionality.

Tunnel-Type

This attribute indicates the type of tunnel used by the subscriber.

Type

64

Vendor ID

N/A

VSA Type

N/A

Length

4

Value

Enumerated integer. It can be tagged. Supported values are:

- PPTP = 1
- L2F = 2
- L2TP = 3
- ATMP = 4
- VTP = 5
- AH = 6
- IP-IP = 7
- MIN-IP-IP = 8
- ESP = 9
- GRE = 10
- DVS = 11
- MIP = 12
- VLAN = 13

User-Name

This attribute indicates the name of the user to be authenticated. This field can contain a stand-alone user name, or a user name and domain name. The format of this field is variable and configurable on a per-context basis. Separation of user and domain names is delineated by a special character, which can be %, -, @, \, #, and /. The user name may appear before the domain name or after. If this attribute is included in the Access-Accept, then the value of that attribute will be the value of the **User-Name** attribute in subsequent Accounting-Request messages for that particular session.

This attribute is also accepted in CoA request and response messages to be used in a currently active subscriber session.

Type

1

Vendor ID

N/A

VSA Type
N/A

Length
1–253

Value
String

User-Password

This attribute contains the encrypted password of the user, when simple password authentication is being used.

Type
2

Vendor ID
N/A

VSA Type
N/A

Length
1–128

Value
String

White-List

This attribute contains the list of IMSIs which are allowed to access through an HNB.

This attribute is also accepted in CoA request message to be used in a currently active subscriber session.

Type
26

Vendor ID
9

VSA Type
117

Length
3–251

Value
Opaque value

WiMAX-Acct-Input-Packets-Giga

Number of packets incremented each time Acct-Input-Packets(47) overflows.

Type
26

Vendor ID
24757

VSA Type
48

Length
4

Value
Unsigned integer

WiMAX-Acct-Output-Packets-Giga

Number of packets incremented each time Acct-Output-Packets(48) overflows.

Type
26

Vendor ID
24757

VSA Type
49

Length
4

Value
Unsigned integer

WiMAX-Active-Time

The period of time the session was NOT in idle state.

Type
26

Vendor ID
24757

VSA Type
39

Length
4

Value
Unsigned integer

WiMAX-Beginning-Of-Session

This attribute indicates whether the session is new or a continuation of previous flow.

Type

26

Vendor ID
24757

VSA Type
22

Length
4

Value
Enumerated integer. Supported values are:

- False = 0
- True = 1

WiMAX-BS-ID

Uniquely identifies an NAP and a Base Station within that NAP. The first three octets representing the NAP operator identifier, and the next three the Base Station ID.

Type
26

Vendor ID
24757

VSA Type
46

Length
6–12

Value
Opaque value

WiMAX-Capability

This compound attribute identifies the supported WiMAX capabilities.

Type
26

Vendor ID
24757

VSA Type
1

Length
1–246

Value
Contains the following subattributes:

WiMAX-Release

Specifies WiMAX release of the sender.

Type

1

Length

4

Value

ASCII string

Accounting-Capabilities

Describes accounting capabilities supported for the session.

Type

2

Length

1

Value

0x00 = No accounting. Only valid at the HA.

- 0x01 = IP-Session-based accounting. Default value for the ASN.
- 0x02 = Flow-based accounting

Hotlining-Capabilities

Supported hotline capabilities.

Type

3

Length

1

Value

- Not-Supported = 0x00 — Hotlining is not supported
- Hotline-Profile-Id = 0x01 — Profile-based Hot lining is supported (using Hotline-Profile-ID VSA)
- NAS-Filter = 0x02 — Rule-based Hot lining is supported using NAS-Filter-Rule
- HTTP-Redirection = 0x04 — Hot lining HTTP Redirection is supported.
- Profile-Id-based-and-HTTP-Redirection-Rule-based = 0x05
- IP-Redirection = 0x08 — Rule-based Hot lining is supported using IP-Redirection rule.

Idle-Mode-Notification-Capabilities

Describes idle mode notification capabilities.

Type

4

Length
1

Value
0x00 = Idle Mode notification is not supported or is not required.

- 0x01 = Idle Mode notification is supported or is required.

ROHC-Support

Describes ROHC capability support for the session

Type
11

Length
1

Value
Enumerated integer. Supported values are:

- Not-Supported = 0x00
- Supported = 0x01

WiMAX-Control-Octets-In

Octet counts for incoming Mobile IP, DHCP, ICMP messages for IPv4 and IPv6.

Type
26

Vendor ID
24757

VSA Type
4

Length
13

Value
Unsigned integer

WiMAX-Control-Octets-Out

Octet counts for outgoing Mobile IP, DHCP, ICMP messages for IPv4 and IPv6.

Type
26

Vendor ID
24757

VSA Type
34

Length

4

Value
Unsigned integer

WiMAX-Control-Packets-In

Packet counts for incoming Mobile IP, DHCP, ICMP messages for IPv4 and IPv6.

Type
26

Vendor ID
24757

VSA Type
4

Length
13

Value
Unsigned integer

WiMAX-Control-Packets-Out

Packet counts for outgoing Mobile IP, DHCP, ICMP messages for IPv4 and IPv6.

Type
26

Vendor ID
24757

VSA Type
33

Length
4

Value
Unsigned Integer

WiMAX-Count-Type

Indicates if the record represents compressed counts over-the-air.

Type
26

Vendor ID
24757

VSA Type
59

Length
4

Value
Enumerated integer. Supported values are:

- Uncompressed = 0
- Compressed = 1

WiMAX-Device-Auth-Indicator

Indicates whether NAS performed device authentication successfully or not.

Type
26

Vendor ID
24757

VSA Type
2

Length
1

Value
Unsigned octet

WiMAX-Flow-Description

Describes a flow classifier.

Type
26

Vendor ID
24757

VSA Type
50

Length
1–240

Value
String

WiMAX GMT-Time-Zone-Offset

The current offset in seconds of the local time at the NAS with respect to GMT time.

Type
26

Vendor ID

24757

VSA Type
3

Length
4

Value
Unsigned integer

WiMAX-Home-HNP-PMIP6

The IPv6 Home Network Prefix assigned by the AAA in HCSN to the MS for PMIP6 mobility session.

Type
26

Vendor ID
24757

VSA Type
133

Length
2–18

Value
Opaque value

WiMAX-Home-IPv4-HoA-PMIP6

The IPv4 Home Address assigned by the CSN to the MS for PMIP6-IPv4 mobility session.

Type
26

Vendor ID
24757

VSA Type
135

Length
4

Value
IPv4 Address

WiMAX-Idle-Mode-Transition

A flag indicating whether the mobile node is in idle mode or not. When the mobile node enters or exits idle mode, an interim accounting message that includes WiMAX-Idle-Mode-Transition(26/44) attribute is generated instantly. The value of this attribute is 1 when mobile enters idle mode, and 0 when mobile exits idle mode. If accounting mode is flow based, then the asynchronous interim message is generated only for an ISF and not for all the flows in the session. Regular interim accountin g

if enabled, is not affected by idle mode entry. Also, the regular interim messages will not include WiMAX-Idle-Mode-Transition attribute.

Type
26

Vendor ID
24757

VSA Type
44

Length
1

Value
Enumerated integer. Supported values are:

- In idle mode = 0x01
- Not in idle mode = 0x00

WiMAX-IP-Technology

Indicates the type of WiMAX session being used.

Type
26

Vendor ID
24757

VSA Type
23

Length
4

Value
Enumerated integer. Supported values are:

- SIP = 1
- PMIP4 = 2
- CMIP4 = 3
- CMIP6 = 4
- Ethernet-CS = 5
- PMIP6 = 6

WiMAX-NAP-ID

Uniquely identifies the Network Access Provider.

Type
26

Vendor ID
24757

VSA Type
45

Length
3

Value
String

WiMAX-NSP-ID

Uniquely identifies the Network Service Provider.

Type
26

Vendor ID
24757

VSA Type
57

Length
3

Value
Opaque value

WiMAX-Packet-Flow-Descriptor

This compound attribute describes a packet flow. A packet flow may describe uni-directional flow and bi-directional flow. The packet flow descriptor may be pre-provisioned. A packet flow descriptor references one or two QoS specifications.

Type
26

Vendor ID
24757

VSA Type
28

Length
4–1400

Value
Contains the following subattributes:

PDF-ID

Used to match all records from the same Packet Data Flow.

Type

1

Length

2

Value

Unsigned integer

SDF-ID

Used to match all PDFs from the same Service Data Flow.

Type

2

Length

2

Value

Unsigned integer

Service-Profile-ID

Identifies a pre configured Flow Descriptor at the NAS.

Type

3

Length

4

Value

Unsigned integer

Direction

Direction of the PDF.

Type

4

Length

1

Value

Enumerated integer. Supported values are:

- Uplink = 1
- Downlink = 2
- Bi-Directional = 3

Activation-Trigger

Specifies the trigger to be used for the activation of Service Flow.

Type

5

Length

1

Value

Enumerated integer. Supported values are:

- Provisioned = 0x01
- Admit = 0x02
- Provisioned-Admit = 0x03
- Activate = 0x04
- Provisioned-Activate = 0x05
- Admit-Activate = 0x06
- Provisioned-Admit-Activate = 0x07
- Dynamic = 0x08
- Dynamic-Admit = 0x0a
- Dynamic-Activate = 0x0c
- Dynamic-Admit-Activate = 0x0e

Transport-Type

Type of transport (IP, Ethernet).

Type

6

Length

1

Value

Enumerated integer

Uplink-QoS-ID

Identifier of the QoS Descriptor for Uplink or Bidirection.

Type

7

Length

1

Value

Unsigned integer

Downlink-QoS-ID

Identifier of the QoS Descriptor for Downlink.

Type

8

Length
1

Value
Unsigned integer

Uplink-Classifier

Classifier to match for traffic flowing in Uplink Direction.

Type
9

Length
1–240

Value
String

Downlink-Classifier

Classifier to match for traffic flowing in Downlink Direction.

Type
10

Length
1–240

Value
String

WiMAX-Packet-Flow-Descriptor-V2

Describes a Unidirectional or Bidirectional Packet Flow Descriptor Version 2.

This attribute is also accepted in CoA request message to be used in a currently active subscriber session.

Type
26

Vendor ID
24757

VSA Type
84

Length
4–1400

Value
Contains the following subattributes:

PDF-ID

Used to match all records from the same Packet Data Flow.

Type
1

Length
2

Value
Unsigned integer

SDF-ID

Used to match all PDFs from the same Service Data Flow.

Type
2

Length
2

Value
Unsigned integer

Service-Profile-ID

Identifies a pre-configured Flow Descriptor at the NAS.

Type
3

Length
4

Value
Unsigned integer

Direction

Direction of the PDF.

Type
4

Length
1

Value
Enumerated integer. Supported values are:

- Uplink = 1
- Downlink = 2
- Bi-Directional = 3

Activation-Trigger

Specifies the trigger to be used for the activation of Service Flow.

Type

5

Length

1

Value

Enumerated integer. Supported values are:

- Provisioned = 0x01
- Admit = 0x02
- Activate = 0x04
- Dynamic = 0x08

Transport-Type

Type of transport (IP, Ethernet).

Type

6

Length

1

Value

Enumerated integer. Supported values are:

- IPv4-CS = 1
- IPv6-CS = 2
- Ethernet = 3

Uplink-QoS-ID

Identifier of the QoS Descriptor for Uplink or Bidirection.

Type

7

Length

1

Value

Unsigned integer

Downlink-QoS-ID

Identifier of the QoS Descriptor for Downlink.

Type

8

Length

1

Value

Unsigned integer

WiMAX-Packet-Flow-Classifier

Describes Packet Flow Classifiers.

Type

9

Value

Contains the following subattributes:

Classifier-ID

WiMAX Classifier ID.

Type

1

Length

1

Value

Unsigned integer

Priority

WiMAX Classifier Priority.

Type

2

Length

1

Value

Unsigned integer

Protocol

WiMAX Classifier Protocol, i.e TCP/UDP.

Type

3

Length

1

Value

In StarOS 10.0 and earlier: Enumerated integer. Supported values are:

- ICMP = 1
- TCP = 6
- UDP = 17

In StarOS 10.2 and later: Unsigned integer.

Direction

Direction of the PDF.

Type

4

Length

1

Value

Enumerated integer. Supported values are:

- Uplink = 1
- Downlink = 2
- Bi-Directional = 3

Source-Specification

Identifies WiMAX classifier rule params for source specification.

Type

5

Value

Contains the following subattributes:

IP-Address

This attribute contains source/destination address.

Type

1

Length

4

Value

IPv4 address

IP-Address-Range

WiMAX Packet Classifier IP Address Range.

Type

2

Length

1

Value

Opaque value

IP-Address-Mask

WiMAX Packet Classifier IP Address Mask.

Type

3

Length

5

Value

Opaque value

Port

WiMAX Packet Classifier Port.

Type

4

Length

2

Value

Unsigned integer

Port-Range

WiMAX Packet Classifier Port Range.

Type

5

Length

4

Value

Unsigned integer

Inverted

WiMAX Classifier Inverted.

Type

6

Length

1

Value

Enumerated integer. Supported values are:

- FALSE = 0
- TRUE = 1

Assigned

WiMAX Classifier Assigned.

Type

7

Length

1

Value

Enumerated integer. Supported values are:

- Src_Assigned = 1

- Dest_Assigned = 2
- Src_Dest_Assigned = 3

Destination-Specification

Identifies WiMAX classifier rule params for destination specification.

Type

6

Value

Contains the following subattributes:

IP-Address

This attribute contains source/destination address.

Type

1

Length

4

Value

IPv4 address

IP-Address-Range

WiMAX Packet Classifier IP Address Range.

Type

2

Length

8

Value

Opaque value

IP-Address-Mask

WiMAX Packet Classifier IP Address Mask.

Type

3

Length

5

Value

Opaque value

Port

WiMAX Packet Classifier Port.

Type

4

Length

2

Value

Unsigned integer

Port-Range

WiMAX Packet Classifier Port Range.

Type

5

Length

4

Value

Unsigned integer

Inverted

WiMAX Classifier Inverted.

Type

6

Length

1

Value

Enumerated integer. Supported values are:

- FALSE = 0
- TRUE = 1

Assigned

WiMAX Classifier Assigned.

Type

7

Length

1

Value

Enumerated integer. Supported values are:

- Src_Assigned = 1
- Dest_Assigned = 2
- Src_Dest_Assigned = 3

IP-TOS-DSCP-Range-And-Mask

WiMAX Classifier WiMAX-IP-TOS-DSCP-Range-And-Mask.

Type
7

Length
1–3

Value
Opaque value

Action

WiMAX Classifier Action.

Type
8

Length
1

Value
Enumerated integer. Supported values are:

- Reserved = 0
- Permit = 1
- Deny = 2

Paging-Preference

WiMAX Paging Preference.

Type
10

Length
1

Value
Enumerated integer. Supported values are:

- FALSE = 0
- TRUE = 1

WiMAX-PDF-ID

The value of this attribute matches all records from the same packet data flow. PDFID is assigned by the CSN and remains constant through all handover scenarios.

Type
26

Vendor ID
24757

VSA Type
26

Length

2

Value

Unsigned integer

WiMAX-PPAC

The Prepaid-Accounting-Capability (PPAC) attribute is sent in the Access-Request message by a prepaid capable ASNGW, and is used to describe the prepaid capabilities of the ASNGW. The absence of this attribute indicates that the client is not capable of prepaid accounting and the session should not use prepaid accounting.

Type

26

Vendor ID

24757

VSA Type

35

Value

Contains the following subattribute:

Available-In-Client

The optional Available-In-Client subtype, generated by the PPC, indicates the metering capabilities of the NAS and is be bitmap encoded.

Type

1

Length

4

Value

Enumerated integer. Supported values are:

- Supported_None = 0
- Supported_Volume = 1
- Supported_Duration = 2
- Supported_Volume_And_Duration = 3

WiMAX-PPAQ

Prepaid Quota, used for charging, report usage, and request quota. This attribute specifies the characteristics for pre-paid accounting of the volume and/or duration of a packet data session. It should 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. In Authorize-Only Access-Request messages, it is used for one-time charging, report usage and the request for further quota. In an Access-Accept message it is used in order to allocate the (initial and subsequent) quotas.

This attribute is also accepted in CoA request message to be used in a currently active subscriber session.

Type

26

Vendor ID

24757

VSA Type

37

Value

Contains the following subattributes:

Quota-Identifier

Is generated by the PPS together with the allocation of new quota.

This attribute is also accepted in CoA request message to be used in a currently active subscriber session.

Type

1

Length

1-4

Value

Opaque value

Volume-Quota

Indicates the volume in octets excluding control data.

This attribute is also accepted in CoA request message to be used in a currently active subscriber session.

Type

2

Length

4-12

Value

Opaque value

Volume-Threshold

Is generated by the PPS and indicates the volume (in octets) that be consumed before a new quota should be requested.

This attribute is also accepted in CoA request message to be used in a currently active subscriber session.

Type

3

Length

4-12

Value

Opaque value

Duration-Quota

3GPP2 PrePaid Duration Quota. This is optionally present if duration-based charging is used. In RADIUS Access-Accept message, it indicates the duration (in seconds) allocated for the session by the PPS. In an on-line RADIUS Access-Accept message, it indicates the total duration (in seconds) since the start of the accounting session related to the QuotaID of the PPAQ in which it occurs.

This attribute is also accepted in CoA request message to be used in a currently active subscriber session.

Type

4

Length

4

Value

Unsigned integer

Duration-Threshold

3GPP2 PrePaid Duration Quota Threshold. This is optionally present if Duration-Quota is present in a RADIUS Access-Accept message. It is generated by the PPS and indicates the duration (in seconds) that should be consumed before a new quota should be requested. This threshold should not be larger than the Duration-Quota.

This attribute is also accepted in CoA request message to be used in a currently active subscriber session.

Type

5

Length

4

Value

Unsigned integer

Update-Reason

Reason for initiating online quota update operation. This should be present in the Authorize-Only RADIUS Access-Request message. It indicates the reason for initiating the on-line quota update operation. Update reasons 6, 7, 8, and 9 indicate that the associated resources are released at the client side, and that therefore the PPS should not allocate a new quota in the RADIUS Access Accept message.

Type

8

Length

1

Value

Enumerated integer. Supported values are:

- Pre-Initialization = 1
- Initial-Request = 2
- Threshold-Reached = 3

- Quota-Reached = 4
- TITSU-Approaching = 5
- Remote-Forced-Disconnect = 6
- Client-Service-Termination = 7
- Access-Service-Terminated = 8
- Service-Not-Established = 9
- One-Time-Charging = 10

Pre-Paid-Server

PrePaid server IP address. This optional subtype indicates the address IPv4 of the serving PPS. If present, the Home RADIUS server uses this address to route the message to the serving PPS. The attribute may be sent by the Home RADIUS server. Multiple instances of this subtype may be present in a single PPAQ. If present in the incoming RADIUS Access-Accept message, the ASNGW should send this attribute back without modifying it in the subsequent RADIUS Access-Request message.

This attribute is also accepted in CoA request message to be used in a currently active subscriber session.

Type

9

Length

4

Value

IPv4 address

Service-ID

This value is a string that uniquely describes the service instance to which prepaid metering should be applied.

Type

10

Length

1-246

Value

Opaque value

Rating-Group-ID

Rating-Group-ID for which the WiMAX PPAQ is allocated or reported.

Type

11

Length

4

Value

Unsigned integer

Termination-Action

Describes action to take when PPS does not grant additional quota.

This attribute is also accepted in CoA request message to be used in a currently active subscriber session.

Type

12

Length

4

Value

Enumerated integer. Supported values are:

- Reserved = 0
- Terminate = 1
- Request-more-quota = 2
- Redirect/Filter = 3

WiMAX-Prepaid-Indicator

Indicates that this session was associated with a prepaid user (online accounting).

Type

26

Vendor ID

24757

VSA Type

25

Length

1

Value

Enumerated integer. Supported values are:

- Offline = 0
- Online = 1

WiMAX-Prepaid-Tariff-Switch

Attribute to indicate Tariff-Switch-Interval / Time-Interval-After-Tariff-Switch-Update by the PPS and Volume-Used-After-Tariff-Switch by the PPC.

Type

26

Vendor ID

24757

VSA Type

38

Value

Contains the following subattributes:

Quota-Identifier

It is generated by the PPS together with the allocation of new quota.

Type

1

Length

1-4

Value

Opaque value

Volume-Used-After-Tariff-Switch

Volume Quota used after Tariff Switch Happened

Type

2

Length

4

Value

Unsigned integer

Tariff-Switch-Interval

Tariff Switch Interval in seconds

Type

3

Length

4

Value

Unsigned integer

Time-Interval-After-Tariff-Switch-Update

Duration after TSI where an on-line RADIUS Access-Request is sent by PrePaid client to report VUATS before the next TS condition is triggered

Type

4

Length

4

Value

Unsigned integer

WiMAX-QoS-Descriptor

This attribute describes over the air QoS parameter that are associated with a flow. The QoS-Descriptor is only valid for the actual RADIUS transaction.

This attribute is also accepted in CoA request message to be used in a currently active subscriber session.

Type
26

Vendor ID
24757

VSA Type
29

Length
6–700

Value
Contains the following 17 subattributes:

QoS-ID

Unique ID for the QoS specification in the packet

Type
1

Length
1

Value
Unsigned integer

Global-Service-Class-Name

Represents Global Service Class Name as defined in IEEE802.16e

Type
2

Length
6

Value
String

Service-Class-Name

Represents Service Class Name as defined in IEEE802.16e

Type
3

Length
2–127

Value
String

Schedule-Type

Specifies Uplink granted scheduling type.

Type
4

Length
1

Value
Enumerated integer. Supported values are:

- Best-Effort = 2
- nrtPS = 3
- rtPS = 4
- Extended-rtPS = 5
- UGS = 6

Traffic-Priority

Specifies the priority assigned to a Service Flow.

Type
5

Length
1

Value
Unsigned integer

Maximum-Sustained-Traffic-Rate

Defines Peak Information Rate of the service in bits/second.

Type
6

Length
4

Value
Unsigned integer

Minimum-Reserved-Traffic-Rate

Defines Minimum Rate reserved for the Service Flow in bits/second.

Type
7

Length
4

Value
Unsigned integer

Maximum-Traffic-Burst

Defines Maximum Burst Size accommodated for the Service in bytes/second

Type
8

Length
4

Value
Unsigned integer

Tolerated-Jitter

Represents Maximum Delay Variation in milliseconds.

Type
9

Length
4

Value
Unsigned integer

Maximum-Latency

Represents Maximum Latency in milliseconds.

Type
10

Length
4

Value
Unsigned integer

Reduced-Resources-Code

Indicates that requesting entity will accept reduced resources if requested resources are unavailable.

Type
11

Length
1

Value
Unsigned integer

Media-Flow-Type

Describes the application type, used as a hint in admission decisions.

Type

12

Length

1

Value

Enumerated integer. Supported values are:

- VoIP = 1
- Robust-Browser = 2
- Secure-Browser/VPN = 3
- Streaming-Video-On-Demand = 4
- Streaming-Live-TV = 5
- Music-Photo-Download = 6
- Multi-Player-Gaming = 7
- Location-Based-Services = 8
- Text-Audio-Books-With-Graphics = 9
- Video-Conversation = 10
- Message = 11
- Control = 12
- Data = 13

Unsolicited-Grant-Interval

Specifies nominal interval between successive data grant opportunities for the Service Flow, in milliseconds.

Type

13

Length

2

Value

Unsigned integer

SDU-Size

Represents the number of bytes in the fixed size SDU.

Type

14

Length

1

Value

Unsigned integer

Unsolicited-Polling-Interval

Specifies maximal nominal interval between successive polling grant opportunities for the Service Flow.

Type

15

Length

2

Value

Unsigned integer

Transmission-Policy

Include options for PDU formation, and for uplink service flows, restrictions on the types of bandwidth request options that may be use.

Type

17

Length

In StarOS 9.0 and earlier releases: 4

In StarOS 10.0 and later releases: 1

Value

In StarOS 10.0 and earlier releases: Enumerated integer. Supported values are:

- no-bcast = 0x01
- no-mcast = 0x02
- no-piggy-back = 0x04
- no-fragment = 0x08
- no-sup-payload-header = 0x10
- no-multiple-sdu = 0x20
- no-crc = 0x40
- no-rohc-compression = 0x80

In StarOS 10.2 and later releases: Unsigned integer.

DSCP

DSCP

Type

18

Length

4

Value

Enumerated integer. Supported values are:

- Best-Effort=0
- AF11=10
- AF12=12
- AF13=14
- AF21=18
- AF22=20
- AF23=22
- AF31=26
- AF32=28
- AF33=30
- AF41=34
- AF42=36
- AF43=38
- EF=46

WiMAX-RRQ-HA-IP

IPv4 or IPv6 address of the HA as contained in the MIP Registration Request or the BU.

Type
26

Vendor ID
24757

VSA Type
18

Length
4-16

Value
Opaque value

WiMAX-SDF-ID

The value of this attribute matches all records from the same packet data flow. SDFID is assigned by the CSN and remains constant through all handover scenarios.

Type
26

Vendor ID
24757

VSA Type
27

Length

2

Value

Unsigned integer

WiMAX-Session-Continue

The value of this attribute matches all records from the same packet data flow. SDFID is assigned by the CSN and remains constant through all handover scenarios.

Type

26

Vendor ID

24757

VSA Type

21

Length

4

Value

Enumerated integer. Supported values are:

- False = 0
- True = 1

WiMAX-Session-Term-Capability

WiMAX session term capability. This attribute is included in a RADIUS Access-Request message to the RADIUS server and indicates whether or not the NAS supports Dynamic Authorization.

Type

26

Vendor ID

24757

VSA Type

36

Length

4

Value

Enumerated integer. Supported values are:

- Only_Dynamic_Auth_Extn_to_Radius = 0x00000001
- Only_Reg_Revocation_in_MIP = 0x00000002
- Both_Dynamic_Auth_And_Reg_Revocation_in_MIP = 0x00000003

Win-Call-Id

Customer-specific attribute used in custom dictionary. Contains opaque 1 byte value received from customer RADIUS server in access request.

Type
136

Vendor ID
5535 (Reusing the 3GPP2 VID in a non-standard way.)

VSA Type
205

Length
1

Value
The system does not interpret this value, but it is copied in accounting messages.

Win-Service-Name

Opaque value value received from customer RADIUS server in access request. We need to retain this value and return it back in all future accounting messages. Used in custom dictionary.

Type
136

Vendor ID
5535 (Reusing the 3GPP2 VID in a non-standard way.)

VSA Type
206

Length
1 – 256

Value
The system does not interpret this value, but it is copied in accounting messages.

WSType

Opaque one byte value received from customer RADIUS server in access request. We need to retain this value and return it back in all future accounting messages.

Type
136

Vendor ID
5535 (Reusing the 3GPP2 VID in a non-standard way.)

VSA Type
197

Length
1

Value

The system does not interpret this value, but it is copied in accounting messages.

Attribute Notes

This section contains notes that apply to groups of attributes that have been included in support of specific features and/or functionality.

RFC 2868 Tunneling Attributes

Tunnel attributes may be tagged, which means the leading byte in the value field may be used to group attributes together. This is used to return a number of different tunnel configurations that are available to the subscriber. The tagged group with the highest tunnel preference (the lowest value of the Tunnel-Preference attribute) has precedence over other tunnel configurations.

Tags can be a value from 1 through 31. Any value outside of this range for the leading byte means the attribute is not tagged, and the leading byte is then interpreted as part of the attribute value. Integer attributes that are tagged are three bytes in length (the leading byte is ignored), but are four bytes in length when not tagged (the leading byte is incorporated).

If Tunnel attributes appear more than once in the RADIUS Accept-Accept but are not tagged, then the system treats the attributes as having an implicit tag. The first instance of the attribute has a tag value of 32, the second instance has a tag value of 33, etc.

Chapter 6
GTPP Accounting Overview

This chapter provides an overview of GPRS Tunneling Protocol Prime (GTPP) protocol accounting, and the following Charging Data Records (CDRs) in the Cisco ASR 5x00 Multimedia Core Platform:

- Gateway GPRS Support Node (GGSN) CDRs (G-CDRs), Enhanced GGSN CDRs (eG-CDRs)
- Packet Data Network Gateway (P-GW) CDRs (PGW-CDRs)
- Serving Gateway (S-GW) CDRs (SGW-CDRs)
- Serving GPRS Support Node (SGSN) CDRs (S-CDRs, SM-MO-CDRs, SM-MT-CDRs), Mobility CDRs (M-CDRs)
- Wireless Local Area Network CDRs (WLAN-CDRs)

GTPP Interface Overview

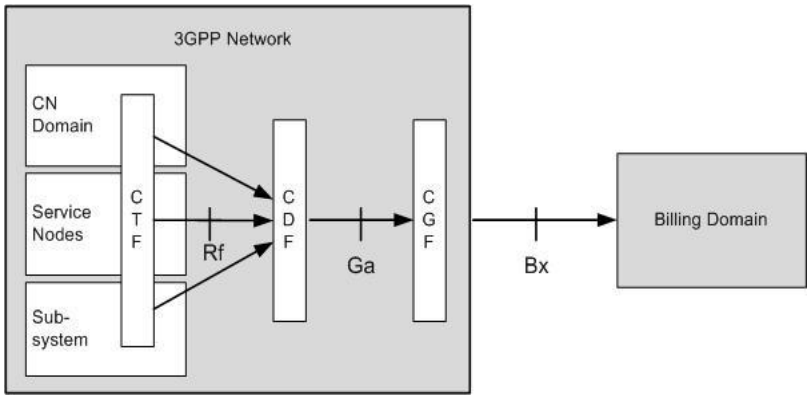
This section provides information on GTPP interface between Charging Gateway Function (CGF) and Cisco Systems' licensed products running on the ASR 5x00 core platforms, including the GGSN, P-GW, S-GW, and SGSN in General Packet Radio Service (GPRS), Universal Mobile Telecommunications System (UMTS) data networks, 3GPP2 evolved High Rate Packet Data (eHRPD) and Long Term Evolution-System Architecture Evolution (LTE-SAE) wireless data networks.

The Ga is the reference point from Charging Data Function (CDF) to the CGF, which is intended for the transport of CDRs. The CDF could either be GGSN, P-GW, S-GW, or any other similar products.

By definition, dealing with CDRs only implies that Ga is solely related to offline charging.

The following figure depicts the position of the Ga reference point within the overall 3GPP offline charging architecture.

Figure 4. 3GPP Offline Charging Architecture



As illustrated in the above figure, the CDF in each network domain, service or subsystem is relevant for the network side of the Ga reference point. Different mappings of the ubiquitous offline charging functions, CDF and CGF, onto physical implementations are possible.

The transport protocol associated to the Ga reference point, providing functions for transfer of CDRs from CDF to CGF, is GTPP.

Each CDF will have an O&M configurable address list of CGFs (Charging Gateways) to which it can send its CDRs. The list will be organized in CGF address priority order. If the primary CGF is not available (for example, out of service), then the CDF will send the CDRs to the secondary CGF and so on.

Each CDR generating function will only send the records to the CGF(s) of the same PLMN, not to CGF(s) located in other PLMNs.

Each CGF in the PLMN will know the other CGFs' network addresses (for example, for redundancy reasons, to be able to recommend another CGF address). This is achieved by O&M configuration facilities that will enable each CGF to have a configurable list of peer CGF addresses.

The GTPP charging support is currently available for the following core multimedia gateway products:

- Gateway GPRS Support Node (GGSN)
- IP Services Gateway (IPSG)

- Packet Data Gateway/Tunnel Termination Gateway (PDG/TTG)
- Packet Data Network (PDN) Gateway (P-GW)
- Serving Gateway (S-GW)
- Serving GPRS Support Node (SGSN)

CDR Transport by GTPP

GTPP has been designed to deliver the CDR(s) from the CDF to the CGF(s). This protocol is required if the CGF resides outside the CDFs. It utilizes some aspects of GTPP, which is used for packet data tunneling in the backbone network.

GTPP operates on the Ga interface and does not imply the use of any specific backbone network.

GTPP performs the following functions:

- CDR transfer between the CDF and the CGF
- Redirection of CDRs to another CGF
- Advertise to peers about its CDR transfer capability (for example, after a period of service downtime)
- Prevents duplicate CDRs that might arise during redundancy operations. If so configured, the CDR duplication prevention function may also be carried out by marking potentially duplicated CDR packets, and, delegating the final duplicate deletion task to a CGF or the Billing Domain (instead of handling the possible duplicates solely by GTPP messaging).

Path Protocol

GTPP uses path protocol to transport CDRs from CDF to CGF over the Ga interface so as to facilitate charging.

The following path protocols are supported for GTPP:

- UDP as the Path Protocol

  Ports for signaling the request messages:

  - The UDP Destination Port may be the server port number 3386 which has been reserved for GTPP. Alternatively, another port can be used as configured by O&M.
  - The UDP Source Port is a locally allocated port number at the sending network element.

  Ports for signaling the response messages:

  - The UDP Destination Port can be the value of the Source Port of the corresponding request message.
  - The UDP Source Port can be the value from the Destination Port of the corresponding request message.

- TCP as the Path Protocol

  The TCP Destination Port may be the server port number 3386, which has been reserved for G-PDUs. Alternatively, another port may be used as configured by O&M. Extra implementation-specific destination ports are possible but all CGFs shall support the server port number.

  The TCP Source Port is a random port locally assigned at the sending network element.

Important: ASR chassis supports IPV4 only as a transport layer IP.

GTPP Message Types

GTPP defines a set of messages between two associated nodes. The GTPP messages defined are shown in the following table.

Table 6. GTPP Messages

Message Type value (Decimal)	GTPP Message
1	Echo Request
2	Echo Response
3	Version Not Supported
4	**Node Alive Request**
5	**Node Alive Response**
6	**Redirection Request**
7	**Redirection Response**
240	**Data Record Transfer Request**
241	**Data Record Transfer Response**
Others	Reserved for future use

The messages introduced by GTPP are in boldface letters. The other messages are inherited from GTPP protocol.

The GTPP introduced the following signaling message types as Path Management Messages:

- Node Alive Request
- Node Alive Response
- Redirection Request
- Redirection Response

Important: Echo messages and node-alive messages are not supported if the transport layer protocol is TCP.

The following signaling messages are grouped under the category “Record Transmission Messages”:

- Data Record Transfer Request
- Data Record Transfer Response

The reserved fields in the signaling messages can be filled with ones, and are intended for future use.

GTPP reuses the GTPP Cause values. The message type numbers required for the newly introduced GTPP messages have been derived from the unallocated message type number space specified in the GTPP message table defined in TS 29.060.

The number ranges allocated for GTPP are as follows:

For Information Elements: 117-127 (TV type fields) and 239-254 (for TLV type fields).

The following table provides the information on the TLV and TV Information Element types introduced in this document:

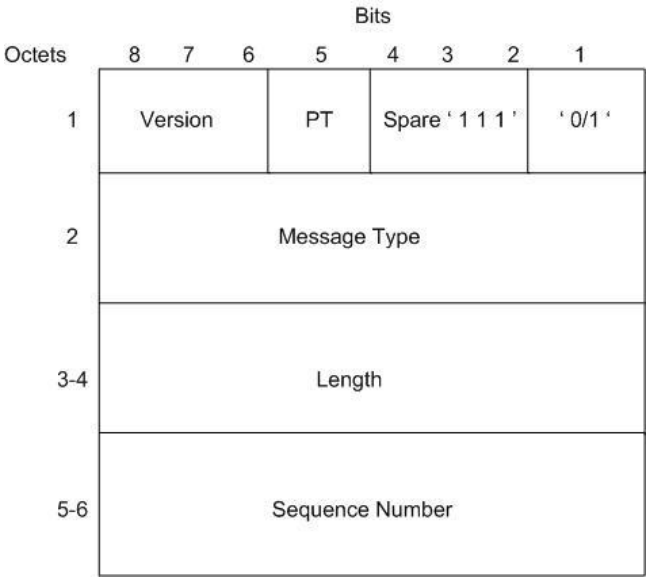
Table 7. TLV and TV Information Element Types

TLV Information Element Types	
254	Address of Recommended Node
253	Requests Responded
252	Data Record Packet
251	Charging Gateway Address (this IE is also used in TS 29.060 [200])
250	Sequence Numbers of Canceled Packets
249	Sequence Numbers of Released Packets
TV Information Element Types	
127	Charging ID
126	Packet Transfer Command

Usage of GTPP Header in Charging

In GTPP messaging only the signalling plane of GTPP is partly reused. The GTPP header is shown in the following figure.

Figure 5. GTPP Header



Bit 5 of octet 1 of the GTPP header is the Protocol Type (PT) flag: it is '0' if the message is GTPP.

The Version bits indicate the GTPP protocol version when the Protocol Type flag is '0'.

Bit 1 of octet 1 is not used in GTPP (except in v0), and it is marked '0' in the GTPP header. It is in use in GTPP v0 and distinguishes the used header-length. In the case of GTPP v0, this bit being marked one (1) indicates the usage of the 6 octets header. If the bit is set to '0' (usually the case) the 20-octet header is used. For all other versions of GTPP, this bit is not used and is set to '0'. However, this does not suggest the use of the 20-octet header, rather a shorter 6-octet header.

The Length indicates the length of payload (number of octets after the GTPP header). The Sequence Number of the packet is part of the GTPP header.

Information Elements

The messages contain several Information Elements (IEs). The TLV (Type, Length, Value) or TV (Type, Value) encoding formats will be used for the GTPP IEs. The GTPP messages have the IEs sorted with the *Type* fields in ascending order. The *Length* field contains the IE length excluding the Type and Length fields.

Within the *Type* field the most significant bit will be set to 0 when the TV format is used and set to 1 when the TLV format is used.

GTPP Messages

This section provides the detailed information on the GTPP message types.

Node Alive Request

The Node Alive Request message may be used to inform that a node in the network has started its service (e.g. after a service break due to software or hardware maintenance or data service interruption after an error condition). A node may send a different Node Address than its own in the Information Element, e.g. informing the “next node in the chain” that the “previous node in the chain” (which is located on the other side of the sender of this message) is now ready for service.

The Node Alive Request message allows a quicker reconnect capability than the Echo Request message based polling can provide, and its usage will have a reduced load effect on the network, particularly when the number of network nodes using GTPP is high. It may also be used to inform when a new network node has become available for service. If the Echo Request message is also used, then the usage of the Node Alive Request message allows the interval of Echo Requests to be longer, thus reducing network load by reducing number of Echo Requests.

Important: Node Alive request messages are not supported if the transport layer protocol is TCP.

The Information elements in a Node Alive Request message are shown in the following table:

Table 8. Node Alive Request Message

Information Element	Presence Requirement
Node Address	Mandatory
Alternative Node Address	Optional
Private Extension	Optional

The Node Address format is the same as for the Charging Gateway Address format described in TS 29.060.

The format definition for the Node Address information element is the same as the format of the source and destination address of the IP packet that transports the GTPP messages. The optional Alternative Node Address IE can be used in the Node Alive Request if the message sender wants to advertise an IP address that is different from the node address format. This way both the IPv4 and IPv6 node address formats can be supported simultaneously in the messaging, regardless of whether IPv4 or IPv6 is used in the underlying transport.

The optional Private Extension IE contains vendor- or operator-specific information.

Node Alive Response

The *Node Alive Response* message, shown in the following table, shall be sent as a response to a received *Node Alive Request*.

Table 9. Node Alive Response Message

Information Element	Presence Requirement
Private Extension	Optional

The optional Private Extension IE contains vendor- or operator-specific information.

Redirection Request

There are two use cases for the Redirection Request message:

- One is to advise that received CDR traffic is to be redirected to another CGF due to the sending CGF node is about to stop service (due to an outage for maintenance or an error condition).
- The second purpose is to inform a CDF which is currently sending data to this node (e.g. CGF), that the next node in the chain (e.g. a mediator device or Billing Computer) has lost connection to this node (e.g. CGF).

The Information Elements in a Redirection Request Message are listed in the following table. An *Address of Recommended Node* may be given if, for example, a CGF maintenance outage is handled by first introducing another CGF ready to take incoming CDRs. This way, the network performance can be maintained. The *Address of Recommended Node* shall only describe an intra-PLMN node containing a CGF, and not a node in any other PLMN.

Table 10. Redirection Request Message

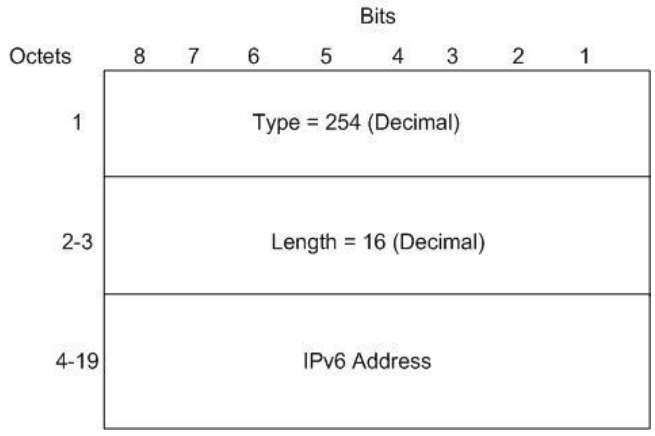
Information Element	Presence Requirement
Cause	Mandatory
Address of Recommended Node	Optional
Alternative Address of Recommended Node	Optional
Private Extension	Optional

Possible Cause values are:

- This node is about to go down
- Another node is about to go down
- System failure
- Receive buffers becoming full
- Send buffers becoming full

The Address of Recommended Node IE, shown in the following figure, defines the IPv4 or IPv6 format address that the node is identified by in the UMTS network.

Figure 6. Address of Recommended Node IE



The format definition for the Address of Recommended Node information element is the same as the format of the source and destination address of the IP packet that transports the GTPP messages. The optional Alternative Address of Recommended Node IE can be used in the Node Alive Request if the message sender wants to advertise an IP address that is different from the node address format. This way both the IPv4 and IPv6 node address formats can be supported simultaneously in the messaging, regardless of whether IPv4 or IPv6 is used in the underlying transport.

The optional Private Extension contains vendor- or operator- specific information.

Redirection Response

A Redirection Response message shall be sent as a response of a received Redirection Request.

The information elements of this message are listed in the following table.

Table 11. Redirection Response Message

Information Element	Presence Requirement
Cause	Mandatory
Private Extension	Optional

Possible Cause values are:

- Request Accepted
- No resources available
- Service not supported
- System failure
- Mandatory IE incorrect
- Mandatory IE missing
- Optional IE incorrect
- Invalid message format

- Version not supported

The optional Private Extension contains vendor- or operator-specific information.

Data Record Transfer Request

This message is used to transmit the CDR(s) to the CGF.

The CDRs are placed in the Data Record Packet information element.

Information Elements in Data Record Transfer Request

The IEs in Data Record Transfer Request message are specified in the following table.

Table 12. Data Record Transfer Request Message

Information Element	Presence Requirement
Packet Transfer Command	Mandatory
Data Record Packet	Conditional
Sequence Numbers of Released Packets	Conditional
Sequence Numbers of Canceled Packets	Conditional
Private Extension	Optional

Packet Transfer Command IE

The value of the Packet Transfer Command in its Information Element tells the nature of the message:

- 1 = 'Send Data Record Packet'
- 2 = 'Send possibly duplicated Data Record Packet'
- 3 = 'Cancel Data Record Packet'
- 4 = 'Release Data Record Packet'

The following describes the usage of each Packet Transfer Command. The first command is for normal CDR transfer while the other values are only used as part of the redundancy mechanism.The following describes the usage of each Packet Transfer Command. The first command is for normal CDR transfer while the other values are only used as part of the redundancy mechanism.

Send Data Record Packet: This is the usual command used for sending CDRs under normal conditions when no error recovery is needed or the redirection mechanism is not involved. The other three commands are being used only in error recovery cases. Out of the three conditional IEs, only the “Data Record Packet” is present in this message.

Send possibly duplicated Data Record Packet: When the CDR packet is redirected to a secondary CGF (by a CDF) because the currently used CGF is not working or the CDR transfer is not working properly, or if there is an error in the link between the CDF and the CGF, then this Packet Transfer Command is used instead of the normal 'Send Data Record Packet'. Of the conditional IEs, the “Data Record Packet” is present in the message, when sending the message to a CGF acting as temporary storage, when the original primary CGF could not be contacted. This Packet Transfer Command is used also when sending “empty” test packets with older (but not yet acknowledged) sequence numbers

after a peer node or link recovery, to check if the CGF had received some Data Record Packets (whose acknowledgement did not come to the Data Record Packet sending node) before the link to the recipient node became inoperable.

Cancel Data Record Packet: Of the conditional IEs, the “Sequence Numbers of Canceled Packets” is present in the message.

Release Data Record Packet: Of the conditional IEs, the “Sequence Numbers of Released Packets” is present in the message.

After the CGF has received the Packet Transfer Command 'Release Data Record Packet' with the Sequence Number(s) for earlier sent 'Send possibly duplicated Data Record Packet' command(s), it can consider itself authorized to send the Data Record Packets previously marked as possibly duplicated towards the BD as normal (not duplicated) CDRs.

Data Record Packet IE

The Data Record Packet element, which is present conditionally if the Packet Transfer Command is 'Send Data Record Packet' or 'Send possibly duplicated Data Record Packet', may contain one or more CDRs. If an “empty packet” is to be sent, then the Data Record Packet IE contains only the Type (with value 252 in decimal) and the Length (with value 0) fields.

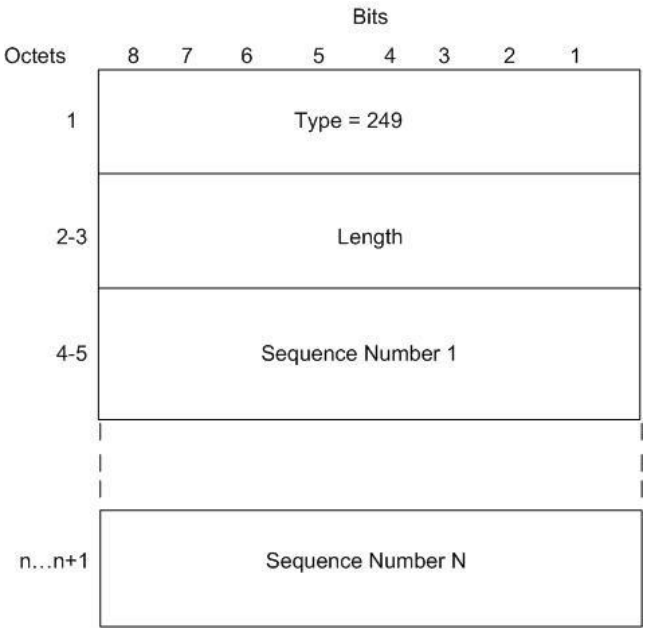
There are two fields identifying the CDR format: Data Record Format and Data Record Format Version.

The format of the CDRs is ASN.1 or some other format, as identified by the value of Data Record Format. The Data Record Format Version identifies the TS release and version numbers that were used for the CDR encoding.

Sequence Numbers of Released Packets IE

The Sequence Numbers of Released Packets is present if the Packet Transfer Command is 'Release Data Record Packet'. The format of the Information Element is described in the following figure:

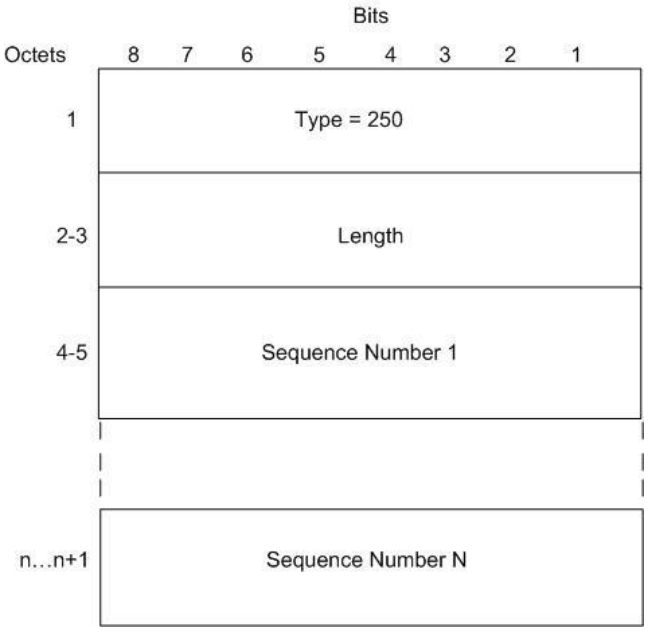
Figure 7. Sequence Numbers of Released Packets IE



Sequence Numbers of Canceled Packets IE

The following figure shows the sequence numbers of Canceled Packets IE that contains the IE Type, Length and the Sequence Number(s) (each 2 octets) of the canceled Data Record Transfer Request(s). It is present if the Packet Transfer Command is “Cancel Data Record Packet”.

Figure 8. Sequence Numbers of Canceled Packets IE



Private Extension IE

The optional Private Extension contains vendor- or operator- specific information.

Data Record Transfer Response

The message shall be sent as a response to a received Data Record Transfer Request. Also, several Data Record Transfer Requests can be responded by a single Data Record Transfer Response.

The Cause (whatever the value may be) applies for all those Data Record Transfer Requests, responded by that particular Data Record Transfer Response.

Possible Cause values are:

- Request Accepted
- No resources available
- Service not supported
- System failure
- Mandatory IE incorrect
- Mandatory IE missing

- Optional IE incorrect
- Invalid message format
- Version not supported
- Request not fulfilled
- CDR decoding error
- Request already fulfilled
- Request related to possibly duplicated packet already fulfilled
- Sequence numbers of released/canceled packets IE incorrect

The cause value “CDR decoding error” is optional, primarily intended to inform the CDF that the receiving node cannot decode the CDR. Thus, special features in the receiving node that are based on information within the CDR, would not be operable. This message alerts the operator of a remote generating node of incompatible CDR encoding. It is optional and no action or response is required.

The Requests Responded IE contains the IE Type, Length and the Sequence Numbers (each 2 octets) of the Data Record Transfer Requests.

The optional Private Extension contains vendor- or operator- specific information. Depending on the Cause value severity and general occurrence frequency, the node that sent the corresponding Data Record Transfer Request, may start to direct its CDRs to another CGF.

Handling Error Response Cause

By default, on getting an error response, the request is retried to the same CGF server until max-retries is reached. Then the server is marked as NOT ACTIVE and the request is retried to the secondary server. This behavior is seen for the below response causes.

- Mandatory IE incorrect
- Mandatory IE missing
- Optional IE incorrect
- Invalid message format

On getting the following error response causes, the request will NOT retried and the server will be marked as NOT ACTIVE immediately.

- No resources available
- Service not supported
- System failure

No special action is taken on getting “CDR Decoding error” response cause and the behavior is similar to getting a "Request Accepted" cause.

On getting “Version not supported” cause, the request is resent with the version supported by the CGF server (by default, GTPP v2 is supported).

Charging Characteristics

Whether or not the GGSN accepts charging characteristics from the SGSN, the accounting protocol can be configured on a per-APN basis based on whether the subscriber is visiting, roaming, or home.

By default, the GGSN always accepts the charging characteristics from the SGSN. They will be provided by the SGSN for GTPv1 requests for primary PDP contexts. If they are not provided for secondary PDP contexts, the GGSN re-uses those from the primary. The charging characteristics field is optional. If not provided by SGSN, the GGSN selects the locally configured values. Also, there is a provision to override the values from RADIUS as indicated in the following table.

Table 13. Charging Characteristics Selection Mechanism

CLI command configured on GGSN	Sent by SGSN	Sent by AAA	CC used	chargingCharSelMode
`no cc-sgsn`	`no cc`	`no cc`	Default	Home/Visiting/Roaming Default
		`cc`	Default	Home/Visiting/Roaming Default
	`cc`	`no cc`	SGSN	SGSN Supplied
		`cc`	SGSN	SGSN Supplied
`cc-sgsn use-ggsn`	`no cc`	`no cc`	GGSN	GGSN Override
		`cc`	GGSN	GGSN Override
	`cc`	`no cc`	GGSN	GGSN Override
		`cc`	GGSN	GGSN Override
`cc-sgsn radius-returned`	`no cc`	`no cc`	Default	Home/Visiting/Roaming Default
		`cc`	AAA	AAA Supplied
	`cc`	`no cc`	SGSN	SGSN Supplied
		`cc`	AAA	AAA Supplied
`cc-sgsn radius-returned use-ggsn`	`no cc`	`no cc`	GGSN	GGSN Override
		`cc`	AAA	AAA Supplied
	`cc`	`no cc`	GGSN	GGSN Override
		`cc`	AAA	AAA Supplied

Please note that “Default” refers to the value set with the **`cc-home`**, **`cc-roaming`**, and **`cc-visiting`** commands. The “GGSN Override” and “AAA Override” are applicable ONLY for custom5 dictionary. Others will use Home/Visiting/Roaming Default based on the PLMN type.

If the system is configured to reject the charging characteristics from the SGSN, the GGSN can be configured with its own that can be applied based on the subscriber type (visiting, roaming, or home) at the APN level. The charging characteristics consists of a string of 16 bits designated as profile index and behavior settings. The GGSN supports up to 16 profile indexes numbered 0 through 15 whereas P-GW/S-GW supports up to a maximum of 256 charging profiles.

The profile indexes specify the criteria for closing accounting records based on specific criteria.

When a bearer is activated, an appropriate charging profile will be selected based on the following sources of input:

- Downloaded AAA attribute (ONLY in P-GW)
- MME/HSS via charging characteristics IE
- Local defaults

Following is the order of precedence when charging profile value is received from multiple sources.

- Profile index in the override rule on the APN
- Profile index in the override rule on the gateway
- Profile index from AAA in case of P-GW
- Profile index from non-override rule on the APN
- Profile index from non-override rule on the gateway

For more information on the commands that configure additional GTPP accounting properties, refer to the *Command Line Interface Reference*.

Charging Records

Charging records support details of the termination such as which end initiated the termination, termination type e.g. RST, FIN, etc. and in case of HTTP 1.1, whether or not the connection is still open. It is possible to pipeline up to 15 HTTP requests on the same TCP connection. The billing system, based on this information, decides upon the success or failure of the connection and charge or refund accordingly.

To cover the requirements of standard solutions and at the same time, provide flexible and detailed information on service usage, the following types of usage records are provided:

- Standard G-CDRs
- eG-CDRs
- PGW-CDRs
- SGW-CDRs
- S-CDRs
- WLAN-CDRs

The Multimedia Core Platform supports multiple fields for use in these CDRs. The CDRs are encoded using the ASN.1 format and are sent to the CGF using the GTPP.

Important: The behavior for several of the fields supported in CDRs can be modified. For more information, refer to the *Command Line Interface Reference*.

File Format for CDRs

The file format determines the information organization and structure -- format -- of the generated data files. All file formats are different and are customizable.

The following file formats are supported for CDRs:

- **custom1 Format**: This file format encodes CDRs according to the following conventions:
  - **Header**: No header
  - **Contents**: *CDR1CDR2CDR3...CDRn*
  - **EoF marker**: \n
  - **File name format**:

    <node-id-suffix+vpn-id>_<date>+<time>_<total-cdrs>_file<fileseqnum>

    The *<fileseqnum>* denotes the file sequence number ranging from 1 through 4294967295.
  - **Example**:

    default3_07_15_2009+07_53_02_5_file1
- **custom2 Format**: This customer-specific file format encodes CDRs according to the following conventions:
  - **Header**: 24 byte header incorporating the following information:

Field	Description	Value
0x00 - 0x03	Offset	Offset from EoH to first Unread CDR (4 Bytes)

Field	Description	Value
0x04 - 0x07	Encoding	Basic Encoding Rule (BER) i.e. 1 (4 Bytes)
0x08 - 0x0b	Number of CDRs	Total number of CDRs in the file (4 Bytes)
0x0c - 0x0f	Number of read CDRs	Total number of read CDRs in the file (4 Bytes)
0x10 - 0x13	File size	Size of CDR file in bytes (4 Bytes)
0x14 - 0x17	Abstract Syntax Notation One (ASN.1) format definition version	ASN.1 definition version information (4 Bytes)

- **Contents**: *LEN1CDR1LEN2CDR2LEN3CDR3...LENnCDRn*
- **EoF marker**: No EoF marker
- **File name format:**

  <node-id-suffix+vpn-id>_<date>+<time>_<total-cdrs>_file<fileseqnum>.u

  The *<fileseqnum>* denotes the file sequence number ranging from 1 through 4294967295.
- **Example**:

  default3_07_15_2009_07_59_32_5_file2.u

  Important: With file format **custom2**, the files are generated with **.u** file extension indicating an unprocessed file by the billing system. Typically, the billing system would rename the file with **.p** extension after processing the files with CDR information.

- **custom3 Format**: This customer-specific file format encodes CDRs according to the following conventions:
  - **Header**: No header
  - **Contents**: *CDR1CDR2CDR3...CDRn*
  - **EoF marker**: No EoF marker
  - **File name format:**

    <node-id-suffix+vpn-id>_<date>+<time>_<total-cdrs>_file<fileseqnum>.u

    The *<fileseqnum>* denotes the file sequence number ranging from 1 through 4294967295.
  - **Example**:

    default3_07_15_2009_07_59_32_5_file2.u
- **custom4 Format**: This custom4 format was created to support writing CDRs in blocks. This file format is similar to custom3 file format except CDRs will be written in 2Kbyte blocks in a file.
  - **Header:** No Header
  - **Contents:** CDR1|CDR2FFFFFF|CDR3FFFFF..|..CDRnFFFF|

    where | represents the end of a 2K block
  - **EoF marker:** No EoF marker
  - **File name format:**

    <node-id-suffix+vpn-id>_<date>+<time>_<total-cdrs>_file<fileseqnum>.u

    The *<fileseqnum>* denotes the file sequence number ranging from 1 through 4294967295.
  - **Example**:

default3_07_15_2009_07_59_32_5_file2.u

- **custom5 Format**: This file format is similar to custom3 file format except that the sequence number for CDR file name is of six digits in length ranging from 000001 to 999999.
  - **Header:** No Header
  - **Contents**: *CDR1CDR2CDR3...CDRn*
  - **EoF marker:** No EoF marker
  - **File name format**:

    <node-id-suffix+vpn-id>_<date>+<time>_<total-cdrs>_file<fixed-length-seqnum>.u
  - **Example**:

    default3_07_15_2009_08_09_25_4_file000003.u
- **custom6 Format**: This file format is similar to custom4 file format except CDRs will be written in 8Kbyte blocks in a file.
  - **Header:** No Header
  - **Contents:** CDR1|CDR2FFFFFF|CDR3FFFFF..|..CDRnFFFF|

    where | represents the end of a 8K block
  - **EoF marker:** No EoF marker
  - **File name format:**

    <node-id-suffix+vpn-id>_<date>+<time>_<total-cdrs>_file<fileseqnum>.u

    The *<fileseqnum>* denotes the file sequence number ranging from 1 through 4294967295.
  - **Example**:

    default3_07_15_2009_07_59_32_5_file2.u

Important: These file formats are customer-specific. For more information on the file formats, contact your Cisco account representative.

Standard G-CDRs

G-CDRs are generated according to 3GPP TS 32.251 V6.6.0. Currently ECS supports generation of CDRs using AAAMgrs only.

G-CDR Format

The G-CDRs can be in ASN.1 Format.

Enhanced G-CDRs

The ECS also supports enhanced G-CDRs, which is an enhanced format of standard G-CDRs to provide greater portability of charging information. eG-CDRs are compliant with 3GPP TS 32.298 v6.5.0 for Rel. 6 based dictionaries, and with 3GPP TS 32.298 v7.4.0 for Rel. 7 based dictionaries.

By default, the G-CDR does not support the traffic and vendor specific records. To support a traffic and vendor specific record, the ECS must be configured to generate eG-CDRs. eG-CDRs are useful to implement Time Based Charging (TBC) and Flow Based bearer Charging (FBC) to ECS.

eG-CDR supports customer specific formats configured in Ga context in a GGSN service with standard or custom specific GTPP dictionaries.

eG-CDR Format

The eG-CDRs can be in ASN.1 Format.

For more information on G-CDR and eG-CDR attributes and definitions, refer to the *G-CDR and Enhanced G-CDR Field Descriptions* chapter in this reference guide.

PDN Gateway Call Detail Records (PGW-CDRs)

PGW-CDRs are generated according to 3GPP TS 32.298 V8.5.0.

PGW-CDR Format

The PGW-CDRs can be in ASN.1 Format.

Serving Gateway Call Detail Records (SGW-CDRs)

SGW-CDRs are generated according to 3GPP TS 32.298 V8.7.0.

SGW-CDR Format

The SGW-CDRs can be in ASN.1 Format.

Standard SGSN CDRs

S-CDRs are generated according to 3GPP TS 32.215 V4.5.0 for Release 4 dictionaries, and 3GPP TS 32.298 V6.4.1 for Release 6 dictionaries.

S-CDR Format

The S-CDRs can be in ASN.1 Format.

Wireless LAN Call Detail Records (WLAN-CDRs)

WLAN-CDRs are generated according to 3GPP TS 32.298 V6.4.1.

WLAN-CDR Format

The WLAN-CDRs can be in ASN.1 Format.

Triggers for Generation of Charging Records

The following sections describe the triggers for the generation of partial and final CDRs.

GGSN CDR Triggers

The following sections describe the triggers for the generation of partial and final G-CDRs and eG-CDRs.

G-CDR Triggers

G-CDRs are updated (not closed) for any of the following conditions:

- SGSN IP address change

  When the SGSN IP address changes, i.e. an Update PDP Context Request is received with a new SGSN IP address, the old address (if not already added) and the new address are added to the field “List of SGSN Addresses”.

- QoS change

  When a QoS change is detected, i.e. an Update PDP Context Request is received with a new QoS value) and the maximum number of configured “buckets” has not been reached, then a traffic data volume container for the previous QoS and volume is added to the field “List of Traffic Data Volumes”.

- Tariff Time Change

  When the tariff time changes and the maximum number of configured “buckets” has not been reached, then a traffic data volume container is added to the field “List of Traffic Data Volumes” for the volume before the tariff time.

The following events trigger closure and sending of a partial G-CDR:

- the number of SGSN changes has reached the configured number of “sgsns”. Before this, the new SGSN address is added to the list of SGSN IP addresses in the CDR. If “sgsns 4” is configured, this means that after 4 handovers the record is closed and the G-CDR will contain 5 SGSN IP addresses. The parameter can be set to 1 to 4 with a default of 4.
- the number of QoS changes or tariff time changes, with up to 4 timestamps which can be configured using the tariff statement, has reached the configured number of “buckets” (1 to 4 with default of 4). Before this, another traffic data volume container is added to the CDR for every change.
- every x seconds configured using “interval x”
- every x octets configured using “volume x” (up/down/total)

A G-CDR is closed as the final record of a subscriber session for the following events:

- Delete PDP context received from SGSN
- Delete PDP context initiated by GGSN (e.g. expiry of idle or absolute timer)
- Abnormal Releases such as PDP context replacements

eG-CDR Triggers

eG-CDRs are updated (not closed) for any of the following conditions:

- PDP context modification

  When a change of PDP context conditions occurs (QoS change, SGSN change, PLMN Id change, RAT change) the List of Service Data (LOSDV) and the List of Traffic Volume (LOTV) containers are updated.

  In case of SGSN change condition only LOSDV containers are updated and also the List of SGSN addresses is updated.

- Tariff time change

  When a change of tariff time occurs a set of LOSDV and LOTV containers, i.e. all active service data flow containers, will be added to eG-CDR.

- Failure handling procedure triggering

  When the failure handling mechanism is triggered and the failure action is set to “continue” a set of LOSDV and LOTV containers, i.e. all active service data flow containers, will be added to eG-CDR.

- Service data flow report

  When an expiry of time limit, volume limit or termination is detected for a service data flow a set of LOSDV container is added to eG-CDR.

- CDR closure

  When a CDR closure occurs all active LOSDV containers are added to eG-CDR.

The eG-CDRs will be closed and sent as a partial record for any of the following triggers:

- data volume limit
- time duration limit
- maximum number of charging condition changes (QoS/tariff time change)
- maximum number of service data containers
- management intervention
- MS/Subscriber time zone change
- inter PLMN SGSN change
- Radio Access Technology (RAT) change

When an eG-CDR partial is written, all open LOSDVs will be closed as well with a matching change condition.

The eG-CDRs will be closed and sent as a final record upon the deactivation of the PDP context in the GGSN, both for normal termination and for any abnormal release.

All LOSDV which have been reported in previous partials but did not have a final change condition in the container are repeated in the final eG-CDR with a final change condition (e.g. pDPContextRelease). In case no volume has been transferred for this container since the last eG-CDR, then the timestamps for first and last usage will be set to the default value of "000101000000-0200".

The following table lists the values for the “CauseForRecordClosing” field based on trigger scenarios.

Table 14. Cause for Record Closing

Cause	Scenarios	Partial/Final	Value	Supported
normalRelease	– Delete PDP from SGSN – Manual call clearing on GGSN – Radius disconnect – Idle and absolute timeout	Final	0	Yes

Cause	Scenarios	Partial/Final	Value	Supported
abnormalRelease	– Path failure – Context replacement	Final	4	Yes
volumeLimit	Configured volume threshold has been exceeded	Partial	16	Yes
timeLimit	Configured interval has been reached	Partial	17	Yes
sGSNChange	– Configured limit of SGSN changes has been reached – inter-PLMN SGSN change	Partial	18	Yes
maxChangeCond	Configured limit of change conditions has been reached	Partial	19	Yes
managementIntervention	For example, using the command **gtpp interim now**	Partial	20	Yes
rATChange	Radio access technology change	Partial	22	Yes
mSTimeZoneChange	MS changes time zone	Partial	23	Yes

PGW-CDR Triggers

The following events trigger closure and the sending of a partial PGW-CDR:

- the number of QoS changes or tariff time changes has reached the configured maximum number of charging condition changes. Before this, service containers are added to the CDR for every change.
- every x seconds configured using “interval x”
- every x octets configured using “volume x” (up/down/total)
- command **gtpp interim now active-charging egcdr**
- Transferring the context to a new SGW/SGSN (serving Node Change).
- changing the access type within the same P-GW (RAT Change)

A PGW-CDR is closed as the final record of a subscriber session for the following events:

- Detach Request received from UE
- Delete bearer context request received from SGW.
- Manual subscriber clearing
- Abnormal Releases such as path failures

The following table lists the values for the “CauseForRecordClosing” field based on trigger scenarios.

Table 15. Cause for Record Closing

Cause	Scenarios	Partial/Final	Value	Supported
normalRelease	IP-CAN bearer release or detach	Final	0	Yes
abnormalRelease	Any other abnormal release	Final	4	Yes
volumeLimit	Configured volume threshold has been exceeded	Partial	16	Yes

Cause	Scenarios	Partial/Final	Value	Supported
timeLimit	Configured interval has been reached	Partial	17	Yes
servingNodeChange	Serving node Address list overflow	Partial	18	Yes
maxChangeCondition	Maximum number of changes in charging conditions	Partial	19	Yes
managementIntervention	For example, using the command **gtpp interim now active-charging egcdr**	Partial	20	Yes
RAT Change	Change of radio interface from (for example, EUTRAN to GSM to UMTS)	Partial	22	Yes
mSTimeZoneChange	MS changes time zone	Partial	23	Yes
PLMN Change	Change of PLMN-ID	Partial	24	Yes

PGW-CDR Charging Information Addition

The "List of Service Data" attribute in the PGW-CDR consists of a set of containers that are added when specific trigger conditions are met. Each container identifies the configured counts (volume separated for uplink and downlink, elapsed time, or number of events) per rating group or combination of the rating group and service id within the same IP-CAN bearer, on encountering that trigger condition.

Table 16. Triggers for PGW-CDR Charging Information Addition

Trigger Conditions	Description/Behavior
IP-CAN bearer modification	A change of IP-CAN bearer conditions (QoS change, SGSN/S-GW change, PLMN Id change, RAT change, user location change) results in a set of "List of Service Data" containers, such as all active service data flow containers, being added to the CDR.
Tariff Time Change	On reaching the Tariff Time Change, a set of "List of Service Data" containers, such as all active service data flow containers, is added to the CDR.
DCCA Failure-Handling procedure triggering	When the Diameter Credit-Control-Failure-Handling mechanism is triggered a "List of Service Data", such as all active service data flow containers, is added to the CDR. The causes are only relevant due to simultaneous usage of an active DCCA session.

Trigger Conditions	Description/Behavior
Service data flow report	For independent online and offline charging, a "List of Service Data" container for the service data flow is added at: • expiry of time limit • expiry of volume limit • expiry of unit limit • termination of service data flow For tight interworking of online and offline charging, a "List of Service Data" container for the service data flow is added when: • time threshold reached • volume threshold reached • unit threshold reached • time quota exhausted • volume quota exhausted • unit quota exhausted • expiry of quota validity timer • termination of service data flow – re-authorization request by OCS.

SGW-CDR Triggers

The following events trigger closure and sending of a partial SGW-CDR.

- When the number of QoS changes or tariff time changes or number of user location changes have reached the configured number of "buckets". Prior to this, another traffic data volume container is added to the CDR for every change.
- Every x seconds configured using "interval x"
- Every x octets configured using "volume x" (up/down/total)
- Command **`gtpp interim now`**
- Transferring the context to a new S-GW.
- Changing the access type within the same S-GW (RAT Change).

An SGW-CDR is closed as the final record of a subscriber session for the following events:

- Detach Request received from UE
- Delete bearer context request received from MME
- Delete bearer context request received from P-GW
- Manual subscriber clearing
- Abnormal Releases such as path failures

The following table lists the different values for the "CauseForRecordClosing" field depending on the different trigger scenarios.

Table 17. Cause for Record Closing

Cause	Scenarios	Partial/Final	Value	Supported
normalRelease	IP-CAN bearer release or detach	Final	0	Yes
abnormalRelease	Any other abnormal release	Final	4	Yes
volumeLimit	Configured volume threshold has been exceeded	Partial	16	Yes
timeLimit	Configured interval has been reached	Partial	17	Yes
servingNodeChange	Serving node Address list overflow	Partial	18	Yes
maxChangeCondition	Limit for the LOTV containers was exceeded	Partial	19	Yes
managementIntervention	For example, using the command **`gtpp interim now`**	Partial	20	Yes
RAT Change	Change of radio interface from (for example, EUTRAN to GSM to UMTS)	Partial	22	Yes
mSTimeZoneChange	MS changes time zone	Partial	23	Yes

Important: The spec 3GPP TS 32.251 mentions that a CDR must be generated whenever the PLMN-ID of the serving node changes, but does not have a corresponding “cause for record closure” reason in 3GPP TS 32.298. In the case when the MME changed during the call and the PLMN-ID has the same address, the MME is added to the “Serving Node Address” list. If a “Serving Node Address” list overflow occurs, a partial CDR will be generated with "cause for record closure" as “servingNodeChange”.

Important: The unsupported triggers mentioned above will be supported when the functionality is available.

SGW-CDR Charging Information Addition

The “List of Traffic Volumes” attribute of the SGW-CDR consists of a set of containers which are added when specific trigger conditions are met. They identify the volume count per QCI/ARP pair and are separated for uplink and downlink traffic after encountering that trigger condition.

The following table identifies which conditions are supported to trigger SGW-CDR charging information addition. Volume container identifies the uplink/downlink volume since the closure of the last container. The “Serving Node Address” attribute of the SGW-CDR consists of a list of serving node (for example, MME) addresses. A new serving node address is added to the list when MME changes.

Table 18. Triggers for SGW-CDR Charging Information Addition

Trigger Conditions	Description/Behavior
QoS Change	A change in the QoS will occur when the open “List of Traffic Data Volumes” containers are closed and added to the CDR, and a new IP-CAN bearer specific container is opened.
Tariff Time Change	After reaching the Tariff Time Change, open “List of Traffic Data Volumes” containers are closed and added to the CDR.

Trigger Conditions	Description/Behavior
User Location Change	A change in the User Location Info (for example, ECGI, TAI, RAI, SAI or CGI) will close open "List of Traffic Data Volumes" containers. They are then added to the CDR if location reporting is required and a report of User Location Change is received.
CDR Closure	Open "List of Traffic Data Volumes" containers are closed and added to the SGW-CDR.

WLAN-CDR Triggers

The following events trigger closure and sending of a partial WLAN-CDR:

- Time Trigger (every x seconds configured using "interval x")
- Volume Trigger (every x octets configured using "volume x" (up/down/total))
- On reaching maximum number of container limit
- command **`gtpp interim now`**

A WLAN-CDR is closed as the final record of a session for the following events:

- UE initiated call termination
- command **`clear subscribers all`**
- Abnormal Releases due to multiple software failures

The table below lists the different values for the "CauseForRecordClosing" field depending on the different trigger scenarios.

Table 19. Cause for Record Closing

Cause	Scenarios	Partial/Final	Value	Configurable
normalRelease	UE is terminating the call	Final	0	No
abnormalRelease	Failure within the chassis (due to multiple software failures)	Final	4	No
volumeLimit	Configured volume threshold has been exceeded	Partial	16	Yes
timeLimit	Configured interval has been reached	Partial	17	Yes
maxChangeCondition	Limit for the LOTV containers was exceeded	Partial	19	Yes
managementIntervention	For example, using the command **`gtpp interim now`**	Partial	20	No
managementIntervention	For example, using the command **`clear subscribers all`**	Final	20	No

WLAN-CDR Charging Information Addition

The "List of Traffic Volumes" attribute of the WLAN-CDR consists of a set of containers, which are added when specific trigger conditions are met, and identify the volume count per PDP context, separated for uplink and downlink traffic, on encountering that trigger condition.

The following table identifies which conditions are supported to trigger WLAN-CDR charging information addition. Volume container identifies the uplink/downlink volume since the closure of the last container. The "Serving Node Address" attribute of the SGW-CDR consists of a list of serving node (for example, MME) addresses. A new serving node address is added to the list when MME changes.

Table 20. Triggers for WLAN-CDR Charging Information Addition

Cause	Scenarios	Partial/Final	Value	Configurable
QoS Change	A change in the QoS shall result that open "List of Traffic Data Volumes" containers being closed and added to the CDR and new bearer specific container is opened.	Partial	0	Yes
tariffTime	On reaching the Tariff Time Change a "List of Traffic Data Volumes" container will be added to the CDR.	Partial	1	Yes
recordClosure	A list of "List of Traffic Data Volumes" container will be added to the WLAN-CDR.	-	2	No

Chapter 7
GGSN CDR Field Reference

This chapter provides a reference for CDR fields supported by the system for use in GGSN-CDRs (G-CDRs) and enhanced G-CDRs (eG-CDRs).

A complete list of supported CDR fields is provided in the *GGSN CDR Field Descriptions* chapter of this reference.

The specific CDRs reported in G-CDRs/eG-CDRs and their encoding are user-selectable via GTPP dictionaries.

Important: For more information on custom dictionaries, contact your Cisco account representative.

The category column in all tables use keys described in the following table.

Table 21. Dictionary Table Key

Abbreviation	Meaning	Description
M	Mandatory	A field that must be present in the CDR.
C	Conditional	A field that must be present in a CDR if certain conditions are met.
OM	Operator Provisionable: Mandatory	A field that an operator has provisioned and must be included in the CDR for all conditions.
OC	Operator Provisionable: Conditional	A field that an operator has provisioned that must included in the CDR if certain conditions are met.

CDR Fields Supported in G-CDRs

The tables in this section list the G-CDR fields present in the available GTPP dictionaries.

custom1 – custom4 Dictionaries

G-CDR fields based on 3GPP TS 32.015 V3.6.0 (2001-06) (R99).

Field	Category	Description
Record Type	M	GPRS GGSN PDP context record.
Network Initiated PDP Context	C	Present if this is a network-initiated PDP context.
Served IMSI	M	IMSI of the served party (if Anonymous Access Indicator is FALSE or not supplied).
Served MSISDN	O	The primary MSISDN of the subscriber.
GGSN Address	M	The IP address of the GGSN used.
Charging ID	M	PDP context identifier used to identify this PDP context in different records created by GSNs.
SGSN Address	M	List of SGSN addresses used during this record.
Access Point Name Network Identifier	M	The logical name of the connected access point to the external packet data network (network identifier part of APN).
APN Selection Mode	O	An index indicating how the APN was selected.
PDP Type	M	PDP type, i.e. IP, PPP, or IHOSS:OSP.
Served PDP Address	M	PDP address, i.e. IPv4 or IPv6.
Dynamic Address Flag	C	Indicates whether served PDP address is dynamic, which is allocated during PDP context activation.
List of Traffic Data Volumes	M	A list of changes in charging conditions for this PDP context, each time stamped. Charging conditions are used to categorize traffic volumes, such as per tariff period. Initial and subsequently changed QoS and corresponding data values are listed. In GSM, data volumes are in octets above the GTP layer and are separated for uplink and downlink traffic. In 3G, data volumes are in octets above the GTP-U layer and are separated for uplink and downlink traffic.
Record Opening Time	M	Time stamp when this record was opened.
Duration	M	Duration of this record in the GGSN.
Cause for Record Closing	M	The reason for the release of record from this GGSN.
Diagnostics	O	A more detailed reason for the release of the connection.
Record Sequence Number	C	Partial record sequence number, only present in case of partial records.

Field	Category	Description
Node ID	O	Name of the recording entity.
Record Extensions	O	A set of network/manufacturer specific extensions to the record.
Local Record Sequence Number	O	Consecutive record number created by this node. The number is allocated sequentially including all CDR types.
Charging Characteristics	C	The Charging Characteristics flag retrieved from subscriber's data as described in TS 32.015 V3.6.0 sub clause 6.1.6.5.

Notes:

- custom2 and custom3 dictionaries:
  - All IP addresses are encoded in binary format.
- custom4 dictionary:
  - All IP addresses are encoded in binary format.
  - Data Record Format Version IE contains 0x1307 instead of 0x1308.
  - QoSRequested is not present in the LoTV containers.
  - QoSNegotiated is added only for the first container and the container after QoSChange condition.

custom5 – custom7, custom9, custom12, custom14, custom15, custom17, custom19, custom20, and custom22 Dictionaries

G-CDR fields based on 3GPP TS 32.298 V6.6.0 (2006-12) (R6).

Field	Category	Description
Record Type	M	GGSN PDP context record.
Network initiated PDP context	OC	A flag that is present if this is a network-initiated PDP context.
Served IMSI	M	IMSI of the served party.
Served IMEISV	OC	IMEISV of the ME, if available.
GGSN Address	M	The control plane IP address of the GGSN used.
Charging ID	M	PDP context identifier used to identify this PDP context in different records created by GSNs.
SGSN Address	M	List of SGSN addresses used during this record.
Access Point Name Network Identifier	OM	The logical name of the connected access point to the external packet data network (network identifier part of APN).
PDP Type	OM	PDP type, i.e. IP, PPP, or IHOSS:OSP.
Served PDP Address	OC	PDP address, i.e. IPv4 or IPv6. This parameter shall be present except when both the PDP type is PPP and dynamic PDP address assignment is used.
Dynamic Address Flag	OC	Indicates whether served PDP address is dynamic, which is allocated during PDP context activation. This field is missing if address is static.

Field	Category	Description
List of Traffic Data Volumes	OM	A list of changes in charging conditions for this PDP context, each change is time stamped. Charging conditions are used to categorize traffic volumes, such as per tariff period. Initial and subsequently changed QoS and corresponding data values are also listed.
Record Opening Time	M	Time stamp when PDP context is activated in this GGSN or record opening time on subsequent partial records.
MS Time Zone	OC	This field contains the MS Time Zone the MS is currently located as defined in TS 29.060, if provided by SGSN.
Duration	M	Duration of this record in the GGSN.
Cause for Record Closing	M	The reason for the release of record from this GGSN.
Diagnostics	OM	A more detailed reason for the release of the connection.
Record Sequence Number	C	Partial record sequence number, only present in case of partial records.
Node ID	OM	Name of the recording entity.
Record Extensions	OC	A set of network operator/manufacturer specific extensions to the record. Conditioned upon the existence of an extension.
Local Record Sequence Number	OM	Consecutive record number created by this node. The number is allocated sequentially including all CDR types.
APN Selection Mode	OM	An index indicating how the APN was selected.
Served MSISDN	OM	The primary MSISDN of the subscriber.
User Location Information	OC	This field contains the User Location Information of the MS as defined in TS 29.060, if provided by SGSN.
Charging Characteristics	M	The Charging Characteristics applied to the PDP context.
Charging Characteristics Selection Mode	OM	Holds information about how Charging Characteristics were selected.
IMS Signalling Context	OC	Included if the IM-CN Subsystem Signalling Flag is set, TS 23.060 PDP context is used for IMS signalling.
External Charging Identifier	OC	Holds a Charging Identifier and is present only if it is received from a non-GPRS, external network entity.
SGSN PLMN Identifier	OM	SGSN PLMN Identifier (MCC and MNC) used during this record.
CAMEL Information	OC	Set of CAMEL information related to PDP context. This field is present if CAMEL Charging Information is received by the GGSN in the GTP Create PDP context request.
RAT Type	OC	This field indicates the Radio Access Technology (RAT) type currently used by the Mobile Station as defined in TS 29.060. The field is present in the G-CDR if provided by SGSN.

Notes:

- QoSRequested is not present in the LoTV containers.

- QoSNegotiated is added only for first container and container after QoSChange condition.
- Camel Info, IMS Signaling Context, and External Charging Identifier are not supported in the G-CDR.
- custom14 dictionary: All IP addresses are represented in text.
- custom22 dictionary: Supports customer-specific Transparent-Data record extension.

standard, custom8, custom10, custom11, custom13, custom18, custom21, custom23 – custom29 Dictionaries

G-CDR fields based on 3GPP TS 32.215 V4.6.0 (2003-12) (R4).

Field	Category	Description
Record Type	M	GGSN PDP context record.
Network initiated PDP context	OC	A flag that is present if this is a network-initiated PDP context.
Served IMSI	M	IMSI of the served party.
GGSN Address	M	The control plane IP address of the GGSN used.
Charging ID	M	PDP context identifier used to identify this PDP context in different records created by GSNs.
SGSN Address	M	List of SGSN addresses used during this record.
Access Point Name Network Identifier	OM	The logical name of the connected access point to the external packet data network (network identifier part of APN).
PDP Type	OM	PDP type, i.e. IP, PPP, or IHOSS:OSP
Served PDP Address	OC	PDP address, i.e. IPv4 or IPv6. This parameter shall be present except when both the PDP type is PPP and dynamic PDP address assignment is used.
Dynamic Address Flag	OC	Indicates whether served PDP address is dynamic, which is allocated during PDP context activation. This field is missing if address is static.
List of Traffic Data Volumes	OM	A list of changes in charging conditions for this PDP context, each change is time stamped. Charging conditions are used to categorise traffic volumes, such as per tariff period. Initial and subsequently changed QoS and corresponding data values are listed.
Record Opening Time	M	Time stamp when PDP context is activated in this GGSN or record opening time on subsequent partial records.
Duration	M	Duration of this record in the GGSN.
Cause for Record Closing	M	The reason for the release of record from this GGSN.
Diagnostics	OM	A more detailed reason for the release of the connection.
Record Sequence Number	C	Partial record sequence number, only present in case of partial records.
Node ID	OM	Name of the recording entity.

Field	Category	Description
Record Extensions	OC	A set of network operator/manufacturer specific extensions to the record. Conditioned upon the existence of an extension.
Local Record Sequence Number	OM	Consecutive record number created by this node. The number is allocated sequentially including all CDR types.
APN Selection Mode	OM	An index indicating how the APN was selected.
Served MSISDN	OM	The primary MSISDN of the subscriber.
Charging Characteristics	M	The Charging Characteristics applied to the PDP context.
Charging Characteristics Selection Mode	OM	Holds information about how Charging Characteristics were selected.
SGSN PLMN Identifier	OM	SGSN PLMN identifier (MCC and MNC) used during this record.

custom16 Dictionary

G-CDR fields based on 3GPP TS 32.215 V4.5.0 (2003-09) (R4).

Field	Category	Description
Record Type	M	The field identifies the type of the record: G-CDR (ggsnPDPRecord) — 10(0x13)
Served IMSI	M	This field contains the International Mobile Subscriber Identity (IMSI) of the served party.
Served IMEI	OC	The IMEI of the ME, if available.
List of SGSN Address	M	The IP address of the current SGSN.
GGSN Address	M	This field contains an Ipv4 address in hexadecimal format. This field provides the current serving GGSN IP Address for the Control Plane, which is equivalent to the configured ggsn-service address on the GGSN.
Charging ID	M	This field is a charging identifier, which can be used together with the GGSN address to identify all records produced in the GGSN involved in a single PDP context. The Charging ID is generated by the GGSN at PDP context activation and is transferred to the context requesting SGSN. At an inter-SGSN routing area update, the charging ID is transferred to the new SGSN as part of each active PDP context.
Access Point Name Network Identifier	M	This field contains the Network Identifier part of the Access Point Name (APN). It is provided by the SGSN in the Create PDP Context Request message. The APN string consists of alphabetic characters ("A..Z", "a.."z"), digits ("0..9") and the dash "-". In case of a configured virtual APN, the virtual APN is included instead, unless this is overridden by the option **`gcdr apn-name-to-be-included {gn | virtual}`**.

Field	Category	Description
PDP Type	M	This field defines the PDP type, e.g. IP or PPP. Supported Values: • IP = 0121 • PPP = 0001 ***Important:*** The spare bits should be set to 0000. This is a change as compared to 3GPP spec where the spare bits are set to 1111.
Served PDP Address	M	This field contains the PDP address of the served IMSI. This is a network layer address i.e. of type IP version 4. The address for each PDP type is allocated either temporarily or permanently (see "Dynamic Address Flag"). This parameter will be present except when both the PDP type is PPP and dynamic PDP address assignment is used.
List of Traffic Data Volumes	M	This list includes one or more Traffic Volume containers related to a "Change of Charging Condition". The maximum number of containers is configurable. This list includes containers that include the following fields: • QoS Negotiated • Data Volume GPRS Uplink • Data volume GPRS Downlink • Change Condition • Change time
QoS Negotiated	O	This field indicates the applied QoS accepted by the network. The field is defined with a maximum size of 9 bytes. **Note:** • Delay Class, Reliability class, Peak throughput, Precedence class, Mean throughput are not encoded in Wireless Format. • Always 9 bytes will be sent, even if the QoS Negotiated is more than 9 bytes. • If the MS is pre 99, then all 9 bytes should be sent as 0x00.
Data Volume GPRS Uplink	M	This field indicates the number of octets received in the uplink direction during the timeframe specified by the container. For each new container, the counter is reset and does not accumulate. The data counted already includes the IP PDP bearer protocols i.e. IP or PPP. It does not include the overhead between SGSN-GGSN GTPU protocol. The counter contains the volume for the PDP context part for which the record is generated. That is, in case of single record (no exceeding of any threshold) the whole volume account is included. Within a partial record of a record sequence only the volume relating to a context section and not the accumulated sum is written. The whole PDP context volume is the sum of all partial volume counters containing in the intermediate plus the final CDR count. In case of partial record generation due to exceeding of the volume threshold, the volume account equal to or greater than the threshold is written into the CDR due to data collection at time intervals.

Field	Category	Description
Data volume GPRS Downlink	M	This field indicates the number of octets transmitted in the downlink direction during the timeframe specified by the container. For each new container, the counter is reset and does not accumulate. The data counted already includes the IP PDP bearer protocols i.e. IP or PPP. It does not include the overhead between SGSN-GGSN GTPU protocol. The counter contains the volume for the PDP context part for which the record is generated. That is, in case of single record (no exceeding of any threshold) the whole volume account is included. Within a partial record of a record sequence only the volume relating to a context section and not the accumulated sum is written. The whole PDP context volume is the sum of all partial volume counters containing in the intermediate plus the final CDR count. In case of partial record generation due to exceeding of the volume threshold, the volume account equal to or greater than the threshold is written into the CDR due to data collection at time intervals.
Change Condition	M	The Change Condition field is part of the ChangeOfCharCondition element in the List of Traffic Data Volumes. It defines the reason for closing the container, such as tariff time change, QoS change or closing of the CDR. Supported values: • qoSChange (0) • tariffTime (1) • recordClosure (2) • intra-PLMN SGSN Change (12h) **Note**: The post-processing system converts these values into different values.
Change time	M	Change Time is a time stamp, which defines the moment when the volume container is closed or the CDR is closed. **Note**: The time should indicate the number of seconds elapsed since 1970. The encoding mechanism is different as compared to 3GPP specification.
Record Opening Time	M	This field contains the time stamp when a PDP context is activated in GGSN or when a subsequent record is opened after a partial record. The timestamp is determined based on the internal timer which has an accuracy of 10ms. Depending on the configured mechanism (ceiling, floor, round-off) this is translated into the timestamp which only shows the full seconds. **Note**: The time should indicate the number of seconds elapsed since 1970. The encoding mechanism is different as compared to 3GPP specification.
Duration	M	This field contains the duration in seconds for the record. For partial records, only the interval described by the recordOpeningTime and the last ChangeTime in the ListOfTrafficVolumes is counted. The value is reset for each new partial CDR. This value is converted from the internal representation in milliseconds to an integer value representing only seconds. The mechanism for this conversion (ceiling, floor, round-off) can be configured.

Field	Category	Description
Cause for Record Closing	M	This field contains a reason for the closure of the CDR. Normal release is used for PDP context release. For partial record generation, data volume limit, time (duration) limit, maximum number of changes in charging conditions, SGSN Change are used. Abnormal release is used for abnormal termination, that is, when the PDP context deactivation is caused by an error in the GSN network. Supported values: • normalRelease (0) • abnormalRelease (4) • volumeLimit (16) • timeLimit (17) • sGSNChange (18) • maxChangeCond (19) • managementIntervention (20) • rATChange (21) **Note**: The post-processing system maps these values to some other values.
Record Sequence Number	M	A running sequence number with the range of 1 through 4294967295 used to link partial records generated by the GGSN for a specific PDP context (characterized with the same Charging ID and GGSN address pair). **Note**: This should be present even if there is only one record (Final Record) for a CDR.
Charging Type	M	This field contains the charging type used in the G-CDR. **Note**: The exact definition of this field is not known. Also this field is not relevant to billing. By looking at the raw data from customer it is the LSB of charging characteristics. Hence, always LSB of charging characteristics is sent. The following values are used: • NORMAL_RECORD (8) • PREPAID_RECORD (4) • HOTBILLING_RECORD (1)
Charging Characteristics	M	Lists the charging characteristics applied to the PDP context by the GGSN. **Note**: By default, the GGSN always accepts the charging characteristics from the SGSN. If they are not provided for secondary PDP contexts, the GGSN re-uses those from the primary. Whether or not the GGSN accepts charging characteristics from the SGSN can be configured on a per-APN basis based on whether the subscriber is visiting, roaming or, home.
Served MSISDN	M	This field tracks the Mobile Station (MS) ISDN number (MSISDN) of the subscriber which is transparently copied from the Create PDP Context Request message. The MSISDN is TBCD encoded.

Field	Category	Description
Node ID	M	This field contains an identifier string for the node that had generated the CDR. On the GGSN, this NodeID field is a printable string of the ndddSTRING format: n: The first digit is the Sessmgr restart counter having a value between 0 and 7. ddd: The number of the sessmgr instance generating the CDR STRING: This is a configured Node-ID-Suffix having any string from 1 to16 characters, defined using the **`gtpp attribute node-id`** command. If this node-id-suffix is not configured, the GGSN uses the GTPP context name as the Node-id-suffix (truncated to 16 characters). For G-CDRs, this field is only included when the option **`gtpp attribute local-record-sequence-number`** is configured. **Note 1**: If **`centralized-lrsn-creation`**option is enabled node-id is the **`node-id-suffix`** configured in the **`gtpp attribute node-id-suffix`** *`string`*. **Note 2**: If **`centralized-lrsn-creation`** is not enabled, then node-id format is as follows: *`1-byte Sessmgr restart-value 3-byte Sessmgr instance number node-id-suffix`*.
Local Record Sequence Number	M	For each Node ID, this number with the range of 1 through 4294967295 is allocated sequentially for each CDR. This along with a Node ID uniquely identifies a CDR. This field is only included when the option **`gtpp attribute local-record-sequence-number`** is configured. **Note 1**: To generate unique LRSN, the centralized LRSN should be enabled. If 'centralized LRSN' is not enabled, the 'Local Sequence Number' is generated based on per sessmgr. **Note 2**: To enable 'centalized LRSN' use the following command **`gtpp single-source centralized-lrsn-creation`** in the config mode.
Dynamic Address Flag	C	This field indicates that PDP address has been dynamically allocated for that particular PDP context. This field is missing if address is static i.e. part of PDP context subscription. Dynamic address allocation might be relevant for charging e.g. the duration of PDP context as one resource offered and possibly owned by the network operator. This field is set to 0x01 in case if the IP address is dynamically allocated.
APN Selection Mode	M	An index indicating how the APN was selected. The following APN selection mode indexes are possible: 0: MS or network provided APN, subscribed verified 1: MS provided APN, subscription not verified 2: Network provided APN, subscription not verified
Charging Characteristics Selection Mode	M	The charging characteristic type that the GGSN applied to the CDR. The following values for this field are defined in 3GPP TS 32.298: • sGSNSupplied (0) — The GGSN is using the charging characteristics supplied by the SGSN. • homeDefault (3) — GGSN configured charging characteristics for home subscribers are used. Home subscribers are those that belong to the same PLMN as the one on which the GGSN is located. • visitingDefault (5) — GGSN configured charging characteristics for visiting subscribers are used. Visiting subscribers are those that belong to a different PLMN than the one on which the GGSN is located. • roamingDefault (4) — GGSN configured charging characteristics for roaming subscribers are used. Roaming subscribers are those that are serviced by an SGSN belonging to a different PLMN than the one on which the GGSN is located.

Field	Category	Description
Diagnostics	O	This field indicating the concrete cause for why the PDP context was released. This field will be included only in the final CDR. This field can always be present in wireless system in final CDR. For Normal PDP Release: 0x08 Abnormal PDP Release: 0x10
Time Zone	M	The difference between UTC and local time for the record opening time. The value is given in seconds. This field is present in all partial G-CDRs. The value is calculated as follows: If the time zone is : -07:00, then the encoded value is: TimeZone = 2^32 - 7*3600 = ff ff 9d 90
PLMN ID	M	The PLMN ID of the SGSN(s) in this G-CDR. For GGSN, RAI (optionally supplied by the SGSN in the GTP create PDP context request) will be used as the SGSN PLMN Identifier value;
Charging Type Selection Mode	M	This field indicates how the charging type field was selected. **Note**: In wireless system this field is always sent to 1. The value '1' indicates that the 'charging type' is copied from the charging characteristics field.
Access Type	M	This field indicates the Radio Access Technology (RAT) type currently used by the Mobile Station. **Note**: The value for "Unspecified SGSN" is 0xff. In the raw G-CDR this value is always sent as 0xff. Hence, in GGSN, this value is always 1 irrespective of the system.
Charging Profile	M	This field indicates the profile of the user. **Note**: The exact definition of 'charging profile' is not known. Also this value is not relevant to charging. Hence, hard-coded value as in the raw data sample provided by wireless system is sent in G-CDR.

Notes:

- The G-CDRs are encoded in the TLV format. Also the encoding of some of the fields within the CDR is proprietary. (For example, in case of QoS negotiated the throughput / Precedence class / Mean throughput are not included).
- Except diagnostics and IMEI all fields are mandatory.
- Instead of “RAT Change” trigger, “Intra SGSN Inter System” trigger is used.
- IP address is binary encoded.

custom30 Dictionary

G-CDR fields based on 3GPP TS 32.298 V6.4.1 (R6).

Field	Category	Description
Record Type	M	The field identifies the type of the record : G-CDR (ggsnPDPRecord) — 19(0x13) Depending on the APN configuration: G-CDRs: accounting-mode gtpp
Network Initiation	O	Indicates whether the PDP context is initiated by network or PDP.
Served IMSI	M	This field contains the International Mobile Subscriber Identity (IMSI) of the served party. The IMSI is formatted in accordance with 3GPP TS 23.003.

Field	Category	Description
GGSN Address	M	This field provides the current serving GGSN IP Address for the Control Plane. The standard 3GPP 32.298 offers a choice for the encoding of the address to be either in binary or text format. The GGSN encodes the address in binary format and includes the Octet String. The IP address should be in binary format.
GGSN IPv4 Binary Address	M	The octet string included in the field described above includes the Gn address of the GGSN service in binary coding.
Charging ID	M	This field is a charging identifier, which can be used together with the GGSN address to identify all records produced in the GGSN involved in a single PDP context. The Charging ID is generated by the GGSN at PDP context activation and is transferred to the context requesting SGSN. At an inter-SGSN routing area update the charging ID is transferred to the new SGSN as part of each active PDP context.
List of SGSN Addresses	M	This field contains 1-5 SGSN IP addresses (maximum 4 SGSN changes). A CDR is closed as a partial with Cause for Record Closing set to SGSN Change when the maximum number of changes has been recorded. Subsequent SGSN changes will be listed in the next partial. i.e during ISRAU scenario, the call might go to a different SGSN, and the SGSN IP address is added to the list. The IP address should be in binary format.
SGSN IPv4 Binary Address	M	The octet string included in the field described above includes either control plane or user plane address of the SGSN in binary coding.
Access Point Name Network Identifier	M	This field contains the Network Identifier part of the Access Point Name (APN). It is provided by the SGSN in the Create PDP Context Request message. In case of a configured virtual APN, the virtual APN is included instead, unless this is overridden by the option **`gcdr apn-name-to-be-included {gn | virtual}`** **Note**: Length encoding of apname is used.
PDP Type	M	This field defines the PDP type, e.g. IP or PPP. Supported values: • IP = 0121 • PPP = 0001 **Note**: Spare bits are encoded as 0's. This is a non-3GPP STD behavior.
Served PDP Address	O	This field contains the PDP address of the served IMSI for which the standard 3GPP TS 32.298 allows a choice of either IPAddress or ETSIAddress. The IP Address should be in binary format.
PDP IP Address	M	This field contains the IP address for the PDP context.
PDP IPv4 Binary Address	M	The octet string included in the field described above includes the IPv4 address assigned to the subscriber by the GGSN in binary coding.
Dynamic Address Flag	O	This field indicates that the PDP address has been dynamically allocated for that particular PDP context. This field is missing if the address allocation method is "static", i.e. part of PDP context subscription.

Field	Category	Description
List of Traffic Data Volumes	M	This list includes one or more Traffic Volume containers related to a "Change of Charging Condition" as described in the next field. The number of containers is configurable to a maximum of 4 for G-CDRs. A list of changes in charging conditions for this PDP context, each time it is stamped. Charging conditions are used to categorise traffic volumes, such as per tariff period. Initial and subsequently changed QoS and corresponding data values are listed. In GSM, data volumes are in octets above the GTP layer and are separated for the uplink and downlink traffic. In 3G, data volumes are in octets above the GTP-U layer and are separated for uplink and downlink traffic.
ChangeOfCharCondition	M	One traffic data volume container contains a list of change of charging conditions: • QoS Negotiated • Data Volume Uplink • Data Volume Downlink • Change Condition • Change Time The QoS values may only be included in the first container. In later containers their presence depends upon what has been changed.
QoS Negotiated	O	This field indicates the applied QoS accepted by the network. This field is compliant to the 3GPP standards.
GPRS Uplink data volume	M	This field includes the number of octets transmitted during the use of the packet data services in the uplink direction. The amount of data counted in the GGSN is the payload of the GTP-U protocol at the Gn interface. The data counted already includes the IP PDP bearer protocols i.e. IP or PPP. **Note**: A maximum of 2^32 bytes can be counted in this field. A volume trigger should be defined at least for this value to avoid an overflow, if not done already for a smaller amount of traffic.
GPRS Downlink data volume	M	This field includes the number of octets transmitted during the use of the packet data services in the downlink direction. The amount of data counted in the GGSN is the payload of the GTP-U protocol at the Gn interface. The data counted already includes the IP PDP bearer protocols i.e. IP or PPP. **Note**: A maximum of 2^32 bytes can be counted in this field. A volume trigger should be defined at least for this value to avoid an overflow, if not done already for a smaller amount of traffic.
Change Condition	M	This field defines the reason for closing the container such as tariff time change, QoS change or closing of the CDR. Supported values: • qoSChange: 0 • tariffTime: 1 • recordClosure: 2

Field	Category	Description
Change time	M	This field is a time stamp, which defines the moment when the volume container is closed or the CDR is closed.
Record Opening Time	M	This field contains the time stamp when PDP context is activated in GGSN or when a subsequent record is opened after a partial record. The timestamp is determined based on the internal timer which has an accuracy of 10ms. Depending on the configured mechanism (ceiling, floor, round-off) this is translated into the timestamp which only shows the full seconds.
Duration	M	This field contains the relevant duration in seconds for PDP contexts with the range of 0..4294967295 (2^32-1). It is the duration from Record Opening Time to record closure. For partial records, this is the duration of the individual partial record and not the cumulative duration.
Cause for Record Closing	M	This field contains a reason for the release of the CDR. Supported values: • normalRelease: 0 • abnormalRelease: 4 • volumeLimit: 16 • timeLimit: 17 • sGSNChange: 18 • maxChangeCond: 19 • managementIntervention: 20 • rATChange: 22 • mSTimeZoneChange: 23
Diagnostics	O	This field is included in the CDR when the PDP context is released and when the option **`gtpp attribute diagnostics`** is configured. Only the choice of **`gsm0408Value`** is used.
Record Sequence Number	O	A running sequence number with the range of 1 through 4294967295 used to link partial records generated by the GGSN for a specific PDP context (characterized with the same Charging ID and GGSN address pair). This field is not present if the first record is also the final record.
Node ID	M	This field contains an identifier string for the node that had generated the CDR. On the ASR5K GGSN, this NodeID field is a printable string of the ndddSTRING format: n: The first digit is the Sessmgr restart counter having a value between 0 and 7. ddd: The number of the sessmgr instance generating the CDR. STRING: This is a configured Node-ID-Suffix having any string between 1 to16 characters, defined using the gtpp attribute node-id command. If this node-id-suffix is not configured, the GGSN uses the GTPP context name as the Node-id-suffix (truncated to 16 characters). For G-CDRs, this field is only included when the option **`gtpp attribute local-record-sequence-number`** is configured.

Field	Category	Description
Local Record Sequence Number	M	For each Node ID, this number with range 1 through 4294967295 is allocated sequentially for each CDR. This along with a Node ID uniquely identifies a CDR. For G-CDRs, this field is only included when the option **`gtpp attribute local-record-sequence-number`** is configured.
APN Selection Mode	M	An index indicating how the APN was selected. The following APN selection mode indexes are possible: • 0: MS or network provided APN, subscribed verified • 1: MS provided APN, subscription not verified • 2: Network provided APN, subscription not verified
Served MSISDN	M	The field tracks the Mobile Station (MS) ISDN number (MSISDN) of the subscriber which is a part of the Create PDP Context Request message.
Charging Characteristics	M	Lists the charging characteristics applied to the PDP context. The GGSN can accept charging characteristics from the SGSN or AAA or use its own configured value. GGSN configured charging characteristics are specified as part of the GGSN Service and are applied for G-CDRs to subscriber PDP contexts through APN templates.
Charging Characteristics Selection Mode	O	The charging characteristic type that the GGSN applied to the CDR. The following values for this field are defined in 3GPP TS 32.298: sGSNSupplied (0) — For GGSN only homeDefault (3) — For SGSN and GGSN roamingDefault (4) — For SGSN and GGSN visitingDefault (5) — For SGSN and GGSN • SGSN supplied: The GGSN is using the charging characteristics supplied by the SGSN. • Home default: GGSN configured charging characteristics for home subscribers are used. Home subscribers are those that belong to the same PLMN as the one on which the GGSN is located. • Visiting default: GGSN configured charging characteristics for visiting subscribers are used. Visiting subscribers are those that belong to a different PLMN than the one on which the GGSN is located. • Roaming default: GGSN configured charging characteristics for roaming subscribers are used. Roaming subscribers are those that are serviced by an SGSN belonging to a different PLMN than the one on which the GGSN is located.
SGSN PLMN Identifier	O	RAI (optionally supplied by SGSN in the GTP create PDP context request) is used as SGSN PLMN Identifier value. It is omitted if the SGSN does not supply the RAI and is not identified as a "home" SGSN. For home SGSNs without the RAI a locally configured PLMN-ID can be sent instead.
Served IMEISV	O	The International Mobile Equipment Identity and Software Version Number (IMEISV) of the MS, if available. **Note**: The IMEI is stored in the CDR in the "twisted" format as received from the SGSN.

Field	Category	Description
RAT Type	O	This field indicates the Radio Access Technology (RAT) type currently used by the Mobile Station. This field is present in the CDR if provided by SGSN. RAT Type values: • Reserved: 0 • UTRAN: 1 • GERAN: 2 • WLAN: 3 • Spare: 4-255
MS Time Zone	O	This field contains the "Time Zone" IE that the SGSN may provide to the GGSN during the PDP context activation/modification procedure.
User Location Information	O	The User Location Information for the MS if provided by the SGSN to the GGSN during the PDP context activation/modification procedure. Transparently copied from the PDP context request.

Important: Subfields included in other fields are marked MANDATORY even if the main field is optional.

Notes:

The record that differ from the standard implementation defined in 3GPP TS 32.298 is discussed in the following points:

- The PDP Type field is encoded differently. The spare bits are coded as 0000 (0x0) instead of 1111 (0xf). For example: For other dictionaries, pdpType for IPv4 will be coded as "88 02 f1 21", and for custom30 it will be coded as "88 02 01 21".

CDR Fields Supported in eG-CDRs

The tables in this section list the eG-CDR fields present in the available GTPP dictionaries.

custom1 Dictionary

eG-CDR fields for TS 32.015 v 3.6.0 (R99).

Field	Category	Description
Record Type	M	GPRS GGSN PDP context record.
Network Initiated PDP Context	C	Present if this is a network-initiated PDP context.
Served IMSI	M	IMSI of the served party (if Anonymous Access Indicator is FALSE or not supplied).
Served MSISDN	O	The primary MSISDN of the subscriber.
GGSN Address	M	The IP address of the GGSN used.
Charging ID	M	PDP context identifier used to identify this PDP context in different records created by GSNs.
SGSN Address	M	List of SGSN addresses used during this record.
Access Point Name Network Identifier	M	The logical name of the connected access point to the external packet data network (network identifier part of APN).
APN Selection Mode	O	An index indicating how the APN was selected.
PDP Type	M	PDP type, i.e. IP, PPP, or IHOSS:OSP.
Served PDP Address	M	PDP address, i.e. IPv4 or IPv6 address.
Dynamic Address Flag	C	Indicates whether served PDP address is dynamic, which is allocated during PDP context activation.
List of Traffic Data Volumes	M	A list of changes in charging conditions for this PDP context, each time stamped. Charging conditions are used to categorize traffic volumes, such as per tariff period. Initial and subsequently changed QoS and corresponding data values are listed. In GSM, data volumes are in octets above the GTP layer and are separated for uplink and downlink traffic. In 3G, data volumes are in octets above the GTP-U layer and are separated for uplink and downlink traffic. ***Important:*** Only one LOTV container per eG-CDR.
Record Opening Time	M	Time stamp when this record was opened.
Duration	M	Duration of this record in the GGSN.
Cause for Record Closing	M	The reason for the release of record from this GGSN.

Field	Category	Description
Record Sequence Number	C	Partial record sequence number, only present in case of partial records.
Node ID	O	Name of the recording entity.
Local Record Sequence Number	O	Consecutive record number created by this node. The number is allocated sequentially including all CDR types.
Charging Characteristics	C	The Charging Characteristics flag retrieved from subscriber's data as described in TS 32.015 sub clause 6.1.6.5.

custom2 Dictionary

eG-CDR fields for TS 32.015 v 3.6.0 (R99).

Field	Category	Description
Record Type	M	GPRS GGSN PDP context record.
Network initiated PDP context	C	Present if this is a network-initiated PDP context.
Served IMSI	M	IMSI of the served party (if Anonymous Access Indicator is FALSE or not supplied).
Served MSISDN	O	The primary MSISDN of the subscriber.
GGSN Address	M	The IP address of the GGSN used.
Charging ID	M	PDP context identifier used to identify this PDP context in different records created by GSNs.
SGSN Address	M	List of SGSN addresses used during this record.
Access Point Name Network Identifier	M	The logical name of the connected access point to the external packet data network (network identifier part of APN).
APN Selection Mode	O	An index indicating how the APN was selected.
PDP Type	M	PDP type, i.e. IP, PPP, or IHOSS:OSP.
Served PDP Address	M	PDP address, i.e. IPv4 or IPv6 address.
Dynamic Address Flag	C	Indicates whether served PDP address is dynamic, which is allocated during PDP context activation.
List of Traffic Data Volumes	M	A list of changes in charging conditions for this PDP context, each time stamped. Charging conditions are used to categorize traffic volumes, such as per tariff period. Initial and subsequently changed QoS and corresponding data values are listed. In GSM, data volumes are in octets above the GTP layer and are separated for uplink and downlink traffic. In 3G, data volumes are in octets above the GTP-U layer and are separated for uplink and downlink traffic. ***Important:*** Only one LOTV container per eG-CDR.

Field	Category	Description
Record Opening Time	M	Time stamp when this record was opened.
Duration	M	Duration of this record in the GGSN.
Cause for Record Closing	M	The reason for the release of record from this GGSN.
Record Sequence Number	C	Partial record sequence number, only present in case of partial records.
Node ID	O	Name of the recording entity.
Record Extensions	O	A set of network operator specific extensions to the record. This includes up to 10 contend-ids in a specific format.
Local Record Sequence Number	O	Consecutive record number created by this node. The number is allocated sequentially including all CDR types.
Charging Characteristics	C	The Charging Characteristics flag retrieved from subscriber's data as described in TS 32.015 sub clause 6.1.6.5.

Notes:

- custom2 dictionary is license dependant.
- Only Single LOTV container is supported.
- Binary IP addresses are supported.
- Record Extension supports Nortel Content Based Billing V3. 10 content-ids per eG-CDR.
- Both QoS requested and negotiated fields present.
- Release the eG-CDR after traffic for 10th content-id is seen.
- Only single LOTV container is supported.
- RAT change will result in eG-CDR being generated with reason as cause for record closing as “MGMT INTERVENTION”.
- If online charging is in use, in case of OCS (Online Charging System) failure, if Failure handling is set to “continue” then Change condition of LOTV is set to “QoS change”.

custom3 Dictionary

eG-CDR fields for TS 32.015 v 3.6.0 (R99).

Field	Category	Description
Record Type	M	GPRS GGSN PDP context record.
Network Initiated PDP Context	C	Present if this is a network-initiated PDP context.
Served IMSI	M	IMSI of the served party (if Anonymous Access Indicator is FALSE or not supplied).
Served MSISDN	O	The primary MSISDN of the subscriber.

Field	Category	Description
GGSN Address	M	The IP address of the GGSN used.
Charging ID	M	PDP context identifier used to identify this PDP context in different records created by GSNs.
SGSN Address	M	List of SGSN addresses used during this record.
Access Point Name Network Identifier	M	The logical name of the connected access point to the external packet data network (network identifier part of APN).
APN Selection Mode	O	An index indicating how the APN was selected.
PDP Type	M	PDP type, i.e. IP, PPP, or IHOSS:OSP.
Served PDP Address	M	PDP address, i.e. IPv4 or IPv6 address.
Dynamic Address Flag	C	Indicates whether served PDP address is dynamic, which is allocated during PDP context activation.
List of Traffic Data Volumes	M	A list of changes in charging conditions for this PDP context, each time stamped. Charging conditions are used to categorize traffic volumes, such as per tariff period. Initial and subsequently changed QoS and corresponding data values are listed. In GSM, data volumes are in octets above the GTP layer and are separated for uplink and downlink traffic. In 3G, data volumes are in octets above the GTP-U layer and are separated for uplink and downlink traffic. ***Important:*** Only one LOTV container per eG-CDR.
Record Opening Time	M	Time stamp when this record was opened.
Duration	M	Duration of this record in the GGSN.
Cause for Record Closing	M	The reason for the release of record from this GGSN.
Record Sequence Number	C	Partial record sequence number, only present in case of partial records.
Node ID	O	Name of the recording entity.
Local Record Sequence Number	O	Consecutive record number created by this node. The number is allocated sequentially including all CDR types.
Charging Characteristics	C	The Charging Characteristics flag retrieved from subscriber's data as described in TS 32.015 sub clause 6.1.6.5.

Notes:

- Only Single LOTV container is supported.
- Supports R99 QoS only.

custom4 Dictionary

eG-CDR fields for TS 32.015 v 3.6.0 (R99).

Field	Category	Description
Record Type	M	GPRS GGSN PDP context record.
Network Initiated PDP Context	C	Present if this is a network-initiated PDP context.
Served IMSI	M	IMSI of the served party (if Anonymous Access Indicator is FALSE or not supplied).
Served MSISDN	O	The primary MSISDN of the subscriber.
GGSN Address	M	The IP address of the GGSN used.
Charging ID	M	PDP context identifier used to identify this PDP context in different records created by GSNs.
SGSN Address	M	List of SGSN addresses used during this record.
Access Point Name Network Identifier	M	The logical name of the connected access point to the external packet data network (network identifier part of APN).
APN Selection Mode	O	An index indicating how the APN was selected.
PDP Type	M	PDP type, i.e. IP, PPP, or IHOSS:OSP.
Served PDP Address	M	PDP address, i.e. IPv4 or IPv6 address.
Dynamic Address Flag	C	Indicates whether served PDP address is dynamic, which is allocated during PDP context activation.
List of Traffic Data Volumes	M	A list of changes in charging conditions for this PDP context, each time-stamped. Charging conditions are used to categorize traffic volumes, such as per tariff period. Initial and subsequently changed QoS and corresponding data values are listed. In GSM, data volumes are in octets above the GTP layer and are separated for uplink and downlink traffic. In 3G, data volumes are in octets above the GTP-U layer and are separated for uplink and downlink traffic. ***Important:*** Only one LOTV container per eG-CDR.
Record Opening Time	M	Time stamp when this record was opened.
Duration	M	Duration of this record in the GGSN.
Cause for Record Closing	M	The reason for the release of record from this GGSN.
Diagnostics	O	A more detailed reason for the release of the connection.
Record Sequence Number	C	Partial record sequence number, only present in case of partial records.
Node ID	O	Name of the recording entity.
Record Extensions	O	A set of network/manufacturer specific extensions to the record.

Field	Category	Description
Local Record Sequence Number	O	Consecutive record number created by this node. The number is allocated sequentially including all CDR types.
Charging Characteristics	C	The Charging Characteristics flag retrieved from subscriber's data as described in TS 32.015 sub clause 6.1.6.5.

Notes:

- Only Single LOTV container is supported.
- Data Record Format Version IE contains 0x1307 instead of 0x1308.
- QoSRequested is not present in the LoTV containers.
- QoSNegotiated is added only for first container and container after QoSChange condition.
- Single LOTV container is supported.
- Supports R99 QoS only.

custom5 and custom9 Dictionaries

eG-CDR fields for TS 32.298 v 6.5.0 (R6) (with customer specific changes).

Field	Category	Description
Record Type	M	GGSN PDP context record (EGSNPDPRECORD).
Network Initiated PDP Context	OC	A flag that is present if this is a network-initiated PDP context.
Served IMSI	M	IMSI of the served party.
GGSN Address Used	M	The control plane IP address of the GGSN used.
GGSN IPv4 Binary Address	M	
Charging ID	M	PDP context identifier used to identify this PDP context in different records created by GSNs.
SGSN Address	M	List of SGSN addresses used during this record.
SGSN IPv4 Binary Address	M	
Access Point Name Network Identifier	OM	The logical name of the connected access point to the external packet data network (network identifier part of APN).
PDP Type	OM	PDP type, i.e. IP, PPP, or IHOSS:OSP.
Served PDP Address	OC	PDP address, i.e. IPv4 or IPv6. This parameter shall be present except when both the PDP type is PPP and dynamic PDP address assignment is used.
Dynamic Address Flag	OC	Indicates whether served PDP address is dynamic, which is allocated during PDP context activation. This field is missing if address is static.

Field	Category	Description
List of Traffic Data Volumes	OM	A list of changes in charging conditions for this PDP context, each change is time stamped. Charging conditions are used to categorize traffic volumes, such as per tariff period. Initial and subsequently changed QoS and corresponding data values are also listed.
QoS Requested (not in G-CDR)	N/A	
QoS Negotiated	O	QoS Negotiated indicates the applied QoS accepted by the network.
Data Volume Uplink	M	Number of octets in uplink direction
Data Volume Downlink	M	Number of octets in downlink direction
Change Condition	M	The change condition that resulted in this LOTV container.
Change Time	M	Timestamp at change
Failurehandling Continue	O	Boolean indicating offline charging enabled
APN Selection Mode	OM	An index indicating how the APN was selected.
Served MSISDN	OM	The primary MSISDN of the subscriber.
Charging Characteristics	M	The Charging Characteristics applied to the PDP context.
Charging Characteristics Selection Mode	OM	Holds information about how Charging Characteristics were selected.
SGSN PLMN Identifier	OM	SGSN PLMN Identifier (MCC and MNC) used during this record.
Served IMEISV	OC	IMEISV of the ME, if available.
RAT Type	OC	This field indicates the Radio Access Technology (RAT) type currently used by the Mobile Station as defined in TS 29.060. The field is present in the G-CDR if provided by SGSN.
MS Time Zone	OC	This field contains the MS Time Zone the MS is currently located as defined in TS 29.060, if provided by SGSN.
User Location Information	OC	This field contains the User Location Information of the MS as defined in TS 29.060, if provided by SGSN.
List of Service Data Volumes	OC	A list of the changes that occurred in charging conditions for all service data flows for the PDP context.
Rating group	M	This is the service flow identity and has to be used for differentiated evaluation of user's traffic. This is also known as content-id.
Charging Rulebase name	M	The name of the Rulebase used for charging This is the group name of charging rules.
Result Code	O	The result code AVP This contains the result code after the interconnection with the CRF.
Local Sequence number	M	A per service data container sequence number. It starts from 1 for each service, increasing by 1 for each service date container generated for that service within the lifetime of this PDP session.

Field	Category	Description
Time of first usage	M	The time stamp for the first IP packet to be transmitted for the service data flow referred to the current instance of Service Condition Change.
Time of last usage	M	The time stamp for the last IP packet to be transmitted for the service data flow referred to the current instance of Service Condition Change.
Usage time	M	The difference between "time of first usage" and "time of last usage".
Service condition change	M	The reason for closing the service data container for triggers like SGSN change, QoS change, Rat change, time and volume triggers, etc.
QoS negotiated	O	The negotiated QoS applied for the service data flow.
sgsn-Address	M	The valid SGSN IP address during the service data recording interval.
SGSN-IPv4-Binary Address	M	
SGSN PLMN identifier	O	The valid SGSN PLMN ID during the service data recording interval.
FBC Data volume uplink	M	The number of octets transmitted during the use of the packet data services in the uplink direction.
FBC data volume downlink	M	The number of octets transmitted during the use of the packet data services in the downlink direction.
Time of report	M	A time stamp defining the moment when the service data container is closed.
RAT Type	O	The valid radio access technology type during the service data recording interval.
Failurehandling Continue	O	A Boolean expression included if the failure handling condition has been executed.

Notes:

- A maximum of eight LOTV containers and 255 LOSDV containers supported per eG-CDR.
- QoSRequested is not present in the LoTV containers.
- QoSNegotiated is added only for first container and container after QoSChange condition.
- Failure handling continue included in LOTV container.
- Service Identifier *NOT* included in LOSDV.
- Service change condition is encoded as 32 bits.

custom6 – custom8, custom14, custom15, custom17, custom20 Dictionaries

eG-CDR fields for TS 32.298 v 6.5.0 (R6).

Field	Category	Description
Record Type	M	GGSN PDP context record (EGSNPDPRECORD).
Network initiated PDP context	OC	A flag that is present if this is a network-initiated PDP context.

Field	Category	Description
Served IMSI	M	IMSI of the served party.
Served IMEISV	OC	IMEISV of the ME, if available.
GGSN Address	M	The control plane IP address of the GGSN used.
Charging ID	M	PDP context identifier used to identify this PDP context in different records created by GSNs.
SGSN Address	M	List of SGSN addresses used during this record.
Access Point Name Network Identifier	OM	The logical name of the connected access point to the external packet data network (network identifier part of APN).
PDP Type	OM	PDP type, i.e. IP, PPP, or IHOSS:OSP.
Served PDP Address	OC	PDP address, i.e. IPv4 or IPv6. This parameter shall be present except when both the PDP type is PPP and dynamic PDP address assignment is used.
Dynamic Address Flag	OC	Indicates whether served PDP address is dynamic, which is allocated during PDP context activation. This field is missing if address is static.
List of Traffic Data Volumes	OM	A list of changes in charging conditions for this PDP context, each change is time stamped. Charging conditions are used to categorize traffic volumes, such as per tariff period. Initial and subsequently changed QoS and corresponding data values are also listed.
Record Opening Time	M	Time stamp when PDP context is activated in this GGSN or record opening time on subsequent partial records.
MS Time Zone	OC	This field contains the MS Time Zone the MS is currently located as defined in TS 29.060, if provided by SGSN.
Duration	M	Duration of this record in the GGSN.
Cause for Record Closing	M	The reason for the release of record from this GGSN.
Record Sequence Number	C	Partial record sequence number, only present in case of partial records.
Node ID	OM	Name of the recording entity.
Local Record Sequence Number	OM	Consecutive record number created by this node. The number is allocated sequentially including all CDR types.
APN Selection Mode	OM	An index indicating how the APN was selected.
Served MSISDN	OM	The primary MSISDN of the subscriber.
User Location Information	OC	This field contains the User Location Information of the MS as defined in TS 29.060, if provided by SGSN.
Charging Characteristics	M	The Charging Characteristics applied to the PDP context.
Charging Characteristics Selection Mode	OM	Holds information about how Charging Characteristics were selected.
SGSN PLMN Identifier	OM	SGSN PLMN Identifier (MCC and MNC) used during this record.

Field	Category	Description
RAT Type	OC	This field indicates the Radio Access Technology (RAT) type currently used by the Mobile Station as defined in TS 29.060. The field is present in the G-CDR if provided by SGSN.
List of Service Data Volumes	OC	A list of the changes that occurred in charging conditions for all service data flows for the PDP context

Notes:

- A maximum of eight LOTV containers and 10 LOSDV containers supported per eG-CDR.
- QoSRequested is not present in the LoTV containers.
- QoSNegotiated is added only for first container and container after QoSChange condition.
- Failure handling continue included in LOTV container.
- Service change condition is encoded as 21 bits (with 3 bits padding — 24 bits for 8 bit boundary).
- Service-identifier level support available (Service Identifier will be included in LOSDV container if configured in corresponding charging-action).
- custom7, custom15, and custom17 dictionaries: Same as custom6 GTPP dictionary.
- custom8 dictionary: Same as custom6 and custom7 GTPP dictionaries except that the beginning of the eG-CDR is encoded as “0xbc” (binary - 10111100 which is 28) instead of “0xb5” (binary - 10110101 which is 21). The last 5 bits here identify the record type which is tag value of 28 for EGSNPDPRecord.
- custom14 dictionary: Same as custom6 GTPP dictionary with TEXT represented IP addresses.
- custom20 dictionary:
  - CallEventRecordChoiceID value changed to 28 as per customer requirement.
  - ChargingRuleBaseName not included in LOSDV container.
  - Suppression of IE “networkInitiation” in EGSNPDPRECORD.
  - Suppression of IE “diagnostics” attribute in EGSNPDPRECORD.
  - Suppression of IE “failureHandlingContinue” from LOTV. (If Failure handling takes place, changeCondition in LOTV will be Failure Handling Continue.)
  - “managementIntervention” IE value of 20 changed to 100 as per customer requirement.
  - “pLMNChange” IE for CauseForRecClosing handled separately with a value of 101.

List of Traffic Data Volumes

List of Traffic Data Volumes		
QoS Requested (not in G-CDR)	N/A	
QoS Negotiated	O	QoS Negotiated indicates the applied QoS accepted by the network.
Data Volume Uplink	M	Number of octets in uplink direction.
Data Volume Downlink	M	Number of octets in downlink direction.
Change Condition	M	The change condition that resulted in this LOTV container.
Change Time	M	Timestamp at change.

List of Traffic Data Volumes		
Failurehandling Continue (only in eG-CDRs)	O	Boolean indicating offline charging enabled.

List of Service Data Volumes

List of Service Data Volumes		
Rating group	M	This is the service flow identity and has to be used for differentiated evaluation of user's traffic. Also known as content-id.
Charging Rulebase name	M	The name of the Rulebase used for charging. This is the group name of charging rules.
Result Code	O	The result code AVP. This contains the result code after the interconnection with the CRF.
Local Sequence number	M	A per service data container sequence number. It starts from 1 for each service, increasing by 1 for each service date container generated for that service within the lifetime of this PDP session.
Time of first usage	M	The time stamp for the first IP packet to be transmitted for the service data flow referred to the current instance of Service Condition Change.
Time of last usage	M	The time stamp for the last IP packet to be transmitted for the service data flow referred to the current instance of Service Condition Change.
Usage time	M	The difference between "time of first usage" and "time of last usage".
Service condition change	M	The reason for closing the service data container for triggers like SGSN change, QoS change, RAT change, time and volume triggers, etc.
QoS negotiated	O	The negotiated QoS applied for the service data flow.
sgsn-Address	M	The valid SGSN IP address during the service data recording interval.
SGSN PLMN identifier	O	The valid SGSN PLMN ID during the service data recording interval.
FBC Data volume uplink	M	The number of octets transmitted during the use of the packet data services in the uplink direction.
FBC data volume downlink	M	The number of octets transmitted during the use of the packet data services in the downlink direction.
Time of report	M	A time stamp defining the moment when the service data container is closed.
RAT Type	O	The valid RAT type during the service data recording interval.
Failurehandling Continue	O	A Boolean expression included if the failure handling condition has been executed.
Service Identifier	O	The service identifier may designate an end user service, a part of an end user service or an arbitrarily formed group thereof.

standard and custom10 Dictionaries

eG-CDR fields for TS 32.215 v 4.6.0 (R4).

Field	Category	Description
Record Type	M	GPRS GGSN PDP context record.
Network initiated PDP context	C	Present if this is a network-initiated PDP context.
Served IMSI	M	IMSI of the served party (if Anonymous Access Indicator is FALSE or not supplied).
Served MSISDN	O	The primary MSISDN of the subscriber.
GGSN Address	M	The IP address of the GGSN used.
Charging ID	M	PDP context identifier used to identify this PDP context in different records created by GSNs.
SGSN Address	M	List of SGSN addresses used during this record.
Access Point Name Network Identifier	M	The logical name of the connected access point to the external packet data network (network identifier part of APN).
APN Selection Mode	O	An index indicating how the APN was selected.
PDP Type	M	PDP type, i.e. IP, PPP, or IHOSS:OSP.
Served PDP Address	M	PDP address, i.e. IPv4 or IPv6 address.
Dynamic Address Flag	C	Indicates whether served PDP address is dynamic, which is allocated during PDP context activation.
List of Traffic Data Volumes	M	A list of changes in charging conditions for this PDP context, each time stamped. Charging conditions are used to categorize traffic volumes, such as per tariff period. Initial and subsequently changed QoS and corresponding data values are listed. In GSM, data volumes are in octets above the GTP layer and are separated for uplink and downlink traffic. In 3G, data volumes are in octets above the GTP-U layer and are separated for uplink and downlink traffic. ***Important:*** Only one LOTV container per eG-CDR.
Record Opening Time	M	Time stamp when this record was opened.
Duration	M	Duration of this record in the GGSN.
Cause for Record Closing	M	The reason for the release of record from this GGSN.
Record Sequence Number	C	Partial record sequence number, only present in case of partial records.
Node ID	O	Name of the recording entity.
Local Record Sequence Number	O	Consecutive record number created by this node. The number is allocated sequentially including all CDR types.

Field	Category	Description
Charging Characteristics	C	The Charging Characteristics flag retrieved from subscriber's data as described in TS 32.015 sub clause 6.1.6.5.

custom12 and custom19 Dictionaries

eG-CDR fields for TS 32.298 v7.4.0 (R7).

Field	Category	Description
Record Type	M	GGSN PDP context record (EGSNPDPRECORD)
Network initiated PDP context	OC	A flag that is present if this is a network-initiated PDP context.
Served IMSI	M	IMSI of the served party.
GGSN Address	M	The control plane IP address of the GGSN used.
Charging ID	M	PDP context identifier used to identify this PDP context in different records created by GSNs.
SGSN Address	M	List of SGSN addresses used during this record.
Access Point Name Network Identifier	OM	The logical name of the connected access point to the external packet data network (network identifier part of APN).
PDP Type	OM	PDP type, i.e. IP, PPP, or IHOSS:OSP.
Served PDP Address	OC	PDP address, i.e. IPv4 or IPv6. This parameter shall be present except when both the PDP type is PPP and dynamic PDP address assignment is used.
Dynamic Address Flag	OC	Indicates whether served PDP address is dynamic, which is allocated during PDP context activation. This field is missing if address is static.
List of Traffic Data Volumes	OM	A list of changes in charging conditions for this PDP context, each change is time stamped. Charging conditions are used to categorize traffic volumes, such as per tariff period. Initial and subsequently changed QoS and corresponding data values are also listed.
Record Opening Time	M	Time stamp when PDP context is activated in this GGSN or record opening time on subsequent partial records.
Duration	M	Duration of this record in the GGSN.
Cause for Record Closing	M	The reason for the release of record from this GGSN.
Diagnostics	O	A more detailed reason for the release of the connection.
Record Sequence Number	C	Partial record sequence number, only present in case of partial records.
Node ID	OM	Name of the recording entity.
Record Extensions	O	A set of network operator specific extensions to the record.
Local Record Sequence Number	OM	Consecutive record number created by this node. The number is allocated sequentially including all CDR types.

Field	Category	Description
APN Selection Mode	OM	An index indicating how the APN was selected.
Served MSISDN	OM	The primary MSISDN of the subscriber.
Charging Characteristics	M	The Charging Characteristics applied to the PDP context.
Charging Characteristics Selection Mode	OM	Holds information about how Charging Characteristics were selected.
SGSN PLMN Identifier	OM	SGSN PLMN Identifier (MCC and MNC) used during this record.
Served IMEISV	OC	IMEISV of the ME, if available.
RAT Type	OC	This field indicates the Radio Access Technology (RAT) type currently used by the Mobile Station as defined in TS 29.060. The field is present in the G-CDR if provided by SGSN.
MS Time Zone	OC	This field contains the MS Time Zone the MS is currently located as defined in TS 29.060, if provided by SGSN.
User Location Information	OC	This field contains the User Location Information of the MS as defined in TS 29.060, if provided by SGSN.
List of Service Data Volumes	OC	A list of the changes that occurred in charging conditions for all service data flows for the PDP context.

List of Traffic Data Volumes

List of Traffic Data Volumes		
QoS Requested (not in G-CDR)	N/A	
QoS Negotiated	O	QoS Negotiated indicates the applied QoS accepted by the network.
Data Volume Uplink	M	Number of octets in uplink direction.
Data Volume Downlink	M	Number of octets in downlink direction.
Change Condition	M	The change condition that resulted in this LOTV container.
Change Time	M	Timestamp at change.
Failurehandling Continue (only in eG-CDRs)	O	Boolean indicating offline charging enabled.
UserLocationInformation	O	This field contains the User Location Information of the MS.

Notes:

- LOTV related changes:
  - A new IE is included for LOTV container i.e. User location information.
  - The list of traffic data volumes now supports RAI and CGI/SAI changes, i.e. whenever RAI and/or CGI/SAI changes are detected; it will result in a “List of Traffic Data Volumes” container being added to the CDR, if location reporting is required and a report of CGI/SAI change is received.

List of Service Data Volumes

List of Service Data Volumes		
Rating group	M	This is the service flow identity and has to be used for differentiated evaluation of user's traffic. Also known as content-id.
Charging Rulebase name	M	The name of the Rulebase used for charging This is the group name of charging rules.
Result Code	O	The result code AVP This contains the result code after the interconnection with the CRF.
Local Sequence number	M	A per service data container sequence number. It starts from 1 for each service, increasing by 1 for each service date container generated for that service within the lifetime of this PDP session.
Time of first usage	M	The time stamp for the first IP packet to be transmitted for the service data flow referred to the current instance of Service Condition Change.
Time of last usage	M	The time stamp for the last IP packet to be transmitted for the service data flow referred to the current instance of Service Condition Change.
Usage time	M	The difference between "time of first usage" and "time of last usage".
Service condition change	M	The reason for closing the service data container for triggers like SGSN change, QoS change, RAT change, time and volume triggers, etc.
QoS negotiated	O	The negotiated QoS applied for the service data flow.
sgsn-Address	M	The valid SGSN IP address during the service data recording interval.
SGSN PLMN identifier	O	The valid SGSN PLMN ID during the service data recording interval.
FBC Data volume uplink	M	The number of octets transmitted during the use of the packet data services in the uplink direction.
FBC data volume downlink	M	The number of octets transmitted during the use of the packet data services in the downlink direction.
Time of report	M	A time stamp defining the moment when the service data container is closed.
RAT Type	O	The valid RAT type during the service data recording interval.
Failurehandling Continue	O	A Boolean expression included if the failure handling condition has been executed.
Service Identifier	O	The service identifier may designate an end user service, a part of an end user service or an arbitrarily formed group thereof.

Notes:

LOSDV related changes:

- Time Quota mechanism: Contains two further subfields and is included if envelope reporting is required:
  - Time Quota Type identifies the mechanism by which time-based usage should be reported — as defined in TS 32.299.
  - Base Time Interval identifies the length of the base time interval, for controlling the reporting of time-based usage, in seconds.
- User location information will be included in the LOSDV container in the R7 eG-CDRs.

- The “Service Change Condition” cause changes are as follows:
  - Time limit eG-CDRs where the corresponding service change condition now has been changed to “Time Limit”. Earlier there was no specific service change condition and instead “Time Exhausted” was used.
  - Volume limit eG-CDRs where the corresponding service change condition now has been changed to “Volume Limit”. Earlier there was no specific service change condition and instead “Volume Exhausted” was used.
  - eG-CDRs that are generated as a result of MS-TimeZone change will have service change condition as “Record closure”.
- custom12 and custom19 dictionaries have Rel. 7 related changes. However, custom12 also contains few customer-specific items that are not part of plain Rel. 7 features. For example, dataVolumeTotal field in LOSDV container.

custom21 Dictionary

eG-CDR fields for TS 32.215 v 4.5.0 (R4).

Field	Category	Description
Record Type	M	GPRS GGSN PDP context record.
Network initiated PDP context	C	Present if this is a network-initiated PDP context.
Served IMSI	M	IMSI of the served party (if Anonymous Access Indicator is FALSE or not supplied).
GGSN Address	M	The IP address of the GGSN used.
Charging ID	M	PDP context identifier used to identify this PDP context in different records created by GSNs.
SGSN Address	M	List of SGSN addresses used during this record.
Access Point Name Network Identifier	M	The logical name of the connected access point to the external packet data network (network identifier part of APN).
PDP Type	M	PDP type, i.e. IP, PPP, or IHOSS:OSP.
Served PDP Address	M	PDP address, i.e. IPv4 or IPv6 address.
Dynamic Address Flag	C	Indicates whether served PDP address is dynamic, which is allocated during PDP context activation.
List of Traffic Data Volumes	M	A list of changes in charging conditions for this PDP context, each time stamped. Charging conditions are used to categorize traffic volumes, such as per tariff period. Initial and subsequently changed QoS and corresponding data values are listed. In GSM, data volumes are in octets above the GTP layer and are separated for uplink and downlink traffic. In 3G, data volumes are in octets above the GTP-U layer and are separated for uplink and downlink traffic.
Record Opening Time	M	Time stamp when this record was opened.
Duration	M	Duration of this record in the GGSN.

Field	Category	Description
Cause for Record Closing	M	The reason for the release of record from this GGSN.
Diagnostics	M	A more detailed reason for the release of the connection.
Record Sequence Number	C	Partial record sequence number, only present in case of partial records.
Node ID	O	Name of the recording entity.
Record Extensions	O	A set of network operator specific extensions to the record.
Local Record Sequence Number	O	Consecutive record number created by this node. The number is allocated sequentially including all CDR types.
APN Selection Mode	O	An index indicating how the APN was selected.
Served MSISDN	O	The primary MSISDN of the subscriber.
Charging Characteristics	C	The Charging Characteristics flag retrieved from subscriber's data.
Charging Characteristics Selection mode	O	Holds information about how Charging Characteristics were selected.
SGSN PLMN Identifier	OM	SGSN PLMN Identifier (MCC and MNC) used during this record.

Notes:

- custom21 GTPP dictionary contains customer-specific changes. Including:
  - Support for Multiple LOTV containers.
  - Support for SGSN address list overflow.
  - Support for 10 digit service code.

custom27 Dictionary

eG-CDR fields based on 3GPP TS 32.298 V6.6.0 (2006-12) (R6).

Field	Category	Description
sgsnPDPRecord	M	Record field contains the items that may be present in an S-CDR.
Record Type	M	SGSN/GGSN PDP context record.
Served IMSI	M	IMSI of the served party.
Served IMEI	OC	IMEI of the ME, if available in the SGSN.
SGSN Address	M	The control plane IP address of the SGSN used.
MS Network Capability	OC	MS network capability value of the MS network capability information element of the served MS on PDP context activation
Routing Area	OC	Contains the RA code of the area where the MS is located when the (partial) record is opened.

Field	Category	Description
Location Area Code	OC	Contains the Location Area Code of the area where the MS is located when the (partial) record is opened.
Cell Identifier	OC	Contains the CI (GSM) or the SAC (WCDMA) of the cell where the MS is located when the S-CDR is opened. The first partial or single S-CDR reports the current cell identifier at PDP context activation. For any subsequent partial S-CDRs, the accuracy of the reported cell identifier is limited to the cell identifier for the last RA update reported by the MS.
Charging ID	M	PDP context identifier used to identify this PDP context in different records created by GSNs.
GGSN Address	M	List of GGSN addresses used during this record.
Access Point Name Network Identifier	OM	The logical name of the connected access point to the external packet data network (network identifier part of APN).
PDP Type	OM	PDP type, i.e. IP, PPP, or IHOSS:OSP.
Served PDP Address	OC	PDP address, i.e. IPv4 or IPv6 address. This parameter shall be present except when both the PDP type is PPP and dynamic PDP address assignment is used.
List of Traffic Data Volumes	OC	A list of changes in charging conditions for this PDP context, each time stamped. Charging conditions are used to categorize traffic volumes, such as per tariff period. Initial and subsequently changed QoS and corresponding data values are also listed.
Record Opening Time	M	Time stamp when PDP context is activated in this GGSN or record opening time on subsequent partial records.
Duration	M	Duration of this record in the GGSN.
SGSN Change	OC	Indicate that this is the first record after an inter-SGSN routing area update in new SGSN and an intra-SGSN inter-system change.
Cause for Record Closing	M	The reason for the release of record from this SGSN.
Diagnostics	OM	A more detailed reason for the release of the connection.
Record Sequence Number	C	Partial record sequence number, only present in case of partial records.
Node ID	OM	Name of the recording entity.
Local Record Sequence Number	OM	Consecutive record number created by this node. The number is allocated sequentially including all CDR types.
APN Selection Mode Index	OM	Defines in which PLMN GPRS backbone the GGSN is located. The last label must be "gprs". The first and second labels together uniquely identify the GPRS PLMN.
Served MSISDN	OM	The primary MSISDN of the subscriber.
Charging Characteristics	M	The Charging Characteristics flag retrieved from subscriber's data as described in TS 32.015 sub clause 6.1.6.5.
System Type	OC	Indicates the use of a 3G air interface for the provisioning of service recorded by this CDR. In case service is provided by a GSM air interface, the field is not present.
CAMEL Information	OC	Set of CAMEL information related to PDP context. This field is present if CAMEL Charging Information is received by the GGSN in the GTP Create PDP context request.

Field	Category	Description
Charging Characteristics Selection Mode	OM	Holds information about how Charging Characteristics were selected.
Dynamic Address Flag	OC	Indicates whether served PDP address is dynamic, which is allocated during PDP context activation.
PLMN Identifier	OM	Indicates the PLMN Identifier (MCC and MNC) used during this record.

Notes:

- QoSRequested is not present in the LoTV containers.
- QoSNegotiated is added only for first container and container after QoSChange condition.

custom30 Dictionary

Enhanced G-CDR fields based on 3GPP TS 32.298 V6.4.1 (2006-12) (R6).

Field	Category	Description
Record Type	M	GPRS GGSN PDP context record.
Served IMSI	M	IMSI of the served party (if Anonymous Access Indicator is FALSE or not supplied).
GGSN Address	M	The IP address of the GGSN used.
Charging ID	M	PDP context identifier used to identify this PDP context in different records created by GSNs.
SGSN Address	M	List of SGSN addresses used during this record.
Access Point Name Network Identifier	M	The logical name of the connected access point to the external packet data network (network identifier part of APN).
PDP Type	M	PDP type, i.e. IP, PPP, or IHOSS:OSP
Served PDP Address	M	PDP address, i.e. IPv4 or IPv6 address.
Dynamic Address Flag	C	Indicates whether served PDP address is dynamic, which is allocated during PDP context activation.
List of Traffic Data Volumes	M	A list of changes in charging conditions for this PDP context, each time stamped. Charging conditions are used to categorize traffic volumes, such as per tariff period. Initial and subsequently changed QoS and corresponding data values are also listed. In GSM, data volumes are in octets above the GTP layer and are separated for uplink and downlink traffic. In 3G, data volumes are in octets above the GTP-U layer and are separated for uplink and downlink traffic.
Record Opening Time	M	Time stamp when this record was opened.
Duration	M	Duration of this record in the GGSN.
Cause for Record Closing	M	The reason for the release of record from this GGSN.

Field	Category	Description
Record Sequence Number	C	Partial record sequence number, only present in case of partial records.
Node ID	O	Name of the recording entity.
Local Record Sequence Number	O	Consecutive record number created by this node. The number is allocated sequentially including all CDR types.
APN Selection Mode	O	An index indicating how the APN was selected.
Served MSISDN	O	The primary MSISDN of the subscriber.
Charging Characteristics	M	The Charging Characteristics flag retrieved from subscriber's data as described in TS 32.015 sub clause 6.1.6.5.
Charging Characteristics Selection Mode	O	Holds information about how Charging Characteristics were selected.
SGSN PLMN Identifier	O	SGSN PLMN Identifier (MCC and MNC) used during this record.
Served IMEISV	O	IMEISV of the ME, if available.
RAT Type	O	This field indicates the Radio Access Technology (RAT) type currently used by the Mobile Station as defined in TS 29.060. The field is present in the G-CDR if provided by SGSN.
MS Time Zone	O	This field contains the MS Time Zone the MS is currently located as defined in TS 29.060, if provided by SGSN.
User Location Information	O	This field contains the User Location Information of the MS as defined in TS 29.060, if provided by SGSN.
List of Service Data Volumes	O	A list of the changes that occurred in charging conditions for all service data flows for the PDP context.

Notes:

- “Record Extensions” is not present in this version.
- “External Charging Identifier” is not present in this version.
- “CAMEL Information” is not present in this version.

custom33 Dictionary

Enhanced G-CDR fields based on 3GPP TS 32.298 V6.5.0 (R6).

Field	Category	Description
Record Type	M	This field identifies the type of the record.
Network initiated PDP context	O	This field indicates that the PDP context was network initiated. The field is missing in case of mobile activated PDP context. Set to TRUE (0xFF) if PDP context was initiated from network side.

Field	Category	Description
Served IMSI	M	This field contains IMSI of the served party (if Anonymous Access Indicator is FALSE or not supplied).
GGSN Address	M	This field provides the current serving GGSN IP address for the Control Plane. The standard 32.298 offers a choice for the encoding of the address to be either in binary or text format. The GGSN encodes the address in binary format. Indefinite length encoding is used for this field.
Charging ID	M	This field is a charging identifier, which can be used together with the GGSN address to identify all records produced in the GGSN involved in a single PDP context. The Charging ID is generated by the GGSN at PDP context activation and is transferred to the context requesting SGSN. At an inter-SGSN routing area update the charging ID is transferred to the new SGSN as part of each active PDP context.
List of SGSN Addresses	M	List of SGSN addresses used during this record. This field contains 1–5 SGSN IP addresses (max. 4 SGSN changes). A CDR is closed as a partial with Cause for Record Closing set to SGSN Change when the maximum number of changes has been recorded. Subsequent SGSN changes will be listed in the next partial. Indefinite length encoding is used for this field.
Access Point Name Network Identifier	M	This field contain the Network Identifier part of the Access Point Name (APN). It is provided by the SGSN in the Create PDP Context Request message. In case of a configured virtual APN, the virtual APN is included instead, unless this is overridden by the CLI command "**`gcdr apn-name-to-be-included {gn | virtual}`**"
PDP Type	M	This field identifies the PDP type, i.e. IP, PPP, or IHOSS:OSP
Served PDP Address	O	This field contains the PDP address of the served IMSI, for which the standard 3GPP TS 32.298 allows a choice of either IP address or ETSIAddress. Indefinite length encoding is used for this field.
Dynamic Address Flag	O	This field indicates that the PDP address has been dynamically allocated for that particular PDP context. This field is missing if address is static i.e. part of PDP context subscription.
Record Opening Time	M	This field contains the time stamp when PDP context is activated in GGSN or when a subsequent record is opened after a partial record.
Duration	M	This field contains the relevant duration in seconds for PDP contexts with range of 0...4294967295 (2^32-1). It is the duration from Record Opening Time to record closure. For partial records this is the duration of the individual partial record and not the cumulative duration.
Cause for Record Closing	M	This field contains a reason for the release of record from this GGSN.
Record Sequence Number	O	This field contains a running sequence number with range 1...4294967295 used to link partial records generated by the GGSN for a specific PDP context (characterized with the same Charging ID and GGSN address pair). This field is always present in this case.
Node ID	M	This field contains an identifier string for the node that had generated the CDR.
Local Record Sequence Number	M	For each Node ID, this number with range 1...4294967295 is allocated sequentially for each CDR. This along with a Node ID uniquely identifies a CDR.
APN Selection Mode	M	An index indicating how the APN was selected.

Field	Category	Description
Served MSISDN	M	The field tracks the Mobile Station (MS) ISDN number (MSISDN) of the subscriber which is a part of Create PDP Context Request message.
Charging Characteristics	M	Lists the charging characteristics applied to the PDP context. The GGSN can accept charging characteristics from the SGSN or AAA or use its own configured value. GGSN configured charging characteristics are specified as part of the GGSN Service and are applied for G-CDRs to subscriber PDP contexts through APN templates.
Charging Characteristics Selection Mode	O	The charging characteristic type that the GGSN applied to the CDR.
SGSN PLMN Identifier	O	RAI (optionally supplied by SGSN in the GTP create PDP context request) is used as SGSN PLMN Identifier value. It is omitted if the SGSN does not supply the RAI and is not identified as a "home" SGSN. For home SGSNs without the RAI a locally configured PLMN-ID can be sent instead.
Served IMEISV	O	The International Mobile Equipment Identity and Software Version Number (IMEISV) of the MS, if available.
RAT Type	O	This field indicates the Radio Access Technology (RAT) type currently used by the Mobile Station as defined in TS 29.060. The field is present in the CDR if provided by SGSN.
MS Time Zone	O	The "Time Zone" IE that the SGSN may provide to the GGSN during the PDP context activation/modification procedure.
User Location Information	O	The User Location Information for the MS if provided by the SGSN to the GGSN during the PDP context activation/modification procedure. Transparently copied from the PDP context request
List of Service Data Volumes	O	A list of the changes that occurred in charging conditions for all service data flows for the PDP context. Indefinite length encoding is used for this field.

Notes:

- For custom33 dictionary, eG-CDR will always have LOSDV even if no data has been passed for the entire life time of the call.

List of Service Data Volumes

List of Service Data Volumes		
Service Data Volume Block	O	A list of the changes that occurred in charging conditions for all service data flows for the PDP context. Indefinite length encoding is used for this field.
Rating group	M	This is the service flow identity and has to be used for differentiated evaluation of user's traffic. Also known as content-id. Default: 403
Result Code	O	The result code AVP contains the result code after the interconnection with the Diameter server. The Diameter server sends result-codes for each of the content-id for which quota is requested. The GGSN use this to populate the eG-CDR bucket. This is a mandatory AVP that comes in response for every quota request for a category. Default: 0

List of Service Data Volumes		
Local Sequence number	M	A per service data container sequence number. It starts from 1 for each service, increasing by 1 for each service date container generated for that service within the lifetime of this PDP session. Default: Same as "localRecordSequenceNumber" field of main CDR.
Time of first usage	M	The time stamp for the first IP packet to be transmitted for the service data flow referred to the current instance of Service Condition Change. Default: Same as "Record Opening Time" field of main CDR.
Time of last usage	M	The time stamp for the last IP packet to be transmitted for the service data flow referred to the current instance of Service Condition Change. Default: Same as "Record Opening Time" field of main CDR.
Usage time	M	The difference, in seconds with range 0...4294967295, between “time of first usage” and “time of last usage”. Default: 0
Service condition change	M	The reason for closing the service data container for triggers like SGSN change, QoS change, RAT change, time and volume triggers, etc. Default: Value 4 to be encoded as per 3GPP format. 4 denotes "PDPContextRelease" or normal termination.
QoS negotiated	O	The negotiated QoS applied for the service data flow. Default: Negotiated QoS for the PDP context.
sgsn-Address	M	The valid SGSN IP address during the service data recording interval. Default: Same as “sgsn-address” field of main CDR.
SGSN PLMN identifier	O	RAI (optionally supplied by SGSN in the GTP create PDP context request) is used as SGSN PLMN Identifier value. It is omitted if the SGSN does not supply the RAI and is not identified as a “home” SGSN. For home SGSNs without the RAI a locally configured PLMN-ID can be sent instead. Default: Same as “sgsnPLMNIdentifier” field of main CDR.
FBC Data volume uplink	M	The number of octets transmitted during the use of the packet data services in the uplink direction. Default: 0
FBC data volume downlink	M	The number of octets transmitted during the use of the packet data services in the downlink direction. Default: 0
Time of report	M	A time stamp defining the moment when the service data container is closed. Default: Same as "Record Opening Time" field of main CDR.
RAT Type	O	The valid RAT type during the service data recording interval. Default: Same as “RAT Type" field of main CDR.
Failurehandling Continue	O	A Boolean expression included if the failure handling condition has been executed. This can be either configured on the GGSN using the **`failure-handling`** CLI command in the **`credit-control`** mode or can be received from the server in the **Credit-Control-Failure-Handling** AVP. Whichever is received from the server will have higher precedence. There is no negotiation with the Diameter server in this regard and the GGSN will use whatever the server provides.
Service Identifier	O	The service identifier may designate an end user service, a part of an end user service or an arbitrarily formed group thereof. Content-id and service-id are used as unique key to identify FBC Bucket.

Chapter 8
GGSN CDR Field Descriptions

This chapter describes the CDR fields supported by the system for use in GGSN-CDRs (G-CDRs) and enhanced G-CDRs (eG-CDRs).

The following information is provided for each field:

- **Description:** The field's description.
- **Format:** The field's data format.
- **Length:** The field's size, in bytes.

All G-CDRs and eG-CDRs are encoded using the ASN.1 format and are sent to the charging gateway function (CGF) using the GPRS Tunneling Protocol Prime (GTPP) as defined in the following standards:

- 3GPP TS 29.060
- 3GPP TS 32.015
- 3GPP TS 32.215
- 3GPP TS 32.251
- 3GPP TS 32.298 v 6.2.0 (for G-CDRs)
- 3GPP TS 32.298 v 6.4.1 (for eG-CDRs)

Also see the *Field Reference for CDRs in GGSN* chapter for information on CDR fields supported in G-CDRs and eG-CDRs.

Important: The behavior for several of the fields supported in CDRs can be modified. For more information, refer to the **`gtpp attributes`** command in the *Command Line Interface Reference*.

CDR Fields

Access Point Name Network Identifier

The network identifier portion of the Access Point Name (APN). The APN typically corresponds to a registered Internet domain name and represents the external Packet Data Network (PDN) that the GGSN is connected to.

Format
IA5 string

Length
1–65 bytes

APN Selection Mode

An index indicating how the APN was selected.

The following APN selection mode indexes are possible:

- 0: MS or network provided APN, subscribed verified
- 1: MS provided APN, subscription not verified
- 2: Network provided APN, subscription not verified

Format
Unsigned integer.

Length
1 byte.

CAMEL Information

Set of CAMEL information related to PDP context. This field is present if CAMEL Charging Information is received by the GGSN in the GTP Create PDP context request.

Important: Presently E-GCDRs does not support this field.

Format
Octet string.

Cause for Record Closing

The reason the record is released from the GGSN.

Some of the possible reasons are as follows:

- normalRelease (0): The PDP context was terminated normally through a PDP context release (end of context or SGSN change) or a GPRS detach.

- abnormalRelease (4): The PDP context was abnormally terminated.
- cAMELInitCallRelease (5)
- volumeLimit (16): The PDP context was terminated due to exceeding volume limit.
- timeLimit (17): The PDP context was terminated due to exceeding time limit.
- sGSNChange (18): The PDP context was terminated due to change in SGSN.
- maxChangeCond (19): The PDP context was terminated due to exceeding the changed condition limit.
- managementIntervention (20): The record was closed due to an O&M request.
- intraSGSNIntersystemChange (21)
- rATChange (22): The PDP context was terminated due to change in RAT.
- mSTimeZoneChange (23): The PDP context was terminated due to change in time zone of MS.
- unauthorizedRequestingNetwork (52)
- unauthorizedLCSClient (53)
- positionMethodFailure (54)
- unknownOrUnreachableLCSClient (58)
- listofDownstreamNodeChange (59)
- Partial record generation: A partial CDR was generated for reasons such as the reaching of data volume or time (duration) limits, or reaching the maximum number of charging condition changes.

Important: Please note that the following fields – cAMELInitCallRelease (5), unauthorizedRequestingNetwork (52), unauthorizedLCSClient (53), positionMethodFailure (54), unknownOrUnreachableLCSClient (58), and listofDownstreamNodeChange (59) are currently not supported.

Format
Unsigned integer.

Length
1 byte.

Charging Characteristics

Lists the charging characteristics applied to the PDP context.

The GGSN can accept charging characteristics from the SGSN or use its own. GGSN configured charging characteristics are specified as part of the GGSN Service and are applied to subscriber PDP contexts through APN templates. Refer to the *Administration and Configuration Guide* for information on configuring GGSN-based charging characteristics.

Format
Hex value octet string.

Length
2 bytes.

Charging ID

The GGSN-generated value used to identify this PDP context.

Format
Unsigned integer

Length
1-4 bytes

ChSelectionMode

The charging characteristic type that the GGSN applied to the CDR.

The following values for this field are supplied:

- Home default: GGSN configured charging characteristics for home subscribers are used. Home subscribers are those that belong to the same PLMN as the one on which the GGSN is located.
- Visiting default: GGSN configured charging characteristics for visiting subscribers are used. Visiting subscribers are those that belong to a different PLMN than the one on which the GGSN is located.
- Roaming default: GGSN configured charging characteristics for roaming subscribers are used. Roaming subscribers are those that are serviced by an SGSN belonging to a different PLMN than the one on which the GGSN is located.
- SGSN supplied: The GGSN is using the charging characteristics supplied by the SGSN.

Format
Enumerated integer.

Length
1 byte.

Diagnostics

This field is included in the CDR when the PDP context is released.

This field is supported both in GCDRs and E-GCDRs. However, this field will be populated in E-GCDRs only when **`gtpp attribute diagnostics`** command is configured in gttp group. It will contain one of the following values:

- 36: If the SGSN sends Delete PDP context request
- 38: If GGSN sends delete PDP context request due to GTP-C/U echo timeout with SGSN
- 40: If the GGSN sends delete PDP context request due to receiving a RADIUS Disconnect request message.
- 26: If the GGSN sends delete PDP context request for any other reason

Format
Unsigned integer.

Length
1–4 bytes.

Duration

The time period, in seconds, that the record existed in the GGSN. It is the duration from Record Opening Time to record closure. For partial records, only the duration of the individual partial record is provided.

Format

Unsigned integer.

Length
1–4 bytes.

Dynamic Address Flag

The presence of this field indicates that the **Served PDP Address** was dynamically assigned during context activation.

Format
Boolean

Length
1 byte

External Charging Identifier

A charging identifier received from an external, non-GPRS entity.

Important: This field is not supported at this time.

Format
Octet string.

GGSN Address

The binary-represented IPv4 address of the GGSN used.

Format
Hex value octet string

Length
4 bytes

IMS Signalling Context

Indicates whether or not the PDP context is used for IMS signaling based on the setting of the "IM CN Subsystem Signalling Flag" conveyed via the "Activate PDP context request" message from the MS to the network.

Important: This field is not supported at this time.

Format
Octet string.

List of Service Data Volumes

A list of the changes that occurred in charging conditions for all service data flows for the PDP context.

The first container includes an optional field “QoS Negotiated”. In the following containers “QoS Negotiated” is present if the previous change condition is "QoS change". The list will include one or more of the following fields:

- Service Identifier: Service identifier is an identifier for a service. The service identifier may designate an end user service, a part of an end user service or an arbitrarily formed group thereof. Present only if the rating group is online (DCCA) charged.
- Rating Group: This is the service flow identity and has to be used for differentiated evaluation of user’s traffic. This is also known as content-id.
- Charging Rulebase Name: The name of the Rulebase used for charging. This is the group name of charging rules.

  Important: The maximum length of charging rulebase name in the List of Service Data Volumes (LOSDVs) can be trimmed. For more information, refer to the **`gtpp egcdr charging-rulebase-name-max-char-length`** command in the *Context Configuration Mode Commands* chapter of the *Command Line Interface Reference Guide*.

- Result Code: The result code AVP. This contains the result code after the interconnection with the CRF. Present only if the rating group is online (DCCA) charged.
- Local Sequence No: A per service data container sequence number. It starts from 1 for each service, increasing by 1 for each service date container generated for that service within the lifetime of this PDP session.
- Time of first usage: The time stamp for the first IP packet to be transmitted for the service data flow referred to the current instance of Service Condition Change.
- Time of last usage: The time stamp for the last IP packet to be transmitted for the service data flow referred to the current instance of Service Condition Change.
- Usage time: The difference between “time of first usage” and “time of last usage”.
- User Location Information: The User Location Information for the MS if provided by the SGSN to the GGSN during the PDP context activation/modification procedure.
- Service change condition: The reason for closing the service data container for triggers like SGSN change, QoS change, RAT change, time and volume triggers, etc.
- QoS Negotiated: The negotiated QoS applied for the service data flow.
- SGSN-address: The valid SGSN IP address during the service data recording interval.
- SGSN PLMN identifier: The valid SGSN PLMN Id during the service data recording interval.
- FBC Data volume uplink: The number of octets transmitted during the use of the packet data services in the uplink direction.
- FBC data volume downlink: The number of octets transmitted during the use of the packet data services in the downlink direction.
- Time of Report: A time stamp defining the moment when the service data container is closed.
- RAT Type: The valid radio access technology type during the service data recording interval.
- Failure handling Continue: A Boolean expression included if the failure handling condition has been executed. Present only if the rating group is online (DCCA) charged and if failure handling procedure is executed by DCCA.

Format

- Service Identifier: Integer
- Rating Group: Integer
- Charging Rulebase Name: IA5 octet string
- Result Code: Integer
- Local Seq No: Integer
- Time of first usage: BCD encoded octet string
- Time of last usage: BCD encoded octet string
- Usage time: Unsigned integer
- Service change condition: Bit string
- QoS negotiated: Octet string
- Sgsn-address: Hex value octet string
- SGSN PLMN identifier: Hex value octet string
- FBC Data volume uplink: Integer
- FBC data volume downlink: Integer
- Time of Report: BCD encoded octet string
- Rat Type: Integer(1-255)
- Failurehandling Continue: Boolean

Length

- Service Identifier: 4 bytes
- Rating Group: 4 bytes
- Charging Rulebase Name: 1-64 bytes
- Result Code: 4 bytes
- Local Seq No: 4 bytes
- Time of first usage: 9 bytes
- Time of last usage: 9 bytes
- Usage time: 4 bytes
- Service change condition: 32 bits (4 bytes) (see note below)
- QoS negotiated: 12 bytes
- Sgsn-address: 4 bytes
- SGSN PLMN identifier: 3 bytes
- FBC Data volume uplink: 4 bytes
- FBC data volume downlink: 4bytes
- Time of Report: 9 bytes
- Rat Type: 1 byte
- Failurehandling Continue: 1 byte

Important: The maximum length of charging rulebase name in the List of Service Data Volumes (LOSDVs) can be trimmed. For more information, refer to the **`gtpp egcdr charging-rulebase-name-max-char-length`** command in the *Context Configuration Mode Commands* chapter of the *Command Line Interface Reference Guide*.

Important: When encoding the Service Change Condition bit string, the following rule is applied:"In a primitive encoding, the first contents octet gives the number of bits by which the length of the bit string is less than the next multiple of eight (this is called the 'number of unused bits'). The second and following contents octets give the value of the bit string, converted to an octet string." [As stated in *A Layman's Guide to a Subset of ASN.1, BER, and DER - Burton S. Kaliski* section 5.4] For example, serviceConditionChange is set to "88 0403 0400 00" to continue the ongoing session case. "03" represents the number of unused bits according to ASN.1 encoding which indicates that the octet following the length octet actually gives the number of unused bits.

In 12.3 and earlier releases, when the CLI command **`gtpp egcdr service-data-flow threshold interval`** was configured to 'n' seconds, the difference between "timeOfFirstUsage" and "timeOfReport" of LOSDV was always 'n' seconds for the LOSDVs closed due to "service-data-flow" threshold. Here, changeTime of LOSDV was reported incorrectly. It was always timeOfFirstUsage + 'n'. This does not hold true when the traffic for a particular content ID was not continuous.

List of Traffic Data Volumes

A list of the changes that occurred in the charging conditions for this PDP context.

The list will include one or more containers each including the following fields:

- QoS negotiated: Quality of service (QoS) has been negotiated. The initial and final corresponding data values are listed. This is only added for the first container and the container after a QoS change.
- Uplink volume: The number of octets (uncompressed) received from the MS. The initial and final corresponding data values are listed.
- Downlink volume: The number of octets (uncompressed) transmitted to the MS.The initial and final corresponding data values are listed.
- Change Condition: Identifies the reason that the container was closed such as tariff time change, QoS change, or closing of the CDR.
- Change Time: A time stamp identifying the time at which the volume container or the CDR closed.

For GPRS, data volumes are in octets above the GTP layer and are separated for uplink and downlink traffic. In UMTS, data volumes are in octets above the GTP-U layer and are separated for uplink and downlink traffic.

Format

- QoS negotiated: Octet String
- Uplink volume: Integer
- Downlink volume: Integer
- Change Condition: Integer
- Change Time: BCD encoded octet string

Length

- QoS negotiated: 12 bytes
- Uplink volume: 4 bytes
- Downlink volume: 4 bytes

- Change Condition: 1byte
- Change Time: 9 bytes

Local Record Sequence Number

For a Node ID, this number is allocated sequentially for each CDR. This along with a Node ID uniquely identifies a CDR.

Format
Unsigned integer.

Length
1–4 bytes.

MS Time Zone

The "Time Zone" IE that the SGSN may provide to the GGSN during the PDP context activation/modification procedure.

Format
Hex value octet string.

Length
2 bytes.

Network Initiated PDP Context

The presence of this field indicates that the PDP context was initiated by the network.

Format
Boolean

Length
1 byte

Node ID

The identifier string for the GGSN that had generated the CDR. Node ID along with local record sequence number uniquely identifies a CDR.

Format
Octet string.

Length
1–16 bytes.

PDP Type

The PDP context type. The PDP types supported by the GGSN are IP or PPP (including IHOSS:OSP).

Format
Hex value octet string

Length
2 bytes

Radio Access Technology (RAT) Type

The SGSN may include the RAT Type IE along with User Location Information IE, and MS Time Zone IE if they are available. The RAT Type IE shall not be included for the MS-initiated PDP Context Modification procedure.

Format
Integer(1-255).

Length
1 byte.

Record Extensions

A set of network operator or manufacturer specific extensions which may be added to the record if provided. It is used for reporting flows and volumes consumed, and also for passing key information about the session into the downstream charging systems.

Important: This field is customer specific. Service Level CDR is also the part of Record Extension.

Record Opening Time

The timestamp at which the PDP context was activated on the GGSN.

Format
BCD encoded octet string.

Length
9 bytes.

Record Sequence Number

A running sequence number used to link partial records generated by the GGSN for a specific PDP context (characterized with the same Charging ID and GGSN address pair). This field is only present for partial records.

Format
Unsigned integer.

Length
1–4 bytes.

Record Type

Indicates the GGSN PDP context record type. From the GGSN, this will be G-CDR.

Format

Integer

Length
1–4 bytes

Served IMEISV

The International Mobile Equipment Identity and Software Version Number (IMEISV) of the MS, if available.

Format
BCD encoded octet string.

Length
8 bytes.

Served IMSI

The International Mobile Subscriber Identity (IMSI) of the MS. The IMSI is formatted in accordance with 3GPP TS 23.003. This will be present if the Anonymous Access Indicator is FALSE or not supplied.

Format
BCD encoded octet string

Length
3 to 8 bytes

Served MSISDN

The Mobile Station (MS) ISDN number (MSISDN) of the subscriber.

Format
BCD encoded octet string.

Length
1–9 bytes.

Served PDP Address

The binary-represented IPv4/IPv6 address associated with the PDP context for the CDR. This address could either be static or dynamically assigned.

Format
Hex value octet string

Length
4 bytes for IPv4 address

16 bytes for IPv6 address

Service Level CDR

It is a sequence of CSG fields.

It has one or more containers having following fields:

- Session ID: A unique 0-128 byte session id that is assigned to each user session. A user going to multiple services will be assigned a unique session id for each service. Diameter session ID is filled in this field.
- Service ID: It is an OCTET string which denotes the name of the Service. Rating group ID is filled in this field.
- Service IP Volume Usage: IP level volume usage. When this volume is calculated all the L4-L7 headers are counted, i.e. volume equals length of IP packet.
- Quota Server Flags: used to notify the receiver of various conditions or actions of the quota server.
- Qualified Usage: Specifies qualified usage and defining units of service. It is used for credit-control.
- TimeOfFirstUsage: The time stamp for the first IP packet to be transmitted for the service data flow referred to the current instance of Service Condition Change.

Important: There are some more fields in the Service Level CDR which are mapped to other existing fields. Those fields include: Cause, Service Start Timestamp, UserIndex or UserIndexIPv6, or UserDualStackIPv4, and Billing Plan ID.

Format

- Session ID: Octet String
- Service ID: Octet String
- Service IP Volume Usage: Sequence
- Quota Server Flags: Integer
- Qualified Usage: Sequence
- TimeOfFirstUsage: BCD encoded octet string

Length

- Session ID: 0-128 bytes
- Service ID: 0-128 bytes
- Service IP Volume Usage: 0-24 bytes
- Quota Server Flags: 0-4 bytes
- Qualified Usage: 0-13 bytes
- TimeOfFirstUsage: 9 bytes

SGSN Address

A list of all of the SGSN IPv4 addresses (binary-represented) used over the duration of the CDR. The address(es) can be either user or control-plane addresses.

Format

Hex value octet string

Length

4 bytes per address

SGSN PLMN Identifier

RAI (optionally supplied by SGSN in the GTP create PDP context request) is used as SGSN PLMN Identifier value. It is omitted if the SGSN does not supply the RAI.

Format

Hex value octet string.

Length

3 bytes.

User Location Information

The User Location Information for the MS if provided by the SGSN to the GGSN during the PDP context activation/modification procedure.

Format

Octet string.

Length

8 bytes.

Chapter 9
P-GW CDR Field Reference

This chapter provides a reference for CDR fields supported by the system for use in PGW-CDRs.

A complete list and descriptions of supported CDR fields is provided in the *P-GW CDR Field Descriptions* chapter of this reference.

Important: For more information on custom dictionaries, contact your Cisco account representative.

The category column in all tables use keys described in the following table.

Table 22. Dictionary Table Key

Abbreviation	Meaning	Description
M	Mandatory	A field that must be present in the CDR.
C	Conditional	A field that must be present in a CDR if certain conditions are met.
OM	Operator Provisionable: Mandatory	A field that an operator has provisioned and must be included in the CDR for all conditions.
OC	Operator Provisionable: Conditional	A field that an operator has provisioned that must included in the CDR if certain conditions are met.

CDR Fields Supported in PGW-CDRs

The table in this section lists the PGW-CDR fields present in the available GTPP dictionaries.

custom24, custom40, and custom42 Dictionary

PGW-CDR fields are based on 3GPP TS 32.298 V8.5.0.

Field	Category	Description
Record Type	M	P-GW IP CAN bearer record
Served IMSI	M	IMSI of the served party (if Anonymous Access Indicator is FALSE or not supplied)
P-GW Address	M	The control plane IP address of the P-GW used.
Charging ID	M	IP CAN bearer identifier used to identify this IP CAN bearer in different records created by PCNs
Serving Node Address	M	List of serving node control plane IP addresses (e.g. SGSN, MME, etc.) used during this record.
Access Point Name Network Identifier	OM	The logical name of the connected access point to the external packet data network (network identifier part of APN).
PDP/PDN Type	OM	Indicates PDP type (IP, PPP, or IHOSS:OSP) or PDN type (IPv4, IPv6, or IPv4v6).
Served PDP/PDN Address	OC	IP address allocated for the PDP context / PDN connection (IPv4 or IPv6), if available.
Dynamic Address Flag	OC	Indicates whether served PDP/PDN address is dynamic, which is allocated during IP CAN bearer activation, initial attach (E-UTRAN or over S2x) and UE requested PDN connectivity. This field is missing if address is static.
Record Opening Time	M	Timestamp when IP CAN bearer is activated in this P-GW or record opening time on subsequent partial records.
Duration	M	Duration of this record in the P-GW.
Cause for Record Closing	M	The reason for the release of record from this P-GW.
Diagnostics	OM	A more detailed technical reason (as defined in TS 32.250) for the release of the connection.
Record Sequence Number	C	Partial record sequence number, only present in case of partial records.
Node ID	OM	Name of the recording entity.
Local Record Sequence Number	OM	Consecutive record number created by this node. The number is allocated sequentially including all CDR types.
APN Selection Mode	OM	An index indicating how the APN was selected.
Served MSISDN	OM	The primary MSISDN of the subscriber.

Field	Category	Description
Charging Characteristics	M	The Charging Characteristics applied to the IP CAN bearer.
Charging Characteristics Selection Mode	OM	Holds information about how Charging Characteristics were selected.
Serving Node PLMN Identifier	OM	Serving node PLMN Identifier (MCC and MNC) used during this record, if available.
Served IMEISV	OC	IMEISV of the ME, if available.
RAT Type	OC	Indicates the Radio Access Technology (RAT) type currently used by the Mobile Station, when available.
MS Time Zone	OC	Indicates the offset between universal time and local time in steps of 15 minutes where the MS currently resides.
User Location Information	OM	Contains the User Location Information of the MS as defined in TS 29.060 for GPRS case, and in TS 29.274 for EPC case, if available.
List of Service Data	OM	List of changes in charging conditions for all service data flows within this IP CAN bearer categorized per rating group or per combination of the rating group and service id.
Data Service Volume Block	OM	Service data container associated with a service condition change on a service data flow (categorized per rating group or per combination of the rating group and service id) within this IP CAN bearer.
Serving node Type	M	List of serving node types in control plane. The serving node types listed here map to the serving node addresses listed in the field “Serving node Address” in sequence.
Served MNNAI	OC	Mobile Node Identifier in NAI format (based on IMSI), if available.
P-GW PLMN Identifier	OC	PLMN identifier (MCC MNC) of the P-GW.
Start Time	OC	The time when User IP-CAN session starts, available in the CDR for the first bearer in an IP-CAN session.
Stop Time	OC	The time when User IP-CAN session is terminated, available in the CDR for the last bearer in an IP-CAN session.
PDN Connection Id	OM	PDN connection (IP-CAN session) identifier to identify different records belonging to same PDN connection.

Notes:

- For custom40 dictionary, the following specifications are recommended:
  - Diagnostics field is mandated to be present in the final PGW-CDRs.
  - managementIntervention is not set as the cause for record closing (CauseForRecordClosing).
  - Duration of PGW-CDRs will be calculated first and then round-off mechanism will be applied.
  - “Service Identifier” sub-field will not be included in List of Service Data Volume (LOSDV) containers.
- In the case of custom40 GTPP dictionary, the following two values are also supported for the PGW-CDR field “Charging Characteristics Selection Mode” in addition to the standard values as in the custom24 GTPP dictionary.
  - AAASupplied (6)

    - GWOverride (7)
- custom42 dictionary: This customer-specific file format contains PGW-CDRs that are encoded in ASCII format.
- For custom42 dictionary, Record Sequence Number is 12 byte ASCII value and last 2 bytes will always be zero.
- In the case of custom42 dictionary, PGW-CDR is closed as the final record of a subscriber session for the following events:
    - Detach Request received from UE
    - Delete bearer context request received from S-GW.
    - Manual subscriber clearing
    - Abnormal Releases such as path failures

Data Service Volume Block

Field	Category	Description
Rating Group	OM	Service flow identity, also known as content-id.
Charging Rulebase Name	OC	Name of the Rulebase used for charging.
Result Code	OC	Result code shared by OCS.
Local Sequence Number (LOSDV)	OC	Service data container sequence number.
Time of First Usage	OC	Timestamp for the first IP packet to be transmitted for the service data flow.
Time of Last Usage	OC	Timestamp for the last IP packet to be transmitted for the service data flow.
Time Usage	OC	Difference in seconds, within range of 0 to 4294967295, between “time of first usage” and “time of last usage”.
Service Condition Change	OC	Reason for closing the service data container.
QoS Information Negotiated	OC	Authorized QoS for the IP-CAN bearer.
Serving Node Address (LOSDV)	OC	IP address of the serving node (SGSN/S-GW) control plane.
Data Volume FBC Uplink	OC	Number of octets received in the uplink direction for this container.
Data Volume FBC Downlink	OC	Number of octets transmitted in the downlink direction for this container.
Time of Report	OM	Timestamp defining the moment when the service data container is closed.
Failure Handling Continue	OC	Identifier for failure handling.
Service Identifier	OC	Identifier for a service.
User Location Information (LOSDV)	OC	Location of the user known at the time when container is created.

Chapter 10
P-GW CDR Field Descriptions

This chapter describes the CDR fields supported by the system for use in PGW-CDRs.

The following information is provided for each field:

- **Description:** The field's description.
- **Format:** The field's data format.
- **Length:** The field's size, in bytes.

All PGW-CDRs are encoded using the ASN.1 format and are sent to the charging gateway function (CGF) using the GPRS Tunneling Protocol Prime (GTPP) as defined in the following standards:

- 3GPP TS 29.060
- 3GPP TS 32.015
- 3GPP TS 32.215
- 3GPP TS 32.251 (v8.5.0, v8.6.0)
- 3GPP TS 32.298 (v8.4.0, v8.5.0) (PGW-CDRs)

Also see the *Field Reference for CDRs in P-GW* chapter for information on CDR fields supported in PGW-CDRs.

Important: The behavior for several of the fields supported in CDRs can be modified. For more information, refer to the **`gtpp attributes`** command in the *Command Line Interface Reference*.

CDR Fields

Access Point Name Network Identifier

The network identifier portion of the access point name (APN). This APN is sent to the S-GW by the MME and is relayed to the P-GW in the EGTP Create Session Request message.

The APN string may consist of alphabetic characters (“A...Z”, “a...z”), digits (“0...9”) and the dash “-”.

Format

IA5 string

Length

1–63 bytes

APN Selection Mode

An index indicating how the APN was selected.

The following APN selection mode indexes are possible:

- 0: MS or network provided APN, subscription verified
- 1: MS provided APN, subscription not verified
- 2: Network provided APN, subscription not verified

Format

Enumerated

Length

1 byte

Cause for Record Closing

This field contains a reason for the closure of the CDR.

Some of the possible reasons are as follows:

- normalRelease (0): The PDP context was terminated normally through a PDP context release (end of context or SGSN change) or a GPRS detach.
- abnormalRelease (4): The PDP context was abnormally terminated.
- volumeLimit (16): The PDP context was terminated due to exceeding volume limit.
- timeLimit (17): The PDP context was terminated due to exceeding time limit.
- servingNodeChange (18): The PDP context was terminated due to Serving Node Address List Overflow.
- maxChangeCond (19): The PDP context was terminated due to exceeding the changed condition limit.
- managementIntervention (20): The record was closed due to an O&M request.
- rATChange (22): The PDP context was terminated due to change in RAT.

- mSTimeZoneChange (23): The PDP context was terminated due to change in time zone of MS.
- PLMNChange (24): The PDP context was terminated due to change of PLMN-ID.
- Partial record generation: A partial CDR was generated for reasons such as the reaching of data volume or time (duration) limits, or reaching the maximum number of charging condition changes.

Format

Integer

Length

1 byte

Charging Characteristics

Lists the charging characteristics applied to the PDP context by the P-GW.

Format

Octet string

Length

2 bytes

Charging Characteristics Selection Mode

This field specifies how the Charging Characteristics were selected.

Supported values:

- servingNodeSupplied (0)
- homeDefault (3)
- roamingDefault (4)
- visitingDefault (5)
- AAASupplied (6)
- GWOverride (7)

Note: The values AAASupplied (6) and GWOverride (7) are only supported in the custom40 GTPP dictionary.

Format

Enumerated

Length

1 byte

Charging ID

This field contains a charging identifier, which can be used together with the P-GW address to identify all records involved in a single bearer context. The Charging ID is generated by the P-GW during bearer context activation and is transferred to the context requesting P-GW.

Format

Integer

Length

1–5 bytes

Diagnostics

This field is included in the CDR when the bearer is released and when the option **`gtpp attribute diagnostics`** is configured.

Format

Integer

Length

Variable

Duration

This field contains the duration in seconds for the record. The value is reset for each new partial CDR.

This value is converted from the internal representation in milliseconds to an integer value representing only seconds. The mechanism for this conversion (ceiling, floor, round-off) can be configured.

Format

Integer

Length

1–5 bytes

Dynamic Address Flag

This field indicates that the PDN address has been dynamically allocated for that particular IP CAN bearer (PDN connection). This field is missing if the address is static.

Format

Boolean

Length

1 byte

List of Service Data

This list includes one or more service data containers. Each container is associated with a service condition change on a service data flow (categorized per rating group or per combination of the rating group and service id) within this IP CAN bearer.

Format

Sequence

Length

Variable

Data Service Volume Block

This is a service data container. A container is associated with a service condition change on a service data flow (categorized per rating group or per combination of the rating group and service id) within this IP CAN bearer.

A service data container may include the fields in the following subsections.

Format

Sequence

Length

Variable

Charging Rulebase Name

The name of the Rulebase used for charging. This is the group name of charging rules.

Format

IA5string

Length

1–16 bytes

Data Volume FBC Downlink

The number of octets transmitted during the use of the packet data services in the downlink direction.

Format

Integer

Length

1–5 bytes

Data Volume FBC Uplink

The number of octets received during the use of the packet data services in the uplink direction.

Format

Integer

Length

1–5 bytes

Failure Handling Continue

This parameter is included when the failure handling procedure has been executed and new containers are opened. This parameter shall be included in the first and subsequent containers opened after the failure handling execution.

Format

Boolean

Length

1 byte

Local Sequence Number (LOSDV)

A service data container sequence number. It starts from 1 and is increased by 1 for each service data container generated within the lifetime of this IP-CAN bearer.

Format

Integer

Length

1–5 bytes

QoS Information Negotiated

For an IP-CAN bearer-specific container, this contains the authorized QoS for the IP-CAN bearer. The first container for each QCI/ARP pair includes this field. In the following containers this field is present if the previous change condition is "QoS change".

This field contains a sequence of fields which are described in the following subsections:

- qCI [1] Integer
- maxRequestedBandwithUL [2] Integer Optional
- maxRequestedBandwithDL [3] Integer Optional
- guaranteedBitrateUL [4] Integer Optional
- guaranteedBitrateDL [5] Integer Optional
- aRP [6] Integer Optional

Format

Sequence

Length

Variable

Allocation and Retention Priority (ARP)

The ARP contains information about the priority level (scalar), the pre-emption capability (flag) and the pre-emption vulnerability (flag). The primary purpose of ARP is to decide whether a bearer establishment or modification request can be accepted, or needs to be rejected due to resource limitations (typically available radio capacity for GBR bearers). Range: 1-15.

Format

Integer

Length

1–5 bytes

Guaranteed Bit Rate (GBR) Downlink

The GBR denotes the downlink bit rate that can be expected to be provided by a GBR bearer.

Format

Integer

Length

1–5 bytes

Guaranteed Bit Rate (GBR) Uplink

The GBR denotes the uplink bit rate that can be expected to be provided by a GBR bearer.

Format

Integer

Length

1–5 bytes

Maximum Bit Rate (MBR) Downlink

The MBR limits the downlink bit rate that can be expected to be provided by a GBR bearer (for example, excess traffic may get discarded by a rate shaping function).

Important: Note that, if the CLI command **`gtpp attribute apn-ambr`** is configured in the GTPP Server Configuration mode, the values of APN-AMBR attribute will be populated in the PGW-CDR in the custom24 GTPP dictionary.

Format

Integer

Length

1–5 bytes

Maximum Bit Rate (MBR) Uplink

The MBR limits the uplink bit rate that can be expected to be provided by a GBR bearer.

Important: Note that, if the CLI command **`gtpp attribute apn-ambr`** is configured in the GTPP Server Configuration mode, the values of APN-AMBR attribute will be populated in the PGW-CDR in the custom24 GTPP dictionary.

Format

Integer

Length

1–5 bytes

Quality Class Identifier (QCI)

A QCI is a scalar that is used as a reference to access node-specific parameters that control bearer level packet forwarding treatment (for example, scheduling weights, admission thresholds, queue management thresholds, link layer protocol configuration, etc.), and that have been pre-configured by the operator owning the access node (for example, eNodeB). Value Range: 1-9.

Format

Integer

Length

1–5 bytes

Rating Group

This is the service flow identity and must be used for differentiated evaluation of user's traffic. This is also known as content-id.

Format

Integer

Length

1–5 bytes

Result Code

This is filled by OCS on Gy interface.

The following are the values as per RFC 3588 and 4006 (Other Result Codes not defined in the RFCs can also be seen in the Result Code field if sent by OCS):

- DIAMETER_SUCCESS 2001
- DIAMETER_LIMITED_SUCCESS 2002
- DIAMETER_COMMAND_UNSUPPORTED 3001
- DIAMETER_UNABLE_TO_DELIVER 3002
- DIAMETER_REALM_NOT_SERVED 3003
- DIAMETER_TOO_BUSY 3004
- DIAMETER_LOOP_DETECTED 3005
- DIAMETER_REDIRECT_INDICATION 3006
- DIAMETER_APPLICATION_UNSUPPORTED 3007
- DIAMETER_INVALID_HDR_BITS 3008
- DIAMETER_INVALID_AVP_BITS 3009
- DIAMETER_UNKNOWN_PEER 3010
- DIAMETER_AUTHENTICATION_REJECTED 4001
- DIAMETER_OUT_OF_SPACE 4002
- ELECTION_LOST 4003
- DIAMETER_END_USER_SERVICE_DENIED 4010
- DIAMETER_CREDIT_CONTROL_NOT_APPLICABLE 4011
- DIAMETER_CREDIT_LIMIT_REACHED 4012
- DIAMETER_AVP_UNSUPPORTED 5001
- DIAMETER_UNKNOWN_SESSION_ID 5002
- DIAMETER_AUTHORIZATION_REJECTED 5003

- DIAMETER_INVALID_AVP_VALUE 5004
- DIAMETER_MISSING_AVP 5005
- DIAMETER_RESOURCES_EXCEEDED 5006
- DIAMETER_CONTRADICTING_AVPS 5007
- DIAMETER_AVP_NOT_ALLOWED 5008
- DIAMETER_AVP_OCCURS_TOO_MANY_TIMES 5009
- DIAMETER_NO_COMMON_APPLICATION 5010
- DIAMETER_UNSUPPORTED_VERSION 5011
- DIAMETER_UNABLE_TO_COMPLY 5012
- DIAMETER_INVALID_BIT_IN_HEADER 5013
- DIAMETER_INVALID_AVP_LENGTH 5014
- DIAMETER_INVALID_MESSAGE_LENGTH 5015
- DIAMETER_INVALID_AVP_BIT_COMBO 5016
- DIAMETER_NO_COMMON_SECURITY 5017
- DIAMETER_USER_UNKNOWN 5030
- DIAMETER_RATING_FAILED 5031

Format

Integer

Length

1–5 bytes

Service Condition Change

The reason for closing the service data container for triggers like SGSN change, QoS change, RAT change, time and volume triggers, etc.

Bit Setting regarding TS 32.298:

- qoSChange (0), bearer modification
- sGSNChange (1), bearer modification
- sGSNPLMNIDChange (2), bearer modification
- tariffTimeSwitch (3), tariff time change
- pDPContextRelease (4), bearer release
- rATChange (5), bearer modification
- serviceIdledOut (6), IP flow idle out, DCCA QHT expiry
- reserved (7), old: QCTexpiry is no report event
- configurationChange (8), configuration change
- serviceStop (9), IP flow termination
- dCCATimeThresholdReached (10), DCCA quota reauth.
- dCCAVolumeThresholdReached (11), DCCA quota reauth.
- dCCAServiceSpecificUnitThresholdReached (12), DCCA quota reauth.

- dCCATimeExhausted (13), DCCA quota reauth.
- dCCAVolumeExhausted (14), DCCA quota reauth.
- dCCAValidityTimeout (15), DCCA quota validate time (QVT expiry)
- reserved (16), reserved due to no use case, old: return Requested is covered by (17), (18)
- dCCAReauthorisationRequest (17), DCCA quota reauthorization request by OCS
- dCCAContinueOngoingSession (18), DCCA failure handling continue IP flow
- dCCARetryAndTerminateOngoingSession (19), DCCA failure handling terminate IP flow after DCCA retry
- dCCATerminateOngoingSession (20), DCCA failure handling, terminate IP flow
- cGI-SAIChange (21), bearer modification
- rAIChange (22), bearer modification
- dCCAServiceSpecificUnitExhausted (23), DCCA quota reauthorization
- recordClosure (24), PGW-CDR closure
- timeLimit (25), intermediate recording
- volumeLimit (26), intermediate recording
- serviceSpecificUnitLimit (27), intermediate recording
- envelopeClosure (28)
- eCGIChange (29), bearer modification. “ECGI Change”
- tAIChange (30), bearer modification. “TAI Change”
- userLocationChange (31) bearer modification. “User Location Change”

Format

Bit string

Length

5 bytes

Service Identifier

The service identifier may designate an end user service, a part of an end user service, or an arbitrarily formed group thereof. This field is only included if reporting is per combination of the rating group and service id.

Format

Integer

Length

1–5 bytes

Serving Node Address (LOSDV)

This field contains the serving node (for example, SGSN/S-GW) control plane IP address.

Format

Octet string

Length

6 or 18 bytes (depending on v4 or v6 address)

Time of First Usage

The timestamp for the first IP packet to be transmitted for the service data flow referred to the current instance of Service Condition Change.

Format

BCD encoded octet string

Length

9 bytes

Time of Last Usage

The timestamp for the last IP packet to be transmitted for the service data flow referred to the current instance of Service Condition Change.

Format

BCD encoded octet string

Length

9 bytes

Time of Report

A timestamp defining the moment when the service data container is closed.

Format

BCD encoded octet string

Length

9 bytes

Time Usage

The difference in seconds within the range of 0.to.4294967295 between “time of first usage” and “time of last usage”.

Format

Integer

Length

1–5 bytes

User Location Information (LOSDV)

This field indicates details of where the UE is currently located (SAI, TAI, RAI, CGI, ECGI or access-specific user location information).

Format
Octet string

Length
6–13 bytes

Local Sequence Number

This field contains a unique sequence number associated with the Node ID field and independent of the bearer context.

Format
Integer.

Length
1–5 bytes

MS Time Zone

The "Time Zone" IE that the SGSN may provide to the P-GW during the PDP context activation/modification procedure.

Format
Octet string

Length
2 bytes

Node ID

This field contains an identifier string for the node that had generated the CDR.

On the Cisco P-GW, this Node ID field is a printable string in the format ndddSTRING:

- n: The first digit is the Sessmgr restart counter having a value between 0 and 7.
- ddd: The number of the sessmgr instance generating the CDR
- STRING: This is a configured Node-ID-Suffix having any string between 1 to16 characters, defined using the gtpp attribute node-id command.

If this node-id-suffix is not configured, the PGW uses the active-charging service name as the Node-id-suffix (truncated to 16 characters).

This field is only included when the option **`gtpp attribute local-record-sequence-number`** is configured.

Format
IA5string

Length
1–20 bytes

PDN Connection Id

This field defines the PDN connection (IP-CAN session) identifier to identify different records belonging to same PDN connection. This field includes the Charging Id of the first IP-CAN bearer activated within the PDN connection. Together with P-GW address, this uniquely identifies the PDN connection.

Format

Integer

Length

1–5 bytes

PDP PDN Type

-- OCTET 1: PDP Type Organization

```
Spare '1111'        PDP Type Organization Value
```

PDP Type Organization	Value
ETSI	0
IETF	1

Note: In LTE, only IETF is supported.

-- OCTET 2: PDP/PDN Type Number

```
Bits    3  2  1    0  0  1    IPv4    0  1  0    IPv6    0  1  1    IPv4/IP
v6    Bits 8-4 of octet are spare and are coded as zero.
```

Format

Octet string

Length

2 bytes

P-GW Address

These field is the serving P-GW IP address for the Control Plane. If both an IPv4 and an IPv6 address of the P-GW is available, the P-GW shall include the IPv4 address in the CDR.

Format

Octet string

Length

6 or 18 bytes (depending on v4 or v6 address)

P-GW PLMN Identifier

This field is the P-W PMLN Identifier (Mobile Country Code and Mobile Network Code).

The MCC and MNC are coded as described for “User Location Info” in TS 29.274 [91].

Format

Octet string

Length

3 bytes

RAT Type

Holds the value of RAT Type, as provided to S-GW and P-GW, described in TS 29.274 for eGTP case.

RAT Types	Values (Decimal)
<reserved>	0
UTRAN	1
GERAN	2
WLAN	3
GAN	4
HSPA Evolution	5
EUTRAN	6
<spare>	7-255

The field is provided by the SGSN/MME and transferred to the S-GW/P-GW during the IP-CAN bearer activation/modification.

Format

Integer

Length

1 byte

Record Opening Time

This field contains the timestamp when a PDP context is activated in PGW or when a subsequent record is opened after a partial record.

The timestamp is determined based on the internal timer which has an accuracy of 10ms. Depending on the configured mechanism (ceiling, floor, or round-off) this field is translated to only show full seconds.

TimeStamp ::= OCTET STRING (SIZE(6))

The contents of this field are a compact form of the UTC Time format containing local time plus an offset to universal time. Binary coded decimal encoding is employed for the digits to reduce the storage and transmission overhead

-- e.g. YYMMDDhhmmssShhmm

-- where

-- YY = Year 00 to 99 BCD encoded

-- MM = Month 01 to 12 BCD encoded
-- DD = Day 01 to 31 BCD encoded
-- hh = hour 00 to 23 BCD encoded
-- mm = minute 00 to 59 BCD encoded
-- ss = second 00 to 59 BCD encoded
-- S = Sign 0 = "+", "-" ASCII encoded
-- hh = hour 00 to 23 BCD encoded
-- mm = minute 00 to 59 BCD encoded

Format

BCD encoded octet string

Length

9 bytes

Record Sequence Number

A running sequence number within the range of 1 to 4294967296 used to link partial records generated by the P-GW for a specific IP-CAN bearer context (characterized with the same Charging ID and P-GW address). This field is not present if the first record is also the final record.

Format

Integer

Length

1–5 bytes

Record Type

This field identifies the type of the record:

PGW-CDR (pgwPDPRecord) 85 (0x55)

Format

Integer

Length

1 byte

Served IMEISV

This field contains the International Mobile Equipment Identity (IMEISV) of the equipment served.

The structure of the IMEI is defined in TS 23.003.

The IMEI is composed of the following elements:

- Type Allocation Code (TAC). Its length is 8 digits.
- Serial Number (SNR) is an individual serial number uniquely identifying each equipment within each TAC. Its length is 6 digits.

- Software Version Number (SVN) identifies the software version number of the mobile equipment. Its length is 2 digits.

If SV is not available, a filler digit “f” is added after the spare digit to fill up the last byte. Spare digit: this digit shall be zero, when transmitted by the MS.

Format

BCD encoded octet string

Length

8 bytes

Served IMSI

The International Mobile Subscriber Identity (IMSI) of the MS. The IMSI is formatted in accordance with 3GPP TS 23.003. This will be present if the Anonymous Access Indicator is FALSE or not supplied.

The IMSI is formatted in accordance with 3GPP TS 23.003.

Format

BCD encoded octet string

Length

3–8 bytes

Served MNNAI

This field contains the Mobile identifier of the served user in Network Access Identifier (NAI) format based on IMSI, as defined in TS 23.003 [68].

SubscriptionID ::= SET

{

subscriptionIDType [0] SubscriptionIDType,

subscriptionIDData [1] UTF8String

}

SubscriptionIDType ::= ENUMERATED

{

END_USER_E164 (0),

END_USER_IMSI (1),

END_USER_SIP_URI (2),

END_USER_NAI (3),

END_USER_PRIVATE (4)

}

The type will be END_USER_NAI.

For IMSI: 123456789012345 mcc=123 mnc=045

subscriptionIDData is a string will be

0123456789012345@nai.epc.mnc045.mcc123.3gppnetwork.org

Format

Set

Length

Variable (Max 62)

Served MSISDN

The field tracks the Mobile Station (MS) ISDN number (MSISDN) of the subscriber which is transparently copied from the Create Session Request message.

The MSISDN is TBCD encoded as shown in the example below:3GPP TS 23.003 (CCITT Rec. E 213)

ServedMSISDN ::= OCTET STRING (SIZE(1..9))

subscriber identification MSISDN

octet 1 : bit 8 (msb): extension bit

= 1 : no extension

other : not relevant

bit 7..5 : type of number

= 000 : unknown

= 001 : international number

= 010 : national significant number

= 011 : network specific number

= 100 : subscriber number

= 101 : reserved

= 110 : abbreviated number

= 111 : reserved for extension

bit 4..1 : numbering plan indicator

= 0001: ISDN/Telephony Numbering Plan (Rec CCITT E.164)

other : not relevant

octet 2..9: <= 16 digits TBCD-String (twisted)

substructure (without spares or fillers):

1..3 digits - country code (CC)

(only international number)

3 digits - national destination code (NDC)

<= 10 digits - subscriber number (SN)

first and intermediate octet = 2 digits

last octet = 2 digits or 1 digit + 1 fill digit H'F

As per 3GPP TS 29.274 v 8.11.0, “MSISDN value contains only the actual MSISDN number (does not contain the ‘nature of address indicator’ octet, which indicates ‘international number’ as in 3GPP TS 29.002 [37]) and is encoded as TBCD digits.”

To comply with this, octet 1 (nature of address indicator) is not added in the encoded value of MSISDN.

example:

MSISDN: '491720400305'

encoded: H'94 71 02 04 30 50

Format

BCD encoded octet string.

Length

1–9 bytes

Served PDP PDN Address

This field contains the IP address for the PDN connection (PDP context, IP-CAN bearer). This is a network layer address of type IP version 4 (PDN Type is IPv4) or IP version 6 (PDN Type is IPv6 or IPv4v6). The address for each Bearer type is allocated either temporarily or permanently (see “Dynamic Address Flag”). This parameter shall be present except when both the Bearer type is PPP and dynamic address assignment is used.

Format

Octet string

Length

The length can vary based on whether the encoded IP address is IPv4 or IPv6.

Serving Node Address

The serving node control plane IP address of the S-GW used during this record. This is a list of IP addresses. If the list overflows with a configured number of IP addresses, a CDR with “serving node Change” as cause for record closure will be generated. The serving node addresses that are listed here are sequentially mapped to the serving node types listed in the field “Serving node Types”.

Format

Sequence of IPv4 orIPv6 addresses.

Length

6-98 or 18-292 bytes (depending on IPv4 or IPv6 address; for 1-16 S-GW/SGSN addresses)

Serving Node PLMN Identifier

This field contains a serving node (SGSN/S-GW/MME/ePDG/HSGW) PLMN Identifier (Mobile Country Code and Mobile Network Code).

The MCC and MNC are coded as described for “Routing Area Identity” in TS 29.060 [75].

Format

Octet string

Length

3 bytes

Serving Node Type

These fields contain one or several serving node types in the control plane of an S-GW or P-GW, which have been connected during the record. The serving node types listed here are sequentially mapped to the serving node addresses listed in the field "Serving node Address".

The possible values are:

```
ServingNodeType  ::= ENUMERATED

{

        sGSN      (0),

        pMIPSGW   (1),

        gTPSGW    (2),

        ePDG      (3),

        hSGW      (4),

        mME       (5)

}
```

Format

Sequence of serving Node Type

Length

3-48; variable length format (based on number of nodes connected during this period)

Start Time

This field contains the time when the User IP-CAN session starts at the P-GW, available in the CDR for the first bearer in an IP-CAN session.

The timestamp is determined based on the internal timer which has an accuracy of 10ms. Depending on the configured mechanism this is translated into the timestamp which only shows the full seconds.

The format is shown below.

TimeStamp ::= OCTET STRING (SIZE(6))

The contents of this field are a compact form of the UTC Time format containing local time plus an offset to universal time. Binary coded decimal encoding is employed for the digits to reduce the storage and transmission overhead

-- e.g. YYMMDDhhmmssShhmm

-- where

-- YY = Year 00 to 99 BCD encoded

-- MM = Month 01 to 12 BCD encoded

-- DD = Day 01 to 31 BCD encoded

-- hh = hour 00 to 23 BCD encoded

-- mm = minute 00 to 59 BCD encoded

-- ss = second 00 to 59 BCD encoded

-- S = Sign 0 = “+”, “-” ASCII encoded

-- hh = hour 00 to 23 BCD encoded

-- mm = minute 00 to 59 BCD encoded

Format

BCD encoded octet string

Length

9 bytes

Stop Time

This field contains the time when the User IP-CAN session is terminated at the P-GW, available in the CDR for the last bearer in an IP-CAN session.

The timestamp is determined based on the internal timer which has an accuracy of 10ms. Depending on the configured mechanism (ceiling, floor, round-off) this is translated into the timestamp which only shows the full seconds.

The format is shown below.

TimeStamp ::= OCTET STRING (SIZE(6))

The contents of this field are a compact form of the UTC Time format containing local time plus an offset to universal time. Binary coded decimal encoding is employed for the digits to reduce the storage and transmission overhead

-- e.g. YYMMDDhhmmssShhmm

-- where

-- YY = Year 00 to 99 BCD encoded

-- MM = Month 01 to 12 BCD encoded

-- DD = Day 01 to 31 BCD encoded

-- hh = hour 00 to 23 BCD encoded

-- mm = minute 00 to 59 BCD encoded

-- ss = second 00 to 59 BCD encoded

-- S = Sign 0 = “+”, “-” ASCII encoded

-- hh = hour 00 to 23 BCD encoded

-- mm = minute 00 to 59 BCD encoded

Format

BCD encoded octet string

Length

9 bytes

User Location Information

This field contains the User Location Information as described in TS 29.274 for eGTP case (e.g. CGI, SAI, RAI TAI and ECGI).

The field is provided by the SGSN/MME and transferred to the S-GW/P-GW during the IP-CAN bearer activation/modification.

User Location Information contains the location (e.g. CGI/SAI, ECGI/TAI or RAI) where the UE is located and used during the transfer of the data volume captured by the container (applicable only to the SGW-CDR). This is included in the Traffic data container only if previous container's change condition is “user location change”. Note the user location information in SGW-CDR main level contains the location where the UE was when PGW-CDR was opened.

The flags ECGI, TAI, RAI, SAI and CGI in octet 5 indicate if the corresponding fields are present in the IE or not. If one of these flags is set to “0”, the corresponding field is not present at all. The respective identities are defined in 3GPP TS 23.003.

The following subclauses specify the coding of the different identities. For each identity, if an Administration decides to include only two digits in the MNC, then bits 5 to 8 of octet 7 are coded as “1111”.

CGI field:

The Location Area Code (LAC) consists of 2 octets. Bit 8 of Octet 9 is the most significant bit and bit 1 of Octet 10 the least significant bit. The coding of the location area code is the responsibility of each administration. Coding using full hexadecimal representation shall be used.

The Cell Identity (CI) consists of 2 octets. Bit 8 of Octet 11 is the most significant bit and bit 1 of Octet 12 the least significant bit. The coding of the cell identity is the responsibility of each administration. Coding using full hexadecimal representation shall be used.

SAI field:

The Location Area Code (LAC) consists of 2 octets. Bit 8 of Octet 9 is the most significant bit and bit 1 of Octet 10 the least significant bit. The coding of the location area code is the responsibility of each administration. Coding using full hexadecimal representation shall be used.

The Service Area Code (SAC) consists of 2 octets. Bit 8 of Octet 11 is the most significant bit and bit 1 of Octet 12 the least significant bit. The SAC is defined by the operator.

RAI field:

The Location Area Code (LAC) consists of 2 octets. Bit 8 of Octet 9 is the most significant bit and bit 1 of Octet 10 the least significant bit. The coding of the location area code is the responsibility of each administration. Coding using full hexadecimal representation shall be used.

The Routing Area Code (RAC) consists of 2 octets. Only Octet 11 contains the RAC. Octet 12 is coded as all 1's (11111111). The RAC is defined by the operator.

TAI field:

The Tracking Area Code (TAC) consists of 2 octets. Bit 8 of Octet 9 is the most significant bit and bit 1 of Octet 10 the least significant bit. The coding of the tracking area code is the responsibility of each administration. Coding using full hexadecimal representation shall be used.

ECGI field:

The E-UTRAN Cell Identifier (ECI) consists of 28 bits. Bit 4 of octet 10 is the most significant bit and bit 1 of Octet 11 the least significant bit. The coding of the E-UTRAN cell identifier is the responsibility of each administration. Coding using full hexadecimal representation shall be used.

Format

Octet string

Length

Varies based on the type of identity

Chapter 11
SGSN CDR Field Reference

This chapter provides a reference for CDR fields supported by the system for use in SGSN.

Listed below are the types of CDRs supported by SGSN:

- SGSN CDRs (S-CDRs)
- Mobility CDRs (M-CDRs)
- Mobile originated SMS CDRs (S-SMO-CDRs)
- Mobile terminated SMS CDRs (S-SMT-CDRs)

The SGSN provides CDRs that are compliant to the specifications identified in this chapter. When necessary and required, modifications to the standardized behavior can be implemented in different dictionaries which can be selected in the configuration file. This provides the flexibility to adapt to a customer's needs, e.g. to a legacy post-processing billing interface, while keeping the standard behavior for other needs.

A complete list and descriptions of supported CDR fields is provided in the *SGSN CDR Field Descriptions* chapter of this reference.

Important: For more information on custom dictionaries, contact your Cisco account representative.

The category column in all tables use keys described in the following table.

Table 23. Dictionary Table Key

Abbreviation	Meaning	Description
M	Mandatory	A field that must be present in the CDR.
C	Conditional	A field that must be present in a CDR if certain conditions are met.
OM	Operator Provisionable: Mandatory	A field that an operator has provisioned and must be included in the CDR for all conditions.
OC	Operator Provisionable: Conditional	A field that an operator has provisioned that must included in the CDR if certain conditions are met.
A	Added in Charging Gateway	A field included in the Charging Gateway.

CDR Fields Supported in S-CDRs

The tables in this section list the S-CDR fields present in the available GTPP dictionaries.

standard, custom1, custom2, custom4, custom5, custom7, custom9, custom12, custom13, custom15, custom16, custom19, custom20, custom21, custom22, custom24, custom25, custom26, custom28, custom30 Dictionaries

S-CDR fields for TS 32.215 v 4.5.0 (R4).

Field	Category	Description
Record Type	M	SGSN PDP context record.
Network Initiated PDP Context	OC	A flag that is present if this is a network-initiated PDP context.
Served IMSI	M	IMSI of the served party.
Served IMEI	OC	The IMEI of the ME, if available.
SGSN Address	OM	The IP address of the current SGSN.
MS Network Capability	OM	The Mobile Station Network Capability.
Routing Area Code (RAC)	OM	RAC at the time of “Record Opening Time”.
Location Area Code (LAC)	OM	LAC at the time of “Record Opening Time”.
Cell Identifier	OM	Cell identity for GSM or Service Area Code (SAC) for UMTS at the time of “Record Opening Time”.
Charging ID	M	PDP context identifier used to identify this PDP context in different records created by GSNs.
GGSN Address Used	M	The control plane IP address of the GGSN currently used. The GGSN address is always the same for an activated PDP context.
Access Point Name Network Identifier	OM	The logical name of the connected access point to the external packet data network (network identifier part of APN).
PDP Type	OM	PDP type, i.e. IP, PPP, IHOSS:OSP.
Served PDP Address	OC	PDP address of the served IMSI, i.e. IPv4 or IPv6. This parameter shall be present except when both the PDP type is PPP and dynamic PDP address assignment is used.
List of Traffic Data Volumes	OM	A list of changes in charging conditions for this PDP context, each change is time stamped. Charging conditions are used to categorise traffic volumes, such as per QoS/tariff period. Initial and subsequently changed QoS and corresponding data volumes are listed.
Record Opening Time	M	Time stamp when PDP context is activated in this SGSN or record opening time on subsequent partial records.

Field	Category	Description
Duration	M	Duration of this record in the SGSN.
SGSN Change	C	Present if this is first record after SGSN change.
Cause for Record Closing	M	The reason for closure of the record from this SGSN.
Diagnostics	OM	A more detailed reason for the release of the connection.
Record Sequence Number	C	Partial record sequence number in this SGSN. Only present in case of partial records.
Node ID	OM	Name of the recording entity.
Record Extensions	OC	A set of network operator/manufacturer specific extensions to the record. Conditioned upon the existence of an extension.
Local Record Sequence Number	OM	Consecutive record number created by this node. The number is allocated sequentially including all CDR types.
APN Selection Mode	OM	An index indicating how the APN was selected.
Access Point Name Operator Identifier	OM	The Operator Identifier part of the APN.
Served MSISDN	OM	The primary MSISDN of the subscriber.
Charging Characteristics	M	The Charging Characteristics applied to the PDP context.
System Type	OC	Indicates the type of air interface used, e.g. UTRAN. This field is present when either the UTRAN or GERAN air-interface is used. It is omitted when the service is provided by a GSM air interface.
RNC Unsent Downlink Volume	OC	The downlink data volume which the RNC has not sent to MS. This field is present when the RNC has provided unsent downlink volume count at RAB release.
Charging Characteristics Selection Mode	OM	Holds information about how Charging Characteristics were selected.

custom3 Dictionary

S-CDR fields for 32.215 v 4.5.0 (R4).

Field	Category	Description
Record Type	M	SGSN PDP context record.
Network Initiated PDP Context	OC	A flag that is present if this is a network-initiated PDP context.
Served IMSI	M	IMSI of the served party.
Served IMEI	OC	The IMEI of the ME, if available.

Field	Category	Description
SGSN Address	OM	The IP address of the current SGSN.
MS Network Capability	OM	The mobile station Network Capability.
Routing Area Code (RAC)	OM	RAC at the time of “Record Opening Time”.
Location Area Code (LAC)	OM	LAC at the time of “Record Opening Time”.
Cell Identifier	OM	Cell identity for GSM or Service Area Code (SAC) for UMTS at the time of “Record Opening Time”.
Charging ID	M	PDP context identifier used to identify this PDP context in different records created by GSNs.
GGSN Address Used	M	The control plane IP address of the GGSN currently used. The GGSN address is always the same for an activated PDP context.
Access Point Name Network Identifier	OM	The logical name of the connected access point to the external packet data network (network identifier part of APN).
PDP Type	OM	PDP type, i.e. IP, PPP, IHOSS:OSP.
Served PDP Address	OC	PDP address of the served IMSI, i.e. IPv4 or IPv6. This parameter shall be present except when both the PDP type is PPP and dynamic PDP address assignment is used.
List of Traffic Data Volumes	OM	A list of changes in charging conditions for this PDP context, each change is time stamped. Charging conditions are used to categorise traffic volumes, such as per QoS/tariff period. Initial and subsequently changed QoS and corresponding data volumes are listed.
Record Opening Time	M	Time stamp when PDP context is activated in this SGSN or record opening time on subsequent partial records.
Duration	M	Duration of this record in the SGSN.
SGSN Change	C	Present if this is first record after SGSN change.
Cause for Record Closing	M	The reason for closure of the record from this SGSN.
Diagnostics	OM	A more detailed reason for the release of the connection.
Record Sequence Number	C	Partial record sequence number in this SGSN. Only present in case of partial records.
Node ID	OM	Name of the recording entity.
Record Extensions	OC	A set of network operator/manufacturer specific extensions to the record. Conditioned upon the existence of an extension.
Local Record Sequence Number	OM	Consecutive record number created by this node. The number is allocated sequentially including all CDR types.
APN Selection Mode	OM	An index indicating how the APN was selected.
Access Point Name Operator Identifier	OM	The Operator Identifier part of the APN.

Field	Category	Description
Served MSISDN	OM	The primary MSISDN of the subscriber.
Charging Characteristics	M	The Charging Characteristics applied to the PDP context.
System Type	OC	Indicates the type of air interface used, e.g. UTRAN. This field is present when either the UTRAN or GERAN air-interface is used. It is omitted when the service is provided by a GSM air interface.
Charging Characteristics Selection Mode	OM	Holds information about how Charging Characteristics were selected.
pLMNIdentifier	OM	This field defines the PLMN identity (MCC and MNC) as part of the location information. It is present only if the option to include PLMN identity has been set by the operator. This field exists only for “custom3” dictionary.

Notes:

- All IP addresses are encoded in binary format.
- APN name length encoded.
- Context deactivation due to Inter-SGSN RAU results in final CDR with cause “SGSN Change” value:18 (decimal).
- The QoS parameters are present only if there is a QoS change in the previous container or last container of the previous CDR.

custom6 Dictionary

S-CDR fields for TS 32.298 v 6.6.0 (R6).

Field	Category	Description
Record Type	M	SGSN PDP context record.
Network Initiated PDP Context	OC	A flag that is present if this is a network-initiated PDP context.
Served IMSI	M	IMSI of the served party.
Served IMEI	OC	The IMEI of the ME, if available.
SGSN Address	OM	The IP address of the current SGSN.
MS Network Capability	OM	The mobile station Network Capability.
Routing Area Code (RAC)	OM	RAC at the time of “Record Opening Time”.
Location Area Code (LAC)	OM	LAC at the time of “Record Opening Time”.
Cell Identifier	OM	Cell identity for GSM or Service Area Code (SAC) for UMTS at the time of “Record Opening Time”.

Field	Category	Description
Charging ID	M	PDP context identifier used to identify this PDP context in different records created by GSNs.
GGSN Address Used	M	The control plane IP address of the GGSN currently used. The GGSN address is always the same for an activated PDP context.
Access Point Name Network Identifier	OM	The logical name of the connected access point to the external packet data network (network identifier part of APN).
PDP Type	OM	PDP type, i.e. IP, PPP, IHOSS:OSP.
Served PDP Address	OC	PDP address of the served IMSI, i.e. IPv4 or IPv6. This parameter shall be present except when both the PDP type is PPP and dynamic PDP address assignment is used.
List of Traffic Data Volumes	OM	A list of changes in charging conditions for this PDP context, each change is time stamped. Charging conditions are used to categorize traffic volumes, such as per tariff period. Initial and subsequently changed QoS and corresponding data volumes are also listed.
Record Opening Time	M	Time stamp when PDP context is activated in this SGSN or record opening time on subsequent partial records.
Duration	M	Duration of this record in the SGSN.
SGSN Change	C	Present if this is first record after SGSN change.
Cause for Record Closing	M	The reason for closure of the record from this SGSN.
Diagnostics	OM	A more detailed reason for the release of the connection.
Record Sequence Number	C	Partial record sequence number in this SGSN. Only present in case of partial records.
Node ID	OM	Name of the recording entity.
Local Record Sequence Number	OM	Consecutive record number created by this node. The number is allocated sequentially including all CDR types.
APN Selection Mode	OM	An index indicating how the APN was selected.
Access Point Name Operator Identifier	OM	The Operator Identifier part of the APN.
Served MSISDN	OM	The primary MSISDN of the subscriber.
Charging Characteristics	M	The Charging Characteristics applied to the PDP context.
RAT Type	OC	This field indicates the Radio Access Technology (RAT) type, e.g. UTRAN or GERAN, currently used by the Mobile Station as defined in TS 29.060.
RNC Unsent Downlink Volume	OC	The downlink data volume, which the RNC has not sent to MS. This field is present when the RNC has provided unsent downlink volume count at RAB release.
Charging Characteristics Selection Mode	OM	Holds information about how Charging Characteristics were selected.
Dynamic Address Flag	OC	Indicates whether served PDP address is dynamic, which is allocated during PDP context activation. This field is missing if address is static.

custom8 Dictionary

S-CDR fields for TS 32.298 v7.4.0.

Field	Category	Description
Record Type	M	SGSN PDP context record.
Network Initiated PDP Context	OC	A flag that is present if this is a network-initiated PDP context.
Served IMSI	M	IMSI of the served party.
Served IMEI	OC	The IMEI of the ME, if available.
SGSN Address	OM	The IP address of the current SGSN.
MS Network Capability	OM	The mobile station Network Capability.
Routing Area Code (RAC)	OM	RAC at the time of "Record Opening Time".
Location Area Code (LAC)	OM	LAC at the time of "Record Opening Time".
Cell Identifier	OM	Cell identity for GSM or Service Area Code (SAC) for UMTS at the time of "Record Opening Time".
Charging ID	M	PDP context identifier used to identify this PDP context in different records created by GSNs.
GGSN Address Used	M	The control plane IP address of the GGSN currently used. The GGSN address is always the same for an activated PDP context.
Access Point Name Network Identifier	OM	The logical name of the connected access point to the external packet data network (network identifier part of APN).
PDP Type	OM	PDP type, i.e. IP, PPP, IHOSS:OSP.
Served PDP Address	OC	PDP address of the served IMSI, i.e. IPv4 or IPv6. This parameter shall be present except when both the PDP type is PPP and dynamic PDP address assignment is used.
List of Traffic Data Volumes	OM	A list of changes in charging conditions for this PDP context, each change is time stamped. Charging conditions are used to categorize traffic volumes, such as per tariff period. Initial and subsequently changed QoS and corresponding data volumes are also listed.
Record Opening Time	M	Time stamp when PDP context is activated in this SGSN or record opening time on subsequent partial records.
Duration	M	Duration of this record in the SGSN.
SGSN Change	C	Present if this is first record after SGSN change.
Cause for Record Closing	M	The reason for closure of the record from this SGSN.
Diagnostics	OM	A more detailed reason for the release of the connection.

Field	Category	Description
Record Sequence Number	C	Partial record sequence number in this SGSN. Only present in case of partial records.
Node ID	OM	Name of the recording entity.
Record Extensions	OC	A set of network operator/manufacturer specific extensions to the record. Conditioned upon the existence of an extension.
Local Record Sequence Number	OM	Consecutive record number created by this node. The number is allocated sequentially including all CDR types.
APN Selection Mode	OM	An index indicating how the APN was selected.
Access Point Name Operator Identifier	OM	The Operator Identifier part of the APN.
Served MSISDN	OM	The primary MSISDN of the subscriber.
Charging Characteristics	M	The Charging Characteristics applied to the PDP context.
RAT Type	OC	This field indicates the Radio Access Technology (RAT) type, e.g. UTRAN or GERAN, currently used by the Mobile Station as defined in TS 29.060.
RNC Unsent Downlink Volume	OC	The downlink data volume, which the RNC has not sent to MS. This field is present when the RNC has provided unsent downlink volume count at RAB release.
Charging Characteristics Selection Mode	OM	Holds information about how Charging Characteristics were selected.
Dynamic Address Flag	OC	Indicates whether served PDP address is dynamic, which is allocated during PDP context activation. This field is missing if address is static.

Notes:

- Support for Direct Tunnel triggers.
- All IP addresses in Binary format.

custom10 and custom11 Dictionaries

S-CDR fields for TS 32.215 v4.5.0.

Field	Category	Description
Record Type	M	SGSN PDP context record.
Served IMSI	M	IMSI of the served party.
Served IMEI	OC	The IMEI of the ME, if available.
SGSN Address	OM	The IP address of the current SGSN.
MS Network Capability	OM	The mobile station Network Capability.

Field	Category	Description
Routing Area Code (RAC)	OM	RAC at the time of "Record Opening Time".
Location Area Code (LAC)	OM	LAC at the time of "Record Opening Time".
Cell Identifier	OM	Cell identity for GSM or Service Area Code (SAC) for UMTS at the time of "Record Opening Time".
Charging ID	M	PDP context identifier used to identify this PDP context in different records created by GSNs.
GGSN Address Used	M	The control plane IP address of the GGSN currently used. The GGSN address is always the same for an activated PDP context.
Access Point Name Network Identifier	OM	The logical name of the connected access point to the external packet data network (network identifier part of APN).
PDP Type	OM	PDP type, i.e. IP, PPP, IHOSS:OSP.
Served PDP Address	OC	PDP address of the served IMSI, i.e. IPv4 or IPv6. This parameter shall be present except when both the PDP type is PPP and dynamic PDP address assignment is used.
List of Traffic Data Volumes	OM	A list of changes in charging conditions for this PDP context, each change is time stamped. Charging conditions are used to categorise traffic volumes, such as per QoS/tariff period. Initial and subsequently changed QoS and corresponding data volumes are listed.
Record Opening Time	M	Time stamp when PDP context is activated in this SGSN or record opening time on subsequent partial records.
Duration	M	Duration of this record in the SGSN.
SGSN Change	C	Present if this is first record after SGSN change.
Cause for Record Closing	M	The reason for closure of the record from this SGSN.
DiagnosticsSM	OM	A more detailed reason for the release of the connection.
Record Sequence Number	C	Partial record sequence number in this SGSN. Only present in case of partial records.
Node ID	OM	Name of the recording entity
Record Extensions	OC	A set of network operator/manufacturer specific extensions to the record. Conditioned upon the existence of an extension.
Local Record Sequence Number	OM	Consecutive record number created by this node. The number is allocated sequentially including all CDR types.
APN Selection Mode	OM	An index indicating how the APN was selected.
Access Point Name Operator Identifier	OM	The Operator Identifier part of the APN.
Served MSISDN	OM	The primary MSISDN of the subscriber.
Charging Characteristics	M	The Charging Characteristics applied to the PDP context.

Field	Category	Description
System Type	OC	Indicates the type of air interface used, e.g. UTRAN. This field is present when either the UTRAN or GERAN air-interface is used. It is omitted when the service is provided by a GSM air interface.
CAMEL Information	OC	A set of CAMEL information related to PDP context. For more information see section *Description of Record Fields*. This field is present if CAMEL service is activated.
Prepaid Info	OM	This identifier refers to the network address (E.164 number) of the pre-paid system.
RNC Unsent Downlink Volume	OC	The downlink data volume which the RNC has not sent to MS. This field is present when the RNC has provided unsent downlink volume count at RAB release.
Charging Characteristics Selection Mode	OM	Holds information about how Charging Characteristics were selected.

Notes:

- Two new optional fields currently not supported: MS Radio Access Capability and Prepaid-Info.
- No support for choice-id attributes. All IP addresses are plainly encoded in Binary format without any preceding tag value to identify their type. Hence, encoding the attributes in the given order is important.
- Diagnostics has been replaced by DiagnosticsSM which is of type octet string and has size of one byte.
- Charging-id and LRSN have a fixed length as 4bytes.
- Timestamp does not have time-zone offset and is of size 6 bytes.
- Tag value for changeOfCharCondition changed from “0x30” to “0xA0”.
- DynamicAddressflag attribute is not encoded.
- SystemType attribute is not encoded if the value is “GERAN”.
- Context deactivation due to Inter-SGSN RAU results in final CDR with cause “SGSN Change” value:18 (decimal)

custom13 Dictionary

S-CDR fields for TS 32.298 v 6.6.0 (R6).

Field	Category	Description
Record Type	M	SGSN PDP context record.
Network Initiated PDP Context	OC	A flag that is present if this is a network-initiated PDP context.
Served IMSI	M	IMSI of the served party.
Served IMEI	OC	The IMEI of the ME, if available.
SGSN Address	OM	The IP address of the current SGSN.
MS Network Capability	OM	The mobile station Network Capability.

Field	Category	Description
Routing Area Code (RAC)	OM	RAC at the time of "Record Opening Time".
Location Area Code (LAC)	OM	LAC at the time of "Record Opening Time".
Cell Identifier	OM	Cell identity for GSM or Service Area Code (SAC) for UMTS at the time of "Record Opening Time".
Charging ID	M	PDP context identifier used to identify this PDP context in different records created by GSNs.
GGSN Address Used	M	The control plane IP address of the GGSN currently used. The GGSN address is always the same for an activated PDP context.
Access Point Name Network Identifier	OM	The logical name of the connected access point to the external packet data network (network identifier part of APN).
PDP Type	OM	PDP type, i.e. IP, PPP, IHOSS:OSP.
Served PDP Address	OC	PDP address of the served IMSI, i.e. IPv4 or IPv6. This parameter shall be present except when both the PDP type is PPP and dynamic PDP address assignment is used.
List of Traffic Data Volumes	OM	A list of changes in charging conditions for this PDP context, each change is time stamped. Charging conditions are used to categorize traffic volumes, such as per tariff period. Initial and subsequently changed QoS and corresponding data volumes are also listed.
Record Opening Time	M	Time stamp when PDP context is activated in this SGSN or record opening time on subsequent partial records.
Duration	M	Duration of this record in the SGSN.
SGSN Change	C	Present if this is first record after SGSN change.
Cause for Record Closing	M	The reason for closure of the record from this SGSN.
Diagnostics	OM	A more detailed reason for the release of the connection.
Record Sequence Number	C	Partial record sequence number in this SGSN. Only present in case of partial records.
Node ID	OM	Name of the recording entity.
Record Extensions	OC	A set of network operator/manufacturer specific extensions to the record. Conditioned upon the existence of an extension.
Local Record Sequence Number	OM	Consecutive record number created by this node. The number is allocated sequentially including all CDR types.
APN Selection Mode	OM	An index indicating how the APN was selected.
Access Point Name Operator Identifier	OM	The Operator Identifier part of the APN.
Served MSISDN	OM	The primary MSISDN of the subscriber.
Charging Characteristics	M	The Charging Characteristics applied to the PDP context.

Field	Category	Description
RAT Type	OC	This field indicates the Radio Access Technology (RAT) type, e.g. UTRAN or GERAN, currently used by the Mobile Station as defined in TS 29.060.
RNC Unsent Downlink Volume	OC	The downlink data volume, which the RNC has not sent to MS. This field is present when the RNC has provided unsent downlink volume count at RAB release.
Charging Characteristics Selection Mode	OM	Holds information about how Charging Characteristics were selected.
Dynamic Address Flag	OC	Indicates whether served PDP address is dynamic, which is allocated during PDP context activation. This field is missing if address is static.

Notes:

- The IP address is in binary format.
- Context deactivation due to Inter-SGSN RAU results in final CDR with cause “SGSN Change” value:18 (decimal).

custom14 Dictionary

S-CDR fields for TS 32.298 v 6.4.1 (R6).

Field	Category	Description
Record Type	M	SGSN PDP context record.
Served IMSI	M	IMSI of the served party.
Served IMEI	O	The IMEI of the ME, if available.
SGSN Address	M	The IP address of the current SGSN.
MS Network Capability	O	The mobile station Network Capability.
Routing Area Code (RAC)	O	RAC at the time of “Record Opening Time”.
Location Area Code (LAC)	O	LAC at the time of “Record Opening Time”.
Cell Identifier	O	Cell identity for GSM or Service Area Code (SAC) for UMTS at the time of “Record Opening Time”.
Charging ID	M	PDP context identifier used to identify this PDP context in different records created by GSNs.
GGSN Address Used	M	The control plane IP address of the GGSN currently used. The GGSN address is always the same for an activated PDP context.
Access Point Name Network Identifier	M	The logical name of the connected access point to the external packet data network (network identifier part of APN).
PDP Type	O	PDP type, i.e. IP, PPP, IHOSS:OSP.

Field	Category	Description
Served PDP Address	M	PDP address of the served IMSI, i.e. IPv4 address. This parameter shall be present except when both the PDP type is PPP and dynamic PDP address assignment is used.
List of Traffic Data Volumes	M	A list of changes in charging conditions for this PDP context, each change is time stamped. Charging conditions are used to categorize traffic volumes, such as per tariff period. Initial and subsequently changed QoS and corresponding data volumes are also listed.
Change Of Charging Condition	M	Each traffic volume container contains details related to a charging condition . A new container is usually created for a QoS change and for tariff changes.
QoS Requested	O	Identifies the QoS requested by the MS during PDP context activation.
QoS Negotiated	O	Indicates the QoS agreed to by the network.
Data volume GPRS Uplink	M	Indicates the number of downlink octets transmitted during the specified time frame.
Data volume GPRS Downlink	M	Indicates the number of uplink octets received during the specified time frame.
Change Condition	M	Field identifies the reason for closing the container as part of the Change of Charging Condition.
Change time	M	Field identifies the local time when a change condition (for example, record closure) occurred and the container was closed.
Record Opening Time	M	Time stamp when PDP context is activated in this SGSN or record opening time on subsequent partial records.
Duration	M	Duration of this record in the SGSN.
SGSN Change	O	Present if this is first record after SGSN change.
Cause for Record Closing	M	The reason for closure of the record from this SGSN.
Diagnostics	O	A more detailed reason for the release of the connection.
Record Sequence Number	O	Partial record sequence number in this SGSN. Only present in case of partial records.
Node ID	O	Name of the recording entity.
Management Extensions	M	This is a proprietary field which enables network operators and/or manufacturers to add their own information to the standard record definitions.
Ticket LayOut Version	M	This field contains the version of the client ticket layout.
Recovery Flag	O	This parameter contains the information to indicate that the record is written after a recovery.
DiagnosticsMM	O	This field contains the System's internal reasons for the PDP context de-activation at Session Management (SM) level.
subCharacteristics	M	This parameter contains the first octet of the charging characteristics which indicates the type of billing used.
Local Record Sequence Number	O	Consecutive record number created by this node. The number is allocated sequentially including all CDR types.

Field	Category	Description
APN Selection Mode	O	An index indicating how the APN was selected.
Access Point Name Operator Identifier	M	The Operator Identifier part of the APN.
Served MSISDN	O	The primary MSISDN of the subscriber.
Charging Characteristics	M	The Charging Characteristics applied to the PDP context.
RAT Type	O	This field indicates the Radio Access Technology (RAT) type, e.g. UTRAN or GERAN, currently used by the Mobile Station as defined in TS 29.060.
RNC Unsent Downlink Volume	OC	The downlink data volume, which the RNC has not sent to MS. This field is present when the RNC has provided unsent downlink volume count at RAB release.

Notes:

- QoS fields are only defined for a maximum length of “12”.
- The S-CDR contains the 'Management Extension' Field with 'ticketLayoutVersion", "subCharacteristics" and "recoveryFlag". The "recovery Flag" is optional and is sent in S-CDR only if its value is "0x01". The "recovery Flag" is set in S-CDR if the PDP is terminated due to system failure.
- DiagnosticsMM and DiagnosticsSM are present in the S-CDR. The tag values of these diagnostics values are different (Diagnostics MM is included in Management extensions field).

custom17 Dictionary

Important: The custom17 dictionary is supported in Star OS 9.0 releases and later.

Important: The custom17 dictionary is ASCII encoded.

Field	Category	Description
Common Part		
Record Type	M	The CDR type.
Potential Duplicate	A	This value is set always Zero. VF-NZ used HDD and there is no possibility of duplicates (Duplicates are applicable only in case when CDRs are transferred over the network).
System Type	A	This value is always set to 3. This indicates the CG Release Version.
Record Sequence Number	A	This field contains a unique incrementing sequence number which CG generates. The number is represented as decimal digits [0...9] and unused space is padded with zeroes (for example, 000000000012).
Served IMSI	M	This field contains an IMSI number. The number is represented as decimal digits [0...9], filled from right and unused space is padded with zeroes (for example, 0234150101667123).

Field	Category	Description
Record Opening Time	M	This field contains the timestamp (GMT) when PDP context is activated or the record opening time of the first partial record. For SMS CDRs, this field contains the Event Time Stamp. For M-CDRs, the field contains the Record Opening.
Partially Common Part		
Served IMEI	C	This field contains the international mobile equipment identity.
NAPI for MSISDN	O	The value for Numbering Plan Indicator, Nature of Address Indicator and Extension Indicator.
Served MSISDN	M	This field contains the MSISDN number of the mobile terminal.
SGSN Address	M	List of SGSN addresses used during this record (IPv6 encoded).
GGSN Address	M	List of GGSN addresses used during this record (IPv6 encoded).
Charging ID	M	This field contains the PDP context identifier. This ID and the GGSN address are then concatenated for unique identification of the same PDP context records.
Access Point Name	M	This field contains a logical Access Point Name (APN), which is used to determine the actual connected access point.
Served PDP Type Org	M	The PDP type defines the end user protocol to be used between the external packet data network and the MS and is divided into Organization field and a Number field. The PDP Type Organization is the organization that is responsible for the PDP Type Number field and the PDP Address format.
Served PDP Type Number	M	PDP type, i.e. IP, PPP, or IHOSS:OSP.
Served PDP Address	M	PDP address of the served IMSI, i.e. IPv4 or IPv6. This parameter shall be present except when both the PDP type is PPP and dynamic PDP address assignment is used (IPv6 encoded).
MS NW Capability	O	The Mobile Station Network Capability.
Location Area Code	O	This field contains the location area at the time of record creation.
Routing Area	O	This field contains the routing area at the time of record creation.
Cell Identity	O	This field contains the cell ID at the time of record creation.
SGSN Change	C	This field indicates that this is the first record after an SGSN change.
Diagnostics 1	O	Procedure code for the SGSN.
Diagnostics 2	O	Initiation code for the SGSN.
Diagnostics 3	O	Process family identifier.
Diagnostics 4	O	Cause for the SGSN error.
Diagnostics 5	O	Internal cause for the SGSN error.
Charging Characteristics	M	The charging characteristics field contains the user's charging characteristics. It describes the type of the CDR. The field can contain a charging type value, added with cell update bit (assuming the cell ID in S-CDR feature is on). For example, the value 20 means that the charging type is Prepaid and cell accuracy charging is used.

Field	Category	Description
S-CDR Part		
PDP HLR Index	M	The PDP HLR index shows the access information on the server-based prepaid charging. This access information is stored in the HLR. It is retrieved when a user wants to call using the server-based prepaid charging.
Network Initiated PDP Context	C	This flag indicates who initiated the PDP context.
S-Cause for Record Closing	M	This field contains a detailed reason for the release of the record in this SGSN.
S-Complete	A	S-Complete" field is "0" for first and intermediate partial CDR, and "1" for the final CDR (i.e. CDR generated at PDP termination).
S-Uplink	M	Cumulative number of bytes transmitted from the MT since the opening of the PDP context.
S-Downlink	M	Cumulative number of bytes transmitted to the MT since the opening of the PDP context.
S-Quality of Service Requested	M	Quality of Service Requested contains the QoS that the MS wanted at the activation of the PDP context. The first container includes following optional fields: QoS (Quality of Service) Requested (not in G-CDR) and QoS Negotiated. In following containers QoS Negotiated is present if previous change condition is QoS change. Rules for determining R99 attributes from R97/98 attributes are defined in 3rd Generation Partnership Project; QoS Concept and Architecture (3GPP TS 23.107 V4.5.0). Two last bytes are used in SGSN 3.1.
S-Quality of Service Requested	M	Quality of Service Negotiated indicates the applied QoS that the network accepted. Two last bytes are used in SGSN 3.1.
S-Record Opening Time	M	This indicates the record opening local time.
S-Opening Timezone	M	This indicates the record opening time zone.
S-Timestamp	M	This field represents the time when the SGSN closed the last received CDR.
S-Closing Timezone	M	This indicates the record closure time zone.
S-First Sequence Number	C	The "S-First Sequence Number = S-LAST Sequence Number" and these sequence numbers must be incremented for each partial CDRs generated for that PDP context.
S-Last Sequence Number	A	The "S-First Sequence Number = S-LAST Sequence Number" and these sequence numbers must be incremented for each partial CDRs generated for that PDP context.
S-Duration	M	Duration of this record in the SGSN.
G-CDR Part		
G-CDR Part	M	This is not applicable for S-CDRs and always should be padded with zero.
M-CDR Part		
M-CDR Part	M	This is not applicable for S-CDRs and always should be padded with zero.
SMS-CDR Part		

Field	Category	Description
SMS-CDR Part	M	This is not applicable for S-CDRs and always should be padded with zero.

custom18 Dictionary

S-CDR fields for TS 32.215 v4.5.0.

Field	Category	Description
Record Type	M	SGSN PDP context record.
Network Initiated PDP Context	M	A flag that is present if this is a network-initiated PDP context.
Served IMSI	M	IMSI of the served party.
Served IMEI	M	The IMEI of the ME, if available.
SGSN Address	M	The IP address of the current SGSN.
MS Network Capability	M	The mobile station Network Capability.
Routing Area Code (RAC)	M	RAC at the time of “Record Opening Time”.
Location Area Code (LAC)	M	LAC at the time of “Record Opening Time”.
Cell Identifier	M	Cell identity for GSM or Service Area Code (SAC) for UMTS at the time of “Record Opening Time”.
Charging ID	M	PDP context identifier used to identify this PDP context in different records created by GSNs.
GGSN Address Used	M	The control plane IP address of the GGSN currently used. The GGSN address is always the same for an activated PDP context.
Access Point Name (Ni +OI)	M	The logical name of the connected access point to the external packet data network (network identifier part of APN). This should include NI+OI part. The length is 101 bytes.
PDP Type	M	PDP type, i.e. IP, PPP, IHOSS:OSP.
Served PDP Address	M	PDP address of the served IMSI, i.e. IPv4 or IPv6. This parameter shall be present except when both the PDP type is PPP and dynamic PDP address assignment is used. The length of the field is 16 byte.
List of Traffic Data Volumes	M	A list of changes in charging conditions for this PDP context, each change is time stamped. Charging conditions are used to categorize traffic volumes, such as per tariff period. Initial and subsequently changed QoS and corresponding data volumes are also listed.
Record Opening Time	M	Time stamp when PDP context is activated in this SGSN or record opening time on subsequent partial records.
Duration	M	Duration of this record in the SGSN.
SGSN Change	M	Present if this is first record after SGSN change.
Cause for Record Closing	M	The reason for closure of the record from this SGSN.

Field	Category	Description
Diagnostics 1	M	A more detailed reason for the release of the connection.
Diagnostics 2	M	A more detailed reason for the release of the connection.
Diagnostics 3	M	A more detailed reason for the release of the connection.
Diagnostics 4	M	A more detailed reason for the release of the connection.
Diagnostics 5	M	A more detailed reason for the release of the connection.
Record Sequence Number	M	Partial record sequence number in this SGSN. Only present in case of partial records.
Local Record Sequence Number	M	Consecutive record number created by this node. The number is allocated sequentially including all CDR types.
Served MSISDN	M	The primary MSISDN of the subscriber.
Charging Characteristics	M	The Charging Characteristics applied to the PDP context.
CHARGING CHARACTERISTICS PROFILE INDEX	M	Indicates the Charging Profile Index.
PDP HLR Index	M	Indicates the PDP HLR index

Notes:

- The S-CDRs are encoded in fixed length format.
- All fields are mandatory. If not present they should be sent as 0 except in case of IMEI which shall be sent as ffffffffffffffff in case if it is not present.
- The APN name is a combination of OI and NI.
- QoS negotiated/requested fields are present in all containers.
- custom18 supports additional “CELL CHANGE” trigger which generates a partial S-CDR.
- Node-id and Dynamic fields are not encoded in this format.
- The “PDP Type Org” is encoded as 0x01 for IPV4-IETF (As per the 3GPP spec, this field is encoded as 0xf1).
- The “record sequence number” is present in all S-CDRs (Even if a session generates a final SCDR without any interims).

custom27 dictionary

S-CDR fields for TS 32.215 v 4.5.0 (R4).

Field	Category	Description
Record Type	M	SGSN PDP context record.
Served IMSI	M	IMSI of the served party.
Served IMEI	OC	IMEI of the ME, if available.
Served MSISDN	OM	The primary MSISDN of the subscriber.

Field	Category	Description
SGSN Address	OM	The IP address of the current SGSN.
Charging ID	M	PDP context identifier used to identify this PDP context in different records created by GSNs.
GGSN Address Used	M	The control plane IP address of the GGSN currently used. The GGSN address is always the same for an activated PDP context.
APN Selection Mode	OM	An index indicating how the APN was selected.
PDP Type	OM	PDP type, i.e. IP, PPP, or IHOSS:OSP.
Served PDP Address	OC	PDP address, i.e. IPv4 or IPv6 address. This parameter shall be present except when both the PDP type is PPP and dynamic PDP address assignment is used.
Charging Characteristics	M	The Charging Characteristics applied to the PDP content.
Charging Characteristics Selection Mode	OM	Holds information about how Charging Characteristics were selected.
Dynamic Address Flag	OC	The presence of this field indicates that the Served PDP Address was dynamically assigned during context activation.
MS Network Capability	OM	The Mobile Station Network Capability.
Node ID	M	Name of the recording entity.
Access Point Name Network Identifier	M	The logical name of the connected access point to the external packet data network (network identifier part of APN).
Access Point Name Operator Identifier	M	The Operator Identifier part of the APN.
System Type	OC	Indicates the type of air interface used, e.g. UTRAN. This field is present when either the UTRAN or GERAN air-interface is used. It is omitted when the service is provided by a GSM air interface.
Record Opening Time	M	Time stamp when PDP context is activated in this GGSN or record opening time on subsequent partial records.
Duration	M	Duration of this record in the GGSN.
Cause for Record Closing	M	The reason for the release of record from this SGSN.
List of Traffic Data Volumes	M	A list of changes in charging conditions for this PDP context, each time stamped. Charging conditions are used to categorize traffic volumes, such as per tariff period. Initial and subsequently changed QoS and corresponding data values are also listed.
Routing Area Code (RAC)	OM	Contains the RA code of the area where the MS is located when the (partial) record is opened.
Location Area Code	OM	Contains the Location Area Code of the area where the MS is located when the (partial) record is opened.

Field	Category	Description
Cell Identifier	OM	Contains the CI (GSM) or the SAC (WCDMA) of the cell where the MS is located when the S-CDR is opened. The first partial or single S-CDR reports the current cell identifier at PDP context activation. For any subsequent partial S-CDRs, the accuracy of the reported cell identifier is limited to the cell identifier for the last RA update reported by the MS.
SGSN Change	C	Indicate that this is the first record after an inter-SGSN routing area update in new SGSN and an intra-SGSN inter-system change.
Record Sequence Number	C	Partial record sequence number, only present in case of partial records.
Local Record Sequence Number	M	Consecutive record number created by this node. The number is allocated sequentially including all CDR types.

Notes:

- The indefinite length ASN encoding is used. i.e no length part which indicates the total length of CDR.
- All IP addresses are in binary format.
- All bools are encoded as 0x01 (In ASN STD 3GPP they are encoded as 0xff).
- RNCUnsent Volume field is not present.
- The QOS length should limited to max of 12 bytes irrespective of what was requested/negotiated.
- ISRAU 'cause for record closure' is the SGSN Change.
- IMEISV shall be sent if available else IMEI shall be sent.
- System Type field is present in S-CDR only if access type is UTRAN.
- In the case of intra-sgsn-inter-system change (2G<->3G handover within same box), the cause for record closure is ‘SGSN Change’.
- The fields should be sent in same order as per the they are listed in table.

custom29 Dictionary

S-CDR fields for TS 32.215 v4.5.0.

Field	Category	Description
Record Type	M	SGSN PDP context record.
Network Initiated PDP Context	OC	A flag that is present if this is a network-initiated PDP context.
Served IMSI	M	IMSI of the served party.
Served IMEI	OC	The IMEI of the ME, if available.
SGSN Address	OM	The IP address of the current SGSN.
MS Network Capability	OM	The mobile station Network Capability.
Routing Area Code (RAC)	OM	RAC at the time of “Record Opening Time”.

Field	Category	Description
Location Area Code (LAC)	OM	LAC at the time of "Record Opening Time".
Cell Identifier	OM	Cell identity for GSM or Service Area Code (SAC) for UMTS at the time of "Record Opening Time".
Charging ID	M	PDP context identifier used to identify this PDP context in different records created by GSNs.
GGSN Address Used	M	The control plane IP address of the GGSN currently used. The GGSN address is always the same for an activated PDP context.
Access Point Name Network Identifier	OM	The logical name of the connected access point to the external packet data network (network identifier part of APN).
PDP Type	OM	PDP type, i.e. IP, PPP, IHOSS:OSP.
Served PDP Address	OC	PDP address of the served IMSI, i.e. IPv4 or IPv6. This parameter shall be present except when both the PDP type is PPP and dynamic PDP address assignment is used.
List of Traffic Data Volumes	OM	A list of changes in charging conditions for this PDP context, each change is time stamped. Charging conditions are used to categorize traffic volumes, such as per tariff period. Initial and subsequently changed QoS and corresponding data volumes are also listed.
Record Opening Time	M	Time stamp when PDP context is activated in this SGSN or record opening time on subsequent partial records.
Duration	M	Duration of this record in the SGSN.
SGSN Change	C	Present if this is first record after SGSN change.
Cause for Record Closing	M	The reason for closure of the record from this SGSN.
Diagnostics	OM	A more detailed reason for the release of the connection.
Record Sequence Number	C	Partial record sequence number in this SGSN. Only present in case of partial records.
Node ID	OM	Name of the recording entity.
Local Record Sequence Number	OM	Consecutive record number created by this node. The number is allocated sequentially including all CDR types.
APN Selection Mode	OM	An index indicating how the APN was selected.
Access Point Name Operator Identifier	OM	The Operator Identifier part of the APN.
Served MSISDN	OM	The primary MSISDN of the subscriber.
Charging Characteristics	M	The Charging Characteristics applied to the PDP context.
RAT Type	OC	This field indicates the Radio Access Technology (RAT) type, e.g. UTRAN or GERAN, currently used by the Mobile Station as defined in TS 29.060.
RNC Unsent Downlink Volume	OC	The downlink data volume, which the RNC has not sent to MS. This field is present when the RNC has provided unsent downlink volume count at RAB release.

Field	Category	Description
Charging Characteristics Selection Mode	OM	Holds information about how Charging Characteristics were selected.
Dynamic Address Flag	OC	Indicates whether served PDP address is dynamic, which is allocated during PDP context activation. This field is missing if address is static.

Notes: This record is a standard R4 CDR format.

- The MSISDN field has only the actual MSISDN part in G-CDR. that is it does not have the Nature of Address and Numbering Plan indicator.
- All IP addresses are in binary format and not in ASCII format. (This is not a deviation with respect to 3GPP).
- The QoS length should be restricted to 12 bytes. The QoS is truncated to R4 Qos format.

custom31 Dictionary

S-CDR fields for TS 32.298 v6.4.1(R6).

Field	Category	Description
Record Type	M	SGSN PDP context record.
Network Initiated PDP Context	O	A flag that is present if this is a network-initiated PDP context.
Served IMSI	M	IMSI of the served party.
Served IMEI	O	The IMEI of the ME, if available.
SGSN Address	M	The IP address of the current SGSN.
MS Network Capability	O	The Mobile Station Network Capability.
Routing Area Code (RAC)	O	Routing Area Code at the "Record Opening Time".
Location Area Code (LAC)	O	Location Area Code at the "Record Opening Time".
Cell Identifier	O	Cell identity for GSM or Service Area Code (SAC) for UMTS at the "Record Opening Time".
Charging ID	M	PDP context identifier used to identify this PDP context in different records created by GSNs.
GGSN IPv4 Binary Address Used	M	The control plane IP address of the GGSN currently used. The GGSN address is always the same for an activated PDP context.
Access Point Name Network Identifier	M	The logical name of the connected Access Point to the external Packet Data Network (Network Identifier part of APN).
PDP Type	O	PDP type, i.e. IP, PPP, IHOSS:OSP.
Served PDP Address	O	The served PDP address supports both IPV4/IPV6 address.

Field	Category	Description
List of Traffic Data Volumes	M	A list of changes in charging conditions for this PDP context, each time stamped. Charging conditions are used to categorize traffic volumes, such as per tariff period. Initial and subsequently changed QoS and corresponding data values are also listed.
Record Opening Time	M	Time stamp when PDP context is activated in this SGSN or record opening time on subsequent partial records.
Duration	M	Duration of this record in the SGSN.
SGSN Change	O	Present if this is first record after SGSN change.
Cause for Record Closing	M	The reason for closure of the record from this SGSN.
DiagnosticsSM	O	A more detailed reason for the release of the connection.
Record Sequence Number	O	Partial record sequence number in this SGSN. Only present in case of partial records.
Node ID	O	Name of the recording entity.
Local RecordSequence Number	O	Consecutive record number created by this node. The number is allocated sequentially including all CDR types.
APN Selection Mode	O	An index indicating how the APN was selected.
Access Point Name Operator Identifier	M	The Operator Identifier part of the APN.
Served MSISDN	O	The primary MSISDN of the subscriber.
Charging Characteristics	M	The Charging Characteristics applied to the PDP context.
RAT Type	O	This field indicates the Radio Access Technology (RAT) type, for example, UTRAN or GERAN, currently used by the Mobile Station as defined in TS 29.060.
SCF Address	O	This field is currently not supported. And will be blank.
Service Key	O	This field identifies the CAMEL service logic applied.
Default Transaction/ SMS Handling	O	This field indicates whether or not a CAMEL encountered default GPRS or SMS-handling.
Number of DPs encountered	O	The number of armed CAMEL detection points (TDP and EDP) encountered and complements the "Level of CAMEL service" field.
Level of CAMEL services	O	This field describes the complexity of CAMEL invocation.
RNC Unsent Downlink Volume	O	The downlink data volume, which the RNC has not sent to MS. This field is present when the RNC has provided unsent downlink volume count at RAB release.
Charging Characteristics Selection Mode	O	Holds information about how Charging Characteristics were selected.
Dynamic Address Flag	O	Indicates whether served PDP address is dynamic, which is allocated during PDP context activation. This field is missing if address is static.

Field	Category	Description
pLMNIdentifier	O	This field defines the PLMN identity (MCC and MNC) as part of the location information. It is present only if the option to include PLMN identity has been set by the operator. This field is specific to this dictionary.

Notes:

- The GGSN Address is a Binary IPv4 address.

custom33 Dictionary

S-CDR fields for TS 32.298 v6.0.0.

Field	Category	Description
Record Type	M	SGSN PDP context record.
Served IMSI	M	IMSI of the served party.
Served IMEI	O	The IMEI of the ME, if available.
Served MSISDN	O	The primary MSISDN of the subscriber.
SGSN IPv4 Binary Address	M	The IP address of the current SGSN.
Charging ID	M	PDP context identifier used to identify this PDP context in different records created by GSNs.
GGSN IPv4 Binary Address Used	M	The control plane IP address of the GGSN currently used. The GGSN address is always the same for an activated PDP context.
APN Selection Mode	O	An index indicating how the APN was selected.
PDP Type	O	PDP type, i.e. IP, PPP, IHOSS:OSP.
Served PDP Address	O	The served PDP address supports both IPV4/IPV6 address.
PDP IP Address	M	The address can be in either an IPv4 or an IPv6 binary format.
IPv4 Binary Address OR IPv6 Binary Address	M	This field contains an IPv4 address in hexadecimal format. OR This field contains an IPv6 address in hexadecimal format.
Charging Characteristics	M	The charging characteristics (cc) applied to the PDP context.
Charging Characteristics Selection Mode	O	Includes information about how charging characteristics (CC) were selected. Supported values: • subscriptionSpecific (1) • aPNSpecific (2) • homeDefault (3)
Dynamic Address Flag	O	Indicates whether served PDP address is dynamic, which is allocated during PDP context activation. This field is missing if address is static.
MS Network Capability	O	The mobile station Network Capability.
Node ID	M	Name of the recording entity.

Field	Category	Description
Access Point Name Network Identifier	M	The logical name of the connected access point to the external packet data network (network identifier part of APN).
Access Point Name Operator Identifier	M	The Operator Identifier part of the APN.
System Type	O	Indicates the type of air interface used, e.g. UTRAN. This field is present when either the UTRAN or GERAN air-interface is used. It is omitted when the service is provided by a GSM air interface.
Record Opening Time	M	Time stamp when PDP context is activated in this SGSN or record opening time on subsequent partial records.
Duration	M	Duration of this record in the SGSN.
Cause for Record Closing	M	The reason for closure of the record from this SGSN. Supported values: • normalRelease (0) • abnormalRelease (4) • volumeLimit (16) • timeLimit (17) • sgsnChange (18) • maxChangeCond (19) • managementIntervention (20) • Rat Change (22) • plmn change (101)
List of Traffic Volumes	M	A list of changes in charging conditions for this PDP context. Each change is time stamped. Charging conditions are used to categorize traffic volumes, such as per QoS/tariff period. Initial and subsequently changed QoS and corresponding data volumes are listed.
ChangeOfCharCondition	M	Identifies details related to the change in the charging conditions.
QoS Requested	O	Identifies the QoS requested by the MS during PDP context activation.
QoS Negotiated	O	Indicates the QoS agreed to by the network.
Data Volume GPRS Uplink	M	Indicates the number of downlink octets transmitted during the specified timeframe.
Data Volume GPRS Downlink	M	Indicates the number of uplink octets received during the specified timeframe.
Change Condition	M	Field identifies the reason for closing the container as part of the Change of Charging Condition.
Change Time	M	Field identifies the local time when a change condition (e.g., record closure) occurred and the container was closed.
pLMNIdentifier	M	This field defines the PLMN identity (MCC and MNC) as part of the location information. It is present only if the option to include PLMN identity has been set by the operator.
Routing Area	O	Routing area code (RAC) at the time of “Record Opening Time”.

Field	Category	Description
Location Area Code	O	Location area code (LAC) at the time of "Record Opening Time".
Cell Identifier	O	Cell identity for GSM or Service Area Code (SAC) for UMTS at the time of "Record Opening Time".
Record Sequence Number	C	Partial record sequence number in this SGSN. Only present in case of partial records.
Local Record Sequence Number	M	Consecutive record number created by this node. The number is allocated sequentially including all CDR types.

CDR Fields Supported in S-SMO-CDRs

The tables in this section list the S-SMO-CDR fields present in the available GTPP dictionaries.

standard, custom1 – custom30 Dictionaries

For TS 32.215 v4.5.0 (R4) / 32.298 v7.4.0 (R7)

Field	Category	Description
Record Type	M	SGSN Mobile Originated SMS.
Served IMSI	M	The IMSI of the subscriber.
Served IMEI	OC	The IMEI of the ME, if available.
Served MSISDN	OM	The primary MSISDN of the subscriber.
MS Network Capability	OM	The mobile station network capability.
Service Centre	OM	The address (E.164) of the SMS-service centre.
Recording Entity	OM	The E.164 number of the SGSN.
Location Area Code	OM	The Location Area Code from which the message originated.
Routing Area Code	OM	The Routing Area Code from which the message originated.
Cell Identifier	OM	The Cell Identity for GSM or Service Area Code (SAC) for UMTS from which the message originated.
Message Reference	M	A reference provided by the MS uniquely identifying this message.
Event Time Stamp	M	The time at which the message was received by the SGSN from the subscriber.
SMS Result	C	The result of the attempted delivery if unsuccessful.
Record Extensions	OC	A set of network operator/ manufacturer specific extensions to the record. Conditioned upon the existence of an extension.
Node ID	OM	Name of the recording entity.
Local Record Sequence Number	OM	Consecutive record number created by this node. The number is allocated sequentially including all CDR types.
Charging Characteristics	M	The Charging Characteristics flag set used by the SGSN.
System Type	OC	Indicates the type of air interface used, e.g. UTRAN. This field is present when either the UTRAN or GERAN air-interface is used. It is omitted when the service is provided by a GSM air interface.
Destination Number	OM	The destination short message subscriber number.
Charging Characteristics Selection Mode	OM	Holds information about how Charging Characteristics were selected.

Important: Based on TS 32.215 v4.5.0 (R4) or TS 32.298 v7.4.0 (R7). The only difference is that from R6 onwards the “System Type” field is renamed to “RAT Type”.

CDR Fields Supported in S-SMT-CDRs

The tables in this section list the S-SMT-CDR fields present in the available GTPP dictionaries.

standard, custom1 – custom30 Dictionaries

For TS 32.215 v4.5.0 (R4) / TS 32.298 v7.4.0 (R7).

Field	Category	Description
Record Type	M	SGSN Mobile Terminated SMS.
Served IMSI	M	The IMSI of the subscriber.
Served IMEI	OC	The IMEI of the ME, if available.
Served MSISDN	OM	The primary MSISDN of the subscriber.
MS Network Capability	OM	The mobile station network capability.
Service Centre	OM	The address (E.164) of the SMS-service centre.
Recording Entity	OM	The E.164 number of the SGSN.
Location Area Code	OM	The Location Area Code to which the message was delivered.
Routing Area Code	OM	The Routing Area Code to which the message was delivered.
Cell Identifier	OM	The Cell Identity for GSM or Service Area Code (SAC) for UMTS to which the message was delivered.
Event Time Stamp	M	Delivery time stamp, time at which message was sent to the MS by the SGSN.
SMS Result	C	The result of the attempted delivery if unsuccessful.
Record Extensions	OC	A set of network operator/manufacturer specific extensions to the record. Conditioned upon the existence of an extension.
Node ID	OM	Name of the recording entity.
Local Record Sequence Number	OM	Consecutive record number created by this node. The number is allocated sequentially including all CDR types.
Charging Characteristics	M	The Charging Characteristics flag set used by the SGSN.
System Type	OC	Indicates the type of air interface used, e.g. UTRAN. This field is present when either the UTRAN or GERAN air-interface is used. It is omitted when the service is provided by a GSM air interface.
Charging Characteristics Selection Mode	OM	Holds information about how Charging Characteristics were selected.

Important: Based on TS 32.215 v4.5.0 (R4) / TS 32.298 v7.4.0 (R7). No change in fields from R4 to R7.

CDR Fields Supported in M-CDR

The tables in this section list the M-CDR fields present in the available GTPP dictionaries.

standard, custom1 – custom5, custom7, custom9 – 12, and custom14 – custom30 Dictionaries

For TS 32.215 v 4.5.0 (R4).

Field	Category	Description
Record Type	M	SGSN mobility management record.
Served IMSI	M	IMSI of the MS.
Served IMEI	OC	The IMEI of the ME, if available.
SGSN Address	OM	The IP address of the current SGSN.
MS Network Capability	OM	The mobile station network capability.
Routing Area Code	OM	Routing Area at the time of the Record Opening Time.
Local Area Code	OM	Location Area Code at the time of Record Opening Time.
Cell Identifier	OM	The Cell Identity for GSM or Service Area Code (SAC) for UMTS at the time of the Record Opening Time.
Change of Location	OC	A list of changes in Routing Area Code, each with a time stamp. This field is not required if partial records are generated when the location changes.
Record Opening Time	M	Timestamp when MS is attached to this SGSN or record opening time on following partial record.
Duration	OM	Duration of this record.
SGSN Change	C	Present if this is first record after SGSN change.
Cause for Record Closing	M	The reason for the closure of the record in this SGSN.
Diagnostics	OM	A more detailed reason for the release of the connection.
Record Sequence Number	C	Partial record sequence number in this SGSN; only present in case of partial records.
Node ID	OM	Name of the recording entity.
Record Extensions	OC	A set of network operator/manufacturer specific extensions to the record. Conditioned upon the existence of an extension.
Local Record Sequence Number	OM	Consecutive record number created by this node. The number is allocated sequentially including all CDR types.
Served MSISDN	OM	The primary MSISDN of the subscriber.
Charging Characteristics	M	The Charging Characteristics used by the SGSN.

Field	Category	Description
System Type	OC	Indicates the type of air interface used, e.g. UTRAN. This field is present when either the UTRAN or GERAN air-interface is used. It is omitted when the service is provided by a GSM air interface.
Charging Characteristics Selection Mode	OM	Holds information about how Charging Characteristics were selected.

custom6 and custom13 Dictionaries

For TS 32.298 v6.6.0.

Field	Category	Description
Record Type	M	SGSN mobility management record.
Served IMSI	M	IMSI of the MS.
Served IMEI	OC	The IMEI of the ME, if available.
SGSN Address	OM	The IP address of the current SGSN.
MS Network Capability	OM	The mobile station network capability.
Routing Area Code	OM	Routing Area at the time of the Record Opening Time.
Local Area Code	OM	Location Area Code at the time of Record Opening Time.
Cell Identifier	OM	The Cell Identity for GSM or Service Area Code (SAC) for UMTS at the time of the Record Opening Time.
Change of Location	OC	A list of changes in Routing Area Code, each with a time stamp. This field is not required if partial records are generated when the location changes.
Record Opening Time	M	Timestamp when MS is attached to this SGSN or record opening time on following partial record.
Duration	OM	Duration of this record.
SGSN Change	C	Present if this is first record after SGSN change.
Cause for Record Closing	M	The reason for the closure of the record in this SGSN.
Diagnostics	OM	A more detailed reason for the release of the connection.
Record Sequence Number	C	Partial record sequence number in this SGSN; only present in case of partial records.
Node ID	OM	Name of the recording entity.
Record Extensions	OC	A set of network operator/manufacturer specific extensions to the record. Conditioned upon the existence of an extension.
Local Record Sequence Number	OM	Consecutive record number created by this node. The number is allocated sequentially including all CDR types.
Served MSISDN	OM	The primary MSISDN of the subscriber.
Charging Characteristics	M	The Charging Characteristics used by the SGSN.

Field	Category	Description
RAT Type	OC	This field indicates the Radio Access Technology (RAT) type, e.g. UTRAN or GERAN, currently used by the Mobile Station as defined in TS 29.060.
Charging Characteristics Selection Mode	OM	Holds information about how Charging Characteristics were selected.

Important: The only difference between R4 and R6 is that the "System Type" field is renamed to "Rat Type".

custom8 Dictionary

For TS 32.298 v7.4.0.

Field	Category	Description
Record Type	M	SGSN mobility management record.
Served IMSI	M	IMSI of the MS.
Served IMEI	OC	The IMEI of the ME, if available.
SGSN Address	OM	The IP address of the current SGSN.
MS Network Capability	OM	The mobile station network capability.
Routing Area Code	OM	Routing Area at the time of the Record Opening Time.
Local Area Code	OM	Location Area Code at the time of Record Opening Time.
Cell Identifier	OM	The Cell Identity for GSM or Service Area Code (SAC) for UMTS at the time of the Record Opening Time.
Cell PLMN Id	OM	The MCC and MNC of the Cell at the time of Record Opening Time.
Change of Location	OC	A list of changes in Routing Area Code including MCC and MNC, each with a time stamp. This field is not required if partial records are generated when the location changes.
Record Opening Time	M	Timestamp when MS is attached to this SGSN or record opening time on following partial record.
Duration	OM	Duration of this record.
SGSN Change	C	Present if this is first record after SGSN change.
Cause for Record Closing	M	The reason for the closure of the record in this SGSN.
Diagnostics	OM	A more detailed reason for the release of the connection.
Record Sequence Number	C	Partial record sequence number in this SGSN; only present in case of partial records.
Node ID	OM	Name of the recording entity.
Record Extensions	OC	A set of network operator/manufacturer specific extensions to the record. Conditioned upon the existence of an extension.

Field	Category	Description
Local Record Sequence Number	OM	Consecutive record number created by this node. The number is allocated sequentially including all CDR types.
Served MSISDN	OM	The primary MSISDN of the subscriber.
Charging Characteristics	M	The Charging Characteristics used by the SGSN.
RAT Type	OC	This field indicates the Radio Access Technology (RAT) type, e.g. UTRAN or GERAN, currently used by the Mobile Station as defined in TS 29.060.
Charging Characteristics Selection Mode	OM	Holds information about how Charging Characteristics were selected.

Notes:

- New field “cell PLMN-ID” added.
- All IP addresses is in binary format.

Chapter 12
SGSN CDR Field Descriptions

This chapter describes the CDR fields supported by the system for use in SGSN.

Listed below are the types of CDRs supported by SGSN:

- SGSN CDRs (S-CDRs)
- Mobility CDRs (M-CDRs)
- Mobile originated SMS CDRs (S-SMO-CDRs)
- Mobile terminated SMS CDRs (S-SMT-CDRs)

The following information is provided for each field:

- **Description:** The field's description.
- **Format:** The field's data format.
- **Length:** The field's size, in bytes.

Based on the following standards:

- 3GPP TS 32.298 V6.5.0 (2006-09): 3rd Generation Partnership Project; Technical Specification Group Service and System Aspects; Telecommunication management; Charging management; Charging Data Record (CDR) parameter description (Release 6)
- 3GPP TS 32.251 V6.10.0 (2007-06): 3rd Generation Partnership Project; Group Services and System Aspects; Telecommunication management; Charging management; Packet Switched (PS) domain charging (Release 6)

Also, refer the *Field Reference for CDRs in SGSN* chapter for information on CDR fields supported in S-CDRs and M-CDRs.

CDR Fields

Access Point Name Network Identifier

The network identifier (NI) portion of the access point name (APN). The APN typically corresponds to a registered Internet domain name and represents the external packet data network (PDN). It is sent to the SGSN by the MS (or determined locally by the HLR or configuration) and is relayed to the GGSN in the Create PDP Context Request message.

The APN string may consist of 1 to 63 characters composed of alphanumerics (upper- and/or lowercase letters and digits 0-9), periods and dashes

Format
IA5 String

Length
1–65 Bytes

Access Point Name Operator Identifier

The operator identifier (OI) part of the APN. The OI is composed of three parts (<operator's MNC>.<operator's MCC>.gprs) and the first two combined uniquely identify the network operator's PLMN.

Format
IA5 String

Length
1–37 Bytes

APN Selection Mode

An index indicating how the APN was selected.

The following APN selection mode indexes are possible:

- 0: MS or network provided APN, subscribed verified
- 1: MS provided APN, subscription not verified
- 2: Network provided APN, subscription not verified

Format
Unsigned Integer

Enumerated for custom33

Enumerated integer for custom41

Length
1 Byte

CAMEL Information

Set of CAMEL information related to PDP context. This field is present if CAMEL Charging Information is received by the HLR in ISD message.

Format
Octet String

Length
N/A

Cause for Record Closing

The reason the record is closed and released from the SGSN.

Some of the possible reasons are:

- normalRelease (0): The PDP context was terminated normally through a PDP context release (end of context or SGSN change) or a GPRS detach.
- abnormalRelease (4): The PDP context was abnormally terminated.
- volumeLimit (16): The CDR is released due to exceeding volume limit.
- timeLimit (17): The CDR is released due to exceeding time limit.
- sGSNChange (18):
- maxChangeCond (19): The CDR is released due to exceeding the changed condition limit.
- managementIntervention (20): The record was closed due to an O&M request.
- intraSGSNIntersystemChange (21): The CDR is released when MS moves from 3G<->2G and vice versa within the same SGSN.
- RAT Change (22): The CDR is released when the MS moves from one radio access technology RAT) to another.
- plmn change (101): The CDR is released when the MS moves from one PLMN to another PLMN.
- Partial Record Generation: A partial CDR was generated for reasons such as the reaching of data volume or time (duration) limits, or reaching the maximum number of charging condition changes, or intraSGSNIntersystemChange change.

Format
Unsigned Integer

Length
1 Byte

Cell Identifier

For GSM, the Cell Identifier is defined as the Cell Id, reference 24.008. For UMTS, it is defined as the Service Area Code in TS 25.413. This field contains the CI (GSM) or the SAC (WCDMA) where the MS is located when the S-CDR is opened. The first partial or single S-CDR reports the value at PDP context activation. For any subsequent partial S-CDRs, the accuracy of the reported value is limited to the value at the last RA update reported by the MSCell identity for GSM or Service Area Code (SAC) for UMTS at “Record Opening Time”.

Format

Octet String

Length
2 Bytes

Change Condition

The Change Condition field is part of the ChangeOfCharCondition element in the List of Traffic Data Volumes.

Change Condition defines the reason for closing the container; supported values include:

- qoSChange
- tariffTime
- recordClosure

Format
Enumerated

Length
1 Byte

Change of Charging Characteristics

Lists the charging characteristics applied to the PDP context.

The SGSN can accept charging characteristics from the HLR or use its own. SGSN-configured charging characteristics are specified as part of the operator policy and are applied to subscriber PDP contexts through SGSN-Operator-Policy templates.

Format
Hex Value Octet String

Length
2 Bytes

Change of Charging Condition

Each traffic volume container contains details related to a charging condition as described in the following subsections. A new container is usually created for a QoS change and for tariff changes.

Format
Sequence

Length
Variable

Change Time

The Change Time field is part of the ChangeOfCharCondition element in the List of Traffic Volumes. Change Time identifies the local time when a change condition occurred and the container was closed. The contents of this field are a compact form of the UTC Time format containing local time plus an offset to universal time. Binary coded decimal

encoding is employed for the digits to reduce the storage and transmission overhead, for example: e.g. YYMMDDhhmmssShhmm.

Format
BCD encoded octet string

Length
6 Bytes

Charging Characteristics

Lists the charging characteristics (CC) applied to the PDP context by the SGSN. The SGSN can accept charging characteristics from the HLR, default values, or use its own configured values.

Format
Octet string

Length
2 Bytes

Charging Characteristics Selection Mode

The charging characteristic (CC) type that the SGSN applied to the CDR. The following values for this field are supplied:

- homeDefault: SGSN configured charging characteristics for home subscribers are used. Home subscribers are those that belong to the same PLMN as the one on which the GGSN is located.
- visitingDefault: SGSN configured charging characteristics for visiting subscribers are used. Visiting subscribers are those that belong to a different PLMN than the one on which the GGSN is located.
- roamingDefault: SGSN configured charging characteristics for roaming subscribers are used. Roaming subscribers are those that are serviced by an SGSN belonging to a different PLMN than the one on which the GGSN is located.
- subscriptionSpecific: This CC will be applied to S-CDR only if aPNSpecific CC is absent.
- aPNSpecific: For S-CDR priority will be given to aPNSpecific Charging Characteristics Selection mode. The aPNSpecific mode is from HLR (ISD Message).

Format
Enumerated Integer

Length
1 Byte

Charging ID

Field specifies the charging identifier, which can be used together with the GGSN address to identify all records involved in a single PDP context. The charging ID is generated by the GGSN at PDP context activation and is transferred to the SGSN requesting the context. At an inter-SGSN routing area update (ISRAU) the charging ID is transferred to the new SGSN as part of each active PDP context. Each GGSN allocates the charging ID independently and may allocate the same number prefix, so the charging ID must always be combined with the GGSN address to form a unique identifier for the PDP context.

Format

Integer (0..4294967295)

Length
1–4 Bytes / 1-5 Bytes (custom33 only)

Data Volume GPRS Downlink

The Data Volume GPRS Downlink field is a part of the ChangeOfCharCondition element in the List of Traffic Volumes. It includes the number of octets transmitted in the downlink direction during the timeframe specified by the container. For each new container, the counter is reset and does not accumulate. The data volume tabulated by the SGSN covers the amount of user data transferred in the SNDCP PDUs (GSM) and GTP-U T-PDUs (WCDMA). Data volumes retransmitted by RLC or LLC, due to poor radio link conditions, are not tabulated. The data counted includes the IP PDP bearer protocols, i.e. IP or PPP.

Format
Integer

Length
1–5 Bytes

Data Volume GPRS Uplink

The Data Volume GPRS Uplink field is a part of the ChangeOfCharCondition element in the List of Traffic Volumes. It includes the number of octets received in the uplink direction during the timeframe specified by the container. For each new container, the counter is reset and does not accumulate. The data volume tabulated by the SGSN covers the amount of user data transferred in the SNDCP PDUs (GSM) and GTP-U T-PDUs (WCDMA). Data volumes retransmitted by RLC or LLC, due to poor radio link conditions, are not tabulated. The data counted includes the IP PDP bearer protocols, i.e. IP or PPP.

Format
Integer

Length
1–5 Bytes

Default Transaction/SMS Handling

This field indicates whether or not a CAMEL encountered default GPRS- or SMS-handling. This field is present only if default call handling has been applied. Parameter is defined in HLR as part of CAMEL subscription information.

Format
Enumeration (Integer)

Diagnostics

This field is included in the CDR when the PDP context is released. This field is supported in G-CDRs but not for eG-CDRs.

It will contain one of the following values:

- 36: If the SGSN sends Delete PDP Context request

- 38: If the SGSN sends Delete PDP Context request due to GTP-C/U echo timeout with SGSN
- 26: If the SGSN sends Delete PDP Context request for any other reason

Format
Unsigned Integer

Length
1 Byte

Duration

This field contains the duration for the record in seconds. For partial records, only the interval described by the recordOpeningTime and the last ChangeTime in the ListOfTrafficVolumes is counted. The Duration value is reset for each new partial CDR. This value is converted from the internal representation in milliseconds to an integer value representing only seconds. The mechanism for this conversion (ceiling, floor, round-off) can be configured.

Format
Unsigned Integer

Length
1–5 Bytes

Dynamic Address Flag

The presence of this field indicates that the PDP Address was dynamically allocated for that particular PDP context during context activation. This field is missing if the address is static (part of the PDP context subscription).

Format
Boolean

Length
1 Byte

GGSN Address

This field provides the IP address for the control plane of the current serving GGSN, which is equivalent to the configured ggsn-service address on the GGSN. The standard 3GPP 32.298 offers a choice for the encoding of the address to be either in binary or text format. The SGSN encodes the address in binary format and includes the Octet String.

Format
Hex Value Octet String

Length
4-6 Bytes

IP Address

The IP address format is used by multiple fields in the CDR, such as the GGSN address or the Served PDP address. This entry is included here to avoid duplication. For the IP address, both the binary and text format and both IPv4 and IPv6 are specified in 3GPP 32.298.

For custom33 only, served PDP IP address will be in IPV4 or IPV6. The SGSN and GGSN transport interfaces should be IPV4 encoded.

- iPBinV4Address -- [0] -- OCTET STRING -- (SIZE(4))
- iPBinV6Address -- [1] -- OCTET STRING -- (SIZE(16))
- iPTextV4Address -- [2] -- IA5String -- (SIZE(7..15))
- iPTextV6Address -- [3] -- IA5String -- (SIZE(15..45))

Format
Hex Value Octet String

Length
4-6 Bytes

IPv4 Binary Address

This field contains an IPv4 address in hexadecimal format. Depending on where the field is used in the sequence of the CDR, it may contain either an SGSN or GGSN address or the PDP IP address of the mobile subscriber. Note: Note the difference between how the GSN address and the PDP address are encoded. Currently, only IPV4 support is provided.

Format
Hex Value Octet String

Length
Varies for GSN address or PDP address

IPv6 Binary Address

This field contains an IPv6 address in hexadecimal format. Depending on where the field is used in the sequence of the CDR, it may contain either an SGSN or GGSN address or the PDP IP address of the mobile subscriber. Note: Note the difference between how the GSN address and the PDP address are encoded. Currently, only IPV4 support is provided.

Format
Hex Value Octet String

Length
Varies for GSN address or PDP address

Level of CAMEL services

This field describes the complexity of CAMEL invocation. Categories are the same as in circuit switched services and measure of resource usage in VPLMN requested by HPLMN.

- Basic: The CAMEL feature is invoked only during the PDP context activation phase. (For example, to modify APN_NI/APN_OI).
- Call duration supervision: The PDP context duration or volume supervision is applied in the gprsSSF of the VPLMN (Apply Charging message is received from the gsmSCF).

Format
Octet String

List of Traffic Data Volumes

A list of the changes that occurred in the charging conditions for this PDP context.

The list will include one or more containers each including the following fields:

- QoS negotiated: Quality of service (QoS) has been negotiated. The initial and final corresponding data values are listed. This is only added for the first container and the container after a QoS change.
- Uplink volume: The number of octets (uncompressed) received from the MS. The initial and final corresponding data values are listed.
- Downlink volume: The number of octets (uncompressed) transmitted to the MS.The initial and final corresponding data values are listed.
- Change Condition: Identifies the reason that the container was closed such as tariff time change, QoS change, or closing of the CDR.
- Change Time: A timestamp identifying the time at which the volume container or the CDR closed.

For GPRS, data volumes are in octets above the GTP layer and are separated for uplink and downlink traffic. In UMTS, data volumes are in octets above the GTP-U layer and are separated for uplink and downlink traffic.

Format

- QoS negotiated: Octet String
- Uplink volume: Integer
- Downlink volume: Integer
- Change Condition: Integer
- Change Time: BCD Encoded Octet String

Length

- QoS negotiated: 12 Bytes
- Uplink volume: 4 Bytes
- Downlink volume: 4 Bytes
- Change Condition: 1 Byte
- Change Time: 9 Bytes

List of Traffic Volumes

This list includes one or more Traffic Volume containers related to a “Change of Charging Condition” as described in 6.7. The maximum number of containers is configurable, see chapter 2.

This list includes containers that include the following fields:

- QoS requested (optional)
- QoS negotiated (optional)
- data volume uplink
- data volume downlink
- change condition
- change time

Format

Sequence

Length
Variable

Local Record Sequence Number

This field contains a unique sequence number associated with the NodeId field and independent of the PDP context. Unless the LRSN rewrite feature is used on the HDD, the Cisco SGSN will generate multiple NodeIds (one for each internal process generating CDRs), each with its own sequence number. The number, allocated sequentially and including all CDR types, is unique within one physical node, which is identified either by field Node ID or by record-dependent node address (SGSN address, GGSN address, Record Entity). The local sequence number will be restarted at 0 when, for example, the node is reloaded.

Note: Since node-id is unique centralized LRSN feature must be enabled.

Format
Unsigned Integer (0..4294967295)

Length
1–4 Bytes / 1-5 Bytes (custom33)

Location Area Code (LAC)

This field contains the location area code (LAC) identifying the location area in which the served party is currently located. When the (partial) record is opened. The LAC is coded according to 3GPP TS 24.008.

Format
Octet String

Length
2 Bytes

MS Network Capability

This field identifies the mobile station network capability value or information element for the served MS at PDP Context Activation or at GPRS Attach as defined in 3GPP TS 24.008

Format
Octet String

Length
1–8 Bytes

Network Initiated PDP Context

The presence of this field indicates that the PDP context was initiated by the network.

Format
Boolean

Length
1 Byte

Node ID

The identifier string for the SGSN that had generated the CDR. Node ID, along with local record sequence number, uniquely identifies a CDR.

On the ASR5K SGSN, this NodeID field is a printable string of the ndddSTRING format:

- n: The first digit is the Sessmgr restart counter having a value between 0 and 7.
- ddd: The number of the sessmgr instance generating the CDR
- STRING: This is a configured Node-ID-Suffix having any string between 1 to16 characters, defined using the gtpp attribute node-id command.

If this node-id-suffix is not configured, the SGSN uses the GTPP context name as the Node-id-suffix (truncated to 16 characters).

This field is only included when the option "**`gtpp attribute local-record-sequence-number`**" is configured.

Format
Octet String

Length
1–20 Bytes / 5-20 Bytes for custom33

PDP Type

The PDP context type. The PDP types supported by the SGSN are IP or PPP (including IHOSS:OSP).

Format
Hex Value Octet String

Length
2 Bytes

- Value “0” : PDP type IPv4
- Value “1”: PDP type IPv6
- Value “2”: PDP type IPv4v6

pLMNIdentifier

This field defines the PLMN identity (MCC and MNC) as part of the location information. It is present only if the option to include PLMN identity has been set by the operator.

Note: Bits 5-8 of octet 2 contain third MNC digit, or 1111 used as filler when MNC has only two digits.

Format
Octet String

Length
3 Bytes

QoS Negotiated

QoS Negotiated indicates the applied QoS accepted by the network.

Note:

- If a pre-release '99-capable terminal is served, only octets 1 to4 are included.
- The field is defined with a maximum size of 12 bytes.
- This field is present in first container of all CDRs.
- In next container this field is present if there is QOS change.

Format
Octet String

Length
4-12 Bytes

QoS Requested

The Quality of Service Requested field contains the QoS desired by the MS at PDP context activation.

Note:

- If a pre-release '99-capable terminal is served, only octets 1 to4 are included.
- The field is defined with a maximum size of 12 bytes.
- This field is present in first container of all CDRs.
- In next container this field is present if there is QoS change. Qos Requested field may be absent if QoS change is initiated by network (GGSN/HLR).

Format
Octet String

Length
4-12 Bytes

Radio Access Technology (RAT) Type

The SGSN may include the RAT Type IE along with User Location Information IE, and MS Time Zone IE if they are available. The RAT Type IE is not included for the MS-initiated PDP Context Modification procedure.

Format
Integer (1-255).

Length
1 Byte

Record Extensions

A set of network operator or manufacturer specific extensions that may be added to the record if provided. It is used for reporting flows and volumes consumed, and also for passing key information about the session into the downstream charging systems.

Important: This field is customer specific.

Record Opening Time

The timestamp at which the PDP context was activated on the SGSN or when a subsequent record is opened after a partial record. The timestamp is determined based on the internal timer which has an accuracy of 10ms. Depending on the configured mechanism (ceiling, floor, round-off) this is translated into the timestamp which only shows the full seconds.

Format
BCD Encoded Octet String

Length
9 Bytes

Record Sequence Number

A running sequence number used to link partial records generated by the SGSN for a specific PDP context (characterized with the same Charging ID and SGSN address pair). This field is only present in case of partial records or if the first record is also the final record.

Format
Unsigned Integer

Length
1–5 Bytes

Record Type

Indicates type of the record: S-CDR(sgsnPDPRecord) >>> 18 (0x12).

Format
Integer

Length
1–4 Bytes

RNC Unsent Downlink Volume

The downlink data volume that the RNC has not sent to MS. This field is present when the RNC has provided unsent downlink volume count at RAB release.

Format
Unsigned Integer

Length
1–5 Bytes

Routing Area Code (RAC)

This field contains the Routing Area Code (RAC) of the routing area in which the served party is currently located when the (partial) record is opened. The RAC is coded according to 3GPP TS 24.008.

Format
Octet String

Length
1 Byte

Served IMEI

This field contains the international mobile equipment identity (IMEI) of the equipment served. If IMEISV (IMEI softare version) is available, then IMEISV shall be sent in the CDR. The structure of the IMEI is defined in TS 23.003.

The IMEI is composed of the following elements:

- Type Allocation Code (TAC) with a length of 8 digits
- Serial Number (SNR) is an individual serial number uniquely identifying each equipment within each TAC. Its length is 6 digits
- Spare digit: this digit shall be zero, when transmitted by the MS

  A filler digit "f" is added after the spare digit to fill up the last byte.

Format
BCD Encoded Octet String

Length
8 Bytes

Served IMSI

The International Mobile Subscriber Identity (IMS) of the MS. The IMSI is formatted in accordance with 3GPP TS 23.003. This will be present if the Anonymous Access Indicator is FALSE or not supplied.

Format
BCD Encoded Octet String

Length
3–8 Bytes

Served PDP Address

The binary-represented IP address associated with the PDP context of the served IMSI for the CDR. This address could be either static or dynamically assigned. The standard 3GPP TS32.298 allows a choice of either IPAddress or ETSIAddress - a binary IPv4 address (iPBINV4Address) or IPv6 address (iPBinV6Address).

Format
Choice

Length
4 bytes for IPv4 address

16 bytes for IPv6 address

Served MSISDN

The primary Mobile Station (MS) ISDN number (MSISDN) of the subscriber.

Format
BCD Encoded Octet String

Length
1–9 Bytes

SGSN Address

The SGSN IPv4 addresses (binary-represented) used over the duration of the CDR. The address(es) can be either user or control-plane addresses.

Format
Hex Value Octet String

Length
4 Bytes per address, field max is 30 Bytes

SGSN Change

Present if this is first record after SGSN change.

Format
Boolean

Length
1 Byte

Chapter 13
S-GW CDR Field Reference

This chapter provides a reference for CDR fields supported by the system for use in SGW-CDRs.

A complete list and descriptions of supported CDR fields is provided in the *S-GW CDR Field Descriptions* chapter of this reference.

Important: For more information on custom dictionaries, contact your Cisco account representative.

The category column in all tables use keys described in the following table.

Table 24. Dictionary Table Key

Abbreviation	Meaning	Description
M	Mandatory	A field that must be present in the CDR.
C	Conditional	A field that must be present in a CDR if certain conditions are met.
OM	Operator Provisionable: Mandatory	A field that an operator has provisioned and must be included in the CDR for all conditions.
OC	Operator Provisionable: Conditional	A field that an operator has provisioned that must included in the CDR if certain conditions are met.

CDR Fields Supported in SGW-CDRs

The tables in this section list the SGW-CDR fields present in the available GTPP dictionaries.

custom6, and custom11 Dictionaries

For custom6 and custom24 dictionaries, CDR fields are based on 3GPP TS 32.298 v8.7.0, 3GPP TS 32.251 v8.8.0, and 3GPP TS 32.298 V9.6.0 .

For the custom11 dictionary, CDR fields are based on 3GPP TS 32.298 v8.5.0 and 3GPP TS 32.251 v8.6.0.

Field	Category	Description
Record Type	M	S-GW IP CAN bearer record
Served IMSI	M	IMSI of the served party (if Anonymous Access Indicator is FALSE or not supplied)
Served IMEISV	OC	IMEISV of the ME, if available
S-GW Address used	M	The control plane IP address of the S-GW used.
Charging ID	M	IP CAN bearer identifier used to identify this IP CAN bearer in different records created by PCNs
PDN Connection Id	OM	The PDN connection (IP-CAN session) identifier to identify different records belonging to same PDN connection.
Serving Node Address	M	List of serving node control plane IP addresses (e.g. SGSN, MME, etc.) used during this record.
Serving Node Type	M	List of serving node types in control plane. The serving node types listed here map to the serving node addresses listed in the field “Serving node Address” in sequence.
S-GW Change	OC	Present if this is the first record after S-GW change.
PGW PLMN Identifier	OM	PLMN identifier (MCC MNC) of the P-GW used.
Access Point Name Network Identifier	OM	The logical name of the connected access point to the external packet data network (network identifier part of APN).
PDP/PDN Type	OM	Indicates PDN type (i.e IPv4, IPv6 or IPv4v6).
Served PDP/PDN Address	OC	IP address allocated for the PDP context / PDN connection, i.e. IPv4 or IPv6, if available.
Dynamic Address Flag	OC	Indicates whether served PDP/PDN address is dynamic, which is allocated during IP CAN bearer activation, initial attach (E-UTRAN or over S2x) and UE requested PDN connectivity. This field is missing if address is static.
List of Traffic Data Volumes	OM	A list of changes in charging conditions for this QCI/ARP pair, each change is time stamped. Charging conditions are used to categorize traffic volumes, such as per tariff period. Initial and subsequently changed QoS and corresponding data values are also listed. Refer to the List of Data Traffic Volumes table in this chapter.

Field	Category	Description
Record Opening Time	M	Time stamp when IP CAN bearer is activated in this S-GW or record opening time on subsequent partial records.
MS Time Zone	OC	Contains the MS Time Zone the MS is currently located as defined in TS 29.060 [203], if available.
Duration	M	Duration of this record in the S-GW.
Cause for Record Closing	M	The reason for the release of record from this S-GW.
Diagnostics	OM	A more detailed reason for the release of the connection.
Record Sequence Number	C	Partial record sequence number, only present in case of partial records.
Node ID	OM	Name of the recording entity.
Record Extensions	OC	A set of network operator/manufacturer specific extensions to the record. Conditioned upon the existence of an extension.
Local Record Sequence Number	OM	Consecutive record number created by this node. The number is allocated sequentially including all CDR types.
APN Selection Mode	OM	An index indicating how the APN was selected.
Served MSISDN	OM	The primary MSISDN of the subscriber.
User Location Information	OC	Contains the User Location Information of the MS as defined in TS 29.060 [203] for GPRS case, and in TS 29.274 [210] for EPC case, if available.
Charging Characteristics	M	The Charging Characteristics applied to the IP CAN bearer.
Charging Characteristics Selection Mode	OM	Information about how Charging Characteristics were selected.
IMS Signalling Context	OC	Included if the IM-CN Subsystem Signalling Flag is set. IP CAN bearer is used for IMS signalling.
P-GW Address used	OC	The P-GW IP Address for the Control Plane.
Serving Node PLMN Identifier	OC	Serving node PLMN Identifier (MCC and MNC) used during this record, if available.
RAT Type	OC	Indicates the Radio Access Technology (RAT) type currently used by the Mobile Station, when available. This RAT type is defined in TS 29.060 [204] for GTP case, in TS 29.274 [210] for eGTP case and in TS 29.275 [211] for PMIP case.
Start Time	OC	The time when User IP-CAN session starts, available in the CDR for the first bearer in an IP-CAN session.
Stop Time	OC	The time when User IP-CAN session is terminated, available in the CDR for the last bearer in an IP-CAN session.

Notes:

- custom11 and custom24 dictionaries: All IP addresses are encoded in binary format.

- custom6 dictionary: All IP addresses are in ASCII format.
- custom11 dictionary: User CSG Information is not encoded.

List of Traffic Data Volumes

Traffic Data Volume	Category	Description
Change Of Charging Condition	M	Each traffic volume container contains details related to a charging condition as described in the following subsections. A new container is usually created for a QoS change and for tariff changes.
Data Volume GPRS Uplink	M	The Data Volume GPRS Uplink field is a part of the ChangeOfCharCondition element in the List of Traffic Volumes. It includes the number of octets received in the uplink direction during the timeframe specified by the container. For each new container, the counter is reset and does not accumulate. The data counted already includes the IP PDP bearer protocols i.e. IP or PPP.
Data volume GPRS Downlink	M	The Data Volume GPRS Downlink field is a part of the ChangeOfCharCondition element in the List of Traffic Volumes. It includes the number of octets transmitted in the downlink direction during the timeframe specified by the container. For each new container, the counter is reset and does not accumulate. The data counted already includes the IP PDP bearer protocols i.e. IP or PPP.
Change Condition	M	The Change Condition field is part of the ChangeOfCharCondition element in the List of Traffic Volumes. It defines the reason for closing the container.
Change time	M	The Change Time field is part of the ChangeOfCharCondition element in the List of Traffic Volumes. It provides the local time when a change condition (e.g. record closure) occurred and the container was closed.
User Location Information	OC	This field contains the User Location Information as described in TS 29.274 for eGTP case (e.g. CGI, SAI, RAI TAI and ECGI). The field is provided by the SGSN/MME and transferred to the S-GW/P-GW during the IP-CAN bearer activation/modification. User Location Information contains the location (e.g. CGI/SAI, ECGI/TAI or RAI) where the UE is located and used during the transfer of the data volume captured by the container (applicable only to the SGW-CDR). This is included in the Traffic data container only if previous container's change condition is “user location change”. Note the user location information in SGW-CDR main level contains the location where the UE was when CDR was opened.
EPC Qos Requested	OC	In case of IP-CAN bearer specific container this contains authorized QoS for the IP-CAN bearer. First container for each QCI/ARP pair includes this field. In following containers this field is present if previous change condition is “QoS change”. This field is applicable only in SGW-CDR.

custom24 Dictionary

CDR fields are based on 3GPP TS 32.298 v8.7.0, 3GPP TS 32.251 v8.8.0, and 3GPP TS 32.298 V9.6.0 .

Field	Category	Description
Record Type	M	The field identifies the type of the record.

Field	Category	Description
Served IMSI	M	This field contains the International Mobile Subscriber Identity (IMSI) of the served party. The IMSI is formatted in accordance with 3GPP TS 23.003.
s-GW Address	M	The control plane IP address of the S-GW used.
SGW BINARY IPV4 ADDRESS	M	This field is the serving control plane S-GW IPv4 address on the S5 interface.
SGW BINARY IPV6 ADDRESS	M	This field is the serving control plane S-GW IPv6 address on the S5 interface.
Charging ID	M	IP CAN bearer identifier used to identify this IP CAN bearer in different records created by PCNs
List of Serving Node Address	M	This field contains 1-16 Serving Node control plane IP used during this record (max of 15 Serving Node Changes). This is a list of IP addresses.
Serving Node BINARY IPV4 ADDRESS	M	The octet string included in the field described above includes the IPV4 address of the MME.
Serving Node BINARY IPV6 ADDRESS	M	The octet string included in the field described above includes the IPV6 address of the MME.
Access Point Name Network Identifier	M	The logical name of the connected access point to the external packet data network (network identifier part of APN).
PDP/PDN Type	M	Indicates PDP type (IP, PPP, or IHOSS:OSP) or PDN type (IPv4, IPv6, or IPv4v6).
Served PDP/PDN Address	O	IP address allocated for the PDP context / PDN connection (IPv4 or IPv6), if available.
PDP IP Address	M	This field contains the IP address for the PDP context.
PDP IPV4 Address	M	The octet string included in the field described above includes the IPV4 address assigned to the subscriber by of the PGW in binary coding.
PDP IPV6 Address	M	The octet string included in the field described above includes the IPV6 address assigned to the subscriber by of the PGW in binary coding.
Dynamic Address Flag	OC	Indicates whether served PDP/PDN address is dynamic, which is allocated during IP CAN bearer activation, initial attach (E-UTRAN or over S2x) and UE requested PDN connectivity. This field is missing if address is static.
List of Traffic Data Volumes	M	A list of changes in charging conditions for this QCI/ARP pair, each change is time stamped. Charging conditions are used to categorize traffic volumes, such as per tariff period. Initial and subsequently changed QoS and corresponding data values are also listed.
Change of charging condition	M	Each traffic volume container contains details related to a charging condition as described in the following subsections. A new container is usually created for a QoS change and for tariff changes.
dataVolumeGPRSUplink	M	The Data Volume GPRS Uplink field is a part of the ChangeOfCharCondition element in the List of Traffic Volumes. It includes the number of octets received in the uplink direction during the timeframe specified by the container. For each new container, the counter is reset and does not accumulate.

Field	Category	Description
dataVolumeGPRSDownlink	M	The Data Volume GPRS Downlink field is a part of the ChangeOfCharCondition element in the List of Traffic Volumes. It includes the number of octets transmitted in the downlink direction during the timeframe specified by the container. For each new container, the counter is reset and does not accumulate.
changeCondition	M	The Change Condition field is part of the ChangeOfCharCondition element in the List of Traffic Volumes. It defines the reason for closing the container.
changeTime	M	The Change Time field is part of the ChangeOfCharCondition element in the List of Traffic Volumes. It provides the local time when a change condition (e.g. record closure) occurred and the container was closed.
userLocationInformation	O	This field contains the User Location Information as described in TS 29.274 for eGTP cases (e.g. CGI, SAI, RAI TAI and ECGI). The field is provided by the SGSN/MME and transferred to the S-GW/P-GW during the IP-CAN bearer activation/modification.
ePCQoSInformation	O	In case of IP-CAN bearer specific container, this contains authorized QoS for the IPCAN bearer. First container for each QCI/ARP pair includes this field. In following containers, this field is present if previous change condition is “QoS change”. This field is applicable only in SGW-CDR.
qci	M	A QCI is a scalar that is used as a reference to access node-specific parameters that control bearer level packet forwarding treatment (for example, scheduling weights, admission thresholds, queue management thresholds, link layer protocol configuration, etc.), and that have been pre-configured by the operator owning the access node (for example, eNodeB).
Uplnk MBR	O	The MBR limits the uplink bit rate that can be expected to be provided by a GBR bearer.
Dnlnk MBR	O	The MBR limits the downlink bit rate that can be expected to be provided by a GBR bearer (for example, excess traffic may get discarded by a rate shaping function).
Uplnk GBR	O	The GBR denotes the uplink bit rate that can be expected to be provided by a GBR bearer
Dnlnk GBR	O	The GBR denotes the downlink bit rate that can be expected to be provided by a GBR bearer.
arp	O	The ARP contains information about the priority level (scalar), the pre-emption capability (flag) and the pre-emption vulnerability (flag). The primary purpose of ARP is to decide whether a bearer establishment or modification request can be accepted, or needs to be rejected due to resource limitations (typically available radio capacity for GBR bearers).
Record Opening Time	M	Timestamp when IP CAN bearer is activated in this S-GW or record opening time on subsequent partial records.
Duration	M	Duration of this record in the S-GW.
Cause for Record Closing	M	The reason for the release of a record from this S-GW.
Diagnostics	OC	Includes a more detailed technical reason (as defined in TS 32.250) for the release of the connection.
gsm408cause	M	Refer to TS 24.008 for more information.

Field	Category	Description
Record Sequence Number	O	Partial record sequence number, only present in case of partial records.
Node ID	O	Name of the recording entity.
recordExtensions	O	A set of network operator/manufacturer specific extensions to the record. Conditioned upon the existence of an extension.
Local Sequence Number	O	Consecutive record number created by this node. The number is allocated sequentially including all CDR types.
APN Selection Mode	M	An index indicating how the APN was selected.
Served MSISDN	M	The primary MSISDN of the subscriber.
Charging Characteristics	M	The Charging Characteristics applied to the IP CAN bearer.
Charging Characteristics Selection Mode	O	Holds information about how Charging Characteristics were selected.
IMSsignalingContext	O	Included if the IM-CN Subsystem Signalling Flag is set, see [201] IP CAN bearer is used for IMS signalling.
Serving Node PLMN Identifier	O	Serving node PLMN Identifier (MCC and MNC) used during this record, if available.
Served IMEISV	O	IMEISV of the ME, if available.
RAT Type	OC	Indicates the Radio Access Technology (RAT) type currently used by the Mobile Station, when available.
mSTimeZone	O	This field contains the MS Time Zone the MS is currently located as defined in TS 29.060 [203], if available.
userLocationInformation	O	Contains the User Location Information of the MS as defined in TS 29.060 for GPRS case, and in TS 29.274 for EPC case, if available.
sGWChange	O	Present if this is first record after S-GW change.
servingNodeType	M	List of serving node types in control plane. The serving node types listed here map to the serving node addresses listed in the field "Serving node Address" in sequence.
ServingNodeTypeenum	M	These fields contain one or several serving node types in the control plane of an S-GW or P-GW, which have been connected during the record. The serving node types listed here are sequentially mapped to the serving node addresses listed in the field “Serving node Address”.
p-GWAddressUsed	M	This field is the P-GW IP Address for the Control Plane.
PGW BINARY IPV4 ADDRESS	M	The octet string included in the field described above includes the IPV4 address assigned to the subscriber by of the P-GW in binary coding.
PGW BINARY IPV6 ADDRESS	M	The octet string included in the field described above includes the IPV6 address assigned to the subscriber by of the P-GW in binary coding.
PGW PLMNIdentifier	O	PLMN identifier (MCC MNC) of the P-GW used. This field is present in CDR if P-GW PLMN-ID is available in the CSR message from Serving Node (For e,g. MME).
startTime	O	This field holds the time when User IP-CAN session starts, available in the CDR for the first bearer in an IP-CAN session.

Field	Category	Description
stopTime	O	This field holds the time when User IP-CAN session is terminated, available in the CDR for the last bearer in an IP-CAN session.
pDNConnectionID	O	This field defines the PDN connection (IP-CAN session) identifier to identify different records belonging to same PDN connection. This field includes Charging ID of first IP-CAN bearer activated within the PDN connection. Together with P-GW address this uniquely identifies the PDN connection.
servedPDPPDNAddressExt	O	This field contains the IPv4 address for the PDN connection (PDP context, IP-CAN bearer) when dual-stack IPv4 IPv6 is used, and the IPv6 adress is included in Served PDP Address or Served PDP/PDN Address. This field is missing if the PDP/PDN address is IPV4 or IPV6. By default this field is not sent even if the PDP Type is IPV46 (This field should be enabled using the CLI).
PDP IP Address	M	This field contains the IP address for the PDP context.
PDP IPV4 Address	M	The octet string included in the field described above includes the IPv4 address assigned to the subscriber by of the P-GW in binary coding.

Notes:

- All IP addresses are encoded in binary format.

custom34 Dictionary

For the custom34 dictionary, CDR fields are based on 3GPP TS 32.298 v8.4.0 and 3GPP TS 32.251 v8.5.0.

Field	Category	Description
Record Type	M	S-GW IP CAN bearer record
Served IMSI	M	IMSI of the served party (if Anonymous Access Indicator is FALSE or not supplied)
S-GW Address used	M	The control plane IP address of the S-GW used.
Charging ID	M	IP CAN bearer identifier used to identify this IP CAN bearer in different records created by PCNs
Serving Node Address	M	List of serving node control plane IP addresses (e.g. SGSN, MME, etc.) used during this record.
Access Point Name Network Identifier	OM	The logical name of the connected access point to the external packet data network (network identifier part of APN).
PDP/PDN Type	OM	Indicates PDN type (i.e IPv4, IPv6 or IPv4v6).
Served PDP/PDN Address	OM	IP address allocated for the PDP context / PDN connection, i.e. IPv4 or IPv6, if available.
Dynamic Address Flag	OC	Indicates whether served PDP/PDN address is dynamic, which is allocated during IP CAN bearer activation, initial attach (E-UTRAN or over S2x) and UE requested PDN connectivity. This field is missing if address is static.

Field	Category	Description
List of Traffic Data Volumes	OM	A list of changes in charging conditions for this QCI/ARP pair, each change is time stamped. Charging conditions are used to categorize traffic volumes, such as per tariff period. Initial and subsequently changed QoS and corresponding data values are also listed. Refer to the List of Data Traffic Volumes table in this chapter.
Record Opening Time	M	Time stamp when IP CAN bearer is activated in this S-GW or record opening time on subsequent partial records.
Duration	M	Duration of this record in the S-GW.
Cause for Record Closing	M	The reason for the release of record from this S-GW.
Diagnostics	OC	A more detailed reason for the release of the connection.
Record Sequence Number	C	Partial record sequence number, only present in case of partial records.
Node ID	OC	Name of the recording entity.
Record Extensions	OC	A set of network operator/manufacturer specific extensions to the record. Conditioned upon the existence of an extension.
Local Record Sequence Number	OC	Consecutive record number created by this node. The number is allocated sequentially including all CDR types.
APN Selection Mode	OM	An index indicating how the APN was selected.
Served MSISDN	OM	The primary MSISDN of the subscriber.
Charging Characteristics	M	The Charging Characteristics applied to the IP CAN bearer.
Charging Characteristics Selection Mode	OC	Information about how Charging Characteristics were selected.
Serving Node PLMN Identifier	OC	Serving node PLMN Identifier (MCC and MNC) used during this record, if available.
Served IMEISV	OC	IMEISV of the ME, if available
RAT Type	OC	Indicates the Radio Access Technology (RAT) type currently used by the Mobile Station, when available. This RAT type is defined in TS 29.060 [204] for GTP case, in TS 29.274 [210] for eGTP case and in TS 29.275 [211] for PMIP case.
MS Time Zone	OC	Contains the MS Time Zone the MS is currently located as defined in TS 29.060 [203], if available.
User Location Information	OC	Contains the User Location Information of the MS as defined in TS 29.060 [203] for GPRS case, and in TS 29.274 [210] for EPC case, if available.
S-GW Change	OC	Present if this is the first record after S-GW change.
Serving Node Type	M	List of serving node types in control plane. The serving node types listed here map to the serving node addresses listed in the field “Serving node Address” in sequence.
P-GW Address used.	OM	The P-GW IP Address for the Control Plane.

Notes:

- Proprietary “recordExtensions” field supported.
- Spare filler bytes (high order) in PDP Type are reported as zeros (0) rather than ones (1).
- The ASN encoding length for servingNodeAddress and servingNodeType are reported with the 0x82 tag, which has a 2-byte length.
- QoS negotiated information is reported in string format (v8.4) rather than EPC Qos format (v8.7).

List of Traffic Data Volumes

Traffic Data Volume	Category	Description
Change Of Charging Condition	M	Each traffic volume container contains details related to a charging condition as described in the following subsections. A new container is usually created for a QoS change and for tariff changes.
Data Volume GPRS Uplink	M	The Data Volume GPRS Uplink field is a part of the ChangeOfCharCondition element in the List of Traffic Volumes. It includes the number of octets received in the uplink direction during the timeframe specified by the container. For each new container, the counter is reset and does not accumulate. The data counted already includes the IP PDP bearer protocols i.e. IP or PPP.
Data volume GPRS Downlink	M	The Data Volume GPRS Downlink field is a part of the ChangeOfCharCondition element in the List of Traffic Volumes. It includes the number of octets transmitted in the downlink direction during the timeframe specified by the container. For each new container, the counter is reset and does not accumulate. The data counted already includes the IP PDP bearer protocols i.e. IP or PPP.
Change Condition	M	The Change Condition field is part of the ChangeOfCharCondition element in the List of Traffic Volumes. It defines the reason for closing the container.
Change time	M	The Change Time field is part of the ChangeOfCharCondition element in the List of Traffic Volumes. It provides the local time when a change condition (e.g. record closure) occurred and the container was closed.
User Location Information	O	This field contains the User Location Information as described in TS 29.274 for eGTP case (e.g. CGI, SAI, RAI TAI and ECGI). The field is provided by the SGSN/MME and transferred to the S-GW/P-GW during the IP-CAN bearer activation/modification. User Location Information contains the location (e.g. CGI/SAI, ECGI/TAI or RAI) where the UE is located and used during the transfer of the data volume captured by the container (applicable only to the SGW-CDR). This is included in the Traffic data container only if previous container's change condition is “user location change”. Note the user location information in SGW-CDR main level contains the location where the UE was when CDR was opened.
QoS Negotiated	O	Authorized QoS for the IP-CAN bearer.

Chapter 14
S-GW CDR Field Descriptions

This chapter describes the CDR fields supported by the system for use in SGW-CDRs.

The following information is provided for each field:

- **Description:** The field's description.
- **Format:** The field's data format.
- **Length:** The field's size, in bytes.

All SGW-CDRs are encoded using the ASN.1 format and are sent to the charging gateway function (CGF) using the GPRS Tunneling Protocol Prime (GTPP) as defined in the following standards:

- 3GPP TS 29.060
- 3GPP TS 32.015
- 3GPP TS 32.215
- 3GPP TS 32.251 (v 8.6.0, v 8.8.0)
- 3GPP TS 32.298 (v 8.5.0, v 8.7.0) (SGW-CDRs)

Also see the *Field Reference for CDRs in S-GW* chapter for information on CDR fields supported in SGW-CDRs.

Important: The behavior for several of the fields supported in CDRs can be modified. For more information, refer to the **`gtpp attributes`** command in the *Command Line Interface Reference*.

CDR Fields

Access Point Name Network Identifier

This field contain the Network Identifier part of the Access Point Name (APN). This APN is sent to the S-GW by the MME and is relayed to the P-GW in the Create PDP Context Request message.

Format

IA5string

Length

1-63 bytes

APN Selection Mode

An index indicating how the APN was selected.

The following APN selection mode indexes are possible:

0: MS or network provided APN, subscribed verified

1: MS provided APN, subscription not verified

2: Network provided APN, subscription not verified.

Format

Enumerated

Length

1 byte

Cause for Record Closing

This field contains a reason for the closure of the CDR.

Supported values:

- normalRelease (0)
- abnormalRelease (4)
- cAMELInitCallRelease (5)
- volumeLimit (16)
- timeLimit (17)
- servingNodeChange (18)
- maxChangeCond (19)
- managementIntervention (20)
- intraSGSNIntersystemChange (21)

- rATChange (22)
- mSTimeZoneChange (23)
- sGSNPLMNIDChange (24)
- unauthorizedRequestingNetwork (52)
- unauthorizedLCSClient (53)
- positionMethodFailure (54)
- unknownOrUnreachableLCSClient (58)
- listofDownstreamNodeChange (59)

Format

Integer

Length

1 byte

Charging Characteristics

Lists the charging characteristics applied to the PDP context by the S-GW. The S-GW shall accept the charging characteristics from the MME or use its own configured values.

Format

Octet string

Length

2 bytes

Charging Characteristics Selection Mode

This field specifies how the Charging Characteristics was selected.

Supported values:

servingNodeSupplied (0),

homeDefault (3),

roamingDefault (4),

visitingDefault (5)

Format

Enumerated

Length

1 byte

Charging ID

This field is a charging identifier, which can be used together with the P-GW address to identify all records involved in a single bearer context. The Charging ID is generated by the P-GW during bearer context activation and is transferred to the context requesting SGW.

Format

Integer

Length

1-5 bytes

Diagnostics

This field is included in the CDR when the bearer context is released and when the option "gtpp attribute diagnostics" is configured. Only the choice of "gsm0408Value" is used (see below).

Format

Choice (gsm0408 only).

Length

3 bytes

gsm0408Cause

Refer to TS 24.008 for more information.

Format

Integer

Length

1 byte

Duration

This field contains the duration in seconds for the record. For partial records, only the interval described by the recordOpeningTime and the last ChangeTime in the ListOfTrafficVolumes is counted. The value is reset for each new partial CDR. This value is converted from the internal representation in milliseconds to an integer value representing only seconds. The mechanism for this conversion (ceiling, floor, round-off) can be configured.

Format

Integer

Length

1-5 bytes

Dynamic Address Flag

This field indicates that PDN address has been dynamically allocated for that particular IP CAN bearer (PDN connection). This field is missing if address is static. Dynamic address allocation might be relevant for charging e.g. as one resource

offered and possible owned by network operator. The presence of this field indicates that the **Served PDP Address** was dynamically assigned during context activation.

Format
Boolean

Length
1 byte

List of Traffic Data Volumes

This list includes one or more Traffic Volume containers related to a “Change of Charging Condition”. The maximum number of containers is configurable.

Format
Sequence

Length
Variable

Change Of Charging Condition

Each traffic volume container contains details related to a charging condition as described in the following subsections. A new container is usually created for a QoS change and for tariff changes.

The data counted already includes the IP PDP bearer protocols i.e. IP or PPP.

Format
Sequence

Length
Variable

GPRS Uplink data volume

The Data Volume GPRS Uplink field is a part of the ChangeOfCharCondition element in the List of Traffic Volumes. It includes the number of octets received in the uplink direction during the timeframe specified by the container. For each new container, the counter is reset and does not accumulate.

The data counted already includes the IP PDP bearer protocols i.e. IP or PPP.

Format
Integer

Length
1-5 bytes

GPRS Downlink data volume

The Data Volume GPRS Downlink field is a part of the ChangeOfCharCondition element in the List of Traffic Volumes. It includes the number of octets transmitted in the downlink direction during the timeframe specified by the container. For each new container, the counter is reset and does not accumulate.

The data counted already includes the IP PDP bearer protocols i.e. IP or PPP.

Format

Integer

Length

1-5 bytes

Change Condition

The Change Condition field is part of the ChangeOfCharCondition element in the List of Traffic Volumes. It defines the reason for closing the container:

Supported values:

```
ChangeCondition  ::=  ENUMERATED

{

    qoSChange       (0),

    tariffTime      (1),

    recordClosure   (2),

    cGI-SAICHange   (6),     -- bearer modification. "CHI SAI
Change"

    rAIChange       (7),     -- bearer modification. "RAI Change"

    eCGIChange      (10),    -- bearer modification. "ECGI Change"

    tAIChange       (11),    -- bearer modification. "TAI Change"

}
```

1. The change condition is based on the current ULI type and not on new ULI. i.e if the ULI type is ECGI during CSRequest and while changing the ULI, whatever be the ULI type in MBRequest, the "changeCondition" should be ECGI change.
2. If the initial ULI has one or more ULI Types(i.e ECGI, TAI, RAI, CGI), then the change condition the priority will be as follows:
   - CGI-SAI Change
   - RAI Change
   - TAI Change
   - ECGI Change
3. If the current ULI type is not present (optional) the change condition is based on the new ULI contents. i.e if new ULI has ECGI, then we will consider it as ECGI change.
4. The ULI in main CDR part indicates the ULI at the time of record opening time. i.e If CSReq comes with ULI U1 and then the ULI is changed to U2, U3 and if we generate a CDR the main ULI in CDR contains ULI as U1, but the next CDR generated contains the ULI as U3 and so on.
5. In container the ULI is present in next container if the previous change condition is either RAI Change, CGI-SAI Change, TAI Change, ECGI Change.

Format

Enumerated

Length

1 byte

Change time

The Change Time field is part of the ChangeOfCharCondition element in the List of Traffic Volumes. It provides the local time when a change condition (e.g. record closure) occurred and the container was closed.

The format is shown below.

TimeStamp ::= OCTET STRING (SIZE(6))

-- The contents of this field are a compact form of the UTC Time format containing local time plus an offset to universal time. Binary coded decimal encoding is employed for the digits to reduce the storage and transmission overhead

-- e.g. YYMMDDhhmmssShhmm

-- where

-- YY = Year 00 to 99 BCD encoded

-- MM = Month 01 to 12 BCD encoded

-- DD = Day 01 to 31 BCD encoded

-- hh = hour 00 to 23 BCD encoded

-- mm = minute 00 to 59 BCD encoded

-- ss = second 00 to 59 BCD encoded

-- S = Sign 0 = “+”, “-” ASCII encoded

-- hh = hour 00 to 23 BCD encoded

-- mm = minute 00 to 59 BCD encoded

Format

BCD encoded octet string

Length

9 bytes

User Location Information

This field contains the User Location Information as described in TS 29.274 for eGTP cases (e.g. CGI, SAI, RAI TAI and ECGI).

The field is provided by the SGSN/MME and transferred to the S-GW/P-GW during the IP-CAN bearer activation/modification.

User Location Information contains the location (e.g. CGI/SAI, ECGI/TAI or RAI) where the UE is located and used during the transfer of the data volume captured by the container (applicable only to the SGW-CDR). This is included in the Traffic data container only if previous container's change condition is “user location change”. Note the user location information in SGW-CDR main level contains the location where the UE was when CDR was opened.

Format

Octet string

Length

Based on the type of identity it may vary.

EPC QoS Requested

EPC QoS Information: In case of IP-CAN bearer specific container, this contains authorized QoS for the IP-CAN bearer. First container for each QCI/ARP pair includes this field. In following containers, this field is present if previous change condition is “QoS change”. This field is applicable only in SGW-CDR.

Format

```
EPCQoSInformation  ::= SEQUENCE

{

    --

    -- See TS 29.212 for more information

    --

    qCI                         [1] INTEGER,

    maxRequestedBandwithUL      [2] INTEGER OPTIONAL,

    maxRequestedBandwithDL      [3] INTEGER OPTIONAL,

    guaranteedBitrateUL         [4] INTEGER OPTIONAL,

    guaranteedBitrateDL         [5] INTEGER OPTIONAL,

    aRP                         [6] INTEGER OPTIONAL

}
```

Length

Variable length format (Will vary based on the values).

iMSsignalingContext

Indicates if the IP-CAN bearer is used for IMS signalling. It is only present if the IP-CAN bearer is an IMS signalling bearer. A IP-CAN bearer for IMS signalling is determined via the “IM CN Subsystem Signalling Flag” conveyed via the “Activate PDP context request” message from the MS to the network (refer to TS 24.008).

Format

Null

Length

Zero

List of Served Node Addresses

This field contains 1-16 Serving Node control plane IP used during this record (max of 15 Serving Node Changes). This is a list of IP addresses. If the PLMN-ID of the MME is same after Handover to new MME, one more IP address is added to the list. If the list is overflowed, with configured number of IP addresses, a CDR with “serving node Change” as cause for record

closure will be generated. The serving node addresses, listed here map to the serving node types listed in the field “Serving node Types” in sequence.

Format

Octet String containing list of IPV4 or IPV6 IP addresses.

Length

The length can vary based on whether the encoded IP address is IPV4 or IPV6.

Served Node IPv4 Binary Address

The octet string included in the field described above includes the IPV4 address of the MME.

Format

Octet String

Length

4 bytes

Served Node IPv6 Binary Address

The octet string included in the field described above includes the IPV6 address of the MME.

Format

Octet String

Length

16 bytes

Local Record Sequence Number

This field contains a unique sequence number associated with the NodeId field and independent of the bearer context. For each Node ID, this number with range 1..4294967295 is allocated sequentially for each CDR. This along with a Node ID uniquely identifies a CDR.For SGW-CDRs, this field is only included when the option “gtpp attribute local-record-sequence” number is configured.

Format

Octet String

Length

1-5 bytes

MS Time Zone

The “Time Zone” IE that the MME may provide to the SGW during the PDN context activation/modification procedure.

Format

Octet String

Length

2 bytes

Node ID

This field contains an identifier string for the node that had generated the CDR.

The NodeID field is a printable string of the ndddSTRING format:

n: The first digit is the Sessmgr restart counter having a value between 0 and 7.

ddd: The number of the sessmgr instance generating the CDR.

STRING: This is a configured Node-ID-Suffix having any string between 1 to16 characters, defined using the gtpp attribute node-id command.

If this node-id-suffix is not configured, the S-GW uses the GTPP context name as the Node-id-suffix (truncated to 16 characters).

This field is only included when the option "gtpp attribute local-record-sequence-number" is configured.

Format

IA5string

Length

5-20 bytes

PDN Connection Id

This field defines the PDN connection (IP-CAN session) identifier to identify different records belonging to same PDN connection. This field includes Charging Id of first IP-CAN bearer activated within the PDN connection. Together with P-GW address this uniquely identifies the PDN connection.

Format

Integer.

Length

1-5 bytes

PDP PDN Type

-- OCTET 1: PDP Type Organization

```
Spare '1111'     PDP Type Organization Value
```

PDP Type Organization	Value
ETSI	0
IETF	1

Note: In LTE, only IETF is supported.

-- OCTET 2: PDP/PDN Type Number

```
Bits

3  2  1
```

```
0  0  1    IPv4

0  1  0    IPv6

0  1  1    IPv4/IPv6

Bits 8-4 of octet are spare and are coded as zero.
```

Format

Octet string

Length

2 bytes

PGW Address used

These field is the serving P-GW IP address for the Control Plane. If both an IPv4 and an Ipv6 address of the P-GW is available, the P-GW shall include the Ipv4 address in the CDR. This is a choice attribute and the CDR can contain the Binary format or the ASCII format in the CDR.

Format

Octet string

Length

The length can vary based on whether the encoded IP address is IPv4 or IPv6.

PGW IPv4 Binary Address

The octet string included in the field described above includes the IPv4 address assigned to the subscriber by of the P-GW in binary coding.

Format

Octet string

Length

4 bytes

PGW IPv6 Binary Address

The octet string included in the field described above includes the IPv6 address assigned to the subscriber by of the P-GW in binary coding.

Format

Octet string

Length

16 bytes

RAT Type

Holds the value of RAT Type, as provided to S-GW and P-GW, described in TS 29.274 for eGTP case.

RAT Types	Values (Decimal)
<reserved>	0
UTRAN	1
GERAN	2
WLAN	3
GAN	4
HSPA Evolution	5
EUTRAN	6
<spare>	7-255

The field is provided by the SGSN/MME and transferred to the S-GW/P-GW during the IP-CAN bearer activation/modification.

Format

Integer

Length

1 byte

Record Extensions

A set of network operator/manufacturer specific extensions to the record.

This field is used to report a maximum of three RAN cause codes and packet counts.

Important: This field is operator-defined and is not encoded in any S-GW CDR dictionary until release v14.0.

Format

Sequence

Length

Variable Length Format

Record Opening Time

This field contains the time stamp when a PDP context is activated in SGSN or when a subsequent record is opened after a partial record.

The timestamp is determined based on the internal timer which has an accuracy of 10ms. Depending on the configured mechanism this is translated into the timestamp which only shows the full seconds.

The format is shown below.

TimeStamp ::= OCTET STRING (SIZE(6))

The contents of this field are a compact form of the UTC Time format containing local time plus an offset to universal time. Binary coded decimal encoding is employed for the digits to reduce the storage and transmission overhead

-- e.g. YYMMDDhhmmssShhmm

-- where

-- YY = Year 00 to 99 BCD encoded

-- MM = Month 01 to 12 BCD encoded

-- DD = Day 01 to 31 BCD encoded

-- hh = hour 00 to 23 BCD encoded

-- mm = minute 00 to 59 BCD encoded

-- ss = second 00 to 59 BCD encoded

-- S = Sign 0 = “+”, “-” ASCII encoded

-- hh = hour 00 to 23 BCD encoded

-- mm = minute 00 to 59 BCD encoded

Format

BCD encoded octet string

Length

9 bytes

Record Sequence Number

A running sequence number with range 1.. 4294967296 used to link partial records generated by the SGW for a specific IP-CAN bearer context (characterized with the same Charging ID and P-GW address). This field is not present if the first record is also the final record.

Format

Integer

Length

1-5 bytes

Record Type

The field identifies the type of the record:

SGW-CDR (sgwPDPRecord) 84 (0x54)

Format

Integer

Length

1 byte

Served IMEISV

This fields contains the international mobile equipment identity (IMEISV) of the equipment served, if available.

The structure of the IMEI is defined in TS 23.003.

The IMEI is composed of the following elements:

- Type Allocation Code (TAC). Its length is 8 digits;
- Serial Number (SNR) is an individual serial number uniquely identifying each equipment within each TAC. Its length is 6 digits;
- Software Version Number (SVN) identifies the software version number of the mobile equipment. Its length is 2 digits.

If SV is not available, a filler digit “f” is added after the spare digit to fill up the last byte. Spare digit: this digit shall be zero, when transmitted by the MS.

Format

BCD encoded octet string

Length

8 bytes

Served IMSI

This field contains the International Mobile Subscriber Identity (IMSI) of the served party. The IMSI is formatted in accordance with 3GPP TS 23.003.

Format

BCD encoded octet string

Length

3-8 bytes

Served MSISDN

The field tracks the Mobile Station (MS) ISDN number (MSISDN) of the subscriber which is transparently copied from the Create Session Request message.

The MSISDN is TBCD encoded as shown in the example below:

3GPP TS 23.003 (CCITT Rec. E 213)

ServedMSISDN ::= OCTET STRING (SIZE(1..9))

MSISDN in CDR is 1:1 copy of the MSISDN sent in GTP-V2 message. MSISDN value contains only the actual MSISDN number (does not contain the “nature of address indicator” octet, which indicates “international number” as in 3GPP TS 29.002 [41]) and is encoded as TBCD digits (i.e., digits from 0 through 9 are encoded “0000” to “1001”). When there is an odd number of digits, bits 8 to 5 of the last octet are encoded with the filler “1111”.

example:

encoded: H' 94 71 02 04 30 50

Format

BCD encoded octet string

Length

1-9 bytes

Served PDP PDN Address

This field contains the IP address for the PDN connection (PDP context, IP-CAN bearer) if available. This is a network layer address of type IP version 4 (PDN Type is IPv4) or IP version 6 (PDN Type is IPv6 or IPv4v6). The address for each Bearer type is allocated either temporarily or permanently (see "Dynamic Address Flag"). This parameter shall be present except when both the Bearer type is PPP and dynamic address assignment is used.

Format

Octet string

Length

The length can vary based on whether the encoded IP address is IPv4 or IPv6.

PDP IP Address

This field contains the IP address for the PDP context.

Format

IP address

Length

The length can vary based on whether the encoded IP address is IPv4 or IPv6.

PDP IPv4 Binary Address

The octet string included in the field described above includes the IPv4 address assigned to the subscriber by of the P-GW in binary coding.

Format

Octet string

Length

4 bytes

PDP Ipv6 Binary Address

The octet string included in the field described above includes the IPv6 address assigned to the subscriber by of the P-GW in binary coding.

Format

Octet string

Length

16 bytes

Serving Node PLMN Identifier

PLMN identifier (MCC and MNC) of the P-GW used. This field is present in CDRs if the P-GW PLMN-ID is available in the CSR message from Serving Node (MME).

MCC and MNC are coded as described for “Routing Area Identity” in TS 29.060.

Format

Octet string

Serving Node Type

These fields contain one or several serving node types in control plane of S-GW or P-GW, which have been connected during the record. The serving node types listed here map to the serving node addresses listed in the field “Serving node Address” in sequence.

The possible values are:

```
ServingNodeType  ::= ENUMERATED

{

        sGSN      (0),

        pMIPSGW   (1),

        gTPSGW    (2),

        ePDG      (3),

        hSGW      (4),

        mME       (5)

}
```

Note: In the SGW-CDR, the possible values are SGSN(0) and MME(5).

Format

Sequence of serving Node Type.

Length

Variable length format (Based on number of nodes connected during this period).

SGW Address Used

These field is the serving S-GW IP address for the Control Plane. If both an IPv4 and an IPv6 address of the S-GW is available, the S-GW shall include the IPv4 address in the CDR. This is a choice attribute and the CDR can contain the Binary format or the ASCII format in the CDR.

Format

Octet string

Length

The length can vary based on whether the encoded IP address is IPv4 or IPv6.

SGW IPv4 Binary Address

This field is the serving control plane S-GW IPv4 address on the S5 interface.

Format

Octet string

Length

4 bytes

SGW IPv6 Binary Address

This field is the serving control plane S-GW IPv6 address on the S5 interface.

Format

Octet string

Length

16 bytes

SGW Change

This field is present only in the SGW-CDR to indicate that this is the first record after an S-GW change. In this case, it is set to TRUE (“FF”)

Format

Boolean

Length

1 byte

Start Time

This field contains the time when the IP-CAN session starts at the S-GW/P-GW, available in the CDR for the first bearer in an IP-CAN session.

The timestamp is determined based on the internal timer which has an accuracy of 10ms. Depending on the configured mechanism this is translated into the timestamp which only shows the full seconds.

The format is shown below.

TimeStamp ::= OCTET STRING (SIZE(6))

The contents of this field are a compact form of the UTC Time format containing local time plus an offset to universal time. Binary coded decimal encoding is employed for the digits to reduce the storage and transmission overhead

-- e.g. YYMMDDhhmmssShhmm

-- where

-- YY = Year 00 to 99 BCD encoded

-- MM = Month 01 to 12 BCD encoded

-- DD = Day 01 to 31 BCD encoded

-- hh = hour 00 to 23 BCD encoded

-- mm = minute 00 to 59 BCD encoded

-- ss = second 00 to 59 BCD encoded

-- S = Sign 0 = “+”, “-” ASCII encoded

-- hh = hour 00 to 23 BCD encoded

-- mm = minute 00 to 59 BCD encoded

Format

BCD encoded octet string

Length

9 bytes

Stop Time

This field contains the time when the IP-CAN session is terminated at the S-GW/P-GW, available in the CDR for the last bearer in an IP-CAN session.

The timestamp is determined based on the internal timer which has an accuracy of 10ms. Depending on the configured mechanism (ceiling, floor, round-off) this is translated into the timestamp which only shows the full seconds.

The format is shown below.

TimeStamp ::= OCTET STRING (SIZE(6))

The contents of this field are a compact form of the UTC Time format containing local time plus an offset to universal time. Binary coded decimal encoding is employed for the digits to reduce the storage and transmission overhead

-- e.g. YYMMDDhhmmssShhmm

-- where

-- YY = Year 00 to 99 BCD encoded

-- MM = Month 01 to 12 BCD encoded

-- DD = Day 01 to 31 BCD encoded

-- hh = hour 00 to 23 BCD encoded

-- mm = minute 00 to 59 BCD encoded

-- ss = second 00 to 59 BCD encoded

-- S = Sign 0 = “+”, “-” ASCII encoded

-- hh = hour 00 to 23 BCD encoded

-- mm = minute 00 to 59 BCD encoded

Format

BCD encoded octet string

Length

9 bytes

User CSG Information

This field contains the User CSG Information (UCI) status of the user accessing a CSG cell. Closed Subscriber Group identifies a group of subscribers who are permitted to access one or more CSG cells of the PLMN as a member of the CSG.

Length

Varies

CSG ID

This field is a unique identifier within the scope of PLMN which identifies a Closed Subscriber Group (CSG) in the PLMN associated with a CSG cell or group of CSG cells. The value of CSG ID will be printed as the hexadecimal value received in AAA.

Format

Octet string

Length

4 bytes

CSG Access Mode

This field is the CGI access mode of the user accessing a CSG cell.

Possible access modes are:

- Closed
- Hybrid

Format

Enumeration (Integer)

Length

1 byte

CSG Membership Indication

This field indicates CSG membership for the user when hybrid access applies, as defined in TS 29.060 [215] for GPRS case, and in TS 29.274 [223] for EPC case.

Format

Null

Length

Zero

User Location Information

This field contains the User Location Information as described in TS 29.274 for eGTP case (e.g. CGI, SAI, RAI TAI and ECGI).

The field is provided by the SGSN/MME and transferred to the S-GW/P-GW during the IP-CAN bearer activation/modification.

User Location Information contains the location (e.g. CGI/SAI, ECGI/TAI or RAI) where the UE is located and used during the transfer of the data volume captured by the container (applicable only to the SGW-CDR). This is included in the Traffic data container only if previous container's change condition is “user location change”. Note the user location information in SGW-CDR main level contains the location where the UE was when PGW-CDR was opened.

The flags ECGI, TAI, RAI, SAI and CGI in octet 1 indicate if the corresponding fields are present in the IE or not. If one of these flags is set to “0”, the corresponding field is not present at all. The respective identities are defined in 3GPP TS 23.003.

The following subclauses specify the coding of the different identities. For each identity, if an Administration decides to include only two digits in the MNC, then bits 5 to 8 of octet 7 are coded as “1111”.

CGI field:

The Location Area Code (LAC) consists of 2 octets. Bit 8 of Octet 9 is the most significant bit and bit 1 of Octet 10 the least significant bit. The coding of the location area code is the responsibility of each administration. Coding using full hexadecimal representation shall be used.

The Cell Identity (CI) consists of 2 octets. Bit 8 of Octet 11 is the most significant bit and bit 1 of Octet 12 the least significant bit. The coding of the cell identity is the responsibility of each administration. Coding using full hexadecimal representation shall be used.

SAI field:

The Location Area Code (LAC) consists of 2 octets. Bit 8 of Octet 9 is the most significant bit and bit 1 of Octet 10 the least significant bit. The coding of the location area code is the responsibility of each administration. Coding using full hexadecimal representation shall be used.

The Service Area Code (SAC) consists of 2 octets. Bit 8 of Octet 11 is the most significant bit and bit 1 of Octet 12 the least significant bit. The SAC is defined by the operator.

RAI field:

The Location Area Code (LAC) consists of 2 octets. Bit 8 of Octet 9 is the most significant bit and bit 1 of Octet 10 the least significant bit. The coding of the location area code is the responsibility of each administration. Coding using full hexadecimal representation shall be used.

The Routing Area Code (RAC) consists of 2 octets. Only Octet 11 contains the RAC. Octet 12 is coded as all 1's (11111111). The RAC is defined by the operator.

TAI field:

The Tracking Area Code (TAC) consists of 2 octets. Bit 8 of Octet 9 is the most significant bit and bit 1 of Octet 10 the least significant bit. The coding of the tracking area code is the responsibility of each administration. Coding using full hexadecimal representation shall be used.

ECGI field:

The E-UTRAN Cell Identifier (ECI) consists of 28 bits. Bit 4 of octet 10 is the most significant bit and bit 1 of Octet 11 the least significant bit. The coding of the E-UTRAN cell identifier is the responsibility of each administration. Coding using full hexadecimal representation shall be used.

Format

Octet string

Length

Varies based on the type of identity.

Chapter 15
WLAN CDR Field Reference

This chapter provides a reference for WLAN-CDR fields supported by PDG and TTG.

The PDG/TTG provides CDRs that are compliant with the definitions in 3GPP TS32.298. When modifications are required, changes to the standard behavior can be implemented in different dictionaries which can be selected in the configuration file. This provides the flexibility to adapt to a customer's needs, and therefore, to a legacy post-processing billing interface, while retaining the standard behavior.

A complete list and descriptions of supported CDR fields is provided in the *WLAN CDR Field Descriptions* chapter of this reference.

Important: For more information on custom dictionaries, contact your Cisco account representative.

The Category column in all tables use key described in the following table.

Table 25. Dictionary Table Key

Abbreviation	Meaning	Description
M	Mandatory	A field that must be present in the CDR.
C	Conditional	A field that must be in a CDR if certain conditions are met.
OM	Operator Provisonable: Mandatory	A field that an operator has provisioned and must be included in the CDR for all conditions.
OC	Operator Provisionable: Conditional	A field that an operator has provisioned that must be included in the CDR if certain conditions are met.

CDR Fields Supported in WLAN-CDRs

The table in this section lists the WLAN fields present in GTPP dictionaries.

standard, and custom1 - custom6 Dictionaries

WLAN-CDR fields for TS 32.252

Field	Category	Description
Record Type	M	This field identifies the type of record. The 3GPP 32298 does not define any values for record type.
Network Initiated PDP Context	O	This field indicates that the PDP context was network-initiated. This field is missing in case of UE-activated PDP context.
Served IMSI	M	This field contains the International Mobile Subscriber Identity (IMSI) of the served party. The IMSI is formatted in accordance with 3GPP TS 23.003.
PDG Address	M	This field provides the current service PDG IP address for the control plane.
PDG IPv4 Binary Address	M	The octet string in this field includes the IPv4 address of the PDG service in binary coding.
Charging ID	M	This field contains a charging identifier, which can be used with the PDG address to identify all records produced in the PDG involved in a single PDP context. The charging ID is generated by the PDG at PDP context activation.
Access Point Name Network Identifier	M	This field contains the Network Identifier part of the Access Point Name (APN). It is provided by WMN during the IPSec or SSL establishment procedure.
PDP Type	O	This field defines the PDG type, IP or PPP.
Served WLAN PDP Address	M	This field contains the PDP address of the served IMSI. The standard 3GPP TS 32.298 allows a choice of either IPAddress or ETSIAddress.
WLAN UE Remote Address	M	This field contains the PDP address of the served IMSI, which is supported only in IPAddress by the PDG.
WLAN UE Remote IPv4 Binary Address	M	The octet string in this field contains the IPv4 address assigned to the subscriber by the PDG/TTG in binary coding.
Dynamic Address Flag	O	This field indicates that the PDP address has been dynamically allocated for that particular PDP context. This field is missing if the address is static, that is, part of the PDP context subscription.
List of Traffic Data Volumes	M	This list includes one or more Traffic Data Volume containers. The number of containers is configurable with a maximum of 4 for WLAN-CDRs.

Field	Category	Description
Change of Charging Condition	M	One traffic data volume container contains a list of change of charging conditions: • Data Volume Uplink • Data Volume Downlink • Change Condition • Change Time • Failurehandling Continue The QoS values may only be included in the first container. In later containers, the presence depends on what was changed.
QoS Negotiated	O	This field indicates that the applied QoS is accepted by the network. This field is compliant with 3GPP standards.
GPRS Uplink Data Volume	M	This field includes the number of octets transmitted during the use of the packet data services in the uplink direction. Note that a maximum of 2^32 bytes can be counted in this field. A volume trigger should be defined for this value to avoid an overflow, if not already done for a smaller amount of traffic.
GPRS Downlink Data Volume	M	This field includes the number of octets transmitted during the use of the packet data services in the downlink direction. Note that a maximum of 2^32 bytes can be counted in this field. A volume trigger should be defined for this value to avoid an overflow, if not already done for a smaller amount of traffic.
Change Condition	M	This field defines the reason for closing the container, such as tariff time change, QoS change, or closing of the CDR. Values according to 3GPP TS 32.298 are: • qoSChange = 0 • tariffTime = 1 • recordClosure = 2
Change Time	M	A time stamp that defines the moment when the volume container or the CDR is closed.
Record Opening Time	M	This field contains the time stamp of when the PDP context is activated in the PDG or when a subsequent record is opened after a partial record. The timestamp is determined based on the internal timer which has an accuracy of 10ms. Depending on the configured mechanism (ceiling, floor, or round-off) this field is translated to only show full seconds.
Duration	M	This field contains the duration in seconds of the PDP contexts with the range of 0 to 4294967295 (2^32-1). It is the duration from Record Opening Time to record closure. For partial records, this is the duration of the individual partial record and not the cumulative duration.
Cause for Record Closing	M	This field shows the reason for the release of the CDR. The values are: • normalRelease = 0 • abnormalRelease = 4 • volumeLimit = 16 • timeLimit = 17 • maxChangeCond = 19 • managementIntervention = 20

Field	Category	Description
Diagnostics	O	This field is included in the CDR when the PDP context is released and when the option **gtpp-attribute diagnostics** is configured.
gsm0408Cause	M	This cause is used in the Diagnostics field and contains one of the following values: • 36: If the PDP context is terminated gracefully • 40: AAA Server disconnect • 26: If the PDG sends delete PDP context request for any other reason
Record Sequence Number	O	A running sequence number with range 1 to 4294967295 that links partial records generated by the PDG for a specific PDP context (characterized with the same Charging ID and PDG address pair). This field is not present if the first record is also the final record.
Node ID	O	This field contains an identifier string for the node that generated the CDR. The NodeID field is a printable string of the ndddSTRING format: • n: the first digit is the sessmgr restart counter having a value between 0 and 7. • ddd: The number of the sessmgr instance generating the CDR. • STRING: A configured Node-ID-Suffix string of 1 to 16 characters. Defined with the **gtpp attribute node-id** command.
recordExtensions	O	
Local Record Sequence Number	O	For each Node ID, this number with range 1 to 4294967295, is allocated sequentially for each CDR. With the Node ID, it uniquely identifies a CDR. For WLAN-CDRs, this field is only included when the option **gtpp attribute local-record-sequence number** is configured.
APN Selection Mode	O	An index that shows how the APN is selected: • 0 = MS or network provided APN, subscribed verified • 1 = MS provided APN, subscription not verified • 2 = Network provided APN, subscription not verified
Served MSISDN	O	This field tracks the Mobile Station (MS) ISDN number (MSISDN) of the subscriber, which is sent by the AAA server.
Charging Characteristics	M	Lists the charging characteristics applied to the PDP context. The PDG can accept charging characteristics from the AAA server or use its own configured value. PDG-configured charging characteristics are specified as part of the PDG Service and are applied for WLAN-CDRs to subscriber PDP contexts through APN templates.

Field	Category	Description
Charging Characteristics Selection Mode	O	Lists the charging characteristic type that the PDG applied to the CDR. The values for this field are defined in 3GPP TS 32.298: • AAASupplied (0): The PDG is using the charging characteristics supplied by the AAA Server. • homeDefault (3): PDG configured charging characteristics for home subscribers are used. • roamingDefault (4): PDG configured charging characteristics for roaming subscribers are used. • visitingDefault (5): PDG configured charging characteristics for visiting subscribers are used.
Rat Type	O	This field shows the Radio Access Technology (RAT) type currently used by the Mobile Station. This field is present in the CDR if provided by WLAN. RAT Type values: • 0 = Reserved • 1 = UTRAN • 2 = GERAN • **3 = WLAN** • 4-255 = Spare

Chapter 16
WLAN CDR Field Descriptions

This chapter describes the WLAN-CDR fields supported by PDG/TTG.

The following information is provided for each field:

- **Description:** The field's description.
- **Format:** The field's data format.
- **Length:** The field's size, in bytes.

All WLAN-CDRs are encoded using the ASN.1 format and are sent to the charging gateway function (CGF) using the GPRS Tunneling Protocol Prime (GTPP) as defined in the following standards:

- 3GPP TS 32.015
- 3GPP TS 32.215
- 3GPP TS 32.251 (v8.5.0, v8.6.0)
- 3GPP TS 32.252 (WLAN-CDRs)

Also see the *WLAN CDR Field Reference* chapter for information on CDR fields supported in WLAN-CDRs.

Important: The behavior for several of the fields supported in CDRs can be modified. For more information, refer to the **`gtpp attributes`** command in the *Command Line Interface Reference*.

CDR Fields

Access Point Name Network Identifier

This field contains the Network Identifier part of the Access Point Name (APN). It is provided by WMN during IPSEC or SSL establishment procedure.

Format
IA5 string

Length
1-63 bytes

APN Selection Mode

An index indicating how the APN is selected.

The following APN selection mode indexes are possible:

- 0: MS or network provided APN, subscribed verified
- 1: MS provided APN, subscription not verified
- 2: Network provided APN, subscription not verified

Format
Enumerated

Length
1 byte

Cause for Record Closing

This field contains a reason for the release of the CDR.

Supported values:

- normalRelease 0
- abnormalRelease 4
- volumeLimit 16
- timeLimit 17
- maxChangeCond 19
- managementIntervention 20

Format
Integer

Length
1 byte

Charging Characteristics

This field lists the charging characteristics applied to the PDP context.

The PDG can accept charging characteristics from the AAA Server or use its own configured value. PDG configured charging characteristics are specified as part of the PDG Service and are applied for WLAN-CDRs to subscriber PDP contexts through APN templates.

Format
Octet string

Length
2 bytes

Charging Characteristics Selection Mode

The charging characteristic type that the PDG applied to the CDR.

The following values for this field are defined in 3GPP TS 32.298:

- AAASupplied (0): The PDG is using the charging characteristics supplied by the AAA Server.
- homeDefault (3): PDG configured charging characteristics for home subscribers are used.
- roamingDefault (4): PDG configured charging characteristics for roaming subscribers are used.
- visitingDefault (5): PDG configured charging characteristics for visiting subscribers are used.

Format
Enumerated (Integer)

Length
1 byte

Charging ID

This field contains a charging identifier, which can be used together with the PDG address to identify all records produced in the PDG involved in a single PDP context. The Charging ID is generated by the PDG at PDP context activation.

The possible values for the charging ID, which are defined in TS 29.060 are 1 - 4,294,967,295 and those values are encapsulated in the following scheme in the CDR field:

1 - 127 850101-85017F

128 - 32,767 85020080-85027FFF

32,768 - 8,388,607 8503008000-85037FFFFF

8,388,608 - 2,147,483,647 850400800000-85047FFFFFF

2,147,483,648 - 4,294,967,295 85050080000000 - 850500FFFFFFFF

Format
Integer

Length
1–5 bytes

Diagnostics

This field is included in the CDR when the PDP context is released and when the option **gtpp attribute diagnostics** is configured. Only the choice of "gsm0408Value" is used.

Format
Choice

Length
3 bytes

gsm0408Cause

This cause is used in the Diagnostics field and contains one of the following values:

- 36: If the PDP context is terminated gracefully
- 40: AAA Server disconnect
- 26: If the PDG sends delete PDP context request for any other reason

Format
Integer

Length
1 byte

Dynamic Address Flag

This field indicates that the PDP address has been dynamically allocated for that particular PDP context. This field is missing if address is static i.e. part of PDP context subscription.

Format
Boolean

Length
1 byte

Duration

This field contains the relevant duration in seconds for PDP contexts with the range of 0 through 4294967295 (2^32-1).

It is the duration from Record Opening Time to record closure. For partial records, this is the duration of the individual partial record and not the cumulative duration.

Format
Integer

Length
1–5 bytes

Local Record Sequence Number

For each Node ID, this number with the range of 1 through 4294967295 is allocated sequentially for each CDR. This along with a Node ID uniquely identifies a CDR.

For WLAN-CDRs, this field is only included when the option **`gtpp attribute local-record-sequence number`** is configured.

Format
Integer

Length
1-5 bytes

List of Traffic Data Volumes

This list includes one or more traffic data volume containers. The number of containers is configurable with a maximum of 4 for WLAN-CDRs.

Format
Sequence

Length
Variable

Change Of Charging Condition

One traffic data volume container contains a list of change of charging conditions:

- Data Volume Uplink
- Data Volume Downlink
- Change Condition
- Change Time
- Failurehandling Continue

The QoS values may only be included in the first container, in later containers the presence depends upon what was changed.

Format
Sequence

Length
Variable

QoS Negotiated

This field indicates the applied QoS is accepted by the network. It is compliant to 3GPP standards.

Format
Octet string

Length
4–15 bytes

GPRS Uplink data volume

This field includes the number of octets transmitted during the use of the packet data services in the uplink direction.

Note that a maximum of 2^32 bytes can be counted in this field. A volume trigger should be defined at least for this value to avoid an overflow, if not done already for a smaller amount of traffic.

Format

Integer

Length

1–5 bytes

GPRS Downlink data volume

This field includes the number of octets transmitted during the use of the packet data services in the downlink direction.

Note that a maximum of 2^32 bytes can be counted in this field. A volume trigger should be defined at least for this value to avoid an overflow, if not done already for a smaller amount of traffic.

Format

Integer

Length

1–5 bytes

Change Condition

This field defines the reason for closing the container, such as tariff time change, QoS change or closing of the CDR.

The following values are defined according to 3GPP TS 32.298:

- qoSChange 0
- tariffTime 1
- recordClosure 2

Format

Enumerated (Integer)

Length

1 byte

Change time

Change Time is a time stamp, which defines the moment when the volume container is closed or the CDR is closed.

3GPP Format definition:

TimeStamp ::= OCTET STRING (SIZE(9))

-- UTC time (compact form: local time + offset to GMT)

-- YYMMDDhhssShhmm

-- octet 1..6: local time

-- octet 1: YY .. decade (2 digits BCD non-twisted, readable)

-- octet 2: MM ... month (2 digits BCD non-twisted, readable)

-- octet 3: DD ... day (2 digits BCD non-twisted, readable)

-- octet 4: hh ... hour (2 digits BCD non-twisted, readable)

-- octet 5: mm ... minute (2 digits BCD non-twisted, readable)

-- octet 6: ss ... second (2 digits BCD non-twisted, readable)

-- octet 7..9: … offset to GMT (universal time)

-- octet 7: S ... H'2B: "+" H'2D: "-"(ASCII)

-- octet 8: hh ... hour (2 digits BCD non-twisted, readable)

-- octet 9: mm ... minute (2 digits BCD non-twisted, readable)

Format

BCD encoded octet string

Length

9 bytes

Node ID

This field contains an identifier string for the node that generated the CDR.

On the PDG, this NodeID field is a printable string of the ndddSTRING format:

n: The first digit is the sessmgr restart counter having a value between 0 and 7.

ddd: The number of the sessmgr instance generating the CDR.

STRING: This is a configured node-id-suffix having any string from 1 to16 characters, defined using the **gtpp attribute node-id** command.

If this node-id-suffix is not configured, the PDG uses the GTPP context name as the node-id-suffix (truncated to 16 characters).

For WLAN-CDRs, this field is only included when the option **gtpp attribute local-record-sequence number** is configured.

Format

IA5string

Length

5-20 bytes

PDG Address

This field provides the current serving PDG IP address for the Control Plane. The standard 32.298 offers a choice for the encoding of the address to be either in binary or text format.

The PDG encodes the address in binary format and includes the octet string.

Format

Choice

Length
6 bytes

PDG IPv4 Binary Address

The octet string in this field includes the IPv4 address of the PDG service in binary coding.

Format
Octet string

Length
4 bytes

PDP Type

This field defines the PDP type, e.g. IP or PPP.

Supported values:

- IP = f121
- PPP = f001

Format
Octet string

Length
2 bytes

RAT Type

This field indicates the Radio Access Technology (RAT) type currently used by the Mobile Station. This field is present in the CDR if provided by WLAN.

RAT Type values:

- Reserved 0
- UTRAN 1
- GERAN 2
- WLAN 3
- Spare 4-255

Format
Integer

Length
1 byte

Record Opening Time

This field contains the time stamp when PDP context is activated in PDG or when a subsequent record is opened after a partial record.

The timestamp is determined based on the internal timer which has an accuracy of 10ms. Depending on the configured mechanism (ceiling, floor, or round-off) this field is translated to only show full seconds.

The contents of this field are a compact form of the UTC Time format containing local time plus an offset to universal time. Binary coded decimal encoding is employed for the digits to reduce the storage and transmission overhead

Format
BCD encoded octet string

Length
9 bytes

Record Sequence Number

A running sequence number with the range of 1 through 4294967295 used to link partial records generated by the PDG for a specific PDP context (characterized with the same Charging ID and PDG address pair). This field is not present if the first record is also the final record.

Format
Integer

Length
1–5 bytes

Record Type

This field identifies the type of the record:

WLAN-CDR(WLANPDGRecord) 95 (0x5F)

WLAN-CDR(WLANTTGRecord) 96 (0x60)

The 3GPP 32.298 does not define any values for record type. This value is selected as this is not yet reserved by any CDRs.

Format
Integer

Length
1 byte

Served IMSI

This field contains the International Mobile Subscriber Identity (IMSI) of the served party.

The IMSI is formatted in accordance with 3GPP TS 23.003.

Example for Coding: (Set by PDG)

```
3GPP TS 23.003 (CCITT Rec. E 212)
```

```
ServedIMSI ::= OCTET STRING (SIZE(1..8))

-- subscriber identification IMSI

-- octet 1..8: <= 15 digits TBCD-String (twisted)

-- substructure (without spares or fillers):

-- 3 digits - mobile country code (MCC)

-- 2 digits - mobile network code (MNC)

-- <= 10 digits - mobile subscriber identification number (MSIN)

-- first and intermediate octet = 2 digits

-- last octet = 2 digits or 1 digit + 1 fill digit H'F

--

-- example:

-- IMSI: '262025600010020'

-- filled: '262025600010020F'

-- encoded: H'62 02 52 06 00 01 20 F0
```

Format
BCD encoded octet string

Length
3–8 bytes

Served MSISDN

The field tracks the Mobile Station (MS) ISDN number (MSISDN) of the subscriber, which is sent by AAA server.

The MSISDN is TBCD encoded as shown in the example below:

```
3GPP TS 23.003 (CCITT Rec. E 213)

ServedMSISDN ::= OCTET STRING (SIZE(1..9))

subscriber identification MSISDN

octet 1 : bit 8 (msb): extension bit

= 1 : no extension

other : not relevant


bit 7..5 : type of number
```

```
= 000 : unknown

= 001 : international number

= 010 : national significant number

= 011 : network specific number

= 100 : subscriber number

= 101 : reserved

= 110 : abbreviated number

= 111 : reserved for extension


bit 4..1 : numbering plan indicator

= 0001: ISDN/Telephony Numbering Plan (Rec CCITT E.164)

other : not relevant


octet 2..9: <= 16 digits TBCD-String (twisted)

substructure (without spares or fillers):

1..3 digits - country code (CC)

(only international number)

3 digits - national destination code (NDC)

<= 10 digits - subscriber number (SN)

first and intermediate octet = 2 digits

last octet = 2 digits or 1 digit + 1 fill digit H'F


example:

MSISDN: '<internat #><E.164>491720400305'

encoded: H'91 94 71 02 04 30 50
```

Format

BCD encoded octet string

Length

1–9 bytes

Served WLAN PDP Address

This field contains the PDP address of the served IMSI, for which the standard 3GPP TS 32.298 allows a choice of either IPAddress or ETSIAddress.

Format
Choice

Length
8 bytes

WLAN UE Remote Address

This field contains the PDP address of the served IMSI, which is supported only in IPAddress by the PDG.

Format
Choice

Length
6 bytes

WLAN UE REMOTE IPV4 Binary Address

The octet string in this field contains the IPv4 address assigned to the subscriber by the PDG/TTG in binary coding.

Format
Octet string

Length
4 bytes

Chapter 17
HDD Storage

This chapter describes the mechanism implemented in the ASR 5x00 platform for short term storage of charging records (CDRs) in the event of loss of communication with an external Charging Gateway Function (CGF).

Overview

The hard disk was introduced in the ASR 5x00 platform to add storage capability. The first application is used in CDMA environments to increase buffering for I/O between the gateway and L-ESS to alleviate tight linkage required to avoid record loss due to overrun on the ASR 5x00 PSC buffers.

The External Storage System (ESS) is a high availability, fault tolerant, redundant solution for short-term storage of files containing detail records (UDRs/EDRs/FDRs (xDRs)). To avoid loss of xDRs on the chassis due to overwriting, deletion, or unforeseen events such as power or network failure or unplanned chassis switchover, xDRs are off-loaded to ESS for storage and analysis to avoid loss of charging and network analysis information contained in the xDRs. The xDR files can be pulled by the L-ESS from the chassis, or the chassis can push the xDR files to the L-ESS using SFTP protocol. In the Push mode, the L-ESS URL to which the xDR files need to be transferred to is specified. The configuration allows a primary and a secondary server to be configured. Configuring the secondary server is optional. Whenever a file transfer to the primary server fails for four consecutive times, the files will be transferred to the secondary server. The system running with ECS stores xDRs on an L-ESS, and the billing system collects the xDRs form the L-ESS and correlates them with the AAA accounting messages using 3GPP2-Correlation-IDs (for PDSN) or Charging IDs (for GGSN).

The second application is intended for UMTS environment. Records generated on ASR 5x00 are sent through UDP to an external storage application running on possibly clustered SUN servers utilizing shared storage. In parallel, records are sent over GTPP to a CGF. In addition to (e)GCDRs, the hard disk supports SCDRs and MCDRs generated by SGSN.

Important: The hard disk is not designed to support all features supported by the external storage application and not intended to replace this application in all situations.

The hard disk is useful for other applications:

- Store the Content Filtering static ratings database instead of using FLASH; valuable for other users including recovery scenarios.
- IPMS
- Large volume firewall and other DPI information such as applications/particular user, and users/bay station heretofore not store-able embedded.

The hard drive serves a number of uses in providing storage for various records generated by the mobile gateway that formerly require buffering or treatment outside of the gateway, necessitating purchase and operation of auxiliary servers. For 3GPP2 accounts the hard disk is an enhancement to service, and not a replacement. The hard drive is required to provide non-volatile storage in the ASR 5x00. For 3GPP accounts the hard disk can be used instead of external storage in networks where storage and record formatting needs can be met by the hard disk. The communication link between the ASR 5x00 and external storage is removed. GTPP continues to be supported. Files can be accessed by either GTPP (streaming) or sFTP (file I/O), but not both. At the same time, different files can be accessed by GTPP or sFTP.

Benefits

The HDD functionality provides an additional level of protection to the wireless operator by ensuring the charging records are preserved in case the Charging Gateway (CGF) goes down or loses connectivity with the ASR 5x00 gateway. At the same time, this was implemented in a way that does not require any addition or modification to the existing mediation/billing systems.

Supported Records on HDD

This section describes the various records supported on the HDD:

- Accounting Request Records (ACR)
- Charging Data Records (CDR)
- Event Data Records (EDR)
- Event Records
- Reporting Event Data Records (REDR)
- Usage Data Records (UDR)

Accounting Request Records (ACR)

The Accounting Request Records are types of CDRs that contain offline charging information generated by the Diameter Rf interface. If all the Diameter servers configured in a group are down, ACRs are written to files in formats supported by the external node and stored on the HDD. These files are created when the chassis does not have connection with the CDF. From the HDD, ACR files can be pushed/pulled using FTP/SFTP protocols.

Important: ACRs are supported in 10.0 and later releases.

Directory Structure: By default, the ACR records are placed in the following directory paths:

- RAM-disk: */records/acr/<policy_name>/*
- HDD: */hd-raid/data/records/acr/<policy_name>/*

File Formats: Currently, file format1 to format10 are supported.

Supported Products: HSGW, P-GW, S-GW

Charging Data Records (CDR)

A Charging Data Record is a formatted collection of information about a chargeable event. The CDRs generated by GGSN/SGSN are sent to an external node for storage. CDRs are written to files in formats supported by the external node and stored on the HDD. From the HDD, CDR files can be pushed/pulled using FTP/SFTP protocols.

For information on how to configure push functionality, refer to the section in this chapter.

Directory Structure: By default, the CDRs are placed in the following directory paths:

- RAM-disk: */records/cdr/<gtpp_group_name>+<vpn_id>/*
- HDD: */hd-raid/data/records/cdr/<gtpp_group_name>+<vpn_id>/*

File Formats: The GSS file formats, Custom1 to Custom8 are supported.

Supported Products: GGSN, SGSN, P-GW, S-GW

Event Data Records (EDR)

The Event Data Records are responsible for definition, generation, and offloading of EDRs generated in the system (as a result of occurrence of an event) to the external billing system. EDRs are basically used for content billing purposes, wherein it is required that a different charging unit be employed for different types of content e.g. HTTP, SMTP, MMS,

etc. EDRs are a type of usage records that are configurable by the operator. EDRs are generated per flow subject to available configuration.

Directory Structure: By default, the EDRs are placed in the following directory paths:

- RAM-disk: */records/edr/*
- HDD: */hd-raid/data/records/edr/*

File Formats: In this release, EDRs are supported in the Comma Separated Values (CSV) format.

Supported Products: ECS and other products/features using ECS

Event Records

The Event reporting is a mechanism using which subscriber activities like session creation/deletion, bearer creation/modification/update/deletion are reported to the external server (RTT server). The event report logs assist network operators in maintaining and troubleshooting the network. The event records are stored as files in the HDD and these files are later SFTPd to the external RTT server. To store the event records in the form of files, compress the event record file using the Call Detail Records Module (CDRMOD) which provides support for collecting, storing, and compressing the event records.

Important: Event Records are supported in 12.2 and later releases.

Directory Structure: By default, the Event records are placed in the following directory paths:

- RAM-disk: */records/event/*
- HDD: */hd-raid/data/records/event/*

File Formats: In this release, Event Records are supported in the Comma Separated Values (CSV) format.

Supported Products: SGSN, S-GW

Reporting Event Data Records (REDR)

Reporting Event Data Records are a type of CDRs that contain EDRs generated on flow end conditions, that is reporting flow end EDRs and HTTP transaction EDRs. REDR records are written to files in formats supported by the external node and stored in the HDD. From the HDD, REDR records can be pushed/pulled using FTP/SFTP protocols.

Important: REDRs are supported in 12.2 and later releases.

Directory Structure: By default, the REDRs are placed in the following directory paths:

- RAM-disk: */records/redr/*
- HDD: */hd-raid/data/records/redr/*

File Formats: In this release, REDRs are supported in the Comma Separated Values (CSV) format.

Supported Products: ECS and other products/features using ECS

Usage Data Records (UDR)

The Usage Data Records contain accounting information related to a specific mobile subscriber. UDRs are generated and stored on the system as records in CSV format (comma separated values). The CDR subsystem in conjunction with

the External Storage Server (ESS) are responsible for offloading of UDRs. UDRs are generated per content type. The fields required as part of usage data records are configurable and stored in the System Configuration Task (SCT). UDRs are generated at the end of a call, i.e. call termination, time threshold, volume threshold, and handoffs.

Directory Structure: By default, the UDRs are placed in the following directory paths:

- RAM-disk: */records/udr/*
- HDD: */hd-raid/data/records/udr/*

File Formats: In this release, UDRs are supported in the Comma Separated Values (CSV) format.

Supported Products: GGSN, HA, PDSN

Hardware Overview

This section provides information on the hardware components that comprise the HDD feature in the ASR 5x00.

The HDD functionality takes advantage of the Hard Disk available in the System Management Card (SMC) of the ASR 5x00. The System Management Card (SMC) serves as the primary controller and is responsible for initializing the entire system, and loading the software's configuration image into other cards in the chassis as applicable. SMCs are installed in the chassis slots 8 and 9. During normal operation, the SMC in slot 8 serves as the primary (Active), while the SMC in slot 9 serves as the secondary (Standby).

Each SMC contains an enterprise-class Serial Attached SCSI (SAS) hard disk to load and store configuration data, software updates, buffer accounting information, and store diagnostic or troubleshooting information. Space for CDR storage in the internal Hard Disk is 100 Gigabytes (GB). Redundant control mechanisms allow for data to be written to the hard disks on both the active and standby SMCs.

Important: No hardware changes (PSC, SMC, chassis, etc.) are required to enable the CDR Storage and Retransmission. However, an appropriate software version has to be loaded in the ASR 5x00.

How HDD Works

This section describes the working of the HDD functionality.

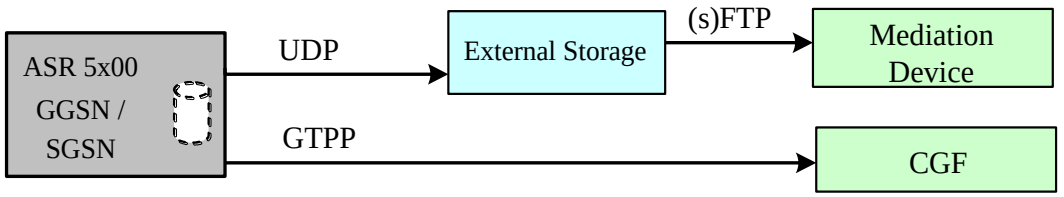
The functionality for CDR Storage and Retransmission works without requiring an external storage. In normal operating mode, when CGF is up and reachable, the ASR 5x00 streams CDRs to the CGF. If the CGF becomes unreachable, the ASR 5x00 starts temporarily storing CDRs into the internal hard disk. Once the CGF is up again, the ASR 5x00 streams those records stored in its hard disk to the external CGF via GTP protocol. This is called the **streaming** mode of operation.

When CDR Internal Storage and Retransmission is configured, the ASR 5x00 continuously checks for reachability of configured CGFs. When there is no reply to Echo Requests or responses to signaling messages from the CGF, the ASR 5x00 assumes that the CGF is down and starts storing the CDRs into its internal hard disk.

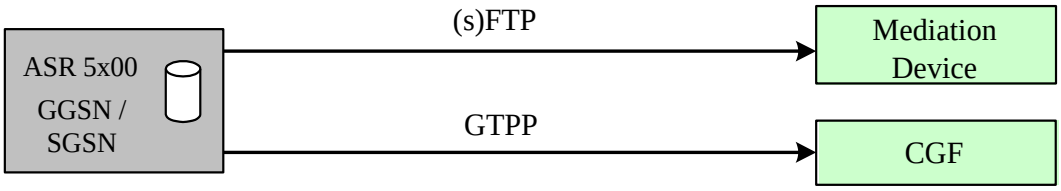
Important: Only one CGF server per GTPP group is supported.

This function in the ASR 5x00 incorporates partial external storage functionality inside the ASR 5x00 gateway. The following diagram depicts the mechanism using external storage (no hard disk configured in the ASR 5x00) and using the hard disk.

Figure 9. HDD Mechanism



Before hard disk support or with hard disk disabled



With hard disk support enabled

The following example shows the amount of time that CDRs can be stored in the internal hard disk and the coverage in case CGF is down. Assuming a CDR size of 350 bytes, approximately 285 million CDRs can be stored in 100 GB of hard disk. Based on information from deployed systems, a peak rate of 4M (million) records/hour provides 2.9 days of storage. This means that assuming 2M sessions per gateway (say GGSN) at peak busy hour, and each session generates approximately 2 GCDRs per hour, 4 million CDRs/hour represents the worst case scenario for the Busy Hour. Assuming an average 75% of that busy hour, 0.75 X 96M CDR = 72M CDR per day; for 350 bytes per CDR, it yields approximately 4 days of storage.

Deployment Scenarios

The HDD functionality is enabled in the ASR 5x00 gateway in the following deployment scenarios:

- **CGF configured but not reachable:** The ASR 5x00 attempts to stream the CDRs to the configured CGF. If the CGF does not respond to queries from ASR 5x00 or GTP messages, CDRs are stored in the internal HDD for future retransmission when CGF becomes reachable again
- **CGF configured and active, then goes down:** The ASR 5x00 was sending CDRs to CGF (via GTPP) normally. Upon loss of reachability of the CGF, the ASR 5x00 determines that CGF is down and starts storing CDRs in its internal HDD.
- **CGF configured, goes down and later becomes available:** CDRs were sent (streamed) to CGF until it becomes unreachable. After ASR 5x00 determines CGF is down/unreachable, it starts storing CDRs in internal HDD. When CGF becomes available again, CDRs are streamed to CGF, starting from the older CDR first.

HDD Configuration

This section describes how to configure the HDD.

This section covers the following topics:

- Configuring HDD
- Configuring EDRUDR Parameters

Configuring HDD

This section describes how to configure the HDD feature.

Important: This feature is disabled by default in the ASR 5x00.

In GTPP group mode, an option is added to enable this functionality with local-fallback option to existing **gtpp storage-server mode** in the ASR 5x00:

```
default gtpp storage-server mode { local | remote | streaming }
```

Notes:

- **default**: Returns the GTPP group configuration to the default 'remote' value (the ASR 5x00 streams CDRs to the configured external CGF) for the GTPP.
- If **remote** is configured, the ASR 5x00 sends CDRs to the external CGF. In case CGF is down or unreachable, CDRs will be lost.
- If **local** is configured, records are stored in the ASR 5x00's internal hard disk. Mediation / billing system can retrieve the records through Secure FTP (SFTP).
- If **streaming** is configured, then the CDRs are sent to CGF by default. If the CGF is down or unreachable, CDRs are temporarily stored in the internal hard disk and streamed to CGF once it becomes available.

Configuring EDR/UDR Parameters

This section provides an example configuration to configure EDR/UDR file transfer and file properties parameters, including configuring hard disk support on SMC card on ASR 5x00, transfer modes, transfer interval, etc.

To configure EDR/UDR file parameters:

```
configure

   context <context_name>

      edr-module active-charging-service

         cdr { push-interval push_interval | push-trigger space-usage-percent
trigger_percentage | remove-file-after-transfer | transfer-mode { pull | push primary {
encrypted-url encrypted_url | url url } [ [ secondary { encrypted-secondary-url
```

```
encrypted_secondary_url | secondary-url secondary_url } ] [ via local-context ] + ] |
use-harddisk }

         file [ charging-service-name { include | omit } ] [ compression { gzip | none }
] [ current-prefix string ] [ delete-timeout seconds ] [ directory directory_name ] [
edr-format-name ] [ exclude-checksum-record ] [ field-separator { hyphen | omit |
underscore } ] [ file-sequence-number rulebase-seq-num ] [ headers ] [ name file_name ] [
reset-indicator ] [ rotation [ num-records number | time seconds | volume bytes ] ] [
sequence-number { length length | omit | padded | padded-six-length | unpadded } ] [
storage-limit limit ] [ single-edr-format ] [ time-stamp { expanded-format | rotated-
format | unix-format } ] [ trailing-text string ] [ trap-on-file-delete ] [ xor-final-
record ] +

         exit

      udr-module active-charging-service

         cdr { push-interval push_interval | push-trigger space-usage-percent
trigger_percentage | remove-file-after-transfer | transfer-mode { pull | push primary {
encrypted-url encrypted_url | url url } [ [ secondary { encrypted-secondary-url
encrypted_secondary_url | secondary-url secondary_url } ] [ via local-context ] + ] |
use-harddisk }

         file [ charging-service-name { include | omit } ] [ compression { gzip | none }
] [ current-prefix string ] [ delete-timeout seconds ] [ directory directory_name ] [
exclude-checksum-record ] [ field-separator { hyphen | omit | underscore } ] [ file-
sequence-number rulebase-seq-num ] [ headers ] [ name file_name ] [ reset-indicator ] [
rotation [ num-records number | time seconds | volume bytes ] ] [ sequence-number {
length length | omit | padded | padded-six-length | unpadded } ] [ storage-limit limit ]
[ time-stamp { expanded-format | rotated-format | unix-format } ] [ trailing-text string
] [ trap-on-file-delete ] [ udr-seq-num ] [ xor-final-record ] +

         end
```

Notes:

- The **cdr** command can be configured either in the EDR or the UDR Configuration Mode. Configuring in one mode prevents the configurations from being applied in the other mode.
- The **use-harddisk** keyword is only available on the ASR 5x00.
- The **push** keyword is used to send the EDR/UDR files to the configured L-ESS or any other external server.

For more information on this command, refer to the *Command Line Interface Reference*.

Viewing Statistics

To view EDR-UDR file statistics, in the Exec Mode, enter the following command:

show cdr statistics

Pushing EDR/UDR Files Manually

To manually push EDR/UDR files to the configured L-ESS, in the Exec mode, use the following command:

cdr-push { all | local-filename *file_name* **}**

Notes:

- Before you can use this command, the EDR/UDR transfer mode and file locations must be set to push in the EDR/UDR Module Configuration Mode.
- The **cdr-push** command is available in the Exec Mode.
- *file_name* must be absolute path of the local file to push.

Retrieving EDR and UDR Files

To retrieve UDR or EDR files you must SFTP into the context that was configured for EDR or UDR file generation.

This was done with the FTP-enabled account that you configured in the *Enabling Charging Record Retrieval* section.

The following commands use SFTP to log on to a context named **ECP** as a user named **ecpadmin**, through an interface configured in the ECS context that has the IP address *192.168.1.10* and retrieve all EDR or UDR files from the default locations:

sftp -oUser=ecpadmin@ECP *192.168.1.10***:/records/edr/***

sftp -oUser=ecpadmin@ECP *192.168.1.10***:/records/udr/***

Appendix A
AAA Engineering Rules

This section provides AAA engineering rules and guidelines that must be considered prior to configuring the system for AAA functionality.

AAA Interface Rules

The following engineering rules apply to the AAA interface including RADIUS and Diameter:

- AAA interfaces are specified by assigning the IP address of a logical interface within a specific context as the RADIUS NAS IP Address (RFC-2865 and RFC-2866) within the same context. This is done using the **radius attribute nas-ip-address** command in the context configuration mode.
- AAA interfaces in support of data services can be configured within any context.

  Typically it exists in the:

  - Ingress context for PDSN and ASNGW services
  - Egress context for GGSN services
- A AAA interface is selected in the following order:
  - NAI-based selection
  - Default AAA context
  - Last-resort AAA context
  - If all else fails defaults to the Ingress Context
- AAA servers can be configured with “primary” and “backup” servers for any context.
- Authentication and Accounting servers can be configured individually per context.
- Multiple AAA contexts can be configured to support different accounting and authentication servers based on the domain where that the subscriber belongs.
- AAA server group provides AAA functionality to the each subscriber separately with in the same context.
- AAA server group for AAA functionality can be configured with following limits:
  - A total of 800 AAA server groups (including “default” server group) are available per context or system.
  - A maximum number of authentication/accounting servers per AAA server group is 128.
  - A maximum of 1600 servers can be configured in a context or a system, regardless of the number of server groups, with any combination for authentication and/or accounting.
  - A maximum of 800 NAS-IP addresses/NAS identifier (1 primary and 1 secondary per server group) can be configured per context.

Appendix B
RADIUS Server State Behavior

This appendix provides an explanation of RADIUS server states and the commands that affect them. It also provides a list of triggers that change servers in a “Down” state to “Active”.

Understanding RADIUS Server States and Commands

Server States

The system defines three server states for connected RADIUS servers:

- **Active**: The server is believed to be operational.
- **Not Responding**: The server has failed to respond to a message from the system a configured number of times (retries).
- **Down**: The system is no longer sending requests to the server.

RADIUS Server Commands

RADIUS server states are controlled by parameters set in the RADIUS Server Group Configuration Mode. The commands are:

- **`detect-dead-server`**: Configures how the system determines that a RADIUS server is not functioning. One or both of the following parameters should be set:
  - **`consecutive-failures`**: Configures the consecutive number of times the RADIUS server is unreachable by any single aaamgr on the system based on the **`max-retries`** command. If this command is enabled, each time the maximum number of retries is exceeded, this counter increments by one for the particular aaamgr and server. When any aaamgr exceeds this counter for a specific RADIUS server, the server's state is changed to "Down" and the deadtime timer is started. The default is enabled and 4.
  - **`response-timeout`**: Configures a specific delay, in seconds, in receiving a response from the RADIUS server before the server's state is changed to "Down" and the deadtime timer is started. The default is disabled.

    Important: If **`response-timeout`** is configured and **`consecutive-failures`** is not, the system will only wait for the specified period of time before changing the server's state to "Down", ignoring other settings such as **`radius timeout`**, and **`max-retries`**.

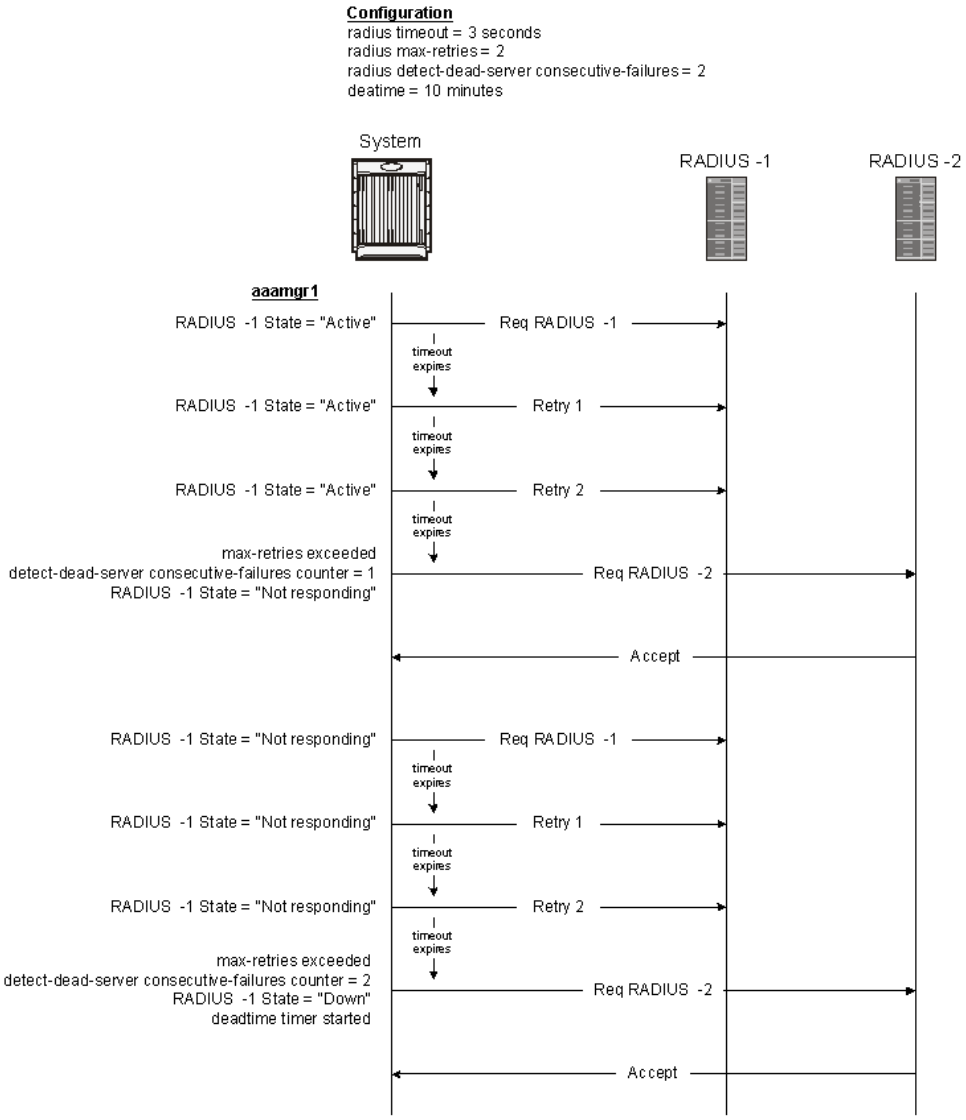
    If **`response-timeout`** is configured and **`consecutive-failures`** is not, **`consecutive-failures`** is removed entirely from the system, including default configuration. If both parameters are configured, then both conditions must be met to change a RADIUS server's state to "Down".
- **`deadtime`**: Configure the maximum amount of time, in minutes, that must elapse after a context has exceeded one or both of the **`detect-dead-server`** parameters, depending on which parameter is configured. Once this timer has elapsed, the system reclassifies the RADIUS server as "Active" and subsequent requests to it can be made. If **`radius deadtime`** is not explicitly configured, the default value of 10 minutes is used.
- **`max-retries`**: Configures maximum number of times the system attempts to retry communication with a RADIUS server. Once exceeded, the system changes the state of the server to "Not Responding", increments the **`detect-dead-server consecutive-failures`** counter (if configured), and attempts to communicate with another RADIUS server. The default value for this parameter is 5.

- **`max-transmissions`**: Configures the maximum number of times the system transmits authentication requests to a server before it fails the authentication due to lack of response. The absolute maximum number of transmissions is equal to NS * (N + 1), where NS is the number of configured authentication servers, and N is the setting for **`radius max-retries`**. The default for this command is disabled.
- **`timeout`**: Specifies how many seconds the system waits for a response from a RADIUS server before re-transmitting the request.

More information regarding each command can be found in the *Command Line Interface Reference*.

The following figure shows a simple flow of events and how the system reacts based on configured parameters.

Figure 10. Sample RADIUS Communication Flow



Server State Triggers

A number of triggers, events, and conditions can occur that change the state of a RADIUS server from "Down" to "Active" as defined by the system. They are:

- When the timer, based on the RADIUS Server Group Configuration Mode command: **deadtime** has expired, the server's state on the system is returned to "Active".

  Important: This parameter should be set to allow enough time to solve the issue that originally caused the server's state to be changed to "Down". After the deadtime timer expires, the system returns the server's state to "Active" regardless of whether or not the issue has been fixed.

- When a RADIUS authentication server is configured, the server state is initialized as "Active".
- When a RADIUS accounting server is configured and after receiving response for Acct-On message, the server state is made "Active".
- When a RADIUS accounting server is configured and after the Acct-On message exceeds the max retries setting and times-out, the server state is made "Active".
- When a RADIUS accounting server is configured with Acct-On disabled, the server state is made "Active".
- When a response from a RADIUS server is received, the server state is made "Active".
- When a RADIUS server responds to the Exec Mode command **radius test**, the server state is made "Active".
- When a RADIUS probe is enabled and the probe response is received, the server state is made "Active".
- When a RADIUS probe request times-out after max retries, the server state is made "Active".
- If only one RADIUS authentication server is "Active" and goes down, all RADIUS authentication servers are made "Active".
- If only one RADIUS accounting server is "Active" and goes down, all RADIUS accounting servers are made "Active".

  Important: The system uses the above triggers to mark RADIUS servers as "Active", however, this does not necessarily mean that the actual server is functional. When the system changes a server state, a trap is automatically sent to the management station. Action should be taken to identify the cause of the failure.

Appendix C
Switching CDRs

This appendix describes the following procedures:

- Switching CDRs from HDD to GSS
- Switching CDRs from GSS to HDD

Switching CDRs from HDD to GSS

This section describes how to switch CDRs from HDD to GSS with:

- LRSN Enabled
- LRSN Disabled

LRSN Enabled

To switch CDRs from HDD to GSS with LRSN enabled:

Important: This configuration change must be undertaken in a maintenance window, when the load is minimum.

Step 1 Configure the GSS server, and ensure that GSS and GGSN have no connectivity issues.

- If configuring to the *default* GTPP group:

```
configure
   gtpp single-source centralized-lrsn-creation
   context <billing>
      gtpp charging-agent address <address>
      gtpp storage-server <address> port <port>
      gtpp max-cdrs  255 wait-time 300
      end
show configuration | grep gtpp
```

- If configuring to a specific GTPP group:

```
configure
   gtpp single-source centralized-lrsn-creation
   context <billing>
      gtpp group <gtpp_group>
         gtpp charging-agent address <address>
         gtpp storage-server <address> port <port>
         gtpp max-cdrs 255 wait-time 300
         end
```

```
show configuration | grep gtpp
```

Step 2 Change the GTPP storage server mode to "Remote".

- If configuring to the *default* GTPP group:

```
configure
   context <billing>
      gtpp storage-server mode remote
      gtpp max-cdrs 255 wait-time 300
      end
show configuration | grep gtpp
```

- If configuring to a specific GTPP group:

```
configure
   context <billing>
      gtpp group <gtpp_group>
         gtpp storage-server mode remote
         gtpp max-cdrs 255 wait-time  300
         end
show configuration | grep gtpp
```

Important: Ensure that the file format, GTPP dictionary and LRSN Enabled are set properly on GSS in the *gss.cfg* file. Also, the correct version of GSS has to be installed and started on the Solaris machine.

Step 3 Check and confirm that new CDRs are being written to files by GSS.

On the HDD side, remaining CDRs are immediately flushed to a CDR file. At this point, the transition is complete.

LRSN Disabled

To switch CDRs from HDD to GSS with LRSN disabled:

Important: This configuration change must be undertaken in a maintenance window, when the load is minimum.

Step 1 Configure the GSS server, and ensure that GSS and GGSN have no connectivity issues.

- If configuring to the *default* GTPP group:

```
configure
   context <billing>
```

```
gtpp charging-agent address <address>
gtpp storage-server <address> port <port>
gtpp max-cdrs 255 wait-time  300
end
show configuration | grep gtpp
```

- If configuring to a specific GTPP group:

```
configure
   context <billing>
      gtpp group <gtpp_group>
      gtpp charging-agent address <address>
      gtpp storage-server <address> port <port>
      gtpp max-cdrs 255 wait-time  300
      end
show configuration | grep gtpp
```

Step 2 Change the GTPP storage server mode to “Remote”.

- If configuring to the *default* GTPP group:

```
configure
   context <billing>
      gtpp storage-server mode remote
      gtpp max-cdrs 255 wait-time  300
      end
show configuration | grep gtpp
```

- If configuring to a specific GTPP group:

```
configure
   context <billing>
      gtpp group <gtpp_group>
      gtpp storage-server mode remote
      gtpp max-cdrs 255 wait-time  300
      end
```

```
show configuration | grep gtpp
```

Step 3 Check and confirm that new CDRs are being written to files by GSS.

On the HDD side, remaining CDRs are immediately flushed to a CDR file. At this point, the transition is complete.

Important: Ensure that the file format, GTPP dictionary and LRSN Disabled are set properly on GSS in the *gss.cfg* file. Also, the correct version of GSS has to be installed and started on the Solaris machine.

Switching CDRs from GSS to HDD

This section describes how to switch CDRs from GSS to HDD with:

- LRSN Enabled
- LRSN Disabled

LRSN Enabled

To switch CDRs from GSS to HDD with LRSN enabled:

Important: This configuration change must be undertaken in a maintenance window, when the load is minimum.

Step 1 Ensure that GSS is up and running, and that GGSN is able to deliver CDRs to GSS.

Start the changes from a known good state.

Step 2 Add the HDD configuration.

- If configuring to the *default* GTPP group:

```
configure

   gtpp single-source centralized-lrsn-creation

   context <billing>

      gtpp storage-server local file format <file_format_as_in_gss.cfg>

      gtpp storage-server local file rotation volume mb 40

      gtpp storage-server local file rotation cdr-count
<max_CDR_per_file_as_in_gss.cfg>

      gtpp storage-server local file rotation time-interval
<max_file_gen_period_as_in_gss.cfg>

      gtpp dictionary <gtpp_dict_as_in_gss.cfg>

      gtpp storage-server mode local

      end

show configuration | grep gtpp
```

Important: Note that **gtpp storage-server mode local** must be added at the end.

- If configuring to a specific GTPP group:

```
configure
```

```
gtpp single-source centralized-lrsn-creation

context <billing>

   gtpp storage-server local file format <file_format_as_in_gss.cfg>

   gtpp storage-server local file rotation volume mb 40

   gtpp storage-server local file rotation cdr-count
<max_CDR_per_file_as_in_gss.cfg>

   gtpp storage-server local file rotation time-interval
<max_file_gen_period_as_in_gss.cfg>

   gtpp dictionary <gtpp_dict_as_in_gss.cfg>

   gtpp storage-server mode local

   end

show configuration | grep gtpp
```

Important: Note that **gtpp storage-server mode local** must be added at the end.

Step 3 Ensure that GSS is still up and running so that already pending requests towards GSS are fully delivered. Without flushing out the existing pending requests to GSS, GGSN will not switch to HDD.

Step 4 Check and confirm that new CDRs are being written to HDD.

Step 5 On the GSS side, you must wait for the time period it takes for the hard file generation, so that remaining CDRs are flushed to CDR file.

Step 6 At this point, the transition is complete and you can bring the GSS offline.

LRSN Disabled

To switch CDRs from GSS to HDD with LRSN disabled:

Important: This configuration change must be undertaken in a maintenance window, when the load is minimum.

Step 1 Ensure that GSS is up and running and GGSN is able to deliver CDRs to GSS.

Start the changes from a known good state.

Step 2 Add the HDD configuration.

- If configuring to the *default* GTPP group:

```
configure

   context <billing>

      gtpp storage-server local file format <file_format_as_in_gss.cfg>
```

```
      gtpp storage-server local file rotation volume mb 40

      gtpp storage-server local file rotation cdr-count
<max_CDR_per_file_as_in_gss.cfg>

      gtpp storage-server local file rotation time-interval
<max_file_gen_period_as_in_gss.cfg>

      gtpp dictionary <gtpp_dict_as_in_gss.cfg>

      gtpp storage-server mode local

      end

show configuration | grep gtpp
```

Important: Note that **gtpp storage-server mode local** must be added at the end.

- If configuring to a specific GTPP group:

```
configure

   context <billing>

      gtpp group <gtpp_group>

      gtpp storage-server local file format <file_format_as_in_gss.cfg>

      gtpp storage-server local file rotation volume mb 40

      gtpp storage-server local file rotation cdr-count
<max_CDR_per_file_as_in_gss.cfg>

      gtpp storage-server local file rotation time-interval
<max_file_gen_period_as_in_gss.cfg>

      gtpp dictionary <gtpp_dict_as_in_gss.cfg>

      gtpp storage-server mode local

      end

show configuration | grep gtpp
```

Important: Note that **gtpp storage-server mode local** must be added at the end.

Step 3 Ensure that GSS is still up and running so that already pending requests towards GSS is fully delivered. Without flushing out the existing pending requests to GSS, GGSN will not switch to HDD.

Step 4 Check and confirm that new CDRs are being written to HDD.

Step 5 On the GSS side, you must wait for the time period it takes for the hard file generation, so that remaining CDRs are flushed to CDR file.

Step 6 At this point, the transition is complete and you can bring the GSS offline.

Appendix D
Diameter Attribute Quick Reference

This appendix presents Diameter attribute quick reference tables.

The following table describes the indicators used in the quick reference tables.

Indicator	Description
0	The AVP MUST NOT be present in the message.
0+	Zero or more instances of the AVP MAY be present in the message.
0-1	Zero or one instance of the AVP MAY be present in the message. If there are more than one instance of the AVP, it is considered an error.
1	One instance of the AVP MUST be present in the message.
1+	At least one instance of the AVP MUST be present in the message.

The following table describes the column headers in the quick reference tables.

Term	Expansion	Term	Expansion
ACA	AC-Answer	MEICR	ME-Identity-Check-Request
ACR	AC-Request	MAA	Multimedia-Auth-Answer
ASA	Abort-Session-Answer	MAR	Multimedia-Auth-Request
ASR	Abort-Session-Request	NA	Notify-Answer
AIA	Authentication-Information-Answer	NR	Notify-Request
AIR	Authentication-Information-Request	PUA	Profile-Update-Answer
AAA	Authorization-Authentication-Answer	PUR	Profile-Update-Request
AAR	Authorization-Authentication-Request	PUAM	Purge-UE-Answer-MME
CLA	Cancel-Location-Answer	PURM	Purge-UE-Request-MME
CLR	Cancel-Location-Request	PPA	Push-Profile-Answer
CEA	Capabilities-Exchange-Answer	PPR	Push-Profile-Request
CER	Capabilities-Exchange-Request	RAA	Re-Auth-Answer
CCA	Credit-Control-Answer	RAR	Re-Auth-Request
CCR	Credit-Control-Request	RTA	Registration-Termination-Answer
DSDA	Delete-Subscriber-Data-Answer	RTR	Registration-Termination-Request
DSDR	Delete-Subscriber-Data-Request	RA	Reset-Answer
DWA	Device-Watchdog-Answer	RR	Reset-Request
DWR	Device-Watchdog-Request	SAA	Server-Assignment-Answer

Term	Expansion	Term	Expansion
DEA	Diameter-EAP-Answer	SAR	Server-Assignment-Request
DER	Diameter-EAP-Request	STA	Session-Termination-Answer
DPA	Disconnect-Peer-Answer	STR	Session-Termination-Request
DPR	Disconnect-Peer-Request	ULA	Update-Location-Answer
ISDA	Insert-Subscriber-Data-Answer	ULR	Update-Location-Request
ISDR	Insert-Subscriber-Data-Request	UAA	User-Authorization-Answer
LIA	Location-Info-Answer	UAR	User-Authorization-Request
LIR	Location-Info-Request	UDA	User-Data-Answer
MEICA	ME-Identity-Check-Answer	UDR	User-Data-Request

Standard 3GPP Gy (32.299) Dictionary

Attribute	AVP Code	Vendor-Id	AVP Type	M Flag	P Flag	ASA	ASR	CCA	CCR	RAA	RAR
3GPP2-BSID	9010	5535	OCTETSTRING	1	0	0	0	0-1	0-1	0	0
3GPP-Charging-Characteristics	13	10415	UTF8STRING	1	0	0	0	0-1	0-1	0	0
3GPP-Charging-Id	2	10415	UINT32	1	0	0	0	0-1	0-1	0	0
3GPP-GGSN-MCC-MNC	9	10415	UTF8STRING	1	0	0	0	0-1	0-1	0	0
3GPP-GPRS-QoS-Negotiated-Profile	5	10415	UTF8STRING	1	0	0	0	0-1	0-1	0	0
3GPP-IMSI-MCC-MNC	8	10415	UTF8STRING	1	0	0	0	0-1	0-1	0	0
3GPP-MS-TimeZone	23	10415	OCTETSTRING	1	0	0	0	0-1	0-1	0	0
3GPP-NSAPI	10	10415	UTF8STRING	1	0	0	0	0-1	0-1	0	0
3GPP-PDP-Type	3	10415	ENUM	1	0	0	0	0-1	0-1	0	0
3GPP-Quota-Consumption-Time	881	10415	UINT32	1	0	0	0	0-1	0-1	0	0
3GPP-Quota-Holding-Time	871	10415	UINT32	1	0	0	0	0-1	0-1	0	0
3GPP-RAT-Type	21	10415	OCTETSTRING	1	0	0	0	0-1	0-1	0	0
3GPP-Reporting-Reason	872	10415	ENUM	1	0	0	0	0+	0+	0	0
3GPP-Selection-Mode	12	10415	UTF8STRING	1	0	0	0	0-1	0-1	0	0
3GPP-Session-Stop-Indicator	11	10415	OCTETSTRING	1	0	0	0	0-1	0-1	0	0
3GPP-SGSN-MCC-MNC	18	10415	UTF8STRING	1	0	0	0	0-1	0-1	0	0
3GPP-Time-Quota-Threshold	868	10415	UINT32	1	0	0	0	0-1	0-1	0	0
3GPP-Unit-Quota-Threshold	1226	10415	UINT32	1	0	0	0	0-1	0-1	0	0
3GPP-User-Location-Info	22	10415	UTF8STRING	1	0	0	0	0-1	0-1	0	0
3GPP-Volume-Quota-Threshold	869	10415	UINT32	1	0	0	0	0-1	0-1	0	0
AF-Correlation-Information	1276	10415	GROUPED	1	0	0	0	0+	0+	0	0
Auth-Application-Id	258	0	UINT32	1	0	0	1	1	1	0	1
Called-Station-Id	30	0	OCTETSTRING	1	0	0	0	0-1	0-1	0	0
CC-Input-Octets	412	0	UINT64	1	0	0	0	0-1	0-1	0	0
CC-Output-Octets	414	0	UINT64	1	0	0	0	0-1	0-1	0	0
CC-Request-Number	415	0	UINT32	1	0	0	0	1	1	0	0
CC-Request-Type	416	0	ENUM	1	0	0	0	1	1	0	0
CC-Service-Specific-Units	417	0	UINT64	1	0	0	0	0-1	0-1	0	0
CC-Session-Failover	418	0	ENUM	1	0	0	0	0-1	0	0	0
CC-Time	420	0	UINT32	1	0	0	0	0-1	0-1	0	0
CC-Total-Octets	421	0	UINT64	1	0	0	0	0-1	0-1	0	0
CG-Address	846	10415	ADDRESS	1	0	0	0	0-1	0-1	0	0
Charging-Rule-Base-Name	1004	10415	UTF8STRING	1	0	0	0	0-1	0-1	0	0
Cost-Information	423	0	GROUPED	1	0	0	0	0-1	0	0	0
Credit-Control-Failure-Handling	427	0	ENUM	1	0	0	0	0-1	0	0	0
Destination-Host	293	0	DIAMIDENT	1	0	0	0-1	0	0-1	0	0-1

Attribute	AVP Code	Vendor-Id	AVP Type	M Flag	P Flag	ASA	ASR	CCA	CCR	RAA	RAR
Destination-Realm	283	0	DIAMIDENT	1	0	0	1	0	1	0	1
Direct-Debiting-Failure-Handling	428	0	ENUM	1	0	0	0	0-1	0	0	0
Dynamic-Address-Flag	2051	10415	ENUM	1	0	0	0	0-1	0-1	0	0
Envelope	1266	10415	GROUPED	1	0	0	0	0+	0+	0	0
Envelope-End-Time	1267	10415	TIME	1	0	0	0	0-1	0-1	0	0
Envelope-Reporting	1268	10415	ENUM	1	0	0	0	0-1	0-1	0	0
Envelope-Start-Time	1269	10415	TIME	1	0	0	0	1	1	0	0
Error-Message	281	0	UTF8STRING	0	0	0	0	0	0	0-1	0
Event-Timestamp	55	0	TIME	1	0	0	0	0	0-1	0	0
Failed-AVP	279	0	GROUPED	1	0	0+	0	0+	0	0+	0
Final-Unit-Indication	430	0	GROUPED	1	0	0	0	0-1	0-1	0	0
GGSN-Address	847	10415	ADDRESS	1	0	0	0	0-1	0-1	0	0
Granted-Service-Unit	431	0	GROUPED	1	0	0	0	0-1	0-1	0	0
G-S-U-Pool-Reference	457	0	GROUPED	1	0	0	0	0+	0+	0	0
Multiple-Services-Credit-Control	456	0	GROUPED	1	0	0	0	0+	0+	0	0
Multiple-Services-Indicator	455	0	ENUM	1	0	0	0	0	0-1	0	0
Offline-Charging	1278	10415	GROUPED	1	0	0	0	0-1	0-1	0	0
Origin-Host	264	0	DIAMIDENT	1	0	1	1	1	1	1	1
Origin-Realm	296	0	DIAMIDENT	1	0	1	1	1	1	1	1
Origin-State-Id	278	0	UINT32	1	0	0	0	0	0-1	0	0
PDN-Connection-ID	2050	10415	UINT32	1	0	0	0	0-1	0-1	0	0
PDP-Address	1227	10415	ADDRESS	1	0	0	0	0+	0+	0	0
PDP-Context-Type	1247	10415	ENUM	1	0	0	0	0-1	0-1	0	0
Proxy-Info	284	0	GROUPED	1	0	0	0	0+	0+	0	0
PS-Furnish-Charging-Information	865	10415	GROUPED	1	0	0	0	0-1	0-1	0	0
PS-Information	874	10415	GROUPED	1	0	0	0	0-1	0-1	0	0
QoS-Information	1016	10415	GROUPED	1	0	0	0	0-1	0-1	0	0
Rating-Group	432	0	UINT32	1	0	0	0	0-1	0-1	0	0-1
Re-Auth-Request-Type	285	0	ENUM	1	0	0	0	0	0	0	1
Redirect-Host	292	0	OCTETSTRING	1	0	0	0	0+	0	0	0
Redirect-Host-Usage	261	0	ENUM	1	0	0	0	0-1	0	0	0
Redirect-Max-Cache-Time	262	0	UINT32	1	0	0	0	0-1	0	0	0
Requested-Action	436	0	ENUM	1	0	0	0	0	0-1	0	0
Requested-Service-Unit	437	0	GROUPED	1	0	0	0	0-1	0-1	0	0
Result-Code	268	0	ENUM	1	0	1	0	1	0-1	1	0
Route-Record	282	0	DIAMIDENT	1	0	0	0	0+	0+	0	0
Service-Context-Id	461	0	UTF8STRING	1	0	0	0	0	1	0	0
Service-Identifier	439	0	UINT32	1	0	0	0	0+	0+	0	0-1
Service-Information	873	10415	GROUPED	1	0	0	0	0-1	0-1	0	0

Attribute	AVP Code	Vendor-Id	AVP Type	M Flag	P Flag	ASA	ASR	CCA	CCR	RAA	RAR
Serving-Node-Type	2047	10415	ENUM	1	0	0	0	0-1	0-1	0	0
Session-Id	263	0	UTF8STRING	1	0	1	1	1	1	1	1
SGSN-Address	1228	10415	ADDRESS	1	0	0	0	0-1	0-1	0	0
Start-Time	2041	10415	TIME	1	0	0	0	0-1	0-1	0	0
Stop-Time	2042	10415	TIME	1	0	0	0	0-1	0-1	0	0
Subscription-Id	443	0	GROUPED	1	0	0	0	0	0+	0	0
Tariff-Time-Change	451	0	TIME	1	0	0	0	0-1	0-1	0	0
Terminal-Information	6002	10415	GROUPED	1	0	0	0	0-1	0-1	0	0
Termination-Cause	295	0	ENUM	1	0	0	0	0	0-1	0	0
Time-Quota-Mechanism	1270	10415	GROUPED	1	0	0	0	0-1	0-1	0	0
Trigger	1264	10415	GROUPED	1	0	0	0	0-1	0-1	0	0
Used-Service-Unit	446	0	GROUPED	1	0	0	0	0+	0+	0	0
User-Equipment-Info	458	0	GROUPED	1	0	0	0	0-1	0-1	0	0
User-Name	1	0	UTF8STRING	1	0	0-1	0-1	0	0-1	0-1	0-1
Validity-Time	448	0	UINT32	1	0	0	0	0-1	0-1	0	0

Standard Cx Dictionary

Attribute	AVP Code	Vendor-Id	AVP Type	M Flag	P Flag	LIA	LIR	MAA	MAR	PPA	PPR	RTA	RTR	SAA	SAR	UAA	UAR
3GPP-User-Data	606	10415	OCTETSTRING	1	0	0	0	0	0	0	0-1	0	0	0-1	0	0	0
Acct-Application-Id	259	0	UINT32	1	0	0-1	0-1	0-1	0-1	0-1	0-1	0-1	0-1	0-1	0-1	0-1	0-1
Associated-Identities	632	10415	GROUPED	0	0	0	0	0	0	0	0	0-1	0-1	0-1	0	0	0
Auth-Application-Id	258	0	UINT32	1	0	0-1	0-1	0-1	0-1	0-1	0-1	0-1	0-1	0-1	0-1	0-1	0-1
Auth-Session-State	277	0	ENUM	1	0	1	1	1	1	1	1	1	1	1	1	1	1
Charging-Information	618	10415	GROUPED	1	0	0	0	0	0	0	0-1	0	0	0-1	0	0	0
Confidentiality-Key	625	10415	OCTETSTRING	1	0	0	0	0-1	0-1	0	0	0	0	0	0	0	0
Deregistration-Reason	615	10415	GROUPED	1	0	0	0	0	0	0	0	0	1	0	0	0	0
Destination-Host	293	0	DIAMIDENT	1	0	0	0-1	0	0-1	0	1	0	1	0	0-1	0	0-1
Destination-Realm	283	0	DIAMIDENT	1	0	0	1	0	1	0	1	0	1	0	1	0	1
Experimental-Result	297	0	GROUPED	1	0	0-1	0	0-1	0	0-1	0	0-1	0	0-1	0	0-1	0
Experimental-Result-Code	298	0	ENUM	1	0	1	0	1	0	1	0	1	0	1	0	1	0
Failed-AVP	279	0	GROUPED	1	0	0+	0	0+	0	0+	0	0+	0	0+	0	0+	0
Feature-List	630	10415	UINT32	0	0	1	1	1	1	1	1	1	1	1	1	1	1
Feature-List-ID	629	10415	UINT32	0	0	1	1	1	1	1	1	1	1	1	1	1	1
Framed-Interface-Id	96	0	UINT64	1	0	0	0	0-1	0-1	0	0	0	0	0	0	0	0
Framed-IP-Address	8	0	OCTETSTRING	1	0	0	0	0-1	0-1	0	0	0	0	0	0	0	0
Framed-IPv6-Prefix	97	0	OCTETSTRING	1	0	0	0	0-1	0-1	0	0	0	0	0	0	0	0
Integrity-Key	626	10415	OCTETSTRING	1	0	0	0	0-1	0-1	0	0	0	0	0	0	0	0
Mandatory-Capability	604	10415	UINT32	1	0	0+	0	0	0	0	0	0	0	0	0	0+	0
Optional-Capability	605	10415	UINT32	1	0	0+	0	0	0	0	0	0	0	0	0	0+	0
Originating-Request	633	10415	ENUM	1	0	0	0-1	0	0	0	0	0	0	0	0	0	0
Origin-Host	264	0	DIAMIDENT	1	0	1	1	1	1	1	1	1	1	1	1	1	1
Origin-Realm	296	0	DIAMIDENT	1	0	1	1	1	1	1	1	1	1	1	1	1	1
Primary-Charging-Collection-Function-Name	621	10415	DIAMURI	1	0	0	0	0	0	0	0-1	0	0	0-1	0	0	0
Primary-Event-Charging-Function-Name	619	10415	DIAMURI	1	0	0	0	0	0	0	0-1	0	0	0-1	0	0	0
Proxy-Host	280	0	DIAMIDENT	1	0	1	1	1	1	1	1	1	1	1	1	1	1
Proxy-Info	284	0	GROUPED	1	0	0+	0+	0+	0+	0+	0+	0+	0+	0+	0+	0+	0+
Proxy-State	33	0	OCTETSTRING	1	0	1	1	1	1	1	1	1	1	1	1	1	1
Public-Identity	601	10415	UTF8STRING	1	0	0	1	0-1	1	0	0	0	0+	0	0+	0	1
Reason-Code	616	10415	ENUM	1	0	0	0	0	0	0	0	0	1	0	0	0	0
Reason-Info	617	10415	UTF8STRING	1	0	0	0	0	0	0	0	0	0-1	0	0	0	0
Redirect-Host	292	0	DIAMURI	1	0	0+	0	0+	0	0	0	0	0	0+	0	0+	0
Redirect-Host-Usage	261	0	ENUM	1	0	0-1	0	0-1	0	0	0	0	0	0-1	0	0-1	0
Result-Code	268	0	ENUM	1	0	0-1	0	0-1	0	0-1	0	0-1	0	0-1	0	0-1	0
Route-Record	282	0	DIAMIDENT	1	0	0+	0+	0+	0+	0+	0+	0+	0+	0+	0+	0+	0+
Secondary-Charging-Collection-Function-Name	622	10415	DIAMURI	1	0	0	0	0	0	0	0-1	0	0	0-1	0	0	0
Secondary-Event-Charging-Function-Name	620	10415	DIAMURI	1	0	0	0	0	0	0	0-1	0	0	0-1	0	0	0
Server-Assignment-Type	614	10415	ENUM	1	0	0	0	0	0	0	0	0	0	0	1	0	0
Server-Capabilities	603	10415	GROUPED	1	0	0-1	0	0	0	0	0	0	0	0	0	0-1	0
Server-Name	602	10415	UTF8STRING	1	0	0-1	0	0	1	0	0	0	0	0	1	0-1	0
Session-Id	263	0	UTF8STRING	1	0	1	1	1	1	1	1	1	1	1	1	1	1
SIP-Auth-Data-Item	612	10415	GROUPED	1	0	0	0	0+	0-1	0	0	0	0	0	0	0	0
SIP-Authenticate	609	10415	OCTETSTRING	1	0	0	0	0-1	0-1	0	0	0	0	0	0	0	0
SIP-Authentication-Context	611	10415	OCTETSTRING	1	0	0	0	0-1	0-1	0	0	0	0	0	0	0	0
SIP-Authentication-Scheme	608	10415	UTF8STRING	1	0	0	0	0-1	0-1	0	0	0	0	0	0	0	0
SIP-Authorization	610	10415	OCTETSTRING	1	0	0	0	0-1	0-1	0	0	0	0	0	0	0	0
SIP-Digest-Authenticate	635	10415	GROUPED	1	0	0	0	0-1	0-1	0	0	0	0	0	0	0	0
SIP-Item-Number	613	10415	UINT32	1	0	0	0	0-1	0-1	0	0	0	0	0	0	0	0
SIP-Number-Auth-Items	607	10415	UINT32	1	0	0	0	0-1	0-1	0	0	0	0	0	0	0	0

Attribute	AVP Code	Vendor-Id	AVP Type	M Flag	P Flag	LIA	LIR	MAA	MAR	PPA	PPR	RTA	RTR	SAA	SAR	UAA	UAR
Supported-Applications	631	10415	GROUPED	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Supported-Features	628	10415	GROUPED	1	0	0+	0+	0+	0+	0+	0+	0+	0+	0+	0+	0+	0+
UAR-Flags	637	10415	UINT32	0	0	0	0	0	0	0	0	0	0	0	0	0	0-1
User-Authorization-Type	623	10415	ENUM	1	0	0	0	0	0	0	0	0	0	0	0	0	0-1
User-Data-Already-Available	624	10415	ENUM	1	0	0	0	0	0	0	0	0	0	0	1	0	0
User-Name	1	0	UTF8STRING	1	0	0	0	0-1	1	0	1	0+	1	0-1	0-1	0	1
Vendor-Id	266	0	UINT32	1	0	1	1	1	1	1	1	1	1	1	1	1	1
Vendor-Specific-Application-Id	260	0	GROUPED	1	0	1	1	1	1	1	1	1	1	1	1	1	1
Visited-Network-Identifier	600	10415	OCTETSTRING	1	0	0	0	0	0	0	0	0	0	0	0	0	1
Wildcarded-PSI	634	10415	UTF8STRING	0	0	0-1	0	0	0	0	0	0	0	0	0-1	0	0

Standard Sh/HSS Dictionary

Attribute	AVP Code	Vendor-Id	AVP Type	M Flag	P Flag	PUA	PUR	PNA	PNR	SNA	SNR	UDA	UDR
Auth-Session-State	277	0	ENUM	1	0	1	1	1	1	1	1	1	1
Current-Location	707	10415	ENUM	1	0	0	0	0	0	0	0-1	0	0-1
Data-Reference	703	10415	ENUM	1	0	0	1	0	1	0	1	0	1
Destination-Host	293	0	DIAMIDENT	1	0	0	0-1	0	0-1	0	0-1	0	0-1
Destination-Realm	283	0	DIAMIDENT	1	0	0	1	0	1	0	1	0	1
Experimental-Result	297	0	GROUPED	1	0	0-1	0	0-1	0	0-1	0	0-1	0
Experimental-Result-Code	298	0	ENUM	1	0	1	0	1	0	1	0	1	0
Failed-AVP	279	0	GROUPED	1	0	0+	0	0+	0	0+	0	0+	0
Feature-List	630	10415	UINT32	0	0	1	1	1	1	1	1	1	1
Feature-List-ID	629	10415	UINT32	0	0	1	1	1	1	1	1	1	1
Identity-Set	708	10415	ENUM	0	0	0	0	0	0	0	0-1	0	0-1
MSISDN	701	10415	OCTETSTRING	1	0	0	0-1	0	0-1	0	0-1	0	0-1
Origin-Host	264	0	DIAMIDENT	1	0	1	1	1	1	1	1	1	1
Origin-Realm	296	0	DIAMIDENT	1	0	1	1	1	1	1	1	1	1
Proxy-Info	284	0	GROUPED	1	0	0+	0+	0+	0+	0+	0+	0+	0+
Public-Identity	601	10415	UTF8STRING	1	0	0	0-1	0	0-1	0	0-1	0	0-1
Requested-Domain	706	10415	ENUM	1	0	0	0	0	0	0	0-1	0	0-1
Result-Code	268	0	ENUM	1	0	0-1	0	0-1	0	0-1	0	0-1	0
Route-Record	282	0	DIAMIDENT	1	0	0+	0+	0+	0+	0+	0+	0+	0+
Send-Data-Indication	710	0	ENUM	1	0	0	0	0	0	0	0-1	0	0
Server-Name	602	10415	UTF8STRING	1	0	0	0	0	0	0	0-1	0	0-1
Service-Indication	704	10415	OCTETSTRING	1	0	0	0	0	0	0	0+	0	0-1
Session-Id	263	0	UTF8STRING	1	0	1	1	1	1	1	1	1	1
Subs-Req-Type	705	0	ENUM	1	0	0	0	0	0	0	0-1	0	0
Supported-Features	628	10415	GROUPED	1	0	0+	0+	0+	0+	0+	0+	0+	0+
User-Data	702	10415	OCTETSTRING	1	0	0	1	0	1	0-1	0	0-1	0
User-Identity	700	10415	GROUPED	1	0	0	1	0	1	0	1	0	1
User-Name	1	0	UTF8STRING	1	0	0	0-1	0	0-1	0	0	0	0
Vendor-Id	266	0	UINT32	1	0	1	1	1	1	1	1	1	1
Vendor-Specific-Application-Id	260	0	GROUPED	1	0	1	1	1	1	1	1	1	1

Standard Gmb Proxy Interface Dictionary

Attribute	AVP Code	Vendor-Id	AVP Type	M Flag	P Flag	ASA	ASR	AAA	AAR	RAA	RAR	STA	STR
3GPP-IMEISV	20	10415	OCTETSTRING	1	0	0	0	0	0-1	0	0	0	0
3GPP-IMSI	1	10415	UTF8STRING	1	0	0	0	0-1	0-1	0	0	0	0
3GPP-MS-TimeZone	23	10415	OCTETSTRING	1	0	0	0	0	0-1	0	0	0	0
3GPP-RAT-Type	21	10415	OCTETSTRING	1	0	0	0	0	0-1	0	0	0	0
3GPP-SGSN-Address	6	10415	OCTETSTRING	1	0	0	0	0	0	0	0+	0	0
3GPP-User-Location-Info	22	10415	UTF8STRING	1	0	0	0	0	0-1	0	0	0	0
Additional-MBMS-Trace-Info	910	10415	OCTETSTRING	1	0	0	0	0	0-1	0	0	0	0-1
Alternative-APN	905	10415	UTF8STRING	1	0	0	0	0-1	0	0	0	0	0
Auth-Application-Id	258	0	UINT32	1	0	0	1	1	1	0	1	0	1
Auth-Request-Type	274	0	ENUM	1	0	0	0	0	1	0	0	0	0
Called-Station-Id	30	0	OCTETSTRING	1	0	0	0	0	0-1	0	0-1	0	0
Calling-Station-Id	31	0	UTF8STRING	1	0	0	0	0	0-1	0	0	0	0
Class	25	0	OCTETSTRING	1	0	0	0	0	0	0	0	0+	0+
Destination-Host	293	0	DIAMIDENT	1	0	0	1	0	0-1	0	1	0	0-1
Destination-Realm	283	0	DIAMIDENT	1	0	0	1	0	1	0	1	0	1
Error-Message	281	0	UTF8STRING	0	0	0-1	0	0-1	0	0-1	0	0-1	0
Error-Reporting-Host	294	0	DIAMIDENT	1	0	0-1	0	0-1	0	0-1	0	0-1	0
Experimental-Result	297	0	GROUPED	1	0	0	0	0-1	0	0-1	0	0	0
Failed-AVP	279	0	GROUPED	1	0	0+	0	0+	0	0+	0	0+	0
Framed-Interface-Id	96	0	UINT64	1	0	0	0	0	0-1	0	0-1	0	0
Framed-IP-Address	8	0	OCTETSTRING	1	0	0	0	0	0-1	0	0-1	0	0
Framed-IPv6-Prefix	97	0	OCTETSTRING	1	0	0	0	0	0-1	0	0-1	0	0
MBMS-2G-3G-Indicator	907	10415	ENUM	1	0	0	0	0	0	0	0-1	0	0
MBMS-BMSC-SSM-IP-Address	918	10415	UTF8STRING	1	0	0	0	0	0	0	0-1	0	0
MBMS-BMSC-SSM-IPv6-Address	919	10415	UTF8STRING	1	0	0	0	0	0	0	0-1	0	0
MBMS-Counting-Information	914	10415	ENUM	1	0	0	0	0	0	0	0-1	0	0
MBMS-GGSN-Address	916	10415	UTF8STRING	1	0	0	0	0	0	0-1	0	0	0
MBMS-GGSN-IPv6-Address	917	10415	UTF8STRING	1	0	0	0	0	0	0-1	0	0	0
MBMS-Required-QoS	913	10415	UTF8STRING	1	0	0	0	0	0	0	0-1	0	0
MBMS-Service-Area	903	10415	OCTETSTRING	1	0	0	0	0	0	0	0-1	0	0
MBMS-Service-Type	906	10415	ENUM	1	0	0	0	0	0	0	0-1	0	0
MBMS-Session-Duration	904	10415	OCTETSTRING	1	0	0	0	0	0	0	0-1	0	0
MBMS-Session-Identity	908	10415	OCTETSTRING	1	0	0	0	0	0	0	0-1	0	0
MBMS-Session-Repetition-number	912	10415	OCTETSTRING	1	0	0	0	0	0	0	0-1	0	0
MBMS-StartStop-Indication	902	10415	ENUM	1	0	0	0	0	0	0-1	0-1	0	0
MBMS-Time-To-Data-Transfer	911	10415	OCTETSTRING	1	0	0	0	0	0	0	0-1	0	0
MBMS-User-Data-Mode-Indication	915	10415	ENUM	1	0	0	0	0	0	0-1	0-1	0	0
Origin-Host	264	0	DIAMIDENT	1	0	1	1	1	1	1	1	1	1
Origin-Realm	296	0	DIAMIDENT	1	0	1	1	1	1	1	1	1	1
Origin-State-Id	278	0	UINT32	1	0	0-1	0-1	0	0	0-1	0-1	0-1	0-1

Attribute	AVP Code	Vendor-Id	AVP Type	M Flag	P Flag	ASA	ASR	AAA	AAR	RAA	RAR	STA	STR
Proxy-Info	284	0	GROUPED	1	0	0+	0+	0+	0+	0+	0+	0+	0+
RAI	909	10415	UTF8STRING	1	0	0	0	0	0-1	0	0	0	0
Re-Auth-Request-Type	285	0	ENUM	1	0	0	0	0	0	0	1	0	0
Redirect-Host	292	0	OCTETSTRING	1	0	0+	0	0	0	0+	0	0+	0
Redirect-Host-Usage	261	0	ENUM	1	0	0-1	0	0	0	0-1	0	0-1	0
Redirect-Max-Cache-Time	262	0	UINT32	1	0	0-1	0	0	0	0-1	0	0-1	0
Required-MBMS-Bearer-Capabilities	901	10415	UTF8STRING	1	0	0	0	0-1	0	0	0	0	0
Result-Code	268	0	ENUM	1	0	1	0	0-1	0	0-1	0	1	0
Route-Record	282	0	DIAMIDENT	1	0	0	0+	0	0+	0	0+	0	0+
Session-Id	263	0	UTF8STRING	1	0	1	1	1	1	1	1	1	1
Termination-Cause	295	0	ENUM	1	0	0	0	0	0	0	0	0	1
TMGI	900	10415	OCTETSTRING	1	0	0	0	0-1	0	0	0-1	0	0

Standard Rel. 7 Gx Dictionary

Attribute	AVP Code	Vendor-Id	AVP Type	M Flag	P Flag	ASA	ASR	CEA	CER	CCA	CCR	DWA	DWR	DPA	DPR	RAA	RAR
3GPP-MS-TimeZone	23	10415	OCTETSTRING	1	0	0	0	0	0	0	0-1	0	0	0	0	0	0
3GPP-RAT-Type	21	10415	OCTETSTRING	1	0	0	0	0	0	0	0-1	0	0	0	0	0-1	0
3GPP-SGSN-Address	6	10415	OCTETSTRING	1	0	0	0	0	0	0	0-1	0	0	0	0	0-1	0
3GPP-SGSN-IPv6-Address	15	10415	OCTETSTRING	1	0	0	0	0	0	0	0	0	0	0	0	0-1	0
3GPP-SGSN-MCC-MNC	18	10415	UTF8STRING	1	0	0	0	0	0	0	0-1	0	0	0	0	0-1	0
3GPP-User-Location-Info	22	10415	UTF8STRING	1	0	0	0	0	0	0	0-1	0	0	0	0	0-1	0
Access-Network-Charging-Address	501	10415	ADDRESS	1	0	0	0	0	0	0	0-1	0	0	0	0	0-1	0
Access-Network-Charging-Identifier-Gx	1022	10415	GROUPED	1	0	0	0	0	0	0	0+	0	0	0	0	0+	0
Acct-Application-Id	259	0	UINT32	1	0	0	0	0+	0+	0	0	0	0	0	0	0	0
Auth-Application-Id	258	0	UINT32	1	0	1	1	0+	0+	1	1	0	0	0	0	0	1
Bearer-Control-Mode	1023	10415	ENUM	1	0	0	0	0	0	0-1	0	0	0	0	0	0	0
Bearer-Identifier	1020	10415	OCTETSTRING	1	0	0	0	0	0	0-1	0-1	0	0	0	0	0	0-1
Bearer-Operation	1021	10415	ENUM	1	0	0	0	0	0	0	0-1	0	0	0	0	0	0
Bearer-Usage	1000	10415	ENUM	1	0	0	0	0	0	0	0-1	0	0	0	0	0	0
Called-Station-Id	30	0	OCTETSTRING	1	0	0	0	0	0	0	0-1	0	0	0	0	0	0
CC-Request-Number	415	0	UINT32	1	0	0	0	0	0	1	1	0	0	0	0	0	0
CC-Request-Type	416	0	ENUM	1	0	0	0	0	0	1	1	0	0	0	0	0	0
Charging-Information	618	10415	GROUPED	1	0	0	0	0	0	0-1	0	0	0	0	0	0	0
Charging-Rule-Base-Name	1004	10415	UTF8STRING	1	0	0	0	0	0	0+	0+	0	0	0	0	0+	0+
Charging-Rule-Definition	1003	10415	GROUPED	1	0	0	0	0	0	0+	0	0	0	0	0	0	0+
Charging-Rule-Install	1001	10415	GROUPED	1	0	0	0	0	0	0+	0	0	0	0	0	0	0+
Charging-Rule-Name	1005	10415	OCTETSTRING	1	0	0	0	0	0	0+	0+	0	0	0	0	0+	0+
Charging-Rule-Remove	1002	10415	GROUPED	1	0	0	0	0	0	0+	0	0	0	0	0	0	0+
Charging-Rule-Report	1018	10415	GROUPED	1	0	0	0	0	0	0	0+	0	0	0	0	0+	0
Destination-Host	293	0	DIAMIDENT	1	0	0	0-1	0	0	0	0-1	0	0	0	0	0	1
Destination-Realm	283	0	DIAMIDENT	1	0	0	1	0	0	0	1	0	0	0	0	0	1
Disconnect-Cause	273	0	ENUM	1	0	0	0	0	0	0	0	0	0	0	1	0	0
Error-Message	281	0	UTF8STRING	0	0	0	0	0-1	0	0-1	0	0-1	0	0-1	0	0-1	0
Error-Reporting-Host	294	0	DIAMIDENT	1	0	0	0	0	0	0-1	0	0	0	0	0	0-1	0
Event-Trigger	1006	10415	ENUM	1	0	0	0	0	0	0+	0+	0	0	0	0	0	0+
Experimental-Result	297	0	GROUPED	1	0	0	0	0	0	0-1	0	0	0	0	0	0-1	0
Failed-AVP	279	0	GROUPED	1	0	0	0	0+	0	0+	0	0-1	0	0+	0	0+	0
Feature-List	630	10415	UINT32	0	0	0	0	0	0	1	1	0	0	0	0	0	0
Feature-List-ID	629	10415	UINT32	0	0	0	0	0	0	1	1	0	0	0	0	0	0
Final-Unit-Indication	430	0	GROUPED	1	0	0	0	0	0	0	0-1	0	0	0	0	0-1	0
Firmware-Revision	267	0	UINT32	0	0	0	0	0-1	0-1	0	0	0	0	0	0	0	0
Framed-IP-Address	8	0	OCTETSTRING	1	0	0	0	0	0	0	0-1	0	0	0	0	0	0
Framed-IPv6-Prefix	97	0	OCTETSTRING	1	0	0	0	0	0	0	0-1	0	0	0	0	0	0
Granted-Service-Unit	431	0	GROUPED	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Guaranteed-Bitrate-DL	1025	10415	UINT32	1	0	0	0	0	0	0-1	0-1	0	0	0	0	0	0-1
Guaranteed-Bitrate-UL	1026	10415	UINT32	1	0	0	0	0	0	0-1	0-1	0	0	0	0	0	0-1
Host-IP-Address	257	0	ADDRESS	1	0	0	0	0+	0+	0	0	0	0	0	0	0	0
Inband-Security-Id	299	0	ENUM	1	0	0	0	0+	0+	0	0	0	0	0	0	0	0
IP-CAN-Type	1027	10415	ENUM	1	0	0	0	0	0	0	0-1	0	0	0	0	0-1	0
Max-Requested-Bandwidth-DL	515	10415	UINT32	1	0	0	0	0	0	0-1	0-1	0	0	0	0	0	0-1
Max-Requested-Bandwidth-UL	516	10415	UINT32	1	0	0	0	0	0	0-1	0-1	0	0	0	0	0	0-1
Network-Request-Support	1024	10415	ENUM	1	0	0	0	0	0	0	0-1	0	0	0	0	0	0
Offline	1008	10415	ENUM	1	0	0	0	0	0	0-1	0-1	0	0	0	0	0	0
Online	1009	10415	ENUM	1	0	0	0	0	0	0-1	0-1	0	0	0	0	0	0
Origin-Host	264	0	DIAMIDENT	1	0	1	1	1	1	1	1	1	1	1	1	1	1

Attribute	AVP Code	Vendor-Id	AVP Type	M Flag	P Flag	ASA	ASR	CEA	CER	CCA	CCR	DWA	DWR	DPA	DPR	RAA	RAR
Origin-Realm	296	0	DIAMIDENT	1	0	1	1	1	1	1	1	1	1	1	1	1	1
Origin-State-Id	278	0	UINT32	1	0	0	0	0-1	0-1	0-1	0-1	0-1	0-1	0	0	0-1	0-1
PCC-Rule-Status	1019	10415	ENUM	1	0	0	0	0	0	0	0-1	0	0	0	0	0-1	0
Precedence	1010	10415	UINT32	1	0	0	0	0	0	0	0-1	0	0	0	0	0	0
Primary-Charging-Collection-Function-Name	621	10415	DIAMURI	1	0	0	0	0	0	0-1	0	0	0	0	0	0	0
Primary-Event-Charging-Function-Name	619	10415	DIAMURI	1	0	0	0	0	0	0-1	0	0	0	0	0	0	0
Product-Name	269	0	UTF8STRING	0	0	0	0	1	1	0	0	0	0	0	0	0	0
Proxy-Info	284	0	GROUPED	1	0	0	0	0	0	0+	0+	0	0	0	0	0+	0+
QoS-Class-Identifier	1028	10415	ENUM	1	0	0	0	0	0	0-1	0-1	0	0	0	0	0	0-1
QoS-Information	1016	10415	GROUPED	1	0	0	0	0	0	0-1	0-1	0	0	0	0	0	0-1
QoS-Negotiation	1029	10415	ENUM	1	0	0	0	0	0	0	0-1	0	0	0	0	0	0
QoS-Upgrade	1030	10415	ENUM	1	0	0	0	0	0	0	0-1	0	0	0	0	0	0
RAI	909	10415	UTF8STRING	1	0	0	0	0	0	0	0-1	0	0	0	0	0-1	0
Re-Auth-Request-Type	285	0	ENUM	1	0	0	0	0	0	0	0	0	0	0	0	0	1
Result-Code	268	0	ENUM	1	0	1	0	1	0	0-1	0	1	0	1	0	0-1	0
Revalidation-Time	1042	10415	TIME	1	0	0	0	0	0	0-1	0	0	0	0	0	0	0-1
Route-Record	282	0	DIAMIDENT	1	0	0	0	0	0	0+	0+	0	0	0	0	0	0+
Rule-Activation-Time	1043	10415	TIME	1	0	0	0	0	0	0-1	0	0	0	0	0	0	0-1
Rule-Deactivation-Time	1044	10415	TIME	1	0	0	0	0	0	0-1	0	0	0	0	0	0	0-1
Rule-Failure-Code	1031	10415	ENUM	1	0	0	0	0	0	0	0-1	0	0	0	0	0-1	0
Secondary-Charging-Collection-Function-Na	622	10415	DIAMURI	1	0	0	0	0	0	0-1	0	0	0	0	0	0	0
Secondary-Event-Charging-Function-Name	620	10415	DIAMURI	1	0	0	0	0	0	0-1	0	0	0	0	0	0	0
Session-Id	263	0	UTF8STRING	1	0	1	1	0	0	1	1	0	0	0	0	1	1
Session-Release-Cause	1045	10415	ENUM	1	0	0	0	0	0	0	0	0	0	0	0	0	0-1
Subscription-Id	443	0	GROUPED	1	0	0	0	0	0	0	0+	0	0	0	0	0	0
Supported-Features	628	10415	GROUPED	0	0	0	0	0	0	0+	0+	0	0	0	0	0	0
Supported-Vendor-Id	265	0	UINT32	1	0	0	0	0+	0+	0	0	0	0	0	0	0	0
Termination-Cause	295	0	ENUM	1	0	0	0	0	0	0	0-1	0	0	0	0	0	0
TFT-Filter	1012	10415	IPFILTERRULE	1	0	0	0	0	0	0	0-1	0	0	0	0	0	0
TFT-Packet-Filter-Information	1013	10415	GROUPED	1	0	0	0	0	0	0	0+	0	0	0	0	0	0
ToS-Traffic-Class	1014	10415	OCTETSTRING	1	0	0	0	0	0	0	0-1	0	0	0	0	0	0
Usage-Monitoring-Information	1067	10415	GROUPED	0	0	0	0	0	0	0+	0+	0	0	0	0	0	0+
Used-Service-Unit	446	0	GROUPED	0	0	0	0	0	0	0	0	0	0	0	0	0	0
User-Equipment-Info	458	0	GROUPED	1	0	0	0	0	0	0	0-1	0	0	0	0	0	0
User-Name	1	0	UTF8STRING	1	0	0-1	0-1	0	0	0	0	0	0	0	0	0	0
Vendor-Id	266	0	UINT32	1	0	0	0	1	1	1	1	0	0	0	0	0	0
Vendor-Specific-Application-Id	260	0	GROUPED	1	0	0	0	0+	0+	0	0	0	0	0	0	0	0

S6a Dictionary 3GPP 29.272

Attribute	AVP Code	Vendor-Id	AVP Type	M Flag	P Flag	AIA	AIR	CLA	CLR	DSDA	DSDR	ISDA	ISDR	NA	NR	PUAM	PURM	RA	RR	ULA	ULR
3GPP2-MEID	1471	10415	OCTETSTRING	1	0	0	0	0	0	0	0	0	0	0	0-1	0	0	0	0	0	0-1
3GPP-Charging-Characteristics	13	10415	UTF8STRING	1	0	0	0	0	0	0	0	0	0-1	0	0	0	0	0	0	0-1	0
Access-Restriction-Data	1426	10415	UINT32	1	0	0	0	0	0	0	0	0	0-1	0	0	0	0	0	0	0-1	0
Alert-Reason	1434	10415	ENUM	1	0	0	0	0	0	0	0	0	0	0	0-1	0	0	0	0	0	0
All-APN-Configurations-Included-Indicator	1428	10415	ENUM	1	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	1	0
Allocation-Retention-Priority	1034	10415	GROUPED	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AMBR	1435	10415	GROUPED	1	0	0	0	0	0	0	0	0	0-1	0	0	0	0	0	0	0-1	0
APN-Configuration	1430	10415	GROUPED	1	0	0	0	0	0	0	0	0	0+	0	0	0	0	0	0	0+	0
APN-Configuration-Profile	1429	10415	GROUPED	1	0	0	0	0	0	0	0	0	0-1	0	0	0	0	0	0	0-1	0
APN-OI-Replacement	1427	10415	UTF8STRING	1	0	0	0	0	0	0	0	0	0-1	0	0	0	0	0	0	0-1	0
Authentication-Info	1413	10415	GROUPED	1	0	0-1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Auth-Session-State	277	0	ENUM	1	0	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
AUTN	1449	10415	OCTETSTRING	1	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Call-Barring-Info-List	1488	10415	GROUPED	1	0	0	0	0	0	0	0	0	0-1	0	0	0	0	0	0	0-1	0
Cancellation-Type	1420	10415	ENUM	1	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0
Complete-Data-List-Included-Indicator	1468	10415	ENUM	1	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	1	0
Confidentiality-Key	625	10415	OCTETSTRING	1	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Context-Identifier	1423	10415	UINT32	1	0	0	0	0	0	0	0+	0	1	0	0-1	0	0	0	0	1	0
CSG-Id	1437	10415	UINT32	1	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	1	0
CSG-Subscription-Data	1436	10415	GROUPED	1	0	0	0	0	0	0	0	0	0+	0	0	0	0	0	0	0+	0
Destination-Host	293	0	DIAMIDENT	1	0	0	0-1	0	1	0	1	0	1	0	0-1	0	0-1	0	1	0	0-1
Destination-Realm	283	0	DIAMIDENT	1	0	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1
DSA-Flags	1422	10415	UINT32	1	0	0	0	0	0	0-1	0	0	0	0	0	0	0	0	0	0	0
DSR-Flags	1421	10415	UINT32	1	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0
EPS-Subscribed-QoS-Profile	1431	10415	GROUPED	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
EUTRAN-Vector	1414	10415	GROUPED	1	0	0+	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Experimental-Result	297	0	GROUPED	1	0	0-1	0	0-1	0	0-1	0	0-1	0	0-1	0	0-1	0	0-1	0	0-1	0
Expiration-Date	1439	0	TIME	1	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	1	0
External-Client	1479	10415	GROUPED	1	0	0	0	0	0	0	0	0	0+	0	0	0	0	0	0	0+	0
Failed-AVP	279	0	GROUPED	1	0	0+	0	0+	0	0+	0	0+	0	0+	0	0+	0	0+	0	0+	0
Feature-List	630	10415	UINT32	0	0	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
Feature-List-ID	629	10415	UINT32	0	0	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
GERAN-Vector	1416	10415	GROUPED	1	0	0+	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
GMLC-Number	1474	10415	OCTETSTRING	1	0	0	0	0	0	0	0	0	0+	0	0	0	0	0	0	0+	0
GMLC-Restriction	1481	10415	ENUM	1	0	0	0	0	0	0	0	0	0-1	0	0	0	0	0	0	0-1	0
GPRS-Subscription-Data	1467	10415	GROUPED	1	0	0	0	0	0	0	0	0	0-1	0	0	0	0	0	0	0-1	0
HPLMN-ODB	1418	10415	UINT32	1	0	0	0	0	0	0	0	0	0-1	0	0	0	0	0	0	0-1	0
IDA-Flags	1441	10415	UINT32	1	0	0	0	0	0	0	0	0-1	0	0	0	0	0	0	0	0	0
IDR-Flags	1490	10415	UINT32	1	0	0	0	0	0	0	0	0	0-1	0	0	0	0	0	0	0	0
IMEI	1402	10415	UTF8STRING	1	0	0	0	0	0	0	0	0	0	0	0-1	0	0	0	0	0	0-1
Immediate-Response-Preferred	1412	10415	UINT32	1	0	0	0-1	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Integrity-Key	626	10415	OCTETSTRING	1	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Item-Number	1419	10415	UINT32	1	0	0-1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
LCS-Info	1473	10415	GROUPED	1	0	0	0	0	0	0	0	0	0-1	0	0	0	0	0	0	0-1	0
LCS-PrivacyException	1475	10415	GROUPED	1	0	0	0	0	0	0	0	0	0+	0	0	0	0	0	0	0+	0
Max-Requested-Bandwidth-DL	515	10415	UINT32	1	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	1	0
Max-Requested-Bandwidth-UL	516	10415	UINT32	1	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	1	0
MIP6-Agent-Info	486	0	GROUPED	1	0	0	0	0	0	0	0	0	0	0	0-1	0	0	0	0	0	0
MME-Service-Type	1483	10415	GROUPED	1	0	0	0	0	0	0	0	0	0+	0	0	0	0	0	0	0+	0
MO-LR	1485	10415	GROUPED	1	0	0	0	0	0	0	0	0	0+	0	0	0	0	0	0	0+	0
MSISDN	701	10415	OCTETSTRING	1	0	0	0	0	0	0	0	0	0-1	0	0	0	0	0	0	0-1	0
Network-Access-Mode	1417	10415	ENUM	1	0	0	0	0	0	0	0	0	0-1	0	0	0	0	0	0	0-1	0
NOR-Flags	1443	10415	UINT32	1	0	0	0	0	0	0	0	0	0	0	0-1	0	0	0	0	0	0
Notification-To-UE-User	1478	10415	ENUM	1	0	0	0	0	0	0	0	0	0-1	0	0	0	0	0	0	0-1	0
Number-Of-Requested-Vectors	1410	10415	UINT32	1	0	0	0-1	0	0	0	0	0	0	0	0	0	0	0	0	0	0
OMC-Id	1466	10415	OCTETSTRING	1	0	0	0	0	0	0	0	0	0-1	0	0	0	0	0	0	0-1	0
Operator-Determined-Barring	1425	10415	UINT32	1	0	0	0	0	0	0	0	0	0-1	0	0	0	0	0	0	0-1	0
Origin-Host	264	0	DIAMIDENT	1	0	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
Origin-Realm	296	0	DIAMIDENT	1	0	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1

Attribute	AVP Code	Vendor-Id	AVP Type	M Flag	P Flag	AIA	AIR	CLA	CLR	DSDA	DSDR	ISDA	ISDR	NA	NR	PUAM	PURM	RA	RR	ULA	ULR
PDN-GW-Identity	6044	10415	GROUPED	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
PDP-Context	1469	10415	GROUPED	1	0	0	0	0	0	0	0	0	0+	0	0	0	0	0	0	0+	0
PLMN-Client	1482	10415	ENUM	1	0	0	0	0	0	0	0	0	0+	0	0	0	0	0	0	0+	0
Proxy-Info	284	0	GROUPED	1	0	0+	0+	0+	0+	0+	0+	0+	0+	0+	0+	0+	0+	0+	0+	0+	0+
PUA-Flags	1442	10415	UINT32	1	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0
RAND	1447	10415	OCTETSTRING	1	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
RAT-Frequency-Selection-Priority	1440	10415	UINT32	1	0	0	0	0	0	0	0	0	0-1	0	0	0	0	0	0	0-1	0
RAT-Type	1032	10415	ENUM	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1
Regional-Subscription-Zone-Code	1446	10415	OCTETSTRING	1	0	0	0	0	0	0	0	0	0+	0	0	0	0	0	0	0+	0
Requested-EUTRAN-Authentication-Info	1408	10415	GROUPED	1	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Requested-GERAN-Authentication-Info	6012	10415	GROUPED	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Requested-UTRAN-GERAN-Authentication-	1409	10415	GROUPED	1	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Result-Code	268	0	ENUM	1	0	0-1	0	0-1	0	0-1	0	0-1	0	0-1	0	0-1	0	0-1	0	0-1	0
Re-Synchronization-Info	1411	10415	OCTETSTRING	1	0	0	0-1	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Roaming-Restricted-Due-To-Unsupported-F	1461	10415	ENUM	1	0	0	0	0	0	0	0	0	0-1	0	0	0	0	0	0	0-1	0
Route-Record	282	0	DIAMIDENT	1	0	0+	0+	0+	0+	0+	0+	0+	0+	0+	0+	0+	0+	0+	0+	0+	0+
Service-Selection	493	0	OCTETSTRING	1	0	0	0	0	0	0	0	0	0	0	0-1	0	0	0	0	0	0
ServiceTypeIdentity	1484	10415	UINT32	1	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	1	0
Session-Id	263	0	UTF8STRING	1	0	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
SGSN-Number	1489	10415	OCTETSTRING	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0-1
Software-Version	1403	10415	UTF8STRING	1	0	0	0	0	0	0	0	0	0	0	0-1	0	0	0	0	0	0-1
Specific-APN-Info	1472	10415	GROUPED	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
SS-Code	1478	10415	OCTETSTRING	1	0	0	0	0	0	0	0-1	0	1	0	0	0	0	0	0	1	0
SS-Status	1477	10415	OCTETSTRING	1	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	1	0
STN-SR	1433	10415	UTF8STRING	1	0	0	0	0	0	0	0	0	0-1	0	0	0	0	0	0	0-1	0
Subscriber-Status	1424	10415	ENUM	1	0	0	0	0	0	0	0	0	0-1	0	0	0	0	0	0	0-1	0
Subscription-Data	1400	10415	GROUPED	1	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0-1	0
Supported-Features	628	10415	GROUPED	1	0	0+	0+	0+	0+	0+	0+	0+	0+	0+	0+	0+	0+	0-1	0-1	0+	0+
Teleservice-List	1486	10415	GROUPED	1	0	0	0	0	0	0	0	0	0-1	0	0	0	0	0	0	0-1	0
Terminal-Information	1401	10415	GROUPED	1	0	0	0	0	0	0	0	0	0	0	0-1	0	0	0	0	0	0-1
Trace-Collection-Entity	1452	10415	ADDRESS	1	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	1	0
Trace-Data	1458	10415	GROUPED	1	0	0	0	0	0	0	0	0	0-1	0	0	0	0	0	0	0-1	0
Trace-Depth	1462	10415	ENUM	1	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	1	0
Trace-Depth-List	1460	10415	GROUPED	1	0	0	0	0	0	0	0	0	0-1	0	0	0	0	0	0	0-1	0
Trace-Depth-Per-NE-Type	7015	10415	GROUPED	1	0	0	0	0	0	0	0	0	0+	0	0	0	0	0	0	0+	0
Trace-Event-List	1465	10415	OCTETSTRING	1	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	1	0
Trace-Interface-List	1464	10415	OCTETSTRING	1	0	0	0	0	0	0	0	0	0-1	0	0	0	0	0	0	0-1	0
Trace-NE-Type-List	1463	10415	OCTETSTRING	1	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	1	0
Trace-Reference	1459	10415	OCTETSTRING	1	0	0	0	0	0	0	0-1	0	1	0	0	0	0	0	0	1	0
TS-Code	1487	10415	OCTETSTRING	1	0	0	0	0	0	0	0	0	0+	0	0	0	0	0	0	0+	0
ULA-Flags	1406	10415	UINT32	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0
ULR-Flags	1405	10415	UINT32	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1
User-Id	1444	10415	UTF8STRING	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0+	0	0
User-Name	1	0	UTF8STRING	1	0	0	1	0	1	0	1	0	1	0	1	0	1	0	0	0	1
UTRAN-Vector	1415	10415	GROUPED	1	0	0+	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Vendor-Id	266	0	UINT32	1	0	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
Vendor-Specific-Application-Id	260	0	GROUPED	1	0	0-1	0-1	0-1	0-1	0-1	0-1	0-1	0-1	0-1	0-1	0-1	0-1	0-1	0-1	0-1	0-1
Visited-PLMN-Id	1407	10415	UTF8STRING	1	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	1
XRES	1448	10415	OCTETSTRING	1	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

S13 Dictionary 3GPP 29.272

Attribute	AVP Code	Vendor-Id	AVP Type	M Flag	P Flag	MICA	MICR
3GPP2-MEID	1471	10415	OCTETSTRING	1	0	0	0-1
Auth-Session-State	277	0	ENUM	1	0	1	1
Destination-Host	293	0	DIAMIDENT	1	0	0	0-1
Destination-Realm	283	0	DIAMIDENT	1	0	0	1
Equipment-Status	1445	10415	ENUM	1	0	0-1	0
Experimental-Result	297	0	GROUPED	1	0	0-1	0
Failed-AVP	279	0	GROUPED	1	0	0+	0
IMEI	1402	10415	UTF8STRING	1	0	0	0-1
Origin-Host	264	0	DIAMIDENT	1	0	1	1
Origin-Realm	296	0	DIAMIDENT	1	0	1	1
Proxy-Info	284	0	GROUPED	1	0	0+	0+
Result-Code	268	0	ENUM	1	0	0-1	0
Route-Record	282	0	DIAMIDENT	1	0	0+	0+
Session-Id	263	0	UTF8STRING	1	0	1	1
Software-Version	1403	10415	UTF8STRING	1	0	0	0-1
Terminal-Information	1401	10415	GROUPED	1	0	0	1
User-Name	1	0	UTF8STRING	1	0	0	0-1

S6b Dictionary 3GPP 29.273

Attribute	AVP Code	Vendor-Id	AVP Type	M Flag	P Flag	ASA	ASR	AAA	AAR	RAA	RAR	STA	STR
Auth-Application-Id	258	0	UINT32	1	0	0	1	1	1	0	1	0	1
Auth-Grace-Period	276	0	UINT32	1	0	0	0	0-1	0-1	0	0	0	0
Authorization-Lifetime	291	0	UINT32	1	0	0	0	0-1	0-1	0	0	0	0
Auth-Request-Type	274	0	ENUM	1	0	0	0	1	1	0	0	0	0
Auth-Session-State	277	0	ENUM	1	0	0	0	0-1	0-1	0	0	0	0
Class	25	0	OCTETSTRING	1	0	0	0+	0+	0	0+	0+	0+	0+
Destination-Host	293	0	DIAMIDENT	1	0	0	1	0	0-1	0	1	0	0-1
Destination-Realm	283	0	DIAMIDENT	1	0	0	1	0	1	0	1	0	1
Error-Message	281	0	UTF8STRING	0	0	0-1	0	0-1	0	0-1	0	0-1	0
Error-Reporting-Host	294	0	DIAMIDENT	1	0	0-1	0	0-1	0	0-1	0	0-1	0
Experimental-Result	297	0	GROUPED	1	0	0	0	0-1	0	0	0	0	0
Experimental-Result-Code	298	0	ENUM	1	0	0	0	1	0	0	0	0	0
Extended-QoS-Filter-Rule	6066	0	UINT32	1	0	0	0	0+	0	0	0	0	0
Failed-AVP	279	0	GROUPED	1	0	0+	0	0+	0	0+	0	0+	0
Feature-List	630	10415	UINT32	0	0	0	0	1	1	0	0	0	0
Feature-List-ID	629	10415	UINT32	0	0	0	0	1	1	0	0	0	0
Idle-Timeout	28	0	UINT32	1	0	0	0	0-1	0-1	0	0	0	0
MIP6-Agent-Info	486	0	GROUPED	1	0	0	0	0	0+	0	0	0	0
MIP6-Feature-Vector	124	0	UINT64	1	0	0	0	0-1	0-1	0	0	0	0
MIP6-Home-Link-Prefix	125	0	OCTETSTRING	1	0	0	0	0	0-1	0	0	0	0
MIP-Home-Agent-Address-IETF	334	0	ADDRESS	1	0	0	0	0	0+	0	0	0	0
MIP-Home-Agent-Host	348	0	GROUPED	1	0	0	0	0	0-1	0	0	0	0
Origin-Host	264	0	DIAMIDENT	1	0	1	1	1	1	1	1	1	1
Origin-Realm	296	0	DIAMIDENT	1	0	1	1	1	1	1	1	1	1
Origin-State-Id	278	0	UINT32	1	0	0-1	0-1	0-1	0-1	0-1	0-1	0-1	0-1
Proxy-Host	280	0	DIAMIDENT	1	0	1	1	1	1	1	1	1	1
Proxy-Info	284	0	GROUPED	1	0	0+	0+	0+	0+	0+	0+	0+	0+
Proxy-State	33	0	OCTETSTRING	1	0	1	1	1	1	1	1	1	1
QoS-Capability	6063	0	GROUPED	1	0	0	0	0	0-1	0	0	0	0
QoS-Profile-Template	6067	0	UINT32	1	0	0	0	0	0+	0	0	0	0
QoS-Resources	6065	0	GROUPED	1	0	0	0	0-1	0	0	0	0	0
Re-Auth-Request-Type	285	0	ENUM	1	0	0	0	0-1	0	0	1	0	0
Redirect-Host	292	0	OCTETSTRING	1	0	0+	0	0+	0	0+	0	0+	0
Redirect-Host-Usage	261	0	ENUM	1	0	0-1	0	0-1	0	0-1	0	0-1	0
Redirect-Max-Cache-Time	262	0	UINT32	1	0	0-1	0	0-1	0	0-1	0	0-1	0
Reply-Message	18	0	UTF8STRING	1	0	0	0+	0	0	0	0	0	0
Result-Code	268	0	ENUM	1	0	1	0	1	0	1	0	1	0
Route-Record	282	0	DIAMIDENT	1	0	0	0+	0	0+	0	0+	0	0+
Service-Selection	493	0	OCTETSTRING	1	0	0	0	0	0-1	0	0	0	0
Session-Id	263	0	UTF8STRING	1	0	1	1	1	1	1	1	1	1

Attribute	AVP Code	Vendor-Id	AVP Type	M Flag	P Flag	ASA	ASR	AAA	AAR	RAA	RAR	STA	STR
Session-Timeout	27	0	UINT32	1	0	0	0	0-1	0	0	0	0	0
State	24	0	OCTETSTRING	1	0	0-1	0-1	0	0	0-1	0-1	0	0
Supported-Features	628	10415	GROUPED	1	0	0	0	0+	0+	0	0	0	0
Termination-Cause	295	0	ENUM	1	0	0	0	0	0	0	0	0	1
User-Name	1	0	UTF8STRING	1	0	0	0-1	0	0-1	0-1	0-1	0	0-1
Vendor-Id	266	0	UINT32	1	0	0	0	1	1	0	0	0	0
Vendor-Specific-QoS-Profile-Template	6064	0	GROUPED	1	0	0	0	0	0+	0	0	0	0

STa Dictionary 3GPP 29.273

Attribute	AVP Code	Vendor-Id	AVP Type	M Flag	P Flag	ASA	ASR	AAA	AAR	DEA	DER	RAA	RAR	STA	STR
3GPP2-MEID	1471	10415	OCTETSTRING	1	0	0	0	0	0	0	0-1	0	0	0	0
3GPP-Charging-Characteristics	13	10415	UTF8STRING	1	0	0	0	0-1	0	0-1	0	0	0	0	0
Acct-Interim-Interval	85	0	UINT32	0	0	0	0	0-1	0	0-1	0	0	0	0	0
Allocation-Retention-Priority	1034	10415	GROUPED	1	0	0	0	1	0	1	0	0	0	0	0
AMBR	1435	10415	GROUPED	1	0	0	0	0-1	0	0-1	0	0	0	0	0
ANID	1504	10415	UTF8STRING	1	0	0	0	0	0	0	0-1	0	0	0	0
AN-Trusted	1503	10415	ENUM	1	0	0	0	0	0	0	0-1	0	0	0	0
APN-Configuration	1430	10415	GROUPED	1	0	0	0	0+	0	0+	0	0	0	0	0
APN-OI-Replacement	1427	10415	UTF8STRING	1	0	0	0	0-1	0	0-1	0	0	0	0	0
Auth-Application-Id	258	0	UINT32	1	0	0	1	1	1	1	1	0	1	0	1
Auth-Grace-Period	276	0	UINT32	1	0	0	0	0-1	0-1	0-1	0-1	0	0	0	0
Authorization-Lifetime	291	0	UINT32	1	0	0	0	0-1	0-1	0-1	0-1	0	0	0	0
Auth-Request-Type	274	0	ENUM	1	0	0	0	1	1	1	1	0	0	0	0
Auth-Session-State	277	0	ENUM	1	0	0	0	0-1	0-1	0-1	0-1	0	0	0	0
Calling-Station-Id	31	0	UTF8STRING	1	0	0	0	0	0	0	0-1	0	0	0	0
Class	25	0	OCTETSTRING	1	0	0	0+	0+	0	0+	0	0+	0+	0+	0+
Context-Identifier	1423	10415	UINT32	1	0	0	0	0-1	0	0-1	0	0	0	0	0
Destination-Host	293	0	DIAMIDENT	1	0	0	1	1	0-1	1	0-1	0	1	0	0-1
Destination-Realm	283	0	DIAMIDENT	1	0	0	1	1	1	1	1	0	1	0	1
EAP-Master-Session-Key	464	0	OCTETSTRING	1	0	0	0	0	0	0-1	0	0	0	0	0
EAP-Payload	462	0	OCTETSTRING	1	0	0	0	0	0	1	1	0	0	0	0
EPS-Subscribed-QoS-Profile	1431	10415	GROUPED	1	0	0	0	0-1	0	0-1	0	0	0	0	0
Error-Message	281	0	UTF8STRING	0	0	0-1	0	0-1	0	0-1	0	0-1	0	0-1	0
Error-Reporting-Host	294	0	DIAMIDENT	1	0	0-1	0	0-1	0	0-1	0	0-1	0	0-1	0
Experimental-Result	297	0	GROUPED	1	0	0	0	0-1	0	0-1	0	0	0	0	0
Experimental-Result-Code	298	0	ENUM	1	0	0	0	1	0	1	0	0	0	0	0
Failed-AVP	279	0	GROUPED	1	0	0+	0	0+	0	0+	0	0+	0	0+	0
Feature-List	630	10415	UINT32	0	0	0	0	0	0	1	1	0	0	0	0
Feature-List-ID	629	10415	UINT32	0	0	0	0	0	0	1	1	0	0	0	0
Idle-Timeout	28	0	UINT32	1	0	0	0	0-1	0	0-1	0	0	0	0	0
IMEI	1402	10415	UTF8STRING	1	0	0	0	0	0	0	0-1	0	0	0	0
IP-MMS	6076	10415	UINT32	1	0	0	0	0	0	0-1	0	0	0	0	0
Max-Requested-Bandwidth-DL	515	10415	UINT32	1	0	0	0	1	0	1	0	0	0	0	0
Max-Requested-Bandwidth-UL	516	10415	UINT32	1	0	0	0	1	0	1	0	0	0	0	0
MIP6-Agent-Info	486	0	GROUPED	1	0	0	0	0-1	0	0-1	0	0	0	0	0
MIP6-Feature-Vector	124	0	UINT64	1	0	0	0	0	0	0-1	0-1	0	0	0	0
MIP6-Home-Link-Prefix	125	0	OCTETSTRING	1	0	0	0	0-1	0	0-1	0	0	0	0	0
MIP-Home-Agent-Address-IETF	334	0	ADDRESS	1	0	0	0	0+	0	0+	0	0	0	0	0
MIP-Home-Agent-Host	348	0	GROUPED	1	0	0	0	0-1	0	0-1	0	0	0	0	0
Mobile-Node-Identifier	506	0	OCTETSTRING	1	0	0	0	0	0	0-1	0	0	0	0	0
Multi-Round-Time-Out	272	0	UINT32	0	0	0	0	0	0	0-1	0	0	0	0	0
Origin-Host	264	0	DIAMIDENT	1	0	1	1	1	1	1	1	1	1	1	1
Origin-Realm	296	0	DIAMIDENT	1	0	1	1	1	1	1	1	1	1	1	1
Origin-State-Id	278	0	UINT32	1	0	0-1	0-1	0-1	0-1	0-1	0-1	0-1	0-1	0-1	0-1
PDN-GW-Allocation-Type	1438	10415	ENUM	1	0	0	0	0-1	0	0-1	0	0	0	0	0

Attribute	AVP Code	Vendor-Id	AVP Type	M Flag	P Flag	ASA	ASR	AAA	AAR	DEA	DER	RAA	RAR	STA	STR
PDN-Type	1456	10415	ENUM	1	0	0	0	1	0	1	0	0	0	0	0
Proxy-Host	280	0	DIAMIDENT	1	0	1	1	1	1	1	1	1	1	1	1
Proxy-Info	284	0	GROUPED	1	0	0+	0+	0+	0+	0+	0+	0+	0+	0+	0+
Proxy-State	33	0	OCTETSTRING	1	0	1	1	1	1	1	1	1	1	1	1
QoS-Capability	6063	0	GROUPED	1	0	0	0	0	0-1	0	0-1	0	0	0	0
QoS-Class-Identifier	1028	10415	ENUM	1	0	0	0	1	0	1	0	0	0	0	0
QoS-Profile-Template	6067	0	UINT32	1	0	0	0	0	0+	0	0+	0	0	0	0
RAT-Type	1032	10415	ENUM	1	0	0	0	0	0-1	0	0-1	0	0	0	0
Re-Auth-Request-Type	285	0	ENUM	1	0	0	0	0	0	0	0	0	1	0	0
Redirect-Host	292	0	OCTETSTRING	1	0	0+	0	0+	0	0+	0	0+	0	0+	0
Redirect-Host-Usage	261	0	ENUM	1	0	0-1	0	0-1	0	0-1	0	0-1	0	0-1	0
Redirect-Max-Cache-Time	262	0	UINT32	1	0	0-1	0	0-1	0	0-1	0	0-1	0	0-1	0
Reply-Message	18	0	UTF8STRING	1	0	0	0+	0	0	0	0	0	0	0	0
Result-Code	268	0	ENUM	1	0	1	0	0-1	0	0-1	0	1	0	1	0
Route-Record	282	0	DIAMIDENT	1	0	0	0+	0	0+	0	0+	0	0+	0	0+
Served-Party-IP-Address	848	10415	ADDRESS	1	0	0	0	0-1	0	0-1	0	0	0	0	0
Service-Selection	493	0	OCTETSTRING	1	0	0	0	1	0	1	0-1	0	0	0	0
Session-Id	263	0	UTF8STRING	1	0	1	1	1	1	1	1	1	1	1	1
Session-Timeout	27	0	UINT32	1	0	0	0	0-1	0	0-1	0	0	0	0	0
Software-Version	1403	10415	UTF8STRING	1	0	0	0	0	0	0	0-1	0	0	0	0
State	24	0	OCTETSTRING	1	0	0-1	0-1	0-1	0	0-1	0-1	0-1	0-1	0	0
Supported-Features	628	10415	GROUPED	1	0	0	0	0	0	0+	0+	0	0	0	0
Terminal-Information	1401	10415	GROUPED	1	0	0	0	0	0	0	0-1	0	0	0	0
Termination-Cause	295	0	ENUM	1	0	0	0	0	0	0	0	0	0	0	1
User-Name	1	0	UTF8STRING	1	0	0	0-1	0	0-1	0-1	0-1	0	0-1	0	0-1
Vendor-Id	266	0	UINT32	1	0	0	0	1	0	1	1	0	0	0	0
Vendor-Specific-QoS-Profile-Template	6064	0	GROUPED	1	0	0	0	0	0+	0	0+	0	0	0	0
Visited-Network-Identifier	600	10415	OCTETSTRING	1	0	0	0	0	0-1	0	0-1	0	0	0	0
VPLMN-Dynamic-Address-Allowed	1432	10415	ENUM	1	0	0	0	0-1	0	0-1	0	0	0	0	0

Gx Dictionary 3GPP 29.212

Attribute	AVP Code	Vendor-Id	AVP Type	M Flag	P Flag	CCA	CCR	RAA	RAR
3GPP2-BSID	9010	5535	OCTETSTRING	1	0	0	0-1	0	0-1
3GPP-MS-TimeZone	23	10415	OCTETSTRING	1	0	0	0-1	0-1	0-1
3GPP-SGSN-Address	6	10415	OCTETSTRING	1	0	0	0-1	0-1	0-1
3GPP-SGSN-IPv6-Address	15	10415	OCTETSTRING	1	0	0	0-1	0-1	0-1
3GPP-SGSN-MCC-MNC	18	10415	UTF8STRING	1	0	0	0-1	0-1	0
3GPP-User-Location-Info	22	10415	UTF8STRING	1	0	0	0-1	0-1	0-1
Access-Network-Charging-Address	501	10415	ADDRESS	1	0	0	0-1	0-1	0
Access-Network-Charging-Identifier-Gx	1022	10415	GROUPED	1	0	0	0+	0+	0
Allocation-Retention-Priority	1034	10415	GROUPED	1	0	0-1	0-1	0	0-1
AN-GW-Address	1050	10415	ADDRESS	1	0	0	0+	0-1	0
APN-Aggregate-Max-Bitrate-DL	1040	10415	UINT32	1	0	0-1	0-1	0	0-1
APN-Aggregate-Max-Bitrate-UL	1041	10415	UINT32	1	0	0-1	0-1	0	0-1
Auth-Application-Id	258	0	UINT32	1	0	1	1	0	1
Bearer-Control-Mode	1023	10415	ENUM	1	0	0-1	0	0	0
Bearer-Identifier	1020	10415	OCTETSTRING	1	0	0-1	0-1	0	0-1
Bearer-Operation	1021	10415	ENUM	1	0	0	0-1	0	0
Bearer-Usage	1000	10415	ENUM	1	0	0	0-1	0	0
Called-Station-Id	30	0	OCTETSTRING	1	0	0	0-1	0	0
CC-Request-Number	415	0	UINT32	1	0	1	1	0	0
CC-Request-Type	416	0	ENUM	1	0	1	1	0	0
Charging-Information	618	10415	GROUPED	1	0	0-1	0	0	0
Charging-Rule-Base-Name	1004	10415	UTF8STRING	1	0	0+	0	0	0+
Charging-Rule-Definition	1003	10415	GROUPED	1	0	0+	0	0	0+
Charging-Rule-Install	1001	10415	GROUPED	1	0	0+	0	0	0+
Charging-Rule-Name	1005	10415	OCTETSTRING	1	0	0+	0	0	0+
Charging-Rule-Remove	1002	10415	GROUPED	1	0	0+	0	0	0+
Charging-Rule-Report	1018	10415	GROUPED	1	0	0	0+	0+	0
CoA-Information	1039	10415	GROUPED	1	0	0	0+	0	0
Default-EPS-Bearer-QoS	1049	10415	GROUPED	1	0	0-1	0-1	0	0-1
Destination-Host	293	0	DIAMIDENT	1	0	0	0-1	0	1
Destination-Realm	283	0	DIAMIDENT	1	0	0	1	0	1
Error-Message	281	0	UTF8STRING	0	0	0-1	0	0-1	0
Error-Reporting-Host	294	0	DIAMIDENT	1	0	0-1	0	0-1	0

Attribute	AVP Code	Vendor-Id	AVP Type	M Flag	P Flag	CCA	CCR	RAA	RAR
Event-Report-Indication	1033	10415	GROUPED	1	0	0	0-1	0	0-1
Event-Trigger	1006	10415	ENUM	1	0	0+	0+	0	0+
Experimental-Result	297	0	GROUPED	1	0	0-1	0	0-1	0
Failed-AVP	279	0	GROUPED	1	0	0+	0	0+	0
Feature-List	630	10415	UINT32	0	0	1	1	1	1
Feature-List-ID	629	10415	UINT32	0	0	1	1	1	1
Flow-Label	1057	10415	OCTETSTRING	1	0	0	0-1	0	0
Framed-IP-Address	8	0	OCTETSTRING	1	0	0	0-1	0	0
Framed-IPv6-Prefix	97	0	OCTETSTRING	1	0	0	0-1	0	0
Granted-Service-Unit	431	0	GROUPED	0	0	0	0	0	0
Guaranteed-Bitrate-DL	1025	10415	UINT32	1	0	0-1	0-1	0	0-1
Guaranteed-Bitrate-UL	1026	10415	UINT32	1	0	0-1	0-1	0	0-1
IP-CAN-Type	1027	10415	ENUM	1	0	0	0-1	0-1	0
Max-Requested-Bandwidth-DL	515	10415	UINT32	1	0	0-1	0-1	0	0-1
Max-Requested-Bandwidth-UL	516	10415	UINT32	1	0	0-1	0-1	0	0-1
Network-Request-Support	1024	10415	ENUM	1	0	0	0-1	0	0
Offline	1008	10415	ENUM	1	0	0-1	0-1	0	0
Online	1009	10415	ENUM	1	0	0-1	0-1	0	0
Origin-Host	264	0	DIAMIDENT	1	0	1	1	1	1
Origin-Realm	296	0	DIAMIDENT	1	0	1	1	1	1
Origin-State-Id	278	0	UINT32	1	0	0-1	0-1	0-1	0-1
Packet-Filter-Content	1059	10415	IPFILTERRULE	1	0	0	0-1	0	0
Packet-Filter-Identifier	1060	10415	OCTETSTRING	1	0	0	0-1	0	0
Packet-Filter-Information	1061	10415	GROUPED	0	0	0	0+	0	0
Packet-Filter-Operation	1062	10415	ENUM	1	0	0	0-1	0	0
Precedence	1010	10415	UINT32	1	0	0	0-1	0-1	0
Proxy-Info	284	0	GROUPED	1	0	0+	0+	0+	0+
QoS-Class-Identifier	1028	10415	ENUM	1	0	0-1	0-1	0	0-1
QoS-Information	1016	10415	GROUPED	1	0	0+	0-1	0	0+
QoS-Negotiation	1029	10415	ENUM	1	0	0	0-1	0	0
QoS-Upgrade	1030	10415	ENUM	1	0	0	0-1	0	0
RAI	909	10415	UTF8STRING	1	0	0	0-1	0-1	0-1
RAT-Type	1032	10415	ENUM	1	0	0	0-1	0-1	0-1
Re-Auth-Request-Type	285	0	ENUM	1	0	0	0	0	1
Redirect-Host	292	0	OCTETSTRING	1	0	0+	0	0	0
Redirect-Host-Usage	261	0	ENUM	1	0	0-1	0	0	0

Attribute	AVP Code	Vendor-Id	AVP Type	M Flag	P Flag	CCA	CCR	RAA	RAR
Redirect-Max-Cache-Time	262	0	UINT32	1	0	0-1	0	0	0
Resource-Allocation-Notification	1063	10415	ENUM	1	0	0-1	0	0	0-1
Result-Code	268	0	ENUM	1	0	0-1	0	0-1	0
Revalidation-Time	1042	10415	TIME	1	0	0-1	0	0	0-1
Route-Record	282	0	DIAMIDENT	1	0	0+	0+	0	0+
Rule-Activation-Time	1043	10415	TIME	1	0	0-1	0	0	0-1
Rule-Deactivation-Time	1044	10415	TIME	1	0	0-1	0	0	0-1
Security-Parameter-Index	1056	10415	OCTETSTRING	1	0	0	0-1	0	0
Session-Id	263	0	UTF8STRING	1	0	1	1	1	1
Session-Release-Cause	1045	10415	ENUM	1	0	0	0	0	0-1
Subscription-Id	443	0	GROUPED	1	0	0	0+	0	0
Supported-Features	628	10415	GROUPED	1	0	0+	0+	0+	0+
Termination-Cause	295	0	ENUM	1	0	0	0-1	0	0
TFT-Filter	1012	10415	IPFILTERRULE	1	0	0	0	0-1	0
TFT-Packet-Filter-Information	1013	10415	GROUPED	1	0	0	0+	0	0
ToS-Traffic-Class	1014	10415	OCTETSTRING	1	0	0	0-1	0-1	0
Trace-Data	1458	10415	GROUPED	1	0	0	0-1	0	0-1
Trace-Reference	1459	10415	OCTETSTRING	1	0	0	0-1	0	0-1
Usage-Monitoring-Information	1067	10415	GROUPED	0	0	0+	0+	0	0+
Used-Service-Unit	446	0	GROUPED	0	0	0	0	0	0
User-Equipment-Info	458	0	GROUPED	1	0	0	0-1	0	0
Vendor-Id	266	0	UINT32	1	0	1	1	1	1

Gxa Dictionary 3GPP 29.212

Attribute	AVP Code	Vendor-Id	AVP Type	M Flag	P Flag	CCA	CCR	RAA	RAR
3GPP2-BSID	9010	5535	OCTETSTRING	1	0	0	0-1	0-1	0
3GPP-MS-TimeZone	23	10415	OCTETSTRING	1	0	0	0	0-1	0
3GPP-SGSN-Address	6	10415	OCTETSTRING	1	0	0	0	0-1	0
3GPP-SGSN-IPv6-Address	15	10415	OCTETSTRING	1	0	0	0	0-1	0
3GPP-SGSN-MCC-MNC	18	10415	UTF8STRING	1	0	0	0-1	0-1	0
3GPP-User-Location-Info	22	10415	UTF8STRING	1	0	0	0	0-1	0
Allocation-Retention-Priority	1034	10415	GROUPED	1	0	0-1	0-1	0	0-1
APN-Aggregate-Max-Bitrate-DL	1040	10415	UINT32	1	0	0-1	0-1	0	0-1
APN-Aggregate-Max-Bitrate-UL	1041	10415	UINT32	1	0	0-1	0-1	0	0-1
Auth-Application-Id	258	0	UINT32	1	0	1	1	0	1
Bearer-Control-Mode	1023	10415	ENUM	1	0	0-1	0	0	0
Called-Station-Id	30	0	OCTETSTRING	1	0	0	0-1	0	0
CC-Request-Number	415	0	UINT32	1	0	1	1	0	0
CC-Request-Type	416	0	ENUM	1	0	1	1	0	0
Default-EPS-Bearer-QoS	1049	10415	GROUPED	1	0	0-1	0-1	0	0-1
Destination-Host	293	0	DIAMIDENT	1	0	0	0-1	0	1
Destination-Realm	283	0	DIAMIDENT	1	0	0	1	0	1
Error-Message	281	0	UTF8STRING	0	0	0-1	0	0-1	0
Error-Reporting-Host	294	0	DIAMIDENT	1	0	0-1	0	0-1	0
Event-Trigger	1006	10415	ENUM	1	0	0+	0+	0	0+
Experimental-Result	297	0	GROUPED	1	0	0-1	0	0-1	0
Failed-AVP	279	0	GROUPED	1	0	0+	0	0+	0
Feature-List	630	10415	UINT32	0	0	1	1	1	1
Feature-List-ID	629	10415	UINT32	0	0	1	1	1	1
Framed-IP-Address	8	0	OCTETSTRING	1	0	0	0-1	0	0
Framed-IPv6-Prefix	97	0	OCTETSTRING	1	0	0	0-1	0	0
Guaranteed-Bitrate-DL	1025	10415	UINT32	1	0	0-1	0-1	0	0-1
Guaranteed-Bitrate-UL	1026	10415	UINT32	1	0	0-1	0-1	0	0-1
IP-CAN-Type	1027	10415	ENUM	1	0	0	0-1	0	0
Max-Requested-Bandwidth-DL	515	10415	UINT32	1	0	0-1	0-1	0	0-1
Max-Requested-Bandwidth-UL	516	10415	UINT32	1	0	0-1	0-1	0	0-1
Network-Request-Support	1024	10415	ENUM	1	0	0	0-1	0	0
Origin-Host	264	0	DIAMIDENT	1	0	1	1	1	1

Attribute	AVP Code	Vendor-Id	AVP Type	M Flag	P Flag	CCA	CCR	RAA	RAR
Origin-Realm	296	0	DIAMIDENT	1	0	1	1	1	1
Origin-State-Id	278	0	UINT32	1	0	0-1	0-1	0-1	0-1
Precedence	1010	10415	UINT32	1	0	0-1	0-1	0	0-1
Proxy-Info	284	0	GROUPED	1	0	0+	0+	0+	0+
QoS-Class-Identifier	1028	10415	ENUM	1	0	0-1	0-1	0	0-1
QoS-Information	1016	10415	GROUPED	1	0	0+	0-1	0	0+
QoS-Rule-Install	1051	10415	GROUPED	1	0	0+	0	0	0+
QoS-Rule-Remove	1052	10415	GROUPED	1	0	0+	0	0	0+
QoS-Rule-Report	1055	10415	GROUPED	1	0	0	0+	0+	0
RAI	909	10415	UTF8STRING	1	0	0	0	0-1	0
RAT-Type	1032	10415	ENUM	1	0	0	0-1	0-1	0
Re-Auth-Request-Type	285	0	ENUM	1	0	0	0	0	1
Redirect-Host	292	0	OCTETSTRING	1	0	0+	0	0	0
Redirect-Host-Usage	261	0	ENUM	1	0	0-1	0	0	0
Redirect-Max-Cache-Time	262	0	UINT32	1	0	0-1	0	0	0
Result-Code	268	0	ENUM	1	0	0-1	0	0-1	0
Route-Record	282	0	DIAMIDENT	1	0	0+	0+	0	0+
Session-Id	263	0	UTF8STRING	1	0	1	1	1	1
Session-Linking-Indicator	1064	10415	ENUM	1	0	0	0-1	0	0
Session-Release-Cause	1045	10415	ENUM	1	0	0	0	0	0-1
Subscription-Id	443	0	GROUPED	1	0	0	0+	0	0
Supported-Features	628	10415	GROUPED	0	0	0+	0+	0+	0+
TFT-Filter	1012	10415	IPFILTERRULE	1	0	0-1	0-1	0	0-1
TFT-Packet-Filter-Information	1013	10415	GROUPED	1	0	0	0+	0	0
ToS-Traffic-Class	1014	10415	OCTETSTRING	1	0	0-1	0-1	0	0-1
User-Equipment-Info	458	0	GROUPED	1	0	0	0-1	0	0
Vendor-Id	266	0	UINT32	1	0	1	1	1	1

Gxc Dictionary 3GPP 29.212

Attribute	AVP Code	Vendor-Id	AVP Type	M Flag	P Flag	CCA	CCR	RAA	RAR
3GPP2-BSID	9010	5535	OCTETSTRING	1	0	0	0-1	0-1	0
3GPP-MS-TimeZone	23	10415	OCTETSTRING	1	0	0	0-1	0-1	0
3GPP-SGSN-Address	6	10415	OCTETSTRING	1	0	0	0-1	0-1	0
3GPP-SGSN-IPv6-Address	15	10415	OCTETSTRING	1	0	0	0-1	0-1	0
3GPP-SGSN-MCC-MNC	18	10415	UTF8STRING	1	0	0	0-1	0-1	0
3GPP-User-Location-Info	22	10415	UTF8STRING	1	0	0	0	0-1	0
Access-Network-Charging-Address	501	10415	ADDRESS	1	0	0	0-1	0-1	0
Access-Network-Charging-Identifier-Gx	1022	10415	GROUPED	1	0	0	0+	0+	0
AN-GW-Address	1050	10415	ADDRESS	1	0	0	0-1	0	0
Auth-Application-Id	258	0	UINT32	1	0	1	1	0	1
Called-Station-Id	30	0	OCTETSTRING	1	0	0	0-1	0	0
CC-Request-Number	415	0	UINT32	1	0	1	1	0	0
CC-Request-Type	416	0	ENUM	1	0	1	1	0	0
Charging-Information	618	10415	GROUPED	1	0	0-1	0	0	0
Default-EPS-Bearer-QoS	1049	10415	GROUPED	1	0	0-1	0-1	0	0-1
Destination-Host	293	0	DIAMIDENT	1	0	0	0-1	0	1
Destination-Realm	283	0	DIAMIDENT	1	0	0	1	0	1
Error-Message	281	0	UTF8STRING	0	0	0-1	0	0-1	0
Error-Reporting-Host	294	0	DIAMIDENT	1	0	0-1	0	0-1	0
Event-Trigger	1006	10415	ENUM	1	0	0+	0+	0	0+
Experimental-Result	297	0	GROUPED	1	0	0-1	0	0-1	0
Failed-AVP	279	0	GROUPED	1	0	0+	0	0+	0
Framed-IP-Address	8	0	OCTETSTRING	1	0	0	0-1	0	0
Framed-IPv6-Prefix	97	0	OCTETSTRING	1	0	0	0-1	0	0
IP-CAN-Type	1027	10415	ENUM	1	0	0	0-1	0	0
Origin-Host	264	0	DIAMIDENT	1	0	1	1	1	1
Origin-Realm	296	0	DIAMIDENT	1	0	1	1	1	1
Origin-State-Id	278	0	UINT32	1	0	0-1	0-1	0-1	0-1
Proxy-Info	284	0	GROUPED	1	0	0+	0+	0+	0+
QoS-Information	1016	10415	GROUPED	1	0	0+	0-1	0	0+
QoS-Resource-Request	6106	10415	GROUPED	1	0	0	0-1	0	0
QoS-Rule-Install	1051	10415	GROUPED	1	0	0+	0	0	0+
QoS-Rule-Remove	1052	10415	GROUPED	1	0	0+	0	0	0+

Attribute	AVP Code	Vendor-Id	AVP Type	M Flag	P Flag	CCA	CCR	RAA	RAR
QoS-Rule-Report	1055	10415	GROUPED	1	0	0	0+	0+	0
RAI	909	10415	UTF8STRING	1	0	0	0	0-1	0
RAT-Type	1032	10415	ENUM	1	0	0	0-1	0-1	0
Re-Auth-Request-Type	285	0	ENUM	1	0	0	0	0	1
Redirect-Host	292	0	OCTETSTRING	1	0	0+	0	0	0
Redirect-Host-Usage	261	0	ENUM	1	0	0-1	0	0	0
Redirect-Max-Cache-Time	262	0	UINT32	1	0	0-1	0	0	0
Result-Code	268	0	ENUM	1	0	0-1	0	0-1	0
Route-Record	282	0	DIAMIDENT	1	0	0+	0+	0	0+
Session-Id	263	0	UTF8STRING	1	0	1	1	1	1
Session-Linking-Indicator	1064	10415	ENUM	1	0	0	0-1	0	0
Session-Release-Cause	1045	10415	ENUM	1	0	0	0	0	0-1
Subscription-Id	443	0	GROUPED	1	0	0	0+	0	0
Supported-Features	628	10415	GROUPED	1	0	0+	0+	0+	0+
Termination-Cause	295	0	ENUM	1	0	0	0-1	0	0
TFT-Packet-Filter-Information	1013	10415	GROUPED	1	0	0	0+	0	0
User-Equipment-Info	458	0	GROUPED	1	0	0	0-1	0	0

Standard Rf Dictionary

Attribute	AVP Code	Vendor-Id	AVP Type	M Flag	P Flag	AA	AR
3GPP2-BSID	9010	5535	OCTETSTRING	1	0	0	0-1
3GPP-Charging-Characteristics	13	10415	UTF8STRING	1	0	0	0-1
3GPP-Charging-Id	2	10415	OCTETSTRING	1	0	0	0-1
3GPP-GGSN-MCC-MNC	9	10415	UTF8STRING	1	0	0	0-1
3GPP-IMSI-MCC-MNC	8	10415	UTF8STRING	1	0	0	0-1
3GPP-MS-TimeZone	23	10415	OCTETSTRING	1	0	0	0-1
3GPP-PDP-Type	3	10415	ENUM	1	0	0	0-1
3GPP-RAT-Type	21	10415	OCTETSTRING	1	0	0	0-1
3GPP-Selection-Mode	12	10415	UTF8STRING	1	0	0	0-1
3GPP-SGSN-MCC-MNC	18	10415	UTF8STRING	1	0	0	0-1
3GPP-User-Location-Info	22	10415	OCTETSTRING	1	0	0	0-1
Accounting-Record-Number	485	0	UINT32	1	0	1	1
Accounting-Record-Type	480	0	ENUM	1	0	1	1
Acct-Application-Id	259	0	UINT32	1	0	0-1	0-1
Acct-Interim-Interval	85	0	UINT32	1	0	0-1	0-1
AF-Correlation-Information	1276	10415	GROUPED	1	0	0	0
Called-Station-Id	30	10415	UTF8STRING	1	0	0	0-1
Change-Condition	2037	10415	ENUM	1	0	0	0-1
Destination-Host	293	0	DIAMIDENT	1	0	0	0-1
Destination-Realm	283	0	DIAMIDENT	1	0	0	1
Diagnostics	2039	10415	ENUM	1	0	0	0-1
Dynamic-Address-Flag	2051	10415	ENUM	1	0	0	0-1
Error-Reporting-Host	294	0	DIAMIDENT	1	0	0-1	0
Event-Timestamp	55	0	TIME	1	0	0-1	0-1
GGSN-Address	847	10415	ADDRESS	1	0	0	0-1
IMS-Information	876	10415	GROUPED	1	0	0	0-1
Node-Functionality	862	10415	ENUM	1	0	0	1
Node-Id	2064	10415	UTF8STRING	1	0	0	0-1
Origin-Host	264	0	DIAMIDENT	1	0	1	1
Origin-Realm	296	0	DIAMIDENT	1	0	1	1
Origin-State-Id	278	0	UINT32	1	0	0-1	0-1
PDP-Address	1227	10415	ADDRESS	1	0	0	0+
Proxy-Info	284	0	GROUPED	1	0	0+	0+

Attribute	AVP Code	Vendor-Id	AVP Type	M Flag	P Flag	AA	AR
PS-Information	874	10415	GROUPED	1	0	0	0-1
Result-Code	268	0	ENUM	1	0	1	0
Route-Record	282	0	DIAMIDENT	1	0	0+	0+
Service-Context-Id	461	0	UTF8STRING	1	0	0	0-1
Service-Data-Container	2040	10415	GROUPED	1	0	0	0+
Service-Information	873	10415	GROUPED	1	0	0	0-1
Service-Specific-Info	1249	10415	GROUPED	1	0	0	0
Serving-Node-Type	2047	10415	ENUM	1	0	0	0-1
Session-Id	263	0	UTF8STRING	1	0	1	1
SGSN-Address	1228	10415	ADDRESS	1	0	0	0-1
SGW-Change	2065	10415	ENUM	1	0	0	0-1
Start-Time	2041	10415	TIME	1	0	0	0-1
Stop-Time	2042	10415	TIME	1	0	0	0-1
Subscription-Id	443	0	GROUPED	1	0	0	0+
Traffic-Data-Volumes	2046	10415	GROUPED	1	0	0	0+
User-Equipment-Info	458	0	GROUPED	1	0	0	0-1
User-Name	1	0	UTF8STRING	1	0	0-1	0-1

ETSI-E2 Dictionary for CSCF

Attribute	AVP Code	Vendor-Id	AVP Type	M Flag	P Flag	UDA	UDR
Access-Network-Type	306	0	GROUPED	1	0	0-1	0
AF-Application-Identifier	504	10415	OCTETSTRING	1	0	0	0-1
Auth-Session-State	277	0	ENUM	1	0	1	1
Destination-Host	293	0	DIAMIDENT	1	0	0	0-1
Destination-Realm	283	0	DIAMIDENT	1	0	0	1
Experimental-Result	297	0	GROUPED	1	0	0-1	0
Failed-AVP	279	0	GROUPED	1	0	0+	0
Globally-Unique-Address	300	13019	GROUPED	1	0	0	0-1
Location-Information	350	13019	GROUPED	1	0	0-1	0
Logical-Access-Id	302	0	OCTETSTRING	1	0	0-1	0
Origin-Host	264	0	DIAMIDENT	1	0	1	1
Origin-Realm	296	0	DIAMIDENT	1	0	1	1
Physical-Access-Id	313	0	UTF8STRING	1	0	0-1	0
Proxy-Info	284	0	GROUPED	1	0	0+	0+
RACS-Contact-Point	351	0	DIAMIDENT	1	0	0-1	0
Requested-Information	353	13019	ENUM	1	0	0	0-1
Result-Code	268	0	ENUM	1	0	0-1	0
Route-Record	282	0	DIAMIDENT	1	0	0+	0+
Session-Id	263	0	UTF8STRING	1	0	1	1
Terminal-Type	352	13019	OCTETSTRING	1	0	0-1	0
User-Name	1	0	UTF8STRING	1	0	0-1	0-1
Vendor-Specific-Application-Id	260	0	GROUPED	1	0	1	1

STa Dictionary 3GPP 29.273

Attribute	AVP Code	Vendor-Id	AVP Type	M Flag	P Flag	ASA	ASR	AAA	AAR	DEA	DER	RAA	RAR	STA	STR
3GPP-Charging-Characteristics	13	10415	UTF8STRING	1	0	0	0	0-1	0	0-1	0	0	0	0	0
Acct-Interim-Interval	85	0	UINT32	0	0	0	0	0-1	0	0-1	0	0	0	0	0
Allocation-Retention-Priority	1034	10415	GROUPED	1	0	0	0	1	0	1	0	0	0	0	0
AMBR	1435	10415	GROUPED	1	0	0	0	0-1	0	0-1	0	0	0	0	0
ANID	1504	10415	UTF8STRING	1	0	0	0	0	0	0	0-1	0	0	0	0
AN-Trusted	1503	10415	ENUM	1	0	0	0	0	0	0	0-1	0	0	0	0
APN-Configuration	1430	10415	GROUPED	1	0	0	0	0+	0	0+	0	0	0	0	0
APN-OI-Replacement	1427	10415	UTF8STRING	1	0	0	0	0-1	0	0-1	0	0	0	0	0
Auth-Application-Id	258	0	UINT32	1	0	0	1	1	1	1	1	0	1	0	1
Auth-Grace-Period	276	0	UINT32	1	0	0	0	0-1	0-1	0-1	0-1	0	0	0	0
Authorization-Lifetime	291	0	UINT32	1	0	0	0	0-1	0-1	0-1	0-1	0	0	0	0
Auth-Request-Type	274	0	ENUM	1	0	0	0	1	1	1	1	0	0	0	0
Auth-Session-State	277	0	ENUM	1	0	0	0	0-1	0-1	0-1	0-1	0	0	0	0
Calling-Station-Id	31	0	UTF8STRING	1	0	0	0	0	0	0	0-1	0	0	0	0
Class	25	0	OCTETSTRING	1	0	0	0+	0+	0	0+	0	0+	0+	0+	0+
Context-Identifier	1423	10415	UINT32	1	0	0	0	0-1	0	0-1	0	0	0	0	0
Destination-Host	293	0	DIAMIDENT	1	0	0	1	1	0-1	1	0-1	0	1	0	0-1
Destination-Realm	283	0	DIAMIDENT	1	0	0	1	1	1	1	1	0	1	0	1
EAP-Master-Session-Key	464	0	OCTETSTRING	1	0	0	0	0	0	0-1	0	0	0	0	0
EAP-Payload	462	0	OCTETSTRING	1	0	0	0	0	0	1	1	0	0	0	0
EPS-Subscribed-QoS-Profile	1431	10415	GROUPED	1	0	0	0	0-1	0	0-1	0	0	0	0	0
Error-Message	281	0	UTF8STRING	0	0	0-1	0	0-1	0	0-1	0	0-1	0	0-1	0
Error-Reporting-Host	294	0	DIAMIDENT	1	0	0-1	0	0-1	0	0-1	0	0-1	0	0-1	0
ESN	6109	10415	OCTETSTRING	1	0	0	0	0	0	0	0-1	0	0	0	0
Experimental-Result	297	0	GROUPED	1	0	0	0	0-1	0	0-1	0	0	0	0	0
Experimental-Result-Code	298	0	ENUM	1	0	0	0	1	0	1	0	0	0	0	0
Failed-AVP	279	0	GROUPED	1	0	0+	0	0+	0	0+	0	0+	0	0+	0
Feature-List	630	10415	UINT32	0	0	0	0	0	0	1	1	0	0	0	0
Feature-List-ID	629	10415	UINT32	0	0	0	0	0	0	1	1	0	0	0	0
Idle-Timeout	28	0	UINT32	1	0	0	0	0-1	0	0-1	0	0	0	0	0
IMEI	1402	10415	UTF8STRING	1	0	0	0	0	0	0	0-1	0	0	0	0
IP-MMS	6076	10415	UINT32	1	0	0	0	0	0	0-1	0	0	0	0	0
Max-Requested-Bandwidth-DL	515	10415	UINT32	1	0	0	0	1	0	1	0	0	0	0	0
Max-Requested-Bandwidth-UL	516	10415	UINT32	1	0	0	0	1	0	1	0	0	0	0	0
MEID	6110	10415	OCTETSTRING	1	0	0	0	0	0	0	0-1	0	0	0	0
MIP6-Agent-Info	486	0	GROUPED	1	0	0	0	0-1	0	0-1	0	0	0	0	0
MIP6-Feature-Vector	124	0	UINT64	1	0	0	0	0	0	0-1	0-1	0	0	0	0
MIP6-Home-Link-Prefix	125	0	OCTETSTRING	1	0	0	0	0-1	0	0-1	0	0	0	0	0
MIP-Home-Agent-Address-IETF	334	0	ADDRESS	1	0	0	0	0+	0	0+	0	0	0	0	0
MIP-Home-Agent-Host	348	0	GROUPED	1	0	0	0	0-1	0	0-1	0	0	0	0	0
Mobile-Node-Identifier	89	0	OCTETSTRING	1	0	0	0	0	0	0-1	0	0	0	0	0
Multi-Round-Time-Out	272	0	UINT32	0	0	0	0	0	0	0-1	0	0	0	0	0
Origin-Host	264	0	DIAMIDENT	1	0	1	1	1	1	1	1	1	1	1	1
Origin-Realm	296	0	DIAMIDENT	1	0	1	1	1	1	1	1	1	1	1	1
Origin-State-Id	278	0	UINT32	1	0	0-1	0-1	0-1	0-1	0-1	0-1	0-1	0-1	0-1	0-1

Attribute	AVP Code	Vendor-Id	AVP Type	M Flag	P Flag	ASA	ASR	AAA	AAR	DEA	DER	RAA	RAR	STA	STR
PDN-GW-Allocation-Type	1438	10415	ENUM	1	0	0	0	0-1	0	0-1	0	0	0	0	0
PDN-Type	1456	10415	ENUM	1	0	0	0	1	0	1	0	0	0	0	0
Proxy-Host	280	0	DIAMIDENT	1	0	1	1	1	1	1	1	1	1	1	1
Proxy-Info	284	0	GROUPED	1	0	0+	0+	0+	0+	0+	0+	0+	0+	0+	0+
Proxy-State	33	0	OCTETSTRING	1	0	1	1	1	1	1	1	1	1	1	1
QoS-Capability	6063	0	GROUPED	1	0	0	0	0	0-1	0	0-1	0	0	0	0
QoS-Class-Identifier	1028	10415	ENUM	1	0	0	0	1	0	1	0	0	0	0	0
QoS-Profile-Template	6067	0	UINT32	1	0	0	0	0	0+	0	0+	0	0	0	0
RAT-Type	1032	10415	ENUM	1	0	0	0	0	0-1	0	0-1	0	0	0	0
Re-Auth-Request-Type	285	0	ENUM	1	0	0	0	0	0	0	0	0	1	0	0
Redirect-Host	292	0	OCTETSTRING	1	0	0+	0	0+	0	0+	0	0+	0	0+	0
Redirect-Host-Usage	261	0	ENUM	1	0	0-1	0	0-1	0	0-1	0	0-1	0	0-1	0
Redirect-Max-Cache-Time	262	0	UINT32	1	0	0-1	0	0-1	0	0-1	0	0-1	0	0-1	0
Reply-Message	18	0	UTF8STRING	1	0	0	0+	0	0	0	0	0	0	0	0
Result-Code	268	0	ENUM	1	0	1	0	0-1	0	0-1	0	1	0	1	0
Route-Record	282	0	DIAMIDENT	1	0	0	0+	0	0+	0	0+	0	0+	0	0+
Served-Party-IP-Address	848	10415	ADDRESS	1	0	0	0	0-1	0	0-1	0	0	0	0	0
Service-Selection	493	0	OCTETSTRING	1	0	0	0	1	0	1	0-1	0	0	0	0
Session-Id	263	0	UTF8STRING	1	0	1	1	1	1	1	1	1	1	1	1
Session-Timeout	27	0	UINT32	1	0	0	0	0-1	0	0-1	0	0	0	0	0
Software-Version	1403	10415	UTF8STRING	1	0	0	0	0	0	0	0-1	0	0	0	0
State	24	0	OCTETSTRING	1	0	0-1	0-1	0-1	0	0-1	0-1	0-1	0-1	0	0
Supported-Features	628	10415	GROUPED	1	0	0	0	0	0	0+	0+	0	0	0	0
Terminal-Information	1401	10415	GROUPED	1	0	0	0	0	0	0	0-1	0	0	0	0
Termination-Cause	295	0	ENUM	1	0	0	0	0	0	0	0	0	0	0	1
User-Name	1	0	UTF8STRING	1	0	0	0-1	0	0-1	0-1	0-1	0	0-1	0	0-1
Vendor-Id	266	0	UINT32	1	0	0	0	1	0	1	0	0	0	0	0
Vendor-Specific-QoS-Profile-Template	6064	0	GROUPED	1	0	0	0	0	0+	0	0+	0	0	0	0
Visited-Network-Identifier	600	10415	OCTETSTRING	1	0	0	0	0	0-1	0	0-1	0	0	0	0
VPLMN-Dynamic-Address-Allowed	1432	10415	ENUM	1	0	0	0	0-1	0	0-1	0	0	0	0	0

Appendix E
RADIUS Attribute Quick Reference

This appendix presents RADIUS attribute quick reference tables listing RADIUS attributes and their relationships to generated RADIUS packets and the dictionaries to which they belong.

The following table describes the indicators used in the quick reference table.

Entry	Description
0	The AVP MUST NOT be present in the message.
0-1	Zero or one instance of the AVP MAY be present in the message. If there are more than one instance of the AVP, it is considered an error.
0+	Zero or more instances of the AVP MAY be present in the message.
1	One instance of the AVP MUST be present in the message.

Attributes not listed in a particular table do not appear in RADIUS packets generated for a session of the corresponding service.

Management Attribute/Packet Table

Attribute	MGMT Access-Request	MGMT Access-Reject	MGMT Access-Accept	MGMT Acct-Request-Start	MGMT Acct-Request-Interim	MGMT Acct-Request-Stop
3GPP2-DNS-Server-IPV6-Addr	0	0	0-1	0	0	0
3GPP2-ESN	1	0	0	0	0	0
Acct-Authentic	0	0	0	1	1	1
Acct-Interim-Interval	0	0	0-1	0	0	0
Acct-Session-Id	0	0	0	1	1	1
Callback-Id	0	0-1	0-1	0	0	0
Class	0	0	0-1	0-1	0-1	0-1
EAP-Message	0+	1	0+	0	0	0
Error-Cause	0	0-1	0	0	0	0
Framed-IPv6-Prefix	0	0	0	0	0+	0+
Idle-Timeout	0	0	0-1	0	0	0
NAS-Port	1	0	0	1	1	1
NAS-Port-Type	1	0	0	1	1	1
Reply-Message	0	0-1	0-1	0	0	0
Service-Type	1	0	0-1	1	1	1
Session-Timeout	0	0	0-1	0	0	0
SN1-Admin-Expiry	0	0	0-1	0	0	0
SN1-Admin-Permission	0	0	0-1	0	0	0
SN1-DHCP-Lease-Expiry-Policy	0	0	0-1	0	0	0
SN1-Disconnect-Reason	0	0	0	0	0	1
SN1-DNS-Proxy-Intercept-List	0	0	1	0	0	0
SN1-DNS-Proxy-Use-Subscr-Addr	0	0	1	0	0	0
SN1-Enable-QoS-Renegotiation	0	0	0-1	0	0	0
SN1-Long-Duration-Action	0	0	0-1	0	0	0
SN1-Long-Duration-Notification	0	0	0-1	0	0	0
SN1-Long-Duration-Timeout	0	0	0-1	0	0	0
SN1-MIP-HA-Assignment-Table	0	0	1	0	0	0
SN1-Overload-Disc-Connect-Time	0	0	0-1	0	0	0
SN1-Overload-Disc-Inact-Time	0	0	0-1	0	0	0
SN1-Overload-Disconnect	0	0	0-1	0	0	0
SN1-QoS-Renegotiation-Timeout	0	0	0-1	0	0	0
SN1-Rulebase	0	0	0-1	1	1	1
SN1-Subscriber-Accounting	0	0	0-1	1	1	1
SN1-Subscriber-Acct-Interim	0	0	0-1	0	0	0
SN1-Subscriber-Acct-Mode	0	0	0-1	0	0	0
SN1-Subscriber-Acct-Rsp-Action	0	0	0-1	0	0	0
SN1-Subscriber-Acct-Start	0	0	0-1	0	0	0
SN1-Subscriber-Acct-Stop	0	0	0-1	0	0	0
SN1-Subscriber-Class	0	0	0-1	0-1	0-1	0-1
SN1-Subscriber-Nexthop-Address	0	0	0-1	1	1	1
SN1-Subscriber-No-Interims	0	0	0-1	0	0	0
SN1-Subscriber-Permission	0	0	0-1	0	0	0
SN-Acs-Credit-Control-Group	0	0	0-1	0-1	0-1	0-1

Attribute	MGMT Access-Request	MGMT Access-Reject	MGMT Access-Accept	MGMT Acct-Request-Start	MGMT Acct-Request-Interim	MGMT Acct-Request-Stop
SN-Admin-Expiry	0	0	0-1	0	0	0
SN-Admin-Permission	0	0	0-1	0	0	0
SN-DHCP-Lease-Expiry-Policy	0	0	0-1	0	0	0
SN-Disconnect-Reason	0	0	0	0	0	1
SN-DNS-Proxy-Intercept-List	0	0	1	0	0	0
SN-DNS-Proxy-Use-Subscr-Addr	0	0	1	0	0	0
SN-Enable-QoS-Renegotiation	0	0	0-1	0	0	0
SN-Fast-Reauth-Username	0	0	0-1	0	0	0
SN-Long-Duration-Action	0	0	0-1	0	0	0
SN-Long-Duration-Notification	0	0	0-1	0	0	0
SN-Long-Duration-Timeout	0	0	0-1	0	0	0
SN-MIP-HA-Assignment-Table	0	0	1	0	0	0
SN-Overload-Disc-Connect-Time	0	0	0-1	0	0	0
SN-Overload-Disc-Inact-Time	0	0	0-1	0	0	0
SN-Overload-Disconnect	0	0	0-1	0	0	0
SN-Pseudonym-Username	0	0	0-1	0	0	0
SN-QoS-Renegotiation-Timeout	0	0	0-1	0	0	0
SN-Rulebase	0	0	0-1	1	1	1
SN-Subscriber-Accounting	0	0	0-1	1	1	1
SN-Subscriber-Acct-Interim	0	0	0-1	0	0	0
SN-Subscriber-Acct-Mode	0	0	0-1	0	0	0
SN-Subscriber-Acct-Rsp-Action	0	0	0-1	0	0	0
SN-Subscriber-Acct-Start	0	0	0-1	0	0	0
SN-Subscriber-Acct-Stop	0	0	0-1	0	0	0
SN-Subscriber-Class	0	0	0-1	0-1	0-1	0-1
SN-Subscriber-Nexthop-Address	0	0	0-1	1	1	1
SN-Subscriber-No-Interims	0	0	0-1	0	0	0
SN-Subscriber-Permission	0	0	0-1	0	0	0
State	1	0	0-1	0	0	0
User-Name	1	0	0-1	1	1	1
User-Password	1	0	0	0	0	0
WiMAX-Home-HNP-PMIP6	0	0	0	0	0+	0+

PSDN or FA Attribute/Packet Table

Attribute	PDSN or FA Access-Request	PDSN or FA Access-Reject	PDSN or FA Access-Accept	PDSN or FA Acct-Request-Start	PDSN or FA Acct-Request-Interim	PDSN or FA Acct-Request-Stop
3GPP2-Active-Time	0	0	0	1	1	1
3GPP2-Airlink-Record-Type	0	0	0	1	1	1
3GPP2-Airlink-Sequence-Number	0	0	0	1	1	1
3GPP2-Air-QOS	0	0	0	1	1	1
3GPP2-Allowed-Persistent-TFTs	0	0-1	0-1	0	0	0
3GPP2-Always-On	0	0	0-1	0-1	0-1	0-1
3GPP2-Bad-PPP-Frame-Count	0	0	0	1	1	1
3GPP2-BCMCS-Flow-ID	0-1	0	0	1	1	1
3GPP2-BCMCS-Flow-Transmit-Time	0	0	0	1	1	1
3GPP2-BCMCS-Mcast-IP-Addr	0	0	0-1	1	0	1
3GPP2-BCMCS-Mcast-Port	0	0	0-1	1	0	1
3GPP2-BCMCS-Reason-Code	1	0	0	0	0	0
3GPP2-Beginning-Session	0	0	0	1	0	0
3GPP2-BSID	1	0	0	1	1	1
3GPP2-Comp-Tunnel-Indicator	0	0	0	1	1	1
3GPP2-Correlation-Id	1	0	0	1	1	1
3GPP2-DCCH-Frame-Size	0	0	0	1	1	1
3GPP2-DNS-Server-IPV6-Addr	0	0	0-1	0	0	0
3GPP2-ESN	1	0	0	1	1	1
3GPP2-FA-Address	0-1	0	0	0-1	0-1	0-1
3GPP2-FEID	0	0	0	1	1	1
3GPP2-Flow-Status	0	0	0	0	0	0-1
3GPP2-Forward-Fundamental-Rate	0	0	0	1	1	1
3GPP2-Forward-Fundamental-RC	0	0	0	1	1	1
3GPP2-Forward-Mux-Option	0	0	0	1	1	1
3GPP2-Forward-Traffic-Type	0	0	0	1	1	1
3GPP2-Fundamental-Frame-Size	0	0	0	1	1	1
3GPP2-Fwd-Dcch-Mux-Option	0	0	0	0-1	0-1	0-1
3GPP2-Fwd-Dcch-Rc	0	0	0	0-1	0-1	0-1
3GPP2-Fwd-Pdch-Rc	0	0	0	0-1	0-1	0-1
3GPP2-IKE-Secret	0	0	0-1	0	0	0
3GPP2-IKE-Secret-Request	0-1	0	0	0	0	0
3GPP2-Inter-User-Priority	0	0-1	0-1	0	0	0
3GPP2-IP-QOS	0	0	0-1	1	1	1
3GPP2-IP-Services-Authorized	0	0-1	0-1	0	0	0
3GPP2-IP-Technology	0-1	0	0-1	1	1	1
3GPP2-KeyID	0	0	0-1	0	0	0
3GPP2-Last-Activity	0	0	0	0	0-1	1
3GPP2-Max-Auth-Aggr-Bw-BET	0	0-1	0-1	0	0	0
3GPP2-Max-Per-Fl-Pri-ForTheUser	0	0-1	0-1	0	0	0
3GPP2-MEID	1	0	0	1	1	1
3GPP2-MIP6-Home-Address	0	0	0-1	0	0	0
3GPP2-MIP6-Home-Agent	0	0	0-1	0	0	0

Attribute	PDSN or FA Access-Request	PDSN or FA Access-Reject	PDSN or FA Access-Accept	PDSN or FA Acct-Request-Start	PDSN or FA Acct-Request-Interim	PDSN or FA Acct-Request-Stop
3GPP2-MIP6-Home-Link-Prefix	0	0	0-1	0	0	0
3GPP2-MIP-HA-Address	1	0	0+	1	1	1
3GPP2-MIP-Rev-Tunnel-Required	0	0	0-1	0	0	0
3GPP2-MIP-Sig-Octet-Count-In	0	0	0	1	1	1
3GPP2-MIP-Sig-Octet-Count-Out	0	0	0	1	1	1
3GPP2-MN-AAA-Removal-Indication	0	0	0-1	0	0	0
3GPP2-MN-HA-SPI	0-1	0	0	0	0	0
3GPP2-Mobile-Term-Orig-Ind	0	0	0	1	1	1
3GPP2-Number-Active-Transitions	0	0	0	1	1	1
3GPP2-Num-Bytes-Received-Total	0	0	0	1	1	1
3GPP2-Num-SDB-Input	0	0	0	1	1	1
3GPP2-Num-SDB-Output	0	0	0	1	1	1
3GPP2-PMIP-Capability	0-1	0	0	0-1	0-1	0-1
3GPP2-PMIP-IPv4Session-Info	0-1	0	0-1	0-1	0-1	0-1
3GPP2-PMIP-IPv6Session-Info	0-1	0	0-1	0-1	0-1	0-1
3GPP2-PMIP-NAI	0	0	0-1	0-1	0-1	0-1
3GPP2-Release-Indicator-Prepaid	0-1	0	0-1	0-1	0-1	0-1
3GPP2-Rev-Dcch-Mux-Option	0	0	0	0-1	0-1	0-1
3GPP2-Rev-Dcch-Rc	0	0	0	0-1	0-1	0-1
3GPP2-Reverse-Fundamental-Rate	0	0	0	1	1	1
3GPP2-Reverse-Fundamental-RC	0	0	0	1	1	1
3GPP2-Reverse-Mux-Option	0	0	0	1	1	1
3GPP2-Reverse-Traffic-Type	0	0	0	1	1	1
3GPP2-Rev-Pdch-Rc	0	0	0	0-1	0-1	0-1
3GPP2-RP-Session-ID	1	0	0	1	1	1
3GPP2-Rsvp-Signal-In-Count	0	0	0	0	0-1	0-1
3GPP2-Rsvp-Signal-In-Packets	0	0	0	0	0-1	0-1
3GPP2-Rsvp-Signal-Out-Count	0	0	0	0	0-1	0-1
3GPP2-Rsvp-Signal-Out-Packets	0	0	0	0	0-1	0-1
3GPP2-SDB-Output-Octets	0	0	0	1	1	1
3GPP2-Security-Level	0	0	0-1	0	0	0
3GPP2-Service-Option	0-1	0-1	0-1	1	1	1
3GPP2-Serving-PCF	1	0	0	1	1	1
3GPP2-Session-Continue	0	0	0	0	1	1
3GPP2-Session-Term-Capability	0	0	0-1	0	0	0
3GPP2-User-Zone	1	0	0	1	1	1
3GPP-Charging-Id	1	0	0	0	0	0
3GPP-Chrg-Char	0	0-1	0-1	0	0	0
Acct-Authentic	0	0	0	1	1	1
Acct-Input-Packets	0-1	0	0	0	1	1
Acct-Interim-Interval	0	0	0-1	0	0	0
Acct-Output-Packets	0-1	0	0	0	1	1
Acct-Session-Id	0	0	0	1	1	1
Callback-Id	0	0-1	0-1	0	0	0
Called-Station-ID	1	0-1	0-1	1	1	1
Calling-Station-Id	1	0	1	1	1	1

Attribute	PDSN or FA Access-Request	PDSN or FA Access-Reject	PDSN or FA Access-Accept	PDSN or FA Acct-Request-Start	PDSN or FA Acct-Request-Interim	PDSN or FA Acct-Request-Stop
CHAP-Challenge	0-1	0	0	0	0	0
Class	0-1	0-1	0+	0+	0+	0+
Connect-Info	1	0	0-1	1	1	1
CS-Prepaid-Quota	0-1	0	0-1	0-1	0-1	0-1
CS-Prepaid-Time-Quota	0-1	0	0-1	0-1	0-1	0-1
CS-Prepaid-Volume-Quota	0-1	0	0-1	0-1	0-1	0-1
CS-Service-Name	0-1	0	0-1	0-1	0-1	0-1
CUI	0-1	0-1	0-1	0-1	0-1	0-1
EAP-Message	0+	1	0+	0	0	0
Error-Cause	0	0-1	0	0	0	0
Framed-Compression	0	0	0-1	0-1	0-1	0-1
Framed-Interface-Id	0-1	0	0-1	0-1	0-1	0-1
Framed-IP-Address	0-1	0-1	0-1	1	1	1
Framed-IP-Netmask	0-1	0	0-1	0-1	0-1	0-1
Framed-IPv6-Pool	0	0	0-1	0	0	0
Framed-IPv6-Prefix	0+	0	0+	0+	0+	0+
Framed-MTU	0	0	0-1	0-1	0-1	0-1
Framed-Pool	0	0-1	0+	0	0	0
Framed-Protocol	1	0	0-1	1	1	1
Idle-Timeout	0	0	0-1	0	0	0
NAS-Port	1	0	0	1	1	1
NAS-Port-Type	1	0	0	1	1	1
Primary-DNS-Server	0	0	0-1	1	1	1
Reply-Message	0	0-1	0-1	0	0	0
Secondary-DNS-Server	0	0	0-1	1	1	1
Service-Type	1	0	0-1	1	1	1
Session-Timeout	0	0	0-1	0	0	0
SN1-Access-link-IP-Frag	0	0	0-1	0	0	0
SN1-Admin-Permission	0	0	0-1	0	0	0
SN1-Assigned-VLAN-ID	0	0	0-1	1	1	1
SN1-CFPolicy-ID	0	0	0-1	0	0	0
SN1-Data-Tunnel-Ignore-DF-Bit	0	0	0-1	0	0	0
SN1-DHCP-Lease-Expiry-Policy	0	0	0-1	0	0	0
SN1-Disconnect-Reason	0	0	0	0	0	1
SN1-DNS-Proxy-Intercept-List	0	0	1	0	0	0
SN1-DNS-Proxy-Use-Subscr-Addr	0	0	1	0	0	0
SN1-Enable-QoS-Renegotiation	0	0	0-1	0	0	0
SN1-Ext-Inline-Srvr-Context	0	0	0-1	0	0	0
SN1-Ext-Inline-Srvr-Down-Addr	0	0	0-1	0	0	0
SN1-Ext-Inline-Srvr-Down-VLAN	0	0	0-1	0	0	0
SN1-Ext-Inline-Srvr-Preference	0	0	0-1	0	0	0
SN1-Ext-Inline-Srvr-Up-Addr	0	0	0-1	0	0	0
SN1-Ext-Inline-Srvr-Up-VLAN	0	0	0-1	0	0	0
SN1-Firewall-Enabled	0	0	0	1	1	1
SN1-FMC-Location	0	0	0	0-1	0-1	0-1
SN1-HA-Send-DNS-Address	0	0	0-1	0	0	0

Attribute	PDSN or FA Access-Request	PDSN or FA Access-Reject	PDSN or FA Access-Accept	PDSN or FA Acct-Request-Start	PDSN or FA Acct-Request-Interim	PDSN or FA Acct-Request-Stop
SN1-Inactivity-Time	0	0	0-1	0	0	0
SN1-IP-Alloc-Method	0	0	0-1	0	0	0
SN1-IP-Filter-In	0	0	0+	0	0	0
SN1-IP-Filter-Out	0	0	0+	0	0	0
SN1-IP-Header-Compression	0	0	0-1	0-1	0-1	0-1
SN1-IP-Hide-Service-Address	0	0	0-1	0	0	0
SN1-IP-In-Plcy-Grp	0	0	0-1	0	0	0
SN1-IP-Out-Plcy-Grp	0	0	0-1	0	0	0
SN1-IP-Pool-Name	0	0-1	0+	0	0	0
SN1-IP-Source-Validation	0	0	0-1	0	0	0
SN1-IP-Source-Violate-No-Acct	0	0	0-1	0	0	0
SN1-IPv6-DNS-Proxy	0	0	0-1	0	0	0
SN1-IPv6-Egress-Filtering	0	0	0-1	0	0	0
SN1-IPv6-Min-Link-MTU	0	0	0-1	0	0	0
SN1-IPv6-num-rtr-advt	0	0	0-1	0	0	0
SN1-IPv6-Primary-DNS	0	0	0-1	0	0	0
SN1-IPv6-rtr-advt-interval	0	0	0-1	0	0	0
SN1-IPv6-Secondary-DNS	0	0	0-1	0	0	0
SN1-IPv6-Sec-Pool	0	0	0+	0	0	0
SN1-IPv6-Sec-Prefix	0	0	0+	0	0	0
SN1-L3-to-L2-Tun-Addr-Policy	0	0	0-1	0	0	0
SN1-Local-IP-Address	0-1	0	0-1	1	1	1
SN1-Long-Duration-Action	0	0	0-1	0	0	0
SN1-Long-Duration-Notification	0	0	0-1	0	0	0
SN1-Long-Duration-Timeout	0	0	0-1	0	0	0
SN1-Min-Compress-Size	0	0	0-1	0	0	0
SN1-MIP-AAA-Assign-Addr	0	0	0-1	0	0	0
SN1-MIP-ANCID	0	0	0	0-1	0-1	0-1
SN1-MIP-HA-Assignment-Table	0	0	1	0	0	0
SN1-MIP-Match-AAA-Assign-Addr	0	0	0-1	0	0	0
SN1-MIP-Send-Ancid	0	0	0-1	0	0	0
SN1-MIP-Send-Correlation-Info	0	0	0-1	0	0	0
SN1-MIP-Send-Imsi	0	0	0-1	0	0	0
SN1-MIP-Send-Term-Verification	0	0	0-1	0	0	0
SN1-NAI-Construction-Domain	0	0	0-1	0	0	0
SN1-NPU-Qos-Priority	0	0	0-1	0	0	0
SN1-Overload-Disc-Connect-Time	0	0	0-1	0	0	0
SN1-Overload-Disc-Inact-Time	0	0	0-1	0	0	0
SN1-Overload-Disconnect	0	0	0-1	0	0	0
SN1-PDIF-MIP-Release-TIA	0	0	0-1	0	0	0
SN1-PDIF-MIP-Required	0	0	0-1	0	0	0
SN1-PDIF-MIP-Simple-IP-Fallback	0	0	0-1	0	0	0
SN1-PDSN-Handoff-Req-IP-Addr	0	0	0-1	0	0	0
SN1-Permit-User-Mcast-PDUs	0	0	0-1	0	0	0
SN1-PPP-Accept-Peer-v6Ifid	0	0	0-1	0	0	0
SN1-PPP-Always-On-Vse	0	0	0-1	0	0	0

Attribute	PDSN or FA Access-Request	PDSN or FA Access-Reject	PDSN or FA Access-Accept	PDSN or FA Acct-Request-Start	PDSN or FA Acct-Request-Interim	PDSN or FA Acct-Request-Stop
SN1-PPP-Data-Compression	0	0	0-1	0-1	0-1	0-1
SN1-PPP-Data-Compression-Mode	0	0	0-1	0-1	0-1	0-1
SN1-PPP-Keepalive	0	0	0-1	0	0	0
SN1-PPP-NW-Layer-IPv4	0	0	0-1	0	0	0
SN1-PPP-NW-Layer-IPv6	0	0	0-1	0	0	0
SN1-PPP-Outbound-Password	0	0	0-1	0	0	0
SN1-PPP-Outbound-Username	0	0	0-1	0	0	0
SN1-PPP-Progress-Code	0	0	0	0	0	0-1
SN1-PPP-Reneg-Disc	0	0	0-1	0	0	0
SN1-Prepaid	0	0	0-1	0	0	0
SN1-Prepaid-Compressed-Count	0-1	0	0-1	0	0	0
SN1-Prepaid-Final-Duration-Alg	0	0	0-1	0	0	0
SN1-Prepaid-Inbound-Octets	0-1	0	0-1	0	0	0
SN1-Prepaid-Outbound-Octets	0-1	0	0-1	0	0	0
SN1-Prepaid-Preference	0	0	0-1	0	0	0
SN1-Prepaid-Timeout	0-1	0	0-1	0	0	0
SN1-Prepaid-Total-Octets	0-1	0	0-1	0	0	0
SN1-Prepaid-Watermark	0-1	0	0-1	0	0	0
SN1-Primary-DCCA-Peer	0	0	0-1	0	0	0
SN1-Primary-DNS-Server	0	0	0-1	1	1	1
SN1-Primary-NBNS-Server	0	0	0-1	1	1	1
SN1-Proxy-MIP	0	0	0-1	0-1	0-1	0-1
SN1-QoS-Background-Class	0	0	0-1	0	0	0
SN1-QoS-Conversation-Class	0	0	0-1	0	0	0
SN1-QoS-Interactive1-Class	0	0	0-1	0	0	0
SN1-QoS-Interactive2-Class	0	0	0-1	0	0	0
SN1-QoS-Interactive3-Class	0	0	0-1	0	0	0
SN1-QoS-Renegotiation-Timeout	0	0	0-1	0	0	0
SN1-QoS-Streaming-Class	0	0	0-1	0	0	0
SN1-QoS-Tp-Dnlk	0	0	0-1	0	0	0
SN1-QoS-Tp-Uplk	0	0	0-1	0	0	0
SN1-Re-CHAP-Interval	0	0	0-1	0-1	0-1	0-1
SN1-ROHC-Direction	0	0	0-1	0-1	0-1	0-1
SN1-ROHC-Flow-Marking-Mode	0	0	0-1	0	0	0
SN1-ROHC-Mode	0	0	0-1	0-1	0-1	0-1
SN1-ROHC-Profile-Name	0	0	0-1	0	0	0
SN1-Rulebase	0	0	0-1	1	1	1
SN1-Secondary-DCCA-Peer	0	0	0-1	0	0	0
SN1-Secondary-DNS-Server	0	0	0-1	1	1	1
SN1-Secondary-NBNS-Server	0	0	0-1	1	1	1
SN1-Service-Address	0-1	0	0	0	0	0
SN1-Simultaneous-SIP-MIP	0	0	0-1	0	0	0
SN1-Subs-Acc-Flow-Traffic-Valid	0	0	0-1	0	0	0
SN1-Subscriber-Accounting	0	0	0-1	1	1	1
SN1-Subscriber-Acct-Interim	0	0	0-1	0	0	0
SN1-Subscriber-Acct-Mode	0	0	0-1	0	0	0

Attribute	PDSN or FA Access-Request	PDSN or FA Access-Reject	PDSN or FA Access-Accept	PDSN or FA Acct-Request-Start	PDSN or FA Acct-Request-Interim	PDSN or FA Acct-Request-Stop
SN1-Subscriber-Acct-Rsp-Action	0	0	0-1	0	0	0
SN1-Subscriber-Acct-Start	0	0	0-1	0	0	0
SN1-Subscriber-Acct-Stop	0	0	0-1	0	0	0
SN1-Subscriber-Class	0	0	0-1	0-1	0-1	0-1
SN1-Subscriber-Dormant-Activity	0	0	0-1	0	0	0
SN1-Subscriber-IP-Hdr-Neg-Mode	0	0	0-1	0	0	0
SN1-Subscriber-IP-TOS-Copy	0	0	0-1	0	0	0
SN1-Subscriber-Nexthop-Address	0	0	0-1	1	1	1
SN1-Subscriber-No-Interims	0	0	0-1	0	0	0
SN1-Subscriber-Permission	0	0	0-1	0	0	0
SN1-Subs-IMSA-Service-Name	0	0	0-1	0	0	0
SN1-Subs-VJ-Slotid-Cmp-Neg-Mode	0	0	0-1	0	0	0
SN1-Tp-Dnlk-Burst-Size	0	0	0-1	0	0	0
SN1-Tp-Dnlk-Committed-Data-Rate	0	0	0-1	0	0	0
SN1-Tp-Dnlk-Exceed-Action	0	0	0-1	0	0	0
SN1-Tp-Dnlk-Peak-Data-Rate	0	0	0-1	0	0	0
SN1-Tp-Dnlk-Violate-Action	0	0	0-1	0	0	0
SN1-Tp-Uplk-Burst-Size	0	0	0-1	0	0	0
SN1-Tp-Uplk-Committed-Data-Rate	0	0	0-1	0	0	0
SN1-Tp-Uplk-Exceed-Action	0	0	0-1	0	0	0
SN1-Tp-Uplk-Peak-Data-Rate	0	0	0-1	0	0	0
SN1-Tp-Uplk-Violate-Action	0	0	0-1	0	0	0
SN1-Tun-Addr-Policy	0	0	0-1	0	0	0
SN1-Tunnel-ISAKMP-Crypto-Map	0	0	0-1	0	0	0
SN1-Tunnel-ISAKMP-Secret	0	0	0-1	0	0	0
SN1-Tunnel-Load-Balancing	0	0	0-1	0	0	0
SN1-Unclassify-List-Name	0	0	0-1	0	0	0
SN1-Voice-Push-List-Name	0	0	0-1	0	0	0
SN1-VPN-ID	0	0	0-1	0-1	0-1	0-1
SN1-VPN-Name	0	0	1	0-1	0-1	0-1
SN-Access-link-IP-Frag	0	0	0-1	0	0	0
SN-Acs-Credit-Control-Group	0	0	0-1	0-1	0-1	0-1
SN-Admin-Permission	0	0	0-1	0	0	0
SN-Assigned-VLAN-ID	0	0	0-1	1	1	1
SN-Bandwidth-Policy	0	0	1	0	0	0
SN-CBB-Policy	0	0	1	0	0	0
SN-CFPolicy-ID	0	0	0-1	0	0	0
SN-Data-Tunnel-Ignore-DF-Bit	0	0	0-1	0	0	0
SN-DHCP-Lease-Expiry-Policy	0	0	0-1	0	0	0
SN-DHCP-Options	0	0	0-1	0	0	0
SN-Direction	0	0	0-1	0-1	0-1	0-1
SN-Disconnect-Reason	0	0	0	0	0	1
SN-DNS-Proxy-Intercept-List	0	0	1	0	0	0
SN-DNS-Proxy-Use-Subscr-Addr	0	0	1	0	0	0
SN-Enable-QoS-Renegotiation	0	0	0-1	0	0	0
SN-Ext-Inline-Srvr-Context	0	0	0-1	0	0	0

Attribute	PDSN or FA Access-Request	PDSN or FA Access-Reject	PDSN or FA Access-Accept	PDSN or FA Acct-Request-Start	PDSN or FA Acct-Request-Interim	PDSN or FA Acct-Request-Stop
SN-Ext-Inline-Srvr-Down-Addr	0	0	0-1	0	0	0
SN-Ext-Inline-Srvr-Down-VLAN	0	0	0-1	0	0	0
SN-Ext-Inline-Srvr-Preference	0	0	0-1	0	0	0
SN-Ext-Inline-Srvr-Up-Addr	0	0	0-1	0	0	0
SN-Ext-Inline-Srvr-Up-VLAN	0	0	0-1	0	0	0
SN-Fast-Reauth-Username	0	0	0-1	0	0	0
SN-Firewall-Enabled	0	0	0	1	1	1
SN-Firewall-Policy	0	0	1	0	0	0
SN-FMC-Location	0	0	0	0-1	0-1	0-1
SN-HA-Send-DNS-Address	0	0	0-1	0	0	0
SN-Inactivity-Time	0	0	0-1	0	0	0
SN-IP-Alloc-Method	0	0	0-1	0	0	0
SN-IP-Filter-In	0	0	0+	0	0	0
SN-IP-Filter-Out	0	0	0+	0	0	0
SN-IP-Header-Compression	0	0	0-1	0-1	0-1	0-1
SN-IP-Hide-Service-Address	0	0	0-1	0	0	0
SN-IP-In-Plcy-Grp	0	0	0-1	0	0	0
SN-IP-Out-Plcy-Grp	0	0	0-1	0	0	0
SN-IP-Pool-Name	0	0-1	0+	0	0	0
SN-IP-Source-Validation	0	0	0-1	0	0	0
SN-IP-Source-Violate-No-Acct	0	0	0-1	0	0	0
SN-IPv6-DNS-Proxy	0	0	0-1	0	0	0
SN-IPv6-Egress-Filtering	0	0	0-1	0	0	0
SN-IPv6-Min-Link-MTU	0	0	0-1	0	0	0
SN-IPv6-num-rtr-advt	0	0	0-1	0	0	0
SN-IPv6-Primary-DNS	0	0	0-1	0	0	0
SN-IPv6-rtr-advt-interval	0	0	0-1	0	0	0
SN-IPv6-Secondary-DNS	0	0	0-1	0	0	0
SN-IPv6-Sec-Pool	0	0	0+	0	0	0
SN-IPv6-Sec-Prefix	0	0	0+	0	0	0
SN-L3-to-L2-Tun-Addr-Policy	0	0	0-1	0	0	0
SN-Local-IP-Address	0-1	0	0-1	1	1	1
SN-Long-Duration-Action	0	0	0-1	0	0	0
SN-Long-Duration-Notification	0	0	0-1	0	0	0
SN-Long-Duration-Timeout	0	0	0-1	0	0	0
SN-Min-Compress-Size	0	0	0-1	0	0	0
SN-MIP-AAA-Assign-Addr	0	0	0-1	0	0	0
SN-MIP-ANCID	0	0	0	0-1	0-1	0-1
SN-MIP-HA-Assignment-Table	0	0	1	0	0	0
SN-MIP-Match-AAA-Assign-Addr	0	0	0-1	0	0	0
SN-MIP-Send-Ancid	0	0	0-1	0	0	0
SN-MIP-Send-Correlation-Info	0	0	0-1	0	0	0
SN-MIP-Send-Host-Config	0	0	0-1	0	0	0
SN-MIP-Send-Imsi	0	0	0-1	0	0	0
SN-MIP-Send-Term-Verification	0	0	0-1	0	0	0
SN-Mode	0	0	0-1	0-1	0-1	0-1

Attribute	PDSN or FA Access-Request	PDSN or FA Access-Reject	PDSN or FA Access-Accept	PDSN or FA Acct-Request-Start	PDSN or FA Acct-Request-Interim	PDSN or FA Acct-Request-Stop
SN-NAI-Construction-Domain	0	0	0-1	0	0	0
SN-NPU-Qos-Priority	0	0	0-1	0	0	0
SN-Overload-Disc-Connect-Time	0	0	0-1	0	0	0
SN-Overload-Disc-Inact-Time	0	0	0-1	0	0	0
SN-Overload-Disconnect	0	0	0-1	0	0	0
SN-PDG-TTG-Required	0	0	0-1	0	0	0
SN-PDIF-MIP-Release-TIA	0	0	0-1	0	0	0
SN-PDIF-MIP-Required	0	0	0-1	0	0	0
SN-PDIF-MIP-Simple-IP-Fallback	0	0	0-1	0	0	0
SN-PDSN-Handoff-Req-IP-Addr	0	0	0-1	0	0	0
SN-Permit-User-Mcast-PDUs	0	0	0-1	0	0	0
SN-PPP-Accept-Peer-v6Ifid	0	0	0-1	0	0	0
SN-PPP-Always-On-Vse	0	0	0-1	0	0	0
SN-PPP-Data-Compression	0	0	0-1	0-1	0-1	0-1
SN-PPP-Data-Compression-Mode	0	0	0-1	0-1	0-1	0-1
SN-PPP-Keepalive	0	0	0-1	0	0	0
SN-PPP-NW-Layer-IPv4	0	0	0-1	0	0	0
SN-PPP-NW-Layer-IPv6	0	0	0-1	0	0	0
SN-PPP-Outbound-Password	0	0	0-1	0	0	0
SN-PPP-Outbound-Username	0	0	0-1	0	0	0
SN-PPP-Progress-Code	0	0	0	0	0	0-1
SN-PPP-Reneg-Disc	0	0	0-1	0	0	0
SN-Prepaid	0	0	0-1	0	0	0
SN-Prepaid-Compressed-Count	0-1	0	0-1	0	0	0
SN-Prepaid-Final-Duration-Alg	0	0	0-1	0	0	0
SN-Prepaid-Inbound-Octets	0-1	0	0-1	0	0	0
SN-Prepaid-Outbound-Octets	0-1	0	0-1	0	0	0
SN-Prepaid-Preference	0	0	0-1	0	0	0
SN-Prepaid-Timeout	0-1	0	0-1	0	0	0
SN-Prepaid-Total-Octets	0-1	0	0-1	0	0	0
SN-Prepaid-Watermark	0-1	0	0-1	0	0	0
SN-Primary-DCCA-Peer	0	0	0-1	0	0	0
SN-Primary-DNS-Server	0	0	0-1	1	1	1
SN-Primary-NBNS-Server	0	0	0-1	1	1	1
SN-Proxy-MIP	0	0	0-1	0-1	0-1	0-1
SN-Pseudonym-Username	0	0	0-1	0	0	0
SN-QoS-Background-Class	0	0	0-1	0	0	0
SN-QoS-Conversation-Class	0	0	0-1	0	0	0
SN-QOS-HLR-Profile	0	0	0-1	0	0	0
SN-QoS-Interactive1-Class	0	0	0-1	0	0	0
SN-QoS-Interactive2-Class	0	0	0-1	0	0	0
SN-QoS-Interactive3-Class	0	0	0-1	0	0	0
SN-QoS-Renegotiation-Timeout	0	0	0-1	0	0	0
SN-QoS-Streaming-Class	0	0	0-1	0	0	0
SN-QoS-Tp-Dnlk	0	0	0-1	0	0	0
SN-QoS-Tp-Uplk	0	0	0-1	0	0	0

Attribute	PDSN or FA Access-Request	PDSN or FA Access-Reject	PDSN or FA Access-Accept	PDSN or FA Acct-Request-Start	PDSN or FA Acct-Request-Interim	PDSN or FA Acct-Request-Stop
SN-Re-CHAP-Interval	0	0	0-1	0-1	0-1	0-1
SN-ROHC-Flow-Marking-Mode	0	0	0-1	0	0	0
SN-ROHC-Profile-Name	0	0	0-1	0	0	0
SN-Rulebase	0	0	0-1	1	1	1
SN-Sec-IP-Pool-Name	0	0	0+	0	0	0
SN-Secondary-DCCA-Peer	0	0	0-1	0	0	0
SN-Secondary-DNS-Server	0	0	0-1	1	1	1
SN-Secondary-NBNS-Server	0	0	0-1	1	1	1
SN-Service-Address	0-1	0	0	0	0	0
SN-Simultaneous-SIP-MIP	0	0	0-1	0	0	0
SN-Subs-Acc-Flow-Traffic-Valid	0	0	0-1	0	0	0
SN-Subscriber-Accounting	0	0	0-1	1	1	1
SN-Subscriber-Acct-Interim	0	0	0-1	0	0	0
SN-Subscriber-Acct-Mode	0	0	0-1	0	0	0
SN-Subscriber-Acct-Rsp-Action	0	0	0-1	0	0	0
SN-Subscriber-Acct-Start	0	0	0-1	0	0	0
SN-Subscriber-Acct-Stop	0	0	0-1	0	0	0
SN-Subscriber-Class	0	0	0-1	0-1	0-1	0-1
SN-Subscriber-Dormant-Activity	0	0	0-1	0	0	0
SN-Subscriber-IP-Hdr-Neg-Mode	0	0	0-1	0	0	0
SN-Subscriber-IP-TOS-Copy	0	0	0-1	0	0	0
SN-Subscriber-Nexthop-Address	0	0	0-1	1	1	1
SN-Subscriber-No-Interims	0	0	0-1	0	0	0
SN-Subscriber-Permission	0	0	0-1	0	0	0
SN-Subs-IMSA-Service-Name	0	0	0-1	0	0	0
SN-Subs-VJ-Slotid-Cmp-Neg-Mode	0	0	0-1	0	0	0
SN-Tp-Dnlk-Burst-Size	0	0	0-1	0	0	0
SN-Tp-Dnlk-Committed-Data-Rate	0	0	0-1	0	0	0
SN-Tp-Dnlk-Exceed-Action	0	0	0-1	0	0	0
SN-Tp-Dnlk-Peak-Data-Rate	0	0	0-1	0	0	0
SN-Tp-Dnlk-Violate-Action	0	0	0-1	0	0	0
SN-TPO-Policy	0	0	0-1	0	0	0
SN-Tp-Uplk-Burst-Size	0	0	0-1	0	0	0
SN-Tp-Uplk-Committed-Data-Rate	0	0	0-1	0	0	0
SN-Tp-Uplk-Exceed-Action	0	0	0-1	0	0	0
SN-Tp-Uplk-Peak-Data-Rate	0	0	0-1	0	0	0
SN-Tp-Uplk-Violate-Action	0	0	0-1	0	0	0
SN-TrafficSelector-Class	0	0	0-1	0	0	0
SN-Tun-Addr-Policy	0	0	0-1	0	0	0
SN-Tunnel-ISAKMP-Crypto-Map	0	0	0-1	0	0	0
SN-Tunnel-ISAKMP-Secret	0	0	0-1	0	0	0
SN-Tunnel-Load-Balancing	0	0	0-1	0	0	0
SN-Unclassify-List-Name	0	0	0-1	0	0	0
SN-Voice-Push-List-Name	0	0	0-1	0	0	0
SN-VPN-ID	0	0	0-1	0-1	0-1	0-1
SN-VPN-Name	0	0	1	0-1	0-1	0-1

Attribute	PDSN or FA Access-Request	PDSN or FA Access-Reject	PDSN or FA Access-Accept	PDSN or FA Acct-Request-Start	PDSN or FA Acct-Request-Interim	PDSN or FA Acct-Request-Stop
SN-WiMAX-Auth-Only	0	0	0-1	0	0	0
State	1	0-1	0-1	0	0	0
Termination-Action	0	0	0-1	0	0	0
Tunnel-Assignment-ID	0	0	0-1	1	1	1
Tunnel-Client-Auth-ID	0	0	0-1	1	1	1
Tunnel-Client-Endpoint	0	0	0-1	1	1	1
Tunnel-Medium-Type	0	0	0-1	1	1	1
Tunnel-Preference	0	0	0-1	0	0	0
Tunnel-Private-Group-ID	0	0	0-1	1	1	1
Tunnel-Server-Auth-ID	0	0	0-1	1	1	1
Tunnel-Server-Endpoint	0	0	0-1	1	1	1
Tunnel-Type	0	0	0-1	1	1	1
User-Name	1	0	0-1	1	1	1
User-Password	0-1	0	0	0	0	0

HA Attribute/Packet Table

Attribute	HA Access-Request	HA Access-Reject	HA Access-Accept	HA Acct-Request-Start	HA Acct-Request-Interim	HA Acct-Request-Stop
3GPP2-Beginning-Session	0	0	0	0-1	0	0
3GPP2-BSID	0	0	0	0-1	0-1	0-1
3GPP2-Comp-Tunnel-Indicator	0	0	0	1	1	1
3GPP2-Correlation-Id	1	0	0	1	1	1
3GPP2-DNS-Server-IPV6-Addr	0	0	0-1	0	0	0
3GPP2-DNS-Update-Required	0	0	0-1	0	0	0
3GPP2-ESN	1	0	0	0	0	0
3GPP2-FA-Address	0-1	0	0	0-1	0-1	0-1
3GPP2-IP-QOS	0	0	0-1	1	1	1
3GPP2-IP-Technology	0-1	0	0-1	0	0	0
3GPP2-MEID	0	0	0-1	0	0	0
3GPP2-MIP6-Authenticator	0-1	0	0	0	0	0
3GPP2-MIP6-CoA	0-1	0	0	0-1	0-1	0
3GPP2-MIP6-HA	0-1	0	0	0	0	0
3GPP2-MIP6-HoA	0-1	0	0	0-1	0-1	0
3GPP2-MIP6-HoA-Not-Authorized	0	0	0-1	0	0	0
3GPP2-MIP6-MAC-Mobility-Data	0-1	0	0	0	0	0
3GPP2-MIP6-Mesg-ID	0-1	0	0	0	0	0
3GPP2-MIP6-Session-Key	0	0	0-1	0	0	0
3GPP2-MN-HA-Shared-Key	0	0	0-1	0	0	0
3GPP2-MN-HA-SPI	0-1	0	0	0	0	0
3GPP2-Mobile-Term-Orig-Ind	0	0	0	1	1	1
3GPP2-Service-Option	0	0	0	0-1	0-1	0-1
3GPP2-Serving-PCF	0	0	0	1	1	1
3GPP2-Session-Continue	0	0	0	0	0	0-1
Acct-Authentic	0	0	0	1	1	1
Acct-Input-Packets	0-1	0	0	0	1	1
Acct-Interim-Interval	0	0	0-1	0	0	0
Acct-Multi-Session-Id	0	0	0	0-1	0-1	0-1
Acct-Output-Packets	0-1	0	0	0	1	1
Acct-Session-Id	0	0	0	1	1	1
Calling-Station-Id	1	0	1	1	1	1
CHAP-Challenge	1	0	0	0	0	0
Class	0	0	0-1	0-1	0-1	0-1
CUI	0-1	0	0-1	0	0	0
Error-Cause	0	0-1	0	0	0	0
Framed-IP-Address	0-1	0	0-1	1	1	1
Framed-IP-Netmask	0-1	0	0-1	0-1	0-1	0-1
Framed-IPv6-Pool	0	0	0-1	0	0	0
Framed-MTU	0	0	0-1	0-1	0-1	0-1
Framed-Pool	0	0	0+	0	0	0
Idle-Timeout	0	0	0-1	0	0	0
NAS-Port	1	0	0	1	1	1

Attribute	HA Access-Request	HA Access-Reject	HA Access-Accept	HA Acct-Request-Start	HA Acct-Request-Interim	HA Acct-Request-Stop
NAS-Port-Type	1	0	0	1	1	1
Primary-DNS-Server	0	0	0-1	1	1	1
Reply-Message	0	0-1	0-1	0	0	0
Secondary-DNS-Server	0	0	0-1	1	1	1
Service-Type	1	0	0-1	1	1	1
Session-Timeout	0	0	0-1	0	0	0
SN1-Access-link-IP-Frag	0	0	0-1	0	0	0
SN1-Admin-Permission	0	0	0-1	0	0	0
SN1-Assigned-VLAN-ID	0	0	0-1	0-1	0-1	0-1
SN1-CFPolicy-ID	0	0	0-1	0	0	0
SN1-Data-Tunnel-Ignore-DF-Bit	0	0	0-1	0	0	0
SN1-DHCP-Lease-Expiry-Policy	0	0	0-1	0	0	0
SN1-Disconnect-Reason	0	0	0	0	0	1
SN1-DNS-Proxy-Intercept-List	0	0	1	0	0	0
SN1-DNS-Proxy-Use-Subscr-Addr	0	0	1	0	0	0
SN1-Enable-QoS-Renegotiation	0	0	0-1	0	0	0
SN1-Ext-Inline-Srvr-Context	0	0	0-1	0	0	0
SN1-Ext-Inline-Srvr-Down-Addr	0	0	0-1	0	0	0
SN1-Ext-Inline-Srvr-Down-VLAN	0	0	0-1	0	0	0
SN1-Ext-Inline-Srvr-Preference	0	0	0-1	0	0	0
SN1-Ext-Inline-Srvr-Up-Addr	0	0	0-1	0	0	0
SN1-Ext-Inline-Srvr-Up-VLAN	0	0	0-1	0	0	0
SN1-Firewall-Enabled	0	0	0	1	1	1
SN1-FMC-Location	0	0	0	0-1	0-1	0-1
SN1-Gratuitous-ARP-Aggressive	0	0	0-1	0	0	0
SN1-Ignore-Unknown-HA-Addr-Err	0	0	0-1	0	0	0
SN1-IMS-AM-Address	0	0	0-1	0	0	0
SN1-IMS-AM-Domain-Name	0	0	0-1	0	0	0
SN1-Inactivity-Time	0	0	0-1	0	0	0
SN1-IP-Filter-In	0	0	0+	0	0	0
SN1-IP-Filter-Out	0	0	0+	0	0	0
SN1-IP-Hide-Service-Address	0	0	0-1	0	0	0
SN1-IP-Pool-Name	0	0	0+	0	0	0
SN1-IP-Source-Validation	0	0	0-1	0	0	0
SN1-IP-Source-Violate-No-Acct	0	0	0-1	0	0	0
SN1-IPv6-Sec-Pool	0	0	0+	0	0	0
SN1-IPv6-Sec-Prefix	0	0	0+	0	0	0
SN1-L3-to-L2-Tun-Addr-Policy	0	0	0-1	0	0	0
SN1-Local-IP-Address	0-1	0	0-1	1	1	1
SN1-Long-Duration-Action	0	0	0-1	0	0	0
SN1-Long-Duration-Notification	0	0	0-1	0	0	0
SN1-Long-Duration-Timeout	0	0	0-1	0	0	0
SN1-MIP-ANCID	0	0	0	0-1	0-1	0-1
SN1-MIP-Dual-Anchor	0	0	0-1	0	0	0
SN1-MIP-HA-Assignment-Table	0	0	1	0	0	0
SN1-MIP-Reg-Lifetime-Realm	0	0	0-1	0	0	0

Attribute	HA Access-Request	HA Access-Reject	HA Access-Accept	HA Acct-Request-Start	HA Acct-Request-Interim	HA Acct-Request-Stop
SN1-MN-HA-Timestamp-Tolerance	0	0	0-1	0	0	0
SN1-NPU-Qos-Priority	0	0	0-1	0	0	0
SN1-Nw-Reachability-Server-Name	0	0	0-1	0	0	0
SN1-Overload-Disc-Connect-Time	0	0	0-1	0	0	0
SN1-Overload-Disc-Inact-Time	0	0	0-1	0	0	0
SN1-Overload-Disconnect	0	0	0-1	0	0	0
SN1-PDSN-Correlation-Id	0	0	0	0-1	0-1	0-1
SN1-PDSN-NAS-Id	0	0	0	0-1	0-1	0-1
SN1-PDSN-NAS-IP-Address	0	0	0	0-1	0-1	0-1
SN1-Permit-User-Mcast-PDUs	0	0	0-1	0	0	0
SN1-Prepaid	0	0	0-1	0	0	0
SN1-Prepaid-Compressed-Count	0-1	0	0-1	0	0	0
SN1-Prepaid-Final-Duration-Alg	0	0	0-1	0	0	0
SN1-Prepaid-Inbound-Octets	0-1	0	0-1	0	0	0
SN1-Prepaid-Outbound-Octets	0-1	0	0-1	0	0	0
SN1-Prepaid-Preference	0	0	0-1	0	0	0
SN1-Prepaid-Timeout	0-1	0	0-1	0	0	0
SN1-Prepaid-Total-Octets	0-1	0	0-1	0	0	0
SN1-Prepaid-Watermark	0-1	0	0-1	0	0	0
SN1-Primary-DCCA-Peer	0	0	0-1	0	0	0
SN1-Primary-DNS-Server	0	0	0-1	1	1	1
SN1-Primary-NBNS-Server	0	0	0-1	1	1	1
SN1-QoS-Background-Class	0	0	0-1	0	0	0
SN1-QoS-Conversation-Class	0	0	0-1	0	0	0
SN1-QoS-Interactive1-Class	0	0	0-1	0	0	0
SN1-QoS-Interactive2-Class	0	0	0-1	0	0	0
SN1-QoS-Interactive3-Class	0	0	0-1	0	0	0
SN1-QoS-Renegotiation-Timeout	0	0	0-1	0	0	0
SN1-QoS-Streaming-Class	0	0	0-1	0	0	0
SN1-QoS-Tp-Dnlk	0	0	0-1	0	0	0
SN1-QoS-Tp-Uplk	0	0	0-1	0	0	0
SN1-Re-CHAP-Interval	0	0	0-1	0-1	0-1	0-1
SN1-Rulebase	0	0	0-1	1	1	1
SN1-Secondary-DCCA-Peer	0	0	0-1	0	0	0
SN1-Secondary-DNS-Server	0	0	0-1	1	1	1
SN1-Secondary-NBNS-Server	0	0	0-1	1	1	1
SN1-Service-Address	0-1	0	0	0	0	0
SN1-Subscriber-Accounting	0	0	0-1	1	1	1
SN1-Subscriber-Acct-Interim	0	0	0-1	0	0	0
SN1-Subscriber-Acct-Mode	0	0	0-1	0	0	0
SN1-Subscriber-Acct-Rsp-Action	0	0	0-1	0	0	0
SN1-Subscriber-Acct-Start	0	0	0-1	0	0	0
SN1-Subscriber-Acct-Stop	0	0	0-1	0	0	0
SN1-Subscriber-Class	0	0	0-1	0-1	0-1	0-1
SN1-Subscriber-IP-TOS-Copy	0	0	0-1	0	0	0
SN1-Subscriber-Nexthop-Address	0	0	0-1	1	1	1

Attribute	HA Access-Request	HA Access-Reject	HA Access-Accept	HA Acct-Request-Start	HA Acct-Request-Interim	HA Acct-Request-Stop
SN1-Subscriber-No-Interims	0	0	0-1	0	0	0
SN1-Subscriber-Permission	0	0	0-1	0	0	0
SN1-Subs-IMSA-Service-Name	0	0	0-1	0	0	0
SN1-Tp-Dnlk-Burst-Size	0	0	0-1	0	0	0
SN1-Tp-Dnlk-Committed-Data-Rate	0	0	0-1	0	0	0
SN1-Tp-Dnlk-Exceed-Action	0	0	0-1	0	0	0
SN1-Tp-Dnlk-Peak-Data-Rate	0	0	0-1	0	0	0
SN1-Tp-Dnlk-Violate-Action	0	0	0-1	0	0	0
SN1-Tp-Uplk-Burst-Size	0	0	0-1	0	0	0
SN1-Tp-Uplk-Committed-Data-Rate	0	0	0-1	0	0	0
SN1-Tp-Uplk-Exceed-Action	0	0	0-1	0	0	0
SN1-Tp-Uplk-Peak-Data-Rate	0	0	0-1	0	0	0
SN1-Tp-Uplk-Violate-Action	0	0	0-1	0	0	0
SN1-Tun-Addr-Policy	0	0	0-1	0	0	0
SN1-Tunnel-ISAKMP-Crypto-Map	0	0	0-1	0	0	0
SN1-Tunnel-ISAKMP-Secret	0	0	0-1	0	0	0
SN1-Tunnel-Load-Balancing	0	0	0-1	0	0	0
SN1-Unclassify-List-Name	0	0	0-1	0	0	0
SN1-Voice-Push-List-Name	0	0	0-1	0	0	0
SN1-VPN-ID	0	0	0-1	0-1	0-1	0-1
SN1-VPN-Name	0	0	1	0-1	0-1	0-1
SN-Access-link-IP-Frag	0	0	0-1	0	0	0
SN-Acs-Credit-Control-Group	0	0	0-1	0-1	0-1	0-1
SN-Admin-Permission	0	0	0-1	0	0	0
SN-Assigned-VLAN-ID	0	0	0-1	0-1	0-1	0-1
SN-Bandwidth-Policy	0	0	1	0	0	0
SN-CBB-Policy	0	0	1	0	0	0
SN-CFPolicy-ID	0	0	0-1	0	0	0
SN-Data-Tunnel-Ignore-DF-Bit	0	0	0-1	0	0	0
SN-DHCP-Lease-Expiry-Policy	0	0	0-1	0	0	0
SN-Disconnect-Reason	0	0	0	0	0	1
SN-DNS-Proxy-Intercept-List	0	0	1	0	0	0
SN-DNS-Proxy-Use-Subscr-Addr	0	0	1	0	0	0
SN-Enable-QoS-Renegotiation	0	0	0-1	0	0	0
SN-Ext-Inline-Srvr-Context	0	0	0-1	0	0	0
SN-Ext-Inline-Srvr-Down-Addr	0	0	0-1	0	0	0
SN-Ext-Inline-Srvr-Down-VLAN	0	0	0-1	0	0	0
SN-Ext-Inline-Srvr-Preference	0	0	0-1	0	0	0
SN-Ext-Inline-Srvr-Up-Addr	0	0	0-1	0	0	0
SN-Ext-Inline-Srvr-Up-VLAN	0	0	0-1	0	0	0
SN-Firewall-Enabled	0	0	0	1	1	1
SN-Firewall-Policy	0	0	1	0	0	0
SN-FMC-Location	0	0	0	0-1	0-1	0-1
SN-Gratuitous-ARP-Aggressive	0	0	0-1	0	0	0
SN-Ignore-Unknown-HA-Addr-Error	0	0	0-1	0	0	0
SN-IMS-AM-Address	0	0	0-1	0	0	0

Attribute	HA Access-Request	HA Access-Reject	HA Access-Accept	HA Acct-Request-Start	HA Acct-Request-Interim	HA Acct-Request-Stop
SN-IMS-AM-Domain-Name	0	0	0-1	0	0	0
SN-Inactivity-Time	0	0	0-1	0	0	0
SN-IP-Filter-In	0	0	0+	0	0	0
SN-IP-Filter-Out	0	0	0+	0	0	0
SN-IP-Hide-Service-Address	0	0	0-1	0	0	0
SN-IP-Pool-Name	0	0	0+	0	0	0
SN-IP-Source-Validation	0	0	0-1	0	0	0
SN-IP-Source-Violate-No-Acct	0	0	0-1	0	0	0
SN-IPv6-Sec-Pool	0	0	0+	0	0	0
SN-IPv6-Sec-Prefix	0	0	0+	0	0	0
SN-L3-to-L2-Tun-Addr-Policy	0	0	0-1	0	0	0
SN-Local-IP-Address	0-1	0	0-1	1	1	1
SN-Long-Duration-Action	0	0	0-1	0	0	0
SN-Long-Duration-Notification	0	0	0-1	0	0	0
SN-Long-Duration-Timeout	0	0	0-1	0	0	0
SN-MIP-ANCID	0	0	0	0-1	0-1	0-1
SN-MIP-Dual-Anchor	0	0	0-1	0	0	0
SN-MIP-HA-Assignment-Table	0	0	1	0	0	0
SN-MIP-Reg-Lifetime-Realm	0	0	0-1	0	0	0
SN-MN-HA-Timestamp-Tolerance	0	0	0-1	0	0	0
SN-NPU-Qos-Priority	0	0	0-1	0	0	0
SN-Nw-Reachability-Server-Name	0	0	0-1	0	0	0
SN-Overload-Disc-Connect-Time	0	0	0-1	0	0	0
SN-Overload-Disc-Inact-Time	0	0	0-1	0	0	0
SN-Overload-Disconnect	0	0	0-1	0	0	0
SN-PDSN-Correlation-Id	0	0	0	0-1	0-1	0-1
SN-PDSN-NAS-Id	0	0	0	0-1	0-1	0-1
SN-PDSN-NAS-IP-Address	0	0	0	0-1	0-1	0-1
SN-Permit-User-Mcast-PDUs	0	0	0-1	0	0	0
SN-Prepaid	0	0	0-1	0	0	0
SN-Prepaid-Compressed-Count	0-1	0	0-1	0	0	0
SN-Prepaid-Final-Duration-Alg	0	0	0-1	0	0	0
SN-Prepaid-Inbound-Octets	0-1	0	0-1	0	0	0
SN-Prepaid-Outbound-Octets	0-1	0	0-1	0	0	0
SN-Prepaid-Preference	0	0	0-1	0	0	0
SN-Prepaid-Timeout	0-1	0	0-1	0	0	0
SN-Prepaid-Total-Octets	0-1	0	0-1	0	0	0
SN-Prepaid-Watermark	0-1	0	0-1	0	0	0
SN-Primary-DCCA-Peer	0	0	0-1	0	0	0
SN-Primary-DNS-Server	0	0	0-1	1	1	1
SN-Primary-NBNS-Server	0	0	0-1	1	1	1
SN-QoS-Background-Class	0	0	0-1	0	0	0
SN-QoS-Conversation-Class	0	0	0-1	0	0	0
SN-QoS-Interactive1-Class	0	0	0-1	0	0	0
SN-QoS-Interactive2-Class	0	0	0-1	0	0	0
SN-QoS-Interactive3-Class	0	0	0-1	0	0	0

Attribute	HA Access-Request	HA Access-Reject	HA Access-Accept	HA Acct-Request-Start	HA Acct-Request-Interim	HA Acct-Request-Stop
SN-QoS-Renegotiation-Timeout	0	0	0-1	0	0	0
SN-QoS-Streaming-Class	0	0	0-1	0	0	0
SN-QoS-Tp-Dnlk	0	0	0-1	0	0	0
SN-QoS-Tp-Uplk	0	0	0-1	0	0	0
SN-Re-CHAP-Interval	0	0	0-1	0-1	0-1	0-1
SN-Rulebase	0	0	0-1	1	1	1
SN-Secondary-DCCA-Peer	0	0	0-1	0	0	0
SN-Secondary-DNS-Server	0	0	0-1	1	1	1
SN-Secondary-NBNS-Server	0	0	0-1	1	1	1
SN-Service-Address	0-1	0	0	0	0	0
SN-Subscriber-Accounting	0	0	0-1	1	1	1
SN-Subscriber-Acct-Interim	0	0	0-1	0	0	0
SN-Subscriber-Acct-Mode	0	0	0-1	0	0	0
SN-Subscriber-Acct-Rsp-Action	0	0	0-1	0	0	0
SN-Subscriber-Acct-Start	0	0	0-1	0	0	0
SN-Subscriber-Acct-Stop	0	0	0-1	0	0	0
SN-Subscriber-Class	0	0	0-1	0-1	0-1	0-1
SN-Subscriber-IP-TOS-Copy	0	0	0-1	0	0	0
SN-Subscriber-Nexthop-Address	0	0	0-1	1	1	1
SN-Subscriber-No-Interims	0	0	0-1	0	0	0
SN-Subscriber-Permission	0	0	0-1	0	0	0
SN-Subs-IMSA-Service-Name	0	0	0-1	0	0	0
SN-Tp-Dnlk-Burst-Size	0	0	0-1	0	0	0
SN-Tp-Dnlk-Committed-Data-Rate	0	0	0-1	0	0	0
SN-Tp-Dnlk-Exceed-Action	0	0	0-1	0	0	0
SN-Tp-Dnlk-Peak-Data-Rate	0	0	0-1	0	0	0
SN-Tp-Dnlk-Violate-Action	0	0	0-1	0	0	0
SN-TPO-Policy	0	0	0-1	0	0	0
SN-Tp-Uplk-Burst-Size	0	0	0-1	0	0	0
SN-Tp-Uplk-Committed-Data-Rate	0	0	0-1	0	0	0
SN-Tp-Uplk-Exceed-Action	0	0	0-1	0	0	0
SN-Tp-Uplk-Peak-Data-Rate	0	0	0-1	0	0	0
SN-Tp-Uplk-Violate-Action	0	0	0-1	0	0	0
SN-TrafficSelector-Class	0	0	0-1	0	0	0
SN-Tun-Addr-Policy	0	0	0-1	0	0	0
SN-Tunnel-ISAKMP-Crypto-Map	0	0	0-1	0	0	0
SN-Tunnel-ISAKMP-Secret	0	0	0-1	0	0	0
SN-Tunnel-Load-Balancing	0	0	0-1	0	0	0
SN-Unclassify-List-Name	0	0	0-1	0	0	0
SN-Voice-Push-List-Name	0	0	0-1	0	0	0
SN-VPN-ID	0	0	0-1	0-1	0-1	0-1
SN-VPN-Name	0	0	1	0-1	0-1	0-1
SN-WiMAX-Auth-Only	0	0	0-1	0	0	0
State	1	0	0-1	0	0	0
Tunnel-Assignment-ID	0	0	0-1	1	1	1
Tunnel-Client-Auth-ID	0	0	0-1	1	1	1

Attribute	HA Access-Request	HA Access-Reject	HA Access-Accept	HA Acct-Request-Start	HA Acct-Request-Interim	HA Acct-Request-Stop
Tunnel-Client-Endpoint	0	0	0-1	1	1	1
Tunnel-Medium-Type	0	0	0-1	1	1	1
Tunnel-Preference	0	0	0-1	0	0	0
Tunnel-Private-Group-ID	0	0	0-1	1	1	1
Tunnel-Server-Auth-ID	0	0	0-1	1	1	1
Tunnel-Server-Endpoint	0	0	0-1	1	1	1
Tunnel-Type	0	0	0-1	1	1	1
User-Name	1	0	0-1	1	1	1

GGSN Attribute/Packet Table

Attribute	GGSN Access-Request	GGSN Access-Reject	GGSN Access-Accept	GGSN Acct-Request-Start	GGSN Acct-Request-Interim	GGSN Acct-Request-Stop
3GPP2-BSID	0	0	0	0-1	0-1	0-1
3GPP-Allocate-IPType	0-1	0	0	0	0	0
3GPP-CAMEL-Charging-Info	0-1	0	0	0-1	0-1	0-1
3GPP-CG-Address	0-1	0	0	0-1	0-1	0-1
3GPP-Charging-Id	0-1	0	0	0-1	0-1	0-1
3GPP-Chrg-Char	0-1	0-1	0-1	0-1	0-1	0-1
3GPP-GGSN-Address	0-1	0	0	0-1	0-1	0-1
3GPP-GGSN-IPv6-Address	0-1	0	0	0-1	0-1	0-1
3GPP-GGSN-Mcc-Mnc	0-1	0	0	0-1	0-1	0-1
3GPP-IMEISV	0-1	0	0	0-1	0-1	0-1
3GPP-IMSI	0-1	0	0	0-1	0-1	0-1
3GPP-IMSI-Mcc-Mnc	0-1	0	0	0-1	0-1	0-1
3GPP-IPv6-DNS-Servers	0	0	0-1	0	0	0
3GPP-MS-TimeZone	0-1	0	0	0-1	0-1	0-1
3GPP-Negotiated-DSCP	0-1	0	0	0-1	0-1	0-1
3GPP-Negotiated-QoS-Profile	0-1	0	0	0-1	0-1	0-1
3GPP-NSAPI	0-1	0	0	0-1	0-1	0-1
3GPP-PDP-Type	0-1	0	0	0-1	0-1	0-1
3GPP-RAT-Type	0-1	0	0	0-1	0-1	0-1
3GPP-Selection-Mode	0-1	0	0	0-1	0-1	0-1
3GPP-Session-Stop-Ind	0	0	0	0	0	0-1
3GPP-SGSN-Address	0-1	0	0	0-1	0-1	0-1
3GPP-SGSN-IPv6-Address	0-1	0	0	0-1	0-1	0-1
3GPP-SGSN-Mcc-Mnc	0-1	0	0	0-1	0-1	0-1
3GPP-User-Location-Info	0-1	0	0	0-1	0-1	0-1
Acct-Authentic	0	0	0	1	1	1
Acct-Input-Packets	0-1	0	0	0	0	0-1
Acct-Interim-Interval	0	0	0-1	0	0	0
Acct-Multi-Session-Id	0-1	0	0	1	1	1
Acct-Output-Packets	0-1	0	0	0	0	0-1
Acct-Session-Id	0-1	0	0	1	1	1
Callback-Id	0	0-1	0-1	0	0	0
Called-Station-ID	1	0	0	1	1	1
Calling-Station-Id	0-1	0	0	0-1	0-1	0-1
CHAP-Challenge	0-1	0	0	0	0	0
Class	0	0	0+	0-1	0-1	0-1
CUI	0	0	0-1	0-1	0-1	0-1
EAP-Message	0+	1	0+	0	0	0
Error-Cause	0	0-1	0	0	0	0
Framed-Compression	0	0	0-1	0-1	0-1	0-1
Framed-Interface-Id	0-1	0	0-1	0-1	0-1	0-1
Framed-IP-Address	0-1	0	1	0-1	0-1	0-1
Framed-IP-Netmask	0	0	0	0-1	0-1	0-1

Attribute	GGSN Access-Request	GGSN Access-Reject	GGSN Access-Accept	GGSN Acct-Request-Start	GGSN Acct-Request-Interim	GGSN Acct-Request-Stop
Framed-IPv6-Prefix	0+	0	0+	0+	0+	0+
Framed-MTU	0-1	0	0-1	0-1	0-1	0-1
Framed-Protocol	0-1	0	0-1	0-1	0-1	0-1
Geographical-Location	0-1	0	0	0	0	0
HNB-Internet-Information	0-1	0	0	0	0	0
HNB-Parameters	1	0	0	0	0	0
Idle-Timeout	0	0	0-1	0	0	0
Macro-Coverage-Information	0-1	0	0	0	0	0
NAS-Port-Type	0-1	0	0	0-1	0	0-1
Primary-DNS-Server	0	0	0-1	0	0	0
Reject-Cause	0	1	0	0	0	0
Reply-Message	0	0-1	0-1	0	0	0
Secondary-DNS-Server	0	0	0-1	0	0	0
Service-Type	0-1	0	0-1	0-1	0	0-1
Session-Timeout	0-1	0	0-1	0	0	0
SN1-Access-link-IP-Frag	0	0	0-1	0	0	0
SN1-Assigned-VLAN-ID	0	0	0-1	0-1	0-1	0-1
SN1-CFPolicy-ID	0	0	0-1	0	0	0
SN1-Data-Tunnel-Ignore-DF-Bit	0	0	0-1	0	0	0
SN1-DHCP-Lease-Expiry-Policy	0	0	0-1	0	0	0
SN1-Disconnect-Reason	0	0	0	0	0-1	0-1
SN1-DNS-Proxy-Intercept-List	0	0	1	0	0	0
SN1-DNS-Proxy-Use-Subscr-Addr	0	0	1	0	0	0
SN1-Ecs-Data-Volume	0	0	0	0-1	0-1	0-1
SN1-Enable-QoS-Renegotiation	0	0	0-1	0	0	0
SN1-Ext-Inline-Srvr-Context	0	0	0-1	0	0	0
SN1-Ext-Inline-Srvr-Down-Addr	0	0	0-1	0	0	0
SN1-Ext-Inline-Srvr-Down-VLAN	0	0	0-1	0	0	0
SN1-Ext-Inline-Srvr-Preference	0	0	0-1	0	0	0
SN1-Ext-Inline-Srvr-Up-Addr	0	0	0-1	0	0	0
SN1-Ext-Inline-Srvr-Up-VLAN	0	0	0-1	0	0	0
SN1-Firewall-Enabled	0	0	0	1	1	1
SN1-GTP-Version	0-1	0	0	0-1	0-1	0-1
SN1-Home-Behavior	0	0	0-1	0	0	0
SN1-Home-Profile	0	0	0-1	0	0	0
SN1-Home-Sub-Use-GGSN	0	0	0-1	0	0	0
SN1-Inactivity-Time	0	0	0-1	0	0	0
SN1-IP-Filter-In	0	0	0+	0	0	0
SN1-IP-Filter-Out	0	0	0+	0	0	0
SN1-IP-Hide-Service-Address	0	0	0-1	0	0	0
SN1-IP-In-Plcy-Grp	0	0	0-1	0	0	0
SN1-IP-Out-Plcy-Grp	0	0	0-1	0	0	0
SN1-IP-Source-Validation	0	0	0-1	0	0	0
SN1-IP-Source-Violate-No-Acct	0	0	0-1	0	0	0
SN1-IPv6-DNS-Proxy	0	0	0-1	0	0	0
SN1-IPv6-Egress-Filtering	0	0	0-1	0	0	0

Attribute	GGSN Access-Request	GGSN Access-Reject	GGSN Access-Accept	GGSN Acct-Request-Start	GGSN Acct-Request-Interim	GGSN Acct-Request-Stop
SN1-IPv6-Min-Link-MTU	0	0	0-1	0	0	0
SN1-IPv6-num-rtr-advt	0	0	0-1	0	0	0
SN1-IPv6-Primary-DNS	0	0	0-1	0	0	0
SN1-IPv6-rtr-advt-interval	0	0	0-1	0	0	0
SN1-IPv6-Secondary-DNS	0	0	0-1	0	0	0
SN1-IPv6-Sec-Pool	0	0	0+	0	0	0
SN1-IPv6-Sec-Prefix	0	0	0+	0	0	0
SN1-L3-to-L2-Tun-Addr-Policy	0	0	0-1	0	0	0
SN1-Local-IP-Address	0-1	0	0-1	1	1	1
SN1-Long-Duration-Action	0	0	0-1	0	0	0
SN1-Long-Duration-Notification	0	0	0-1	0	0	0
SN1-Long-Duration-Timeout	0	0	0-1	0	0	0
SN1-Mediation-Acct-Rsp-Action	0	0	0-1	1	1	1
SN1-Mediation-Enabled	0	0	0-1	1	1	1
SN1-Mediation-No-Interims	0	0	0-1	1	1	1
SN1-Mediation-VPN-Name	0	0	0-1	1	1	1
SN1-Min-Compress-Size	0	0	0-1	0	0	0
SN1-MIP-HA-Assignment-Table	0	0	1	0	0	0
SN1-NPU-Qos-Priority	0	0	0-1	0	0	0
SN1-Overload-Disc-Connect-Time	0	0	0-1	0	0	0
SN1-Overload-Disc-Inact-Time	0	0	0-1	0	0	0
SN1-Overload-Disconnect	0	0	0-1	0	0	0
SN1-Permit-User-Mcast-PDUs	0	0	0-1	0	0	0
SN1-PPP-Accept-Peer-v6Ifid	0	0	0-1	0	0	0
SN1-PPP-Always-On-Vse	0	0	0-1	0	0	0
SN1-PPP-Data-Compression	0	0	0-1	0-1	0-1	0-1
SN1-PPP-Data-Compression-Mode	0	0	0-1	0-1	0-1	0-1
SN1-PPP-Keepalive	0	0	0-1	0	0	0
SN1-PPP-NW-Layer-IPv4	0	0	0-1	0	0	0
SN1-PPP-NW-Layer-IPv6	0	0	0-1	0	0	0
SN1-PPP-Outbound-Username	0	0	0-1	0	0	0
SN1-PPP-Reneg-Disc	0	0	0-1	0	0	0
SN1-Primary-DCCA-Peer	0	0	0-1	0-1	0-1	0-1
SN1-Primary-DNS-Server	0	0	0-1	0	0	0
SN1-Primary-NBNS-Server	0	0	0-1	0	0	0
SN1-QoS-Background-Class	0	0	0-1	0	0	0
SN1-QoS-Conversation-Class	0	0	0-1	0	0	0
SN1-QoS-Interactive1-Class	0	0	0-1	0	0	0
SN1-QoS-Interactive2-Class	0	0	0-1	0	0	0
SN1-QoS-Interactive3-Class	0	0	0-1	0	0	0
SN1-QoS-Renegotiation-Timeout	0	0	0-1	0	0	0
SN1-QoS-Streaming-Class	0	0	0-1	0	0	0
SN1-QoS-Tp-Dnlk	0	0	0-1	0	0	0
SN1-QoS-Tp-Uplk	0	0	0-1	0	0	0
SN1-Radius-Returned-Username	0	0	0-1	0	0	0
SN1-Re-CHAP-Interval	0	0	0-1	0	0	0

Attribute	GGSN Access-Request	GGSN Access-Reject	GGSN Access-Accept	GGSN Acct-Request-Start	GGSN Acct-Request-Interim	GGSN Acct-Request-Stop
SN1-Roaming-Behavior	0	0	0-1	0	0	0
SN1-Roaming-Profile	0	0	0-1	0	0	0
SN1-Roaming-Sub-Use-GGSN	0	0	0-1	0	0	0
SN1-ROHC-Flow-Marking-Mode	0	0	0-1	0	0	0
SN1-ROHC-Profile-Name	0	0	0-1	0	0	0
SN1-Rulebase	0	0	0-1	1	1	1
SN1-Secondary-DCCA-Peer	0	0	0-1	0	0	0
SN1-Secondary-DNS-Server	0	0	0-1	0	0	0
SN1-Secondary-NBNS-Server	0	0	0-1	0	0	0
SN1-Subs-Acc-Flow-Traffic-Valid	0	0	0-1	0	0	0
SN1-Subscriber-Accounting	0	0	0-1	1	1	1
SN1-Subscriber-Acct-Interim	0	0	0-1	0	0	0
SN1-Subscriber-Acct-Mode	0	0	0-1	0	0	0
SN1-Subscriber-Acct-Rsp-Action	0	0	0-1	0	0	0
SN1-Subscriber-Acct-Start	0	0	0-1	0	0	0
SN1-Subscriber-Acct-Stop	0	0	0-1	0	0	0
SN1-Subscriber-Dormant-Activity	0	0	0-1	0	0	0
SN1-Subscriber-IP-Hdr-Neg-Mode	0	0	0-1	0	0	0
SN1-Subscriber-IP-TOS-Copy	0	0	0-1	0	0	0
SN1-Subscriber-Nexthop-Address	0	0	0-1	1	1	1
SN1-Subscriber-No-Interims	0	0	0-1	0	0	0
SN1-Subscriber-Permission	0	0	0-1	0	0	0
SN1-Subs-IMSA-Service-Name	0	0	0-1	0	0	0
SN1-Subs-VJ-Slotid-Cmp-Neg-Mode	0	0	0-1	0	0	0
SN1-Tp-Dnlk-Burst-Size	0	0	0-1	0	0	0
SN1-Tp-Dnlk-Committed-Data-Rate	0	0	0-1	0	0	0
SN1-Tp-Dnlk-Exceed-Action	0	0	0-1	0	0	0
SN1-Tp-Dnlk-Peak-Data-Rate	0	0	0-1	0	0	0
SN1-Tp-Dnlk-Violate-Action	0	0	0-1	0	0	0
SN1-Tp-Uplk-Burst-Size	0	0	0-1	0	0	0
SN1-Tp-Uplk-Committed-Data-Rate	0	0	0-1	0	0	0
SN1-Tp-Uplk-Exceed-Action	0	0	0-1	0	0	0
SN1-Tp-Uplk-Peak-Data-Rate	0	0	0-1	0	0	0
SN1-Tp-Uplk-Violate-Action	0	0	0-1	0	0	0
SN1-Transparent-Data	0	0	0-1	0-1	0-1	0-1
SN1-Tun-Addr-Policy	0	0	0-1	0	0	0
SN1-Tunnel-Gn	0	0	0-1	1	1	1
SN1-Tunnel-ISAKMP-Crypto-Map	0	0	0-1	0	0	0
SN1-Tunnel-ISAKMP-Secret	0	0	0-1	0	0	0
SN1-Tunnel-Load-Balancing	0	0	0-1	0	0	0
SN1-Virtual-APN-Name	0-1	0	0-1	0-1	0-1	0-1
SN1-Visiting-Behavior	0	0	0-1	0	0	0
SN1-Visiting-Profile	0	0	0-1	0	0	0
SN1-Visiting-Sub-Use-GGSN	0	0	0-1	0	0	0
SN1-VPN-ID	0	0	0-1	0-1	0-1	0-1
SN1-VPN-Name	0	0	1	0-1	0-1	0-1

Attribute	GGSN Access-Request	GGSN Access-Reject	GGSN Access-Accept	GGSN Acct-Request-Start	GGSN Acct-Request-Interim	GGSN Acct-Request-Stop
SN-Access-link-IP-Frag	0	0	0-1	0	0	0
SN-Acs-Credit-Control-Group	0	0	0-1	0-1	0-1	0-1
SN-Assigned-VLAN-ID	0	0	0-1	0-1	0-1	0-1
SN-Bandwidth-Policy	0	0	1	0	0	0
SN-CBB-Policy	0	0	1	0	0	0
SN-CFPolicy-ID	0	0	0-1	0	0	0
SN-Data-Tunnel-Ignore-DF-Bit	0	0	0-1	0	0	0
SN-DHCP-Lease-Expiry-Policy	0	0	0-1	0	0	0
SN-Disconnect-Reason	0	0	0	0	0-1	0-1
SN-DNS-Proxy-Intercept-List	0	0	1	0	0	0
SN-DNS-Proxy-Use-Subscr-Addr	0	0	1	0	0	0
SN-Ecs-Data-Volume	0	0	0	0-1	0-1	0-1
SN-Enable-QoS-Renegotiation	0	0	0-1	0	0	0
SN-Ext-Inline-Srvr-Context	0	0	0-1	0	0	0
SN-Ext-Inline-Srvr-Down-Addr	0	0	0-1	0	0	0
SN-Ext-Inline-Srvr-Down-VLAN	0	0	0-1	0	0	0
SN-Ext-Inline-Srvr-Preference	0	0	0-1	0	0	0
SN-Ext-Inline-Srvr-Up-Addr	0	0	0-1	0	0	0
SN-Ext-Inline-Srvr-Up-VLAN	0	0	0-1	0	0	0
SN-Fast-Reauth-Username	0	0	0-1	0	0	0
SN-Firewall-Enabled	0	0	0	1	1	1
SN-Firewall-Policy	0	0	1	0	0	0
SN-GTP-Version	0-1	0	0	0-1	0-1	0-1
SN-Home-Behavior	0	0	0-1	0	0	0
SN-Home-Profile	0	0	0-1	0	0	0
SN-Home-Sub-Use-GGSN	0	0	0-1	0	0	0
SN-Inactivity-Time	0	0	0-1	0	0	0
SN-IP-Filter-In	0	0	0+	0	0	0
SN-IP-Filter-Out	0	0	0+	0	0	0
SN-IP-Hide-Service-Address	0	0	0-1	0	0	0
SN-IP-In-Plcy-Grp	0	0	0-1	0	0	0
SN-IP-Out-Plcy-Grp	0	0	0-1	0	0	0
SN-IP-Source-Validation	0	0	0-1	0	0	0
SN-IP-Source-Violate-No-Acct	0	0	0-1	0	0	0
SN-IPv6-DNS-Proxy	0	0	0-1	0	0	0
SN-IPv6-Egress-Filtering	0	0	0-1	0	0	0
SN-IPv6-Min-Link-MTU	0	0	0-1	0	0	0
SN-IPv6-num-rtr-advt	0	0	0-1	0	0	0
SN-IPv6-Primary-DNS	0	0	0-1	0	0	0
SN-IPv6-rtr-advt-interval	0	0	0-1	0	0	0
SN-IPv6-Secondary-DNS	0	0	0-1	0	0	0
SN-IPv6-Sec-Pool	0	0	0+	0	0	0
SN-IPv6-Sec-Prefix	0	0	0+	0	0	0
SN-L3-to-L2-Tun-Addr-Policy	0	0	0-1	0	0	0
SN-Local-IP-Address	0-1	0	0-1	1	1	1
SN-Long-Duration-Action	0	0	0-1	0	0	0

Attribute	GGSN Access-Request	GGSN Access-Reject	GGSN Access-Accept	GGSN Acct-Request-Start	GGSN Acct-Request-Interim	GGSN Acct-Request-Stop
SN-Long-Duration-Notification	0	0	0-1	0	0	0
SN-Long-Duration-Timeout	0	0	0-1	0	0	0
SN-Mediation-Acct-Rsp-Action	0	0	0-1	1	1	1
SN-Mediation-Enabled	0	0	0-1	1	1	1
SN-Mediation-No-Interims	0	0	0-1	1	1	1
SN-Mediation-VPN-Name	0	0	0-1	1	1	1
SN-Min-Compress-Size	0	0	0-1	0	0	0
SN-MIP-HA-Assignment-Table	0	0	1	0	0	0
SN-NPU-Qos-Priority	0	0	0-1	0	0	0
SN-Overload-Disc-Connect-Time	0	0	0-1	0	0	0
SN-Overload-Disc-Inact-Time	0	0	0-1	0	0	0
SN-Overload-Disconnect	0	0	0-1	0	0	0
SN-Permit-User-Mcast-PDUs	0	0	0-1	0	0	0
SN-PPP-Accept-Peer-v6Ifid	0	0	0-1	0	0	0
SN-PPP-Always-On-Vse	0	0	0-1	0	0	0
SN-PPP-Data-Compression	0	0	0-1	0-1	0-1	0-1
SN-PPP-Data-Compression-Mode	0	0	0-1	0-1	0-1	0-1
SN-PPP-Keepalive	0	0	0-1	0	0	0
SN-PPP-NW-Layer-IPv4	0	0	0-1	0	0	0
SN-PPP-NW-Layer-IPv6	0	0	0-1	0	0	0
SN-PPP-Outbound-Username	0	0	0-1	0	0	0
SN-PPP-Reneg-Disc	0	0	0-1	0	0	0
SN-Primary-DCCA-Peer	0	0	0-1	0-1	0-1	0-1
SN-Primary-DNS-Server	0	0	0-1	0	0	0
SN-Primary-NBNS-Server	0	0	0-1	0	0	0
SN-Pseudonym-Username	0	0	0-1	0	0	0
SN-QoS-Background-Class	0	0	0-1	0	0	0
SN-QoS-Conversation-Class	0	0	0-1	0	0	0
SN-QoS-Interactive1-Class	0	0	0-1	0	0	0
SN-QoS-Interactive2-Class	0	0	0-1	0	0	0
SN-QoS-Interactive3-Class	0	0	0-1	0	0	0
SN-QoS-Renegotiation-Timeout	0	0	0-1	0	0	0
SN-QoS-Streaming-Class	0	0	0-1	0	0	0
SN-QoS-Tp-Dnlk	0	0	0-1	0	0	0
SN-QoS-Tp-Uplk	0	0	0-1	0	0	0
SN-Radius-Returned-Username	0	0	0-1	0	0	0
SN-Re-CHAP-Interval	0	0	0-1	0	0	0
SN-Roaming-Behavior	0	0	0-1	0	0	0
SN-Roaming-Profile	0	0	0-1	0	0	0
SN-Roaming-Sub-Use-GGSN	0	0	0-1	0	0	0
SN-ROHC-Flow-Marking-Mode	0	0	0-1	0	0	0
SN-ROHC-Profile-Name	0	0	0-1	0	0	0
SN-Rulebase	0	0	0-1	1	1	1
SN-Secondary-DCCA-Peer	0	0	0-1	0	0	0
SN-Secondary-DNS-Server	0	0	0-1	0	0	0
SN-Secondary-NBNS-Server	0	0	0-1	0	0	0

Attribute	GGSN Access-Request	GGSN Access-Reject	GGSN Access-Accept	GGSN Acct-Request-Start	GGSN Acct-Request-Interim	GGSN Acct-Request-Stop
SN-Subs-Acc-Flow-Traffic-Valid	0	0	0-1	0	0	0
SN-Subscriber-Accounting	0	0	0-1	1	1	1
SN-Subscriber-Acct-Interim	0	0	0-1	0	0	0
SN-Subscriber-Acct-Mode	0	0	0-1	0	0	0
SN-Subscriber-Acct-Rsp-Action	0	0	0-1	0	0	0
SN-Subscriber-Acct-Start	0	0	0-1	0	0	0
SN-Subscriber-Acct-Stop	0	0	0-1	0	0	0
SN-Subscriber-Dormant-Activity	0	0	0-1	0	0	0
SN-Subscriber-IP-Hdr-Neg-Mode	0	0	0-1	0	0	0
SN-Subscriber-IP-TOS-Copy	0	0	0-1	0	0	0
SN-Subscriber-Nexthop-Address	0	0	0-1	1	1	1
SN-Subscriber-No-Interims	0	0	0-1	0	0	0
SN-Subscriber-Permission	0	0	0-1	0	0	0
SN-Subs-IMSA-Service-Name	0	0	0-1	0	0	0
SN-Subs-VJ-Slotid-Cmp-Neg-Mode	0	0	0-1	0	0	0
SN-Tp-Dnlk-Burst-Size	0	0	0-1	0	0	0
SN-Tp-Dnlk-Committed-Data-Rate	0	0	0-1	0	0	0
SN-Tp-Dnlk-Exceed-Action	0	0	0-1	0	0	0
SN-Tp-Dnlk-Peak-Data-Rate	0	0	0-1	0	0	0
SN-Tp-Dnlk-Violate-Action	0	0	0-1	0	0	0
SN-TPO-Policy	0	0	0-1	0	0	0
SN-Tp-Uplk-Burst-Size	0	0	0-1	0	0	0
SN-Tp-Uplk-Committed-Data-Rate	0	0	0-1	0	0	0
SN-Tp-Uplk-Exceed-Action	0	0	0-1	0	0	0
SN-Tp-Uplk-Peak-Data-Rate	0	0	0-1	0	0	0
SN-Tp-Uplk-Violate-Action	0	0	0-1	0	0	0
SN-Transparent-Data	0	0	0-1	0-1	0-1	0-1
SN-Tun-Addr-Policy	0	0	0-1	0	0	0
SN-Tunnel-Gn	0	0	0-1	1	1	1
SN-Tunnel-ISAKMP-Crypto-Map	0	0	0-1	0	0	0
SN-Tunnel-ISAKMP-Secret	0	0	0-1	0	0	0
SN-Tunnel-Load-Balancing	0	0	0-1	0	0	0
SN-Virtual-APN-Name	0-1	0	0-1	0-1	0-1	0-1
SN-Visiting-Behavior	0	0	0-1	0	0	0
SN-Visiting-Profile	0	0	0-1	0	0	0
SN-Visiting-Sub-Use-GGSN	0	0	0-1	0	0	0
SN-VPN-ID	0	0	0-1	0-1	0-1	0-1
SN-VPN-Name	0	0	1	0-1	0-1	0-1
State	1	0	0-1	0	0	0
Tunnel-Assignment-ID	0	0	0-1	1	1	1
Tunnel-Client-Auth-ID	0	0	0-1	1	1	1
Tunnel-Client-Endpoint	0	0	0-1	1	1	1
Tunnel-Medium-Type	0	0	0-1	1	1	1
Tunnel-Preference	0	0	0-1	0	0	0
Tunnel-Private-Group-ID	0	0	0-1	1	1	1
Tunnel-Server-Auth-ID	0	0	0-1	1	1	1

Attribute	GGSN Access-Request	GGSN Access-Reject	GGSN Access-Accept	GGSN Acct-Request-Start	GGSN Acct-Request-Interim	GGSN Acct-Request-Stop
Tunnel-Server-Endpoint	0	0	0-1	1	1	1
Tunnel-Type	0	0	0-1	1	1	1
User-Name	1	0	0-1	0-1	0	0-1
User-Password	0-1	0	0	0	0	0
White-List	0	0	1	0	0	0
WiMAX-BS-ID	0	0	0	0-1	0-1	0-1
WiMAX-Home-HNP-PMIP6	0+	0	0+	0+	0+	0+
WiMAX-Home-IPv4-HoA-PMIP6	0-1	0	1	0-1	0-1	0-1
WiMAX-Prepaid-Indicator	0	0	0	0-1	0-1	0-1

WIMAX Attribute/Packet Table

Attribute	WIMAX Access-Request	WIMAX Access-Reject	WIMAX Access-Accept	WIMAX Acct-Request-Start	WIMAX Acct-Request-Interim	WIMAX Acct-Request-Stop
3GPP2-Active-Time	0	0	0	0	0-1	0-1
3GPP2-Beginning-Session	0	0	0	1	0	0
3GPP2-BSID	0-1	0	0	0-1	0-1	0-1
3GPP2-IP-QOS	0	0	0-1	0	0	0
3GPP2-IP-Technology	0	0	0	1	1	1
3GPP2-MIP-Sig-Octet-Count-In	0	0	0	0	0-1	0-1
3GPP2-MIP-Sig-Octet-Count-Out	0	0	0	0	0-1	0-1
3GPP2-MN-HA-Shared-Key	0	0	0-1	0	0	0
3GPP2-MN-HA-SPI	0	0	0-1	0	0	0
3GPP2-Session-Continue	0	0	0	0	0	1
AAA-Session-ID	0-1	0-1	1	0	0	0
Acct-Authentic	0	0	0	0-1	0-1	0-1
Acct-Input-Packets	0	0	0	0	0-1	0-1
Acct-Interim-Interval	0	0	0	0-1	0-1	0-1
Acct-Multi-Session-Id	0	0	0	1	1	1
Acct-Output-Packets	0	0	0	0	0-1	0-1
Acct-Session-Id	0	0	0	1	1	1
Calling-Station-Id	1	0	0	1	1	1
Class	0	0	0-1	0-1	0-1	0-1
Connect-Info	1	0	0-1	1	1	1
CUI	0-1	0	0-1	0-1	0-1	0-1
DHCPMSG-Server-IP	0	0	0-1	0	0	0
DHCP-RK	0	0	0-1	0	0	0
DHCP-RK-Key-ID	0	0	0-1	0	0	0
DHCP-RK-Lifetime	0	0	0-1	0	0	0
EAP-Message	1+	1+	1+	0	0	0
Error-Cause	0	0-1	0	0	0	0
Framed-Interface-Id	0	0	0	0-1	0-1	0-1
Framed-IP-Address	0	0	0-1	1	1	1
Framed-IP-Netmask	0	0	0	0-1	0-1	0-1
Framed-IPv6-Prefix	0	0	0	0-1	0-1	0-1
Framed-MTU	0-1	0	0	0	0	0
HA-IP-MIP4	0	0	0	1	1	1
HA-IP-MIP6	0	0	0	1	1	1
Hotline-Indicator	0	0	0-1	0-1	0-1	0-1
Hotline-Profile-ID	0	0	0-1	0	0	0
Hotline-Session-Timer	0	0	0-1	0	0	0
HTTP-Redirection-Rule	0	0	0+	0	0	0
IP-Redirection-Rule	0	0	0+	0	0	0
MSK	0	0	0-1	0	0	0
NAS-Port-Type	0	0	0	0-1	0-1	0-1
PMIP6-RK-KEY	0	0	0-1	0	0	0
PMIP6-RK-SPI	0	0	0-1	0	0	0

Attribute	WIMAX Access-Request	WIMAX Access-Reject	WIMAX Access-Accept	WIMAX Acct-Request-Start	WIMAX Acct-Request-Interim	WIMAX Acct-Request-Stop
PMIP6-Service-Info	0-1	0	0-1	0	0	0
Primary-DNS-Server	0	0	0	0-1	0-1	0-1
Reply-Message	0	0-1	0-1	0	0	0
Secondary-DNS-Server	0	0	0	0-1	0-1	0-1
Service-Type	0	0	0	0-1	0-1	0-1
Session-Timeout	0	0-1	0-1	0	0	0
SN1-Disconnect-Reason	0	0	0	0	0	1
SN1-Prepaid-Compressed-Count	0	0	0	0	0-1	0-1
SN1-Primary-DNS-Server	0	0	0	0-1	0-1	0-1
SN1-Proxy-MIP	0	0	0	0-1	0-1	0-1
SN1-Secondary-DNS-Server	0	0	0	0-1	0-1	0-1
SN1-Subscriber-Accounting	0	0	0	1	1	1
SN1-VPN-ID	0	0	0-1	0-1	0-1	0-1
SN1-VPN-Name	0	0	0-1	0-1	0-1	0-1
SN-DHCP-Options	0	0	0-1	0	0	0
SN-Disconnect-Reason	0	0	0	0	0	1
SN-Handoff-Indicator	0	0	0	0	0-1	0
SN-Prepaid-Compressed-Count	0	0	0	0	0-1	0-1
SN-Primary-DNS-Server	0	0	0	0-1	0-1	0-1
SN-Proxy-MIP	0	0	0	0-1	0-1	0-1
SN-Secondary-DNS-Server	0	0	0	0-1	0-1	0-1
SN-Subscriber-Accounting	0	0	0	1	1	1
SN-VPN-ID	0	0	0-1	0-1	0-1	0-1
SN-VPN-Name	0	0	0-1	0-1	0-1	0-1
SN-WiMAX-Auth-Only	0	0	0-1	0	0	0
State	0-1	0-1	0-1	0	0	0
User-Name	1	0	0-1	1	1	1
WiMAX-Active-Time	0	0	0	0	0-1	0-1
WiMAX-Beginning-Of-Session	0	0	0	1	0	0
WiMAX-BS-ID	0-1	0	0	0-1	0-1	0-1
WiMAX-Control-Octets-In	0	0	0	0	0-1	0-1
WiMAX-Control-Octets-Out	0	0	0	0	0-1	0-1
WiMAX-Control-Packets-In	0	0	0	0	0-1	0-1
WiMAX-Control-Packets-Out	0	0	0	0	0-1	0-1
WiMAX-Count-Type	0	0	0	0	0-1	0-1
WiMAX-Device-Auth-Indicator	0-1	0	0	0	0	0
WiMAX-Home-HNP-PMIP6	0	0	0	0-1	0-1	0-1
WiMAX-Home-IPv4-HoA-PMIP6	0	0	0-1	1	1	1
WiMAX-Idle-Mode-Transition	0	0	0	0	0-1	0
WiMAX-IP-Technology	0	0	0	1	1	1
WiMAX-NAP-ID	0-1	0	0	0-1	0-1	0-1
WiMAX-NSP-ID	0-1	0	0	0-1	0-1	0-1
WiMAX-Packet-Flow-Descriptor	0	0	0+	0	0	0
WiMAX-Packet-Flow-Descriptor-V2	0	0	0+	0	0	0
WiMAX-PDF-ID	0	0	1	0-1	0-1	0-1
WiMAX-Prepaid-Indicator	0	0	0	0-1	0-1	0-1

Attribute	WIMAX Access-Request	WIMAX Access-Reject	WIMAX Access-Accept	WIMAX Acct-Request-Start	WIMAX Acct-Request-Interim	WIMAX Acct-Request-Stop
WiMAX-QoS-Descriptor	0	0	0+	0	0	0
WiMAX-SDF-ID	0	0	0-1	0-1	0-1	0-1
WiMAX-Session-Continue	0	0	0	0	0	1

CSCF Attribute/Packet Table

Attribute	CSCF Access-Request	CSCF Access-Reject	CSCF Access-Accept	CSCF Acct-Request-Start	CSCF Acct-Request-Interim	CSCF Acct-Request-Stop
Acct-Interim-Interval	0	0	0	0-1	0-1	0-1
Called-Station-ID	0	0	0	1	1	1
Digest-AKA-Auts	0-1	0	0	0	0	0
Digest-Algorithm	0-1	0	0-1	0	0	0
Digest-Auth-Param	0+	0	0+	0	0	0
Digest-CNonce	0-1	0	0	0	0	0
Digest-Domain	0	0	0+	0	0	0
Digest-Entity-Body-Hash	0-1	0	0	0	0	0
Digest-HA1	0	0	0-1	0	0	0
Digest-Method	0-1	0	0	0	0	0
Digest-Nextnonce	0-1	0	0-1	0	0	0
Digest-Nonce	0-1	0	0-1	0	0	0
Digest-Nonce-Count	0-1	0	0	0	0	0
Digest-Opaque	0-1	0	0-1	0	0	0
Digest-Qop	0-1	0	0+	0	0	0
Digest-Realm	0-1	0	0-1	0	0	0
Digest-Response	0-1	0	0-1	0	0	0
Digest-Response-Auth	0-1	0	0-1	0	0	0
Digest-Stale	0	0	0-1	0	0	0
Digest-URI	0-1	0	0-1	0	0	0
Digest-Username	0-1	0	0	0	0	0
Framed-Interface-Id	0-1	0	0-1	0	0	0
Framed-IP-Address	0-1	0	0-1	0	0	0
Framed-IPv6-Prefix	0-1	0	0-1	0	0	0
NAS-Port-Type	1	0	0	1	1	1
SIP-AOR	0-1	0	0	0	0	0
SN-Cause-Code	0	0	0	0	0	0-1
SN-CF-Call-International	0	0	0-1	0	0	0
SN-CF-Call-Local	0	0	0-1	0	0	0
SN-CF-Call-LongDistance	0	0	0-1	0	0	0
SN-CF-Call-Premium	0	0	0-1	0	0	0
SN-CF-Call-RoamingInternatnl	0	0	0-1	0	0	0
SN-CF-Call-Transfer	0	0	0-1	0	0	0
SN-CF-Call-Waiting	0	0	0-1	0	0	0
SN-CF-CId-Display	0	0	0-1	0	0	0
SN-CF-CId-Display-Blocked	0	0	0-1	0	0	0
SN-CF-Follow-Me	0	0	0+	0	0	0
SN-CF-Forward-Busy-Line	0	0	0-1	0	0	0
SN-CF-Forward-No-Answer	0	0	0-1	0	0	0
SN-CF-Forward-Not-Regd	0	0	0-1	0	0	0
SN-CF-Forward-Unconditional	0	0	0-1	0	0	0
SN-Content-Disposition	0	0	0	0-1	0-1	0-1
SN-Content-Length	0	0	0	0-1	0-1	0-1

Attribute	CSCF Access-Request	CSCF Access-Reject	CSCF Access-Accept	CSCF Acct-Request-Start	CSCF Acct-Request-Interim	CSCF Acct-Request-Stop
SN-Content-Type	0	0	0	0-1	0-1	0-1
SN-CR-International-Cid	0	0	0-1	0	0	0
SN-CR-LongDistance-Cid	0	0	0-1	0	0	0
SN-Cscf-Subscriber-Ip-Address	0	0	0-1	0	0	0
SN-Event	0	0	0	0-1	0-1	0-1
SN-GGSN-Address	0	0	0	0-1	0-1	0
SN-IMS-Charging-Identifier	0	0	0	0-1	0-1	0-1
SN-ISC-Template-Name	0	0	0-1	0	0	0
SN-Is-Unregistered-Subscriber	0	0	0	0-1	0-1	0-1
SN-Node-Functionality	0	0	0	0-1	0-1	0-1
SN-Originating-IOI	0	0	0	0-1	0-1	0-1
SN-Role-Of-Node	0	0	0	0-1	0-1	0-1
SN-SDP-Session-Description	0	0	0	0-1	0-1	0
SN-Session-Id	0	0	0	0-1	0-1	0-1
SN-SIP-Method	0	0	0	0-1	0-1	0-1
SN-SIP-Request-Time-Stamp	0	0	0	0-1	0-1	0-1
SN-SIP-Response-Time-Stamp	0	0	0	0-1	0-1	0-1
SN-Terminating-IOI	0	0	0	0-1	0-1	0-1
State	0-1	0	0-1	0	0	0
User-Name	1	0	0	1	1	1
WiMAX-Home-HNP-PMIP6	0-1	0	0-1	0	0	0
WiMAX-Home-IPv4-HoA-PMIP6	0-1	0	0-1	0	0	0

MIPv6HA Attribute/Packet Table

Attribute	MIPv6HA Access-Request	MIPv6HA Access-Reject	MIPv6HA Access-Accept	MIPv6HA Acct-Request-Start	MIPv6HA Acct-Request-Interim	MIPv6HA Acct-Request-Stop
3GPP2-Beginning-Session	0	0	0	0-1	0	0
3GPP2-BSID	0	0	0	0-1	0-1	0-1
3GPP2-Comp-Tunnel-Indicator	0	0	0	1	1	1
3GPP2-Correlation-Id	1	0	0	1	1	1
3GPP2-DNS-Server-IPV6-Addr	0	0	0-1	0	0	0
3GPP2-DNS-Update-Required	0	0	0-1	0	0	0
3GPP2-ESN	1	0	0	0-1	0-1	0-1
3GPP2-IP-QOS	0	0	0-1	1	1	1
3GPP2-IP-Technology	0-1	0	0-1	0	0	0
3GPP2-MEID	0	0	0-1	0-1	0-1	0-1
3GPP2-MIP6-Authenticator	0-1	0	0	0	0	0
3GPP2-MIP6-CoA	0-1	0	0	0-1	0-1	0
3GPP2-MIP6-HA	0-1	0	0	0	0	0
3GPP2-MIP6-HoA	0-1	0	0	0-1	0-1	0
3GPP2-MIP6-HoA-Not-Authorized	0	0	0-1	0	0	0
3GPP2-MIP6-MAC-Mobility-Data	0-1	0	0	0	0	0
3GPP2-MIP6-Mesg-ID	0-1	0	0	0	0	0
3GPP2-MIP6-Session-Key	0	0	0-1	0	0	0
3GPP2-MN-HA-Shared-Key	0	0	0-1	0	0	0
3GPP2-MN-HA-SPI	0-1	0	0	0	0	0
3GPP2-Mobile-Term-Orig-Ind	0	0	0	1	1	1
3GPP2-PMIP-IPv4Session-Info	0-1	0	0-1	0-1	0-1	0-1
3GPP2-PMIP-IPv6Session-Info	0-1	0	0-1	0-1	0-1	0-1
3GPP2-PMIP-NAI	0-1	0	0-1	0-1	0-1	0-1
3GPP2-Service-Option	0	0	0	0-1	0-1	0-1
3GPP2-Serving-PCF	0	0	0	1	1	1
AAA-Session-ID	0-1	0	1	0	0	0
Acct-Authentic	0	0	0	1	1	1
Acct-Input-Packets	0-1	0	0	0	1	1
Acct-Interim-Interval	0	0	0-1	0	0	0
Acct-Multi-Session-Id	0	0	0	0-1	0-1	0-1
Acct-Output-Packets	0-1	0	0	0	1	1
Acct-Session-Id	0	0	0	1	1	1
BU-CoA-Ipv6	0-1	0	0	0	0	0
Called-Station-ID	0	0	0	1	1	1
Calling-Station-Id	1	0	1	1	1	1
CHAP-Challenge	1	0	0	0	0	0
Class	0	0	0-1	0-1	0-1	0-1
CUI	0-1	0	0-1	0	0	0
Error-Cause	0	0-1	0	0	0	0
Framed-Interface-Id	0	0	0	0-1	0-1	0-1
Framed-IPv6-Pool	0	0	0-1	0	0	0
Framed-IPv6-Prefix	0	0	0	0+	0+	0+

Attribute	MIPv6HA Access-Request	MIPv6HA Access-Reject	MIPv6HA Access-Accept	MIPv6HA Acct-Request-Start	MIPv6HA Acct-Request-Interim	MIPv6HA Acct-Request-Stop
Framed-MTU	0	0	0-1	0-1	0-1	0-1
Framed-Pool	0	0	0+	0	0	0
HA-IP-MIP4	1	0	0	1	1	1
HA-IP-MIP6	1	0	0	1	1	1
HA-RK-KEY	0	0	0-1	0	0	0
HA-RK-Lifetime	0	0	0-1	0	0	0
HA-RK-SPI	0-1	0	0-1	0	0	0
hLMA-IPv6-PMIP6	0-1	0	0	0	0	0
Idle-Timeout	0	0	0-1	0	0	0
MN-HA-MIP4-KEY	0	0	1	0	0	0
MN-HA-MIP4-SPI	1	0	1	0	0	0
MN-HA-MIP6-KEY	0	0	0-1	0	0	0
MN-HA-MIP6-SPI	0	0	0-1	0	0	0
NAS-Port	1	0	0	1	1	1
NAS-Port-Type	1	0	0	1	1	1
PMIP6-RK-KEY	0	0	0-1	0	0	0
PMIP6-RK-SPI	0-1	0	0	0	0	0
Reply-Message	0	0-1	0-1	0	0	0
RRQ-HA-IP	0-1	0	0	0	0	0
RRQ-MN-HA-KEY	0	0	0-1	0	0	0
Service-Type	1	0	0-1	1	1	1
Session-Timeout	0	0	0-1	0	0	0
SN1-Access-link-IP-Frag	0	0	0-1	0	0	0
SN1-Admin-Permission	0	0	0-1	0	0	0
SN1-Assigned-VLAN-ID	0	0	0-1	0-1	0-1	0-1
SN1-CFPolicy-ID	0	0	0-1	0	0	0
SN1-Data-Tunnel-Ignore-DF-Bit	0	0	0-1	0	0	0
SN1-DHCP-Lease-Expiry-Policy	0	0	0-1	0	0	0
SN1-Disconnect-Reason	0	0	0	0	0	1
SN1-DNS-Proxy-Intercept-List	0	0	1	0	0	0
SN1-Enable-QoS-Renegotiation	0	0	0-1	0	0	0
SN1-Ext-Inline-Srvr-Context	0	0	0-1	0	0	0
SN1-Ext-Inline-Srvr-Down-Addr	0	0	0-1	0	0	0
SN1-Ext-Inline-Srvr-Down-VLAN	0	0	0-1	0	0	0
SN1-Ext-Inline-Srvr-Preference	0	0	0-1	0	0	0
SN1-Ext-Inline-Srvr-Up-Addr	0	0	0-1	0	0	0
SN1-Ext-Inline-Srvr-Up-VLAN	0	0	0-1	0	0	0
SN1-Firewall-Enabled	0	0	0	1	1	1
SN1-FMC-Location	0	0	0	0-1	0-1	0-1
SN1-Gratuitous-ARP-Aggressive	0	0	0-1	0	0	0
SN1-Ignore-Unknown-HA-Addr-Err	0	0	0-1	0	0	0
SN1-IMS-AM-Address	0	0	0-1	0	0	0
SN1-IMS-AM-Domain-Name	0	0	0-1	0	0	0
SN1-Inactivity-Time	0	0	0-1	0	0	0
SN1-IP-Filter-In	0	0	0+	0	0	0
SN1-IP-Filter-Out	0	0	0+	0	0	0

Attribute	MIPv6HA Access-Request	MIPv6HA Access-Reject	MIPv6HA Access-Accept	MIPv6HA Acct-Request-Start	MIPv6HA Acct-Request-Interim	MIPv6HA Acct-Request-Stop
SN1-IP-Hide-Service-Address	0	0	0-1	0	0	0
SN1-IP-Pool-Name	0	0	0+	0	0	0
SN1-IP-Source-Validation	0	0	0-1	0	0	0
SN1-IP-Source-Violate-No-Acct	0	0	0-1	0	0	0
SN1-IPv6-Primary-DNS	0	0	0-1	0	0	0
SN1-IPv6-Secondary-DNS	0	0	0-1	0	0	0
SN1-IPv6-Sec-Pool	0	0	0+	0	0	0
SN1-IPv6-Sec-Prefix	0	0	0+	0	0	0
SN1-L3-to-L2-Tun-Addr-Policy	0	0	0-1	0	0	0
SN1-Local-IP-Address	0-1	0	0-1	1	1	1
SN1-Long-Duration-Action	0	0	0-1	0	0	0
SN1-Long-Duration-Notification	0	0	0-1	0	0	0
SN1-Long-Duration-Timeout	0	0	0-1	0	0	0
SN1-Mediation-Enabled	0	0	0-1	1	1	1
SN1-Mediation-VPN-Name	0	0	0-1	1	1	1
SN1-MIP-ANCID	0	0	0	0-1	0-1	0-1
SN1-MIP-Dual-Anchor	0	0	0-1	0	0	0
SN1-MIP-HA-Assignment-Table	0	0	1	0	0	0
SN1-MIP-Reg-Lifetime-Realm	0	0	0-1	0	0	0
SN1-MN-HA-Timestamp-Tolerance	0	0	0-1	0	0	0
SN1-NPU-Qos-Priority	0	0	0-1	0	0	0
SN1-Nw-Reachability-Server-Name	0	0	0-1	0	0	0
SN1-Overload-Disc-Connect-Time	0	0	0-1	0	0	0
SN1-Overload-Disc-Inact-Time	0	0	0-1	0	0	0
SN1-Overload-Disconnect	0	0	0-1	0	0	0
SN1-PDSN-Correlation-Id	0	0	0	0-1	0-1	0-1
SN1-PDSN-NAS-Id	0	0	0	0-1	0-1	0-1
SN1-PDSN-NAS-IP-Address	0	0	0	0-1	0-1	0-1
SN1-Permit-User-Mcast-PDUs	0	0	0-1	0	0	0
SN1-Prepaid	0	0	0-1	0	0	0
SN1-Prepaid-Compressed-Count	0-1	0	0-1	0	0	0
SN1-Prepaid-Final-Duration-Alg	0	0	0-1	0	0	0
SN1-Prepaid-Inbound-Octets	0-1	0	0-1	0	0	0
SN1-Prepaid-Outbound-Octets	0-1	0	0-1	0	0	0
SN1-Prepaid-Preference	0	0	0-1	0	0	0
SN1-Prepaid-Timeout	0-1	0	0-1	0	0	0
SN1-Prepaid-Total-Octets	0-1	0	0-1	0	0	0
SN1-Prepaid-Watermark	0-1	0	0-1	0	0	0
SN1-Primary-DCCA-Peer	0	0	0-1	0	0	0
SN1-QoS-Background-Class	0	0	0-1	0	0	0
SN1-QoS-Conversation-Class	0	0	0-1	0	0	0
SN1-QoS-Interactive1-Class	0	0	0-1	0	0	0
SN1-QoS-Interactive2-Class	0	0	0-1	0	0	0
SN1-QoS-Interactive3-Class	0	0	0-1	0	0	0
SN1-QoS-Renegotiation-Timeout	0	0	0-1	0	0	0
SN1-QoS-Streaming-Class	0	0	0-1	0	0	0

Attribute	MIPv6HA Access-Request	MIPv6HA Access-Reject	MIPv6HA Access-Accept	MIPv6HA Acct-Request-Start	MIPv6HA Acct-Request-Interim	MIPv6HA Acct-Request-Stop
SN1-QoS-Tp-Dnlk	0	0	0-1	0	0	0
SN1-QoS-Tp-Uplk	0	0	0-1	0	0	0
SN1-Re-CHAP-Interval	0	0	0-1	0-1	0-1	0-1
SN1-Rulebase	0	0	0-1	1	1	1
SN1-Secondary-DCCA-Peer	0	0	0-1	0	0	0
SN1-Subscriber-Accounting	0	0	0-1	1	1	1
SN1-Subscriber-Acct-Interim	0	0	0-1	0	0	0
SN1-Subscriber-Acct-Mode	0	0	0-1	0	0	0
SN1-Subscriber-Acct-Rsp-Action	0	0	0-1	0	0	0
SN1-Subscriber-Acct-Start	0	0	0-1	0	0	0
SN1-Subscriber-Acct-Stop	0	0	0-1	0	0	0
SN1-Subscriber-Class	0	0	0-1	0-1	0-1	0-1
SN1-Subscriber-IP-TOS-Copy	0	0	0-1	0	0	0
SN1-Subscriber-Nexthop-Address	0	0	0-1	1	1	1
SN1-Subscriber-No-Interims	0	0	0-1	0	0	0
SN1-Subscriber-Permission	0	0	0-1	0	0	0
SN1-Subs-IMSA-Service-Name	0	0	0-1	0	0	0
SN1-Tp-Dnlk-Burst-Size	0	0	0-1	0	0	0
SN1-Tp-Dnlk-Committed-Data-Rate	0	0	0-1	0	0	0
SN1-Tp-Dnlk-Exceed-Action	0	0	0-1	0	0	0
SN1-Tp-Dnlk-Peak-Data-Rate	0	0	0-1	0	0	0
SN1-Tp-Dnlk-Violate-Action	0	0	0-1	0	0	0
SN1-Tp-Uplk-Burst-Size	0	0	0-1	0	0	0
SN1-Tp-Uplk-Committed-Data-Rate	0	0	0-1	0	0	0
SN1-Tp-Uplk-Exceed-Action	0	0	0-1	0	0	0
SN1-Tp-Uplk-Peak-Data-Rate	0	0	0-1	0	0	0
SN1-Tp-Uplk-Violate-Action	0	0	0-1	0	0	0
SN1-Tun-Addr-Policy	0	0	0-1	0	0	0
SN1-Tunnel-ISAKMP-Crypto-Map	0	0	0-1	0	0	0
SN1-Tunnel-ISAKMP-Secret	0	0	0-1	0	0	0
SN1-Tunnel-Load-Balancing	0	0	0-1	0	0	0
SN1-Unclassify-List-Name	0	0	0-1	0	0	0
SN1-Voice-Push-List-Name	0	0	0-1	0	0	0
SN1-VPN-ID	0	0	0-1	0-1	0-1	0-1
SN1-VPN-Name	0	0	1	0-1	0-1	0-1
SN-Access-link-IP-Frag	0	0	0-1	0	0	0
SN-Acs-Credit-Control-Group	0	0	0-1	0-1	0-1	0-1
SN-Admin-Permission	0	0	0-1	0	0	0
SN-Assigned-VLAN-ID	0	0	0-1	0-1	0-1	0-1
SN-Bandwidth-Policy	0	0	1	0	0	0
SN-CBB-Policy	0	0	1	0	0	0
SN-CFPolicy-ID	0	0	0-1	0	0	0
SN-Data-Tunnel-Ignore-DF-Bit	0	0	0-1	0	0	0
SN-DHCP-Lease-Expiry-Policy	0	0	0-1	0	0	0
SN-Disconnect-Reason	0	0	0	0	0	1
SN-DNS-Proxy-Intercept-List	0	0	1	0	0	0

Attribute	MIPv6HA Access-Request	MIPv6HA Access-Reject	MIPv6HA Access-Accept	MIPv6HA Acct-Request-Start	MIPv6HA Acct-Request-Interim	MIPv6HA Acct-Request-Stop
SN-Enable-QoS-Renegotiation	0	0	0-1	0	0	0
SN-Ext-Inline-Srvr-Context	0	0	0-1	0	0	0
SN-Ext-Inline-Srvr-Down-Addr	0	0	0-1	0	0	0
SN-Ext-Inline-Srvr-Down-VLAN	0	0	0-1	0	0	0
SN-Ext-Inline-Srvr-Preference	0	0	0-1	0	0	0
SN-Ext-Inline-Srvr-Up-Addr	0	0	0-1	0	0	0
SN-Ext-Inline-Srvr-Up-VLAN	0	0	0-1	0	0	0
SN-Firewall-Enabled	0	0	0	1	1	1
SN-Firewall-Policy	0	0	1	0	0	0
SN-FMC-Location	0	0	0	0-1	0-1	0-1
SN-Gratuitous-ARP-Aggressive	0	0	0-1	0	0	0
SN-Ignore-Unknown-HA-Addr-Error	0	0	0-1	0	0	0
SN-IMS-AM-Address	0	0	0-1	0	0	0
SN-IMS-AM-Domain-Name	0	0	0-1	0	0	0
SN-Inactivity-Time	0	0	0-1	0	0	0
SN-IP-Filter-In	0	0	0+	0	0	0
SN-IP-Filter-Out	0	0	0+	0	0	0
SN-IP-Hide-Service-Address	0	0	0-1	0	0	0
SN-IP-Pool-Name	0	0	0+	0	0	0
SN-IP-Source-Validation	0	0	0-1	0	0	0
SN-IP-Source-Violate-No-Acct	0	0	0-1	0	0	0
SN-IPv6-Primary-DNS	0	0	0-1	0	0	0
SN-IPv6-Secondary-DNS	0	0	0-1	0	0	0
SN-IPv6-Sec-Pool	0	0	0+	0	0	0
SN-IPv6-Sec-Prefix	0	0	0+	0	0	0
SN-L3-to-L2-Tun-Addr-Policy	0	0	0-1	0	0	0
SN-Local-IP-Address	0-1	0	0-1	1	1	1
SN-Long-Duration-Action	0	0	0-1	0	0	0
SN-Long-Duration-Notification	0	0	0-1	0	0	0
SN-Long-Duration-Timeout	0	0	0-1	0	0	0
SN-Mediation-Enabled	0	0	0-1	1	1	1
SN-Mediation-VPN-Name	0	0	0-1	1	1	1
SN-MIP-ANCID	0	0	0	0-1	0-1	0-1
SN-MIP-Dual-Anchor	0	0	0-1	0	0	0
SN-MIP-HA-Assignment-Table	0	0	1	0	0	0
SN-MIP-Reg-Lifetime-Realm	0	0	0-1	0	0	0
SN-MN-HA-Timestamp-Tolerance	0	0	0-1	0	0	0
SN-NPU-Qos-Priority	0	0	0-1	0	0	0
SN-Nw-Reachability-Server-Name	0	0	0-1	0	0	0
SN-Overload-Disc-Connect-Time	0	0	0-1	0	0	0
SN-Overload-Disc-Inact-Time	0	0	0-1	0	0	0
SN-Overload-Disconnect	0	0	0-1	0	0	0
SN-PDSN-Correlation-Id	0	0	0	0-1	0-1	0-1
SN-PDSN-NAS-Id	0	0	0	0-1	0-1	0-1
SN-PDSN-NAS-IP-Address	0	0	0	0-1	0-1	0-1
SN-Permit-User-Mcast-PDUs	0	0	0-1	0	0	0

Attribute	MIPv6HA Access-Request	MIPv6HA Access-Reject	MIPv6HA Access-Accept	MIPv6HA Acct-Request-Start	MIPv6HA Acct-Request-Interim	MIPv6HA Acct-Request-Stop
SN-Prepaid	0	0	0-1	0	0	0
SN-Prepaid-Compressed-Count	0-1	0	0-1	0	0	0
SN-Prepaid-Final-Duration-Alg	0	0	0-1	0	0	0
SN-Prepaid-Inbound-Octets	0-1	0	0-1	0	0	0
SN-Prepaid-Outbound-Octets	0-1	0	0-1	0	0	0
SN-Prepaid-Preference	0	0	0-1	0	0	0
SN-Prepaid-Timeout	0-1	0	0-1	0	0	0
SN-Prepaid-Total-Octets	0-1	0	0-1	0	0	0
SN-Prepaid-Watermark	0-1	0	0-1	0	0	0
SN-Primary-DCCA-Peer	0	0	0-1	0	0	0
SN-QoS-Background-Class	0	0	0-1	0	0	0
SN-QoS-Conversation-Class	0	0	0-1	0	0	0
SN-QoS-Interactive1-Class	0	0	0-1	0	0	0
SN-QoS-Interactive2-Class	0	0	0-1	0	0	0
SN-QoS-Interactive3-Class	0	0	0-1	0	0	0
SN-QoS-Renegotiation-Timeout	0	0	0-1	0	0	0
SN-QoS-Streaming-Class	0	0	0-1	0	0	0
SN-QoS-Tp-Dnlk	0	0	0-1	0	0	0
SN-QoS-Tp-Uplk	0	0	0-1	0	0	0
SN-Re-CHAP-Interval	0	0	0-1	0-1	0-1	0-1
SN-Rulebase	0	0	0-1	1	1	1
SN-Secondary-DCCA-Peer	0	0	0-1	0	0	0
SN-Subscriber-Accounting	0	0	0-1	1	1	1
SN-Subscriber-Acct-Interim	0	0	0-1	0	0	0
SN-Subscriber-Acct-Mode	0	0	0-1	0	0	0
SN-Subscriber-Acct-Rsp-Action	0	0	0-1	0	0	0
SN-Subscriber-Acct-Start	0	0	0-1	0	0	0
SN-Subscriber-Acct-Stop	0	0	0-1	0	0	0
SN-Subscriber-Class	0	0	0-1	0-1	0-1	0-1
SN-Subscriber-IP-TOS-Copy	0	0	0-1	0	0	0
SN-Subscriber-Nexthop-Address	0	0	0-1	1	1	1
SN-Subscriber-No-Interims	0	0	0-1	0	0	0
SN-Subscriber-Permission	0	0	0-1	0	0	0
SN-Subs-IMSA-Service-Name	0	0	0-1	0	0	0
SN-Tp-Dnlk-Burst-Size	0	0	0-1	0	0	0
SN-Tp-Dnlk-Committed-Data-Rate	0	0	0-1	0	0	0
SN-Tp-Dnlk-Exceed-Action	0	0	0-1	0	0	0
SN-Tp-Dnlk-Peak-Data-Rate	0	0	0-1	0	0	0
SN-Tp-Dnlk-Violate-Action	0	0	0-1	0	0	0
SN-TPO-Policy	0	0	0-1	0	0	0
SN-Tp-Uplk-Burst-Size	0	0	0-1	0	0	0
SN-Tp-Uplk-Committed-Data-Rate	0	0	0-1	0	0	0
SN-Tp-Uplk-Exceed-Action	0	0	0-1	0	0	0
SN-Tp-Uplk-Peak-Data-Rate	0	0	0-1	0	0	0
SN-Tp-Uplk-Violate-Action	0	0	0-1	0	0	0
SN-TrafficSelector-Class	0	0	0-1	0	0	0

Attribute	MIPv6HA Access-Request	MIPv6HA Access-Reject	MIPv6HA Access-Accept	MIPv6HA Acct-Request-Start	MIPv6HA Acct-Request-Interim	MIPv6HA Acct-Request-Stop
SN-Tun-Addr-Policy	0	0	0-1	0	0	0
SN-Tunnel-ISAKMP-Crypto-Map	0	0	0-1	0	0	0
SN-Tunnel-ISAKMP-Secret	0	0	0-1	0	0	0
SN-Tunnel-Load-Balancing	0	0	0-1	0	0	0
SN-Unclassify-List-Name	0	0	0-1	0	0	0
SN-Voice-Push-List-Name	0	0	0-1	0	0	0
SN-VPN-ID	0	0	0-1	0-1	0-1	0-1
SN-VPN-Name	0	0	1	0-1	0-1	0-1
State	1	0	0-1	0	0	0
Tunnel-Assignment-ID	0	0	0-1	1	1	1
Tunnel-Client-Auth-ID	0	0	0-1	1	1	1
Tunnel-Client-Endpoint	0	0	0-1	1	1	1
Tunnel-Medium-Type	0	0	0-1	1	1	1
Tunnel-Preference	0	0	0-1	0	0	0
Tunnel-Private-Group-ID	0	0	0-1	1	1	1
Tunnel-Server-Auth-ID	0	0	0-1	1	1	1
Tunnel-Server-Endpoint	0	0	0-1	1	1	1
Tunnel-Type	0	0	0-1	1	1	1
User-Name	1	0	0-1	1	1	1
WiMAX-Beginning-Of-Session	0	0	0	0-1	0	0
WiMAX-BS-ID	0	0	0	0-1	0-1	0-1
WiMAX-Count-Type	0-1	0	0-1	0	0	0
WiMAX-Home-HNP-PMIP6	0	0	0	0+	0+	0+
WiMAX-IP-Technology	0-1	0	0-1	0	0	0
WiMAX-Prepaid-Indicator	0	0	0	0-1	0-1	0-1

Dictionary Quick Reference

Attribute	standard	3gpp	3gpp2	3gpp2-835	starent	starent-835	starent-vsa1	starent-vsa1-835
3GPP2-835-Release-Indicator	No	No	No	Yes	No	Yes	No	Yes
3GPP2-Acct-Session-Time	No	No	No	Yes	No	Yes	No	Yes
3GPP2-Active-Time	No	No	Yes	Yes	Yes	Yes	Yes	Yes
3GPP2-Active-Time-Corrected	No	No	No	No	No	No	No	No
3GPP2-Airlink-Record-Type	No	No	Yes	Yes	Yes	Yes	Yes	Yes
3GPP2-Airlink-Sequence-Number	No	No	Yes	Yes	Yes	Yes	Yes	Yes
3GPP2-Air-QOS	No	No	Yes	Yes	Yes	Yes	Yes	Yes
3GPP2-Allowed-Diffserv	No	No	Yes	Yes	Yes	Yes	Yes	Yes
3GPP2-Allowed-Persistent-TFTs	No	No	Yes	Yes	Yes	Yes	Yes	Yes
3GPP2-Alternate-Billing-ID	No	No	No	Yes	No	Yes	No	Yes
3GPP2-Always-On	No	No	Yes	Yes	Yes	Yes	Yes	Yes
3GPP2-Auth-Flow-Profile-Id	No	No	Yes	Yes	Yes	Yes	Yes	Yes
3GPP2-Bad-PPP-Frame-Count	No	No	Yes	Yes	Yes	Yes	Yes	Yes
3GPP2-BCMCS-Auth-Parameters	No	No	Yes	Yes	Yes	Yes	Yes	Yes
3GPP2-BCMCS-BSN-Session-Info	No	No	Yes	Yes	Yes	Yes	Yes	Yes
3GPP2-BCMCS-Capability	No	No	Yes	Yes	Yes	Yes	Yes	Yes
3GPP2-BCMCS-Common-Session-Info	No	No	Yes	Yes	Yes	Yes	Yes	Yes
3GPP2-BCMCS-Flow-ID	No	No	Yes	Yes	Yes	Yes	Yes	Yes
3GPP2-BCMCS-Flow-Transmit-Time	No	No	Yes	Yes	Yes	Yes	Yes	Yes
3GPP2-BCMCS-Mcast-IP-Addr	No	No	Yes	Yes	Yes	Yes	Yes	Yes
3GPP2-BCMCS-Mcast-Port	No	No	Yes	Yes	Yes	Yes	Yes	Yes
3GPP2-BCMCS-Reason-Code	No	No	Yes	Yes	Yes	Yes	Yes	Yes
3GPP2-BCMCS-RN-Session-Info	No	No	Yes	Yes	Yes	Yes	Yes	Yes
3GPP2-Beginning-Session	No	No	Yes	Yes	Yes	Yes	Yes	Yes
3GPP2-BSID	No	No	Yes	Yes	Yes	Yes	Yes	Yes
3GPP2-Carrier-ID	No	No	Yes	Yes	Yes	Yes	Yes	Yes
3GPP2-Comp-Tunnel-Indicator	No	No	Yes	Yes	Yes	Yes	Yes	Yes
3GPP2-Container	No	No	Yes	Yes	Yes	Yes	Yes	Yes
3GPP2-Correlation-Id	No	No	Yes	Yes	Yes	Yes	Yes	Yes
3GPP2-Correlation-Id-Long	No	No	No	No	No	No	No	No
3GPP2-Correlation-Id-Old	No	No	No	No	No	No	No	No
3GPP2-DCCH-Frame-Size	No	No	Yes	Yes	Yes	Yes	Yes	Yes
3GPP2-Diff-Service-Class-Option	No	No	No	No	No	No	No	No
3GPP2-Disconnect-Reason	No	No	Yes	Yes	Yes	Yes	Yes	Yes
3GPP2-DNS-Server-IP-Address	No	No	Yes	Yes	Yes	Yes	Yes	Yes
3GPP2-DNS-Server-IPV6-Addr	No	No	Yes	Yes	Yes	Yes	Yes	Yes
3GPP2-DNS-Update-Required	No	No	Yes	Yes	Yes	Yes	Yes	Yes
3GPP2-ESN	No	No	Yes	Yes	Yes	Yes	Yes	Yes
3GPP2-FA-Address	No	No	Yes	Yes	Yes	Yes	Yes	Yes
3GPP2-FEID	No	No	Yes	Yes	Yes	Yes	Yes	Yes
3GPP2-Flow-Id	No	No	Yes	Yes	Yes	Yes	Yes	Yes
3GPP2-Flow-Status	No	No	Yes	Yes	Yes	Yes	Yes	Yes
3GPP2-Forward-Fundamental-Rate	No	No	Yes	Yes	Yes	Yes	Yes	Yes
3GPP2-Forward-Fundamental-RC	No	No	Yes	Yes	Yes	Yes	Yes	Yes

Attribute	standard	3gpp	3gpp2	3gpp2-835	starent	starent-835	starent-vsa1	starent-vsa1-835
3GPP2-Forward-Mux-Option	No	No	Yes	Yes	Yes	Yes	Yes	Yes
3GPP2-Forward-Traffic-Type	No	No	Yes	Yes	Yes	Yes	Yes	Yes
3GPP2-Fundamental-Frame-Size	No	No	Yes	Yes	Yes	Yes	Yes	Yes
3GPP2-Fwd-Dcch-Mux-Option	No	No	Yes	Yes	Yes	Yes	Yes	Yes
3GPP2-Fwd-Dcch-Rc	No	No	Yes	Yes	Yes	Yes	Yes	Yes
3GPP2-Fwd-Pdch-Rc	No	No	Yes	Yes	Yes	Yes	Yes	Yes
3GPP2-GMT-Timezone-Offset	No	No	Yes	Yes	Yes	Yes	Yes	Yes
3GPP2-Granted-QoS	No	No	Yes	Yes	Yes	Yes	Yes	Yes
3GPP2-IKE-Secret	No	No	Yes	Yes	Yes	Yes	Yes	Yes
3GPP2-IKE-Secret-Request	No	No	Yes	Yes	Yes	Yes	Yes	Yes
3GPP2-IKE-Secret-Unencrypted	No	No	No	No	No	No	No	No
3GPP2-IMSI	No	No	No	No	No	No	No	No
3GPP2-Interconnect-IP	No	No	No	Yes	No	Yes	No	Yes
3GPP2-Interconnect-QOS	No	No	No	Yes	No	Yes	No	Yes
3GPP2-Inter-User-Priority	No	No	Yes	Yes	Yes	Yes	Yes	Yes
3GPP2-IP-QOS	No	No	Yes	Yes	Yes	Yes	Yes	Yes
3GPP2-IP-Services-Authorized	No	No	Yes	Yes	Yes	Yes	Yes	Yes
3GPP2-IP-TechNology	No	No	Yes	Yes	Yes	Yes	Yes	Yes
3GPP2-KeyID	No	No	Yes	Yes	Yes	Yes	Yes	Yes
3GPP2-Last-Activity	No	No	Yes	Yes	Yes	Yes	Yes	Yes
3GPP2-Max-Auth-Aggr-Bw-BET	No	No	Yes	Yes	Yes	Yes	Yes	Yes
3GPP2-Max-Per-Fl-Pri-ForTheUser	No	No	Yes	Yes	Yes	Yes	Yes	Yes
3GPP2-MEID	No	No	Yes	Yes	Yes	Yes	Yes	Yes
3GPP2-MIP6-Authenticator	No	No	Yes	Yes	Yes	Yes	Yes	Yes
3GPP2-MIP6-CoA	No	No	Yes	Yes	Yes	Yes	Yes	Yes
3GPP2-MIP6-HA	No	No	Yes	Yes	Yes	Yes	Yes	Yes
3GPP2-MIP6-HoA	No	No	Yes	Yes	Yes	Yes	Yes	Yes
3GPP2-MIP6-HoA-Not-Authorized	No	No	Yes	Yes	Yes	Yes	Yes	Yes
3GPP2-MIP6-Home-Address	No	No	Yes	Yes	Yes	Yes	Yes	Yes
3GPP2-MIP6-Home-Agent	No	No	Yes	Yes	Yes	Yes	Yes	Yes
3GPP2-MIP6-Home-Link-Prefix	No	No	Yes	Yes	Yes	Yes	Yes	Yes
3GPP2-MIP6-MAC-Mobility-Data	No	No	Yes	Yes	Yes	Yes	Yes	Yes
3GPP2-MIP6-Mesg-ID	No	No	Yes	Yes	Yes	Yes	Yes	Yes
3GPP2-MIP6-Session-Key	No	No	Yes	Yes	Yes	Yes	Yes	Yes
3GPP2-MIP-HA-Address	No	No	Yes	Yes	Yes	Yes	Yes	Yes
3GPP2-MIP-Lifetime	No	No	Yes	Yes	Yes	Yes	Yes	Yes
3GPP2-MIP-Rev-Tunnel-Required	No	No	Yes	Yes	Yes	Yes	Yes	Yes
3GPP2-MIP-Sig-Octet-Count-In	No	No	Yes	Yes	Yes	Yes	Yes	Yes
3GPP2-MIP-Sig-Octet-Count-Out	No	No	Yes	Yes	Yes	Yes	Yes	Yes
3GPP2-MN-AAA-Removal-Indication	No	No	Yes	Yes	Yes	Yes	Yes	Yes
3GPP2-MN-HA-Shared-Key	No	No	Yes	Yes	Yes	Yes	Yes	Yes
3GPP2-MN-HA-Shared-Key-No-Enc	No	No	No	No	No	No	No	No
3GPP2-MN-HA-SPI	No	No	Yes	Yes	Yes	Yes	Yes	Yes
3GPP2-Mobile-Term-Orig-Ind	No	No	Yes	Yes	Yes	Yes	Yes	Yes
3GPP2-Number-Active-Transitions	No	No	Yes	Yes	Yes	Yes	Yes	Yes
3GPP2-Num-Bytes-Received-Total	No	No	Yes	Yes	Yes	Yes	Yes	Yes
3GPP2-Num-SDB-Input	No	No	Yes	Yes	Yes	Yes	Yes	Yes
3GPP2-Num-SDB-Output	No	No	Yes	Yes	Yes	Yes	Yes	Yes

Attribute	standard	3gpp	3gpp2	3gpp2-835	starent	starent-835	starent-vsa1	starent-vsa1-835
3GPP2-PMIP-Capability	No	No	Yes	Yes	Yes	Yes	Yes	Yes
3GPP2-PMIP-IPv4Session-Info	No	No	Yes	Yes	Yes	Yes	Yes	Yes
3GPP2-PMIP-IPv6Session-Info	No	No	Yes	Yes	Yes	Yes	Yes	Yes
3GPP2-PMIP-NAI	No	No	Yes	Yes	Yes	Yes	Yes	Yes
3GPP2-Pre-Paid-Accounting-Quota	No	No	Yes	Yes	Yes	Yes	Yes	Yes
3GPP2-Pre-Paid-Acct-Capability	No	No	Yes	Yes	Yes	Yes	Yes	Yes
3GPP2-Pre-Paid-TariffSwitch	No	No	Yes	Yes	Yes	Yes	Yes	Yes
3GPP2-QoS-Service-Opt-Profile	No	No	Yes	Yes	Yes	Yes	Yes	Yes
3GPP2-Release-Indicator	No	No	Yes	No	Yes	No	Yes	No
3GPP2-Release-Indicator-custom9	No	No	No	No	No	No	No	No
3GPP2-Release-Indicator-Old	No	No	No	No	No	No	No	No
3GPP2-Release-Indicator-Prepaid	No	No	No	No	Yes	No	Yes	No
3GPP2-Remote-Addr-Table-Idx-Old	No	No	No	Yes	No	Yes	No	Yes
3GPP2-Remote-Addr-Table-Index	No	No	Yes	No	Yes	No	Yes	No
3GPP2-Remote-IPv4-Address	No	No	Yes	Yes	Yes	Yes	Yes	Yes
3GPP2-Remote-IPv4-Addr-Octets	No	No	Yes	Yes	Yes	Yes	Yes	Yes
3GPP2-Rev-Dcch-Mux-Option	No	No	Yes	Yes	Yes	Yes	Yes	Yes
3GPP2-Rev-Dcch-Rc	No	No	Yes	Yes	Yes	Yes	Yes	Yes
3GPP2-Reverse-Fundamental-Rate	No	No	Yes	Yes	Yes	Yes	Yes	Yes
3GPP2-Reverse-Fundamental-RC	No	No	Yes	Yes	Yes	Yes	Yes	Yes
3GPP2-Reverse-Mux-Option	No	No	Yes	Yes	Yes	Yes	Yes	Yes
3GPP2-Reverse-Traffic-Type	No	No	Yes	Yes	Yes	Yes	Yes	Yes
3GPP2-Rev-Pdch-Rc	No	No	Yes	Yes	Yes	Yes	Yes	Yes
3GPP2-RP-Session-ID	No	No	Yes	Yes	Yes	Yes	Yes	Yes
3GPP2-Rsvp-Signal-In-Count	No	No	Yes	Yes	Yes	Yes	Yes	Yes
3GPP2-Rsvp-Signal-In-Packets	No	No	Yes	Yes	Yes	Yes	Yes	Yes
3GPP2-Rsvp-Signal-Out-Count	No	No	Yes	Yes	Yes	Yes	Yes	Yes
3GPP2-Rsvp-Signal-Out-Packets	No	No	Yes	Yes	Yes	Yes	Yes	Yes
3GPP2-SDB-Input-Octets	No	No	Yes	Yes	Yes	Yes	Yes	Yes
3GPP2-SDB-Output-Octets	No	No	Yes	Yes	Yes	Yes	Yes	Yes
3GPP2-Security-Level	No	No	Yes	Yes	Yes	Yes	Yes	Yes
3GPP2-Service-Option	No	No	Yes	Yes	Yes	Yes	Yes	Yes
3GPP2-Service-Option-Profile	No	No	No	No	No	No	No	No
3GPP2-Service-Reference-ID	No	No	Yes	Yes	Yes	Yes	Yes	Yes
3GPP2-Serving-PCF	No	No	Yes	Yes	Yes	Yes	Yes	Yes
3GPP2-Session-Continue	No	No	Yes	Yes	Yes	Yes	Yes	Yes
3GPP2-Session-Term-Capability	No	No	Yes	Yes	Yes	Yes	Yes	Yes
3GPP2-S-Key	No	No	Yes	Yes	Yes	Yes	Yes	Yes
3GPP2-S-Lifetime	No	No	Yes	Yes	Yes	Yes	Yes	Yes
3GPP2-S-Request	No	No	Yes	Yes	Yes	Yes	Yes	Yes
3GPP2-Subnet	No	No	Yes	Yes	Yes	Yes	Yes	Yes
3GPP2-S-Unencrypted	No	No	No	No	No	No	No	No
3GPP2-User-Zone	No	No	Yes	Yes	Yes	Yes	Yes	Yes
3GPP-Allocate-IPType	No	Yes	No	No	Yes	No	Yes	No
3GPP-CAMEL-Charging-Info	No	Yes	No	No	Yes	No	Yes	No
3GPP-CG-Address	No	Yes	No	No	Yes	No	Yes	No
3GPP-Charging-Id	No	Yes	No	No	Yes	No	Yes	No
3GPP-Chrg-Char	No	Yes	No	No	Yes	No	Yes	No

Attribute	standard	3gpp	3gpp2	3gpp2-835	starent	starent-835	starent-vsa1	starent-vsa1-835
3GPP-GGSN-Address	No	Yes	No	No	Yes	No	Yes	No
3GPP-GGSN-IPv6-Address	No	Yes	No	No	Yes	No	Yes	No
3GPP-GGSN-Mcc-Mnc	No	Yes	No	No	Yes	No	Yes	No
3GPP-IMEISV	No	Yes	No	No	Yes	No	Yes	No
3GPP-IMSI	No	Yes	No	No	Yes	No	Yes	No
3GPP-IMSI-Mcc-Mnc	No	Yes	No	No	Yes	No	Yes	No
3GPP-IPv6-DNS-Servers	No	Yes	No	No	Yes	No	Yes	No
3GPP-MS-TimeZone	No	Yes	No	No	Yes	No	Yes	No
3GPP-Negotiated-DSCP	No	Yes	No	No	Yes	No	Yes	No
3GPP-Negotiated-QoS-Profile	No	Yes	No	No	Yes	No	Yes	No
3GPP-NSAPI	No	Yes	No	No	Yes	No	Yes	No
3GPP-Packet-Filter	No	Yes	No	No	Yes	No	Yes	No
3GPP-PDP-Type	No	Yes	No	No	Yes	No	Yes	No
3GPP-RAT-Type	No	Yes	No	No	Yes	No	Yes	No
3GPP-Selection-Mode	No	Yes	No	No	Yes	No	Yes	No
3GPP-Session-Stop-Ind	No	Yes	No	No	Yes	No	Yes	No
3GPP-SGSN-Address	No	Yes	No	No	Yes	No	Yes	No
3GPP-SGSN-IPv6-Address	No	Yes	No	No	Yes	No	Yes	No
3GPP-SGSN-Mcc-Mnc	No	Yes	No	No	Yes	No	Yes	No
3GPP-Teardown-Indicator	No	Yes	No	No	Yes	No	Yes	No
3GPP-User-Location-Info	No	Yes	No	No	Yes	No	Yes	No
AAA-Session-ID	No	No	No	No	Yes	No	Yes	No
Access-IN-Subs	No	No	No	No	No	No	No	No
Acct-Authentic	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Acct-Delay-Time	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Acct-Input-Gigawords	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Acct-Input-Octets	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Acct-Input-Packets	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Acct-Interim-Interval	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Acct-Link-Count	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Acct-Multi-Session-Id	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Acct-Output-Gigawords	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Acct-Output-Octets	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Acct-Output-Packets	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Acct-Session-Id	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Acct-Session-Id-Long	No	No	No	No	No	No	No	No
Acct-Session-Time	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes
Acct-Status-Type	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Acct-Termination-Cause	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Acct-Tunnel-Connection	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Acct-Tunnel-Packets-Lost	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
ARAP-Challenge-Response	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
ARAP-Features	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
ARAP-Password	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
ARAP-Security	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
ARAP-Security-Data	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
ARAP-Zone-Access	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
BU-CoA-Ipv6	No	No	No	No	Yes	No	Yes	No

Attribute	standard	3gpp	3gpp2	3gpp2-835	starent	starent-835	starent-vsa1	starent-vsa1-835
Callback-Id	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Callback-Number	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Called-Station-ID	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Calling-Station-Id	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Calling-Subscriber-Type	No	No	No	No	No	No	No	No
CHAP-Challenge	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
CHAP-Password	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Charging-Id	No	No	No	No	No	No	No	No
Class	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Configuration-Token	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Connect-Info	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
CS-AVPair	No	No	No	No	Yes	Yes	Yes	Yes
CS-Prepaid-Quota	No	No	No	No	Yes	Yes	Yes	Yes
CS-Prepaid-Time-Quota	No	No	No	No	Yes	Yes	Yes	Yes
CS-Prepaid-Volume-Quota	No	No	No	No	Yes	Yes	Yes	Yes
CS-Service-Name	No	No	No	No	Yes	Yes	Yes	Yes
CUI	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
custom54-Dial-Number	No	No	No	No	No	No	No	No
custom54-IPX-Alias	No	No	No	No	No	No	No	No
custom54-Metric	No	No	No	No	No	No	No	No
custom54-PRI-Number-Type	No	No	No	No	No	No	No	No
custom54-Route-IP	No	No	No	No	No	No	No	No
Custom-Prepaid-Ind	No	No	No	No	No	No	No	No
DHCPMSG-Server-IP	No	No	No	No	Yes	No	Yes	No
DHCP-RK	No	No	No	No	Yes	No	Yes	No
DHCP-RK-Key-ID	No	No	No	No	Yes	No	Yes	No
DHCP-RK-Lifetime	No	No	No	No	Yes	No	Yes	No
Digest-AKA-Auts	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Digest-Algorithm	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Digest-Auth-Param	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Digest-CNonce	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Digest-Domain	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Digest-Entity-Body-Hash	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Digest-HA1	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Digest-Method	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Digest-NextNonce	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Digest-Nonce	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Digest-Nonce-Count	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Digest-Opaque	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Digest-Qop	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Digest-Realm	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Digest-Response	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Digest-Response-Auth	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Digest-Stale	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Digest-URI	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Digest-Username	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
DNS	No	No	No	No	Yes	No	Yes	No
Draft5-Digest-Response	No	No	No	No	No	No	No	No

Attribute	standard	3gpp	3gpp2	3gpp2-835	starent	starent-835	starent-vsa1	starent-vsa1-835
DSCP_IP_Address	No	No	No	No	No	No	No	No
EAP-Message	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Error-Cause	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Event-Timestamp	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
FA-RK-KEY	No	No	No	No	Yes	No	Yes	No
FA-RK-SPI	No	No	No	No	Yes	No	Yes	No
Filter-Id	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Framed-AppleTalk-Link	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Framed-AppleTalk-Network	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Framed-AppleTalk-Zone	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Framed-Compression	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Framed-Interface-Id	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Framed-IP-Address	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Framed-IP-Netmask	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Framed-IPv6-Pool	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Framed-IPv6-Prefix	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Framed-IPv6-Route	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Framed-IPX-Network	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Framed-MTU	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Framed-Pool	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Framed-Protocol	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Framed-Route	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Framed-Routing	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Geographical-Location	No	No	No	No	Yes	Yes	Yes	Yes
GGSN-GTP-IP-Address	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
GGSN-IP-Address	No	No	No	No	No	No	No	No
GMT-Time-Zone-Offset	No	No	No	No	Yes	No	Yes	No
HA-IP-MIP4	No	No	No	No	Yes	No	Yes	No
HA-IP-MIP6	No	No	No	No	Yes	No	Yes	No
HA-RK-KEY	No	No	No	No	Yes	No	Yes	No
HA-RK-Lifetime	No	No	No	No	Yes	No	Yes	No
HA-RK-SPI	No	No	No	No	Yes	No	Yes	No
hLMA-IPv6-PMIP6	No	No	No	No	Yes	No	Yes	No
HNB-Internet-Information	No	No	No	No	Yes	Yes	Yes	Yes
HNB-Parameters	No	No	No	No	Yes	Yes	Yes	Yes
Hotline-Indicator	No	No	No	No	Yes	No	Yes	No
Hotline-Profile-ID	No	No	No	No	Yes	No	Yes	No
Hotline-Session-Timer	No	No	No	No	Yes	No	Yes	No
HTTP-Redirection-Rule	No	No	No	No	Yes	No	Yes	No
Idle-Timeout	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
IMSI	No	No	No	No	No	No	No	No
IMSI-MCC-MNC	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
IN-Packet-Period	No	No	No	No	No	No	No	No
IN-Time-Period	No	No	No	No	No	No	No	No
IP-Redirection-Rule	No	No	No	No	Yes	No	Yes	No
KTF_VSA1	No	No	No	No	No	No	No	No
KTF_VSA2	No	No	No	No	No	No	No	No
Login-IP-Host	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes

Attribute	standard	3gpp	3gpp2	3gpp2-835	starent	starent-835	starent-vsa1	starent-vsa1-835
Login-IPv6-Host	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Login-LAT-Group	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Login-LAT-Node	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Login-LAT-Port	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Login-LAT-Service	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Login-Service	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Login-TCP-Port	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Macro-Coverage-Information	No	No	No	No	Yes	Yes	Yes	Yes
Message-Authenticator	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
MN-HA-MIP4-KEY	No	No	No	No	Yes	No	Yes	No
MN-HA-MIP4-SPI	No	No	No	No	Yes	No	Yes	No
MN-HA-MIP6-KEY	No	No	No	No	Yes	No	Yes	No
MN-HA-MIP6-SPI	No	No	No	No	Yes	No	Yes	No
MSISDN	No	No	No	No	No	No	No	No
MSK	No	No	No	No	Yes	No	Yes	No
NAS-Filter-Rule	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
NAS-Identifier	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
NAS-IP-Address	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
NAS-IPv6-Address	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
NAS-Port	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
NAS-Port-Id	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
NAS-Port-Type	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Password-Retry	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
PMIP6-RK-KEY	No	No	No	No	Yes	No	Yes	No
PMIP6-RK-SPI	No	No	No	No	Yes	No	Yes	No
PMIP6-Service-Info	No	No	No	No	Yes	No	Yes	No
PMIP-Authenticated-Nwk-Id	No	No	No	No	Yes	No	Yes	No
Port-Limit	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Prepaid-Ind	No	No	No	No	No	No	No	No
Price-Plan	No	No	No	No	No	No	No	No
Primary-DNS-Server	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Prohibit-Payload-Compression	No	No	No	No	Yes	Yes	No	No
Prohibit-Payload-Compression1	No	No	No	No	No	No	Yes	Yes
Prompt	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Proxy-State	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Reject-Cause	No	No	No	No	Yes	Yes	Yes	Yes
Reply-Message	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
RRQ-HA-IP	No	No	No	No	Yes	No	Yes	No
RRQ-MN-HA-KEY	No	No	No	No	Yes	No	Yes	No
Secondary-DNS-Server	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Selection-Mode	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Service-Type	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Session-Timeout	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
SGSN-IP-Address	No	No	No	No	No	No	No	No
SIP-AOR	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
SN1-Access-link-IP-Frag	No	No	No	No	No	No	Yes	Yes
SN1-Acct-Input-Giga-Dropped	No	No	No	No	No	No	Yes	Yes
SN1-Acct-Input-Octets-Dropped	No	No	No	No	No	No	Yes	Yes

Attribute	standard	3gpp	3gpp2	3gpp2-835	starent	starent-835	starent-vsa1	starent-vsa1-835
SN1-Acct-Input-Packets-Dropped	No	No	No	No	No	No	Yes	Yes
SN1-Acct-Output-Giga-Dropped	No	No	No	No	No	No	Yes	Yes
SN1-Acct-Output-Octets-Dropped	No	No	No	No	No	No	Yes	Yes
SN1-Acct-Output-Packets-Dropped	No	No	No	No	No	No	Yes	Yes
SN1-Admin-Expiry	No	No	No	No	No	No	Yes	Yes
SN1-Admin-Permission	No	No	No	No	No	No	Yes	Yes
SN1-Assigned-VLAN-ID	No	No	No	No	No	No	Yes	Yes
SN1-Call-Id	No	No	No	No	No	No	Yes	Yes
SN1-Cause-For-Rec-Closing	No	No	No	No	No	No	Yes	Yes
SN1-CFPolicy-ID	No	No	No	No	No	No	Yes	Yes
SN1-Change-Condition	No	No	No	No	No	No	Yes	Yes
SN1-Charging-VPN-Name	No	No	No	No	No	No	Yes	Yes
SN1-Chrg-Char-Selection-Mode	No	No	No	No	No	No	Yes	Yes
SN1-Data-Tunnel-IgNore-DF-Bit	No	No	No	No	No	No	Yes	Yes
SN1-DHCP-Lease-Expiry-Policy	No	No	No	No	No	No	Yes	Yes
SN1-Disconnect-Reason	No	No	No	No	No	No	Yes	Yes
SN1-DNS-Proxy-Intercept-List	No	No	No	No	No	No	Yes	Yes
SN1-DNS-Proxy-Use-Subscr-Addr	No	No	No	No	No	No	Yes	Yes
SN1-Dynamic-Addr-Alloc-Ind-Flag	No	No	No	No	No	No	Yes	Yes
SN1-Ecs-Data-Volume	No	No	No	No	No	No	Yes	Yes
SN1-Enable-QoS-Renegotiation	No	No	No	No	No	No	Yes	Yes
SN1-Ext-Inline-Srvr-Context	No	No	No	No	No	No	Yes	Yes
SN1-Ext-Inline-Srvr-Down-Addr	No	No	No	No	No	No	Yes	Yes
SN1-Ext-Inline-Srvr-Down-VLAN	No	No	No	No	No	No	Yes	Yes
SN1-Ext-Inline-Srvr-Preference	No	No	No	No	No	No	Yes	Yes
SN1-Ext-Inline-Srvr-Up-Addr	No	No	No	No	No	No	Yes	Yes
SN1-Ext-Inline-Srvr-Up-VLAN	No	No	No	No	No	No	Yes	Yes
SN1-Firewall-Enabled	No	No	No	No	No	No	Yes	Yes
SN1-FMC-Location	No	No	No	No	No	No	Yes	Yes
SN1-GGSN-MIP-Required	No	No	No	No	No	No	Yes	Yes
SN1-Gratuitous-ARP-Aggressive	No	No	No	No	No	No	Yes	Yes
SN1-GTP-Version	No	No	No	No	No	No	Yes	Yes
SN1-HA-Send-DNS-Address	No	No	No	No	No	No	Yes	Yes
SN1-Home-Behavior	No	No	No	No	No	No	Yes	Yes
SN1-Home-Profile	No	No	No	No	No	No	Yes	Yes
SN1-Home-Sub-Use-GGSN	No	No	No	No	No	No	Yes	Yes
SN1-IgNore-UnkNown-HA-Addr-Err	No	No	No	No	No	No	Yes	Yes
SN1-IMS-AM-Address	No	No	No	No	No	No	Yes	Yes
SN1-IMS-AM-Domain-Name	No	No	No	No	No	No	Yes	Yes
SN1-IMSI	No	No	No	No	No	No	Yes	Yes
SN1-Inactivity-Time	No	No	No	No	No	No	Yes	Yes
SN1-Internal-SM-Index	No	No	No	No	No	No	Yes	Yes
SN1-IP-Alloc-Method	No	No	No	No	No	No	Yes	Yes
SN1-IP-Filter-In	No	No	No	No	No	No	Yes	Yes
SN1-IP-Filter-Out	No	No	No	No	No	No	Yes	Yes
SN1-IP-Header-Compression	No	No	No	No	No	No	Yes	Yes
SN1-IP-Hide-Service-Address	No	No	No	No	No	No	Yes	Yes
SN1-IP-In-ACL	No	No	No	No	No	No	Yes	Yes

Attribute	standard	3gpp	3gpp2	3gpp2-835	starent	starent-835	starent-vsa1	starent-vsa1-835
SN1-IP-In-Plcy-Grp	No	No	No	No	No	No	Yes	Yes
SN1-IP-Out-ACL	No	No	No	No	No	No	Yes	Yes
SN1-IP-Out-Plcy-Grp	No	No	No	No	No	No	Yes	Yes
SN1-IP-Pool-Name	No	No	No	No	No	No	Yes	Yes
SN1-IP-Source-Validation	No	No	No	No	No	No	Yes	Yes
SN1-IP-Source-Violate-No-Acct	No	No	No	No	No	No	Yes	Yes
SN1-IP-Src-Valid-Drop-Limit	No	No	No	No	No	No	Yes	Yes
SN1-IPv6-DNS-Proxy	No	No	No	No	No	No	Yes	Yes
SN1-IPv6-Egress-Filtering	No	No	No	No	No	No	Yes	Yes
SN1-IPv6-Min-Link-MTU	No	No	No	No	No	No	Yes	Yes
SN1-IPv6-num-rtr-advt	No	No	No	No	No	No	Yes	Yes
SN1-IPv6-Primary-DNS	No	No	No	No	No	No	Yes	Yes
SN1-IPv6-rtr-advt-interval	No	No	No	No	No	No	Yes	Yes
SN1-IPv6-Secondary-DNS	No	No	No	No	No	No	Yes	Yes
SN1-IPv6-Sec-Pool	No	No	No	No	No	No	Yes	Yes
SN1-IPv6-Sec-Prefix	No	No	No	No	No	No	Yes	Yes
SN1-L3-to-L2-Tun-Addr-Policy	No	No	No	No	No	No	Yes	Yes
SN1-Local-IP-Address	No	No	No	No	No	No	Yes	Yes
SN1-Long-Duration-Action	No	No	No	No	No	No	Yes	Yes
SN1-Long-Duration-Notification	No	No	No	No	No	No	Yes	Yes
SN1-Long-Duration-Timeout	No	No	No	No	No	No	Yes	Yes
SN1-Mediation-Acct-Rsp-Action	No	No	No	No	No	No	Yes	Yes
SN1-Mediation-Enabled	No	No	No	No	No	No	Yes	Yes
SN1-Mediation-No-Interims	No	No	No	No	No	No	Yes	Yes
SN1-Mediation-VPN-Name	No	No	No	No	No	No	Yes	Yes
SN1-Min-Compress-Size	No	No	No	No	No	No	Yes	Yes
SN1-MIP-AAA-Assign-Addr	No	No	No	No	No	No	Yes	Yes
SN1-MIP-ANCID	No	No	No	No	No	No	Yes	Yes
SN1-MIP-Dual-Anchor	No	No	No	No	No	No	Yes	Yes
SN1-MIP-HA-Assignment-Table	No	No	No	No	No	No	Yes	Yes
SN1-MIP-Match-AAA-Assign-Addr	No	No	No	No	No	No	Yes	Yes
SN1-MIP-Reg-Lifetime-Realm	No	No	No	No	No	No	Yes	Yes
SN1-MIP-Send-Ancid	No	No	No	No	No	No	Yes	Yes
SN1-MIP-Send-Correlation-Info	No	No	No	No	No	No	Yes	Yes
SN1-MIP-Send-Imsi	No	No	No	No	No	No	Yes	Yes
SN1-MIP-Send-Term-Verification	No	No	No	No	No	No	Yes	Yes
SN1-MN-HA-Hash-Algorithm	No	No	No	No	No	No	Yes	Yes
SN1-MN-HA-Timestamp-Tolerance	No	No	No	No	No	No	Yes	Yes
SN1-MS-ISDN	No	No	No	No	No	No	Yes	Yes
SN1-NAI-Construction-Domain	No	No	No	No	No	No	Yes	Yes
SN1-NAT-Bind-Record	No	No	No	No	No	No	Yes	Yes
SN1-NAT-Info-Record	No	No	No	No	No	No	Yes	Yes
SN1-NAT-IP-Address	No	No	No	No	No	No	Yes	Yes
SN1-NAT-IP-Address-Old	No	No	No	No	No	No	Yes	Yes
SN1-NPU-Qos-Priority	No	No	No	No	No	No	Yes	Yes
SN1-Ntk-Initiated-Ctx-Ind-Flag	No	No	No	No	No	No	Yes	Yes
SN1-Ntk-Session-Disconnect-Flag	No	No	No	No	No	No	Yes	Yes
SN1-Nw-Reachability-Server-Name	No	No	No	No	No	No	Yes	Yes

Attribute	standard	3gpp	3gpp2	3gpp2-835	starent	starent-835	starent-vsa1	starent-vsa1-835
SN1-Overload-Disc-Connect-Time	No	No	No	No	No	No	Yes	Yes
SN1-Overload-Disc-Inact-Time	No	No	No	No	No	No	Yes	Yes
SN1-Overload-Disconnect	No	No	No	No	No	No	Yes	Yes
SN1-PDIF-MIP-Release-TIA	No	No	No	No	No	No	Yes	Yes
SN1-PDIF-MIP-Required	No	No	No	No	No	No	Yes	Yes
SN1-PDIF-MIP-Simple-IP-Fallback	No	No	No	No	No	No	Yes	Yes
SN1-PDSN-Correlation-Id	No	No	No	No	No	No	Yes	Yes
SN1-PDSN-Handoff-Req-IP-Addr	No	No	No	No	No	No	Yes	Yes
SN1-PDSN-NAS-Id	No	No	No	No	No	No	Yes	Yes
SN1-PDSN-NAS-IP-Address	No	No	No	No	No	No	Yes	Yes
SN1-Permit-User-Mcast-PDUs	No	No	No	No	No	No	Yes	Yes
SN1-PPP-Accept-Peer-v6Ifid	No	No	No	No	No	No	Yes	Yes
SN1-PPP-Always-On-Vse	No	No	No	No	No	No	Yes	Yes
SN1-PPP-Data-Compression	No	No	No	No	No	No	Yes	Yes
SN1-PPP-Data-Compression-Mode	No	No	No	No	No	No	Yes	Yes
SN1-PPP-Keepalive	No	No	No	No	No	No	Yes	Yes
SN1-PPP-NW-Layer-IPv4	No	No	No	No	No	No	Yes	Yes
SN1-PPP-NW-Layer-IPv6	No	No	No	No	No	No	Yes	Yes
SN1-PPP-Outbound-Password	No	No	No	No	No	No	Yes	Yes
SN1-PPP-Outbound-Username	No	No	No	No	No	No	Yes	Yes
SN1-PPP-Progress-Code	No	No	No	No	No	No	Yes	Yes
SN1-PPP-Reneg-Disc	No	No	No	No	No	No	Yes	Yes
SN1-Prepaid	No	No	No	No	No	No	Yes	Yes
SN1-Prepaid-Compressed-Count	No	No	No	No	No	No	Yes	Yes
SN1-Prepaid-Final-Duration-Alg	No	No	No	No	No	No	Yes	Yes
SN1-Prepaid-Inbound-Octets	No	No	No	No	No	No	Yes	Yes
SN1-Prepaid-Outbound-Octets	No	No	No	No	No	No	Yes	Yes
SN1-Prepaid-Preference	No	No	No	No	No	No	Yes	Yes
SN1-Prepaid-Profile	No	No	No	No	No	No	Yes	Yes
SN1-Prepaid-Timeout	No	No	No	No	No	No	Yes	Yes
SN1-Prepaid-Total-Octets	No	No	No	No	No	No	Yes	Yes
SN1-Prepaid-Watermark	No	No	No	No	No	No	Yes	Yes
SN1-Primary-DCCA-Peer	No	No	No	No	No	No	Yes	Yes
SN1-Primary-DNS-Server	No	No	No	No	No	No	Yes	Yes
SN1-Primary-NBNS-Server	No	No	No	No	No	No	Yes	Yes
SN1-Proxy-MIP	No	No	No	No	No	No	Yes	Yes
SN1-QoS-Background-Class	No	No	No	No	No	No	Yes	Yes
SN1-QoS-Class-Background-PHB	No	No	No	No	No	No	Yes	Yes
SN1-QoS-Class-Converstional-PHB	No	No	No	No	No	No	Yes	Yes
SN1-QoS-Class-Interactive-1-PHB	No	No	No	No	No	No	Yes	Yes
SN1-QoS-Class-Interactive-2-PHB	No	No	No	No	No	No	Yes	Yes
SN1-QoS-Class-Interactive-3-PHB	No	No	No	No	No	No	Yes	Yes
SN1-QoS-Class-Streaming-PHB	No	No	No	No	No	No	Yes	Yes
SN1-QoS-Conversation-Class	No	No	No	No	No	No	Yes	Yes
SN1-QoS-Interactive1-Class	No	No	No	No	No	No	Yes	Yes
SN1-QoS-Interactive2-Class	No	No	No	No	No	No	Yes	Yes
SN1-QoS-Interactive3-Class	No	No	No	No	No	No	Yes	Yes
SN1-QoS-Negotiated	No	No	No	No	No	No	Yes	Yes

Attribute	standard	3gpp	3gpp2	3gpp2-835	starent	starent-835	starent-vsa1	starent-vsa1-835
SN1-QoS-Renegotiation-Timeout	No	No	No	No	No	No	Yes	Yes
SN1-QoS-Streaming-Class	No	No	No	No	No	No	Yes	Yes
SN1-QoS-Tp-Dnlk	No	No	No	No	No	No	Yes	Yes
SN1-QoS-Tp-Uplk	No	No	No	No	No	No	Yes	Yes
SN1-QoS-Traffic-Policy	No	No	No	No	No	No	Yes	Yes
SN1-Rad-APN-Name	No	No	No	No	No	No	Yes	Yes
SN1-Radius-Returned-Username	No	No	No	No	No	No	Yes	Yes
SN1-Re-CHAP-Interval	No	No	No	No	No	No	Yes	Yes
SN1-Roaming-Behavior	No	No	No	No	No	No	Yes	Yes
SN1-Roaming-Profile	No	No	No	No	No	No	Yes	Yes
SN1-Roaming-Sub-Use-GGSN	No	No	No	No	No	No	Yes	Yes
SN1-ROHC-Direction	No	No	No	No	No	No	Yes	Yes
SN1-ROHC-Flow-Marking-Mode	No	No	No	No	No	No	Yes	Yes
SN1-ROHC-Mode	No	No	No	No	No	No	Yes	Yes
SN1-ROHC-Profile-Name	No	No	No	No	No	No	Yes	Yes
SN1-Routing-Area-Id	No	No	No	No	No	No	Yes	Yes
SN1-Rulebase	No	No	No	No	No	No	Yes	Yes
SN1-Secondary-DCCA-Peer	No	No	No	No	No	No	Yes	Yes
SN1-Secondary-DNS-Server	No	No	No	No	No	No	Yes	Yes
SN1-Secondary-NBNS-Server	No	No	No	No	No	No	Yes	Yes
SN1-Service-Address	No	No	No	No	No	No	Yes	Yes
SN1-Service-Type	No	No	No	No	No	No	Yes	Yes
SN1-Simultaneous-SIP-MIP	No	No	No	No	No	No	Yes	Yes
SN1-Subs-Acc-Flow-Traffic-Valid	No	No	No	No	No	No	Yes	Yes
SN1-Subscriber-Accounting	No	No	No	No	No	No	Yes	Yes
SN1-Subscriber-Acct-Interim	No	No	No	No	No	No	Yes	Yes
SN1-Subscriber-Acct-Mode	No	No	No	No	No	No	Yes	Yes
SN1-Subscriber-Acct-Rsp-Action	No	No	No	No	No	No	Yes	Yes
SN1-Subscriber-Acct-Start	No	No	No	No	No	No	Yes	Yes
SN1-Subscriber-Acct-Stop	No	No	No	No	No	No	Yes	Yes
SN1-Subscriber-Class	No	No	No	No	No	No	Yes	Yes
SN1-Subscriber-Dormant-Activity	No	No	No	No	No	No	Yes	Yes
SN1-Subscriber-IP-Hdr-Neg-Mode	No	No	No	No	No	No	Yes	Yes
SN1-Subscriber-IP-TOS-Copy	No	No	No	No	No	No	Yes	Yes
SN1-Subscriber-Nexthop-Address	No	No	No	No	No	No	Yes	Yes
SN1-Subscriber-No-Interims	No	No	No	No	No	No	Yes	Yes
SN1-Subscriber-Permission	No	No	No	No	No	No	Yes	Yes
SN1-Subscriber-Template-Name	No	No	No	No	No	No	Yes	Yes
SN1-Subs-IMSA-Service-Name	No	No	No	No	No	No	Yes	Yes
SN1-Subs-VJ-Slotid-Cmp-Neg-Mode	No	No	No	No	No	No	Yes	Yes
SN1-Tp-Dnlk-Burst-Size	No	No	No	No	No	No	Yes	Yes
SN1-Tp-Dnlk-Committed-Data-Rate	No	No	No	No	No	No	Yes	Yes
SN1-Tp-Dnlk-Exceed-Action	No	No	No	No	No	No	Yes	Yes
SN1-Tp-Dnlk-Peak-Data-Rate	No	No	No	No	No	No	Yes	Yes
SN1-Tp-Dnlk-Violate-Action	No	No	No	No	No	No	Yes	Yes
SN1-Tp-Uplk-Burst-Size	No	No	No	No	No	No	Yes	Yes
SN1-Tp-Uplk-Committed-Data-Rate	No	No	No	No	No	No	Yes	Yes
SN1-Tp-Uplk-Exceed-Action	No	No	No	No	No	No	Yes	Yes

Attribute	standard	3gpp	3gpp2	3gpp2-835	starent	starent-835	starent-vsa1	starent-vsa1-835
SN1-Tp-Uplk-Peak-Data-Rate	No	No	No	No	No	No	Yes	Yes
SN1-Tp-Uplk-Violate-Action	No	No	No	No	No	No	Yes	Yes
SN1-Traffic-Group	No	No	No	No	No	No	Yes	Yes
SN1-Transparent-Data	No	No	No	No	No	No	Yes	Yes
SN1-Tun-Addr-Policy	No	No	No	No	No	No	Yes	Yes
SN1-Tunnel-Gn	No	No	No	No	No	No	Yes	Yes
SN1-Tunnel-ISAKMP-Crypto-Map	No	No	No	No	No	No	Yes	Yes
SN1-Tunnel-ISAKMP-Secret	No	No	No	No	No	No	Yes	Yes
SN1-Tunnel-Load-Balancing	No	No	No	No	No	No	Yes	Yes
SN1-Tunnel-Password	No	No	No	No	No	No	Yes	Yes
SN1-Unclassify-List-Name	No	No	No	No	No	No	Yes	Yes
SN1-Virtual-APN-Name	No	No	No	No	No	No	Yes	Yes
SN1-Visiting-Behavior	No	No	No	No	No	No	Yes	Yes
SN1-Visiting-Profile	No	No	No	No	No	No	Yes	Yes
SN1-Visiting-Sub-Use-GGSN	No	No	No	No	No	No	Yes	Yes
SN1-Voice-Push-List-Name	No	No	No	No	No	No	Yes	Yes
SN1-VPN-ID	No	No	No	No	No	No	Yes	Yes
SN1-VPN-Name	No	No	No	No	No	No	Yes	Yes
SNA1-PPP-Unfr-data-In-Gig	No	No	No	No	No	No	Yes	Yes
SNA1-PPP-Unfr-data-In-Oct	No	No	No	No	No	No	Yes	Yes
SNA1-PPP-Unfr-data-Out-Gig	No	No	No	No	No	No	Yes	Yes
SNA1-PPP-Unfr-data-Out-Oct	No	No	No	No	No	No	Yes	Yes
SN-Access-link-IP-Frag	No	No	No	No	Yes	Yes	No	No
SN-Acct-Input-Giga-Dropped	No	No	No	No	Yes	Yes	No	No
SN-Acct-Input-Octets-Dropped	No	No	No	No	Yes	Yes	No	No
SN-Acct-Input-Packets-Dropped	No	No	No	No	Yes	Yes	No	No
SN-Acct-Output-Giga-Dropped	No	No	No	No	Yes	Yes	No	No
SN-Acct-Output-Octets-Dropped	No	No	No	No	Yes	Yes	No	No
SN-Acct-Output-Packets-Dropped	No	No	No	No	Yes	Yes	No	No
SN-Acs-Credit-Control-Group	No	No	No	No	Yes	Yes	No	No
SN-Admin-Expiry	No	No	No	No	Yes	Yes	No	No
SN-Admin-Permission	No	No	No	No	Yes	Yes	No	No
SNA-Input-Gigawords	No	No	No	No	No	No	No	No
SNA-Input-Octets	No	No	No	No	No	No	No	No
SN-ANID	No	No	No	No	No	No	No	No
SNA-Output-Gigawords	No	No	No	No	No	No	No	No
SNA-Output-Octets	No	No	No	No	No	No	No	No
SNA-PPP-Bad-Addr	No	No	No	No	Yes	Yes	No	No
SNA-PPP-Bad-Ctrl	No	No	No	No	Yes	Yes	No	No
SNA-PPP-Bad-FCS	No	No	No	No	Yes	Yes	No	No
SNA-PPP-Ctrl-Input-Octets	No	No	No	No	Yes	Yes	No	No
SNA-PPP-Ctrl-Input-Packets	No	No	No	No	Yes	Yes	No	No
SNA-PPP-Ctrl-Output-Octets	No	No	No	No	Yes	Yes	No	No
SNA-PPP-Ctrl-Output-Packets	No	No	No	No	Yes	Yes	No	No
SNA-PPP-Discards-Input	No	No	No	No	Yes	Yes	No	No
SNA-PPP-Discards-Output	No	No	No	No	Yes	Yes	No	No
SNA-PPP-Echo-Req-Input	No	No	No	No	Yes	Yes	No	No
SNA-PPP-Echo-Req-Output	No	No	No	No	Yes	Yes	No	No

Attribute	standard	3gpp	3gpp2	3gpp2-835	starent	starent-835	starent-vsa1	starent-vsa1-835
SNA-PPP-Echo-Rsp-Input	No	No	No	No	Yes	Yes	No	No
SNA-PPP-Echo-Rsp-Output	No	No	No	No	Yes	Yes	No	No
SNA-PPP-Errors-Input	No	No	No	No	Yes	Yes	No	No
SNA-PPP-Errors-Output	No	No	No	No	Yes	Yes	No	No
SNA-PPP-Framed-Input-Octets	No	No	No	No	Yes	Yes	No	No
SNA-PPP-Framed-Output-Octets	No	No	No	No	Yes	Yes	No	No
SNA-PPP-Packet-Too-Long	No	No	No	No	Yes	Yes	No	No
SNA-PPP-Unfr-data-In-Gig	No	No	No	No	Yes	Yes	No	No
SNA-PPP-Unfr-data-In-Oct	No	No	No	No	Yes	Yes	No	No
SNA-PPP-Unfr-data-Out-Gig	No	No	No	No	Yes	Yes	No	No
SNA-PPP-Unfr-data-Out-Oct	No	No	No	No	Yes	Yes	No	No
SNA-RPRAK-Rcvd-Acc-Ack	No	No	No	No	Yes	Yes	No	No
SNA-RPRAK-Rcvd-Mis-ID	No	No	No	No	Yes	Yes	No	No
SNA-RPRAK-Rcvd-Msg-Auth-Fail	No	No	No	No	Yes	Yes	No	No
SNA-RPRAK-Rcvd-Total	No	No	No	No	Yes	Yes	No	No
SNA-RP-Reg-Reply-Sent-Acc-Dereg	No	No	No	No	Yes	Yes	No	No
SNA-RP-Reg-Reply-Sent-Acc-Reg	No	No	No	No	Yes	Yes	No	No
SNA-RP-Reg-Reply-Sent-Bad-Req	No	No	No	No	Yes	Yes	No	No
SNA-RP-Reg-Reply-Sent-Denied	No	No	No	No	Yes	Yes	No	No
SNA-RP-Reg-Reply-Sent-Mis-ID	No	No	No	No	Yes	Yes	No	No
SNA-RP-Reg-Reply-Sent-Send-Err	No	No	No	No	Yes	Yes	No	No
SNA-RP-Reg-Reply-Sent-Total	No	No	No	No	Yes	Yes	No	No
SNA-RP-Reg-Upd-Re-Sent	No	No	No	No	Yes	Yes	No	No
SNA-RP-Reg-Upd-Send-Err	No	No	No	No	Yes	Yes	No	No
SNA-RP-Reg-Upd-Sent	No	No	No	No	Yes	Yes	No	No
SNA-RPRRQ-Rcvd-Acc-Dereg	No	No	No	No	Yes	Yes	No	No
SNA-RPRRQ-Rcvd-Acc-Reg	No	No	No	No	Yes	Yes	No	No
SNA-RPRRQ-Rcvd-Badly-Formed	No	No	No	No	Yes	Yes	No	No
SNA-RPRRQ-Rcvd-Mis-ID	No	No	No	No	Yes	Yes	No	No
SNA-RPRRQ-Rcvd-Msg-Auth-Fail	No	No	No	No	Yes	Yes	No	No
SNA-RPRRQ-Rcvd-T-Bit-Not-Set	No	No	No	No	Yes	Yes	No	No
SNA-RPRRQ-Rcvd-Total	No	No	No	No	Yes	Yes	No	No
SNA-RPRRQ-Rcvd-VID-Unsupported	No	No	No	No	Yes	Yes	No	No
SN-Assigned-VLAN-ID	No	No	No	No	Yes	Yes	No	No
SN-Authorised-Qos	No	No	No	No	Yes	Yes	No	No
SN-Bandwidth-Policy	No	No	No	No	Yes	Yes	No	No
SN-Call-Id	No	No	No	No	Yes	Yes	No	No
SN-Cause-Code	No	No	No	No	Yes	Yes	No	No
SN-Cause-For-Rec-Closing	No	No	No	No	Yes	Yes	No	No
SN-CBB-Policy	No	No	No	No	Yes	Yes	No	No
SN-CF-Call-International	No	No	No	No	Yes	Yes	No	No
SN-CF-Call-Local	No	No	No	No	Yes	Yes	No	No
SN-CF-Call-LongDistance	No	No	No	No	Yes	Yes	No	No
SN-CF-Call-Premium	No	No	No	No	Yes	Yes	No	No
SN-CF-Call-RoamingInternatnl	No	No	No	No	Yes	Yes	No	No
SN-CF-Call-Transfer	No	No	No	No	Yes	Yes	No	No
SN-CF-Call-Waiting	No	No	No	No	Yes	Yes	No	No
SN-CF-CId-Display	No	No	No	No	Yes	Yes	No	No

Attribute	standard	3gpp	3gpp2	3gpp2-835	starent	starent-835	starent-vsa1	starent-vsa1-835
SN-CF-CId-Display-Blocked	No	No	No	No	Yes	Yes	No	No
SN-CF-Follow-Me	No	No	No	No	Yes	Yes	No	No
SN-CF-Forward-Busy-Line	No	No	No	No	Yes	Yes	No	No
SN-CF-Forward-No-Answer	No	No	No	No	Yes	Yes	No	No
SN-CF-Forward-Not-Regd	No	No	No	No	Yes	Yes	No	No
SN-CF-Forward-Unconditional	No	No	No	No	Yes	Yes	No	No
SN-CFPolicy-ID	No	No	No	No	Yes	Yes	No	No
SN-Change-Condition	No	No	No	No	Yes	Yes	No	No
SN-Charging-VPN-Name	No	No	No	No	Yes	Yes	No	No
SN-Chrg-Char-Selection-Mode	No	No	No	No	Yes	Yes	No	No
SN-Content-Disposition	No	No	No	No	Yes	Yes	No	No
SN-Content-Length	No	No	No	No	Yes	Yes	No	No
SN-Content-Type	No	No	No	No	Yes	Yes	No	No
SN-CR-International-Cid	No	No	No	No	Yes	Yes	No	No
SN-CR-LongDistance-Cid	No	No	No	No	Yes	Yes	No	No
SN-CSCF-App-Server-Info	No	No	No	No	Yes	Yes	No	No
SN-CSCF-Rf-SDP-Media-Components	No	No	No	No	Yes	Yes	No	No
SN-Cscf-Subscriber-Ip-Address	No	No	No	No	Yes	Yes	No	No
SN-Data-Tunnel-IgNore-DF-Bit	No	No	No	No	Yes	Yes	No	No
SN-DHCP-Lease-Expiry-Policy	No	No	No	No	Yes	Yes	No	No
SN-DHCP-Options	No	No	No	No	Yes	Yes	No	No
SN-Direction	No	No	No	No	Yes	Yes	No	No
SN-Disconnect-Reason	No	No	No	No	Yes	Yes	No	No
SN-DNS-Proxy-Intercept-List	No	No	No	No	Yes	Yes	No	No
SN-DNS-Proxy-Use-Subscr-Addr	No	No	No	No	Yes	Yes	No	No
SN-Dynamic-Addr-Alloc-Ind-Flag	No	No	No	No	Yes	Yes	No	No
SN-Ecs-Data-Volume	No	No	No	No	Yes	Yes	No	No
SN-Enable-QoS-Renegotiation	No	No	No	No	Yes	Yes	No	No
SN-Event	No	No	No	No	Yes	Yes	No	No
SN-Ext-Inline-Srvr-Context	No	No	No	No	Yes	Yes	No	No
SN-Ext-Inline-Srvr-Down-Addr	No	No	No	No	Yes	Yes	No	No
SN-Ext-Inline-Srvr-Down-VLAN	No	No	No	No	Yes	Yes	No	No
SN-Ext-Inline-Srvr-Preference	No	No	No	No	Yes	Yes	No	No
SN-Ext-Inline-Srvr-Up-Addr	No	No	No	No	Yes	Yes	No	No
SN-Ext-Inline-Srvr-Up-VLAN	No	No	No	No	Yes	Yes	No	No
SN-Fast-Reauth-Username	No	No	No	No	Yes	Yes	No	No
SN-Firewall-Enabled	No	No	No	No	Yes	Yes	No	No
SN-Firewall-Policy	No	No	No	No	Yes	Yes	No	No
SN-FMC-Location	No	No	No	No	Yes	Yes	No	No
SN-GGSN-Address	No	No	No	No	Yes	Yes	No	No
SN-GGSN-MIP-Required	No	No	No	No	Yes	Yes	No	No
SN-Gratuitous-ARP-Aggressive	No	No	No	No	Yes	Yes	No	No
SN-GTP-Version	No	No	No	No	Yes	Yes	No	No
SN-Handoff-Indicator	No	No	No	No	Yes	Yes	No	No
SN-HA-Send-DNS-Address	No	No	No	No	Yes	Yes	No	No
SN-Home-Behavior	No	No	No	No	Yes	Yes	No	No
SN-Home-Profile	No	No	No	No	Yes	Yes	No	No
SN-Home-Sub-Use-GGSN	No	No	No	No	Yes	Yes	No	No

Attribute	standard	3gpp	3gpp2	3gpp2-835	starent	starent-835	starent-vsa1	starent-vsa1-835
SN-IgNore-UnkNown-HA-Addr-Error	No	No	No	No	Yes	Yes	No	No
SN-IMS-AM-Address	No	No	No	No	Yes	Yes	No	No
SN-IMS-AM-Domain-Name	No	No	No	No	Yes	Yes	No	No
SN-IMS-Charging-Identifier	No	No	No	No	Yes	Yes	No	No
SN-IMSI	No	No	No	No	Yes	Yes	No	No
SN-Inactivity-Time	No	No	No	No	Yes	Yes	No	No
SN-Internal-SM-Index	No	No	No	No	Yes	Yes	No	No
SN-IP-Alloc-Method	No	No	No	No	Yes	Yes	No	No
SN-IP-Filter-In	No	No	No	No	Yes	Yes	No	No
SN-IP-Filter-Out	No	No	No	No	Yes	Yes	No	No
SN-IP-Header-Compression	No	No	No	No	Yes	Yes	No	No
SN-IP-Hide-Service-Address	No	No	No	No	Yes	Yes	No	No
SN-IP-In-ACL	No	No	No	No	Yes	Yes	No	No
SN-IP-In-Plcy-Grp	No	No	No	No	Yes	Yes	No	No
SN-IP-Out-ACL	No	No	No	No	Yes	Yes	No	No
SN-IP-Out-Plcy-Grp	No	No	No	No	Yes	Yes	No	No
SN-IP-Pool-Name	No	No	No	No	Yes	Yes	No	No
SN-IP-Source-Validation	No	No	No	No	Yes	Yes	No	No
SN-IP-Source-Violate-No-Acct	No	No	No	No	Yes	Yes	No	No
SN-IP-Src-Validation-Drop-Limit	No	No	No	No	Yes	Yes	No	No
SN-IPv6-DNS-Proxy	No	No	No	No	Yes	Yes	No	No
SN-IPv6-Egress-Filtering	No	No	No	No	Yes	Yes	No	No
SN-IPv6-Min-Link-MTU	No	No	No	No	Yes	Yes	No	No
SN-IPv6-num-rtr-advt	No	No	No	No	Yes	Yes	No	No
SN-IPv6-Primary-DNS	No	No	No	No	Yes	Yes	No	No
SN-IPv6-rtr-advt-interval	No	No	No	No	Yes	Yes	No	No
SN-IPv6-Secondary-DNS	No	No	No	No	Yes	Yes	No	No
SN-IPv6-Sec-Pool	No	No	No	No	Yes	Yes	No	No
SN-IPv6-Sec-Prefix	No	No	No	No	Yes	Yes	No	No
SN-ISC-Template-Name	No	No	No	No	Yes	Yes	No	No
SN-Is-Unregistered-Subscriber	No	No	No	No	Yes	Yes	No	No
SN-L3-to-L2-Tun-Addr-Policy	No	No	No	No	Yes	Yes	No	No
SN-Local-IP-Address	No	No	No	No	Yes	Yes	No	No
SN-Long-Duration-Action	No	No	No	No	Yes	Yes	No	No
SN-Long-Duration-Notification	No	No	No	No	Yes	Yes	No	No
SN-Long-Duration-Timeout	No	No	No	No	Yes	Yes	No	No
SN-Max-Sec-Contexts-Per-Subs	No	No	No	No	Yes	Yes	No	No
SN-Mediation-Acct-Rsp-Action	No	No	No	No	Yes	Yes	No	No
SN-Mediation-Enabled	No	No	No	No	Yes	Yes	No	No
SN-Mediation-No-Interims	No	No	No	No	Yes	Yes	No	No
SN-Mediation-VPN-Name	No	No	No	No	Yes	Yes	No	No
SN-Min-Compress-Size	No	No	No	No	Yes	Yes	No	No
SN-MIP-AAA-Assign-Addr	No	No	No	No	Yes	Yes	No	No
SN-MIP-ANCID	No	No	No	No	Yes	Yes	No	No
SN-MIP-Dual-Anchor	No	No	No	No	Yes	Yes	No	No
SN-MIP-HA-Assignment-Table	No	No	No	No	Yes	Yes	No	No
SN-MIP-Match-AAA-Assign-Addr	No	No	No	No	Yes	Yes	No	No
SN-MIP-Reg-Lifetime-Realm	No	No	No	No	Yes	Yes	No	No

Attribute	standard	3gpp	3gpp2	3gpp2-835	starent	starent-835	starent-vsa1	starent-vsa1-835
SN-MIP-Send-Ancid	No	No	No	No	Yes	Yes	No	No
SN-MIP-Send-Correlation-Info	No	No	No	No	Yes	Yes	No	No
SN-MIP-Send-Host-Config	No	No	No	No	Yes	Yes	No	No
SN-MIP-Send-Imsi	No	No	No	No	Yes	Yes	No	No
SN-MIP-Send-Term-Verification	No	No	No	No	Yes	Yes	No	No
SN-MN-HA-Hash-Algorithm	No	No	No	No	Yes	Yes	No	No
SN-MN-HA-Timestamp-Tolerance	No	No	No	No	Yes	Yes	No	No
SN-Mode	No	No	No	No	Yes	Yes	No	No
SN-MS-ISDN	No	No	No	No	Yes	Yes	No	No
SN-NAI-Construction-Domain	No	No	No	No	Yes	Yes	No	No
SN-NAT-IP-Address	No	No	No	No	Yes	Yes	No	No
SN-Node-Functionality	No	No	No	No	Yes	Yes	No	No
SN-NPU-Qos-Priority	No	No	No	No	Yes	Yes	No	No
SN-Ntk-Initiated-Ctx-Ind-Flag	No	No	No	No	Yes	Yes	No	No
SN-Ntk-Session-Disconnect-Flag	No	No	No	No	Yes	Yes	No	No
SN-Nw-Reachability-Server-Name	No	No	No	No	Yes	Yes	No	No
SN-Originating-IOI	No	No	No	No	Yes	Yes	No	No
SN-Overload-Disc-Connect-Time	No	No	No	No	Yes	Yes	No	No
SN-Overload-Disc-Inact-Time	No	No	No	No	Yes	Yes	No	No
SN-Overload-Disconnect	No	No	No	No	Yes	Yes	No	No
SN-PDG-TTG-Required	No	No	No	No	Yes	Yes	No	No
SN-PDIF-MIP-Release-TIA	No	No	No	No	Yes	Yes	No	No
SN-PDIF-MIP-Required	No	No	No	No	Yes	Yes	No	No
SN-PDIF-MIP-Simple-IP-Fallback	No	No	No	No	Yes	Yes	No	No
SN-PDSN-Correlation-Id	No	No	No	No	Yes	Yes	No	No
SN-PDSN-Handoff-Req-IP-Addr	No	No	No	No	Yes	Yes	No	No
SN-PDSN-NAS-Id	No	No	No	No	Yes	Yes	No	No
SN-PDSN-NAS-IP-Address	No	No	No	No	Yes	Yes	No	No
SN-Permit-User-Mcast-PDUs	No	No	No	No	Yes	Yes	No	No
SN-PPP-Accept-Peer-v6Ifid	No	No	No	No	Yes	Yes	No	No
SN-PPP-Always-On-Vse	No	No	No	No	Yes	Yes	No	No
SN-PPP-Data-Compression	No	No	No	No	Yes	Yes	No	No
SN-PPP-Data-Compression-Mode	No	No	No	No	Yes	Yes	No	No
SN-PPP-Keepalive	No	No	No	No	Yes	Yes	No	No
SN-PPP-NW-Layer-IPv4	No	No	No	No	Yes	Yes	No	No
SN-PPP-NW-Layer-IPv6	No	No	No	No	Yes	Yes	No	No
SN-PPP-Outbound-Password	No	No	No	No	Yes	Yes	No	No
SN-PPP-Outbound-Username	No	No	No	No	Yes	Yes	No	No
SN-PPP-Progress-Code	No	No	No	No	Yes	Yes	No	No
SN-PPP-Reneg-Disc	No	No	No	No	Yes	Yes	No	No
SN-Prepaid	No	No	No	No	Yes	Yes	No	No
SN-Prepaid-Compressed-Count	No	No	No	No	Yes	Yes	No	No
SN-Prepaid-Final-Duration-Alg	No	No	No	No	Yes	Yes	No	No
SN-Prepaid-Inbound-Octets	No	No	No	No	Yes	Yes	No	No
SN-Prepaid-Outbound-Octets	No	No	No	No	Yes	Yes	No	No
SN-Prepaid-Preference	No	No	No	No	Yes	Yes	No	No
SN-Prepaid-Timeout	No	No	No	No	Yes	Yes	No	No
SN-Prepaid-Total-Octets	No	No	No	No	Yes	Yes	No	No

Attribute	standard	3gpp	3gpp2	3gpp2-835	starent	starent-835	starent-vsa1	starent-vsa1-835
SN-Prepaid-Watermark	No	No	No	No	Yes	Yes	No	No
SN-Primary-DCCA-Peer	No	No	No	No	Yes	Yes	No	No
SN-Primary-DNS-Server	No	No	No	No	Yes	Yes	No	No
SN-Primary-NBNS-Server	No	No	No	No	Yes	Yes	No	No
SN-Proxy-MIP	No	No	No	No	Yes	Yes	No	No
SN-Pseudonym-Username	No	No	No	No	Yes	Yes	No	No
SN-QoS-Background-Class	No	No	No	No	Yes	Yes	No	No
SN-QoS-Class-Background-PHB	No	No	No	No	Yes	Yes	No	No
SN-QoS-Class-Conversational-PHB	No	No	No	No	Yes	Yes	No	No
SN-QoS-Class-Interactive-1-PHB	No	No	No	No	Yes	Yes	No	No
SN-QoS-Class-Interactive-2-PHB	No	No	No	No	Yes	Yes	No	No
SN-QoS-Class-Interactive-3-PHB	No	No	No	No	Yes	Yes	No	No
SN-QoS-Class-Streaming-PHB	No	No	No	No	Yes	Yes	No	No
SN-QoS-Conversation-Class	No	No	No	No	Yes	Yes	No	No
SN-QOS-HLR-Profile	No	No	No	No	Yes	Yes	No	No
SN-QoS-Interactive1-Class	No	No	No	No	Yes	Yes	No	No
SN-QoS-Interactive2-Class	No	No	No	No	Yes	Yes	No	No
SN-QoS-Interactive3-Class	No	No	No	No	Yes	Yes	No	No
SN-QoS-Negotiated	No	No	No	No	Yes	Yes	No	No
SN-QoS-Renegotiation-Timeout	No	No	No	No	Yes	Yes	No	No
SN-QoS-Streaming-Class	No	No	No	No	Yes	Yes	No	No
SN-QoS-Tp-Dnlk	No	No	No	No	Yes	Yes	No	No
SN-QoS-Tp-Uplk	No	No	No	No	Yes	Yes	No	No
SN-QoS-Traffic-Policy	No	No	No	No	Yes	Yes	No	No
SN-Rad-APN-Name	No	No	No	No	Yes	Yes	No	No
SN-Radius-Returned-Username	No	No	No	No	Yes	Yes	No	No
SN-Re-CHAP-Interval	No	No	No	No	Yes	Yes	No	No
SN-Roaming-Behavior	No	No	No	No	Yes	Yes	No	No
SN-Roaming-Profile	No	No	No	No	Yes	Yes	No	No
SN-Roaming-Sub-Use-GGSN	No	No	No	No	Yes	Yes	No	No
SN-ROHC-Flow-Marking-Mode	No	No	No	No	Yes	Yes	No	No
SN-ROHC-Profile-Name	No	No	No	No	Yes	Yes	No	No
SN-Role-Of-Node	No	No	No	No	Yes	Yes	No	No
SN-Routing-Area-Id	No	No	No	No	Yes	Yes	No	No
SN-Rulebase	No	No	No	No	Yes	Yes	No	No
SN-SDP-Session-Description	No	No	No	No	Yes	Yes	No	No
SN-Sec-IP-Pool-Name	No	No	No	No	Yes	Yes	No	No
SN-Secondary-DCCA-Peer	No	No	No	No	Yes	Yes	No	No
SN-Secondary-DNS-Server	No	No	No	No	Yes	Yes	No	No
SN-Secondary-NBNS-Server	No	No	No	No	Yes	Yes	No	No
SN-Service-Address	No	No	No	No	Yes	Yes	No	No
SN-Service-Type	No	No	No	No	Yes	Yes	No	No
SN-Session-Id	No	No	No	No	Yes	Yes	No	No
SN-Simultaneous-SIP-MIP	No	No	No	No	Yes	Yes	No	No
SN-SIP-Method	No	No	No	No	Yes	Yes	No	No
SN-SIP-Request-Time-Stamp	No	No	No	No	Yes	Yes	No	No
SN-SIP-Response-Time-Stamp	No	No	No	No	Yes	Yes	No	No
SN-Software-Version	No	No	No	No	Yes	Yes	No	No

Attribute	standard	3gpp	3gpp2	3gpp2-835	starent	starent-835	starent-vsa1	starent-vsa1-835
SN-Subs-Acc-Flow-Traffic-Valid	No	No	No	No	Yes	Yes	No	No
SN-Subscriber-Accounting	No	No	No	No	Yes	Yes	No	No
SN-Subscriber-Acct-Interim	No	No	No	No	Yes	Yes	No	No
SN-Subscriber-Acct-Mode	No	No	No	No	Yes	Yes	No	No
SN-Subscriber-Acct-Rsp-Action	No	No	No	No	Yes	Yes	No	No
SN-Subscriber-Acct-Start	No	No	No	No	Yes	Yes	No	No
SN-Subscriber-Acct-Stop	No	No	No	No	Yes	Yes	No	No
SN-Subscriber-Class	No	No	No	No	Yes	Yes	No	No
SN-Subscriber-Dormant-Activity	No	No	No	No	Yes	Yes	No	No
SN-Subscriber-IP-Hdr-Neg-Mode	No	No	No	No	Yes	Yes	No	No
SN-Subscriber-IP-TOS-Copy	No	No	No	No	Yes	Yes	No	No
SN-Subscriber-Nexthop-Address	No	No	No	No	Yes	Yes	No	No
SN-Subscriber-No-Interims	No	No	No	No	Yes	Yes	No	No
SN-Subscriber-Permission	No	No	No	No	Yes	Yes	No	No
SN-Subscriber-Template-Name	No	No	No	No	Yes	Yes	No	No
SN-Subs-IMSA-Service-Name	No	No	No	No	Yes	Yes	No	No
SN-Subs-VJ-Slotid-Cmp-Neg-Mode	No	No	No	No	Yes	Yes	No	No
SN-Terminating-IOI	No	No	No	No	Yes	Yes	No	No
SN-Tp-Dnlk-Burst-Size	No	No	No	No	Yes	Yes	No	No
SN-Tp-Dnlk-Committed-Data-Rate	No	No	No	No	Yes	Yes	No	No
SN-Tp-Dnlk-Exceed-Action	No	No	No	No	Yes	Yes	No	No
SN-Tp-Dnlk-Peak-Data-Rate	No	No	No	No	Yes	Yes	No	No
SN-Tp-Dnlk-Violate-Action	No	No	No	No	Yes	Yes	No	No
SN-TPO-Policy	No	No	No	No	Yes	Yes	No	No
SN-Tp-Uplk-Burst-Size	No	No	No	No	Yes	Yes	No	No
SN-Tp-Uplk-Committed-Data-Rate	No	No	No	No	Yes	Yes	No	No
SN-Tp-Uplk-Exceed-Action	No	No	No	No	Yes	Yes	No	No
SN-Tp-Uplk-Peak-Data-Rate	No	No	No	No	Yes	Yes	No	No
SN-Tp-Uplk-Violate-Action	No	No	No	No	Yes	Yes	No	No
SN-Traffic-Group	No	No	No	No	Yes	Yes	No	No
SN-TrafficSelector-Class	No	No	No	No	Yes	Yes	No	No
SN-Transparent-Data	No	No	No	No	Yes	Yes	No	No
SN-Tun-Addr-Policy	No	No	No	No	Yes	Yes	No	No
SN-Tunnel-Gn	No	No	No	No	Yes	Yes	No	No
SN-Tunnel-ISAKMP-Crypto-Map	No	No	No	No	Yes	Yes	No	No
SN-Tunnel-ISAKMP-Secret	No	No	No	No	Yes	Yes	No	No
SN-Tunnel-Load-Balancing	No	No	No	No	Yes	Yes	No	No
SN-Tunnel-Password	No	No	No	No	Yes	Yes	No	No
SN-Unclassify-List-Name	No	No	No	No	Yes	Yes	No	No
SN-Virtual-APN-Name	No	No	No	No	Yes	Yes	No	No
SN-Visiting-Behavior	No	No	No	No	Yes	Yes	No	No
SN-Visiting-Profile	No	No	No	No	Yes	Yes	No	No
SN-Visiting-Sub-Use-GGSN	No	No	No	No	Yes	Yes	No	No
SN-Voice-Push-List-Name	No	No	No	No	Yes	Yes	No	No
SN-VPN-ID	No	No	No	No	Yes	Yes	No	No
SN-VPN-Name	No	No	No	No	Yes	Yes	No	No
SN-WiMAX-Auth-Only	No	No	No	No	Yes	Yes	No	No
State	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes

Attribute	standard	3gpp	3gpp2	3gpp2-835	starent	starent-835	starent-vsa1	starent-vsa1-835
Terminal-Capability	No	No	No	No	No	No	No	No
Termination-Action	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Tunnel-Assignment-ID	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Tunnel-Client-Auth-ID	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Tunnel-Client-Endpoint	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Tunnel-Medium-Type	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Tunnel-Password	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Tunnel-Preference	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Tunnel-Private-Group-ID	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Tunnel-Server-Auth-ID	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Tunnel-Server-Endpoint	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Tunnel-Type	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
User-Name	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
User-Password	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
White-List	No	No	No	No	Yes	Yes	Yes	Yes
WiMAX-Acct-Input-Packets-Giga	No	No	No	No	Yes	No	Yes	No
WiMAX-Acct-Output-Packets-Giga	No	No	No	No	Yes	No	Yes	No
WiMAX-Active-Time	No	No	No	No	Yes	No	Yes	No
WiMAX-Beginning-Of-Session	No	No	No	No	Yes	No	Yes	No
WiMAX-BS-ID	No	No	No	No	Yes	No	Yes	No
WiMAX-Capability	No	No	No	No	Yes	No	Yes	No
WiMAX-Control-Octets-In	No	No	No	No	Yes	No	Yes	No
WiMAX-Control-Octets-Out	No	No	No	No	Yes	No	Yes	No
WiMAX-Control-Packets-In	No	No	No	No	Yes	No	Yes	No
WiMAX-Control-Packets-Out	No	No	No	No	Yes	No	Yes	No
WiMAX-Count-Type	No	No	No	No	Yes	No	Yes	No
WiMAX-Device-Auth-Indicator	No	No	No	No	Yes	No	Yes	No
WiMAX-Flow-Description	No	No	No	No	Yes	No	Yes	No
WiMAX-Home-HNP-PMIP6	No	No	No	No	Yes	No	Yes	No
WiMAX-Home-IPv4-HoA-PMIP6	No	No	No	No	Yes	No	Yes	No
WiMAX-Idle-Mode-Transition	No	No	No	No	Yes	No	Yes	No
WiMAX-IP-TechNology	No	No	No	No	Yes	No	Yes	No
WiMAX-NAP-ID	No	No	No	No	Yes	No	Yes	No
WiMAX-NSP-ID	No	No	No	No	Yes	No	Yes	No
WiMAX-Packet-Flow-Descriptor	No	No	No	No	Yes	No	Yes	No
WiMAX-Packet-Flow-Descriptor-V2	No	No	No	No	Yes	No	Yes	No
WiMAX-PDF-ID	No	No	No	No	Yes	No	Yes	No
WiMAX-PPAC	No	No	No	No	Yes	No	Yes	No
WiMAX-PPAQ	No	No	No	No	Yes	No	Yes	No
WiMAX-Prepaid-Indicator	No	No	No	No	Yes	No	Yes	No
WiMAX-Prepaid-Tariff-Switch	No	No	No	No	Yes	No	Yes	No
WiMAX-QoS-Descriptor	No	No	No	No	Yes	No	Yes	No
WiMAX-SDF-ID	No	No	No	No	Yes	No	Yes	No
WiMAX-Session-Continue	No	No	No	No	Yes	No	Yes	No
WiMAX-Session-Term-Capability	No	No	No	No	Yes	No	Yes	No
Win-Call-Id	No	No	No	No	No	No	No	No
Win-Service-Name	No	No	No	No	No	No	No	No
WSType	No	No	No	No	No	No	No	No