Cisco ASR 5000 Series AAA Interface Administration and Reference

Release 8.x and 9.0

Last Updated June 30, 2010

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-22955-01

Cisco ASR 5000 Series AAA Interface Administration and Reference

CONTENTS

About this Guide

This document pertains to features and functionality that run on and/or that are related to the Cisco® ASR 5000 Chassis, formerly the Starent Networks ST40.

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.
	Electro-Static Discharge (ESD)	Alerts you to take proper grounding precautions before handling a product.

Typeface Conventions	Description
Text represented as a `screen display`	This typeface represents displays that appear on your terminal screen, for example: `Login:`
Text represented as **`commands`**	This typeface represents commands that you enter, 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 grouped brackets. Required keywords and variables are those components that are required to be entered as part of the command syntax.

Command Syntax Conventions	Description
[**keyword** or *variable*]	Optional keywords or variables, or those that a user may or may not choose to use, are surrounded by square brackets.
|	With some commands there may be a group of variables from which the user chooses one. These are called alternative variables and are documented by separating each variable with a vertical bar (also known as a pipe filter). Pipe filters 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

Use the information in this section to contact customer support.

For New Customers: Refer to the support area of http://www.cisco.com for up-to-date product documentation or to submit a service request. A valid username and password is required to this site. Please contact your local sales or service representative for additional information.

For Existing Customers with support contracts through Starent Networks: Refer to the support area of https://support.starentnetworks.com/ for up-to-date product documentation or to submit a service request. A valid username and password is required to this site. Please contact your local sales or service representative for additional information.

Important: For warranty and repair information, please be sure to include the Return Material Authorization (RMA) tracking number on the outside of the package.

Chapter 1
AAA Introduction and Overview

This reference describes the procedures to configure the AAA interface to enable authentication, authorization, and accounting (AAA) functionality for your core network service subscribers in a wireless carrier network.

Procedures to configure and administer core network services are described in detail in the respective product Administration Guides, and 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 along with the *System Administration Guide*.

Important: This reference provides procedure to configure basic AAA interface functionality or your service. Some of the RADIUS and Diameter interface support are license enabled. Contact your sales representative for more information.

Supported Products and License

AAA interface support is available for all services running on the ASR 5000.

Some of the functionality pertaining to prepaid accounting or Diameter-based support are part of enhanced feature support. For more information on these features, refer the *System Enhanced Feature Configuration Guide*.

Important: Information to configure product-specific AAA interfaces are provided in the respective Administration Guides.

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.

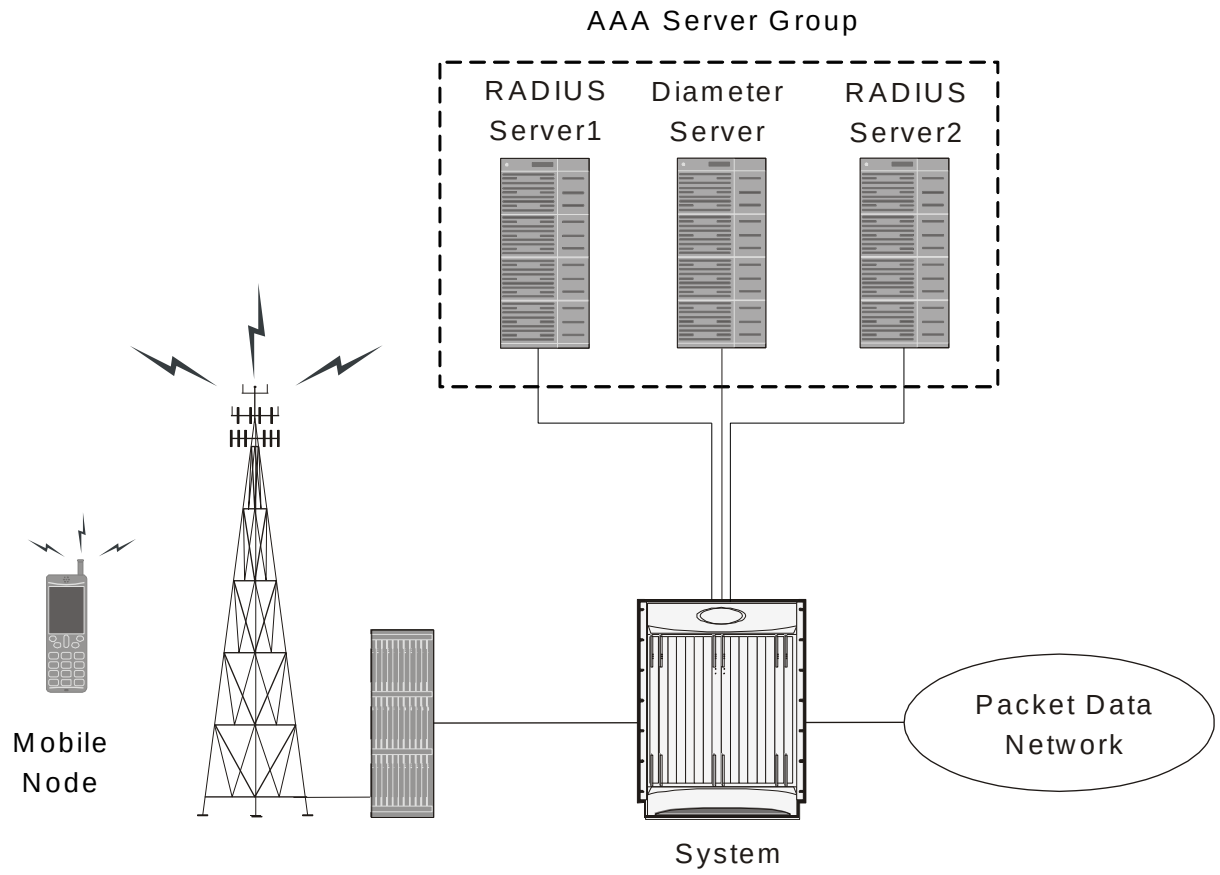
  Accounting enables operator to analyze the services users are accessing as well as the amount of network resources they are consuming. Accounting records are comprised of accounting AVPs and are stored on the accounting server. This accounting information can then be analyzed for network management,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



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.

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.

This chapter includes the following information:

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 as described in the *Verifying and Saving Your Configuration* chapter.

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 <ip_address> key <shared_secret> [ max <value> ] [
oldports | port <tcp_port> ] [ priority <priority> ]
```

```
radius [ mediation-device ] accounting server <ip_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_address> [ backup
<second_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*.
- *<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 *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 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 *System Enhanced Feature Configuration 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 as described in the *Verifying and Saving Your Configuration* chapter.

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 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 <ip_address> [ port
<port_number> ] [ accept-incoming-connections ] [ address
<ip_address_secondary> ]

         peer <peer_name> [ realm <realm_name> ] address <ip_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 { 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 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>* **}**

- Option. 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 Configuring System-Level AAA Functionality .

> ***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 as described in the *Verifying and Saving Your Configuration* chapter.

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>*

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.

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
Verifying and Saving Your Configuration

This chapter describes how to save the system configuration.

Verifying the Configuration

You can use a number of command to verify the configuration of your feature, service, or system. Many are hierarchical in their implementation and some are specific to portions of or specific lines in the configuration file.

Feature Configuration

In many configurations, specific features are set and need to be verified. Examples include APN and IP address pool configuration. Using these examples, enter the following commands to verify proper feature configuration:

show apn all

The output displays the complete configuration for the APN. In this example, an APN called apn1 is configured.

```
access point name (APN): apn1

authentication context: test

pdp type: ipv4

Selection Mode: subscribed

ip source violation: Checked drop limit: 10

accounting mode: gtpp No early PDUs: Disabled

max-primary-pdp-contexts: 1000000 total-pdp-contexts: 1000000

primary contexts: not available total contexts: not available

local ip: 0.0.0.0

primary dns: 0.0.0.0 secondary dns: 0.0.0.0

ppp keep alive period : 0 ppp mtu : 1500

absolute timeout : 0 idle timeout : 0

long duration timeout: 0 long duration action: Detection

ip header compression: vj

data compression: stac mppc deflate compression mode: normal

min compression size: 128

ip output access-group: ip input access-group:

ppp authentication:

allow noauthentication: Enabled imsi
```

```
 authentication:Disabled
```

Enter the following command to display the IP address pool configuration:

show ip pool

The output from this command should look similar to the sample shown below. In this example, all IP pools were configured in the *isp1* context.

```
context : isp1:

+-----Type: (P) - Public (R) - Private

 | (S) - Static (E) - Resource

 |

 |+----State: (G) - Good (D) - Pending Delete (R)-Resizing

 ||

 ||++--Priority: 0..10 (Highest (0) .. Lowest (10))

 ||||

 ||||+-Busyout: (B) - Busyout configured

 |||| |||||| vvvvv Pool Name Start Address Mask/End Address Used Avail

 ----- --------- --------------- --------------- -------- --------

PG00 ipsec 12.12.12.0 255.255.255.0 0 254 PG00

pool1 10.10.0.0 255.255.0.0 0 65534 SG00

vpnpool 192.168.1.250 192.168.1.254 0 5 Total Pool Count: 5
```

Important: Many features can be configured on the system. There are show commands specifically for these features. Refer to the *Command Line Interface Reference* for more information.

Service Configuration

Verify that your service was created and configured properly by entering the following command:

show *<service_type> <service_name>*

The output is a concise listing of the service parameter settings similar to the sample displayed below. In this example, a P-GW service called pgw is configured.

```
Service name : pgw1

Service-Id : 1
```

```
Context : test1

Status : STARTED

Restart Counter : 8

EGTP Service : egtp1

LMA Service : Not defined

Session-Delete-Delay Timer : Enabled

Session-Delete-Delay timeout : 10000(msecs)

PLMN ID List : MCC: 100, MNC: 99

Newcall Policy : None
```

Context Configuration

Verify that your context was created and configured properly by entering the following command:

show context name *<name>*

The output shows the active context. Its ID is similar to the sample displayed below. In this example, a context named *test1* is configured.

```
Context Name     ContextID     State

------------     ---------     -----

test1            2          Active
```

System Configuration

Verify that your entire configuration file was created and configured properly by entering the following command:

show configuration

This command displays the entire configuration including the context and service configurations defined above.

Finding Configuration Errors

Identify errors in your configuration file by entering the following command:

show configuration errors

This command displays errors it finds within the configuration. For example, if you have created a service named "service1", but entered it as "srv1" in another part of the configuration, the system displays this error.

You must refine this command to specify particular sections of the configuration. Add the **section** keyword and choose a section from the help menu:

show configuration errors section ggsn-service

or

show configuration errors section aaa-config

If the configuration contains no errors, an output similar to the following is displayed:

```
##################################################################################

Displaying Global
AAA-configuration errors
##################################################################################

Total 0 error(s) in this section !
```

Saving the Configuration

Save system configuration information to a file locally or to a remote node on the network. You can use this configuration file on any other systems that require the same configuration.

Files saved locally can be stored in the SPC's/SMC's CompactFlash or on an installed PCMCIA memory card on the SPC/SMC. Files that are saved to a remote network node can be transmitted using either FTP, or TFTP.

Saving the Configuration on the Chassis

These instructions assume that you are at the root prompt for the Exec mode:

```
[local]host_name#
```

To save your current configuration, enter the following command:

```
save configuration url [-redundant] [-noconfirm] [showsecrets] [verbose]
```

Keyword/Variable	Description
url	Specifies the path and name to which the configuration file is to be stored. *url* may refer to a local or a remote file. *url* must be entered using one of the following formats: • **{ /flash | /pcmcia1 | /pcmcia2 }** *[/dir] /file_name* • **file:/{ /flash | /pcmcia1 | /pcmcia2 }** *[/dir] /file_name* • **tftp://**{ *ipaddress*|*host_name*[*:port#*]} [*/directory*] */file_name* • **ftp://**[*username*[*:pwd*] *@*] { *ipaddress*|*host_name*} [*:port#*] [*/directory*] */file_name* • **sftp://**[*username*[:*pwd*] *@*] { *ipaddress*|*host_name*} [*:port#*] [*/directory*] */file_name* **/flash** corresponds to the CompactFlash on the SPC/SMC. **/pcmcia1** corresponds to PCMCIA slot 1. **/pcmcia2** corresponds to PCMCIA slot 2. *ipaddress* is the IP address of the network server. *host_name* is the network server's *hostname*. *port#* is the network server's logical port number. Defaults are: • tftp: 69 - data • ftp: 20 - data, 21 - control • sftp: 115 - data Note: *host_name* can only be used if the **networkconfig** parameter is configured for DHCP and the DHCP server returns a valid nameserv er.dx *username* is the username required to gain access to the server if necessary. *password* is the password for the specified username if required. */directory* specifies the directory where the file is located if one exists. */file_name* specifies the name of the configuration file to be saved. Note: Configuration files should be named with a .cfg extension.
-redundant	Optional: This keyword directs the system to save the CLI configuration file to the local device, defined by the url variable, and then automatically copy that same file to the like device on the Standby SPC/SMC, if available. Note: This keyword will only work for like local devices that are located on both the active and standby SPCs/SMCs. For example, if you save the file to the /pcmcia1 device on the active SPC/SMC, that same type of device (a PC-Card in Slot 1 of the standby SPC/SMC) must be available. Otherwise, a failure message is displayed. Note: If saving the file to an external network (non-local) device, the system disregards this keyword.

Keyword/Variable	Description
-noconfirm	Optional: Indicates that no confirmation is to be given prior to saving the configuration information to the specified filename (if one was specified) or to the currently active configuration file (if none was specified).
showsecrets	Optional: This keyword causes the CLI configuration file to be saved with all passwords in plain text, rather than their default encrypted format.
verbose	Optional: Specifies that every parameter that is being saved to the new configuration file should be displayed.

Important: The **`-redundant`** keyword is only applicable when saving a configuration file to local devices.This command does not synchronize the local file system. If you have added, modified, or deleted other files or directories to or from a local device for the active SPC/SMC, then you must synchronize the local file system on both SPCs/SMCs.

To save a configuration file called system.cfg to a directory that was previously created called cfgfiles on the SPC's/SMC's CompactFlash, enter the following command:

```
save configuration /flash/cfgfiles/system.cfg
```

To save a configuration file called simple_ip.cfg to a directory called host_name_configs using an FTP server with an IP address of 192.168.34.156 on which you have an account with a username of administrator and a password of secure, use the following command:

```
save configuration
ftp://administrator:secure@192.168.34.156/host_name_configs/
simple_ip.cfg
```

To save a configuration file called init_config.cfg to the root directory of a TFTP server with a hostname of config_server, enter the following command:

`save configuration` *`tftp://config_server/init_config.cfg`*

Chapter 4
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

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

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, please refer to the *Command Line Reference*.

Session Recovery and AAA Statistics Behavior

Important: 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.

Chapter 5
Diameter Attribute Definitions

This chapter presents Diameter attribute definitions.

For the quick reference table, see the *Diameter Attribute Quick Reference* appendix.

Diameter Dictionary Types

DPCA

The Diameter Policy Control Application (DPCA) dictionaries are used by the PDSN, GGSN, HA, IPSG product(s).

To specify the Diameter dictionary for Policy Control Configuration, in Policy Control Configuration mode use the following command:

```
diameter dictionary { Standard | dpca-custom1 | dpca-custom10 | dpca-custom11 |
dpca-custom12 | dpca-custom13 | dpca-custom14 | dpca-custom15 | dpca-custom16 |
dpca-custom17 | dpca-custom18 | dpca-custom19 | dpca-custom2 | dpca-custom20 |
dpca-custom3 | dpca-custom4 | dpca-custom5 | dpca-custom6 | dpca-custom7 | dpca-
custom8 | dpca-custom9 | gxa-3gpp2-standard | gxc-standard | pdsn-ty | r8-gx-
standard | std-pdsn-ty | ty-plus | ty-standard }
```

Dictionary	Description
Standard	Specifies standard attributes for the Rel 6 Gx interface.
dpca-custom1...dpca-custom*n*	Custom-defined dictionaries.
gxa-3gpp2-standard	Specifies standard Gxa 3GPP2 Standard attributes.
gxc-standard	Specifies Gxc Standard attributes.
pdsn-ty	Specifies the standard attributes for the PDSN Ty interface.
r8-gx-standard	Specifies standard R8 Gx attributes.
std-pdsn-ty	Specifies standard attributes for the Ty interface.
ty-plus	Specifies customer-specific enhanced attributes for the Ty interface.
ty-standard	Specifies standard Ty attributes.

Important: For information on custom-defined dictionaries, please contact your local service representative.

DCCA

The Diameter Credit Control Application (DCCA) dictionaries are used by the GGSN and IPSG product(s).

To specify the DCCA dictionary for Active Charging service, in Credit Control Configuration mode use the following command:

Dictionary	Description
dcca-custom1...dcca-custom*n*	Custom-defined dictionaries.
standard	Specifies standard attributes for the Gy interface.

```
diameter dictionary { dcca-custom1 | dcca-custom10 | dcca-custom11 | dcca-
custom12 | dcca-custom13 | dcca-custom14 | dcca-custom15 | dcca-custom16 | dcca-
custom17 | dcca-custom18 | dcca-custom19 | dcca-custom2 | dcca-custom20 | dcca-
custom3 | dcca-custom4 | dcca-custom5 | dcca-custom6 | dcca-custom7 | dcca-
custom8 | dcca-custom9 | standard }
```

Important: For information on custom-defined dictionaries, please contact your local service representative.

CSCF

The Diameter Policy Control dictionaries for Call Session Control Function (CSCF) Diameter Policy External Control Application (DPECA) service are used by the SCM P-CSCF product.

In Star OS 8.1 and later releases, to specify the Diameter Policy Control dictionary, in CSCF Proxy-CSCF Configuration mode use the following command:

```
diameter policy-control dictionary { Gq-custom | Gq-standard | Rq-custom | Rx-
rel8 | Rx-standard | Tx-standard | custom01 | custom02 | custom03 | custom04 |
custom05 | custom06 | custom07 | custom08 | custom09 }
```

Dictionary	Description
Cx-standard	Specifies standard attributes for the Cx interface.
Gq-custom	Specifies customized attributes for the 3GPP Gq interface.
Gq-standard	Specifies standard attributes for the 3GPP Gq interface.
Rq-custom	Custom-defined dictionary.
Rx-rel8	Rel. 8 Rx dictionary.
Rx-standard	Specifies standard attributes for the 3GPP Rx interface.
Tx-standard	Specifies the standard attributes for the 3GPP2 Tx interface.
custom01...custom*n*	Custom-defined dictionaries.

Important: For information on custom-defined dictionaries, please please contact your local service representative.

Diameter AAA

The Diameter Authentication, Authorization, and Accounting (AAA) dictionaries are used by the S-CSCF and AIMS product(s).

To specify the AAA dictionary to be used when Diameter is being used for accounting, in the AAA Server Group Configuration mode or in the Context Configuration mode, use the following command:

```
diameter accounting dictionary { aaa-custom1 | aaa-custom10 | aaa-custom2 | aaa-custom3 | aaa-custom4 | aaa-custom5 | aaa-custom6 | aaa-custom7 | aaa-custom8 | aaa-custom9 | nasreq | rf-plus }
```

To specify the AAA dictionary to be used when Diameter is being used for authentication, in the AAA Server Group Configuration mode or in the Context Configuration mode, use the following command:

```
diameter authentication dictionary { aaa-custom1 | aaa-custom10 | aaa-custom11 | aaa-custom12 | aaa-custom13 | aaa-custom14 | aaa-custom15 | aaa-custom16 | aaa-custom17 | aaa-custom18 | aaa-custom19 | aaa-custom2 | aaa-custom20 | aaa-custom3 | aaa-custom4 | aaa-custom5 | aaa-custom6 | aaa-custom7 | aaa-custom8 | aaa-custom9 | nasreq }
```

Dictionary	Description
aaa-custom1...aaa-custom*n*	Custom-defined dictionaries.
nasreq	Specifies the NASREQ attributes defined by RFC 4005.
rf-plus	Specifies customer-specific enhanced attributes for the Rf interface.

Important: For information on custom-defined dictionaries, please contact your local service representative.

Attributes

Important: Diameter attributes received by the system from the Diameter server always take precedence over local-subscriber attributes and parameters configured on the system.

3GPP-Called-Station-Id

This AVP identifies the layer 2 addresses the user contacted in the request.

AVP Header
30 10415

Vendor ID
10415

VSA Type
30

AVP Type
OCTETSTRING

Group Value
N/A

AVP Flag
N/A

3GPP-CAMEL-Charging-Info

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

AVP Header
24 10415

Vendor ID
10415

VSA Type
24

AVP Type
UTF8STRING

Group Value
N/A

AVP Flag
N/A

3GPP-CF-IPv6-Address

3GPP-CF-IPv6-Address.

AVP Header
14 10415

Vendor ID
10415

VSA Type
14

AVP Type
OCTETSTRING

Group Value
N/A

AVP Flag
M

3GPP-CG-Address

This AVP contains the Charging Gateway address.

AVP Header
846 10415

Vendor ID
10415

VSA Type
846

AVP Type
OCTETSTRING

Group Value
N/A

AVP Flag
M

3GPP-Charging-Characteristics

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

AVP Header
13 10415

Vendor ID
10415

VSA Type
13

AVP Type

UTF8STRING

Group Value
N/A

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.

AVP Header
2 10415

Vendor ID
10415

VSA Type
2

AVP Type
UINT32

Group Value
N/A

AVP Flag
M

3GPP-Charging-Rule-Based-Name

This AVP indicates the group name of charging rules residing in the TPF.

AVP Header
1004 10415

Vendor ID
10415

VSA Type
1004

AVP Type
UTF8STRING

Group Value
N/A

AVP Flag
M

3GPP-Feature-List

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

AVP Header
630 10415

Vendor ID
10415

VSA Type
630

AVP Type
UINT32

Group Value
N/A

AVP Flag
M

3GPP-Feature-List-ID

This AVP contains the identity of a feature list.

AVP Header
629 10415

Vendor ID
10415

VSA Type
629

AVP Type
UINT32

Group Value
N/A

AVP Flag
M

3GPP-GGSN-Address

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

AVP Header
7 10415

Vendor ID
10415

VSA Type
7

AVP Type
OCTETSTRING

Group Value
N/A

AVP Flag
M

3GPP-GGSN-MCC-MNC

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

AVP Header
9 10415

Vendor ID
10415

VSA Type
9

AVP Type
UTF8STRING

Group Value
N/A

AVP Flag
M

3GPP-GPRS-QoS-Negotiated-Profile

This AVP contains QoS profile applied by GGSN.

AVP Header
5 10415

Vendor ID
10415

VSA Type
5

AVP Type
UTF8STRING

Group Value
N/A

AVP Flag
M

3GPP-IMEISV

This AVP contains International Mobile Equipment ID and its Software Version.

AVP Header
20 10415

Vendor ID
10415

VSA Type
20

AVP Type
OCTETSTRING

Group Value
N/A

AVP Flag
M

3GPP-IMSI

This AVP contains an IMSI of the user.

AVP Header
1 10415

Vendor ID
10415

VSA Type
1

AVP Type
UTF8STRING

Group Value
N/A

AVP Flag
M

3GPP-IMSI-MCC-MNC

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

AVP Header
8 10415

Vendor ID
10415

VSA Type
8

AVP Type
UTF8STRING

Group Value
N/A

AVP Flag
M

3GPP-MS-TimeZone

Indicates the Mobile Station Time Zone.

AVP Header
23 10415

Vendor ID
10415

VSA Type
23

AVP Type
OCTETSTRING

Group Value
N/A

AVP Flag
M

3GPP-NSAPI

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

AVP Header
10 10415

Vendor ID
10415

VSA Type
10

AVP Type
UTF8STRING

Group Value
N/A

AVP Flag
M

3GPP-PDP-Type

Type of PDP context, for example IP or PPP.

AVP Header
3 10415

Vendor ID
10415

VSA Type
3

AVP Type
ENUM. Supported values are:

IPv4 (0)

PPP (1)

IPv6 (2)

IPv4v6 (3)

Group Value
N/A

AVP Flag
M

3GPP-Public-Identity

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

AVP Header
601 10415

Vendor ID
10415

VSA Type
601

AVP Type
UTF8STRING

Group Value
N/A

AVP Flag
M

3GPP-Quota-Consumption-Time

This AVP contains an idle traffic threshold time in seconds.

AVP Header
881 10415

Vendor ID
10415

VSA Type
881

AVP Type
UINT32

Group Value
N/A

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.

AVP Header
871 10415

Vendor ID
10415

VSA Type
871

AVP Type
UINT32

Group Value
N/A

AVP Flag
M

3GPP-RAT-Type

Indicates which Radio Access Technology is currently serving the UE.

AVP Header
21 10415

Vendor ID
10415

VSA Type
21

AVP Type
ENUM

Group Value
N/A

AVP Flag
M

3GPP-RAT-Type-Enum

Type of Radio Access Technology.

AVP Header
21 10415

Vendor ID
10415

VSA Type
21

AVP Type
ENUM. Supported values are:

UTRAN (1)

GERAN (2)

WLAN (3)

GAN (4)

HSPA (5)

EUTRAN (6)

3GPP2_eHRPD (102)

Group Value
N/A

AVP Flag
M

3GPP-Reporting-Reason

Specifies the reason for usage reporting for one or more types of quota for a particular category.

AVP Header
872 10415

Vendor ID
10415

VSA Type
872

AVP Type
ENUM. Supported values are:

THRESHOLD (0)

QHT (1)

FINAL (2)

QUOTA_EXAUSTED (3)

VALIDITY_TIME (4)

OTHER_QUOTA_TYPE (5)

RATING_CONDITION_CHANGE (6)

FORCED_REAUTHORIZATION (7)

POOL_EXAISTED (8)

Group Value
N/A

AVP Flag
M

3GPP-Selection-Mode

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

AVP Header
12 10415

Vendor ID
10415

VSA Type
12

AVP Type
UTF8STRING

Group Value
N/A

AVP Flag
M

3GPP-Server-Name

This AVP contains a SIP-URL of the S-CSCF server.

AVP Header
602 10415

Vendor ID
10415

VSA Type
602

AVP Type
UTF8STRING

Group Value
N/A

AVP Flag
M

3GPP-Session-Stop-Indicator

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

AVP Header
11 10415

Vendor ID
10415

VSA Type
11

AVP Type

OCTETSTRING

Group Value
N/A

AVP Flag
M

3GPP-SGSN-Address

This AVP contains the SGSN address 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.

AVP Header
6 10415

Vendor ID
10415

VSA Type
6

AVP Type
OCTETSTRING

Group Value
N/A

AVP Flag
M

3GPP-SGSN-IPv6-Address

This AVP contains the SGSN IPv6 address 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.

AVP Header
15 10415

Vendor ID
10415

VSA Type
15

AVP Type
OCTETSTRING

Group Value
N/A

AVP Flag
M

3GPP-SGSN-MCC-MNC

Specifies the MCC-MNC of the network the SGSN belongs to.

AVP Header
18 10415

Vendor ID
10415

VSA Type
18

AVP Type
UTF8STRING

Group Value
N/A

AVP Flag
M

3GPP-Supported-Features

This AVP contains a list of supported features of the origin host.

AVP Header
628 10415

Vendor ID
10415

VSA Type
628

AVP Type
GROUPED

Group Value
[VENDOR_ID]

[3GPP_FEATURE_LIST_ID]

[3GPP_FEATURE_LIST]

AVP Flag
M

3GPP-Time-Quota-Threshold

This AVP contains a threshold value in seconds.

AVP Header
868 10415

Vendor ID
10415

VSA Type
868

AVP Type
UINT32

Group Value
N/A

AVP Flag
M

3GPP-Trigger-Type

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

AVP Header
870 10415

Vendor ID
10415

VSA Type
870

AVP Type
ENUM. Supported values are:

CHANGE_IN_SGSN_IP_ADDRESS (1)

CHANGE_IN_QOS (2)

CHANGE_IN_LOCATION (3)

CHANGE_IN_RAT (4)

Group Value
N/A

AVP Flag
M

3GPP-Unit-Quota-Threshold

This AVP contains a threshold value in service specific units.

AVP Header
1226 10415

Vendor ID
10415

VSA Type
1226

AVP Type
UINT32

Group Value
N/A

AVP Flag
M

3GPP-User-Data

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

AVP Header
606 10415

Vendor ID
10415

VSA Type
606

AVP Type
OCTETSTRING

Group Value
N/A

AVP Flag
M

3GPP-User-Location-Info

This AVP contains information about the users current geographical location.

AVP Header
22 10415

Vendor ID
10415

VSA Type
22

AVP Type
UTF8STRING

Group Value
N/A

AVP Flag
M

3GPP-Volume-Quota-Threshold

This AVP contains a threshold value in octets.

AVP Header
869 10415

Vendor ID
10415

VSA Type
869

AVP Type
UINT32

Group Value
N/A

AVP Flag
M

3GPP2-Allowed-Persistent-TFTS

Maximum allowed persistent TFTs.

AVP Header
6083 5535

Vendor ID
5535

VSA Type
6083

AVP Type
UINT32

Group Value
N/A

AVP Flag
M

3GPP2-BSID

3GPP2 BSID.

AVP Header
9010 5535

Vendor ID
5535

VSA Type
9010

AVP Type
OCTETSTRING

Group Value
N/A

AVP Flag
M

3GPP2-Correlation-Id

Correlation ID in 3GPP2 networks.

AVP Header
6071 5535

Vendor ID
5535

VSA Type
6071

AVP Type
OCTETSTRING

Group Value
N/A

AVP Flag
M

3GPP2-Information

AVP Header
6077 5535

Vendor ID
5535

VSA Type
6077

AVP Type
GROUPED

Group Value
[SUBSCRIBER_PRIORITY]

[AUTH_PROFILE_ID_FORWARD]

[AUTH_PROFILE_ID_REVERSE]

[AUTH_PROFILE_ID_BI_DIRECTION]

AVP Flag
M

3GPP2-Inter-User-Priority

Inter user priority.

AVP Header
139 5535

Vendor ID
5535

VSA Type
139

AVP Type
UINT32

Group Value
N/A

AVP Flag
M

3GPP2-MEID

This AVP contains the International Mobile Equipment Identity.

AVP Header
1471 10415

Vendor ID
10415

VSA Type
1471

AVP Type
OCTETSTRING

Group Value
N/A

AVP Flag
M

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

Maximum allowed bandwidth for best effort link.

AVP Header
130 5535

Vendor ID
5535

VSA Type
130

AVP Type
UINT32

Group Value
N/A

AVP Flag
M

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

Maximum service option instances.

AVP Header
6082 5535

Vendor ID
5535

VSA Type
6082

AVP Type
UINT32

Group Value
N/A

AVP Flag
M

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

Per flow priority for the user.

AVP Header
6088 5535

Vendor ID
5535

VSA Type
6088

AVP Type
UINT32

Group Value
N/A

AVP Flag
M

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

Maximum allowed link flows per service instance.

AVP Header
6084 5535

Vendor ID
5535

VSA Type
6084

AVP Type
UINT32

Group Value
N/A

AVP Flag
M

3GPP2-RAT-Type

3GPP2-RAT type.

AVP Header
1001 5535

Vendor ID
5535

VSA Type
1001

AVP Type
ENUM. Supported values are:

3G1X (0)

HRPD (1)

WLAN (2)

Group Value
N/A

AVP Flag
M

3GPP2-RP-Session-ID

3GPP2 RP Session Identifier.

AVP Header
6074 5535

Vendor ID
5535

VSA Type
6074

AVP Type
OCTETSTRING

Group Value
N/A

AVP Flag
M

3GPP2-Service-Option

3GPP2 Service option number.

AVP Header
16 5535

Vendor ID
5535

VSA Type
16

AVP Type
UINT32

Group Value
N/A

AVP Flag
M

3GPP2-Service-Option-Profile

3GPP2-Service-Option-Profile.

AVP Header
74 5535

Vendor ID
5535

VSA Type
74

AVP Type
GROUPED

Group Value
[3GPP2_SERVICE_OPTION]

[3GPP2_MAX_INST_PER_SERVICE_OPTION]

AVP Flag
M

3GPP2-Serving-PCF

3GPP2 Serving PCF Address

AVP Header
6073 5535

Vendor ID
5535

VSA Type
6073

AVP Type
ADDRESS

Group Value
N/A

AVP Flag
M

3GPP2-User-Zone

3GPP2 User Zone.

AVP Header
6075 5535

Vendor ID
5535

VSA Type
6075

AVP Type
OCTETSTRING

Group Value
N/A

AVP Flag
M

Abort-Cause

Determines the cause of a session abort request or of an RAR indicating a PDP context release.

AVP Header
500 10415

Vendor ID
10415

VSA Type
500

AVP Type
ENUM

Group Value
N/A

AVP Flag
M

Acceptable-Service-Info

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

AVP Header
526 10415

Vendor ID
10415

VSA Type
526

AVP Type
GROUPED

Group Value
[MEDIA_COMPONENT_DESCRIPTION]
[MAX_REQUESTED_BANDWIDTH_DL]
[MAX_REQUESTED_BANDWIDTH]

AVP Flag
M

Access-Network-Charging-Address

Indicates the IP address of the network entity within the access network performing charging (e.g. the GGSN IP address).

AVP Header
501 10415

Vendor ID
10415

VSA Type
501

AVP Type
ADDRESS

Group Value
N/A

AVP Flag
M

Access-Network-Charging-Identifier

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

AVP Header
502 10415

Vendor ID
10415

VSA Type
502

AVP Type
GROUPED

Group Value
[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.

AVP Header
1022 10415

Vendor ID
10415

VSA Type
1022

AVP Type
GROUPED

Group Value
[ACCESS_NETWORK_CHARGING_IDENTIFIER_VALUE]

[CHARGING_RULE_BASE_NAME]

[CHARGING_RULE_NAME]

AVP Flag
M

Access-Network-Charging-Identifier-Ty

This grouped 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.

AVP Header
1022 10415

Vendor ID
10415

VSA Type
1022

AVP Type
GROUPED

Group Value
[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 (e.g. GCID).

AVP Header

503 10415

Vendor ID
10415

VSA Type
503

AVP Type
OCTETSTRING

Group Value
N/A

AVP Flag
M

Access-Network-Charging-Physical-Access-Id

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

AVP Header
1472 10415

Vendor ID
10415

VSA Type
1472

AVP Type
GROUPED

Group Value
[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 indicates the domain of the physical device the user is connected for charging.

AVP Header
1474 10415

Vendor ID
10415

VSA Type
1474

AVP Type
OCTETSTRING

Group Value
N/A

AVP Flag
M

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

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

AVP Header
1473 10415

Vendor ID
10415

VSA Type
1473

AVP Type
OCTETSTRING

Group Value
N/A

AVP Flag
M

Access-Network-Information

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

AVP Header
1263 0

Vendor ID
0

VSA Type
1263

AVP Type
OCTETSTRING

Group Value
N/A

AVP Flag
M

Access-Network-Physical-Access-Id

Conveys an identifier that represents the topological segment hosting the AT within the serving IP-CAN.

AVP Header
1472 5535

Vendor ID
5535

VSA Type
1472

AVP Type
GROUPED

Group Value
[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.

AVP Header
1474 5535

Vendor ID
5535

VSA Type
1474

AVP Type
OCTETSTRING

Group Value
N/A

AVP Flag
M

Access-Network-Physical-Access-Id-Value

Access-Network-Physical-Access ID Value.

AVP Header
1473 5535

Vendor ID
5535

VSA Type
1473

AVP Type
OCTETSTRING

Group Value
N/A

AVP Flag
M

Access-Network-Type

Access Network Type.

AVP Header
306 0

Vendor ID
0

VSA Type
306

AVP Type
GROUPED

Group Value
N/A

AVP Flag
M

Access-Restriction-Data

Contains a bit mask indicating the services of a subscriber that are barred by the operator.

AVP Header
1426 10415

Vendor ID
10415

VSA Type
1426

AVP Type
UINT32

Group Value
N/A

AVP Flag
M

Accounting-EAP-Auth-Method

Indicates the EAP method(s) used to authenticate the user.

AVP Header
465 0

Vendor ID
0

VSA Type
465

AVP Type
UINT64

Group Value
N/A

AVP Flag
N/A

Accounting-Input-Octets

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

AVP Header
363 0

Vendor ID
0

VSA Type
363

AVP Type
UINT64

Group Value
N/A

AVP Flag
M

Accounting-Input-Packets

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

AVP Header
365 0

Vendor ID
0

VSA Type
365

AVP Type
UINT64

Group Value
N/A

AVP Flag
M

Accounting-Output-Octets

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

AVP Header
364 0

Vendor ID
0

VSA Type
364

AVP Type
UINT64

Group Value
N/A

AVP Flag
M

Accounting-Output-Packets

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

AVP Header
366 0

Vendor ID
0

VSA Type
366

AVP Type
UINT64

Group Value
N/A

AVP Flag
M

Accounting-Record-Number

This AVP identifies this record within one session.

AVP Header
485 0

Vendor ID
0

VSA Type
485

AVP Type
UINT32

Group Value
N/A

AVP Flag
M

Accounting-Record-Type

This AVP contains the type of accounting record being sent.

AVP Header
480 0

Vendor ID
0

VSA Type
480

AVP Type
ENUM. Supported values are:

EVENT_RECORD (1)

START_RECORD (2)

INTERIM_RECORD (3)

STOP_RECORD (4)

Group Value
N/A

AVP Flag
M

Accounting-Sub-Session-Id

This AVP contains the accounting sub-session identifier.

AVP Header
287 0

Vendor ID
0

VSA Type
287

AVP Type
UINT64

Group Value
N/A

AVP Flag
M

Acct-Application-Id

Advertise support of the Accounting portion of an application.

AVP Header
259 0

Vendor ID

0

VSA Type
259

AVP Type
UINT32

Group Value
N/A

AVP Flag
M

Acct-Interim-Interval

Sent from the Diameter Home Authorization Server to the Diameter client.

AVP Header
85 0

Vendor ID
0

VSA Type
85

AVP Type
UINT32

Group Value
N/A

AVP Flag
N/A

Acct-Multi-Session-Id

Link multiple related accounting sessions.

AVP Header
50 0

Vendor ID
0

VSA Type
50

AVP Type
UTF8STRING

Group Value
N/A

AVP Flag
M

Acct-Realtime-Required

Acct-Realtime-Required.

AVP Header
483 0

Vendor ID
0

VSA Type
483

AVP Type
ENUM. Supported values are:

DELIVER_AND_GRANT (1)

GRANT_AND_STORE (2)

GRANT_AND_LOSE (3)

Group Value
N/A

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.

AVP Header
44 0

Vendor ID
0

VSA Type
44

AVP Type
OCTETSTRING

Group Value
N/A

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.

AVP Header
46 10415

Vendor ID
10415

VSA Type
46

AVP Type
UINT32

Group Value
N/A

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.

AVP Header
910 10415

Vendor ID
10415

VSA Type
910

AVP Type
OCTETSTRING

Group Value
N/A

AVP Flag
M

Address-Realm

This AVP contains the realm that the user belongs to.

AVP Header
1005 0

Vendor ID
0

VSA Type
1005

AVP Type
OCTETSTRING

Group Value
N/A

AVP Flag
M

AF-Application-Identifier

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

AVP Header
504 10415

Vendor ID
10415

VSA Type
504

AVP Type
OCTETSTRING

Group Value
N/A

AVP Flag
M

AF-Charging-Identifier

The Application Function (AF) charging identifier that may be used in charging correlation.

AVP Header
505 10415

Vendor ID
10415

VSA Type
505

AVP Type
OCTETSTRING

Group Value
N/A

AVP Flag
M

AF-Correlation-Information

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

AVP Header
1276 10415

Vendor ID
10415

VSA Type
1276

AVP Type
GROUPED

Group Value
[AF_CHARGING_IDENTIFIER]

[FLOWS]

AVP Flag
M

AGW-IP-Address

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

AVP Header
806 5535

Vendor ID
5535

VSA Type
806

AVP Type
OctetString

Group Value
N/A

AVP Flag
M

AGW-IPv6-Address

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

AVP Header
807 5535

Vendor ID
5535

VSA Type
807

AVP Type
OctetString

Group Value
N/A

AVP Flag
M

AGW-MCC-MNC

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

AVP Header
1002 5535

Vendor ID
5535

VSA Type
1002

AVP Type
OCTETSTRING

Group Value
N/A

AVP Flag
M

Alert-Reason

Alert reason.

AVP Header
1434 10415

Vendor ID
10415

VSA Type
1434

AVP Type
ENUM. Supported values are:

UE_PRESENT (0)

UE_MEMORY_AVAILABLE (1)

Group Value
N/A

AVP Flag
M

All-APN-Configurations-Included-Indicator

All APN configurations included indicator.

AVP Header
1428 10415

Vendor ID
10415

VSA Type

1428

AVP Type
ENUM. Supported values are:

ALL_APN_CONFIGURATIONS_INCLUDED (0)

MODIFIED_ADDED_APN_CONFIGURATIONS_INCLUDED (1)

Group Value
N/A

AVP Flag
M

Allocation-Retention-Priority

Allocation and retention priority.

AVP Header
1034 10415

Vendor ID
10415

VSA Type
1034

AVP Type
GROUPED

Group Value
[AVP_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.

AVP Header
905 10415

Vendor ID
10415

VSA Type
905

AVP Type
UTF8STRING

Group Value
N/A

AVP Flag
M

AMBR

AMBR.

AVP Header
1435 10415

Vendor ID
10415

VSA Type
1435

AVP Type
GROUPED

Group Value
[MAX_REQUESTED_BANDWIDTH_UL]

[MAX_REQUESTED_BANDWIDTH_DL]

AVP Flag
M

AN-GW-Address

Access network gateway address.

AVP Header
1050 10415

Vendor ID
10415

VSA Type
1050

AVP Type
ADDRESS

Group Value
N/A

AVP Flag
M

AN-Trusted

AN-Trusted

AVP Header
1503 10415

Vendor ID

10415

VSA Type
1503

AVP Type
ENUM. Supported values are:

TRUSTED (0)

UNTRUSTED (1)

Group Value
N/A

AVP Flag
M

ANID

Access Network Identity.

AVP Header
6112 10415

Vendor ID
10415

VSA Type
6112

AVP Type
UTF8STRING

Group Value
N/A

AVP Flag
M

APN-Aggregate-Max-Bitrate-DL

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

AVP Header
1040 10415

Vendor ID
10415

VSA Type
1040

AVP Type
UINT32

Group Value
N/A

AVP Flag
M

APN-Aggregate-Max-Bitrate-UL

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

AVP Header
1041 10415

Vendor ID
10415

VSA Type
1041

AVP Type
UINT32

Group Value
N/A

AVP Flag
M

APN-Authorized

APN-Authorized.

AVP Header
6090 10415

Vendor ID
10415

VSA Type
6090

AVP Type
GROUPED

Group Value
[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

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

AVP Header
6091 10415

Vendor ID
10415

VSA Type
6091

AVP Type
ENUM. Supported values are:

NON_3GPP_APNS_ENABLE (0)

NON_3GPP_APNS_DISABLE (1)

Group Value
N/A

AVP Flag
M

APN-Configuration

AVP Header
1430 10415

Vendor ID
10415

VSA Type
1430

AVP Type
GROUPED

Group Value
[CONTEXT_IDENTIFIER]

[PDN_TYPE]

[SERVICE_SELECTION]

[EPS_SUBSCRIBED_QOS_PROFILE]

[VPLMN_DYNAMIC_ADDRESS_ALLOWED]

[MIP6_AGENT_INFO]

[PDN_GW_ALLOCATION_TYPE]

[3GPP_CHARGING_CHARACTERISTICS]

[AMBR]

[SERVED_PARTY_IP_ADDRESS]

[SPECIFIC_APN_INFO]

AVP Flag
M

APN-Configuration-Profile

APN-Configuration-Profile.

AVP Header
1429 10415

Vendor ID
10415

VSA Type
1429

AVP Type
GROUPED

Group Value
[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.

AVP Header
1427 10415

Vendor ID
10415

VSA Type
1427

AVP Type
UTF8STRING

Group Value
N/A

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.

AVP Header
837 10415

Vendor ID
10415

VSA Type
837

AVP Type
UTF8STRING

Group Value
N/A

AVP Flag
M

Application-Server

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

AVP Header
836 10415

Vendor ID
10415

VSA Type
836

AVP Type
UTF8STRING

Group Value
N/A

AVP Flag
M

Application-Server-Information

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

AVP Header
850 10415

Vendor ID
10415

VSA Type
850

AVP Type
GROUPED

Group Value
[APPLICATION_SERVER]

[APPLICATION_PROVIDED_CALLED_PARTY_ADDRESS]

AVP Flag
M

ARP

Allocation and retention priority for the corresponding APN configuration.

AVP Header
6039 10415

Vendor ID
10415

VSA Type
6039

AVP Type
UINT32

Group Value
N/A

AVP Flag
M

Associated-Identities

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

AVP Header
632 10415

Vendor ID
10415

VSA Type
632

AVP Type
GROUPED

Group Value
[USER_NAME]

AVP Flag
M

Associated-URI

Associated-URI.

AVP Header

856 10415

Vendor ID
10415

VSA Type
856

AVP Type
UTF8STRING

Group Value
N/A

AVP Flag
M

Auth-Application-Id

This AVP contains the Diameter supported authorization application ID.

AVP Header
258 0

Vendor ID
0

VSA Type
258

AVP Type
UINT32

Group Value
N/A

AVP Flag
N

Auth-Grace-Period

Auth-Grace-Period.

AVP Header
276 0

Vendor ID
0

VSA Type
276

AVP Type
UINT32

Group Value
N/A

AVP Flag
N

Authentication-Info

Authentication information.

AVP Header
6016 10415

Vendor ID
10415

VSA Type
6016

AVP Type
GROUPED

Group Value
[EPS_VECTOR]

[UMTS_VECTOR]

[GERAN_VECTOR]

AVP Flag
M

Authorised-QoS

This AVP holds the authorized QoS.

AVP Header
849 0

Vendor ID
0

VSA Type
849

AVP Type
UTF8STRING

Group Value
N/A

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.

AVP Header
291 0

Vendor ID
0

VSA Type
291

AVP Type
UINT32

Group Value
N/A

AVP Flag
N

Authorization-Token

This AVP contains the authorization token defined in RFC 3520.

AVP Header
506 10415

Vendor ID
10415

VSA Type
506

AVP Type
OCTETSTRING

Group Value
N/A

AVP Flag
M

Authorized-QoS

Used to carry the authorized QoS from the E-PDF to the IPC/GGSN.

AVP Header
1016 10415

Vendor ID
10415

VSA Type
1016

AVP Type
Grouped

Group Value
[QoS-Class]

[Max-Requested-Bandwidth-UL]

[Max-Requested-Bandwidth-DL]

AVP Flag
M

Auth-Profile-Id-Bi-Direction

3GPP2 Auth profile ID bi-direction.

AVP Header
6081 5535

Vendor ID
5535

VSA Type
6081

AVP Type
UINT32

Group Value
N/A

AVP Flag
M

Auth-Profile-Id-Forward

3GPP2 Auth profile ID forward.

AVP Header
6079 5535

Vendor ID
5535

VSA Type
6079

AVP Type
UINT32

Group Value
N/A

AVP Flag
M

Auth-Profile-Id-Reverse

3GPP2 Auth profile ID reverse.

AVP Header
6080 5535

Vendor ID
5535

VSA Type
6080

AVP Type
UINT32

Group Value
N/A

AVP Flag
M

Auth-Request-Type

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

AVP Header
274 0

Vendor ID
0

VSA Type
274

AVP Type
ENUM. Supported values are:

AUTHENTICATE_ONLY (1)

AUTHORIZE_ONLY (2)

AUTHORIZE_AUTHENTICATE (3)

Group Value
N/A

AVP Flag
M

Auth-Session-State

Specifies whether state is maintained for a particular session.

AVP Header
277 0

Vendor ID
0

VSA Type
277

AVP Type
ENUM. Supported values are:

STATE_MAINTAINED (0)

NO_STATE_MAINTAINED (1)

Group Value
N/A

AVP Flag
M

AUTN

This AVP contains the AUTN.

AVP Header
1449 10415

Vendor ID
10415

VSA Type
1449

AVP Type
OCTETSTRING

Group Value
N/A

AVP Flag
M

Base-Time-Interval

This AVP contains the length of the base time interval for controlling the consumption of time quota, in seconds.

AVP Header
1265 10415

Vendor ID
10415

VSA Type
1265

AVP Type
UINT32

Group Value
N/A

AVP Flag
M

BCID

This AVP holds 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.

AVP Header
200 4491

Vendor ID
4491

VSA Type
200

AVP Type

UTF8STRING

Group Value
N/A

AVP Flag
M

Bearer-Control-Mode

This AVP indicates the preferred bearer control mode.

AVP Header
1023 10415

Vendor ID
10415

VSA Type
1023

AVP Type
ENUM. Supported values are:

UE_ONLY (0)

RESERVED (1)

UE_NW (2)

Group Value
N/A

AVP Flag
M

Bearer-Identifier

This AVP indicates the bearer to which the information belongs.

AVP Header
1020 10415

Vendor ID
10415

VSA Type
1020

AVP Type
OCTETSTRING

Group Value
N/A

AVP Flag
M

Bearer-Operation

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

AVP Header
1021 10415

Vendor ID
10415

VSA Type
1021

AVP Type
ENUM. Supported values are:

TERMINATION (0)

ESTABLISHMENT (1)

MODIFICATION (2)

Group Value
N/A

AVP Flag
M

Bearer-Service

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

AVP Header
854 10415

Vendor ID
10415

VSA Type
854

AVP Type
OCTETSTRING

Group Value
N/A

AVP Flag
M

Bearer-Usage

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

AVP Header
1000 10415

Vendor ID
10415

VSA Type
1000

AVP Type
ENUM. Supported values are:

GENERAL (0)

IMS_SIGNALLING (1)

DEDICATED (2) - This is specific to customer.

Group Value
N/A

AVP Flag
M

Binding-Information

Used to convey binding information required for NA(P)T, hosted NA(P)T, and NA(P)T-PT control.

AVP Header
450 13019

Vendor ID
13019

VSA Type
450

AVP Type
GROUPED

Group Value
[BINDING_INPUT_LIST]

[BINDING_OUTPUT_LIST]

AVP Flag
N/A

Binding-Input-List

Contains a list of transport addresses for which a binding is requested.

AVP Header
451 13019

Vendor ID
13019

VSA Type
451

AVP Type
GROUPED

Group Value
[V6_TRANSPORT_ADDRESS]

[V4_TRANSPORT_ADDRESS]

AVP Flag
N/A

Binding-Output-List

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

AVP Header
452 13019

Vendor ID
13019

VSA Type
452

AVP Type
GROUPED

Group Value
[V6_TRANSPORT_ADDRESS]

[V4_TRANSPORT_ADDRESS]

AVP Flag
N/A

BM-Correlation-ID

Indicates unique correlation identifier for entire MIP session.

AVP Header
527 10415

Vendor ID
10415

VSA Type
527

AVP Type
UTF8STRING

Group Value
N/A

AVP Flag
M

BM-Type

Indicates home and visited Bearer Manager in current service flow.

AVP Header

1454 10415

Vendor ID
10415

VSA Type
1454

AVP Type
ENUM. Supported values are:

HBM (0)

VBM (1)

Group Value
N/A

AVP Flag
M

BSID

AVP Header
10003 0

Vendor ID
0

VSA Type
10003

AVP Type
OCTETSTRING

Group Value
N/A

AVP Flag
M

Callback-Id

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

AVP Header
20 0

Vendor ID
0

VSA Type
20

AVP Type
UTF8STRING

Group Value
N/A

AVP Flag
M

Callback-Number

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

AVP Header
19 0

Vendor ID
0

VSA Type
19

AVP Type
UTF8STRING

Group Value
N/A

AVP Flag
M

Call-Barring-Info-List

Call barring list.

AVP Header
1488 10415

Vendor ID
10415

VSA Type
1488

AVP Type
GROUPED

Group Value
[SS_CODE]

AVP Flag
M

Called-Asserted-Identity

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

AVP Header
1250 10415

Vendor ID
10415

VSA Type
1250

AVP Type
UTF8STRING

Group Value
N/A

AVP Flag
M

Called-Party-Address

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

AVP Header
832 0

Vendor ID
0

VSA Type
832

AVP Type
UTF8STRING

Group Value
N/A

AVP Flag
M

Called-Station-Id

Describing the layer 2 addresses the user contacted in the request.

AVP Header
30 0

Vendor ID
0

VSA Type
30

AVP Type
OCTETSTRING

Group Value
N/A

AVP Flag
M

Calling-Party-Address

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

AVP Header
831 10415

Vendor ID
10415

VSA Type
831

AVP Type
UTF8STRING

Group Value
N/A

AVP Flag
M

Calling-Station-Id

Allows the NAS to send the ASCII string describing the layer 2 address from which the user connected in the request.

AVP Header
31 0

Vendor ID
0

VSA Type
31

AVP Type
UTF8STRING

Group Value
N/A

AVP Flag
N/A

Cancellation-Type

Indicates the type of cancellation.

AVP Header
1420 10415

Vendor ID
10415

VSA Type
1420

AVP Type
ENUM. Supported values are:

MME_UPDATE_PROCEDURE (0)

SGSN_UPDATE_PROCEDURE (1)

SUBSCRIPTION_WITHDRAWAL (2)

UPDATE_PROCEDURE_IWF (3)

Group Value
N/A

AVP Flag
M

Cause-Code

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

AVP Header
861 0

Vendor ID
0

VSA Type
861

AVP Type
INT32

Group Value
N/A

AVP Flag
M

CC-Correlation-Id

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

AVP Header
411 0

Vendor ID
0

VSA Type
411

AVP Type
OCTETSTRING

Group Value
N/A

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.

AVP Header
412 0

Vendor ID
0

VSA Type
412

AVP Type
UINT64

Group Value
N/A

AVP Flag
M

CC-Money

Monetary amount in the given currency.

AVP Header
413 0

Vendor ID
0

VSA Type
413

AVP Type
Grouped

Group Value
N/A

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.

AVP Header
414 0

Vendor ID
0

VSA Type
414

AVP Type
UINT64

Group Value
N/A

AVP Flag
M

CC-Request-Number

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

AVP Header
415 0

Vendor ID
0

VSA Type
415

AVP Type
UINT32

Group Value
N/A

AVP Flag
M

CC-Request-Type

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

AVP Header
416 0

Vendor ID
0

VSA Type
416

AVP Type
ENUM. Supported values are:

INITIAL_REQUEST (1)

UPDATE_REQUEST (2)

TERMINATION_REQUEST (3)

EVENT_REQUEST (4)

Group Value
N/A

AVP Flag
M

CC-Service-Specific-Units

This AVP specifies the number of service-specific units (e.g. number of events, points) given in a selected service.

AVP Header
417 0

Vendor ID
0

VSA Type
417

AVP Type
UINT64

Group Value
N/A

AVP Flag
M

CC-Session-Failover

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

AVP Header
418 0

Vendor ID
0

VSA Type
418

AVP Type
ENUM. Supported values are:

FAILOVER_NOT_SUPPORTED (0)

FAILOVER_SUPPORTED (1)

Group Value
N/A

AVP Flag
M

CC-Sub-Session-Id

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

AVP Header
419 0

Vendor ID
0

VSA Type
419

AVP Type
UINT64

Group Value
N/A

AVP Flag
M

CC-Time

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

AVP Header
420 0

Vendor ID
0

VSA Type
420

AVP Type
UINT32

Group Value
N/A

AVP Flag
M

CC-Total-Octets

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

AVP Header
421 0

Vendor ID
0

VSA Type
421

AVP Type
UINT64

Group Value
N/A

AVP Flag
M

CC-Unit-Type

This AVP indicates the type of units.

AVP Header
454 0

Vendor ID
0

VSA Type
454

AVP Type
ENUM. Supported values are:

TIME (0)

MONEY(1)

TOTAL-OCTETS (2)

INPUT-OCTETS (3)

OUTPUT-OCTETS (4)

SERVICE-SPECIFIC-UNITS(5)

Group Value
N/A

AVP Flag
M

CG-Address

This AVP holds the IP-address of the charging gateway.

AVP Header
846 10415

Vendor ID
10415

VSA Type
846

AVP Type
ADDRESS

Group Value
N/A

AVP Flag
M

Change-Condition

Change condition.

AVP Header
2037 10415

Vendor ID
10415

VSA Type
2037

AVP Type
ENUM. Supported values are:

NORMAL_RELEASE (0)

ABNORMAL_RELEASE(1)

QOS_CHANGE(2)

VOLUME_LIMIT(3)

TIME_LIMIT(4)

SERVING_NODE_CHANGE(5)

SERVING_NODE_PLMN_CHANGE(6)

USER_LOCATION_CHANGE(7)

RAT_CHANGE(8)

UE_TIME_ZONE_CHANGE(9)

TARIFF_TIME_CHANGE(10)

SERVICE_IDLED_OUT(11)

SERVICE_SPECIFIC_UNIT_LIMIT(12)

MAX_NUMBER_OF_CHARGING_CONDITIONS(13)

MANAGEMENT_INTERVENTION(14)

Group Value
N/A

AVP Flag
M

Change-Time

Change-Time.

AVP Header
2038 10415

Vendor ID
10415

VSA Type
2038

AVP Type
TIME

Group Value
N/A

AVP Flag
M

Chargeable-User-Id

MN-NAI identfying the user in EPS network.

AVP Header
89 0

Vendor ID
0

VSA Type
89

AVP Type
OCTETSTRING

Group Value
N/A

AVP Flag
M

Charging-Information

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

AVP Header
618 10415

Vendor ID
10415

VSA Type
618

AVP Type
Grouped

Group Value
[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

Indicates the name of a pre defined group of charging rules residing at the TPF.

AVP Header

1004 10415

Vendor ID
10415

VSA Type
1004

AVP Type
UTF8STRING

Group Value
N/A

AVP Flag
M

Charging-Rule-Definition

Defines the charging rule for a service flow sent by the CRF to the TPF.

AVP Header
1003 10415

Vendor ID
10415

VSA Type
1003

AVP Type
Grouped

Group Value
[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.

AVP Header
1001 10415

Vendor ID
10415

VSA Type
1001

AVP Type
Grouped

Group Value
[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

Specifies the charging rule name provided by the CRF. It uniquely identifies a charging rule for a bearer.

AVP Header
1005 10415

Vendor ID
10415

VSA Type
1005

AVP Type
OCTETSTRING

Group Value
N/A

AVP Flag
M

Charging-Rule-Name-LI

Charging rule name for LI-Indicator-Gx.

AVP Header
1005 10415

Vendor ID
10415

VSA Type
1005

AVP Type
OCTETSTRING

Group Value
N/A

AVP Flag
M

Charging-Rule-Remove

Specifies 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.

AVP Header
1002 10415

Vendor ID
10415

VSA Type
1002

AVP Type
GROUPED

Group Value
[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.

AVP Header

1018 5535

Vendor ID
5535

VSA Type
1018

AVP Type
Grouped

Group Value
[CHARGING_RULE_NAME]

[CHARGING_RULE_BASE_NAME]

[PCC_RULE_STATUS]

[RULE_FAILURE_CODE]

[FINAL_UNIT_INDICATION]

AVP Flag
M

Check-Balance-Result

Result of the balance check. Applicable only when requested-Action AVP indicates CHECK_BALANCE.

AVP Header
422 0

Vendor ID
0

VSA Type
422

AVP Type
ENUM. Supported values are:

ENOUGH_CREDIT (0)

NO_CREDIT (1)

Group Value
N/A

AVP Flag
M

Civic-Location

Civic-Location.

AVP Header
355 13019

Vendor ID
13019

VSA Type
355

AVP Type
OCTETSTRING

Group Value
N/A

AVP Flag
M

Class

Used by Diameter servers to return state information to the access device.

AVP Header
25 0

Vendor ID
0

VSA Type
25

AVP Type
OCTETSTRING

Group Value
N/A

AVP Flag
M

Client-Identity

Client identity.

AVP Header
1480 10415

Vendor ID
10415

VSA Type
1480

AVP Type
OCTETSTRING

Group Value
N/A

AVP Flag
M

CoA-Information

CoA Information.

AVP Header
1039 10415

Vendor ID
10415

VSA Type
1039

AVP Type
GROUPED

Group Value
[TUNNEL_INFORMATION]

[COA_IP_ADDRESS]

AVP Flag
M

CoA-IP-Address

Care of IP address for DSMIP6 access.

AVP Header
1035 10415

Vendor ID
10415

VSA Type
1035

AVP Type
ADDRESS

Group Value
N/A

AVP Flag
M

Codec-Data

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

AVP Header
524 10415

Vendor ID
10415

VSA Type
524

AVP Type
OCTETSTRING

Group Value
N/A

AVP Flag
M

Complete-Data-List-Included-Indicator

Complete Data List Included indicator.

AVP Header
1468 10415

Vendor ID
10415

VSA Type
1468

AVP Type
ENUM. Supported values are:

ALL_PDP_CONTEXTS_INCLUDED (0)

MODIFIED_ADDED_PDP_CONTEXTS_INCLUDED (1)

Group Value
N/A

AVP Flag
M

Confidentiality-Key

This AVP contains the Confidentiality Key (CK).

AVP Header
625 10415

Vendor ID
10415

VSA Type
625

AVP Type
OCTETSTRING

Group Value
N/A

AVP Flag
M

Configuration-Token

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.

AVP Header
78 0

Vendor ID
0

VSA Type
78

AVP Type
OCTETSTRING

Group Value
N/A

AVP Flag
N/A

Connect-Info

Sent in the AA-Request message or ACR STOP message.

AVP Header
77 0

Vendor ID
0

VSA Type
77

AVP Type
UTF8STRING

Group Value
N/A

AVP Flag
M

Content-Disposition

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

AVP Header
828 10415

Vendor ID
10415

VSA Type
828

AVP Type

UTF8STRING

Group Value
N/A

AVP Flag
M

Content-Length

This AVP holds the size of the message body.

AVP Header
827 10415

Vendor ID
10415

VSA Type
827

AVP Type
UINT32

Group Value
N/A

AVP Flag
M

Content-Type

This AVP holds the media type (e.g. application/sdp, text/html) of the message-body.

AVP Header
826 10415

Vendor ID
10415

VSA Type
826

AVP Type
UTF8STRING

Group Value
N/A

AVP Flag
M

Context-Identifier

Context identifier.

AVP Header

1423 10415

Vendor ID
10415

VSA Type
1423

AVP Type
UINT32

Group Value
N/A

AVP Flag
M

Correlate-Reason

Indicates the reason that the Correlate message was sent.

AVP Header
202 4491

Vendor ID
4491

VSA Type
202

AVP Type
ENUM. Supported values are:

UNKNOWN (0)

B2BUA (1)

INITIAL_SIP_MESSAGE (2) — Initial SIP Message sent by target's S-CSCF

ADDITIONAL_TARGET_ENCOUNTERED (3)

HAND_OFF_OCCURED (4)

ORIGINATION_FROM_APP_SERVER (5) — Origination from an Application Server as a result of a termination on that Application Server.

BCID (6) — BCID received in the P-DCS-LAES header.

Group Value
N/A

AVP Flag
M

Cost-Information

Cost information of service transferred by the credit-control client to the end user.

AVP Header
423 0

Vendor ID
0

VSA Type
423

AVP Type
Grouped

Group Value
[Unit-Value]

[Currency-Code]

[Cost-Unit]

AVP Flag
M

Cost-Unit

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

AVP Header
424 0

Vendor ID
0

VSA Type
424

AVP Type
UTF8STRING

Group Value
N/A

AVP Flag
M

CSG-Id

CSG ID.

AVP Header
1437 10415

Vendor ID
10415

VSA Type
1437

AVP Type
UINT32

Group Value
N/A

AVP Flag
M

CSG-Subscription-Data

CSG subscription data.

AVP Header
1436 10415

Vendor ID
10415

VSA Type
1436

AVP Type
GROUPED

Group Value
[CSG_ID]

[EXPIRATION_DATE]

AVP Flag
M

Credit-Control

Included in AA requests when the service element has credit-control application.

AVP Header
426 0

Vendor ID
0

VSA Type
426

AVP Type
ENUM. Supported values are:

CREDIT_AUTHORIZATION (0)

RE_AUTHORIZATION (1)

Group Value
N/A

AVP Flag
M

Credit-Control-Failure-Handling

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

AVP Header

427 0

Vendor ID
0

VSA Type
427

AVP Type
ENUM. Supported values are:

TERMINATE (0)

CONTINUE (1)

RETRY_AND_TERMINATE (2)

Group Value
N/A

AVP Flag
M

CT-Time-Quota-Threshold

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

AVP Header
868 10415

Vendor ID
10415

VSA Type
868

AVP Type
UINT64

Group Value
N/A

AVP Flag
M

CT-Volume-Quota-Threshold

This AVP contains a threshold value in octets. This is customer-specific AVP.

AVP Header
869 10415

Vendor ID
10415

VSA Type
869

AVP Type
UINT64

Group Value
N/A

AVP Flag
M

Currency-Code

Currency in which the values of AVPs containing monetary units were given.

AVP Header
425 0

Vendor ID
0

VSA Type
425

AVP Type
UINT32

Group Value
N/A

AVP Flag
M

Current-Location

Indicates whether an active location retrieval has to be initiated or not.

AVP Header
707 0

Vendor ID
0

VSA Type
707

AVP Type
ENUM

Group Value
N/A

AVP Flag
M

Customer-Id

Customer ID; used in header enrichment scenarios.

AVP Header
1146 8164

Vendor ID
8164

VSA Type
1146

AVP Type
UTF8STRING

Group Value
N/A

AVP Flag
M

Data-Reference

Indicates the type of the requested used data in the operation UDR and SNR.

AVP Header
703 0

Vendor ID
0

VSA Type
703

AVP Type
ENUM

Group Value
N/A

AVP Flag
M

Default-EPS-Bearer-QoS

Defines the QoS information for the EPS default bearer.

AVP Header
1049 10415

Vendor ID
10415

VSA Type
1049

AVP Type
GROUPED

Group Value
[QOS_CLASS_IDENTIFIER]

[ALLOCATION_RETENTION_PRIORITY]

AVP Flag
M

Deregistration-Reason

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

AVP Header
615 10415

Vendor ID
10415

VSA Type
615

AVP Type
GROUPED

Group Value
[REASON_CODE]

[REASON_INFO]

AVP Flag
M

Destination-Host

The destination endpoint of the message. This attribute is present in all request messages.

AVP Header
293 0

Vendor ID
0

VSA Type
293

AVP Type
DIAMIDENT

Group Value
N/A

AVP Flag
M

Destination-Realm

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

AVP Header
283 0

Vendor ID
0

VSA Type
283

AVP Type
DIAMIDENT

Group Value
N/A

AVP Flag
M

Diagnostics

Diagnostics

AVP Header
2039 10415

Vendor ID
10415

VSA Type
2039

AVP Type
ENUM. Supported values are:

UNSPECIFIED (0)

SESSION_TIMEOUT (1)

RESOURCE_LIMITATION (2)

ADMIN_DISCONNECT (3)

IDLE_TIMEOUT (4)

PCRF_UNREACHABLE (5)

AAA_UNREACHABLE (6)

AAA_INITIATED_SESSION_TERMINATION (7)

REAUTHENTICATION_FAILED (8)

PCRF_INITIATED_SESSION_TERMINATION (9)

PCRF_INITIATED_FLOW_TERMINATION (10)

PCRF_ACCOUNTING_PARAMETERS_CHANGED (11)

PMIP_INITIATED_SESSION_TERMINATION (12)

PPP_INITIATED_SESSION_TERMINATION (13)

GTP_INITIATED_SESSION_TERMINATION (14)

PMIP_REVOCATION (15)

HANDOVER_ERROR (16)

PMIP_LIFETIME_EXPIRED (17)

Group Value
N/A

AVP Flag
M

Dialog-Id

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.

AVP Header
203 4491

Vendor ID
4491

VSA Type
203

AVP Type
UTF8STRING

Group Value
N/A

AVP Flag
M

Digest-Algorithm

Holds the algorithm parameter that influences the HTTP Digest calculation.

AVP Header
111 0

Vendor ID
0

VSA Type
111

AVP Type
OCTETSTRING

Group Value
N/A

AVP Flag
M

Digest-Auth-Param

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

AVP Header
117 0

Vendor ID
0

VSA Type

117

AVP Type
OCTETSTRING

Group Value
N/A

AVP Flag
M

Digest-Domain

Consists of a single URI that defines a protection space component.

AVP Header
119 0

Vendor ID
0

VSA Type
119

AVP Type
OCTETSTRING

Group Value
N/A

AVP Flag
M

Digest-HA1

Contains the hexadecimal representation of H(A1) as described in [RFC2617].

AVP Header
121 0

Vendor ID
0

VSA Type
121

AVP Type
OCTETSTRING

Group Value
N/A

AVP Flag
M

Digest-QoP

Holds the Quality of Protection parameter that influences the HTTP Digest calculation.

AVP Header
110 0

Vendor ID
0

VSA Type
110

AVP Type
OCTETSTRING

Group Value
N/A

AVP Flag
M

Digest-Realm

Describes a protection space component of the RADIUS server.

AVP Header
104 0

Vendor ID
0

VSA Type
104

AVP Type
OCTETSTRING

Group Value
N/A

AVP Flag
M

DIR

AVP Header
11000 0

Vendor ID
0

VSA Type
11000

AVP Type
OCTETSTRING

Group Value

N/A

AVP Flag
M

Direct-Debiting-Failure-Handling

Specifies the action to handle the failure of request message to the credit control server with DIRECT_DEBITING attribute.

AVP Header
428 0

Vendor ID
0

VSA Type
428

AVP Type
ENUM. Supported values are:

TERMINATE_OR_BUFFER (0)

CONTINUE (1)

Group Value
N/A

AVP Flag
M

Direction

Indicates whether the reported message was sent “to" or "from" the intercept target.

AVP Header
210 4491

Vendor ID
4491

VSA Type
210

AVP Type
ENUM. Supported values are:

UNDEFINED (0)

TO_TARGET (1)

FROM_TARGET (2)

Group Value
N/A

AVP Flag
M

Direct-Message

Indicates if the reported message is exchanged directly between the IAP and the intercept target.

AVP Header
211 4491

Vendor ID
4491

VSA Type
211

AVP Type
ENUM. Supported values are:

FALSE (0)

TRUE (1)

Group Value
N/A

AVP Flag
M

Disconnect-Cause

Specifies the reason or cause of disconnection with peer.

AVP Header
273 0

Vendor ID
0

VSA Type
273

AVP Type
ENUM. Supported values are:

REBOOTING (0)

BUSY (1)

DO_NOT_WANT_TO_TALK_TO_YOU (2)

Group Value
N/A

AVP Flag
N/A

DSA-Flags

This AVP contains a bit mask.

AVP Header
1422 10415

Vendor ID
10415

VSA Type
1422

AVP Type
UINT32

Group Value
N/A

AVP Flag
M

DSR-Flags

This AVP contains a bit mask.

AVP Header
1421 10415

Vendor ID
10415

VSA Type
1421

AVP Type
UINT32

Group Value
N/A

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.

AVP Header
2051 10415

Vendor ID
10415

VSA Type
2051

AVP Type
ENUM. Supported values are:

STATIC (0)

DYNAMIC (1)

Group Value
N/A

AVP Flag
M

EAP-Key-Name

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

AVP Header
102 0

Vendor ID
0

VSA Type
102

AVP Type
OCTETSTRING

Group Value
N/A

AVP Flag
M

EAP-Master-Session-Key

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

AVP Header
464 0

Vendor ID
0

VSA Type
464

AVP Type
OCTETSTRING

Group Value
N/A

AVP Flag
N/A

EAP-Payload

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

AVP Header
462 0

Vendor ID
0

VSA Type
462

AVP Type
OCTETSTRING

Group Value
N/A

AVP Flag
M

EAP-Reissued-Payload

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

AVP Header
463 0

Vendor ID
0

VSA Type
463

AVP Type
OCTETSTRING

Group Value
N/A

AVP Flag
M

Early-Media-Description

This grouped AVP describes 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.

AVP Header
1272 10415

Vendor ID
10415

VSA Type
1272

AVP Type
GROUPED

Group Value
[SDP_TIMESTAMPS]

[SDP_MEDIA_COMPONENT]

[SDP_SESSION_DESCRIPTION]

AVP Flag

M

Element-ID

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

AVP Header
212 4491

Vendor ID
4491

VSA Type
212

AVP Type
UTF8STRING

Group Value
N/A

AVP Flag
M

Element-Type

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

AVP Header
213 4491

Vendor ID
4491

VSA Type
213

AVP Type
ENUM. Supported values are:

S_CSCF (0)

P_CSCF (1)

I_CSCF(2)

MRFC (3)

MGCF (4)

BGCF (5)

AS (6)

UE (7)

Group Value
N/A

AVP Flag
M

Envelope

Reports the start and end time of one time envelope using the **AttributeEnvelope-Start-Time** and **AttributeEnvelope-End-Time** AVPs.

AVP Header
1266 10415

Vendor ID
10415

VSA Type
1266

AVP Type
GROUPED

Group Value
[ENVELOPE_START_TIME]

[ENVELOPE_END_TIME]

[CC_TOTAL_OCTETS]

[CC_INPUT_OCTETS]

[CC_OUTPUT_OCTETS]

[CC_SERVICE_SPECIFIC_UNITS]

AVP Flag
M

Envelope-End-Time

Time of the end of the time envelope.

AVP Header
1267 10415

Vendor ID
10415

VSA Type
1267

AVP Type
TIME

Group Value
N/A

AVP Flag
M

Envelope-Reporting

Indicate whether the CLCI-C shall report the start and end of each time envelope, in those cases in which quota is consumed in envelopes.

AVP Header
1268 10415

Vendor ID
10415

VSA Type
1268

AVP Type
ENUM

Group Value
N/A

AVP Flag
M

Envelope-Start-Time

Time of the packet of user data which caused the time envelope to start.

AVP Header
1269 10415

Vendor ID
10415

VSA Type
1269

AVP Type
TIME

Group Value
N/A

AVP Flag
M

EPS-Information

EPS information.

AVP Header
1041 10415

Vendor ID
10415

VSA Type
1041

AVP Type
GROUPED

Group Value
[AF_CORRELATION_INFORMATION]

[SGW_ADDRESS]

[PGW_ADDRESS]
[HSGW_ADDRESS]
[3GPP_CF_IPV6_ADDRESS]
[PGW_MCC_MNC]
[EPS_CAUSE_CODE]
[NODE_FUNCTIONALITY]
[CALLED_STATION_ID]
[ACCOUNTING_INPUT_OCTETS]
[ACCOUNTING_OUTPUT_OCTETS]
[ACCOUNTING_INPUT_PACKETS]
[ACCOUNTING_OUTPUT_PACKETS]
[START_TIME]
[STOP_TIME]
[ACCT_SESSION_TIME]
[OPERATOR_STRING]
[ACCESS_NETWORK_CHARGING_IDENTIFIER_VALUE]
[FIRST_PACKET_DIRECTION]
[PSCID]
[FID]
[CHARGING_RULE_BASE_NAME]
[CHARGING_RULE_NAME]
[FLOW_DESCRIPTION]
[QOS_INFORMATION]
[PMIP_MOBILE_NODE_ADDRESS]
[3GPP2_BSID]
[USER_EQUIPMENT_INFO]

AVP Flag
M

EPS-Subscribed-QoS-Profile

EPS subscribed QoS profile.

AVP Header
1431 10415

Vendor ID
10415

VSA Type
1431

AVP Type
GROUPED

Group Value
[QOS_CLASS_IDENTIFIER]

[ARP]

[AMBR]

AVP Flag
M

EPS-Vector

EPS Vector.

AVP Header
6017 10415

Vendor ID
10415

VSA Type
6017

AVP Type
GROUPED

Group Value
[ITEM_NUMBER]

[RAND]

[XRES]

[AUTN]

[KASME]

AVP Flag
M

Equipment-Status

Equipment status.

AVP Header
1445 10415

Vendor ID
10415

VSA Type
1445

AVP Type
ENUM. Supported values are:

WHITELISTED (0)

BLACKLISTED (1)

GREYLISTED (2)

Group Value
N/A

AVP Flag
M

ESN

ESN.

AVP Header
6109 10415

Vendor ID
10415

VSA Type
6109

AVP Type
OCTETSTRING

Group Value
N/A

AVP Flag
M

Error-Message

Human Readable Error Message.

AVP Header
281 0

Vendor ID
0

VSA Type
281

AVP Type
UTF8STRING

Group Value
N/A

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.

AVP Header
294 0

Vendor ID
0

VSA Type
294

AVP Type
DIAMIDENT

Group Value
N/A

AVP Flag
M

EUTRAN-Vector

EUTRAN Vector.

AVP Header
1414 10415

Vendor ID
10415

VSA Type
1414

AVP Type
GROUPED

Group Value
[ITEM_NUMBER]

[RAND]

[XRES]

[AUTN]

[KASME]

AVP Flag
M

Event

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

AVP Header
825 10415

Vendor ID
10415

VSA Type
825

AVP Type
UTF8STRING

Group Value
N/A

AVP Flag
M

Event-Message-Type

Identifies the type of surveillance message.

AVP Header
214 4491

Vendor ID
4491

VSA Type
214

AVP Type
ENUM. Supported values are:

REPORT (0)

CORRELATE (1)

CARRIER_INFO (2)

Group Value
N/A

AVP Flag
M

Event-Report-Indication

Event Report Indication.

AVP Header
1033 10415

Vendor ID
10415

VSA Type
1033

AVP Type
GROUPED

Group Value
[EVENT_TRIGGER]

[RAT_TYPE]

AVP Flag
M

Event-Timestamp

Records the time the event was reported.

AVP Header
55 0

Vendor ID
0

VSA Type
55

AVP Type
TIME

Group Value
N/A

AVP Flag
M

Event-Trigger

Indicates an event that shall cause a re-request of charging rules.

AVP Header
1006 10415

Vendor ID
10415

VSA Type
1006

AVP Type
ENUM. Supported values are:

SGSN_CHANGE (0)

QOS_CHANGE (1)

RAT_CHANGE (2)

TFT_CHANGE (3)

PLMN_CHANGE (4)

LOSS_OF_FLOW (5)

RECOVERY_OF_FLOW (6)

IP_CAN_CHANGE (7)

GW_PCEF_MALFUNCTION (8) — obsolete; must not be used

RESOURCES_LIMITATION (9) — obsolete; must not be used

MAX_NR_BEARERS_REACHED (10) — obsolete; must not be used

QOS_CHANGE_EXCEEDING_AUTHORIZATION (11)

RAI_CHANGE (12)

USER_LOCATION_CHANGE (13)

NO_EVENT_TRIGGERS (14)

OUT_OF_CREDIT (15)

REALLOCATION_OF_CREDIT (16)

REVALIDATION_TIMEOUT (17)

UE_IP_ADDRESS_ALLOCATE (18)

UE_IP_ADDRESS_RELEASE (19)

DEFAULT_EPS_BEARER_QOS_CHANGE (20)

AN_GW_CHANGE (21)

SUCCESSFUL_RESOURCE_ALLOCATION (22)

RESOURCE_MODIFICATION_REQUEST (23)

PGW_TRACE_CONTROL (24)

UE_TIME_ZONE_CHANGE (25)

USAGE_THRESHOLD_REACHED (33)

SERVICE_FLOW_DETECTION (34)

PRESERVATION_CHANGED (2000)

REACTIVATION_CHANGED (2001)

TFT_DELETED (1000)

LOSS_OF_BEARER (1001)

RECOVERY_OF_BEARER (1002)

POLICY_ENFORCEMENT_FAILED (1003)

Group Value
N/A

AVP Flag
M

Event-Type

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

AVP Header
823 10415

Vendor ID
10415

VSA Type
823

AVP Type
GROUPED

Group Value
[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.

AVP Header
297 0

Vendor ID
0

VSA Type
297

AVP Type
GROUPED

Group Value
[VENDOR_ID]

[EXPERIMENTAL_RESULT_CODE]

AVP Flag
M

Experimental-Result-Code

SUCCESS or FAILURE.

AVP Header
298 0

Vendor ID
0

VSA Type
298

AVP Type
ENUM. Supported values are:

DIAMETER_MULTI_ROUND_AUTH (1001)

DIAMETER_SUCCESS (2001)

DIAMETER_LIMITED_SUCCESS (2002)

DIAMETER_PDP_CONTEXT_DELETION_INDICATION (2021)

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)

INSUFFICIENT-RESOURCES (4041)

COMMIT-FAILURE (4043)

REFRESH-FAILURE (4044)

QOS-PROFILE-FAILURE (4045)

ACCESS-PROFILE-FAILURE (4046)

PRIORITY-NOT-GRANTED (4047)

DIAMETER_ERROR_OUT_OF_RESOURCES (4121)

DIAMETER_PCC_BEARER_EVENT (4141)

AUTHENTICATION_DATA_UNAVAILABLE (4181)

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)

BINDING-FAILURE (5021)

DIAMETER_USER_UNKNOWN (5030)

DIAMETER_RATING_FAILED (5031)

MODIFICATION-FAILURE (5041)

INVALID_SERVICE_INFORMATION (5061)

FILTER_RESTRICTIONS (5062)

REQUESTED_SERVICE_NOT_AUTHORIZED (5063)

DUPLICATED_AF_SESSION (5064)

IP_CAN_SESSION_NOT_AVAILABLE (5065)

DIAMETER_ERROR_START_INDICATION (5120)

DIAMETER_ERROR_STOP_INDICATION (5121)

DIAMETER_ERROR_UNKNOWN_MBMS_BEARER_SERVICE (5122)

DIAMETER_ERROR_SERVICE_AREA (5123)

DIAMETER_ERROR_INITIAL_PARAMETERS (5140)

DIAMETER_ERROR_TRIGGER_EVENT (5141)

DIAMETER_PCC_RULE_EVENT (5142)

DIAMETER_ERROR_BEARER_NOT_AUTHORIZED (5143)

DIAMETER_ERROR_TRAFFIC_MAPPING_INFO_REJECTED (5144)

DIAMETER_QOS_RULE_EVENT (5145)

DIAMETER_BEARER_EVENT (5146)

DIAMETER_ERROR_CONFLICTING_REQUEST (5147)

ERROR_UNKNOWN_EPS_SUBSCRIPTION (5420)

ERROR_RAT_NOT_ALLOWED (5421)

ERROR_ROAMING_NOT_ALLOWED (5402)

ERROR_EQUIPMENT_UNKNOWN (5422)

Group Value

N/A

AVP Flag

M

Expiration-Date

Expiration date.

AVP Header

1439 10415

Vendor ID

10415

VSA Type
1439

AVP Type
TIME

Group Value
N/A

AVP Flag
M

Expires

Expires.

AVP Header
888 10415

Vendor ID
10415

VSA Type
888

AVP Type
UINT32

Group Value
N/A

AVP Flag
M

Exponent

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

AVP Header
429 0

Vendor ID
0

VSA Type
429

AVP Type
INT32

Group Value
N/A

AVP Flag
M

Extended-QoS-Filter-Rule

Extended QoS Filter Rule.

AVP Header
6066 0

Vendor ID
0

VSA Type
6066

AVP Type
INT32

Group Value
N/A

AVP Flag
M

External-Client

External Client.

AVP Header
1479 10415

Vendor ID
10415

VSA Type
1479

AVP Type
GROUPED

Group Value
[CLIENT_IDENTITY]

[GMLC_RESTRICTION]

[NOTIFICATION_TO_UE_USER]

AVP Flag
M

Failed-AVP

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

AVP Header
279 0

Vendor ID
0

VSA Type

279

AVP Type
Grouped

Group Value
N/A

AVP Flag
M

FDR-Reason

Indicates the reason for FDR cut.

AVP Header
1501 10415

Vendor ID
10415

VSA Type
1501

AVP Type
ENUM. Supported values are:

END_FLOW (0)

IPGW_HO (1)

FORCED_CLOSURE (2)

Group Value
N/A

AVP Flag
M

Feature-List

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

AVP Header
630 10415

Vendor ID
10415

VSA Type
630

AVP Type
UINT32

Group Value
N/A

AVP Flag
N/A

Feature-List-ID

This AVP contains the identity of the featured list.

AVP Header
629 10415

Vendor ID
10415

VSA Type
629

AVP Type
UINT32

Group Value
N/A

AVP Flag
N/A

Feature-List-ID-Resp

Contains the identity of the featured list.

AVP Header
629 10415

Vendor ID
10415

VSA Type
629

AVP Type
UINT32

Group Value
N/A

AVP Flag
N/A

Feature-List-Resp

Contains a bit mask indicating the supported features of an application.

AVP Header
630 10415

Vendor ID
10415

VSA Type
630

AVP Type
UINT32

Group Value
N/A

AVP Flag
N/A

FID

Flow Correlation ID.

AVP Header
7003 10415

Vendor ID
10415

VSA Type
7003

AVP Type
OCTETSTRING

Group Value
N/A

AVP Flag
M

Filter-Id

The name of the filter list for this user.

AVP Header
11 0

Vendor ID
0

VSA Type
11

AVP Type
UTF8STRING

Group Value
N/A

AVP Flag
M

Final-Unit-Action

The Final-Unit-Action AVP defines the behavior of the service element when the user's account cannot cover the cost of the service.

AVP Header
449 0

Vendor ID
0

VSA Type
449

AVP Type
ENUM. Supported values are:

TERMINATE(0)

REDIRECT(1)

RESTRICT_ACCESS (2)

Group Value
N/A

AVP Flag
M

Final-Unit-Indication

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

AVP Header
430 0

Vendor ID
0

VSA Type
430

AVP Type
Grouped

Group Value
[FINAL_UNIT_ACTION]

[RESTRICTION_FILTER_RULE]

[FILTER_ID]

[REDIRECT_SERVER]

AVP Flag
M

Firmware-Revision

Support for Vendor Specific Applications.

AVP Header
267 0

Vendor ID
0

VSA Type

267

AVP Type
UINT32

Group Value
N/A

AVP Flag
N/A

Flow-Description

Defines the service flow filter parameters for a charging rule.

AVP Header
507 10415

Vendor ID
10415

VSA Type
507

AVP Type
IPFILTERRULE

Group Value
N/A

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.

AVP Header
1022 5535

Vendor ID
5535

VSA Type
1022

AVP Type
GROUPED

Group Value
[FLOW_DESCRIPTION]

[PRECEDENCE]

AVP Flag
M

Flow-Grouping

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

AVP Header
508 10415

Vendor ID
10415

VSA Type
508

AVP Type
Grouped

Group Value
[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.

AVP Header
810 5535

Vendor ID
5535

VSA Type
810

AVP Type
OCTETSTRING

Group Value
N/A

AVP Flag
MV

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.

AVP Header
809 5535

Vendor ID
5535

VSA Type

809

AVP Type
GROUPED

Group Value
[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.

AVP Header
1058 10415

Vendor ID
10415

VSA Type
1058

AVP Type
GROUPED

Group Value
[FLOW_DESCRIPTION]

[PACKET_FILTER_IDENTIFIER]

[TOS_TRAFFIC_CLASS]

[SECURITY_PARAMETER_INDEX]

[FLOW_LABEL]

AVP Flag
M

Flow-Label

Contains the IPv6 flow label header field.

AVP Header
1057 10415

Vendor ID
10415

VSA Type
1057

AVP Type
OCTETSTRING

Group Value
N/A

AVP Flag
M

Flow-Number

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

AVP Header
509 10415

Vendor ID
10415

VSA Type
509

AVP Type
UINT32

Group Value
N/A

AVP Flag
M

Flow-Operation

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

AVP Header
800 5535

Vendor ID
5535

VSA Type
800

AVP Type
ENUM. Supported values are:

TERMINATION (0)

ESTABLISHMENT (1)

MODIFICATION (2)

Group Value
N/A

AVP Flag
M

Flows

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

AVP Header
510 10415

Vendor ID
10415

VSA Type
510

AVP Type
GROUPED

Group Value
[MEDIA_COMPONENT_NUMBER]

[FLOW_NUMBER]

AVP Flag
M

Flow-Status

Describes whether the IP flow(s) are enabled or disabled.

AVP Header
511 10415

Vendor ID
10415

VSA Type
511

AVP Type
ENUM. Supported values are:

ENABLED-UPLINK (0)

ENABLED-DOWNLINK (1)

ENABLED (2)

DISABLED (3)

REMOVED (4)

TERMINATE (5)

Group Value
N/A

AVP Flag
M

Flow-Usage

Provides information about the usage of IP Flows.

AVP Header
512 10415

Vendor ID
10415

VSA Type
512

AVP Type
ENUM

Group Value
N/A

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.

AVP Header
37 0

Vendor ID
0

VSA Type
37

AVP Type
UINT32

Group Value
N/A

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.

AVP Header
38 0

Vendor ID
0

VSA Type
38

AVP Type

UINT32

Group Value
N/A

AVP Flag
M

Framed-Appletalk-Zone

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

AVP Header
39 0

Vendor ID
0

VSA Type
39

AVP Type
OCTETSTRING

Group Value
N/A

AVP Flag
M

Framed-Compression

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

AVP Header
13 0

Vendor ID
0

VSA Type
13

AVP Type
ENUM. Supported values are:

None (0)

VJ_TCP-IP_header_compression (1)

IPX-header-compression (2)

Stac-LZS-compression (3)

Group Value
N/A

AVP Flag
M

Framed-Interface-Id

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

AVP Header
96 0

Vendor ID
0

VSA Type
96

AVP Type
UINT64

Group Value
N/A

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.

AVP Header
8 0

Vendor ID
0

VSA Type
8

AVP Type
OCTETSTRING

Group Value
N/A

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.

AVP Header
9 0

Vendor ID
0

VSA Type
9

AVP Type

OCTETSTRING

Group Value
N/A

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.

AVP Header
100 0

Vendor ID
0

VSA Type
100

AVP Type
OCTETSTRING

Group Value
N/A

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.

AVP Header
97 0

Vendor ID
0

VSA Type
97

AVP Type
OctetString

Group Value
N/A

AVP Flag
M

Framed-IPv6-Route

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

AVP Header
99 0

Vendor ID
0

VSA Type
99

AVP Type
UTF8STRING

Group Value
N/A

AVP Flag
N/A

Framed-IPX-Network

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

AVP Header
23 0

Vendor ID
0

VSA Type
23

AVP Type
UINT32

Group Value
N/A

AVP Flag
M

Framed-MTU

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

AVP Header
12 0

Vendor ID
0

VSA Type
12

AVP Type
UINT32

Group Value
N/A

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.

AVP Header
88 0

Vendor ID
0

VSA Type
88

AVP Type
OCTETSTRING

Group Value
N/A

AVP Flag
M

Framed-Protocol

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

AVP Header
7 0

Vendor ID
0

VSA Type
7

AVP Type
ENUM. Supported values are:

PPP (1)

SLIP (2)

AppleTalk-Remote-Access-Protocol_ARAP (3)

Gandalf-proprietary-SingleLink_MultiLink-protocol (4)

Xylogics-proprietary_IPX-SLIP (5)

X75-Synchronous (6)

Group Value
N/A

AVP Flag
M

Framed-Route

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

AVP Header
22 0

Vendor ID
0

VSA Type
22

AVP Type
UTF8STRING

Group Value
N/A

AVP Flag
M

Framed-Routing

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

AVP Header
10 0

Vendor ID
0

VSA Type
10

AVP Type
ENUM. Supported values are:

None (0)

Send-routing-packets (1)

Listen-for-routing-packets (2)

Send-and-Listen (3)

Group Value
N/A

AVP Flag
M

Geospatial-Location

Geospatial-Location.

AVP Header
356 13019

Vendor ID

13019

VSA Type
356

AVP Type
OCTETSTRING

Group Value
N/A

AVP Flag
M

GERAN-Vector

GERAN-Vector.

AVP Header
6019 10415

Vendor ID
10415

VSA Type
6019

AVP Type
GROUPED

Group Value
[ITEM_NUMBER]

[RAND]

[SRES]

[KC_KEY]

AVP Flag
M

GGSN-Address

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

AVP Header
847 10415

Vendor ID
10415

VSA Type
847

AVP Type
ADDRESS

Group Value

N/A

AVP Flag
M

Globally-Unique-Address

Globally-Unique-Address

AVP Header
300 13019

Vendor ID
13019

VSA Type
300

AVP Type
GROUPED

Group Value
[Framed_IP_Address]

[Address_Realm]

AVP Flag
M

GMLC-Address

GMLC address.

AVP Header
1474 10415

Vendor ID
10415

VSA Type
1474

AVP Type
OCTETSTRING

Group Value
N/A

AVP Flag
M

GMLC-Restriction

GMLC restriction.

AVP Header
1481 10415

Vendor ID
10415

VSA Type
1481

AVP Type
ENUM. Supported values are:

GMLC_LIST (0)

HOME_COUNTRY (1)

Group Value
N/A

AVP Flag
M

GPRS-Subscription-Data

GPRS-Subscription-Data.

AVP Header
1467 10415

Vendor ID
10415

VSA Type
1467

AVP Type
GROUPED

Group Value
[COMPLETE_DATA_LIST_INCLUDED_INDICATOR]

[PDP_CONTEXT]

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.

AVP Header
811 5535

Vendor ID
5535

VSA Type
811

AVP Type
Grouped

Group Value
[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.

AVP Header
431 0

Vendor ID
0

VSA Type
431

AVP Type
Grouped

Group Value
[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

G-S-U-Pool-Identifier

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

AVP Header
453 0

Vendor ID
0

VSA Type
453

AVP Type

UINT32

Group Value
N/A

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.

AVP Header
457 0

Vendor ID
0

VSA Type
457

AVP Type
GROUPED

Group Value
[G_S_U_POOL_IDENTIFIER]

[CC_UNIT_TYPE]

[UNIT_VALUE]

AVP Flag
M

Guaranteed-Bitrate-DL

Defines the guaranteed bit rate allowed for the downlink direction.

AVP Header
1025 10415

Vendor ID
10415

VSA Type
1025

AVP Type
UINT32

Group Value
N/A

AVP Flag
M

Guaranteed-Bitrate-UL

Defines the guaranteed bit rate allowed for the uplink direction.

AVP Header
1026 10415

Vendor ID
10415

VSA Type
1026

AVP Type
UINT32

Group Value
N/A

AVP Flag
M

HBM-Address

HBM-Address.

AVP Header
1462 10415

Vendor ID
10415

VSA Type
1462

AVP Type
ADDRESS

Group Value
N/A

AVP Flag
M

Home-Agent

Used to convey the HA IPv4 address that the MS requests or the HA IPv4 address that the H-AAA assigns.

AVP Header
3 5535

Vendor ID
5535

VSA Type
3

AVP Type
ADDRESS

Group Value
N/A

AVP Flag
M

Host-IP-Address

Mobile station IP address.

AVP Header
257 0

Vendor ID
0

VSA Type
257

AVP Type
ADDRESS

Group Value
N/A

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.

AVP Header
1418 10415

Vendor ID
10415

VSA Type
1418

AVP Type
UINT32

Group Value
N/A

AVP Flag
M

HSGW-Address

HSGW IP address.

AVP Header
1415 10415

Vendor ID
10415

VSA Type
1415

AVP Type
ADDRESS

Group Value
N/A

AVP Flag
M

IDA-Flags

The IDA-Flags AVP contains a bit mask.

AVP Header
1441 10415

Vendor ID
10415

VSA Type
1441

AVP Type
UINT32

Group Value
N/A

AVP Flag
M

Identity-Set

Indicates the requested set of IMS Public identities.

AVP Header
708 0

Vendor ID
0

VSA Type
708

AVP Type
ENUM

Group Value
N/A

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.

AVP Header
28 0

Vendor ID
0

VSA Type
28

AVP Type
UINT32

Group Value
N/A

AVP Flag
M

IDR-Flags

Contains a bit mask.

AVP Header
1490 10415

Vendor ID
10415

VSA Type
1490

AVP Type
UINT32

Group Value
N/A

AVP Flag
M

IMEI

This AVP contains the International Mobile Equipment Identity.

AVP Header
6003 10415

Vendor ID
10415

VSA Type
6003

AVP Type

UTF8STRING

Group Value
N/A

AVP Flag
M

Immediate-Response-Preferred

Indicates which type of AV is requested for immediate use in the MME/SGSN.

AVP Header
6015 10415

Vendor ID
10415

VSA Type
6015

AVP Type
UINT32

Group Value
N/A

AVP Flag
M

IMS-3GPP-Charging-Id

IMS-3GPP-Charging ID.

AVP Header
2 10415

Vendor ID
10415

VSA Type
2

AVP Type
OCTETSTRING

Group Value
N/A

AVP Flag
M

IMS-Charging-Identifier

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

AVP Header

841 10415

Vendor ID
10415

VSA Type
841

AVP Type
UTF8STRING

Group Value
N/A

AVP Flag
M

IMS-Communication-Service-Identifier

Holds 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.

AVP Header
1281 10415

Vendor ID
10415

VSA Type
1281

AVP Type
UTF8STRING

Group Value
N/A

AVP Flag
M

IMS-Information

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

AVP Header
876 10415

Vendor ID
10415

VSA Type
876

AVP Type
GROUPED

Group Value
[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]

[SDP_SESSION_DESCRIPTION]

[SDP_MEDIA_COMPONENT]

[MESSAGE_BODY]

[CAUSE_CODE]

[ACCESS_NETWORK_INFORMATION]

[EARLY_MEDIA_DESCRIPTION]

AVP Flag
M

Inband-Security-Id

Advertise support of the Security portion of the application.

AVP Header
299 0

Vendor ID
0

VSA Type
299

AVP Type
UINT32

Group Value
N/A

AVP Flag
M

Incoming-Trunk-Group-ID

This AVP identifies the incoming PSTN leg.

AVP Header
852 0

Vendor ID
0

VSA Type
852

AVP Type
UTF8STRING

Group Value
N/A

AVP Flag
M

Integrity-Key

This AVP contains the Integrity Key (IK).

AVP Header
626 10415

Vendor ID
10415

VSA Type
626

AVP Type
OCTETSTRING

Group Value
N/A

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.

AVP Header
838 10415

Vendor ID
10415

VSA Type
838

AVP Type
GROUPED

Group Value
[ORIGINATING_IOI]

[TERMINATING_IOI]

AVP Flag

M

IP-CAN-Type

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

AVP Header
1027 10415

Vendor ID
10415

VSA Type
1027

AVP Type
ENUM. Supported values are:

3GPP (0)

DOCSIS (1)

xDSL (2)

WiMAX (3)

3GPP2 (4)

3GPP-EPS (5)

Group Value
N/A

AVP Flag
M

IP-MMS

IP mobility selector.

AVP Header
6076 10415

Vendor ID
10415

VSA Type
6076

AVP Type
UINT32

Group Value
N/A

AVP Flag
M

IP-Version-Authorized

Used to indicate whether the MS is authorised for using IPv4 and/or IPv6.

AVP Header
11 5535

Vendor ID
5535

VSA Type
11

AVP Type
ENUM. Supported values are:

IPv4_or_IPv6 (0)

IPv4_ONLY (1)

IPv6_ONLY (2)

Group Value
N/A

AVP Flag
M

Item-Number

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

AVP Header
1419 10415

Vendor ID
10415

VSA Type
1419

AVP Type
UINT32

Group Value
N/A

AVP Flag
M

KASME

This AVP contains the KASME.

AVP Header
1450 10415

Vendor ID

10415

VSA Type
1450

AVP Type
OCTETSTRING

Group Value
N/A

AVP Flag
M

KC-Key

This AVP contains the Ciphering Key.

AVP Header
1453 10415

Vendor ID
10415

VSA Type
1453

AVP Type
OCTETSTRING

Group Value
N/A

AVP Flag
M

Last-CellSector-ID

String contains last Cell ID and Sector ID.

AVP Header
1420 10415

Vendor ID
10415

VSA Type
1420

AVP Type
UTF8STRING

Group Value
N/A

AVP Flag
M

Last-CellSector-Location

Indicates subscriber last cell/sector location.

AVP Header
536 10415

Vendor ID
10415

VSA Type
536

AVP Type
UTF8STRING

Group Value
N/A

AVP Flag
M

Latching-Indication

This AVP contains the latching indication.

AVP Header
457 13019

Vendor ID
13019

VSA Type
457

AVP Type
ENUM. Supported values are:

LATCH (0)

RELATCH (1)

Group Value
N/A

AVP Flag
N/A

LCS-Info

LCS information.

AVP Header
1473 10415

Vendor ID
10415

VSA Type

1473

AVP Type
GROUPED

Group Value
[GMLC_ADDRESS]

[LCS_PRIVACYEXCEPTION]

[MO_LR]

AVP Flag
M

LCS-PrivacyException

LCS-PrivacyException.

AVP Header
1475 10415

Vendor ID
10415

VSA Type
1475

AVP Type
GROUPED

Group Value
[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.

AVP Header
218 4491

Vendor ID
4491

VSA Type
218

AVP Type

GROUPED

Group Value

[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

Line-Identifier

Line-Identifier.

AVP Header

500 13019

Vendor ID

13019

VSA Type

500

AVP Type

OCTETSTRING

Group Value

N/A

Encryption

M

Local-Sequence-Number

Local-Sequence-Number.

AVP Header

2063 10415

Vendor ID

10415

VSA Type

2063

AVP Type
UINT32

Group Value
N/A

AVP Flag
M

Location-Information

Location-Information.

AVP Header
350 13019

Vendor ID
13019

VSA Type
350

AVP Type
GROUPED

Group Value
[LINE_IDENTIFIER]

[CIVIC_LOCATION]

[GEOSPATIAL_LOCATION]

Encryption
M

Logical-Access-Id

Logical-Access-Id.

AVP Header
302 0

Vendor ID
0

VSA Type
302

AVP Type
OCTETSTRING

Group Value
N/A

Encryption
M

Mandatory-Capability

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

AVP Header
604 10415

Vendor ID
10415

VSA Type
604

AVP Type
UINT32

Group Value
N/A

AVP Flag
M

Max-Requested-Bandwidth-DL

Indicates the maximum requested bandwidth in bits per second for a downlink IP flow.

AVP Header
515 10415

Vendor ID
10415

VSA Type
515

AVP Type
UINT32

Group Value
N/A

AVP Flag
M

Max-Requested-Bandwidth-UL

Indicates the maximum requested bandwidth in bits per second for an uplink IP flow.

AVP Header
516 10415

Vendor ID
10415

VSA Type
516

AVP Type
UINT32

Group Value
N/A

AVP Flag
M

MBMS-2G-3G-Indicator

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

AVP Header
907 10415

Vendor ID
10415

VSA Type
907

AVP Type
ENUM. Supported values are:

2G (0)

3G (1)

2G_AND_3G (2)

Group Value
N/A

AVP Flag
M

MBMS-BMSC-SSM-IP-Address

Contains the value of BM-SCs IPv4 address for Source Specific Multicasting.

AVP Header
918 10415

Vendor ID
10415

VSA Type
918

AVP Type
UTF8STRING

Group Value
N/A

AVP Flag
M

MBMS-BMSC-SSM-IPv6-Address

Contains the value of BM-SCs IPv6 address for Source Specific Multicasting.

AVP Header
919 10415

Vendor ID
10415

VSA Type
919

AVP Type
UTF8STRING

Group Value
N/A

AVP Flag
M

MBMS-Counting-Information

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

AVP Header
914 10415

Vendor ID
10415

VSA Type
914

AVP Type
ENUM. Supported values are:

COUNTING_NOT_APPLICABLE (0)

COUNTING_APPLICABLE (1)

Group Value
N/A

AVP Flag
M

MBMS-GGSN-Address

Contains the value of GGSN's IPv4 address for user plane data.

AVP Header
916 10415

Vendor ID
10415

VSA Type
916

AVP Type
UTF8STRING

Group Value
N/A

AVP Flag
M

MBMS-GGSN-IPv6-Address

Contains the value of GGSN's IPv6 address for user plane data.

AVP Header
917 10415

Vendor ID
10415

VSA Type
917

AVP Type
UTF8STRING

Group Value
N/A

AVP Flag
M

MBMS-Required-QoS

Indicates the quality of service required for the MBMS bearer service.

AVP Header
913 10415

Vendor ID
10415

VSA Type
913

AVP Type
UTF8STRING

Group Value
N/A

AVP Flag
M

MBMS-Service-Area

Indicates the area over which the MBMS bearer service has to be distributed

AVP Header
903 10415

Vendor ID
10415

VSA Type
903

AVP Type
OCTETSTRING

Group Value
N/A

AVP Flag
M

MBMS-Service-Type

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

AVP Header
906 10415

Vendor ID
10415

VSA Type
906

AVP Type
ENUM. Supported values are:

MULTICAST (0)

BROADCAST (1)

Group Value
N/A

AVP Flag
M

MBMS-Session-Duration

Indicates the estimated session duration, if available.

AVP Header
904 10415

Vendor ID
10415

VSA Type

904

AVP Type
OCTETSTRING

Group Value
N/A

AVP Flag
M

MBMS-Session-Identity

Identifies a transmission of a specific MBMS session along with TMGI.

AVP Header
908 10415

Vendor ID
10415

VSA Type
908

AVP Type
OCTETSTRING

Group Value
N/A

AVP Flag
M

MBMS-Session-Repetition-number

Contains the session identity repetition number of the MBMS transmission session on the Gmb interface.

AVP Header
912 10415

Vendor ID
10415

VSA Type
912

AVP Type
OCTETSTRING

Group Value
N/A

AVP Flag
M

MBMS-StartStop-Indication

Indicates whether it is session start or stop procedure.

AVP Header
902 10415

Vendor ID
10415

VSA Type
902

AVP Type
ENUM. Supported values are:

START (0)

STOP (1)

UPDATE (2)

Group Value
N/A

AVP Flag
M

MBMS-Time-To-Data-Transfer

Indicates the expected time between reception of the MBMS Session Start and the commencement of the MBMS Data flow.

AVP Header
911 10415

Vendor ID
10415

VSA Type
911

AVP Type
OCTETSTRING

Group Value
N/A

AVP Flag
M

MBMS-User-Data-Mode-Indication

Specifies whether the sending entity supports unicast or multicast mode of operation.

AVP Header
915 10415

Vendor ID

10415

VSA Type
915

AVP Type
ENUM. Supported values are:

UNICAST (0)

MULTICAST_AND_UNICAST (1)

Group Value
N/A

AVP Flag
M

Media-Component-Description

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

AVP Header
517 10415

Vendor ID
10415

VSA Type
517

AVP Type
Grouped

Group Value
[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.

AVP Header
518 10415

Vendor ID
10415

VSA Type
518

AVP Type
UINT32

Group Value
N/A

AVP Flag
M

Media-Initiator-Flag

This AVP indicates which party has requested the session modification.

The default value is "0" indicating the called party initiated the modification

- [0] called party
- [1] calling party
- [2] unknown

AVP Header
882 10415

Vendor ID
10415

VSA Type
882

AVP Type
ENUM

Group Value
N/A

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.

AVP Header
1288 10415

Vendor ID
10415

VSA Type
1288

AVP Type

UTF8STRING

Group Value
N/A

AVP Flag
M

Media-Sub-Component

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

AVP Header
519 10415

Vendor ID
10415

VSA Type
519

AVP Type
GROUPED

Group Value
[FLOW_NUMBER]

[FLOW_DESCRIPTION]

[FLOW_STATUS]

[FLOW_USAGE]

[MAX_REQUESTED_BANDWIDTH_UL]

[MAX_REQUESTED_BANDWIDTH_DL]

AVP Flag
M

Media-Type

The media types indicate the type of media in the same way as the SDP media types with the same names like AUDIO, VIDEO.

AVP Header
520 10415

Vendor ID
10415

VSA Type
520

AVP Type
ENUM

Group Value
N/A

AVP Flag

M

MEID

MEID.

AVP Header
6110 10415

Vendor ID
10415

VSA Type
6110

AVP Type
OCTETSTRING

Group Value
N/A

AVP Flag
M

Message-Body

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

AVP Header
889 10415

Vendor ID
10415

VSA Type
889

AVP Type
GROUPED

Group Value
[CONTENT_TYPE]

[CONTENT_LENGTH]

[CONTENT_DISPOSITION]

[ORIGINATOR]

AVP Flag
M

Metering-Method

Defines what parameters shall be metered for offline charging.

AVP Header
1007 10415

Vendor ID
10415

VSA Type
1007

AVP Type
ENUM. Supported values are:

DURATION (0)

VOLUME (1)

DURATION_VOLUME (2)

Group Value
N/A

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.

AVP Header
1012 5535

Vendor ID
5535

VSA Type
1012

AVP Type
UINT32

Group Value
N/A

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.

AVP Header
1013 5535

Vendor ID
5535

VSA Type
1013

AVP Type
UINT32

Group Value
N/A

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.

AVP Header
337 10415

Vendor ID
10415

VSA Type
337

AVP Type
UINT32

Group Value
N/A

AVP Flag
M

MIP-Home-Agent-Address

This AVP contains the mobile node's home agent IP address.

AVP Header
334 10415

Vendor ID
10415

VSA Type
334

AVP Type
ADDRESS

Group Value
N/A

AVP Flag
M

MIP-Home-Agent-Address-IETF

MIP-Home-Agent-Address-IETF.

AVP Header

334 0

Vendor ID
0

VSA Type
334

AVP Type
ADDRESS

Group Value
N/A

AVP Flag
M

MIP-Home-Agent-Host

MIP-Home-Agent-Host.

AVP Header
348 0

Vendor ID
0

VSA Type
348

AVP Type
GROUPED

Group Value
[DESTINATION_REALM]

[DESTINATION_HOST]

AVP Flag
M

MIP-Mobile-Node-Address

This AVP contains the mobile node's home IP address.

AVP Header
333 10415

Vendor ID
10415

VSA Type
333

AVP Type
ADDRESS

Group Value
N/A

AVP Flag
M

MIP6-Agent-Info

MIP6 agent information.

AVP Header
486 0

Vendor ID
0

VSA Type
486

AVP Type
GROUPED

Group Value
[MIP_HOME_AGENT_ADDRESS_IETF]

[MIP_HOME_AGENT_HOST]

[MIP6_HOME_LINK_PREFIX]

AVP Flag
M

MIP6-Feature-Vector

MIP6-Feature-Vector.

AVP Header
6062 0

Vendor ID
0

VSA Type
6062

AVP Type
UINT64

Group Value
N/A

AVP Flag
M

MIP6-Home-Link-Prefix

MIP6-Home-Link-Prefix.

AVP Header
6061 0

Vendor ID
0

VSA Type
6061

AVP Type
OCTETSTRING

Group Value
N/A

AVP Flag
M

MME-Service-Type

MME service type.

AVP Header
1483 10415

Vendor ID
10415

VSA Type
1483

AVP Type
GROUPED

Group Value
[SERVICETYPEIDENTITY]

[GMLC_RESTRICTION]

[NOTIFICATION_TO_UE_USER]

AVP Flag
M

MO-LR

MO-LR.

AVP Header
1485 10415

Vendor ID
10415

VSA Type
1485

AVP Type
GROUPED

Group Value
[SS_CODE]

[SS_STATUS]

AVP Flag
M

Mobile-Node-Identifier

Contains MN-NAI identifying the user in EPS network.

AVP Header
89 0

Vendor ID
0

VSA Type
89

AVP Type
OCTETSTRING

Group Value
N/A

AVP Flag
M

Monitoring-Key

Monitoring-Key.

AVP Header
1066 10415

Vendor ID
10415

VSA Type
1066

AVP Type
OCTETSTRING

Group Value
N/A

AVP Flag
N/A

MSISDN

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

AVP Header
701 0

Vendor ID

0

VSA Type
701

AVP Type
OCTETSTRING

Group Value
N/A

AVP Flag
M

Multiple-Auth-Profile

This attribute indicates Multiple Authentication requirements for a particular user.

AVP Header
30 5535

Vendor ID
5535

VSA Type
30

AVP Type
ENUM

Group Value
N/A

AVP Flag
M

Multiple-Auth-Support

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

AVP Header
29 5535

Vendor ID
5535

VSA Type
29

AVP Type
ENUM

Group Value
N/A

AVP Flag
M

Multiple-Services-Credit-Control

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

AVP Header
456 0

Vendor ID
0

VSA Type
456

AVP Type
Grouped

Group Value
[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

Indicates support for independent credit-control of multiple services within the session.

AVP Header
455 0

Vendor ID
0

VSA Type
455

AVP Type
ENUM. Supported values are:

MULTIPLE_SERVICES_NOT_SUPPORTED (0)

MULTIPLE_SERVICES_SUPPORTED (1)

Group Value
N/A

AVP Flag

M

Multi-Round-Time-Out

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

AVP Header
272 0

Vendor ID
0

VSA Type
272

AVP Type
UINT32

Group Value
N/A

AVP Flag
N/A

NAS-Filter-Rule

Provides filter rules that need to be configured on the NAS for the user.

AVP Header
400 0

Vendor ID
0

VSA Type
400

AVP Type
IPFILTERRULE

Group Value
N/A

AVP Flag
M

NAS-Identifier

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

AVP Header
32 0

Vendor ID
0

VSA Type
32

AVP Type
UTF8STRING

Group Value
N/A

AVP Flag
M

NAS-IP-Address

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

AVP Header
4 0

Vendor ID
0

VSA Type
4

AVP Type
OCTETSTRING

Group Value
N/A

AVP Flag
M

NAS-IPv6-Address

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

AVP Header
95 0

Vendor ID
0

VSA Type
95

AVP Type
OCTETSTRING

Group Value
N/A

AVP Flag
M

NAS-Port

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

AVP Header
5 0

Vendor ID
0

VSA Type
5

AVP Type
UINT32

Group Value
N/A

AVP Flag
M

NAS-Port-Id

Consists of ASCII text identifying the port of the NAS authenticating the user.

AVP Header
87 0

Vendor ID
0

VSA Type
87

AVP Type
UTF8STRING

Group Value
N/A

AVP Flag
M

NAS-Port-Type

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

AVP Header
61 0

Vendor ID
0

VSA Type
61

AVP Type
ENUM. Supported values are:

Async (0)

Sync (1)

ISDN_Sync (2)

ISDN_Async_V120 (3)

ISDN_Async_V110 (4)

Virtual (5)

PIAFS (6)

HDLC_Clear_Channel (7)

X25 (8)

X75 (9)

G3_Fax (10)

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

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

IDSL-ISDN-Digital-Subscriber-Line (14)

Ethernet (15)

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

Cable (17)

Wireless-Other (18)

Wireless-IEEE802_11 (19)

Token-Ring_RAD802_1X (20)

FDDI_RAD802_1X (21)

Wireless-CDMA2000 (22)

Wireless-UMTS (23)

Wireless-1X-EV (24)

IAPP_IEEE-802_11f (25)

Group Value
N/A

AVP Flag
M

Network-Access-Mode

Network-Access-Mode.

AVP Header
1417 10415

Vendor ID
10415

VSA Type
1417

AVP Type
ENUM. Supported values are:

PACKET_AND_CIRCUIT (0)

ONLY_CIRCUIT (1)

ONLY_PACKET(2)

Group Value
N/A

Encryption
M

Network-Element-Type

Network element tNode-Functionalitype.

AVP Header
1461 10415

Vendor ID
10415

VSA Type
1461

AVP Type
ENUM. Supported values are:

MME (0)

SGSN (1)

Serving-GW (2)

PDN-GW (3)

eNodeB (4)

RNC (5)

Group Value
N/A

Encryption
M

Network-Request-Support

Indicates the UE and network support of the network requested bearer control mode.

AVP Header
1024 10415

Vendor ID
10415

VSA Type
1024

AVP Type
ENUM. Supported values are:

NETWORK_REQUEST_NOT_SUPPORTED (0)

NETWORK_REQUEST_SUPPORTED (1)

Group Value
N/A

AVP Flag
M

New-Dialog-Id

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.

AVP Header
219 4491

Vendor ID
4491

VSA Type
219

AVP Type
UTF8STRING

Group Value
N/A

AVP Flag
M

Node-Functionality

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

AVP Header
862 0

Vendor ID
0

VSA Type
862

AVP Type
ENUM. Supported values are:

S-CSCF (0)

P-CSCF (1)

I-CSCF (2)

Group Value

N/A

AVP Flag
M

Node-Id

Node ID.

AVP Header
2064 10415

Vendor ID
10415

VSA Type
2064

AVP Type
UTF8STRING

Group Value
N/A

AVP Flag
M

NOR-Flags

NOR-Flags.

AVP Header
1443 10415

Vendor ID
10415

VSA Type
1443

AVP Type
UINT32

Group Value
N/A

AVP Flag
M

Nortel-Data-Reference

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

AVP Header
301 0

Vendor ID

0

VSA Type
301

AVP Type
ENUM

Group Value
N/A

AVP Flag
M

Notification-To-UE-User

Notification-To-UE-User

AVP Header
1478 10415

Vendor ID
10415

VSA Type
1478

AVP Type
ENUM. Supported values are:

NOTIFY_LOCATION_ALLOWED (0)

NOTIFYANDVERIFY_ALLOWED_IF_NO_RESPONSE (1)

NOTIFYANDVERIFY_NOT_ALLOWED_IF_NO_RESPONSE (2)

LOCATION_NOT_ALLOWED (3)

Group Value
N/A

AVP Flag
M

Number-Of-Requested-Vectors

Contains the number of AVs the MME is prepared to receive.

AVP Header
6013 10415

Vendor ID
10415

VSA Type
6013

AVP Type
UINT32

Group Value

N/A

Encryption
M

Offline

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

AVP Header
1008 10415

Vendor ID
10415

VSA Type
1008

AVP Type
ENUM. Supported values are:

DISABLE (0)

ENABLE (1)

Group Value
N/A

AVP Flag
M

Offline-Charging

Holds the parameters required for offline charging.

AVP Header
1278 10415

Vendor ID
10415

VSA Type
1278

AVP Type
GROUPED

Group Value
[RULEBASE_ID]

[QUOTA_CONSUMPTION_TIME]

[TIME_QUOTA_MECHANISM]

[ENVELOPE_REPORTING]

[MULTIPLE_SERVICES_CREDIT_CONTROL]

AVP Flag
M

Online

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

AVP Header
1009 10415

Vendor ID
10415

VSA Type
1009

AVP Type
ENUM. Supported values are:

DISABLE (0)

ENABLE (1)

Group Value
N/A

AVP Flag
M

OMC-Id

OMC ID.

AVP Header
1466 10415

Vendor ID
10415

VSA Type
1466

AVP Type
OCTETSTRING

Group Value
N/A

Encryption
M

Operator-Determined-Barring

Contains a bit mask indicating the services of a subscriber that are barred by the operator.

AVP Header
1425 10415

Vendor ID
10415

VSA Type

1425

AVP Type
UINT32

Group Value
N/A

Encryption
M

Optional-Capability

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

AVP Header
605 10415

Vendor ID
10415

VSA Type
605

AVP Type
UINT32

Group Value
N/A

AVP Flag
M

Originating-IOI

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

AVP Header
839 0

Vendor ID
0

VSA Type
839

AVP Type
UTF8STRING

Group Value
N/A

AVP Flag
M

Originating-Line-Info

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

AVP Header
94 0

Vendor ID
0

VSA Type
94

AVP Type
OCTETSTRING

Group Value
N/A

AVP Flag
N/A

Originating-Request

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

AVP Header
633 10415

Vendor ID
10415

VSA Type
633

AVP Type
ENUM. Supported values are:

ORIGINATING (0)

Group Value
N/A

AVP Flag
M

Originator

This AVP indicates the originating party of the message body.

The following values are defined

- Calling Party (0)
- Called Party (1)

AVP Header
864 10415

Vendor ID

10415

VSA Type
864

AVP Type
ENUM

Group Value
N/A

AVP Flag
M

Origin-Host

The endpoint that originated the Diameter message.

AVP Header
264 0

Vendor ID
0

VSA Type
264

AVP Type
DIAMIDENT

Group Value
N/A

AVP Flag
M

Origin-Realm

The realm of the originator of any Diameter message, and is present in all messages.

AVP Header
296 0

Vendor ID
0

VSA Type
296

AVP Type
DIAMIDENT

Group Value
N/A

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.

AVP Header
278 0

Vendor ID
0

VSA Type
278

AVP Type
UINT32

Group Value
N/A

AVP Flag
M

Outgoing-Trunk-Group-ID

This AVP identifies the outgoing PSTN leg.

AVP Header
853 0

Vendor ID
0

VSA Type
853

AVP Type
UTF8STRING

Group Value
N/A

AVP Flag
M

Packet-Filter-Content

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

AVP Header
1059 10415

Vendor ID
10415

VSA Type
1059

AVP Type
IPFILTERRULE

Group Value
N/A

AVP Flag
M

Packet-Filter-Identifier

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.

AVP Header
1060 10415

Vendor ID
10415

VSA Type
1060

AVP Type
OCTETSTRING

Group Value
N/A

AVP Flag
M

Packet-Filter-Information

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

AVP Header
1061 10415

Vendor ID
10415

VSA Type
1061

AVP Type
GROUPED

Group Value
[PACKET_FILTER_IDENTIFIER]

[PRECEDENCE]

[PACKET_FILTER_CONTENT]

[TOS_TRAFFIC_CLASS]

[SECURITY_PARAMETER_INDEX]

[FLOW_LABEL]

AVP Flag
M

Packet-Filter-Operation

Indicates a UE initiated resource operation that causes a request for PCC rules.

AVP Header
1062 10415

Vendor ID
10415

VSA Type
1062

AVP Type
ENUM. Supported values are:

DELETION (0)

ADDITION (1)

MODIFICATION (2)

Group Value
N/A

AVP Flag
M

Paging-Group-Id

AVP Header
1001 0

Vendor ID
0

VSA Type
1001

AVP Type
UINT32

Group Value
N/A

AVP Flag
M

PCC-Rule-Status

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

AVP Header
1019 5535

Vendor ID
5535

VSA Type
1019

AVP Type
ENUM. Supported values are:

ACTIVE (0) -This value is used to indicate that the PCC rule(s) are successfully installed (for those provisioned from Policy and Charging Rule Functions (PCRF)) or activated (for those pre-provisioned in Access Gateway (AGW).

INACTIVE (1) - This value is used to indicate that the PCC rule(s) are removed (for those provisioned from PCRF) or inactive (for those pre-provisioned in AGW).

TEMPORARY INACTIVE (2)- This value is used to indicate that, for some reason (e.g. loss of IP flow), already installed or activated PCC rules are temporary disabled.

Group Value
N/A

AVP Flag
M

PDG-Address

This AVP contains the PDG IP address.

AVP Header
895 10415

Vendor ID
10415

VSA Type
895

AVP Type
ADDRESS

Group Value
N/A

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.

AVP Header
896 0

Vendor ID
0

VSA Type
896

AVP Type
UINT32

Group Value
N/A

AVP Flag
M

PDN-Connection-ID

Contains the charging identifier to identify different records belonging to same PDN connection.

AVP Header
2050 10415

Vendor ID
10415

VSA Type
2050

AVP Type
UINT32

Group Value
N/A

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.

AVP Header
6041 10415

Vendor ID
10415

VSA Type
6041

AVP Type
ADDRESS

Group Value
N/A

AVP Flag
M

PDN-GW-Allocation-Type

PDN-GW allocation type.

AVP Header
1438 10415

Vendor ID
10415

VSA Type
1438

AVP Type
ENUM. Supported values are:

STATIC (0)

DYNAMIC (1)

Group Value
N/A

AVP Flag
M

PDN-GW-Identity

PDN-GW identity.

AVP Header
6044 10415

Vendor ID
10415

VSA Type
6044

AVP Type
GROUPED

Group Value
[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.

AVP Header
6042 10415

Vendor ID
10415

VSA Type
6042

AVP Type

UTF8STRING

Group Value
N/A

AVP Flag
M

PDN-Type

PDN type.

AVP Header
1456 10415

Vendor ID
10415

VSA Type
1456

AVP Type
ENUM. Supported values are:

IPv4 (0)

IPv6 (1)

IPv4v6 (2)

Group Value
N/A

AVP Flag
M

PDP-Address

This AVP contains the PDP context Address.

AVP Header
1227 10415

Vendor ID
10415

VSA Type
1227

AVP Type
ADDRESS

Group Value
N/A

AVP Flag
M

PDP-Context

PDP context.

AVP Header
1469 10415

Vendor ID
10415

VSA Type
1469

AVP Type
GROUPED

Group Value
[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 PDP Context.

AVP Header
1247 10415

Vendor ID
10415

VSA Type
1247

AVP Type
ENUM

Group Value
N/A

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.

AVP Header

1015 10415

Vendor ID
10415

VSA Type
1015

AVP Type
ENUM

Group Value
N/A

AVP Flag
M

PDP-Type

PDP Type.

AVP Header
1470 10415

Vendor ID
10415

VSA Type
1470

AVP Type
OCTETSTRING

Group Value
N/A

AVP Flag
M

PGW-Address

P-GW IP address.

AVP Header
1405 10415

Vendor ID
10415

VSA Type
1405

AVP Type
ADDRESS

Group Value
N/A

AVP Flag
M

PGW-MCC-MNC

MCC MNC of the network to which the P-GW belongs.

AVP Header
1406 10415

Vendor ID
10415

VSA Type
1406

AVP Type
OCTETSTRING

Group Value
N/A

AVP Flag
M

PGW-Type

Type of P-GW of current flow.

AVP Header
7002 10415

Vendor ID
10415

VSA Type
7002

AVP Type
UINT32

Group Value
N/A

AVP Flag
M

Physical-Access-Id

Physical-Access-Id.

AVP Header
313 0

Vendor ID
0

VSA Type
313

AVP Type
UTF8STRING

Group Value
N/A

Encryption
M

PLMN-Client

PLMN client.

AVP Header
1482 10415

Vendor ID
10415

VSA Type
1482

AVP Type
ENUM. Supported values are:

BROADCAST_SERVICE (0)

O_AND_M_HPLMN (1)

O_AND_M_VPLMN (2)

ANONYMOUS_LOCATION (3)

TARGET_UE_SUBSCRIBED_SERVICE (4)

Group Value
N/A

AVP Flag
M

PMIP-Mobile-Node-Address

PMIP mobile node address.

AVP Header
1408 1751

Vendor ID
1751

VSA Type
1408

AVP Type
ADDRESS

Group Value
N/A

AVP Flag
M

PMIP6-MAG-Address

This AVP contains IP address of MAG.

AVP Header
6070 10415

Vendor ID
10415

VSA Type
6070

AVP Type
ADDRESS

Group Value
N/A

AVP Flag
M

Port-Limit

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

AVP Header
62 0

Vendor ID
0

VSA Type
62

AVP Type
UINT32

Group Value
N/A

AVP Flag
M

Port-Number

Contains the endpoint port number.

AVP Header
455 13091

Vendor ID
13091

VSA Type
455

AVP Type
UINT32

Group Value
N/A

AVP Flag
N/A

Pre-emption-Capability

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

AVP Header
1047 10415

Vendor ID
10415

VSA Type
1047

AVP Type
ENUM. Supported values are:

PRE-EMPTION_CAPABILITY_ENABLED (0)

PRE-EMPTION_CAPABILITY_DISABLED (1)

Group Value
N/A

AVP Flag
M

Pre-emption-Vulnerability

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.

AVP Header
1048 10415

Vendor ID
10415

VSA Type
1048

AVP Type
ENUM. Supported values are:

PRE-EMPTION_VULNERABILITY_ENABLED (0)

PRE-EMPTION_VULNERABILITY_DISABLED (1)

Group Value
N/A

AVP Flag
M

Precedence

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

AVP Header
1010 10415

Vendor ID
10415

VSA Type
1010

AVP Type
UINT32

Group Value
N/A

AVP Flag
M

Primary-Charging-Collection-Function-Name

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

AVP Header
621 10415

Vendor ID
10415

VSA Type
621

AVP Type
UTF8STRING

Group Value
N/A

AVP Flag
M

Primary-Event-Charging-Function-Name

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

AVP Header
619 10415

Vendor ID
10415

VSA Type
619

AVP Type
UTF8STRING

Group Value
N/A

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.

AVP Header
1046 10415

Vendor ID
10415

VSA Type
1046

AVP Type
UINT32

Group Value
N/A

AVP Flag
M

Product-Name

This AVP contains the vendor assigned name for the product.

AVP Header
269 0

Vendor ID
0

VSA Type
269

AVP Type
UTF8STRING

Group Value
N/A

AVP Flag
M

Proxy-Host

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

AVP Header
280 0

Vendor ID
0

VSA Type
280

AVP Type
DIAMIDENT

Group Value
N/A

AVP Flag
M

Proxy-Info

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

AVP Header
284 0

Vendor ID
0

VSA Type
284

AVP Type
Grouped

Group Value
[Proxy-Host]

[Proxy-State]

AVP Flag
M

Proxy-State

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

AVP Header
33 0

Vendor ID
0

VSA Type
33

AVP Type
UTF8STRING

Group Value
N/A

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.

AVP Header
867 10415

Vendor ID
10415

VSA Type
867

AVP Type
ENUM. Supported values are:

APPEND (0)

OVERWRITE (1)

Group Value
N/A

AVP Flag
M

PS-Free-Format-Data

This AVP holds online charging session specific data.

AVP Header
866 10415

Vendor ID
10415

VSA Type
866

AVP Type
OCTETSTRING

Group Value
N/A

AVP Flag
M

PS-Furnish-Charging-Information

This grouped AVP contains online charging session specific information.

AVP Header
865 10415

Vendor ID
10415

VSA Type
865

AVP Type
GROUPED

Group Value
[3GPP_CHARGING_ID]

[PS_FREE_FORMAT_DATA]

[PS_APPEND_FREE_FORMAT]

AVP Flag
M

PS-Information

Its purpose is to allow the transmission of additional PS service specific information elements.

AVP Header
874 10415

Vendor ID
10415

VSA Type
874

AVP Type
Grouped

Group Value
[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

Contains the P-GW Session Correlation ID.

AVP Header
1450 10415

Vendor ID
10415

VSA Type
1450

AVP Type
OCTETSTRING

Group Value
N/A

AVP Flag
M

PUA-Flags

PUA-Flags.

AVP Header
1442 10415

Vendor ID
10415

VSA Type
1442

AVP Type
UINT32

Group Value
N/A

AVP Flag
M

Public-Identity

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

AVP Header
601 10415

Vendor ID
10415

VSA Type
601

AVP Type
UTF8STRING

Group Value
N/A

AVP Flag
M

QoS-Capability

QoS-Capability.

AVP Header
6063 0

Vendor ID
0

VSA Type
6063

AVP Type
GROUPED

Group Value
[QOS_PROFILE_TEMPLATE]

[VENDOR_SPECIFIC_QOS_PROFILE_TEMPLATE]

AVP Flag
M

QoS-Class

Defines the authorized traffic class for the PDP context.

AVP Header
1017 10415

Vendor ID
10415

VSA Type
1017

AVP Type
ENUM

Group Value
N/A

AVP Flag
M

QoS-Class-Identifier

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

AVP Header
1028 10415

Vendor ID
10415

VSA Type
1028

AVP Type
ENUM. Supported values are:

TRAFFIC_CLASS_A (1)

TRAFFIC_CLASS_B (2)

TRAFFIC_CLASS_C (3)

TRAFFIC_CLASS_D (4)

TRAFFIC_CLASS_E (5)

TRAFFIC_CLASS_F (6)

TRAFFIC_CLASS_G (7)

TRAFFIC_CLASS_H (8)

TRAFFIC_CLASS_I (9)

Group Value
N/A

AVP Flag
M

QoS-Information

efines the QoS information for an IP-CAN bearer or PCC rule.

AVP Header
1016 10415

Vendor ID
10415

VSA Type
1016

AVP Type
GROUPED

Group Value
[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

Indicates QoS negotiation capability. I.e., if the PCRF is allowed to negotiate the QoS.

AVP Header
1029 10415

Vendor ID
10415

VSA Type
1029

AVP Type
ENUM. Supported values are:

NO_QoS_NEGOTIATION (0)

QoS_NEGOTIATION_SUPPORTED (1)

Group Value
N/A

AVP Flag
M

QoS-Profile-Template

QoS Profile Template.

AVP Header
6067 0

Vendor ID
0

VSA Type
6067

AVP Type
UINT32

Group Value
N/A

AVP Flag
M

QoS-Resource-Request

Resource requested by UE to PCRF.

AVP Header
6106 10415

Vendor ID
10415

VSA Type
6106

AVP Type
GROUPED

Group Value
[QOS_RESOURCE_IDENTIFIER]

[QOS_RESOURCE_OPERATION]

[TFT_PACKET_FILTER_INFORMATION]

[QOS_INFORMATION]

AVP Flag
M

QoS-Resources

QoS-Resources.

AVP Header
6065 0

Vendor ID
0

VSA Type
6065

AVP Type
GROUPED

Group Value
[EXTENDED_QOS_FILTER_RULE]

AVP Flag
M

QoS-Rule-Definition

Defines the QoS rule for a service flow sent by PCRF to the BBERF.

AVP Header
1053 10415

Vendor ID
10415

VSA Type
1053

AVP Type
GROUPED

Group Value
[QOS_RULE_NAME]

[FLOW_DESCRIPTION]

[QOS_INFORMATION]

[PRECEDENCE]

AVP Flag
M

QoS-Rule-Install

Contains the QoS rules that need to be installed.

AVP Header
1051 10415

Vendor ID
10415

VSA Type
1051

AVP Type
GROUPED

Group Value
[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.

AVP Header
1054 10415

Vendor ID
10415

VSA Type
1054

AVP Type
OCTETSTRING

Group Value

N/A

AVP Flag
M

QoS-Rule-Remove

Used to remove QoS rules from a Gateway Control Session.

AVP Header
1052 10415

Vendor ID
10415

VSA Type
1052

AVP Type
GROUPED

Group Value
[QOS_RULE_NAME]

AVP Flag
M

QoS-Rule-Report

Report the status of QoS rules.

AVP Header
1055 10415

Vendor ID
10415

VSA Type
1055

AVP Type
GROUPED

Group Value
[QOS_RULE_NAME]

[PCC_RULE_STATUS]

[RULE_FAILURE_CODE]

AVP Flag
M

QoS-Subscribed

QoS subscribed.

AVP Header

1404 10415

Vendor ID
10415

VSA Type
1404

AVP Type
OCTETSTRING

Group Value
N/A

AVP Flag
M

QoS-Upgrade

Indicates whether SGSN supports upgrade of QoS by GGSN.

AVP Header
1030 10415

Vendor ID
10415

VSA Type
1030

AVP Type
ENUM. Supported values are:

QoS_UPGRADE_NOT_SUPPORTED (0)

QoS_UPGRADE_SUPPORTED (1)

Group Value
N/A

AVP Flag
M

RACS-Contact-Point

RACS-Contact-Point.

AVP Header
351 0

Vendor ID
0

VSA Type
351

AVP Type
DIAMIDENT

Group Value

N/A

AVP Flag
M

RAI

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

AVP Header
909 10415

Vendor ID
10415

VSA Type
909

AVP Type
UTF8STRING

Group Value
N/A

AVP Flag
M

RAND

This AVP contains the RAND.

AVP Header
1447 10415

Vendor ID
10415

VSA Type
1447

AVP Type
OCTETSTRING

Group Value
N/A

AVP Flag
M

RAS-Id

This AVP contains the RAS identifier.

AVP Header
10000 0

Vendor ID

0

VSA Type
10000

AVP Type
UINT32

Group Value
N/A

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.

AVP Header
432 0

Vendor ID
0

VSA Type
432

AVP Type
UINT32

Group Value
N/A

AVP Flag
M

RAT-Frequency-Selection-Priority

RAT frequency selection priority.

AVP Header
1440 10415

Vendor ID
10415

VSA Type
1440

AVP Type
UINT32

Group Value
N/A

AVP Flag
M

RAT-Type

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

AVP Header
1032 10415

Vendor ID
10415

VSA Type
1032

AVP Type
ENUM. Supported values are:

WLAN (0)

UTRAN (1000)

GERAN (1001)

GAN (1002)

HSPA_EVOLUTION (1003)

EUTRAN (1004)

CDMA2000_1X (2000)

HRPD (2001)

UMB (2002)

Group Value
N/A

AVP Flag
M

Re-Synchronization-Info

This AVP contains the concatenation of RAND and AUTS.

AVP Header
6014 10415

Vendor ID
10415

VSA Type
6014

AVP Type
UINT32

Group Value
N/A

AVP Flag
M

Reason-Code

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

AVP Header
616 10415

Vendor ID
10415

VSA Type
616

AVP Type
ENUM. Supported values are:

PERMANENT_TERMINATION (0)

NEW_SERVER_ASSIGNED (1)

SERVER_CHANGE (2)

REMOVE_S-CSCF (3)

Group Value
N/A

AVP Flag
M

Reason-Info

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

AVP Header
617 10415

Vendor ID
10415

VSA Type
617

AVP Type
UTF8STRING

Group Value
N/A

AVP Flag
M

Reservation-Class

Contains an integer used as an index pointing to the traffic characteristic of the flow.

AVP Header
456 13019

Vendor ID

13019

VSA Type
456

AVP Type
UINT32

Group Value
N/A

AVP Flag
N/A

Resource-Allocation-Notification

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

AVP Header
1063 10415

Vendor ID
10415

VSA Type
1063

AVP Type
ENUM. Supported values are:

ENABLE_NOTIFICATION (0)

Group Value
N/A

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.

AVP Header
285 0

Vendor ID
0

VSA Type
285

AVP Type
ENUM. Supported values are:

AUTHORIZE_ONLY (0)

AUTHORIZE_AUTHENTICATE (1)

Group Value

N/A

AVP Flag
M

Redirect-Address-Type

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

AVP Header
433 0

Vendor ID
0

VSA Type
433

AVP Type
ENUM. Supported values are:

IPv4 Address (0)

IPv6 Address (1)

URL (2)

SIP URL (2)

Group Value
N/A

AVP Flag
M

Redirect-Host

The alternate routing details to which the request need to be redirected to.

AVP Header
292 0

Vendor ID
0

VSA Type
292

AVP Type
DIAMIDENT

Group Value
N/A

AVP Flag
M

Redirect-Host-Usage

Dictates how the routing entry resulting from the Redirect-Host is to be used.

AVP Header
261 0

Vendor ID
0

VSA Type
261

AVP Type
ENUM. Supported values are:

DONT_CACHE (0)

ALL_SESSION (1)

ALL_REALM (2)

REALM_AND_APPLICATION (3)

ALL_APPLICATION (4)

ALL_HOST (5)

ALL_USER (6)

Group Value
N/A

AVP Flag
M

Redirect-Max-Cache-Time

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

AVP Header
262 0

Vendor ID
0

VSA Type
262

AVP Type
UINT32

Group Value
N/A

AVP Flag
M

Redirect-Server

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

AVP Header
434 0

Vendor ID
0

VSA Type
434

AVP Type
Grouped

Group Value
{ Redirect-Address-Type }

{ Redirect-Server-Address }

AVP Flag
M

Redirect-Server-Address

Defines the address of the redirect server.

AVP Header
435 0

Vendor ID
0

VSA Type
435

AVP Type
UTF8STRING

Group Value
N/A

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.

AVP Header
1446 10415

Vendor ID
10415

VSA Type

1446

AVP Type
OCTETSTRING

Group Value
N/A

AVP Flag
M

Reply-Message

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

AVP Header
18 0

Vendor ID
0

VSA Type
18

AVP Type
UTF8STRING

Group Value
N/A

AVP Flag
M

Reporting-Level

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

AVP Header
1011 10415

Vendor ID
10415

VSA Type
1011

AVP Type
ENUM

Group Value
N/A

AVP Flag
M

Requested-Action

The action requested when the CC_Request_Type is EVENT_REQUEST.

AVP Header
436 0

Vendor ID
0

VSA Type
436

AVP Type
ENUM. Supported values are:

DIRECT_DEBITING (0)

REFUND_ACCOUNT (1)

CHECK_BALANCE (2)

PRICE_ENQUIRY (3)

Group Value
N/A

AVP Flag
M

Requested-Domain

Indicates the access domain for which certain data are requested.

AVP Header
706 0

Vendor ID
0

VSA Type
706

AVP Type
ENUM

Group Value
N/A

AVP Flag
M

Requested-EUTRAN-Authentication-Info

This AVP contains the EU Tran authentication information.

AVP Header
6010 10415

Vendor ID

10415

VSA Type
6010

AVP Type
GROUPED

Group Value
[NUMBER_OF_REQUESTED_VECTORS]

[IMMEDIATE_RESPONSE_PREFERRED]

[RE_SYNCHRONIZATION_INFO]

AVP Flag
M

Requested-GERAN-Authentication-Info

This AVP contains GE RAN authentication information.

AVP Header
6012 10415

Vendor ID
10415

VSA Type
6012

AVP Type
GROUPED

Group Value
[NUMBER_OF_REQUESTED_VECTORS]

[IMMEDIATE_RESPONSE_PREFERRED]

[RE_SYNCHRONIZATION_INFO]

AVP Flag
M

Requested-Information

Requested-Information.

AVP Header
353 13019

Vendor ID
13019

VSA Type
353

AVP Type
ENUM. Supported values are:

NASS-USER-ID (0)

LOCATION-INFORMATION (1)

RACS-CONTACT-POINT (2)

ACCESS-NETWORK-TYPE (3)

TERMINAL-TYPE (4)

LOGICAL-ACCESS-ID (5)

PHYSICAL-ACCESS-ID (6)

ACCESS-NETWORK-TYPE-RESERVED (7)

INITIAL-GATE-SETTING-RESERVED (8)

QOS-PROFILE-RESERVED (9)

IP-CONNECTIVITY-STATUS-RESERVED (10)

Group Value
N/A

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.

AVP Header
1251 10415

Vendor ID
10415

VSA Type
1215

AVP Type
UTF8STRING

Group Value
N/A

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.

AVP Header
812 5535

Vendor ID
5535

VSA Type

812

AVP Type
Grouped

Group Value
[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.

AVP Header
437 0

Vendor ID
0

VSA Type
437

AVP Type
Grouped

Group Value
[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

Requested-UTRAN-Authentication-Info.

AVP Header
6011 10415

Vendor ID
10415

VSA Type

6011

AVP Type
GROUPED

Group Value
[NUMBER_OF_REQUESTED_VECTORS]

[IMMEDIATE_RESPONSE_PREFERRED]

[RE_SYNCHRONIZATION_INFO]

AVP Flag
M

Requested-UTRAN-GERAN-Authentication-Info

Requested-UTRAN-GERAN-Authentication information.

AVP Header
1409 10415

Vendor ID
10415

VSA Type
1409

AVP Type
GROUPED

Group Value
[NUMBER_OF_REQUESTED_VECTORS]

[IMMEDIATE_RESPONSE_PREFERRED]

[RE_SYNCHRONIZATION_INFO]

AVP Flag
M

Requesting-Node-Type

Requesting node type.

AVP Header
1455 10415

Vendor ID
10415

VSA Type
1455

AVP Type
ENUM. Supported values are:

MME (0)

SGSN (1)

MME-SGSN (2)

Group Value
N/A

AVP Flag
M

Required-MBMS-Bearer-Capabilities

Contains the minimum bearer capabilities the UE needs to support.

AVP Header
901 10415

Vendor ID
10415

VSA Type
901

AVP Type
UTF8STRING

Group Value
N/A

AVP Flag
M

Reservation-Priority

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

AVP Header
458 13019

Vendor ID
13019

VSA Type
458

AVP Type
ENUM. Supported values are:

DEFAULT (0)

PRIORITY-ONE (1)

PRIORITY-TWO (2)

PRIORITY-THREE (3)

PRIORITY-FOUR (4)

PRIORITY-FIVE (5)

PRIORITY-SIX (6)

PRIORITY-SEVEN (7)

Group Value
N/A

AVP Flag
N/A

Restriction-Filter-Rule

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

AVP Header
438 0

Vendor ID
0

VSA Type
438

AVP Type
IPFILTERRULE

Group Value
N/A

AVP Flag
M

Result-Code

Indicates whether a particular request was completed successfully or whether an error occurred.

AVP Header
268 0

Vendor ID
0

VSA Type
268

AVP Type
ENUM. Supported values are:

DIAMETER_MULTI_ROUND_AUTH (1001)

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_BALANCE_IS_ZERO (4212)

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)

Group Value

N/A

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.

AVP Header
1042 10415

Vendor ID
10415

VSA Type
1042

AVP Type
TIME

Group Value
N/A

AVP Flag
M

Roaming-Restricted-Due-To-Unsupported-Feature

Roaming restricted due to unsupported feature.

AVP Header
1457 10415

Vendor ID
10415

VSA Type
1457

AVP Type
ENUM. Supported values are:

ROAMING_RESTRICTED_DUE_TO_UNSUPPORTED_FEATURE (0)

Group Value
N/A

AVP Flag
M

Role-Of-Node

This AVP specifies the role of the AS/CSCF.

The identifier can be one of the following

- ORIGINATING_ROLE (0) The AS/CSCF is applying a originating role, serving the calling subscriber.
- TERMINATING_ROLE (1) The AS/CSCF is applying a terminating role, serving the called subscriber.
- PROXY ROLE (2) The AS is applying a proxy role.
- B2BUA_ROLE (3) The AS is applying a B2BUA role.

AVP Header
829 10415

Vendor ID
10415

VSA Type
829

AVP Type
ENUM

Group Value
N/A

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.

AVP Header
282 0

Vendor ID
0

VSA Type
282

AVP Type
DIAMIDENT

Group Value
N/A

AVP Flag
M

RR-Bandwidth

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

AVP Header
521 10415

Vendor ID
10415

VSA Type
521

AVP Type
UINT32

Group Value
N/A

AVP Flag
M

RS-Bandwidth

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

AVP Header
522 10415

Vendor ID
10415

VSA Type
522

AVP Type
UINT32

Group Value
N/A

AVP Flag
M

Rule-Activation-Time

Contains the value indicating the NTP time at which the PCC rule has to be enforced.

AVP Header
1043 10415

Vendor ID
10415

VSA Type
1043

AVP Type
TIME

Group Value
N/A

AVP Flag
M

Rule-Deactivation-Time

Contains the value indicating the NTP time at which the PCEF has to stop enforcing the PCC rule.

AVP Header
1044 10415

Vendor ID
10415

VSA Type
1044

AVP Type
TIME

Group Value
N/A

AVP Flag
M

Rule-Failure-Code

Rule failure code.

AVP Header
1031 10415

Vendor ID
10415

VSA Type
1031

AVP Type
ENUM. Supported values are:

UNKNOWN_RULE_NAME (1)

RATING_GROUP_ERROR (2)

SERVICE_IDENTIFIER_ERROR (3)

GW_PCEF_MALFUNCTION (4)

RESOURCES_LIMITATION (5)

MAX_NR_BEARERS_REACHED (6)

UNKNOWN_BEARER_ID (7)

MISSING_BEARER_ID (8)

MISSING_FLOW_DESCRIPTION (9)

RESOURCE_ALLOCATION_FAILURE (10)

UNSUCCESSFUL_QOS_VALIDATION (11)

Group Value
N/A

AVP Flag
M

Rule-Reason-Code

Rule-Reason-Code.

AVP Header
814 10415

Vendor ID
10415

VSA Type
814

AVP Type
ENUM. Supported values are:

UNKNOWN_FLOW_IDENTIFIER (0)

UNKNOWN_RULE_NAME (1)

RATING_GROUP_ERROR (2)

SERVICE_IDENTIFIER_ERROR (3)

AGW_MALFUNCTION (4)

RESOURCES_LIMITATION (5)

Group Value
N/A

AVP Flag
M

SDP-Answer-Timestamp

SDP answer timestamp.

AVP Header
1275 0

Vendor ID
0

VSA Type
1275

AVP Type
TIME

Group Value
N/A

AVP Flag
M

SDP-Media-Component

Defines an interface representing the SDP-Media-Component grouped AVP type.

AVP Header
843 10415

Vendor ID
10415

VSA Type
843

AVP Type
GROUPED

Group Value
[SDP_MEDIA_NAME]

[SDP_MEDIA_DESCRIPTION]

[MEDIA_INITIATOR_FLAG]

[AUTHORISED_QOS]

[3GPP_CHARGING_ID]

AVP Flag
M

SDP-Media-Description

This AVP holds 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.

AVP Header
845 10415

Vendor ID
10415

VSA Type
845

AVP Type
UTF8STRING

Group Value
N/A

AVP Flag
M

SDP-Media-Name

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

AVP Header
844 10415

Vendor ID
10415

VSA Type
844

AVP Type
UTF8STRING

Group Value
N/A

AVP Flag
M

SDP-Offer-Timestamp

SDP offer timestamp.

AVP Header
1274 0

Vendor ID
0

VSA Type
1274

AVP Type
TIME

Group Value
N/A

AVP Flag
M

SDP-Session-Description

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

AVP Header
842 10415

Vendor ID
10415

VSA Type
842

AVP Type
UTF8STRING

Group Value
N/A

AVP Flag
M

SDP-TimeStamps

SDP timestamps.

AVP Header
1273 0

Vendor ID
0

VSA Type
1273

AVP Type
GROUPED

Group Value
[SDP_OFFER_TIMESTAMP]
[SDP_ANSWER_TIMESTAMP]

AVP Flag
M

Secondary-Charging-Collection-Function-Name

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

AVP Header
622 10415

Vendor ID
10415

VSA Type
622

AVP Type
UTF8STRING

Group Value
N/A

AVP Flag
M

Secondary-Event-Charging-Function-Name

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

AVP Header
620 10415

Vendor ID
10415

VSA Type
620

AVP Type
UTF8STRING

Group Value
N/A

AVP Flag
M

Sector-Id

The identifier of sector that MS exists.

AVP Header

10002

Vendor ID
N/A

VSA Type
1002

AVP Type
UINT32

Group Value
N/A

AVP Flag
M

Security-Parameter-Index

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

AVP Header
1056 10415

Vendor ID
10415

VSA Type
1056

AVP Type
OCTETSTRING

Group Value
N/A

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.

AVP Header
848 10415

Vendor ID
10415

VSA Type
848

AVP Type
ADDRESS

Group Value
N/A

AVP Flag

M

Server-Assignment-Type

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

AVP Header
614 10415

Vendor ID
10415

VSA Type
614

AVP Type
ENUM. Supported values are:

NO_ASSIGNMENT (0)

REGISTRATION (1)

RE_REGISTRATION (2)

UNREGISTERED_USER (3)

TIMEOUT_DEREGISTRATION (4)

USER_DEREGISTRATION (5)

TIMEOUT_DEREGISTRATION_STORE_SERVER_NAME (6)

USER_DEREGISTRATION_STORE_SERVER_NAME (7)

ADMINISTRATIVE_DEREGISTRATION (8)

AUTHENTICATION_FAILURE (9)

AUTHENTICATION_TIMEOUT (10)

DEREGISTRATION_TOO_MUCH_DATA (11)

Group Value
N/A

AVP Flag
M

Server-Capabilities

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

AVP Header
603 10415

Vendor ID
10415

VSA Type
603

AVP Type

GROUPED

Group Value

[MANDATORY_CAPABILITY]

[OPTIONAL_CAPABILITY]

[SERVER_NAME]

AVP Flag

M

Server-Name

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

AVP Header

602 10415

Vendor ID

10415

VSA Type

602

AVP Type

UTF8STRING

Group Value

N/A

AVP Flag

M

Service-Class

Contains the service class requested by the AF.

AVP Header

459 13019

Vendor ID

13019

VSA Type

459

AVP Type

UTF8STRING

Group Value

N/A

AVP Flag

N/A

Service-Context-Id

Unique identifier of credit-control service.

AVP Header
461 0

Vendor ID
0

VSA Type
461

AVP Type
UTF8STRING

Group Value
N/A

AVP Flag
M

Service-Data-Container

Service data container.

AVP Header
2040 10415

Vendor ID
10415

VSA Type
2040

AVP Type
GROUPED

Group Value
[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.

AVP Header
439 0

Vendor ID
0

VSA Type
439

AVP Type
UINT32

Group Value
N/A

AVP Flag
M

Service-Indication

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

AVP Header
704 0

Vendor ID
0

VSA Type
704

AVP Type
OCTETSTRING

Group Value
N/A

AVP Flag
M

Service-Information

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

AVP Header
873 10415

Vendor ID
10415

VSA Type
873

AVP Type
Grouped

Group Value
[IMS-Information]

AVP Flag
M

Service-Info-Status

Indicates the status of the service information that the AF is providing to the PCRF.

AVP Header
527 10415

Vendor ID
10415

VSA Type
527

AVP Type
ENUM. Supported values are:

FINAL_SERVICE_INFORMATION (0)

PRELIMINARY_SERVICE_INFORMATION (1)

Group Value
N/A

AVP Flag
M

Service-Parameter-Info

Service-specific information used for rating.

AVP Header
440 0

Vendor ID
0

VSA Type
440

AVP Type
Grouped

Group Value
{ Service-Parameter-Type }

{ Service-Parameter-Value }

AVP Flag
M

Service-Parameter-Type

Service event specific parameter (e.g. end-user location or service name.

AVP Header
441 0

Vendor ID
0

VSA Type
441

AVP Type
UINT32

Group Value
N/A

AVP Flag
M

Service-Parameter-Value

Value of the service parameter type.

AVP Header
442 0

Vendor ID
0

VSA Type
442

AVP Type
OCTETSTRING

Group Value
N/A

AVP Flag
M

Service-Selection

Service-Selection.

AVP Header
493 0

Vendor ID
0

VSA Type
493

AVP Type
OCTETSTRING

Group Value
N/A

AVP Flag
M

Service-Specific-Data

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

AVP Header
1249 0

Vendor ID
0

VSA Type
1249

AVP Type
GROUPED

Group Value
[SERVICE_SPECIFIC_TYPE]

[SERVICE_SPECIFIC_VALUE]

AVP Flag
M

Service-Specific-Info

Service specific information.

AVP Header
1249 10415

Vendor ID
10415

VSA Type
1249

AVP Type
GROUPED

Group Value
[SERVICE_SPECIFIC_DATA]

[SERVICE_SPECIFIC_TYPE]

AVP Flag
M

Service-Specific-Type

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

AVP Header
1248 0

Vendor ID
0

VSA Type
1248

AVP Type
UINT32

Group Value
N/A

AVP Flag
M

Service-Specific-Value

This AVP holds service specific value.

AVP Header
863 0

Vendor ID
0

VSA Type
863

AVP Type
UTF8STRING

Group Value
N/A

AVP Flag
M

Service-Type

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

AVP Header
6 0

Vendor ID
0

VSA Type
6

AVP Type
ENUM. Supported values are:

Login (1)

Framed (2)

Callback-Login (3)

Callback-Framed (4)

Outbound (5)

Administrative (6)

NAS-Prompt (7)

Authenticate-Only (8)

Callback-NAS-Prompt (9)

Call-Check (10)

Callback-Administrative (11)

Voice (12)

Fax (13)

Modem-Relay (14)

IAPP-Register_IEEE-802_11f (15)

IAPP-AP-Check_IEEE-802_11f (16)

Authorize-Only-RADDynAuth (17)

Group Value
N/A

AVP Flag
M

ServiceTypeIdentity

Service type identity.

AVP Header
1484 10415

Vendor ID
10415

VSA Type
1484

AVP Type
UINT32

Group Value
N/A

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.

AVP Header
525 10415

Vendor ID
10415

VSA Type
525

AVP Type
OCTETSTRING

Group Value
N/A

AVP Flag
M

Serving-Node-Type

This AVP identifies the Serving Node type.

AVP Header
2047 10415

Vendor ID
10415

VSA Type
2047

AVP Type
ENUM. Supported values are:

SGSN (0)

PMIPSGW (1)

GTPSGW (2)

ePDG (3)

hSGW (4)

MME (5)

Group Value
N/A

AVP Flag
M

Session-Bundle-Id

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

AVP Header
400 13019

Vendor ID
13019

VSA Type
400

AVP Type
UINT32

Group Value
N/A

AVP Flag
M

Session-Id

Specifies the specific session with an identifier.

AVP Header
263 0

Vendor ID
0

VSA Type
263

AVP Type
UTF8STRING

Group Value
N/A

AVP Flag
M

Session-Release-Cause

Determines the release cause of the IP-CAN session.

AVP Header

1045 10415

Vendor ID
10415

VSA Type
1045

AVP Type
ENUM. Supported values are:

UNSPECIFIED_REASON (0)

UE_SUBSCRIPTION_REASON (1)

INSUFFICIENT_SERVER_RESOURCES (2)

Group Value
N/A

AVP Flag
M

Session-Start-Indicator

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

AVP Header
522 8164

Vendor ID
8164

VSA Type
522

AVP Type
OCTETSTRING

Group Value
N/A

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.

AVP Header
27 0

Vendor ID
0

VSA Type
27

AVP Type

UINT32

Group Value
N/A

AVP Flag
M

SGSN-Address

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

AVP Header
1228 10415

Vendor ID
10415

VSA Type
1228

AVP Type
ADDRESS

Group Value
N/A

AVP Flag
M

SGW-Address

SGW IP address.

AVP Header
1403 10415

Vendor ID
10415

VSA Type
1403

AVP Type
ADDRESS

Group Value
N/A

AVP Flag
M

SGW-Change

SGW-Change.

AVP Header

2065 10415

Vendor ID
10415

VSA Type
2065

AVP Type
ENUM. Supported values are:

ACR_START_NOT_DUE_TO_SGW_CHANGE (0)

ACR_START_DUE_TO_SGW_CHANGE (1)

Group Value
N/A

AVP Flag
M

SGW-Type

Type of SGW of current flow.

AVP Header
7001 10415

Vendor ID
10415

VSA Type
7001

AVP Type
UINT32

Group Value
N/A

AVP Flag
M

SIP-Auth-Data-Item

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

AVP Header
612 10415

Vendor ID
10415

VSA Type
612

AVP Type
GROUPED

Group Value

[SIP_ITEM_NUMBER]

[SIP_AUTHENTICATION_SCHEME]

[SIP_AUTHENTICATE]

[SIP_DIGEST_AUTHENTICATE]

[SIP_AUTHORIZATION]

[SIP_AUTHENTICATION_CONTEXT]

[CONFIDENTIALITY_KEY]

[INTEGRITY_KEY]

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.

AVP Header
609 10415

Vendor ID
10415

VSA Type
609

AVP Type
OCTETSTRING

Group Value
N/A

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.

AVP Header
611 10415

Vendor ID
10415

VSA Type
611

AVP Type
OCTETSTRING

Group Value
N/A

AVP Flag
M

SIP-Authentication-Scheme

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

AVP Header
608 10415

Vendor ID
10415

VSA Type
608

AVP Type
UTF8STRING

Group Value
N/A

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.

AVP Header
610 10415

Vendor ID
10415

VSA Type
610

AVP Type
OCTETSTRING

Group Value
N/A

AVP Flag
M

SIP-Digest-Authenticate

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

AVP Header
635 10415

Vendor ID

10415

VSA Type
635

AVP Type
GROUPED

Group Value
[DIGEST_REALM]

[DIGEST_DOMAIN]

[DIGEST_ALGORITHM]

[DIGEST_QOP]

[DIGEST_HA1]

[DIGEST_AUTH_PARAM]

AVP Flag
M

SIP-Forking-Indication

Describes if several SIP dialogues are related to one Diameter session.

AVP Header
523 10415

Vendor ID
10415

VSA Type
523

AVP Type
ENUM

Group Value
N/A

AVP Flag
M

SIP-Item-Number

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

AVP Header
613 10415

Vendor ID
10415

VSA Type
613

AVP Type
UINT32

Group Value
N/A

AVP Flag
M

SIP-Message

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

AVP Header
229 4491

Vendor ID
4491

VSA Type
229

AVP Type
OCTETSTRING

Group Value
N/A

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.

AVP Header
824 10415

Vendor ID
10415

VSA Type
824

AVP Type
UTF8STRING

Group Value
N/A

AVP Flag
M

SIP-Number-Auth-Items

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

AVP Header
607 10415

Vendor ID
10415

VSA Type
607

AVP Type
UINT32

Group Value
N/A

AVP Flag
M

SIP-Request-Timestamp

This AVP holds the time in UTC format of the initial SIP request (e.g. Invite).

AVP Header
834 10415

Vendor ID
10415

VSA Type
834

AVP Type
TIME

Group Value
N/A

AVP Flag
M

SIP-Response-Timestamp

This AVP holds the time in UTC format of the response to the initial SIP request (e.g. 200 OK).

AVP Header
835 10415

Vendor ID
10415

VSA Type
835

AVP Type
TIME

Group Value
N/A

AVP Flag
M

SN-Absolute-Validity-Time

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

AVP Header
505 8164

Vendor ID
8164

VSA Type
505

AVP Type
TIME

Group Value
N/A

AVP Flag
N/A

SN-Bandwidth-Control

Contains the value to control bandwidth usage.

AVP Header
512 8164

Vendor ID
8164

VSA Type
512

AVP Type
ENUM. Supported values are:

HIGH (0)

LOW (1)

Group Value
N/A

AVP Flag
M

SN-Firewall-Policy

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

AVP Header
515 8164

Vendor ID
8164

VSA Type

515

AVP Type
UTF8STRING

Group Value
N/A

AVP Flag
N/A

SN-Monitoring-Key

SN-Monitoring-Key.

AVP Header
518 8164

Vendor ID
8164

VSA Type
518

AVP Type
UINT32

Group Value
N/A

AVP Flag
N/A

SN-Service-Flow-Detection

SN-Service-Flow-Detection.

AVP Header
520 8164

Vendor ID
8164

VSA Type
520

AVP Type
ENUM. Supported values are:

ENABLE_DETECTION (0)

DISABLE_DETECTION (1)

Group Value
N/A

AVP Flag
N/A

SN-Time-Quota-Threshold

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

AVP Header
503 8164

Vendor ID
8164

VSA Type
503

AVP Type
UINT32

Group Value
N/A

AVP Flag
M

SN-Total-Used-Service-Unit

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

AVP Header
504 8164

Vendor ID
8164

VSA Type
504

AVP Type
GROUPED

Group Value
[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 the Traffic Policing policy name.

AVP Header
514 8164

Vendor ID
8164

VSA Type
514

AVP Type
UTF8STRING

Group Value
N/A

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.

AVP Header
513 8164

Vendor ID
8164

VSA Type
513

AVP Type
OCTETSTRING

Group Value
N/A

AVP Flag
N/A

SN-Unit-Quota-Threshold

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

AVP Header
502 8164

Vendor ID
8164

VSA Type
502

AVP Type
UINT32

Group Value
N/A

AVP Flag
M

SN-Usage-Monitoring

SN-Usage-Monitoring.

AVP Header
521 8164

Vendor ID
8164

VSA Type
521

AVP Type
ENUM. Supported values are:

USAGE_MONITORING_DISABLED (0)

USAGE_MONITORING_ENABLED (1)

Group Value
N/A

AVP Flag
N/A

SN-Usage-Monitoring-Control

SN-Usage-Monitoring-Control.

AVP Header
517 8164

Vendor ID
8164

VSA Type
517

AVP Type
GROUPED

Group Value
[SN_MONITORING_KEY]

[SN_USAGE_MONITORING]

[SN_USAGE_VOLUME]

AVP Flag
N/A

SN-Usage-Volume

SN-Usage-Volume.

AVP Header
519 8164

Vendor ID
8164

VSA Type
519

AVP Type
UINT64

Group Value
N/A

AVP Flag
N/A

SN-Volume-Quota-Threshold

This AVP contains a volume threshold value in percent value. This is a vendor-specific AVP.

AVP Header
501 8164

Vendor ID
8164

VSA Type
501

AVP Type
UINT32

Group Value
N/A

AVP Flag
M

Software-Version

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

AVP Header
6004 10415

Vendor ID
10415

VSA Type
6004

AVP Type
UTF8STRING

Group Value
N/A

AVP Flag
M

Specific-Action

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

AVP Header
513 10415

Vendor ID
10415

VSA Type
513

AVP Type
ENUM. Supported values are:

SERVICE_INFORMATION_REQUEST (0)

CHARGING_CORRELATION_EXCHANGE (1)

INDICATION_OF_LOSS_OF_BEARER (2)

INDICATION_OF_RECOVERY_OF_BEARER (3)

INDICATION_OF_RELEASE_OF_BEARER (4)

INDICATION_OF_ESTABLISHMENT_OF_BEARER (5)

IP_CAN_CHANGE (6)

INDICATION_OF_SUBSCRIBER_DETACHMENT (6)

INDICATION_OF_RESERVATION_EXPIRATION (7)

Group Value
N/A

AVP Flag
M

Specific-APN-Info

Specific APN information.

AVP Header
1472 10415

Vendor ID
10415

VSA Type
1472

AVP Type
GROUPED

Group Value
[SERVICE_SELECTION]
[MIP6_AGENT_INFO]

AVP Flag
M

SRES

This AVP contains the SRES.

AVP Header
1454 10415

Vendor ID
10415

VSA Type
1454

AVP Type
OCTETSTRING

Group Value
N/A

AVP Flag
M

SS-Code

SS code.

AVP Header
1476 10415

Vendor ID
10415

VSA Type
1476

AVP Type
OCTETSTRING

Group Value
N/A

AVP Flag
M

SS-Status

SS status.

AVP Header

1477 10415

Vendor ID
10415

VSA Type
1477

AVP Type
OCTETSTRING

Group Value
N/A

AVP Flag
M

Start-Time

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

AVP Header
2041 10415

Vendor ID
10415

VSA Type
2041

AVP Type
TIME

Group Value
N/A

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".

AVP Header
24 0

Vendor ID
0

VSA Type
24

AVP Type
OCTETSTRING

Group Value
N/A

AVP Flag

M

STN-SR

This AVP contains the session transfer number for SRVCC.

AVP Header
1433 10415

Vendor ID
10415

VSA Type
1433

AVP Type
UTF8STRING

Group Value
N/A

AVP Flag
M

Stop-Time

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.

AVP Header
2042 10415

Vendor ID
10415

VSA Type
2042

AVP Type
TIME

Group Value
N/A

AVP Flag
M

Subscriber-Priority

Subscriber-Priority.

AVP Header
6078 5535

Vendor ID
5535

VSA Type
6078

AVP Type
GROUPED

Group Value
[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

Indicates if the service is barred or granted.

AVP Header
1424 10415

Vendor ID
10415

VSA Type
1424

AVP Type
ENUM. Supported values are:

SERVICEGRANTED (0)

OPERATORDETERMINEDBARRING (1)

Group Value
N/A

AVP Flag
M

Subscription-Data

APN list for subscription.

AVP Header
6001 10415

Vendor ID
10415

VSA Type
6001

AVP Type
GROUPED

Group Value
[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.).

AVP Header
443 0

Vendor ID
0

VSA Type
443

AVP Type
GROUPED

Group Value
[Subscription-Id-Type]

[Subscription-Id-Data]

AVP Flag
M

Subscription-Id-Data

Used to identify the end user information.

AVP Header

444 0

Vendor ID
0

VSA Type
444

AVP Type
UTF8STRING

Group Value
N/A

AVP Flag
M

Subscription-Id-Type

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

AVP Header
450 0

Vendor ID
0

VSA Type
450

AVP Type
ENUM. Supported values are:

END_USER_E164 (0)

END_USER_IMSI (1)

END_USER_SIP_URI (2)

END_USER_NAI (3)

END_USER_PRIVATE (4)

Group Value
N/A

AVP Flag
M

Supported-Applications

This AVP contains supported application identifiers of a Diameter node.

AVP Header
631 10415

Vendor ID
10415

VSA Type
631

AVP Type
GROUPED

Group Value
[AUTH_APPLICATION_ID]

[ACCT_APPLICATION_ID]

[VENDOR_SPECIFIC_APPLICATION_ID]

AVP Flag
M

Supported-Features

May inform the destination host about the features supported by the origin host.

AVP Header
628 10415

Vendor ID
10415

VSA Type
628

AVP Type
GROUPED

Group Value
[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).

AVP Header
628 10415

Vendor ID
10415

VSA Type
628

AVP Type
GROUPED

Group Value
[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.

AVP Header
6005 10415

Vendor ID
10415

VSA Type
6005

AVP Type
UTF8STRING

Group Value
N/A

AVP Flag
M

Supported-Vendor-Id

Specifies the vendor id other than the device vendor.

AVP Header
265 0

Vendor ID
0

VSA Type
265

AVP Type
UINT32

Group Value
N/A

AVP Flag
M

Tap-Id

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

AVP Header
231 4491

Vendor ID
4491

VSA Type
231

AVP Type
UTF8STRING

Group Value
N/A

AVP Flag
M

Tariff-Change-Usage

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

AVP Header
452 0

Vendor ID
0

VSA Type
452

AVP Type
ENUM. Supported values are:

UNIT_BEFORE_TARIFF_CHANGE (0)

UNIT_AFTER_TARIFF_CHANGE (1)

UNIT_INDETERMINATE (2)

Group Value
N/A

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.

AVP Header
451 0

Vendor ID
0

VSA Type
451

AVP Type
TIME

Group Value
N/A

AVP Flag
M

Teleservice-List

Teleservice list.

AVP Header
1486 10415

Vendor ID
10415

VSA Type
1486

AVP Type
GROUPED

Group Value
[TS_CODE]

AVP Flag
M

Terminal-Information

Terminal information.

AVP Header
6002 10415

Vendor ID
10415

VSA Type
6002

AVP Type
GROUPED

Group Value
[ESN]

[MEID]

[IMEI]

[SOFTWARE_VERSION]

AVP Flag
M

Terminal-Type

Terminal type.

AVP Header

352 13019

Vendor ID
13019

VSA Type
352

AVP Type
OCTETSTRING

Group Value
N/A

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.

AVP Header
840 0

Vendor ID
0

VSA Type
840

AVP Type
UTF8STRING

Group Value
N/A

AVP Flag
M

Termination-Cause

Indicates the reason why a session was terminated on the access device.

AVP Header
295 0

Vendor ID
0

VSA Type
295

AVP Type
ENUM. Supported values are:

DIAMETER_LOGOUT (1)

DIAMETER_SERVICE_NOT_PROVIDED (2)

DIAMETER_BAD_ANSWER (3)

DIAMETER_ADMINISTRATIVE (4)

DIAMETER_LINK_BROKEN (5)

DIAMETER_AUTH_EXPIRED (6)

DIAMETER_USER_MOVED (7)

DIAMETER_SESSION_TIMEOUT (8)

Group Value
N/A

AVP Flag
M

TFT-Filter

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

AVP Header
1012 10415

Vendor ID
10415

VSA Type
1012

AVP Type
IPFILTERRULE

Group Value
N/A

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.

AVP Header
1013 10415

Vendor ID
10415

VSA Type
1013

AVP Type
Grouped

Group Value
[Precedence]

[TFT-Filter]

[ToS-Traffic-Class]

AVP Flag
M

Time-First-Usage

Time-First-Usage.

AVP Header
2043 10415

Vendor ID
10415

VSA Type
2043

AVP Type
TIME

Group Value
N/A

AVP Flag
M

Time-Last-Usage

Time-Last-Usage.

AVP Header
2044 10415

Vendor ID
10415

VSA Type
2044

AVP Type
TIME

Group Value
N/A

AVP Flag
M

Time-Quota-Mechanism

Include this AVP in a Multiple-Services-Credit-Control AVP, when granting time quota.

AVP Header
1270 10415

Vendor ID

10415

VSA Type
1270

AVP Type
Grouped

Group Value
[Base-Time-Interval]

[Time-Quota-Type]

AVP Flag
M

Time-Quota-Type

Indicate which time quota consumption mechanism shall be used for the associated category.

AVP Header
1271 10415

Vendor ID
10415

VSA Type
1271

AVP Type
ENUM

Group Value
N/A

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.

AVP Header
833 0

Vendor ID
0

VSA Type
833

AVP Type
GROUPED

Group Value
[SIP_REQUEST_TIMESTAMP]

[SIP_RESPONSE_TIMESTAMP]

AVP Flag

M

Time-Usage

Time-Usage.

AVP Header
2045 10415

Vendor ID
10415

VSA Type
2045

AVP Type
UINT32

Group Value
N/A

AVP Flag
M

TMGI

Contains the Temporary Mobile Group Identity allocated to a particular MBMS bearer service.

AVP Header
900 10415

Vendor ID
10415

VSA Type
900

AVP Type
OCTETSTRING

Group Value
N/A

AVP Flag
M

ToS-Traffic-Class

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

AVP Header
1014 10415

Vendor ID
10415

VSA Type

1014

AVP Type
OCTETSTRING

Group Value
N/A

AVP Flag
M

Trace-Collection-Entity

Trace-Collection-Entity.

AVP Header
1452 10415

Vendor ID
10415

VSA Type
1452

AVP Type
ADDRESS

Group Value
N/A

AVP Flag
M

Trace-Data

Trace data.

AVP Header
1458 10415

Vendor ID
10415

VSA Type
1458

AVP Type
GROUPED

Group Value
[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

Trace-Depth.

AVP Header
1462 10415

Vendor ID
10415

VSA Type
1462

AVP Type
ENUM

Group Value
N/A

AVP Flag
M

Trace-Depth-List

Trace depth list.

AVP Header
1460 10415

Vendor ID
10415

VSA Type
1460

AVP Type
GROUPED

Group Value
[TRACE_DEPTH_PER_NE_TYPE]

AVP Flag
M

Trace-Depth-Per-NE-Type

Trace-Depth-Per-NE-Type.

AVP Header
145110415

Vendor ID

10415

VSA Type
1451

AVP Type
GROUPED

Group Value
[NETWORK_ELEMENT_TYPE]

[TRACE_DEPTH]

AVP Flag
M

Trace-Event-List

Trace-Event-List.

AVP Header
1465 10415

Vendor ID
10415

VSA Type
1465

AVP Type
OCTETSTRING

Group Value
N/A

AVP Flag
M

Trace-Interface-List

Trace-Interface-List.

AVP Header
1464 10415

Vendor ID
10415

VSA Type
1464

AVP Type
OCTETSTRING

Group Value
N/A

AVP Flag
M

Trace-NE-Type-List

This AVP contains concat of MCC MNC.

AVP Header
1463 10415

Vendor ID
10415

VSA Type
1463

AVP Type
OCTETSTRING

Group Value
N/A

AVP Flag
M

Trace-NE-TypeList

Trace-NE-TypeList.

AVP Header
1461 10415

Vendor ID
10415

VSA Type
1461

AVP Type
OCTETSTRING

Group Value
N/A

AVP Flag
M

Trace-Reference

This AVP contains concat of MCC MNC.

AVP Header
1459 10415

Vendor ID
10415

VSA Type
1459

AVP Type
OCTETSTRING

Group Value
N/A

AVP Flag
M

Traffic-Data-Volumes

Traffic data volumes.

AVP Header
2046 10415

Vendor ID
10415

VSA Type
2046

AVP Type
GROUPED

Group Value
[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

Contains an integer used as an index pointing to a class of transport services to be applied.

AVP Header
311 13019

Vendor ID
13019

VSA Type
311

AVP Type
UNIT32

Group Value
N/A

AVP Flag
N/A

Trigger

Triggers in the client and to identify the triggers which caused re-authorization in usage.

AVP Header
1264 10415

Vendor ID
10415

VSA Type
1264

AVP Type
Grouped

Group Value
[Trigger-Type]

AVP Flag
M

Trunk-Group-ID

This grouped AVP identifies the incoming and outgoing PSTN legs.

AVP Header
851 10415

Vendor ID
10415

VSA Type
851

AVP Type
GROUPED

Group Value
[INCOMING_TRUNK_GROUP_ID]

[OUTGOING_TRUNK_GROUP_ID]

AVP Flag
M

TS-Code

TS code.

AVP Header
1487 10415

Vendor ID

10415

VSA Type
1487

AVP Type
OCTETSTRING

Group Value
N/A

AVP Flag
M

Tunnel-Assignment-Id

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

AVP Header
82 0

Vendor ID
0

VSA Type
82

AVP Type
OCTETSTRING

Group Value
N/A

AVP Flag
M

Tunnel-Client-Auth-Id

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

AVP Header
90 0

Vendor ID
0

VSA Type
90

AVP Type
UTF8STRING

Group Value
N/A

AVP Flag
M

Tunnel-Client-Endpoint

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

AVP Header
66 0

Vendor ID
0

VSA Type
66

AVP Type
UTF8STRING

Group Value
N/A

AVP Flag
M

Tunnel-Header-Filter

Tunnel Header Filter.

AVP Header
1036 10415

Vendor ID
10415

VSA Type
1036

AVP Type
IPFILTERRULE

Group Value
N/A

AVP Flag
M

Tunnel-Header-Length

Tunnel Header Length.

AVP Header
1037 10415

Vendor ID
10415

VSA Type
1037

AVP Type
UINT32

Group Value
N/A

AVP Flag
M

Tunnel-Information

Tunnel Information.

AVP Header
1038 10415

Vendor ID
10415

VSA Type
1038

AVP Type
GROUPED

Group Value
[TUNNEL_HEADER_LENGTH]

[TUNNEL_HEADER_FILTER]

AVP Flag
M

Tunneling

Used to describe a compulsory tunnel service.

AVP Header
401 0

Vendor ID
0

VSA Type
401

AVP Type
GROUPED

Group Value
[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

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.

AVP Header
65 0

Vendor ID
0

VSA Type
65

AVP Type
ENUM. Supported values are:

IPv4_IPversion4 (1)

IPv6_IPversion6 (2)

NSAP (3)

HDLC-8-bit_multidrop (4)

BBN-1822 (5)

802-includes-all-802-media-plus-Ethernet-canonical_format (6)

E163_POTS (7)

E164_SMDS_Frame-Relay_ATM (8)

F69_Telex (9)

X121_X25_Frame-Relay (10)

IPX (11)

Appletalk (12)

Decnet_IV (13)

Banyan_Vines (14)

E164-with-NSAP-format-subaddress (15)

Group Value
N/A

AVP Flag
M

Tunnel-Password

This AVP contains a password to be used to authenticate to a remote server.

AVP Header
69 0

Vendor ID
0

VSA Type
69

AVP Type
OCTETSTRING

Group Value
N/A

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-AVP AVPs.

AVP Header
83 0

Vendor ID
0

VSA Type
83

AVP Type
UINT32

Group Value
N/A

AVP Flag
M

Tunnel-Private-Group-Id

This AVP contains the group ID for a particular tunneled session.

AVP Header
81 0

Vendor ID
0

VSA Type
81

AVP Type

OCTETSTRING

Group Value
N/A

AVP Flag
M

Tunnel-Server-Auth-Id

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

AVP Header
91 0

Vendor ID
0

VSA Type
91

AVP Type
UTF8STRING

Group Value
N/A

AVP Flag
M

Tunnel-Server-Endpoint

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

AVP Header
67 0

Vendor ID
0

VSA Type
67

AVP Type
UTF8STRING

Group Value
N/A

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).

AVP Header
64 0

Vendor ID
0

VSA Type
64

AVP Type
ENUM. Supported values are:

Point-to-Point_Tunneling_Protocol-PPTP (1)

Layer-Two-Forwarding_L2F (2)

Layer-Two-Tunneling_Protocol-L2TP (3)

Ascend-Tunnel-Management-Protocol-ATMP (4)

Virtual-Tunneling-Protocol-VTP (5)

IP-Authentication-Header-in-the-Tunnel-mode_AH (6)

IP-in-IP_Encapsulation_IP-IP (7)

Minimal_IP-in-IP_Encapsulation_MIN-IP-IP (8)

IP_Encapsulating_Security_Payload_in_the_Tunnel-mode_ESP (9)

Generic_Route_Encapsulation_GRE (10)

Bay_Dial_Virtual_Services-DVS (11)

IP-in-IP-Tunneling (12)

Virtual-LANs-VLAN (13)

Group Value
N/A

AVP Flag
M

UAR-Flags

Contains a bit mask, if the bit 0 is set, it indicates that the request corresponds to an IMS Emergency Registration.

AVP Header
637 0

Vendor ID
0

VSA Type
637

AVP Type
UINT32

Group Value
N/A

AVP Flag
M

ULA-Flags

The ULR-Flags AVP is of type Unsigned32 and it contains a bit mask.

AVP Header
6007 10415

Vendor ID
10415

VSA Type
6007

AVP Type
UINT32

Group Value
N/A

AVP Flag
M

ULR-Flags

The ULR-Flags AVP is of type Unsigned32 and it contains a bit mask.

AVP Header
6006 10415

Vendor ID
10415

VSA Type
6006

AVP Type
UINT32

Group Value
N/A

AVP Flag
M

UMTS-Vector

UMTS-Vector.

AVP Header
6018 10415

Vendor ID
10415

VSA Type
6018

AVP Type
GROUPED

Group Value
[ITEM_NUMBER]
[RAND]
[XRES]
[AUTN]
[CONFIDENTIALITY_KEY]
[INTEGRITY_KEY]

AVP Flag
M

Unit-Value

Cost estimate (type of money) of the service.

AVP Header
445 0

Vendor ID
0

VSA Type
445

AVP Type
Grouped

Group Value
[VALUE_DIGITS]
[EXPONENT]

AVP Flag
M

Used-Service-Unit

The used service unit measured from the point when service is active.

AVP Header
446 0

Vendor ID
0

VSA Type
446

AVP Type
Grouped

Group Value
[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.

AVP Header
623 10415

Vendor ID
10415

VSA Type
623

AVP Type
ENUM. Supported values are:

REGISTRATION (0)

DE_REGISTRATION (1)

REGISTRATION_AND_CAPABILITIES (2)

Group Value
N/A

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.

AVP Header
702 0

Vendor ID
0

VSA Type
702

AVP Type
OCTETSTRING

Group Value

N/A

AVP Flag
M

User-Data-Already-Available

Indicates whether S-CSCF is already storing the user data or not.

AVP Header
624 10415

Vendor ID
10415

VSA Type
624

AVP Type
ENUM. Supported values are:

USER_DATA_NOT_AVAILABLE (0)

USER_DATA_ALREADY_AVAILABLE (1)

Group Value
N/A

AVP Flag
M

User-Equipment-Info

Indicate the identification and capabilities of the terminal.

AVP Header
458 0

Vendor ID
0

VSA Type
458

AVP Type
GROUPED

Group Value
[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.

AVP Header
459 0

Vendor ID
0

VSA Type
459

AVP Type
ENUM. Supported values are:

IMEISV (0)

MAC (1)

EUI64 (2)

MODIFIED_EUI64 (3)

ESN (4)

MEID (5)

Group Value
N/A

AVP Flag
M

User-Equipment-Info-Value

Defines the type of identifier used.

AVP Header
460 0

Vendor ID
0

VSA Type
460

AVP Type
OCTETSTRING

Group Value
N/A

AVP Flag
M

User-Id

User ID.

AVP Header
1444 10415

Vendor ID
10415

VSA Type
1444

AVP Type
UTF8STRING

Group Value
N/A

AVP Flag
M

User-Identity

This grouped AVP contains either a Public-Identity AVP or an MSISDN AVP.

AVP Header
700 10415

Vendor ID
10415

VSA Type
700

AVP Type
GROUPED

Group Value
[PUBLIC_IDENTITY]

[MSISDN]

AVP Flag
M

User-Name

Identification of the service user in a format consistent with the NAI specification.

AVP Header
1 0

Vendor ID
0

VSA Type
1

AVP Type
UTF8STRING

Group Value
N/A

AVP Flag
M

User-Session-Id

This AVP holds the session identifier.

AVP Header
830 10415

Vendor ID
10415

VSA Type
830

AVP Type
UTF8STRING

Group Value
N/A

AVP Flag
M

UTRAN-Vector

UTRAN-vector.

AVP Header
1415 10415

Vendor ID
10415

VSA Type
1415

AVP Type
GROUPED

Group Value
[ITEM_NUMBER]

[RAND]

[XRES]

[AUTN]

[CONFIDENTIALITY_KEY]

[INTEGRITY_KEY]

AVP Flag
M

V4-Transport-Address

Contains a single IPv4 address and a single port number.

AVP Header
454 13019

Vendor ID
13019

VSA Type
454

AVP Type
GROUPED

Group Value
[FRAMED_IP_ADDRESS]

[PORT_NUMBER]

AVP Flag
N/A

V6-Transport-Address

Contains a single IPv6 address and a single port number.

AVP Header
453 13019

Vendor ID
13019

VSA Type
453

AVP Type
GROUPED

Group Value
[FRAMED_IPV6_PREFIX]

[PORT_NUMBER]

AVP Flag
N/A

Validity-Time

Validity time of the granted service units. Measurement starts upon receipt of the Credit-Control-Answer Message containing this AVP.

AVP Header
448 0

Vendor ID
0

VSA Type
448

AVP Type
UINT32

Group Value
N/A

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.

AVP Header
447 0

Vendor ID
0

VSA Type
447

AVP Type
INT64

Group Value
N/A

AVP Flag
M

VBM-Address

VBM Address.

AVP Header
1460 10415

Vendor ID
10415

VSA Type
1460

AVP Type
ADDRESS

Group Value
N/A

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.

AVP Header
266 0

Vendor ID

0

VSA Type
266

AVP Type
UINT32

Group Value
N/A

AVP Flag
M

Vendor-Id-Resp

Unique identifier of the vendor.

AVP Header
266 10415

Vendor ID
10415

VSA Type
266

AVP Type
UINT32

Group Value
N/A

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.

AVP Header
260 0

Vendor ID
0

VSA Type
260

AVP Type
GROUPED

Group Value
[VENDOR_ID]

[AUTH_APPLICATION_ID]

[ACCT_APPLICATION_ID]

AVP Flag

M

Vendor-Specific-QoS-Profile-Template

Vendor-Specific-QoS-Profile-Template.

AVP Header
6064 0

Vendor ID
0

VSA Type
3GPP2-BSID
6064

AVP Type
GROUPED

Group Value
[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 (e.g. the visited network domain name).

AVP Header
600 10415

Vendor ID
10415

VSA Type
600

AVP Type
OCTETSTRING

Group Value
N/A

AVP Flag
M

Visited-PLMN-Id

Contains concatenation of MCC and MNC.

AVP Header
6008 10415

Vendor ID
10415

VSA Type
6008

AVP Type
UTF8STRING

Group Value
N/A

AVP Flag
M

VOA-Session-ID

VOA-Session-ID.

AVP Header
1464 10415

Vendor ID
10415

VSA Type
1464

AVP Type
UTF8STRING

Group Value
N/A

AVP Flag
M

VPLMN-Dynamic-Address-Allowed

VPLMN-Dynamic-Address-Allowed.

AVP Header
1432 10415

Vendor ID
10415

VSA Type
1432

AVP Type
ENUM. Supported values are:

NOTALLOWED (0)

ALLOWED (1)

Group Value
N/A

AVP Flag
M

Wildcarded-PSI

This AVP contains a wild-carded PSI stored in the HSS.

AVP Header
634 10415

Vendor ID
10415

VSA Type
634

AVP Type
UTF8STRING

Group Value
N/A

AVP Flag
M

XRES

This AVP contains the XRES.

AVP Header
1448 10415

Vendor ID
10415

VSA Type
1448

AVP Type
OCTETSTRING

Group Value
N/A

AVP Flag
M

Chapter 6
RADIUS Attribute Definitions

This chapter presents RADIUS attribute definitions.

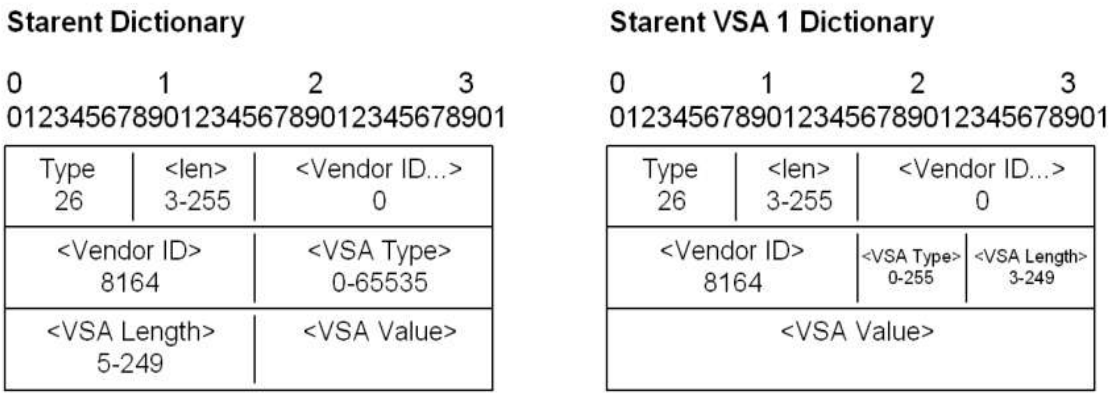
Dictionary Types

The CLI command to specify the dictionary is:

```
radius dictionary [ 3gpp | 3gpp2 | 3gpp2-835 | customX | 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). Refer to the *Enhanced Charging Service Configuration and Reference Guide* for more information.
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.
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.
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 2. Difference in VSA Value Lengths per Dictionary



Important: Customer-specific attributes are not documented in this reference. For information on customer-specific attributes, please contact your local service 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).

Attributes

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-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).

Type
26

Vendor ID
10415

VSA Type
13

Length
4

Value
Opaque value

3GPP-GGSN-Address

This attribute contains IP address of the GGSN.

Type
26

Vendor ID
10415

VSA Type
7

Length
4

Value
IPv4 address

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.

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-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.

Type
26

Vendor ID
10415

VSA Type
5

Length
1–35

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.

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 four 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 and specifies the IPv4 Source Address and Netmask if the direction is Downlink or Destination Address & Netmask if the direction is Downlink or Destination Address & Netmask if the direction is Uplink.

Type

5

Length

8

Value

Contains the following two subattributes:

Address

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

Contains netmask of the IPv4 address

Type

2

Length

4

Value

IPv4 address

IPv6-Address-Type

This is a compound attribute and specifies 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

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

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 IP address of the SGSN.

Type
26

Vendor ID
10415

VSA Type
6

Length
4

Value
IPv4 address

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.

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
8

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 amount 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 values are:

- 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

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.

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.

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-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 DSN update
- Yes = 1 — HA needs to send DNS update

3GPP2-ESN

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-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.

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
- 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

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-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.

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 and is the future replacement for ESN.

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-Reverse-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:

- Not Required = 0
- Required = 1

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.

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 values are:

- 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

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-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

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

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

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

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. Possible values are:

- HSPD = 0x21
- HRPD = 0x3b
- LLAROHC = 0x3d
- HRPD-AUX = 0x40
- HRPD-AUX-IP = 0x43

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 values are:

- 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

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

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.

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.

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

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.

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.

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.

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

BU-CoA-Ipv6

CoA from the BU message.

Type
26

Vendor ID
24757

VSA Type
51

Length
16

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.

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 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.

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.

Type
55

Vendor ID
N/A

VSA Type
N/A

Length
4

Value
Unsigned integer

FA-RK-KEY

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 associated with FA-RK.

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. 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>

Type
11

Vendor ID
N/A

VSA Type
N/A

Length
1–32

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.

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.

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 value of 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.

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 contains the IP route to be installed specific to this session.

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

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

SPI associated with HA-RK.

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

Hotline-Profile-ID

A unique identifier of a hotline profile to be applied to the session.

Type
26

Vendor ID
24757

VSA Type
53

Length
1–246

Value
Opaque value

Hotline-Session-Timer

The time period, in seconds, the session can remain hotlined.

Type
26

Vendor ID
24757

VSA Type
56

Length
4

Value
Unsigned Integer

HTTP-Redirection-Rule

An HTTP redirection rule.

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 this 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

An IP redirection rule.

Type
26

Vendor ID
24757

VSA Type
55

Length
1–246

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.

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.

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
58

Length
1–246

Value
Opaque value

PMIP6-RK-KEY

PMIP6-RK-KEY

Type
26

Vendor ID
24757

VSA Type
131

Length
1–251

Value

Opaque value

PMIP6-RK-SPI

PMIP6-RK-SPI

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. Possible 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

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).

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

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

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-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.

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 value.

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

Content Filtering policy ID.

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 holds 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-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.

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

SN-DNS-Proxy-Intercept-List

DNS proxy list.

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

SN-Dynamic-Addr-Alloc-Ind-Flag.

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 value.

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

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-Home-Behavior

Configuration for the behavior bits settings for a home subscriber in an APN

Type
26

Vendor ID
8164

VSA Type
119

Length
4

Value
Unsigned integer

SN-Home-Profile

Configuration for the profile bits settings for a subscriber in an APN

Type
26

Vendor ID
8164

VSA Type
109

Length
4

Value
Unsigned integer

SN-Home-Sub-Use-GGSN

Configures GGSN to accept GGSN's charging characteristics for home subscribers defined for the APN, if the subscriber is home.

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
275

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

IP input filter rules.

Type
26

Vendor ID
8164

VSA Type
10

Length
1–253

Value
String

SN-IP-Filter-Out

IP output filter.

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

When enabled, This attribute excludes the Source Violated IP packets and byte counts when reporting the Octet and Packet count in an accounting message.

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 response to the GGSN until a response for the accounting start message is received from the Mediation Accounting server.

Type
Type 26

Vendor ID
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

Mediation Accounting Enabled or Disabled settings for GGSN

Type
26

Vendor ID
8164

VSA Type
123

Length
2

Value
Enumerated integer. Supported values are:

- Disabled = 0
- Enabled = 1

SN-Mediation-No-Interims

Disable or Enable mediation Interim records for this session.

Type
26

Vendor ID
8164

VSA Type
146

Length
4

Value
Enumerated integer. Supported values are:

- Disabled = 0
- Enabled = 1

SN-Mediation-VPN-Name

Mediation context name.

Type
26

Vendor ID
8164

VSA Type
104

Length
1–128

Value
String

SN-Min-Compress-Size

This attribute indicates 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

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

SN-MIP-Send-Correlation-Info

AAA Attribute to enable/disable 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-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.

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 values are:

- 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

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-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-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

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.

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

SN-Primary-DCCA-Peer

This attribute indicates the name of the primary DCCA peer and primary DCCA realm.

Type
26

Vendor ID
8164

VSA Type
223

Length
2

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-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.

Type
26

Vendor ID
8164

VSA Type
303

Length
1–35

Value
Opaque

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

4-17

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.

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.

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.

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.

SN-Rad-APN-Name

RADIUS returned APN name.

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 username 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

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

Configuration for the behavior bits settings for a roaming subscriber in an APN.

Type
26

Vendor ID
8164

VSA Type
121

Length
4

Value
Unsigned integer

SN-Roaming-Profile

Configuration for the profile bits settings for a roaming subscriber in an APN.

Type
26

Vendor ID
8164

VSA Type
118

Length
4

Value
Unsigned integer

SN-Roaming-Sub-Use-GGSN

Configures GGSN to accept GGSN's charging characteristics for roaming subscribers defined for the APN, if the subscriber is roaming.

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.

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.

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 the 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

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 indicates the accounting method to be used for subscriber sessions.

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.

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 displays the SN 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.

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.

Type
26

Vendor ID
8164

VSA Type
71

Length
4

Value
Enumerated integer. Supported values are:

- Normal = 0
- Suppress = 1

SN-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

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.

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 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

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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-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

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 indicates the virtual APN name.

Type
26

Vendor ID
8164

VSA Type
94

Length
1–64

Value
ASCII string

SN-Visiting-Behavior

Configuration for the behavior bits settings for a visiting subscriber in an APN.

Type
26

Vendor ID
8164

VSA Type
120

Length
4

Value
Unsigned integer

SN-Visiting-Profile

Configuration for the profile bits settings for a visiting subscriber in an APN.

Type
26

Vendor ID
8164

VSA Type

117

Length
4

Value
Unsigned integer

SN-Visiting-Sub-Use-GGSN

Configures GGSN to accept GGSN's charging characteristics for visiting subscribers defined for the APN, if the subscriber is visiting.

Type
26

Vendor ID
8164

VSA Type
107

Length
2

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 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

SN-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

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

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

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

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

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

Contains the number of output bytes dropped.

Type
26

Vendor ID
8164

VSA Type
229

Length
4

Value
Integer

SN1-Acct-Output-Packets-Dropped

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

Content Filtering policy ID.

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 indicates 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 indicates the reason the user was disconnected from service.

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

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.

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 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

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

SN1-Home-Behavior

SN1-Home-Behavior

Type
26

Vendor ID
8164

VSA Type
119

Length
4

Value
Unsigned integer

SN1-Home-Profile

SN1-Home-Profile

Type
26

Vendor ID
8164

VSA Type
109

Length
4

Value
Unsigned integer

SN1-Home-Sub-Use-GGSN

GGSN

Type
26

Vendor ID
8164

VSA Type
106

Length
2

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
275

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 indicates 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

When enabled, This attribute excludes the Source Violated IP packets and byte counts when reporting the Octet and Packet count in an accounting message.

Type
26

Vendor ID
8164

VSA Type
196

Length
2

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 indicates 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 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

SN1-IPv6-Sec-Pool

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 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

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 response to the GGSN until a response for the accounting start message is received from the Mediation Accounting server.

Type
Type 26

Vendor ID
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

Mediation Accounting Enabled or Disabled settings for GGSN.

Type

26

Vendor ID

8164

VSA Type

123

Length

4

Value

Enumerated integer. Supported values are:

- Disabled = 0
- Enabled = 1

SN1-Mediation-No-Interims

Mediation no interims.

Type

26

Vendor ID

8164

VSA Type

146

Length

4

Value

Enumerated integer. Supported values are:

- Disabled = 0
- Enabled = 1

SN1-Mediation-VPN-Name

Mediation context name.

Type
26

Vendor ID
8164

VSA Type
104

Length
1–128

Value
String

SN1-Min-Compress-Size

This attribute indicates 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

AAA Attribute to enable/disable 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 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

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

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.

Type
26

Vendor ID
8164

VSA Type
246

Length
Compound

Value
Contains the following subattributes:

Framed-IP-Address

Framed IP address.

Type

1

Length

4

Value

IPv4 address

NAT-IP-Address

NAT IP address.

Type

2

Length

4

Value

IPv4 address

NAT-Port-Block-Start

Start port of the port chunk

Type

3

Length

2

Value

Unsigned integer

NAT-Port-Block-End

End port of the port chunk.

Type

4

Length

2

Value

Unsigned integer

Acct-Session-Id

Accounting Session ID.

Type

5

Length
1–17

Value
String

User-Name

User name.

Type
6

Length
1–128

Value
String

Correlation-Id

Correlation ID.

Type
7

Length
1–17

Value
String

SN1-NAT-IP-Address

This attribute includes the NAT (public) IP address used for the call.

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

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 values are:

- 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 values are:

- 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

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-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-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

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.

Type
26

Vendor ID
8164

VSA Type
135

Length
2

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.

Type
26

Vendor ID
8164

VSA Type
223

Length
1

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
4-17

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.

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.

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.

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.

SN1-Rad-APN-Name

RADIUS returned APN name.

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-Profile

SN1-Roaming-Profile

Type
26

Vendor ID
8164

VSA Type
118

Length
4

Value
Unsigned integer

SN1-Roaming-Behavior

SN1-Roaming-Behavior

Type
26

Vendor ID
8164

VSA Type
121

Length
4

Value
Unsigned integer

SN1-Roaming-Sub-Use-GGSN

SN1-Roaming-Sub-Use-GGSN

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.

Type
26

Vendor ID
8164

VSA Type
249

Length

1–64

Value

ASCII string

SN1-Secondary-DCCA-Peer

This attribute indicates the name of the Secondary DCCA peer and Secondary DCCA realm.

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

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.

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.

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.

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.

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

Subscriber No Interims.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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

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

SN1-Visiting-Behavior

Type
26

Vendor ID
8164

VSA Type
120

Length
4

Value
Unsigned integer

SN1-Visiting-Profile

Visiting Profile.

Type
26

Vendor ID
8164

VSA Type
117

Length
4

Value
Unsigned integer

SN1-Visiting-Sub-Use-GGSN

Accept Visiting.

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. Please 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.

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

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 amount 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

WiMAX beginning of session.

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

Describes hotline capabilities supported.

Type
3

Length
1

Value
0x00 = Hot lining is not Supported

- 0x01 = Profile-based Hot lining is supported (using Hotline-Profile-ID VSA)
- 0x02 = Rule-based Hot lining is supported using NAS-Filter-Rule
- 0x04 = Hot lining HTTP Redirection is supported.
- 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.

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

WiMAX-Home-HNP-PMIP6

Type
26

Vendor ID
24757

VSA Type
133

Length
2–18

Value
Opaque value

WiMAX-Home-IPv4-HoA-PMIP6

WiMAX-Home-IPv4-HoA-PMIP6

Type
26

Vendor ID
24757

VSA Type
135

Length

4

Value

IPv4 Address

WiMAX-Hotline-Indicator

WiMAX-Hotline-Indicator

Type

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

Type

26

Vendor ID

24757

VSA Type

24

Length

1–246

Value

Opaque value

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 accounting 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
- Activate = 0x04
- Dynamic = 0x08

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.

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

Enumerated integer. Supported values are:

- ICMP = 1
- TCP = 6
- UDP = 17

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

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

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.

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.

Type
1

Length
1-4

Value
Opaque value

Volume-Quota

Indicates the volume in octets excluding control data.

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.

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.

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.

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.

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

Termination-Action

Describes action to take when PPS does not grant additional quota.

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-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.

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: 4; in StarOS 10.0 and later: 1

Value

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

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

Opaque 1 byte value received from customer RADIUS server in access request. Used in custom dictionary.

Type
136

Vendor ID
5535 (Reusing the 3GPP2 VID in a non-standard way.)

VSA Type
205

Length
1 byte value.

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 7
G-CDR and Enhanced G-CDR Field Reference Tables

This chapter provides reference tables for the CDR fields reported as part of GGSN-CDRs (G-CDRs) and enhanced G-CDRs (eG-CDRs) generated by the system.

A complete list of supported CDR fields is provided in the *G-CDR and Enhanced G-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. The use of GTPP dictionaries is configurable using the **`gtpp dictionary`** command in the Context Configuration Mode of the system's Command Line Interface (CLI).

This section provides information on the fields reported in G-CDRs/eG-CDRs for the GTPP dictionaries.

Important: For more information on custom dictionaries, contact your local service representative.

The category column in all tables use keys described in the following table.

Table 1. 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.
O	Operator Provisionable: Mandatory	A field that an operator has provisioned and must be included in the CDR for all conditions.
O	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 for 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.

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.
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 for 3GPP TS 32.298 V6.6.0 (2006-12) (R6).

Field	Category	Description
Record Type	M	GGSN 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 IMEISV	O	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	O	The logical name of the connected access point to the external packet data network (network identifier part of APN).

Field	Category	Description
PDP Type	O	PDP type, i.e. IP, PPP, or IHOSS:OSP.
Served PDP Address	O	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	O	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	O	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	O	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	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 operator/manufacturer specific extensions to the record. Conditioned upon the existence of an extension.
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.
User Location Information	O	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	O	Holds information about how Charging Characteristics were selected.
IMS Signalling Context	O	Included if the IM-CN Subsystem Signalling Flag is set, TS 23.060 PDP context is used for IMS signalling.
External Charging Identifier	O	Holds a Charging Identifier and is present only if it is received from a non-GPRS, external network entity.
SGSN PLMN Identifier	O	SGSN PLMN Identifier (MCC and MNC) used during this record.

Field	Category	Description
CAMEL Information	O	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	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.

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 – custom30 Dictionaries

G-CDR fields for 3GPP TS 32.215 V4.6.0 (2003-12) (R4).

Field	Category	Description
Record Type	M	GGSN 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.
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	O	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, or IHOSS:OSP
Served PDP Address	O	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	O	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	O	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.

Field	Category	Description
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	O	Name of the recording entity.
Record Extensions	O	A set of network operator/manufacturer specific extensions to the record. Conditioned upon the existence of an extension.
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 applied to the PDP context.
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.

custom16 Dictionary

G-CDR fields for 3GPP TS 32.215 V4.5.0 (2003-09) (R4).

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.
List of SGSN 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 Address	M	The control plane IP address of the GGSN currently used. The GGSN address is always the same for an activated PDP context.

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).
Dynamic Address Flag	M	The flag indicating that the PDP address has been dynamically allocated.
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.
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 categorise traffic volumes, such as per QoS/tariff period. Initial and subsequently changed QoS and corresponding data volumes are listed (Only QOS negotiated is present).
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.
Diagnostics	O	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.
Node ID	M	Name of the recording entity.
Local Record Sequence Number	M	Consecutive record number created by this node. The number is allocated sequentially including all CDR types.
Time Zone	M	Customer-specific. The difference between UTC and local time for the change time.
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 PDP context.
Charging Characteristics Selection Mode	M	Holds information about how charging characteristics were selected.
SGSN PLMN identifier	M	PLMN ID of the SGSN.
Charging Type Selection Mode	M	The field indicating how the charging type field was selected.
Charging Profile	M	Customer-specific. The field indicates the user profile. The possible values are: • prepaid • post-paid • HLR

Field	Category	Description
Charging Type	M	Customer-specific. The field indicates the type of the G-CDR generated. The possible values are: • normal record • prepaid record • hot billing record • Flat billing
access type	M	Customer-specific. The field indicates the user's access type.

Notes:

- 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.

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.

Field	Category	Description
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.

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.

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 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.
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.
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.

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.
- 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.

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 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.
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	O	A flag that is present if this is a network-initiated PDP context.
Served IMSI	M	IMSI of the served party.
Served IMEISV	O	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	O	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, or IHOSS:OSP.
Served PDP Address	O	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	O	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	O	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	O	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	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.
User Location Information	O	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.

Field	Category	Description
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.
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.
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:

- 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 Identifier *NOT* included in LOSDV.
- Service change condition is encoded as 32 bits.

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 e-GCDRs)	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.

List of Service Data Volumes		
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 radio access technology type during the service data recording interval.
Failurehandling Continue (only in e-GCDRs)	O	A Boolean expression included if the failure handling condition has been executed.

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	O	A flag that is present if this is a network-initiated PDP context.
Served IMSI	M	IMSI of the served party.
Served IMEISV	O	IMEISV of the ME, if available.
GGSN Address	M	The control plane IP address of the GGSN used.

Field	Category	Description
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	O	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, or IHOSS:OSP.
Served PDP Address	O	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	O	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	O	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	O	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	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.
User Location Information	O	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	O	Holds information about how Charging Characteristics were selected.
SGSN PLMN Identifier	O	SGSN PLMN Identifier (MCC and MNC) used during this record.
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.
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:

- 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.
Failurehandling Continue (only in e-GCDRs)	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.

Field	Category	Description
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.
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	O	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	O	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, or IHOSS:OSP.
Served PDP Address	O	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	O	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	O	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	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	M	The Charging Characteristics applied to the PDP context.

Field	Category	Description
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.

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 e-GCDRs)	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-CDR-S 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	O	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

S-CDR fields for 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	O	IMEI of the ME, if available in the SGSN.
SGSN Address	M	The control plane IP address of the SGSN used.

Field	Category	Description
MS Network Capability	O	MS network capability value of the MS network capability information element of the served MS on PDP context activation
Routing Area	O	Contains the RA code of the area where the MS is located when the (partial) record is opened.
Location Area Code	O	Contains the Location Area Code of the area where the MS is located when the (partial) record is opened.
Cell Identifier	O	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	O	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, or IHOSS:OSP.
Served PDP Address	O	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	O	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	O	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	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.
Local Record Sequence Number	O	Consecutive record number created by this node. The number is allocated sequentially including all CDR types.
APN Selection Mode Index	O	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	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.
System Type	O	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.

Field	Category	Description
CAMEL Information	O	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.
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.
PLMN Identifier	O	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.

Chapter 8
G-CDR and Enhanced G-CDR Field Descriptions

This chapter lists and describes the fields supported by the system for use in GGSN charging data records (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 *G-CDR and Enhanced G-CDR Field Reference Tables* 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

Record Type

Indicates the GGSN PDP context record type. From the GGSN, this will be G-CDR.

Format
Integer

Length
1–4 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

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

GGSN Address

The binary-represented IPv4 address of the GGSN used.

Format
Hex value octet string

Length
4 bytes

Charging ID

The GGSN-generated value used to identify this PDP context.

Format

Unsigned integer

Length
1-4 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

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

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

Served PDP Address

The binary-represented IPv4 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 per address

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

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

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 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.
- 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 Seq 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".
- 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: 1-16 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: 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.

Record Opening Time

The timestamp at which the PDP context was activated on the GGSN.

Format

BCD encoded octet string.

Length

9 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
1–5 bytes.

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.

Format
Unsigned integer.

Length
1 byte.

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
1–5 bytes.

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
1–20 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.

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.

Served MSISDN

The Mobile Station (MS) ISDN number (MSISDN) of the subscriber.

Format
BCD encoded octet string.

Length
1–9 bytes.

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.

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 in GCDRs but not for E-GCDRs. 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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

Format
Octet string.

Chapter 9
SGSN and Mobility Management Charging Detail Record Field Reference Tables

The SGSN provides CDRs that are compliant to the definitions in 3GPP TS32.298. 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.

The use of GTPP dictionaries is configurable using the **`gtpp dictionary`** command in the Context Configuration Mode of the system's Command Line Interface (CLI).

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.

Important: For more information on custom dictionaries, contact your local service representative.

The category column in all tables use keys described in the following table.

Table 2. 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.
O	Operator Provisionable: Mandatory	A field that an operator has provisioned and must be included in the CDR for all conditions.
O	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 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, custom14 – custom16, custom19 – custom22, custom24 – 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	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	O	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	O	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	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	O	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.

Field	Category	Description
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	O	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	O	Name of the recording entity.
Record Extensions	O	A set of network operator/manufacturer specific extensions to the record. Conditioned upon the existence of an extension.
Record Extensions	O	A set of network operator/manufacturer specific extensions to the record. Conditioned upon the existence of an extension.
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.
Access Point Name Operator Identifier	O	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.
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.
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.

custom3 Dictionary

S-CDR fields for 32.215 v 4.5.0 (R4).

Field	Category	Description
Record Type	M	SGSN PDP context record.

Field	Category	Description
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	O	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	O	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	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	O	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	O	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	O	Name of the recording entity.
Record Extensions	O	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	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	O	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.
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.
Charging Characteristics Selection Mode	O	Holds information about how Charging Characteristics were selected.
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 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	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	O	The IP address of the current SGSN.

Field	Category	Description
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	O	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	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	O	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	O	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	O	Name of the recording entity.
Record Extensions	O	A set of network operator/manufacturer specific extensions to the record. Conditioned upon the existence of an extension.
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.
Access Point Name Operator Identifier	O	The Operator Identifier part of the APN.
Served MSISDN	O	The primary MSISDN of the subscriber.

Field	Category	Description
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	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.

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	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	O	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	O	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	O	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	O	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	O	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	O	Name of the recording entity.
Record Extensions	O	A set of network operator/manufacturer specific extensions to the record. Conditioned upon the existence of an extension.
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.
Access Point Name Operator Identifier	O	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	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.

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	O	The IMEI of the ME, if available.
SGSN Address	O	The IP address of the current SGSN.
MS Network Capability	O	The mobile station Network Capability.
MS Radio Access Capability	O	The mobile station Radio Access 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	O	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	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	O	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	O	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	O	Name of the recording entity
Record Extensions	O	A set of network operator/manufacturer specific extensions to the record. Conditioned upon the existence of an extension.
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.
Access Point Name Operator Identifier	O	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.
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.
CAMEL Information	O	Set of CAMEL information related to PDP context. For more information see Description of Record Fields. This field is present if CAMEL service is activated.
Prepaid Info	O	This identifier refers to the network address (E.164 number) of the pre-paid system.
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.

Notes:

- Two new optional fields - MS Radio Access capability and Prepaid-Info. These attributes are currently not supported.
- 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	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	O	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	O	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	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	O	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	O	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	O	Name of the recording entity.
Record Extensions	O	A set of network operator/manufacturer specific extensions to the record. Conditioned upon the existence of an extension.
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.
Access Point Name Operator Identifier	O	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	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.

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).

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

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).
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 Organisation field and a Number field. The PDP Type Organisation is the organisation 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.

Field	Category	Description
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.
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.

Field	Category	Description
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		
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.

Field	Category	Description
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.
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	O	IMEI of the ME, if available.
Served MSISDN	O	The primary MSISDN of the subscriber.
SGSN Address	O	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	O	An index indicating how the APN was selected.
PDP Type	O	PDP type, i.e. IP, PPP, or IHOSS:OSP.
Served PDP Address	O	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	O	Holds information about how Charging Characteristics were selected.
Dynamic Address Flag	O	The presence of this field indicates that the Served PDP Address was dynamically assigned during context activation.
MS Network Capability	O	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	O	Indicates the type of air interface used, e.g. UTRAN. This field ispresent when either the UTRAN or GERAN air-interface is used. It isomitted when the service is provided by a GSM air interface.

Field	Category	Description
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)	O	Contains the RA code of the area where the MS is located when the (partial) record is opened.
Location Area Code	O	Contains the Location Area Code of the area where the MS is located when the (partial) record is opened.
Cell Identifier	O	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 table.

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	O	The IMEI of the ME, if available.
Served MSISDN	O	The primary MSISDN of the subscriber.
MS Network Capability	O	The mobile station network capability.
Service Centre	O	The address (E.164) of the SMS-service centre.
Recording Entity	O	The E.164 number of the SGSN.
Location Area Code	O	The Location Area Code from which the message originated.
Routing Area Code	O	The Routing Area Code from which the message originated.
Cell Identifier	O	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	O	A set of network operator/ manufacturer specific extensions to the record. Conditioned upon the existence of an extension.
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	M	The Charging Characteristics flag set used by the SGSN.
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.
Destination Number	O	The destination short message subscriber number.
Charging Characteristics Selection Mode	O	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	O	The IMEI of the ME, if available.
Served MSISDN	O	The primary MSISDN of the subscriber.
MS Network Capability	O	The mobile station network capability.
Service Centre	O	The address (E.164) of the SMS-service centre.
Recording Entity	O	The E.164 number of the SGSN.
Location Area Code	O	The Location Area Code to which the message was delivered.
Routing Area Code	O	The Routing Area Code to which the message was delivered.
Cell Identifier	O	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	O	A set of network operator/manufacturer specific extensions to the record. Conditioned upon the existence of an extension.
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	M	The Charging Characteristics flag set used by the SGSN.
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.
Charging Characteristics Selection Mode	O	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	O	The IMEI of the ME, if available.
SGSN Address	O	The IP address of the current SGSN.
MS Network Capability	O	The mobile station network capability.
Routing Area Code	O	Routing Area at the time of the Record Opening Time.
Local Area Code	O	Location Area Code at the time of Record Opening Time.
Cell Identifier	O	The Cell Identity for GSM or Service Area Code (SAC) for UMTS at the time of the Record Opening Time.
Change of Location	O	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	O	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	O	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	O	Name of the recording entity.
Record Extensions	O	A set of network operator/manufacturer specific extensions to the record. Conditioned upon the existence of an extension.
Local Record Sequence Number	O	Consecutive record number created by this node. The number is allocated sequentially including all CDR types.
Served MSISDN	O	The primary MSISDN of the subscriber.

Field	Category	Description
Charging Characteristics	M	The Charging Characteristics used by the SGSN.
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.
Charging Characteristics Selection Mode	O	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	O	The IMEI of the ME, if available.
SGSN Address	O	The IP address of the current SGSN.
MS Network Capability	O	The mobile station network capability.
Routing Area Code	O	Routing Area at the time of the Record Opening Time.
Local Area Code	O	Location Area Code at the time of Record Opening Time.
Cell Identifier	O	The Cell Identity for GSM or Service Area Code (SAC) for UMTS at the time of the Record Opening Time.
Change of Location	O	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	O	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	O	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	O	Name of the recording entity.
Record Extensions	O	A set of network operator/manufacturer specific extensions to the record. Conditioned upon the existence of an extension.
Local Record Sequence Number	O	Consecutive record number created by this node. The number is allocated sequentially including all CDR types.

Field	Category	Description
Served MSISDN	O	The primary MSISDN of the subscriber.
Charging Characteristics	M	The Charging Characteristics used by the SGSN.
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.
Charging Characteristics Selection Mode	O	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	O	The IMEI of the ME, if available.
SGSN Address	O	The IP address of the current SGSN.
MS Network Capability	O	The mobile station network capability.
Routing Area Code	O	Routing Area at the time of the Record Opening Time.
Local Area Code	O	Location Area Code at the time of Record Opening Time.
Cell Identifier	O	The Cell Identity for GSM or Service Area Code (SAC) for UMTS at the time of the Record Opening Time.
Cell PLMN Id	O	The MCC and MNC of the Cell at the time of Record Opening Time.
Change of Location	O	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	O	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	O	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.

Field	Category	Description
Node ID	O	Name of the recording entity.
Record Extensions	O	A set of network operator/manufacturer specific extensions to the record. Conditioned upon the existence of an extension.
Local Record Sequence Number	O	Consecutive record number created by this node. The number is allocated sequentially including all CDR types.
Served MSISDN	O	The primary MSISDN of the subscriber.
Charging Characteristics	M	The Charging Characteristics used by the SGSN.
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.
Charging Characteristics Selection Mode	O	Holds information about how Charging Characteristics were selected.

Notes:

- New field “cell PLMN- ID” added.
- All IP addresses is in binary format.

Chapter 10
S-CDR Field Descriptions

This chapter lists and describes the fields supported by the system for use in SGSN Charging Data Records (S-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 *SGSN and Mobility Management Charging Detail Record Field Reference Tables* chapter for information on CDR fields supported in S-CDRs.

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).

Format
IA5 String

Length
1–65 Bytes

Access Point Operator Identifier

The Operator Identifier part of the APN.

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

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 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.
- 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.
- 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

Cell identity for GSM or Service Area Code (SAC) for UMTS at “Record Opening Time”.

Format
Octet String

Length
2 Bytes

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

Charging Characteristics Selection Mode

The charging characteristic (CC) type that the SGSN applied to the CDR. The following values for this field are supplied:

- Home Default: 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.
- Visiting Default: 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.
- Roaming Default: 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

The PDP context identifier used to identify the PDP context in different records created by GSNs.

Format
Unsigned Integer

Length
1–4 Bytes

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

The time period, in seconds, that the record existed in the SGSN. 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
1–5 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

GGSN Address

The binary-represented IPv4 address of the GGSN used.

Format
Hex Value Octet String

Length
4 Bytes

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

Local Record Sequence Number

Consecutive record number created by the node. 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

Location Area Code (LAC)

Indicates the LAC at "Record Opening Time".

Format

Octet String

Length

2 Bytes

MS Network Capability

The mobile station network capability.

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.

Format
Octet String

Length
1–20 Bytes

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

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.

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.

Format
Unsigned Integer

Length
1–5 Bytes

Record Type

Indicates the SGSN PDP context record type.

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)

Indicates the RAC at “Record Opening Time”.

Format
Octet String

Length
1 Byte

Served IMEI

The International Mobile Equipment Identity (IMEI) of the MS, if available.

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 IPv4 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 per 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

SGSN Change

Present if this is first record after SGSN change.

Format

Boolean

Length

1 Byte

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".

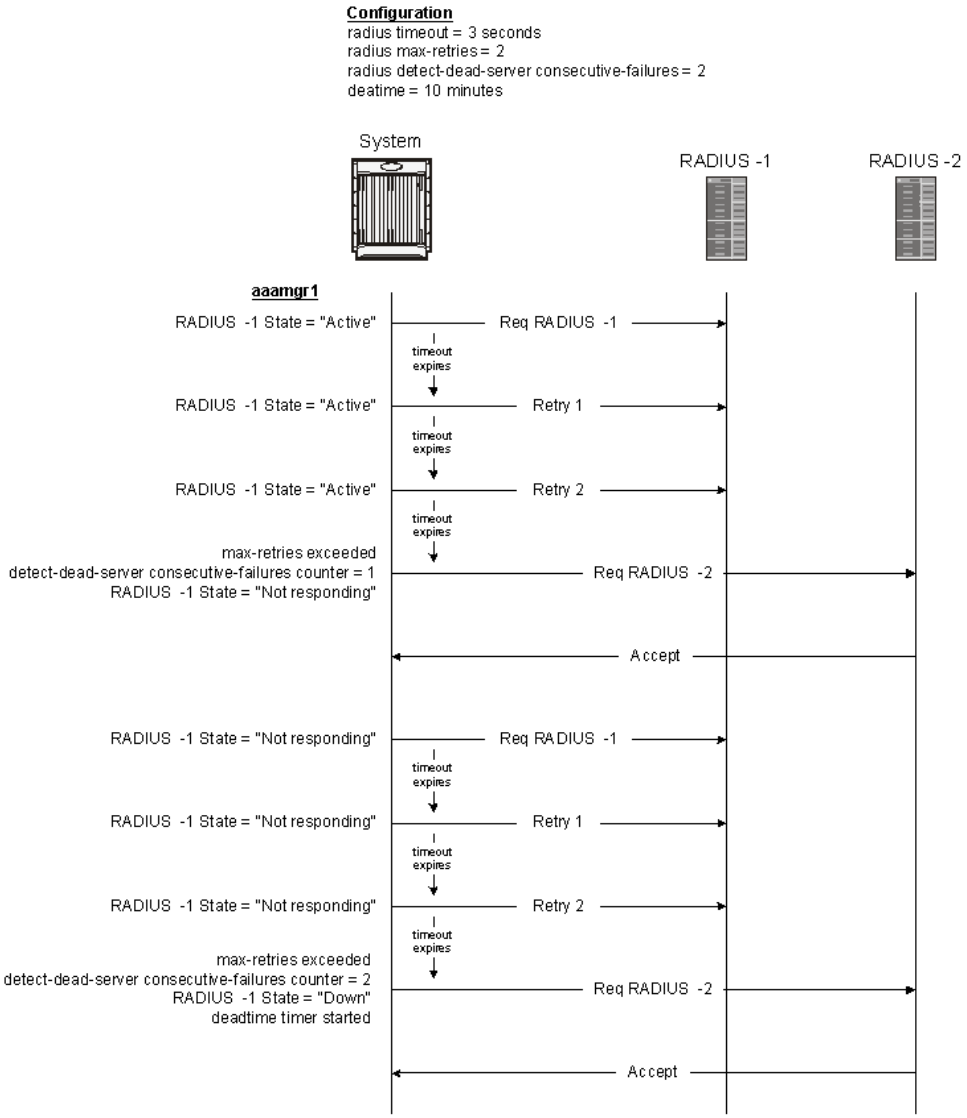
  - **`deadtime`**: Configure the maximum amount of time, in minutes, that must elapse after a context has exceeded one or both of the **`detect-dead-server`** parameters, depending on which parameter is configured. Once this timer has elapsed, the system reclassifies the RADIUS server as "Active" and 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 3. 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 Table

This appendix presents Diameter attribute quick reference table.

The following table describes the indicators used in the quick reference table.

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 table.

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

Term	Expansion	Term	Expansion
DWA	Device-Watchdog-Answer	RR	Reset-Request
DWR	Device-Watchdog-Request	SAA	Server-Assignment-Answer
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

Attribute	AVP Code	Vendor-Id	AVP Type	M Flag	P Flag	ACA	ACR	ASA	ASR	AIA	AIR	AAA	AAR	CLA	CLR	CEA	CER	CCA	CCR	DSDA	DSDR	DWA	DWR	DEA	DER	DPA	DPR	ISDA	ISDR	LIA	LIR	MEICA	MEICR	MAA	MAR	NA	NR	PUA	PUR	PUAM	PURM	PPA	PPR	RAA	RAR	RTA	RTR	RA	RR	SAA	SAR	STA	STR	ULA	ULR	UAA	UAR	UDA	UDR
3GPP2-Allowed-Persistent-TFTS	6083	5535	UINT32	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
3GPP2-BSID	10	5535	OCTETSTRING	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
3GPP2-Correlation-Id	6071	5535	OCTETSTRING	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
3GPP2-Information	6077	5535	GROUPED	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
3GPP2-Inter-User-Priority	139	5535	UINT32	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
3GPP2-Max-Auth-Aggr-BW-BET	130	5535	UINT32	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
3GPP2-Max-Inst-Per-Service-Option	6082	5535	UINT32	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
3GPP2-Max-Per-Flow-Priority-User	6088	5535	UINT32	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
3GPP2-Max-Svc-Inst-Link-Flow-Total	6084	5535	UINT32	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
3GPP2-RP-Session-ID	6074	5535	OCTETSTRING	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
3GPP2-Service-Option	16	5535	UINT32	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
3GPP2-Service-Option-Profile	74	5535	GROUPED	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
3GPP2-Serving-PCF	6073	5535	ADDRESS	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
3GPP2-User-Zone	6075	5535	OCTETSTRING	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
3GPP-Called-Station-Id	30	10415	OCTETSTRING	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
3GPP-CAMEL-Charging-Info	24	10415	UTF8STRING	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
3GPP-CG-Address	4	10415	OCTETSTRING	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
3GPP-Charging-Characteristics	13	10415	UTF8STRING	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
3GPP-Charging-Id	2	10415	UINT32	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
3GPP-Feature-List	630	10415	UINT32	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
3GPP-Feature-List-ID	629	10415	UINT32	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
3GPP-GGSN-Address	7	10415	OCTETSTRING	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
3GPP-GGSN-MCC-MNC	9	10415	UTF8STRING	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
3GPP-GPRS-QoS-Negotiated-Profile	5	10415	UTF8STRING	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
3GPP-IMEISV	20	10415	OCTETSTRING	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
3GPP-IMSI	1	10415	UTF8STRING	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
3GPP-IMSI-MCC-MNC	8	10415	UTF8STRING	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
3GPP-MS-TimeZone	23	10415	OCTETSTRING	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
3GPP-NSAPI	10	10415	UTF8STRING	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
3GPP-PDP-Type	3	10415	ENUM	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
3GPP-Public-Identity	601	10415	UTF8STRING	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
3GPP-Quota-Consumption-Time	881	10415	UINT32	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
3GPP-Quota-Holding-Time	871	10415	UINT32	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
3GPP-RAT-Type	21	10415	OCTETSTRING	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
3GPP-RAT-Type-Enum	21	10415	ENUM	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
3GPP-Reporting-Reason	872	10415	ENUM	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
3GPP-Selection-Mode	12	10415	UTF8STRING	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
3GPP-Server-Name	602	10415	UTF8STRING	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
3GPP-Session-Stop-Indicator	11	10415	OCTETSTRING	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
3GPP-SGSN-Address	6	10415	OCTETSTRING	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
3GPP-SGSN-IPv6-Address	15	10415	OCTETSTRING	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
3GPP-SGSN-MCC-MNC	18	10415	UTF8STRING	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
3GPP-Supported-Features	628	10415	GROUPED	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
3GPP-Time-Quota-Threshold	868	10415	UINT32	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
3GPP-Trigger-Type	870	10415	ENUM	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
3GPP-Unit-Quota-Threshold	1226	10415	UINT32	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
3GPP-User-Data	606	10415	OCTETSTRING	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
3GPP-User-Location-Info	22	10415	UTF8STRING	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
3GPP-Volume-Quota-Threshold	869	10415	UINT32	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Abort-Cause	500	10415	ENUM	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Acceptable-Service-Info	526	10415	GROUPED	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Access-Network-Charging-Address	501	10415	ADDRESS	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Access-Network-Charging-Identifier	502	10415	GROUPED	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Access-Network-Charging-Identifier-Gx	1022	10415	GROUPED	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Access-Network-Charging-Identifier-Ty	1022	10415	GROUPED	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Access-Network-Charging-Identifier-Value	503	10415	OCTETSTRING	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Access-Network-Charging-Physical-Access-Id	1472	10415	GROUPED	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Access-Network-Charging-Physical-Access-Id-Realm	1474	10415	OCTETSTRING	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Access-Network-Charging-Physical-Access-Id-Value	1473	10415	OCTETSTRING	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Access-Network-Information	1263	0	OCTETSTRING	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Access-Network-Physical-Access-Id	1472	5535	GROUPED	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Access-Network-Physical-Access-Id-Realm	1474	5535	OCTETSTRING	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Access-Network-Physical-Access-Id-Value	1473	5535	OCTETSTRING	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Access-Network-Type	306	0	GROUPED	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Access-Restriction-Data	6030	10415	UINT32	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Accounting-EAP-Auth-Method	465	0	UINT64	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0-1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Accounting-Input-Octets	363	10415	UINT64	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Accounting-Input-Packets	365	10415	UINT64	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Accounting-Output-Octets	364	10415	UINT64	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Accounting-Output-Packets	366	10415	UINT64	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Accounting-Record-Number	485	0	UINT32	1	0	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Accounting-Record-Type	480	0	ENUM	1	0	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Accounting-Sub-Session-Id	287	0	UINT64	1	0	0-1	0-1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Acct-Application-Id	259	0	UINT32	1	0	0-1	0-1	0	0	0-1	0-1	0	0	0-1	0-1	0+	0+	0	0	0-1	0-1	0	0	0	0	0	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	0	0	0-1	0-1	0-1	0-1	0-1	0-1	0	0	0-1	0-1	0-1	0-1	0-1	0-1
Acct-Interim-Interval	85	0	UINT32	0	0	0-1	0-1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0-1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Acct-Multi-Session-Id	50	0	UTF8STRING	1	0	0-1	0-1	0	0	0	0	0	0	0	0	0	0	0-1	0-1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Acct-Realtime-Required	483	0	ENUM	1	0	0-1	0-1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Acct-Session-Id	44	0	OCTETSTRING	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Acct-Session-Time	46	10415	UINT32	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Additional-MBMS-Trace-Info	910	10415	OCTETSTRING	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Address-Realm	1005	0	OCTETSTRING	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AF-Application-Identifier	504	10415	OCTETSTRING	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AF-Charging-Identifier	505	10415	OCTETSTRING	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AF-Correlation-Information	1276	10415	GROUPED	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AGW-IP-Address	1003	5535	OCTETSTRING	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AGW-IPv6-Address	1004	5535	OCTETSTRING	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AGW-MCC-MNC	1002	5535	OCTETSTRING	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
All-APN-Configurations-Included-Indicator	6032	10415	ENUM	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Allocation-Retention-Priority	1034	10415	UINT32	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Alternative-APN	905	10415	UTF8STRING	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AMBR	6040	10415	GROUPED	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AN-GW-Address	1050	10415	ADDRESS	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
APN-Authorized	6090	10415	GROUPED	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
APN-Barring-Type	6091	10415	ENUM	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
APN-Configuration	6034	10415	GROUPED	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
APN-Configuration-Profile	6033	10415	GROUPED	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
APN-OI-Replacement	6031	10415	UTF8STRING	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Application-Provided-Called-Party-Address	837	10415	UTF8STRING	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Application-Server	836	10415	UTF8STRING	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Application-Server-Information	850	10415	GROUPED	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
ARP	6039	10415	UINT32	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Associated-Identities	632	10415	GROUPED	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Associated-URI	856	10415	UTF8STRING	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Auth-Application-Id	258	0	UINT32	1	0	0	0	0	1	0-1	0-1	1	1	0-1	0-1	0+	0+	1	1	0-1	0-1	0	0	1	1	0	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	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
Authentication-Info	6016	10415	GROUPED	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Auth-Grace-Period	276	0	UINT32	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0-1	0-1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Authorised-QoS	849	0	UTF8STRING	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Authorization-Lifetime	291	0	UINT32	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0-1	0-1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Authorization-Token	506	10415	OCTETSTRING	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Authorized-QoS	1016	10415	GROUPED	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Auth-Profile-Id-Bi-Direction	6081	5535	UINT32	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Auth-Profile-Id-Forward	6079	5535	UINT32	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Auth-Profile-Id-Reverse	6080	5535	UINT32	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Auth-Request-Type	274	0	ENUM	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Auth-Session-State	277	0	ENUM	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0-1	0-1	0	0	0	0	1	1	0	0	1	1	0	0	1	1	0	0	1	1	0	0	1	1	0	0	1	1	0	0	0	0	1	1	1	1
AUTN	6054	10415	OCTETSTRING	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
BCID	200	4491	UTF8STRING	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Bearer-Control-Mode	1023	10415	ENUM	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Bearer-Identifier	1020	10415	OCTETSTRING	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Bearer-Operation	1021	10415	ENUM	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Bearer-Service	854	10415	OCTETSTRING	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Bearer-Usage	1000	10415	ENUM	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Binding-Information	450	13019	GROUPED	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Binding-Input-List	451	13019	GROUPED	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Binding-Output-List	452	13019	GROUPED	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
BM-Address	1451	10415	ADDRESS	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
BM-Cause-Code	1452	10415	INT32	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
BM-Correlation-ID	527	10415	UTF8STRING	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
BM-Information	1465	10415	GROUPED	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
BM-Type	1454	10415	ENUM	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
BSID	10003	0	OCTETSTRING	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0+	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Callback-Id	20	0	UTF8STRING	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0-1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Callback-Number	19	0	UTF8STRING	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0-1	0-1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Called-Asserted-Identity	1250	10415	UTF8STRING	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Called-Party-Address	832	0	UTF8STRING	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Called-Station-Id	30	0	OCTETSTRING	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0-1	0	0	0	0	0	0	0	0	0	0	0	0-1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Calling-Party-Address	831	10415	UTF8STRING	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Calling-Station-Id	31	0	UTF8STRING	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0-1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Cancellation-Type	6023	10415	ENUM	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Carrier-ID	1500	10415	UTF8STRING	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Cause-Code	861	0	INT32	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
CC-Correlation-Id	411	0	OCTETSTRING	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0-1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
CC-Input-Octets	412	0	UINT64	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0-1	0-1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
CC-Money	413	0	GROUPED	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0-1	0-1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
CC-Output-Octets	414	0	UINT64	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0-1	0-1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
CC-Request-Number	415	0	UINT32	1	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
CC-Request-Type	416	0	ENUM	1	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
CC-Service-Specific-Units	417	0	UINT64	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0-1	0-1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
CC-Session-Failover	418	0	ENUM	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0-1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
CC-Sub-Session-Id	419	0	UINT64	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0-1	0-1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
CC-Time	420	0	UINT32	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0-1	0-1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

Attribute	AVP Code	Vendor-Id	AVP Type	M Flag	P Flag	ACA	ACR	ASA	ASR	AIA	AIR	AAA	AAR	CLA	CLR	CEA	CER	CCA	CCR	DSDA	DSDR	DWA	DWR	DEA	DER	DPA	DPR	ISDA	ISDR	LIA	LIR	MEICA	MEICR	MAA	MAR	NA	NR	PUA	PUR	PUAM	PURM	PPA	PPR	RAA	RAR	RTA	RTR	RA	RR	SAA	SAR	STA	STR	ULA	ULR	UAA	UAR	UDA	UDR
CC-Total-Octets	421	0	UINT64	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0-1	0-1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
CC-Unit-Type	454	0	ENUM	1	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
CG-Address	846	10415	ADDRESS	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Chargeable-User-Id	89	0	OCTETSTRING	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Charging-Information	618	0	GROUPED	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	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	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	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	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	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	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	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	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	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	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	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	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Check-Balance-Result	422	0	ENUM	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0-1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Civic-Location	355	13019	OCTETSTRING	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Class	25	0	OCTETSTRING	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0+	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0+	0	0	0	0	0	0
CoA-Information	1039	10415	GROUPED	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
CoA-IP-Address	1035	10415	ADDRESS	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Codec-Data	524	10415	OCTETSTRING	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Confidentiality-Key	625	10415	OCTETSTRING	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Configuration-Token	78	0	OCTETSTRING	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0+	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Connect-Info	77	0	UTF8STRING	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0-1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Content-Disposition	828	10415	UTF8STRING	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Content-Length	827	10415	UINT32	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Content-Type	826	10415	UTF8STRING	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Context-Identifier	6026	10415	UINT32	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Correlate-Reason	202	4491	ENUM	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Cost-Information	423	0	GROUPED	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0-1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Cost-Unit	424	0	UTF8STRING	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0-1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Credit-Control	426	0	ENUM	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Credit-Control-Failure-Handling	427	0	ENUM	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0-1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Currency-Code	425	0	UINT32	1	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0-1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Current-Location	707	0	ENUM	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0-1
Customer-Id	1146	8164	UTF8STRING	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Data-Reference	703	0	ENUM	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1
Deregistration-Reason	615	10415	GROUPED	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	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	0	0-1	0	0-1	0	0	0	1	0	0	0	0-1	0	1	0	0	0	0-1	0	0	0	1	0	0-1	0	0-1	0	0-1	0	0-1	0	0-1	0	0-1	0	1	0	0-1	0	1	0	1	0	0-1	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	0	1	0	0	0	1	0	1	0	0	0	1	0	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
Dialog-Id	203	4491	UTF8STRING	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Digest-Algorithm	111	0	OCTETSTRING	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Digest-Auth-Param	117	0	OCTETSTRING	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Digest-Domain	119	0	OCTETSTRING	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Digest-HA1	121	0	OCTETSTRING	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Digest-QoP	110	0	OCTETSTRING	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Digest-Realm	104	0	OCTETSTRING	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
DIR	11000	0	OCTETSTRING	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0+	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Direct-Debiting-Failure-Handling	428	0	ENUM	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0-1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Direction	210	4491	ENUM	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Direct-Message	211	4491	ENUM	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Disconnect-Cause	273	0	ENUM	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
DSA-Flags	6025	10415	UINT32	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
DSR-Flags	6024	10415	UINT32	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
EAP-Key-Name	102	0	OCTETSTRING	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0-1	0-1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
EAP-Master-Session-Key	464	0	OCTETSTRING	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0-1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
EAP-Payload	462	0	OCTETSTRING	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0-1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
EAP-Reissued-Payload	463	0	OCTETSTRING	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0-1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Early-Media-Description	1272	10415	GROUPED	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Element-ID	212	4491	UTF8STRING	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Element-Type	213	4491	ENUM	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
EPS-Cause-Code	1407	10415	ENUM	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
EPS-Information	1401	10415	GROUPED	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
EPS-Subscribed-QoS-Profile	6036	10415	GROUPED	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
EPS-Vector	6017	10415	GROUPED	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Equipment-Status	6050	10415	ENUM	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Error-Message	281	0	UTF8STRING	0	0	0	0	0	0	0	0	0-1	0	0	0	0-1	0	0	0	0	0	0-1	0	0-1	0	0-1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0-1	0	0	0	0	0	0	0	0-1	0	0	0	0	0	0	0
Error-Reporting-Host	294	0	DIAMIDENT	1	0	0	0	0	0	0	0	0-1	0	0	0	0	0	0	0	0	0	0	0	0-1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
ESN	6109	10415	OCTETSTRING	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Event	825	10415	UTF8STRING	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Event-Message-Type	214	4491	ENUM	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Event-Report-Indication	1033	10415	GROUPED	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Event-Timestamp	55	0	TIME	1	0	0-1	0-1	0	0	0	0	0	0	0	0	0	0	0-1	0-1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Event-Trigger	1006	10415	ENUM	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Event-Type	823	10415	GROUPED	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	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	0	0	0	0-1	0	0-1	0	0-1	0	0	0	0	0	0-1	0	0	0	0	0	0	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	0	0	0-1	0	0-1	0	0-1	0	1	0	0-1	0	0-1	0	0-1	0
Experimental-Result-Code	298	0	ENUM	1	0	0	0	0	0	1	0	1	0	1	0	0	0	0	0	1	0	0	0	0	0	0	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	0	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0
Expires	888	10415	UINT32	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Exponent	429	0	INT32	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0-1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Extended-QoS-Filter-Rule	6066	0	UINT32	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	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	0-1	0	0+	0	0+	0	0+	0	0+	0	0+	0	0+	0	0+	0	0+	0	0+	0	0+	0	0	0	0+	0	0+	0	0+	0	0+	0	0+	0	0+	0	0+	0
FDR-Reason	1501	10415	ENUM	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Feature-List	630	0	UINT32	0	0	0	0	0	0	1	1	0	0	1	1	0	0	0	0	1	1	0	0	0	0	0	0	1	1	0	0	0	0	0	0	1	1	1	1	1	1	0	0	0	0	0	0	1	1	0	0	0	0	1	1	0	0	1	1
Feature-List-ID	629	0	UINT32	0	0	0	0	0	0	1	1	0	0	1	1	0	0	0	0	1	1	0	0	0	0	0	0	1	1	0	0	0	0	0	0	1	1	1	1	1	1	0	0	0	0	0	0	1	1	0	0	0	0	1	1	0	0	1	1
Filter-Id	11	0	UTF8STRING	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0+	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Final-Unit-Action	449	0	ENUM	1	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Final-Unit-Indication	430	0	GROUPED	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0-1	0-1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Firmware-Revision	267	0	UINT32	0	0	0	0	0	0	0	0	0	0	0	0	0-1	0-1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
First-Packet-Direction	1455	10415	ENUM	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Flow-Description	507	10415	IPFILTERRULE	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Flow-Description-Info	1022	5535	GROUPED	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Flow-Grouping	508	10415	GROUPED	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Flow-Identifier	1008	5535	OCTETSTRING	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Flow-Info	1007	5535	GROUPED	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Flow-Number	509	10415	UINT32	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Flow-Operation	1006	5535	ENUM	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Flows	510	10415	GROUPED	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Flow-Status	511	10415	ENUM	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Flow-Usage	512	10415	ENUM	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Framed-Appletalk-Link	37	0	UINT32	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0-1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Framed-Appletalk-Network	38	0	UINT32	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0+	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Framed-Appletalk-Zone	39	0	OCTETSTRING	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0-1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Framed-Compression	13	0	ENUM	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0+	0+	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Framed-Interface-Id	96	0	UINT64	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0-1	0	0	0	0	0-1	0-1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Framed-IP-Address	8	0	OCTETSTRING	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0-1	0-1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Framed-IP-Netmask	9	0	OCTETSTRING	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0-1	0-1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Framed-IPv6-Pool	100	0	OCTETSTRING	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0-1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Framed-IPv6-Prefix	97	0	OCTETSTRING	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0+	0+	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Framed-IPv6-Route	99	0	UTF8STRING	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0+	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Framed-IPX-Network	23	0	UINT32	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0-1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Framed-MTU	12	0	UINT32	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0-1	0-1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Framed-Pool	88	0	OCTETSTRING	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0-1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Framed-Protocol	7	0	ENUM	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0-1	0-1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Framed-Route	22	0	UTF8STRING	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0+	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Framed-Routing	10	0	ENUM	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0-1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Geospatial-Location	356	13019	OCTETSTRING	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
GERAN-Vector	6019	10415	GROUPED	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
GGSN-Address	847	10415	ADDRESS	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Globally-Unique-Address	300	13019	GROUPED	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
GMT-Timezone-Offset	1502	10415	TIME	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Granted-QoS	1011	5535	GROUPED	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Granted-Service-Unit	431	0	GROUPED	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0-1	0-1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Group-ID	1503	10415	UTF8STRING	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
G-S-U-Pool-Identifier	453	0	UINT32	1	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
G-S-U-Pool-Reference	457	0	GROUPED	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0+	0+	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	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	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Guaranteed-Bitrate-UL	1026	10415	UINT32	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
HBM-Address	1462	10415	ADDRESS	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
HOA-Session-ID	1463	10415	UTF8STRING	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Home-Agent	3	5535	ADDRESS	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Host-IP-Address	257	0	ADDRESS	1	0	0	0	0	0	0	0	0	0	0	0	0+	0+	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
HPLMN-ODB	6021	10415	UINT32	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
HSGW-Address	1404	10415	ADDRESS	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
IDA-Flags	6046	10415	UINT32	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Identity-Set	708	0	ENUM	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0-1
Idle-Timeout	28	0	UINT32	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0-1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
IMEI	6003	10415	UTF8STRING	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Immediate-Response-Preferred	6015	10415	UINT32	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
IMS-Charging-Identifier	841	10415	UTF8STRING	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
IMS-Communication-Service-Identifier	1281	10415	UTF8STRING	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
IMS-Information	876	10415	GROUPED	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	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+	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Incoming-Trunk-Group-ID	852	0	UTF8STRING	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Initial-CellSector-ID	1419	10415	UTF8STRING	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Integrity-Key	626	10415	OCTETSTRING	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Inter-Operator-Identifier	838	10415	GROUPED	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	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	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
IPGW-Address	1456	10415	ADDRESS	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
IP-MMS	6076	10415	UINT32	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
IP-Version-Authorized	11	5535	ENUM	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Item-Number	6022	10415	UINT32	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
KASME	6055	10415	OCTETSTRING	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
KC-Key	6058	10415	OCTETSTRING	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Last-CellSector-ID	1420	10415	UTF8STRING	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Last-CellSector-Location	536	10415	UTF8STRING	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

Attribute	AVP Code	Vendor-Id	AVP Type	M Flag	P Flag	ACA	ACR	ASA	ASR	AIA	AIR	AAA	AAR	CLA	CLR	CEA	CER	CCA	CCR	DSDA	DSDR	DWA	DWR	DEA	DER	DPA	DPR	ISDA	ISDR	LIA	LIR	MEICA	MEICR	MAA	MAR	NA	NR	PUA	PUR	PUAM	PURM	PPA	PPR	RAA	RAR	RTA	RTR	RA	RR	SAA	SAR	STA	STR	ULA	ULR	UAA	UAR	UDA	UDR
Latching-Indication	457	13019	ENUM	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
LI-Information	218	4491	GROUPED	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Line-Identifier	500	13019	OCTETSTRING	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Location-Information	350	13019	GROUPED	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Logical-Access-Id	302	0	OCTETSTRING	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	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	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	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	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Max-Requested-Bandwidth-UL	516	10415	UINT32	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
MBMS-2G-3G-Indicator	907	10415	ENUM	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
MBMS-BMSC-SSM-IP-Address	918	10415	UTF8STRING	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
MBMS-BMSC-SSM-IPv6-Address	919	10415	UTF8STRING	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
MBMS-Counting-Information	914	10415	ENUM	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
MBMS-GGSN-Address	916	10415	UTF8STRING	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
MBMS-GGSN-IPv6-Address	917	10415	UTF8STRING	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
MBMS-Required-QoS	913	10415	UTF8STRING	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
MBMS-Service-Area	903	10415	OCTETSTRING	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
MBMS-Service-Type	906	10415	ENUM	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
MBMS-Session-Duration	904	10415	OCTETSTRING	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
MBMS-Session-Identity	908	10415	OCTETSTRING	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
MBMS-Session-Repetition-number	912	10415	OCTETSTRING	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
MBMS-StartStop-Indication	902	10415	ENUM	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
MBMS-Time-To-Data-Transfer	911	10415	OCTETSTRING	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
MBMS-User-Data-Mode-Indication	915	10415	ENUM	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Media-Component-Description	517	10415	GROUPED	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Media-Component-Number	518	10415	UINT32	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Media-Initiator-Flag	882	10415	ENUM	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Media-Initiator-Party	1288	10415	UTF8STRING	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Media-Sub-Component	519	10415	GROUPED	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Media-Type	520	10415	ENUM	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
MEID	6110	10415	OCTETSTRING	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Message-Body	889	10415	GROUPED	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Metering-Method	1007	10415	ENUM	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Min-Bandwidth-DL	1012	5535	UINT32	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Min-Bandwidth-UL	1013	5535	UINT32	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
MIP6-Agent-Info	6060	0	GROUPED	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
MIP6-Feature-Vector	6062	0	UINT64	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
MIP6-Home-Link-Prefix	6061	0	OCTETSTRING	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
MIP-Feature-Vector	337	10415	UINT32	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	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	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
MIP-Home-Agent-Host	348	0	GROUPED	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
MIP-Mobile-Node-Address	333	10415	ADDRESS	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
MSISDN	701	0	OCTETSTRING	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0-1	0	0	0	0	0	0-1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0-1
Multiple-Auth-Profile	30	5535	ENUM	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Multiple-Auth-Support	29	5535	ENUM	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Multiple-Services-Credit-Control	456	0	GROUPED	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0-1	0+	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Multiple-Services-Indicator	455	0	ENUM	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0-1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Multi-Round-Time-Out	272	0	UINT32	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0-1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
NAS-Filter-Rule	400	0	IPFILTERRULE	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0+	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
NAS-Identifier	32	0	UTF8STRING	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0-1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
NAS-IP-Address	4	0	OCTETSTRING	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0-1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
NAS-IPv6-Address	95	0	OCTETSTRING	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0-1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
NAS-Port	5	0	UINT32	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0-1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
NAS-Port-Id	87	0	UTF8STRING	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0-1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
NAS-Port-Type	61	0	ENUM	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0-1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Network-Access-Mode	6020	10415	ENUM	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Network-Request-Support	1024	10415	ENUM	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
New-Dialog-Id	219	4491	UTF8STRING	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Node-Functionality	862	0	ENUM	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
NOR-Flags	6048	10415	UINT32	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Nortel-Data-Reference	301	0	ENUM	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0-1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0-1
Number-Of-Requested-Vectors	6013	10415	UINT32	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Offline	1008	10415	ENUM	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Online	1009	10415	ENUM	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Operator-Determined-Barring	6029	10415	UINT32	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Operator-String	1411	10415	OCTETSTRING	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	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	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Originating-IOI	839	0	UTF8STRING	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Originating-Line-Info	94	0	OCTETSTRING	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0-1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Originating-Request	633	10415	ENUM	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Originator	864	10415	ENUM	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	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	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	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	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
Origin-State-Id	278	0	UINT32	1	0	0-1	0-1	0	0	0	0	0	0	0	0	0-1	0-1	0-1	0-1	0	0	0-1	0-1	0-1	0-1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0-1	0-1	0	0	0	0	0	0
Outgoing-Trunk-Group-ID	853	0	UTF8STRING	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Paging-Group-Id	10001	0	UINT32	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0+	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
PCC-Rule-Status	1019	10415	ENUM	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
PC-Digest-Algorithm	204	4491	OCTETSTRING	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
PC-Digest-Auth-Param	205	4491	OCTETSTRING	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
PC-Digest-Domain	206	4491	OCTETSTRING	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
PC-Digest-HA1	207	4491	OCTETSTRING	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
PC-Digest-QoP	208	4491	OCTETSTRING	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
PC-Digest-Realm	209	4491	OCTETSTRING	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
PC-SIP-Digest-Authenticate	228	4491	GROUPED	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
PDG-Address	895	10415	ADDRESS	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
PDG-Charging-Id	896	0	UINT32	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
PDN-GW-Address	6041	10415	ADDRESS	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
PDN-GW-Allocation-Type	6043	10415	ENUM	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
PDN-GW-Identity	6044	10415	GROUPED	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
PDN-GW-Name	6042	10415	UTF8STRING	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
PDP-Address	1227	10415	ADDRESS	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
PDP-Context-Type	1247	10415	ENUM	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
PDP-Session-Operation	1015	10415	ENUM	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
PGW-Address	1405	10415	ADDRESS	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
PGW-MCC-MNC	1406	10415	OCTETSTRING	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Physical-Access-Id	313	0	UTF8STRING	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
PMIP6-MAG-Address	6070	10415	ADDRESS	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
PMIP-Mobile-Node-Address	1408	10415	ADDRESS	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Port-Limit	62	0	UINT32	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0-1	0-1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Port-Number	455	13091	UINT32	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Precedence	1010	10415	UINT32	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Primary-Charging-Collection-Function-Name	621	0	UTF8STRING	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Primary-Event-Charging-Function-Name	619	0	UTF8STRING	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Product-Name	269	0	UTF8STRING	0	0	0	0	0	0	0	0	0	0	0	0	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Proxy-Host	280	0	DIAMIDENT	1	0	1	1	0	0	1	1	1	1	1	1	0	0	1	1	1	1	0	0	1	1	0	0	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	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	0+	0+	0+	0+	0	0	0+	0+	0	0	0+	0+	0+	0+	0+	0+	0+	0+	0+	0+	0+	0+	0+	0+	0+	0+	0+	0+	0+	0+	0+	0+	0+	0+	0+	0+	0+	0+	0+	0+	0+	0+
Proxy-State	33	0	OCTETSTRING	1	0	1	1	0	0	1	1	1	1	1	1	0	0	1	1	1	1	0	0	1	1	0	0	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
PS-Append-Free-Format-Data	867	10415	ENUM	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
PSCID	1450	10415	OCTETSTRING	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
PS-Free-Format-Data	866	10415	OCTETSTRING	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
PS-Furnish-Charging-Information	865	10415	GROUPED	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
PS-Information	874	10415	GROUPED	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
PUA-Flags	6047	10415	UINT32	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Public-Identity	601	0	UTF8STRING	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0-1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0-1
QoS-Capability	6063	0	GROUPED	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
QoS-Class	1017	10415	ENUM	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	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	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
QoS-Information	1016	10415	GROUPED	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
QoS-Negotiation	1029	10415	ENUM	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
QoS-Profile-Template	6067	0	UINT32	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
QoS-Resource-Identifier	6107	10415	UINT32	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
QoS-Resource-Operation	6108	10415	ENUM	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
QoS-Resource-Request	6106	10415	GROUPED	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
QoS-Resources	6065	0	GROUPED	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
QoS-Rule-Definition	6102	10415	GROUPED	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
QoS-Rule-Install	6101	10415	GROUPED	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
QoS-Rule-Name	6104	10415	OCTETSTRING	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
QoS-Rule-Remove	6103	10415	GROUPED	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
QoS-Rule-Report	6105	10415	GROUPED	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
QoS-Upgrade	1030	10415	ENUM	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
RACS-Contact-Point	351	0	DIAMIDENT	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
RAI	909	10415	UTF8STRING	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
RAND	6052	10415	OCTETSTRING	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
RAS-Id	10000	0	UINT32	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
RAT-Frequency-Selection-Priority	6045	10415	UINT32	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Rating-Group	432	0	UINT32	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0-1	0-1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0-1	0	0	0	0	0	0	0	0	0	0	0	0	0	0
RAT-Type	1001	5535	ENUM	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Reason-Code	616	10415	ENUM	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Reason-Info	617	10415	UTF8STRING	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Re-Auth-Request-Type	285	0	ENUM	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0-1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Redirect-Address-Type	433	0	ENUM	1	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Redirect-Host	292	0	OCTETSTRING	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0-1	0	0	0	0	0	0+	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0+	0	0	0	0	0	0	0
Redirect-Host-Usage	261	0	ENUM	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0-1	0	0	0	0	0	0-1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0+	0	0	0	0	0	0	0
Redirect-Max-Cache-Time	262	0	UINT32	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0-1	0	0	0	0	0	0-1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Redirect-Server	434	0	GROUPED	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0-1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Redirect-Server-Address	435	0	UTF8STRING	1	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
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	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Reply-Message	18	0	UTF8STRING	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0+	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Reporting-Level	1011	10415	ENUM	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Requested-Action	436	0	ENUM	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0-1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Requested-Domain	706	0	ENUM	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0-1
Requested-EUTRAN-Authentication-Info	6010	10415	GROUPED	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

Attribute	AVP Code	Vendor-Id	AVP Type	M Flag	P Flag	ACA	ACR	ASA	ASR	AIA	AIR	AAA	AAR	CLA	CLR	CEA	CER	CCA	CCR	DSDA	DSDR	DWA	DWR	DEA	DER	DPA	DPR	ISDA	ISDR	LIA	LIR	MEICA	MEICR	MAA	MAR	NA	NR	PUA	PUR	PUAM	PURM	PPA	PPR	RAA	RAR	RTA	RTR	RA	RR	SAA	SAR	STA	STR	ULA	ULR	UAA	UAR	UDA	UDR
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	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Requested-Information	353	13019	ENUM	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Requested-Party-Address	1251	10415	UTF8STRING	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Requested-QoS	1010	5535	GROUPED	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Requested-Service-Unit	437	0	GROUPED	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0-1	0-1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Requested-UTRAN-Authentication-Info	6011	10415	GROUPED	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Requesting-Node-Type	6060	10415	ENUM	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Required-MBMS-Bearer-Capabilities	901	10415	UTF8STRING	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Reservation-Class	456	13019	UINT32	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Reservation-Priority	458	13019	ENUM	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Restriction-Filter-Rule	438	0	IPFILTERRULE	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0+	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Result-Code	268	0	ENUM	1	0	1	0	1	0	0-1	0	0-1	0	0-1	0	1	0	1	0-1	0-1	0	1	0	1	0	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	1	0	0-1	0	0-1	0	0-1	0	0	0	0-1	0	0-1	0	0-1	0
Re-Synchronization-Info	6014	10415	UINT32	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Revalidation-Time	1042	10415	TIME	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Role-Of-Node	829	10415	ENUM	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Route-Record	282	0	DIAMIDENT	1	0	0	0+	0	0	0+	0+	0	0+	0+	0+	0	0	0+	0+	0+	0+	0	0	0	0+	0	0	0+	0+	0+	0+	0+	0+	0+	0+	0+	0+	0+	0+	0+	0+	0+	0+	0	0	0+	0+	0+	0+	0+	0+	0	0+	0+	0+	0+	0+	0+	0+
RR-Bandwidth	521	10415	UINT32	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
RS-Bandwidth	522	10415	UINT32	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	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	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Rule-Deactivation-Time	1044	10415	TIME	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Rule-Failure-Code	1031	10415	ENUM	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Rule-Reason-Code	814	5535	ENUM	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
SDP-Answer-Timestamp	1275	0	TIME	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
SDP-Media-Component	843	10415	GROUPED	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
SDP-Media-Description	845	10415	UTF8STRING	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
SDP-Media-Name	844	10415	UTF8STRING	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
SDP-Offer-Timestamp	1274	0	TIME	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
SDP-Session-Description	842	10415	UTF8STRING	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
SDP-TimeStamps	1273	0	GROUPED	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Secondary-Charging-Collection-Function-Name	622	0	UTF8STRING	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Secondary-Event-Charging-Function-Name	620	0	UTF8STRING	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Sector-Id	10002	0	UINT32	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Served-Party-IP-Address	848	10415	ADDRESS	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Server-Assignment-Type	614	10415	ENUM	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Server-Capabilities	603	10415	GROUPED	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Server-Name	602	0	UTF8STRING	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0-1
Service-Class	459	13019	UTF8STRING	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Service-Context-Id	461	0	UTF8STRING	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Service-Identifier	439	0	UINT32	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0+	0-1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0-1	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Service-Indication	704	0	OCTETSTRING	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0-1
Service-Information	873	10415	GROUPED	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Service-Info-Status	527	10415	ENUM	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Service-Parameter-Info	440	0	GROUPED	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0+	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Service-Parameter-Type	441	0	UINT32	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Service-Parameter-Value	442	0	OCTETSTRING	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Service-Specific-Data	1249	0	GROUPED	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Service-Specific-Type	1248	0	UINT32	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Service-Specific-Value	863	0	UTF8STRING	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Service-Type	6	0	ENUM	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0-1	0-1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Service-URN	525	10415	OCTETSTRING	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Session-Bundle-Id	400	13019	UINT32	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Session-Id	263	0	UTF8STRING	1	0	1	1	1	1	1	1	1	1	1	1	0	0	1	1	1	1	0	0	1	1	0	0	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
Session-Release-Cause	1045	10415	ENUM	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Session-Start-Indicator	522	8164	OCTETSTRING	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Session-Timeout	27	0	UINT32	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0-1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
SGSN-Address	1228	10415	ADDRESS	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
SGW-Address	1403	10415	ADDRESS	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
SIP-Auth-Data-Item	612	10415	GROUPED	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
SIP-Authenticate	609	10415	OCTETSTRING	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
SIP-Authentication-Context	611	10415	OCTETSTRING	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
SIP-Authentication-Scheme	608	10415	UTF8STRING	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
SIP-Authorization	610	10415	OCTETSTRING	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
SIP-Digest-Authenticate	635	10415	GROUPED	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
SIP-Forking-Indication	523	10415	ENUM	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
SIP-Item-Number	613	10415	UINT32	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
SIP-Message	229	4491	OCTETSTRING	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
SIP-Method	824	10415	UTF8STRING	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
SIP-Number-Auth-Items	607	10415	UINT32	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
SIP-Request-Timestamp	834	0	TIME	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
SIP-Response-Timestamp	835	0	TIME	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
SN-Absolute-Validity-Time	505	8164	TIME	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
SN-Bandwidth-Control	512	8164	ENUM	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
SN-Firewall-Policy	515	8164	UTF8STRING	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
SN-Monitoring-Key	518	8164	UINT32	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
SN-Service-Flow-Detection	520	8164	ENUM	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
SN-Time-Quota-Threshold	503	8164	UINT32	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
SN-Total-Used-Service-Unit	504	8164	GROUPED	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
SN-Traffic-Policy	514	8164	UTF8STRING	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
SN-Transparent-Data	513	8164	OCTETSTRING	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
SN-Unit-Quota-Threshold	502	8164	UINT32	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
SN-Usage-Monitoring	521	8164	ENUM	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
SN-Usage-Monitoring-Control	517	8164	GROUPED	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
SN-Usage-Volume	519	8164	UINT64	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
SN-Volume-Quota-Threshold	501	8164	UINT32	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Software-Version	6004	10415	UTF8STRING	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Specific-Action	513	10415	ENUM	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
SRES	6059	10415	OCTETSTRING	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Start-Time	1457	10415	TIME	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
State	24	0	OCTETSTRING	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0-1	0-1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
STN-SR	6038	10415	UTF8STRING	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Stop-Time	1458	10415	TIME	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Subscriber-Priority	6078	5535	GROUPED	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Subscriber-Status	6028	10415	ENUM	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Subscription-Data	6001	10415	GROUPED	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Subscription-Id	443	0	GROUPED	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Subscription-Id-Data	444	0	UTF8STRING	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Subscription-Id-Type	450	0	ENUM	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Supported-Applications	631	10415	GROUPED	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Supported-Features	628	0	GROUPED	1	0	0	0	0	0	0+	0+	0	0	0+	0+	0	0	0	0	0+	0+	0	0	0	0	0	0	0+	0+	0	0	0	0	0	0	0+	0+	0+	0+	0+	0+	0	0	0	0	0	0	0-1	0-1	0	0	0	0	0+	0+	0	0	0+	0+
Supported-RAT-Type	6005	10415	UTF8STRING	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	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+	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Tap-Id	231	4491	UTF8STRING	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Tariff-Change-Usage	452	0	ENUM	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0-1	0-1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Tariff-Time-Change	451	0	TIME	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0-1	0-1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Terminal-Information	6002	10415	GROUPED	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Terminal-Type	352	13019	OCTETSTRING	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Terminating-IOI	840	0	UTF8STRING	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	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	0	0	0	0	0	0	0	0-1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	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	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	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	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Time-Stamps	833	0	GROUPED	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
TMGI	900	10415	OCTETSTRING	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
TMO-Subscriber-Roaming-Status	2	5611	OCTETSTRING	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	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	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Transport-Class	311	13019	UINT32	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Transport-Protocol	1459	10415	ENUM	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Trunk-Group-ID	851	10415	GROUPED	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Tunnel-Assignment-Id	82	0	OCTETSTRING	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0-1	0-1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Tunnel-Client-Auth-Id	90	0	UTF8STRING	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0-1	0-1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Tunnel-Client-Endpoint	66	0	UTF8STRING	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Tunnel-Header-Filter	1036	10415	IPFILTERRULE	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Tunnel-Header-Length	1037	10415	UINT32	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Tunnel-Information	1038	10415	GROUPED	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Tunneling	401	0	GROUPED	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0+	0+	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Tunnel-Medium-Type	65	0	ENUM	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Tunnel-Password	69	0	OCTETSTRING	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0-1	0-1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Tunnel-Preference	83	0	UINT32	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0-1	0-1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Tunnel-Private-Group-Id	81	0	OCTETSTRING	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0-1	0-1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Tunnel-Server-Auth-Id	91	0	UTF8STRING	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0-1	0-1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Tunnel-Server-Endpoint	67	0	UTF8STRING	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Tunnel-Type	64	0	ENUM	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
UAR-Flags	637	0	UINT32	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
ULA-Flags	6007	10415	UINT32	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
ULR-Flags	6006	10415	UINT32	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
UMTS-Vector	6018	10415	GROUPED	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Unit-Value	445	0	GROUPED	1	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Used-Service-Unit	446	0	GROUPED	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0+	0+	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
User-Authorization-Type	623	10415	ENUM	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
User-Data	606	0	OCTETSTRING	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0-1	0
User-Data-Already-Available	624	10415	ENUM	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	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	0	0	0	0	0	0	0	0-1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
User-Equipment-Info-Type	459	0	ENUM	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
User-Equipment-Info-Value	460	0	OCTETSTRING	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
User-Id	6049	10415	UTF8STRING	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
User-Identity	700	0	GROUPED	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1
User-Name	1	0	UTF8STRING	1	0	0-1	0-1	0-1	0-1	0	1	0	0	0	1	0	0	0-1	0-1	0	1	0	0	0-1	0-1	0	0	0	1	0	0	0	0-1	0-1	1	0	1	0	0-1	0	1	0	1	0-1	0-1	0	1	0	0	0-1	0-1	0	0	0	1	0	1	0	0
User-Session-Id	830	10415	UTF8STRING	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
V4-Transport-Address	454	13019	GROUPED	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
V6-Transport-Address	453	13019	GROUPED	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Validity-Time	448	0	UINT32	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0-1	0-1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Value-Digits	447	0	INT64	1	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

Diameter Attribute Quick Reference Table

Attribute	AVP Code	Vendor-Id	AVP Type	M Flag	P Flag	ACA	ACR	ASA	ASR	AIA	AIR	AAA	AAR	CLA	CLR	CEA	CER	CCA	CCR	DSDA	DSDR	DWA	DWR	DEA	DER	DPA	DPR	ISDA	ISDR	LIA	LIR	MEICA	MEICR	MAA	MAR	NA	NR	PUA	PUR	PUAM	PURM	PPA	PPR	RAA	RAR	RTA	RTR	RA	RR	SAA	SAR	STA	STR	ULA	ULR	UAA	UAR	UDA	UDR
VBM-Address	1460	10415	ADDRESS	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Vendor-Id	266	0	UINT32	1	0	0	0	0	0	1+	1+	1	0	1+	1+	1	1	0	0	1+	1+	0	0	0	0	0	0	1+	1+	1+	1+	1+	1+	1+	1+	1+	1+	1+	1+	1+	1+	1+	1+	0	0	1+	1+	1+	1+	1+	1+	1+	1+	1	0	1+	1+	1+	1+	1+	1+
Vendor-Specific-Application-Id	260	0	GROUPED	1	0	0	0	0	0	1	1	0	0	1	1	0+	0+	0	0	1	1	0	0	0	0	0	0	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	0	0	1	1	1	1	1	1	1	1	0	0	1	1	1	1	1	1
Vendor-Specific-QoS-Profile-Template	6064	0	GROUPED	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Visited-Network-Identifier	600	10415	OCTETSTRING	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Visited-PLMN-Id	6008	10415	UTF8STRING	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
VOA-Session-ID	1464	10415	UTF8STRING	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
VPLMN-Dynamic-Address-Allowed	6037	10415	ENUM	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
VZW-String	1461	10415	UTF8STRING	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Wildcarded-PSI	634	10415	UTF8STRING	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
XRES	6053	10415	OCTETSTRING	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

Appendix E
RADIUS Attribute Quick Reference Tables

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.

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-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
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
SN-Admin-Expiry	0	0	0-1	0	0	0
SN-Admin-Permission	0	0	0-1	0	0	0

Attribute	MGMT Access-Request	MGMT Access-Reject	MGMT Access-Accept	MGMT Acct-Request-Start	MGMT Acct-Request-Interim	MGMT Acct-Request-Stop
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-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

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-ESN	1	0	0	1	1	1
3GPP2-FA-Address	0-1	0	0	0-1	0-1	0-1
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-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
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

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-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-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
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
Called-Station-ID	1	0-1	0-1	1	1	1
Calling-Station-Id	1	0	1	1	1	1
Class	0-1	0-1	0-1	0-1	0-1	0-1
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	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

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
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	0+	0	0	0
Framed-Protocol	1	0	0-1	1	1	1
Idle-Timeout	0	0	0-1	0	0	0
MS-CHAP-Domain	0	0	0-1	0-1	0-1	0-1
MS-CHAP-Error	0	0-1	0	0	0	0
MS-Primary-NBNS-Server	0	0	0-1	1	1	1
MS-Secondary-NBNS-Server	0	0	0-1	1	1	1
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
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-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

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-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-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
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

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-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
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

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-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-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
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

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-HA-Send-DNS-Address	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-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	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-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
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

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-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-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
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

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-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-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-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	0-1	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

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-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-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
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

Attribute	HA Access-Request	HA Access-Reject	HA Access-Accept	HA Acct-Request-Start	HA Acct-Request -Interim	HA Acct-Request -Stop
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
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

Attribute	HA Access-Request	HA Access-Reject	HA Access-Accept	HA Acct-Request-Start	HA Acct-Request -Interim	HA Acct-Request -Stop
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
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

Attribute	HA Access-Request	HA Access-Reject	HA Access-Accept	HA Acct-Request-Start	HA Acct-Request -Interim	HA Acct-Request -Stop
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
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

Attribute	HA Access-Request	HA Access-Reject	HA Access-Accept	HA Acct-Request-Start	HA Acct-Request -Interim	HA Acct-Request -Stop
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
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

Attribute	HA Access-Request	HA Access-Reject	HA Access-Accept	HA Acct-Request-Start	HA Acct-Request -Interim	HA Acct-Request -Stop
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-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-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

Attribute	HA Access-Request	HA Access-Reject	HA Access-Accept	HA Acct-Request-Start	HA Acct-Request -Interim	HA Acct-Request -Stop
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
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	0-1	0-1	0-1	0-1
3GPP-GGSN-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-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	0-1	0-1
3GPP-SGSN-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
Called-Station-ID	1	0	0	1	1	1
Calling-Station-Id	0-1	0	0	0-1	0-1	0-1
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
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
Idle-Timeout	0	0	0-1	0	0	0
MS-Primary-NBNS-Server	0	0	0-1	0	0	0
MS-Secondary-NBNS-Server	0	0	0-1	0	0	0
NAS-Port-Type	0-1	0	0	0-1	0	0-1

Attribute	GGSN Access-Request	GGSN Access-Reject	GGSN Access-Accept	GGSN Acct-Request -Start	GGSN Acct-Request -Interim	GGSN Acct-Request -Stop
Primary-DNS-Server	0	0	0-1	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-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
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

Attribute	GGSN Access-Request	GGSN Access-Reject	GGSN Access-Accept	GGSN Acct-Request -Start	GGSN Acct-Request -Interim	GGSN Acct-Request -Stop
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-Rad-APN-Name	0-1	0	0-1	0-1	0-1	0-1
SN1-Radius-Returned-Username	0	0	0-1	0	0	0
SN1-Re-CHAP-Interval	0	0	0-1	0	0	0
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

Attribute	GGSN Access-Request	GGSN Access-Reject	GGSN Access-Accept	GGSN Acct-Request -Start	GGSN Acct-Request -Interim	GGSN Acct-Request -Stop
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
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-DNS-Proxy-Intercept-List	0	0	1	0	0	0
SN-DNS-Proxy-Use-Subscr-Addr	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-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
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

Attribute	GGSN Access-Request	GGSN Access-Reject	GGSN Access-Accept	GGSN Acct-Request -Start	GGSN Acct-Request -Interim	GGSN Acct-Request -Stop
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-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-Rad-APN-Name	0-1	0	0-1	0-1	0-1	0-1
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
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

Attribute	GGSN Access-Request	GGSN Access-Reject	GGSN Access-Accept	GGSN Acct-Request -Start	GGSN Acct-Request -Interim	GGSN Acct-Request -Stop
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-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
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
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-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-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-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
EAP-Message	1+	1+	1+	0	0	0
Error-Cause	0	0-1	0	0	0	0
Framed-IP-Address	0	0	0-1	1	1	1
Framed-IP-Netmask	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
MSK	0	0	0-1	0	0	0
NAS-Port-Type	0	0	0	0-1	0-1	0-1
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-Disconnect-Reason	0	0	0	0	0	1
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

Attribute	WIMAX Access-Request	WIMAX Access-Reject	WIMAX Access-Accept	WIMAX Acct-Request-Start	WIMAX Acct-Request-Interim	WIMAX Acct-Request-Stop
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
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-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
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
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	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	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
SN-Content-Type	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-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
User-Name	1	0	0	1	1	1

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-Comp-Tunnel-Indicator	0	0	0	1	1	1
3GPP2-Correlation-Id	1	0	0	1	1	1
3GPP2-DNS-Update-Required	0	0	0-1	0	0	0
3GPP2-ESN	1	0	0	0	0	0
3GPP2-IP-QOS	0	0	0-1	1	1	1
3GPP2-IP-Technology	0-1	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-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
Calling-Station-Id	1	0	1	1	1	1
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-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
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
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

Attribute	MIPv6HA Access-Request	MIPv6HA Access-Reject	MIPv6HA Access-Accept	MIPv6HA Acct-Request-Start	MIPv6HA Acct-Request-Interim	MIPv6HA Acct-Request-Stop
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
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
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	MIPv6HA Access-Request	MIPv6HA Access-Reject	MIPv6HA Access-Accept	MIPv6HA Acct-Request-Start	MIPv6HA Acct-Request-Interim	MIPv6HA 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-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-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

Attribute	MIPv6HA Access-Request	MIPv6HA Access-Reject	MIPv6HA Access-Accept	MIPv6HA Acct-Request-Start	MIPv6HA Acct-Request-Interim	MIPv6HA Acct-Request-Stop
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-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

Attribute	MIPv6HA Access-Request	MIPv6HA Access-Reject	MIPv6HA Access-Accept	MIPv6HA Acct-Request-Start	MIPv6HA Acct-Request-Interim	MIPv6HA Acct-Request-Stop
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-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

Attribute	MIPv6HA Access-Request	MIPv6HA Access-Reject	MIPv6HA Access-Accept	MIPv6HA Acct-Request-Start	MIPv6HA Acct-Request-Interim	MIPv6HA Acct-Request-Stop
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-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-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-Count-Type	0-1	0	0-1	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-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-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
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

Attribute	standard	3gpp	3gpp2	3gpp2-835	starent	starent-835	starent-vsa1	starent-vsa1-835
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-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-FI-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
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

Attribute	standard	3gpp	3gpp2	3gpp2-835	starent	starent-835	starent-vsa1	starent-vsa1-835
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-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
3GPP-GGSN-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-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

Attribute	standard	3gpp	3gpp2	3gpp2-835	starent	starent-835	starent-vsa1	starent-vsa1-835
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-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
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
Charging-Rules-Name	No	No	No	No	No	No	No	No
Charging-Server	No	No	No	No	No	No	No	No
Charging-Type	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

Attribute	standard	3gpp	3gpp2	3gpp2-835	starent	starent-835	starent-vsa1	starent-vsa1-835
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
Custom-Correlation-Id	No	No	No	No	No	No	No	No
Custom-Prepaid-Ind	No	No	No	No	No	No	No	No
Custom-Primary-OCS	No	No	No	No	No	No	No	No
Custom-Requested-APN	No	No	No	No	No	No	No	No
Custom-Secondary-OCS	No	No	No	No	No	No	No	No
Custom-Session-Access-Method	No	No	No	No	No	No	No	No
Custom-Session-Charging-Type	No	No	No	No	No	No	No	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
DSCP_IP_Address	No	No	No	No	No	No	No	No
EAP-Message	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Ecs-List-of-Service-Data	No	No	No	No	No	No	No	No
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

Attribute	standard	3gpp	3gpp2	3gpp2-835	starent	starent-835	starent-vsa1	starent-vsa1-835
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
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
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
Intelligent-Network-Service-Key	No	No	No	No	No	No	No	No
IN-Time-Period	No	No	No	No	No	No	No	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
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
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
MS-CHAP-Challenge	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
MS-CHAP-Domain	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
MS-CHAP-Error	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
MS-CHAP-Response	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
MSISDN	No	No	No	No	No	No	No	No
MSK	No	No	No	No	Yes	No	Yes	No
MS-MPPE-Recv-Key	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
MS-MPPE-Send-Key	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
MS-Primary-DNS-Server	No	No	No	No	No	No	Yes	No
MS-Primary-NBNS-Server	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
MS-Secondary-DNS-Server	No	No	No	No	No	No	Yes	No
MS-Secondary-NBNS-Server	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes

Attribute	standard	3gpp	3gpp2	3gpp2-835	starent	starent-835	starent-vsa1	starent-vsa1-835
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
NEtype	No	No	No	No	No	No	No	No
Password-Retry	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
PMA-Capability-Indicator	No	No	No	No	No	No	No	No
PMA-Indicator	No	No	No	No	No	No	No	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
Preservation-Indicator	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
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
Served-MDN	No	No	No	No	No	No	No	No
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
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

Attribute	standard	3gpp	3gpp2	3gpp2-835	starent	starent-835	starent-vsa1	starent-vsa1-835
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
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

Attribute	standard	3gpp	3gpp2	3gpp2-835	starent	starent-835	starent-vsa1	starent-vsa1-835
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-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
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

Attribute	standard	3gpp	3gpp2	3gpp2-835	starent	starent-835	starent-vsa1	starent-vsa1-835
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
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

Attribute	standard	3gpp	3gpp2	3gpp2-835	starent	starent-835	starent-vsa1	starent-vsa1-835
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
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

Attribute	standard	3gpp	3gpp2	3gpp2-835	starent	starent-835	starent-vsa1	starent-vsa1-835
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
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
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

Attribute	standard	3gpp	3gpp2	3gpp2-835	starent	starent-835	starent-vsa1	starent-vsa1-835
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
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-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

Attribute	standard	3gpp	3gpp2	3gpp2-835	starent	starent-835	starent-vsa1	starent-vsa1-835
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-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
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

Attribute	standard	3gpp	3gpp2	3gpp2-835	starent	starent-835	starent-vsa1	starent-vsa1-835
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
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-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

Attribute	standard	3gpp	3gpp2	3gpp2-835	starent	starent-835	starent-vsa1	starent-vsa1-835
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
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-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

Attribute	standard	3gpp	3gpp2	3gpp2-835	starent	starent-835	starent-vsa1	starent-vsa1-835
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
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-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-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

Attribute	standard	3gpp	3gpp2	3gpp2-835	starent	starent-835	starent-vsa1	starent-vsa1-835
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
State	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Terminal-Capability	No	No	No	No	No	No	No	No
Termination-Action	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Transparent-Data	No	No	No	No	No	No	Yes	No
Transparent-VSA	No	No	No	No	No	No	No	No
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
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-Hotline-Indicator	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

Attribute	standard	3gpp	3gpp2	3gpp2-835	starent	starent-835	starent-vsa1	starent-vsa1-835
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-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
XGP-AAA-CoS	No	No	No	No	No	No	No	No
XGP-AAA-QoS-Number	No	No	No	No	No	No	No	No
XGP-AAA-TIME	No	No	No	No	No	No	No	No
XGP-BS-IP-Address	No	No	No	No	No	No	No	No
XGP-FILE-VERSION	No	No	No	No	No	No	No	No
XGP-QoS-Number	No	No	No	No	No	No	No	No
XGP-Sequence-Number	No	No	No	No	No	No	No	No