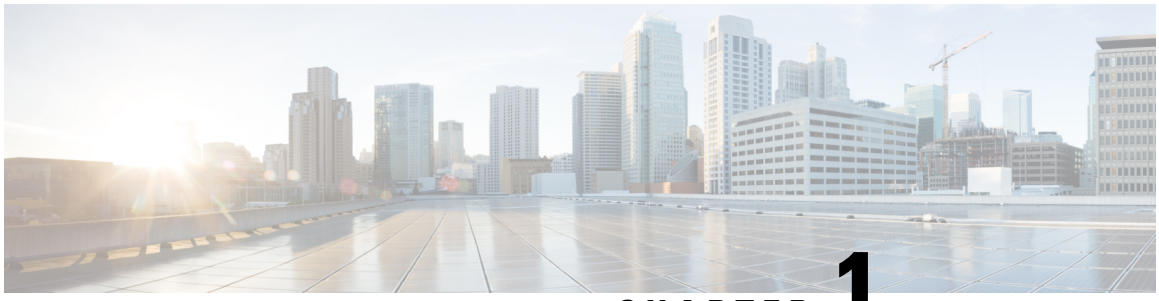
AAA Interface Administration and Reference, StarOS Release 21.19

First Published: 2020-04-30

Last Modified: 2020-05-11

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

CONTENTS



CHAPTER 1

About this Guide

Note Control and User Plane Separation (CUPS) represents a significant architectural change in the way StarOS-based products are deployed in the 3G, 4G, and 5G networks. Unless otherwise specified, it should not be assumed that any constructs (including, but not limited to, commands, statistics, attributes, MIB objects, alarms, logs, services) referenced in this document imply functional parity between legacy/non-CUPS and CUPS products. Please contact your Cisco Account or Support representative for any questions about parity between these products

Note The documentation set for this product strives to use bias-free language. For purposes of this documentation set, bias-free is defined as language that does not imply discrimination based on age, disability, gender, racial identity, ethnic identity, sexual orientation, socioeconomic status, and intersectionality. Exceptions may be present in the documentation due to language that is hardcoded in the user interfaces of the product software, language used based on RFP documentation, or language that is used by a referenced third-party product.

Note The HA, HSGW, PDSN, and SecGW products have reached end of life and are not supported in this release. Any references to these products (specific or implied) their components or functions including CLI commands and parameters in this document are coincidental and are not supported. Full details on the end of life for these products are available at https://www.cisco.com/c/en/us/products/collateral/wireless/asr-5000-series/eos-eol-notice-c51-740422.html.

This preface describes the *AAA Interface Administration and Reference*, how it is organized and its document conventions.

Authentication, Authorization, and Accounting (AAA) is a StarOS™ service that runs on Cisco® ASR 5500 and virtualized platforms.

This document provides information on basic AAA features, and how to configure the AAA interface to enable AAA functionality for your core network service subscribers in a wireless carrier network.

Conventions Used

The following tables describe the conventions used throughout this documentation.

Icon	Notice Type	Description
Image missing	Information Note	information about important features or instructions.
Image missing	Caution	Alerts you of potential damage to a program, device, or system.
Image missing	Warning	Alerts you of potential personal injury or fatality. May also alert you of potential electrical hazards.

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**

Supported Documents and Resources

Related Documentation

The most up-to-date information for this product is available in the product *Release Notes* provided with each software release.

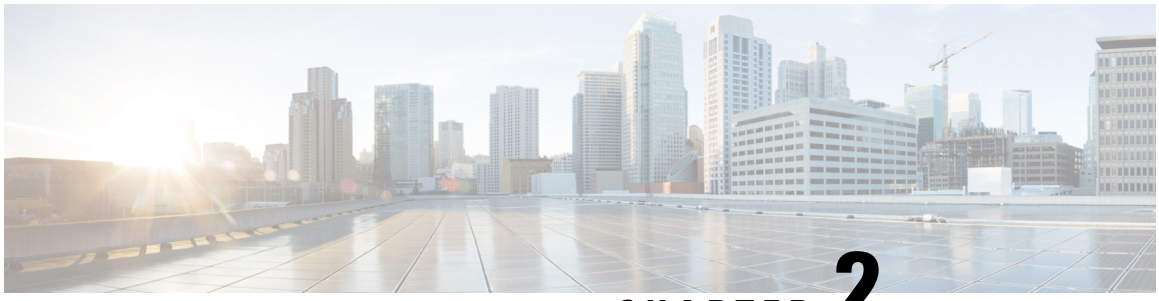
The following related product documents are also available:

- *ASR 5500 Installation Guide*
- *Command Line Interface Reference*
- *GTPP Interface Administration and Reference*
- *IPSec Reference*
- Platform-specific System Administration Guides
- Product-specific Administration Guides
- *Release Change Reference*
- *SNMP MIB Reference*
- *Statistics and Counters Reference*
- *Statistics and Counters Reference - Bulk Statistics Descriptions*
- *Thresholding Configuration Guide*

Contacting Customer Support

Use the information in this section to contact customer support.

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 are required to access this site. Please contact your Cisco sales or service representative for additional information.



CHAPTER 2

AAA Introduction and Overview

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

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

Overview

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

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

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

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

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

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

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

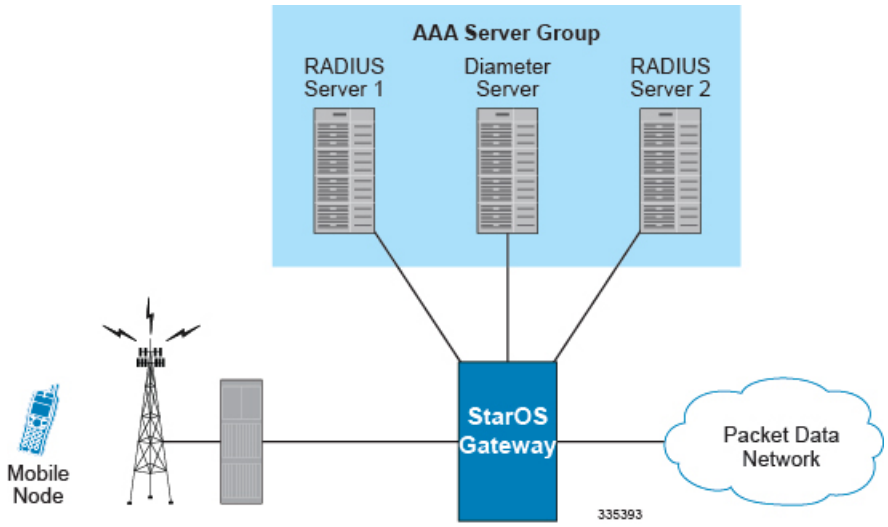
  Accounting enables operator to analyze the services users are accessing as well as the amount of network resources they are consuming. Accounting records are comprised of accounting AVPs and are stored on the accounting server. This accounting information can then be analyzed for network management,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

Advantages of using AAA are:

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

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

Figure 1: AAA Server Group Configuration in Core Network



Product Support Matrix for AAA

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

Note In Release 20.0 and later, HNBGW is not supported. For more information, contact your Cisco account representative.

Product Name	Diameter Accounting	Diameter Authentication	RADIUS
Access Service Network Gateway (ASN-GW)	X	X (EAP)	X

Product Name	Diameter Accounting	Diameter Authentication	RADIUS
Femto Network Gateway (FN-GW)	N/A	N/A	X
Gateway GPRS Support Node (GGSN)	X	X (S6b)	X
Home Agent (HA)	N/A	N/A	X
Home NodeB Gateway (HNB-GW)	N/A	N/A	X
HRPD Serving Gateway (HS-GW)	X	X (STa)	N/A
IP Services Gateway (IPSG)	N/A	N/A	X
Mobility Management Entity (MME)	N/A	X (S6a/S13)	N/A
Packet Data Gateway/Tunnel Termination Gateway (PDG/TTG)	N/A	X (SWm)	X
Packet Data Interworking Function (PDIF)	N/A	X (EAP)	X
Packet Data Support Node (PDSN)	N/A	N/A	X
Packet Data Network (PDN) Gateway (P-GW)	X	X (S6b)	X
Session Control Manager (SCM)	X	X (Cx)	X
Serving GPRS Support Node (SGSN)	N/A	X (S6d)	N/A
Serving Gateway (S-GW)	X	N/A	X

Qualified Platforms

AAA is a StarOS service that runs on Cisco ASR 5500 and virtualized platforms. For additional platform information, refer to the appropriate *System Administration Guide* and/or contact your Cisco account representative.

License Requirements

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

Diameter Proxy

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

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

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

In 18.0 and later releases, Diameter Proxy has been scaled to handle more number of transactions per proxy, and support the requirement for the DPC2 card in ASR 5500. To support this scaling architecture, a new framework "proclet-map-frwk" has been developed. This framework works in Client-Server model. For diamproxy enhancement, diactrl will act as the server and the proclets (sessmgr and aaamgr) act as client. The framework will maintain a set of tables in both Client and Server which contains details about the endpoint to diamproxy association.

In support of this feature, the existing CLI command **require diameter-proxy** has been enhanced to allow multiple Diameter proxies per card and specify the proxy selection algorithm type in ASR 5500. For more information on this command, refer to the *Command Line Interface Reference*.

Important After you configure the **require diameter-proxy** CLI command, you must save the configuration and then reload the chassis for the command to take effect. For information on saving the configuration file and reloading the chassis, refer to the *System Administration Guide* for your deployment.

Supported Features

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

Diameter Host Select Template Configuration

This feature allows the user to configure Diameter host template at Global Configuration level. Diameter host template is a table of peer servers that can be shared by different Diameter services. This template can be configured using **diameter-host-template** command in the Global Configuration Mode.

Note Currently, only Gx service can be associated with the template.

When this command is configured, it allows the user to specify the name of a new or existing Diameter host template and then enters the Diameter Host Select mode. You can configure up to 256 templates on the system.

To use the template, Diameter applications must be associated with the template. For example, using **diameter host-select-template** command in Policy Control Configuration Mode will bind the IMS authorization service to the configured Diameter host select template. When an association is made to the template, the system selects the Diameter peer to be contacted based on rows configured in the table and the algorithm configured for selecting rows in the table. The system uses the returned host name(s) to contact the primary PCRF (and secondary if configured) and establish the call.

If no association is made to the template then the **diameter peer-select** command configured at the application level will be used for peer selection.

If more than one service is using the same set of **peer-select** commands, then it is better to define all the peer selection CLI commands in the template and associate the services to the template.

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

Diameter Server Selection for Load-balancing

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

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

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

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

DSCP Marking for Signaling Traffic

This feature is introduced to prioritize the signaling traffic based on DSCP marking on the IP packets of the signaling messages. Diameter signaling messages also need to be marked with DS code points to classify/manage network traffic and provide Quality of Service (QoS).

Command **dscp** in the Diameter endpoint configuration mode is used to set the Differential Services Code Point (DSCP) in the IP header of the Diameter messages sent from the Diameter endpoint.

The following recommended Per-Hop-Behaviours are predefined:

PHB	Description	DSCP value	TOS value
BE	Best effort PHB (Default)	000 000 (0)	0

PHB	Description	DSCP value	TOS value
EF	Expedited Forwarding PHB	101 110 (46)	184
AF11	Assured Forwarding Class 1 low drop PHB	001 010 (10)	40
AF12	Assured Forwarding Class 1 medium drop PHB	001 100 (12)	48
AF13	Assured Forwarding Class 1 high drop PHB	001 110 (14)	56
AF21	Assured Forwarding Class 2 low drop PHB	001 010 (18)	72
AF22	Assured Forwarding Class 2 medium drop PHB	001 100 (20)	80
AF23	Assured Forwarding Class 2 high drop PHB	001 110 (22)	88
AF31	Assured Forwarding Class 3 low drop PHB	001 010 (26)	104
AF32	Assured Forwarding Class 3 medium drop PHB	001 100 (28)	112
AF33	Assured Forwarding Class 3 high drop PHB	001 110 (30)	120
AF41	Assured Forwarding Class 4 low drop PHB	001 010 (34)	136
AF42	Assured Forwarding Class 4 medium drop PHB	001 100 (36)	144
AF43	Assured Forwarding Class 4 high drop PHB	001 110 (38)	152
CS1	Class Selector 1 PHB	001 000 (8)	32
CS2	Class Selector 2 PHB	010 000 (16)	64
CS3	Class Selector 3 PHB	011 000 (24)	96
CS4	Class Selector 4 PHB	100 000 (32)	128
CS5	Class Selector 5 PHB	101 000 (40)	160
CS6	Class Selector 6 PHB	110 000 (48)	192
CS7	Class Selector 7 PHB	111 000 (56)	224

Note the difference between DSCP and the TOS values. TOS is an 8 bit field, but DSCP uses only the leading 6 bits of the TOS field.

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

Dynamic Diameter Dictionary Configuration

Apart from the standard and customer-specific dictionaries supported currently in the Diameter application, this feature allows the dynamic configuration of any new Diameter dictionaries at run time. This feature can be configured using **diameter dynamic-dictionary** command in the Global Configuration Mode. For more information on this command, refer to the *Command Line Interface Reference*.

Note Up to a maximum of 10 dynamic dictionaries can be configured and loaded in to the system.

To perform this configuration, a text file should be created in ABNF format and all the required Diameter AVPs and command codes should be configured in the file. Then, the file should be saved in flash or some URL that will be accessible by the system. Now, run the **dict_validate.exe** authentication tool on the created dynamic dictionary text file. This authentication tool does basic syntax checks on the file and prepends the file contents with an MD5 checksum. This checksum ensures that the dictionary cannot be modified once created. Currently, only Cisco personnel can access the authentication tool **dict_validate.exe**.

Note It is highly necessary that you must not create dynamic dictionary for your customization needs. Contact your Cisco account representative for any new dynamic dictionary creation request.

Now, configure a dynamic dictionary with an unique name and map it to the URL of the file to be loaded dynamically in to the system at the global configuration level.

When the names of the dynamic dictionaries and their URLs are configured, the corresponding files at the respective URLs are parsed and populated in all SessMgr and AAAmgr facilities as new dictionaries and kept available to be used when these dictionary names are configured under any Diameter application level or AAA group.

When a dynamic dictionary name is configured under an application such as IMS authorization service or in a AAA group, the corresponding dictionary (which is already loaded in SessMgrs and AAAMgrs) entry will be used.

There will be only one instance of a dynamic dictionary loaded in to a task for one dynamic dictionary name even if the same dictionary name is configured in multiple AAA groups or multiple application configurations. That is, even if the same dictionary name is configured in several applications or several AAA groups, all these applications and AAA groups will refer to the same dynamic dictionary instance.

Failure Handling Template Configuration

This feature allows the user to configure Failure Handling template at Global Configuration level. The failure handling template defines the action to be taken when the Diameter application encounters a failure for example, a result-code failure, tx-expiry or response-timeout. The application will take the action given by the template. This template can be configured using **failure-handling-template** command in the Global Configuration Mode.

Note A maximum of 64 templates can be configured on the system.

This command specifies the name of a new or existing failure handling template and enters the Failure Handling Template mode. Lookup is done first to identify if there is an exact match for message-type and failure-type. If not present, lookup is done for 'any' match for message and failure type.

If there are different failure handling configurations present within the template for the same message type, the action is applied as per the latest error encountered.

To use the template, Diameter applications must be associated with the template. For example, using **associate failure-handling-template** command in Credit Control Configuration Mode will bind the Diameter Credit Control Application (DCCA) service to the configured failure handling template. When an association is made to the template, in the event of a failure, the system takes the action as defined in the failure handling template. Both IMS Authorization (Gx) and DCCA (Gy) services can be currently associated with the template.

If the association is not made to the template then failure handling behavior configured in the application with the **failure-handling** command will take effect.

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

Fire-and-Forget Feature

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

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

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

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

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

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

Realm-based Routing

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

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

Dynamic Route Addition

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

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

Dynamic Route Deletion

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

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

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

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

Wildcard based Diameter Routing

This feature provides customers the ability to configure wildcard based Diameter realm routing to avoid configuring individual Diameter peers and/or realms for all possible Diameter servers in their network.

The wildcard Diameter routes can be statically configured under a Diameter endpoint configuration using the CLI "**route-entry realm * peer** *peer_name*".

These route entries are treated as default route entries and they will be selected when there is no matching host@realm based or no realm based route entry available.

The wildcard route entry can be configured in the following ways:

route-entry realm * peer *peer_name*

- or -

route-entry host * realm * peer *peer_name*

Both these configurations have the same effect; matches to any host and any realm.

The wildcard Diameter route is added along with other realm based route entries in diabase. The wildcard route entry will be selected to route a message only if the message's destination realm does not match with any of the other static realm based routes.

For example,

route-entry realm abc.com peer *peer1*

route-entry realm def.com peer *peer2*

route-entry realm * peer peer-default

If the message's destination realm is *abc.com* then the message will be routed to *peer1*. If the message's destination realm is *def.com* then the message will be routed to *peer2*. If the destination realm is *xyz.com* then the message will be routed to "*peer-default*".

When multiple wildcard route entries are configured with same weights, then the routes are selected in a round robin fashion. When multiple wildcard route entries are configured with different weights, then the route with the highest weight will be selected.

In case when there are multiple wildcard routes with higher and equal weights and some routes with lower weights, then only the higher weight routes will be selected in round robin-fashion. The lower weight route can be selected only when the higher weight routes are not valid because of the peers being not in good state.

Rate Limiting Function (RLF)

Note Rate Limiting Function (RLF) is a license-controlled feature. A valid feature license must be installed prior to configuring this feature. Contact your Cisco account representative for more information.

Th RLF feature implements a generic framework that can be used by multiple interfaces and products for rate-limiting/throttling outgoing messages like Diameter messages on Gx, Gy interface towards PCRF.

When applications send messages to peers at a high rate, (e.g. when a large number of sessions goes down at the same time, accounting stop messages for all the sessions are generated at the same time) the peer may not be able to handle the messages at such high rates. To overcome this situation, the Rate Limiting Function (RLF) framework is developed so that the application sends messages at an optimal rate such that peer is capable of receiving all the messages and does not enter an overload condition.

This feature can be enabled using the CLI command **rlf-template**in the Global Configuration mode. The users can define the rate limiting configurations within this template. For more information on the command, see the *Command Line Interface Reference*.

Note RLF template cannot be deleted if it is bound to any application (peers/endpoints).

When RLF feature is enabled, all the messages from the application are pushed to the RLF module for throttling and rate control, and depending on the message-rate configured the RLF module sends the messages to the peer. Once the rate or a threshold value is reached, the RLF module notifies the application to slow down or stop sending messages. RLF module also notifies the application when it is capable of accepting more messages to be sent to the peer. RLF module typically uses a Token Bucket Algorithm to achieve rate limiting.

Currently in the deployment of the Diameter applications (Gx, Gy, etc.), many operators make use of "**max-outstanding** <*number*>" as a means of achieving some rate-limiting on the outgoing control traffic. With RLF in place, this is no longer required since RLF takes care of rate-limiting in all cases. If RLF is used and **max-outstanding** is also used, there might be undesirable results.

Note If RLF is being used with an "**diameter endpoint**", then set the **max-outstanding** value of the peer to be 255.

To use the template, Diameter or any other applications must be associated with the template. The RLF provides only the framework to perform the rate limiting at the configured Transactions Per Second (TPS). The applications (like Diameter) should perform the configuration specific to each application.

Truncation of Diameter Origin Host Name

Diameter host name is too long for the customer network to handle and process. The host name cannot be changed as it remains constant throughout the lifecycle of client application. So, a new CLI configuration **require diameter origin-host-abbreviation** is introduced in the Global Configuration mode to control the truncation of Diameter origin-host name.

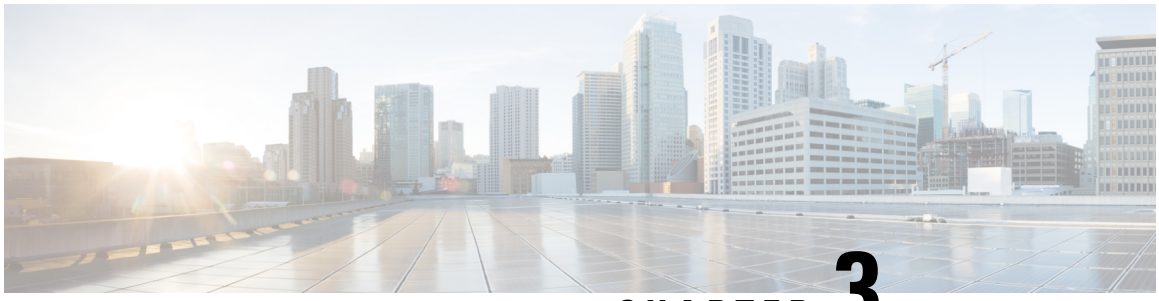
The Diameter origin-host-name is represented as <*instance-number*>-<*procletname*>.<*name*>, where the proclet name can be sessmgr, diamproxy or aaamgr.

The **require diameter origin-host-abbreviation** CLI command aids in reducing the length of Diameter origin-host names by using "d" instead of "diamproxy", "s" instead of "sessmgr", and "a" instead of "aaamgr". If this CLI command is configured then the Diameter origin-host-name value is constructed with the corresponding proclet name abbreviations.

For example, if a Diameter proxy is used to connect to a peer then the origin host will be *0001-diamproxy.endpoint* without the CLI configuration. When the **require diameter origin-host-abbreviation** CLI command is enabled, the origin host will be *0001-d.endpoint*.

Note This CLI configuration is applicable only at the time of system boot. If the CLI command is configured during run time, the following warning message is displayed "Warning: System already has running services, save config and reboot to take effect".

For more information on CLI configuration, see the *Command Line Interface Reference* guide.



CHAPTER 3

AAA Interface Configuration

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

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

This chapter includes the following information:

Configuring RADIUS AAA Functionality

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, on page 17 section.

Step 2 Configure system-level AAA parameters as described in the Configuring System-Level AAA Functionality, on page 27 section.

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

Note 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.

Note 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*.

Note 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, on page 28 section.

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

```
configure
     context <context_name>
          radius server <ipv4/ipv6_address> key <shared_secret> [ max <value> ]
[ oldports | port <tcp_port> ] [ priority <priority> ]
          radius [ mediation-device ] accounting server <ipv4/ipv6_address>
key <shared_secret> [ acct-on { enable | disable } ] [ acct-off { enable |
disable } ] [ max <msgs> ] [ oldports ] [ port <port_number> ] [ priority
<priority> ] [ type standard ]
          radius attribute nas-identifier <identifier>
          radius attribute nas-ip-address address <primary_ipv4/ipv6_address>
 [ backup <secondary_ipv4/ipv6_address> ]
          radius strip-domain [ authentication-only | accounting-only ]
          end
```

Notes:

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

  aaa large-configuration

Important After you configure this command, you must save the configuration and then reload the chassis for the command to take effect. For information on saving the configuration file and reloading the chassis, refer to the *System Administration Guide* for your deployment.

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

  radius dictionary { 3gpp | 3gpp2 | 3gpp2-835 | custom*XX* **| standard | starent | starent-835 | starent-vsa1 | starent-vsa1-835 }**
- *Optional.* Configure the system to support NAI-based authentication in the event that the system cannot authenticate the subscriber using a supported authentication protocol. To enable NAI-construction, in the Context Configuration Mode, use the following command:

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

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

  If authentication type is set to allow-noauth or msid-auth and aaa constructed-nai authentication use-shared-secret-password is issued then the system will use RADIUS shared secret as password. In case the authentication type is msid-auth it will always send RADIUS shared secret as password by default in ACCESS-REQUEST.
- *Optional.* To configure the system to allow a user session even when all authentication servers are unreachable, in the Context Configuration Mode, use the following command. When enabled, the session is allowed without authentication. However, the accounting information is still sent to the RADIUS accounting server, if it is reachable.

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

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

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

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

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

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

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

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

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

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

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

Verifying your configuration

To verify your 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 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, on page 21 section.

Step 2 Configure Diameter context-level AAA parameters as described in the Configuring Diameter AAA Functionality at Context Level, on page 23 section.

Step 3 Configure system-level AAA parameters as described in the Configuring System-Level AAA Functionality, on page 27 section.

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

Note 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.

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

Configuring Diameter Endpoint

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

Use the following configuration example to configure Diameter endpoint:

```
configure
     context <context_name>
          diameter endpoint <endpoint_name>
               origin host <host_name> address <ipv4/ipv6_address> [ port
<port_number> ] [ accept-incoming-connections ] [ address
<ipv4/ipv6_address_secondary> ]
              peer <peer_name> [ realm <realm_name> ] address <ipv4/ipv6_address>
 [ [ port <port_number> ] [ connect-on-application-access ] [
send-dpr-before-disconnect [ disconnect-cause <disconnect_cause> ] ] [ sctp
] ]+
               end
```

Notes:

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

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

  Important After you configure this command, you must save the configuration and then reload the chassis for the command to take effect. For information on saving the configuration file and reloading the chassis, refer to the *System Administration Guide* for your deployment.

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

  use-proxy

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

  origin realm <*realm_name*>

- <*realm_name*> is typically a company or service name. The realm is the Diameter identity and will be present in all Diameter messages.

- *Optional.* To create an entry in the route table for the Diameter peer, in the Diameter Endpoint Configuration Mode, use the following command:

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

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

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

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

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

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

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

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

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

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

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

  connection timeout <*timeout*>

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

  connection retry-timeout <*retry_timeout*>

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

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

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

  max-outstanding <*msgs*>

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

  response-timeout <*duration*>

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

  watchdog-timeout <*duration*>

Configuring Diameter AAA Functionality at Context Level

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

This section describes how to configure the Diameter-based AAA parameters at the context level. To configure Diameter-based AAA parameters at the system level, see the Configuring System-Level AAA Functionality, on page 27 section.

Note 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, on page 21 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 Diameter Failure Handling Template

This section describes how to configure Diameter Failure Handling Template at the global level.

The failure handling template defines the action to be taken when the Diameter application encounters a failure for example, a result-code failure, tx-expiry or response-timeout. The template can be used by any Diameter application that needs failure handling behavior.

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

```
configure
     failure-handling <template_name>
          msg-type { any | authentication info request |
authorization-request | check-identity-request | credit-control-initial
| credit-control-terminate | credit-control-update | eap-request |
eap-termination-request | notify-request | profile-update-request |
purge-ue-request | update-location-request | user-data-request }
failure-type { any | diabase-error | diameter result-code { any-error |
result-code [ to end-result-code ] } | diameter exp-result-code { any-error |
result-code [ to end-result-code ] } | resp-timeout | tx-expiry } action {
continue [ local-fallback | send-ccrt-on-call-termination | without-retry
 ] | retry-and-terminate | terminate }
          end
```

Notes:

- A maximum of 64 templates can be configured on the system.
- Diameter applications (Gx, Gy) must be associated with the template. For example, using **associate failure-handling-template** command in Credit Control Configuration Mode will bind the Diameter Credit Control Application (DCCA) service to the configured failure handling template. When an association is made to the template, in the event of a failure, the system takes the action as defined in the failure handling template.
- For information on the commands, refer to the *Diameter Failure Handling Template Configuration Mode Commands* chapter of the *Command Line Interface Reference*.

Configuring Dynamic Diameter Dictionary

This section describes how to configure Dynamic Diameter dictionary at the global level.

The Diameter dictionaries can be configured dynamically at run time.

To configure Dynamic Diameter dictionary at the global level use the following configuration:

```
configure
     diameter dynamic-dictionary <dict_name> <url>
     end
```

Notes:

- A maximum of 10 dynamic dictionaries can be configured and loaded in to the system.
- The dynamically loaded dictionaries can be configured under application group or AAA group using the option **dynamic-load** in the **diameter accounting dictionary** or **diameter authentication dictionary** command.
- For more information on the command, refer to the *Global Configuration Mode (A-K) Commands* chapter of the *Command Line Interface Reference*.

Verifying Your Configuration

To verify your configurations:

In the Exec mode, enter the following command:

show diameter dynamic-dictionary all [contents]

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

Configuring Rate Limiting Function Template

This section describes how to configure Rate LimitingFunction (RLF) Template at the global level.

Note Rate Limiting Function (RLF) is a license-controlled feature. A valid feature license must be installed prior to configuring this feature. Contact your Cisco account representative for more information.

The RLF template defines the rate limiting configurations for example, a threshold for rate-limiting the outgoing messages. The template can be used by any product/interface that needs to throttle and rate control the messages sent to the external network interfaces.

To configure RLF template at the global level use the following configuration:

```
configure
      rlf-template <template_name>
            delay-tolerance tolerance_value [ -noconfirm ]
            msg-rate tps_value burst-size size [ -noconfirm ]
            threshold { lower lowerThreshold_value | upper
upperThreshold_value } [ -noconfirm ]
            end
```

For information on the commands, refer to the *Rate Limiting Function Template Configuration Mode Commands* chapter of the *Command Line Interface Reference*.

Verifying Your Configuration

To verify your configurations:

In the Exec mode, enter the following command:

show rlf-template all

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

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.

Note 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, on page 29 section.

- Apply the AAA Server Group to subscriber as described in the Applying a AAA Server Group to a Subscriber, on page 31 section.

  –or–

- Apply the AAA server-group to an APN as described in the Applying a AAA Server Group to an APN, on page 32 section.

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

Note 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.

Note 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.

Important After you configure the **aaa large-configuration** CLI command, you must save the configuration and then reload the chassis for the command to take effect. For information on saving the configuration file and reloading the chassis, refer to the *System Administration Guide* for your deployment.

- *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

Important After you configure the **aaa large-configuration** CLI command, you must save the configuration and then reload the chassis for the command to take effect. For information on saving the configuration file and reloading the chassis, refer to the *System Administration Guide* for your deployment.

- *<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.

Important After you configure the **aaa large-configuration** CLI command, you must save the configuration and then reload the chassis for the command to take effect. For information on saving the configuration file and reloading the chassis, refer to the *System Administration Guide* for your deployment.

- 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, on page 17 section.
- To configure and verify Diameter authentication and accounting servers and parameters within the AAA server group, refer to the Configuring Diameter AAA Functionality, on page 20 section.

Verifying Your Configuration

To verify your configuration:

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

Step 2 Display the context's configuration by entering the following command:
show configuration context <*context_name*>

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

Note 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, on page 29 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, on page 29 section.

Verifying APN Configuration

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

Step 2 Display the APN's configuration by entering the following command:
show apn name <*apn_name*>

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

Configuring the Destination Context Attribute

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

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

Note Note that when RADIUS servers are not configured in the selected AAA group, the servers in the default group will be considered for destination context selection. If there are no servers in the default group, then the call will be dropped.

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.

Note 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.

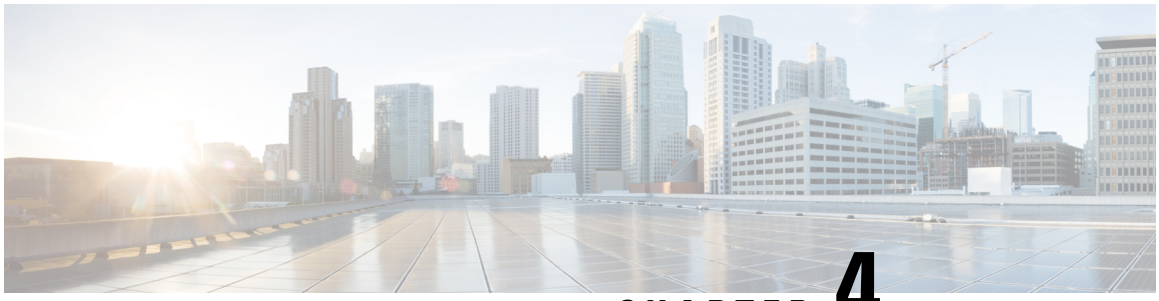
Verifying Your Configuration

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 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.

Note 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.

Note 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 **Note** 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 **Note** 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**

To do this:	Enter this command:
View RADIUS protocol counter summary of RADIUS authentication and accounting	**show radius counters summary**

Clearing Statistics and Counters

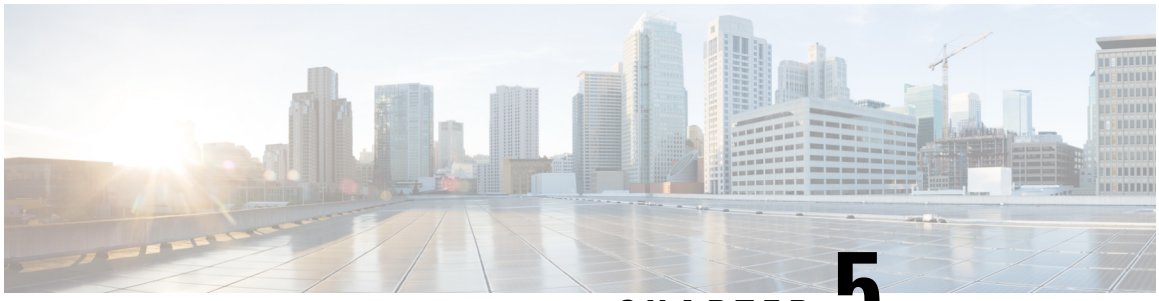
It may be necessary to periodically clear statistics and counters in order to gather new information. The system provides the ability to clear statistics and counters based on their grouping (PPP, MIPHA, MIPFA, etc.).

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

Session Recovery and AAA Statistics Behavior

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

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



CHAPTER 5

Diameter Overload Control

This chapter describes the overview and implementation of Diameter Overload Control feature on ePDG and P-GW.

This chapter discusses the following topics for this feature:

Feature Description

Overview

This feature is implemented to support Overload Control on Diameter interfaces such as Gx, S6b and SWm and also to prevent network overload and outages. Whenever there is an overload condition at the Diameter Servers or DRA and request times out, the clients (ePDG/P-GW) are typically unaware of the overload condition and attempt to send the message on an alternate connection with the Diameter server causing some more traffic in the network. In order to handle this overload condition effectively, a new vendor-specific Diameter Experimental Result-Code 5198 (DIAMETER_OVERLOAD_RETRY_NOT_ALLOWED_TO_ANY) is defined.

When the overloaded PCRF/DRA receives a message, it includes the result-code 5198 in the response message. On receiving the experimental result-code, call is terminated based on the failure-handling configuration. If failure-handling is configured as local-policy, then the call is continued with local-policy without retrying the secondary server.

In Releases prior to 19, no indication was available to P-GW and ePDG when the Diameter Server or the DRA is overloaded. When a message sent to the primary link on Diameter is dropped or unanswered, P-GW/ePDG tried the same message on the secondary peer and resulted in the overloading of Diameter Server.

In 19 and later releases, the following changes are implemented to support Overload Control on Gx interface:

- A new vendor-specific Diameter Experimental Result-Code 5198 (DIAMETER_OVERLOAD_RETRY_NOT_ALLOWED_TO_ANY) is added to indicate the overload state of PCRF.
- When the failure handling template is not configured and if the Experimental Result-Code (5198) is received in CCR-U, then the current call is terminated.
- If the Assume Positive feature is configured, the call is continued without retrying the secondary server.

- The default action for Experimental Result-Code error (5198) is retry and terminate. Retry and terminate will be the failure handing action irrespective of the configured value.
- New statistics are added to the output of **show ims-authorization policy-control statistics** command to display the number of times the Experimental Result-Code 5198 has been received. Separate statistics are also introduced to display the message level information.

To support Overload Control on S6b and SWm interfaces, the following changes are implemented:

- A new vendor-specific Diameter Experimental Result-Code 5198 (DIAMETER_OVERLOAD_RETRY_NOT_ALLOWED_TO_ANY) is added to indicate the overload state of Diameter agent.
- Failure handling template is introduced for S6b and SWm interfaces, and associated to AAA group authentication.
- The default action for Experimental Result-Code (5198) is retry and terminate. For Diabase error, the failure-handling action will be retry and terminate irrespective of the configured value.
- When the Experimental Result-Code (5198) is received and the **failure-handling** command is configured as **continue**, then call is continued without retrying the secondary server. The **continue** action is applicable only to aaa-custom15 dictionary.
- When the Result-Code (5198) is received in DEA/AAA request, the call is terminated without the Session Terminate Request (STR) for S6b and SWm interfaces.
- New statistics are added to the output of **show diameter aaa-statistics** to indicate the number of times the specific failure handling actions are applied through the failure-handling template.
- When GGSN/P-GW receives the experimental result code 5198, the GTP cause code is mapped to NO_RESOURCES_AVAILABLE.

Relationships to Other Features

Diameter Overload Control feature interworks with Assume Positive feature. The failure handling action depends on the configuration of Assume Positive feature and Diameter Overload Control feature. If the Assume Positive feature is configured and Diameter Overload Control feature is enabled, the call is continued without retrying the secondary PCRF server.

Limitations

The following are the limitations of this feature:

- It is assumed that the Diameter Agent (DRA or MRA on PCRF) should be able to identify that the servers within its own segment and in alternate segments are overloaded as well.
- If the failure handling template is present, then the configuration to terminate the call on receiving the Experimental-Result-Code (5198) should be enabled. If the configuration is to retry and terminate, then the message is retried to the secondary server.
- CLI command to not send terminate message should be configured under the failure handling template.
- For S6b/SWm, for diabase error, the failure-handling action will be retry and terminate irrespective of the configured value.
- For terminate wo-term-req will work only when Experimental-Result-Code (5198) is received. For rest, it will be treated as terminate.

Configuring Diameter Overload Control

The following sections provide the configuration commands to enable the Overload Control on Diameter Interfaces.

Defining Failure Handling Template

The failure handling template defines the action to be taken when the Diameter application encounters a failure supposing a result-code failure, Tx-expiry or response-timeout. The application will take the action given by the template.

The commands illustrated below define the failure handling template.

```
configure
    failure-handling-template template_name
         end
```

Configuring Local Policy Parameters

The commands illustrated below configure the failure handling parameters. In support of the Diameter Overload Control feature, the **without-retry** keyword has been added to the failure handling template configuration to fallback to local-policy without retrying the secondary PCRF server.

```
configure
    failure-handling-template template_name
         msg-type { any | authentication info request |
authorization-request | check-identity-request | credit-control-initial
| credit-control-terminate | credit-control-update | eap-request |
eap-termination-request | notify-request | profile-update-request |
purge-ue-request | update-location-request | user-data-request }
failure-type { any | diabase-error | diameter result-code { any-error |
result-code [ to end-result-code ] } | diameter exp-result-code { any-error |
result-code [ to end-result-code ] } | resp-timeout | tx-expiry } action {
continue [ local-fallback [ without-retry ] | retry-server-on-event |
send-ccrt-on-call-termination | without-retry ] | retry-and-terminate [
max-transmissions | without-term-req ] | terminate [ without-term-req ]
}
         end
```

Notes:

- **without-retry**: This keyword specifies to continue the session without retrying the secondary PCRF server, when in Assume Positive mode. By default, the Diameter message is retried to secondary PCRF before falling back to local-policy.
- This keyword is introduced to support Overload Control on Diameter interfaces such as Gx, S6b and SWm and also to prevent network overload and outages. For more information on the commands used in this configuration, refer to the *Command Line Interface Reference* guide.

Associating Failure Handling Template

The commands illustrated below associate a configured failure handling template with the AAA group authentication application.

```
configure
    context context_name
        aaa group group_name
           diameter authentication failure-handling-template template_name

             end
```

Notes:

- **failure-handling-template**: Associates the failure handling template to the authentication interface. By default, the template is not associated in the AAA Group.
- When the **failure-handling-template** is configured and the **failure-handling** CLI is also enabled in the AAA Group configuration, the template is given the higher preference.

Verifying the Diameter Overload Control Configuration

Use the following commands in Exec mode to display/verify the configuration of Diameter Overload Control feature.

show diameter aaa-statistics

show ims-authorization policy-control statistics

Monitoring and Troubleshooting the Diameter Overload Control Feature

This section provides information regarding show commands and/or their outputs in support of the Diameter Overload feature on the ePDG and P-GW.

show diameter aaa-statistics

The following statistics are added to the output of the **show diameter aaa-statistics** command to track the number of times the Experimental Result-Code (5198) is received from PCRF.

- FH Behavior – Indicates the number of times the specific failure handling action is applied through the failure-handling-template.
  - Continue
    - With Retry
    - Without Retry
  - Retry and Terminate
    - Retry and Terminate
    - Retry Term without STR

  - Termination
    - Terminate
    - Terminate without STR

- Diameter Overload Control Stats – Indicates the number of times the Result-Code 5198 is received in a message.
  - AAA
  - DEA

show ims-authorization policy-control statistics

The following statistics are added to the output of the **show ims-authorization policy-control statistics** command to track the number of times the Experimental Result-Code (5198) is received from PCRF.

- Diameter Overload Control – Added under DPCA Experimental Result Code Stats
- Diameter Overload Control Stats
  - CCA-Initial
  - CCA-Update
  - CCA-Terminate
- Fallback – Added under FB Behavior statistics
- Fallback Without Retry – Added under FB Behavior statistics

Debugging Statistics

When the Experimental-Result-Code 5198 is received, the call is terminated and the GTP cause code should be mapped to "No Resources Available".

```
Extension Header Flag: 0
                                  Message Type: CREATE_SESSION_RSP
EGTP-Packet:
 CAUSE(2, 0): NO_RESOURCES_AVAILABLE
```

Bulk Statistics for Diameter Overload Control Feature

Diameter Authentication Schema

The following statistics are included in the Diameter Authentication Schema in support of the Diameter Overload Control feature.

- overload-ctrl-aaa
- overload-ctrl-dea
- fh-continue-retry
- fh-continue-wo-retry
- fh-retry-and-term
- fh-retry-and-term-wo-str
- fh-terminate
- fh-terminate-wo-str

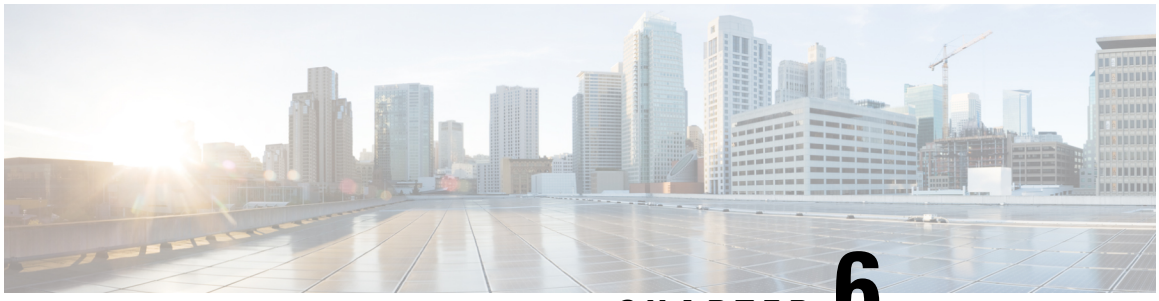
For descriptions of these variables, see the *Statistics and Counters Reference* guide.

IMSA Schema

The following statistics are included in the IMSA Schema in support of the Diameter Overload Control feature.

- dpca-expres-overload-ctrl-ccai
- dpca-expres-overload-ctrl-ccau
- dpca-expres-overload-ctrl-ccat
- dpca-ccfh-continue-lp-wo-retry

For descriptions of these variables, see the *Statistics and Counters Reference* guide.



CHAPTER 6

Diameter Records Storage on HDD

This chapter describes the overview and implementation of the feature for storing Diameter (CCR-T) Records on Hard Disk Drive (HDD) during OCS failure.

This chapter discusses the following topics for this feature:

Feature Description

Overview

ASR 5500 supports Assume Positive configurations, and this feature is tailored to provide the service to users even when the Online Charging Server (OCS) is unreachable. This Assume Positive configuration allows the users to configure the interim-quota (either volume or time or both together along with the number of retries) that can be used when the charging servers are unreachable or not responding. This feature also lets the user to configure the action to be taken when the interim-quota and retries are exhausted.

In the existing implementation with Assume Positive feature, there are high chances of losing the usage data reported through the CCR-T when the session is being terminated while in Assume Positive mode. This problem is addressed by allowing the DCCA module to write the CCR-T messages (with locally assigned quota details) in the HDD of the chassis.

In cases where the Assume-Positive interim-quota is allocated, and CCR-T is not reported/answered, the CCR-T message is written to a local file, and saved in the HDD. This local file and directory information can be fetched and parsed to account for the lost bytes/usage. The retrieval of the file can be done with the PULL mechanism.

Note This feature requires a valid license to be installed prior to configuring this feature. Contact your Cisco account representative for more information on the licensing requirements.

In releases prior to 20, failed CCR-T is written to HDD only if the session is in Assume Positive state. In Release 20 and later, the existing behavior is modified such that, even if the sessions are not in Assume Positive

state, the failed CCR-Ts are written to HDD for later processing. This enhancement is applicable for all CCR-T failures like Tx/response timeouts, result code errors, diabase errors, etc.

In case of Session Recovery, if a DCCA session which is in pending-terminate state is recovered, then a fresh CCR-T will be initiated. This CCR-T will be written to hard disk if it fails. In case of ICSR, the sessions which are already in terminating state are not recovered.

Once the bearer/session gets terminated, the same in the standby will be deleted and that session will not come up in case of ICSR.

This feature is controlled through the CLI command "**diameter hdd**" introduced in the Credit Control Group configuration mode. When the CLI configuration is enabled, the DCCA application sends the failed CCR-T messages to the CDR module for storing in the HDD.

Relationships to Other Features

This feature is applicable for sessions that are in Server-Unreachable state. That is, this feature is applicable only when Assume Positive feature is enabled.

This dependency is no longer valid in Release 20 and later. In Release 20, this feature works even if the sessions are not in Assume Positive state.

License Requirements

This feature requires a valid license to be installed prior to configuring this feature. Contact your Cisco account representative for detailed information on specific licensing requirements. For information on installing and verifying licenses, refer to the *Managing License Keys* section of the *Software Management Operations* chapter in the *System Administration Guide*.

Limitations

The following are the limitations of this feature:

- When an ICSR event occurs unexpectedly before the CCR-T is written, the CCR-T will not written to the HDD and hence the usage will be lost.
- It is expected that the customers requiring this feature should monitor the HDD and periodically pull and delete the files so that the subsequent records can be buffered.
- It is recommended not to configure PUSH mechanism for the diameter-hdd-module.
- Diameter records will not be written to the HDD when CCR-T is not generated during session termination resulting due to certain error result codes in CCA-I/CCA-U.
- If Diameter records should be dumped to the HDD for all session terminations resulting from failed CCR-Us, then it is recommended to configure the **failure-handling template** CLI command in the Global Configuration mode. In this case, the CCR-T is generated during session termination for all CCR-U failures.
- T bit is set in the HDD records for CCR-T message failures (response/tx timeout and result code errors).

Configuring Diameter Records Storage on HDD

The following sections provide the configuration commands to enable the writing of Diameter records on HDD.

Enabling HDD for Credit Control Group

The commands illustrated below enable the HDD to store the failed CCR-T messages for the corresponding credit control group.

Note This command is license dependent. For more information, contact your Cisco account representative.

```
configure
    require active-charging-service
    active-charging-service service_name
         credit-control group  ccgroup_name
              diameter hdd
              end
```

Notes:

- **diameter hdd**: This CLI enables the HDD to store the failed CCR-T messages. When enabled, the Gy application sends the failed CCR-T messages to the CDR module for storing in the HDD. By default, this feature is disabled.
- **no diameter hdd**: Removes the HDD configuration for DCCA.

Important After you configure **require active-charging-service**, **active-charging-service** *service_name*, and **credit-control group** *ccgroup_name* CLI commands, you must save the configuration and then reload the chassis for the command to take effect. For information on saving the configuration file and reloading the chassis, refer to the *System Administration Guide* for your deployment.

Configuring HDD Module for Diameter Records

The commands illustrated below configure the HDD module for saving the failed CCR-T messages.

Note This command is license dependent. For more information, contact your Cisco account representative.

```
configure
    context  context_name
         diameter-hdd-module
              end
```

Notes:

- **diameter-hdd-module**: This command enters the Diameter HDD Module Configuration mode.
- **no diameter-hdd-module**: Deletes the HDD module from the context.

Configuring HDD Parameters

The commands illustrated below configure the the HDD specific parameters such as file creation properties for Diameter records.

Note This command is license dependent. For more information, contact your Cisco account representative.

```
configure
    context  context_name
         diameter-hdd-module
              diameter-event { purge { storage-limit storage_limit |
time-limit time_limit } [ max-files max_records_to_purge ] | push-interval
push_interval | push-trigger space-usage-percent trigger_percentage |
remove-file-after-transfer | transfer-mode { pull [ module-only ] | push
 primary { encrypted-url encrypted_url | url url } [ [ max-files max_records ]
 [ max-tasks task_num ] [ module-only ] [ secondary { encrypted-secondary-url
 encrypted_secondary_url | secondary-url secondary_url } ] [ via local-context ]
 + ] | use-harddisk }
              file [ compression { gzip | none } ] [ current-prefix string
 ] [ delete-timeout seconds ] [ directory directory_name ] [
exclude-checksum-record ] [ field-separator { hyphen | omit | underscore
 } ] [ name string ] [ reset-indicator ] [ rotation [ num-records number |
tariff-time minute seconds | time seconds | volume bytes ] ] [ sequence-number
 { length length | omit | padded | padded-six-length | unpadded } ] [
storage-limit limit ] [ time-stamp { expanded-format | rotated-format |
unix-format } ] [ trailing-text string ] [ trap-on-file-delete ] [
xor-final-record ] +
              end
```

Notes:

- **purge**: Specifies to purge/delete the Diameter records based on "time" or "volume" limit.
- **push-interval**: Specifies the transfer interval (in seconds) to push Diameter files to an external server.
- **push-trigger**: Specifies the record disk space utilization percentage, upon reaching which an automatic push is triggered and files are transferred to the configured external server.
- **remove-file-after-transfer**: Specifies that the system must delete Diameter files after they are transferred to the external server. Default: Disabled
- **transfer-mode**: Specifies the file transfer mode—how the Diameter files are transferred to the external server.
- **use-harddisk**: Specifies that the hard disk be used to store Diameter files.
- **compression**: Configures the file compression option for the Diameter records.
- **current-prefix**: Prefix to use for currently used Diameter file
- **delete-timeout**: Time to delete completed files in seconds
- **directory**: Creates the record files in the directory under */records/diameter*
- **exclude-checksum-record**: Excludes checksum record in the file
- **field-separator**: Separator to be used between the file format fields
- **name**: Base filename to use to generate file
- **reset-indicator**: Includes the reset-indicator counter value in the file name
- **rotation**: Criteria to rotate the record file
- **sequence-number**: Sequence number related configuration in the file name
- **storage-limit**: Total available storage for all the record (EDR/UDR/EVENT/DIAMETER) files.
- **time-stamp**: Time stamp format to be included in the file name.
- **trailing-text**: Text to be included in the file name

- **trap-on-file-delete**: Sends an SNMP notification (trap) when an EDR/UDR/EVENT/DIAMETER file is deleted
- **xor-final-record**: xor checksum record in the file

Verifying the Diameter HDD Configuration

Use the following command in Exec mode to display whether the HDD is enabled for each of the respective credit-control groups.

```
show active-charging service all
```

Use the following command in Exec mode to display/verify the configured and used file-space statistics.

```
show diameter-hdd-module file-space-usage
```

Monitoring and Troubleshooting the Diameter Records Storage on HDD

This section provides information regarding show commands and/or their outputs in support of this feature.

show active-charging service all

The following field has been added to the output of this show command to indicate whether or not the corresponding credit-control group has been configured to write the failed CCR-Ts in HDD.

- HDD

For descriptions of this statistics, see the *Statistics and Counters Reference* guide.

show active-charging credit-control statistics

The following fields have been added to the output of this show command to display the number of records written to HDD per credit-control group.

- HDD Stats
  - CCR-T

For descriptions of these statistics, see the *Statistics and Counters Reference* guide.

show cdr statistics

The following fields have been added to the output of this show command.

- Diameter-hdd-module Record Specific Statistics
  - Diameter-hdd-module files rotated
  - Diameter-hdd-module files rotated due to volume limit
  - Diameter-hdd-module files rotated due to time limit
  - Diameter-hdd-module files rotated due to tariff-time

- Diameter-hdd-module files rotated due to records limit
- Diameter-hdd-module file rotation failures
- Diameter-hdd-module files deleted
- Diameter-hdd-module records deleted
- Diameter-hdd-module records received
- Current open Diameter-hdd-module files
- Time of last Diameter-hdd-module file deletion

For descriptions of these statistics, see the *Statistics and Counters Reference* guide.

show diameter-hdd-module file-space-usage

The following fields have been added to the output of this show command.

- CDRMOD Instance Id
- Diameter-hdd-module File Storage LIMIT
- Diameter-hdd-module File Storage USAGE
- Percentage of Diameter-hdd-module file store usage

For descriptions of these statistics, see the *Statistics and Counters Reference* guide.

show diameter-hdd-module statistics

The following fields have been added to the output of this show command.

- Diameter-hdd-Module file Statistics:
  - CDRMOD Instance Id
  - Diameter-hdd-module files rotated
  - Diameter-hdd-module files rotated due to volume limit
  - Diameter-hdd-module files rotated due to time limit
  - Diameter-hdd-module files rotated due to tariff-time
  - Diameter-hdd-module files rotated due to records limit
  - Diameter-hdd-module file rotation failures
  - Diameter-hdd-module files deleted
  - Diameter-hdd-module records deleted
  - Diameter-hdd-module records received
  - Current open Diameter-hdd-module files
  - Time of last Diameter-hdd-module file deletion
- Diameter-hdd-module PUSH Statistics:
  - Successful File Transfers
  - Failed File Transfers
  - Num of times PUSH initiated
  - Num of times PUSH Failed
  - Num of times PUSH cancelled due to HD failure
  - Num of periodic PUSH
  - Num of manual PUSH
  - Current status of PUSH

- Last completed PUSH time
- Primary Server Statistics:
  - Successful File Transfers
  - Failed File Transfers
  - Num of times PUSH initiated
  - Num of times PUSH Failed
  - Num of periodic PUSH
  - Num of manual PUSH
  - Current status of PUSH
  - Last completed PUSH time
- Secondary Server Statistics:
  - Successful File Transfers
  - Failed File Transfers
  - Num of times PUSH initiated
  - Num of times PUSH Failed
  - Num of periodic PUSH
  - Num of manual PUSH
  - Current status of PUSH
  - Last completed PUSH time

For descriptions of these statistics, see the *Statistics and Counters Reference* guide.

Debugging Statistics

If an error is encountered, it is recommended to check the error level logs (if possible trace level as well) of "acsmgr" facility.

Search for the acsmgr-error log output "Maximum size exceeded for CCRT.." to see if the HDD writing is disabled due to the max-size limit. The acsmgr-trace message "CCRT-Msg (size xxxx) has been recorded to HDD" will be displayed when a CCR-T is saved in HDD successfully.

Bulk Statistics for Diameter Records Storage on HDD

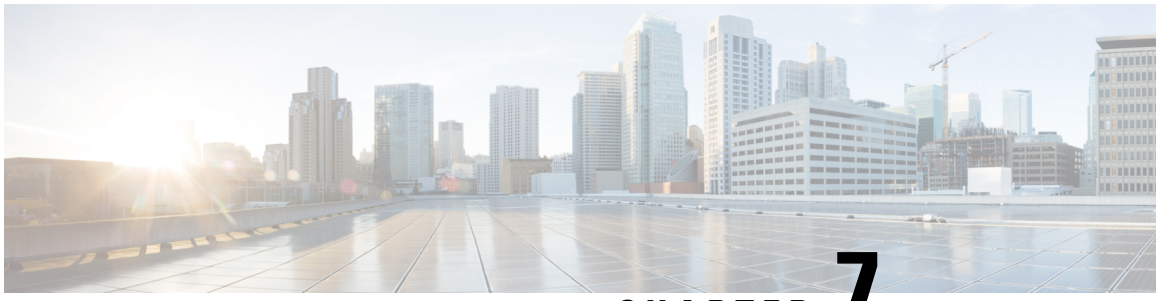
DCCA Group Schema

The following statistics is included in the DCCA Group Schema in support of this feature.

Monitoring and Troubleshooting the Diameter Records Storage on HDD, on page 49

- cc-msg-ccrt-hdd

For descriptions of this variable, see the *Statistics and Counters Reference* guide.



CHAPTER 7

Diameter Routing Message Priority (DRMP) for S6b Interface

Feature Information

Summary Data

Status	New Functionality
Introduced-In Release	21.2
Modified-In Release(s)	Not Applicable
Applicable Product(s)	All products using Diameter S6b interface
Applicable Platform(s)	ASR 5500
Default Setting	Disabled
Related CDETS ID(s)	CSCvc77714
Related Changes in This Release	Not Applicable
Related Documentation	AAA Interface Administration and Reference Command Line Interface Reference

Revision History

Important Revision history details are not provided for features introduced before release 21.2.

Revision Details	Release	Release Date
New in this release.	21.2	April 27, 2017

Feature Description

The Diameter nodes can pass overload information with the introduction of Diameter Overload Indication Conveyance (DOIC) specification. The current techniques used by the Diameter agents using S6b interface to prioritize the Diameter messages are based on static configuration in the agents. There are different use cases and needs that require a standard mechanism to choose which messages get throttled or discarded, when they go to act on the Overload information.

DRMP is a new AVP that signifies the relative priority of Diameter messages which can be used to make routing and throttling decisions. The DRMP (AVP code 301) is of type Enumerated. The value of the AVP indicates the routing message priority of the message.

How it Works

This feature allows sending of DRMP AVP in the Authentication/Authorization Request (AAR) and Session-Termination-Request (STR) messages in S6b interface through a configurable CLI command. The value to be sent in this AVP can be configured through the newly introduced CLI command, specifically and independently for below 3 types of messages:

1. AAR-Initial: The AAR message that is sent during PDN creation.
2. AAR-Interim: The AAR message that is sent during different types of Handovers and after expiry of Authorize lifetime timer, or any other AAR not sent as a part of PDN creation.
3. STR: The STR message that is sent during the PDN deletion.

When the CLI is not configured, there will not be any change in behavior and the DRMP AVP will not be sent in any message. In order to enable this feature and send DRMP AVP in the mentioned diameter messages, the CLI needs to be explicitly configured with either default or relevant values.

Standards Compliance

This feature complies with the following standard(s):

- 3GPP TS 29.273 - 3GPP EPS AAA interfaces

Configuring DRMP for S6b Interface

This section explains the configuration procedures required to enable or disable the feature.

Enabling or Disabling DRMP AVP in S6b Interface

Use the following configuration under the AAA Server Group Configuration Mode to enable or disable the inclusion of DRMP AVP in S6b communication and to configure DRMP value based on AAR-Initial, AAR-Interim and STR message types:

```
configure
   context <context_name>
       aaa group<group_name>
  diameter authentication drmp [ [aar-initial <drmp-value> [ aar-interim
 <drmp-value> [ str  <drmp-value> ] ] ] | [ aar-initial <drmp-value> [ str
<drmp-value> [ aar-interim <drmp-value> ] ] ] | [ aar-interim <drmp-value> [
aar-initial <drmp-value> [ str <drmp-value> ] ] ] | [ aar-interim <drmp-value>
 [ str <drmp-value> [ aar-initial <drmp-value> ] ] ] | [ str <drmp-value> [
aar-interim <drmp-value> [ aar-initial <drmp-value> ] ] ] | [ str
<drmp-value> [ aar-initial <drmp-value> [ aar-interim <drmp-value> ] ] ] ]
        end
```

Notes:

- **drmp:** Specifies the settings of Diameter Routing Message Priority.
- **aar-initial:** Includes the DRMP value in AAR-initial message. The default value is 10.
- **aar-interim:** Includes the DRMP value in AAR-interim message. The default value is 10.
- **str:** Includes the DRMP value in STR message. The default value is 10.
- *drmp-value:* Specifies the DRMP value and must be an integer from 0 through 15. Zero (0) has the highest priority and 15 has the lowest. That is, lower the value, higher the priority. The above command will individually configure DRMP values for the AAR-initial, AAR-interim and STR messages.
- If previously configured, use the **no diameter authentication drmp** command to prevent encoding of DRMP AVP in S6b messages. The **no diameter authentication drmp** command is the default configuration.
- If message type priority is not specified in the CLI, default value (10) will be used. The last configured CLI line will override all values previously configured, irrespective of how many priorities are explicitly configured.
- In case of configuring specific values for message types, each time the CLI is invoked, all the 3 values will be modified with the new values. If a value is not specified in CLI, it will be overwritten by default value, which is 10.

Monitoring and Troubleshooting

The following sections describe commands available to monitor the feature.

Show Commands and Outputs

This section provides information regarding show commands and their outputs for the DRMP for S6b feature.

show aaa group { name group_name | all }

The output of the above command has been enhanced to display the new (DRMP) parameter. The following sample display is only a portion of the output:

```
Group name:         default
  Context:          pgw
Diameter config:
  Authentication:
  Strip-leading-digit user-name:    Disabled
  DRMP: AAR-Initial 10 AAR-Interim 10 STR 10
```

where:

- **DRMP:** Displays the status as 'Disabled' if it's not configured through the CLI. When enabled, it displays the priority values for the corresponding messages.

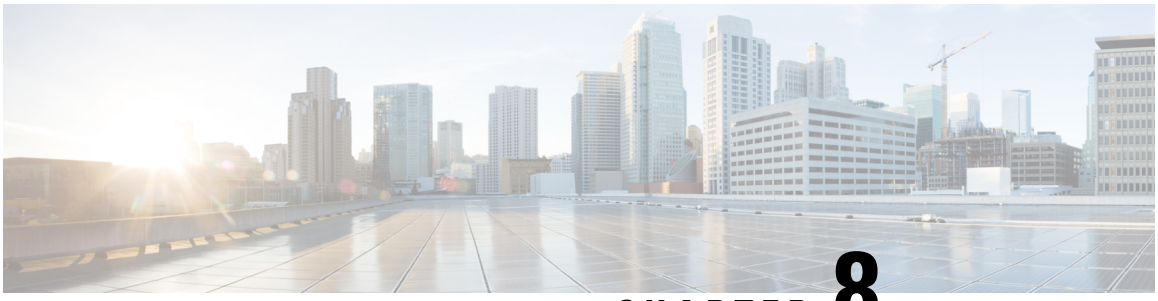
show configuration [verbose]

The output of the above command has been enhanced to display the following new fields:

```
diameter authentication drmp aar-initial <value> aar-interim <value> str <value>
```

where:

- **drmp**: Indicates Diameter Routing Message Priority.
- <*value*>: Indicates the configured priority values for the corresponding messages.



CHAPTER 8

Diameter Transaction Rate KPIs

This chapter describes the overview and implementation of Transaction Rate KPI feature on per Diameter interfaces configured in the StarOS software.

Feature Description

The existing StarOS software does not provide clearly defined Key Performance Indicators (KPIs) for measuring the session and Voice-over-LTE (VoLTE) signaling transaction rates on the gateway platforms such as eHRPD, ePDG, P-GW, SAEGW, S-GW.

Previously, KPIs did not differentiate between successful or unsuccessful PDN session activations and deactivations. In addition, the KPIs did not provide any information related to the VoLTE service.

In releases prior to 20, an external server collects bulkstats data every 2 minutes from the gateway node. The bulkstats data such as PDN session activations and deactivations events counters are used to calculate the Network Initiated Setup/Teardown KPIs per second on the external server. The gateway node does not calculate the Network Initiated Setup/Teardown KPIs; but it only provides the counters to the external server for additional processing of relevant bulkstats data.

To address these issues, Network Initiated Setup/Teardown KPIs, Session Events Per Second (SEPS), Gx Transactions Per Second (TPS), Gy-TPS, S6b-TPS, Rf-TPS, SWm-TPS KPIs have been implemented. The SEPS and Network Initiated Setup/Teardown KPIs measure the signaling load on the gateway, and also the event rate for VoLTE call setup and tear down respectively. These KPIs assist operators in performing network dimensioning/planning for the gateway node.

New show CLI commands are provided to display SEPS, network initiated setup/teardown KPIs per second, and Transactions Per Second (TPS) per Diameter application/endpoint in the specified/configured bucket intervals. The show CLI will display both the cumulative statistics as well as the historical statistics. The gateway will also provide option to fetch the new set of KPIs using bulkstats framework.

A sampling counter interval for SEPS and Network Initiated Setup/Teardown KPIs is the same as bulkstats sampling interval and is currently set to 2 minutes. The show CLI commands are capable of providing the following for all signaling interfaces:

- SEPS and Network Initiated Setup/Teardown KPI values per second, but averaged over configured bucket interval (1 to 20)

- 8 historical SEPS and Network Initiated Setup/Teardown KPI values
- Gx-TPS, Gy-TPS, S6b-TPS, Rf-TPS, and SWm-TPS KPIs per second, but averaged over 1, 10 seconds, 30 seconds, 1 minute, 5 minutes, 10 minutes and 15 minutes

Note TPS is computed based on average of sent and received Diameter messages per second.

Average values of all KPIs will be provided by the gateway to the external servers using bulkstats data every 2 minutes if requested. The total KPI TPS value as well as breakdown TPS values by each card (i.e., Diameter proxy) on every Diameter interface will be provided using the show CLI command and bulkstats data.

The SEPS KPI provides the following values using the CLI command and bulkstats:

- Total Session Events (session setup and session tear down) per second
- Successful Session Events (session setup and session tear down) per second
- Unsuccessful Session Events (session setup and session tear down) per second

The Network Initiated Setup/Teardown Events Per Second KPI provides the following values:

- Total Network Initiated Setup/Teardown Events (VoLTE bearer setup and tear down) per second
- Successful Network Initiated Setup/Teardown Events (VoLTE bearer setup and tear down) per second
- Unsuccessful Network Initiated Setup/Teardown Events (VoLTE bearer setup and tear down) per second

The Gx-TPS, Gy-TPS, S6b-TPS, Rf-TPS and SWm-TPS KPI counters will be incremented based on the received and sent Diameter messages.

How It Works

This section describes the counting procedures for all KPIs.

SEPS:

The SEPS KPI is implemented such that each session setup and session tear down is considered as a separate event.

SEPS counter is incremented by 1 in the following scenarios:

- After receiving the "Create Session Request" message or "Delete Session Request" message
- After sending the "Create Session Response" message or "Delete Session Response" message
- If "Create Session Response" message contains a failure cause
- If "Delete Session Response" message does not have the cause IE equal "Request Accepted"

Network Initiated Setup/Teardown Events Per Second KPI:

The Network Initiated Setup/Teardown KPI is implemented such that each created and deleted VoLTE (configured QCI value) dedicated bearers are considered as a separate event.

Network Initiated Setup/Teardown KPI counter is incremented by 1 in the following scenarios for the configured QCI value:

- After receiving the "Create Bearer Response" message or "Delete Bearer Response" message
- After sending the "Create Bearer Request" message or "Delete Bearer Request" message
- If "Create Bearer Response" message does not have the cause IE equal "Request Accepted"
- If "Delete Bearer Response" message does not have the cause IE equal "Request Accepted"

Gx-TPS:

Gx Events Per Seconds (Gx-EPS) KPI measures the rate of sent and received Gx event/messages. This KPI indicates the number of received CCA and RAR Diameter messages (each received CCA and RAR message is used to peg the counter) and sent CCR and RAA Diameter messages (each sent CCR and RAA message is used to peg the counter). Gx-EPS KPI considers each received message (CCA and RAR) and each sent message (CCR and RAA) as a separate event.

Gy-TPS:

Gy Events Per Seconds (Gy-EPS) KPI measures the rate of sent and received Gy event/messages. This KPI indicates the number of received CCA Diameter messages (each received CCA message is used to peg the counter) and sent CCR Diameter messages (each sent CCR message is used to peg the counter). Gy-EPS KPI considers each received message (CCA) and each sent message (CCR) as a separate event.

S6b-TPS:

S6b Events Per Seconds (S6b-EPS) KPI measures the rate of sent and received S6b event/messages. This KPI indicates the number of received (AAA, ASR, STA) Diameter messages and sent (AAR, STR, ASA) Diameter messages (each received AAA, ASR, STA messages are used to peg the counter and each sent AAR, STR, and ASA messages are used to peg the counter). S6b-EPS KPI considers each received message (AAA, ASR, STA) and each sent message (AAR, STR, ASA) as a separate event.

Rf-TPS:

Rf Events Per Seconds (Rf-EPS) KPI measures the rate of sent and received Rf event/messages. This KPI indicates the number of received ACA Diameter message and sent ACR Diameter message (each received ACA message is used to peg the counter and each sent ACR message is used to peg the counter). Rf-EPS KPI considers each ACA received message and each ACR sent message as a separate event.

SWm-TPS:

SWm Events Per Seconds (SWm-EPS) KPI measures the rate of sent and received SWm event/messages. This KPI indicates the number of received STA and DEA Diameter messages and sent STR and DER Diameter messages (each received STA and DEA message is used to peg the counter and each sent STR and DER message is used to peg the counter). SWm-EPS KPI considers each STA and DEA received message and each STR and DER sent message as a separate event.

This feature does not require any specific configuration for enabling but minimal configuration of bucket intervals and QCIs is required for calculating the KPIs. For more on this feature and the configuration details, refer to the *P-GW Administration Guide*.

Limitations

This section identifies the limitations of Transaction Rate KPI feature.

- Diameter applications do not share the same Diameter endpoints configured on ASR 5500 platforms. For example, Gx and Gy should have separate Diameter endpoints configured.
- The transaction rate statistics will be lost when the session manager/demux manager restarts.

Monitoring and Troubleshooting the Transaction Rate KPI Feature

This section provides information regarding show commands and/or their outputs in support of the Transaction Rate KPI feature.

Transaction Rate KPI Show Command(s) and/or Outputs

The show commands in this section are available in support of the Transaction Rate KPI feature.

show diameter tps-statistics

This new command has been added to the Exec mode. This command enables operators to gather the Diameter message transaction rate KPI information.

These KPI statistics information are used to monitor signaling load on the gateway node, specifically session and VoLTE signaling transaction rates, so that operators can perform network dimensioning/planning for the node accordingly.

show diameter tps-statistics [diamproxy *diamproxy_num* **| application { auth-eap | e2 | gmb | gx | gy | rf | s6a | s6b | sgmb | sta | swm } | endpoint** *endpoint_name* **| summary | verbose] + [| { grep** *grep_options* **| more }]**

- **diamproxy** *diamproxy_num*: Displays the TPS KPI information for the specified diamproxy instance number specified as an integer from 1 to 144.
- **application { auth-eap | e2 | gmb | gx | gy | rf | s6a | s6b | sgmb | sta | swm }**: Displays the TPS KPI information for specified Diameter application.
- **endpoint** *endpoint_name*: Displays the TPS KPI information for the configured endpoint.

clear diameter tps-statistics

This new command has been added to the Exec mode. This command clears both historical as well as cumulative KPIs for Session and Network Initiated Setup/Teardown events.

clear diameter tps-statistics application { auth-eap | e2 | gmb | gx | gy | rf | s6a | s6b | sgmb | sta | swm } | endpoint *endpoint_name* **[| { grep** *grep_options* **| more }]**

- **application { auth-eap | e2 | gmb | gx | gy | rf | s6a | s6b | sgmb | sta | swm }**: Clears the TPS KPI information for specified Diameter application.
- **endpoint** *endpoint_name*: Clears the TPS KPI information for the configured endpoint.

show diameter tps-statistics Command Output

This show command displays the following fields that are added as part of the Transaction Rate KPI feature.

- Application/ID: The name and the identifier of configured Diameter applications for which the TPS KPI statistics are collected.
- Average TPS: This is the sum average of all TPS values computed.
- Maximum TPS Time: Indicates the maximum TPS value for the specified configuration.

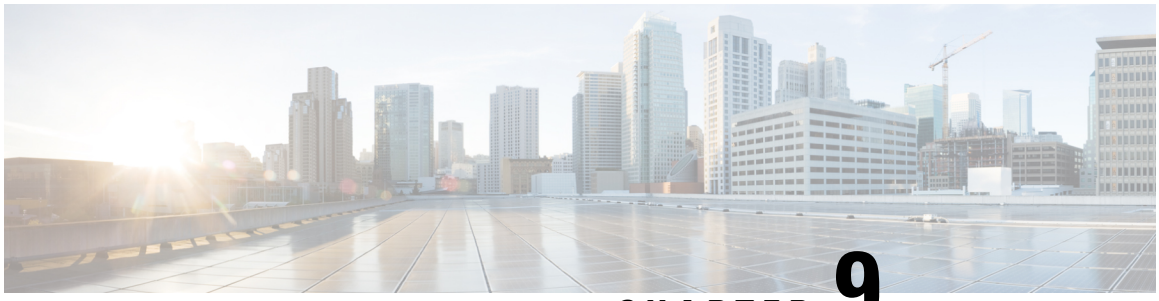
- Last 1 Sec Average TPS: Average value of TPS computed for the last 1 second.
- Last 10 Secs Average TPS: Average value of TPS computed for the last 10 seconds.
- Last 30 Secs Average TPS: Average value of TPS computed for the last 30 seconds.
- Last 60 Secs Average TPS: Average value of TPS computed for the last 60 seconds.
- Last 5 Mins Average TPS: Average value of TPS computed for the last 5 minutes.
- Last 10 Mins Average TPS: Average value of TPS computed for the last 10 minutes.
- Last 15 Mins Average TPS: Average value of TPS computed for the last 15 minutes.

Bulk Statistics Support

Diameter TPS Schema

This schema is new in release 20. The following statistics are included in this schema in support of the Transaction Rate KPI feature:

- diameter-tps-application-id – Indicates the Application ID exchanged in CER/CEA.
- diameter-tps-application-name – Indicates the Application Name.
- diameter-tps-value – Indicates the two minutes average Diameter Transactions per Second (TPS).



CHAPTER 9

Encoding Destination-Host AVP in Redirected Requests

This chapter provides the implementation details to include the Destination-Host AVP in Diameter Redirected requested messages on S6b, SWm and STa interfaces.

This chapter discusses the following topics for this feature:

Feature Description

Note This feature is applicable to 18.4.3 and later releases.

When an application receives the Result-Code 3006 -DIAMETER_REDIRECT_INDICATION from the AAA server, the Diameter request message is forwarded to the Redirect-Host specified in the server's response. The message gets routed properly in case the Diameter host is directly connected to the AAA server. If there is a DRA between P-GW/ePDG and AAA server, the message goes into a loop as DRA always routes the packet to the AAA server which had redirected the message. To overcome this problem, the Destination-Host AVP should be included in the redirected messages. This functionality is supported by extending the existing CLI command "**destination-host-avp**" to include "**redirected-request**" as an optional configuration.

This option "**redirected-request**" encodes Destination-Host AVP in any type of Diameter redirected messages. Since any redirected request is considered as retried request, if the option "**retried-request**" is used, by default Update (Interims) or Terminate (Stop) redirected-request will be encoded with Destination-Host AVP without the "**redirected-request**" option being configured. The reason to configure "**redirected-request**" as part of "**retried-request**" option is, in case of Initial-Retried request the Destination-Host AVP is not encoded if "**retried-request**" option alone is configured. To enable encoding Destination-Host AVP for Initial-Retried request, "**redirected-request**" is supported as an extension to "**retried-request**" as well.

In releases prior to 18, the Destination-Host AVP was encoded in the redirected message only if the original request included Destination-Host AVP. In release 18 and beyond, the encoding of Destination-Host AVP in redirected message is based on the new configurable option **redirected-request** in "**destination-host-avp**" CLI command. If the CLI command is enabled, Destination-Host AVP will be included in any type of Diameter redirected messages.

Limitations

As per the current implementation, it is not possible to send retried messages to a different host using the same peer. This behavior is applicable for normal retry and failure-handling scenarios.

Standards Compliance

This feature is implemented to be compliant with 3GPP TS 29.273 specification.

Configuring Destination-Host AVP in Redirected Request

This section provides information on the commands used to include the Destination-Host AVP in the redirected request messages.

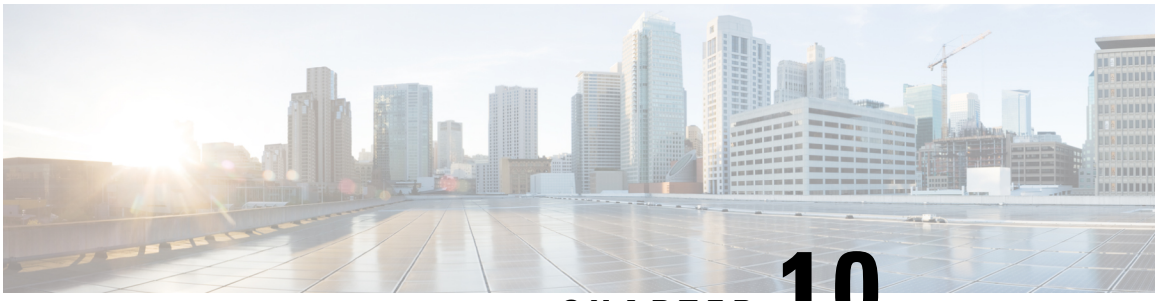
Encoding Destination-Host AVP in Redirected Requests

Use the following configuration commands to include the Destination-Host AVP in the redirected request messages on ePDG, P-GW and SaMOG sent over the respective authentication interfaces (SWm, S6b and STa).

```
configure
    context context_name
         diameter endpoint endpoint_name
              destination-host-avp { always | initial-request [
redirected-request ] | retried-request [ redirected-request ] |
session-binding [ redirected-request ] }
              default destination-host-avp
              end
```

Notes:

- **redirected-request**: Encodes the Destination-Host AVP in any redirected request message.
- **always**: Encodes the Destination-Host AVP in all types of request messages.
- **initial-request**: Encodes the Destination-Host AVP in initial request but not in retried request.
- **retried-request**: Encodes the Destination-Host AVP in retried request but not in initial request.
- **session-binding**: Encodes the Destination-Host AVP after the Diameter session is bound with a host.



CHAPTER 10

Origin-State-Id AVP Support on P-GW

This chapter describes the following topics:

Feature Summary and Revision History

Summary Data

Applicable Product(s) or Functional Area	P-GW
Applicable Platform(s)	• ASR 5500 • VPC - DI • VPC - SI
Feature Default	Disabled - Configuration Required
Related Changes in This Release	Not Applicable
Related Documentation	• *AAA Administration Guide* • *Command Line Interface Reference* • *Statistics and Counters Reference*

Revision History

Revision Details	Release
Introduced support for indirectly connected Policy and Charging Rules Functions (PCRFs) through Diameter Routing Agent (DRA).	21.17

Revision Details	Release
First introduced.	21.6

Feature Description

The interfaces connected to the P-GW use Diameter protocol for communcation. This protocol provides a mechanism through the Origin-State-Id AVP to detect sessions that are terminated due to unanticipated shutdown of a peer node.

Storing the Origin-State-Id AVP of a peer node enables the P-GW to detect and clear sessions whenever there is a change in the Origin-State-Id of the diameter peer node. This ensures that the diameter-nodes are always synchronized with the P-GW. To enable this functionality of storing the Origin-State-Id AVP on the P-GW, the **osid-change** CLI command is introduced at the diameter endpoint level.

Origin-State-Id change detection is applicable only for PCRF nodes.

How It Works

When the **osid-change** CLI command is configured, the diabase starts storing the Origin-State-Id of each peer configured under a diameter endpoint. On receiving a diameter message from a peer, if the Origin-State-Id AVP is present, it is compared with the stored Origin-State-Id. If the received Origin-State-Id is greater than the stored one, gateway will start clearing calls. The Session Manager marks all the subscribers connected to the diameter-session for deletion and starts clearing sessions in a staggered manner. Clearing calls in a staggered manner helps avoid a storm of messages on other connected interfaces. When a subscriber is marked for deletion, the GW drops all the outbound diameter messages on the interface.

As per RFC 6733 (Diameter Base Protocol) Origin-State-Id could come in any diameter message, so the Gateway provides support to detect the change in CEA, CCA and RAR messages.

This feature is supported only with diamproxy mode (single and multiple).

Configuring Origin State Identifier AVP Support on P-GW

The following section provides the configuration command to enable or disable the functionality.

Configuring Origin-State-Id AVP on P-GW

Use the following CLI commands to store the Origin-State-Id AVP of a Diameter peer node on the P-GW. This command is introduced at the diameter endpoint level.

```
configure
  context context_name
    diameter endpoint endpoint_name
      [no] osid-change action clear-subscribers
      end
```

NOTES:

- **no:** Disables the command.
- **action:** Specifies the action to be taken.
- **clear subscribers:** Clears subscribers connected to the peer.
- This functionality is disabled by default.

Monitoring and Troubleshooting

This section provides information regarding show commands and/or their outputs in support of this feature.

Show Commands and/or Outputs

The output of the following CLI command has been enhanced in support of the feature.

show diameter

As part of this functionality, the **show diameter** CLI now includes the values for the following new fields:

- osid-info sessmgr all
- osid-info sessmgr instance_number

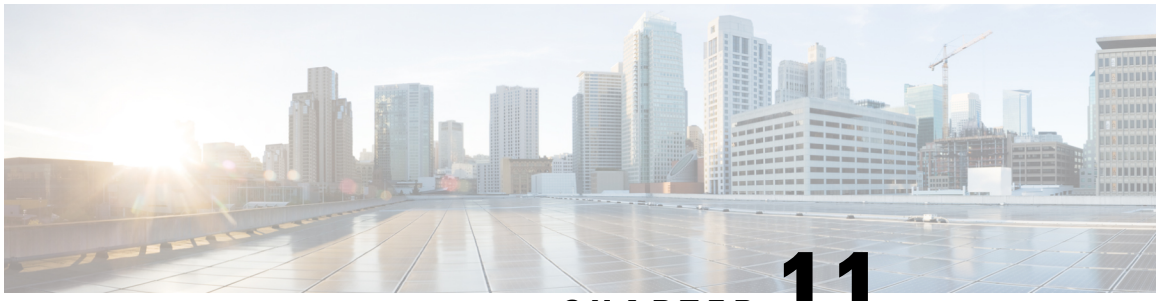
show session disconnect-reasons

The **show session disconnect-reasons** CLI now includes the **osid-change** field.

Bulk Statistics

The following bulk statistics are added in the System schema to support this feature:

Bulk Statistics	Description
disc-reason-656	Indicates the total number of sessions cleared due to change in Origin-State-Id of the Diameter peer.



CHAPTER 11

Ratio-based Load Distribution

This chapter describes the following topics:

Feature Summary and Revision History

Summary Data

Applicable Product(s) or Functional Area	P-GW
Applicable Platform(s)	ASR 5500
Feature Default	Disabled - Configuration Required
Related Changes in This Release	Not Applicable
Related Documentation	• *AAA Interface Administration and Reference* • *Command Line Interface Reference*

Revision History

Revision Details	**Release**
First introduced.	21.4

Feature Description

The Ratio-based Load Distribution feature provides a CLI-controlled mechanism to enable ratio-based session binding distribution among Diameter peers in an endpoint. You can configure ratios for each peer based on their capacity of load.

How It Works

Following is a brief overview of how Ratio-based Load Distribution feature works:

- The new **load-ratio** keyword in **peer** CLI command under Diameter Endpoint Configuration Mode allows to configure Load Ratio for an individual peer. The configurable Load Ratio is in the range of 0-65535.
- Configuring 0 (zero) Load Ratio exempts the peer from having a share in binding sessions. Configuring 0 Load Ratio for all the peers in an endpoint effectively disables the usage of the endpoint, while keeping the peers open and ready. This prevents set-up of calls if the calls require Diameter authentication or authorization.
- If no peers have Load Ratio configured, Diameter binds new sessions in a round robin manner, which is the existing behavior.
- If Dynamic Peer Discovery (DPD) peers are added to the endpoint using ratio-based load balancing, then SeRVice Record (SRV) weight of DPD peers is used as Load Ratio.

Important For the feature to be active, an open peer with non-default Load Ratio value is required.

- If the application chooses the peer as per its own load balancing configuration, then ratio-based load balancing will not be active. For example:
  - If Gy selects peer with **diameter peer-select** CLI command (under Credit Control Configuration Mode), it will have precedence over the ratio-based selection.
  - The Gx interface has **diameter host-select row-precedence** and **diameter host-select-template** CLI commands (under Policy Control Configuration Mode) which will choose peers from the application. To override this behavior and to activate the ratio-based peer selection, both the host-select CLI commands should not be configured. However, the **endpoint-peer-select** CLI command (under Policy Control Configuration Mode) has to be enabled.
- If the endpoint has multiple realms, the selection will match a peer which has the same realm as the session-chosen realm.

Configuring Ratio-based Load Distribution

This section provides information about the CLI commands available in support of the feature.

Enabling Load Ratio

Use the following commands under the Diameter Endpoint Configuration Mode to enable Diameter-based peer load balancing, by defining relative Load Ratios in peer configuration.

```
configure
  context context_name
```

```
    diameter endpoint endpoint_name
      peer [*] peer_name [*] [ realm realm_name ] { address { ipv4_address |
ipv6_address } [ load-ratio load_ratio_range ]
      end
```

Notes:

- **peer**: This command specifies a peer address for the Diameter endpoint.
- **[*]** *peer_name* **[*]** : Specifies the peer's name as an alphanumeric string of 1 through 63 characters that allows punctuation characters. The Diameter server endpoint can be a wildcarded peer name (with * as a valid wildcard character). Client peers which satisfy the wild-carded pattern are treated as valid peers and the connection will be accepted. The wildcarded token indicates that the peer name is wildcarded and any '*' in the preceding string is treated as a wildcard.
- **realm** *realm_name*: Specifies the realm of this peer as an alphanumeric string of 1 through 127 characters. The realm name can be a company or service name.
- **address {** *ipv4_address* **|** *ipv6_address* **}**: Specifies the Diameter peer IP address in IPv4 dotted-decimal or IPv6 colon-separated-hexadecimal notation. This address must be the IP address of the device with which the chassis is communicating.
- **load-ratio** *load_ratio_range*: Specifies the Load Ratio for the peer. The Load Ratio can be configured in the range of 0 through 65535.
- As a default behavior, the CLI command is not enabled for a peer and the default Load Ratio is 1, which will be used in load balancing only when at least one peer has non-default Load Ratio configured.
- Not specifying the **load-ratio** *load_ratio_range* keyword from peer configuration will put the peer in default Load Ratio, and when all the peers have default Load Ratio, Diameter load balancing will be round robin.
- The CLI takes effect when Diameter application starts using an endpoint for sending messages.

Monitoring and Troubleshooting the Ratio-based Load Distribution

This section describes the CLI commands available to monitor and/or troubleshoot the feature.

Show Commands and/or Outputs

The output of the following CLI commands has been enhanced in support of the feature.

show configuration

The output of this command has been modified to display the following:

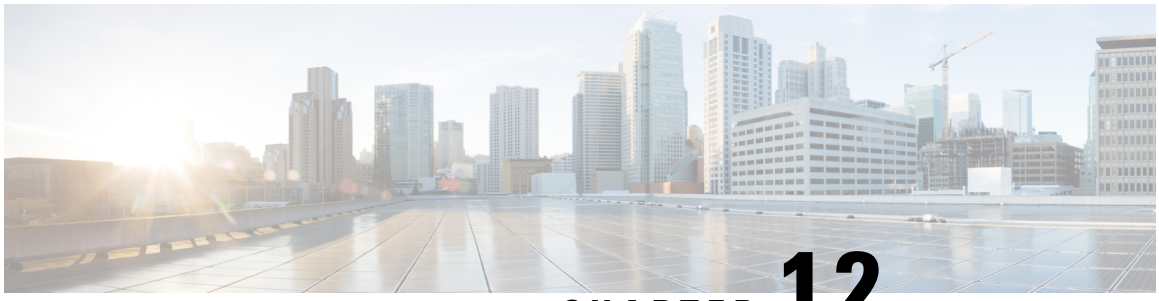
```
show configuration
config
  context ingress
    diameter endpoint st16.starentnetworks.com
      peer gx1 realm starentnetworks.com address 192.10.2.1 load-ratio 2
      peer gx2 realm starentnetworks.com address 192.10.2.2 load-ratio 10
```

```
      peer gx3 realm starentnetworks.com address 192.10.2.3 load-ratio 0
         peer gx4 realm starentnetworks.com address 192.10.2.3
```

show configuration verbose

The output of this command has been modified to display the following:

```
show configuration verbose
config
  context ingress
    diameter endpoint st16.starentnetworks.com
      peer gx1 realm starentnetworks.com address 192.10.2.1 load-ratio 2
      peer gx2 realm starentnetworks.com address 192.10.2.2 load-ratio 10
      peer gx3 realm starentnetworks.com address 192.10.2.3 load-ratio 0
         peer gx4 realm starentnetworks.com address 192.10.2.3 load-ratio 1
```



CHAPTER 12

Support for AAA Failure Indication

This chapter provides information on how the AAA-Failure-Indication AVP is supported on ePDG, P-GW, and SaMOG nodes.

Feature Description

Note This enhancement is applicable to 18.4.3 and later releases.

ePDG, P-GW and SaMOG connects with the AAA server over SWm, S6b and STa Diameter interfaces respectively. When a subscriber PDN connects, the PDN is authenticated over these authentication interfaces. P-GW sends AAR whereas ePDG/SaMOG sends DER to authorize the subscriber. ePDG/P-GW/SaMOG has the capability to select one of the available AAA servers based on priority or round robin method. ePDG/P-GW/SaMOG sends DER/AAR to the selected AAA server. If the HSS indicates that the subscriber is currently being served by a different AAA server, it sends the DIAMETER_REDIRECT_INDICATION Result-Code (3006) over SWm/S6b/STa interfaces requesting ePDG/P-GW/SaMOG to redirect the AAR/DER request to the already bound AAA server.

If the redirection of DER/AAR fails for some reason (Diameter TCP connection being down or Diameter Response-Timeout), the ePDG/P-GW/SaMOG redirects this message to any other available AAA server with the AAA-Failure-Indication AVP set to 1. AAA server forwards the AAA-Failure-Indication AVP to HSS, which will reset the initial binding of the PDN with the failed AAA and bind the PDN with the AAA server that forwarded the AAA-Failure-Indication AVP.

On successful authentication at ePDG/P-GW/SaMOG, the ePDG/P-GW/SaMOG disconnects any other previously connected PDN for the same subscriber. This is done so that the PDNs are reestablished and are bound to the new AAA server.

In order to support a geo-redundant architecture for VoWiFi service, ePDG/P-GW/SaMOG supports the AAA-Failure-Indication AVP as described in 3GPP TS 29.273 specification. This AVP value is set to 1 to indicate that a previously assigned AAA Server is unavailable.

In support of this feature, a new bulk statistics field is added to the output of **show diameter aaa-statistics** command to track the number of times the AAA-Failure-Indication AVP is sent over these authentication interfaces.

Limitations and Dependencies

This section identifies the known limitations and dependencies for this feature.

- It is assumed that the Redirect-Host AVP contains a valid known host. If the host is invalid, ePDG/P-GW/SaMOG will terminate the connecting PDN.
- When the AAA server sends redirection indication, it is expected that the Result-Code is 3006 (DIAMETER_REDIRECT_INDICATION) and it should also send the Redirect-Host-Usage AVP with its value as 1 (ALL_SESSION) and set the Redirect-Max-Cache-Time AVP to the validity time for the Redirect-Route to exist. By default, the Redirect-Host-Usage is DON'T-CACHE (0) and in this scenario, only the redirected message will be forwarded to Redirect-Host. Any further messages belonging to the same Diameter session will undergo a fresh route-lookup and might contact a different AAA server.
- AAA-Failure-Indication AVP is included only in these Diameter dictionaries:
  - aaa-custom21 for S6b
  - aaa-custom22 for SWm
  - aaa-custom23 for STa

Monitoring and Troubleshooting the AAA Failure Indication Feature

This section provides information regarding show commands and/or their outputs in support of the AAA Failure Indication feature.

Show Command(s) and/or Outputs for AAA Failure Indication

show diameter aaa-statistics

The following field is added to the output of this show command to track the number of times AAA-Failure-Indication AVP is sent over Diameter Authentication interfaces.

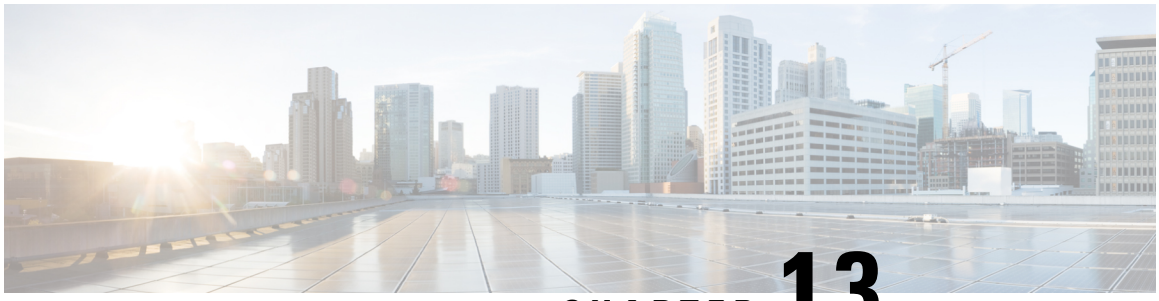
- AAA-Failure-Indication

Bulk Statistics for AAA Failure Indication

The following statistics are included in the Diameter Authentication Schema in support of the AAA Failure Indication feature:

- aaa-failure-indication

For description of this variable, see the *Diameter Authentication Schema Statistics* chapter in the *Statistics and Counters Reference*.



CHAPTER 13

Diameter Dictionaries and Attribute Definitions

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

Diameter Attributes

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

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

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

AVP Header

The AVP header contains the following three fields that requires IANA namespace management.

- AVP Code
- Vendor-ID
- Flags

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

Figure 2: AVP Header

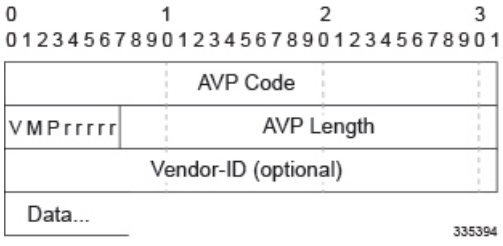


Table 1: AVP Header Details

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

Field	Description
AVP Flags	

Field	Description
	The AVP Flags field informs the receiver how each attribute must be handled. The 'r' (reserved) bits are unused and SHOULD be set to 0. Note that subsequent Diameter applications may define additional bits within the AVP Header, and an unrecognized bit SHOULD be considered an error. The 'P' bit indicates the need for encryption for end-to-end security. The 'M' Bit, known as the Mandatory bit, indicates whether support of the AVP is required. If an AVP with the 'M' bit set is received by a Diameter client, server, proxy, or translation agent and either the AVP or its value is unrecognized, the message MUST be rejected. Diameter Relay and redirect agents MUST NOT reject messages with unrecognized AVPs. The 'M' bit MUST be set according to the rules defined for the AVP containing it. In order to preserve interoperability, a Diameter implementation MUST be able to exclude from a Diameter message any Mandatory AVP which is neither defined in the base Diameter protocol nor in any of the Diameter Application specifications governing the message in which it appears. It may do this in one of the following ways: • If a message is rejected because it contains a Mandatory AVP which is neither defined in the base Diameter standard nor in any of the Diameter Application specifications governing the message in which it appears, the implementation may resend the message without the AVP, possibly inserting additional standard AVPs instead. • A configuration option may be provided on a system wide, per peer, or per realm basis that would allow/prevent particular Mandatory AVPs to be sent. Thus an administrator could change the configuration to avoid interoperability problems. Diameter implementations are required to support all Mandatory AVPs which are allowed by the message's formal syntax and defined either in the base Diameter standard or in one of the Diameter Application specifications governing the message. AVPs with the 'M' bit cleared are informational only and a receiver that receives a message with such an AVP that is not supported, or whose value is not supported, MAY simply ignore the AVP.

Field	Description
	The 'V' bit, known as the Vendor-Specific bit, indicates whether the optional Vendor-ID field is present in the AVP header. When set the AVP Code belongs to the specific vendor code address space. Unless otherwise noted, AVPs will have the following default AVP Flags field settings: The 'M' bit MUST be set. The 'V' bit MUST NOT be set.
AVP Length	The AVP Length field is three octets, and indicates the number of octets in this AVP including the AVP Code, AVP Length, AVP Flags, Vendor-ID field (if present) and the AVP data. If a message is received with an invalid attribute length, the message SHOULD be rejected.
Vendor-ID	This field is optional. The Vendor-ID field is present if the 'V' bit is set in the AVP Flags field. The optional four-octet Vendor-ID field contains the IANA assigned "SMI Network Management Private Enterprise Codes" value, encoded in network byte order. Any vendor wishing to implement a vendor-specific Diameter AVP MUST use their own Vendor-ID along with their privately managed AVP address space, guaranteeing that they will not collide with any other vendor's vendor-specific AVP(s), nor with future IETF applications. A vendor ID value of zero (0) corresponds to the IETF adopted AVP values, as managed by the IANA. Since the absence of the vendor ID field implies that the AVP in question is not vendor specific, implementations MUST NOT use the zero (0) vendor ID.

Basic AVP Data Formats

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

Table 2: Basic AVP Formats

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

Derived AVP Data Formats

In addition to using the Basic AVP Data Formats, applications may define data formats derived from the Basic AVP Data Formats. An application that defines new AVP Derived Data Formats MUST include them in a

section entitled "AVP Derived Data Formats", using the same format as the definitions below. Each new definition must be either defined or listed with a reference to the RFC that defines the format.

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

Address

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

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

Time

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

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

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

UTF8String

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

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

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

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

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

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

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

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

DiameterIdentity

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

DiameterIdentity = FQDN

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

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

DiameterURI

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

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

– or –

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

Table 3: DiameterURI Field Description

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

The following are examples of valid Diameter host identities:

```
aaa://host.example.com;transport=tcp
aaa://host.example.com:6666;transport=tcp
aaa://host.example.com;protocol=diameter
aaa://host.example.com:6666;protocol=diameter
aaa://host.example.com:6666;transport=tcp;protocol=diameter
aaa://host.example.com:1813;transport=udp;protocol=radius
```

Enumerated

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

IPFilterRule

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

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

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

IPFilterRule filters MUST follow the format:

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

Table 4: IPFilterRule Field Description

Field	Description
action	This field can be set to one of the following: • permit – Allow packets that match the rule. • deny – Drop packets that match the rule.
dir	"in" is from the terminal and "out" is to the terminal.
proto	An IP protocol specified by number. The "ip" keyword means any protocol will match.

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

Field	Description
options	

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

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

QoSFilterRule

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

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

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

QoSFilterRule filters MUST follow the format:

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

Table 5: QoSFilterRule Field Description

Field	Description
action	This field can be set to one of the following: • tag — Mark packet with a specific DSCP [DIFFSERV]. The DSCP option MUST be included. • meter — Meter traffic. The metering options MUST be included.
dir	The format is as described under IPFilterRule.
proto	The format is as described under IPFilterRule.
src and dst	The format is as described under IPFilterRule.

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

Grouped AVP Values

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

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

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

```
grouped-avp-def = name "::=" avp
name-fmt = ALPHA *(ALPHA / DIGIT / "-")
name = name-fmt
avp = header [ *fixed] [ *required] [ *optional] [ *fixed]
header = "<" "AVP-Header:" avpcode [vendor] ">"
avpcode = 1*DIGIT
vendor = 1*DIGIT
```

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

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

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

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

```
Example-AVP  ::= < AVP Header: 999999 >
                     { Origin-Host }
                   1*{ Session-Id }
                    *[ AVP ]
```

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

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

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

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

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

Optional AVPs included are:

```
Recovery-Policy = <binary> 2163bc1d0ad82371f6bc09484133c3f09ad74a0dd5346d54195a7cf0b35
2cabc881839a4fdcfbc1769e2677a4c1fb499284c5f70b48f58503a45c5
c2d6943f82d5930f2b7c1da640f476f0e9c9572a50db8ea6e51e1c2c7bd
f8bb43dc995144b8dbe297ac739493946803e1cee3e15d9b765008a1b2a
cf4ac777c80041d72c01e691cf751dbf86e85f509f3988e5875dc905119
26841f00f0e29a6d1ddc1a842289d440268681e052b30fb638045f7779c
1d873c784f054f688f5001559ecff64865ef975f3e60d2fd7966b8c7f92
Futuristic-Acct-Record = <binary> fe19da5802acd98b07a5b86cb4d5d03f0314ab9ef1ad0b67111ff3b90a0
 57fe29620bf3585fd2dd9fcc38ce62f6cc208c6163c008f4258d1bc88b8
17694a74ccad3ec69269461b14b2e7a4c111fb239e33714da207983f58c
41d018d56fe938f3cbf089aac12a912a2f0d1923a9390e5f789cb2e5067 d3427475e49968f841
```

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

Diameter Dictionaries

This section presents information on Diameter dictionary types.

DPCA

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

To configure the Diameter dictionary for Policy Control Configuration, use the following configuration:

```
configure
     context <context_name>
          ims-auth-service <ims_auth_service_name>
               policy-control
                    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-custom21 | dpcacustom22 | dpca-custom23 | dpca-custom24 |
dpca-custom25 | dpca-custom26 | dpca-custom27 | dpca-custom28 |
dpca-custom29 | dpca-custom3 | dpca-custom30 | dpca-custom4 | dpca-custom5
 | dpca-custom6 | dpca-custom7 | dpca-custom8 | dpca-custom9 | dynamic-load
 | gx-wimax-standard | gxa-3gpp2-standard | gxc-standard | pdsn-ty |
r8-gx-standard | std-pdsn-ty | ty-plus | ty-standard }
                    end
```

Dictionary	Description
Standard	Specifies standard attributes for the Rel 6 Gx interface.
dpca-custom1...dpca-custom*n*	Custom-defined dictionaries.
dynamic load	Specifies the dynamically loaded Diameter dictionary attributes.
gx-wimax-standard	Specifies standard Gx WiMAX Standard attributes.
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.

Note For information on custom-defined dictionaries, contact your Cisco account representative.

DCCA

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

To configure the DCCA dictionary for Active Charging service, use the following configuration:

```
configure
     active-charging service <acs_service_name>
          credit-control
               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-custom21 |
dcca-custom22 | dcca-custom23 | dcca-custom24 | dcca-custom25 |
dcca-custom26 | dcca-custom27 | dcca-custom28 | dcca-custom29 |
```

```
dcca-custom3 | dcca-custom30 | dcca-custom4 | dcca-custom5 | dcca-custom6
 | dcca-custom7 | dcca-custom8 | dcca-custom9 | dynamic-load | standard
}
                end
```

Dictionary	Description
dcca-custom1 ... dcca-custom*n*	Custom-defined dictionaries.
standard	Specifies standard attributes for the Gy interface.
dynamic load	Specifies the dynamically loaded Diameter dictionary attributes.

Note For information on custom-defined dictionaries, contact your Cisco account 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 configure the Diameter Policy Control dictionary, use the following configuration:

```
configure
     context <context_name>
          cscf service <cscf_service_name>
               proxy-cscf
                    diameter policy-control { dictionary { dynamic-load
| gq-custom | gq-standard | rq-custom | rx-custom01 | rx-custom02 |
rx-custom03 | rx-custom04 | rx-custom05 | rx-rel8 | rx-standard |
tx-standard }
                    end
```

Dictionary	Description
dynamic load	Specifies the dynamically loaded Diameter dictionary attributes.
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.

Dictionary	Description
tx-standard	Specifies the standard attributes for the 3GPP2 Tx interface.
rx-custom01...rx-custom05	Custom-defined dictionaries.

Note For information on custom-defined dictionaries, contact your Cisco account 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 | dynamic-load | 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 | dynamic-load | nasreq }
```

Dictionary	Description
aaa-custom1... aaa-custom8, aaa-custom10 ... aaa-custom*n*	Custom-defined dictionaries.
aaa-custom9	Specifies standard attributes for the STa interface.
nasreq	Specifies the NASREQ attributes defined by RFC 4005.
rf-plus	Specifies customer-specific enhanced attributes for the Rf interface.
dynamic load	Specifies the dynamically loaded Diameter dictionary attributes.

Note For information on custom-defined dictionaries, contact your Cisco account representative.

Diameter AVP Definitions

This section presents Diameter attribute definitions.

3GPP-AAA-Server-Name

3GPP-AAA-Server-Name

Vendor ID 10415

VSA Type 318

AVP Type DIAMURI

AVP Flag M

3GPP-CAMEL-Charging-Info

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

Vendor ID 10415

VSA Type 24

AVP Type UTF8STRING

AVP Flag N/A

3GPP-CF-IPv6-Address

3GPP-CF-IPv6-Address

Vendor ID 10415

VSA Type 14

AVP Type OCTETSTRING

AVP Flag M

3GPP-CG-Address

This AVP contains address of the Charging Gateway.

Vendor ID 10415

VSA Type 4

AVP Type OCTETSTRING

AVP Flag M

3GPP-Called-Station-Id

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

Vendor ID 10415

VSA Type 30

AVP Type OCTETSTRING

AVP Flag N/A

3GPP-Charging-Characteristics

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

Vendor ID 10415

VSA Type 13

AVP Type UTF8STRING

AVP Flag M

3GPP-Charging-Id

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

Vendor ID 10415

VSA Type 2

AVP Type UINT32

AVP Flag M

3GPP-GGSN-Address

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

Vendor ID 10415

VSA Type 7

AVP Type OCTETSTRING

AVP Flag M

3GPP-GGSN-MCC-MNC

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

Vendor ID 10415

VSA Type 9

AVP Type UTF8STRING

AVP Flag M

3GPP-GPRS-QoS-Negotiated-Profile

This AVP contains QoS profile applied by GGSN.

Vendor ID 10415

VSA Type 5

AVP Type UTF8STRING

AVP Flag M

3GPP-IMEISV

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

Vendor ID 10415

VSA Type 20

AVP Type OCTETSTRING

AVP Flag M

3GPP-IMSI

This AVP contains an IMSI of the user.

Vendor ID 10415

VSA Type 1

AVP Type UTF8STRING

AVP Flag M

3GPP-IMSI-MCC-MNC

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

Vendor ID 10415

VSA Type 8

AVP Type UTF8STRING

AVP Flag M

3GPP-MS-TimeZone

This AVP contains the Mobile Station Time Zone.

Vendor ID 10415

VSA Type 23

AVP Type OCTETSTRING

AVP Flag M

3GPP-NSAPI

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

Vendor ID 10415

VSA Type 10

AVP Type UTF8STRING

AVP Flag M

3GPP-PDP-Type

This AVP contains type of the PDP context.

Vendor ID 10415

VSA Type 3

AVP Type ENUM

Supported enumerated value(s):

0 IPv4

1 PPP

2 IPv6

3 IPv4v6

AVP Flag M

3GPP-Quota-Consumption-Time

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

Vendor ID 10415

VSA Type 881

AVP Type UINT32

AVP Flag M

3GPP-Quota-Holding-Time

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

Vendor ID 10415

VSA Type 871

AVP Type UINT32

AVP Flag M

3GPP-RAT-Type

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

Vendor ID 10415

VSA Type 21

AVP Type OCTETSTRING

AVP Flag M

3GPP-RAT-Type-Enum

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

Vendor ID 10415

VSA Type 21

AVP Type ENUM

Supported enumerated value(s):

1 UTRAN

2 GERAN

3 WLAN

4 GAN

5 HSPA

6 EUTRAN

7 VIRTUAL

8 NB-IOT

102 3GPP2_eHRPD

33 CDMA_1XRTT

59 CDMA_EVDO

64 CDMA_EVDO_REVA

AVP Flag M

3GPP-Reporting-Reason

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

Vendor ID 10415

VSA Type 872

AVP Type ENUM

Supported enumerated value(s):

0 THRESHOLD

1 QHT

2 FINAL

3 QUOTA_EXHAUSTED

4 VALIDITY_TIME

5 OTHER_QUOTA_TYPE

6 RATING_CONDITION_CHANGE

7 FORCED_REAUTHORIZATION

AVP Flag M

3GPP-SGSN-Address

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

Vendor ID 10415

VSA Type 6

AVP Type OCTETSTRING

AVP Flag M

3GPP-SGSN-IPv6-Address

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

Vendor ID 10415

VSA Type 15

AVP Type OCTETSTRING

AVP Flag M

3GPP-SGSN-MCC-MNC

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

Vendor ID 10415

VSA Type 18

AVP Type UTF8STRING

AVP Flag M

3GPP-Selection-Mode

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

Vendor ID 10415

VSA Type 12

AVP Type UTF8STRING

AVP Flag M

3GPP-Session-Stop-Indicator

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

Vendor ID 10415

VSA Type 11

AVP Type OCTETSTRING

AVP Flag M

3GPP-Time-Quota-Threshold

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

Vendor ID 10415

VSA Type 868

AVP Type UINT32

AVP Flag M

3GPP-Trigger-Type

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

Vendor ID 10415

VSA Type 870

AVP Type ENUM

Supported enumerated value(s):

1 CHANGE_IN_SGSN_IP_ADDRESS

2 CHANGEINQOS_ANY

3 CHANGEINLOCATION_ANY

4 CHANGEINRAT

5 CHANGEINTIMEZONE

10 CHANGEINQOS_TRAFFIC_CLASS

11 CHANGEINQOS_RELIABILITY_CLASS

12 CHANGEINQOS_DELAY_CLASS

13 CHANGEINQOS_PEAK_THROUGHPUT

14 CHANGEINQOS_PRECEDENCE_CLASS

15 CHANGEINQOS_MEAN_THROUGHPUT

16 CHANGEINQOS_MAXIMUM_BIT_RATE_FOR_UPLINK

17 CHANGEINQOS_MAXIMUM_BIT_RATE_FOR_DOWNLINK

18 CHANGEINQOS_RESIDUAL_BER

19 CHANGEINQOS_SDU_ERROR_RATIO

20 CHANGEINQOS_TRANSFER_DELAY

21 CHANGEINQOS_TRAFFIC_HANDLING_PRIORITY

22 CHANGEINQOS_GUARANTEED_BIT_RATE_FOR_UPLINK

23 CHANGEINQOS_GUARANTEED_BIT_RATE_FOR_DOWNLINK

30 CHANGEINLOCATION_MCC

31 CHANGEINLOCATION_MNC

32 CHANGEINLOCATION_RAC

33 CHANGEINLOCATION_LAC

34 CHANGEINLOCATION_CellId

61 CHANGE_IN_SERVING_NODE

AVP Flag M

3GPP-Unit-Quota-Threshold

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

Vendor ID 10415

VSA Type 1226

AVP Type UINT32

AVP Flag M

3GPP-User-Data

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

Vendor ID 10415

VSA Type 606

AVP Type OCTETSTRING

AVP Flag M

3GPP-User-Location-Info

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

Vendor ID 10415

VSA Type 22

AVP Type UTF8STRING

AVP Flag M

3GPP-Volume-Quota-Threshold

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

Vendor ID 10415

VSA Type 869

AVP Type UINT32

AVP Flag M

3GPP-WLAN-APN-Id

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

Vendor ID 10415

VSA Type 11003

AVP Type OCTETSTRING

AVP Flag M

3GPP2-Allowed-Persistent-TFTS

Maximum allowed persistent TFTs.

Vendor ID 5535

VSA Type 6083

AVP Type UINT32

AVP Flag M

3GPP2-BSID

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

Vendor ID 5535

VSA Type 9010

AVP Type OCTETSTRING

AVP Flag M

3GPP2-Correlation-Id

This AVP contains correlation ID in 3GPP2 networks.

Vendor ID 5535

VSA Type 6071

AVP Type OCTETSTRING

AVP Flag M

3GPP2-Information

3GPP2-Information

Vendor ID 5535

VSA Type 6077

AVP Type GROUPED

Supported group value(s):

[SUBSCRIBER_PRIORITY]

[AUTH_PROFILE_ID_FORWARD]

[AUTH_PROFILE_ID_REVERSE]

[AUTH_PROFILE_ID_BI_DIRECTION]

AVP Flag M

3GPP2-Inter-User-Priority

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

Vendor ID 5535

VSA Type 139

AVP Type UINT32

AVP Flag M

3GPP2-MEID

This AVP contains the International Mobile Equipment Identity.

Vendor ID 10415

VSA Type 1471

AVP Type OCTETSTRING

AVP Flag M

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

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

Vendor ID 5535

VSA Type 130

AVP Type UINT32

AVP Flag M

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

This AVP indicates the maximum service option instances.

Vendor ID 5535

VSA Type 6082

AVP Type UINT32

AVP Flag M

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

This AVP contains the per flow priority for the user.

Vendor ID 5535

VSA Type 6088

AVP Type UINT32

AVP Flag M

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

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

Vendor ID 5535

VSA Type 6084

AVP Type UINT32

AVP Flag M

3GPP2-RAT-Type

3GPP2-RAT-Type

Vendor ID 5535

VSA Type 1001

AVP Type ENUM

Supported enumerated value(s):

0 3G1X

1 HRPD

2 WLAN

AVP Flag M

3GPP2-RP-Session-ID

3GPP2-RP-Session-ID

Vendor ID 5535

VSA Type 6074

AVP Type OCTETSTRING

AVP Flag M

3GPP2-Service-Option

This AVP specifies the authorized packet data service option number.

Vendor ID 5535

VSA Type 16

AVP Type UINT32

AVP Flag M

3GPP2-Service-Option-Profile

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

Vendor ID 5535

VSA Type 74

AVP Type GROUPED

Supported group value(s):

[3GPP2_SERVICE_OPTION]

[3GPP2_MAX_INST_PER_SERVICE_OPTION]

AVP Flag M

3GPP2-Serving-PCF

This AVP specifies the IP address of the serving PCF, that is, the PCF in the serving RAN.

Vendor ID 5535

VSA Type 6073

AVP Type ADDRESS

AVP Flag M

3GPP2-User-Zone

This AVP indicates the Tiered Services user zone.

Vendor ID 5535

VSA Type 6075

AVP Type OCTETSTRING

AVP Flag M

A-MSISDN

A-MSISDN

Vendor ID 10415

VSA Type 1643

AVP Type OCTETSTRING

AVP Flag N/A

AAA-Failure-Indication

AAA-Failure-Indication

Vendor ID 10415

VSA Type 1518

AVP Type UINT32

AVP Flag N/A

AAR-Flags

AAR-Flags

Vendor ID 10415

VSA Type 1539

AVP Type UINT32

AVP Flag N/A

Absent-User-Diagnostic-SM

Absent-User-Diagnostic-SM

Vendor ID 10415

VSA Type 3322

AVP Type UINT32

AVP Flag M

ACL-Name

ACL-Name

Vendor ID 9

VSA Type 131145

AVP Type OCTETSTRING

AVP Flag M

ACL-Number

ACL-Number

Vendor ID 9

VSA Type 131144

AVP Type UINT32

AVP Flag N/A

AF-Application-Identifier

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

Vendor ID 10415

VSA Type 504

AVP Type OCTETSTRING

AVP Flag M

AF-Charging-Identifier

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

Vendor ID 10415

VSA Type 505

AVP Type OCTETSTRING

AVP Flag M

AF-Correlation-Information

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

Vendor ID 10415

VSA Type 1276

AVP Type GROUPED

Supported group value(s):

[AF_CHARGING_IDENTIFIER]

[FLOWS]

AVP Flag M

AF-Signalling-Protocol

AF-Signalling-Protocol

Vendor ID 10415

VSA Type 529

AVP Type ENUM

Supported enumerated value(s):

0 NO_INFORMATION

1 SIP

AVP Flag N/A

AGW-IP-Address

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

Vendor ID 5535

VSA Type 1003

AVP Type OCTETSTRING

AVP Flag M

AGW-IPv6-Address

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

Vendor ID 5535

VSA Type 1004

AVP Type OCTETSTRING

AVP Flag M

AGW-MCC-MNC

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

Vendor ID 5535

VSA Type 1002

AVP Type OCTETSTRING

AVP Flag M

AIR-Flags

These flags are used by the MME or SGSN to retrieve the UE Usage Type information from the HSS during ATTACH and TAU procedures.

Vendor ID 10415

VSA Type 1679

AVP Type UINT32

AVP Flag M

AMBR

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

Vendor ID 10415

VSA Type 1435

AVP Type GROUPED

Supported group value(s):

[MAX_REQUESTED_BANDWIDTH_UL]

[MAX_REQUESTED_BANDWIDTH_DL]

[EXTENDED-MAX-REQUESTED-BW-UL]

[EXTENDED-MAX-REQUESTED-BW-DL]

AVP Flag M

AN-GW-Address

This AVP contains address of the Access Network Gateway.

Vendor ID 10415

VSA Type 1050

AVP Type ADDRESS

AVP Flag N/A

AN-GW-Status

This AVP indicates status of the Access Network Gateway. This is used to inform PCRF that S-GW is down.

Vendor ID 10415

VSA Type 2811

AVP Type ENUM

Supported enumerated value(s):

0 AN_GW_FAILED

AVP Flag N/A

AN-Trusted

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

Vendor ID 10415

VSA Type 1503

AVP Type ENUM

Supported enumerated value(s):

0 TRUSTED

1 UNTRUSTED

AVP Flag M

ANID

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

Vendor ID 10415

VSA Type 1504

AVP Type UTF8STRING

AVP Flag M

APN-Aggregate-Max-Bitrate-DL

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

Vendor ID 10415

VSA Type 1040

AVP Type UINT32

AVP Flag M

APN-Aggregate-Max-Bitrate-UL

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

Vendor ID 10415

VSA Type 1041

AVP Type UINT32

AVP Flag M

APN-Authorized

APN-Authorized

Vendor ID 10415

VSA Type 6090

AVP Type GROUPED

Supported group value(s):

[CONTEXT_IDENTIFIER]

[CALLED_STATION_ID]

[APN_BARRING_TYPE]

[FRAMED_IP_ADDRESS]

[FRAMED_IPV6_PREFIX]

[MIP6_AGENT_INFO]

[PDN_GW_ALLOCATION_TYPE]

[VPLMN_DYNAMIC_ADDRESS_ALLOWED]

[EPS_SUBSCRIBED_QOS_PROFILE]

AVP Flag M

APN-Barring-Type

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

Vendor ID 10415

VSA Type 6091

AVP Type ENUM

Supported enumerated value(s):

0 NON_3GPP_APNS_ENABLE

1 NON_3GPP_APNS_DISABLE

AVP Flag M

APN-Configuration

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

Vendor ID 10415

VSA Type 1430

AVP Type GROUPED

Supported group value(s):

[CONTEXT_IDENTIFIER]

[PDN_TYPE]

[SERVICE_SELECTION]

[EPS_SUBSCRIBED_QOS_PROFILE]

[VPLMN_DYNAMIC_ADDRESS_ALLOWED]

[MIP6_AGENT_INFO]

[VISITED_NETWORK_IDENTIFIER]

[PDN_GW_ALLOCATION_TYPE]

[3GPP_CHARGING_CHARACTERISTICS]

[AMBR]

[SERVED_PARTY_IP_ADDRESS]

[SPECIFIC_APN_INFO]

[APN_OI_REPLACEMENT]

[RESTORATION_PRIORITY]

AVP Flag M

APN-Configuration-Profile

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

Vendor ID 10415

VSA Type 1429

AVP Type GROUPED

Supported group value(s):

[CONTEXT_IDENTIFIER]

[ALL_APN_CONFIGURATIONS_INCLUDED_INDICATOR]

[APN_CONFIGURATION]

AVP Flag M

APN-OI-Replacement

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

Vendor ID 10415

VSA Type 1427

AVP Type UTF8STRING

AVP Flag M

ARP

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

Vendor ID 10415

VSA Type 6039

AVP Type UINT32

AVP Flag M

AUTN

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

Vendor ID 10415

VSA Type 1449

AVP Type OCTETSTRING

AVP Flag M

Abort-Cause

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

Vendor ID 10415

VSA Type 500

AVP Type ENUM

Supported enumerated value(s):

0 BEARER_RELEASED

1 INSUFFICIENT_SERVER_RESOURCES

2 INSUFFICIENT_BEARER_RESOURCES

4 SPONSORED_DATA_CONNECTIVITY_DISALLOWED

AVP Flag M

Acceptable-Service-Info

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

Vendor ID 10415

VSA Type 526

AVP Type GROUPED

Supported group value(s):

[MEDIA_COMPONENT_DESCRIPTION]

[MAX_REQUESTED_BANDWIDTH_DL]

[MAX_REQUESTED_BANDWIDTH_UL]

AVP Flag M

Access-Network-Charging-Address

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

Vendor ID 10415

VSA Type 501

AVP Type ADDRESS

AVP Flag M

Access-Network-Charging-Identifier

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

Vendor ID 10415

VSA Type 502

AVP Type GROUPED

Supported group value(s):

[ACCESS_NETWORK_CHARGING_IDENTIFIER_VALUE]

[FLOWS]

AVP Flag M

Access-Network-Charging-Identifier-Gx

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

Vendor ID 10415

VSA Type 1022

AVP Type GROUPED

Supported group value(s):

[ACCESS_NETWORK_CHARGING_IDENTIFIER_VALUE]

[CHARGING_RULE_BASE_NAME]

[CHARGING_RULE_NAME]

AVP Flag M

Access-Network-Charging-Identifier-Ty

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

Vendor ID 10415

VSA Type 1022

AVP Type GROUPED

Supported group value(s):

[ACCESS_NETWORK_CHARGING_IDENTIFIER_VALUE]

[CHARGING_RULE_BASE_NAME]

[CHARGING_RULE_NAME]

AVP Flag M

Access-Network-Charging-Identifier-Value

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

Vendor ID 10415

VSA Type 503

AVP Type OCTETSTRING

AVP Flag M

Access-Network-Charging-Physical-Access-Id

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

Vendor ID 8164

VSA Type 1472

AVP Type GROUPED

Supported group value(s):

[ACCESS_NETWORK_CHARGING_PHYSICAL_ACCESS_ID_VALUE]

[ACCESS_NETWORK_CHARGING_PHYSICAL_ACCESS_ID_REALM]

AVP Flag M

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

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

Vendor ID 8164

VSA Type 1474

AVP Type OCTETSTRING

AVP Flag M

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

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

Vendor ID 8164

VSA Type 1473

AVP Type OCTETSTRING

AVP Flag M

Access-Network-Info

Access-Network-Info

Vendor ID 10415

VSA Type 1526

AVP Type GROUPED

Supported group value(s):

[SSID]

[BSSID]

[LOCATION_INFORMATION_RADIUS]

[LOCATION_DATA]

[OPERATOR_NAME]

[LOGICAL_ACCESS_ID]

AVP Flag N/A

Access-Network-Information

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

Vendor ID 0

VSA Type 1263

AVP Type OCTETSTRING

AVP Flag M

Access-Network-Physical-Access-Id

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

Vendor ID 5535

VSA Type 1472

AVP Type GROUPED

Supported group value(s):

[ACCESS_NETWORK_PHYSICAL_ACCESS_ID_VALUE]

[ACCESS_NETWORK_PHYSICAL_ACCESS_ID_REALM]

AVP Flag M

Access-Network-Physical-Access-Id-Realm

Access-Network-Physical-Access-Id-Realm

Vendor ID 5535

VSA Type 1474

AVP Type OCTETSTRING

AVP Flag M

Access-Network-Physical-Access-Id-Value

Access-Network-Physical-Access-Id-Value

Vendor ID 5535

VSA Type 1473

AVP Type OCTETSTRING

AVP Flag M

Access-Network-Type

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

Vendor ID 0

VSA Type 306

AVP Type GROUPED

Supported group value(s): none

AVP Flag M

Access-Restriction-Data

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

Vendor ID 10415

VSA Type 1426

AVP Type UINT32

AVP Flag M

Account-Expiration

Account-Expiration

Vendor ID 10415

VSA Type 2309

AVP Type TIME

AVP Flag M

Accounting

Accounting

Vendor ID 9

VSA Type 131126

AVP Type GROUPED

Supported group value(s):

[ACCOUNTING_CUSTOMER_STRING]

AVP Flag M

Accounting-Customer-String

Accounting-Customer-String

Vendor ID 9

VSA Type 131127

AVP Type OCTETSTRING

AVP Flag M

Accounting-EAP-Auth-Method

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

Vendor ID 0

VSA Type 465

AVP Type UINT64

AVP Flag N/A

Accounting-Input-Octets

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

Vendor ID 0

VSA Type 363

AVP Type UINT64

AVP Flag M

Accounting-Input-Packets

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

Vendor ID 0

VSA Type 365

AVP Type UINT64

AVP Flag M

Accounting-Output-Octets

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

Vendor ID 0

VSA Type 364

AVP Type UINT64

AVP Flag M

Accounting-Output-Packets

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

Vendor ID 0

VSA Type 366

AVP Type UINT64

AVP Flag M

Accounting-PCC-R3-P-Capability

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

Vendor ID 24757

VSA Type 403

AVP Type ENUM

Supported enumerated value(s):

0 Online

1 Offline

2 Online_and_Offline

AVP Flag M

Accounting-Record-Number

This AVP contains this record within one session.

Vendor ID 0

VSA Type 485

AVP Type UINT32

AVP Flag M

Accounting-Record-Type

This AVP contains the type of accounting record being sent.

Vendor ID 0

VSA Type 480

AVP Type ENUM

Supported enumerated value(s):

1 EVENT_RECORD

2 START_RECORD

3 INTERIM_RECORD

4 STOP_RECORD

AVP Flag M

Accounting-Sub-Session-Id

This AVP contains the accounting sub-session identifier.

Vendor ID 0

VSA Type 287

AVP Type UINT64

AVP Flag M

Acct-Application-Id

Advertise support of the Accounting portion of an application.

Vendor ID 0

VSA Type 259

AVP Type UINT32

AVP Flag M

Acct-Interim-Interval

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

Vendor ID 0

VSA Type 85

AVP Type UINT32

AVP Flag M

Acct-Multi-Session-Id

Link multiple related accounting sessions.

Vendor ID 0

VSA Type 50

AVP Type UTF8STRING

AVP Flag M

Acct-Realtime-Required

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

Vendor ID 0

VSA Type 483

AVP Type ENUM

Supported enumerated value(s):

1 DELIVER_AND_GRANT

2 GRANT_AND_STORE

3 GRANT_AND_LOSE

AVP Flag M

Acct-Session-Id

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

Vendor ID 0

VSA Type 44

AVP Type OCTETSTRING

AVP Flag M

Acct-Session-Time

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

Vendor ID 10415

VSA Type 46

AVP Type UINT32

AVP Flag M

Accuracy

Accuracy

Vendor ID 10415

VSA Type 3137

AVP Type UINT32

AVP Flag M

Accuracy-Fulfilment-Indicator

Accuracy-Fulfilment-Indicator

Vendor ID 10415

VSA Type 2513

AVP Type ENUM

Supported enumerated value(s):

0 REQUESTED_ACCURACY_FULFILLED

1 REQUESTED_ACCURACY_NOT_FULFILLED

AVP Flag M

Active-APN

This AVP indicates the active APN.

Vendor ID 10415

VSA Type 1612

AVP Type GROUPED

Supported group value(s):

[CONTEXT_IDENTIFIER]

[SERVICE_SELECTION]

[MIP6_AGENT_INFO]

[VISITED_NETWORK_IDENTIFIER]

[SPECIFIC_APN_INFO]

AVP Flag M

Additional-Context-Identifier

Additional-Context-Identifier

Vendor ID 10415

VSA Type 1683

AVP Type UINT32

AVP Flag N/A

Additional-MBMS-Trace-Info

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

Vendor ID 10415

VSA Type 910

AVP Type OCTETSTRING

AVP Flag M

Address-Realm

This AVP contains the realm that the user belongs to.

Vendor ID 0

VSA Type 1005

AVP Type OCTETSTRING

AVP Flag M

Advice-Of-Charge

Advice-Of-Charge

Vendor ID 9

VSA Type 131097

AVP Type GROUPED

Supported group value(s):

[APPEND_URL]

[CONFIRM_TOKEN]

AVP Flag M

Age-Of-Location-Estimate

This AVP indicates how long ago the location estimate was obtained, in minutes.

Vendor ID 10415

VSA Type 2514

AVP Type UINT32

AVP Flag M

Age-Of-Location-Information

Age-Of-Location-Information

Vendor ID 10415

VSA Type 1611

AVP Type UINT32

AVP Flag N/A

Aggr-Prefix-Len

Aggr-Prefix-Len

Vendor ID 9

VSA Type 131262

AVP Type UINT32

AVP Flag N/A

Alert-Reason

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

Vendor ID 10415

VSA Type 1434

AVP Type ENUM

Supported enumerated value(s):

0 UE_PRESENT

1 UE_MEMORY_AVAILABLE

AVP Flag M

All-APN-Configurations-Included-Indicator

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

Vendor ID 10415

VSA Type 1428

AVP Type ENUM

Supported enumerated value(s):

0 ALL_APN_CONFIGURATIONS_INCLUDED

1 MODIFIED_ADDED_APN_CONFIGURATIONS_INCLUDED

AVP Flag M

Allocation-Retention-Priority

Allocation-Retention-Priority

Vendor ID 10415

VSA Type 1034

AVP Type GROUPED

Supported group value(s):

[PRIORITY_LEVEL]

[PRE_EMPTION_CAPABILITY]

[PRE_EMPTION_VULNERABILITY]

AVP Flag M

Alternative-APN

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

Vendor ID 10415

VSA Type 905

AVP Type UTF8STRING

AVP Flag M

Anchor-Data-Path-Address

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

Vendor ID 24757

VSA Type 401

AVP Type OCTETSTRING

AVP Flag M

Append-URL

Append-URL

Vendor ID 9

VSA Type 131098

AVP Type ENUM

Supported enumerated value(s):

0 DISABLE_APPEND_URL

1 ENABLE_APPEND_URL

AVP Flag M

Application-Detection-Information

This AVP is used to report once the start/stop of the application traffic, defined by TDF-Application-Identifier, has been detected, in case PCRF has subscribed for APPLICATION_START/APPLICATION_STOP Event-Triggers, unless a request to mute such a notification (Mute-Notification AVP) is part of the corresponding Charging-Rule-Definition AVP to the PCEF.

Vendor ID 10415

VSA Type 1098

AVP Type GROUPED

Supported group value(s):

[TDF_APPLICATION_IDENTIFIER]

[TDF_APPLICATION_INSTANCE_IDENTIFIER]

[FLOW_INFORMATION]

AVP Flag N/A

Application-Provided-Called-Party-Address

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

Vendor ID 10415

VSA Type 837

AVP Type UTF8STRING

AVP Flag M

Application-Server

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

Vendor ID 10415

VSA Type 836

AVP Type UTF8STRING

AVP Flag M

Application-Server-Information

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

Vendor ID 10415

VSA Type 850

AVP Type GROUPED

Supported group value(s):

[APPLICATION_SERVER]

[APPLICATION_PROVIDED_CALLED_PARTY_ADDRESS]

AVP Flag M

Application-Service-Provider-Identity

Application-Service-Provider-Identity

Vendor ID 0

VSA Type 532

AVP Type UTF8STRING

AVP Flag N/A

Associated-Identities

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

Vendor ID 10415

VSA Type 632

AVP Type GROUPED

Supported group value(s):

[USER_NAME]

AVP Flag M

Associated-Registered-Identities

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

Vendor ID 10415

VSA Type 647

AVP Type GROUPED

Supported group value(s):

[USER_NAME]

AVP Flag N/A

Associated-URI

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

Vendor ID 10415

VSA Type 856

AVP Type UTF8STRING

AVP Flag M

Attribute-String

Attribute-String

Vendor ID 9

VSA Type 131092

AVP Type UTF8STRING

AVP Flag M

Auth-Application-Id

This AVP contains the Diameter supported authorization application ID.

Vendor ID 0

VSA Type 258

AVP Type UINT32

AVP Flag M

Auth-Grace-Period

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

Vendor ID 0

VSA Type 276

AVP Type UINT32

AVP Flag M

Auth-Profile-Id-Bi-Direction

3GPP2 Auth-Profile-Id-Bi-Direction

Vendor ID 5535

VSA Type 6081

AVP Type UINT32

AVP Flag M

Auth-Profile-Id-Forward

3GPP2 Auth-Profile-Id-Forward

Vendor ID 5535

VSA Type 6079

AVP Type UINT32

AVP Flag M

Auth-Profile-Id-Reverse

3GPP2 Auth-Profile-Id-Reverse

Vendor ID 5535

VSA Type 6080

AVP Type UINT32

AVP Flag M

Auth-Request-Type

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

Vendor ID 0

VSA Type 274

AVP Type ENUM

Supported enumerated value(s):

1 AUTHENTICATE_ONLY

2 AUTHORIZE_ONLY

3 AUTHORIZE_AUTHENTICATE

AVP Flag M

Auth-Session-State

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

Vendor ID 0

VSA Type 277

AVP Type ENUM

Supported enumerated value(s):

0 STATE_MAINTAINED

1 NO_STATE_MAINTAINED

AVP Flag M

Authentication-Info

This AVP contains the Authentication Vectors.

Vendor ID 10415

VSA Type 6016

AVP Type GROUPED

Supported group value(s):

[EPS_VECTOR]

[UMTS_VECTOR]

[GERAN_VECTOR]

AVP Flag M

Authorised-QoS

This AVP contains the authorized QoS.

Vendor ID 0

VSA Type 849

AVP Type UTF8STRING

AVP Flag M

Authorization-Lifetime

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

Vendor ID 0

VSA Type 291

AVP Type UINT32

AVP Flag M

Authorization-Token

This AVP contains the authorization token defined in RFC 3520.

Vendor ID 10415

VSA Type 506

AVP Type OCTETSTRING

AVP Flag M

Authorized-QoS

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

Vendor ID 10415

VSA Type 1016

AVP Type GROUPED

Supported group value(s):

[QOS_CLASS]

[MAX_REQUESTED_BANDWIDTH_UL]

[MAX_REQUESTED_BANDWIDTH_DL]

AVP Flag M

BCID

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

Vendor ID 4491

VSA Type 200

AVP Type UTF8STRING

AVP Flag M

BSID

BSID

Vendor ID 0

VSA Type 10003

AVP Type OCTETSTRING

AVP Flag M

BSSGP-Cause

BSSGP-Cause

Vendor ID 10415

VSA Type 4309

AVP Type UINT32

AVP Flag M

BSSID

BSSID

Vendor ID 10415

VSA Type 2716

AVP Type UTF8STRING

AVP Flag M

Bearer-Control-Mode

This AVP indicates the preferred Bearer Control Mode.

Vendor ID 10415

VSA Type 1023

AVP Type ENUM

Supported enumerated value(s):

0 UE_ONLY

1 RESERVED

2 UE_NW

AVP Flag M

Bearer-Identifier

This AVP indicates the bearer to which the information belongs.

Vendor ID 10415

VSA Type 1020

AVP Type OCTETSTRING

AVP Flag M

Bearer-Operation

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

Vendor ID 10415

VSA Type 1021

AVP Type ENUM

Supported enumerated value(s):

0 TERMINATION

1 ESTABLISHMENT

2 MODIFICATION

AVP Flag M

Bearer-Service

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

Vendor ID 10415

VSA Type 854

AVP Type OCTETSTRING

AVP Flag M

Bearer-Usage

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

Vendor ID 10415

VSA Type 1000

AVP Type ENUM

Supported enumerated value(s):

0 GENERAL

1 IMS_SIGNALLING

2 DEDICATED

AVP Flag M

Billing-Plan-Definition

Billing-Plan-Definition

Vendor ID 9

VSA Type 131079

AVP Type GROUPED

Supported group value(s):

[BILLING_PLAN_NAME]

[ONLINE]

[OFFLINE]

[VIRTUAL_ONLINE]

[USER_IDLE_TIMER]

[USER_IDLE_POD]

[USER_DEFAULT]

[CISCO_QOS_PROFILE_UPLINK]

[CISCO_QOS_PROFILE_DOWNLINK]

[SERVICE_INFO]

AVP Flag M

Billing-Plan-Install

Billing-Plan-Install

Vendor ID 9

VSA Type 131187

AVP Type GROUPED

Supported group value(s):

[BILLING_PLAN_DEFINITION]

AVP Flag M

Billing-Plan-Name

Billing-Plan-Name

Vendor ID 9

VSA Type 131140

AVP Type OCTETSTRING

AVP Flag M

Billing-Plan-Remove

Billing-Plan-Remove

Vendor ID 9

VSA Type 131188

AVP Type GROUPED

Supported group value(s):

[BILLING_PLAN_NAME]

AVP Flag M

Billing-Policy-Definition

Billing-Policy-Definition

Vendor ID 9

VSA Type 131074

AVP Type GROUPED

Supported group value(s):

[BILLING_POLICY_NAME]

[POLICY_MAP_NAME]

[CLASS_MAP_NAME]

[HEADER_GROUP_NAME]

[ACCOUNTING]

AVP Flag M

Billing-Policy-Install

Billing-Policy-Install

Vendor ID 9

VSA Type 131181

AVP Type GROUPED

Supported group value(s):

[BILLING_POLICY_DEFINITION]

AVP Flag M

Billing-Policy-Name

Billing-Policy-Name

Vendor ID 9

VSA Type 131088

AVP Type OCTETSTRING

AVP Flag M

Billing-Policy-Remove

Billing-Policy-Remove

Vendor ID 9

VSA Type 131182

AVP Type GROUPED

Supported group value(s):

[BILLING_POLICY_NAME]

AVP Flag M

Binding-Information

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

Vendor ID 13019

VSA Type 450

AVP Type GROUPED

Supported group value(s):

[BINDING_INPUT_LIST]

[BINDING_OUTPUT_LIST]

AVP Flag N/A

Binding-Input-List

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

Vendor ID 13019

VSA Type 451

AVP Type GROUPED

Supported group value(s):

[V6_TRANSPORT_ADDRESS]

[V4_TRANSPORT_ADDRESS]

AVP Flag N/A

Binding-Output-List

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

Vendor ID 13019

VSA Type 452

AVP Type GROUPED

Supported group value(s):

[V6_TRANSPORT_ADDRESS]

[V4_TRANSPORT_ADDRESS]

AVP Flag N/A

CC-Correlation-Id

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

Vendor ID 0

VSA Type 411

AVP Type OCTETSTRING

AVP Flag M

CC-Input-Octets

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

Vendor ID 0

VSA Type 412

AVP Type UINT64

AVP Flag M

CC-Money

This AVP indicates the monetary amount in the given currency.

Vendor ID 0

VSA Type 413

AVP Type GROUPED

Supported group value(s):

[UNIT_VALUE]

[CURRENCY_CODE]

AVP Flag M

CC-Output-Octets

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

Vendor ID 0

VSA Type 414

AVP Type UINT64

AVP Flag M

CC-Request-Number

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

Vendor ID 0

VSA Type 415

AVP Type UINT32

AVP Flag M

CC-Request-Type

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

Vendor ID 0

VSA Type 416

AVP Type ENUM

Supported enumerated value(s):

1 INITIAL_REQUEST

2 UPDATE_REQUEST

3 TERMINATION_REQUEST

4 EVENT_REQUEST

AVP Flag M

CC-Service-Specific-Units

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

Vendor ID 0

VSA Type 417

AVP Type UINT64

AVP Flag M

CC-Session-Failover

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

Vendor ID 0

VSA Type 418

AVP Type ENUM

Supported enumerated value(s):

0 FAILOVER_NOT_SUPPORTED

1 FAILOVER_SUPPORTED

AVP Flag M

CC-Sub-Session-Id

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

Vendor ID 0

VSA Type 419

AVP Type UINT64

AVP Flag M

CC-Time

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

Vendor ID 0

VSA Type 420

AVP Type UINT32

AVP Flag M

CC-Total-Octets

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

Vendor ID 0

VSA Type 421

AVP Type UINT64

AVP Flag M

CC-Unit-Type

This AVP contains the type of units.

Vendor ID 0

VSA Type 454

AVP Type ENUM

Supported enumerated value(s): none

AVP Flag M

CDR-Generation-Delay

CDR-Generation-Delay

Vendor ID 9

VSA Type 131131

AVP Type UINT32

AVP Flag N/A

CDR-Time-Threshold

CDR-Time-Threshold

Vendor ID 9

VSA Type 131096

AVP Type UINT32

AVP Flag N/A

CDR-Volume-Threshold

CDR-Volume-Threshold

Vendor ID 9

VSA Type 131095

AVP Type UINT32

AVP Flag N/A

CG-Address

This AVP contains IP address of the Charging Gateway.

Vendor ID 10415

VSA Type 846

AVP Type ADDRESS

AVP Flag M

CHAP-Auth

CHAP-Authentication

Vendor ID 10415

VSA Type 402

AVP Type GROUPED

Supported group value(s):

[CHAP_IDENT]

[CHAP_RESPONSE]

AVP Flag M

CHAP-Challenge

CHAP-Challenge

Vendor ID 10415

VSA Type 60

AVP Type OCTETSTRING

AVP Flag M

CHAP-Ident

CHAP-Identifier

Vendor ID 10415

VSA Type 404

AVP Type OCTETSTRING

AVP Flag M

CHAP-Response

CHAP-Response

Vendor ID 10415

VSA Type 405

AVP Type OCTETSTRING

AVP Flag M

CIPA

CIPA

Vendor ID 7898

VSA Type 2005

AVP Type OCTETSTRING

AVP Flag N/A

CLR-Flags

CLR-Flags

Vendor ID 10415

VSA Type 1638

AVP Type UINT32

AVP Flag N/A

CMR-Flags

CMR-Flags

Vendor ID 10415

VSA Type 4317

AVP Type UINT32

AVP Flag M

CN-IP-Multicast-Distribution

CN-IP-Multicast-Distribution

Vendor ID 10415

VSA Type 921

AVP Type ENUM

Supported enumerated value(s): none

AVP Flag M

CSG-Access-Mode

This AVP contains the mode in which the CSG cell user is accessing to, operates.

Vendor ID 10415

VSA Type 2317

AVP Type ENUM

Supported enumerated value(s):

0 CLOSED_MODE

1 HYBRID_MODE

AVP Flag M

CSG-Id

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

Vendor ID 10415

VSA Type 1437

AVP Type UINT32

AVP Flag M

CSG-Membership-Indication

This AVP indicates the UE is a member of the accessing CSG cell, if the access mode is Hybrid, as described in TS 29.060, and in TS 29.274. If this indication is not present, this means the UE is a not member of the CSG cell for hybrid access mode.

Vendor ID 10415

VSA Type 2318

AVP Type ENUM

Supported enumerated value(s):

0 NOT_CSG_MEMBER

1 CSG_MEMBER

AVP Flag M

CSG-Subscription-Data

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

Vendor ID 10415

VSA Type 1436

AVP Type GROUPED

Supported group value(s):

[CSG_ID]

[EXPIRATION_DATE]

AVP Flag M

Call-Barring-Info-List

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

Vendor ID 10415

VSA Type 1488

AVP Type GROUPED

Supported group value(s):

[SS_CODE]

AVP Flag M

Call-ID-SIP-Header

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

Vendor ID 10415

VSA Type 643

AVP Type OCTETSTRING

AVP Flag N/A

Callback-Id

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

Vendor ID 0

VSA Type 20

AVP Type UTF8STRING

AVP Flag M

Callback-Number

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

Vendor ID 0

VSA Type 19

AVP Type UTF8STRING

AVP Flag M

Called-Asserted-Identity

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

Vendor ID 10415

VSA Type 1250

AVP Type UTF8STRING

AVP Flag M

Called-Party-Address

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

Vendor ID 10415

VSA Type 832

AVP Type UTF8STRING

AVP Flag M

Called-Station-Id

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

Vendor ID 0

VSA Type 30

AVP Type OCTETSTRING

AVP Flag M

Calling-Party-Address

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

Vendor ID 10415

VSA Type 831

AVP Type UTF8STRING

AVP Flag M

Calling-Station-Id

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

Vendor ID 0

VSA Type 31

AVP Type UTF8STRING

AVP Flag M

Cancellation-Type

This AVP indicates the type of cancellation.

Vendor ID 10415

VSA Type 1420

AVP Type ENUM

Supported enumerated value(s):

0 MME_UPDATE_PROCEDURE

1 SGSN_UPDATE_PROCEDURE

2 SUBSCRIPTION_WITHDRAWAL

3 UPDATE_PROCEDURE_IWF

AVP Flag M

Carrier-Select-Routing-Information

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

Vendor ID 10415

VSA Type 2023

AVP Type UTF8STRING

AVP Flag M

Cause

Cause

Vendor ID 10415

VSA Type 860

AVP Type GROUPED

Supported group value(s):

[CAUSE_CODE]

[NODE_FUNCTIONALITY]

AVP Flag M

Cause-Code

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

Vendor ID 0

VSA Type 861

AVP Type INT32

AVP Flag M

Cause-Type

Cause-Type

Vendor ID 10415

VSA Type 4301

AVP Type UINT32

AVP Flag M

Cell-Global-Identity

This AVP contains the Cell Global Identification of the user.

Vendor ID 10415

VSA Type 1604

AVP Type OCTETSTRING

AVP Flag M

Change-Condition

This AVP indicates the change in charging condition.

Vendor ID 10415

VSA Type 2037

AVP Type ENUM

Supported enumerated value(s):

0 NORMAL_RELEASE

1 ABNORMAL_RELEASE

2 QOS_CHANGE

3 VOLUME_LIMIT

4 TIME_LIMIT

5 SERVING_NODE_CHANGE

6 SERVING_NODE_PLMN_CHANGE

7 USER_LOCATION_CHANGE

8 RAT_CHANGE

9 UE_TIME_ZONE_CHANGE

10 TARIFF_TIME_CHANGE

11 SERVICE_IDLED_OUT

12 SERVICE_SPECIFIC_UNIT_LIMIT

13 MAX_NUMBER_OF_CHARGING_CONDITIONS

14 MANAGEMENT_INTERVENTION

AVP Flag M

Change-Time

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

Vendor ID 10415

VSA Type 2038

AVP Type TIME

AVP Flag M

Charged-Party

Charged-Party

Vendor ID 10415

VSA Type 857

AVP Type UTF8STRING

AVP Flag M

Charging-Action-Definition

Charging-Action-Definition

Vendor ID 9

VSA Type 132014

AVP Type GROUPED

Supported group value(s):

[CHARGING_ACTION_NAME]

[QOS_INFORMATION]

[FLOW_STATUS]

[REDIRECT_SERVER]

AVP Flag N/A

Charging-Action-Install

Charging-Action-Install

Vendor ID 9

VSA Type 132012

AVP Type GROUPED

Supported group value(s):

[CHARGING_ACTION_DEFINITION]

AVP Flag N/A

Charging-Action-Name

Charging-Action-Name

Vendor ID 9

VSA Type 132015

AVP Type OCTETSTRING

AVP Flag N/A

Charging-Action-Remove

Charging-Action-Remove

Vendor ID 9

VSA Type 132013

AVP Type GROUPED

Supported group value(s):

[CHARGING_ACTION_NAME]

AVP Flag N/A

Charging-Characteristics

This AVP contains the charging mode to be applied.

Vendor ID 10415

VSA Type 11006

AVP Type UINT32

AVP Flag M

Charging-Characteristics-Selection-Mode

Charging-Characteristics-Selection-Mode

Vendor ID 10415

VSA Type 2066

AVP Type ENUM

Supported enumerated value(s):

0 SERVING-NODE-SUPPLIED

1 SUBSCRIPTION-SPECIFIC

2 APN-SPECIFIC

3 HOME-DEFAULT

4 ROAMING-DEFAULT

5 VISITING-DEFAULT

AVP Flag M

Charging-Correlation-Indicator

Charging-Correlation-Indicator

Vendor ID 10415

VSA Type 1073

AVP Type ENUM

Supported enumerated value(s):

0 CHARGING_IDENTIFIER_REQUIRED

AVP Flag M

Charging-Data

This AVP contains addresses of the charging functions.

Vendor ID 10415

VSA Type 11005

AVP Type GROUPED

Supported group value(s):

[CHARGING_CHARACTERISTICS]

AVP Flag M

Charging-Information

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

Vendor ID 10415

VSA Type 618

AVP Type GROUPED

Supported group value(s):

[PRIMARY_EVENT_CHARGING_FUNCTION_NAME]

[SECONDARY_EVENT_CHARGING_FUNCTION_NAME]

[PRIMARY_CHARGING_COLLECTION_FUNCTION_NAME]

[SECONDARY_CHARGING_COLLECTION_FUNCTION_NAME]

AVP Flag M

Charging-Rule-Base-Name

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

Vendor ID 10415

VSA Type 1004

AVP Type UTF8STRING

AVP Flag M

Charging-Rule-Definition

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

Vendor ID 10415

VSA Type 1003

AVP Type GROUPED

Supported group value(s):

[CHARGING_RULE_NAME]

[SERVICE_IDENTIFIER]

[RATING_GROUP]

[FLOW_DESCRIPTION]

[REPORTING_LEVEL]

[ONLINE]

[OFFLINE]

[FLOW_STATUS]

[QOS_INFORMATION]

[METERING_METHOD]

[PRECEDENCE]

[AF_CHARGING_IDENTIFIER]

[MUTE_NOTIFICATION]

[TDF_APPLICATION_IDENTIFIER]

[REDIRECT_INFORMATION]

[FLOWS]

AVP Flag M

Charging-Rule-Event

Charging-Rule-Event

Vendor ID 9

VSA Type 131124

AVP Type GROUPED

Supported group value(s):

[CHARGING_RULE_NAME]

[CHARGING_RULE_TRIGGER_TYPE]

[CISCO_VOLUME_USAGE]

[CISCO_TIME_USAGE]

[CISCO_REPORT_USAGE]

AVP Flag M

Charging-Rule-Event-Trigger

Charging-Rule-Event-Trigger

Vendor ID 9

VSA Type 131139

AVP Type GROUPED

Supported group value(s):

[CHARGING_RULE_TRIGGER_TYPE]

[VOLUME_THRESHOLD]

[TIME_THRESHOLD]

[CISCO_REPORT_USAGE]

[VOLUME_THRESHOLD_64]

AVP Flag M

Charging-Rule-Install

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

Vendor ID 10415

VSA Type 1001

AVP Type GROUPED

Supported group value(s):

[CHARGING_RULE_DEFINITION]

[CHARGING_RULE_NAME]

[CHARGING_RULE_BASE_NAME]

[BEARER_IDENTIFIER]

[RULE_ACTIVATION_TIME]

[RULE_DEACTIVATION_TIME]

[RESOURCE_ALLOCATION_NOTIFICATION]

AVP Flag M

Charging-Rule-Name

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

Vendor ID 10415

VSA Type 1005

AVP Type OCTETSTRING

AVP Flag M

Charging-Rule-Name-LI

Charging rule name for LI-Indicator-Gx.

Vendor ID 10415

VSA Type 1005

AVP Type OCTETSTRING

AVP Flag M

Charging-Rule-Remove

This AVP contains the deactivated or removed Charging/Firewall rules from the Policy server. Charging/Firewall ruledefs for a subscriber can be dynamically deactivated from gx server. If the incoming

rule fails to match in the charging ruledefs of a rulebase, then there will be a lookup with the Firewall ruledefs of the rulebase.

Vendor ID 10415

VSA Type 1002

AVP Type GROUPED

Supported group value(s):

[CHARGING_RULE_NAME]

[CHARGING_RULE_BASE_NAME]

[REQUIRED_ACCESS_INFO]

AVP Flag M

Charging-Rule-Report

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

Vendor ID 10415

VSA Type 1018

AVP Type GROUPED

Supported group value(s):

[CHARGING_RULE_NAME]

[CHARGING_RULE_BASE_NAME]

[PCC_RULE_STATUS]

[RULE_FAILURE_CODE]

[FINAL_UNIT_INDICATION]

[RAN_NAS_RELEASE_CAUSE]

AVP Flag M

Charging-Rule-Trigger-Type

Charging-Rule-Trigger-Type

Vendor ID 9

VSA Type 131123

AVP Type ENUM

Supported enumerated value(s):

0 NO_TRIGGERS

1 VOL_THRESHOLD

2 TIME_THRESHOLD

3 SVC_FLOW_DETECT

4 CHRG_RULE_REMOVE

AVP Flag M

Check-Balance-Result

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

Vendor ID 0

VSA Type 422

AVP Type ENUM

Supported enumerated value(s):

0 ENOUGH_CREDIT

1 NO_CREDIT

AVP Flag M

Cisco-Answer-Charging-Rule-Usage

Cisco-Answer-Charging-Rule-Usage

Vendor ID 9

VSA Type 131254

AVP Type GROUPED

Supported group value(s):

[CHARGING_RULE_NAME]

[CISCO_REQUEST_USAGE_TYPE]

[CISCO_VOLUME_USAGE]

[CISCO_TIME_USAGE]

AVP Flag M

Cisco-Answer-Service-Group-Usage

Cisco-Answer-Service-Group-Usage

Vendor ID 9

VSA Type 131255

AVP Type GROUPED

Supported group value(s):

[SERVICE_GROUP_NAME]

[CISCO_REQUEST_USAGE_TYPE]

[CISCO_VOLUME_USAGE]

[CISCO_TIME_USAGE]

AVP Flag M

Cisco-Answer-User-Usage

Cisco-Answer-User-Usage

Vendor ID 9

VSA Type 131250

AVP Type GROUPED

Supported group value(s):

[CISCO_REQUEST_USAGE_TYPE]

[CISCO_VOLUME_USAGE]

[CISCO_TIME_USAGE]

AVP Flag M

Cisco-CC-Failure-Type

This attribute indicates the OCS failure reasons to the PCRF.

Vendor ID 9

VSA Type 132077

AVP Type UINT32

AVP Flag M

Cisco-Charging-Rule-Definition

Cisco-Charging-Rule-Definition

Vendor ID 9

VSA Type 131072

AVP Type GROUPED

Supported group value(s):

[CHARGING_RULE_NAME]

[SERVICE_NAME]

[RATING_GROUP]

[CISCO_FLOW_DESCRIPTION]

[CISCO_FLOW_STATUS]

[QOS_INFORMATION]

[ONLINE]

[OFFLINE]

[PRECEDENCE]

[AF_CHARGING_IDENTIFIER]

[CHARGING_RULE_EVENT_TRIGGER]

[REDIRECT_SERVER]

[MONITORING_KEY]

AVP Flag M

Cisco-Event

Cisco-Event

Vendor ID 9

VSA Type 131195

AVP Type GROUPED

Supported group value(s):

[CISCO_EVENT_TRIGGER_TYPE]

[TCP_SYN]

[CISCO_VOLUME_USAGE]

[CISCO_TIME_USAGE]

[CISCO_REPORT_USAGE]

[CISCO_USER_AGENT]

[CISCO_CC_FAILURE_TYPE]

AVP Flag M

Cisco-Event-Trigger

Cisco-Event-Trigger

Vendor ID 9

VSA Type 131193

AVP Type GROUPED

Supported group value(s):

[CISCO_EVENT_TRIGGER_TYPE]

[VOLUME_THRESHOLD]

[TIME_THRESHOLD]

[CISCO_REPORT_USAGE]

[VOLUME_THRESHOLD_64]

AVP Flag M

Cisco-Event-Trigger-Type

Cisco-Event-Trigger-Type

Vendor ID 9

VSA Type 131192

AVP Type ENUM

Supported enumerated value(s):

0 NO_CISCO_EVENT_TRIGGERS

1 TCP_SYN_DETECTION

2 VOL_THRESHOLD

3 TIME_THRESHOLD

4 USER_AGENT_DETECTION

5 CREDIT_CONTROL_FAILURE

AVP Flag M

Cisco-Flow-Description

Cisco-Flow-Description

Vendor ID 9

VSA Type 131160

AVP Type GROUPED

Supported group value(s):

[CONTENT_NAME]

[PRECEDENCE]

[FLOW_DESCRIPTION]

[FLOW_INFORMATION]

AVP Flag M

Cisco-Flow-Status

Cisco-Flow-Status

Vendor ID 9

VSA Type 131169

AVP Type ENUM

Supported enumerated value(s):

0 FORWARD

1 BLOCK

2 REDIRECT

AVP Flag M

Cisco-QoS

Cisco-QoS

Vendor ID 9

VSA Type 131170

AVP Type GROUPED

Supported group value(s):

[QOS_RATE_LIMIT_UL]

[QOS_RATE_LIMIT_DL]

AVP Flag M

Cisco-QoS-Profile

Cisco-QoS-Profile

Vendor ID 9

VSA Type 131237

AVP Type GROUPED

Supported group value(s):

[CISCO_QOS_PROFILE_NAME]

[QOS_RATE_LIMIT]

AVP Flag M

Cisco-QoS-Profile-Downlink

Cisco-QoS-Profile-Downlink

Vendor ID 9

VSA Type 131241

AVP Type GROUPED

Supported group value(s):

[CISCO_QOS_PROFILE_NAME]

AVP Flag M

Cisco-QoS-Profile-Install

Cisco-QoS-Profile-Install

Vendor ID 9

VSA Type 131238

AVP Type GROUPED

Supported group value(s):

[CISCO_QOS_PROFILE]

AVP Flag M

Cisco-QoS-Profile-Name

Cisco-QoS-Profile-Name

Vendor ID 9

VSA Type 131229

AVP Type UTF8STRING

AVP Flag M

Cisco-QoS-Profile-Remove

Cisco-QoS-Profile-Remove

Vendor ID 9

VSA Type 131239

AVP Type GROUPED

Supported group value(s):

[CISCO_QOS_PROFILE_NAME]

AVP Flag M

Cisco-QoS-Profile-Uplink

Cisco-QoS-Profile-Uplink

Vendor ID 9

VSA Type 131240

AVP Type GROUPED

Supported group value(s):

[CISCO_QOS_PROFILE_NAME]

AVP Flag M

Cisco-Quota-Consumption-Time

Cisco-Quota-Consumption-Time

Vendor ID 9

VSA Type 131213

AVP Type UINT32

AVP Flag N/A

Cisco-Report-Usage

Cisco-Report-Usage

Vendor ID 9

VSA Type 131248

AVP Type ENUM

Supported group value(s):

[EVENT_TRIGGER]

AVP Flag M

Cisco-Request-Charging-Rule-Usage

Cisco-Request-Charging-Rule-Usage

Vendor ID 9

VSA Type 131252

AVP Type GROUPED

Supported group value(s):

[CHARGING_RULE_NAME]

[CISCO_REQUEST_USAGE_TYPE]

AVP Flag M

Cisco-Request-Service-Group-Usage

Cisco-Request-Service-Group-Usage

Vendor ID 9

VSA Type 131253

AVP Type GROUPED

Supported group value(s):

[SERVICE_GROUP_NAME]

[CISCO_REQUEST_USAGE_TYPE]

AVP Flag M

Cisco-Request-Usage-Type

Cisco-Request-Usage-Type

Vendor ID 9

VSA Type 131251

AVP Type ENUM

Supported enumerated value(s):

0 VOL_USAGE

1 TIME_USAGE

AVP Flag M

Cisco-Time-Usage

Cisco-Time-Usage

Vendor ID 9

VSA Type 131156

AVP Type GROUPED

Supported group value(s):

[DURATION]

[FIRST_PACKET_TIMESTAMP]

[LAST_PACKET_TIMESTAMP]

AVP Flag M

Cisco-User-Agent

Cisco-User-Agent

Vendor ID 9

VSA Type 131256

AVP Type UTF8STRING

AVP Flag M

Cisco-User-Location

Cisco-User-Location

Vendor ID 9

VSA Type 132000

AVP Type GROUPED

Supported group value(s):

[AN_GW_ADDRESS]

[3GPP_SGSN_MCC_MNC]

[3GPP_SGSN_ADDRESS]

[3GPP_SGSN_IPV6_ADDRESS]

[RAI]

[3GPP_USER_LOCATION_INFO]

AVP Flag N/A

Cisco-Volume-Usage

Cisco-Volume-Usage

Vendor ID 9

VSA Type 131155

AVP Type UINT64

AVP Flag N/A

Civic-Addr

Civic-Addr

Vendor ID 9

VSA Type 132068

AVP Type UTF8STRING

AVP Flag N/A

Civic-Location

This AVP contains location information.

Vendor ID 13019

VSA Type 355

AVP Type OCTETSTRING

AVP Flag M

Class

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

Vendor ID 0

VSA Type 25

AVP Type OCTETSTRING

AVP Flag M

Class-Map-Name

Class-Map-Name

Vendor ID 9

VSA Type 131214

AVP Type UTF8STRING

AVP Flag M

Client-Group-Id

Client-Group-Id

Vendor ID 9

VSA Type 131143

AVP Type GROUPED

Supported group value(s):

[ACL_NUMBER]

[ACL_NAME]

AVP Flag M

Client-Identity

This AVP contains the ISDN number of the external client.

Vendor ID 10415

VSA Type 1480

AVP Type OCTETSTRING

AVP Flag M

CoA-IP-Address

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

Vendor ID 10415

VSA Type 1035

AVP Type ADDRESS

AVP Flag M

CoA-Information

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

Vendor ID 10415

VSA Type 1039

AVP Type GROUPED

Supported group value(s):

[TUNNEL_INFORMATION]

[COA_IP_ADDRESS]

AVP Flag M

Codec-Data

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

Vendor ID 10415

VSA Type 524

AVP Type OCTETSTRING

AVP Flag M

Communication-Failure-Information

Communication-Failure-Information

Vendor ID 10415

VSA Type 4300

AVP Type GROUPED

Supported group value(s):

[CAUSE_TYPE]

[S1AP_CAUSE]

[RANAP_CAUSE]

[BSSGP_CAUSE]

[GMM_CAUSE]

[SM_CAUSE]

AVP Flag M

Complete-Data-List-Included-Indicator

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

Vendor ID 10415

VSA Type 1468

AVP Type ENUM

Supported enumerated value(s):

0 ALL_PDP_CONTEXTS_INCLUDED

1 MODIFIED_ADDED_PDP_CONTEXTS_INCLUDED

AVP Flag M

Conditional-APN-Aggregate-Max-Bitrate

Conditional-APN-Aggregate-Max-Bitrate

Vendor ID 10415

VSA Type 2818

AVP Type GROUPED

Supported group value(s):

[APN_AGGREGATE_MAX_BITRATE_UL]

[APN_AGGREGATE_MAX_BITRATE_DL]

[EXTENDED-APN-AMBR-UL]

[EXTENDED-APN-AMBR-DL]

[IP_CAN_TYPE]

[RAT_TYPE]

AVP Flag N/A

Conditional-Policy-Information

Conditional-Policy-Information

Vendor ID 10415

VSA Type 2840

AVP Type GROUPED

Supported group value(s):

[EXECUTION_TIME]

[DEFAULT_EPS_BEARER_QOS]

[APN_AGGREGATE_MAX_BITRATE_UL]

[APN_AGGREGATE_MAX_BITRATE_DL]

[CONDITIONAL_APN_AGGREGATE_MAX_BITRATE]

AVP Flag N/A

Confidentiality-Key

This AVP contains the Confidentiality Key (CK).

Vendor ID 10415

VSA Type 625

AVP Type OCTETSTRING

AVP Flag M

Configuration-Token

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

Vendor ID 0

VSA Type 78

AVP Type OCTETSTRING

AVP Flag N/A

Confirm-Token

Confirm-Token

Vendor ID 9

VSA Type 131099

AVP Type OCTETSTRING

AVP Flag M

Confirm-Token-V

Confirm-Token-V

Vendor ID 9

VSA Type 131117

AVP Type OCTETSTRING

AVP Flag M

Connect-Info

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

Vendor ID 0

VSA Type 77

AVP Type UTF8STRING

AVP Flag M

Connection-Action

Connection-Action

Vendor ID 10415

VSA Type 4314

AVP Type UINT32

AVP Flag M

Contact

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

Vendor ID 10415

VSA Type 641

AVP Type OCTETSTRING

AVP Flag N/A

Content-Definition

Content-Definition

Vendor ID 9

VSA Type 131073

AVP Type GROUPED

Supported group value(s):

[CONTENT_NAME]

[CONTENT_FLOW_DESCRIPTION]

[CONTENT_SCOPE]

[CONTENT_IDLE_TIMER]

[NEXTHOP]

[L7_PARSE_PROTOCOL_TYPE]

[L7_PARSE_LENGTH]

[BILLING_POLICY_NAME]

[REPLICATE_SESSION]

[INTERMEDIATE_CDR_THRESHOLD]

[CDR_GENERATION_DELAY]

[CONTENT_PENDING_TIMER]

[OPERATION_STATUS]

[SUBSCRIBER_IP_SOURCE]

[FLOW_STATUS_POLICY_MISMATCH]

[RELATIVE_URL]

[CONTROL_URL]

[DOMAIN_GROUP_NAME]

[MINING]

[NEXTHOP_MEDIA]

[NEXTHOP_OVERRIDE]

AVP Flag M

Content-Disposition

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

Vendor ID 10415

VSA Type 828

AVP Type UTF8STRING

AVP Flag M

Content-Flow-Description

Content-Flow-Description

Vendor ID 9

VSA Type 131141

AVP Type GROUPED

Supported group value(s):

[CONTENT_FLOW_FILTER]

[VRF_NAME]

[VLAN_ID]

AVP Flag M

Content-Flow-Filter

Content-Flow-Filter

Vendor ID 9

VSA Type 131142

AVP Type GROUPED

Supported group value(s):

[CLIENT_GROUP_ID]

[DESTINATION_IP_ADDRESS]

[DESTINATION_MASK]

[PROTOCOL_ID]

[START_OF_PORT_RANGE]

[END_OF_PORT_RANGE]

AVP Flag M

Content-Idle-Timer

Content-Idle-Timer

Vendor ID 9

VSA Type 131082

AVP Type UINT32

AVP Flag N/A

Content-Install

Content-Install

Vendor ID 9

VSA Type 131183

AVP Type GROUPED

Supported group value(s):

[CONTENT_DEFINITION]

AVP Flag M

Content-Length

This AVP contains the size of the message body.

Vendor ID 10415

VSA Type 827

AVP Type UINT32

AVP Flag M

Content-Name

Content-Name

Vendor ID 9

VSA Type 131151

AVP Type OCTETSTRING

AVP Flag M

Content-Pending-Timer

Content-Pending-Timer

Vendor ID 9

VSA Type 131134

AVP Type UINT32

AVP Flag N/A

Content-Policy-Map

Content-Policy-Map

Vendor ID 9

VSA Type 131077

AVP Type GROUPED

Supported group value(s):

[CONTENT_NAME]

[BILLING_POLICY_NAME]

[WEIGHT]

AVP Flag M

Content-Remove

Content-Remove

Vendor ID 9

VSA Type 131184

AVP Type GROUPED

Supported group value(s):

[CONTENT_NAME]

AVP Flag M

Content-Scope

Content-Scope

Vendor ID 9

VSA Type 131163

AVP Type ENUM

Supported enumerated value(s):

0 GLOBAL

1 USER

AVP Flag M

Content-Type

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

Vendor ID 10415

VSA Type 826

AVP Type UTF8STRING

AVP Flag M

Context-Identifier

Context-Identifier

Vendor ID 10415

VSA Type 1423

AVP Type UINT32

AVP Flag M

Control-URL

Control-URL

Vendor ID 9

VSA Type 131197

AVP Type GROUPED

Supported group value(s):

[INTERLEAVED]

AVP Flag M

Correlate-Reason

This AVP contains the reason the Correlate message was sent.

Vendor ID 4491

VSA Type 202

AVP Type ENUM

Supported enumerated value(s):

0 UNKNOWN

1 B2BUA

2 INITIAL_SIP_MESSAGE

3 ADDITIONAL_TARGET_ENCOUNTERED

4 HAND_OFF_OCCURED

5 ORIGINATION_FROM_APP_SERVER

6 BCID

AVP Flag M

Cost-Information

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

Vendor ID 0

VSA Type 423

AVP Type GROUPED

Supported group value(s):

[UNIT_VALUE]

[CURRENCY_CODE]

[COST_UNIT]

AVP Flag M

Cost-Unit

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

Vendor ID 0

VSA Type 424

AVP Type UTF8STRING

AVP Flag M

Credit-Control

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

Vendor ID 0

VSA Type 426

AVP Type ENUM

Supported enumerated value(s):

0 CREDIT_AUTHORIZATION

1 RE_AUTHORIZATION

AVP Flag M

Credit-Control-Failure-Handling

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

Vendor ID 0

VSA Type 427

AVP Type ENUM

Supported enumerated value(s):

0 TERMINATE

1 CONTINUE

2 RETRY_AND_TERMINATE

AVP Flag M

Cumulative-Acct-Input-Octets

This AVP represents the cumulative number of input octets. This attribute is included in the Service-Data-Container AVP and sent only in ACR-Interim and ACR-Stop messages to track the cumulative data usage per Rating Group (RG).

Vendor ID 9

VSA Type 132044

AVP Type UINT64

AVP Flag N/A

Cumulative-Acct-Output-Octets

This AVP represents the cumulative number of output octets. This attribute is included in the Service-Data-Container AVP and sent only in ACR-Interim and ACR-Stop messages to track the cumulative data usage per Rating Group (RG).

Vendor ID 9

VSA Type 132045

AVP Type UINT64

AVP Flag N/A

Currency-Code

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

Vendor ID 0

VSA Type 425

AVP Type UINT32

AVP Flag M

Current-Location

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

Vendor ID 0

VSA Type 707

AVP Type ENUM

Supported enumerated value(s): none

AVP Flag M

Current-Location-Retrieved

Current-Location-Retrieved

Vendor ID 10415

VSA Type 1610

AVP Type ENUM

Supported enumerated value(s):

0 ACTIVE-LOCATION-RETRIEVAL

AVP Flag M

Custom-Mute-Notification

Custom-Mute-Notification

Vendor ID 9

VSA Type 132056

AVP Type ENUM

Supported enumerated value(s):

0 MUTE_APPLICATION_START

1 UNMUTE_APPLICATION_START

AVP Flag N/A

Customer-Id

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

Vendor ID 8164

VSA Type 1146

AVP Type UTF8STRING

AVP Flag M

DEA-Flags

DEA-Flags

Vendor ID 10415

VSA Type 1521

AVP Type UINT32

AVP Flag M

DER-Flags

DER-Flags

Vendor ID 10415

VSA Type 1520

AVP Type UINT32

AVP Flag M

DIR

DIR

Vendor ID 0

VSA Type 11000

AVP Type OCTETSTRING

AVP Flag M

DL-Buffering-Suggested-Packet-Count

DL-Buffering-Suggested-Packet-Count

Vendor ID 10415

VSA Type 1674

AVP Type INT32

AVP Flag N/A

DRMP

DRMP

Vendor ID 0

VSA Type 301

AVP Type ENUM

Supported enumerated value(s):

0 PRIORITY_0

1 PRIORITY_1

2 PRIORITY_2

3 PRIORITY_3

4 PRIORITY_4

5 PRIORITY_5

6 PRIORITY_6

7 PRIORITY_7

8 PRIORITY_8

9 PRIORITY_9

10 PRIORITY_10

11 PRIORITY_11

12 PRIORITY_12

13 PRIORITY_13

14 PRIORITY_14

15 PRIORITY_15

AVP Flag N/A

DSA-Flags

This AVP contains a bit mask.

Vendor ID 10415

VSA Type 1422

AVP Type UINT32

AVP Flag M

DSCP

DSCP

Vendor ID 9

VSA Type 131178

AVP Type UINT32

AVP Flag N/A

DSR-Application-Invoked

DSR-Application-Invoked

Vendor ID 323

VSA Type 2468

AVP Type ENUM

Supported enumerated value(s):

3 RBAR

4 FABR

5 CPA

6 P-DRA

AVP Flag M

DSR-Flags

This AVP contains a bit mask.

Vendor ID 10415

VSA Type 1421

AVP Type UINT32

AVP Flag M

Data-Reference

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

Vendor ID 0

VSA Type 703

AVP Type ENUM

Supported enumerated value(s): none

AVP Flag M

Default-EPS-Bearer-QoS

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

Vendor ID 10415

VSA Type 1049

AVP Type GROUPED

Supported group value(s):

[QOS_CLASS_IDENTIFIER]

[ALLOCATION_RETENTION_PRIORITY]

AVP Flag M

Delegated-IP-Install

Delegated-IP-Install

Vendor ID 9

VSA Type 131259

AVP Type GROUPED

Supported group value(s):

[DELEGATED_IPV4_DEFINITION]

[DELEGATED_IPV6_DEFINITION]

AVP Flag M

Delegated-IPv4-Definition

Delegated-IPv4-Definition

Vendor ID 9

VSA Type 131260

AVP Type GROUPED

Supported group value(s):

[FRAMED_IP_ADDRESS]

[FRAMED_IP_NETMASK]

[AGGR_PREFIX_LEN]

AVP Flag M

Delegated-IPv6-Definition

Delegated-IPv6-Definition

Vendor ID 9

VSA Type 131261

AVP Type GROUPED

Supported group value(s):

[DELEGATED_IPV6_PREFIX]

[AGGR_PREFIX_LEN]

AVP Flag M

Delegated-IPv6-Prefix

Delegated-IPv6-Prefix

Vendor ID 0

VSA Type 123

AVP Type OCTETSTRING

AVP Flag M

Deregistration-Reason

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

Vendor ID 10415

VSA Type 615

AVP Type GROUPED

Supported group value(s):

[REASON_CODE]

[REASON_INFO]

AVP Flag M

Destination-Host

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

Vendor ID 0

VSA Type 293

AVP Type DIAMIDENT

AVP Flag M

Destination-IP-Address

Destination-IP-Address

Vendor ID 9

VSA Type 131146

AVP Type ADDRESS

AVP Flag M

Destination-Mask

Destination-Mask

Vendor ID 9

VSA Type 131147

AVP Type ADDRESS

AVP Flag M

Destination-PGW

Destination-PGW

Vendor ID 9

VSA Type 2300

AVP Type UTF8STRING

AVP Flag N/A

Destination-Realm

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

Vendor ID 0

VSA Type 283

AVP Type DIAMIDENT

AVP Flag M

Destination-SIP-URI

Destination-SIP-URI

Vendor ID 10415

VSA Type 3327

AVP Type UTF8STRING

AVP Flag N/A

Diagnostics

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

Vendor ID 10415

VSA Type 2039

AVP Type ENUM

Supported enumerated value(s):

0 UNSPECIFIED

1 SESSION_TIMEOUT

2 RESOURCE_LIMITATION

3 ADMIN_DISCONNECT

4 IDLE_TIMEOUT

5 PCRF_UNREACHABLE

6 AAA_UNREACHABLE

7 AAA_INITIATED_SESSION_TERMINATION

8 REAUTHENTICATION_FAILED

9 PCRF_INITIATED_SESSION_TERMINATION

10 PCRF_INITIATED_FLOW_TERMINATION

11 PCRF_ACCOUNTING_PARAMETERS_CHANGED

12 PMIP_INITIATED_SESSION_TERMINATION

13 PPP_INITIATED_SESSION_TERMINATION

14 GTP_INITIATED_SESSION_TERMINATION

15 PMIP_REVOCATION

16 HANDOVER_ERROR

17 PMIP_LIFETIME_EXPIRED

AVP Flag M

Dialog-Id

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

Vendor ID 4491

VSA Type 203

AVP Type UTF8STRING

AVP Flag M

Digest-Algorithm

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

Vendor ID 0

VSA Type 111

AVP Type OCTETSTRING

AVP Flag M

Digest-Auth-Param

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

Vendor ID 0

VSA Type 117

AVP Type OCTETSTRING

AVP Flag M

Digest-Domain

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

Vendor ID 0

VSA Type 119

AVP Type OCTETSTRING

AVP Flag M

Digest-HA1

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

Vendor ID 0

VSA Type 121

AVP Type OCTETSTRING

AVP Flag M

Digest-QoP

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

Vendor ID 0

VSA Type 110

AVP Type OCTETSTRING

AVP Flag M

Digest-Realm

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

Vendor ID 0

VSA Type 104

AVP Type OCTETSTRING

AVP Flag M

Direct-Debiting-Failure-Handling

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

Vendor ID 0

VSA Type 428

AVP Type ENUM

Supported enumerated value(s):

0 TERMINATE_OR_BUFFER

1 CONTINUE

AVP Flag M

Direct-Message

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

Vendor ID 4491

VSA Type 211

AVP Type ENUM

Supported enumerated value(s):

0 FALSE

1 TRUE

AVP Flag M

Direction

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

Vendor ID 4491

VSA Type 210

AVP Type ENUM

Supported enumerated value(s):

0 UNDEFINED

1 TO_TARGET

2 FROM_TARGET

AVP Flag M

Disable-Override-Control

This AVP is used to disable Override Control (OC) completely or per parameter basis.

Vendor ID 9

VSA Type 132053

AVP Type GROUPED

Supported group value(s):

[OVERRIDE_CONTROL_NAME]

[DISABLE_OVERRIDE_CONTROL_PARAMETER]

AVP Flag N/A

Disable-Override-Control-Parameter

This AVP specifies the Override Control parameter to be disabled. This AVP may be included more than once if multiple parameters need to be disabled.

Vendor ID 9

VSA Type 132057

AVP Type ENUM

Supported enumerated value(s):

0 OVERRIDE_SERVICE_IDENTIFIER

1 OVERRIDE_RATING_GROUP

2 OVERRIDE_ONLINE

3 OVERRIDE_OFFLINE

4 OVERRIDE_MAX_REQUESTED_BANDWIDTH_UL

5 OVERRIDE_MAX_REQUESTED_BANDWIDTH_DL

6 OVERRIDE_GUARANTEED_BITRATE_UL

7 OVERRIDE_GUARANTEED_BITRATE_DL

8 OVERRIDE_PRIORITY_LEVEL

9 OVERRIDE_PRE_EMPTION_CAPABILITY

10 OVERRIDE_PRE_EMPTION_VULNERABILITY

11 OVERRIDE_QOS_CLASS_IDENTIFIER

12 OVERRIDE_NEXTHOP_ADDRESS

13 OVERRIDE_VLAN_ID

14 OVERRIDE_TOS_VALUE_STANDARD_UL

15 OVERRIDE_TOS_VALUE_STANDARD_DL

16 OVERRIDE_TOS_VALUE_CUSTOM_UL

17 OVERRIDE_TOS_VALUE_CUSTOM_DL

AVP Flag N/A

Disconnect-Cause

This AVP contains the cause of disconnection with peer.

Vendor ID 0

VSA Type 273

AVP Type ENUM

Supported enumerated value(s):

0 REBOOTING

1 BUSY

2 DO_NOT_WANT_TO_TALK_TO_YOU

AVP Flag M

Domain-Group-Activation

Domain-Group-Activation

Vendor ID 9

VSA Type 131206

AVP Type ENUM

Supported enumerated value(s):

0 DISABLED

1 ENABLED

AVP Flag M

Domain-Group-Clear

Domain-Group-Clear

Vendor ID 9

VSA Type 131235

AVP Type ENUM

Supported enumerated value(s):

0 DISABLED

1 ENABLED

AVP Flag M

Domain-Group-Definition

Domain-Group-Definition

Vendor ID 9

VSA Type 131203

AVP Type GROUPED

Supported group value(s):

[DOMAIN_GROUP_NAME]

[PRIORITY]

[MATCH_STRING]

AVP Flag M

Domain-Group-Install

Domain-Group-Install

Vendor ID 9

VSA Type 131204

AVP Type GROUPED

Supported group value(s):

[DOMAIN_GROUP_DEFINITION]

AVP Flag M

Domain-Group-Name

Domain-Group-Name

Vendor ID 9

VSA Type 131202

AVP Type OCTETSTRING

AVP Flag M

Domain-Group-Remove

Domain-Group-Remove

Vendor ID 9

VSA Type 131205

AVP Type GROUPED

Supported group value(s):

[DOMAIN_GROUP_NAME]

AVP Flag M

Downlink-Rate-Limit

Downlink-Rate-Limit

Vendor ID 10415

VSA Type 4312

AVP Type UINT32

AVP Flag M

Dual-Billing-Basis

Dual-Billing-Basis

Vendor ID 9

VSA Type 131207

AVP Type ENUM

Supported enumerated value(s):

0 INVALID

1 EVENT

2 IP_BYTE

3 TCP_BYTE

4 DURATION

5 DURATION_CONNECT

6 DURATION_TRANSACTION

AVP Flag M

Dual-Passthrough-Quota

Dual-Passthrough-Quota

Vendor ID 9

VSA Type 131208

AVP Type UINT32

AVP Flag N/A

Dual-Reauthorization-Threshold

Dual-Reauthorization-Threshold

Vendor ID 9

VSA Type 131209

AVP Type UINT32

AVP Flag N/A

Duration

Duration

Vendor ID 9

VSA Type 131157

AVP Type UINT32

AVP Flag N/A

Dynamic-Address-Flag

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

Vendor ID 10415

VSA Type 2051

AVP Type ENUM

Supported enumerated value(s):

0 STATIC

1 DYNAMIC

AVP Flag M

EAP-Key-Name

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

Vendor ID 0

VSA Type 102

AVP Type OCTETSTRING

AVP Flag M

EAP-Master-Session-Key

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

Vendor ID 0

VSA Type 464

AVP Type OCTETSTRING

AVP Flag N/A

EAP-Payload

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

Vendor ID 0

VSA Type 462

AVP Type OCTETSTRING

AVP Flag M

EAP-Reissued-Payload

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

Vendor ID 0

VSA Type 463

AVP Type OCTETSTRING

AVP Flag M

ECGI

This attribute indicates the E-UTRAN Cell Global Identifier. It is coded according to 3GPP TS 29.274, clause 8.21.5.

Vendor ID 10415

VSA Type 2517

AVP Type OCTETSTRING

AVP Flag M

EPS-Location-Information

EPS-Location-Information

Vendor ID 10415

VSA Type 1496

AVP Type GROUPED

Supported group value(s):

[MME_LOCATION_INFORMATION]

[SGSN_LOCATION_INFORMATION]

AVP Flag M

EPS-Subscribed-QoS-Profile

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

Vendor ID 10415

VSA Type 1431

AVP Type GROUPED

Supported group value(s):

[QOS_CLASS_IDENTIFIER]

[ALLOCATION_RETENTION_PRIORITY]

AVP Flag M

EPS-User-State

EPS-User-State

Vendor ID 10415

VSA Type 1495

AVP Type GROUPED

Supported group value(s):

[MME_USER_STATE]

[SGSN_USER_STATE]

AVP Flag M

EPS-Vector

This AVP contains Authentication Information for EPS.

Vendor ID 10415

VSA Type 6017

AVP Type GROUPED

Supported group value(s):

[ITEM_NUMBER]

[RAND]

[XRES]

[AUTN]

[KASME]

AVP Flag M

ESN

ESN

Vendor ID 10415

VSA Type 6109

AVP Type OCTETSTRING

AVP Flag M

EUTRAN-Cell-Global-Identity

This AVP contains E-UTRAN cell global identity of the user.

Vendor ID 10415

VSA Type 1602

AVP Type OCTETSTRING

AVP Flag M

EUTRAN-Positioning-Data

This attribute contains the encoded content of the "Positioning-Data" Information Element as defined in 3GPP TS 29.171.

Vendor ID 10415

VSA Type 2516

AVP Type OCTETSTRING

AVP Flag M

EUTRAN-Vector

EUTRAN-Vector

Vendor ID 10415

VSA Type 1414

AVP Type GROUPED

Supported group value(s):

[ITEM_NUMBER]

[RAND]

[XRES]

[AUTN]

[KASME]

AVP Flag M

Early-Media-Description

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

Vendor ID 10415

VSA Type 1272

AVP Type GROUPED

Supported group value(s):

[SDP_TIMESTAMPS]

[SDP_MEDIA_COMPONENT]

[SDP_SESSION_DESCRIPTION]

AVP Flag M

Element-ID

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

Vendor ID 4491

VSA Type 212

AVP Type UTF8STRING

AVP Flag M

Element-Type

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

Vendor ID 4491

VSA Type 213

AVP Type ENUM

Supported enumerated value(s):

0 S_CSCF

1 P_CSCF

2 I_CSCF

3 MRFC

4 MGCF

5 BGCF

6 AS

7 UE

AVP Flag M

Emergency-Indication

Emergency-Indication

Vendor ID 10415

VSA Type 1538

AVP Type UINT32

AVP Flag N/A

End-of-Port-range

End-of-Port-range

Vendor ID 9

VSA Type 131150

AVP Type UINT32

AVP Flag N/A

Equipment-Status

This AVP contains the status of the mobile equipment.

Vendor ID 10415

VSA Type 1445

AVP Type ENUM

Supported enumerated value(s):

0 WHITELISTED

1 BLACKLISTED

2 GREYLISTED

AVP Flag M

Error-Diagnostic

Error-Diagnostic

Vendor ID 10415

VSA Type 1614

AVP Type ENUM

Supported enumerated value(s):

0 GPRS_DATA_SUBSCRIBED

1 NO_GPRS_DATA_SUBSCRIBED

AVP Flag M

Error-Message

Human Readable Error Message.

Vendor ID 0

VSA Type 281

AVP Type UTF8STRING

AVP Flag N/A

Error-Reporting-Host

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

Vendor ID 0

VSA Type 294

AVP Type DIAMIDENT

AVP Flag M

Event

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

Vendor ID 10415

VSA Type 825

AVP Type UTF8STRING

AVP Flag M

Event-Message-Type

This AVP contains the type of surveillance message.

Vendor ID 4491

VSA Type 214

AVP Type ENUM

Supported enumerated value(s):

0 REPORT

1 CORRELATE

2 CARRIER_INFO

AVP Flag M

Event-Report-Indication

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

Vendor ID 10415

VSA Type 1033

AVP Type GROUPED

Supported group value(s):

[EVENT_TRIGGER]

[RAT_TYPE]

[QOS_INFORMATION]

[RAI]

[3GPP_USER_LOCATION_INFO]

[TRACE_DATA]

[TRACE_REFERENCE]

[3GPP2_BSID]

[3GPP_MS_TIMEZONE]

[3GPP_SGSN_ADDRESS]

[3GPP_SGSN_IPV6_ADDRESS]

AVP Flag M

Event-Timestamp

This AVP contains the time the event was reported.

Vendor ID 0

VSA Type 55

AVP Type TIME

AVP Flag M

Event-Trigger

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

Vendor ID 10415

VSA Type 1006

AVP Type ENUM

Supported enumerated value(s):

0 SGSN_CHANGE

1 QOS_CHANGE

2 RAT_CHANGE

3 TFT_CHANGE

4 PLMN_CHANGE

5 LOSS_OF_FLOW

6 RECOVERY_OF_FLOW

7 IP_CAN_CHANGE

8 GW_PCEF_MALFUNCTION

9 RESOURCES_LIMITATION

10 MAX_NR_BEARERS_REACHED

11 QOS_CHANGE_EXCEEDING_AUTHORIZATION

12 RAI_CHANGE

13 USER_LOCATION_CHANGE

14 NO_EVENT_TRIGGERS

15 OUT_OF_CREDIT

16 REALLOCATION_OF_CREDIT

17 REVALIDATION_TIMEOUT

18 UE_IP_ADDRESS_ALLOCATE

19 UE_IP_ADDRESS_RELEASE

20 DEFAULT_EPS_BEARER_QOS_CHANGE

21 AN_GW_CHANGE

22 SUCCESSFUL_RESOURCE_ALLOCATION

23 RESOURCE_MODIFICATION_REQUEST

24 PGW_TRACE_CONTROL

25 UE_TIME_ZONE_CHANGE

26 TAI_CHANGE

27 ECGI_CHANGE

28 CHARGING_CORRELATION_EXCHANGE

29 APN_AMBR_MODIFICATION_FAILURE

33 USAGE_REPORT

34 DEFAULT_EPS_BEARER_QOS_MODIFICATION_FAILURE

39 APPLICATION_START

40 APPLICATION_STOP

44 SERVICE_FLOW_DETECTION

45 ACCESS_NETWORK_INFO_REPORT

2000 PRESERVATION_CHANGED

2001 REACTIVATION_CHANGED

1000 TFT_DELETED

1001 LOSS_OF_BEARER

1002 RECOVERY_OF_BEARER

1003 POLICY_ENFORCEMENT_FAILED

2003 TETHERING_FLOW_DETECTED

10001 SESSION_RECOVERY

10002 SESSION_SYNC

AVP Flag M

Event-Type

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

Vendor ID 10415

VSA Type 823

AVP Type GROUPED

Supported group value(s):

[SIP_METHOD]

[EVENT]

[EXPIRES]

AVP Flag M

Execution-Time

Execution-Time

Vendor ID 9

VSA Type 132025

AVP Type TIME

AVP Flag N/A

Experimental-Result

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

Vendor ID 0

VSA Type 297

AVP Type GROUPED

Supported group value(s):

[VENDOR_ID]

[EXPERIMENTAL_RESULT_CODE]

AVP Flag M

Experimental-Result-Code

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

Vendor ID 0

VSA Type 298

AVP Type ENUM

Supported enumerated value(s):

1001 DIAMETER_MULTI_ROUND_AUTH

2001 DIAMETER_SUCCESS

2002 DIAMETER_LIMITED_SUCCESS

2021 DIAMETER_PDP_CONTEXT_DELETION_INDICATION

2003 DIAMETER_UNREGISTERED_SERVICE

2004 DIAMETER_SUCCESS_NOT_SUPPORTED_USER_DATA

2005 DIAMETER_SUCCESS_SERVER_NAME_NOT_STORED

3001 DIAMETER_COMMAND_UNSUPPORTED

3002 DIAMETER_UNABLE_TO_DELIVER

3003 DIAMETER_REALM_NOT_SERVED

3004 DIAMETER_TOO_BUSY

3005 DIAMETER_LOOP_DETECTED

3006 DIAMETER_REDIRECT_INDICATION

3007 DIAMETER_APPLICATION_UNSUPPORTED

3008 DIAMETER_INVALID_HDR_BITS

3009 DIAMETER_INVALID_AVP_BITS

3010 DIAMETER_UNKNOWN_PEER

4001 DIAMETER_AUTHENTICATION_REJECTED

4002 DIAMETER_OUT_OF_SPACE

4003 ELECTION_LOST

4010 DIAMETER_END_USER_SERVICE_DENIED

4011 DIAMETER_CREDIT_CONTROL_NOT_APPLICABLE

4012 DIAMETER_CREDIT_LIMIT_REACHED

4041 INSUFFICIENT-RESOURCES

4043 COMMIT-FAILURE

4044 REFRESH-FAILURE

4045 QOS-PROFILE-FAILURE

4046 ACCESS-PROFILE-FAILURE

4047 PRIORITY-NOT-GRANTED

4100 DIAMETER_USER_DATA_NOT_AVAILABLE

4101 DIAMETER_PRIOR_UPDATE_IN_PROGRESS

4121 DIAMETER_ERROR_OUT_OF_RESOURCES

4141 DIAMETER_PCC_BEARER_EVENT

4142 DIAMETER_BEARER_EVENT

4143 DIAMETER_AN_GW_FAILED

4144 DIAMETER_PENDING_TRANSACTION

4181 AUTHENTICATION_DATA_UNAVAILABLE

4196 DIAMETER_REQUESTED_SESSION_NOT_FOUND

4197 DIAMETER_SESSION_RECOVERY_REQUESTED

4199 DIAMETER_PCRF_TOO_BUSY

5001 DIAMETER_AVP_UNSUPPORTED

5002 DIAMETER_UNKNOWN_SESSION_ID

5003 DIAMETER_AUTHORIZATION_REJECTED

5004 DIAMETER_INVALID_AVP_VALUE

5005 DIAMETER_MISSING_AVP

5006 DIAMETER_RESOURCES_EXCEEDED

5007 DIAMETER_CONTRADICTING_AVPS

5008 DIAMETER_AVP_NOT_ALLOWED

5009 DIAMETER_AVP_OCCURS_TOO_MANY_TIMES

5010 DIAMETER_NO_COMMON_APPLICATION

5011 DIAMETER_UNSUPPORTED_VERSION

5012 DIAMETER_UNABLE_TO_COMPLY

5013 DIAMETER_INVALID_BIT_IN_HEADER

5014 DIAMETER_INVALID_AVP_LENGTH

5015 DIAMETER_INVALID_MESSAGE_LENGTH

5016 DIAMETER_INVALID_AVP_BIT_COMBO

5017 DIAMETER_NO_COMMON_SECURITY

5021 BINDING-FAILURE

5030 DIAMETER_USER_UNKNOWN

5031 DIAMETER_RATING_FAILED

5041 MODIFICATION-FAILURE

5061 INVALID_SERVICE_INFORMATION

5062 FILTER_RESTRICTIONS

5063 REQUESTED_SERVICE_NOT_AUTHORIZED

5064 DUPLICATED_AF_SESSION

5065 IP_CAN_SESSION_NOT_AVAILABLE

5066 UNAUTHORIZED_NON_EMERGENCY_SESSION

5067 UNAUTHORIZED_SPONSORED_DATA_CONNECTIVITY

5100 DIAMETER_ERROR_USER_DATA_NOT_RECOGNIZED

5101 DIAMETER_ERROR_OPERATION_NOT_ALLOWED

5102 DIAMETER_ERROR_USER_DATA_CANNOT_BE_READ

5103 DIAMETER_ERROR_USER_DATA_CANNOT_BE_MODIFIED

5104 DIAMETER_ERROR_USER_DATA_CANNOT_BE_NOTIFIED

5106 DIAMETER_ERROR_SUBS_DATA_ABSENT

5107 DIAMETER_ERROR_NO_SUBSCRIPTION_TO_DATA

5108 DIAMETER_ERROR_DSAI_NOT_AVAILABLE

5120 DIAMETER_ERROR_START_INDICATION

5121 DIAMETER_ERROR_STOP_INDICATION

5122 DIAMETER_ERROR_UNKNOWN_MBMS_BEARER_SERVICE

5123 DIAMETER_ERROR_SERVICE_AREA

5140 DIAMETER_ERROR_INITIAL_PARAMETERS

5141 DIAMETER_ERROR_TRIGGER_EVENT

5142 DIAMETER_PCC_RULE_EVENT

5143 DIAMETER_ERROR_BEARER_NOT_AUTHORIZED

5144 DIAMETER_ERROR_TRAFFIC_MAPPING_INFO_REJECTED

5145 DIAMETER_QOS_RULE_EVENT

5147 DIAMETER_ERROR_CONFLICTING_REQUEST

5199 DIAMETER_NEWER_SESSION_DETECTED

5420 ERROR_UNKNOWN_EPS_SUBSCRIPTION

5421 ERROR_RAT_NOT_ALLOWED

5402 ERROR_ROAMING_NOT_ALLOWED

5422 ERROR_EQUIPMENT_UNKNOWN

5198 DIAMETER_OVERLOAD_RETRY_NOT_ALLOWED_TO_ANY

5999 DIAMETER_GX_APN_CHANGE

5510 DIAMETER_ERROR_UNAUTHORIZED_REQUESTING_ENTITY

5511 DIAMETER_ERROR_UNAUTHORIZED_SERVICE

5513 DIAMETER_ERROR_CONFIGURATION_EVENT_STORAGE_NOT_SUCCESSFUL

5514 DIAMETER_ERROR_CONFIGURATION_EVENT_NON_EXISTANT

5650 DIAMETER_ERROR_REQUESTED_LOCATION_NOT_SERVED

5651 DIAMETER_ERROR_INVALID_EPS_BEARER

5998 DIAMETER_ERROR_NIDD_CONFIGURATION_NOT_AVAILABLE

5997 DIAMETER_ERROR_SCEF_REFERENCE_ID_UNKNOWN

5653 DIAMETER_ERROR_USER_TEMPORARILY_UNREACHABLE

4221 DIAMETER_ERROR_UNREACHABLE_USER

AVP Flag M

Expiration-Date

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

Vendor ID 10415

VSA Type 1439

AVP Type TIME

AVP Flag M

Expires

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

Vendor ID 10415

VSA Type 888

AVP Type UINT32

AVP Flag M

Exponent

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

Vendor ID 0

VSA Type 429

AVP Type INT32

AVP Flag M

Extended-APN-AMBR-DL

Extended-APN-AMBR-DL

Vendor ID 10415

VSA Type 2848

AVP Type UINT32

AVP Flag M

Extended-APN-AMBR-UL

Extended-APN-AMBR-UL

Vendor ID 10415

VSA Type 2849

AVP Type UINT32

AVP Flag M

Extended-Max-Requested-BW-DL

Extended-Max-Requested-BW-DL

Vendor ID 10415

VSA Type 554

AVP Type UINT32

AVP Flag M

Extended-Max-Requested-BW-UL

Extended-Max-Requested-BW-DL

Vendor ID 10415

VSA Type 555

AVP Type UINT32

AVP Flag M

Extended-GBR-DL

Extended-GBR-DL

Vendor ID 10415

VSA Type 2850

AVP Type UINT32

AVP Flag M

Extended-GBR-UL

Extended-GBR-UL

Vendor ID 10415

VSA Type 2851

AVP Type UINT32

AVP Flag M

Ext-PDP-Address

Ext-PDP-Address

Vendor ID 10415

VSA Type 1621

AVP Type ADDRESS

AVP Flag M

Ext-PDP-Type

Ext-PDP-Type

Vendor ID 10415

VSA Type 1620

AVP Type OCTETSTRING

AVP Flag M

Extended-PCO

Extended-PCO

Vendor ID 10415

VSA Type 4313

AVP Type OCTETSTRING

AVP Flag M

Extended-QoS-Filter-Rule

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

Vendor ID 0

VSA Type 6066

AVP Type UINT32

AVP Flag M

External-Client

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

Vendor ID 10415

VSA Type 1479

AVP Type GROUPED

Supported group value(s):

[CLIENT_IDENTITY]

[GMLC_RESTRICTION]

[NOTIFICATION_TO_UE_USER]

AVP Flag M

External-Identifier

External-Identifier

Vendor ID 10415

VSA Type 3111

AVP Type UTF8STRING

AVP Flag M

FID

This AVP contains the Flow Correlation ID.

Vendor ID 10415

VSA Type 7003

AVP Type OCTETSTRING

AVP Flag M

Failed-AVP

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

Vendor ID 0

VSA Type 279

AVP Type GROUPED

Supported group value(s): none

AVP Flag M

Failed-Preload-Obj-Name

Failed-Preload-Obj-Name

Vendor ID 9

VSA Type 131191

AVP Type ENUM

Supported group value(s):

[POLICY_PRELOAD_ERROR_CODE]

[POLICY_MAP_NAME]

[BILLING_POLICY_NAME]

[CONTENT_NAME]

[SERVICE_NAME]

[BILLING_PLAN_NAME]

AVP Flag M

Failed-Preload-Object

Failed-Preload-Object

Vendor ID 9

VSA Type 131152

AVP Type GROUPED

Supported group value(s):

[POLICY_PRELOAD_OBJECT_TYPE]

[FAILED_PRELOAD_OBJ_NAME]

AVP Flag M

Feature-List

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

Vendor ID 10415

VSA Type 630

AVP Type UINT32

AVP Flag M

Feature-List-ID

This AVP contains the identity of the featured list.

Vendor ID 10415

VSA Type 629

AVP Type UINT32

AVP Flag M

Feature-List-ID-Resp

This AVP contains the identity of the featured list.

Vendor ID 10415

VSA Type 629

AVP Type UINT32

AVP Flag N/A

Feature-List-Resp

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

Vendor ID 10415

VSA Type 630

AVP Type UINT32

AVP Flag N/A

Filter-Id

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

Vendor ID 0

VSA Type 11

AVP Type UTF8STRING

AVP Flag M

Filter-Rule

Filter-Rule

Vendor ID 0

VSA Type 509

AVP Type UINT32

AVP Flag M

Final-Unit-Action

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

Vendor ID 0

VSA Type 449

AVP Type ENUM

Supported enumerated value(s):

0 TERMINATE

1 REDIRECT

2 RESTRICT_ACCESS

AVP Flag M

Final-Unit-Indication

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

Vendor ID 0

VSA Type 430

AVP Type GROUPED

Supported group value(s):

[FINAL_UNIT_ACTION]

[RESTRICTION_FILTER_RULE]

[FILTER_ID]

[REDIRECT_SERVER]

AVP Flag M

Firmware-Revision

Support for Vendor Specific Applications.

Vendor ID 0

VSA Type 267

AVP Type UINT32

AVP Flag N/A

First-Packet-Timestamp

First-Packet-Timestamp

Vendor ID 9

VSA Type 131158

AVP Type UINT32

AVP Flag N/A

Flow-Description

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

Vendor ID 10415

VSA Type 507

AVP Type IPFILTERRULE

AVP Flag M

Flow-Description-Info

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

Vendor ID 5535

VSA Type 1022

AVP Type GROUPED

Supported group value(s):

[FLOW_DESCRIPTION]

[PRECEDENCE]

AVP Flag M

Flow-Direction

This AVP indicates the direction/directions that a filter is applicable, downlink only, uplink only or both down- and uplink (bidirectional).

Vendor ID 10415

VSA Type 1080

AVP Type ENUM

Supported enumerated value(s):

0 UNSPECIFIED

1 DOWNLINK

2 UPLINK

3 BIDIRECTIONAL

AVP Flag M

Flow-Grouping

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

Vendor ID 10415

VSA Type 508

AVP Type GROUPED

Supported group value(s):

[FLOWS]

AVP Flag M

Flow-Identifier

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

Vendor ID 5535

VSA Type 1008

AVP Type OCTETSTRING

AVP Flag M

Flow-Info

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

Vendor ID 5535

VSA Type 1007

AVP Type GROUPED

Supported group value(s):

[FLOW_IDENTIFIER]

[FLOW_DESCRIPTION_INFO]

[REQUESTED_QOS]

[GRANTED_QOS]

[FLOW_STATUS]

AVP Flag M

Flow-Information

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

Vendor ID 10415

VSA Type 1058

AVP Type GROUPED

Supported group value(s):

[FLOW_DESCRIPTION]

[PACKET_FILTER_IDENTIFIER]

[TOS_TRAFFIC_CLASS]

[SECURITY_PARAMETER_INDEX]

[FLOW_LABEL]

[FLOW_DIRECTION]

AVP Flag M

Flow-Label

This AVP contains the IPv6 flow label header field.

Vendor ID 10415

VSA Type 1057

AVP Type OCTETSTRING

AVP Flag M

Flow-Number

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

Vendor ID 10415

VSA Type 509

AVP Type UINT32

AVP Flag M

Flow-Operation

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

Vendor ID 5535

VSA Type 1006

AVP Type ENUM

Supported enumerated value(s):

0 TERMINATION

1 ESTABLISHMENT

2 MODIFICATION

AVP Flag M

Flow-Status

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

Vendor ID 10415

VSA Type 511

AVP Type ENUM

Supported enumerated value(s):

0 ENABLED-UPLINK

1 ENABLED-DOWNLINK

2 ENABLED

3 DISABLED

4 REMOVED

5 TERMINATE

AVP Flag M

Flow-Status-Policy-Mismatch

Flow-Status-Policy-Mismatch

Vendor ID 9

VSA Type 131164

AVP Type ENUM

Supported enumerated value(s):

0 FORWARD

1 BLOCK

AVP Flag M

Flow-Usage

This AVP contains information about the usage of IP Flows.

Vendor ID 10415

VSA Type 512

AVP Type ENUM

Supported enumerated value(s):

0 NO_INFORMATION

1 RTCP

2 AF_SIGNALLING

AVP Flag M

Flows

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

Vendor ID 10415

VSA Type 510

AVP Type GROUPED

Supported group value(s):

[MEDIA_COMPONENT_NUMBER]

[FLOW_NUMBER]

AVP Flag M

Framed-Appletalk-Link

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

Vendor ID 0

VSA Type 37

AVP Type UINT32

AVP Flag M

Framed-Appletalk-Network

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

Vendor ID 0

VSA Type 38

AVP Type UINT32

AVP Flag M

Framed-Appletalk-Zone

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

Vendor ID 0

VSA Type 39

AVP Type OCTETSTRING

AVP Flag M

Framed-Compression

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

Vendor ID 0

VSA Type 13

AVP Type ENUM

Supported enumerated value(s):

0 None

1 VJ_TCP-IP_header_compression

2 IPX-header-compression

3 Stac-LZS-compression

AVP Flag M

Framed-IP-Address

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

Vendor ID 0

VSA Type 8

AVP Type OCTETSTRING

AVP Flag M

Framed-IP-Netmask

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

Vendor ID 0

VSA Type 9

AVP Type OCTETSTRING

AVP Flag M

Framed-IPX-Network

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

Vendor ID 0

VSA Type 23

AVP Type UINT32

AVP Flag M

Framed-IPv6-Pool

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

Vendor ID 0

VSA Type 100

AVP Type OCTETSTRING

AVP Flag M

Framed-IPv6-Prefix

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

Vendor ID 0

VSA Type 97

AVP Type OCTETSTRING

AVP Flag M

Framed-IPv6-Route

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

Vendor ID 0

VSA Type 99

AVP Type UTF8STRING

AVP Flag N/A

Framed-Interface-Id

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

Vendor ID 0

VSA Type 96

AVP Type UINT64

AVP Flag M

Framed-MTU

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

Vendor ID 0

VSA Type 12

AVP Type UINT32

AVP Flag M

Framed-Pool

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

Vendor ID 0

VSA Type 88

AVP Type OCTETSTRING

AVP Flag M

Framed-Protocol

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

Vendor ID 0

VSA Type 7

AVP Type ENUM

Supported enumerated value(s):

1 PPP

2 SLIP

3 AppleTalk-Remote-Access-Protocol_ARAP

4 Gandalf-proprietary-SingleLink_MultiLink-protocol

5 Xylogics-proprietary_IPX-SLIP

6 X75-Synchronous

AVP Flag M

Framed-Route

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

Vendor ID 0

VSA Type 22

AVP Type UTF8STRING

AVP Flag M

Framed-Routing

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

Vendor ID 0

VSA Type 10

AVP Type ENUM

Supported enumerated value(s):

0 None

1 Send-routing-packets

2 Listen-for-routing-packets

3 Send-and-Listen

AVP Flag M

From-SIP-Header

This AVP contains the information in the "From" header

Vendor ID 10415

VSA Type 644

AVP Type OCTETSTRING

AVP Flag N/A

G-S-U-Pool-Identifier

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

Vendor ID 0

VSA Type 453

AVP Type UINT32

AVP Flag M

G-S-U-Pool-Reference

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

Vendor ID 0

VSA Type 457

AVP Type GROUPED

Supported group value(s):

[G_S_U_POOL_IDENTIFIER]

[CC_UNIT_TYPE]

[UNIT_VALUE]

AVP Flag M

GERAN-Vector

This AVP contains Authentication Information for GERAN.

Vendor ID 10415

VSA Type 6019

AVP Type GROUPED

Supported group value(s):

[ITEM_NUMBER]

[RAND]

[SRES]

[KC_KEY]

AVP Flag M

GGSN-Address

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

Vendor ID 10415

VSA Type 847

AVP Type ADDRESS

AVP Flag M

GMLC-Address

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

Vendor ID 10415

VSA Type 1474

AVP Type OCTETSTRING

AVP Flag M

GMLC-Number

This AVP contains the ISDN number of the GMLC.

Vendor ID 10415

VSA Type 1474

AVP Type OCTETSTRING

AVP Flag M

GMLC-Restriction

This attritbue contains GMLC Restriction List.

Vendor ID 10415

VSA Type 1481

AVP Type ENUM

Supported enumerated value(s):

0 GMLC_LIST

1 HOME_COUNTRY

AVP Flag M

GMM-Cause

GMM-Cause

Vendor ID 10415

VSA Type 4304

AVP Type UINT32

AVP Flag M

GPRS-Subscription-Data

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

Vendor ID 10415

VSA Type 1467

AVP Type GROUPED

Supported group value(s):

[COMPLETE_DATA_LIST_INCLUDED_INDICATOR]

[PDP_CONTEXT]

AVP Flag M

Geodetic-Information

This AVP provides geodetic location information of the user.

Vendor ID 10415

VSA Type 1609

AVP Type OCTETSTRING

AVP Flag M

Geographical-Information

This AVP contains geographical location information of the user.

Vendor ID 10415

VSA Type 1608

AVP Type OCTETSTRING

AVP Flag M

Geospatial-Location

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

Vendor ID 13019

VSA Type 356

AVP Type OCTETSTRING

AVP Flag M

Globally-Unique-Address

This AVP contains the UE's address.

Vendor ID 13019

VSA Type 300

AVP Type GROUPED

Supported group value(s):

[FRAMED_IP_ADDRESS]

[ADDRESS_REALM]

AVP Flag M

Granted-QoS

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

Vendor ID 5535

VSA Type 1011

AVP Type GROUPED

Supported group value(s):

[QOS_CLASS]

[MIN_BANDWIDTH_UL]

[MIN_BANDWIDTH_DL]

AVP Flag M

Granted-Service-Unit

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

Vendor ID 0

VSA Type 431

AVP Type GROUPED

Supported group value(s):

[TARIFF_TIME_CHANGE]

[TARIFF_CHANGE_USAGE]

[CC_TIME]

[CC_MONEY]

[CC_TOTAL_OCTETS]

[CC_INPUT_OCTETS]

[CC_OUTPUT_OCTETS]

[CC_SERVICE_SPECIFIC_UNITS]

AVP Flag M

Guaranteed-Bitrate-DL

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

Vendor ID 10415

VSA Type 1025

AVP Type UINT32

AVP Flag M

Guaranteed-Bitrate-UL

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

Vendor ID 10415

VSA Type 1026

AVP Type UINT32

AVP Flag M

Hash-Value

Hash-Value

Vendor ID 9

VSA Type 132080

AVP Type OCTETSTRING

AVP Flag N/A

HPLMN-ODB

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

Vendor ID 10415

VSA Type 1418

AVP Type UINT32

AVP Flag M

Header-Class

Header-Class

Vendor ID 9

VSA Type 131223

AVP Type ENUM

Supported group value(s):

[HEADER_CLASS_NAME]

[HEADER_CLASS_MODE]

AVP Flag M

Header-Class-Mode

Header-Class-Mode

Vendor ID 9

VSA Type 131222

AVP Type ENUM

Supported enumerated value(s):

0 EXCLUDE

1 INCLUDE

AVP Flag M

Header-Class-Name

Header-Class-Name

Vendor ID 9

VSA Type 131221

AVP Type UTF8STRING

AVP Flag M

Header-Field-Name

Header-Field-Name

Vendor ID 9

VSA Type 131220

AVP Type UTF8STRING

AVP Flag M

Header-Group-Definition

Header-Group-Definition

Vendor ID 9

VSA Type 131216

AVP Type GROUPED

Supported group value(s):

[HEADER_GROUP_NAME]

[HEADER_INSERT_NAME]

AVP Flag M

Header-Group-Install

Header-Group-Install

Vendor ID 9

VSA Type 131217

AVP Type GROUPED

Supported group value(s):

[HEADER_GROUP_DEFINITION]

AVP Flag M

Header-Group-Name

Header-Group-Name

Vendor ID 9

VSA Type 131215

AVP Type UTF8STRING

AVP Flag M

Header-Group-Remove

Header-Group-Remove

Vendor ID 9

VSA Type 131218

AVP Type GROUPED

Supported group value(s):

[HEADER_GROUP_NAME]

AVP Flag M

Header-Insert-Definition

Header-Insert-Definition

Vendor ID 9

VSA Type 131231

AVP Type GROUPED

Supported group value(s):

[HEADER_INSERT_NAME]

[HEADER_FIELD_NAME]

[HEADER_CLASS]

[HEADER_ITEM_CONTAINER]

AVP Flag M

Header-Insert-Install

Header-Insert-Install

Vendor ID 9

VSA Type 131232

AVP Type GROUPED

Supported group value(s):

[HEADER_INSERT_DEFINITION]

AVP Flag M

Header-Insert-Name

Header-Insert-Name

Vendor ID 9

VSA Type 131219

AVP Type UTF8STRING

AVP Flag M

Header-Insert-Remove

Header-Insert-Remove

Vendor ID 9

VSA Type 131233

AVP Type GROUPED

Supported group value(s):

[HEADER_INSERT_NAME]

AVP Flag M

Header-Item

Header-Item

Vendor ID 9

VSA Type 131228

AVP Type ENUM

Supported enumerated value(s):

0 TIMESTAMP

1 QUOTA_SERVER

AVP Flag M

Header-Item-Container

Header-Item-Container

Vendor ID 9

VSA Type 131230

AVP Type GROUPED

Supported group value(s):

[HEADER_ITEM_ENCRYPTION]

[HEADER_ITEM]

[HEADER_ITEM_STRING]

[HEADER_ITEM_RADIUS]

AVP Flag M

Header-Item-Encryption

Header-Item-Encryption

Vendor ID 9

VSA Type 131242

AVP Type ENUM

Supported enumerated value(s):

0 UNENCRYPTED

1 ENCRYPTED

AVP Flag M

Header-Item-Radius

Header-Item-Radius

Vendor ID 9

VSA Type 131227

AVP Type GROUPED

Supported group value(s):

[RADIUS_ATTRIBUTE_TYPE]

[RADIUS_VSA_VENDOR_ID]

[RADIUS_VSA_SUBATTRIBUTE_TYPE]

AVP Flag M

Header-Item-String

Header-Item-String

Vendor ID 9

VSA Type 131229

AVP Type UTF8STRING

AVP Flag M

Home-Agent

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

Vendor ID 5535

VSA Type 3

AVP Type ADDRESS

AVP Flag M

Homogeneous-Support-of-IMS-Voice-Over-PS-Sessions

Homogeneous-Support-of-IMS-Voice-Over-PS-Sessions

Vendor ID 10415

VSA Type 1493

AVP Type ENUM

Supported enumerated value(s):

0 NOT_SUPPORTED

1 SUPPORTED

AVP Flag M

Horizontal-Accuracy

This AVP is of type Unsigned32. Bits 6-0 correspond to Uncertainty Code defined in 3GPP TS 23.032. The horizontal location error should be less than the error indicated by the uncertainty code with 67% confidence. Bits 7 to 31 can be ignored.

Vendor ID 10415

VSA Type 2505

AVP Type UINT32

AVP Flag M

Host-IP-Address

This AVP contains IP address of the mobile station.

Vendor ID 0

VSA Type 257

AVP Type ADDRESS

AVP Flag M

HSS-ID

HSS-ID

Vendor ID 10415

VSA Type 3325

AVP Type OCTETSTRING

AVP Flag N/A

ICS-Indicator

ICS-Indicator

Vendor ID 10415

VSA Type 1491

AVP Type ENUM

Supported enumerated value(s):

0 FALSE

1 TRUE

AVP Flag M

IDA-Flags

The IDA-Flags AVP contains a bit mask.

Vendor ID 10415

VSA Type 1441

AVP Type UINT32

AVP Flag M

IDR-Flags

This AVP contains a bit mask.

Vendor ID 10415

VSA Type 1490

AVP Type UINT32

AVP Flag M

IMEI

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

Vendor ID 10415

VSA Type 6003

AVP Type UTF8STRING

AVP Flag M

IMS-Charging-Identifier

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

Vendor ID 10415

VSA Type 841

AVP Type UTF8STRING

AVP Flag M

IMS-Communication-Service-Identifier

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

Vendor ID 10415

VSA Type 1281

AVP Type UTF8STRING

AVP Flag M

IMS-Information

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

Vendor ID 10415

VSA Type 876

AVP Type GROUPED

Supported group value(s):

[EVENT_TYPE]

[ROLE_OF_NODE]

[NODE_FUNCTIONALITY]

[USER_SESSION_ID]

[CALLING_PARTY_ADDRESS]

[CALLED_PARTY_ADDRESS]

[CALLED_ASSERTED_IDENTITY]

[ASSOCIATED_URI]

[TIME_STAMPS]

[APPLICATION_SERVER_INFORMATION]

[INTER_OPERATOR_IDENTIFIER]

[IMS_CHARGING_IDENTIFIER]

[IMS_COMMUNICATION_SERVICE_IDENTIFIER]

[ONLINE_CHARGING_FLAG]

[SDP_SESSION_DESCRIPTION]

[SDP_MEDIA_COMPONENT]

[MESSAGE_BODY]

[CAUSE_CODE]

[ACCESS_NETWORK_INFORMATION]

[EARLY_MEDIA_DESCRIPTION]

[REAL_TIME_TARIFF_INFORMATION]

AVP Flag M

IMS-Voice-Over-PS-Sessions-Supported

IMS-Voice-Over-PS-Sessions-Supported

Vendor ID 10415

VSA Type 1492

AVP Type ENUM

Supported enumerated value(s):

0 NOT_SUPPORTED

1 SUPPORTED

AVP Flag M

IMSI-Unauthenticated-Flag

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

Vendor ID 10415

VSA Type 2308

AVP Type ENUM

Supported enumerated value(s):

0 AUTHENTICATED

1 UNAUTHENTICATED

AVP Flag M

IP-CAN-Type

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

Vendor ID 10415

VSA Type 1027

AVP Type ENUM

Supported enumerated value(s):

0 3GPP-GPRS

1 DOCSIS

2 xDSL

3 WiMAX

4 3GPP2

5 3GPP-EPS

6 NON-3GPP-EPS

AVP Flag M

IP-MMS

IP mobility selector.

Vendor ID 10415

VSA Type 6076

AVP Type UINT32

AVP Flag M

IP-Realm-Default-Indication

IP-Realm-Default-Indication

Vendor ID 10415

VSA Type 2603

AVP Type ENUM

Supported enumerated value(s): none

AVP Flag M

IP-SM-GW-SM-Delivery-Outcome

IP-SM-GW-SM-Delivery-Outcome

Vendor ID 10415

VSA Type 3320

AVP Type GROUPED

Supported group value(s):

[SM_DELIVERY_CAUSE]

[ABSENT_USER_DIAGNOSTIC_SM]

AVP Flag M

IP-Version-Authorized

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

Vendor ID 5535

VSA Type 11

AVP Type ENUM

Supported enumerated value(s):

0 IPv4_or_IPv6

1 IPv4_ONLY

2 IPv6_ONLY

AVP Flag M

Identity-Set

This AVP contains the requested set of IMS Public identities.

Vendor ID 0

VSA Type 708

AVP Type ENUM

Supported enumerated value(s): none

AVP Flag N/A

Identity-with-Emergency-Registration

Identity-with-Emergency-Registration

Vendor ID 10415

VSA Type 651

AVP Type GROUPED

Supported group value(s):

[USER_NAME]

[PUBLIC_IDENTITY]

[RESTORATION_INFO]

AVP Flag N/A

Idle-Timeout

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

Vendor ID 0

VSA Type 28

AVP Type UINT32

AVP Flag M

Immediate-Response-Preferred

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

Vendor ID 10415

VSA Type 6015

AVP Type UINT32

AVP Flag M

Inband-Security-Id

Advertise support of the Security portion of the application.

Vendor ID 0

VSA Type 299

AVP Type ENUM

Supported enumerated value(s):

0 NO_INBAND_SECURITY

1 TLS

AVP Flag M

Incoming-Trunk-Group-ID

This AVP contains the incoming PSTN leg.

Vendor ID 0

VSA Type 852

AVP Type UTF8STRING

AVP Flag M

Initial-IMS-Charging-Identifier

Initial-IMS-Charging-Identifier

Vendor ID 10415

VSA Type 2321

AVP Type UTF8STRING

AVP Flag M

Initial-Timeout

Initial-Timeout

Vendor ID 9

VSA Type 131107

AVP Type UINT32

AVP Flag N/A

Integrity-Key

This AVP contains the Integrity Key (IK).

Vendor ID 10415

VSA Type 626

AVP Type OCTETSTRING

AVP Flag M

Inter-Operator-Identifier

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

Vendor ID 10415

VSA Type 838

AVP Type GROUPED

Supported group value(s):

[ORIGINATING_IOI]

[TERMINATING_IOI]

AVP Flag M

Interleaved

Interleaved

Vendor ID 9

VSA Type 131196

AVP Type ENUM

Supported enumerated value(s):

0 DISABLED

1 ENABLED

AVP Flag M

Intermediate-CDR-Threshold

Intermediate-CDR-Threshold

Vendor ID 9

VSA Type 131130

AVP Type GROUPED

Supported group value(s):

[CDR_VOLUME_THRESHOLD]

[CDR_TIME_THRESHOLD]

AVP Flag M

Item-Number

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

Vendor ID 10415

VSA Type 1419

AVP Type UINT32

AVP Flag M

KASME

This AVP contains the KASME (EAP Authentication Vector).

Vendor ID 10415

VSA Type 1450

AVP Type OCTETSTRING

AVP Flag M

KC-Key

This AVP contains the Ciphering Key.

Vendor ID 10415

VSA Type 1453

AVP Type OCTETSTRING

AVP Flag M

L7-Application-Description

This AVP carries L7 information with the L7 dynamic rule. This L7 filter is used by rule matching logic.

Vendor ID 9

VSA Type 132058

AVP Type GROUPED

Supported group value(s):

[L7_PROTOCOL_NAME]

[L7_FIELD]

[L7_OPERATOR]

[L7_VALUE]

[L7_CASE_SENSITIVITY]

[L7_CONTENT_FILTERING_STATE]

AVP Flag N/A

L7-Case-Sensitivity

This AVP indicates if the L7-Value field has to be compared with or without case-sensitivity.

Vendor ID 9

VSA Type 132063

AVP Type ENUM

Supported enumerated value(s):

1 CASE_SENSTIVE

2 NOT_CASE_SENSTIVE

AVP Flag N/A

L7-Content-Filtering-State

This attribute carries information about Content Filtering status (CF state) of L7 rules. This attribute indicates whether or not the ICAP functionality is enabled or disabled for L7 charging rule definition received for installation from PCRF. Based on this attribute value, the traffic matching to the dynamic rule is sent to ICAP server.

Vendor ID 9

VSA Type 132067

AVP Type ENUM

Supported enumerated value(s):

0 DISABLE_CF

1 ENABLE_CF

AVP Flag N/A

L7-Field

This AVP specifies the name of field to be matched from the protocol.

Vendor ID 9

VSA Type 132060

AVP Type ENUM

Supported enumerated value(s):

1 URL

2 ANY-MATCH

AVP Flag N/A

L7-Operator

This AVP specifies the operator to be used for matching the values.

Vendor ID 9

VSA Type 132061

AVP Type ENUM

Supported enumerated value(s):

1 EQUALS

2 STARTS_WITH

3 ENDS_WITH

4 CONTAINS

5 NOT_EQUALS

6 NOT_START_WITH

7 NOT_END_WITH

8 NOT_CONTAINS

AVP Flag N/A

L7-Parse-Length

L7-Parse-Length

Vendor ID 9

VSA Type 131128

AVP Type UINT32

AVP Flag N/A

L7-Parse-Protocol-Type

L7-Parse-Protocol-Type

Vendor ID 9

VSA Type 131085

AVP Type ENUM

Supported enumerated value(s):

0 HTTP

1 IMAP

2 OTHER

3 POP3

4 RTSP

5 SMTP

8 SIP

9 FTP

10 NBAR

11 DNS

12 HTTP-INSERT

AVP Flag M

L7-Protocol-Name

This AVP specifies the protocol name for the application. This is an enumerated value received from PCRF.

Vendor ID 9

VSA Type 132059

AVP Type ENUM

Supported enumerated value(s):

1 HTTP

AVP Flag N/A

L7-Value

This AVP mentions the value that is to be compared with the one received in the user packet. This is a string with length of 256 characters.

Vendor ID 9

VSA Type 132062

AVP Type OCTETSTRING

AVP Flag N/A

LCS-Capabilities-Sets

LCS-Capabilities-Sets

Vendor ID 10415

VSA Type 2404

AVP Type UINT32

AVP Flag M

LCS-Client-Type

LCS-Client-Type

Vendor ID 10415

VSA Type 1241

AVP Type ENUM

Supported enumerated value(s):

0 EMERGENCY_SERVICES

1 VALUE_ADDED_SERVICES

2 PLMN_OPERATOR_SERVICES

3 LAWFUL_INTERCEPT_SERVICES

AVP Flag M

LCS-Codeword

This AVP indicates the potential codeword string to send in a notification message to the UE.

Vendor ID 10415

VSA Type 2511

AVP Type UTF8STRING

AVP Flag M

LCS-EPS-Client-Name

LCS-EPS-Client-Name

Vendor ID 10415

VSA Type 2501

AVP Type GROUPED

Supported group value(s):

[LCS_NAME_STRING]

[LCS_FORMAT_INDICATOR]

AVP Flag M

LCS-Format-Indicator

This AVP contains the format of the LCS Client name.

Vendor ID 10415

VSA Type 1237

AVP Type ENUM

Supported enumerated value(s):

0 LOGICAL_NAME

1 EMAIL_ADDRESS

2 MSISDN

3 URL

4 SIP_URL

AVP Flag M

LCS-Info

This AVP contains LCS related information for a subscriber.

Vendor ID 10415

VSA Type 1473

AVP Type GROUPED

Supported group value(s):

[GMLC_ADDRESS]

[LCS_PRIVACYEXCEPTION]

[MO_LR]

AVP Flag M

LCS-Name-String

This AVP contains the LCS Client name.

Vendor ID 10415

VSA Type 1238

AVP Type UTF8STRING

AVP Flag M

LCS-Priority

This AVP indicates the priority of the location request. The value 0 indicates the highest priority, and the value 1 indicates normal priority. All other values are treated as 1 (normal priority).

Vendor ID 10415

VSA Type 2503

AVP Type UINT32

AVP Flag M

LCS-Privacy-Check

LCS-Privacy-Check

Vendor ID 10415

VSA Type 2512

AVP Type ENUM

Supported enumerated value(s):

0 ALLOWED_WITHOUT_NOTIFICATION

1 ALLOWED_WITH_NOTIFICATION

2 ALLOWED_IF_NO_RESPONSE

3 RESTRICTED_IF_NO_RESPONSE

4 NOT_ALLOWED

AVP Flag M

LCS-Privacy-Check-Non-Session

LCS-Privacy-Check-Non-Session

Vendor ID 10415

VSA Type 2521

AVP Type GROUPED

Supported group value(s):

[LCS_PRIVACY_CHECK]

AVP Flag M

LCS-Privacy-Check-Session

LCS-Privacy-Check-Session

Vendor ID 10415

VSA Type 2522

AVP Type GROUPED

Supported group value(s):

[LCS_PRIVACY_CHECK]

AVP Flag M

LCS-PrivacyException

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

Vendor ID 10415

VSA Type 1475

AVP Type GROUPED

Supported group value(s):

[SS_CODE]

[SS_STATUS]

[NOTIFICATION_TO_UE_USER]

[EXTERNAL_CLIENT]

[PLMN_CLIENT]

[SERVICE_TYPE]

AVP Flag M

LCS-QoS

LCS-QoS

Vendor ID 10415

VSA Type 2504

AVP Type GROUPED

Supported group value(s):

[LCS_QOS_CLASS]

[HORIZONTAL_ACCURACY]

[VERTICAL_ACCURACY]

[VERTICAL_REQUESTED]

[RESPONSE_TIME]

AVP Flag M

LCS-QoS-Class

LCS-QoS-Class

Vendor ID 10415

VSA Type 2523

AVP Type ENUM

Supported enumerated value(s):

0 ASSURED

AVP Flag M

LCS-Requestor-Id-String

LCS-Requestor-Id-String

Vendor ID 10415

VSA Type 1240

AVP Type UTF8STRING

AVP Flag M

LCS-Requestor-Name

LCS-Requestor-Name

Vendor ID 10415

VSA Type 2502

AVP Type GROUPED

Supported group value(s):

[LCS_REQUESTOR_ID_STRING]

[LCS_FORMAT_INDICATOR]

AVP Flag M

LCS-Service-Type-ID

This AVP specifies the identifier associated to one of the Service Types for which the LCS client is allowed to locate the particular UE.

Vendor ID 10415

VSA Type 2520

AVP Type UINT32

AVP Flag M

LI-Information

This AVP holds all the other surveillance AVPs.

Vendor ID 4491

VSA Type 218

AVP Type GROUPED

Supported group value(s):

[EVENT_MESSAGE_TYPE]

[ELEMENT_TYPE]

[ELEMENT_ID]

[TAP_ID]

[SIP_MESSAGE]

[DIRECT_MESSAGE]

[DIRECTION]

[DIALOG_ID]

[NEW_DIALOG_ID]

[CORRELATE_REASON]

[BCID]

AVP Flag M

LIPA-Permission

LIPA-Permission

Vendor ID 10415

VSA Type 1618

AVP Type ENUM

Supported enumerated value(s):

0 LIPA-PROHIBITED

1 LIPA-ONLY

2 LIPA-CONDITIONAL

AVP Flag M

Last-Packet-Timestamp

Last-Packet-Timestamp

Vendor ID 9

VSA Type 131159

AVP Type UINT32

AVP Flag N/A

Last-UE-Activity-Time

Last-UE-Activity-Time

Vendor ID 10415

VSA Type 1494

AVP Type TIME

AVP Flag M

Latching-Indication

This AVP contains the latching indication.

Vendor ID 13019

VSA Type 457

AVP Type ENUM

Supported enumerated value(s):

0 LATCH

1 RELATCH

AVP Flag N/A

Line-Identifier

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

Vendor ID 13019

VSA Type 500

AVP Type OCTETSTRING

AVP Flag M

Local-GW-Inserted-Indication

Local-GW-Inserted-Indication

Vendor ID 10415

VSA Type 2604

AVP Type ENUM

Supported enumerated value(s): none

AVP Flag M

Local-Sequence-Number

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

Vendor ID 10415

VSA Type 2063

AVP Type UINT32

AVP Flag M

Location-Area-Identity

This AVP contains the location area identification of the user.

Vendor ID 10415

VSA Type 1606

AVP Type OCTETSTRING

AVP Flag M

Location-Data

Location-Data

Vendor ID 0

VSA Type 128

AVP Type OCTETSTRING

AVP Flag N/A

Location-Estimate

Location-Estimate

Vendor ID 10415

VSA Type 1242

AVP Type OCTETSTRING

AVP Flag M

Location-Event

Location-Event

Vendor ID 10415

VSA Type 2518

AVP Type ENUM

Supported enumerated value(s):

0 EMERGENCY_CALL_ORIGINATION

1 EMERGENCY_CALL_RELEASE

2 MO_LR

3 EMERGENCY_CALL_HANDOVER

AVP Flag M

Location-Information

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

Vendor ID 13019

VSA Type 350

AVP Type GROUPED

Supported group value(s):

[LINE_IDENTIFIER]

[CIVIC_LOCATION]

[GEOSPATIAL_LOCATION]

AVP Flag M

Location-Information-Configuration

Location-Information-Configuration

Vendor ID 10415

VSA Type 3135

AVP Type GROUPED

Supported group value(s):

[MONTE_LOCATION_TYPE]

[ACCURACY]

AVP Flag M

Location-Information-Radius

Location-Information-Radius

Vendor ID 0

VSA Type 127

AVP Type OCTETSTRING

AVP Flag N/A

Location-Type

Location-Type

Vendor ID 10415

VSA Type 2500

AVP Type ENUM

Supported enumerated value(s):

0 CURRENT_LOCATION

1 CURRENT_OR_LAST_KNOWN_LOCATION

2 INITIAL_LOCATION

3 RESERVED

5 NOTIFICATION_VERIFICATION_ONLY

AVP Flag M

Logical-Access-Id

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

Vendor ID 0

VSA Type 302

AVP Type OCTETSTRING

AVP Flag M

Loose-Route-Indication

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

Vendor ID 10415

VSA Type 638

AVP Type ENUM

Supported enumerated value(s):

0 LOOSE_ROUTE_NOT_REQUIRED

1 LOOSE_ROUTE_REQUIRED

AVP Flag N/A

MBMS-2G-3G-Indicator

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

Vendor ID 10415

VSA Type 907

AVP Type ENUM

Supported enumerated value(s):

0 2G

1 3G

2 2G_AND_3G

AVP Flag M

MBMS-Access-Indicator

MBMS-Access-Indicator

Vendor ID 10415

VSA Type 923

AVP Type ENUM

Supported enumerated value(s):

0 UTRAN

1 E-UTRAN

2 UTRAN-AND-E-UTRAN

AVP Flag M

MBMS-BMSC-SSM-IP-Address

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

Vendor ID 10415

VSA Type 918

AVP Type UTF8STRING

AVP Flag M

MBMS-BMSC-SSM-IPv6-Address

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

Vendor ID 10415

VSA Type 919

AVP Type UTF8STRING

AVP Flag M

MBMS-BMSC-SSM-UDP-Port

MBMS-BMSC-SSM-UDP-Port

Vendor ID 10415

VSA Type 926

AVP Type OCTETSTRING

AVP Flag M

MBMS-Counting-Information

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

Vendor ID 10415

VSA Type 914

AVP Type ENUM

Supported enumerated value(s):

0 COUNTING_NOT_APPLICABLE

1 COUNTING_APPLICABLE

AVP Flag M

MBMS-Data-Transfer-Start

MBMS-Data-Transfer-Start

Vendor ID 10415

VSA Type 929

AVP Type UINT64

AVP Flag M

MBMS-Data-Transfer-Stop

MBMS-Data-Transfer-Stop

Vendor ID 10415

VSA Type 930

AVP Type UINT64

AVP Flag M

MBMS-Flags

MBMS-Flags

Vendor ID 10415

VSA Type 931

AVP Type UINT32

AVP Flag M

MBMS-Flow-Identifier

MBMS-Flow-Identifier

Vendor ID 10415

VSA Type 920

AVP Type OCTETSTRING

AVP Flag M

MBMS-GGSN-Address

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

Vendor ID 10415

VSA Type 916

AVP Type UTF8STRING

AVP Flag M

MBMS-GGSN-IPv6-Address

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

Vendor ID 10415

VSA Type 917

AVP Type UTF8STRING

AVP Flag M

MBMS-GW-SSM-IP-Address

MBMS-GW-SSM-IP-Address

Vendor ID 10415

VSA Type 924

AVP Type OCTETSTRING

AVP Flag M

MBMS-GW-SSM-IPv6-Address

MBMS-GW-SSM-IPv6-Address

Vendor ID 10415

VSA Type 925

AVP Type OCTETSTRING

AVP Flag M

MBMS-GW-UDP-Port

MBMS-GW-UDP-Port

Vendor ID 10415

VSA Type 927

AVP Type OCTETSTRING

AVP Flag M

MBMS-GW-UDP-Port-Indicator

MBMS-GW-UDP-Port-Indicator

Vendor ID 10415

VSA Type 928

AVP Type ENUM

Supported enumerated value(s):

1 UDP-PORT-REQUIRED

AVP Flag M

MBMS-HC-Indicator

MBMS-HC-Indicator

Vendor ID 10415

VSA Type 922

AVP Type ENUM

Supported enumerated value(s): none

AVP Flag M

MBMS-Required-QoS

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

Vendor ID 10415

VSA Type 913

AVP Type UTF8STRING

AVP Flag M

MBMS-Service-Area

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

Vendor ID 10415

VSA Type 903

AVP Type OCTETSTRING

AVP Flag M

MBMS-Service-Type

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

Vendor ID 10415

VSA Type 906

AVP Type ENUM

Supported enumerated value(s):

0 MULTICAST

1 BROADCAST

AVP Flag M

MBMS-Session-Duration

This AVP indicates the estimated session duration, if available.

Vendor ID 10415

VSA Type 904

AVP Type OCTETSTRING

AVP Flag M

MBMS-Session-Identity

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

Vendor ID 10415

VSA Type 908

AVP Type OCTETSTRING

AVP Flag M

MBMS-Session-Repetition-number

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

Vendor ID 10415

VSA Type 912

AVP Type OCTETSTRING

AVP Flag M

MBMS-StartStop-Indication

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

Vendor ID 10415

VSA Type 902

AVP Type ENUM

Supported enumerated value(s):

0 START

1 STOP

2 UPDATE

AVP Flag M

MBMS-Time-To-Data-Transfer

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

Vendor ID 10415

VSA Type 911

AVP Type OCTETSTRING

AVP Flag M

MBMS-User-Data-Mode-Indication

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

Vendor ID 10415

VSA Type 915

AVP Type ENUM

Supported enumerated value(s):

0 UNICAST

1 MULTICAST_AND_UNICAST

AVP Flag M

MBR-Burst-Size-DL

MBR-Burst-Size-DL

Vendor ID 9

VSA Type 132010

AVP Type UINT32

AVP Flag N/A

MBR-Burst-Size-UL

MBR-Burst-Size-UL

Vendor ID 9

VSA Type 132009

AVP Type UINT32

AVP Flag N/A

MBR-Limit-Conform-Action-DL

MBR-Limit-Conform-Action-DL

Vendor ID 9

VSA Type 132007

AVP Type GROUPED

Supported group value(s):

[RATE_LIMIT_ACTION]

[DSCP]

AVP Flag N/A

MBR-Limit-Conform-Action-UL

MBR-Limit-Conform-Action-UL

Vendor ID 9

VSA Type 132005

AVP Type GROUPED

Supported group value(s):

[RATE_LIMIT_ACTION]

[DSCP]

AVP Flag N/A

MBR-Limit-Exceed-Action-DL

MBR-Limit-Exceed-Action-DL

Vendor ID 9

VSA Type 132008

AVP Type GROUPED

Supported group value(s):

[RATE_LIMIT_ACTION]

[DSCP]

AVP Flag N/A

MBR-Limit-Exceed-Action-UL

MBR-Limit-Exceed-Action-UL

Vendor ID 9

VSA Type 132006

AVP Type GROUPED

Supported group value(s):

[RATE_LIMIT_ACTION]

[DSCP]

AVP Flag N/A

MEID

This AVP contains the International Mobile Equipment Identity.

Vendor ID 10415

VSA Type 6110

AVP Type OCTETSTRING

AVP Flag M

MIP-Feature-Vector

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

Vendor ID 10415

VSA Type 337

AVP Type UINT32

AVP Flag M

MIP-Home-Agent-Address-IETF

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

Vendor ID 0

VSA Type 334

AVP Type ADDRESS

AVP Flag M

MIP-Home-Agent-Host

This AVP contains the identity of the assigned MIPv6 HA.

Vendor ID 0

VSA Type 348

AVP Type GROUPED

Supported group value(s):

[DESTINATION_REALM]

[DESTINATION_HOST]

AVP Flag M

MIP-Mobile-Node-Address

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

Vendor ID 10415

VSA Type 333

AVP Type ADDRESS

AVP Flag M

MIP6-Agent-Info

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

Vendor ID 0

VSA Type 486

AVP Type GROUPED

Supported group value(s):

[MIP_HOME_AGENT_ADDRESS_IETF]

[MIP_HOME_AGENT_HOST]

[MIP6_HOME_LINK_PREFIX]

AVP Flag M

MIP6-Feature-Vector

This AVP contains the subset of the MIPv6 features supported.

Vendor ID 0

VSA Type 6062

AVP Type UINT64

AVP Flag M

MIP6-Home-Link-Prefix

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

Vendor ID 0

VSA Type 125

AVP Type OCTETSTRING

AVP Flag M

MME-Location-Information

This AVP contains the location information of the MME user.

Vendor ID 10415

VSA Type 1600

AVP Type GROUPED

Supported group value(s):

[EUTRAN_CELL_GLOBAL_IDENTITY]

[TRACKING_AREA_IDENTITY]

[GEOGRAPHICAL_INFORMATION]

[GEODETIC_INFORMATION]

[CURRENT_LOCATION_RETRIEVED]

[AGE_OF_LOCATION_INFORMATION]

AVP Flag M

MME-Name

MME-Name

Vendor ID 10415

VSA Type 2402

AVP Type DIAMURI

AVP Flag M

MME-Number-For-MT-SMS

MME-Number-For-MT-SMS

Vendor ID 10415

VSA Type 1645

AVP Type OCTETSTRING

AVP Flag N/A

MME-SM-Delivery-Outcome

MME-SM-Delivery-Outcome

Vendor ID 10415

VSA Type 3317

AVP Type GROUPED

Supported group value(s):

[SM_DELIVERY_CAUSE]

[ABSENT_USER_DIAGNOSTIC_SM]

AVP Flag M

MME-Realm

MME-Realm

Vendor ID 10415

VSA Type 2408

AVP Type DIAMURI

AVP Flag M

MME-Service-Type

MME-Service-Type

Vendor ID 10415

VSA Type 1483

AVP Type GROUPED

Supported group value(s):

[SERVICETYPEIDENTITY]

[GMLC_RESTRICTION]

[NOTIFICATION_TO_UE_USER]

AVP Flag M

MME-User-State

This AVP contains the location information of the MME user.

Vendor ID 10415

VSA Type 1497

AVP Type GROUPED

Supported group value(s):

[USER_STATE]

AVP Flag M

MO-LR

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

Vendor ID 10415

VSA Type 1485

AVP Type GROUPED

Supported group value(s):

[SS_CODE]

[SS_STATUS]

AVP Flag M

MONTE-Location-Type

MONTE-Location-Type

Vendor ID 10415

VSA Type 3136

AVP Type UINT32

AVP Flag M

MPS-Identifier

MPS-Identifier

Vendor ID 10415

VSA Type 528

AVP Type OCTETSTRING

AVP Flag N/A

MPS-Priority

MPS-Priority

Vendor ID 10415

VSA Type 1616

AVP Type UINT32

AVP Flag N/A

MSC-Number

MSC-Number

Vendor ID 10415

VSA Type 2403

AVP Type OCTETSTRING

AVP Flag M

MSC-SM-Delivery-Outcome

MSC-SM-Delivery-Outcome

Vendor ID 10415

VSA Type 3318

AVP Type GROUPED

Supported group value(s):

[SM_DELIVERY_CAUSE]

[ABSENT_USER_DIAGNOSTIC_SM]

AVP Flag M

MSISDN

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

Vendor ID 0

VSA Type 701

AVP Type OCTETSTRING

AVP Flag M

MVNO-Reseller-Id

This AVP contains the Reseller ID. This attribute is included in Gx messages like CCA-I/CCA-U and RAR messages, and also included in Gy messages like CCR-I/U/T.

Vendor ID 9

VSA Type 131507

AVP Type UTF8STRING

AVP Flag N/A

MVNO-Sub-Class-Id

This AVP contains the Sub-Class-Id. This AVP is included in Gx messages like CCA-I/CCA-U and RAR messages, and also included in Gy messages like CCR-I/U/T.

Vendor ID 9

VSA Type 131508

AVP Type UTF8STRING

AVP Flag N/A

Mandatory-Capability

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

Vendor ID 10415

VSA Type 604

AVP Type UINT32

AVP Flag M

Match-String

Match-String

Vendor ID 9

VSA Type 131091

AVP Type UTF8STRING

AVP Flag M

Max-Bandwidth

Max-Bandwidth

Vendor ID 9

VSA Type 131174

AVP Type UINT32

AVP Flag N/A

Max-Burst-Size

Max-Burst-Size

Vendor ID 9

VSA Type 131190

AVP Type UINT32

AVP Flag N/A

Max-Requested-Bandwidth

This AVP contains the maximum subscriber requested bandwidth.

Vendor ID 10415

VSA Type 313

AVP Type OCTETSTRING

AVP Flag M

Max-Requested-Bandwidth-DL

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

Vendor ID 10415

VSA Type 515

AVP Type UINT32

AVP Flag M

Max-Requested-Bandwidth-UL

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

Vendor ID 10415

VSA Type 516

AVP Type UINT32

AVP Flag M

Max-Wait-Time

This AVP indicates the validity of the request message. It is a 4-byte value that is encoded as milliseconds and is an offset from the Origin Timestamp.

Vendor ID 9

VSA Type 132051

AVP Type UINT32

AVP Flag N/A

Maximum-Latency

Maximum-Latency

Vendor ID 10415

VSA Type 3133

AVP Type UINT32

AVP Flag M

Maximum-Number-of-Reports

Maximum-Number-of-Reports

Vendor ID 10415

VSA Type 3128

AVP Type UINT32

AVP Flag M

Maximum-Response-Time

Maximum-Response-Time

Vendor ID 10415

VSA Type 3134

AVP Type UINT32

AVP Flag M

Maximum-Retransmission-Time

Maximum-Retransmission-Time

Vendor ID 10415

VSA Type 3330

AVP Type TIME

AVP Flag N/A

Maximum-Timeout

Maximum-Timeout

Vendor ID 9

VSA Type 131108

AVP Type UINT32

AVP Flag N/A

Maximum-UE-Availability-Time

Maximum-UE-Availability-Time

Vendor ID 10415

VSA Type 3329

AVP Type TIME

AVP Flag N/A

Media-Component-Description

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

Vendor ID 10415

VSA Type 517

AVP Type GROUPED

Supported group value(s):

[MEDIA_COMPONENT_NUMBER]

[MEDIA_SUB_COMPONENT]

[AF_APPLICATION_IDENTIFIER]

[MEDIA_TYPE]

[MAX_REQUESTED_BANDWIDTH_UL]

[MAX_REQUESTED_BANDWIDTH_DL]

[FLOW_STATUS]

[RS_BANDWIDTH]

[RR_BANDWIDTH]

AVP Flag M

Media-Component-Number

This AVP contains the ordinal number of the media component.

Vendor ID 10415

VSA Type 518

AVP Type UINT32

AVP Flag M

Media-Initiator-Flag

This AVP indicates which party has requested the session modification.

Vendor ID 10415

VSA Type 882

AVP Type ENUM

Supported enumerated value(s): none

AVP Flag M

Media-Initiator-Party

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

Vendor ID 10415

VSA Type 1288

AVP Type UTF8STRING

AVP Flag M

Media-Sub-Component

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

Vendor ID 10415

VSA Type 519

AVP Type GROUPED

Supported group value(s):

[FLOW_NUMBER]

[FLOW_DESCRIPTION]

[FLOW_STATUS]

[FLOW_USAGE]

[MAX_REQUESTED_BANDWIDTH_UL]

[MAX_REQUESTED_BANDWIDTH_DL]

AVP Flag M

Media-Type

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

Vendor ID 10415

VSA Type 520

AVP Type ENUM

Supported enumerated value(s):

0 AUDIO

1 VIDEO

2 DATA

3 APPLICATION

4 CONTROL

5 TEXT

6 MESSAGE

AVP Flag M

Message-Body

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

Vendor ID 10415

VSA Type 889

AVP Type GROUPED

Supported group value(s):

[CONTENT_TYPE]

[CONTENT_LENGTH]

[CONTENT_DISPOSITION]

[ORIGINATOR]

AVP Flag M

Meter-Exclude

Meter-Exclude

Vendor ID 9

VSA Type 131110

AVP Type ENUM

Supported enumerated value(s):

0 MMS_WAP

1 RTSP_PAUSE

2 SERVICE_IDLE

3 NETWORK_INIT_SIP

AVP Flag M

Meter-Include-Imap

Meter-Include-Imap

Vendor ID 9

VSA Type 131111

AVP Type ENUM

Supported enumerated value(s):

0 BODY_AND_HEADER

1 BODY_ONLY

2 BODY_AND_OTHER

AVP Flag M

Meter-Increment

Meter-Increment

Vendor ID 9

VSA Type 131113

AVP Type UINT32

AVP Flag N/A

Meter-Initial

Meter-Initial

Vendor ID 9

VSA Type 131114

AVP Type UINT32

AVP Flag N/A

Meter-Minimum

Meter-Minimum

Vendor ID 9

VSA Type 131115

AVP Type UINT32

AVP Flag N/A

Metering-Granularity

Metering-Granularity

Vendor ID 9

VSA Type 131112

AVP Type GROUPED

Supported group value(s):

[METER_INCREMENT]

[METER_INITIAL]

[METER_MINIMUM]

AVP Flag M

Metering-Method

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

Vendor ID 10415

VSA Type 1007

AVP Type ENUM

Supported enumerated value(s):

0 DURATION

1 VOLUME

2 DURATION_VOLUME

AVP Flag M

Min-Bandwidth-DL

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

Vendor ID 5535

VSA Type 1012

AVP Type UINT32

AVP Flag M

Min-Bandwidth-UL

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

Vendor ID 5535

VSA Type 1013

AVP Type UINT32

AVP Flag M

Mining

Mining

Vendor ID 9

VSA Type 131199

AVP Type ENUM

Supported enumerated value(s):

0 DISABLED

1 ENABLED

AVP Flag M

Mobile-Node-Identifier

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

Vendor ID 0

VSA Type 89

AVP Type OCTETSTRING

AVP Flag M

Monitoring-Duration

Monitoring-Duration

Vendor ID 10415

VSA Type 3130

AVP Type TIME

AVP Flag M

Monitoring-Event-Config-Status

Monitoring-Event-Config-Status

Vendor ID 10415

VSA Type 3142

AVP Type GROUPED

Supported group value(s):

[SERVICE_REPORT]

[SCEF_REFERENCE_ID]

[SCEF_ID]

AVP Flag M

Monitoring-Event-Configuration

Monitoring-Event-Configuration

Vendor ID 10415

VSA Type 3122

AVP Type GROUPED

Supported group value(s):

[SCEF_REFERENCE_ID]

[SCEF_ID]

[MONITORING_TYPE]

[SCEF_REFERENCE_ID_FOR_DELETION]

[MAXIMUM_NUMBER_OF_REPORTS]

[MONITORING_DURATION]

[CHARGED_PARTY]

[UE_REACHABILITY_CONFIGURATION]

[LOCATION_INFORMATION_CONFIGURATION]

[NUMBER_OF_UE_PER_LOCATION_CONFIGURATION]

AVP Flag M

Monitoring-Event-Report

Monitoring-Event-Report

Vendor ID 10415

VSA Type 3123

AVP Type GROUPED

Supported group value(s):

[SCEF_REFERENCE_ID]

[SCEF_ID]

[MONITORING_TYPE]

[REACHABILITY_INFORMATION]

[EPS_LOCATION_INFORMATION]

[COMMUNICATION_FAILURE_INFORMATION]

[NUMBER_OF_UE_PER_LOCATION_REPORT]

AVP Flag M

Monitoring-Key

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

Vendor ID 10415

VSA Type 1066

AVP Type OCTETSTRING

AVP Flag N/A

Monitoring-Type

Monitoring-Type

Vendor ID 10415

VSA Type 3127

AVP Type UINT32

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".

Vendor ID 0

VSA Type 272

AVP Type UINT32

AVP Flag N/A

Multiple-Auth-Profile

This AVP indicates Multiple Authentication requirements for a particular user.

Vendor ID 5535

VSA Type 30

AVP Type ENUM

Supported enumerated value(s): none

AVP Flag M

Multiple-Auth-Support

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

Vendor ID 5535

VSA Type 29

AVP Type ENUM

Supported enumerated value(s): none

AVP Flag M

Multiple-Registration-Indication

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

Vendor ID 10415

VSA Type 648

AVP Type ENUM

Supported enumerated value(s):

0 NOT_MULTIPLE_REGISTRATION

1 MULTIPLE_REGISTRATION

AVP Flag N/A

Multiple-Services-Credit-Control

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

Vendor ID 0

VSA Type 456

AVP Type GROUPED

Supported group value(s):

[REQUESTED_SERVICE_UNIT]

[GRANTED_SERVICE_UNIT]

[USED_SERVICE_UNIT]

[TARIFF_CHANGE_USAGE]

[SERVICE_IDENTIFIER]

[RATING_GROUP]

[G_S_U_POOL_REFERENCE]

[VALIDITY_TIME]

[RESULT_CODE]

[FINAL_UNIT_INDICATION]

AVP Flag M

Multiple-Services-Indicator

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

Vendor ID 0

VSA Type 455

AVP Type ENUM

Supported enumerated value(s):

0 MULTIPLE_SERVICES_NOT_SUPPORTED

1 MULTIPLE_SERVICES_SUPPORTED

AVP Flag M

Mute-Notification

This AVP is used to mute the notification to the PCRF of the detected application's start/stop for the specific ADC/PCC rule from PCEF.

Vendor ID 10415

VSA Type 2809

AVP Type ENUM

Supported enumerated value(s):

0 MUTE_REQUIRED

AVP Flag N/A

NAS-Filter-Rule

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

Vendor ID 0

VSA Type 400

AVP Type IPFILTERRULE

AVP Flag M

NAS-IP-Address

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

Vendor ID 0

VSA Type 4

AVP Type OCTETSTRING

AVP Flag M

NAS-IPv6-Address

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

Vendor ID 0

VSA Type 95

AVP Type OCTETSTRING

AVP Flag M

NAS-Identifier

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

Vendor ID 0

VSA Type 32

AVP Type UTF8STRING

AVP Flag M

NAS-Port

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

Vendor ID 0

VSA Type 5

AVP Type UINT32

AVP Flag M

NAS-Port-Id

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

Vendor ID 0

VSA Type 87

AVP Type UTF8STRING

AVP Flag M

NAS-Port-Type

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

Vendor ID 0

VSA Type 61

AVP Type ENUM

Supported enumerated value(s):

0 Async

1 Sync

2 ISDN_Sync

3 ISDN_Async_V120

4 ISDN_Async_V110

5 Virtual

6 PIAFS

7 HDLC_Clear_Channel

8 X25

9 X75

10 G3_Fax

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

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

14 IDSL-ISDN-Digital-Subscriber-Line

15 Ethernet

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

17 Cable

18 Wireless-Other

19 Wireless-IEEE802_11

20 Token-Ring_RAD802_1X

21 FDDI_RAD802_1X

22 Wireless-CDMA2000

23 Wireless-UMTS

24 Wireless-1X-EV

25 IAPP_IEEE-802_11f

AVP Flag M

NOR-Flags

The NOR-Flags AVP contains a bit mask.

Vendor ID 10415

VSA Type 1443

AVP Type UINT32

AVP Flag M

NetLoc-Access-Support

NetLoc-Access-Support

Vendor ID 10415

VSA Type 2824

AVP Type ENUM

Supported enumerated value(s):

0 NETLOC_ACCESS_NOT_SUPPORTED

AVP Flag N/A

Network-Access-Mode

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

Vendor ID 10415

VSA Type 1417

AVP Type ENUM

Supported enumerated value(s):

0 PACKET_AND_CIRCUIT

1 ONLY_CIRCUIT

2 ONLY_PACKET

AVP Flag M

Network-Element-Type

Network-Element-Type

Vendor ID 10415

VSA Type 1461

AVP Type ENUM

Supported enumerated value(s):

0 MME

1 SGSN

2 Serving-GW

3 PDN-GW

4 eNodeB

5 RNC

AVP Flag M

Network-Request-Support

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

Vendor ID 10415

VSA Type 1024

AVP Type ENUM

Supported enumerated value(s):

0 NETWORK_REQUEST_NOT_SUPPORTED

1 NETWORK_REQUEST_SUPPORTED

AVP Flag M

New-Dialog-Id

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

Vendor ID 4491

VSA Type 219

AVP Type UTF8STRING

AVP Flag M

Nexthop

Nexthop

Vendor ID 9

VSA Type 131137

AVP Type ADDRESS

AVP Flag M

Nexthop-Downlink

Nexthop-Downlink

Vendor ID 9

VSA Type 131084

AVP Type ADDRESS

AVP Flag M

Nexthop-Media

Nexthop-Media

Vendor ID 9

VSA Type 131211

AVP Type ADDRESS

AVP Flag M

Nexthop-Override

Nexthop-Override

Vendor ID 9

VSA Type 131212

AVP Type ENUM

Supported enumerated value(s):

0 DISABLED

1 ENABLED

AVP Flag M

Nexthop-Uplink

Nexthop-Uplink

Vendor ID 9

VSA Type 131083

AVP Type ADDRESS

AVP Flag M

Node-Functionality

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

Vendor ID 0

VSA Type 862

AVP Type ENUM

Supported enumerated value(s):

0 S-CSCF

1 P-CSCF

2 I-CSCF

AVP Flag M

Node-Id

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

Vendor ID 10415

VSA Type 2064

AVP Type UTF8STRING

AVP Flag M

Node-Type

Node-Type

Vendor ID 10415

VSA Type 3162

AVP Type UINT32

AVP Flag M

Non-IP-Data

Non-IP-Data

Vendor ID 10415

VSA Type 4315

AVP Type OCTETSTRING

AVP Flag M

Non-IP-Data-Delivery-Mechanism

Non-IP-Data-Delivery-Mechanism

Vendor ID 10415

VSA Type 1682

AVP Type ENUM

Supported enumerated value(s):

0 SGi-BASED-DATA-DELIVERY

1 SCEF-BASED-DATA-DELIVERY

AVP Flag N/A

Non-IP-PDN-Type-Indicator

Non-IP-PDN-Type-Indicator

Vendor ID 10415

VSA Type 1681

AVP Type ENUM

Supported enumerated value(s):

0 FALSE

1 TRUE

AVP Flag N/A

Nortel-Data-Reference

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

Vendor ID 0

VSA Type 301

AVP Type ENUM

Supported enumerated value(s): none

AVP Flag M

Notification-To-UE-User

Notification-To-UE-User

Vendor ID 10415

VSA Type 1478

AVP Type ENUM

Supported enumerated value(s):

0 NOTIFY_LOCATION_ALLOWED

1 NOTIFYANDVERIFY_ALLOWED_IF_NO_RESPONSE

2 NOTIFYANDVERIFY_NOT_ALLOWED_IF_NO_RESPONSE

3 LOCATION_NOT_ALLOWED

AVP Flag M

Number-Of-Requested-Vectors

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

Vendor ID 10415

VSA Type 6013

AVP Type UINT32

AVP Flag M

Number-Of-UE-Per-Location-Configuration

Number-Of-UE-Per-Location-Configuration

Vendor ID 10415

VSA Type 4306

AVP Type GROUPED

Supported group value(s):

[EPS_LOCATION_INFORMATION]

AVP Flag M

Number-Of-UE-Per-Location-Report

Number-Of-UE-Per-Location-Report

Vendor ID 10415

VSA Type 4307

AVP Type GROUPED

Supported group value(s):

[EPS_LOCATION_INFORMATION]

[UE_COUNT]

AVP Flag M

Number-Portability-Routing-Information

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

Vendor ID 10415

VSA Type 2024

AVP Type UTF8STRING

AVP Flag M

OC-Feature-Vector

OC-Feature-Vector

Vendor ID 10415

VSA Type 622

AVP Type UINT64

AVP Flag M

OC-OLR

OC-OLR

Vendor ID 10415

VSA Type 623

AVP Type GROUPED

Supported group value(s):

[OC_SEQUENCE_NUMBER]

[OC_REPORT_TYPE]

[OC_REDUCTION_PERCENTAGE]

[OC_VALIDITY_DURATION]

AVP Flag M

OC-Reduction-Percentage

OC-Reduction-Percentage

Vendor ID 10415

VSA Type 627

AVP Type UINT32

AVP Flag M

OC-Report-Type

OC-Report-Type

Vendor ID 10415

VSA Type 626

AVP Type ENUM

Supported enumerated value(s):

0 HOST-REPORT

1 REALM-REPORT

AVP Flag M

OC-Sequence-Number

OC-Sequence-Number

Vendor ID 10415

VSA Type 624

AVP Type UINT64

AVP Flag M

OC-Supported-Features

OC-Supported-Features

Vendor ID 10415

VSA Type 621

AVP Type GROUPED

Supported group value(s):

[OC_FEATURE_VECTOR]

AVP Flag M

OC-Validity-Duration

OC-Validity-Duration

Vendor ID 10415

VSA Type 625

AVP Type UINT32

AVP Flag M

OMC-Id

OMC-Id

Vendor ID 10415

VSA Type 1466

AVP Type OCTETSTRING

AVP Flag M

Offline

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

Vendor ID 10415

VSA Type 1008

AVP Type ENUM

Supported enumerated value(s):

0 DISABLE_OFFLINE

1 ENABLE_OFFLINE

AVP Flag M

OFR-Flags

OFR-Flags

Vendor ID 10415

VSA Type 3328

AVP Type UINT32

AVP Flag N/A

Online

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

Vendor ID 10415

VSA Type 1009

AVP Type ENUM

Supported enumerated value(s):

0 DISABLE_ONLINE

1 ENABLE_ONLINE

AVP Flag M

Online-Billing-Basis

Online-Billing-Basis

Vendor ID 9

VSA Type 131093

AVP Type ENUM

Supported enumerated value(s):

0 INVALID

1 EVENT

2 IP_BYTE

3 TCP_BYTE

4 DURATION

5 DURATION_OF_CONNECTION

6 DURATION_OF_TRANSACTION

AVP Flag M

Online-Charging-Flag

Online-Charging-Flag

Vendor ID 10415

VSA Type 2303

AVP Type ENUM

Supported enumerated value(s): none

AVP Flag M

Online-Passthrough-Quota

Online-Passthrough-Quota

Vendor ID 9

VSA Type 131104

AVP Type UINT32

AVP Flag N/A

Online-Reauthorization-Threshold

Online-Reauthorization-Threshold

Vendor ID 9

VSA Type 131105

AVP Type UINT32

AVP Flag N/A

Online-Reauthorization-Timeout

Online-Reauthorization-Timeout

Vendor ID 9

VSA Type 131106

AVP Type GROUPED

Supported group value(s):

[INITIAL_TIMEOUT]

[MAXIMUM_TIMEOUT]

AVP Flag M

Operation-Status

Operation-Status

Vendor ID 9

VSA Type 131135

AVP Type ENUM

Supported enumerated value(s):

0 OUT_OF_SERVICE

1 IN_SERVICE

AVP Flag M

Operator-Determined-Barring

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

Vendor ID 10415

VSA Type 1425

AVP Type UINT32

AVP Flag M

Operator-Name

Operator-Name

Vendor ID 0

VSA Type 126

AVP Type OCTETSTRING

AVP Flag N/A

Optional-Capability

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

Vendor ID 10415

VSA Type 605

AVP Type UINT32

AVP Flag M

Origin-Host

This AVP indicates the endpoint that originated the Diameter message.

Vendor ID 0

VSA Type 264

AVP Type DIAMIDENT

AVP Flag M

Origin-Realm

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

Vendor ID 0

VSA Type 296

AVP Type DIAMIDENT

AVP Flag M

Origin-State-Id

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

Vendor ID 0

VSA Type 278

AVP Type UINT32

AVP Flag M

Originating-IOI

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

Vendor ID 0

VSA Type 839

AVP Type UTF8STRING

AVP Flag M

Originating-Line-Info

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

Vendor ID 0

VSA Type 94

AVP Type OCTETSTRING

AVP Flag N/A

Originating-Request

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

Vendor ID 10415

VSA Type 633

AVP Type ENUM

Supported enumerated value(s):

0 ORIGINATING

AVP Flag M

Originating-SIP-URI

Originating-SIP-URI

Vendor ID 10415

VSA Type 3326

AVP Type UTF8STRING

AVP Flag N/A

Origination-TimeStamp

This AVP indicates the time (NTP synced) when the request message is sent to AAA Server from ePDG/MME. It is an 8-byte value that is encoded as the number of milliseconds elapsed since NTP time.

Vendor ID 9

VSA Type 132050

AVP Type UINT64

AVP Flag N/A

Originator

This AVP indicates the originating party of the message body.

Vendor ID 10415

VSA Type 864

AVP Type ENUM

Supported enumerated value(s): none

AVP Flag M

Outgoing-Trunk-Group-ID

This AVP identifies the outgoing PSTN leg.

Vendor ID 0

VSA Type 853

AVP Type UTF8STRING

AVP Flag M

Override-Allocation-Retention-Priority

This AVP is of type grouped and is used to override the pre-configured value of ARP.

Vendor ID 9

VSA Type 132036

AVP Type GROUPED

Supported group value(s):

[OVERRIDE_PRIORITY_LEVEL]

[OVERRIDE_PRE_EMPTION_CAPABILITY]

[OVERRIDE_PRE_EMPTION_VULNERABILITY]

AVP Flag N/A

Override-Charging-Action-Exclude-Rule

This AVP defines the rule name for which override-control will not be applied. This AVP may be included more than once if more than one rule needs to be excluded.

Vendor ID 9

VSA Type 132021

AVP Type OCTETSTRING

AVP Flag N/A

Override-Charging-Action-Name

This AVP specifies the charging action name that has to be overridden.

Vendor ID 9

VSA Type 132020

AVP Type OCTETSTRING

AVP Flag N/A

Override-Charging-Action-Parameters

This AVP is used to override pre-configured values of a charging action. If Override-Rule-Name is not present, all rules (static and predefined) configured with the specified charging action are effected. The overriding parameters will not be applied for all rules specified by Exclude-Rule AVP.

Vendor ID 9

VSA Type 132019

AVP Type GROUPED

Supported group value(s):

[EXECUTION_TIME]

[OVERRIDE_CONTROL_PENDING_QUEUE_ACTION]

[OVERRIDE_CHARGING_ACTION_NAME]

[OVERRIDE_CHARGING_ACTION_EXCLUDE_RULE]

[OVERRIDE_CHARGING_PARAMETERS]

[OVERRIDE_POLICY_PARAMETERS]

AVP Flag N/A

Override-Charging-Parameters

This AVP is used to override the charging parameters configured at P-GW for a rule (static/predefined) or for a charging action. If Override-Rule-Name AVP is present, these parameters apply only to that rule(s). Else, all rules (static and predefined) configured with the specified charging action are effected.

Vendor ID 9

VSA Type 132022

AVP Type GROUPED

Supported group value(s):

[OVERRIDE_SERVICE_IDENTIFIER]

[OVERRIDE_RATING_GROUP]

[OVERRIDE_ONLINE]

[OVERRIDE_OFFLINE]

AVP Flag N/A

Override-Content-Filtering-State

This attribute carries information about Content Filtering status (CF state) of rules or charging-action. This AVP is used for overriding the content-filtering status of static and predefined rules. This attribute is included in the Override-Control grouped AVP.

Vendor ID 9

VSA Type 132028

AVP Type ENUM

Supported enumerated value(s):

0 DISABLE_CF

1 ENABLE_CF

AVP Flag N/A

Override-Control

This AVP is used to enable the PCRF to override charging and policy parameters for a specified set of rules or charging actions. This AVP may be present more than once if override at rule level and charging action level are to be sent in the same message.

Vendor ID 9

VSA Type 132017

AVP Type GROUPED

Supported group value(s):

[OVERRIDE_CONTROL_NAME]

[OVERRIDE_RULE_NAME]

[OVERRIDE_CHARGING_ACTION_PARAMETERS]

AVP Flag N/A

Override-Control-Merge-Wildcard

Override-Control-Merge-Wildcard

Vendor ID 9

VSA Type 132079

AVP Type ENUM

Supported enumerated value(s):

0 TRUE

AVP Flag N/A

Override-Control-Name

This AVP specifies the name of the Override-Control. This AVP may be included more than once if multiple overrides need to be disabled.

Vendor ID 9

VSA Type 132052

AVP Type OCTETSTRING

AVP Flag N/A

Override-Control-Pending-Queue-Action

Override-Control-Pending-Queue-Action

Vendor ID 9

VSA Type 132078

AVP Type ENUM

Supported enumerated value(s):

0 FLUSH

1 RETAIN

AVP Flag N/A

Override-Guaranteed-Bitrate-DL

This AVP defines the guaranteed bit rate allowed for downlink direction. This AVP will be included only for rules on dedicated bearers.

Vendor ID 9

VSA Type 132035

AVP Type UINT32

AVP Flag N/A

Override-Guaranteed-Bitrate-UL

This AVP defines the guaranteed bit rate allowed for uplink direction. This AVP will be included only for rules on dedicated bearers.

Vendor ID 9

VSA Type 132034

AVP Type UINT32

AVP Flag N/A

Override-Max-Requested-Bandwidth-DL

This AVP defines the maximum bit rate allowed for the downlink direction.

Vendor ID 9

VSA Type 132033

AVP Type UINT32

AVP Flag N/A

Override-Max-Requested-Bandwidth-UL

This AVP defines the maximum bit rate allowed for the uplink direction.

Vendor ID 9

VSA Type 132032

AVP Type UINT32

AVP Flag N/A

Override-Nexthop-Address

This attribute indicates the override next hop address in dotted decimal format.

Vendor ID 9

VSA Type 132054

AVP Type ADDRESS

AVP Flag N/A

Override-Offline

This AVP is used to override the Offline flag configured in the charging action specified by Charging-Action-Name.

Vendor ID 9

VSA Type 132027

AVP Type ENUM

Supported enumerated value(s):

0 DISABLE_OFFLINE

1 ENABLE_OFFLINE

AVP Flag N/A

Override-Online

This AVP is used to override the Online flag configured in the charging action specified by Charging-Action-Name.

Vendor ID 9

VSA Type 132026

AVP Type ENUM

Supported enumerated value(s):

0 DISABLE_ONLINE

1 ENABLE_ONLINE

AVP Flag N/A

Override-Policy-Parameters

This AVP is used to override the Policy parameters configured at P-GW for a rule (static/predefined) or for a charging action. If Override-Rule-Name AVP is present, these parameters apply only to that rule(s). Else, all rules (static and predefined) configured with the specified charging action are effected.

Vendor ID 9

VSA Type 132029

AVP Type GROUPED

Supported group value(s):

[OVERRIDE_QOS_INFORMATION]

[OVERRIDE_NEXTHOP_ADDRESS]

[OVERRIDE_TOS_VALUE]

[OVERRIDE_CONTENT_FILTERING_STATE]

AVP Flag N/A

Override-Pre-Emption-Capability

Override-Pre-Emption-Capability

Vendor ID 9

VSA Type 132038

AVP Type ENUM

Supported enumerated value(s):

0 PRE-EMPTION_CAPABILITY_ENABLED

1 PRE-EMPTION_CAPABILITY_DISABLED

AVP Flag N/A

Override-Pre-Emption-Vulnerability

Override-Pre-Emption-Vulnerability

Vendor ID 9

VSA Type 132039

AVP Type ENUM

Supported enumerated value(s):

0 PRE-EMPTION_VULNERABILITY_ENABLED

1 PRE-EMPTION_VULNERABILITY_DISABLED

AVP Flag N/A

Override-Priority-Level

Override-Priority-Level

Vendor ID 9

VSA Type 132037

AVP Type UINT32

AVP Flag N/A

Override-QoS-Class-Identifier

This AVP denotes the value of Override QoS Class Identifier. The allowed values for the nine standard QCIs are defined in 3GPP TS 23.203 specification.

Vendor ID 9

VSA Type 132031

AVP Type ENUM

Supported enumerated value(s):

1 TRAFFIC_CLASS_A

2 TRAFFIC_CLASS_B

3 TRAFFIC_CLASS_C

4 TRAFFIC_CLASS_D

5 TRAFFIC_CLASS_E

6 TRAFFIC_CLASS_F

7 TRAFFIC_CLASS_G

8 TRAFFIC_CLASS_H

9 TRAFFIC_CLASS_I

AVP Flag N/A

Override-QoS-Information

This AVP is used to override QoS-Information for a predefined rule or charging action. These values are ignored (if present) while applying override values to a static rule.

Vendor ID 9

VSA Type 132030

AVP Type GROUPED

Supported group value(s):

[OVERRIDE_MAX_REQUESTED_BANDWIDTH_UL]

[OVERRIDE_MAX_REQUESTED_BANDWIDTH_DL]

[OVERRIDE_GUARANTEED_BITRATE_UL]

[OVERRIDE_GUARANTEED_BITRATE_DL]

[OVERRIDE_ALLOCATION_RETENTION_PRIORITY]

[OVERRIDE_QOS_CLASS_IDENTIFIER]

AVP Flag N/A

Override-Rating-Group

This AVP is used to override the value of Rating group configured in the charging action specified by Charging-Action-Name.

Vendor ID 9

VSA Type 132024

AVP Type UINT32

AVP Flag N/A

Override-Rule-Name

Specifies the name of the rule (predefined or static) for which override values are sent. This AVP may be included more than once if the override values apply for multiple rules. Charging-Action-Name and Exclude-Rule AVPs should not be sent and will be ignored if this AVP is present.

Vendor ID 9

VSA Type 132018

AVP Type OCTETSTRING

AVP Flag N/A

Override-Service-Identifier

This AVP is used to override the value of Service Identifier configured in the charging action.

Vendor ID 9

VSA Type 132023

AVP Type UINT32

AVP Flag N/A

Override-Tos-Direction

This AVP indicates the Override Type of Service (ToS) direction. Value 0 indicates Uplink direction, 1 denotes Downlink direction, 2 denotes both Uplink and Downlink. If AVP is not present it denotes both Uplink and Downlink.

Vendor ID 9

VSA Type 132047

AVP Type ENUM

Supported enumerated value(s):

0 UPLINK_DIRECTION

1 DOWNLINK_DIRECTION

2 BIDIRECTIONAL

AVP Flag N/A

Override-Tos-Value

This AVP is of type grouped and is used to override IP ToS value. This AVP may be included more than once if different ToS value needs to be overridden for uplink and downlink direction.

Vendor ID 9

VSA Type 132046

AVP Type GROUPED

Supported group value(s):

[OVERRIDE_TOS_DIRECTION]

[OVERRIDE_TOS_VALUE_STANDARD]

[OVERRIDE_TOS_VALUE_CUSTOM]

AVP Flag N/A

Override-Tos-Value-Custom

This AVP specifies the custom ToS value. Customized value can be a decimal from 0 to 63. This AVP will be present only when Override-Tos-Value-standard is not provided.

Vendor ID 9

VSA Type 132049

AVP Type UINT32

AVP Flag N/A

Override-Tos-Value-Standard

This AVP specifies the standard ToS value. Valid standard value can be af11 or af12 or af13 or af21 or af22 or af23 or af31 or af32 or af33 or af41 or af42 or af43 or be or ef, since these are the only standard ToS values configured through CLI as per RFC 2597. This AVP will be present only if Override-Tos-Value-Custom AVP is not present.

Vendor ID 9

VSA Type 132048

AVP Type ENUM

Supported enumerated value(s):

0 be

10 af11

12 af12

14 af13

18 af21

20 af22

22 af23

26 af31

28 af32

30 af33

34 af41

36 af42

38 af43

46 ef

AVP Flag N/A

Owner-Id

Owner-Id

Vendor ID 9

VSA Type 131102

AVP Type OCTETSTRING

AVP Flag M

Owner-Name

Owner-Name

Vendor ID 9

VSA Type 131103

AVP Type OCTETSTRING

AVP Flag M

PC-Digest-Algorithm

PC-Digest-Algorithm

Vendor ID 4491

VSA Type 204

AVP Type OCTETSTRING

AVP Flag M

PC-Digest-Auth-Param

PC-Digest-Auth-Param

Vendor ID 4491

VSA Type 205

AVP Type OCTETSTRING

AVP Flag M

PC-Digest-Domain

PC-Digest-Domain

Vendor ID 4491

VSA Type 206

AVP Type OCTETSTRING

AVP Flag M

PC-Digest-HA1

PC-Digest-HA1

Vendor ID 4491

VSA Type 207

AVP Type OCTETSTRING

AVP Flag M

PC-Digest-QoP

PC-Digest-QoP

Vendor ID 4491

VSA Type 208

AVP Type OCTETSTRING

AVP Flag M

PC-Digest-Realm

PC-Digest-Realm

Vendor ID 4491

VSA Type 209

AVP Type OCTETSTRING

AVP Flag M

PC-SIP-Digest-Authenticate

PC-SIP-Digest-Authenticate

Vendor ID 4491

VSA Type 228

AVP Type GROUPED

Supported group value(s):

[PC_DIGEST_REALM]

[PC_DIGEST_DOMAIN]

[PC_DIGEST_ALGORITHM]

[PC_DIGEST_QOP]

[PC_DIGEST_HA1]

[PC_DIGEST_AUTH_PARAM]

AVP Flag M

PCC-Rule-Status

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

Vendor ID 10415

VSA Type 1019

AVP Type ENUM

Supported enumerated value(s):

0 ACTIVE

1 INACTIVE

2 TEMPORARILY_INACTIVE

10 ACTIVE_WITHOUT_CREDIT_CONTROL

AVP Flag M

PCRF-Correlation-Id

PCRF-Correlation-Id

Vendor ID 9

VSA Type 132043

AVP Type OCTETSTRING

AVP Flag N/A

PCSCF-Restoration-Indication

This AVP indicates to the PCEF that a P-CSCF Restoration is requested.

Vendor ID 10415

VSA Type 2826

AVP Type UINT32

AVP Flag N/A

PDFID

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

Vendor ID 24757

VSA Type 26

AVP Type OCTETSTRING

AVP Flag M

PDG-Address

This AVP contains IP address of the PDG.

Vendor ID 10415

VSA Type 895

AVP Type ADDRESS

AVP Flag M

PDG-Charging-Id

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

Vendor ID 10415

VSA Type 896

AVP Type UINT32

AVP Flag M

PDN-Connection-Charging-Id

PDN-Connection-Charging-Id

Vendor ID 10415

VSA Type 2050

AVP Type UINT32

AVP Flag M

PDN-Connection-ID

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

Vendor ID 10415

VSA Type 2050

AVP Type UINT32

AVP Flag M

PDN-GW-Address

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

Vendor ID 10415

VSA Type 6041

AVP Type ADDRESS

AVP Flag M

PDN-GW-Allocation-Type

PDN-GW-Allocation-Type

Vendor ID 10415

VSA Type 1438

AVP Type ENUM

Supported enumerated value(s):

0 STATIC

1 DYNAMIC

AVP Flag M

PDN-GW-Identity

PDN-GW-Identity

Vendor ID 10415

VSA Type 6044

AVP Type GROUPED

Supported group value(s):

[PDN_GW_ADDRESS]

[PDN_GW_NAME]

AVP Flag M

PDN-GW-Name

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

Vendor ID 10415

VSA Type 6042

AVP Type UTF8STRING

AVP Flag M

PDN-Type

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

Vendor ID 10415

VSA Type 1456

AVP Type ENUM

Supported enumerated value(s):

0 IPv4

1 IPv6

2 IPv4v6

AVP Flag M

PDP-Address

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

Vendor ID 10415

VSA Type 1227

AVP Type ADDRESS

AVP Flag M

PDP-Context

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

Vendor ID 10415

VSA Type 1469

AVP Type GROUPED

Supported group value(s):

[CONTEXT_IDENTIFIER]

[PDP_TYPE]

[QOS_SUBSCRIBED]

[VPLMN_DYNAMIC_ADDRESS_ALLOWED]

[SERVICE_SELECTION]

[3GPP_CHARGING_CHARACTERISTICS]

AVP Flag M

PDP-Context-Type

This AVP contains the type of a PDP Context.

Vendor ID 10415

VSA Type 1247

AVP Type ENUM

Supported enumerated value(s):

0 PRIMARY

1 SECONDARY

AVP Flag M

PDP-Session-Operation

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

Vendor ID 10415

VSA Type 1015

AVP Type ENUM

Supported enumerated value(s):

0 PDP-SESSION-TERMINATION

AVP Flag M

PDP-Type

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

Vendor ID 10415

VSA Type 1470

AVP Type OCTETSTRING

AVP Flag M

PGW-Type

Type of P-GW of current flow.

Vendor ID 10415

VSA Type 7002

AVP Type UINT32

AVP Flag M

PLMN-Client

PLMN-Client

Vendor ID 10415

VSA Type 1482

AVP Type ENUM

Supported enumerated value(s):

0 BROADCAST_SERVICE

1 O_AND_M_HPLMN

2 O_AND_M_VPLMN

3 ANONYMOUS_LOCATION

4 TARGET_UE_SUBSCRIBED_SERVICE

AVP Flag M

PMIP6-MAG-Address

This AVP contains IP address of MAG.

Vendor ID 10415

VSA Type 6070

AVP Type ADDRESS

AVP Flag M

PS-Append-Free-Format-Data

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

Vendor ID 10415

VSA Type 867

AVP Type ENUM

Supported enumerated value(s):

0 APPEND

1 OVERWRITE

AVP Flag M

PS-Free-Format-Data

This AVP holds online charging session specific data.

Vendor ID 10415

VSA Type 866

AVP Type OCTETSTRING

AVP Flag M

PS-Furnish-Charging-Information

This grouped AVP contains online charging session specific information.

Vendor ID 10415

VSA Type 865

AVP Type GROUPED

Supported group value(s):

[3GPP_CHARGING_ID]

[PS_FREE_FORMAT_DATA]

[PS_APPEND_FREE_FORMAT_DATA]

AVP Flag M

PS-Information

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

Vendor ID 10415

VSA Type 874

AVP Type GROUPED

Supported group value(s):

[3GPP_CHARGING_ID]

[3GPP_PDP_TYPE]

[PDP_ADDRESS]

[3GPP_GPRS_QOS_NEGOTIATED_PROFILE]

[3GPP_SGSN_ADDRESS]

[3GPP_GGSN_ADDRESS]

[3GPP_CG_ADDRESS]

[3GPP_IMSI_MCC_MNC]

[3GPP_GGSN_MCC_MNC]

[3GPP_NSAPI]

[CALLED_STATION_ID]

[3GPP_SESSION_STOP_INDICATOR]

[3GPP_SELECTION_MODE]

[3GPP_CHARGING_CHARACTERISTICS]

[3GPP_SGSN_MCC_MNC]

[3GPP_RAT_TYPE]

[PDP_CONTEXT_TYPE]

AVP Flag M

PSCID

This AVP contains the P-GW Session Correlation ID.

Vendor ID 10415

VSA Type 1450

AVP Type OCTETSTRING

AVP Flag M

PUA-Flags

The PUA-Flags AVP contains a bit mask.

Vendor ID 10415

VSA Type 1442

AVP Type UINT32

AVP Flag M

PUR-Flags

PUR-Flags

Vendor ID 10415

VSA Type 1635

AVP Type UINT32

AVP Flag N/A

Packet-Data-Flow-Info

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

Vendor ID 24757

VSA Type 405

AVP Type GROUPED

Supported group value(s):

[PDFID]

[PRECEDENCE]

[FLOW_DESCRIPTION]

[WIMAX_QOS_INFORMATION]

AVP Flag M

Packet-Filter-Content

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

Vendor ID 10415

VSA Type 1059

AVP Type IPFILTERRULE

AVP Flag M

Packet-Filter-Identifier

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

Vendor ID 10415

VSA Type 1060

AVP Type OCTETSTRING

AVP Flag M

Packet-Filter-Information

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

Vendor ID 10415

VSA Type 1061

AVP Type GROUPED

Supported group value(s):

[PACKET_FILTER_IDENTIFIER]

[PRECEDENCE]

[PACKET_FILTER_CONTENT]

[TOS_TRAFFIC_CLASS]

[SECURITY_PARAMETER_INDEX]

[FLOW_LABEL]

[FLOW_DIRECTION]

AVP Flag M

Packet-Filter-Operation

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

Vendor ID 10415

VSA Type 1062

AVP Type ENUM

Supported enumerated value(s):

0 DELETION

1 ADDITION

2 MODIFICATION

AVP Flag M

Packet-Interval

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

Vendor ID 24757

VSA Type 414

AVP Type UINT32

AVP Flag M

Packet-Size

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

Vendor ID 24757

VSA Type 415

AVP Type UINT32

AVP Flag M

Paging-Group-Id

Paging-Group-Id

Vendor ID 0

VSA Type 10001

AVP Type UINT32

AVP Flag M

Path

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

Vendor ID 10415

VSA Type 640

AVP Type OCTETSTRING

AVP Flag N/A

Physical-Access-Id

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

Vendor ID 0

VSA Type 313

AVP Type UTF8STRING

AVP Flag M

Policy-Map-Definition

Policy-Map-Definition

Vendor ID 9

VSA Type 131075

AVP Type GROUPED

Supported group value(s):

[POLICY_MAP_NAME]

[POLICY_MAP_TYPE]

[POLICY_MAP_REPLACE]

[POLICY_MAP_MATCH_REMOVE]

[POLICY_MAP_MATCH_INSTALL]

AVP Flag M

Policy-Map-Install

Policy-Map-Install

Vendor ID 9

VSA Type 131179

AVP Type GROUPED

Supported group value(s):

[POLICY_MAP_DEFINITION]

AVP Flag M

Policy-Map-Match

Policy-Map-Match

Vendor ID 9

VSA Type 131090

AVP Type GROUPED

Supported group value(s):

[MATCH_STRING]

[ATTRIBUTE_STRING]

AVP Flag M

Policy-Map-Match-Install

Policy-Map-Match-Install

Vendor ID 9

VSA Type 131166

AVP Type GROUPED

Supported group value(s):

[POLICY_MAP_MATCH]

AVP Flag M

Policy-Map-Match-Remove

Policy-Map-Match-Remove

Vendor ID 9

VSA Type 131167

AVP Type GROUPED

Supported group value(s):

[POLICY_MAP_MATCH]

AVP Flag M

Policy-Map-Name

Policy-Map-Name

Vendor ID 9

VSA Type 131089

AVP Type OCTETSTRING

AVP Flag M

Policy-Map-Remove

Policy-Map-Remove

Vendor ID 9

VSA Type 131180

AVP Type GROUPED

Supported group value(s):

[POLICY_MAP_NAME]

AVP Flag M

Policy-Map-Replace

Policy-Map-Replace

Vendor ID 9

VSA Type 131168

AVP Type ENUM

Supported enumerated value(s):

0 DISABLED

1 ENABLED

AVP Flag M

Policy-Map-Type

Policy-Map-Type

Vendor ID 9

VSA Type 131165

AVP Type ENUM

Supported enumerated value(s):

0 URL_MAP

1 HEADER_MAP

2 METHOD_MAP

3 ATTRIBUTE_MAP

AVP Flag M

Policy-Preload-Error-Code

Policy-Preload-Error-Code

Vendor ID 9

VSA Type 131189

AVP Type ENUM

Supported enumerated value(s):

0 INCONSISTENT_PRELOAD_DATA

1 MANDATORY_AVP_MISSING

2 FAILURE_TO_ENFORCE

3 WRONG_ORDER

4 CONFLICT_WITH_STATIC_CONFIG

AVP Flag M

Policy-Preload-Object-Type

Policy-Preload-Object-Type

Vendor ID 9

VSA Type 131121

AVP Type ENUM

Supported enumerated value(s):

0 POLICY_MAP

1 BILLING_POLICY

2 CONTENT

3 SERVICE

4 BILLING_PLAN

5 DOMAIN_GROUP

6 HEADER_INSERT

7 HEADER_GROUP

8 QOS_PROFILE

AVP Flag M

Policy-Preload-Req-Type

Policy-Preload-Req-Type

Vendor ID 9

VSA Type 131120

AVP Type ENUM

Supported enumerated value(s):

0 POLICY_PRELOAD_REQ

1 POLICY_PRELOAD_RESP

2 POLICY_PRELOAD_PUSH

3 POLICY_PRELOAD_PUSH_ACK

AVP Flag M

Port-Limit

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

Vendor ID 0

VSA Type 62

AVP Type UINT32

AVP Flag M

Port-Number

Port-Number

Vendor ID 13091

VSA Type 455

AVP Type UINT32

AVP Flag N/A

PRA-Install

Used to provision a list of new or updated Presence Reporting Area(s) for an IP-CAN session

Vendor ID 10415

VSA Type 2845

AVP Type GROUPED

AVP Flag N/A

PRA-Remove

Used to stop the reporting of a list of Presence Reporting Area(s) for an IP-CAN session.

Vendor ID 10415

VSA Type 2846

AVP Type GROUPED

AVP Flag N/A

Pre-emption-Capability

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

Vendor ID 10415

VSA Type 1047

AVP Type ENUM

Supported enumerated value(s):

0 PRE-EMPTION_CAPABILITY_ENABLED

1 PRE-EMPTION_CAPABILITY_DISABLED

AVP Flag M

Pre-emption-Vulnerability

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

Vendor ID 10415

VSA Type 1048

AVP Type ENUM

Supported enumerated value(s):

0 PRE-EMPTION_VULNERABILITY_ENABLED

1 PRE-EMPTION_VULNERABILITY_DISABLED

AVP Flag M

Precedence

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

Vendor ID 10415

VSA Type 1010

AVP Type UINT32

AVP Flag M

Preload-Completion-Status

Preload-Completion-Status

Vendor ID 9

VSA Type 131122

AVP Type ENUM

Supported enumerated value(s):

0 ONGOING

1 COMPLETE

AVP Flag M

Presence-Reporting-Area-Elements-List

This AVP contains, for a UE-dedicated presence area, the elements of the Presence Reporting Area. For a core network pre-configured presence reporting area, the element list shall not be present. When the presence area is UE-dedicated, the PCRF may acquire the presence reporting area information from the SPR.

Vendor ID 10415

VSA Type 2820

AVP Type OCTETSTRING

AVP Flag N/A

Presence-Reporting-Area-Identifier

This AVP defines a unique identifier for presence reporting area or presence reporting area set.

Vendor ID 10415

VSA Type 2821

AVP Type OCTETSTRING

AVP Flag N/A

Presence-Reporting-Area-Information

This AVP contains the information which describes a Presence Reporting Area.

Vendor ID 10415

VSA Type 2822

AVP Type GROUPED

Supported group value(s):

[PRESENCE_REPORTING_AREA_IDENTIFIER]

[PRESENCE_REPORTING_AREA_STATUS]

[PRESENCE_REPORTING_AREA_ELEMENTS_LIST]

AVP Flag N/A

Presence-Reporting-Area-Status

This AVP indicates the status of UE for presence reporting area or the status of the presence reporting area.

Vendor ID 10415

VSA Type 2823

AVP Type UINT32

AVP Flag N/A

Primary-Charging-Collection-Function-Name

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

Vendor ID 10415

VSA Type 621

AVP Type DIAMURI

AVP Flag M

Primary-Event-Charging-Function-Name

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

Vendor ID 10415

VSA Type 619

AVP Type DIAMURI

AVP Flag M

Priority

Priority

Vendor ID 9

VSA Type 131201

AVP Type UINT32

AVP Flag N/A

Priority-Level

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

Vendor ID 10415

VSA Type 1046

AVP Type UINT32

AVP Flag M

Priviledged-Sender-Indication

Priviledged-Sender-Indication

Vendor ID 10415

VSA Type 652

AVP Type ENUM

Supported enumerated value(s):

0 NOT_PRIVILEDGED_SENDER

1 PRIVILEDGED_SENDER

AVP Flag N/A

Product-Name

This AVP contains the vendor assigned name for the product.

Vendor ID 0

VSA Type 269

AVP Type UTF8STRING

AVP Flag N/A

Profile-Name

Profile-Name.

Vendor ID 9

VSA Type 132090

AVP Type OCTETSTRING

AVP Flag N/A

Protocol-ID

Protocol-ID

Vendor ID 9

VSA Type 131148

AVP Type UINT32

AVP Flag N/A

Proxy-Host

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

Vendor ID 0

VSA Type 280

AVP Type DIAMIDENT

AVP Flag M

Proxy-Info

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

Vendor ID 0

VSA Type 284

AVP Type GROUPED

Supported group value(s):

[PROXY_HOST]

[PROXY_STATE]

AVP Flag M

Proxy-State

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

Vendor ID 0

VSA Type 33

AVP Type OCTETSTRING

AVP Flag M

Pseudonym-Indicator

This ABP indicates whether or not a pseudonym is requested.

Vendor ID 10415

VSA Type 2519

AVP Type ENUM

Supported enumerated value(s):

0 PSEUDONYM_NOT_REQUESTED

1 PSEUDONYM_REQUESTED

AVP Flag M

Public-Identity

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

Vendor ID 10415

VSA Type 601

AVP Type UTF8STRING

AVP Flag M

QoS-Capability

QoS-Capability

Vendor ID 0

VSA Type 6063

AVP Type GROUPED

Supported group value(s):

[QOS_PROFILE_TEMPLATE]

[VENDOR_SPECIFIC_QOS_PROFILE_TEMPLATE]

AVP Flag M

QoS-Class

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

Vendor ID 10415

VSA Type 1017

AVP Type ENUM

Supported enumerated value(s):

0 Traffic_Class_A

1 Traffic_Class_B

2 Traffic_Class_C

3 Traffic_Class_D

4 Traffic_Class_E

5 Traffic_Class_F

AVP Flag M

QoS-Class-Identifier

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

Vendor ID 10415

VSA Type 1028

AVP Type ENUM

Supported enumerated value(s):

1 TRAFFIC_CLASS_A

2 TRAFFIC_CLASS_B

3 TRAFFIC_CLASS_C

4 TRAFFIC_CLASS_D

5 TRAFFIC_CLASS_E

6 TRAFFIC_CLASS_F

7 TRAFFIC_CLASS_G

8 TRAFFIC_CLASS_H

9 TRAFFIC_CLASS_I

AVP Flag M

QoS-Group-Rule-Definition

QoS-Group-Rule-Definition

Vendor ID 9

VSA Type 132003

AVP Type GROUPED

Supported group value(s):

[QOS_GROUP_RULE_NAME]

[QOS_INFORMATION]

[FLOW_STATUS]

[REDIRECT_SERVER]

[MONITORING_KEY]

[PRECEDENCE]

AVP Flag N/A

QoS-Group-Rule-Install

QoS-Group-Rule-Install

Vendor ID 9

VSA Type 132001

AVP Type GROUPED

Supported group value(s):

[QOS_GROUP_RULE_DEFINITION]

AVP Flag N/A

QoS-Group-Rule-Name

QoS-Group-Rule-Name

Vendor ID 9

VSA Type 132004

AVP Type OCTETSTRING

AVP Flag N/A

QoS-Group-Rule-Remove

QoS-Group-Rule-Remove

Vendor ID 9

VSA Type 132002

AVP Type GROUPED

Supported group value(s):

[QOS_GROUP_RULE_NAME]

AVP Flag N/A

QoS-Information

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

Vendor ID 10415

VSA Type 1016

AVP Type GROUPED

Supported group value(s):

[QOS_CLASS_IDENTIFIER]

[MAX_REQUESTED_BANDWIDTH_UL]

[MAX_REQUESTED_BANDWIDTH_DL]

[EXTENDED-MAX-REQUESTED-BW-UL]

[EXTENDED-MAX-REQUESTED-BW-DL]

[GUARANTEED_BITRATE_UL]

[GUARANTEED_BITRATE_DL]

[EXTENDED-GBR-UL]

[EXTENDED-GBR-DL]

[BEARER_IDENTIFIER]

[ALLOCATION_RETENTION_PRIORITY]

[APN_AGGREGATE_MAX_BITRATE_UL]

[APN_AGGREGATE_MAX_BITRATE_DL]

[EXTENDED-APN-AMBR-UL]

[EXTENDED-APN-AMBR-DL]

AVP Flag M

QoS-Level

QoS-Level

Vendor ID 9

VSA Type 132011

AVP Type ENUM

Supported enumerated value(s):

1 SUBSCRIBER_LEVEL

AVP Flag N/A

QoS-Negotiation

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

Vendor ID 10415

VSA Type 1029

AVP Type ENUM

Supported enumerated value(s):

0 NO_QoS_NEGOTIATION

1 QoS_NEGOTIATION_SUPPORTED

AVP Flag M

QoS-Profile-Template

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

Vendor ID 0

VSA Type 6067

AVP Type UINT32

AVP Flag M

QoS-Rate-Limit

QoS-Rate-Limit

Vendor ID 9

VSA Type 131173

AVP Type GROUPED

Supported group value(s):

[MAX_BANDWIDTH]

[MAX_BURST_SIZE]

[RATE_LIMIT_CONFORM_ACTION]

[RATE_LIMIT_EXCEED_ACTION]

AVP Flag M

QoS-Rate-Limit-DL

QoS-Rate-Limit-DL

Vendor ID 9

VSA Type 131172

AVP Type GROUPED

Supported group value(s):

[QOS_RATE_LIMIT]

AVP Flag M

QoS-Rate-Limit-UL

QoS-Rate-Limit-UL

Vendor ID 9

VSA Type 131171

AVP Type GROUPED

Supported group value(s):

[QOS_RATE_LIMIT]

AVP Flag M

QoS-Resource-Request

Resource requested by UE to PCRF.

Vendor ID 10415

VSA Type 6106

AVP Type GROUPED

Supported group value(s):

[QOS_RESOURCE_IDENTIFIER]

[QOS_RESOURCE_OPERATION]

[TFT_PACKET_FILTER_INFORMATION]

[QOS_INFORMATION]

AVP Flag M

QoS-Resources

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

Vendor ID 0

VSA Type 6065

AVP Type GROUPED

Supported group value(s):

[EXTENDED_QOS_FILTER_RULE]

AVP Flag M

QoS-Rule-Base-Name

This AVP indicates the name of a predefined group of charging rules residing at the TPF.

Vendor ID 10415

VSA Type 1074

AVP Type UTF8STRING

AVP Flag M

QoS-Rule-Definition

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

Vendor ID 10415

VSA Type 1053

AVP Type GROUPED

Supported group value(s):

[QOS_RULE_NAME]

[FLOW_INFORMATION]

[FLOW_DESCRIPTION]

[QOS_INFORMATION]

[PRECEDENCE]

AVP Flag M

QoS-Rule-Install

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

Vendor ID 10415

VSA Type 1051

AVP Type GROUPED

Supported group value(s):

[QOS_RULE_DEFINITION]

[QOS_RULE_NAME]

[QOS_RULE_BASE_NAME]

[TUNNEL_INFORMATION]

[ACCESS_NETWORK_CHARGING_IDENTIFIER_VALUE]

[RESOURCE_ALLOCATION_NOTIFICATION]

[RULE_ACTIVATION_TIME]

[RULE_DEACTIVATION_TIME]

AVP Flag M

QoS-Rule-Name

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

Vendor ID 10415

VSA Type 1054

AVP Type OCTETSTRING

AVP Flag M

QoS-Rule-Remove

Used to remove QoS rules from a Gateway Control Session.

Vendor ID 10415

VSA Type 1052

AVP Type GROUPED

Supported group value(s):

[QOS_RULE_NAME]

[QOS_RULE_BASE_NAME]

AVP Flag M

QoS-Rule-Report

Report the status of QoS rules.

Vendor ID 10415

VSA Type 1055

AVP Type GROUPED

Supported group value(s):

[QOS_RULE_NAME]

[QOS_RULE_BASE_NAME]

[PCC_RULE_STATUS]

[RULE_FAILURE_CODE]

AVP Flag M

QoS-Subscribed

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

Vendor ID 10415

VSA Type 1404

AVP Type OCTETSTRING

AVP Flag M

QoS-Upgrade

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

Vendor ID 10415

VSA Type 1030

AVP Type ENUM

Supported enumerated value(s):

0 QoS_UPGRADE_NOT_SUPPORTED

1 QoS_UPGRADE_SUPPORTED

AVP Flag M

RACS-Contact-Point

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

Vendor ID 0

VSA Type 351

AVP Type DIAMIDENT

AVP Flag M

RAI

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

Vendor ID 10415

VSA Type 909

AVP Type UTF8STRING

AVP Flag M

RAN-End-Timestamp

It holds the time in UTC format of the volume container reported was collected, the end time of the reported usage.

Vendor ID 10415

VSA Type 1301

AVP Type TIME

AVP Flag N/A

RAN-Secondary-RAT-Usage-Report

It contains the volume count as reported by the RAN for the secondary RAT including the time of the report.

Vendor ID 10415

VSA Type 1302

AVP Type GROUPED

Supported group value(s):

[SECONDARY_RAT_TYPE]

[RAN_START_TIMESTAMP]

[RAN_END_TIMESTAMP]

[ACCOUNTING_INPUT_OCTETS]

[ACCOUNTING_OUTPUT_OCTETS]

AVP Flag N/A

RAN-Start-Timestamp

It holds the time in UTC format of the volume container reported was collected, the start time of the reported usage.

Vendor ID 10415

VSA Type 1303

AVP Type TIME

AVP Flag N/A

RAN-NAS-Release-Cause

RAN-NAS-Release-Cause

Vendor ID 10415

VSA Type 2819

AVP Type OCTETSTRING

AVP Flag N/A

RANAP-Cause

RANAP-Cause

Vendor ID 10415

VSA Type 4303

AVP Type UINT32

AVP Flag M

RAND

This AVP contains the RAND (EAP Authentication Vector).

Vendor ID 10415

VSA Type 1447

AVP Type OCTETSTRING

AVP Flag M

RAR-Flags

This AVP contains the bit 1 set to indicate that the AAA server requests the execution of HSS-based P-CSCF restoration procedures for WLAN.

Vendor ID 10415

VSA Type 1522

AVP Type UINT32

AVP Flag N/A

RAS-Id

This AVP contains the RAS identifier.

Vendor ID 0

VSA Type 10000

AVP Type UINT32

AVP Flag M

RAT-Frequency-Selection-Priority

This AVP contains the RAT frequency selection priority.

Vendor ID 10415

VSA Type 1440

AVP Type UINT32

AVP Flag M

RAT-Type

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

Vendor ID 10415

VSA Type 1032

AVP Type ENUM

Supported enumerated value(s):

0 WLAN

1 VIRTUAL

1000 UTRAN

1001 GERAN

1002 GAN

1003 HSPA_EVOLUTION

1004 EUTRAN

1005 NB-IoT

2000 CDMA2000_1X

2001 HRPD

2002 UMB

2003 EHRPD

AVP Flag M

RR-Bandwidth

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

Vendor ID 10415

VSA Type 521

AVP Type UINT32

AVP Flag M

RS-Bandwidth

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

Vendor ID 10415

VSA Type 522

AVP Type UINT32

AVP Flag M

Radius-Attribute-Type

Radius-Attribute-Type

Vendor ID 9

VSA Type 131224

AVP Type UINT32

AVP Flag N/A

Radius-Vsa-Subattribute-Type

Radius-Vsa-Subattribute-Type

Vendor ID 9

VSA Type 131226

AVP Type UINT32

AVP Flag N/A

Radius-Vsa-Vendor-Id

Radius-Vsa-Vendor-Id

Vendor ID 9

VSA Type 131225

AVP Type UINT32

AVP Flag N/A

Rate-Limit-Action

Rate-Limit-Action

Vendor ID 9

VSA Type 131177

AVP Type ENUM

Supported enumerated value(s):

0 FORWARD

1 DROP

2 MARK_DSCP

AVP Flag M

Rate-Limit-Conform-Action

Rate-Limit-Conform-Action

Vendor ID 9

VSA Type 131175

AVP Type GROUPED

Supported group value(s):

[RATE_LIMIT_ACTION]

[DSCP]

AVP Flag M

Rate-Limit-Exceed-Action

Rate-Limit-Exceed-Action

Vendor ID 9

VSA Type 131176

AVP Type GROUPED

Supported group value(s):

[RATE_LIMIT_ACTION]

[DSCP]

AVP Flag M

Rating-Group

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

Vendor ID 0

VSA Type 432

AVP Type UINT32

AVP Flag M

Re-Auth-Request-Type

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

Vendor ID 0

VSA Type 285

AVP Type ENUM

Supported enumerated value(s):

0 AUTHORIZE_ONLY

1 AUTHORIZE_AUTHENTICATE

AVP Flag M

Re-Synchronization-Info

This AVP contains the concatenation of RAND and AUTS.

Vendor ID 10415

VSA Type 6014

AVP Type UINT32

AVP Flag M

Reachability-Information

Reachability-Information

Vendor ID 10415

VSA Type 3140

AVP Type UINT32

AVP Flag M

Reachability-Type

Reachability-Type

Vendor ID 10415

VSA Type 3132

AVP Type UINT32

AVP Flag M

Real-Time-Tariff-Information

Real-Time-Tariff-Information

Vendor ID 10415

VSA Type 2305

AVP Type GROUPED

Supported group value(s):

[TARIFF_XML]

AVP Flag M

Reason-Code

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

Vendor ID 10415

VSA Type 616

AVP Type ENUM

Supported enumerated value(s):

0 PERMANENT_TERMINATION

1 NEW_SERVER_ASSIGNED

2 SERVER_CHANGE

3 REMOVE_S-CSCF

AVP Flag M

Reason-Info

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

Vendor ID 10415

VSA Type 617

AVP Type UTF8STRING

AVP Flag M

Record-Route

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

Vendor ID 10415

VSA Type 646

AVP Type OCTETSTRING

AVP Flag N/A

Redirect-Address-Type

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

Vendor ID 0

VSA Type 433

AVP Type ENUM

Supported enumerated value(s):

0 IPv4-Address

1 IPv6-Address

2 URL

3 SIP-URI

AVP Flag M

Redirect-Host

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

Vendor ID 0

VSA Type 292

AVP Type OCTETSTRING

AVP Flag M

Redirect-Host-Usage

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

Vendor ID 0

VSA Type 261

AVP Type ENUM

Supported enumerated value(s):

0 DONT_CACHE

1 ALL_SESSION

2 ALL_REALM

3 REALM_AND_APPLICATION

4 ALL_APPLICATION

5 ALL_HOST

6 ALL_USER

AVP Flag M

Redirect-Information

This AVP contains the address information of the redirect server to which the detected application traffic is sent.

Vendor ID 10415

VSA Type 1085

AVP Type GROUPED

Supported group value(s):

[REDIRECT_SUPPORT]

[REDIRECT_ADDRESS_TYPE]

[REDIRECT_SERVER_ADDRESS]

AVP Flag N/A

Redirect-Max-Cache-Time

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

Vendor ID 0

VSA Type 262

AVP Type UINT32

AVP Flag M

Redirect-Server

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

Vendor ID 0

VSA Type 434

AVP Type GROUPED

Supported group value(s):

[REDIRECT_ADDRESS_TYPE]

[REDIRECT_SERVER_ADDRESS]

AVP Flag M

Redirect-Server-Address

This AVP contains address of the redirect server.

Vendor ID 0

VSA Type 435

AVP Type UTF8STRING

AVP Flag M

Redirect-Support

This AVP indicates whether redirection is disabled or enabled for an ADC rule. If the redirection is enabled, the Traffic Detection Function (TDF) will redirect the detected application's traffic to the redirect address provided through Redirect-Information AVP.

Vendor ID 10415

VSA Type 1086

AVP Type ENUM

Supported enumerated value(s):

0 REDIRECTION_DISABLED

1 REDIRECTION_ENABLED

AVP Flag N/A

Refund-Policy

Refund-Policy

Vendor ID 9

VSA Type 131109

AVP Type OCTETSTRING

AVP Flag M

Regional-Subscription-Zone-Code

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

Vendor ID 10415

VSA Type 1446

AVP Type OCTETSTRING

AVP Flag M

Relative-URL

Relative-URL

Vendor ID 9

VSA Type 131198

AVP Type ENUM

Supported enumerated value(s):

0 DISABLED

1 ENABLED

AVP Flag M

Replicate-Session

Replicate-Session

Vendor ID 9

VSA Type 131132

AVP Type UINT32

AVP Flag N/A

Replicate-Session-Delay

Replicate-Session-Delay

Vendor ID 9

VSA Type 131133

AVP Type UINT32

AVP Flag N/A

Reply-Message

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

Vendor ID 0

VSA Type 18

AVP Type UTF8STRING

AVP Flag M

Reporting-Level

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

Vendor ID 10415

VSA Type 1011

AVP Type ENUM

Supported enumerated value(s):

0 SERVICE_IDENTIFIER_LEVEL

1 RATING_GROUP_LEVEL

2 SPONSORED_CONNECTIVITY_LEVEL

AVP Flag M

Requested-Action

The action requested when the CC_Request_Type is EVENT_REQUEST.

Vendor ID 0

VSA Type 436

AVP Type ENUM

Supported enumerated value(s):

0 DIRECT_DEBITING

1 REFUND_ACCOUNT

2 CHECK_BALANCE

3 PRICE_ENQUIRY

4 LOCATION_UPDATE

AVP Flag M

Requested-Domain

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

Vendor ID 0

VSA Type 706

AVP Type ENUM

Supported enumerated value(s): none

AVP Flag M

Requested-EUTRAN-Authentication-Info

This AVP contains the EU Tran authentication information.

Vendor ID 10415

VSA Type 6010

AVP Type GROUPED

Supported group value(s):

[NUMBER_OF_REQUESTED_VECTORS]

[IMMEDIATE_RESPONSE_PREFERRED]

[RE_SYNCHRONIZATION_INFO]

AVP Flag M

Requested-GERAN-Authentication-Info

This AVP contains GE RAN authentication information.

Vendor ID 10415

VSA Type 6012

AVP Type GROUPED

Supported group value(s):

[NUMBER_OF_REQUESTED_VECTORS]

[IMMEDIATE_RESPONSE_PREFERRED]

[RE_SYNCHRONIZATION_INFO]

AVP Flag M

Requested-Information

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

Vendor ID 13019

VSA Type 353

AVP Type ENUM

Supported enumerated value(s):

0 NASS-USER-ID

1 LOCATION-INFORMATION

2 RACS-CONTACT-POINT

3 ACCESS-NETWORK-TYPE

4 TERMINAL-TYPE

5 LOGICAL-ACCESS-ID

6 PHYSICAL-ACCESS-ID

7 ACCESS-NETWORK-TYPE-RESERVED

8 INITIAL-GATE-SETTING-RESERVED

9 QOS-PROFILE-RESERVED

10 IP-CONNECTIVITY-STATUS-RESERVED

AVP Flag M

Requested-Party-Address

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

Vendor ID 10415

VSA Type 1251

AVP Type UTF8STRING

AVP Flag M

Requested-QoS

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

Vendor ID 5535

VSA Type 1010

AVP Type GROUPED

Supported group value(s):

[QOS_CLASS]

[MIN_BANDWIDTH_UL]

[MIN_BANDWIDTH_DL]

AVP Flag M

Requested-Retransmission-Time

Requested-Retransmission-Time

Vendor ID 10415

VSA Type 3331

AVP Type TIME

AVP Flag N/A

Requested-Service-Unit

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

Vendor ID 0

VSA Type 437

AVP Type GROUPED

Supported group value(s):

[TARIFF_TIME_CHANGE]

[TARIFF_CHANGE_USAGE]

[CC_TIME]

[CC_MONEY]

[CC_TOTAL_OCTETS]

[CC_INPUT_OCTETS]

[CC_OUTPUT_OCTETS]

[CC_SERVICE_SPECIFIC_UNITS]

AVP Flag M

Requested-UTRAN-Authentication-Info

This AVP contains the UTRAN authentication information.

Vendor ID 10415

VSA Type 6011

AVP Type GROUPED

Supported group value(s):

[NUMBER_OF_REQUESTED_VECTORS]

[IMMEDIATE_RESPONSE_PREFERRED]

[RE_SYNCHRONIZATION_INFO]

AVP Flag M

Requested-UTRAN-GERAN-Authentication-Info

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

Vendor ID 10415

VSA Type 1409

AVP Type GROUPED

Supported group value(s):

[NUMBER_OF_REQUESTED_VECTORS]

[IMMEDIATE_RESPONSE_PREFERRED]

[RE_SYNCHRONIZATION_INFO]

AVP Flag M

Requesting-Node-Type

Requesting-Node-Type

Vendor ID 10415

VSA Type 1455

AVP Type ENUM

Supported enumerated value(s):

0 MME

1 SGSN

2 MME_SGSN

AVP Flag M

Required-Access-Info

Required-Access-Info

Vendor ID 10415

VSA Type 536

AVP Type ENUM

Supported enumerated value(s):

0 USER_LOCATION

1 MS_TIME_ZONE

AVP Flag N/A

Required-MBMS-Bearer-Capabilities

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

Vendor ID 10415

VSA Type 901

AVP Type UTF8STRING

AVP Flag M

Reservation-Class

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

Vendor ID 13019

VSA Type 456

AVP Type UINT32

AVP Flag N/A

Reservation-Priority

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

Vendor ID 13019

VSA Type 458

AVP Type ENUM

Supported enumerated value(s):

0 DEFAULT

1 PRIORITY-ONE

2 PRIORITY-TWO

3 PRIORITY-THREE

4 PRIORITY-FOUR

5 PRIORITY-FIVE

6 PRIORITY-SIX

7 PRIORITY-SEVEN

AVP Flag N/A

Resource-Allocation-Notification

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

Vendor ID 10415

VSA Type 1063

AVP Type ENUM

Supported enumerated value(s):

0 ENABLE_NOTIFICATION

AVP Flag M

Response-Time

Response-Time

Vendor ID 10415

VSA Type 2509

AVP Type ENUM

Supported enumerated value(s):

0 LOW_DELAY

1 DELAY_TOLERANT

AVP Flag M

Restoration-Info

This AVP contains the information related to a specific registration.

Vendor ID 10415

VSA Type 649

AVP Type GROUPED

Supported group value(s):

[PATH]

[CONTACT]

[SUBSCRIPTION_INFO]

AVP Flag N/A

Restoration-Priority

This attribute specifies the relative priority of the user when restoring PDN connections affected by an S-GW or P-GW failure/restart.

Vendor ID 10415

VSA Type 1663

AVP Type UINT32

AVP Flag N/A

Restriction-Filter-Rule

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

Vendor ID 0

VSA Type 438

AVP Type IPFILTERRULE

AVP Flag M

Result-Code

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

Vendor ID 0

VSA Type 268

AVP Type ENUM

Supported enumerated value(s):

1001 DIAMETER_MULTI_ROUND_AUTH

2001 DIAMETER_SUCCESS

2002 DIAMETER_LIMITED_SUCCESS

3001 DIAMETER_COMMAND_UNSUPPORTED

3002 DIAMETER_UNABLE_TO_DELIVER

3003 DIAMETER_REALM_NOT_SERVED

3004 DIAMETER_TOO_BUSY

3005 DIAMETER_LOOP_DETECTED

3006 DIAMETER_REDIRECT_INDICATION

3007 DIAMETER_APPLICATION_UNSUPPORTED

3008 DIAMETER_INVALID_HDR_BITS

3009 DIAMETER_INVALID_AVP_BITS

3010 DIAMETER_UNKNOWN_PEER

4001 DIAMETER_AUTHENTICATION_REJECTED

4002 DIAMETER_OUT_OF_SPACE

4003 ELECTION_LOST

4010 DIAMETER_END_USER_SERVICE_DENIED

4011 DIAMETER_CREDIT_CONTROL_NOT_APPLICABLE

4012 DIAMETER_CREDIT_LIMIT_REACHED

4212 DIAMETER_BALANCE_IS_ZERO

5001 DIAMETER_AVP_UNSUPPORTED

5002 DIAMETER_UNKNOWN_SESSION_ID

5003 DIAMETER_AUTHORIZATION_REJECTED

5004 DIAMETER_INVALID_AVP_VALUE

5005 DIAMETER_MISSING_AVP

5006 DIAMETER_RESOURCES_EXCEEDED

5007 DIAMETER_CONTRADICTING_AVPS

5008 DIAMETER_AVP_NOT_ALLOWED

5009 DIAMETER_AVP_OCCURS_TOO_MANY_TIMES

5010 DIAMETER_NO_COMMON_APPLICATION

5011 DIAMETER_UNSUPPORTED_VERSION

5012 DIAMETER_UNABLE_TO_COMPLY

5013 DIAMETER_INVALID_BIT_IN_HEADER

5014 DIAMETER_INVALID_AVP_LENGTH

5015 DIAMETER_INVALID_MESSAGE_LENGTH

5016 DIAMETER_INVALID_AVP_BIT_COMBO

5017 DIAMETER_NO_COMMON_SECURITY

5030 DIAMETER_USER_UNKNOWN

5031 DIAMETER_RATING_FAILED

AVP Flag M

Revalidation-Time

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

Vendor ID 10415

VSA Type 1042

AVP Type TIME

AVP Flag M

Roaming-Restricted-Due-To-Unsupported-Feature

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

Vendor ID 10415

VSA Type 1457

AVP Type ENUM

Supported enumerated value(s):

0 ROAMING_RESTRICTED_DUE_TO_UNSUPPORTED_FEATURE

AVP Flag M

Role-Of-Node

This AVP specifies the role of the AS/CSCF.

Vendor ID 10415

VSA Type 829

AVP Type ENUM

Supported enumerated value(s): none

AVP Flag M

Route-Record

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

Vendor ID 0

VSA Type 282

AVP Type DIAMIDENT

AVP Flag M

Routing-Area-Identity

This AVP contains the routing area identifier of the user.

Vendor ID 10415

VSA Type 1605

AVP Type OCTETSTRING

AVP Flag M

Routing-Policy

This AVP is used to describe a single IP flow.

Vendor ID 10415

VSA Type 312

AVP Type IPFILTERRULE

AVP Flag M

Rule-Action

This AVP indicates the action to be taken when the rule condition occurred for the call.

Vendor ID 9

VSA Type 132066

AVP Type ENUM

Supported enumerated value(s):

1 ALLOWED

AVP Flag N/A

Rule-Activation-Time

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

Vendor ID 10415

VSA Type 1043

AVP Type TIME

AVP Flag M

Rule-Condition

This AVP indicates the condition with the action that has to be applied for the call.

Vendor ID 9

VSA Type 132065

AVP Type ENUM

Supported enumerated value(s):

1 OUT_OF_CREDIT

AVP Flag N/A

Rule-Condition-Action

This AVP specifies the special action to be taken by PCEF when the dynamic rule is matched and conditions are met. This is part of Charging-Rule-Definition AVP and can be received in CCA-I/CCA-U/RAR.

Vendor ID 9

VSA Type 132064

AVP Type GROUPED

Supported group value(s):

[RULE_CONDITION]

[RULE_ACTION]

AVP Flag N/A

Rule-Deactivation-Time

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

Vendor ID 10415

VSA Type 1044

AVP Type TIME

AVP Flag M

Rule-Failure-Code

This AVP contains the rule failure code.

Vendor ID 10415

VSA Type 1031

AVP Type ENUM

Supported enumerated value(s):

1 UNKNOWN_RULE_NAME

2 RATING_GROUP_ERROR

3 SERVICE_IDENTIFIER_ERROR

4 GW/PCEF_MALFUNCTION

5 RESOURCES_LIMITATION

6 MAX_NR_BEARERS_REACHED

7 UNKNOWN_BEARER_ID

8 MISSING_BEARER_ID

9 MISSING_FLOW_DESCRIPTION

10 RESOURCE_ALLOCATION_FAILURE

11 UNSUCCESSFUL_QOS_VALIDATION

12 INCORRECT_FLOW_INFORMATION

13 PS_TO_CS_HANDOVER

14 TDF_APPLICATION_IDENTIFIER_ERROR

15 NO_BEARER_BOUND

17 AN_GW_FAILED

18 MISSING_REDIRECT_SERVER_ADDRESS

AVP Flag M

Rule-Reason-Code

This AVP contains the rule reason code.

Vendor ID 5535

VSA Type 814

AVP Type ENUM

Supported enumerated value(s):

0 UNKNOWN_FLOW_IDENTIFIER

1 UNKNOWN_RULE_NAME

2 RATING_GROUP_ERROR

3 SERVICE_IDENTIFIER_ERROR

4 AGW_MALFUNCTION

5 RESOURCES_LIMITATION

AVP Flag M

S1AP-Cause

S1AP-Cause

Vendor ID 10415

VSA Type 4302

AVP Type UINT32

AVP Flag M

SC-Address

SC-Address

Vendor ID 10415

VSA Type 3300

AVP Type OCTETSTRING

AVP Flag M

SCEF-ID

SCEF-ID

Vendor ID 10415

VSA Type 3125

AVP Type DIAMIDENT

AVP Flag M

SCEF-Realm

SCEF-Realm

Vendor ID 10415

VSA Type 1684

AVP Type DIAMIDENT

AVP Flag N/A

SCEF-Reference-ID

SCEF-Reference-ID

Vendor ID 10415

VSA Type 3124

AVP Type UINT32

AVP Flag M

SCEF-Reference-ID-for-Deletion

SCEF-Reference-ID-for-Deletion

Vendor ID 10415

VSA Type 3126

AVP Type UINT32

AVP Flag M

SCEF-Wait-Time

SCEF-Wait-Time

Vendor ID 10415

VSA Type 4316

AVP Type TIME

AVP Flag M

SCSCF-Restoration-Info

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

Vendor ID 10415

VSA Type 639

AVP Type GROUPED

Supported group value(s):

[USER_NAME]

[RESTORATION_INFO]

[SIP_AUTHENTICATION_SCHEME]

AVP Flag N/A

SD-Action

SD-Action

Vendor ID 9

VSA Type 132042

AVP Type ENUM

Supported enumerated value(s):

0 QUERY

1 QUERY_AND_RECOVER

AVP Flag N/A

SDP-Answer-Timestamp

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

Vendor ID 0

VSA Type 1275

AVP Type TIME

AVP Flag M

SDP-Media-Component

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

Vendor ID 10415

VSA Type 843

AVP Type GROUPED

Supported group value(s):

[SDP_MEDIA_NAME]

[SDP_MEDIA_DESCRIPTION]

[MEDIA_INITIATOR_FLAG]

[AUTHORISED_QOS]

[3GPP_CHARGING_ID]

AVP Flag M

SDP-Media-Description

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

Vendor ID 10415

VSA Type 845

AVP Type UTF8STRING

AVP Flag M

SDP-Media-Name

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

Vendor ID 10415

VSA Type 844

AVP Type UTF8STRING

AVP Flag M

SDP-Offer-Timestamp

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

Vendor ID 0

VSA Type 1274

AVP Type TIME

AVP Flag M

SDP-Session-Description

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

Vendor ID 10415

VSA Type 842

AVP Type UTF8STRING

AVP Flag M

SDP-TimeStamps

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

Vendor ID 0

VSA Type 1273

AVP Type GROUPED

Supported group value(s):

[SDP_OFFER_TIMESTAMP]

[SDP_ANSWER_TIMESTAMP]

AVP Flag M

SDP-Type

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

Vendor ID 10415

VSA Type 2036

AVP Type ENUM

Supported enumerated value(s):

0 SDP_OFFER

1 SDP_ANSWER

AVP Flag M

SGSN-Address

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

Vendor ID 10415

VSA Type 1228

AVP Type ADDRESS

AVP Flag M

SGSN-Location-Information

This AVP contains the location information of the SGSN user.

Vendor ID 10415

VSA Type 1601

AVP Type GROUPED

Supported group value(s):

[CELL_GLOBAL_IDENTITY]

[LOCATION_AREA_IDENTITY]

[SERVICE_AREA_IDENTITY]

[ROUTING_AREA_IDENTITY]

[GEOGRAPHICAL_INFORMATION]

[GEODETIC_INFORMATION]

[CURRENT_LOCATION_RETRIEVED]

[AGE_OF_LOCATION_INFORMATION]

AVP Flag M

SGSN-Number

This AVP contains the ISDN number of the SGSN.

Vendor ID 10415

VSA Type 1489

AVP Type OCTETSTRING

AVP Flag M

SGSN-SM-Delivery-Outcome

SGSN-SM-Delivery-Outcome

Vendor ID 10415

VSA Type 3319

AVP Type GROUPED

Supported group value(s):

[SM_DELIVERY_CAUSE]

[ABSENT_USER_DIAGNOSTIC_SM]

AVP Flag M

SGSN-User-State

This AVP indicates the current state of the SGSN user.

Vendor ID 10415

VSA Type 1498

AVP Type GROUPED

Supported group value(s):

[USER_STATE]

AVP Flag M

SGW-Change

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

Vendor ID 10415

VSA Type 2065

AVP Type ENUM

Supported enumerated value(s):

0 ACR_START_NOT_DUE_TO_SGW_CHANGE

1 ACR_START_DUE_TO_SGW_CHANGE

AVP Flag M

SGW-Type

This AVP specifies the type of SGW of current flow.

Vendor ID 10415

VSA Type 7001

AVP Type UINT32

AVP Flag M

SIP-AOR

SIP-AOR

Vendor ID 0

VSA Type 122

AVP Type UTF8STRING

AVP Flag M

SIP-Auth-Data-Item

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

Vendor ID 10415

VSA Type 612

AVP Type GROUPED

Supported group value(s):

[SIP_ITEM_NUMBER]

[SIP_AUTHENTICATION_SCHEME]

[SIP_AUTHENTICATE]

[SIP_DIGEST_AUTHENTICATE]

[SIP_AUTHORIZATION]

[SIP_AUTHENTICATION_CONTEXT]

[CONFIDENTIALITY_KEY]

[INTEGRITY_KEY]

[LINE_IDENTIFIER]

AVP Flag M

SIP-Authenticate

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

Vendor ID 10415

VSA Type 609

AVP Type OCTETSTRING

AVP Flag M

SIP-Authentication-Context

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

Vendor ID 10415

VSA Type 611

AVP Type OCTETSTRING

AVP Flag M

SIP-Authentication-Scheme

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

Vendor ID 10415

VSA Type 608

AVP Type UTF8STRING

AVP Flag M

SIP-Authorization

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

Vendor ID 10415

VSA Type 610

AVP Type OCTETSTRING

AVP Flag M

SIP-Digest-Authenticate

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

Vendor ID 10415

VSA Type 635

AVP Type GROUPED

Supported group value(s):

[DIGEST_REALM]

[DIGEST_DOMAIN]

[DIGEST_ALGORITHM]

[DIGEST_QOP]

[DIGEST_HA1]

[DIGEST_AUTH_PARAM]

AVP Flag M

SIP-Forking-Indication

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

Vendor ID 10415

VSA Type 523

AVP Type ENUM

Supported enumerated value(s):

0 SINGLE_DIALOGUE

1 SEVERAL_DIALOGUES

AVP Flag M

SIP-Item-Number

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

Vendor ID 10415

VSA Type 613

AVP Type UINT32

AVP Flag M

SIP-Message

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

Vendor ID 4491

VSA Type 229

AVP Type OCTETSTRING

AVP Flag M

SIP-Method

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

Vendor ID 10415

VSA Type 824

AVP Type UTF8STRING

AVP Flag M

SIP-Number-Auth-Items

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

Vendor ID 10415

VSA Type 607

AVP Type UINT32

AVP Flag M

SIP-Request-Timestamp

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

Vendor ID 0

VSA Type 834

AVP Type TIME

AVP Flag M

SIP-Request-Timestamp-Fraction

SIP-Request-Timestamp-Fraction

Vendor ID 0

VSA Type 2301

AVP Type UINT32

AVP Flag M

SIP-Response-Timestamp

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

Vendor ID 0

VSA Type 835

AVP Type TIME

AVP Flag M

SIP-Response-Timestamp-Fraction

SIP-Response-Timestamp-Fraction

Vendor ID 0

VSA Type 2302

AVP Type UINT32

AVP Flag M

SIPTO-Permission

SIPTO-Permission

Vendor ID 10415

VSA Type 1613

AVP Type ENUM

Supported enumerated value(s):

0 SIPTO_ALLOWED

1 SIPTO_NOTALLOWED

AVP Flag M

SM-Cause

SM-Cause

Vendor ID 10415

VSA Type 4305

AVP Type UINT32

AVP Flag M

SM-Delivery-Cause

SM-Delivery-Cause

Vendor ID 10415

VSA Type 3321

AVP Type ENUM

Supported enumerated value(s):

0 UE_MEMORY_CAPACITY_EXCEEDED

1 ABSENT_USER

2 SUCCESSFUL_TRANSFER

AVP Flag M

SM-Delivery-Failure-Cause

SM-Delivery-Failure-Cause

Vendor ID 10415

VSA Type 3303

AVP Type GROUPED

Supported group value(s):

[SM_ENUMERATED_DELIVERY_FAILURE_CAUSE]

[SM_DIAGNOSTIC_INFO]

AVP Flag M

SM-Delivery-Outcome

SM-Delivery-Outcome

Vendor ID 10415

VSA Type 3316

AVP Type GROUPED

Supported group value(s):

[SM_DELIVERY_CAUSE]

[ABSENT_USER_DIAGNOSTIC_SM]

AVP Flag M

SM-Delivery-Start-Time

SM-Delivery-Start-Time

Vendor ID 10415

VSA Type 3307

AVP Type TIME

AVP Flag M

SM-Delivery-Timer

SM-Delivery-Timer

Vendor ID 10415

VSA Type 3306

AVP Type UINT32

AVP Flag M

SM-Diagnostic-Info

SM-Diagnostic-Info

Vendor ID 10415

VSA Type 3305

AVP Type OCTETSTRING

AVP Flag M

SM-Enumerated-Delivery-Failure-Cause

SM-Enumerated-Delivery-Failure-Cause

Vendor ID 10415

VSA Type 3304

AVP Type ENUM

Supported enumerated value(s):

0 MEMORY_CAPACITY_EXCEEDED

1 EQUIPMENT_PROTOCOL_ERROR

2 EQUIPMENT_NOT_SM-EQUIPPED

3 UNKNOWN_SERVICE_CENTRE

4 SC-CONGESTION

5 INVALID_SME-ADDRESS

6 USER_NOT_SC-USER

AVP Flag M

SM-RP-UI

SM-RP-UI

Vendor ID 10415

VSA Type 3301

AVP Type OCTETSTRING

AVP Flag M

SMS-GMSC-Address

SMS-GMSC-Address

Vendor ID 10415

VSA Type 3332

AVP Type OCTETSTRING

AVP Flag N/A

SMS-GMSC-Alert-Event

SMS-GMSC-Alert-Event

Vendor ID 10415

VSA Type 3333

AVP Type UINT32

AVP Flag N/A

SMS-Register-Request

SMS-Register-Request

Vendor ID 10415

VSA Type 1648

AVP Type ENUM

Supported enumerated value(s):

0 SMS_REGISTRATION_REQUIRED

1 SMS_REGISTRATION_NOT_PREFERRED

2 NO_PREFERENCE

AVP Flag N/A

SMSMI-Correlation-ID

SMSMI-Correlation-ID

Vendor ID 10415

VSA Type 3324

AVP Type GROUPED

Supported group value(s):

[HSS_ID]

[ORIGINATING_SIP_URI]

[DESTINATION_SIP_URI]

AVP Flag N/A

SN-Absolute-Validity-Time

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

Vendor ID 8164

VSA Type 505

AVP Type TIME

AVP Flag N/A

SN-Bandwidth-Control

This AVP contains the value to control bandwidth usage.

Vendor ID 8164

VSA Type 512

AVP Type ENUM

Supported enumerated value(s):

0 HIGH

1 LOW

AVP Flag M

SN-CF-Policy-ID

SN-CF-Policy-ID

Vendor ID 8164

VSA Type 529

AVP Type UINT32

AVP Flag M

SN-Charging-Collection-Function-Name

SN-Charging-Collection-Function-Name

Vendor ID 8164

VSA Type 530

AVP Type UTF8STRING

AVP Flag N/A

SN-Charging-Id

This AVP contains the charging identifier.

Vendor ID 8164

VSA Type 525

AVP Type OCTETSTRING

AVP Flag N/A

SN-Fast-Reauth-Username

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

Vendor ID 8164

VSA Type 11010

AVP Type OCTETSTRING

AVP Flag M

SN-Firewall-Policy

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

Vendor ID 8164

VSA Type 515

AVP Type UTF8STRING

AVP Flag N/A

SN-Monitoring-Key

It is an identifier to a usage monitoring control instance.

Vendor ID 8164

VSA Type 518

AVP Type UINT32

AVP Flag N/A

SN-Phase0-PSAPName

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

Vendor ID 8164

VSA Type 523

AVP Type UTF8STRING

AVP Flag N/A

SN-Pseudonym-Username

This AVP is used for reauthentication of subscriber.

Vendor ID 8164

VSA Type 11011

AVP Type OCTETSTRING

AVP Flag M

SN-Remaining-Service-Unit

SN-Remaining-Service-Unit

Vendor ID 8164

VSA Type 526

AVP Type GROUPED

Supported group value(s):

[TARIFF_CHANGE_USAGE]

[CC_TIME]

[CC_TOTAL_OCTETS]

[CC_INPUT_OCTETS]

[CC_OUTPUT_OCTETS]

[CC_SERVICE_SPECIFIC_UNITS]

[3GPP_REPORTING_REASON]

AVP Flag N/A

SN-Rulebase-Id

SN-Rulebase-Id

Vendor ID 8164

VSA Type 528

AVP Type UTF8STRING

AVP Flag M

SN-Service-Flow-Detection

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

Vendor ID 8164

VSA Type 520

AVP Type ENUM

Supported enumerated value(s):

0 ENABLE_DETECTION

AVP Flag N/A

SN-Service-Start-Timestamp

SN-Service-Start-Timestamp

Vendor ID 8164

VSA Type 527

AVP Type TIME

AVP Flag N/A

SN-Time-Quota-Threshold

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

Vendor ID 8164

VSA Type 503

AVP Type UINT32

AVP Flag M

SN-Total-Used-Service-Unit

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

Vendor ID 8164

VSA Type 504

AVP Type GROUPED

Supported group value(s):

[TARIFF_CHANGE_USAGE]

[CC_TIME]

[CC_TOTAL_OCTETS]

[CC_INPUT_OCTETS]

[CC_OUTPUT_OCTETS]

[CC_SERVICE_SPECIFIC_UNITS]

[3GPP_REPORTING_REASON]

AVP Flag N/A

SN-Traffic-Policy

This AVP contains name of the Traffic Policing Policy.

Vendor ID 8164

VSA Type 514

AVP Type UTF8STRING

AVP Flag N/A

SN-Transparent-Data

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

Vendor ID 8164

VSA Type 513

AVP Type OCTETSTRING

AVP Flag N/A

SN-Unit-Quota-Threshold

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

Vendor ID 8164

VSA Type 502

AVP Type UINT32

AVP Flag M

SN-Usage-Monitoring

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

Vendor ID 8164

VSA Type 521

AVP Type ENUM

Supported enumerated value(s):

0 USAGE_MONITORING_DISABLED

1 USAGE_MONITORING_ENABLED

AVP Flag N/A

SN-Usage-Monitoring-Control

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

Vendor ID 8164

VSA Type 517

AVP Type GROUPED

Supported group value(s):

[SN_MONITORING_KEY]

[SN_USAGE_MONITORING]

[SN_USAGE_VOLUME]

AVP Flag N/A

SN-Usage-Volume

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

Vendor ID 8164

VSA Type 519

AVP Type UINT64

AVP Flag N/A

SN-Volume-Quota-Threshold

This AVP contains a volume threshold value in percentage value.

Vendor ID 8164

VSA Type 501

AVP Type UINT32

AVP Flag M

SN1-IPv6-Primary-DNS

SN1-IPv6-Primary-DNS

Vendor ID 8164

VSA Type 101

AVP Type ADDRESS

AVP Flag M

SN1-IPv6-Secondary-DNS

SN1-IPv6-Secondary-DNS

Vendor ID 8164

VSA Type 102

AVP Type ADDRESS

AVP Flag M

SN1-Primary-DNS-Server

SN1-Primary-DNS-Server

Vendor ID 8164

VSA Type 5

AVP Type ADDRESS

AVP Flag M

SN1-Rulebase

SN1-Rulebase

Vendor ID 8164

VSA Type 250

AVP Type UTF8STRING

AVP Flag M

SN1-Secondary-DNS-Server

SN1-Secondary-DNS-Server

Vendor ID 8164

VSA Type 6

AVP Type ADDRESS

AVP Flag M

SN1-VPN-Name

SN1-VPN-Name

Vendor ID 8164

VSA Type 2

AVP Type UTF8STRING

AVP Flag M

SRES

This AVP contains the SRES.

Vendor ID 10415

VSA Type 1454

AVP Type OCTETSTRING

AVP Flag M

SS-Action

SS-Action

Vendor ID 9

VSA Type 132072

AVP Type ENUM

Supported enumerated value(s):

0 QUERY

1 QUERY_AND_RECOVER

AVP Flag N/A

SS-Code

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

Vendor ID 10415

VSA Type 1476

AVP Type OCTETSTRING

AVP Flag M

SS-Status

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

Vendor ID 10415

VSA Type 1477

AVP Type OCTETSTRING

AVP Flag M

SSID

SSID

Vendor ID 10415

VSA Type 1524

AVP Type UTF8STRING

AVP Flag N/A

STN-SR

This AVP contains the session transfer number for SRVCC.

Vendor ID 10415

VSA Type 1433

AVP Type UTF8STRING

AVP Flag M

Secondary-Charging-Collection-Function-Name

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

Vendor ID 10415

VSA Type 622

AVP Type DIAMURI

AVP Flag M

Secondary-Event-Charging-Function-Name

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

Vendor ID 10415

VSA Type 620

AVP Type DIAMURI

AVP Flag M

Secondary-RAT-Type

It holds the value of Secondary RAT Type, as provided by the RAN.

Vendor ID 10415

VSA Type 1304

AVP Type OCTETSTRING

AVP Flag N/A

Sector-Id

The identifier of sector that MS exists.

Vendor ID 0

VSA Type 10002

AVP Type UINT32

AVP Flag M

Security-Parameter-Index

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

Vendor ID 10415

VSA Type 1056

AVP Type OCTETSTRING

AVP Flag M

Send-Data-Indication

This AVP indicates that sender requests user data in SNR.

Vendor ID 0

VSA Type 710

AVP Type ENUM

Supported enumerated value(s): none

AVP Flag M

Served-Party-IP-Address

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

Vendor ID 10415

VSA Type 848

AVP Type ADDRESS

AVP Flag M

Server-Assignment-Type

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

Vendor ID 10415

VSA Type 614

AVP Type ENUM

Supported enumerated value(s):

0 NO_ASSIGNMENT

1 REGISTRATION

2 RE_REGISTRATION

3 UNREGISTERED_USER

4 TIMEOUT_DEREGISTRATION

5 USER_DEREGISTRATION

6 TIMEOUT_DEREGISTRATION_STORE_SERVER_NAME

7 USER_DEREGISTRATION_STORE_SERVER_NAME

8 ADMINISTRATIVE_DEREGISTRATION

9 AUTHENTICATION_FAILURE

10 AUTHENTICATION_TIMEOUT

11 DEREGISTRATION_TOO_MUCH_DATA

AVP Flag M

Server-Capabilities

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

Vendor ID 10415

VSA Type 603

AVP Type GROUPED

Supported group value(s):

[MANDATORY_CAPABILITY]

[OPTIONAL_CAPABILITY]

[SERVER_NAME]

AVP Flag M

Server-Name

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

Vendor ID 10415

VSA Type 602

AVP Type UTF8STRING

AVP Flag M

Service-Feature-Rule-Definition

Service-Feature.

Vendor ID 9

VSA Type 132087

AVP Type GROUPED

Supported group value(s):

[TRIGGER_ACTION_NAME]

[SERVICE_FEATURE_RULE_STATUS]

[PROFILE_NAME]

AVP Flag N/A

Service-Feature-Rule-Install

Service-Feature-Rule-Install.

Vendor ID 9

VSA Type 132086

AVP Type GROUPED

Supported group value(s):

[SERVICE_FEATURE_RULE_DEFINITION]

AVP Flag N/A

Service-Feature-Rule-Remove

Service-Feature-Rule-Remove.

Vendor ID 9

VSA Type 132091

AVP Type GROUPED

Supported group value(s):

[TRIGGER_ACTION_NAME]

AVP Flag N/A

Service-Feature-Rule-Status

Service-Feature-Rule-Status

Vendor ID 9

VSA Type 132089

AVP Type ENUM

Supported enumerated value(s):

0 DISABLE

1 ENABLE

AVP Flag N/A

Service-Feature-Status

Service-Feature-Status

Vendor ID 9

VSA Type 132085

AVP Type ENUM

Supported enumerated value(s):

0 DISABLE

1 ENABLE

AVP Flag N/A

Service-Feature-Type

Service-Feature-Type

Vendor ID 9

VSA Type 132084

AVP Type ENUM

Supported enumerated value(s):

0 INVALID

1 CUSP

2 CUTO

3 UIDH

AVP Flag N/A

Service-Feature

Service-Feature.

Vendor ID 9

VSA Type 132083

AVP Type GROUPED

Supported group value(s):

[SERVICE_FEATURE_TYPE]

[SERVICE_FEATURE_STATUS]

[SERVICE_FEATURE_RULE_INSTALL]

[SERVICE_FEATURE_RULE_REMOVE]

AVP Flag N/A

Service-Activation

Service-Activation

Vendor ID 9

VSA Type 131094

AVP Type ENUM

Supported enumerated value(s):

0 USER_PROFILE

1 AUTOMATIC

AVP Flag M

Service-Area-Identity

This AVP contains the service area identifier of the user.

Vendor ID 10415

VSA Type 1607

AVP Type OCTETSTRING

AVP Flag M

Service-CDR-Threshold

Service-CDR-Threshold

Vendor ID 9

VSA Type 131129

AVP Type GROUPED

Supported group value(s):

[CDR_VOLUME_THRESHOLD]

[CDR_TIME_THRESHOLD]

AVP Flag M

Service-Class

This AVP contains the service class requested by the AF.

Vendor ID 13019

VSA Type 459

AVP Type UTF8STRING

AVP Flag N/A

Service-Class-Type

Service-Class-Type

Vendor ID 9

VSA Type 131100

AVP Type UINT32

AVP Flag N/A

Service-Context-Id

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

Vendor ID 0

VSA Type 461

AVP Type UTF8STRING

AVP Flag M

Service-Data-Container

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

Vendor ID 10415

VSA Type 2040

AVP Type GROUPED

Supported group value(s):

[AF_CORRELATION_INFORMATION]

[CHARGING_RULE_BASE_NAME]

[ACCOUNTING_INPUT_OCTETS]

[ACCOUNTING_OUTPUT_OCTETS]

[ACCOUNTING_INPUT_PACKETS]

[ACCOUNTING_OUTPUT_PACKETS]

[LOCAL_SEQUENCE_NUMBER]

[QOS_INFORMATION]

[RATING_GROUP]

[CHANGE_TIME]

[SERVICE_IDENTIFIER]

[SERVICE_SPECIFIC_INFO]

[SGSN_ADDRESS]

[TIME_FIRST_USAGE]

[TIME_LAST_USAGE]

[TIME_USAGE]

[CHANGE_CONDITION]

[3GPP_USER_LOCATION_INFO]

[FLOW_DESCRIPTION]

[CHARGING_RULE_NAME]

[FIRST_PACKET_DIRECTION]

[3GPP2_BSID]

AVP Flag M

Service-Definition

Service-Definition

Vendor ID 9

VSA Type 131076

AVP Type GROUPED

Supported group value(s):

[SERVICE_NAME]

[ONLINE_BILLING_BASIS]

[DUAL_BILLING_BASIS]

[SERVICE_REPORTING_LEVEL]

[SERVICE_CDR_THRESHOLD]

[SERVICE_ACTIVATION]

[ADVICE_OF_CHARGE]

[SERVICE_CLASS_TYPE]

[SERVICE_IDLE_TIME]

[OWNER_ID]

[OWNER_NAME]

[ONLINE_PASSTHROUGH_QUOTA]

[DUAL_PASSTHROUGH_QUOTA]

[ONLINE_REAUTHORIZATION_THRESHOLD]

[DUAL_REAUTHORIZATION_THRESHOLD]

[ONLINE_REAUTHORIZATION_TIMEOUT]

[REFUND_POLICY]

[METER_EXCLUDE]

[METER_INCLUDE_IMAP]

[METERING_GRANULARITY]

[VERIFY]

[CISCO_QUOTA_CONSUMPTION_TIME]

[SERVICE_RATING_GROUP]

[CISCO_QOS_PROFILE_UPLINK]

[CISCO_QOS_PROFILE_DOWNLINK]

[HEADER_GROUP_NAME]

[CONTENT_POLICY_MAP]

[SERVICE_LIFE_TIME]

AVP Flag M

Service-Group-Definition

Service-Group-Definition

Vendor ID 9

VSA Type 131244

AVP Type GROUPED

Supported group value(s):

[SERVICE_GROUP_NAME]

[CISCO_EVENT_TRIGGER]

[CISCO_QOS]

[CISCO_FLOW_STATUS]

[REDIRECT_SERVER]

AVP Flag M

Service-Group-Event

Service-Group-Event

Vendor ID 9

VSA Type 131247

AVP Type GROUPED

Supported group value(s):

[SERVICE_GROUP_NAME]

[CISCO_EVENT]

AVP Flag M

Service-Group-Install

Service-Group-Install

Vendor ID 9

VSA Type 131245

AVP Type GROUPED

Supported group value(s):

[SERVICE_GROUP_DEFINITION]

AVP Flag M

Service-Group-Name

Service-Group-Name

Vendor ID 9

VSA Type 131243

AVP Type OCTETSTRING

AVP Flag M

Service-Group-Remove

Service-Group-Remove

Vendor ID 9

VSA Type 131246

AVP Type GROUPED

Supported group value(s):

[SERVICE_GROUP_NAME]

AVP Flag M

Service-Identifier

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

Vendor ID 0

VSA Type 439

AVP Type UINT32

AVP Flag M

Service-Idle-Time

Service-Idle-Time

Vendor ID 9

VSA Type 131101

AVP Type UINT32

AVP Flag N/A

Service-Indication

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

Vendor ID 0

VSA Type 704

AVP Type OCTETSTRING

AVP Flag M

Service-Info

Service-Info

Vendor ID 9

VSA Type 131078

AVP Type GROUPED

Supported group value(s):

[SERVICE_NAME]

[ONLINE]

[VIRTUAL_ONLINE]

AVP Flag M

Service-Info-Status

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

Vendor ID 10415

VSA Type 527

AVP Type ENUM

Supported enumerated value(s):

0 FINAL_SERVICE_INFORMATION

1 PRELIMINARY_SERVICE_INFORMATION

AVP Flag M

Service-Information

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

Vendor ID 10415

VSA Type 873

AVP Type GROUPED

Supported group value(s):

[IMS_INFORMATION]

AVP Flag M

Service-Install

Service-Install

Vendor ID 9

VSA Type 131185

AVP Type GROUPED

Supported group value(s):

[SERVICE_DEFINITION]

AVP Flag M

Service-Life-Time

Service-Life-Time

Vendor ID 9

VSA Type 131257

AVP Type UINT32

AVP Flag N/A

Service-Name

Service-Name

Vendor ID 9

VSA Type 131087

AVP Type OCTETSTRING

AVP Flag M

Service-Parameter-Info

Service-specific information used for rating.

Vendor ID 0

VSA Type 440

AVP Type GROUPED

Supported group value(s):

[SERVICE_PARAMETER_TYPE]

[SERVICE_PARAMETER_VALUE]

AVP Flag M

Service-Parameter-Type

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

Vendor ID 0

VSA Type 441

AVP Type UINT32

AVP Flag M

Service-Parameter-Value

Value of the service parameter type.

Vendor ID 0

VSA Type 442

AVP Type OCTETSTRING

AVP Flag M

Service-Rating-Group

Service-Rating-Group

Vendor ID 9

VSA Type 131162

AVP Type UINT32

AVP Flag N/A

Service-Remove

Service-Remove

Vendor ID 9

VSA Type 131186

AVP Type GROUPED

Supported group value(s):

[SERVICE_NAME]

AVP Flag M

Service-Report

Service-Report

Vendor ID 10415

VSA Type 3161

AVP Type GROUPED

Supported group value(s):

[SERVICE_RESULT]

[NODE_TYPE]

AVP Flag M

Service-Reporting-Level

Service-Reporting-Level

Vendor ID 9

VSA Type 131125

AVP Type ENUM

Supported enumerated value(s):

0 TRANSACTION

1 SERVICE

AVP Flag M

Service-Result

Service-Result

Vendor ID 10415

VSA Type 3146

AVP Type GROUPED

Supported group value(s):

[VENDOR_ID]

[SERVICE_RESULT_CODE]

AVP Flag M

Service-Result-Code

Service-Result-Code

Vendor ID 10415

VSA Type 3147

AVP Type UINT32

AVP Flag M

Service-Selection

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

Vendor ID 0

VSA Type 493

AVP Type OCTETSTRING

AVP Flag M

Service-Specific-Data

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

Vendor ID 0

VSA Type 1249

AVP Type GROUPED

Supported group value(s):

[SERVICE_SPECIFIC_TYPE]

[SERVICE_SPECIFIC_VALUE]

AVP Flag M

Service-Specific-Info

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

Vendor ID 10415

VSA Type 1249

AVP Type GROUPED

Supported group value(s):

[SERVICE_SPECIFIC_DATA]

[SERVICE_SPECIFIC_TYPE]

AVP Flag M

Service-Specific-Type

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

Vendor ID 0

VSA Type 1248

AVP Type UINT32

AVP Flag M

Service-Specific-Value

This AVP holds service specific value.

Vendor ID 0

VSA Type 863

AVP Type UTF8STRING

AVP Flag M

Service-Status

Service-Status

Vendor ID 9

VSA Type 131086

AVP Type GROUPED

Supported group value(s):

[SERVICE_NAME]

[CISCO_FLOW_STATUS]

[SERVICE_RATING_GROUP]

[CISCO_QOS]

[REDIRECT_SERVER]

[SERVICE_GROUP_NAME]

AVP Flag M

Service-Type

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

Vendor ID 0

VSA Type 6

AVP Type ENUM

Supported enumerated value(s):

1 Login

2 Framed

3 Callback-Login

4 Callback-Framed

5 Outbound

6 Administrative

7 NAS-Prompt

8 Authenticate-Only

9 Callback-NAS-Prompt

10 Call-Check

11 Callback-Administrative

12 Voice

13 Fax

14 Modem-Relay

15 IAPP-Register_IEEE-802_11f

16 IAPP-AP-Check_IEEE-802_11f

17 Authorize-Only-RADDynAuth

AVP Flag M

Service-URN

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

Vendor ID 10415

VSA Type 525

AVP Type OCTETSTRING

AVP Flag M

Services

Services

Vendor ID 9

VSA Type 132082

AVP Type GROUPED

Supported group value(s):

[SERVICE_FEATURE]

AVP Flag N/A

ServiceTypeIdentity

This AVP contains the LCS service type identity.

Vendor ID 10415

VSA Type 1484

AVP Type UINT32

AVP Flag M

Serving-Node

This AVP contains information about the network node serving the targeted user.

Vendor ID 10415

VSA Type 2401

AVP Type GROUPED

Supported group value(s):

[SGSN_NUMBER]

[MME_NAME]

[MME_REALM]

[MSC_NUMBER]

[3GPP_AAA_SERVER_NAME]

[LCS_CAPABILITIES_SETS]

AVP Flag M

Serving-Node-Type

This AVP contains type of the Serving Node.

Vendor ID 10415

VSA Type 2047

AVP Type ENUM

Supported enumerated value(s):

0 SGSN

1 PMIPSGW

2 GTPSGW

3 ePDG

4 hSGW

5 MME

6 TWAN

AVP Flag M

Serving-PLMN-Rate-Control

Serving-PLMN-Rate-Control

Vendor ID 10415

VSA Type 4310

AVP Type GROUPED

Supported group value(s):

[UPLINK_RATE_LIMIT]

[DOWNLINK_RATE_LIMIT]

AVP Flag M

Session-Bundle-Id

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

Vendor ID 13019

VSA Type 400

AVP Type UINT32

AVP Flag M

Session-Id

Specifies the specific session with an identifier.

Vendor ID 0

VSA Type 263

AVP Type UTF8STRING

AVP Flag M

Session-Linking-Indicator

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

Vendor ID 10415

VSA Type 1064

AVP Type ENUM

Supported enumerated value(s):

0 SESSION_LINKING_IMMEDIATE

1 SESSION_LINKING_DEFERRED

AVP Flag M

Session-Priority

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

Vendor ID 10415

VSA Type 650

AVP Type ENUM

Supported enumerated value(s):

0 PRIORITY-0

1 PRIORITY-1

2 PRIORITY-2

3 PRIORITY-3

4 PRIORITY-4

AVP Flag N/A

Session-Release-Cause

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

Vendor ID 10415

VSA Type 1045

AVP Type ENUM

Supported enumerated value(s):

0 UNSPECIFIED_REASON

1 UE_SUBSCRIPTION_REASON

2 INSUFFICIENT_SERVER_RESOURCES

AVP Flag M

Session-Request-Type

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

Vendor ID 10415

VSA Type 311

AVP Type ENUM

Supported enumerated value(s): none

AVP Flag M

Session-Start-Indicator

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

Vendor ID 8164

VSA Type 522

AVP Type OCTETSTRING

AVP Flag M

Session-Sync-Requested

Session-Sync-Requested

Vendor ID 9

VSA Type 132041

AVP Type ENUM

Supported enumerated value(s):

1 STATE_INFORMATION_REQUIRED

AVP Flag N/A

Session-Timeout

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

Vendor ID 0

VSA Type 27

AVP Type UINT32

AVP Flag M

Software-Version

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

Vendor ID 10415

VSA Type 6004

AVP Type UTF8STRING

AVP Flag M

Specific-APN-Info

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

Vendor ID 10415

VSA Type 1472

AVP Type GROUPED

Supported group value(s):

[SERVICE_SELECTION]

[MIP6_AGENT_INFO]

[VISITED_NETWORK_IDENTIFIER]

AVP Flag M

Specific-Action

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

Vendor ID 10415

VSA Type 513

AVP Type ENUM

Supported enumerated value(s):

1 CHARGING_CORRELATION_EXCHANGE

2 INDICATION_OF_LOSS_OF_BEARER

3 INDICATION_OF_RECOVERY_OF_BEARER

4 INDICATION_OF_RELEASE_OF_BEARER

5 INDICATION_OF_ESTABLISHMENT_OF_BEARER

6 IP_CAN_CHANGE

AVP Flag M

Sponsor-Identity

Sponsor-Identity

Vendor ID 10415

VSA Type 531

AVP Type UTF8STRING

AVP Flag N/A

Sponsored-Connectivity-Data

Sponsored-Connectivity-Data

Vendor ID 10415

VSA Type 530

AVP Type GROUPED

Supported group value(s):

[SPONSOR_IDENTITY]

[APPLICATION_SERVICE_PROVIDER_IDENTITY]

[GRANTED_SERVICE_UNIT]

[USED_SERVICE_UNIT]

AVP Flag N/A

Starent-Subscriber-Permission

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

Vendor ID 8164

VSA Type 20

AVP Type ENUM

Supported enumerated value(s):

0 None

1 Simple-IP

2 Mobile-IP

3 Simple-IP-Mobile-IP

4 HA-Mobile-IP

5 Simple-IP-HA-Mobile-IP

6 Mobile-IP-HA-Mobile-IP

7 SIP-MIP-HA-MIP

8 GGSN-PDP-TYPE-IP

16 GGSN-PDP-TYPE-PPP

32 Network-Mobility

38 FA-HA-NEMO

64 PMIPv6

127 All

AVP Flag M

Start-Time

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

Vendor ID 10415

VSA Type 2041

AVP Type TIME

AVP Flag M

Start-of-Port-Range

Start-of-Port-Range

Vendor ID 9

VSA Type 131149

AVP Type UINT32

AVP Flag N/A

State

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

Vendor ID 0

VSA Type 24

AVP Type OCTETSTRING

AVP Flag M

Stop-Time

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

Vendor ID 10415

VSA Type 2042

AVP Type TIME

AVP Flag M

Subs-Req-Type

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

Vendor ID 0

VSA Type 705

AVP Type ENUM

Supported enumerated value(s): none

AVP Flag M

Subscribed-Periodic-RAU-TAU-Timer

Subscribed-Periodic-RAU-TAU-Timer

Vendor ID 10415

VSA Type 1619

AVP Type UINT32

AVP Flag N/A

Subscriber-IP-Source

Subscriber-IP-Source

Vendor ID 9

VSA Type 131136

AVP Type ENUM

Supported enumerated value(s):

0 DEFAULT

1 HTTP_X_FORWARDED_FOR

AVP Flag M

Subscriber-Priority

Subscriber-Priority

Vendor ID 5535

VSA Type 6078

AVP Type GROUPED

Supported group value(s):

[3GPP2_MAX_AUTH_AGGR_BW_BET]

[3GPP2_MAX_PER_FLOW_PRIORITY_USER]

[3GPP2_INTER_USER_PRIORITY]

[3GPP2_ALLOWED_PERSISTENT_TFTS]

[3GPP2_MAX_SVC_INST_LINK_FLOW_TOTAL]

[3GPP2_SERVICE_OPTION_PROFILE]

AVP Flag M

Subscriber-Profile

Subscriber-Profile

Vendor ID 9

VSA Type 132081

AVP Type OCTETSTRING

AVP Flag N/A

Subscriber-Status

This AVP indicates if the service is barred or granted.

Vendor ID 10415

VSA Type 1424

AVP Type ENUM

Supported enumerated value(s):

0 SERVICEGRANTED

1 OPERATORDETERMINEDBARRING

AVP Flag M

Subscription-Data

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

Vendor ID 10415

VSA Type 6001

AVP Type GROUPED

Supported group value(s):

[SUBSCRIBER_STATUS]

[MSISDN]

[STN_SR]

[ICS_INDICATOR]

[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]

[SUBSCRIBED_PERIODIC_RAU_TAU_TIMER]

[DL_BUFFERING_SUGGESTED_PACKET_COUNT]

AVP Flag M

Subscription-Id

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

Vendor ID 0

VSA Type 443

AVP Type GROUPED

Supported group value(s):

[SUBSCRIPTION_ID_TYPE]

[SUBSCRIPTION_ID_DATA]

AVP Flag M

Subscription-Id-Data

Used to identify the end user information.

Vendor ID 0

VSA Type 444

AVP Type UTF8STRING

AVP Flag M

Subscription-Id-Type

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

Vendor ID 0

VSA Type 450

AVP Type ENUM

Supported enumerated value(s):

0 END_USER_E164

1 END_USER_IMSI

2 END_USER_SIP_URI

3 END_USER_NAI

4 END_USER_PRIVATE

AVP Flag M

Subscription-Info

This AVP contains the UE's subscription information.

Vendor ID 10415

VSA Type 642

AVP Type GROUPED

Supported group value(s):

[CALL_ID_SIP_HEADER]

[FROM_SIP_HEADER]

[TO_SIP_HEADER]

[RECORD_ROUTE]

[CONTACT]

AVP Flag N/A

Supported-Applications

This AVP contains supported application identifiers of a Diameter node.

Vendor ID 10415

VSA Type 631

AVP Type GROUPED

Supported group value(s):

[AUTH_APPLICATION_ID]

[ACCT_APPLICATION_ID]

[VENDOR_SPECIFIC_APPLICATION_ID]

AVP Flag M

Supported-Features

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

Vendor ID 10415

VSA Type 628

AVP Type GROUPED

Supported group value(s):

[VENDOR_ID]

[FEATURE_LIST_ID]

[FEATURE_LIST]

AVP Flag M

Supported-Features-Resp

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

Vendor ID 10415

VSA Type 628

AVP Type GROUPED

Supported group value(s):

[VENDOR_ID_RESP]

[FEATURE_LIST_ID_RESP]

[FEATURE_LIST_RESP]

AVP Flag N/A

Supported-Features-without-M-bit

Supported-Features-without-M-bit

Vendor ID 10415

VSA Type 628

AVP Type GROUPED

Supported group value(s):

[VENDOR_ID]

[FEATURE_LIST_ID]

[FEATURE_LIST]

AVP Flag N/A

Supported-GAD-Shapes

This AVP contains a bitmask. A node shall mark in the BIT STRING all shapes defined in 3GPP TS 23.032. Bits 6-0 indicate the supported shapes defined in 3GPP TS 23.032. Bits 7 to 31 can be ignored.

Vendor ID 10415

VSA Type 2510

AVP Type UINT32

AVP Flag M

Supported-RAT-Type

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

Vendor ID 10415

VSA Type 6005

AVP Type UTF8STRING

AVP Flag M

Supported-Vendor-Id

Specifies the vendor ID other than the device vendor.

Vendor ID 0

VSA Type 265

AVP Type UINT32

AVP Flag M

TCP-SYN

TCP-SYN

Vendor ID 9

VSA Type 131194

AVP Type UTF8STRING

AVP Flag M

TDF-Application-Identifier

It references the application detection filter (e.g. its value may represent an application such as a list of URLs, etc.) which the PCC rule for Application Detection and Control in the PCEF applies. The TDF-Application-Identifier AVP also references the application in the reporting to the PCRF.

Vendor ID 10415

VSA Type 1088

AVP Type OCTETSTRING

AVP Flag N/A

TDF-Application-Instance-Identifier

This AVP will be dynamically assigned by the PCEF supporting ADC feature in order to allow correlation of application Start and Stop events to the specific service data flow description, if service data flow descriptions are deducible and will be reported from the PCEF to the PCRF when the flow description is deducible along with the corresponding Event Trigger.

Vendor ID 10415

VSA Type 2802

AVP Type OCTETSTRING

AVP Flag N/A

TFR-Flags

TFR-Flags

Vendor ID 10415

VSA Type 3302

AVP Type UINT32

AVP Flag M

TFT-Filter

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

Vendor ID 10415

VSA Type 1012

AVP Type IPFILTERRULE

AVP Flag M

TFT-Packet-Filter-Information

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

Vendor ID 10415

VSA Type 1013

AVP Type GROUPED

Supported group value(s):

[PRECEDENCE]

[TFT_FILTER]

[TOS_TRAFFIC_CLASS]

[FLOW_DIRECTION]

AVP Flag M

TMGI

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

Vendor ID 10415

VSA Type 900

AVP Type OCTETSTRING

AVP Flag M

TMO-Clientless-Optimisation-Rule

TMO-Clientless-Optimisation-Rule

Vendor ID 29168

VSA Type 1004

AVP Type UINT32

AVP Flag N/A

TMO-Virtual-Gi-ID

TMO-Virtual-Gi-ID

Vendor ID 29168

VSA Type 120

AVP Type UINT32

AVP Flag N/A

TS-Code

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

Vendor ID 10415

VSA Type 1487

AVP Type OCTETSTRING

AVP Flag M

TWAN-Identifier

TWAN-Identifier

Vendor ID 10415

VSA Type 29

AVP Type OCTETSTRING

AVP Flag N/A

TWAN-User-Location-Info

This AVP indicates the UE location in a Trusted WLAN Access Network (TWAN). This grouped AVP contains BSSID and SSID of the access point.

Vendor ID 10415

VSA Type 2714

AVP Type GROUPED

Supported group value(s):

[SSID]

[BSSID]

AVP Flag M

Tap-Id

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

Vendor ID 4491

VSA Type 231

AVP Type UTF8STRING

AVP Flag M

Tariff-Change-Usage

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

Vendor ID 0

VSA Type 452

AVP Type ENUM

Supported enumerated value(s):

0 UNIT_BEFORE_TARIFF_CHANGE

1 UNIT_AFTER_TARIFF_CHANGE

2 UNIT_INDETERMINATE

AVP Flag M

Tariff-Time-Change

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

Vendor ID 0

VSA Type 451

AVP Type TIME

AVP Flag M

Tariff-XML

Tariff-XML

Vendor ID 10415

VSA Type 2306

AVP Type UTF8STRING

AVP Flag M

Teleservice-List

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

Vendor ID 10415

VSA Type 1486

AVP Type GROUPED

Supported group value(s):

[TS_CODE]

AVP Flag M

Terminal-Information

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

Vendor ID 10415

VSA Type 6002

AVP Type GROUPED

Supported group value(s):

[ESN]

[MEID]

[IMEI]

[SOFTWARE_VERSION]

AVP Flag M

Terminal-Type

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

Vendor ID 13019

VSA Type 352

AVP Type OCTETSTRING

AVP Flag M

Terminate-Bearer

Terminate-Bearer

Vendor ID 10415

VSA Type 131161

AVP Type GROUPED

Supported group value(s):

[BEARER_IDENTIFIER]

AVP Flag M

Terminating-IOI

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

Vendor ID 0

VSA Type 840

AVP Type UTF8STRING

AVP Flag M

Termination-Cause

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

Vendor ID 0

VSA Type 295

AVP Type ENUM

Supported enumerated value(s):

1 DIAMETER_LOGOUT

2 DIAMETER_SERVICE_NOT_PROVIDED

3 DIAMETER_BAD_ANSWER

4 DIAMETER_ADMINISTRATIVE

5 DIAMETER_LINK_BROKEN

6 DIAMETER_AUTH_EXPIRED

7 DIAMETER_USER_MOVED

8 DIAMETER_SESSION_TIMEOUT

AVP Flag M

Time-First-Usage

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

Vendor ID 10415

VSA Type 2043

AVP Type TIME

AVP Flag M

Time-Last-Usage

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

Vendor ID 10415

VSA Type 2044

AVP Type TIME

AVP Flag M

Time-Stamps

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

Vendor ID 0

VSA Type 833

AVP Type GROUPED

Supported group value(s):

[SIP_REQUEST_TIMESTAMP]

[SIP_RESPONSE_TIMESTAMP]

[SIP_REQUEST_TIMESTAMP_FRACTION]

[SIP_RESPONSE_TIMESTAMP_FRACTION]

AVP Flag M

Time-Threshold

Time-Threshold

Vendor ID 9

VSA Type 131081

AVP Type UINT32

AVP Flag N/A

Time-Usage

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

Vendor ID 10415

VSA Type 2045

AVP Type UINT32

AVP Flag M

To-SIP-Header

This AVP contains the information in the To header.

Vendor ID 10415

VSA Type 645

AVP Type OCTETSTRING

AVP Flag N/A

ToS-Traffic-Class

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

Vendor ID 10415

VSA Type 1014

AVP Type OCTETSTRING

AVP Flag M

Trace-Collection-Entity

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

Vendor ID 10415

VSA Type 1452

AVP Type ADDRESS

AVP Flag M

Trace-Data

This AVP contains the information related to trace function.

Vendor ID 10415

VSA Type 1458

AVP Type GROUPED

Supported group value(s):

[TRACE_REFERENCE]

[TRACE_DEPTH_LIST]

[TRACE_NE_TYPE_LIST]

[TRACE_INTERFACE_LIST]

[TRACE_EVENT_LIST]

[OMC_ID]

[TRACE_COLLECTION_ENTITY]

AVP Flag M

Trace-Depth

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

Vendor ID 10415

VSA Type 1462

AVP Type ENUM

Supported enumerated value(s):

0 Minimum

1 Medium

2 Maximum

3 MinimumWithoutVendorSpecificExtension

4 MediumWithoutVendorSpecificExtension

5 MaximumWithoutVendorSpecificExtension

AVP Flag M

Trace-Depth-List

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

Vendor ID 10415

VSA Type 1460

AVP Type GROUPED

Supported group value(s):

[TRACE_DEPTH_PER_NE_TYPE]

AVP Flag M

Trace-Depth-Per-NE-Type

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

Vendor ID 10415

VSA Type 1451

AVP Type GROUPED

Supported group value(s):

[NETWORK_ELEMENT_TYPE]

[TRACE_DEPTH]

AVP Flag M

Trace-Event-List

Trace-Event-List

Vendor ID 10415

VSA Type 1465

AVP Type OCTETSTRING

AVP Flag M

Trace-Interface-List

Trace-Interface-List

Vendor ID 10415

VSA Type 1464

AVP Type OCTETSTRING

AVP Flag M

Trace-NE-Type-List

This AVP contains the concatenation of MCC MNC.

Vendor ID 10415

VSA Type 1463

AVP Type OCTETSTRING

AVP Flag M

Trace-Reference

This AVP contains the concatenation of MCC MNC.

Vendor ID 10415

VSA Type 1459

AVP Type OCTETSTRING

AVP Flag M

Tracking-Area-Identity

This AVP contains the tracking area identifier of the user.

Vendor ID 10415

VSA Type 1603

AVP Type OCTETSTRING

AVP Flag M

Traffic-Data-Volumes

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

Vendor ID 10415

VSA Type 2046

AVP Type GROUPED

Supported group value(s):

[QOS_INFORMATION]

[ACCOUNTING_INPUT_OCTETS]

[ACCOUNTING_INPUT_PACKETS]

[ACCOUNTING_OUTPUT_OCTETS]

[ACCOUNTING_OUTPUT_PACKETS]

[CHANGE_CONDITION]

[CHANGE_TIME]

[3GPP_USER_LOCATION_INFO]

AVP Flag M

Transcoder-Inserted-Indication

Transcoder-Inserted-Indication

Vendor ID 10415

VSA Type 2605

AVP Type ENUM

Supported enumerated value(s): none

AVP Flag M

Transport-Class

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

Vendor ID 13019

VSA Type 311

AVP Type UINT32

AVP Flag N/A

Trigger-Action-Name

Trigger-Action-Name

Vendor ID 9

VSA Type 132088

AVP Type OCTETSTRING

AVP Flag N/A

Trunk-Group-ID

This grouped AVP identifies the incoming and outgoing PSTN legs.

Vendor ID 10415

VSA Type 851

AVP Type GROUPED

Supported group value(s):

[INCOMING_TRUNK_GROUP_ID]

[OUTGOING_TRUNK_GROUP_ID]

AVP Flag M

Tunnel-Assignment-Id

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

Vendor ID 0

VSA Type 82

AVP Type OCTETSTRING

AVP Flag M

Tunnel-Client-Auth-Id

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

Vendor ID 0

VSA Type 90

AVP Type UTF8STRING

AVP Flag M

Tunnel-Client-Endpoint

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

Vendor ID 0

VSA Type 66

AVP Type UTF8STRING

AVP Flag M

Tunnel-Header-Filter

Tunnel-Header-Filter

Vendor ID 10415

VSA Type 1036

AVP Type IPFILTERRULE

AVP Flag M

Tunnel-Header-Length

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

Vendor ID 10415

VSA Type 1037

AVP Type UINT32

AVP Flag M

Tunnel-Information

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

Vendor ID 10415

VSA Type 1038

AVP Type GROUPED

Supported group value(s):

[TUNNEL_HEADER_LENGTH]

[TUNNEL_HEADER_FILTER]

AVP Flag M

Tunnel-Medium-Type

This AVP contains the transport medium to use when creating a tunnel for protocols (such as L2TP) that can operate over multiple transports.

Vendor ID 0

VSA Type 65

AVP Type ENUM

Supported enumerated value(s):

1 IPv4_IPversion4

2 IPv6_IPversion6

3 NSAP

4 HDLC-8-bit_multidrop

5 BBN-1822

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

7 E163_POTS

8 E164_SMDS_Frame-Relay_ATM

9 F69_Telex

10 X121_X25_Frame-Relay

11 IPX

12 Appletalk

13 Decnet_IV

14 Banyan_Vines

15 E164-with-NSAP-format-subaddress

AVP Flag M

Tunnel-Password

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

Vendor ID 0

VSA Type 69

AVP Type OCTETSTRING

AVP Flag M

Tunnel-Preference

Used to identify the relative preference assigned to each tunnel when more than one set of tunneling AVPs is returned within separate Grouped-AVPs.

Vendor ID 0

VSA Type 83

AVP Type UINT32

AVP Flag M

Tunnel-Private-Group-Id

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

Vendor ID 0

VSA Type 81

AVP Type OCTETSTRING

AVP Flag M

Tunnel-Server-Auth-Id

This AVP contains the name used by the tunnel terminator during the authentication phase of tunnel establishment.

Vendor ID 0

VSA Type 91

AVP Type UTF8STRING

AVP Flag M

Tunnel-Server-Endpoint

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

Vendor ID 0

VSA Type 67

AVP Type UTF8STRING

AVP Flag M

Tunnel-Type

This AVP contains the tunneling protocol(s) to be used (in the case of a tunnel initiator) or in use (in the case of a tunnel terminator).

Vendor ID 0

VSA Type 64

AVP Type ENUM

Supported enumerated value(s):

1 Point-to-Point_Tunneling_Protocol-PPTP

2 Layer-Two-Forwarding_L2F

3 Layer-Two-Tunneling_Protocol-L2TP

4 Ascend-Tunnel-Management-Protocol-ATMP

5 Virtual-Tunneling-Protocol-VTP

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

7 IP-in-IP_Encapsulation_IP-IP

8 Minimal_IP-in-IP_Encapsulation_MIN-IP-IP

9 IP_Encapsulating_Security_Payload_in_the_Tunnel-mode_ESP

10 Generic_Route_Encapsulation_GRE

11 Bay_Dial_Virtual_Services-DVS

12 IP-in-IP-Tunneling

13 Virtual-LANs-VLAN

AVP Flag M

Tunneling

Used to describe a compulsory tunnel service.

Vendor ID 0

VSA Type 401

AVP Type GROUPED

Supported group value(s):

[TUNNEL_TYPE]

[TUNNEL_MEDIUM_TYPE]

[TUNNEL_CLIENT_ENDPOINT]

[TUNNEL_SERVER_ENDPOINT]

[TUNNEL_PREFERENCE]

[TUNNEL_CLIENT_AUTH_ID]

[TUNNEL_SERVER_AUTH_ID]

[TUNNEL_ASSIGNMENT_ID]

[TUNNEL_PASSWORD]

[TUNNEL_PRIVATE_GROUP_ID]

AVP Flag M

UAR-Flags

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

Vendor ID 0

VSA Type 637

AVP Type UINT32

AVP Flag M

UDP-Source-Port

This AVP contains the UDP source port number. This AVP is included on S2b interface if NAT is detected and UE Local IP Address is present for Fixed Broadband access network.

Vendor ID 10415

VSA Type 2806

AVP Type UINT32

AVP Flag N/A

UE-Count

UE-Count

Vendor ID 10415

VSA Type 4308

AVP Type UINT32

AVP Flag M

UE-Local-IP-Address

UE-Local-IP-Address

Vendor ID 10415

VSA Type 2805

AVP Type ADDRESS

AVP Flag N/A

UE-Reachability-Configuration

UE-Reachability-Configuration

Vendor ID 10415

VSA Type 3129

AVP Type GROUPED

Supported group value(s):

[REACHABILITY_TYPE]

[MAXIMUM_LATENCY]

[MAXIMUM_RESPONSE_TIME]

AVP Flag M

UE-SRVCC-Capability

UE-SRVCC-Capability

Vendor ID 10415

VSA Type 1615

AVP Type ENUM

Supported enumerated value(s):

0 UE-SRVCC-NOT-SUPPORTED

1 UE-SRVCC-SUPPORTED

AVP Flag M

UE-Usage-Type

This AVP is a subscription information parameter that is stored in the HSS, used by the serving network to select the Dedicated Core Network (DCN) that must serve the UE. Multiple UE Usage Types can be served by the same DCN.

Note A single UE subscription can be associated only with a single UE Usage Type, which describes its characteristics and functions.

Vendor ID 10415

VSA Type 1680

AVP Type UINT32

AVP Flag M

ULA-Flags

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

Vendor ID 10415

VSA Type 6007

AVP Type UINT32

AVP Flag M

ULR-Flags

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

Vendor ID 10415

VSA Type 6006

AVP Type UINT32

AVP Flag M

UMTS-Vector

This AVP contains Authentication Information for UMTS.

Vendor ID 10415

VSA Type 6018

AVP Type GROUPED

Supported group value(s):

[ITEM_NUMBER]

[RAND]

[XRES]

[AUTN]

[CONFIDENTIALITY_KEY]

[INTEGRITY_KEY]

AVP Flag M

UTRAN-Vector

This AVP contains Authentication Information for UTRAN.

Vendor ID 10415

VSA Type 1415

AVP Type GROUPED

Supported group value(s):

[ITEM_NUMBER]

[RAND]

[XRES]

[AUTN]

[CONFIDENTIALITY_KEY]

[INTEGRITY_KEY]

AVP Flag M

UWAN-User-Location-Info

UWAN-User-Location-Info

Vendor ID 10415

VSA Type 3918

AVP Type GROUPED

Supported group value(s):

[UE_LOCAL_IP_ADDRESS]

[UDP_SOURCE_PORT]

[SSID]

[BSSID]

AVP Flag M

Unit-Value

This AVP contains cost estimate (type of money) of the service.

Vendor ID 0

VSA Type 445

AVP Type GROUPED

Supported group value(s):

[VALUE_DIGITS]

[EXPONENT]

AVP Flag M

Uplink-Rate-Limit

Uplink-Rate-Limit

Vendor ID 10415

VSA Type 4311

AVP Type UINT32

AVP Flag M

Usage-Monitoring-Information

This AVP contains the usage monitoring control information.

Vendor ID 10415

VSA Type 1067

AVP Type GROUPED

Supported group value(s):

[MONITORING_KEY]

[GRANTED_SERVICE_UNIT]

[USED_SERVICE_UNIT]

[USAGE_MONITORING_LEVEL]

[USAGE_MONITORING_REPORT]

[USAGE_MONITORING_SUPPORT]

AVP Flag N/A

Usage-Monitoring-Level

This AVP is used by the PCRF to indicate whether the usage monitoring instance applies to the IP-CAN session or to one or more PCC rules.

Vendor ID 10415

VSA Type 1068

AVP Type ENUM

Supported enumerated value(s):

0 SESSION_LEVEL

1 PCC_RULE_LEVEL

AVP Flag N/A

Usage-Monitoring-Report

This AVP is used by the PCRF to indicate that accumulated usage is to be reported by the PCEF regardless of whether a usage threshold is reached for certain usage monitoring key.

Vendor ID 10415

VSA Type 1069

AVP Type ENUM

Supported enumerated value(s):

0 USAGE_MONITORING_REPORT_REQUIRED

AVP Flag N/A

Usage-Monitoring-Support

This AVP is used by the PCRF to indicate whether usage monitoring should be disabled for certain Monitoring Key.

Vendor ID 10415

VSA Type 1070

AVP Type ENUM

Supported enumerated value(s):

0 USAGE_MONITORING_DISABLED

AVP Flag N/A

Used-Service-Unit

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

Vendor ID 0

VSA Type 446

AVP Type GROUPED

Supported group value(s):

[TARIFF_TIME_CHANGE]

[TARIFF_CHANGE_USAGE]

[CC_TIME]

[CC_MONEY]

[CC_TOTAL_OCTETS]

[CC_INPUT_OCTETS]

[CC_OUTPUT_OCTETS]

[CC_SERVICE_SPECIFIC_UNITS]

AVP Flag M

User-Authorization-Type

This AVP contains the type of user authorization being performed in a User Authorization operation.

Vendor ID 10415

VSA Type 623

AVP Type ENUM

Supported enumerated value(s):

0 REGISTRATION

1 DE_REGISTRATION

2 REGISTRATION_AND_CAPABILITIES

AVP Flag M

User-CSG-Information

User-CSG-Information

Vendor ID 10415

VSA Type 2319

AVP Type GROUPED

Supported group value(s):

[CSG_ID]

[CSG_ACCESS_MODE]

[CSG_MEMBERSHIP_INDICATION]

AVP Flag M

User-Data

This AVP contains the user data requested in the PUR and SNR operations and the data to be modified in the UPR operations.

Vendor ID 0

VSA Type 702

AVP Type OCTETSTRING

AVP Flag M

User-Data-Already-Available

This AVP indicates whether S-CSCF is already storing the user data or not.

Vendor ID 10415

VSA Type 624

AVP Type ENUM

Supported enumerated value(s):

0 USER_DATA_NOT_AVAILABLE

1 USER_DATA_ALREADY_AVAILABLE

AVP Flag M

User-Default

User-Default

Vendor ID 9

VSA Type 131200

AVP Type ENUM

Supported enumerated value(s):

0 DISABLED

1 ENABLED

AVP Flag M

User-Equipment-Info

This AVP indicates the identification and capabilities of the terminal.

Vendor ID 0

VSA Type 458

AVP Type GROUPED

Supported group value(s):

[USER_EQUIPMENT_INFO_TYPE]

[USER_EQUIPMENT_INFO_VALUE]

AVP Flag M

User-Equipment-Info-Type

Defines the type of information present in User-Equipment-Info-Value AVP.

Vendor ID 0

VSA Type 459

AVP Type ENUM

Supported enumerated value(s):

0 IMEISV

1 MAC

2 EUI64

3 MODIFIED_EUI64

4 ESN

5 MEID

AVP Flag M

User-Equipment-Info-Value

Defines the type of identifier used.

Vendor ID 0

VSA Type 460

AVP Type OCTETSTRING

AVP Flag M

User-Id

User-Id

Vendor ID 10415

VSA Type 1444

AVP Type UTF8STRING

AVP Flag M

User-Identifier

User-Identifier

Vendor ID 10415

VSA Type 3102

AVP Type GROUPED

Supported group value(s):

[USER_NAME]

AVP Flag M

User-Identity

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

Vendor ID 10415

VSA Type 700

AVP Type GROUPED

Supported group value(s):

[PUBLIC_IDENTITY]

[MSISDN]

AVP Flag M

User-Idle-Pod

User-Idle-Pod

Vendor ID 9

VSA Type 131234

AVP Type ENUM

Supported enumerated value(s):

0 DISABLED

1 ENABLED

AVP Flag M

User-Idle-Timer

User-Idle-Timer

Vendor ID 9

VSA Type 131119

AVP Type UINT32

AVP Flag N/A

User-Location-Info-Time

User-Location-Info-Time

Vendor ID 10415

VSA Type 2812

AVP Type UINT32

AVP Flag N/A

User-Name

This AVP contains identification of the service user in a format consistent with the Network Access Identifier (NAI) specification.

Vendor ID 0

VSA Type 1

AVP Type UTF8STRING

AVP Flag M

User-Password

This AVP indicates PAP for multiauth in PDG.

Vendor ID 0

VSA Type 2

AVP Type OCTETSTRING

AVP Flag M

User-Session-Id

This AVP holds the session identifier.

Vendor ID 10415

VSA Type 830

AVP Type UTF8STRING

AVP Flag M

User-State

User-State

Vendor ID 10415

VSA Type 1499

AVP Type ENUM

Supported enumerated value(s):

0 DETACHED

1 ATTACHED_NOT_REACHABLE_FOR_PAGING

2 ATTACHED_REACHABLE_FOR_PAGING

3 CONNECTED_NOT_REACHABLE_FOR_PAGING

4 CONNECTED_REACHABLE_FOR_PAGING

5 NETWORK_DETERMINED_NOT_REACHABLE

AVP Flag M

V4-Transport-Address

This AVP contains a single IPv4 address and a single port number.

Vendor ID 13019

VSA Type 454

AVP Type GROUPED

Supported group value(s):

[FRAMED_IP_ADDRESS]

[PORT_NUMBER]

AVP Flag N/A

V6-Transport-Address

This AVP contains a single IPv6 address and a single port number.

Vendor ID 13019

VSA Type 453

AVP Type GROUPED

Supported group value(s):

[FRAMED_IPV6_PREFIX]

[PORT_NUMBER]

AVP Flag N/A

VLAN-Id

VLAN-Id

Vendor ID 9

VSA Type 131154

AVP Type UINT32

AVP Flag N/A

VPLMN-Dynamic-Address-Allowed

This AVP indicates whether for this APN, the UE is allowed to use the PDN GW in the domain of the HPLMN only, or additionally, the PDN GW in the domain of the VPLMN.

Vendor ID 10415

VSA Type 1432

AVP Type ENUM

Supported enumerated value(s):

0 NOTALLOWED

1 ALLOWED

AVP Flag M

VRF-Name

VRF-Name

Vendor ID 9

VSA Type 131153

AVP Type OCTETSTRING

AVP Flag M

Validity-Time

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

Vendor ID 0

VSA Type 448

AVP Type UINT32

AVP Flag M

Value-Digits

This AVP contains the significant digits of the number. If decimal values are needed to present the units, the scaling MUST be indicated with the related Exponent AVP.

Vendor ID 0

VSA Type 447

AVP Type INT64

AVP Flag M

Velocity-Estimate

This attribute is composed of 4 or more octets with an internal structure defined according to 3GPP TS 23.032.

Vendor ID 10415

VSA Type 2515

AVP Type OCTETSTRING

AVP Flag M

Velocity-Requested

Velocity-Requested

Vendor ID 10415

VSA Type 2508

AVP Type ENUM

Supported enumerated value(s):

0 VELOCITY_IS_NOT_REQUESTED

1 VELOCITY_IS_REQUESTED

AVP Flag M

Vendor-Id

Unique Identifier of the Vendor and contains the IANA "SMI Network Management Private Enterprise Codes" value assigned to the vendor of the Diameter application.

Vendor ID 0

VSA Type 266

AVP Type UINT32

AVP Flag M

Vendor-Id-Resp

Unique identifier of the vendor.

Vendor ID 10415

VSA Type 266

AVP Type UINT32

AVP Flag N/A

Vendor-Specific-Application-Id

Specifies the Vendor Specific Application ID and is used to advertise support of a vendor-specific Diameter Application.

Vendor ID 0

VSA Type 260

AVP Type GROUPED

Supported group value(s):

[VENDOR_ID]

[AUTH_APPLICATION_ID]

[ACCT_APPLICATION_ID]

AVP Flag M

Vendor-Specific-QoS-Profile-Template

This AVP defines the namespace of the QoS profile (indicated in the Vendor-ID AVP) followed by the specific value for the profile.

Vendor ID 0

VSA Type 6064

AVP Type GROUPED

Supported group value(s):

[VENDOR_ID]

[QOS_PROFILE_TEMPLATE]

AVP Flag M

Verify

Verify

Vendor ID 9

VSA Type 131116

AVP Type GROUPED

Supported group value(s):

[CONFIRM_TOKEN]

AVP Flag M

Vertical-Accuracy

This AVP is of type Unsigned32. Bits 6-0 correspond to Uncertainty Code defined in 3GPP TS 23.032. The vertical location error should be less than the error indicated by the uncertainty code with 67% confidence. Bits 7 to 31 are ignored.

Vendor ID 10415

VSA Type 2506

AVP Type ENUM

Supported enumerated value(s):

1 VERTICAL_COORDINATE_IS_REQUESTED

AVP Flag M

Vertical-Requested

Vertical-Requested

Vendor ID 10415

VSA Type 2507

AVP Type ENUM

Supported enumerated value(s):

1 VERTICAL_COORDINATE_IS_REQUESTED

AVP Flag M

Virtual-Online

Virtual-Online

Vendor ID 9

VSA Type 131210

AVP Type ENUM

Supported enumerated value(s):

0 DISABLED

1 ENABLED

AVP Flag M

Visited-Network-Identifier

This AVP contains an identifier that helps the home network to identify the visited network (for example, the visited network domain name).

Vendor ID 10415

VSA Type 600

AVP Type OCTETSTRING

AVP Flag M

Visited-PLMN-Id

This AVP contains the concatenation of MCC and MNC.

Vendor ID 10415

VSA Type 6008

AVP Type UTF8STRING

AVP Flag M

Volume-Threshold

Volume-Threshold

Vendor ID 9

VSA Type 131080

AVP Type UINT32

AVP Flag N/A

Volume-Threshold-64

Volume-Threshold-64

Vendor ID 9

VSA Type 131258

AVP Type UINT32

AVP Flag N/A

WLAN-Session-Id

This AVP contains the WLAN Session ID that is used to correlate PDG and WLAN AN charging data.

Vendor ID 0

VSA Type 11009

AVP Type UINT32

AVP Flag M

Weight

Weight

Vendor ID 9

VSA Type 131118

AVP Type UINT32

AVP Flag N/A

WiMAX-A-PCEF-Address

This AVP indicates the IP address of the A-PCEF to the PDF.

Vendor ID 24757

VSA Type 411

AVP Type ADDRESS

AVP Flag M

WiMAX-PCC-R3-P-Capability

This AVP contains in a CCR message the WiMAX capabilities supported by the ASN. In a CCA it identifies the options selected by the PCRF.

Vendor ID 24757

VSA Type 404

AVP Type GROUPED

Supported group value(s):

[WIMAX_RELEASE]

[ACCOUNTING_PCC_R3_P_CAPABILITY]

AVP Flag M

WiMAX-QoS-Information

This AVP contains the WiMAX QoS information for ASN GW.

Vendor ID 24757

VSA Type 407

AVP Type GROUPED

Supported group value(s):

[QOS_CLASS_IDENTIFIER]

[MAX_REQUESTED_BANDWIDTH_UL]

[MAX_REQUESTED_BANDWIDTH_DL]

[GUARANTEED_BITRATE_UL]

[GUARANTEED_BITRATE_DL]

[PACKET_INTERVAL]

[PACKET_SIZE]

AVP Flag M

WiMAX-Release

This AVP indicates a WiMAX release formatted as major/minor.

Vendor ID 24757

VSA Type 301

AVP Type OCTETSTRING

AVP Flag M

Wildcarded-IMPU

This AVP contains a wild-carded Public User Identity stored in the HSS.

Vendor ID 10415

VSA Type 636

AVP Type UTF8STRING

AVP Flag N/A

Wildcarded-PSI

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

Vendor ID 10415

VSA Type 634

AVP Type UTF8STRING

AVP Flag M

Wildcarded-Public-Identity

This AVP contains a Wildcarded PSI or Wildcarded Public User Identity stored in the HSS.

Vendor ID 10415

VSA Type 634

AVP Type UTF8STRING

AVP Flag N/A

XRES

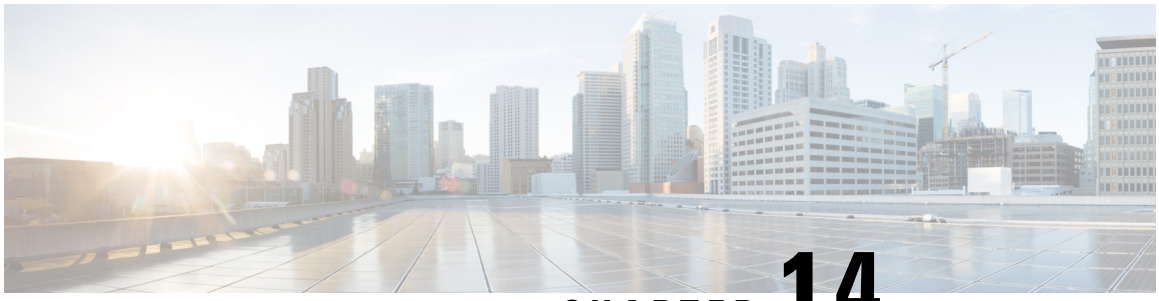
This AVP contains the XRES (Expected Response USIM).

Vendor ID 10415

VSA Type 1448

AVP Type OCTETSTRING

AVP Flag M



CHAPTER 14

RADIUS Dictionaries and Attribute Definitions

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

RADIUS Dictionaries

This section presents information on RADIUS dictionary types.

Dictionary Types

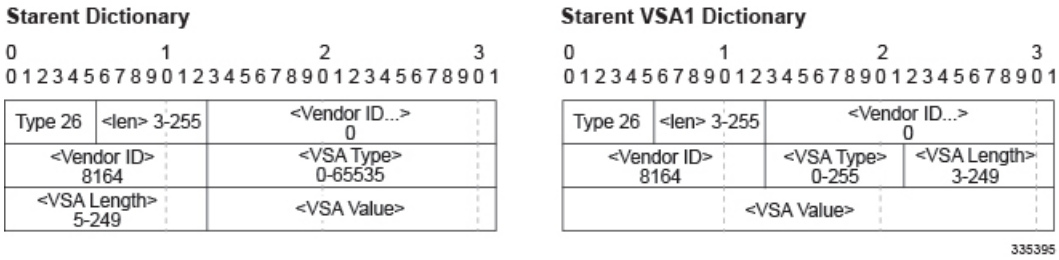
The CLI command to specify the RADIUS dictionary is:

radius dictionary [3gpp | 3gpp2 | 3gpp2-835 | custom *XX* **| standard | starent | starent-835 | starent-vsa1 | starent-vsa1-835]**

Keyword	Description
custom*XX*	These dictionaries can be customized. Customization information can be obtained by contacting your local service representative. *XX* is the integer value of the custom dictionary. **Note** RADIUS dictionary custom23 should be used in conjunction with Enhanced Charging Service (ECS).
standard	This dictionary consists only of the attributes specified in RFC 2865, RFC 2866, and RFC 2869. It also supports 3GPP release 4 and 3GPP Release 5 - extended QoS format.
3gpp	This dictionary consists not only of all of the attributes in the standard dictionary, but also all of the attributes specified in 3GPP 32.015.

Keyword	Description
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. **Note** In 12.0 and later releases, no new RADIUS/Diameter attributes can be added to the **starent-vsa1** dictionary. If there are any new attributes to be added, these can be added to the **starent** dictionary.
starent-vsa1-835	This dictionary consists of the 3GPP2-835 dictionary, and includes the vendor-specific attributes (VSAs) as well. The VSAs in this dictionary support a one-byte wide VSA Type field in order to support certain RADIUS applications. The one-byte limit allows support for only 256 VSAs (0 - 255) as shown in the following figure.
starent	This dictionary consists of all of the attributes in the starent-vsa1 dictionary and incorporates additional VSAs by using a two-byte VSA Type field as shown in the following figure. This dictionary is the master-set of all of the attributes in all of the dictionaries supported by the system.
starent-835	This dictionary consists of all of the attributes in the starent-vsa1-835 dictionary and incorporates additional VSAs by using a two-byte VSA Type field. This dictionary is the master-set of all of the attributes in all of the -835 dictionaries supported by the system.

Figure 3: Difference in VSA Value Lengths per Dictionary



Note Customer-specific attributes are not documented in this reference. For information on customer-specific attributes, contact your Cisco account representative.

Note The length documented for each attribute is the length of the attribute's Value field (data portion) and not length of the attribute (Type + Length + Value fields).

RADIUS Attribute 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.

RADIUS AVP Definitions

This section presents RADIUS attribute definitions.

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

3GPP2-835-Release-Indicator

3GPP2 835 Standard Release Indicator, reason/cause for session release.

Syntax Enumerated Integer. Supports the following value(s):

- Unknown = 0
- PPP-Timeout = 1
- Handoff = 2
- PPP-Termination = 3
- Mobile-IP-Registration-Failure = 4
- Active-To-Dormant = 5

Length 4

Type 26

Vendor ID 5535

VSA Type 24

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.

Syntax Unsigned Integer

Length 4

Type 46

Vendor ID N/A

VSA Type N/A

3GPP2-Active-Time-Corrected

3GPP2 Active session time value.

Syntax Unsigned Integer

Length 4

Type 26

Vendor ID 5535

VSA Type 49

3GPP2-Active-Time

The total period of time spent in the Active state, in seconds.

Syntax Unsigned Integer

Length 4

Type 26

Vendor ID 5535

VSA Type 49

3GPP2-Airlink-Record-Type

This attribute indicates the most recent type of Airlink Record to be received for this subscriber's connection.

Syntax Enumerated Integer. Supports the following value(s):

- Connection-Setup = 1
- Active-Start = 2
- Active-Stop = 3
- SDB = 4 BCMCS-Connection-Setup = 5
- BCMCS-Active-Start = 6
- BCMCS-Active-Stop = 7

Length 4

Type 26

Vendor ID 5535

VSA Type 40

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.

Syntax Unsigned Integer

Length 4

Type 26

Vendor ID 5535

VSA Type 42

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.

Syntax Unsigned Integer

Length 4

Type 26

Vendor ID 5535

VSA Type 39

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

Syntax Compound. Contains the following sub-attribute(s).

Flags

Allowed DSCP flag.

Syntax Enumerated Integer. Supports the following value(s):

- 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

Length 2

Type 1

Max-Class

Allowed max dscp.

Syntax Enumerated Integer. Supports the following value(s):

- 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

Length 2

Type 2

RT-Marking

Allowed max dscp rev. tun.

Syntax Enumerated Integer. Supports the following value(s):

- 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

Length 2

Type 3

3GPP2-Allowed-Persistent-TFTs

3GPP2 Allowed Persistent Traffic Flow Templates.

Syntax Unsigned Integer

Length 4

Type 26

Vendor ID 5535

VSA Type 89

3GPP2-Alternate-Billing-ID

This attribute is currently not supported.

Syntax Unsigned Integer

Length 4

Type 26

Vendor ID 5535

VSA Type 35

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.

Syntax Enumerated Integer. Supports the following value(s):

- Inactive = 0
- Active = 1

Length 4

Type 26

Vendor ID 5535

VSA Type 78

3GPP2-Auth-Flow-Profile-Id

This compound attribute is a list of flow profile IDs.

Type 26

Vendor ID 5535

VSA Type 131

Syntax Compound. Contains the following sub-attribute(s).

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.

Syntax Unsigned Integer

Length 2

Type 1

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.

Syntax Unsigned Integer

Length 2

Type 2

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.

Syntax Unsigned Integer

Length 2

Type 3

3GPP2-Bad-PPP-Frame-Count

The total number of PPP frames from the MS dropped by the PDSN due to uncorrectable errors.

Syntax Unsigned Integer

Length 4

Type 26

Vendor ID 5535

VSA Type 25

3GPP2-BCMCS-Auth-Parameters

This is a grouped attribute 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

Syntax Compound. Contains the following sub-attribute(s).

BAK-Sequence-Number

BAK-Sequence-Number

Syntax Opaque Value

Length 1

Type 1

Timestamp

Timestamp

Syntax Opaque Value

Length 33

Type 2

Auth-Signature

Auth-Signature

Syntax Unsigned Integer

Length 4

Type 3

3GPP2-BCMCS-BSN-Session-Info

This is a grouped attribute 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

Syntax Compound. Contains the following sub-attribute(s).

Flow-Id

This attribute specifies the Granted QoS parameters received from the RAN for the flow identified by FLOW_ID.

Syntax Unsigned Integer

Length 2

Type 2

Mcast-IP-Addr

Mcast-IP-Addr

Syntax IPv4 Address

Length 4

Type 2

Mcast-Port

Mcast-Port

Syntax Unsigned Integer

Length 2

Type 3

Header-Compression-Algorithm

Header-Compression-Algorithm

Syntax Enumerated Integer. Supports the following value(s):

- No_header_compression = 0
- ROHC_U_Mode = 1

Length 2

Type 4

CID-Type-Attribute

CID-Type-Attribute

Syntax Unsigned Integer

Length 1

Type 5

MAX-CID

MAX-CID

Syntax Unsigned Integer

Length 2

Type 6

Compression-Profile

Compression-Profile

Syntax Unsigned Integer

Length 2

Type 7

MAX-Header-Size

MAX-Header-Size

Syntax Unsigned Integer

Length 2

Type 8

MRRU

MRRU

Syntax Unsigned Integer

Length 2

Type 9

Content-Server-Source-IP-Address

Content-Server-Source-IP-Address

Syntax IPv4 Address

Length 4

Type 10

Content-Server-Source-IPv6-Address

Content-Server-Source-IPv6-Address

Syntax Opaque Value

Length 16

Type 11

3GPP2-BCMCS-Capability

This attribute defines the specific BCMCS protocol revision the PDSN supports.

Type 26

Vendor ID 5535

VSA Type 101

Syntax Compound. Contains the following sub-attribute(s).

BCMCS-Protocol-Revision

BCMCS-Protocol-Revision

Syntax Enumerated Integer. Supports the following value(s):

- Release_0 = 1

Length 2

Type 1

3GPP2-BCMCS-Common-Session-Info

This compound attribute 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

Syntax Compound. Contains the following sub-attribute(s).

Flow-ID

Flow-ID

Syntax Opaque Value

Length 2-4

Type 1

Program-Start-Time

Program-Start-Time

Syntax Unsigned Integer

Length 4

Type 2

Program-End-Time

Program-End-Time

Syntax Unsigned Integer

Length 4

Type 3

Program-Allowed-Registration-Time

Program-Allowed-Registration-Time

Syntax Unsigned Integer

Length 4

Type 4

Auth-Required-Flag

Auth-Required-Flag

Syntax Enumerated Integer. Supports the following value(s):

- Authorization_not_required = 0
- Authorization_required = 1

Length 2

Type 5

3GPP2-BCMCS-Flow-ID

This attribute specifies the BCMCS Flow ID.

Syntax Opaque Value

Length 2-4

Type 26

Vendor ID 5535

VSA Type 100

3GPP2-BCMCS-Flow-Transmit-Time

The total BCMCS flow transmission time in seconds.

Syntax Unsigned Integer

Length 4

Type 26

Vendor ID 5535

VSA Type 107

3GPP2-BCMCS-Mcast-IP-Addr

This attribute contains the multicast IP address of the BCMCS flow as it would appear in the source or destination field of an IP header.

Syntax IPv4 Address

Length 4

Type 26

Vendor ID 5535

VSA Type 109

3GPP2-BCMCS-Mcast-Port

The multicast port for the BCMCS flow.

Syntax Unsigned Integer

Length 2

Type 26

Vendor ID 5535

VSA Type 110

3GPP2-BCMCS-Reason-Code

This attribute specifies the reason to send the RADIUS Access-Accept message.

Syntax Opaque Value

Length 1

Type 26

Vendor ID 5535

VSA Type 105

3GPP2-BCMCS-RN-Session-Info

This is a grouped attribute 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

Syntax Compound. Contains the following sub-attribute(s).

Flow-ID

Flow-ID

Syntax Opaque Value

Length 2-4

Type 1

BCMCS-Encryption-Mechanism-Attribute

BCMCS-Encryption-Mechanism-Attribute

Syntax Enumerated Integer. Supports the following value(s):

- High_layer_encryption_in_CS = 0
- Link_layer_encryption_in_RN = 1

Length 2

Type 2

BCMCS-BAK-ID-Attribute

BCMCS-BAK-ID-Attribute

Syntax Unsigned Integer

Length 1

Type 3

BCMCS-BAK

BCMCS-BAK

Syntax Opaque Value

Length 16

Type 4

BCMCS-BAK-Expire-Time

BCMCS-BAK-Expire-Time

Syntax Unsigned Integer

Length 4

Type 5

BCMCS-Session-Bandwidth-attribute

BCMCS-Session-Bandwidth-attribute

Syntax Unsigned Integer

Length 2

Type 6

3GPP2-Beginning-Session

3GPP2 Beginning Session will be TRUE or FALSE depending on if this is a new session.

Syntax Enumerated Integer. Supports the following value(s):

- False = 0
- True = 1

Length 4

Type 26

Vendor ID 5535

VSA Type 51

3GPP2-BSID

The base station ID.

Syntax Opaque Value

Length 6-12

Type 26

Vendor ID 5535

VSA Type 10

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.

Syntax Opaque Value

Length 5-6

Type 26

Vendor ID 5535

VSA Type 142

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.

Syntax Enumerated Integer. Supports the following value(s):

- No-Tunnel = 0
- Non-Secure-Tunnel = 1
- Secure-Tunnel = 2

Length 4

Type 26

Vendor ID 5535

VSA Type 23

3GPP2-Container

A compound attribute that encapsulates the User Data Record for an Airlink Event.

Type 26

Vendor ID 8164

VSA Type 240

Syntax Compound. Contains the following sub-attribute(s). enum16 reason { Tarrif-Boundary = 1, Parameter-Change = 2, Handoff = 3, Active-To-Dormant = 4 } uint32 timestamp attribute ThreeGPP2-BSID attribute ThreeGPP2-MEID attribute ThreeGPP2-FEID reason Parameter-Change { attribute ThreeGPP2-User-Zone attribute ThreeGPP2-Forward-Mux-Option attribute ThreeGPP2-Reverse-Mux-Option attribute ThreeGPP2-Service-Option attribute ThreeGPP2-Fwd-Pdch-Rc attribute ThreeGPP2-Fwd-Dcch-Mux-Option attribute ThreeGPP2-Rev-Dcch-Mux-Option attribute ThreeGPP2-Air-QOS } reason Handoff { attribute NAS-IP-Address attribute ThreeGPP2-Serving-PCF } attribute Acct-Output-Octets attribute Acct-Input-Octets attribute ThreeGPP2-Bad-PPP-Frame-Count attribute ThreeGPP2-Active-Time attribute ThreeGPP2-Number-Active-Transitions attribute ThreeGPP2-SDB-Input-Octets attribute ThreeGPP2-SDB-Output-Octets attribute ThreeGPP2-Num-SDB-Input attribute ThreeGPP2-Num-SDB-Output attribute ThreeGPP2-Num-Bytes-Received-Total attribute ThreeGPP2-MIP-Signaling-Octet-Count-Input attribute ThreeGPP2-MIP-Signaling-Octet-Count-Output attribute ThreeGPP2-Last-Activity attribute Starent-Acct-PPP-Unfr-data-In-Oct attribute Starent-Acct-PPP-Unfr-data-Out-Oct }

Type 26

Vendor ID 5535

VSA Type 6

3GPP2-Correlation-Id-Long

Syntax Opaque Value

Length 1-251

Type 26

Vendor ID 5535

VSA Type 44

3GPP2-Correlation-Id-Old

Custom-11 style correlation ID.

Syntax Opaque Value

Length 1-251

Type 26

Vendor ID 5535

VSA Type 40

3GPP2-Correlation-Id

This attribute contains an ID that correlates all accounting sessions authorized for this NAI by this access request.

Syntax Opaque Value

Length 1-251

Type 26

Vendor ID 5535

VSA Type 44

3GPP2-DCCH-Frame-Size

Specifies the DCCH frame size.

Syntax Enumerated Integer. Supports the following value(s):

- None = 0
- 5ms = 1
- 20ms = 2

Length 4

Type 26

Vendor ID 5535

VSA Type 50

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).

Syntax Unsigned Integer

Length 4

Type 26

Vendor ID 5535

VSA Type 5

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.

Syntax Enumerated Integer. Supports the following value(s):

- MS_Mobility_Detection = 1;

Length 4

Type 26

Vendor ID 5535

VSA Type 96

3GPP2-DNS-Server-IP-Address

DNS server IP address. Used in custom dictionary.

Type 26

Vendor ID 5535

VSA Type 117

Syntax Compound. Contains the following sub-attribute(s).

Primary-DNS-Server-IP

IP address of the primary DNS server.

Syntax IPv4 Address

Length 4

Type 1

Secondary-DNS-Server-IP

IP address of the secondary DNS server.

Syntax IPv4 Address

Length 4

Type 2

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.

Syntax Unsigned Integer

Length 1

Type 3

Entity-Type

Network Entity inserted in the DNS server ID address. Currently the following types are defined. HAAA = 1, VAAA = 1.

Syntax Unsigned Integer

Length 1

Type 4

3GPP2-DNS-Server-IPV6-Addr

DNS server IPv6 address.

Type 26

Vendor ID 5535

VSA Type 214

Syntax Compound. Contains the following sub-attribute(s).

Primary-DNS-Server-IPV6

Primary DNS server IPv6 address.

Syntax Opaque Value

Length 16

Type 1

Secondary-DNS-Server-IPV6

Secondary IPv6 DNS server IP address.

Syntax Opaque Value

Length 16

Type 2

Flag-IPV6

M bit set to 1 indicates to the PDSN that Primary and Secondary IPv6 addresses provided by the Home RADIUS server should override the Primary and Secondary IPv6 addresses provided also by the visited RADIUS server.

Syntax Unsigned Integer

Length 1

Type 3

Entity-Type-IPV6

Network Entity that inserted in the DNS server ID address. Either HAAA = 1, VAAA = 1.

Syntax Unsigned Integer

Length 1

Type 4

3GPP2-DNS-Update-Required

This attribute indicates whether the HA needs to send the DNS update to the DNS server.

Syntax Enumerated Integer. Supports the following value(s):

- No = 0
- Yes = 1

Length 4

Type 26

Vendor ID 5535

VSA Type 75

3GPP2-ESN

This attribute contains the Electronic Serial Number (ESN) of the Mobile Station.

Syntax Opaque Value

Length 1-15

Type 26

Vendor ID 5535

VSA Type 52

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.

Syntax IPv4 Address

Length 4

Type 26

Vendor ID 5535

VSA Type 79

3GPP2-FEID

This attribute specifies the FEID value.

Syntax Opaque Value

Length 0-16

Type 26

Vendor ID 5535

VSA Type 216

3GPP2-Flow-Id

This attribute specifies the 3GPP2-Flow-Id-parameter.

Type 26

Vendor ID 5535

VSA Type 144

Syntax Compound. Contains the following sub-attribute(s).

Direction

Direction of the PDF.

Syntax Enumerated Integer. Supports the following value(s):

- Forward = 0
- Reverse = 1
- Both = 2

Length 2

Type 1

Flow-Id

This attribute specifies the Granted QoS parameters received from the RAN for the flow identified by FLOW_ID.

Syntax Unsigned Integer

Length 2

Type 2

3GPP2-Flow-Status

This attribute specifies the 3GPP2 Flow Status.

Syntax Enumerated Integer. Supports the following value(s):

- Active = 0
- Inactive = 1

Length 4

Type 26

Vendor ID 5535

VSA Type 145

3GPP2-Forward-Fundamental-Rate

As defined in "Wireless IP Network Standard - 3GPP2.P.S0001-A-1".

Syntax Unsigned Integer

Length 4

Type 26

Vendor ID 5535

VSA Type 14

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.

Syntax Unsigned Integer

Length 4

Type 26

Vendor ID 5535

VSA Type 20

3GPP2-Forward-Mux-Option

Forward direction multiplexer option.

Syntax Unsigned Integer

Length 4

Type 26

Vendor ID 5535

VSA Type 12

3GPP2-Forward-Traffic-Type

Specifies the forward traffic type.

Syntax Enumerated Integer. Supports the following value(s):

- Primary = 0
- Secondary = 1

Length 4

Type 26

Vendor ID 5535

VSA Type 17

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.

Syntax Enumerated Integer. Supports the following value(s):

- None = 0
- 5ms = 1
- 20ms = 2

Length 4

Type 26

Vendor ID 5535

VSA Type 19

3GPP2-Fwd-Dcch-Mux-Option

This attribute specifies Forward DCCH Mux option.

Syntax Unsigned Integer

Length 4

Type 26

Vendor ID 5535

VSA Type 84

3GPP2-Fwd-Dcch-Rc

This attribute specifies Radio Configuration of the Forward Packet Data Channel.

Syntax Unsigned Integer

Length 4

Type 26

Vendor ID 5535

VSA Type 86

3GPP2-Fwd-Pdch-Rc

This attribute specifies Radio Configuration of the Forward Packet Data Channel.

Syntax Unsigned Integer

Length 4

Type 26

Vendor ID 5535

VSA Type 83

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.

Syntax Integer

Length 4

Type 26

Vendor ID 5535

VSA Type 143

3GPP2-Granted-QoS

This attribute specifies the 3GPP2-Granted-QoS-Parameter.

Type 26

Vendor ID 5535

VSA Type 132

Syntax Compound. Contains the following sub-attribute(s).

Direction

Direction of the PDF.

Syntax Enumerated Integer. Supports the following value(s):

- Forward = 0
- Reverse = 1
- Both = 2

Length 2

Type 1

Flow-Id

This attribute specifies the Granted QoS parameters received from the RAN for the flow identified by FLOW_ID.

Syntax Unsigned Integer

Length 2

Type 2

Attribute-Set-Id

This attribute specifies the Granted QoS parameters received from the RAN for flow verbose or non-verbose.

Syntax Unsigned Integer

Length 2

Type 3

Flow-Profile-Id

This attribute specifies the Granted QoS parameters received from the RAN for the flow profile ID.

Syntax Unsigned Integer

Length 2

Type 4

Traffic-Class

This attribute specifies the Granted QoS parameters received from the RAN for the flow traffic class.

Syntax Enumerated Integer. Supports the following value(s):

- Unknown = 0

- Conversational = 1
- Streaming = 2
- Interactive = 3
- Background = 4

Length 2

Type 5

Peak-Rate

This attribute specifies the Granted QoS parameters received from the RAN for the flow Peak Rate.

Syntax Unsigned Integer

Length 2

Type 6

Bucket-Rate

This attribute specifies the Granted QoS parameters received from the RAN for the flow Bucket Rate.

Syntax Unsigned Integer

Length 2

Type 7

Token-Rate

This attribute specifies the Granted QoS parameters received from the RAN for the flow Token Rate.

Syntax Unsigned Integer

Length 2

Type 8

Max-Latency

This attribute specifies the Granted QoS parameters received from the RAN for the flow Max Latency.

Syntax Unsigned Integer

Length 2

Type 9

Max-IP-Packet-Loss-Rate

This attribute specifies the Granted QoS parameters received from the RAN for the flow Packet Loss Rate.

Syntax Unsigned Integer

Length 2

Type 10

Packet-Size

This attribute specifies the Granted QoS parameters received from the RAN for the flow Packet Size.

Syntax Unsigned Integer

Length 2

Type 11

Delay-Var-Sensitive

This attribute specifies the Granted QoS parameters received from the RAN for the flow Delay Var Sensitive.

Syntax Enumerated Integer. Supports the following value(s):

- Not-Specified = 0
- Sensitive = 1

Length 2

Type 12

3GPP2-IKE-Secret-Request

This attribute indicates if the IKE secret for the FA/HA pair is to be returned for the subscriber.

Syntax Enumerated Integer. Supports the following value(s):

- No = 0
- Yes = 1

Length 4

Type 26

Vendor ID 5535

VSA Type 1

3GPP2-IKE-Secret

This attribute contains the FA/HA shared secret for the IKE protocol. This attribute is salt-encrypted.

Syntax Opaque Value

Length 1-247

Type 26

Vendor ID 5535

VSA Type 3

3GPP2-IKE-Secret-Unencrypted

IKE Secret key from RADIUS server in Access-Accept message

Syntax Opaque Value

Length 1-247

Type 26

Vendor ID 5535

VSA Type 3

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.

Syntax Opaque Value

Length 1-253

Type 26

Vendor ID 5535

VSA Type 1

3GPP2-Interconnect-IP

This attribute is currently not supported.

Syntax IPv4 Address

Length 4

Type 26

Vendor ID 5535

VSA Type 37

3GPP2-Interconnect-QOS

This attribute is currently not supported.

Syntax Unsigned Integer

Length 4

Type 26

Vendor ID 5535

VSA Type 38

3GPP2-Inter-User-Priority

This attribute specifies the 3GPP2-Inter-User-Priority.

Syntax Unsigned Integer

Length 4

Type 26

Vendor ID 5535

VSA Type 139

3GPP2-IP-QOS

This attribute defines the differentiated Services code points associated with the user data.

Syntax Enumerated Integer. Supports the following value(s):

- Best-Effort = 0
- CS1 = 8
- AF11 = 10
- AF12 = 12
- AF13 = 14
- CS2 = 16
- AF21 = 18
- AF22 = 20
- AF23 = 22
- CS3 = 24
- AF31 = 26
- AF32 = 28
- AF33 = 30
- CS4 = 32
- AF41 = 34
- AF42 = 36
- AF43 = 38
- CS5 = 40
- EF = 46
- CS6 = 48
- CS7 = 56

Length 4

Type 26

Vendor ID 5535

VSA Type 36

3GPP2-IP-Services-Authorized

This attribute specifies the type of IP services (IPv4/CMIPv4/IPv6/CMIPv6/PMIPv4/PMIPv6..etc) authorized.

Syntax Enumerated Integer. Supports the following value(s):

- SIP4 = 1
- SIP6 = 2
- MIP4 = 4
- MIP6 = 8
- IP4_PMIP4 = 16
- IP6_PMIP4 = 32
- IP4_PMIP6 = 64
- IP6_PMIP6 = 128

Length 4

Type 26

Vendor ID 5535

VSA Type 185

3GPP2-IP-Technology

This attribute identifies whether we are using Simple IP, Mobile IP, or another technology.

Syntax Enumerated Integer. Supports the following value(s):

- Simple-IP = 1
- Mobile-IP = 2

Length 4

Type 26

Vendor ID 5535

VSA Type 22

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.

Syntax Opaque Value

Length 20

Type 26

Vendor ID 5535

VSA Type 8

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.

Syntax Unsigned Integer

Length 4

Type 26

Vendor ID 5535

VSA Type 80

3GPP2-Max-Auth-Aggr-Bw-BET

This attribute contains the maximum authorized aggregate bandwidth for Best Effort Traffic.

Syntax Unsigned Integer

Length 4

Type 26

Vendor ID 5535

VSA Type 130

3GPP2-Max-Per-Fl-Pri-ForTheUser

The maximum per flow priority for the user.

Syntax Unsigned Integer

Length 4

Type 26

Vendor ID 5535

VSA Type 133

3GPP2-MEID

Mobile Equipment Identifier (MEID) uniquely identifies the mobile equipment.

Syntax Opaque Value

Length 0-14

Type 26

Vendor ID 5535

VSA Type 116

3GPP2-MIP6-Authenticator

The MN-AAA authenticator obtained from the MN-AAA authentication mobility option in the BU.

Syntax Opaque Value

Length 12

Type 26

Vendor ID 5535

VSA Type 134

3GPP2-MIP6-CoA

MIPv6 CoA received in binding update.

Syntax Opaque Value

Length 16

Type 26

Vendor ID 5535

VSA Type 119

3GPP2-MIP6-HA

MIPv6 Home Agent address received in binding update.

Syntax Opaque Value

Length 16

Type 26

Vendor ID 5535

VSA Type 118

3GPP2-MIP6-HoA-Not-Authorized

Value of 1 indicates to the HA that the HoA is not authorized to be used by HA.

Syntax Enumerated Integer. Supports the following value(s):

- UnAuthorized = 1

Length 4

Type 26

Vendor ID 5535

VSA Type 120

3GPP2-MIP6-HoA

MIPv6 HoA received in binding update.

Syntax Opaque Value

Length 16

Type 26

Vendor ID 5535

VSA Type 141

3GPP2-MIP6-Home-Address

Carries the assigned Home Address during MIP6 bootstrapping.

Syntax Opaque Value

Length 18

Type 26

Vendor ID 5535

VSA Type 129

3GPP2-MIP6-Home-Agent

Carries the assigned MIPv6 Home Agent address received during MIPv6 bootstrapping.

Syntax Opaque Value

Length 18

Type 26

Vendor ID 5535

VSA Type 140

3GPP2-MIP6-Home-Link-Prefix

Carries the assigned Home Link Prefix during MIP6 bootstrapping.

Syntax Opaque Value

Length 2-18

Type 26

Vendor ID 5535

VSA Type 128

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.

Syntax Opaque Value

Length 20

Type 26

Vendor ID 5535

VSA Type 138

3GPP2-MIP6-Mesg-ID

Value of Message ID from Mobility message replay protection option in Binding Update.

Syntax Opaque Value

Length 8

Type 26

Vendor ID 5535

VSA Type 123

3GPP2-MIP6-Session-Key

This VSA carries the Integrity Key (IK) in its encrypted form, from the Home RADIUS server to the HA.

Syntax Opaque Value

Length 16-64

Type 26

Vendor ID 5535

VSA Type 121

3GPP2-MIP-HA-Address

The IP address of the MIP Home Agent.

Syntax IPv4 Address

Length 4

Type 26

Vendor ID 5535

VSA Type 7

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

Syntax Compound. Contains the following sub-attribute(s).

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.

Syntax Unsigned Integer

Length 4

Type 1

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.

Syntax Unsigned Integer

Length 4

Type 2

3GPP2-MIP-Rev-Tunnel-Required

Indicates to the PDSN if MIP Reverse Tunneling is required.

Syntax Enumerated Integer. Supports the following value(s):

- NotRequired = 0
- Required = 1

Length 4

Type 26

Vendor ID 5535

VSA Type 4

3GPP2-MIP-Sig-Octet-Count-In

The total number of octets in registration requests and solicitations sent by the mobile.

Syntax Unsigned Integer

Length 4

Type 26

Vendor ID 5535

VSA Type 46

3GPP2-MIP-Sig-Octet-Count-Out

The total number of octets in registration replies and agent advertisements, sent to the mobile.

Syntax Unsigned Integer

Length 4

Type 26

Vendor ID 5535

VSA Type 47

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.

Syntax Enumerated Integer. Supports the following value(s):

- Allowed = 0
- Not-Required = 1

Length 4

Type 26

Vendor ID 5535

VSA Type 81

3GPP2-MN-HA-Shared-Key-No-Enc

This attribute contains the MN-HA shared key in plain format.

Syntax Opaque Value

Length 1-251

Type 26

Vendor ID 5535

VSA Type 58

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.

Syntax Opaque Value

Length 1-251

Type 26

Vendor ID 5535

VSA Type 58

3GPP2-MN-HA-SPI

The SPI for the MN-HA authentication shared key.

Syntax Unsigned Integer

Length 4

Type 26

Vendor ID 5535

VSA Type 57

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).

Syntax Enumerated Integer. Supports the following value(s):

- Mobile-Originated = 0
- Mobile-Terminated = 1

Length 4

Type 26

Vendor ID 5535

VSA Type 45

3GPP2-Number-Active-Transitions

This attribute counts the total number of non-active to active transitions by the user.

Syntax Unsigned Integer

Length 4

Type 26

Vendor ID 5535

VSA Type 30

3GPP2-Num-Bytes-Received-Total

This attribute counts all bytes received in the reverse direction by the HDLC layer in the PDSN.

Syntax Unsigned Integer

Length 4

Type 26

Vendor ID 5535

VSA Type 43

3GPP2-Num-SDB-Input

This attribute counts the total number of Short Data Burst transactions to the user.

Syntax Unsigned Integer

Length 4

Type 26

Vendor ID 5535

VSA Type 33

3GPP2-Num-SDB-Output

This attribute counts the total number of Short Data Burst transactions from the user.

Syntax Unsigned Integer

Length 4

Type 26

Vendor ID 5535

VSA Type 34

3GPP2-PMIP-Capability

This attribute specifies the AGW's PMIP capability.

Syntax Enumerated Integer. Supports the following value(s):

- PMIPv4_ONLY = 1
- PMIPv6_ONLY = 2
- PMIPv4_PMIPv6 = 3

Length 4

Type 26

Vendor ID 5535

VSA Type 193

3GPP2-PMIP-IPv4Session-Info

This attribute specifies PMIP information for IPv4 session.

Type 26

Vendor ID 5535

VSA Type 194

Syntax Compound. Contains the following sub-attribute(s).

Length 0-160

VAAA-IPv4Session-HA-Addr

An IPv4 address or IPv6 Address of the local HA assigned by the AGW/VAAA for AT's IPv4 Address assignment.

Syntax Opaque Value

Length 0-16

Type 1

HAAA-IPv4Session-HA-Addr

An IPv4 address or IPv6 Address of the home or local HA assigned by the HAAA for AT's IPv4 Address assignment.

Syntax Opaque Value

Length 0-16

Type 2

PMN-HA-KEY

PMN-HA-KEY

Syntax Opaque Value

Length 0-32

Type 3

PMN-HA-SPI

PMN-HA-SPI

Syntax Unsigned Integer

Length 4

Type 4

VAAA-IPv4Session-LMA-Addr

An IPv4 address or IPv6 Address of the local LMA assigned by the AGW/VAAA for AT's IPv4 Address assignment

Syntax Opaque Value

Length 0-16

Type 5

HAAA-IPv4Session-LMA-Addr

An IPv4 address or IPv6 Address of the home or local LMA assigned by the HAAA for AT's IPv4 Address assignment.

Syntax Opaque Value

Length 0-16

Type 6

PMN-LMA-KEY

PMN-LMA-KEY

Syntax Opaque Value

Length 0-32

Type 7

PMN-LMA-SPI

PMN-LMA-SPI

Syntax Unsigned Integer

Length 4

Type 8

3GPP2-PMIP-IPv6Session-Info

This attribute specifies the PMIP information for IPv6 session.

Type 26

Vendor ID 5535

VSA Type 195

Syntax Compound. Contains the following sub-attribute(s).

Length 0-160

VAAA-IPv6Session-HA-Addr

VAAA-IPv6Session-HA-Addr

Syntax Opaque Value

Length 0-16

Type 1

HAAA-IPv6Session-HA-Addr

HAAA-IPv6Session-HA-Addr

Syntax Opaque Value

Length 0-16

Type 2

PMN-HA-KEY

PMN-HA-KEY

Syntax Opaque Value

Length 0-32

Type 3

PMN-HA-SPI

PMN-HA-SPI

Syntax Unsigned Integer

Length 4

Type 4

VAAA-IPv6Session-LMA-Addr

An IPv4 address or IPv6 Address of the local LMA assigned by the AGW/VAAA for AT's IPv6 Address assignment.

Syntax Opaque Value

Length 0-16

Type 5

HAAA-IPv6Session-LMA-Addr

An IPv4 address or IPv6 Address of the home or local LMA assigned by the HAAA for AT's IPv6 Address assignment.

Syntax Opaque Value

Length 0-16

Type 6

PMN-LMA-KEY

PMN-LMA-KEY

Syntax Opaque Value

Length 0-32

Type 7

PMN-LMA-SPI

PMN-LMA-SPI

Syntax Unsigned Integer

Length 4

Type 8

3GPP2-PMIP-NAI

This attribute specifies the PMIP NAI provided by AAA.

Syntax Opaque Value

Length 1-128

Type 26

Vendor ID 5535

VSA Type 192

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

Syntax Compound. Contains the following sub-attribute(s).

Quota-Identifier

It is generated by the PPS together with the allocation of new quota.

Syntax Unsigned Integer

Length 4

Type 1

Volume-Quota

Indicates the volume in octets excluding control data.

Syntax Unsigned Integer

Length 4

Type 2

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.

Syntax Unsigned Integer

Length 2

Type 3

Volume-Threshold

Is generated by the PPS and indicates the volume (in octets) that be consumed before a new quota should be requested.

Syntax Unsigned Integer

Length 4

Type 4

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.

Syntax Unsigned Integer

Length 2

Type 5

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.

Syntax Unsigned Integer

Length 4

Type 6

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.

Syntax Unsigned Integer

Length 4

Type 7

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.

Syntax Enumerated Integer. Supports the following value(s):

- 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

Length 2

Type 8

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.

Syntax IPv4 Address

Length 4

Type 9

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

Syntax Compound. Contains the following sub-attribute(s).

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.

Syntax Enumerated Integer. Supports the following value(s):

- Supported_None = 0
- Supported_Volume = 1
- Supported_Duration = 2
- Supported_Volume_And_Duration = 3
- Supported_Tariff_Switch = 64
- Supported_Volume_And_Duration_And_Tariff_Switch = 67

Length 4

Type 1

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.

Syntax Enumerated Integer. Supports the following value(s):

- Usage_None = 0
- Usage_Volume = 1
- Usage_Duration = 2
- Usage_Volume_And_Duration = 3

Length 4

Type 2

3GPP2-Pre-Paid-TariffSwitch

3GPP2-Pre-Paid-TariffSwitch

Type 26

Vendor ID 5535

VSA Type 98

Syntax Compound. Contains the following sub-attribute(s).

Quota-Identifier

It is generated by the PPS together with the allocation of new quota.

Syntax Unsigned Integer

Length 4

Type 1

Volume-Used-After-Tariff-Switch

Volume quota used after tariff switch happened.

Syntax Unsigned Integer

Length 4

Type 2

Volume-Used-ATS-Overflow

Indicates how many times the VUATS counter has wrapped around 2^32 over the course of the service being provided.

Syntax Unsigned Integer

Length 2

Type 3

Tariff-Switch-Interval

Tariff switch interval in seconds.

Syntax Unsigned Integer

Length 4

Type 4

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

Syntax Unsigned Integer

Length 4

Type 5

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.

Syntax Opaque Value

Length 8-247

Type 26

Vendor ID 5535

VSA Type 74

3GPP2-Release-Indicator-custom9

3GPP2 Release Indicator for custom9, reason/cause for session release.

Syntax Enumerated Integer. Supports the following value(s):

- 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

Length 4

Type 26

Vendor ID 5535

VSA Type 24

3GPP2-Release-Indicator-Old

3GPP2 old Standard Release Indicator, reason/cause for session release.

Syntax Enumerated Integer. Supports the following value(s):

- 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

Length 4

Type 26

Vendor ID 5535

VSA Type 24

3GPP2-Release-Indicator-Prepaid

Syntax Enumerated Integer. Supports the following value(s):

- TOPUP = 0
- AOC = 1
- OHHOLD = 2
- Session_Term_or_OFFLINE = 3
- CATALOG = 4
- BLOCK = 5
- Volume-Quota-Reached = 8
- Duration-Quota-Reached = 9

Length 4

Type 26

Vendor ID 5535

VSA Type 24

3GPP2-Release-Indicator

This attribute specifies reasons for sending a stop record. The enumeration of this attribute conforms to IS-835-1.

Syntax Enumerated Integer. Supports the following value(s):

- 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

Length 4

Type 26

Vendor ID 5535

VSA Type 24

3GPP2-Remote-Addr-Table-Idx-Old

Syntax Unsigned Integer

Length 4

Type 26

Vendor ID 5535

VSA Type 71

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

Syntax Compound. Contains the following sub-attribute(s).

Table-Index

Table-Index

Syntax Unsigned Integer

Length 2

Type 1

Qualifier

Qualifier

Syntax Enumerated Integer. Supports the following value(s):

- Exempt-From-Prepaid = 1
- Summarize-Octet-Count = 2
- Both = 3

Length 2

Type 2

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

Syntax Compound. Contains the following sub-attribute(s).

Address

This attribute contains an IPv4 address to be used for remote address based accounting for the user. The address is used in conjunction with the Netmask subattribute to define the range of addresses to be monitored.

Syntax IPv4 Address

Length 4

Type 1

Netmask

This attribute contains an IPv4 address mask that defines the set of remote addresses to be used for remote address based accounting.

Syntax IPv4 Address

Length 4

Type 2

Qualifier

Qualifier

Syntax Enumerated Integer. Supports the following value(s):

- Exempt-From-Prepaid = 1
- Summarize-Octet-Count = 2
- Both = 3

Length 2

Type 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

Syntax Compound. Contains the following sub-attribute(s).

Address

This attribute contains an IPv4 address to be used for remote address based accounting for the user. The address is used in conjunction with the Netmask subattribute to define the range of addresses to be monitored.

Syntax IPv4 Address

Length 4

Type 1

Netmask

This attribute contains an IPv4 address mask that defines the set of remote addresses to be used for remote address based accounting.

Syntax IPv4 Address

Length 4

Type 2

Octets-Out

Indicates how many bytes have been sent to the remote address specification (corresponds to forward traffic direction).

Syntax Unsigned Integer

Length 4

Type 3

Octets-In

Indicates how many bytes have been received from the remote address specification (corresponds to reverse traffic direction).

Syntax Unsigned Integer

Length 4

Type 4

Table-Index

Table-Index

Syntax Unsigned Integer

Length 2

Type 5

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.

Syntax Unsigned Integer

Length 2

Type 6

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.

Syntax Unsigned Integer

Length 2

Type 7

3GPP2-Rev-Dcch-Mux-Option

This attribute specifies Reverse DCCH Mux option.

Syntax Unsigned Integer

Length 4

Type 26

Vendor ID 5535

VSA Type 85

3GPP2-Rev-Dcch-Rc

This attribute specifies the Radio Configuration of the Reverse Packet Data Channel.

Syntax Unsigned Integer

Length 4

Type 26

Vendor ID 5535

VSA Type 87

3GPP2-Reverse-Fundamental-Rate

As defined in "Wireless IP Network Standard - 3GPP2.P.S0001-A-1".

Syntax Unsigned Integer

Length 4

Type 26

Vendor ID 5535

VSA Type 15

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.

Syntax Unsigned Integer

Length 4

Type 26

Vendor ID 5535

VSA Type 21

3GPP2-Reverse-Mux-Option

Forward direction multiplexer option.

Syntax Unsigned Integer

Length 4

Type 26

Vendor ID 5535

VSA Type 13

3GPP2-Reverse-Traffic-Type

Specifies the reverse traffic type.

Syntax Enumerated Integer. Supports the following value(s):

- Primary = 0
- Secondary = 1

Length 4

Type 26

Vendor ID 5535

VSA Type 18

3GPP2-Rev-Pdch-Rc

This attribute specifies the 3GPP2-Rev-Pdch-Rc.

Syntax Unsigned Integer

Length 4

Type 26

Vendor ID 5535

VSA Type 114

3GPP2-RP-Session-ID

This represents the GRE key selected by the PCF that identifies the A10 traffic for a user session.

Syntax Unsigned Integer

Length 4

Type 26

Vendor ID 5535

VSA Type 41

3GPP2-Rsvp-Signal-In-Count

This attribute specifies the RSVP signaling octets sent by the MS.

Syntax Unsigned Integer

Length 4

Type 26

Vendor ID 5535

VSA Type 162

3GPP2-Rsvp-Signal-In-Packets

This attribute specifies the Number of RSVP signaling packets sent by the MS.

Syntax Unsigned Integer

Length 4

Type 26

Vendor ID 5535

VSA Type 164

3GPP2-Rsvp-Signal-Out-Count

This attribute specifies the RSVP signaling octets sent to the MS.

Syntax Unsigned Integer

Length 4

Type 26

Vendor ID 5535

VSA Type 163

3GPP2-Rsvp-Signal-Out-Packets

This attribute specifies the Number of RSVP signaling packets sent to the MS.

Syntax Unsigned Integer

Length 4

Type 26

Vendor ID 5535

VSA Type 165

3GPP2-SDB-Input-Octets

This attribute counts the total number of octets sent to the user via Short Data Bursts.

Syntax Unsigned Integer

Length 4

Type 26

Vendor ID 5535

VSA Type 31

3GPP2-SDB-Output-Octets

This attribute counts the total number of octets sent by the user via Short Data Bursts.

Syntax Unsigned Integer

Length 4

Type 26

Vendor ID 5535

VSA Type 32

3GPP2-Security-Level

This attribute indicates the type of security that the home network mandates on the visited network.

Syntax Enumerated Integer. Supports the following value(s):

- IPSec = 3
- None = 4

Length 4

Type 26

Vendor ID 5535

VSA Type 2

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.

Syntax Unsigned Integer

Length 4

Type 26

Vendor ID 5535

VSA Type 74

3GPP2-Service-Option

This attribute indicates the service option used for CDMA air interface.

Syntax Enumerated Integer. Supports the following value(s):

- HSPD = 0x21
- HRPD = 0x3b
- LLAROHC = 0x3d
- HRPD-AUX = 0x40
- HRPD-AUX-IP = 0x43
- eHRPD = 0x252
- LTE = 0x253
- UTRAN = 0x254
- GERAN = 0x255 WIFI = 0x806c

Length 4

Type 26

Vendor ID 5535

VSA Type 16

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

Syntax Compound. Contains the following sub-attribute(s).

SR-ID

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

Syntax Unsigned Integer

Length 2

Type 1

Main-SI-Indicator

Only included for the main service instance.

Syntax Enumerated Integer. Supports the following value(s):

- Main-SI = 1

Length 2

Type 2

3GPP2-Serving-PCF

IP address of the serving PCF.

Syntax IPv4 Address

Length 4

Type 26

Vendor ID 5535

VSA Type 9

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.

Syntax Enumerated Integer. Supports the following value(s):

- False = 0
- True = 1

Length 4

Type 26

Vendor ID 5535

VSA Type 48

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.

Syntax Enumerated Integer. Supports the following value(s):

- Only_Dynamic_Auth_Extn_to_Radius = 0x00000001
- Only_Reg_Revocation_in_MIP = 0x00000002

- Both_Dynamic_Auth_And_Reg_Revocation_in_MIP = 0x00000003

Length 4

Type 26

Vendor ID 5535

VSA Type 88

3GPP2-S-Key

This attribute contains the HA IKE key in encrypted format.

Syntax Opaque Value

Length 1-247

Type 26

Vendor ID 5535

VSA Type 54

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.

Syntax Unsigned Integer

Length 4

Type 26

Vendor ID 5535

VSA Type 56

3GPP2-S-Request

This attribute indicates whether the HA requests a shared secret 'S'.

Syntax Enumerated Integer. Supports the following value(s):

- No = 0
- Yes = 1

Length 4

Type 26

Vendor ID 5535

VSA Type 55

3GPP2-Subnet

This attribute specifies the subnet information of the HRPD RAN.

Type 26

Vendor ID 5535

VSA Type 108

Syntax Compound. Contains the following sub-attribute(s).

Rev-A-Subnet

This attribute specifies the subnet information of the HRPD RAN.

Syntax Opaque Value

Length 1-19

Type 1

Rev-A-Sector-Id

This attribute specifies the Sector ID information of the HRPD RAN.

Syntax Opaque Value

Length 1-18

Type 2

3GPP2-S-Unencrypted

This attribute contains the HA IKE key in plain format.

Syntax Opaque Value

Length 1-247

Type 26

Vendor ID 5535

VSA Type 54

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.

Syntax Unsigned Integer

Length 4

Type 26

Vendor ID 5535

VSA Type 11

3GPP-Allocate-IPType

This attribute indicates whether the Access-Request is sent for user authentication only and/or for allocation of IPv4 and/or IPv6 address.

Syntax Enumerated Integer. Supports the following value(s):

- none = 0
- ipv4 = 1
- ipv6 = 2
- ipv4-or-ipv6 = 3

Length 4

Type 26

Vendor ID 10415

VSA Type 27

3GPP-CAMEL-Charging-Info

This attribute contains the received CAMEL charging information. CAMEL charging information is applicable to GGSN.

Syntax Opaque Value

Length 1-255

Type 26

Vendor ID 10415

VSA Type 24

3GPP-CG-Address

This attribute identifies the charging gateway address.

Syntax IPv4 Address

Length 4

Type 26

Vendor ID 10415

VSA Type 4

3GPP-Charging-Id

Syntax Unsigned Integer

Length 4

Type 26

Vendor ID 10415

VSA Type 2

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).

Syntax Opaque Value

Length 4

Type 26

Vendor ID 10415

VSA Type 13

3GPP-GGSN-Address

This attribute contains IPv4 address of the GGSN.

Syntax IPv4 Address

Length 4

Type 26

Vendor ID 10415

VSA Type 7

3GPP-GGSN-IPv6-Address

For GGSN, it represents the GGSN IPv6 address that is used by the GTP control plane for thecontext establishment. For P-GW, it represents the P-GW IPv6 address that is used on S5/S8, S2a, S2b, or S2c control plane for the IP-CAN session establishment.

Syntax Opaque Value

Length 16

Type 26

Vendor ID 10415

VSA Type 16

3GPP-GGSN-Mcc-Mnc

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

Syntax Opaque Value

Length 1-6

Type 26

Vendor ID 10415

VSA Type 9

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.

Syntax Opaque Value

Length 16

Type 26

Vendor ID 10415

VSA Type 20

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).

Syntax Opaque Value

Length 1-6

Type 26

Vendor ID 10415

VSA Type 8

3GPP-IMSI

This attribute contains the IMSI identifying the mobile unit.

Syntax Opaque Value

Length 1-15

Type 26

Vendor ID 10415

VSA Type 1

3GPP-IPv6-DNS-Servers

This attribute contains list of IPv6 DNS server addresses.

Syntax Opaque Value

Length 16-240

Type 26

Vendor ID 10415

VSA Type 17

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.

Syntax Opaque Value

Length 2

Type 26

Vendor ID 10415

VSA Type 23

3GPP-Negotiated-DSCP

This attribute is used to mark IP packets of PDP context on the Gi interface.

Syntax Unsigned Integer

Length 1

Type 26

Vendor ID 10415

VSA Type 26

3GPP-Negotiated-QoS-Profile

This attribute specifies the QoS profile to be used for the subscriber.

Syntax ThreeGPP-Negotiated-QoS-Profile

Type 26

Vendor ID 10415

VSA Type 5

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.

Syntax Opaque Value

Length 1

Type 26

Vendor ID 10415

VSA Type 10

3GPP-Packet-Filter

This compound attribute specifies the Packet Filter used for the PDP context.

Length 65

Type 26

Vendor ID 10415

VSA Type 25

Syntax Compound. Contains the following sub-attribute(s).

Identifier

Identifier of the packet filter.

Syntax Unsigned integer

Length 1

Type 1

Eval-Precedence

Evaluation precedence of the packet filter.

Syntax Unsigned integer

Length 1

Type 2

Length

Length of the packet filter.

Syntax Unsigned integer

Length 1

Type 3

Direction

Direction of the packet filter.

Syntax Unsigned integer

Length 1

Type 4

IPv4-Address-Type

This is a compound attribute specifying the IPv4 source address and netmask if the direction is downlink, or destination address and netmask if the direction is downlink, or destination address and netmask if the direction is uplink.

Length 8

Type 5

Syntax Contains the following two sub-attribute(s):

Address

This attribute contains source address if direction value is set to Downlink, and destination address if direction value is set to Uplink.

Syntax IPv4 address

Length 4

Type 1

Netmask

This attribute contains netmask of the IPv4 address.

Syntax IPv4 address

Length 4

Type 2

IPv6-Address-Type

This is a compound attribute specifying the IPv6 source address and netmask if the direction is Downlink, or Destination Address and Netmask if the direction is Downlink, or Destination Address and Netmask if the direction is Uplink.

Length 32

Type 6

Syntax Contains the following two sub-attribute(s):

Address

This attribute contains source address if direction value is set to Downlink, and destination address if direction value is set to Uplink.

Syntax Opaque value

Length 16

Type 1

Netmask

This attribute contains the Netmask of the IPv6 address.

Syntax Opaque value

Length 16

Type 2

Protocol-Identifier-Or-Next-Header

Specifies the IPv4 Protocol Identifier or IPv6 Next Header.

Syntax Unsigned integer

Length 1

Type 7

Destination-Port

Specifies the Destination Port number of the packet filter.

Syntax An integer in network byte order

Length 2

Type 8

Destination-Port-Range

This is a compound attribute and specifies the destination port range.

Length 4

Type 9

Syntax Contains the following two sub-attribute(s):

Lower

Specifies the lower range of the destination port of the packet filter.

Syntax Unsigned integer

Length 2

Type 1

Higher

Specifies the higher range of the destination port of the packet filter.

Syntax Unsigned integer

Length 2

Type 2

Source-Port

Specifies the source port number of the packet filter.

Syntax Unsigned integer

Length 2

Type 10

Source-Port-Range

Specifies the source port range.

Length 4

Type 11

Syntax Contains the following two sub-attribute(s):

Lower

Specifies lower range of the source port of the packet filter.

Syntax Unsigned integer

Length 2

Type 1

Higher

Specifies the higher range of the source port of the packet filter.

Syntax Unsigned integer

Length 2

Type 2

Security-Parameter-Index

Specifies the IPSec Security Parameter Index(IPv6).

Syntax Unsigned integer

Length 4

Type 12

Type-Of-Service

This is a compound attribute and specifies the Type of Service/ Traffic Class.

Length 2

Type 13

Syntax Contains the following two sub-attribute(s):

Value

Specifies the Type of Service/Traffic Class Value.

Syntax Unsigned integer

Length 1

Type 1

Mask

Specifies the Type of Service/Traffic Class Mask.

Syntax Unsigned integer

Length 1

Type 2

Flow-Label

Specifies the IPv6 Flow Label.

Syntax Opaque value

Length 3

Type 14

3GPP-PDP-Type

This attribute identifies the PDP Context type.

Syntax Enumerated Integer. Supports the following value(s):

- ipv4 = 0
- ppp = 1
- ipv6 = 2
- ipv4-or-ipv6 = 3
- non-ip = 4

Length 4

Type 26

Vendor ID 10415

VSA Type 3

3GPP-RAT-Type

This attribute indicates which Radio Access Technology is currently serving the UE.

Syntax Opaque Value

Length 1

Type 26

Vendor ID 10415

VSA Type 21

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.

Syntax Opaque Value

Length 1

Type 26

Vendor ID 10415

VSA Type 12

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.

Syntax Opaque Value

Length 1

Type 26

Vendor ID 10415

VSA Type 11

3GPP-SGSN-Address

This attribute contains IPv4 address of the SGSN.

Syntax IPv4 Address

Length 4

Type 26

Vendor ID 10415

VSA Type 6

3GPP-SGSN-IPv6-Address

For GGSN, it represents the SGSN IPv6 address that is used by the GTP control plane for the handling of control messages. For P-GW, it represents the IPv6 address of the S-GW, trusted non-3GPP IP access or ePDG that is used on S5/S8, S2a, or S2b for the handling of control messages. The address may beused to identify the PLMN to which the user is attached.

Syntax Opaque Value

Length 16

Type 26

Vendor ID 10415

VSA Type 15

3GPP-SGSN-Mcc-Mnc

For GPRS the MCC and the MNC of the SGSN.

Syntax Opaque Value

Length 1-6

Type 26

Vendor ID 10415

VSA Type 18

3GPP-Teardown-Indicator

If this value is set to 1 in disconnect-request, the whole correlated sessions would be disconnected.

Syntax Opaque Value

Length 1

Type 26

Vendor ID 10415

VSA Type 19

3GPP-User-Location-Info

GTP user location information attribute for the subscriber session.

Syntax Opaque Value

Length 1-37

Type 26

Vendor ID 10415

VSA Type 22

AAA-Session-ID

A unique per realm identifier assigned to WiMAX session by the Home network during network entry.

Syntax String

Length 1-246

Type 26

Vendor ID 24757

VSA Type 4

Access-IN-Subs

Syntax Unsigned Integer

Length 4

Type 26

Vendor ID 5535

VSA Type 224

Acct-Authentic

This attribute is included in Accounting-Request packets to indicate how the session was authenticated (RADIUS or locally).

Syntax Enumerated Integer. Supports the following value(s):

- None = 0
- RADIUS = 1
- Local = 2
- Remote = 3
- Diameter = 4

Length 4

Type 45

Vendor ID N/A

VSA Type N/A

Acct-Delay-Time

This attribute indicates how many seconds the chassis has been trying to send this record for. The standard behavior is that this attribute will be visible in the Accounting Request message only if it has a non-zero value.

Syntax Unsigned Integer

Length 4

Type 41

Vendor ID N/A

VSA Type N/A

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.

Syntax Unsigned Integer

Length 4

Type 52

Vendor ID N/A

VSA Type N/A

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.

Syntax Unsigned Integer

Length 4

Type 42

Vendor ID N/A

VSA Type N/A

Acct-Input-Packets

This attribute indicates how many PPP packets have been received during the session.

Syntax Unsigned Integer

Length 4

Type 47

Vendor ID N/A

VSA Type N/A

Acct-Interim-Interval

This attribute indicates the time (in seconds) between updates to session counters (log file on RADIUS or AAA event log) during the session. Note that the setting for this attribute always takes precedence over interim interval settings configured on the system.

Syntax Unsigned Integer

Length 4

Type 85

Vendor ID N/A

VSA Type N/A

Acct-Link-Count

Syntax Unsigned Integer

Length 4

Type 51

Vendor ID N/A

VSA Type N/A

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.

Syntax String

Length 1-253

Type 50

Vendor ID N/A

VSA Type N/A

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.

Syntax Unsigned Integer

Length 4

Type 53

Vendor ID N/A

VSA Type N/A

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.

Syntax Unsigned Integer

Length 4

Type 43

Vendor ID N/A

VSA Type N/A

Acct-Output-Packets

This attribute indicates how many PPP packets have been sent during the session.

Syntax Unsigned Integer

Length 4

Type 48

Vendor ID N/A

VSA Type N/A

Acct-Session-Id-Long

This attribute contains long format account session ID. This is supported only for custom2 dictionary.

Syntax String

Length 1-253

Type 44

Vendor ID N/A

VSA Type N/A

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 attribute is sent on both Gx and Gy messages.

Syntax String

Length 1-253

Type 44

Vendor ID N/A

VSA Type N/A

Acct-Session-Time

This attribute indicates the duration of the session in seconds.

Syntax Unsigned Integer

Length 4

Type 46

Vendor ID N/A

VSA Type N/A

Acct-Status-Type

This attribute indicates the event for the session.

Syntax Enumerated Integer. Supports the following value(s):

- Start = 1

- Stop = 2
- Interim-Update = 3
- Accounting-On = 7
- Accounting-Off = 8
- Tunnel-Start = 9
- Tunnel-Stop = 10
- Tunnel-Reject = 11
- Tunnel-Link-Start = 12
- Tunnel-Link-Stop = 13
- Tunnel-Link-Reject = 14
- Failed = 15

Length 4

Type 40

Vendor ID N/A

VSA Type N/A

Acct-Termination-Cause

This attribute indicates why the session was terminated.

Syntax Enumerated Integer. Supports the following value(s):

- User_Request = 1
- Lost_Carrier = 2
- Lost_Service = 3
- Idle_Timeout = 4
- Session_Timeout = 5
- Admin_Reset = 6
- Admin_Reboot = 7
- Port_Error = 8
- NAS_Error = 9
- NAS_Request = 10
- NAS_Reboot = 11
- Port_Unneeded = 12
- Port_Preempted = 13

- Port_Suspended = 14
- Service_Unavailable = 15
- Callback = 16
- User_Error = 17
- Host_Request = 18
- Supplicant_Restart = 19
- Reauthentication_Failure = 20
- Port_Reinitialized = 21
- Port_Administratively_Disabled = 22
- Inter-PDSN-Handoff = 99
- Long-Duration-Timeout = 1001
- Invalid-Source-Address = 1002
- Duplicate-IMSI = 1003
- Interim-Update = 1004
- Hotlining-Status-Change = 1005

Length 4

Type 49

Vendor ID N/A

VSA Type N/A

BU-CoA-Ipv6

The IPv6 address extracted from the Careof Address field in the BU and sent in Access Request from HA for WiMAX call.

Syntax Opaque Value

Length 16

Type 26

Vendor ID 24757

VSA Type 51

Callback-Id

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

Syntax Opaque Value

Length 1-253

Type 20

Vendor ID N/A

VSA Type N/A

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.

Syntax Opaque Value

Length 1-128

Type 30

Vendor ID N/A

VSA Type N/A

Calling-Station-Id

This attribute indicates the Mobile Station Identifier in PDSN, and MSISDN in GGSN.

Syntax Opaque Value

Length 1-253

Type 31

Vendor ID N/A

VSA Type N/A

Calling-Subscriber-Type

Opaque one byte value received from customer RADIUS server in Access Request. Used in custom dictionary.

Syntax Opaque Value

Length 1

Type 26

Vendor ID 5535

VSA Type 218

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.

Syntax Opaque Value

Length 1-253

Type 60

Vendor ID N/A

VSA Type N/A

CHAP-Password

This attribute contains the CHAP ID and the CHAP Response when CHAP authentication is used.

Syntax Opaque Value

Length 17

Type 3

Vendor ID N/A

VSA Type N/A

Charging-Id

Same as 3GPP-Charging-ID standard attribute; non-standard behavior for use in custom dictionary.

Syntax Unsigned Integer

Length 4

Type 225

Vendor ID N/A

VSA Type N/A

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.

Syntax Opaque Value

Length 1-253

Type 25

Vendor ID N/A

VSA Type N/A

CS-AVPair

This is a Cisco Vendor Specific Attribute. This attribute may contain any string required for Web Authorization feature for SaMOG.

Syntax String

Length 1-249

Type 26

Vendor ID 9

VSA Type 1

CS-Prepaid-Quota

Syntax String

Length 1-252

Type 26

Vendor ID 9

VSA Type 253

CS-Prepaid-Time-Quota

Syntax String

Length 1-252

Type 26

Vendor ID 9

VSA Type 102

CS-Prepaid-Volume-Quota

Syntax String

Length 1-252

Type 26

Vendor ID 9

VSA Type 101

CS-Service-Name

Syntax String

Length 1-252

Type 26

Vendor ID 9

VSA Type 251

CUI

Chargeable User Identity (CUI) 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.

Syntax Opaque Value

Length 1-253

Type 89

Vendor ID N/A

VSA Type N/A

custom54-Dial-Number

Syntax String

Length 1-252

Type 227

Vendor ID N/A

VSA Type N/A

custom54-IPX-Alias

Syntax Unsigned Integer

Length 4

Type 224

Vendor ID N/A

VSA Type N/A

custom54-Metric

Syntax Unsigned Integer

Length 4

Type 225

Vendor ID N/A

VSA Type N/A

custom54-PRI-Number-Type

Syntax Unsigned Integer

Length 4

Type 226

Vendor ID N/A

VSA Type N/A

custom54-Route-IP

Syntax Unsigned Integer

Length 4

Type 228

Vendor ID N/A

VSA Type N/A

custom54-Session-Svr-Key

Syntax String

Length 1-32

Type 151

Vendor ID N/A

VSA Type N/A

Custom-Prepaid-Ind

Syntax Unsigned Integer

Length 1

Type 226

Vendor ID N/A

VSA Type N/A

Delegated-IPv6-Prefix

For IPv6 subscriber sessions IPSG receives deligated IPv6 prefix or framed IPv6 prefix value from Accounting Start message and assigns that IPv6 prefix to the subscriber.

Syntax Opaque Value

Length 2-18

Type 123

Vendor ID N/A

VSA Type N/A

DHCPMSG-Server-IP

The IPv4 address of the DHCP server.

Syntax IPv4 Address

Length 4

Type 26

Vendor ID 24757

VSA Type 43

DHCP-RK-Key-ID

An integer uniquely identifying the DHCP-RK within the scope of a single DHCP server.

Syntax Unsigned Integer

Length 4

Type 26

Vendor ID 24757

VSA Type 41

DHCP-RK-Lifetime

Lifetime of the DHCP-RK and derived keys.

Syntax Unsigned Integer

Length 4

Type 26

Vendor ID 24757

VSA Type 42

DHCP-RK

DHCP-RK is a 160-bit randomly generated for every DHCP server, the DHCP Key is derived from this.

Syntax Opaque Value

Length 1-250

Type 26

Vendor ID 24757

VSA Type 40

Digest-AKA-Auts

This attribute holds the auts parameter that is used in the Digest AKA calculation.

Syntax Opaque Value

Length 0-253

Type 118

Vendor ID N/A

VSA Type N/A

Digest-Algorithm

This parameter holds the algorithm parameter that influences the HTTP Digest calculation.

Syntax Opaque Value

Length 0-253

Type 111

Vendor ID N/A

VSA Type N/A

Digest-Auth-Param

This attribute is a placeholder for future extensions.

Syntax Opaque Value

Length 0-253

Type 117

Vendor ID N/A

VSA Type N/A

Digest-CNonce

This attribute holds the client nonce that is used in the digest calculation.

Syntax Opaque Value

Length 0-253

Type 113

Vendor ID N/A

VSA Type N/A

Digest-Domain

This attribute consists of single URI that defines a protection space component.

Syntax Opaque Value

Length 0-256

Type 119

Vendor ID N/A

VSA Type N/A

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".

Syntax Opaque Value

Length 0-253

Type 112

Vendor ID N/A

VSA Type N/A

Digest-HA1

This attribute contains the hexadecimal representation on H(A1) as described in RFC 2617.

Syntax Opaque Value

Length 0-253

Type 121

Vendor ID N/A

VSA Type N/A

Digest-Method

This attribute holds the method value to be used in the HTTP digest calculation.

Syntax Opaque Value

Length 0-253

Type 108

Vendor ID N/A

VSA Type N/A

Digest-Nextnonce

This attribute holds a nonce to be used in the HTTP digest calculation.

Syntax Opaque Value

Length 0-253

Type 107

Vendor ID N/A

VSA Type N/A

Digest-Nonce-Count

This attribute holds the nonce count parameter that is used to detect replay attacks.

Syntax Opaque Value

Length 0-253

Type 114

Vendor ID N/A

VSA Type N/A

Digest-Nonce

Syntax Opaque Value

Length 0-253

Type 105

Vendor ID N/A

VSA Type N/A

Digest-Opaque

This attribute holds the opaque parameter that is passed to the SIP client.

Syntax Opaque Value

Length 0-253

Type 116

Vendor ID N/A

VSA Type N/A

Digest-Qop

This attribute holds the quality of protection parameter that influences the HTTP digest calculation.

Syntax Opaque Value

Length 0-253

Type 110

Vendor ID N/A

VSA Type N/A

Digest-Realm

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

Syntax Opaque Value

Length 0-253

Type 104

Vendor ID N/A

VSA Type N/A

Digest-Response-Auth

This enables the RADIUS server to prove possession of the password.

Syntax Opaque Value

Length 0-253

Type 106

Vendor ID N/A

VSA Type N/A

Digest-Response

Syntax Opaque Value

Length 0-256

Type 103

Vendor ID N/A

VSA Type N/A

Digest-Stale

This attribute is sent by RADIUS server in order to notify the RADIUS client whether it has accepted a nonce.

Syntax Opaque Value

Length 0-253

Type 120

Vendor ID N/A

VSA Type N/A

Digest-URI

This attribute is used to transport the contents of the URI of the SIP request.

Syntax Opaque Value

Length 0-253

Type 109

Vendor ID N/A

VSA Type N/A

Digest-Username

This attribute holds the user name used in the HTTP Digest calculation.

Syntax Opaque Value

Length 0-253

Type 115

Vendor ID N/A

VSA Type N/A

DNS

IPv4/IPv6 address of the DNS server to be conveyed to the MS via DHCP.

Syntax Opaque Value

Length 4-16

Type 26

Vendor ID 24757

VSA Type 52

Draft5-Digest-Response

Syntax Opaque Value

Length 0-253

Type 102

Vendor ID N/A

VSA Type N/A

DSCP_IP_Address

radius_attribute_DSCP_IP_Address

Syntax IPv4 Address

Length 4

Type 26

Vendor ID 5535

VSA Type 245

EAP-Message

The EAP exchanged transported over RADIUS.

Syntax Opaque Value

Length 0-253

Type 79

Vendor ID N/A

VSA Type N/A

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.

Syntax Enumerated Integer. Supports the following value(s):

- Residual-Session-Context-Remove = 201
- Inavlid-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

Length 4

Type 101

Vendor ID N/A

VSA Type N/A

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.

Syntax Unsigned Integer

Length 4

Type 55

Vendor ID N/A

VSA Type N/A

FA-RK-KEY

This attribute contains the encrypted FA-RK-KEY. The FA-RK determined during EAP authentication by the RADIUS server and passed on to the NAS upon successful EAP authentication. It is used by the NAS to generate MN-FA keys.

Syntax Opaque Value

Length 1-244

Type 26

Vendor ID 24757

VSA Type 14

FA-RK-SPI

SPI used for the FA-RK associated with FA-RK Key for generating MN-FA key for WiMAX call

Syntax Unsigned Integer

Length 4

Type 26

Vendor ID 24757

VSA Type 61

Filter-Id

This attribute identifies the IP access-list/filter by name.

Syntax String

Length 1-253

Type 11

Vendor ID N/A

VSA Type N/A

Framed-Compression

This attribute indicates the compression protocol to be used.

Syntax Enumerated Integer. Supports the following value(s):

- None = 0
- VJ_TCP_IP_header_compression = 1
- IPX_header_compression = 2
- Stac_LZS_compressions = 3

Length 4

Type 13

Vendor ID N/A

VSA Type N/A

Framed-Interface-Id

This attribute contains the value of IPv6 Interface ID.

Syntax Opaque Value

Length 8

Type 96

Vendor ID N/A

VSA Type N/A

Framed-IP-Address

This attribute indicates the IP address to be configured for the user.

Syntax IPv4 Address

Length 4

Type 8

Vendor ID N/A

VSA Type N/A

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.

Syntax IPv4 Address

Length 4

Type 9

Vendor ID N/A

VSA Type N/A

Framed-IPv6-Pool

This attribute contains the IPv6 pool name.

Syntax String

Length 1-253

Type 100

Vendor ID N/A

VSA Type N/A

Framed-IPv6-Prefix

This attribute contains IPv6 prefix.

Syntax Opaque Value

Length 2-18

Type 97

Vendor ID N/A

VSA Type N/A

Framed-MTU

This attribute indicates the Maximum Transmission Unit that was configured for the PPP session.

Syntax Integer

Length 4

Type 12

Vendor ID N/A

VSA Type N/A

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.

Syntax String

Length 1-253

Type 88

Vendor ID N/A

VSA Type N/A

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.

Syntax Enumerated Integer. Supports the following value(s):

- PPP = 1
- SLIP = 2
- ARAP = 3
- Gandalf_proprietary___ = 4
- Xylogics_proprietary_IPX_SLIP = 5
- X_75_Synchronous = 6
- GPRS_PDP_Context = 7

Length 4

Type 7

Vendor ID N/A

VSA Type N/A

Framed-Route

This attribute specifies the subnet route to be installed in GGSN for the mobile router.

Syntax Opaque Value

Length 1-64

Type 22

Vendor ID N/A

VSA Type N/A

Geographical-Location

This attribute contains the information of geographical location as reported by HNB.

Syntax Opaque Value

Length 10

Type 26

Vendor ID 9

VSA Type 114

GGSN-GTP-IP-Address

Same as 3GPP-GGSN-Address standard attribute; non-standard behavior for use in custom dictionary.

Syntax IPv4 Address

Length 4

Type 230

Vendor ID N/A

VSA Type N/A

GGSN-IP-Address

Syntax IPv4 Address

Length 4

Type 227

Vendor ID N/A

VSA Type N/A

GMT-Time-Zone-Offset

Syntax Integer

Length 4

Type 26

Vendor ID 24757

VSA Type 3

HA-IP-MIP4

IPv4 address of the HA.

Syntax IPv4 Address

Length 4

Type 26

Vendor ID 24757

VSA Type 6

HA-IP-MIP6

IPv6 address of the HA for CMIP4.

Syntax Opaque Value

Length 4-16

Type 26

Vendor ID 24757

VSA Type 7

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.

Syntax Opaque Value

Length 1-244

Type 26

Vendor ID 24757

VSA Type 15

HA-RK-Lifetime

Lifetime of the HA-RK and derived keys.

Syntax Unsigned Integer

Length 4

Type 26

Vendor ID 24757

VSA Type 17

HA-RK-SPI

The SPI associated with the HA-RK for generating MN-HA key for WiMAX call.

Syntax Unsigned Integer

Length 4

Type 26

Vendor ID 24757

VSA Type 16

hLMA-IPv6-PMIP6

MIPv6 Home Agent address received in binding update.

Syntax Opaque Value

Length 16

Type 26

Vendor ID 24757

VSA Type 127

HNB-Internet-Information

This attribute contains public IP address (either IPv4 or IPv6 address) of HNB assigned through the broadband connection.

Syntax Opaque Value

Length 4-16

Type 26

Vendor ID 9

VSA Type 115

HNB-Parameters

This attribute contains PLMN ID, LAC, RAC, SAC, and Cell ID of the HNB as reported to HNB-GW in RADIUS Access-Request during authentication.

Syntax Opaque Value

Length 12

Type 26

Vendor ID 9

VSA Type 112

Hotline-Indicator

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

Syntax String

Length 1-64

Type 26

Vendor ID 24757

VSA Type 24

Hotline-Profile-ID

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

Syntax String

Length 1-64

Type 26

Vendor ID 24757

VSA Type 53

Hotline-Session-Timer

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

Syntax Unsigned Integer

Length 4

Type 26

Vendor ID 24757

VSA Type 56

HTTP-Redirection-Rule

An HTTP redirection rule.

Syntax Opaque Value

Length 1-246

Type 26

Vendor ID 24757

VSA Type 54

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.

Syntax Integer

Length 4

Type 28

Vendor ID N/A

VSA Type N/A

IMSI-MCC-MNC

Same as 3GPP-IMSI-Mcc-Mnc standard attribute; non-standard behavior for use in custom dictionary.

Syntax Opaque Value

Length 1-6

Type 226

Vendor ID N/A

VSA Type N/A

IMSI

Same as 3GPP-IMSI standard attribute; non-standard behavior for use in custom dictionary.

Syntax Opaque Value

Length 1-15

Type 224

Vendor ID N/A

VSA Type N/A

IN-Packet-Period

Syntax Unsigned Integer

Length 4

Type 26

Vendor ID 5535

VSA Type 246

IN-Time-Period

Syntax Unsigned Integer

Length 4

Type 26

Vendor ID 5535

VSA Type 247

IP-Redirection-Rule

This attribute is used to specify which packet flow to redirect and where to redirect it.

Syntax Opaque Value

Length 1-246

Type 26

Vendor ID 24757

VSA Type 55

KTF_VSA1

radius_attribute_KTF_VSA1

Syntax Opaque Value

Length 0-24

Type 26

Vendor ID 5535

VSA Type 249

KTF_VSA2

radius_attribute_KTF_VSA2

Syntax Opaque Value

Length 0-24

Type 26

Vendor ID 5535

VSA Type 255

Macro-Coverage-Information

This attribute contains the marco coverage information as reported by HNB which could be a GERAN or UTRAN cell information.

Syntax Opaque Value

Length 8-11

Type 26

Vendor ID 9

VSA Type 113

MN-HA-MIP4-KEY

MN-HA key for SPI value in the Access request if present.

Syntax Opaque Value

Length 1-244

Type 26

Vendor ID 24757

VSA Type 10

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.

Syntax Unsigned Integer

Length 4

Type 26

Vendor ID 24757

VSA Type 11

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.

Syntax Opaque Value

Length 1-244

Type 26

Vendor ID 24757

VSA Type 12

MN-HA-MIP6-SPI

SPI associated with the MN-HA-MIP6-KEY.

Syntax Unsigned Integer

Length 4

Type 26

Vendor ID 24757

VSA Type 13

MSISDN

MSIDSN of the call. Used in custom dictionary.

Syntax String

Length 1-256

Type 26

Vendor ID 5535

VSA Type 222

MSK

The Master Session Key determined during EAP authentication by the RADIUS server and passed to the NAS upon successful EAP authentication.

Syntax Opaque Value

Length 1-246

Type 26

Vendor ID 24757

VSA Type 5

NAS-Filter-Rule

Indicates filter rules to be applied for the user.

Syntax Opaque Value

Length 1-246

Type 92

Vendor ID N/A

VSA Type N/A

NAS-Identifier

This attribute identifies the NAS generating the record.

Syntax String

Length 1-253

Type 32

Vendor ID N/A

VSA Type N/A

NAS-IP-Address

This attribute identifies the serving NAS.

Syntax IPv4 Address

Length 4

Type 4

Vendor ID N/A

VSA Type N/A

NAS-Port

This attribute describes the resource number assigned to the user session. It is guaranteed to be unique at a particular instance in time for a particular chassis.

Syntax Unsigned Integer

Length 4

Type 5

Vendor ID N/A

VSA Type N/A

NAS-Port-Type

This attribute indicates the physical layer that the session is using.

Syntax Enumerated Integer. Supports the following value(s):

- Async = 0
- Sync = 1
- ISDN_Sync = 2
- ISDN_Async_V_120 = 3
- ISDN_Async_V_110 = 4
- Virtual = 5
- 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
- Wireless_IEEE_802_11 = 19

- Token_Ring = 20
- FDDI = 21
- Wireless_CDMA2000 = 22
- Wireless_UMTS = 23
- HRPD = 24
- IAPP = 25
- FTTP = 26
- Wireless_IEEE_802_16 = 27
- Wireless_IEEE_802_20 = 28
- Wireless_IEEE_802_22 = 29
- Wireless_XGP = 36
- Wireless_DHCP = 41

Length 4

Type 61

Vendor ID N/A

VSA Type N/A

Paging-Grid-Id

Syntax Opaque Value

Length 12

Type 26

Vendor ID 9

VSA Type 119

PMIP6-RK-KEY

The PMIP6-RK-KEY sent by the RADIUS Server to the ASN and hCSN LMA for PMIP6. It is used to calculate the individual LMA-MAG key being the base for PBU and PBA messages protection through mobility authentication options.

Syntax Opaque Value

Length 1-251

Type 26

Vendor ID 24757

VSA Type 131

PMIP6-RK-SPI

The SPI associated with the PMIP6-RK-KEY.

Syntax Unsigned Integer

Length 4

Type 26

Vendor ID 24757

VSA Type 132

PMIP6-Service-Info

Indicates which PMIPv6 features are supported and enabled on ASN/LMA.

Syntax Unsigned Integer

Length 2

Type 26

Vendor ID 24757

VSA Type 126

PMIP-Authenticated-Nwk-Id

The real user identifier returned by hAAA after successful authentication.

Syntax Opaque Value

Length 1-246

Type 26

Vendor ID 24757

VSA Type 78

Prepaid-Ind

Syntax Opaque Value

Length 4

Type 226

Vendor ID N/A

VSA Type N/A

Presence

This attribute is used to indicate the availablility of Location based service on HNB.

Syntax Opaque Value

Length 1

Type 26

Vendor ID 9

VSA Type 118

Price-Plan

Opaque 1 byte value received from customer RADIUS server in Access Request. Used in custom dictionary.

Syntax Unsigned Integer

Length 4

Type 26

Vendor ID 5535

VSA Type 196

Primary-DNS-Server

Same as SN1-Primary-DNS-Server standard attribute; non-standard behavior for use in custom dictionary.

Syntax IPv4 Address

Length 4

Type 135

Vendor ID N/A

VSA Type N/A

Prohibit-Payload-Compression1

Flag to prohibit SGSN from compressing user data on per APN basis.

Type 26

Syntax Enumerated Integer. Supports the following value(s):

- Allowed = 0
- Prohibited = 1

Length 2

Vendor ID 8164

VSA Type 237

Prohibit-Payload-Compression

Flag to prohibit SGSN from compressing user data on per APN basis.

Type 26

Syntax Enumerated Integer. Supports the following value(s):

- Allowed = 0
- Prohibited = 1

Length 2

Vendor ID 8164

VSA Type 237

Reject-Cause

This attribute indicates the cause for sending Access-Reject.

Syntax Opaque Value

Length 1

Type 26

Vendor ID 9

VSA Type 116

Reply-Message

This attribute indicates the text to be displayed to a user upon completion of authentication, whether successful or not.

Syntax String

Length 1-253

Type 18

Vendor ID N/A

VSA Type N/A

RRQ-HA-IP

Syntax Opaque Value

Length 4-16

Type 26

Vendor ID 24757

VSA Type 18

RRQ-MN-HA-KEY

MN-HA key computed using RRQ-HA-IP if sent in Access request.

Syntax Opaque Value

Length 1-244

Type 26

Vendor ID 24757

VSA Type 19

Secondary-DNS-Server

Same as SN1-Secondary-DNS-Server standard attribute; non-standard behavior for use in custom dictionary.

Syntax IPv4 Address

Length 4

Type 136

Vendor ID N/A

VSA Type N/A

Selection-Mode

Same as 3GPP-Selection-Mode standard attribute; non-standard behavior for use in custom dictionary.

Syntax Opaque Value

Length 1

Type 229

Vendor ID N/A

VSA Type N/A

Service-Selection

This attribute specifies the service network of UE (APN name).

Syntax Opaque Value

Length 1-253

Type 146

Vendor ID N/A

VSA Type N/A

Service-Type

This attribute identifies the service that the user is attempting to use (Access-Request), or is granted to use (Access-Accept).

Syntax Enumerated Integer. Supports the following value(s):

- 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 = 15
- IAPP_AP_Check = 16
- Authorize_Only = 17
- Inspector = 19650516
- Security_Admin = 19660618

Length 4

Type 6

Vendor ID N/A

VSA Type N/A

Session-Timeout

This attribute sets the maximum session time in seconds. After this session time expires the chassis will tear down the session.

Syntax Unsigned Integer

Length 4

Type 27

Vendor ID N/A

VSA Type N/A

SGSN-IP-Address

Same as 3GPP-SGSN-Address standard attribute; non-standard behavior for use in custom dictionary.

Syntax IPv4 Address

Length 4

Type 228

Vendor ID N/A

VSA Type N/A

SIP-AOR

This attribute identifies the URI, the use of which must be authenticated and authorized.

Syntax Opaque Value

Length 0-253

Type 122

Vendor ID N/A

VSA Type N/A

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.

Syntax Enumerated Integer. Supports the following value(s):

- Normal = 0
- DF-Ignore = 1
- DF-Fragment-ICMP-Notify = 2

Length 4

Type 26

Vendor ID 8164

VSA Type 63

SN1-Acct-Input-Giga-Dropped

This attribute contains the number of input gigawords dropped if the number of input bytes is greater than 2^32 - 1.

Type 26

Syntax Unsigned Integer

Length 4

Vendor ID 8164

VSA Type 230

SN1-Acct-Input-Octets-Dropped

This attribute contains the number of input bytes dropped.

Type 26

Syntax Unsigned Integer

Length 4

Vendor ID 8164

VSA Type 228

SN1-Acct-Input-Packets-Dropped

This attribute contains the number of input packets dropped.

Type 26

Syntax Unsigned Integer

Length 4

Vendor ID 8164

VSA Type 226

SN1-Acct-Output-Giga-Dropped

This attribute contains the number of output gigawords dropped if the number of output bytes is greater than 2^32 - 1.

Type 26

Syntax Unsigned Integer

Length 4

Vendor ID 8164

VSA Type 231

SN1-Acct-Output-Octets-Dropped

This attribute contains the number of output bytes dropped.

Type 26

Syntax Unsigned Integer

Length 4

Vendor ID 8164

VSA Type 229

SN1-Acct-Output-Packets-Dropped

This attribute contains the number of output packets dropped.

Type 26

Syntax Unsigned Integer

Length 4

Vendor ID 8164

VSA Type 227

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.

Syntax Integer

Length 4

Type 26

Vendor ID 8164

VSA Type 72

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.

Syntax Enumerated Integer. Supports the following value(s):

- 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 NoCons = 16
- CLI-NoCons = 17
- FTP-NoCons = 18
- CLI-FTP-NoCons = 19
- Intercept-NoCons = 20
- CLI-Intercept-NoCons = 21
- CLI-Intercept-FTP-NoCons = 23
- ECS-NoCons = 24
- CLI-ECS-NoCons = 25
- CLI-FTP-ECS-NoCons = 27
- CLI-Intercept-ECS-NoCons = 29
- CLI-Intercept-FTP-ECS-NoCons = 31

Length 4

Type 26

Vendor ID 8164

VSA Type 21

SN1-Assigned-VLAN-ID

The VLAN ID assigned to the subscriber.

Syntax Unsigned Integer

Length 4

Type 26

Vendor ID 8164

VSA Type 152

SN1-Call-Id

Internal system generated call ID number for the session.

Syntax Unsigned Integer

Length 4

Type 26

Vendor ID 8164

VSA Type 251

SN1-Cause-For-Rec-Closing

This attribute contains a reason for the release of the CDR.

Syntax Unsigned Integer

Length 4

Type 26

Vendor ID 8164

VSA Type 139

SN1-CFPolicy-ID

This attribute contains the Content Filtering policy ID.

Syntax Unsigned Integer

Length 4

Type 26

Vendor ID 8164

VSA Type 220

SN1-Change-Condition

This attribute defines the reason for closing the container.

Syntax Enumerated Integer. Supports the following value(s):

- QOSCHANGE = 0
- TARIFFTIMECHANGE = 1
- SGSNCHANGE = 500

Length 4

Type 26

Vendor ID 8164

VSA Type 140

SN1-Charging-VPN-Name

Charging VPN Name.

Syntax String

Length 1-252

Type 26

Vendor ID 8164

VSA Type 137

SN1-Chrg-Char-Selection-Mode

This attribute contains the charging characteristics type that the GSNs applied to the CDR.

Syntax Unsigned Integer

Length 4

Type 26

Vendor ID 8164

VSA Type 138

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.

Syntax Enumerated Integer. Supports the following value(s):

- Disabled = 0
- Enabled = 1

Length 4

Type 26

Vendor ID 8164

VSA Type 49

SN1-DHCP-Lease-Expiry-Policy

This attribute specifies whether to renew or disconnect on expiry of IP address lease time.

Type 26

Syntax Enumerated Integer. Supports the following value(s):

- auto-renew = 0
- disconnect = 1

Length 4

Vendor ID 8164

VSA Type 157

SN1-Disconnect-Reason

This attribute contains the reason the user was disconnected from service.

Syntax Enumerated Integer. Supports the following value(s):

- 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-actv-rejected-due-to-rnc = 274
- sgsn-apn-restrict-vio = 275
- sgsn-actv-rejected-by-sgsn = 276
- sgsn-abnormal-deact = 277
- sgsn-actv-rejected-by-ggsn = 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-pdp-status-mismatch = 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
- sfw-policy-removed-mid-session = 407
- FNG-Auth-failed = 408
- ha-stale-key-disconnect = 409
- No-IPV6-address-for-subscriber = 410
- prefix-registration-failure = 411
- disconnect-from-policy-server = 412
- s6b-auth-failed = 413
- gtpc-err-ind = 414

- gtpu-err-ind = 415
- invalid-pdn-type = 416
- aaa-auth-req-failed = 417
- apn-denied-no-subscription = 418
- Sgw-context-replacement = 419
- dup-static-ip-addr-req = 420
- apn-restrict-violation = 421
- invalid-wapn = 422
- ttg-nsapi-allocation-failed = 423
- mandatory-gtp-ie-missing = 424
- aaa-unreachable = 425
- asngw-service-flow-deletion = 426
- CT-PMIP-RRQ-NVSE-Value-Change = 427
- tcp-read-failed = 428
- tcp-write-failed = 429
- ssl-handshake-failed = 430
- ssl-renegotiate-failed = 431
- ssl-bad-message = 432
- ssl-alert-received = 433
- ssl-disconnect = 434
- ssl-migration = 435
- sgsn-ard-failure = 436
- sgsn-camel-release = 437
- sgsn-egtpc-connection-failed = 438
- sgsn-egtpc-create-sess-failed = 439
- sgsn-hss-detach = 440
- sgsn-hss-connection-failure = 441
- sgsn-pgw-detach = 442
- sgsn-s5-s8-no-support-for-apn = 443
- sgsn-no-rab-for-gbr-bearer = 444
- sgsn-sgw-selection-failure = 445
- sgsn-pgw-selection-failure = 446

- Hotlining-Status-Change = 447
- ggsn-no-rsp-from-sgsn = 448
- diameter-protocol-error = 449
- diameter-request-timeout = 450
- operator-policy = 451
- spr-connection-timeout = 452
- mipha-dup-wimax-session = 453
- invalid-version-attr = 454
- sgsn-zone-code-failure = 455
- invalid-qci = 456
- no_rules = 457
- sgsn-rnc-no-dual-pdp-init-deact = 458
- mme-init-ctxt-setup-failure = 459
- mme-driver-initiated = 460
- mme-s1ap-connection-down = 461
- mme-s1ap-reset-recd = 462
- mme-s6a-response-timeout = 463
- mme-s13-response-timeout = 464
- mme-Illegal-equipment = 465
- mme-unexpected-attach = 466
- mme-sgw-selection-failure = 467
- mme-pgw-selection-failure = 468
- mme-reselection-to-sgsn = 469
- mme-relocation-to-sgsn = 470
- mme-reselection-to-mme = 471
- mme-relocation-to-mme = 472
- mme-tau-attach-collision = 473
- mme-old-sgsn-resolution-failure = 474
- mme-old-mme-resolution-failure = 475
- mme-reloc-ho-notify-timeout = 476
- mme-reloc-ho-req-ack-timeout = 477
- mme-create-session-timeout = 478

- mme-create-session-failure = 479
- mme-s11-path-failure = 480
- mme-policy-no-ue-irat = 481
- mme-x2-handover-failed = 482
- mme-attach-restrict = 483
- mme-reloc-to-non-3GPP = 484
- mme-no-response-from-ue = 485
- mme-sgw-relocation-failed = 486
- mme-implicit-detach = 487
- sgsn-detach-notify = 488
- emergency-inactivity-timeout = 489
- policy-initiated-release = 490
- gy-result-code-system-failure = 491
- mme-zone-code-validation-failed = 492
- sgsn-pgw-init-deact = 493
- s6b-ip-validation-failed = 494
- sgsn-failure-rsp-from-sgw = 495
- tcp-remote-close = 496
- tcp-reset-received = 497
- tcp-socket-error = 498
- ptmsi-signature-mismatch = 499
- camel-invalid-configuration = 500
- 4Gto3G-context-replacement = 501
- mme-isr-sgsn-init-detach = 502
- sgsn-isr-addl-ptmsi-rai = 503
- sgsn-sgw-dbr-cause-isr-deact = 504
- sgsn-isr-mme-init-detach = 505
- mme-sgw-dbr-cause-isr-deact = 506
- sgsn-ptmsi-crunch = 507
- 3Gto4G-context-replacement = 508
- mme-no-eps-bearers-activated = 509
- intra-ggsn-handoff = 510

- WSG-Auth-failed = 511
- Gtp-non-existent-pdp-context = 512
- sgsn-cancel-loc-inital-attach = 513
- Local-fallback-timeout = 514
- sgsn-nrspca-actv-rej-by-sgsn = 515
- sgsn-nrspca-actv-rej-by-ms = 516
- ims-authorization-config-delete = 517
- sgsn-no-ptmsi-signature = 518
- pgw-sel-dns-server-nt-reachable = 519
- pgw-sel-dns-no-resource-records = 520
- pgw-sel-dns-no-service-params = 521
- ePDG-Auth-failed = 522
- ePDG-pgw-sel-failure-initial = 523
- ePDG-pgw-sel-failure-handoff = 524
- sgsn-ho-sgw-reloc-collision = 525
- ePDG-dbr-from-pgw = 526
- ePDG-gtpc-abort-session = 527
- ePDG-gtpu-abort-session = 528
- ePDG-gtpu-error-ind = 529
- ePDG-pgw-not-reachable = 530
- ePDG-reject-from-pgw = 531
- ipsg-session-replacement = 532
- ePDG-rel-due-to-handoff = 533
- mme-foreign-plmn-guti-rejected = 534
- sgsn-dsd-allepswithdrawn = 535
- NAT-Pool-BusyOut-Or-Pend-Delete = 536
- Invalid-APN = 537
- srvcc-ps-to-cs-handover = 538
- henbgw-mme-s1ap-reset-recd = 539
- henbgw-henb-s1ap-reset-recd = 540
- henbgw-ue_sess-mme-conn-down = 541
- henbgw-ue-sess-henb-conn-down = 542

- henbgw-handoff-complete = 543
- henbgw-handover-failed = 544
- henbgw-mme-error-indication = 545
- henbgw-henb-error-indication = 546
- henbgw-henb-initiated-release = 547
- henbgw-mme-initiated-release = 548
- henbgw-duplicate-session = 549
- Transport-mismatch-with-PGW = 550
- icsr-ipsec-chkpt-failed = 551
- sgsn-dbr-cause-isr-deact-detach = 552
- unexpected-scenario = 553
- icsr-delete-standby = 554
- epdg-local-pgw-res-failed = 555
- sgsn-iovui-negotiation-failure = 556
- henbgw-gw2henb-inv-mmeues1apid = 557
- henbgw-gw2mme-inv-mmeues1apid = 558
- henbgw-henb-sess-henb-conn-down = 559
- henbgw-nw-path-unavailable = 560
- pgw-transaction-timeout = 561
- samog-multi-dev-pgw-sel-failure = 562
- samog-multi-dev-demux-failure = 563
- mme-pgw-restarted = 564
- samog-session-replacement = 565
- authorization-failed = 566
- mm-apn-congestion-control = 567
- samog-pgw-init-detach = 568
- samog-ggsn-init-detach = 569
- samog-pgw-rejected = 570
- samog-ggsn-rejected = 571
- samog-pgw-no-response = 572
- samog-ggsn-no-response = 573
- samog-gtpc-path-failure = 574

- samog-gtpu-path-failure = 575
- samog-gtpu-err-ind = 576
- samog-mandatory-ie-missing = 577
- samog-mandatory-ie-incorrect = 578
- samog-ip-alloc-failed = 579
- samog-default-gw-not-found = 580
- samog-dns-unreachable = 581
- samog-dns-no-resource-records = 582
- samog-dns-no-service-params = 583
- samog-internal-error = 584
- handoff-pcf-restriction = 585
- graceful-cleanup-on-audit-fail = 586
- ue-ctxt-normal-del-ntsr-ddn = 587
- session-auto-delete = 588
- mme-qos-pgw-upgrade-reject = 589
- path-failure-s5 = 590
- path-failure-s11 = 591
- path-failure-s4 = 592
- gtpu-path-failure-s5u = 593
- gtpu-path-failure-s1u = 594
- gtpu-path-failure-s4u = 595
- gtpu-path-failure-s12u = 596
- gtpu-err-ind-s5u = 597
- gtpu-err-ind-s1u = 598
- gtpu-err-ind-s4u = 599
- gtpu-err-ind-s12u = 600
- diameter-network-too-busy = 601
- diameter-network-failure = 602
- diameter-roaming-not-allowed = 603
- diameter-rat-disallowed = 604
- diameter-no-subscription = 605
- pcc-data-mismatch = 606

- mme-embms-call_setup-timeout = 607
- mme-embms-normal-disconnect = 608
- mme-embms-sctp-down = 609
- disconnect-from-charging-server = 610
- disconnect-irat-fail-hi-missing = 611
- apn-not-supported-in-plmn-rat = 612
- ue-pcscf-reselect-not-supported = 613
- newer-session-detected = 614
- mme-guti_realloc_failed-detach = 615
- mme-pcscf-rest-detach = 616
- Reject-ho-old-tun-path-failure = 617
- gx-vapn-selection-failed = 618
- dup-static-ipv6-addr-req = 619
- mip-path-failure = 620
- apn-congestion = 621
- ue-redirected = 622
- ePDG-s2b-access-denied = 623
- ePDG-s2b-network-failure = 624
- ePDG-s2b-msg-failure = 625
- ePDG-s2b-rat-disallowed = 626
- ePDG-roaming-mandatory = 627
- gtpv2-peer-context-not-found = 628
- SaMOG-access-switch-timeout = 629
- decrypt-fail-count-exceeded = 630
- emergency-idle-timeout = 631
- gtpu-path-failure-s11u = 632
- gtpu-err-ind-s11u = 633
- mme-gtpu-path-failure-s11u = 634
- mme-gtpu-err-ind-s11u = 635
- ePDG-pcscf-restoration = 636
- samog-lbo-user-logout = 637
- sx-req-rej = 638

- sx-cntxt-not-found = 639
- sx-mand-ie-missing = 640
- sx-cond-ie-missing = 641
- sx-msg-invalid-length = 642
- sx-mand-ie-incorrect = 643
- sx-invld-fwd-policy = 644
- sx-invld-fteid-alloc-opt = 645
- sx-no-establshd-sx-association = 646
- sx-no-response = 647
- sx-no-resource = 648
- sx-fteid-ipaddr-type-mismatch = 649
- sx-invalid-response = 650
- user-plane-info-not-available = 651
- user-plane-info-mismatch = 652
- ikev2-req-rate-exceeded = 653
- mme-decor-call-rerouted = 654
- mme-decor-call-rejected = 655
- origin-state-id-change = 656
- mme-ducon-path-update-failed = 657
- diam-no-non-3gpp-subscription = 658
- diameter-user-unknown = 659
- diameter-illegal-equipment = 660
- epdg-invalid-imei = 661
- sx-path-failure = 662
- sxfail-opr-revert-info = 663
- sxfail-opr-get-usagereport = 664
- sxfail-opr-create-rulebase-pdr = 665
- sxfail-opr-remove-pdr = 666
- gtp-remote-data-teid-invalid = 667
- smp-fp-tep-oper-failure = 668
- smp-fp-ambr-oper-failure = 669
- smp-fp-brr-stream-oper-failure = 670

- smp-fp-brr-strm-chrgng-op-fail = 671
- smp-fp-itc-bw-oper-failure = 672
- smp-fp-strm-chrg-oper-failure = 673
- vpp-next-hop-failure = 674
- graceful-cleanup-up-audit-fail = 675
- sx-max-trans-threshold-reached = 676
- sx-db-ub-collision = 677
- sx-failure-ntsr = 678
- graceful-term-up-self-protectn = 679

Length 4

Type 26

Vendor ID 8164

VSA Type 3

SN1-DNS-Proxy-Intercept-List

DNS proxy list.

Syntax String

Length 1-253

Type 26

Vendor ID 8164

VSA Type 214

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.

Syntax Enumerated Integer. Supports the following value(s):

- Disable = 0
- Enable = 1

Length 4

Type 26

Vendor ID 8164

VSA Type 25

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).

Syntax Opaque Value

Length 1

Type 26

Vendor ID 8164

VSA Type 141

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

Syntax Compound. Contains the following sub-attribute(s).

Rating-Group-ID

Rating-Group-ID for which the WiMAX PPAQ is allocated or reported.

Syntax Unsigned Integer

Length 4

Type 11

GPRS-Uplink

Uplink octet usage for a PDP context per rating group.

Syntax Unsigned Integer

Length 4

Type 2

GPRS-Downlink

Downlink octet usage for a PDP context per rating group.

Syntax Unsigned Integer

Length 4

Type 3

SN1-Enable-QoS-Renegotiation

This attribute configures the enabling of dynamic QoS renegotiation.

Syntax Enumerated Integer. Supports the following value(s):

- No = 0
- Yes = 1

Length 4

Type 26

Vendor ID 8164

VSA Type 144

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.

Syntax String

Length 1-247

Type 26

Vendor ID 8164

VSA Type 41

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.

Syntax IPv4 Address

Length 4

Type 26

Vendor ID 8164

VSA Type 56

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.

Syntax Unsigned Integer

Length 4

Type 26

Vendor ID 8164

VSA Type 59

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.

Syntax Unsigned Integer

Length 4

Type 26

Vendor ID 8164

VSA Type 57

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.

Syntax IPv4 Address

Length 4

Type 26

Vendor ID 8164

VSA Type 55

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.

Syntax Unsigned Integer

Length 4

Type 26

Vendor ID 8164

VSA Type 58

SN1-Firewall-Enabled

Firewall for subscriber enabled.

Syntax Enumerated Integer. Supports the following value(s):

- False = 0

- True = 1

Length 4

Type 26

Vendor ID 8164

VSA Type 198

SN1-FMC-Location

MAC address and CDMA location information.

Syntax String

Length 1-247

Type 26

Vendor ID 8164

VSA Type 171

SN1-GGSN-MIP-Required

This attribute specifies if MIP is required for the GGSN subscriber.

Syntax Enumerated Integer. Supports the following value(s):

- Disabled = 0
- Enabled = 1

Length 4

Type 26

Vendor ID 8164

VSA Type 68

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.

Syntax Enumerated Integer. Supports the following value(s):

- Disabled = 0
- Enabled = 1

Length 4

Type 26

Vendor ID 8164

VSA Type 54

SN1-GTP-Version

This attribute contains the version of GTP the subscriber is using.

Syntax Enumerated Integer. Supports the following value(s):

- GTP_VERSION_0 = 0
- GTP_VERSION_1 = 1
- GTP_VERSION_2 = 2

Length 4

Type 26

Vendor ID 8164

VSA Type 62

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.

Syntax Enumerated Integer. Supports the following value(s):

- Disabled = 0
- Enabled = 1

Length 4

Type 26

Vendor ID 8164

VSA Type 47

SN1-Home-Behavior

This attribute specifies the configuration for the behavior bits settings for a home subscriber in an APN.

Syntax Unsigned Integer

Length 4

Type 26

Vendor ID 8164

VSA Type 119

SN1-Home-Profile

This attribute specifies the configuration for the profile bits settings for a home subscriber in an APN.

Syntax Unsigned Integer

Length 4

Type 26

Vendor ID 8164

VSA Type 109

SN1-Home-Sub-Use-GGSN

This attribute configures GGSN to accept GGSN's charging characteristics for home subscribers defined for the APN.

Syntax Enumerated Integer. Supports the following value(s):

- Deny = 0
- Accept = 1

Length 4

Type 26

Vendor ID 8164

VSA Type 106

SN1-Ignore-Unknown-HA-Addr-Err

Value of 1 enables HA to ignore unknown HA address error for incoming RRQ.

Type 26

Syntax Unsigned Integer

Length 1

Vendor ID 8164

VSA Type 160

SN1-IMS-AM-Address

IMS application manager address.

Syntax IPv4 Address

Length 4

Type 26

Vendor ID 8164

VSA Type 167

SN1-IMS-AM-Domain-Name

IMS application manager domain name.

Syntax String

Length 1-64

Type 26

Vendor ID 8164

VSA Type 168

SN1-IMSI

This is the IMSI that identifies the mobile subscriber.

Syntax Opaque Value

Length 1-8

Type 26

Vendor ID 8164

VSA Type 252

SN1-Inactivity-Time

This attribute contains the inactivity time duration for a subscriber session under long time duration timer configuration.

Syntax Integer

Length 4

Type 26

Vendor ID 8164

VSA Type 232

SN1-Interim-Event

Syntax Enumerated Integer. Supports the following value(s):

- QoS-Change = 1
- RAT-Change = 2

Length 1

Type 26

Vendor ID 8164

VSA Type 241

SN1-Internal-SM-Index

GGSN charging service. For internal use.

Syntax Unsigned Integer

Length 4

Type 26

Vendor ID 8164

VSA Type 122

SN1-IP-Alloc-Method

This attribute specifies the method for allocating an IP address. This feature only applies to the GGSN Service.

Syntax Enumerated Integer. Supports the following value(s):

- Alloc_Local_Pool = 0
- Alloc_Dhcp_Client = 1
- Alloc_Radius = 2
- Alloc_No_Alloc = 3
- Alloc_Static_Alloc = 4
- Alloc_Dhcp_Relay = 5

Length 4

Type 26

Vendor ID 8164

VSA Type 53

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.

Syntax String

Length 1-253

Type 26

Vendor ID 8164

VSA Type 10

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.

Syntax String

Length 1-253

Type 26

Vendor ID 8164

VSA Type 11

SN1-IP-Header-Compression

Specifies the IP header compression method to use.

Syntax Enumerated Integer. Supports the following value(s):

- None = 0
- VJ = 1
- ROHC = 2
- VJ_ROHC = 3

Length 4

Type 26

Vendor ID 8164

VSA Type 150

SN1-IP-Hide-Service-Address

This attribute prevents the IP address bound to a call service from responding to ping and IMCP error packets.

Syntax Enumerated Integer. Supports the following value(s):

- No = 0
- Yes = 1

Length 4

Type 26

Vendor ID 8164

VSA Type 60

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.

Syntax String

Length 1-253

Type 26

Vendor ID 8164

VSA Type 17

SN1-IP-In-Plcy-Grp

This attribute specifies the name of the policy group config applied in the uplink direction.

Syntax String

Length 1-15

Type 26

Vendor ID 8164

VSA Type 193

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.

Syntax String

Length 1-253

Type 26

Vendor ID 8164

VSA Type 18

SN1-IP-Out-Plcy-Grp

This attribute specifies the name of the policy group config applied in the downlink direction.

Syntax String

Length 1-15

Type 26

Vendor ID 8164

VSA Type 194

SN1-IP-Pool-Name

This attribute contains the name of the IP pool, configured on the chassis, from which an IP address should be chosen for the user.

Syntax String

Length 1-253

Type 26

Vendor ID 8164

VSA Type 8

SN1-IP-Source-Validation

This attribute indicates if the source IP address should be validated before forwarding the IP packet.

Syntax Enumerated Integer. Supports the following value(s):

- No = 0
- Yes = 1

Length 4

Type 26

Vendor ID 8164

VSA Type 14

SN1-IP-Source-Violate-No-Acct

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

Syntax Enumerated Integer. Supports the following value(s):

- Disabled = 0
- Enabled = 1

Length 4

Type 26

Vendor ID 8164

VSA Type 196

SN1-IP-Src-Valid-Drop-Limit

Maximum number of packet drops entertained before disconnecting the session for source violated packets for the session

Syntax Unsigned Integer

Length 4

Type 26

Vendor ID 8164

VSA Type 110

SN1-IPv6-DNS-Proxy

IPV6 DNS Proxy Enabled or Disabled Setting for the session.

Syntax Enumerated Integer. Supports the following value(s):

- Disabled = 0
- Enabled = 1

Length 4

Type 26

Vendor ID 8164

VSA Type 126

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.

Syntax Enumerated Integer. Supports the following value(s):

- Disabled = 0
- Enabled = 1

Length 4

Type 26

Vendor ID 8164

VSA Type 103

SN1-IPv6-Min-Link-MTU

SN1-IPv6-Min-Link-MTU

Syntax Unsigned Integer

Length 4

Type 26

Vendor ID 8164

VSA Type 136

SN1-IPv6-num-rtr-advt

This attribute contains the IPv6 number of Initial Router Advertisements. Default value is 3.

Syntax Unsigned Integer

Length 4

Type 26

Vendor ID 8164

VSA Type 97

SN1-IPv6-Primary-DNS

This attribute specifies a Primary DNS server address that the Router Advertisement message sent by the PDSN will include.

Syntax Opaque Value

Length 16

Type 26

Vendor ID 8164

VSA Type 101

SN1-IPv6-rtr-advt-interval

This attribute contains the IPv6 Initial Router Advertisement Interval, specified in milliseconds. The default value is 3000.

Syntax Unsigned Integer

Length 4

Type 26

Vendor ID 8164

VSA Type 96

SN1-IPv6-Secondary-DNS

This attribute specifies a Secondary DNS server address that the Router Advertisement message sent by the PDSN will include.

Syntax Opaque Value

Length 16

Type 26

Vendor ID 8164

VSA Type 102

SN1-IPv6-Sec-Pool

This attribute contains the IPv6 secondary pool name.

Syntax String

Length 1-253

Type 26

Vendor ID 8164

VSA Type 124

SN1-IPv6-Sec-Prefix

IPv6 Secondary Pool name prefix.

Syntax Opaque Value

Length 2-18

Type 26

Vendor ID 8164

VSA Type 125

SN1-L3-to-L2-Tun-Addr-Policy

This attribute specifies the address allocation policy.

Syntax Enumerated Integer. Supports the following value(s):

- no-local-alloc-validate = 0
- local-alloc = 1
- local-alloc-validate = 2

Length 4

Type 26

Vendor ID 8164

VSA Type 43

SN1-LI-Dest-Address

This attribute specifies the Authorized Destination-IP/Port to which LI packets could be forwarded.

Type 26

Vendor ID 8164

VSA Type 240

Syntax Compound. Contains the following sub-attribute(s).

Length 0-16

SN1-LI-Dest-IP

This attribute specifies the authorized Destination IP to which LI packets could be forwarded.

Syntax IPv4 Address

Length 4

Type 1

SN1-LI-Dest-Port

This attribute specifies the authorized Destination Port to which LI packets could be forwarded.

Syntax Unsigned Integer

Length 2

Type 2

SN1-Local-IP-Address

This attribute contains the IP address of the local interface on the chassis for the user's session.

Syntax IPv4 Address

Length 4

Type 26

Vendor ID 8164

VSA Type 13

SN1-Long-Duration-Action

This attribute specifies the action to take place when the long duration timeout expires for a subscriber session.

Syntax Enumerated Integer. Supports the following value(s):

- Detection = 1
- Disconnection = 2
- Dormant-Only-Disconnection = 3
- Dormant-Only-Detection = 4

Length 4

Type 26

Vendor ID 8164

VSA Type 45

SN1-Long-Duration-Notification

Long Duration Notification.

Syntax Enumerated Integer. Supports the following value(s):

- Suppress = 0

- Send = 1

Length 4

Type 26

Vendor ID 8164

VSA Type 253

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.

Syntax Integer

Length 4

Type 26

Vendor ID 8164

VSA Type 44

SN1-Mediation-Acct-Rsp-Action

When this attribute is set to None, there is no action taken while waiting for a response for the accounting start message from the Mediation Accounting server. When this attribute is set to No-Early-PDUs the system buffers all packets from the user (uplink) until a response for the accounting start message is received from the Mediation Accounting server. When set to Delay_GTP_Response, the system does not send a GTP create PDP response to the GGSN until a response for the accounting start message is received from the Mediation Accounting server. If the attribute is not present in Access-Accept message or if the attribute value is invalid, the value "None" is assumed.

Syntax Enumerated Integer. Supports the following value(s):

- None = 0
- No_Early_PDUs = 1
- Delay_GTP_Response = 2

Length 4

Type 26

Vendor ID 8164

VSA Type 105

SN1-Mediation-Enabled

This attribute indicates whether the Mediation Accounting configuration is enabled or disabled for GGSN.

Syntax Enumerated Integer. Supports the following value(s):

- Disabled = 0

- Enabled = 1

Length 4

Type 26

Vendor ID 8164

VSA Type 123

SN1-Mediation-No-Interims

This attribute is used to disable or enable Mediation Interim Accounting Records for the session.

Syntax Enumerated Integer. Supports the following value(s):

- Disabled = 0
- Enabled = 1

Length 4

Type 26

Vendor ID 8164

VSA Type 146

SN1-Mediation-VPN-Name

This attribute specifies the Mediation Context name for the session.

Syntax String

Length 1-128

Type 26

Vendor ID 8164

VSA Type 104

SN1-Min-Compress-Size

This attribute contains the minimum size (in octets) a data packet can have in order to be compressed.

Syntax Unsigned Integer

Length 4

Type 26

Vendor ID 8164

VSA Type 23

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.

Syntax Enumerated Integer. Supports the following value(s):

- Disabled = 0
- Enabled = 1

Length 4

Type 26

Vendor ID 8164

VSA Type 50

SN1-MIP-ANCID

Accounting correlation ID created by IPGW, received by VBM and HBM.

Syntax Opaque Value

Length 12

Type 26

Vendor ID 8164

VSA Type 166

SN1-MIP-Dual-Anchor

Enable/disable dual-anchor service for a subscriber.

Syntax Enumerated Integer. Supports the following value(s):

- Disabled = 0
- Enabled = 1

Length 4

Type 26

Vendor ID 8164

VSA Type 165

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.

Syntax String

Length 1-253

Type 26

Vendor ID 8164

VSA Type 154

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.

Syntax Enumerated Integer. Supports the following value(s):

- Disabled = 0
- Enabled = 1

Length 4

Type 26

Vendor ID 8164

VSA Type 51

SN1-MIP-MIN-Reg-Lifetime-Realm

This attribute configures the minimum MIP registration lifetime for a subscriber/realm.

Syntax Unsigned Integer

Length 4

Type 26

Vendor ID 8164

VSA Type 12

SN1-MIP-Reg-Lifetime-Realm

Configure the maximum MIP registration lifetime for a subscriber/realm.

Syntax Unsigned Integer

Length 4

Type 26

Vendor ID 8164

VSA Type 175

SN1-MIP-Send-Ancid

AAA attribute to enable/disable sending ANCID from FA to HA in MIP RRQ.

Syntax Enumerated Integer. Supports the following value(s):

- Disabled = 0
- Enabled = 1

Length 4

Type 26

Vendor ID 8164

VSA Type 163

SN1-MIP-Send-Correlation-Info

This attribute enables/disables sending of correlation-id from FA to HA in MIP RRQ.

Syntax Enumerated Integer. Supports the following value(s):

- Disabled = 0
- NVSE_Starent = 1
- NVSE_CUstom1 = 2
- NVSE_Custom2 = 3

Length 4

Type 26

Vendor ID 8164

VSA Type 188

SN1-MIP-Send-Imsi

Attribute to enable/disable sending IMSI from FA to HA in MIP RRQ.

Syntax Enumerated Integer. Supports the following value(s):

- Disabled = 0
- NVSE_Starent = 1
- NVSE_Custom1 = 2
- NVSE_Custom2 = 3

Length 4

Type 26

Vendor ID 8164

VSA Type 164

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.

Syntax Enumerated Integer. Supports the following value(s):

- Disabled = 0
- NVSE_Custom1 = 1
- NVSE_Custom2 = 2
- NVSE_Starent = 3

Length 4

Type 26

Vendor ID 8164

VSA Type 48

SN1-MN-HA-Hash-Algorithm

This attribute contains the hash algorithm to use for MN-HA authentication.

Syntax Enumerated Integer. Supports the following value(s):

- MD5 = 1
- MD5-RFC2002 = 2
- HMAC-MD5 = 3

Length 4

Type 26

Vendor ID 8164

VSA Type 99

SN1-MN-HA-Timestamp-Tolerance

This attribute contains the duration of timestamp tolerance, in seconds, to use for MN-HA authentication.

Syntax Unsigned Integer

Length 4

Type 26

Vendor ID 8164

VSA Type 30

SN1-MS-ISDN

SN1-MS-ISDN.

Syntax Opaque Value

Length 1-9

Type 26

Vendor ID 8164

VSA Type 248

SN1-NAI-Construction-Domain

This attribute specifies the domain name to use when constructing the NAI.

Syntax String

Length 1-247

Type 26

Vendor ID 8164

VSA Type 37

SN1-NAT-Bind-Record

This attribute contains the NAT Binding Record.

Type 26

Vendor ID 8164

VSA Type 216

Syntax Compound. Contains the following sub-attribute(s).

NAT-IP-Address

NAT IP address.

Syntax IPv4 Address

Length 4

Type 1

NAT-Port-Block-Start

Start port of the port chunk

Syntax Unsigned Integer

Length 2

Type 2

NAT-Port-Block-End

End port of the port chunk.

Syntax Unsigned Integer

Length 2

Type 3

Alloc-Flag

Port chunk status. Accepted Values are 0(De-Allocated) and 1(Allocated).

Syntax Unsigned Integer

Length 1

Type 4

Correlation-Id

Correlation ID.

Syntax String

Length 1-253

Type 5

Loading-Factor

Indicates maximum number of users per NAT IP address.

Syntax Unsigned Integer

Length 2

Type 6

Binding-Timer

Port chunk hold timer.

Syntax Unsigned Integer

Length 4

Type 7

SN1-NAT-Info-Record

NAT-Record-Info.

Type 26

Vendor ID 8164

VSA Type 246

Syntax Compound. Contains the following sub-attribute(s).

Framed-IP-Address

Framed IP address.

Syntax IPv4 Address

Length 4

Type 1

NAT-IP-Address

NAT IP address.

Syntax IPv4 Address

Length 4

Type 2

NAT-Port-Block-Start

Start port of the port chunk

Syntax Unsigned Integer

Length 2

Type 3

NAT-Port-Block-End

End port of the port chunk.

Syntax Unsigned Integer

Length 2

Type 4

Acct-Session-Id

Accounting Session ID.

Syntax String

Length 1-17

Type 5

User-Name

User name.

Syntax String

Length 1-128

Type 6

Correlation-Id

Correlation ID.

Syntax String

Length 1-17

Type 7

Calling-Station-Id

This attribute indicates the MSISDN/Calling station ID.

Syntax String

Length 1-16

Type 8

3GPP-Charging-Id

This attribute specifies the 3GPP Charging Identifier.

Syntax Unsigned Integer

Length 4

Type 9

SN1-NAT-IP-Address-Old

Public IP address used for the call

Syntax IPv4 Address

Length 4

Type 26

Vendor ID 8164

VSA Type 0

SN1-NAT-IP-Address

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

Syntax IPv4 Address

Length 4

Type 26

Vendor ID 8164

VSA Type 217

SN1-NAT-Port

This attribute specifies the port used along with NAT-IP for N:1 case.

Syntax Unsigned Integer

Length 2

Type 26

Vendor ID 8164

VSA Type 179

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.

Syntax Enumerated Integer. Supports the following value(s):

- Best_Effort = 0
- Bronze = 1
- Silver = 2
- Gold = 3
- From_DSCP = 4

Length 4

Type 26

Vendor ID 8164

VSA Type 98

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.

Syntax Opaque Value

Length 1

Type 26

Vendor ID 8164

VSA Type 142

SN1-Ntk-Session-Disconnect-Flag

SN1-Ntk-Session-Disconnect-Flag.

Syntax Enumerated Integer. Supports the following value(s):

- Session-Disconnect = 1

Length 4

Type 26

Vendor ID 8164

VSA Type 143

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.

Syntax String

Length 1-16

Type 26

Vendor ID 8164

VSA Type 65

SN1-Overload-Disc-Connect-Time

Provides the connect time for a session. When this time expires, the session may become a candidate for disconnection.

Syntax Uint32

Type 26

Vendor ID 8164

VSA Type 233

SN1-Overload-Disc-Inact-Time

Provides inactivity time for a session after which it may become candidate for disconnection.

Syntax Uint32

Type 26

Vendor ID 8164

VSA Type 234

SN1-Overload-Disconnect

Enables/disables the overload-disconnect feature (if 1) and disables if 0

Syntax Uint32

Type 26

Vendor ID 8164

VSA Type 235

SN1-PDIF-MIP-Release-TIA

PDIF mobile IP release TIA.

Syntax Enumerated Integer. Supports the following value(s):

- No = 0
- Yes = 1

Length 4

Type 26

Vendor ID 8164

VSA Type 172

SN1-PDIF-MIP-Required

PDIF mobile IP required.

Syntax Enumerated Integer. Supports the following value(s):

- No = 0
- Yes = 1

Length 4

Type 26

Vendor ID 8164

VSA Type 170

SN1-PDIF-MIP-Simple-IP-Fallback

PDIF mobile IP simple IP fallback.

Syntax Enumerated Integer. Supports the following value(s):

- No = 0
- Yes = 1

Length 4

Type 26

Vendor ID 8164

VSA Type 173

SN1-PDSN-Correlation-Id

Correlation ID received from PDSN to HA.

Syntax Opaque Value

Length 8

Type 26

Vendor ID 8164

VSA Type 189

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.

Syntax Enumerated Integer. Supports the following value(s):

- Disabled = 0
- Enabled = 1

Length 4

Type 26

Vendor ID 8164

VSA Type 46

SN1-PDSN-NAS-Id

NAS Identifier received from PDSN to HA.

Syntax String

Length 1-253

Type 26

Vendor ID 8164

VSA Type 190

SN1-PDSN-NAS-IP-Address

NAS IP address received from PDSN to HA.

Syntax IPv4 Address

Length 4

Type 26

Vendor ID 8164

VSA Type 191

SN1-Permit-User-Mcast-PDUs

Specifies whether or not to let the subscriber discard multicast PDUs.

Syntax Enumerated Integer. Supports the following value(s):

- disabled = 0
- enabled = 1

Length 4

Type 26

Vendor ID 8164

VSA Type 134

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.

Syntax Enumerated Integer. Supports the following value(s):

- Disabled = 0
- Enabled = 1

Length 4

Type 26

Vendor ID 8164

VSA Type 95

SN1-PPP-Always-On-Vse

SN1-PPP-Always-On-Vse.

Syntax Enumerated Integer. Supports the following value(s):

- Disabled = 0
- Enabled = 1

Length 4

Type 26

Vendor ID 8164

VSA Type 130

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.

Syntax Enumerated Integer. Supports the following value(s):

- Normal = 0
- Stateless = 1

Length 4

Type 26

Vendor ID 8164

VSA Type 19

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.

Syntax Enumerated Integer. Supports the following value(s):

- None = 0
- Stac-LZS = 1
- MPPC = 2
- Deflate = 4

Length 4

Type 26

Vendor ID 8164

VSA Type 9

SN1-PPP-Keepalive

This attribute indicates the interval for the PPP keepalive, in seconds.

Syntax Unsigned Integer

Length 4

Type 26

Vendor ID 8164

VSA Type 16

SN1-PPP-NW-Layer-IPv4

This attribute indicates the PPP IPCP negotiation for IPv4. The default is enabled.

Syntax Enumerated Integer. Supports the following value(s):

- Disabled = 0
- Enabled = 1
- Passive = 2

Length 4

Type 26

Vendor ID 8164

VSA Type 92

SN1-PPP-NW-Layer-IPv6

This attribute indicates the PPP IPv6CP negotiation for IPv6. The default is enabled.

Syntax Enumerated Integer. Supports the following value(s):

- Disabled = 0
- Enabled = 1
- Passive = 2

Length 4

Type 26

Vendor ID 8164

VSA Type 93

SN1-PPP-Outbound-Password

This attribute indicates the password to be used when the user side of the PPP connection requires authentication.

Syntax String

Length 1-253

Type 26

Vendor ID 8164

VSA Type 15

SN1-PPP-Outbound-Username

This attribute indicates the username to be used when the user side of the PPP connection requires authentication.

Syntax String

Length 1-253

Type 26

Vendor ID 8164

VSA Type 61

SN1-PPP-Progress-Code

This attribute provides information about the "state" of the PPP connection, when the connection was terminated.

Syntax Enumerated Integer. Supports the following value(s):

- Not-Defined = 0
- Call-Lcp-Down = 10
- Call-Disconnecting = 20
- Call-Ppp-Renegotiating = 30
- Call-Arrived = 40
- Call-Pdg-Tcp-Connecting = 45
- Call-Pdg-Ssl-Connecting = 46
- Call-Lcp-Up = 50
- Call-Authenticating = 60
- Call-Bcmcs-Authenticating = 70
- Call-Authenticated = 80
- Call-Tunnel-Connecting = 85
- Call-Ipcp-Up = 90
- Call-Imsa-Authorizing = 95
- Call-Imsa-Authorized = 97
- Call-MBMS-UE-Authorizing = 98
- Call-MBMS-Bearer-Authorizing = 99
- Call-Simple-IP-Connected = 100
- Call-Mobile-IP-Connected = 110
- Call-Tunnel-Connected = 115
- Call-Pdp-Type-IP-Connected = 120
- Call-Pdp-Type-IPv6-Connected = 125
- Call-Pdp-Type-PPP-Connected = 130

- Call-GTP-Connecting = 131
- Call-GTP-Connected = 132
- Call-Proxy-Mobile-IP-Connected = 140
- Call-Pdg-Ssl-Connected = 141
- Call-Pdg-Connected = 142
- Call-Ipsg-Connected = 145
- Call-Bcmcs-Connected = 150
- Call-MBMS-UE-Connected = 155
- Call-MBMS-Bearer-Connected = 156
- Call-Pending-Addr-From-DHCP = 160
- Call-Got-Addr-From-DHCP = 170
- Call-HA-IPSEC-Tunnel-Connecting = 180
- Call-HA-IPSEC-Connected = 190
- Call-ASN-Non-Anchor-Connected = 200
- Call-ASNPC-Connected = 210 Call-Mobile-IPv6-Connected = 220
- Call-PMIPv6-Connected = 221
- Call-PHSPC-Connected = 230
- Call-GTP-IPv4-Connected = 235
- Call-GTP-IPv6-Connected = 236
- Call-GTP-IPv4-IPv6-Connected = 237
- Call-SGW-Connected = 245
- Call-MME-Attached = 246
- Call-Auth-Only-Connected = 247

Length 4

Type 26

Vendor ID 8164

VSA Type 4

SN1-PPP-Reneg-Disc

PPP remote reneg disconnect policy.

Type 26

Syntax Enumerated Integer. Supports the following value(s):

- Never = 0
- Always = 1
- NAI_Prefix_MSID_Mismatch = 2

Length 4

Vendor ID 8164

VSA Type 187

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.

Syntax Enumerated Integer. Supports the following value(s):

- Uncompressed = 0
- Compressed = 1

Length 4

Type 26

Vendor ID 8164

VSA Type 31

SN1-Prepaid-Final-Duration-Alg

For prepaid, final duration is calculated based on the algorithm specified by the value of this attribute.

Syntax Enumerated Integer. Supports the following value(s):

- current_time = 0
- last-user-layer3-activity-time = 1
- last-airlink-activity-time = 2
- last-airlink-activity-time-last-reported = 3

Length 4

Type 26

Vendor ID 8164

VSA Type 135

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.

Syntax Unsigned Integer

Length 4

Type 26

Vendor ID 8164

VSA Type 32

SN1-Prepaid-Outbound-Octets

SN1-Prepaid-Outbound-Octets.

Syntax Unsigned Integer

Length 4

Type 26

Vendor ID 8164

VSA Type 33

SN1-Prepaid-Preference

This attribute specifies whether prepaid is volume based or duration based.

Syntax Enumerated Integer. Supports the following value(s):

- prepaid_duration = 0
- prepaid_volume = 1

Length 4

Type 26

Vendor ID 8164

VSA Type 129

SN1-Prepaid-Profile

Do not do prepaid, regardless of the Rulebase configuration.

Type 26

Syntax Enumerated Integer. Supports the following value(s):

- Use-Rulebase-Config = 0
- Prohibit = 1

Length 4

Vendor ID 8164

VSA Type 155

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.

Syntax Unsigned Integer

Length 4

Type 26

Vendor ID 8164

VSA Type 35

SN1-Prepaid

Prepaid.

Syntax Enumerated Integer. Supports the following value(s):

- no_prepaid = 0
- custom_prepaid = 1
- standard_prepaid = 2
- wimax_prepaid = 4

Length 4

Type 26

Vendor ID 8164

VSA Type 128

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.

Syntax Unsigned Integer

Length 4

Type 26

Vendor ID 8164

VSA Type 34

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.

Syntax Unsigned Integer

Length 4

Type 26

Vendor ID 8164

VSA Type 36

SN1-Primary-DCCA-Peer

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

Syntax String

Length 1-192

Type 26

Vendor ID 8164

VSA Type 223

SN1-Primary-DNS-Server

This attribute indicates the IP address of the primary DNS server that should be used for the session.

Syntax IPv4 Address

Length 4

Type 26

Vendor ID 8164

VSA Type 5

SN1-Primary-NBNS-Server

Primary NBNS Server IP address.

Syntax IPv4 Address

Length 4

Type 26

Vendor ID 8164

VSA Type 148

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.

Syntax Enumerated Integer. Supports the following value(s):

- Disabled = 0
- Enabled = 1

Length 4

Type 26

Vendor ID 8164

VSA Type 52

SN1-QoS-Background-Class

This attribute defines the QOS Background Traffic Class.

Syntax Opaque Value

Length 28

Type 26

Vendor ID 8164

VSA Type 91

SN1-QoS-Class-Background-PHB

SN1-QoS-Class-Background-PHB

Syntax Enumerated Integer. Supports the following value(s):

- 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

Length 4

Type 26

Vendor ID 10415

VSA Type 113

SN1-QoS-Class-Converstional-PHB

SN1-QoS-Class-Converstional-PHB.

Syntax Enumerated Integer. Supports the following value(s):

- 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

Length 4

Type 26

Vendor ID 10415

VSA Type 111

SN1-QoS-Class-Interactive-1-PHB

SN1-QoS-Class-Interactive-1-PHB

Syntax Enumerated Integer. Supports the following value(s):

- 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

Length 4

Type 26

Vendor ID 10415

VSA Type 114

SN1-QoS-Class-Interactive-2-PHB

SN1-QoS-Class-Interactive-2-PHB

Syntax Enumerated Integer. Supports the following value(s):

- 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

Length 4

Type 26

Vendor ID 10415

VSA Type 115

SN1-QoS-Class-Interactive-3-PHB

SN1-QoS-Class-Interactive-3-PHB

Syntax Enumerated Integer. Supports the following value(s):

- 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

Length 4

Type 26

Vendor ID 10415

VSA Type 116

SN1-QoS-Class-Streaming-PHB

SN1-QoS-Class-Streaming-PHB

Syntax Enumerated Integer. Supports the following value(s):

- 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

Length 4

Type 26

Vendor ID 10415

VSA Type 112

SN1-QoS-Conversation-Class

This attribute defines the QOS Conversation Traffic Class.

Syntax Opaque Value

Length 28

Type 26

Vendor ID 8164

VSA Type 86

SN1-QoS-Interactive1-Class

This attribute defines the QOS Interactive Traffic Class.

Syntax Opaque Value

Length 28

Type 26

Vendor ID 8164

VSA Type 88

SN1-QoS-Interactive2-Class

This attribute defines the QOS Interactive2 Traffic Class.

Syntax Opaque Value

Length 28

Type 26

Vendor ID 8164

VSA Type 89

SN1-QoS-Interactive3-Class

This attribute defines the QOS Interactive3 Traffic Class.

Syntax Opaque Value

Length 28

Type 26

Vendor ID 8164

VSA Type 90

SN1-QoS-Negotiated

Negotiated QoS for GGSN sessions.

Syntax Opaque Value

Length 4-28

Type 26

Vendor ID 8164

VSA Type 147

SN1-QoS-Renegotiation-Timeout

This attribute configures the timeout duration of dampening time for dynamic QoS renegotiation.

Syntax Unsigned Integer

Length 4

Type 26

Vendor ID 8164

VSA Type 145

SN1-QoS-Streaming-Class

This attribute defines the QOS Streaming Traffic Class.

Syntax Opaque Value

Length 28

Type 26

Vendor ID 8164

VSA Type 87

SN1-QoS-Tp-Dnlk

This attribute enables/disables Traffic Policing/Shaping in downlink direction.

Syntax Enumerated Integer. Supports the following value(s):

- Disabled = 0
- Policing = 1
- Shaping = 2

Length 4

Type 26

Vendor ID 8164

VSA Type 73

SN1-QoS-Tp-Uplk

This attribute enables/disables Traffic Policing/Shaping in uplink direction.

Syntax Enumerated Integer. Supports the following value(s):

- Disabled = 0
- Policing = 1
- Shaping = 2

Length 4

Type 26

Vendor ID 8164

VSA Type 79

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.

Type 26

Vendor ID 8164

VSA Type 177

Syntax Compound. Contains the following sub-attribute(s).

Direction

Direction of the PDF.

Syntax Unsigned Integer

Length 1

Type 1

Class

Traffic class.

Syntax Unsigned Integer

Length 1

Type 2

Burst-Size

Peak burst size.

Syntax Unsigned Integer

Length 4

Type 3

Committed-Data-Rate

Committed data rate.

Syntax Unsigned Integer

Length 4

Type 4

Peak-Data-Rate

Peak data rate.

Syntax Unsigned Integer

Length 4

Type 5

Exceed-Action

Action to take on packets that exceed the Committed-Data-Rate but do not violate the Peak-Data-Rate.

Syntax Unsigned Integer

Length 1

Type 6

Violate-Action

Violate action.

Syntax Unsigned Integer

Length 1

Type 7

Auto-Readjust-Enabled

Auto-readjust enabled.

Syntax Unsigned Integer

Length 1

Type 8

Auto-Readjust-Duration

Auto-readjust duration.

Syntax Unsigned Integer

Length 4

Type 9

Qci

Available only in 11.0 and later releases. QOS QCI accepted values are 1 (qci 1), 2 (qci 2), 3 (qci 3), 4 (qci 4), 5 (qci 5), 6 (qci 6), 7 (qci 7), 8 (qci 8), 9 (qci 9).

Syntax Unsigned Integer

Length 1

Type 10

SN1-Rad-APN-Name

This attributes specifies the RADIUS returned APN name.

Type 26

Syntax Opaque Value

Length 1-64

Vendor ID 8164

VSA Type 162

SN1-Radius-Returned-Username

This attribute is used to prefer RADIUS returned user name over constructed username in the accounting messages.

Type 26

Syntax Enumerated Integer. Supports the following value(s):

- No = 0
- Yes = 1

Length 4

Vendor ID 8164

VSA Type 236

SN1-Re-CHAP-Interval

The Periodic CHAP authentication interval for PPP, in seconds.

Syntax Unsigned Integer

Length 4

Type 26

Vendor ID 8164

VSA Type 7

SN1-Roaming-Behavior

This attribute specifies the configuration for the behavior bits settings for a roaming subscriber in an APN.

Syntax Unsigned Integer

Length 4

Type 26

Vendor ID 8164

VSA Type 121

SN1-Roaming-Profile

This attribute specifies the configuration for the profile bits settings for a roaming subscriber in an APN.

Syntax Unsigned Integer

Length 4

Type 26

Vendor ID 8164

VSA Type 118

SN1-Roaming-Status

This attribute specifies if the user is in roaming network for HA/LNS calls.

Syntax Enumerated Integer. Supports the following value(s):

- HOME = 0
- ROAMING = 1

Length 1

Type 26

Vendor ID 8164

VSA Type 244

SN1-Roaming-Sub-Use-GGSN

This attribute configures GGSN to accept GGSN's charging characteristics for roaming subscribers defined for the APN.

Syntax Enumerated Integer. Supports the following value(s):

- Deny = 0
- Accept = 1

Length 4

Type 26

Vendor ID 8164

VSA Type 108

SN1-ROHC-Direction

Specifies in which direction to apply Robust Header Compression (ROHC).

Syntax Enumerated Integer. Supports the following value(s):

- Any = 0
- Uplink = 1
- Downlink = 2

Length 4

Type 26

Vendor ID 8164

VSA Type 153

SN1-ROHC-Flow-Marking-Mode

Configure ROHC compression for marked flows only.

Type 26

Syntax Enumerated Integer. Supports the following value(s):

- False = 0
- True = 1

Length 4

Vendor ID 8164

VSA Type 195

SN1-ROHC-Mode

Sets the mode of operation for Robust Header Compression for IP.

Syntax Enumerated Integer. Supports the following value(s):

- Reliable = 0

- Optimistic = 1
- Unidirectional = 2

Length 4

Type 26

Vendor ID 8164

VSA Type 151

SN1-ROHC-Profile-Name

Specifies the ROHC profile name to use for the subscriber.

Type 26

Syntax String

Length 1-64

Vendor ID 8164

VSA Type 238

SN1-Routing-Area-Id

For GGSN calls this indicates the Routing Area ID of the subscriber.

Syntax Opaque Value

Length 3

Type 26

Vendor ID 8164

VSA Type 249

SN1-Rulebase

When the session is active charging enabled, Rulebase name will specify one of the pre configured ECSv2 rulebases in active charging subsystem.

Syntax String

Length 1-64

Type 26

Vendor ID 8164

VSA Type 250

SN1-Secondary-DCCA-Peer

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

Syntax String

Length 1-192

Type 26

Vendor ID 8164

VSA Type 224

SN1-Secondary-DNS-Server

This attribute indicates the IP address of the secondary DNS server that should be used for the session.

Syntax IPv4 Address

Length 4

Type 26

Vendor ID 8164

VSA Type 6

SN1-Secondary-NBNS-Server

Secondary NBNS Server IP Address.

Syntax IPv4 Address

Length 4

Type 26

Vendor ID 8164

VSA Type 149

SN1-Service-Address

Used to send the bind IP address of the service in RADIUS messages.

Syntax IPv4 Address

Length 4

Type 26

Vendor ID 8164

VSA Type 169

SN1-Service-Type

This attribute signifies the type that the user is accessing.

Syntax Enumerated Integer. Supports the following value(s):

- 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
- EPDG = 13
- MIPV6HA = 14
- PGW = 15
- SGW = 16
- FNG = 17
- MSEG = 18
- HNBGW = 19
- BNG = 20
- WSG = 21
- SAMOG = 22

Length 4

Type 26

Vendor ID 8164

VSA Type 24

SN1-Simultaneous-SIP-MIP

This attribute indicates if a PDSN Subscriber can simultaneously be given Simple IP and Mobile IP service.

Syntax Enumerated Integer. Supports the following value(s):

- Disabled = 0
- Enabled = 1

Length 4

Type 26

Vendor ID 8164

VSA Type 22

SN1-Subs-Acc-Flow-Traffic-Valid

This attribute indicates the subscriber account flow traffic is valid.

Type 26

Syntax Enumerated Integer. Supports the following value(s):

- Disable = 0
- Enable = 1

Length 4

Vendor ID 8164

VSA Type 225

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.

Syntax Enumerated Integer. Supports the following value(s):

- None = 0
- Radius = 1
- GTPP = 2

Length 4

Type 26

Vendor ID 8164

VSA Type 64

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.

Syntax Enumerated Integer. Supports the following value(s):

- Normal = 0
- Suppress = 1

Length 4

Type 26

Vendor ID 8164

VSA Type 70

SN1-Subscriber-Acct-Mode

SN1-Subscriber-Acct-Mode

Syntax Enumerated Integer. Supports the following value(s):

- flow-based-auxilliary = 0
- flow-based-all = 1
- flow-based-none = 2
- session-based = 3
- main-a10-only = 4

Length 4

Type 26

Vendor ID 8164

VSA Type 192

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.

Syntax Enumerated Integer. Supports the following value(s):

- None = 0
- No_Early_PDUs = 1
- Delay_GTP_Response = 2

Length 4

Type 26

Vendor ID 8164

VSA Type 100

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.

Syntax Enumerated Integer. Supports the following value(s):

- Normal = 0
- Suppress = 1

Length 4

Type 26

Vendor ID 8164

VSA Type 69

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.

Syntax Enumerated Integer. Supports the following value(s):

- Normal = 0
- Suppress = 1

Length 4

Type 26

Vendor ID 8164

VSA Type 71

SN1-Subscriber-Class

Customer-requested attribute for supporting specific behavior for their subscriber billing.

Syntax Enumerated Integer. Supports the following value(s):

- 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

Length 4

Type 26

Vendor ID 8164

VSA Type 219

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.

Syntax Enumerated Integer. Supports the following value(s):

- Disabled = 0
- Enabled = 1

Length 4

Type 26

Vendor ID 8164

VSA Type 66

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.

Syntax Enumerated Integer. Supports the following value(s):

- Force = 0
- Detect = 1

Length 4

Type 26

Vendor ID 8164

VSA Type 67

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.

Syntax Enumerated Integer. Supports the following value(s):

- None = 0
- Access-Tunnel = 1
- Data-Tunnel = 2
- Both = 3

Length 4

Type 26

Vendor ID 8164

VSA Type 85

SN1-Subscriber-Nexthop-Address

This attribute specifies the nexthop gateway address to be returned by AAA on a per subscriber basis.

Syntax IPv4 Address

Length 4

Type 26

Vendor ID 8164

VSA Type 127

SN1-Subscriber-No-Interims

This is a GGSN specific attribute. When set to 0 (disabled) interim accounting is generated. When set to 1 (enabled) interim accounting generation is disabled.

Syntax Enumerated Integer. Supports the following value(s):

- Disabled = 0
- Enabled = 1

Length 4

Type 26

Vendor ID 8164

VSA Type 133

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.

Syntax Enumerated Integer. Supports the following value(s):

- 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
- GGSN-PDP-TYPE-PPP = 0x10
- Network-Mobility = 0x20
- FA-HA-NEMO = 0x26
- Pmipv6-interception = 0x40
- HA-Mobile-Pmipv6 = 0x44
- FA-HA-Mobile-Pmipv6 = 0x46
- All = 0x7F

Length 4

Type 26

Vendor ID 8164

VSA Type 20

SN1-Subscriber-Template-Name

RADIUS returned subscriber template.

Type 26

Syntax String

Length 1-127

Vendor ID 8164

VSA Type 158

SN1-Subs-IMSA-Service-Name

IMS Authorization Service name.

Type 26

Syntax String

Length 1-128

Vendor ID 8164

VSA Type 159

SN1-Subs-VJ-Slotid-Cmp-Neg-Mode

Enable/Disable slotid compression in either direction when using VJ compression.

Type 26

Syntax Enumerated Integer. Supports the following value(s):

- None = 0
- Receive = 1
- Transmit = 2
- Both = 3

Length 4

Vendor ID 8164

VSA Type 221

SN1-Tp-Dnlk-Burst-Size

This attribute specifies the Traffic Policing downlink burst size in bytes.

Syntax Unsigned Integer

Length 4

Type 26

Vendor ID 8164

VSA Type 76

SN1-Tp-Dnlk-Committed-Data-Rate

This attribute specifies the Traffic Policing downlink committed data rate in bps.

Syntax Unsigned Integer

Length 4

Type 26

Vendor ID 8164

VSA Type 74

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.

Syntax Enumerated Integer. Supports the following value(s):

- Transmit = 0
- Drop = 1
- Lower-IP-Precedence = 2
- Buffer = 3
- Transmit-On-Buffer-Full = 4

Length 4

Type 26

Vendor ID 8164

VSA Type 77

SN1-Tp-Dnlk-Peak-Data-Rate

This attribute specifies the Traffic Policing downlink peak data rate in bps.

Syntax Unsigned Integer

Length 4

Type 26

Vendor ID 8164

VSA Type 75

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.

Syntax Enumerated Integer. Supports the following value(s):

- Transmit = 0
- Drop = 1
- Lower-IP-Precedence = 2
- Buffer = 3
- Transmit-On-Buffer-Full = 4

Length 4

Type 26

Vendor ID 8164

VSA Type 78

SN1-Tp-Uplk-Burst-Size

This attribute specifies the Traffic Policing uplink burst size in bytes.

Syntax Unsigned Integer

Length 4

Type 26

Vendor ID 8164

VSA Type 82

SN1-Tp-Uplk-Committed-Data-Rate

This attribute specifies the Traffic Policing uplink committed data rate in bps.

Syntax Unsigned Integer

Length 4

Type 26

Vendor ID 8164

VSA Type 80

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.

Syntax Enumerated Integer. Supports the following value(s):

- Transmit = 0
- Drop = 1
- Lower-IP-Precedence = 2
- Buffer = 3
- Transmit-On-Buffer-Full = 4

Length 4

Type 26

Vendor ID 8164

VSA Type 83

SN1-Tp-Uplk-Peak-Data-Rate

This attribute specifies the Traffic Policing uplink peak data rate in bps.

Syntax Unsigned Integer

Length 4

Type 26

Vendor ID 8164

VSA Type 81

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.

Syntax Enumerated Integer. Supports the following value(s):

- Transmit = 0
- Drop = 1
- Lower-IP-Precedence = 2
- Buffer = 3
- Transmit-On-Buffer-Full = 4

Length 4

Type 26

Vendor ID 8164

VSA Type 84

SN1-Traffic-Group

This attribute is used to assign a tag to an FA or a group of FAs, so that traffic policy can be enforced based on the tag value.

Syntax Unsigned Integer

Length 2

Type 26

Vendor ID 8164

VSA Type 161

SN1-Transparent-Data

This attribute is used by RADIUS to provide Global Title information for the GGSN to use in CDRs and Quota Auth.

Syntax Opaque Value

Length 1-247

Type 26

Vendor ID 8164

VSA Type 247

SN1-Tun-Addr-Policy

Describes IP address validation policy for non L2TP tunneled calls.

Syntax Enumerated Integer. Supports the following value(s):

- no-local-alloc-validate = 0
- local-alloc = 1
- local-alloc-validate = 2

Length 4

Type 26

Vendor ID 8164

VSA Type 156

SN1-Tunnel-Gn

Used to enable/disable Gn interface from PDG/TTG to GGSN.

Syntax Enumerated Integer. Supports the following value(s):

- Disabled = 0
- Enabled = 1

Length 4

Type 26

Vendor ID 8164

VSA Type 174

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.

Syntax String

Length 1-128

Type 26

Vendor ID 8164

VSA Type 38

SN1-Tunnel-ISAKMP-Secret

This attribute specifies the secret to use for IKE.

Syntax String

Length 1-128

Type 26

Vendor ID 8164

VSA Type 39

SN1-Tunnel-Load-Balancing

Specifies the load-balancing algorithm to use when tunneling is employed.

Syntax Enumerated Integer. Supports the following value(s):

- random = 1
- balanced = 2
- prioritized = 3

Length 4

Type 26

Vendor ID 8164

VSA Type 27

SN1-Tunnel-Password

This attribute contains a secret for tunneling usage. Currently this is only used for L2TP. It is recommended that if your RADIUS server supports salt-encryption of attributes, that you use the Tunnel-Password attribute instead.

Syntax Opaque Value

Length 1-240

Type 26

Vendor ID 8164

VSA Type 26

SN1-Unclassify-List-Name

SN1-Unclassify-List-Name.

Syntax String

Length 1-32

Type 26

Vendor ID 8164

VSA Type 132

SN1-Virtual-APN-Name

This attribute indicates the virtual APN name.

Syntax Opaque Value

Length 1-64

Type 26

Vendor ID 8164

VSA Type 94

SN1-Visiting-Behavior

This attribute specifies the configuration for the behavior bits settings for a visiting subscriber in an APN.

Syntax Unsigned Integer

Length 4

Type 26

Vendor ID 8164

VSA Type 120

SN1-Visiting-Profile

This attribute specifies the configuration for the profile bits settings for a visiting subscriber in an APN.

Syntax Unsigned Integer

Length 4

Type 26

Vendor ID 8164

VSA Type 117

SN1-Visiting-Sub-Use-GGSN

This attribute configures GGSN to accept GGSN's charging characteristics for visiting subscribers defined for the APN.

Syntax Enumerated Integer. Supports the following value(s):

- Deny = 0
- Accept = 1

Length 4

Type 26

Vendor ID 8164

VSA Type 107

SN1-Voice-Push-List-Name

SN1-Voice-Push-List-Name.

Syntax String

Length 1-32

Type 26

Vendor ID 8164

VSA Type 131

SN1-VPN-ID

This attribute indicates the Destination VPN of the user, specified by a 32-bit identifier.

Syntax Unsigned Integer

Length 4

Type 26

Vendor ID 8164

VSA Type 1

SN1-VPN-Name

This attribute indicates the name of the user's destination VPN.

Syntax String

Length 1-253

Type 26

Vendor ID 8164

VSA Type 2

SN1-VRF-Name

This attribute specifies the IP VRF context to distinguish the RADIUS accounting feeds per enterprise.

Syntax String

Length 1-63

Type 26

Vendor ID 8164

VSA Type 242

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.

Syntax Unsigned Integer

Length 4

Type 26

Vendor ID 8164

VSA Type 202

SNA1-PPP-Unfr-data-In-Oct

This attribute contains the total number of PPP octets without framing sent for the user's session.

Syntax Unsigned Integer

Length 4

Type 26

Vendor ID 8164

VSA Type 200

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.

Syntax Unsigned Integer

Length 4

Type 26

Vendor ID 8164

VSA Type 203

SNA1-PPP-Unfr-data-Out-Oct

This attribute contains the total number of PPP octets without framing received for the user's session.

Syntax Unsigned Integer

Length 4

Type 26

Vendor ID 8164

VSA Type 201

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.

Syntax Enumerated Integer. Supports the following value(s):

- Normal = 0
- DF-Ignore = 1
- DF-Fragment-ICMP-Notify = 2

Length 4

Type 26

Vendor ID 8164

VSA Type 63

SN-Acct-Input-Giga-Dropped

This attribute contains the number of input gigawords dropped if the number of input bytes is greater than 2^32 - 1.

Type 26

Syntax Unsigned Integer

Length 4

Vendor ID 8164

VSA Type 230

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

Syntax Unsigned Integer

Length 4

Vendor ID 8164

VSA Type 228

SN-Acct-Input-Packets-Dropped

This attribute indicates how many PPP packets received have been dropped during the session.

Type 26

Syntax Unsigned Integer

Length 4

Vendor ID 8164

VSA Type 226

SN-Acct-Output-Giga-Dropped

This attribute contains the number of output gigawords dropped if the number of output bytes is greater than 2^32 - 1.

Type 26

Syntax Unsigned Integer

Length 4

Vendor ID 8164

VSA Type 231

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

Syntax Unsigned Integer

Length 4

Vendor ID 8164

VSA Type 229

SN-Acct-Output-Packets-Dropped

This attribute indicates how many output PPP packets have been dropped during the session.

Type 26

Syntax Unsigned Integer

Length 4

Vendor ID 8164

VSA Type 227

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.

Syntax String

Length 1-63

Type 26

Vendor ID 8164

VSA Type 301

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.

Syntax Integer

Length 4

Type 26

Vendor ID 8164

VSA Type 72

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.

Syntax Enumerated Integer. Supports the following value(s):

- 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 NoCons = 16

- CLI-NoCons = 17
- FTP-NoCons = 18
- CLI-FTP-NoCons = 19
- Intercept-NoCons = 20
- CLI-Intercept-NoCons = 21
- CLI-Intercept-FTP-NoCons = 23
- ECS-NoCons = 24
- CLI-ECS-NoCons = 25
- CLI-FTP-ECS-NoCons = 27
- CLI-Intercept-ECS-NoCons = 29
- CLI-Intercept-FTP-ECS-NoCons = 31

Length 4

Type 26

Vendor ID 8164

VSA Type 21

SNA-Input-Gigawords

This attribute contains the total number of input gigawords.

Syntax Unsigned Integer

Length 4

Type 26

Vendor ID 8164

VSA Type 206

SNA-Input-Octets

Syntax Unsigned Integer

Length 4

Type 26

Vendor ID 8164

VSA Type 204

SN-ANID

This attribute contains the Access Network ID.

Syntax Opaque Value

Length 10

Type 26

Vendor ID 5535

VSA Type 178

SNA-Output-Gigawords

This attribute contains the total number of output gigawords.

Syntax Unsigned Integer

Length 4

Type 26

Vendor ID 8164

VSA Type 207

SNA-Output-Octets

Syntax Unsigned Integer

Length 4

Type 26

Vendor ID 8164

VSA Type 205

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.

Syntax Unsigned Integer

Length 4

Type 26

Vendor ID 8164

VSA Type 1011

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.

Syntax Unsigned Integer

Length 4

Type 26

Vendor ID 8164

VSA Type 1012

SNA-PPP-Bad-FCS

This attribute contains the number of frames received, for the user's PPP session, with bad FCS.

Syntax Unsigned Integer

Length 4

Type 26

Vendor ID 8164

VSA Type 1014

SNA-PPP-Ctrl-Input-Octets

This attribute contains the number of PPP Control Octets received for the user's PPP session.

Syntax Unsigned Integer

Length 4

Type 26

Vendor ID 8164

VSA Type 1001

SNA-PPP-Ctrl-Input-Packets

This attribute contains the number of PPP Control packets received for the user's PPP session.

Syntax Unsigned Integer

Length 4

Type 26

Vendor ID 8164

VSA Type 1003

SNA-PPP-Ctrl-Output-Octets

This attribute contains the number of PPP Control Octets sent to the user during the user's PPP session.

Syntax Unsigned Integer

Length 4

Type 26

Vendor ID 8164

VSA Type 1002

SNA-PPP-Ctrl-Output-Packets

This attribute contains the number of PPP Control packets sent to the user during the user's PPP session.

Syntax Unsigned Integer

Length 4

Type 26

Vendor ID 8164

VSA Type 1004

SNA-PPP-Discards-Input

This attribute contains the number of PPP input frames that were discarded during the user's PPP session.

Syntax Unsigned Integer

Length 4

Type 26

Vendor ID 8164

VSA Type 1007

SNA-PPP-Discards-Output

This attribute contains the number of PPP output frames that were discarded during the user's PPP session.

Syntax Unsigned Integer

Length 4

Type 26

Vendor ID 8164

VSA Type 1008

SNA-PPP-Echo-Req-Input

This attribute contains the number of LCP echo packets received, for the user's PPP session.

Syntax Unsigned Integer

Length 4

Type 26

Vendor ID 8164

VSA Type 1015

SNA-PPP-Echo-Req-Output

This attribute contains the number of LCP echo packets sent, for the user's PPP session.

Syntax Unsigned Integer

Length 4

Type 26

Vendor ID 8164

VSA Type 1016

SNA-PPP-Echo-Rsp-Input

This attribute contains the number of LCP echo response packets received, for the user's PPP session.

Syntax Unsigned Integer

Length 4

Type 26

Vendor ID 8164

VSA Type 1017

SNA-PPP-Echo-Rsp-Output

This attribute contains the number of LCP echo response packets sent, for the user's PPP session.

Syntax Unsigned Integer

Length 4

Type 26

Vendor ID 8164

VSA Type 1018

SNA-PPP-Errors-Input

This attribute contains the number of PPP input de-framing errors for the user's PPP session.

Syntax Unsigned Integer

Length 4

Type 26

Vendor ID 8164

VSA Type 1009

SNA-PPP-Errors-Output

This attribute contains the number of PPP output framing errors for the user's PPP session.

Syntax Unsigned Integer

Length 4

Type 26

Vendor ID 8164

VSA Type 1010

SNA-PPP-Framed-Input-Octets

This attribute contains the number of PPP octets received (without framing overhead) for the user's PPP session.

Syntax Unsigned Integer

Length 4

Type 26

Vendor ID 8164

VSA Type 1005

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.

Syntax Unsigned Integer

Length 4

Type 26

Vendor ID 8164

VSA Type 1006

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.

Syntax Unsigned Integer

Length 4

Type 26

Vendor ID 8164

VSA Type 1013

SNA-PPP-Unfr-data-In-Gig

Syntax Unsigned Integer

Length 4

Type 26

Vendor ID 8164

VSA Type 202

SNA-PPP-Unfr-data-In-Oct

This attribute contains the total number of PPP octets without framing sent for the user's session.

Syntax Unsigned Integer

Length 4

Type 26

Vendor ID 8164

VSA Type 200

SNA-PPP-Unfr-data-Out-Gig

Syntax Unsigned Integer

Length 4

Type 26

Vendor ID 8164

VSA Type 203

SNA-PPP-Unfr-data-Out-Oct

This attribute contains the total number of PPP octets without framing received for the user's session.

Syntax Unsigned Integer

Length 4

Type 26

Vendor ID 8164

VSA Type 201

SNA-RPRAK-Rcvd-Acc-Ack

This attribute contains the total number of A11 registration ACK accepted for the user's session.

Syntax Unsigned Integer

Length 4

Type 26

Vendor ID 8164

VSA Type 1028

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.

Syntax Unsigned Integer

Length 4

Type 26

Vendor ID 8164

VSA Type 1030

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.

Syntax Unsigned Integer

Length 4

Type 26

Vendor ID 8164

VSA Type 1029

SNA-RPRAK-Rcvd-Total

This attribute contains the total number of A11 registration ACK received for the user's session.

Syntax Unsigned Integer

Length 4

Type 26

Vendor ID 8164

VSA Type 1027

SNA-RP-Reg-Reply-Sent-Acc-Dereg

This attribute contains the number of Accept A11 registration replies sent for the user's session.

Syntax Unsigned Integer

Length 4

Type 26

Vendor ID 8164

VSA Type 1033

SNA-RP-Reg-Reply-Sent-Acc-Reg

This attribute contains the number of Accept A11 registration replies sent for the user's session.

Syntax Unsigned Integer

Length 4

Type 26

Vendor ID 8164

VSA Type 1032

SNA-RP-Reg-Reply-Sent-Bad-Req

This attribute contains the number of A11 registration replies sent for bad requests for the user's session.

Syntax Unsigned Integer

Length 4

Type 26

Vendor ID 8164

VSA Type 1034

SNA-RP-Reg-Reply-Sent-Denied

This attribute contains the number of denied A11 registration replies sent for the user's session.

Syntax Unsigned Integer

Length 4

Type 26

Vendor ID 8164

VSA Type 1035

SNA-RP-Reg-Reply-Sent-Mis-ID

This attribute contains the number of A11 registration replies sent for mismatched ID for the user's session.

Syntax Unsigned Integer

Length 4

Type 26

Vendor ID 8164

VSA Type 1036

SNA-RP-Reg-Reply-Sent-Send-Err

This attribute contains the number of A11 registration replies sent with send errors for the user's session.

Syntax Unsigned Integer

Length 4

Type 26

Vendor ID 8164

VSA Type 1037

SNA-RP-Reg-Reply-Sent-Total

This attribute contains the total number A11 registration replies sent for the user's session.

Syntax Unsigned Integer

Length 4

Type 26

Vendor ID 8164

VSA Type 1031

SNA-RP-Reg-Upd-Re-Sent

This attribute contains the total number of A11 registration update re-sent for the user's session.

Syntax Unsigned Integer

Length 4

Type 26

Vendor ID 8164

VSA Type 1039

SNA-RP-Reg-Upd-Send-Err

This attribute contains the total number of A11 registration update send errors for the user's session.

Syntax Unsigned Integer

Length 4

Type 26

Vendor ID 8164

VSA Type 1040

SNA-RP-Reg-Upd-Sent

This attribute contains the total number of A11 registration update sent for the user's session.

Syntax Unsigned Integer

Length 4

Type 26

Vendor ID 8164

VSA Type 1038

SNA-RPRRQ-Rcvd-Acc-Dereg

This attribute contains the number of A11 De-registration Requests accepted for the user's session.

Syntax Unsigned Integer

Length 4

Type 26

Vendor ID 8164

VSA Type 1021

SNA-RPRRQ-Rcvd-Acc-Reg

This attribute contains the number of A11 Registration Requests accepted for the user's session.

Syntax Unsigned Integer

Length 4

Type 26

Vendor ID 8164

VSA Type 1020

SNA-RPRRQ-Rcvd-Badly-Formed

This attribute contains the number of badly formed A11 registration requests received for the user's session.

Syntax Unsigned Integer

Length 4

Type 26

Vendor ID 8164

VSA Type 1024

SNA-RPRRQ-Rcvd-Mis-ID

This attribute contains the number of A11 registration requests received with ID-mismatch for the user's session.

Syntax Unsigned Integer

Length 4

Type 26

Vendor ID 8164

VSA Type 1023

SNA-RPRRQ-Rcvd-Msg-Auth-Fail

This attribute contains the number of message authentication failures for A11 registration requests for the user's session.

Syntax Unsigned Integer

Length 4

Type 26

Vendor ID 8164

VSA Type 1022

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.

Syntax Unsigned Integer

Length 4

Type 26

Vendor ID 8164

VSA Type 1026

SNA-RPRRQ-Rcvd-Total

This attribute contains the number of A11 Registration Requests received for the user's session.

Syntax Unsigned Integer

Length 4

Type 26

Vendor ID 8164

VSA Type 1019

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.

Syntax Unsigned Integer

Length 4

Type 26

Vendor ID 8164

VSA Type 1025

SN-Assigned-VLAN-ID

This attribute contains the Assigned VLAN ID.

Syntax Unsigned Integer

Length 4

Type 26

Vendor ID 8164

VSA Type 152

SN-Authorised-Qos

This attribute contains the authorized QoS.

Syntax Authorised-Qos

Type 26

Vendor ID 8164

VSA Type 266

SN-Bandwidth-Policy

This attribute contains the Traffic Policy value.

Syntax String

Length 1-63

Type 26

Vendor ID 8164

VSA Type 300

SN-Call-Id

This attribute contains the Call ID.

Syntax Unsigned Integer

Length 4

Type 26

Vendor ID 8164

VSA Type 251

SN-Cause-Code

This attribute includes the termination cause code value from IMS node.

Syntax Enumerated Integer. Supports the following value(s):

- 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

Length 4

Type 26

Vendor ID 8164

VSA Type 267

SN-Cause-For-Rec-Closing

This attribute contains the GGSN Specific Record Closing Reason Value.

Syntax Unsigned Integer

Length 4

Type 26

Vendor ID 8164

VSA Type 139

SN-CBB-Policy

This attribute contains the CBB policy name.

Syntax String

Length 1-63

Type 26

Vendor ID 8164

VSA Type 302

SN-CF-Call-International

This attribute contains enable/disable config for CF call restriction and dialing permission for international calls.

Syntax Enumerated Integer. Supports the following value(s):

- Disable = 0
- Enable = 1

Length 4

Type 26

Vendor ID 8164

VSA Type 293

SN-CF-Call-Local

This attribute contains enable/disable config for CF call restriction and dialing permission for local calls.

Syntax Enumerated Integer. Supports the following value(s):

- Disable = 0
- Enable = 1

Length 4

Type 26

Vendor ID 8164

VSA Type 291

SN-CF-Call-LongDistance

This attribute contains enable/disable config for CF call restriction and dialing permission for long distance calls.

Syntax Enumerated Integer. Supports the following value(s):

- Disable = 0
- Enable = 1

Length 4

Type 26

Vendor ID 8164

VSA Type 292

SN-CF-Call-Premium

This attribute contains enable/disable config for CF call restriction and dialing permission for premium calls.

Syntax Enumerated Integer. Supports the following value(s):

- Disable = 0
- Enable = 1

Length 4

Type 26

Vendor ID 8164

VSA Type 294

SN-CF-Call-RoamingInternatnl

This attribute contains enable/disable config for CSCF call restriction and dialing permission - Roaming International call.

Syntax Enumerated Integer. Supports the following value(s):

- Disable = 0
- Enable = 1

Length 4

Type 26

Vendor ID 8164

VSA Type 298

SN-CF-Call-Transfer

This attribute contains enable/disable config for CSCF call feature - call transfer.

Syntax Enumerated Integer. Supports the following value(s):

- Disable = 0
- Enable = 1

Length 4

Type 26

Vendor ID 8164

VSA Type 285

SN-CF-Call-Waiting

This attribute contains enable/disable config for CSCF call feature - call waiting.

Syntax Enumerated Integer. Supports the following value(s):

- Disable = 0
- Enable = 1

Length 4

Type 26

Vendor ID 8164

VSA Type 284

SN-CF-Cld-Display-Blocked

This attribute contains enable/disable config for CSCF call feature - caller ID display blocked.

Syntax Enumerated Integer. Supports the following value(s):

- Disable = 0
- Enable = 1

Length 4

Type 26

Vendor ID 8164

VSA Type 283

SN-CF-Cld-Display

This attribute contains enable/disable config for CSCF call feature - caller ID display.

Syntax Enumerated Integer. Supports the following value(s):

- Disable = 0
- Enable = 1

Length 4

Type 26

Vendor ID 8164

VSA Type 282

SN-CF-Follow-Me

This attribute contains URIs for CSCF call feature - follow me.

Syntax String

Length 0-255

Type 26

Vendor ID 8164

VSA Type 281

SN-CF-Forward-Busy-Line

This attribute contains URI for CSCF call feature - forward busy line.

Syntax String

Length 0-255

Type 26

Vendor ID 8164

VSA Type 279

SN-CF-Forward-No-Answer

This attribute contains URI for CSCF call feature - forward no answer.

Syntax String

Length 0-255

Type 26

Vendor ID 8164

VSA Type 278

SN-CF-Forward-Not-Regd

This attribute contains URI for CSCF call feature - forward not registered.

Syntax String

Length 0-255

Type 26

Vendor ID 8164

VSA Type 280

SN-CF-Forward-Unconditional

This attribute contains URI for CSCF call feature - forward unconditional.

Syntax String

Length 0-255

Type 26

Vendor ID 8164

VSA Type 277

SN-CFPolicy-ID

This attribute contains the Content Filtering Policy ID.

Syntax Unsigned Integer

Length 4

Type 26

Vendor ID 8164

VSA Type 220

SN-Change-Condition

The change condition that triggered this record for a GGSN session.

Syntax Enumerated Integer. Supports the following value(s):

- QOSCHANGE = 0
- TARIFFTIMECHANGE = 1
- SGSNCHANGE = 500

Length 4

Type 26

Vendor ID 8164

VSA Type 140

SN-Charging-VPN-Name

The Charging Context Name for GGSN sessions.

Syntax String

Length 1-252

Type 26

Vendor ID 8164

VSA Type 137

SN-Chrg-Char-Selection-Mode

SN-Chrg-Char-Selection-Mode

Syntax Unsigned Integer

Length 4

Type 26

Vendor ID 8164

VSA Type 138

SN-Congestion-Mgmt-Policy

This attribute specifies the Congestion Management Policy.

Syntax String

Length 1-63

Type 26

Vendor ID 8164

VSA Type 315

SN-Content-Disposition

This attribute indicates how the SIP message body or a message body part is to be interpreted.

Syntax String

Length 0-128

Type 26

Vendor ID 8164

VSA Type 272

SN-Content-Length

This attribute contains size of the SIP message body.

Syntax Unsigned Integer

Length 4

Type 26

Vendor ID 8164

VSA Type 271

SN-Content-Type

This attribute contains the media type of the SIP message body.

Syntax String

Length 0-128

Type 26

Vendor ID 8164

VSA Type 270

SN-CR-International-Cid

Carrier ID for routing international calls.

Syntax Unsigned Integer

Length 4

Type 26

Vendor ID 8164

VSA Type 295

SN-CR-LongDistance-Cid

Carrier ID for routing long distance calls.

Syntax Unsigned Integer

Length 4

Type 26

Vendor ID 8164

VSA Type 296

SN-CSCF-App-Server-Info

This is a compound attribute and contains information about application servers.

Type 26

Vendor ID 8164

VSA Type 275

Syntax Compound. Contains the following sub-attribute(s).

App-Server

Holds URL of the application server.

Syntax String

Length 1-128

Type 1

AS-Called-Party-Address

Holds the called party addresses determined by the application server.

Syntax String

Length 1-128

Type 2

SN-CSCF-Rf-SDP-Media-Components

This is a compound attribute for IMS SDP media components.

Type 26

Vendor ID 8164

VSA Type 273

Syntax Compound. Contains the following sub-attribute(s).

Media-Name

Name of the media as available in the SDP data.

Syntax String

Length 0-128

Type 1

Media-Description

Holds the attributes of the media as available in the SDP data.

Syntax SDP-Media-Description

Type 2

Authorised-QoS

Holds the 3GPP Authorised QoS string.

Syntax String

Length 0-128

Type 3

3GPP-Charging-Id

This attribute specifies the 3GPP Charging Identifier.

Syntax String

Length 0-253

Type 4

Access-Network-Charging-Identifier-Value

Holds the access network charging identifier value.

Syntax Opaque Value

Length 1-256

Type 5

SN-Cscf-Subscriber-Ip-Address

This attribute contains the IP address of subscriber, used for early IMS authentication procedures.

Syntax IPv4 Address

Length 4

Type 26

Vendor ID 8164

VSA Type 287

SN-Customer-ID

This attribute contains the internal Customer-ID.

Syntax Opaque Value

Length 1-32

Type 26

Vendor ID 8164

VSA Type 325

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.

Syntax Enumerated Integer. Supports the following value(s):

- Disabled = 0
- Enabled = 1

Length 4

Type 26

Vendor ID 8164

VSA Type 49

SN-DHCP-Lease-Expiry-Policy

This attribute specifies whether to renew or disconnect on expiry of IP address lease time.

Type 26

Syntax Enumerated Integer. Supports the following value(s):

- auto-renew = 0
- disconnect = 1

Length 4

Vendor ID 8164

VSA Type 157

SN-DHCP-Options

Specific information to be sent from the DHCP server to the client.

Syntax Opaque Value

Length 1-245

Type 26

Vendor ID 8164

VSA Type 309

SN-Direction

ROHC protocol control that specifies in which direction to enable Robust Header Compression (ROHC).

Syntax Enumerated Integer. Supports the following value(s):

- Any = 0
- Uplink = 1
- Downlink = 2

Length 4

Type 26

Vendor ID 8164

VSA Type 153

SN-Disconnect-Reason

This attribute indicates the reason the user was disconnected from service.

Syntax Enumerated Integer. Supports the following value(s):

- 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-actv-rejected-due-to-rnc = 274
- sgsn-apn-restrict-vio = 275
- sgsn-actv-rejected-by-sgsn = 276
- sgsn-abnormal-deact = 277
- sgsn-actv-rejected-by-ggsn = 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-pdp-status-mismatch = 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
- sfw-policy-removed-mid-session = 407
- FNG-Auth-failed = 408
- ha-stale-key-disconnect = 409
- No-IPV6-address-for-subscriber = 410
- prefix-registration-failure = 411
- disconnect-from-policy-server = 412
- s6b-auth-failed = 413
- gtpc-err-ind = 414
- gtpu-err-ind = 415
- invalid-pdn-type = 416
- aaa-auth-req-failed = 417
- apn-denied-no-subscription = 418
- Sgw-context-replacement = 419
- dup-static-ip-addr-req = 420
- apn-restrict-violation = 421
- invalid-wapn = 422

- ttg-nsapi-allocation-failed = 423
- mandatory-gtp-ie-missing = 424
- aaa-unreachable = 425
- asngw-service-flow-deletion = 426
- CT-PMIP-RRQ-NVSE-Value-Change = 427
- tcp-read-failed = 428
- tcp-write-failed = 429
- ssl-handshake-failed = 430
- ssl-renegotiate-failed = 431
- ssl-bad-message = 432
- ssl-alert-received = 433
- ssl-disconnect = 434
- ssl-migration = 435
- sgsn-ard-failure = 436
- sgsn-camel-release = 437
- sgsn-egtpc-connection-failed = 438
- sgsn-egtpc-create-sess-failed = 439
- sgsn-hss-detach = 440
- sgsn-hss-connection-failure = 441
- sgsn-pgw-detach = 442
- sgsn-s5-s8-no-support-for-apn = 443
- sgsn-no-rab-for-gbr-bearer = 444
- sgsn-sgw-selection-failure = 445
- sgsn-pgw-selection-failure = 446
- Hotlining-Status-Change = 447
- ggsn-no-rsp-from-sgsn = 448
- diameter-protocol-error = 449
- diameter-request-timeout = 450
- operator-policy = 451
- spr-connection-timeout = 452
- mipha-dup-wimax-session = 453
- invalid-version-attr = 454

- sgsn-zone-code-failure = 455
- invalid-qci = 456
- no_rules = 457
- sgsn-rnc-no-dual-pdp-init-deact = 458
- mme-init-ctxt-setup-failure = 459
- mme-driver-initiated = 460
- mme-s1ap-connection-down = 461
- mme-s1ap-reset-recd = 462
- mme-s6a-response-timeout = 463
- mme-s13-response-timeout = 464
- mme-Illegal-equipment = 465
- mme-unexpected-attach = 466
- mme-sgw-selection-failure = 467
- mme-pgw-selection-failure = 468
- mme-reselection-to-sgsn = 469
- mme-relocation-to-sgsn = 470
- mme-reselection-to-mme = 471
- mme-relocation-to-mme = 472
- mme-tau-attach-collision = 473
- mme-old-sgsn-resolution-failure = 474
- mme-old-mme-resolution-failure = 475
- mme-reloc-ho-notify-timeout = 476
- mme-reloc-ho-req-ack-timeout = 477
- mme-create-session-timeout = 478
- mme-create-session-failure = 479
- mme-s11-path-failure = 480
- mme-policy-no-ue-irat = 481
- mme-x2-handover-failed = 482
- mme-attach-restrict = 483
- mme-reloc-to-non-3GPP = 484
- mme-no-response-from-ue = 485
- mme-sgw-relocation-failed = 486

- mme-implicit-detach = 487
- sgsn-detach-notify = 488
- emergency-inactivity-timeout = 489
- policy-initiated-release = 490
- gy-result-code-system-failure = 491
- mme-zone-code-validation-failed = 492
- sgsn-pgw-init-deact = 493
- s6b-ip-validation-failed = 494
- sgsn-failure-rsp-from-sgw = 495
- tcp-remote-close = 496
- tcp-reset-received = 497
- tcp-socket-error = 498
- ptmsi-signature-mismatch = 499
- camel-invalid-configuration = 500
- 4Gto3G-context-replacement = 501
- mme-isr-sgsn-init-detach = 502
- sgsn-isr-addl-ptmsi-rai = 503
- sgsn-sgw-dbr-cause-isr-deact = 504
- sgsn-isr-mme-init-detach = 505
- mme-sgw-dbr-cause-isr-deact = 506
- sgsn-ptmsi-crunch = 507
- 3Gto4G-context-replacement = 508
- mme-no-eps-bearers-activated = 509
- intra-ggsn-handoff = 510
- WSG-Auth-failed = 511
- Gtp-non-existent-pdp-context = 512
- sgsn-cancel-loc-inital-attach = 513
- Local-fallback-timeout = 514
- sgsn-nrspca-actv-rej-by-sgsn = 515
- sgsn-nrspca-actv-rej-by-ms = 516
- ims-authorization-config-delete = 517
- sgsn-no-ptmsi-signature = 518

- pgw-sel-dns-server-nt-reachable = 519
- pgw-sel-dns-no-resource-records = 520
- pgw-sel-dns-no-service-params = 521
- ePDG-Auth-failed = 522
- ePDG-pgw-sel-failure-initial = 523
- ePDG-pgw-sel-failure-handoff = 524
- sgsn-ho-sgw-reloc-collision = 525
- ePDG-dbr-from-pgw = 526
- ePDG-gtpc-abort-session = 527
- ePDG-gtpu-abort-session = 528
- ePDG-gtpu-error-ind = 529
- ePDG-pgw-not-reachable = 530
- ePDG-reject-from-pgw = 531
- ipsg-session-replacement = 532
- ePDG-rel-due-to-handoff = 533
- mme-foreign-plmn-guti-rejected = 534
- sgsn-dsd-allepswithdrawn = 535
- NAT-Pool-BusyOut-Or-Pend-Delete = 536
- Invalid-APN = 537
- srvcc-ps-to-cs-handover = 538
- henbgw-mme-s1ap-reset-recd = 539
- henbgw-henb-s1ap-reset-recd = 540
- henbgw-ue_sess-mme-conn-down = 541
- henbgw-ue-sess-henb-conn-down = 542
- henbgw-handoff-complete = 543
- henbgw-handover-failed = 544
- henbgw-mme-error-indication = 545
- henbgw-henb-error-indication = 546
- henbgw-henb-initiated-release = 547
- henbgw-mme-initiated-release = 548
- henbgw-duplicate-session = 549
- Transport-mismatch-with-PGW = 550

- icsr-ipsec-chkpt-failed = 551
- sgsn-dbr-cause-isr-deact-detach = 552
- unexpected-scenario = 553
- icsr-delete-standby = 554
- epdg-local-pgw-res-failed = 555
- sgsn-iovui-negotiation-failure = 556
- henbgw-gw2henb-inv-mmeues1apid = 557
- henbgw-gw2mme-inv-mmeues1apid = 558
- henbgw-henb-sess-henb-conn-down = 559
- henbgw-nw-path-unavailable = 560
- pgw-transaction-timeout = 561
- samog-multi-dev-pgw-sel-failure = 562
- samog-multi-dev-demux-failure = 563
- mme-pgw-restarted = 564
- samog-session-replacement = 565
- authorization-failed = 566
- mm-apn-congestion-control = 567
- samog-pgw-init-detach = 568
- samog-ggsn-init-detach = 569
- samog-pgw-rejected = 570
- samog-ggsn-rejected = 571
- samog-pgw-no-response = 572
- samog-ggsn-no-response = 573
- samog-gtpc-path-failure = 574
- samog-gtpu-path-failure = 575
- samog-gtpu-err-ind = 576
- samog-mandatory-ie-missing = 577
- samog-mandatory-ie-incorrect = 578
- samog-ip-alloc-failed = 579
- samog-default-gw-not-found = 580
- samog-dns-unreachable = 581
- samog-dns-no-resource-records = 582

- samog-dns-no-service-params = 583
- samog-internal-error = 584
- handoff-pcf-restriction = 585
- graceful-cleanup-on-audit-fail = 586
- ue-ctxt-normal-del-ntsr-ddn = 587
- session-auto-delete = 588
- mme-qos-pgw-upgrade-reject = 589
- path-failure-s5 = 590
- path-failure-s11 = 591
- path-failure-s4 = 592
- gtpu-path-failure-s5u = 593
- gtpu-path-failure-s1u = 594
- gtpu-path-failure-s4u = 595
- gtpu-path-failure-s12u = 596
- gtpu-err-ind-s5u = 597
- gtpu-err-ind-s1u = 598
- gtpu-err-ind-s4u = 599
- gtpu-err-ind-s12u = 600
- diameter-network-too-busy = 601
- diameter-network-failure = 602
- diameter-roaming-not-allowed = 603
- diameter-rat-disallowed = 604
- diameter-no-subscription = 605
- pcc-data-mismatch = 606
- mme-embms-call_setup-timeout = 607
- mme-embms-normal-disconnect = 608
- mme-embms-sctp-down = 609
- disconnect-from-charging-server = 610
- disconnect-irat-fail-hi-missing = 611
- apn-not-supported-in-plmn-rat = 612
- ue-pcscf-reselect-not-supported = 613
- newer-session-detected = 614

- mme-guti_realloc_failed-detach = 615
- mme-pcscf-rest-detach = 616
- Reject-ho-old-tun-path-failure = 617
- gx-vapn-selection-failed = 618
- dup-static-ipv6-addr-req = 619
- mip-path-failure = 620
- apn-congestion = 621
- ue-redirected = 622
- ePDG-s2b-access-denied = 623
- ePDG-s2b-network-failure = 624
- ePDG-s2b-msg-failure = 625
- ePDG-s2b-rat-disallowed = 626
- ePDG-roaming-mandatory = 627
- gtpv2-peer-context-not-found = 628
- SaMOG-access-switch-timeout = 629
- decrypt-fail-count-exceeded = 630
- emergency-idle-timeout = 631
- gtpu-path-failure-s11u = 632
- gtpu-err-ind-s11u = 633
- mme-gtpu-path-failure-s11u = 634
- mme-gtpu-err-ind-s11u = 635
- ePDG-pcscf-restoration = 636
- samog-lbo-user-logout = 637
- sx-req-rej = 638
- sx-cntxt-not-found = 639
- sx-mand-ie-missing = 640
- sx-cond-ie-missing = 641
- sx-msg-invalid-length = 642
- sx-mand-ie-incorrect = 643
- sx-invld-fwd-policy = 644
- sx-invld-fteid-alloc-opt = 645
- sx-no-establshd-sx-association = 646

- sx-no-response = 647
- sx-no-resource = 648
- sx-fteid-ipaddr-type-mismatch = 649
- sx-invalid-response = 650
- user-plane-info-not-available = 651
- user-plane-info-mismatch = 652
- ikev2-req-rate-exceeded = 653
- mme-decor-call-rerouted = 654
- mme-decor-call-rejected = 655
- origin-state-id-change = 656
- mme-ducon-path-update-failed = 657
- diam-no-non-3gpp-subscription = 658
- diameter-user-unknown = 659
- diameter-illegal-equipment = 660
- epdg-invalid-imei = 661
- sx-path-failure = 662
- sxfail-opr-revert-info = 663
- sxfail-opr-get-usagereport = 664
- sxfail-opr-create-rulebase-pdr = 665
- sxfail-opr-remove-pdr = 666
- gtp-remote-data-teid-invalid = 667
- smp-fp-tep-oper-failure = 668
- smp-fp-ambr-oper-failure = 669
- smp-fp-brr-stream-oper-failure = 670
- smp-fp-brr-strm-chrgng-op-fail = 671
- smp-fp-itc-bw-oper-failure = 672
- smp-fp-strm-chrg-oper-failure = 673
- vpp-next-hop-failure = 674
- graceful-cleanup-up-audit-fail = 675
- sx-max-trans-threshold-reached = 676
- sx-db-ub-collision = 677
- sx-failure-ntsr = 678

- graceful-term-up-self-protectn = 679

Length 4

Type 26

Vendor ID 8164

VSA Type 3

SN-DNS-Proxy-Intercept-List

This attribute is used to specify the list name which contains the rules to intercept and redirect DNS requires received from mobile. This attribute can be configured using either local subscriber template or returned from Access-Accept.

Syntax String

Length 1-253

Type 26

Vendor ID 8164

VSA Type 214

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.

Syntax Enumerated Integer. Supports the following value(s):

- Disable = 0
- Enable = 1

Length 4

Type 26

Vendor ID 8164

VSA Type 25

SN-Dynamic-Addr-Alloc-Ind-Flag

This attribute indicates whether the IP address is allocated statically or dynamically from SGW perspective.

Syntax Opaque Value

Length 1

Type 26

Vendor ID 8164

VSA Type 141

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

Syntax Compound. Contains the following sub-attribute(s).

Rating-Group-Id

Rating Group Id in a PDP context.

Syntax Unsigned Integer

Length 4

Type 1

GPRS-Uplink

Uplink octet usage for a PDP context per rating group.

Syntax Unsigned Integer

Length 4

Type 2

GPRS-Downlink

Downlink octet usage for a PDP context per rating group.

Syntax Unsigned Integer

Length 4

Type 3

SN-Enable-QoS-Renegotiation

This attribute configures the enabling of dynamic QoS renegotiation.

Syntax Enumerated Integer. Supports the following value(s):

- No = 0
- Yes = 1

Length 4

Type 26

Vendor ID 8164

VSA Type 144

SN-Event

This attribute contains the type of SIP event for which the accounting-request message is generated.

Syntax String

Length 0-64

Type 26

Vendor ID 8164

VSA Type 255

SN-Ext-Inline-Srvr-Context

This attribute configures the context name in which the External In-line server resides.

Syntax String

Length 1-247

Type 26

Vendor ID 8164

VSA Type 41

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.

Syntax IPv4 Address

Length 4

Type 26

Vendor ID 8164

VSA Type 56

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.

Syntax Unsigned Integer

Length 4

Type 26

Vendor ID 8164

VSA Type 59

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.

Syntax Unsigned Integer

Length 4

Type 26

Vendor ID 8164

VSA Type 57

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

Syntax IPv4 Address

Length 4

Type 26

Vendor ID 8164

VSA Type 55

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.

Syntax Unsigned Integer

Length 4

Type 26

Vendor ID 8164

VSA Type 58

SN-Fast-Reauth-Username

Fast re-authentication user name.

Syntax Opaque Value

Length 1-128

Type 26

Vendor ID 8164

VSA Type 304

SN-Firewall-Enabled

Firewall for subscriber enabled.

Syntax Enumerated Integer. Supports the following value(s):

- False = 0
- True = 1

Length 4

Type 26

Vendor ID 8164

VSA Type 198

SN-Firewall-Policy

This attribute contains the firewall policy name.

Syntax String

Length 1-63

Type 26

Vendor ID 8164

VSA Type 239

SN-FMC-Location

This attribute contains the MAC address and CDMA location information.

Syntax String

Length 1-247

Type 26

Vendor ID 8164

VSA Type 171

SN-GGSN-Address

The control plane IP address of the GGSN that handles one or more media component(s) of an IMS session.

Syntax IPv4 Address

Length 4

Type 26

Vendor ID 8164

VSA Type 264

SN-GGSN-MIP-Required

This attribute specifies if MIP is required for the GGSN subscriber.

Syntax Enumerated Integer. Supports the following value(s):

- Disabled = 0
- Enabled = 1

Length 4

Type 26

Vendor ID 8164

VSA Type 68

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.

Syntax Enumerated Integer. Supports the following value(s):

- Disabled = 0
- Enabled = 1

Length 4

Type 26

Vendor ID 8164

VSA Type 54

SN-GTP-Version

This attribute indicates the version of GTP the subscriber is using.

Syntax Enumerated Integer. Supports the following value(s):

- GTP_VERSION_0 = 0
- GTP_VERSION_1 = 1
- GTP_VERSION_2 = 2

Length 4

Type 26

Vendor ID 8164

VSA Type 62

SN-Handoff-Indicator

This attribute indicates whether the Accounting Interim is sent because of the interim or not.

Syntax Enumerated Integer. Supports the following value(s):

- Active-Handoff = 0
- Location-Update = 1

Length 1

Type 26

Vendor ID 8164

VSA Type 310

SN-HA-Send-DNS-Address

Syntax Enumerated Integer. Supports the following value(s):

- Disabled = 0
- Enabled = 1

Length 4

Type 26

Vendor ID 8164

VSA Type 47

SN-Home-Behavior

This attribute specifies the configuration for the behavior bits settings for a home subscriber in an APN.

Syntax Unsigned Integer

Length 4

Type 26

Vendor ID 8164

VSA Type 119

SN-Home-Profile

This attribute specifies the configuration for the profile bits settings for a home subscriber in an APN.

Syntax Unsigned Integer

Length 4

Type 26

Vendor ID 8164

VSA Type 109

SN-Home-Sub-Use-GGSN

This attribute configures GGSN to accept GGSN's charging characteristics for home subscribers defined for the APN.

Syntax Enumerated Integer. Supports the following value(s):

- Deny = 0
- Accept = 1

Length 4

Type 26

Vendor ID 8164

VSA Type 106

SN-Ignore-Unknown-HA-Addr-Error

Type 26

Syntax Unsigned Integer

Length 1

Vendor ID 8164

VSA Type 160

SN-IMS-AM-Address

IMS application manager address.

Syntax IPv4 Address

Length 4

Type 26

Vendor ID 8164

VSA Type 167

SN-IMS-AM-Domain-Name

IMS application manager domain name.

Syntax String

Length 1-64

Type 26

Vendor ID 8164

VSA Type 168

SN-IMS-Charging-Identifier

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

Syntax String

Length 0-253

Type 26

Vendor ID 8164

VSA Type 260

SN-IMSI

SN-IMSI

Syntax Opaque Value

Length 1-8

Type 26

Vendor ID 8164

VSA Type 252

SN-Inactivity-Time

This attribute contains the inactivity time duration for a subscriber session under long time duration timer configuration.

Syntax Integer

Length 4

Type 26

Vendor ID 8164

VSA Type 232

SN-Internal-SM-Index

SN-Internal-SM-Index

Syntax Unsigned Integer

Length 4

Type 26

Vendor ID 8164

VSA Type 122

SN-IP-Alloc-Method

This attribute specifies the method for allocating an IP address. This feature only applies to the GGSN service.

Syntax Enumerated Integer. Supports the following value(s):

- Alloc_Local_Pool = 0
- Alloc_Dhcp_Client = 1
- Alloc_Radius = 2
- Alloc_No_Alloc = 3
- Alloc_Static_Alloc = 4
- Alloc_Dhcp_Relay = 5

Length 4

Type 26

Vendor ID 8164

VSA Type 53

SN-IP-Filter-In

This attribute specifies the IP input filter rules to determine whether the traffic should undergo DPI processing.

Syntax String

Length 1-253

Type 26

Vendor ID 8164

VSA Type 10

SN-IP-Filter-Out

This attribute specifies the IP output filter rules to determine whether the traffic should undergo DPI processing.

Syntax String

Length 1-253

Type 26

Vendor ID 8164

VSA Type 11

SN-IP-Header-Compression

Specifies the IP header compression method to use.

Syntax Enumerated Integer. Supports the following value(s):

- None = 0
- VJ = 1
- ROHC = 2
- VJ_ROHC = 3

Length 4

Type 26

Vendor ID 8164

VSA Type 150

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.

Syntax Enumerated Integer. Supports the following value(s):

- No = 0
- Yes = 1

Length 4

Type 26

Vendor ID 8164

VSA Type 60

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.

Syntax String

Length 1-253

Type 26

Vendor ID 8164

VSA Type 17

SN-IP-In-Plcy-Grp

This attribute specifies the name of the policy group configuration applied in the uplink direction.

Syntax String

Length 1-15

Type 26

Vendor ID 8164

VSA Type 193

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.

Syntax String

Length 1-253

Type 26

Vendor ID 8164

VSA Type 18

SN-IP-Out-Plcy-Grp

This attribute specifies the name of the policy group configuration applied in the downlink direction.

Syntax String

Length 1-15

Type 26

Vendor ID 8164

VSA Type 194

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.

Syntax String

Length 1-253

Type 26

Vendor ID 8164

VSA Type 8

SN-IP-Source-Validation

This attribute indicates if the source IP address should be validated before forwarding the IP packet.

Syntax Enumerated Integer. Supports the following value(s):

- No = 0

- Yes = 1

Length 4

Type 26

Vendor ID 8164

VSA Type 14

SN-IP-Source-Violate-No-Acct

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

Syntax Enumerated Integer. Supports the following value(s):

- Disabled = 0
- Enabled = 1

Length 4

Type 26

Vendor ID 8164

VSA Type 196

SN-IP-Src-Validation-Drop-Limit

Maximum number of packet drops entertained before disconnecting the session for source violated packets for the session.

Syntax Unsigned Integer

Length 4

Type 26

Vendor ID 8164

VSA Type 110

SN-IPv6-Alloc-Method

This attribute specifies the method for allocating an IPv6 address. This feature only applies to the GGSN service.

Syntax Enumerated Integer. Supports the following value(s):

- Alloc_Local_Pool = 0
- Alloc_Dhcp_Client = 1
- Alloc_No_Alloc = 2
- Alloc_Static_Alloc = 3

Length 1

Type 26

Vendor ID 8164

VSA Type 314

SN-IPv6-DNS-Proxy

IPV6 DNS proxy enabled or disabled setting for the session.

Syntax Enumerated Integer. Supports the following value(s):

- Disabled = 0
- Enabled = 1

Length 4

Type 26

Vendor ID 8164

VSA Type 126

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.

Syntax Enumerated Integer. Supports the following value(s):

- Disabled = 0
- Enabled = 1

Length 4

Type 26

Vendor ID 8164

VSA Type 103

SN-IPv6-Min-Link-MTU

IPV6 MTU size.

Syntax Unsigned Integer

Length 4

Type 26

Vendor ID 8164

VSA Type 136

SN-IPv6-num-rtr-advt

This attribute indicates the IPv6 number of Initial Router Advertisements. The default value is 3.

Syntax Unsigned Integer

Length 4

Type 26

Vendor ID 8164

VSA Type 97

SN-IPv6-Primary-DNS

This attribute specifies a Primary DNS server address that the Router Advertisement message sent by the PDSN will include.

Syntax Opaque Value

Length 16

Type 26

Vendor ID 8164

VSA Type 101

SN-IPv6-rtr-advt-interval

This attribute indicates the IPv6 Initial Router Advertisement Interval specified in milliseconds. The default value is 3000.

Syntax Unsigned Integer

Length 4

Type 26

Vendor ID 8164

VSA Type 96

SN-IPv6-Secondary-DNS

This attribute specifies a Secondary DNS server address that the Router Advertisement message sent by the PDSN will include.

Syntax Opaque Value

Length 16

Type 26

Vendor ID 8164

VSA Type 102

SN-IPv6-Sec-Pool

IPv6 secondary pool names.

Syntax String

Length 1-253

Type 26

Vendor ID 8164

VSA Type 124

SN-IPv6-Sec-Prefix

IPv6 secondary pool name prefix.

Syntax Opaque Value

Length 2-18

Type 26

Vendor ID 8164

VSA Type 125

SN-ISC-Template-Name

This attribute contains name of the CSCF ISC template to be used for a subscriber.

Syntax String

Length 0-255

Type 26

Vendor ID 8164

VSA Type 276

SN-Is-Unregistered-Subscriber

This attribute specifies if a subscriber is registered or not.

Syntax String

Length 0-256

Type 26

Vendor ID 8164

VSA Type 269

SN-L3-to-L2-Tun-Addr-Policy

This attribute specifies the address allocation policy.

Syntax Enumerated Integer. Supports the following value(s):

- no-local-alloc-validate = 0
- local-alloc = 1
- local-alloc-validate = 2

Length 4

Type 26

Vendor ID 8164

VSA Type 43

SN-LBO-Acct-IN-Octets

This attribute indicates the number of Local Breakout accounting input octets sent by UE directly to the internet. This attribute is sent in the Acct-Interim/Acct-Stop message to AAA server.

Syntax Unsigned Integer

Length 4

Type 26

Vendor ID 8164

VSA Type 323

SN-LBO-Acct-IN-Pkts

This attribute indicates the number of Local Breakout accounting input packets sent by UE directly to the internet. This attribute is sent in the Acct-Interim/Acct-Stop message to AAA server.

Syntax Unsigned Integer

Length 4

Type 26

Vendor ID 8164

VSA Type 321

SN-LBO-Acct-Out-Octets

This attribute indicates the number of Local Breakout accounting output octets received by UE directly from the internet. This attribute is sent in the Acct-Interim/Acct-Stop message to AAA server..

Syntax Unsigned Integer

Length 4

Type 26

Vendor ID 8164

VSA Type 324

SN-LBO-Acct-Out-Pkts

This attribute indicates the number of Local Breakout accounting output packets received by UE directly from the internet. This attribute is sent in the Acct-Interim/Acct-Stop message to AAA server.

Syntax Unsigned Integer

Length 4

Type 26

Vendor ID 8164

VSA Type 322

SN-Local-IP-Address

This attribute indicates the IP address of the local interface on the chassis for the user's session.

Syntax IPv4 Address

Length 4

Type 26

Vendor ID 8164

VSA Type 13

SN-Long-Duration-Action

This attribute specifies the action to take place when the long duration timeout expires for a subscriber session.

Syntax Enumerated Integer. Supports the following value(s):

- Detection = 1
- Disconnection = 2
- Dormant-Only-Disconnection = 3
- Dormant-Only-Detection = 4

Length 4

Type 26

Vendor ID 8164

VSA Type 45

SN-Long-Duration-Notification

SN-Long-Duration-Notification.

Syntax Enumerated Integer. Supports the following value(s):

- Suppress = 0

- Send = 1

Length 4

Type 26

Vendor ID 8164

VSA Type 253

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.

Syntax Integer

Length 4

Type 26

Vendor ID 8164

VSA Type 44

SN-Max-Sec-Contexts-Per-Subs

Maximum secondary PDP contexts per subscriber.

Syntax Unsigned Integer

Length 2

Type 26

Vendor ID 8164

VSA Type 290

SN-Mediation-Acct-Rsp-Action

When this attribute is set to None, there is no action taken while waiting for a response for the accounting start message from the Mediation Accounting server. When this attribute is set to No-Early-PDUs the system buffers all packets from the user (uplink) until a response for the accounting start message is received from the Mediation Accounting server. When set to Delay_GTP_Response, the system does not send a GTP create PDP response to the GGSN until a response for the accounting start message is received from the Mediation Accounting server. If the attribute is not present in Access-Accept message or if the attribute value is invalid, the value "None" is assumed.

Syntax Enumerated Integer. Supports the following value(s):

- None = 0
- No_Early_PDUs = 1
- Delay_GTP_Response = 2

Length 4

Type 26

Vendor ID 8164

VSA Type 105

SN-Mediation-Enabled

This attribute indicates whether the Mediation Accounting configuration is enabled or disabled for GGSN.

Syntax Enumerated Integer. Supports the following value(s):

- Disabled = 0
- Enabled = 1

Length 4

Type 26

Vendor ID 8164

VSA Type 123

SN-Mediation-No-Interims

This attribute is used to disable or enable Mediation Interim Accounting Records for the session.

Syntax Enumerated Integer. Supports the following value(s):

- Disabled = 0
- Enabled = 1

Length 4

Type 26

Vendor ID 8164

VSA Type 146

SN-Mediation-VPN-Name

This attribute specifies the Mediation Context name for the session.

Syntax String

Length 1-128

Type 26

Vendor ID 8164

VSA Type 104

SN-Min-Compress-Size

This attribute specifies the minimum size (in octets) a data packet can have in order to be compressed.

Syntax Unsigned Integer

Length 4

Type 26

Vendor ID 8164

VSA Type 23

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.

Syntax Enumerated Integer. Supports the following value(s):

- Disabled = 0
- Enabled = 1

Length 4

Type 26

Vendor ID 8164

VSA Type 50

SN-MIP-ANCID

Accounting correlation ID created by IPGW, received by VBM and HBM.

Syntax Opaque Value

Length 12

Type 26

Vendor ID 8164

VSA Type 166

SN-MIP-Dual-Anchor

Enable/disable dual-anchor service for a subscriber.

Syntax Enumerated Integer. Supports the following value(s):

- Disabled = 0
- Enabled = 1

Length 4

Type 26

Vendor ID 8164

VSA Type 165

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.

Syntax String

Length 1-253

Type 26

Vendor ID 8164

VSA Type 154

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.

Syntax Enumerated Integer. Supports the following value(s):

- Disabled = 0
- Enabled = 1

Length 4

Type 26

Vendor ID 8164

VSA Type 51

SN-MIP-MIN-Reg-Lifetime-Realm

This attribute configures the minimum MIP registration lifetime for a subscriber/realm.

Syntax Unsigned Integer

Length 4

Type 26

Vendor ID 8164

VSA Type 12

SN-MIP-Reg-Lifetime-Realm

This attribute configures the maximum MIP registration lifetime for a subscriber/realm.

Syntax Unsigned Integer

Length 4

Type 26

Vendor ID 8164

VSA Type 175

SN-MIP-Send-Ancid

This attribute enables/disables sending ANCID from FA to HA in MIP RRQ.

Syntax Enumerated Integer. Supports the following value(s):

- Disabled = 0
- Enabled = 1

Length 4

Type 26

Vendor ID 8164

VSA Type 163

SN-MIP-Send-Correlation-Info

This attribute enables/disables sending of correlation-id from FA to HA in MIP RRQ.

Syntax Enumerated Integer. Supports the following value(s):

- Disabled = 0
- NVSE_Starent = 1
- NVSE_CUstom1 = 2
- NVSE_Custom2 = 3

Length 4

Type 26

Vendor ID 8164

VSA Type 188

SN-MIP-Send-Host-Config

This attribute is used to enable/disable Host Config Extension in MIP RRQ.

Type 26

Syntax Enumerated Integer. Supports the following value(s):

- Disabled = 0

- Enabled = 1

Length 1

Vendor ID 8164

VSA Type 311

SN-MIP-Send-Imsi

AAA attribute to enable/disable sending IMSI from FA to HA in MIP RRQ.

Syntax Enumerated Integer. Supports the following value(s):

- Disabled = 0
- NVSE_Starent = 1
- NVSE_Custom1 = 2
- NVSE_Custom2 = 3

Length 4

Type 26

Vendor ID 8164

VSA Type 164

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.

Syntax Enumerated Integer. Supports the following value(s):

- Disabled = 0
- NVSE_Custom1 = 1
- NVSE_Custom2 = 2
- NVSE_Starent = 3

Length 4

Type 26

Vendor ID 8164

VSA Type 48

SN-MN-HA-Hash-Algorithm

This attribute contains the hash algorithm to use for MN-HA authentication.

Syntax Enumerated Integer. Supports the following value(s):

- MD5 = 1
- MD5-RFC2002 = 2
- HMAC-MD5 = 3

Length 4

Type 26

Vendor ID 8164

VSA Type 99

SN-MN-HA-Timestamp-Tolerance

This attribute indicates the duration of timestamp tolerance, in seconds, to use for MN-HA authentication.

Syntax Unsigned Integer

Length 4

Type 26

Vendor ID 8164

VSA Type 30

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.

Syntax Enumerated Integer. Supports the following value(s):

- Reliable = 0
- Optimistic = 1
- Unidirectional = 2

Length 4

Type 26

Vendor ID 8164

VSA Type 151

SN-MS-ISDN

SN-MS-ISDN.

Syntax Opaque Value

Length 1-9

Type 26

Vendor ID 8164

VSA Type 248

SN-NAI-Construction-Domain

This attribute specifies the domain name to use when constructing the NAI.

Syntax String

Length 1-247

Type 26

Vendor ID 8164

VSA Type 37

SN-NAT-IP-Address

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

Syntax IPv4 Address

Length 4

Type 26

Vendor ID 8164

VSA Type 297

SN-Node-Functionality

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

Syntax Enumerated Integer. Supports the following value(s):

- S-CSCF = 0
- P-CSCF = 1
- I-CSCF = 2

Length 4

Type 26

Vendor ID 8164

VSA Type 268

SN-NPU-Qos-Priority

This attribute configures inter-subscriber priority queueing based on class of service offered. Gold has the highest priority and Best_effort the lowest priority. From_DSCP means the priority queueing will be done based on the DSCP marking that the incoming subscriber packet carries.

Syntax Enumerated Integer. Supports the following value(s):

- Best_Effort = 0
- Bronze = 1
- Silver = 2
- Gold = 3
- From_DSCP = 4

Length 4

Type 26

Vendor ID 8164

VSA Type 98

SN-Ntk-Initiated-Ctx-Ind-Flag

Indicates whether the GGSN call is a network initiated PDP Context.

Syntax Opaque Value

Length 1

Type 26

Vendor ID 8164

VSA Type 142

SN-Ntk-Session-Disconnect-Flag

SN-Ntk-Session-Disconnect-Flag.

Syntax Enumerated Integer. Supports the following value(s):

- Session-Disconnect = 1

Length 4

Type 26

Vendor ID 8164

VSA Type 143

SN-Nw-Reachability-Server-Name

This attribute specifies the name of the Network Reachability Detection Server.

Syntax String

Length 1-16

Type 26

Vendor ID 8164

VSA Type 65

SN-Originating-IOI

This attribute holds the Inter Operator Identifier for the originating network in the home network of the originating end user.

Syntax String

Length 1-253

Type 26

Vendor ID 8164

VSA Type 261

SN-Overload-Disc-Connect-Time

This attribute provides inactivity time for session to become candidate for disconnection during overload.

Syntax Uint32

Type 26

Vendor ID 8164

VSA Type 233

SN-Overload-Disc-Inact-Time

This attribute provides inactivity time for session to become candidate for disconnection during overload.

Syntax Uint32

Type 26

Vendor ID 8164

VSA Type 234

SN-Overload-Disconnect

This attribute enables (if one) and disables the overload-disconnect feature for a subscriber.

Syntax Uint32

Type 26

Vendor ID 8164

VSA Type 235

SN-PDG-TTG-Required

TTG mode of operation Required for PDG.

Syntax Enumerated Integer. Supports the following value(s):

- No = 0
- Yes = 1

Length 1

Type 26

Vendor ID 8164

VSA Type 299

SN-PDIF-MIP-Release-TIA

PDIF mobile IP release TIA.

Syntax Enumerated Integer. Supports the following value(s):

- No = 0
- Yes = 1

Length 4

Type 26

Vendor ID 8164

VSA Type 172

SN-PDIF-MIP-Required

PDIF mobile IP required.

Syntax Enumerated Integer. Supports the following value(s):

- No = 0
- Yes = 1

Length 4

Type 26

Vendor ID 8164

VSA Type 170

SN-PDIF-MIP-Simple-IP-Fallback

PDIF mobile IP simple IP fallback.

Syntax Enumerated Integer. Supports the following value(s):

- No = 0
- Yes = 1

Length 4

Type 26

Vendor ID 8164

VSA Type 173

SN-PDSN-Correlation-Id

Correlation ID received from PDSN to HA.

Syntax Opaque Value

Length 8

Type 26

Vendor ID 8164

VSA Type 189

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.

Syntax Enumerated Integer. Supports the following value(s):

- Disabled = 0
- Enabled = 1

Length 4

Type 26

Vendor ID 8164

VSA Type 46

SN-PDSN-NAS-Id

NAS Identifier received from PDSN to HA

Syntax String

Length 1-253

Type 26

Vendor ID 8164

VSA Type 190

SN-PDSN-NAS-IP-Address

NAS IP address received from PDSN to HA.

Syntax IPv4 Address

Length 4

Type 26

Vendor ID 8164

VSA Type 191

SN-Permit-User-Mcast-PDUs

Specifies whether or not to let the subscriber discard multicast PDUs.

Syntax Enumerated Integer. Supports the following value(s):

- disabled = 0
- enabled = 1

Length 4

Type 26

Vendor ID 8164

VSA Type 134

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.

Syntax Enumerated Integer. Supports the following value(s):

- Disabled = 0
- Enabled = 1

Length 4

Type 26

Vendor ID 8164

VSA Type 95

SN-PPP-Always-On-Vse

SN-PPP-Always-On-Vse.

Syntax Enumerated Integer. Supports the following value(s):

- Disabled = 0
- Enabled = 1

Length 4

Type 26

Vendor ID 8164

VSA Type 130

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.

Syntax Enumerated Integer. Supports the following value(s):

- Normal = 0
- Stateless = 1

Length 4

Type 26

Vendor ID 8164

VSA Type 19

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.

Syntax Enumerated Integer. Supports the following value(s):

- None = 0
- Stac-LZS = 1
- MPPC = 2
- Deflate = 4

Length 4

Type 26

Vendor ID 8164

VSA Type 9

SN-PPP-Keepalive

This attribute indicates the interval for the PPP keepalive, in seconds.

Syntax Unsigned Integer

Length 4

Type 26

Vendor ID 8164

VSA Type 16

SN-PPP-NW-Layer-IPv4

This attribute indicates the PPP IPCP negotiation for IPv4. The default is enabled.

Syntax Enumerated Integer. Supports the following value(s):

- Disabled = 0
- Enabled = 1
- Passive = 2

Length 4

Type 26

Vendor ID 8164

VSA Type 92

SN-PPP-NW-Layer-IPv6

This attribute indicates the PPP IPv6CP negotiation for IPv6. The default is enabled.

Syntax Enumerated Integer. Supports the following value(s):

- Disabled = 0
- Enabled = 1
- Passive = 2

Length 4

Type 26

Vendor ID 8164

VSA Type 93

SN-PPP-Outbound-Password

This attribute indicates the password to be used when the user side of the PPP connection requires authentication.

Syntax String

Length 1-253

Type 26

Vendor ID 8164

VSA Type 15

SN-PPP-Outbound-Username

This attribute indicates the username to be used when the user side of the PPP connection requires authentication.

Syntax String

Length 1-253

Type 26

Vendor ID 8164

VSA Type 61

SN-PPP-Progress-Code

This attribute provides information about the "state" of the PPP connection, when the connection was terminated.

Syntax Enumerated Integer. Supports the following value(s):

- Not-Defined = 0
- Call-Lcp-Down = 10
- Call-Disconnecting = 20
- Call-Ppp-Renegotiating = 30
- Call-Arrived = 40
- Call-Pdg-Tcp-Connecting = 45
- Call-Pdg-Ssl-Connecting = 46
- Call-Lcp-Up = 50
- Call-Authenticating = 60
- Call-Bcmcs-Authenticating = 70
- Call-Authenticated = 80
- Call-Tunnel-Connecting = 85
- Call-Ipcp-Up = 90
- Call-Imsa-Authorizing = 95
- Call-Imsa-Authorized = 97
- Call-MBMS-UE-Authorizing = 98

- Call-MBMS-Bearer-Authorizing = 99
- Call-Simple-IP-Connected = 100
- Call-Mobile-IP-Connected = 110
- Call-Tunnel-Connected = 115
- Call-Pdp-Type-IP-Connected = 120
- Call-Pdp-Type-IPv6-Connected = 125
- Call-Pdp-Type-PPP-Connected = 130
- Call-GTP-Connecting = 131
- Call-GTP-Connected = 132
- Call-Proxy-Mobile-IP-Connected = 140
- Call-Pdg-Ssl-Connected = 141
- Call-Pdg-Connected = 142
- Call-Ipsg-Connected = 145
- Call-Bcmcs-Connected = 150
- Call-MBMS-UE-Connected = 155
- Call-MBMS-Bearer-Connected = 156
- Call-Pending-Addr-From-DHCP = 160
- Call-Got-Addr-From-DHCP = 170
- Call-HA-IPSEC-Tunnel-Connecting = 180
- Call-HA-IPSEC-Connected = 190
- Call-ASN-Non-Anchor-Connected = 200
- Call-ASNPC-Connected = 210 Call-Mobile-IPv6-Connected = 220
- Call-PMIPv6-Connected = 221
- Call-PHSPC-Connected = 230
- Call-GTP-IPv4-Connected = 235
- Call-GTP-IPv6-Connected = 236
- Call-GTP-IPv4-IPv6-Connected = 237
- Call-SGW-Connected = 245
- Call-MME-Attached = 246
- Call-Auth-Only-Connected = 247

Length 4

Type 26

Vendor ID 8164

VSA Type 4

SN-PPP-Reneg-Disc

PPP remote reneg disconnect policy

Type 26

Syntax Enumerated Integer. Supports the following value(s):

- Never = 0
- Always = 1
- NAI_Prefix_MSID_Mismatch = 2

Length 4

Vendor ID 8164

VSA Type 187

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.

Syntax Enumerated Integer. Supports the following value(s):

- Uncompressed = 0
- Compressed = 1

Length 4

Type 26

Vendor ID 8164

VSA Type 31

SN-Prepaid-Final-Duration-Alg

For prepaid, final duration is calculated based on the algorithm specified by the value of this attribute.

Syntax Enumerated Integer. Supports the following value(s):

- current_time = 0
- last-user-layer3-activity-time = 1
- last-airlink-activity-time = 2
- last-airlink-activity-time-last-reported = 3

Length 4

Type 26

Vendor ID 8164

VSA Type 135

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.

Syntax Unsigned Integer

Length 4

Type 26

Vendor ID 8164

VSA Type 32

SN-Prepaid-Outbound-Octets

SN-Prepaid-Outbound-Octets

Syntax Unsigned Integer

Length 4

Type 26

Vendor ID 8164

VSA Type 33

SN-Prepaid-Preference

This attribute specifies whether prepaid is volume based or duration based.

Syntax Enumerated Integer. Supports the following value(s):

- prepaid_duration = 0
- prepaid_volume = 1

Length 4

Type 26

Vendor ID 8164

VSA Type 129

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.

Syntax Unsigned Integer

Length 4

Type 26

Vendor ID 8164

VSA Type 35

SN-Prepaid

Prepaid

Syntax Enumerated Integer. Supports the following value(s):

- no_prepaid = 0
- custom_prepaid = 1
- standard_prepaid = 2
- wimax_prepaid = 4

Length 4

Type 26

Vendor ID 8164

VSA Type 128

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.

Syntax Unsigned Integer

Length 4

Type 26

Vendor ID 8164

VSA Type 34

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.

Syntax Unsigned Integer

Length 4

Type 26

Vendor ID 8164

VSA Type 36

SN-Primary-DCCA-Peer

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

Syntax String

Length 1-192

Type 26

Vendor ID 8164

VSA Type 223

SN-Primary-DNS-Server

This attribute indicates the IP address of the primary DNS server that should be used for the session.

Syntax IPv4 Address

Length 4

Type 26

Vendor ID 8164

VSA Type 5

SN-Primary-NBNS-Server

Primary NBNS Server IP address.

Syntax IPv4 Address

Length 4

Type 26

Vendor ID 8164

VSA Type 148

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.

Syntax Enumerated Integer. Supports the following value(s):

- Disabled = 0
- Enabled = 1

Length 4

Type 26

Vendor ID 8164

VSA Type 52

SN-Pseudonym-Username

This attribute contains the pseudonym user name generated by AAA server.

Syntax Opaque Value

Length 1-256

Type 26

Vendor ID 8164

VSA Type 305

SN-QoS-Background-Class

This attribute defines the QOS Background Traffic Class.

Syntax Opaque Value

Length 28

Type 26

Vendor ID 8164

VSA Type 91

SN-QoS-Class-Background-PHB

Quality of Service DSCP classification value.

Syntax Enumerated Integer. Supports the following value(s):

- 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

Length 4

Type 26

Vendor ID 8164

VSA Type 113

SN-QoS-Class-Conversational-PHB

Quality of Service DSCP classification value.

Syntax Enumerated Integer. Supports the following value(s):

- 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

Length 4

Type 26

Vendor ID 8164

VSA Type 111

SN-QoS-Class-Interactive-1-PHB

Interactive-1 class PHB value.

Syntax Enumerated Integer. Supports the following value(s):

- 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

Length 4

Type 26

Vendor ID 8164

VSA Type 114

SN-QoS-Class-Interactive-2-PHB

Interactive-2 class PHB.

Syntax Enumerated Integer. Supports the following value(s):

- 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

Length 4

Type 26

Vendor ID 8164

VSA Type 115

SN-QoS-Class-Interactive-3-PHB

Interactive-3 class PHB.

Syntax Enumerated Integer. Supports the following value(s):

- 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

Length 4

Type 26

Vendor ID 8164

VSA Type 116

SN-QoS-Class-Streaming-PHB

Quality of Service DSCP classification value.

Syntax Enumerated Integer. Supports the following value(s):

- 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

Length 4

Type 26

Vendor ID 8164

VSA Type 112

SN-QoS-Conversation-Class

This attribute defines the QOS Conversation Traffic Class.

Syntax Opaque Value

Length 28

Type 26

Vendor ID 8164

VSA Type 86

SN-QOS-HLR-Profile

QoS with Allocation Retention bit. QoS structured as per 29.002.

Syntax QoS-HLR-Profile

Type 26

Vendor ID 8164

VSA Type 303

SN-QoS-Interactive1-Class

This attribute defines the QOS Interactive TrafficClass.

Syntax Opaque Value

Length 28

Type 26

Vendor ID 8164

VSA Type 88

SN-QoS-Interactive2-Class

This attribute defines the QOS Interactive2 Traffic Class.

Syntax Opaque Value

Length 28

Type 26

Vendor ID 8164

VSA Type 89

SN-QoS-Interactive3-Class

This attribute defines the QOS Interactive3 Traffic Class.

Syntax Opaque Value

Length 28

Type 26

Vendor ID 8164

VSA Type 90

SN-QoS-Negotiated

Negotiated QoS for GGSN sessions.

Syntax Opaque Value

Length 4-28

Type 26

Vendor ID 8164

VSA Type 147

SN-QoS-Renegotiation-Timeout

This attribute configures the timeout duration of dampening time for dynamic QoS renegotiation.

Syntax Unsigned Integer

Length 4

Type 26

Vendor ID 8164

VSA Type 145

SN-QoS-Streaming-Class

This attribute defines the QOS Streaming Traffic Class.

Syntax Opaque Value

Length 28

Type 26

Vendor ID 8164

VSA Type 87

SN-QoS-Tp-Dnlk

This attribute enables/disables Traffic Policing/Shaping in downlink direction.

Syntax Enumerated Integer. Supports the following value(s):

- Disabled = 0
- Policing = 1
- Shaping = 2

Length 4

Type 26

Vendor ID 8164

VSA Type 73

SN-QoS-Tp-Uplk

This attribute enables/disables Traffic Policing/Shaping in uplink direction.

Syntax Enumerated Integer. Supports the following value(s):

- Disabled = 0
- Policing = 1
- Shaping = 2

Length 4

Type 26

Vendor ID 8164

VSA Type 79

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.

Type 26

Vendor ID 8164

VSA Type 177

Syntax Compound. Contains the following sub-attribute(s).

Direction

Direction of the PDF.

Syntax Unsigned Integer

Length 1

Type 1

Class

Traffic class.

Syntax Unsigned Integer

Length 1

Type 2

Burst-Size

Peak burst size.

Syntax Unsigned Integer

Length 4

Type 3

Committed-Data-Rate

Committed data rate.

Syntax Unsigned Integer

Length 4

Type 4

Peak-Data-Rate

Peak data rate.

Syntax Unsigned Integer

Length 4

Type 5

Exceed-Action

Action to take on packets that exceed the Committed-Data-Rate but do not violate the Peak-Data-Rate.

Syntax Unsigned Integer

Length 1

Type 6

Violate-Action

Violate action.

Syntax Unsigned Integer

Length 1

Type 7

Auto-Readjust-Enabled

Auto-readjust enabled.

Syntax Unsigned Integer

Length 1

Type 8

Auto-Readjust-Duration

Auto-readjust duration.

Syntax Unsigned Integer

Length 4

Type 9

Qci

Available only in 11.0 and later releases. QOS QCI accepted values are 1 (qci 1), 2 (qci 2), 3 (qci 3), 4 (qci 4), 5 (qci 5), 6 (qci 6), 7 (qci 7), 8 (qci 8), 9 (qci 9).

Syntax Unsigned Integer

Length 1

Type 10

SN-Rad-APN-Name

This attributes specifies the RADIUS returned APN name.

Type 26

Syntax Opaque Value

Length 1-64

Vendor ID 8164

VSA Type 162

SN-Radius-Returned-Username

This attribute is used to prefer RADIUS returned user name over constructed user name in the accounting messages.

Type 26

Syntax Enumerated Integer. Supports the following value(s):

- No = 0
- Yes = 1

Length 4

Vendor ID 8164

VSA Type 236

SN-Re-CHAP-Interval

The Periodic CHAP authentication interval for PPP, in seconds.

Syntax Unsigned Integer

Length 4

Type 26

Vendor ID 8164

VSA Type 7

SN-Roaming-Behavior

This attribute specifies the configuration for the behavior bits settings for a roaming subscriber in an APN.

Syntax Unsigned Integer

Length 4

Type 26

Vendor ID 8164

VSA Type 121

SN-Roaming-Profile

This attribute specifies the configuration for the profile bits settings for a roaming subscriber in an APN.

Syntax Unsigned Integer

Length 4

Type 26

Vendor ID 8164

VSA Type 118

SN-Roaming-Sub-Use-GGSN

This attribute configures GGSN to accept GGSN's charging characteristics for roaming subscribers defined for the APN.

Syntax Enumerated Integer. Supports the following value(s):

- Deny = 0
- Accept = 1

Length 4

Type 26

Vendor ID 8164

VSA Type 108

SN-ROHC-Flow-Marking-Mode

Configure ROHC compression for marked flows only.

Type 26

Syntax Enumerated Integer. Supports the following value(s):

- False = 0
- True = 1

Length 4

Vendor ID 8164

VSA Type 195

SN-ROHC-Profile-Name

Specifies the ROHC profile to use for the subscriber.

Type 26

Syntax String

Length 1-64

Vendor ID 8164

VSA Type 238

SN-Role-Of-Node

This attribute denotes the role of the CSCF.

Syntax Enumerated Integer. Supports the following value(s):

- Originating_Role = 0

- Terminating_Role = 1

Length 4

Type 26

Vendor ID 8164

VSA Type 256

SN-Routing-Area-Id

For GGSN calls this indicates the Routing Area ID of the subscriber.

Syntax Opaque Value

Length 3

Type 26

Vendor ID 8164

VSA Type 249

SN-Rulebase

When the session is active charging enabled, Rulebase name will specify one of the pre-configured ECSv2 rulebases in active charging subsystem.

Syntax String

Length 1-64

Type 26

Vendor ID 8164

VSA Type 250

SN-SDP-Session-Description

This attribute contains the Session portion of the SDP data exchanged between the User Agents in the SIP transaction.

Syntax SDP-Session-Description

Type 26

Vendor ID 8164

VSA Type 263

SN-Sec-IP-Pool-Name

This attribute contains the secondary IP pool name.

Syntax String

Length 1-253

Type 26

Vendor ID 8164

VSA Type 265

SN-Secondary-DCCA-Peer

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

Syntax String

Length 1-192

Type 26

Vendor ID 8164

VSA Type 224

SN-Secondary-DNS-Server

This attribute indicates the IP address of the secondary DNS server that should be used for the session.

Syntax IPv4 Address

Length 4

Type 26

Vendor ID 8164

VSA Type 6

SN-Secondary-NBNS-Server

Secondary NBNS server IP address.

Syntax IPv4 Address

Length 4

Type 26

Vendor ID 8164

VSA Type 149

SN-Service-Address

Used to send bind IP address of the service in RADIUS messages.

Syntax IPv4 Address

Length 4

Type 26

Vendor ID 8164

VSA Type 169

SN-Service-Type

This attribute indicates the service type that the user is accessing.

Syntax Enumerated Integer. Supports the following value(s):

- 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
- EPDG = 13
- MIPV6HA = 14
- PGW = 15
- SGW = 16
- FNG = 17
- MSEG = 18
- HNBGW = 19
- BNG = 20
- WSG = 21
- SAMOG = 22

Length 4

Type 26

Vendor ID 8164

VSA Type 24

SN-Session-Id

This attribute contains Call-ID of the SIP session.

Syntax String

Length 0-160

Type 26

Vendor ID 8164

VSA Type 257

SN-Simultaneous-SIP-MIP

This attribute indicates if a PDSN Subscriber can simultaneously be given Simple IP and Mobile IP service.

Syntax Enumerated Integer. Supports the following value(s):

- Disabled = 0
- Enabled = 1

Length 4

Type 26

Vendor ID 8164

VSA Type 22

SN-SIP-Method

This attribute identifies the SIP-method for which acct request is sent.

Syntax String

Length 0-32

Type 26

Vendor ID 8164

VSA Type 254

SN-SIP-Request-Time-Stamp

This attribute specifies the time of initial SIP request.

Syntax Unsigned Integer

Length 4

Type 26

Vendor ID 8164

VSA Type 258

SN-SIP-Response-Time-Stamp

This attribute specifies the time of response to initial SIP request.

Syntax Unsigned Integer

Length 4

Type 26

Vendor ID 8164

VSA Type 259

SN-Software-Version

Specifies the software version. Includes the major version number, minor version number, and build number.

Type 26

Syntax String

Length 1-32

Vendor ID 8164

VSA Type 288

SN-Subs-Acc-Flow-Traffic-Valid

Specifies the subscriber account flow traffic is valid.

Type 26

Syntax Enumerated Integer. Supports the following value(s):

- Disable = 0
- Enable = 1

Length 4

Vendor ID 8164

VSA Type 225

SN-Subscriber-Accounting

This attribute specifically enables or disables subscriber accounting. Note that if enabled, subscriber accounting still needs to be enabled in the subscriber's AAA context for accounting to be performed.

Syntax Enumerated Integer. Supports the following value(s):

- None = 0
- Radius = 1

- GTPP = 2

Length 4

Type 26

Vendor ID 8164

VSA Type 64

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.

Syntax Enumerated Integer. Supports the following value(s):

- Normal = 0
- Suppress = 1

Length 4

Type 26

Vendor ID 8164

VSA Type 70

SN-Subscriber-Acct-Mode

Specifies the subscriber accounting mode.

Syntax Enumerated Integer. Supports the following value(s):

- flow-based-auxilliary = 0
- flow-based-all = 1
- flow-based-none = 2
- session-based = 3
- main-a10-only = 4

Length 4

Type 26

Vendor ID 8164

VSA Type 192

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.

Syntax Enumerated Integer. Supports the following value(s):

- None = 0
- No_Early_PDUs = 1
- Delay_GTP_Response = 2

Length 4

Type 26

Vendor ID 8164

VSA Type 100

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.

Syntax Enumerated Integer. Supports the following value(s):

- Normal = 0
- Suppress = 1

Length 4

Type 26

Vendor ID 8164

VSA Type 69

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.

Syntax Enumerated Integer. Supports the following value(s):

- Normal = 0
- Suppress = 1

Length 4

Type 26

Vendor ID 8164

VSA Type 71

SN-Subscriber-Class

Customer-specific attribute to support specific subscriber billing behavior.

Syntax Enumerated Integer. Supports the following value(s):

- 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

Length 4

Type 26

Vendor ID 8164

VSA Type 219

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.

Syntax Enumerated Integer. Supports the following value(s):

- Disabled = 0
- Enabled = 1

Length 4

Type 26

Vendor ID 8164

VSA Type 66

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.

Syntax Enumerated Integer. Supports the following value(s):

- Force = 0
- Detect = 1

Length 4

Type 26

Vendor ID 8164

VSA Type 67

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.

Syntax Enumerated Integer. Supports the following value(s):

- None = 0
- Access-Tunnel = 1
- Data-Tunnel = 2
- Both = 3

Length 4

Type 26

Vendor ID 8164

VSA Type 85

SN-Subscriber-Nexthop-Address

This attribute specifies the nexthop gateway address to be returned by AAA on a per subscriber basis.

Syntax IPv4 Address

Length 4

Type 26

Vendor ID 8164

VSA Type 127

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.

Syntax Enumerated Integer. Supports the following value(s):

- Disabled = 0

- Enabled = 1

Length 4

Type 26

Vendor ID 8164

VSA Type 133

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.

Syntax Enumerated Integer. Supports the following value(s):

- 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
- GGSN-PDP-TYPE-PPP = 0x10
- Network-Mobility = 0x20
- FA-HA-NEMO = 0x26
- Pmipv6-interception = 0x40
- HA-Mobile-Pmipv6 = 0x44
- FA-HA-Mobile-Pmipv6 = 0x46
- All = 0x7F

Length 4

Type 26

Vendor ID 8164

VSA Type 20

SN-Subscriber-Template-Name

RADIUS returned subscriber template.

Type 26

Syntax String

Length 1-127

Vendor ID 8164

VSA Type 158

SN-Subs-IMSA-Service-Name

IMS authorization service name.

Type 26

Syntax String

Length 1-128

Vendor ID 8164

VSA Type 159

SN-Subs-VJ-Slotid-Cmp-Neg-Mode

Enable/Disable slot ID compression in either direction when using VJ compression.

Type 26

Syntax Enumerated Integer. Supports the following value(s):

- None = 0
- Receive = 1
- Transmit = 2
- Both = 3

Length 4

Vendor ID 8164

VSA Type 221

SN-Terminating-IOI

This attribute holds the Inter Operator Identifier for the originating network in the home network of the terminating end user.

Syntax String

Length 1-253

Type 26

Vendor ID 8164

VSA Type 262

SN-Tp-Dnlk-Burst-Size

This attribute specifies the Traffic Policing downlink burst size in bytes.

Syntax Unsigned Integer

Length 4

Type 26

Vendor ID 8164

VSA Type 76

SN-Tp-Dnlk-Committed-Data-Rate

This attribute specifies the Traffic Policing downlink committed data rate in bps.

Syntax Unsigned Integer

Length 4

Type 26

Vendor ID 8164

VSA Type 74

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.

Syntax Enumerated Integer. Supports the following value(s):

- Transmit = 0
- Drop = 1
- Lower-IP-Precedence = 2
- Buffer = 3
- Transmit-On-Buffer-Full = 4

Length 4

Type 26

Vendor ID 8164

VSA Type 77

SN-Tp-Dnlk-Peak-Data-Rate

This attribute specifies the Traffic Policing downlink peak data rate in bps.

Syntax Unsigned Integer

Length 4

Type 26

Vendor ID 8164

VSA Type 75

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.

Syntax Enumerated Integer. Supports the following value(s):

- Transmit = 0
- Drop = 1
- Lower-IP-Precedence = 2
- Buffer = 3
- Transmit-On-Buffer-Full = 4

Length 4

Type 26

Vendor ID 8164

VSA Type 78

SN-TPO-Policy

This attribute contains the TPO policy name.

Syntax String

Length 1-63

Type 26

Vendor ID 8164

VSA Type 308

SN-Tp-Uplk-Burst-Size

This attribute specifies the Traffic Policing uplink burst size in bytes.

Syntax Unsigned Integer

Length 4

Type 26

Vendor ID 8164

VSA Type 82

SN-Tp-Uplk-Committed-Data-Rate

This attribute specifies the Traffic Policing uplink committed data rate in bps.

Syntax Unsigned Integer

Length 4

Type 26

Vendor ID 8164

VSA Type 80

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.

Syntax Enumerated Integer. Supports the following value(s):

- Transmit = 0
- Drop = 1
- Lower-IP-Precedence = 2
- Buffer = 3
- Transmit-On-Buffer-Full = 4

Length 4

Type 26

Vendor ID 8164

VSA Type 83

SN-Tp-Uplk-Peak-Data-Rate

This attribute specifies the Traffic Policing Uplink Peak Data Rate in bps.

Syntax Unsigned Integer

Length 4

Type 26

Vendor ID 8164

VSA Type 81

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.

Syntax Enumerated Integer. Supports the following value(s):

- Transmit = 0
- Drop = 1
- Lower-IP-Precedence = 2
- Buffer = 3
- Transmit-On-Buffer-Full = 4

Length 4

Type 26

Vendor ID 8164

VSA Type 84

SN-Traffic-Group

This attribute is used to assign a tag to an FA or a group of FAs, so that traffic policy can be enforced based on the tag value.

Syntax Unsigned Integer

Length 2

Type 26

Vendor ID 8164

VSA Type 161

SN-TrafficSelector-Class

The ipsec traffic selector class.

Syntax Unsigned Integer

Length 4

Type 26

Vendor ID 8164

VSA Type 307

SN-Transparent-Data

This attribute is used by RADIUS to provide Global Title information for the GGSN to use in CDRs and Quota Auth.

Syntax Opaque Value

Length 1-247

Type 26

Vendor ID 8164

VSA Type 247

SN-Tun-Addr-Policy

Describes IP address validation policy for non L2TP tunneled calls.

Syntax Enumerated Integer. Supports the following value(s):

- no-local-alloc-validate = 0
- local-alloc = 1
- local-alloc-validate = 2

Length 4

Type 26

Vendor ID 8164

VSA Type 156

SN-Tunnel-Gn

Used to enable/disable Gn interface from PDG/TTG to GGSN.

Syntax Enumerated Integer. Supports the following value(s):

- Disabled = 0
- Enabled = 1

Length 4

Type 26

Vendor ID 8164

VSA Type 174

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.

Syntax String

Length 1-128

Type 26

Vendor ID 8164

VSA Type 38

SN-Tunnel-ISAKMP-Secret

This attribute specifies the secret to use for IKE.

Syntax String

Length 1-128

Type 26

Vendor ID 8164

VSA Type 39

SN-Tunnel-Load-Balancing

This attribute specifies the load-balancing algorithm to use when tunneling is employed.

Syntax Enumerated Integer. Supports the following value(s):

- random = 1
- balanced = 2
- prioritized = 3

Length 4

Type 26

Vendor ID 8164

VSA Type 27

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.

Syntax Opaque Value

Length 1-240

Type 26

Vendor ID 8164

VSA Type 26

SN-Unclassify-List-Name

Unclassify List Name.

Syntax String

Length 1-32

Type 26

Vendor ID 8164

VSA Type 132

SN-User-Privilege

This attribute specifies the user privilege.

Syntax Enumerated Integer. Supports the following value(s):

- Administrative = 6
- NAS_Prompt = 7
- Inspector = 19650516
- Security_Admin = 19660618

Length 4

Type 26

Vendor ID 8164

VSA Type 313

SN-Virtual-APN-Name

This attribute contains the virtual APN name.

Syntax Opaque Value

Length 1-64

Type 26

Vendor ID 8164

VSA Type 94

SN-Visiting-Behavior

This attribute specifies the configuration for the behavior bits settings for a visiting subscriber in an APN.

Syntax Unsigned Integer

Length 4

Type 26

Vendor ID 8164

VSA Type 120

SN-Visiting-Profile

This attribute specifies the configuration for the profile bits settings for a visiting subscriber in an APN.

Syntax Unsigned Integer

Length 4

Type 26

Vendor ID 8164

VSA Type 117

SN-Visiting-Sub-Use-GGSN

This attribute configures GGSN to accept GGSN's charging characteristics for visiting subscribers defined for the APN.

Syntax Enumerated Integer. Supports the following value(s):

- Deny = 0
- Accept = 1

Length 4

Type 26

Vendor ID 8164

VSA Type 107

SN-Voice-Push-List-Name

SN-Voice-Push-List-Name.

Syntax String

Length 1-32

Type 26

Vendor ID 8164

VSA Type 131

SN-VPN-ID

This attribute contains the Destination VPN of the user, specified by a 32-bit identifier.

Syntax Unsigned Integer

Length 4

Type 26

Vendor ID 8164

VSA Type 1

SN-VPN-Name

This attribute contains the name of the user's Destination VPN.

Syntax String

Length 1-253

Type 26

Vendor ID 8164

VSA Type 2

SN-VRF-Name

This attribute specifies the IP VRF context to distinguish the RADIUS accounting feeds per enterprise.

Syntax String

Length 1-63

Type 26

Vendor ID 8164

VSA Type 242

SN-WiMAX-Auth-Only

Specifies whether the call is established for Authentication Mode Only.

Syntax Enumerated Integer. Supports the following value(s):

- Disabled = 0
- Enabled = 1

Length 1

Type 26

Vendor ID 8164

VSA Type 306

SN-WLAN-AP-Identifier

This attribute contains the access point identifier for WLAN UE. This attribute comprises LAC and CI digits separated by an underscore. This AP identifier may include Access point MAC address or MAC/SSID. This attribute is received in Acct-Start / Acct-Interim message from WLC.

Syntax Opaque Value

Length 1-48

Type 26

Vendor ID 8164

VSA Type 319

SN-WLAN-UE-Identifier

This attribute contains the identifier for WLAN UE, i.e. device's MAC address in Calling-Station-Id attribute format according to RFC 3580 (MAC address in ASCII format (upper case only), with octet values separated by a "-"). Example: "00-10-A4-23-19-C0". This attribute is received in Acct-Start / Acct-Interim message from WLC.

Syntax Opaque Value

Length 1-17

Type 26

Vendor ID 8164

VSA Type 320

SN-WSG-MIP-Release-TIA

WSG Mobile IP Release TIA

Syntax Enumerated Integer. Supports the following value(s):

- No = 0
- Yes = 1

Length 4

Type 26

Vendor ID 8164

VSA Type 317

SN-WSG-MIP-Required

This attribute indicates whether or not the WSG Mobile IP is required.

Syntax Enumerated Integer. Supports the following value(s):

- No = 0
- Yes = 1

Length 4

Type 26

Vendor ID 8164

VSA Type 316

SN-WSG-MIP-Simple-IP-Fallback

WSG Mobile IP Simple IP Fallback

Syntax Enumerated Integer. Supports the following value(s):

- No = 0
- Yes = 1

Length 4

Type 26

Vendor ID 8164

VSA Type 318

Terminal-Capability

Opaque one byte value received from customer RADIUS server in Access Request. Used in custom dictionary.

Syntax Opaque Value

Length 1

Type 26

Vendor ID 5535

VSA Type 219

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.

Syntax Enumerated Integer. Supports the following value(s):

- Default = 0
- RADIUS-Request = 1

Length 4

Type 29

Vendor ID N/A

VSA Type N/A

Tunnel-Assignment-ID

This attribute indicates the tunnel to which the session is to be assigned.

Syntax Opaque Value

Length 1-252

Type 82

Vendor ID N/A

VSA Type N/A

Tunnel-Client-Auth-ID

This attribute contains the name of the client for the purposes of tunnel authentication.

Syntax Opaque Value

Length 1-252

Type 90

Vendor ID N/A

VSA Type N/A

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.

Syntax Opaque Value

Length 1-250

Type 66

Vendor ID N/A

VSA Type N/A

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.

Syntax Enumerated Integer. Supports the following value(s):

- 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

Length 4

Type 65

Vendor ID N/A

VSA Type N/A

Tunnel-Password

This attribute contains a shared secret for the Tunnel connection. It is salt-encrypted.

Syntax Opaque Value

Length 1-240

Type 69

Vendor ID N/A

VSA Type N/A

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.

Syntax Unsigned Integer

Length 4

Type 83

Vendor ID N/A

VSA Type N/A

Tunnel-Private-Group-ID

This attribute contains the context of the tunnel.

Syntax String

Length 1-252

Type 81

Vendor ID N/A

VSA Type N/A

Tunnel-Server-Auth-ID

This attribute contains the name of the server for the purposes of tunnel authentication.

Syntax Opaque Value

Length 1-252

Type 91

Vendor ID N/A

VSA Type N/A

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.

Syntax Opaque Value

Length 1-250

Type 67

Vendor ID N/A

VSA Type N/A

Tunnel-Type

This attribute indicates the type of tunnel used by the subscriber.

Syntax Enumerated Integer. Supports the following value(s):

- 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
- GN = 14
- UDP = 15

Length 4

Type 64

Vendor ID N/A

VSA Type N/A

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.

Syntax Opaque Value

Length 1-253

Type 1

Vendor ID N/A

VSA Type N/A

User-Password

This attribute contains the encrypted password of the user, when simple password authentication is being used.

Syntax Opaque Value

Length 16-128

Type 2

Vendor ID N/A

VSA Type N/A

White-List

This attribute contains the list of IMSIs which are allowed to access through an HNB.

Syntax Opaque Value

Length 3-251

Type 26

Vendor ID 9

VSA Type 117

WiMAX-Acct-Input-Packets-Giga

Number of packets incremented each time Acct-Input-Packets(47) overflows.

Syntax Unsigned Integer

Length 4

Type 26

Vendor ID 24757

VSA Type 48

WiMAX-Acct-Output-Packets-Giga

Number of packets incremented each time Acct-Output-Packets(48) overflows.

Syntax Unsigned Integer

Length 4

Type 26

Vendor ID 24757

VSA Type 49

WiMAX-Active-Time

The period of time the session was NOT in idle state.

Syntax Unsigned Integer

Length 4

Type 26

Vendor ID 24757

VSA Type 39

WiMAX-Beginning-Of-Session

This attribute indicates whether the session is new or a continuation of previous flow.

Syntax Enumerated Integer. Supports the following value(s):

- False = 0
- True = 1

Length 4

Type 26

Vendor ID 24757

VSA Type 22

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.

Syntax Opaque Value

Length 6-12

Type 26

Vendor ID 24757

VSA Type 46

WiMAX-Capability

This compound attribute identifies the supported WiMAX capabilities.

Type 26

Vendor ID 24757

VSA Type 1

Syntax Compound. Contains the following sub-attribute(s).

WiMAX-Release

Specifies WiMAX release of the sender.

Syntax String

Length 4

Type 1

Accounting-Capabilities

Describes accounting capabilities supported for the session.

Syntax Enumerated Integer. Supports the following value(s):

- None = 0x00
- IP-Session-Based = 0x01
- Flow-Based = 0x02
- IP-Session-And-Flow-Based = 0x03

Length 1

Type 2

Hotlining-Capabilities

Supported hotline capabilities.

Syntax Enumerated Integer. Supports the following value(s):

- Not-Supported = 0x00
- Hotline-Profile-Id = 0x01
- NAS-Filter = 0x02
- HTTP-Redirection = 0x04
- Profile-Id-based-and-HTTP-Redirection-Rule-based = 0x05
- IP-Redirection = 0x08

Length 1

Type 3

Idle-Mode-Notification-Capabilities

Describes idle mode notification capabilities.

Syntax Enumerated Integer. Supports the following value(s):

- Not-Supported = 0x00
- Supported = 0x01

Length 1

Type 4

ROHC-Support

Describes ROHC capability support for the session

Syntax Enumerated Integer. Supports the following value(s):

- Not-Supported = 0x00
- Supported = 0x01

Length 1

Type 11

WiMAX-Control-Octets-In

Octet counts for incoming Mobile IP, DHCP, ICMP messages for IPv4 and IPv6.

Syntax Unsigned Integer

Length 4

Type 26

Vendor ID 24757

VSA Type 32

WiMAX-Control-Octets-Out

Octet counts for outgoing Mobile IP, DHCP, ICMP messages for IPv4 and IPv6.

Syntax Unsigned Integer

Length 4

Type 26

Vendor ID 24757

VSA Type 34

WiMAX-Control-Packets-In

Packet counts for incoming Mobile IP, DHCP, ICMP messages for IPv4 and IPv6.

Syntax Unsigned Integer

Length 4

Type 26

Vendor ID 24757

VSA Type 31

WiMAX-Control-Packets-Out

Packet counts for outgoing Mobile IP, DHCP, ICMP messages for IPv4 and IPv6.

Syntax Unsigned Integer

Length 4

Type 26

Vendor ID 24757

VSA Type 33

WiMAX-Count-Type

Indicates if the record represents compressed counts over-the-air.

Syntax Unsigned Integer

Length 1

Type 26

Vendor ID 24757

VSA Type 59

WiMAX-Device-Auth-Indicator

Indicates whether NAS performed device authentication successfully or not.

Syntax Unsigned Integer

Length 1

Type 26

Vendor ID 24757

VSA Type 2

WiMAX-Flow-Description

Describes a flow classifier.

Syntax String

Length 1-240

Type 26

Vendor ID 24757

VSA Type 50

WiMAX-Home-HNP-PMIP6

The IPv6 Home Network Prefix assigned by the AAA in HCSN to the MS for PMIP6 mobility session.

Syntax Opaque Value

Length 2-18

Type 26

Vendor ID 24757

VSA Type 133

WiMAX-Home-IPv4-HoA-PMIP6

The IPv4 Home Address assigned by the CSN to the MS for PMIP6-IPv4 mobility session.

Syntax IPv4 Address

Length 4

Type 26

Vendor ID 24757

VSA Type 135

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.

Syntax Enumerated Integer. Supports the following value(s):

- Not-Idle = 0x00
- Idle = 0x01

Length 1

Type 26

Vendor ID 24757

VSA Type 44

WiMAX-IP-Technology

Indicates the type of WiMAX session being used.

Syntax Enumerated Integer. Supports the following value(s):

- SIP = 1
- PMIP4 = 2
- CMIP4 = 3
- CMIP6 = 4
- Ethernet-CS = 5
- PMIP6 = 6

Length 4

Type 26

Vendor ID 24757

VSA Type 23

WiMAX-NAP-ID

Uniquely identifies the Network Access Provider.

Syntax String

Length 3

Type 26

Vendor ID 24757

VSA Type 45

WiMAX-NSP-ID

Uniquely identifies the Network Service Provider.

Syntax Opaque Value

Length 3

Type 26

Vendor ID 24757

VSA Type 57

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

Syntax Compound. Contains the following sub-attribute(s).

Length 4-1400

PDF-ID

Used to match all records from the same Packet Data Flow.

Syntax Unsigned Integer

Length 2

Type 1

SDF-ID

Used to match all PDFs from the same Service Data Flow.

Syntax Unsigned Integer

Length 2

Type 2

Service-Profile-ID

Identifies a pre-configured Flow Descriptor at the NAS.

Syntax Unsigned Integer

Length 4

Type 3

Direction

Direction of the PDF.

Syntax Enumerated Integer. Supports the following value(s):

- Uplink = 1
- Downlink = 2
- Bi-Directional = 3

Length 1

Type 4

Activation-Trigger

Specifies the trigger to be used for the activation of Service Flow.

Syntax Enumerated Integer. Supports the following value(s):

- Provisioned = 0x01
- Admit = 0x02
- Provisioned-Admit = 0x03
- Activate = 0x04
- Provisioned-Activate = 0x05
- Admit-Activate = 0x06
- Provisioned-Admit-Activate = 0x07 Dynamic = 0x08 Dynamic-Admit = 0x0a Dynamic-Activate = 0x0c Dynamic-Admit-Activate = 0x0e

Length 1

Type 5

Transport-Type

Type of transport (IP, Ethernet).

Syntax Enumerated Integer. Supports the following value(s):

- IPv4-CS = 1
- IPv6-CS = 2
- Ethernet = 3

Length 1

Type 6

Uplink-QoS-ID

Identifier of the QoS Descriptor for Uplink or Bidirection.

Syntax Unsigned Integer

Length 1

Type 7

Downlink-QoS-ID

Identifier of the QoS Descriptor for Downlink.

Syntax Unsigned Integer

Length 1

Type 8

Uplink-Classifier

Classifier to match for traffic flowing in Uplink Direction.

Syntax String

Length 1-240

Type 9

Downlink-Classifier

Classifier to match for traffic flowing in Downlink Direction.

Syntax String

Length 1-240

Type 10

WiMAX-Packet-Flow-Descriptor-V2

Describes a Unidirectional or Bidirectional Packet Flow Descriptor Version 2. This attribute is also accepted in CoA request message to be used in a currently active subscriber session.

Length 4-1400

Type 26

Vendor ID 24757

VSA Type 84

Syntax Compound. Contains the following sub-attribute(s).

PDF-ID

Used to match all records from the same Packet Data Flow.

Syntax Unsigned integer

Length 2

Type 1

SDF-ID

Used to match all PDFs from the same Service Data Flow.

Syntax Unsigned integer

Length 2

Type 2

Service-Profile-ID

Identifies a pre-configured Flow Descriptor at the NAS.

Syntax Unsigned integer

Length 4

Type 3

Direction

Direction of the PDF.

Syntax Enumerated integer. Supported values are:

- Uplink = 1
- Downlink = 2
- Bi-Directional = 3

Length 1

Type 4

Activation-Trigger

Specifies the trigger to be used for the activation of Service Flow.

Syntax Enumerated integer. Supported values are:

- Provisioned = 0x01
- Admit = 0x02
- Activate = 0x04
- Dynamic = 0x08

Length 1

Type 5

Transport-Type

Type of transport (IP, Ethernet).

Syntax Enumerated integer. Supported values are:

- IPv4-CS = 1
- IPv6-CS = 2
- Ethernet = 3

Length 1

Type 6

Uplink-QoS-ID

Identifier of the QoS Descriptor for Uplink or Bidirection.

Syntax Unsigned integer

Length 1

Type 7

Downlink-QoS-ID

Identifier of the QoS Descriptor for Downlink.

Syntax Unsigned integer

Length 1

Type 8

WiMAX-Packet-Flow-Classifier

Describes Packet Flow Classifiers.

Type 9

Syntax Contains the following sub-attributes:

Classifier-ID

WiMAX Classifier ID.

Syntax Unsigned integer

Length 1

Type 1

Priority

WiMAX Classifier Priority.

Syntax Unsigned integer

Length 1

Type 2

Protocol

WiMAX Classifier Protocol, i.e TCP/UDP.

Syntax In StarOS 10.0 and earlier: Enumerated integer. Supported values are:

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

In StarOS 10.2 and later: Unsigned integer.

Length 1

Type 3

Direction

Direction of the PDF.

Syntax Enumerated integer. Supported values are:

- Uplink = 1
- Downlink = 2
- Bi-Directional = 3

Length 1

Type 4

Source-Specification

Identifies WiMAX classifier rule params for source specification.

Length 1

Type 5

Syntax Contains the following sub-attributes:

IP-Address

This attribute contains source/destination address.

Syntax IPv4 address

Length 4

Type 1

IP-Address-Range

WiMAX Packet Classifier IP Address Range.

Syntax Opaque value

Length 1

Type 2

IP-Address-Mask

WiMAX Packet Classifier IP Address Mask.

Syntax Opaque value

Length 5

Type 3

Port

WiMAX Packet Classifier Port.

Syntax Unsigned integer

Length 2

Type 4

Port-Range

WiMAX Packet Classifier Port Range.

Syntax Unsigned integer

Length 4

Type 5

Inverted

WiMAX Classifier Inverted.

Syntax Enumerated integer. Supported values are:

- FALSE = 0
- TRUE = 1

Length 1

Type 6

Assigned

WiMAX Classifier Assigned.

Syntax Enumerated integer. Supported values are:

- Src_Assigned = 1
- Dest_Assigned = 2
- Src_Dest_Assigned = 3

Length 1

Type 7

Destination-Specification

Identifies WiMAX classifier rule params for destination specification.

Syntax Contains the following sub-attribute(s):

Type 6

IP-Address

This attribute contains source/destination address.

Syntax IPv4 address

Length 4

Type 1

IP-Address-Range

WiMAX Packet Classifier IP Address Range.

Syntax Opaque value

Length 8

Type 2

IP-Address-Mask

WiMAX Packet Classifier IP Address Mask.

Syntax Opaque value

Length 5

Type 3

Port

WiMAX Packet Classifier Port.

Syntax Unsigned integer

Length 2

Type 4

Port-Range

WiMAX Packet Classifier Port Range.

Syntax Unsigned integer

Length 4

Type 5

Inverted

WiMAX Classifier Inverted.

Syntax Enumerated integer. Supported values are:

- FALSE = 0
- TRUE = 1

Length 1

Type 6

Assigned

WiMAX Classifier Assigned.

Syntax Enumerated integer. Supported values are:

- Src_Assigned = 1
- Dest_Assigned = 2
- Src_Dest_Assigned = 3

Length 1

Type 7

IP-TOS-DSCP-Range-And-Mask

WiMAX Classifier WiMAX-IP-TOS-DSCP-Range-And-Mask.

Syntax Opaque value

Length 1-3

Type 7

Action

WiMAX Classifier Action.

Syntax Enumerated integer. Supported values are:

- Reserved = 0
- Permit = 1
- Deny = 2

Length 1

Type 8

Paging-Preference

WiMAX Paging Preference.

Syntax Enumerated integer. Supported values are:

- FALSE = 0
- TRUE = 1

Length 1

Type 10

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.

Syntax Unsigned Integer

Length 2

Type 26

Vendor ID 24757

VSA Type 26

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

Syntax Compound. Contains the following sub-attribute(s).

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.

Syntax Enumerated Integer. Supports the following value(s):

- Supported_None = 0
- Supported_Volume = 1
- Supported_Duration = 2
- Supported_Volume_And_Duration = 3
- Supported_Tariff_Switch = 64
- Supported_Volume_And_Duration_And_Tariff_Switch = 67

Length 4

Type 1

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

Syntax Compound. Contains the following sub-attribute(s).

Quota-Identifier

It is generated by the PPS together with the allocation of new quota.

Syntax Opaque Value

Length 1-4

Type 1

Volume-Quota

Indicates the volume in octets excluding control data.

Syntax Opaque Value

Length 4-12

Type 2

Volume-Threshold

Is generated by the PPS and indicates the volume (in octets) that be consumed before a new quota should be requested.

Syntax Opaque Value

Length 4-12

Type 3

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.

Syntax Unsigned Integer

Length 4

Type 4

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.

Syntax Unsigned Integer

Length 4

Type 5

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.

Syntax Enumerated Integer. Supports the following value(s):

- 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

Length 1

Type 8

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.

Syntax IPv4 Address

Length 4

Type 9

Service-ID

This value is a string that uniquely describes the service instance to which prepaid metering should be applied.

Syntax Opaque Value

Length 1-246

Type 10

Rating-Group-ID

Rating-Group-ID for which the WiMAX PPAQ is allocated or reported.

Syntax Unsigned Integer

Length 4

Type 11

Termination-Action

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

Syntax Enumerated Integer. Supports the following value(s):

- Reserved = 0
- Terminate = 1
- Request-more-quota = 2
- Redirect/Filter = 3

Length 1

Type 12

WiMAX-Prepaid-Indicator

Indicates that this session was associated with a prepaid user (online accounting).

Syntax Enumerated Integer. Supports the following value(s):

- Offline = 0
- Online = 1

Length 1

Type 26

Vendor ID 24757

VSA Type 25

WiMAX-Prepaid-Tariff-Switch

Attribute to indicate Tariff-Switch-Interval / Time-Interval-After-Tariff-Switch-Update by the PPS and Volume-Used-After-Tariff-Switch by the PPC.

Type 26

Vendor ID 24757

VSA Type 38

Syntax Compound. Contains the following sub-attribute(s).

Quota-Identifier

It is generated by the PPS together with the allocation of new quota.

Syntax Opaque Value

Length 1-4

Type 1

Volume-Used-After-Tariff-Switch

Volume quota used after tariff switch happened.

Syntax Unsigned Integer

Length 4

Type 2

Tariff-Switch-Interval

Tariff switch interval in seconds.

Syntax Unsigned Integer

Length 4

Type 3

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

Syntax Unsigned Integer

Length 4

Type 4

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

Syntax Compound. Contains the following sub-attribute(s).

Length 6-700

QoS-ID

Unique ID for the QoS specification in the packet

Syntax Unsigned Integer

Length 1

Type 1

Global-Service-Class-Name

Specifies global service class name as defined in IEEE802.16e.

Syntax String

Length 6

Type 2

Service-Class-Name

Specifies service class name as defined in IEEE802.16e.

Syntax String

Length 2-127

Type 3

Schedule-Type

Specifies the uplink granted scheduling type.

Syntax Enumerated Integer. Supports the following value(s):

- Best-Effort = 2
- nrtPS = 3
- rtPS = 4
- Extended-rtPS = 5
- UGS = 6

Length 1

Type 4

Traffic-Priority

Specifies the priority assigned to a service flow.

Syntax Unsigned Integer

Length 1

Type 5

Maximum-Sustained-Traffic-Rate

Specifies peak information rate of the service in bits/second.

Syntax Unsigned Integer

Length 4

Type 6

Minimum-Reserved-Traffic-Rate

Syntax Unsigned Integer

Length 4

Type 7

Maximum-Traffic-Burst

Specifies maximum burst size accommodated for the Service in bytes/second.

Syntax Unsigned Integer

Length 4

Type 8

Tolerated-Jitter

Specifies maximum delay variation in milliseconds.

Syntax Unsigned Integer

Length 4

Type 9

Maximum-Latency

Specifies maximum latency in milliseconds.

Syntax Unsigned Integer

Length 4

Type 10

Reduced-Resources-Code

Indicates that requesting entity will accept reduced resources if requested resources are unavailable.

Syntax Unsigned Integer

Length 1

Type 11

Media-Flow-Type

Specifies the application type, used as a hint in admission decisions.

Syntax Enumerated Integer. Supports the following value(s):

- 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

Length 1

Type 12

Unsolicited-Grant-Interval

Specifies nominal interval between successive data grant opportunities for the Service Flow, in milliseconds.

Syntax Unsigned Integer

Length 2

Type 13

SDU-Size

Specifies the number of bytes in the fixed size SDU.

Syntax Unsigned Integer

Length 1

Type 14

Unsolicited-Polling-Interval

Specifies maximal nominal interval between successive polling grant opportunities for the Service Flow.

Syntax Unsigned Integer

Length 2

Type 15

Transmission-Policy

Include options for PDU formation, and for uplink service flows, restrictions on the types of bandwidth request options that may be use.

Syntax Unsigned Integer

Length 1

Type 17

DSCP

DSCP

Syntax Enumerated Integer. Supports the following value(s):

- Best-Effort = 0
- CS1 = 8
- AF11 = 10
- AF12 = 12
- AF13 = 14
- CS2 = 16
- AF21 = 18
- AF22 = 20
- AF23 = 22
- CS3 = 24
- AF31 = 26
- AF32 = 28
- AF33 = 30
- CS4 = 32
- AF41 = 34
- AF42 = 36
- AF43 = 38
- CS5 = 40
- EF = 46
- CS6 = 48

- CS7 = 56

Length 4

Type 18

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.

Syntax Unsigned Integer

Length 2

Type 26

Vendor ID 24757

VSA Type 27

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.

Syntax Enumerated Integer. Supports the following value(s):

- False = 0
- True = 1

Length 4

Type 26

Vendor ID 24757

VSA Type 21

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.

Syntax Enumerated Integer. Supports the following value(s):

- Only_Dynamic_Auth_Extn_to_Radius = 0x00000001
- Only_Reg_Revocation_in_MIP = 0x00000002
- Both_Dynamic_Auth_And_Reg_Revocation_in_MIP = 0x00000003

Length 4

Type 26

Vendor ID 24757

VSA Type 36

Win-Call-Id

Customer-specific attribute used in custom dictionary. Contains opaque 1 byte value received from customer RADIUS server in access request.

Syntax Unsigned Integer

Length 4

Type 26

Vendor ID 5535

VSA Type 205

Win-Service-Name

Opaque value value received from customer RADIUS server in Access Request. Used in custom dictionary.

Syntax String

Length 0-256

Type 26

Vendor ID 5535

VSA Type 206

WSType

Opaque one byte value received from customer RADIUS server in Access Request.

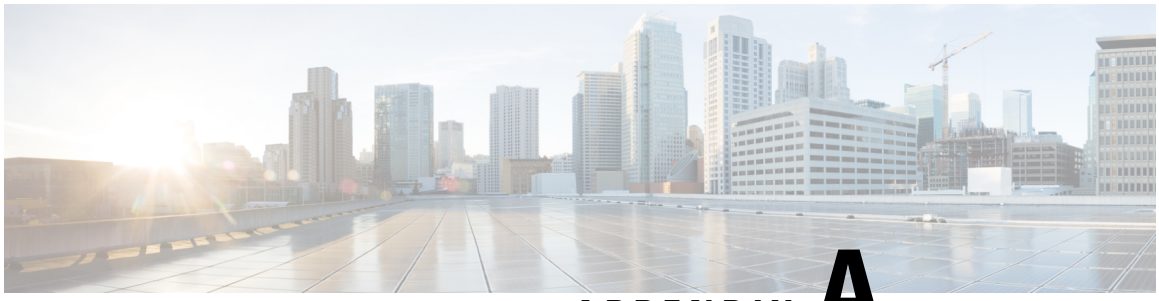
Syntax Unsigned Integer

Length 4

Type 26

Vendor ID 5535

VSA Type 197



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:

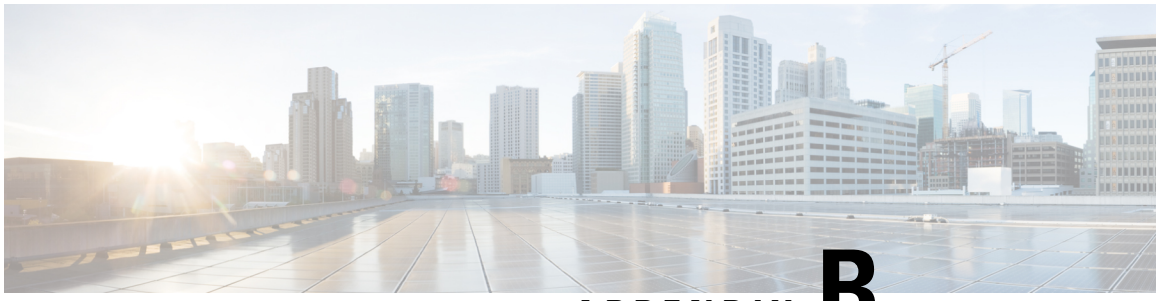
- AAA interfaces are specified by assigning the IP address of a logical interface within a specific context as the RADIUS NAS IP Address (RFC-2865 and RFC-2866) within the same context. This is done using the **radius attribute nas-ip-address** command in the context configuration mode.
- AAA interfaces 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.
- The maximum attribute size in Diameter-EAP-Answer (DEA) message is 3400 bytes.



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.

Note 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.

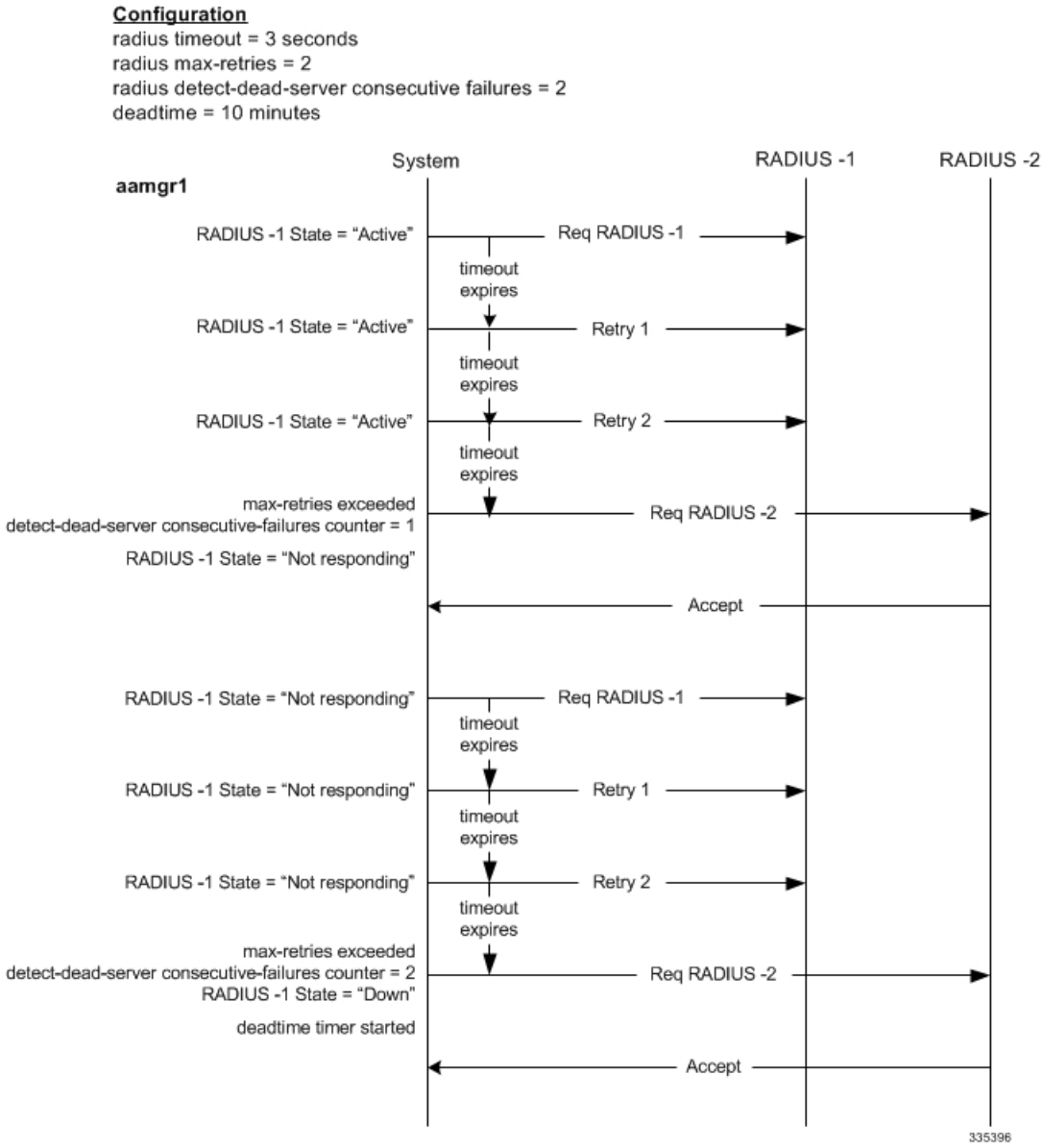
  Note Configuring deadtime as 0 disables the feature and the server is never marked as DOWN.

- **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 across all configured/enabled servers 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 4: 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".

Note 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".

Note These triggers, events and conditions are applicable for each individual AAAmgr instance and the state change will be propagated throughout the system. The state of the server could be set to "Down" even if a single AAAmgr instance is affected and satisfies the **detect-dead-server** parameter criteria. However, even if any one of the non-affected AAAmgr instances receives a response from the RADIUS server, the state of the server is changed back to "Active", so that the affected AAAMgr does not impact all the other working ones.

- 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".
- In releases prior to 18.0, whenever a chassis boots up or when a new RADIUS accounting server or RADIUS mediation-device accounting server is configured with Acct-On configuration enabled, the state of the RADIUS server in all the AAA manager instances is initialized to "Waiting-for-response-to-Accounting-On". The Acct-On transmission and retries are processed by the Admin-AAAmgr.

  When the Acct-On transaction is complete (i.e., when a response for Acct-On message is received or when Acct-On message is retried and timed-out), Admin-AAAmgr changes the state of the RADIUS accounting server to Active in all the AAA manager instances. During the period when the state of the server is in "Waiting-for-response-to-Accounting-On", any new RADIUS accounting messages which are generated as part of a new call will not be transmitted towards the RADIUS accounting server but it will be queued. Only when the state changes to Active, these queued up messages will be transmitted to the server.

During ICSR, if the interface of the radius nas-ip address is srp-activated, then in the standby chassis, the sockets for the nas-ip will not be created. The current behavior is that if the interface is srp-activated Accounting-On transaction will not happen at ICSR standby node and the state of the RADIUS server in all the AAAmgr instances will be shown as "Waiting-for-response-to-Accounting-On" till the standby node becomes Active.

In 18.0 and later releases, whenever the chassis boots up or when a new RADIUS accounting server or RADIUS mediation-device accounting server is configured with Acct-On configuration enabled, the state of the RADIUS server will be set to Active for all the non-Admin-AAAmgr instances and will be set to "Waiting-for-response-to-Accounting-On" for only Admin-AAAmgr instance. The Accounting-On transaction logic still holds good from Admin-AAAmgr perspective. However, when any new RADIUS accounting messages are generated even before the state changes to Active in Admin-AAAmgr, these newly generated RADIUS accounting messages will not be queued at the server level and will be transmitted to the RADIUS server immediately.

During ICSR, even if the interface of radius nas-ip address is srp-activated, the state of the RADIUS accounting server will be set to Active in all non-Admin-AAAmgr instances and will be set to "Waiting-for-response-to-Accounting-On" in Admin-AAAmgr instance.

Note 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.

RADIUS Server State Behavior