Release Change Reference, StarOS Release 21.24

First Published: 2021-06-30

Last Modified: 2021-09-28

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

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

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

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

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

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

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

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.

About this Guide

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.

This RCR is applicable to the ASR5500, VPC-DI, and VPC-SI platforms. This RCR describes new and modified feature and behavior change information for the applicable StarOS release(s).

Conventions Used

The following tables describe the conventions used throughout this documentation.

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

Typeface Conventions	**Description**
Text represented as a `screen display`	This typeface represents displays that appear on your terminal screen, for example: `Login:`

Typeface Conventions	Description
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**

CHAPTER 1

Release 21.24 Features and Changes Quick Reference

Release 21.24 Features and Changes

Features / Behavior Changes	Applicable Product(s) / Functional Area	Release Introduced / Modified
Enhanced Event Logging	MME	21.24
GTPv2 Cause Code Change for S6b Interface	P-GW	21.24
LTE-M RAT Type Support on SAEGW, P-GW, and S-GW Services, on page 29	• P-GW • SAEGW • S-GW	21.24
Multiple Customized PCO Support, on page 47	• GGSN • P-GW	21.24
Maximum Receive Unit Configuration Support, on page 43	P-GW	21.24
S5 S8 Interface Upgrade	P-GW	21.24
SFTP Public Key Authentication Support, on page 59	All	21.24
Tethering Detection Bypass Interface ID, on page 63	P-GW	21.24.2
ULI Encoding Includes only MCC MNC information	P-GW	21.24

Features / Behavior Changes	Applicable Product(s) / Functional Area	Release Introduced / Modified
VPP Metric Enhancement	P-GW	21.24

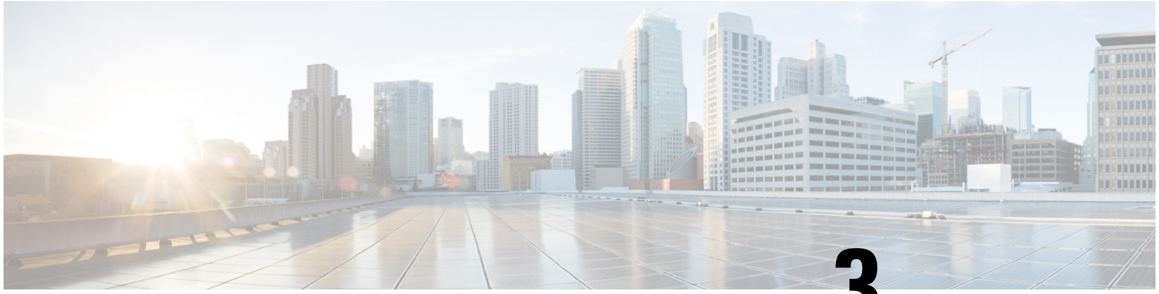
CHAPTER 2

Feature Defaults Quick Reference

Feature Defaults

The following table indicates what features are enabled or disabled by default.

Feature	Default
Enhanced Event Logging	Disabled - Configuration Required
GTPv2 Cause Code Change for S6b Interface	Disabled - Configuration Required
LTE-M RAT Type Support on SAEGW, P-GW and S-GW Services	Enabled-Always-On
Multiple Customized PCO Support	Disabled - Configuration Required
Maximum Receive Unit Configuration Support	Disabled - Configuration Required
S5 and S8 Interface Upgrade	Disabled - Configuration Required
SFTP Public Key Authentication Support	Disabled - Configuration Required
Tethering Detection Bypass Interface ID	Disabled - Configuration Required
ULI Encoding Includes only MCC MNC Information	Disabled - Configuration Required
VPP metric Enhancement	Disabled - Configuration Required



CHAPTER 3

Bulk Statistics Changes Quick Reference

This chapter identifies bulk statistics changes added to, modified for, or deprecated from the StarOS 21.24 software release.

Important For more information regarding bulk statistics identified in this section, see the latest version of the *BulkstatStatistics_document.xls* spreadsheet supplied with the release.

Bulk statistics changes for 21.24 include:

New Bulk Statistics

APN Schema

The following bulk statistics are added in the APN schema to support the LTE-M RAT type feature:

Bulk Statistics	Description
active-lte-m-sessions	The total number of active LTE-M sessions per APN with RAT type LTE-M.
initiated-lte-m-sessions	The total number of initiated LTE-M sessions.

ECS Schema

The following bulk statistics are added in the ECS schema to support the VPP metric feature:

Variables	Description
vpp-tot-flows	Indicates total number of flows through VPP.
vpp-cur-flows	Indicates total number of active current flows through VPP.

Variables	Description
IPv4	
vpp-IPv4-uplk-pkts	Indicates total number of IP packets detected in uplink direction in IPv4 traffic through VPP.
vpp-IPv4-dwnlk-pkts	Indicates total number of IP packets detected in downlink direction in IPv4 traffic through VPP.
vpp-IPv4-uplk-bytes	Indicates total number of IP bytes detected in uplink direction in IPv4 traffic through VPP.
vpp-IPv4-dwnlk-bytes	Indicates total number of IP bytes detected in downlink direction in IPv4 traffic through VPP.
vpp-IPv4-uplk-drop-pkts	Indicates the total number of dropped IP packets detected in uplink direction in IPv4 traffic through VPP.
vpp-IPv4-dwnlk-drop-pkts	Indicates the total number of dropped IP packets detected in downlink direction in IPv4 traffic through VPP.
vpp-IPv4-uplk-drop-bytes	Indicates the total number of dropped IP bytes detected in uplink direction in IPv4 traffic through VPP.
vpp-IPv4-dwnlk-drop-bytes	Indicates the total number of dropped IP bytes detected in downlink direction in IPv4 traffic through VPP.
IPv6	
vpp-IPv6-uplk-pkts	Indicates total number of IP packets detected in uplink direction in IPv6 traffic through VPP.
vpp-IPv6-dwnlk-pkts	Indicates total number of IP packets detected in downlink direction in IPv6 traffic through VPP.
vpp-IPv6-uplk-bytes	Indicates total number of IP bytes detected in uplink direction in IPv6 traffic through VPP.
vpp-IPv6-dwnlk-bytes	Indicates total number of IP bytes detected in downlink direction in IPv6 traffic through VPP.
vpp-IPv6-uplk-drop-pkts	Indicates the total number of dropped IP packets detected in uplink direction in IPv6 traffic through VPP.
vpp-IPv6-dwnlk-drop-pkts	Indicates the total number of dropped IP packets detected in downlink direction in IPv6 traffic through VPP.

Variables	Description
vpp-IPv6-uplk-drop-bytes	Indicates the total number of dropped IP bytes detected in uplink direction in IPv6 traffic through VPP.
vpp-IPv6-dwnlk-drop-bytes	Indicates the total number of dropped IP bytes detected in downlink direction in IPv6 traffic through VPP.

MME-SMS Schema

The following bulk statistic is added in the MME-SMS schema to support the SMS over SGd for EPS only feature.

Counters	Description
eps-attach-nbiot-with-sms	Indicates the total number of EPS Attach requests received for NB-IoT subscribers with SMS option.

P-GW Schema

The following bulk statistics are added in the P-GW schema to support the LTE-M RAT type feature:

Bulk Statistics	Description
sesstat-pdn-rat-lte-m	The total number of active PDN Type Statistics – LTE-M.
sessstat-rat-init-lte-m	The total number of initiated LTE-M PDNs (with RAT Type LTE-M).

S-GW Schema

The following bulk statistics are added in the S-GW schema to support the LTE-M RAT type feature:

Bulk Statistics	Description
sessstat-totcur-ue-lte-m	The total number of active UEs with LTE-M RAT type.
sessstat-totcur-pdn-lte-m	The total number of active PDNs with LTE-M RAT type.

SAEGW Schema

The following bulk statistics are added in the SAEGW schema to support the LTE-M RAT type feature:

Bulk Statistics	Description
sgw-sessstat-totcur-ue-lte-m	The total number of active UEs with LTE-M RAT type.

Bulk Statistics	Description
sgw-sessstat-totcur-pdn-lte-m	The total number of LTE-M PDNs (PGW anchored/Collapsed PDN) with RAT Type LTE-M.
pgw-sesstat-pdn-rat-lte-m	The total number of LTE-M PDNs (PGW anchored/Collapsed PDN) with RAT Type LTE-M.
pgw-sessstat-pdn-rat-init-lte-m	The total number of initiated LTE-M PDNs.
saegw-sgw-anchor-pdn-rat-lte-m	The total number of LTE-M PDNs (SGW anchored) with RAT Type LTE-M.
saegw-pgw-anchor-pdn-rat-lte-sm	The total number of LTE-M PDNs (PGW anchored) with RAT Type LTE-M.
saegw-collapsed-pdn-rat-lte-m	The total number of LTE-M PDNs (PGW anchored/Collapsed PDN) with RAT Type LTE-M.

Modified Bulk Statistics

None in this release.

Deprecated Bulk Statistics

None in this release.

CHAPTER 4

SNMP MIB Changes in StarOS 21.24

This chapter identifies SNMP MIB objects, alarms and conformance statements added to, modified for, or deprecated from the StarOS 21.24 software release.

SNMP MIB Alarm Changes for 21.24

There are no new, modified, or deprecated SNMP MIB alarm changes in this release.

SNMP MIB Conformance Changes for 21.24

There are no new, modified, or deprecated SNMP MIB Conformance changes in this release.

SNMP MIB Object Changes for 21.24

This section provides information on SNMP MIB alarm changes in release 21.24.

Important For more information regarding SNMP MIB alarms in this section, see the *SNMP MIB Reference* for this release.

New SNMP MIB Object

There is no new SNMP MIB alarm changes in this release.

Modified SNMP MIB Object

The starFanStatus is modified in this release 21.24.

Deprecated SNMP MIB Object

There are no deprecated SNMP MIB alarm changes in this release.

CHAPTER 5

Enhanced Event Logging

This chapter describes the MME's Event Logging functionality which occurs at the subscriber level, from the MME to an external server.

Feature Summary and Revision History

Summary Data

Applicable Product(s) or Functional Area	MME
Applicable Platform(s)	• ASR 5500 • VPC-DI • VPC-SI
Feature Default	Enabled- Always-on
Related Changes in This Release	Not applicable
Related Documentation	• *MME Administration Guide* • *Statistics and Counters Reference*

Revision History

Revision Details	**Release**
Customization of Attributes and Events in EDR Profile has been added.	21.24

Revision Details	Release
Customization of Attributes and Events in EDR Profile functionality has been introduced.	21.23.1
First Introduced	21.1

Feature Description

The MME handles numerous subscriber calls from different eNodeBs in the network. In order to troubleshoot any issues for a particular subscriber, the events that caused the issue is recorded. The events could be individual procedures listed below:

- Attach Procedures
- Detach Procedures
- TAU Procedures
- Handover Procedures
- All types of Service Requests
- Paging based on different triggers
- PDN Connectivity Requests
- All types of PDN detach and network initiated PDN detach procedures
- Dedicated Bearer Activation Requests
- Dedicated Bearer Deactivation Requests
- All types of Bearer modification procedures
- CSFB procedures
- SRVCC procedures
- eCSFB procedures
- eSRVCC procedures

The Event Data Record is a proprietary feature of StarOS. In this feature, MME provides a debugging framework to capture procedure level information for each subscriber. On the completion of a procedure successfully or unsuccessfully, the MME generates a procedure summary. This summary provides details of the events and issues, which is nearly comparable to real-time debugging.

Important This feature is license controlled. Please consult your Cisco Account Representative for information about the specific license.

MME supports the following functionality in this feature:

- Event Logging for 4G subscribers.

- The Event Records are stored in CSV file format.
- A framework to collect information and eventually provide log information. The framework is extensible to hold more procedures and information fields.
- The order of fields are not changeable.
- The event logs are generated on completion of the procedure successfully or unsuccessfully. The procedure could be unsuccessful because of local reasons such as – HSS/Peer element triggered reasons, Timeouts for responses, arrival of procedures and so on.
- Each record has a smgr-no and sequence-no field. If there is no guaranteed delivery of events, the sequence number will help in identifying the lost events.
- Event reporting can be enabled or disabled through the CLI command reporting-action mme-event-record under the Call Control Configuration mode. For detailed information on feature configuration see the *Configuring Event Logging* section in this feature chapter.

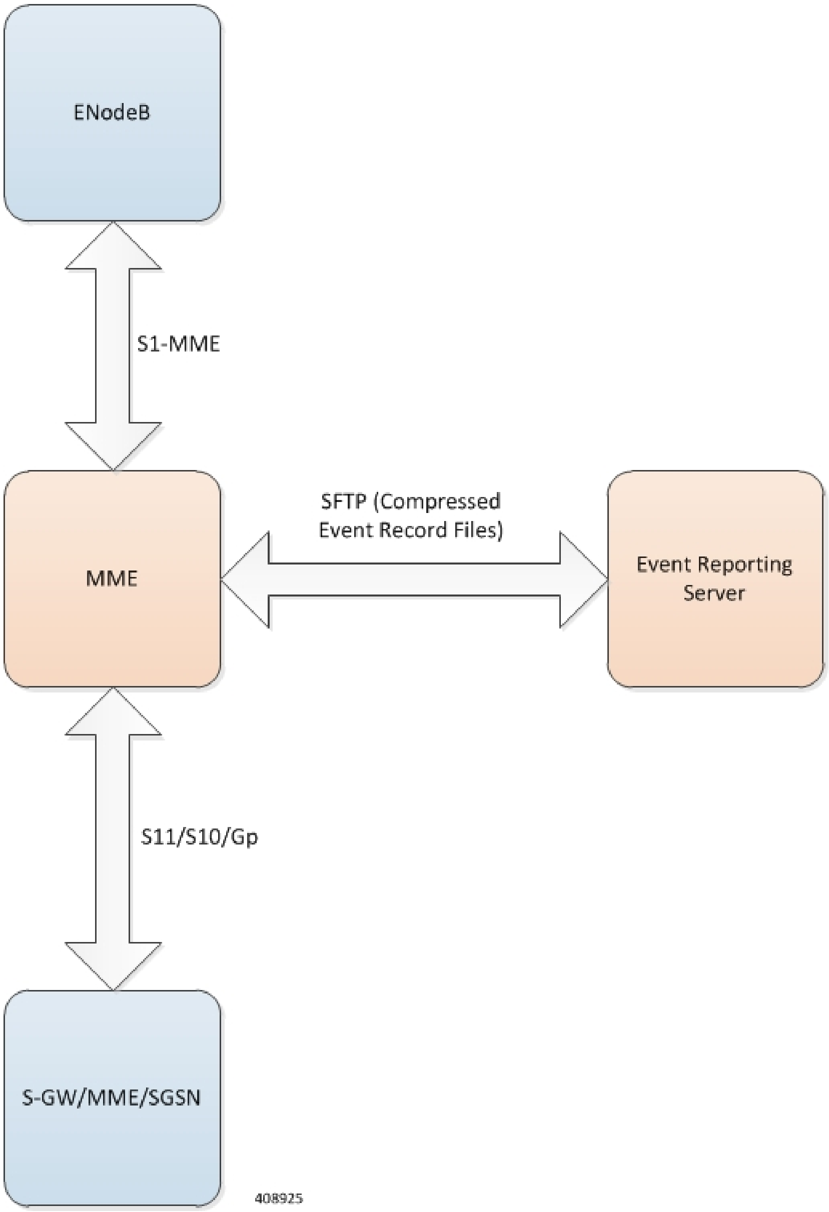
How Event Logging Works

Event Logging in the MME is implemented by providing subscriber event information to an external server. Data analyzers use the event information in the record, which is stored in the external server, to debug and troubleshoot subscriber issues.

Architecture

This section describes the framework designed in the MME to support Event Logging.

Figure 1: Event Logging - Interfaces



The interface between the MME and the external server is based on SFTP. Each record (CSV record) is generated as comma-separated ASCII values. The MME sends one ASCII formatted CSV record per line. The CSV records are stored in a file. If configured, these files can be compressed before sending it to the external server.

The transfer of CSV record files between the MME and the external server is based on either PULL or PUSH model. In case of the PULL model, the external server is responsible for initiating the SFTP with MME, and in the PUSH model, MME is responsible for sending the CSV record file to external server based on the configured PUSH timer interval.

The event report includes the information in CSV format as shown in the table given below.

Table 1: Information Fields in the EDR

Sl.No	Description	Format information	Range
1	smgr_number	Number	1 up to 1023
2	sequence_no	Number	1 up to 4294967295
3	Time	YYYY-MMM-DD+HH:MM:SS	
4	event-idenity	enum: Attach; Detach; TAU; Handover ; Service Request; Paging; PDN Connect/Disconnect; Bearer Activation/Deactivation; CSFB and SRVCC procedures.	
5	Result	enum: 0-Success; 1-failure; 2-Aborted;3-eps_only	
6	mme-address	Dotted-string	
7	Msisdn	String of decimal digits	
8	imsi	String of decimal digits	1 - 15 digits
9	Imei (sv)	String of decimal digits	14 or 16 digits
10	old-guti	mcc: mnc: mmegroup: mmecode: mtmsi	
11	old-guti-type	Enumeration [0 - native, 1 - mapped]	
12	guti	mcc: mnc: mmegroup: mmecode: mtmsi	0 up to 65535
13	Ecgi	mcc: mnc: cellid	
14	current-tac	Tac	
15	enodeB-id	20 bit value	1 - 1048574
16	disc-reason	Number	0 up to 65535
17	ebi	Number	5-15
18	linked-ebi	Number	
19	apn	String	
20	pdn-type	Number	1-4
21	ipv4-address	Dotted String	
22	ipv6-address	Dotted String	
23	pti	Number	1-255
24	qci	Number	1-9,65,66, 69,70,128-254

Sl.No	Description	Format information	Range
25	arp	Number	1-255
26	qos-change	Enum [0-No, 1-Yes]	0/1
27	lai	mcc-mnc-lac	

If a particular information is not relevant for the procedure being logged or if particular information isn't available, the corresponding field of that event record will be left blank. For example, if the IMEI is unavailable after the completion of an Attach procedure, the corresponding field of the EDR record becomes blank.

Important All enumerations will be listed by Cisco for every software release. The external server is designed to be aware of the same listing and to interpret the number accordingly. The event records contain 0-based index value of such enumerations to save space and processing overhead.

The Event IDs that are tracked as part of the EDR logging is shown in the below table:

Events	ENUM Value
Attach Procedures	
MME_EDR_EVENT_ID_EPS_ATTACH	1
MME_EDR_EVENT_ID_EMERGENCY_ATTACH	2
MME_EDR_EVENT_ID_COMBINED_ATTACH	3
MME_EDR_EVENT_ID_EPS_HO_ATTACH	4
MME_EDR_EVENT_ID_ATTACH_TYPE_MAX	
Detach Procedures	
MME_EDR_EVENT_ID_UE_INITIATED_DETACH	51
MME_EDR_EVENT_ID_NW_INITIATED_DETACH	52
MME_EDR_EVENT_ID_HSS_INITIATED_DETACH	53
MME_EDR_EVENT_ID_CSFB_UE_INIT_IMSI_DETACH	54
MME_EDR_EVENT_ID_CSFB_NW_INIT_IMSI_DETACH	55
MME_EDR_EVENT_ID_DETACH_TYPE_MAX	
TAU Procedures	
MME_EDR_EVENT_ID_TAU_SGW_RELOC	101
MME_EDR_EVENT_ID_TAU_NO_SGW_RELOC	102
MME_EDR_EVENT_ID_TAU_COMBINED_SGW_RELOC	103

Events	ENUM Value
MME_EDR_EVENT_ID_TAU_COMBINED_NO_SGW_RELOC	104
MME_EDR_EVENT_ID_TAU_PERIODIC	105
MME_EDR_EVENT_ID_TAU_ATTACH_SGW_RELOC	106
MME_EDR_EVENT_ID_TAU_ATTACH_NO_SGW_RELOC	107
MME_EDR_EVENT_ID_TAU_ATTACH_COMBINED_SGW_RELOC	108
MME_EDR_EVENT_ID_TAU_ATTACH_COMBINED_NO_SGW_RELOC	109
MME_EDR_EVENT_ID_TAU_TYPE_MAX	
Handover Procedures	
MME_EDR_EVENT_ID_S1_HO_SGW_RELOC	151
MME_EDR_EVENT_ID_S1_HO_NO_SGW_RELOC	152
MME_EDR_EVENT_ID_X2_HO_SGW_RELOC	153
MME_EDR_EVENT_ID_X2_HO_NO_SGW_RELOC	154
MME_EDR_EVENT_ID_INBOUND_S10_HO_SGW_RELOC	155
MME_EDR_EVENT_ID_INBOUND_S10_HO_NO_SGW_RELOC	156
MME_EDR_EVENT_ID_INBOUND_S3_HO_SGW_RELOC	157
MME_EDR_EVENT_ID_INBOUND_S3_HO_NO_SGW_RELOC	158
MME_EDR_EVENT_ID_INBOUND_GNGP_HO	159
MME_EDR_EVENT_ID_OUTBOUND_S10_HO	160
MME_EDR_EVENT_ID_OUTBOUND_S3_HO	161
MME_EDR_EVENT_ID_OUTBOUND_GNGP_HO	162
MME_EDR_EVENT_ID_HO_TYPE_MAX	
Service Request Procedures	
MME_EDR_EVENT_ID_SERV_REQ_UE_INITIATED	201
MME_EDR_EVENT_ID_SERV_REQ_NW_INIT_PROC	202
MME_EDR_EVENT_ID_SERV_REQ_EXTENDED	203
MME_EDR_EVENT_ID_SERV_REQ_TYPE_MAX	
Paging Procedures	
MME_EDR_EVENT_ID_PAGING_DDN_TRIGGER	251

Events	ENUM Value
MME_EDR_EVENT_ID_PAGING_DETACH_TRIGGER	252
MME_EDR_EVENT_ID_PAGING_BRR_TRIGGER	253
MME_EDR_EVENT_ID_PAGING_IDR_QUERY_TRIGGER	254
MME_EDR_EVENT_ID_PAGING_PCSCF_RESTORATION	255
MME_EDR_EVENT_ID_PAGING_UE_OFFLOAD_TRIGGER	256
MME_EDR_EVENT_ID_PAGING_SGS_TRIGGER	257
MME_EDR_EVENT_ID_PAGING_GMLC_TRIGGER	258
MME_EDR_EVENT_ID_PAGING_PGW_NODE_RESTORATION	259
MME_EDR_EVENT_ID_PAGING_S102_TRIGGER	260
MME_EDR_EVENT_ID_PAGING_IPNE_QUERY_TRIGGER	261
MME_EDR_EVENT_ID_PAGING_TYPE_MAX	
PDN Connectivity Requests	
MME_EDR_EVENT_ID_PDN_CONN_REQ	301
MME_EDR_EVENT_ID_PDN_EMERGENCY_CONN_REQ	302
MME_EDR_EVENT_ID_PDN_CONN_TYPE_MAX	
UE and Network Initiated PDN Detach	
MME_EDR_EVENT_ID_UE_PDN_DISCONN_REQ	351
MME_EDR_EVENT_ID_MME_PDN_DISCONN_REQ	352
MME_EDR_EVENT_ID_HSS_PDN_DISCONN_REQ	353
MME_EDR_EVENT_ID_NW_PDN_DISCONN_REQ	354
MME_EDR_EVENT_ID_PDN_DISCONN_TYPE_MAX	
Dedicated Bearer Activation Requests	
MME_EDR_EVENT_ID_DED_BEARER_ACT_REQ	401
MME_EDR_EVENT_ID_DED_BEARER_ACT_MAX	
Dedicated Bearer Deactivation Requests	
MME_EDR_EVENT_ID_UE_DED_BEARER_DEACT_REQ	451
MME_EDR_EVENT_ID_MME_DED_BEARER_DEACT_REQ	452
MME_EDR_EVENT_ID_PGW_DED_BEARER_DEACT_REQ	453

Events	ENUM Value
MME_EDR_EVENT_ID_DED_BEARER_DEACT_MAX	
Bearer Modification Requests	
MME_EDR_EVENT_ID_NW_BEARER_MODIF	501
MME_EDR_EVENT_ID_HSS_BEARER_MODIF	502
MME_EDR_EVENT_ID_BEARER_MODIF_TYPE_MAX	
CSFB Prodecures	
MME_EDR_EVENT_ID_CSFB_MO_CALL	551
MME_EDR_EVENT_ID_CSFB_MT_CALL	552
MME_EDR_EVENT_ID_CSFB_MO_PRIORITY_CALL	553
MME_EDR_EVENT_ID_CSFB_MT_PRIORITY_CALL	554
MME_EDR_EVENT_ID_CSFB_MO_EMERGENCY_CALL	555
MME_EDR_EVENT_ID_CSFB_MO_SMS	556
MME_EDR_EVENT_ID_CSFB_MT_SMS	557
MME_EDR_EVENT_ID_ECSFB_MO_CALL	561
MME_EDR_EVENT_ID_ECSFB_MT_CALL	562
MME_EDR_EVENT_ID_ECSFB_EMERGENCY	563
SRVCC Procedures	
MME_EDR_EVENT_ID_SRVCC_SV_CSPS	601
MME_EDR_EVENT_ID_SRVCC_SV_CS	602
MME_EDR_EVENT_ID_SRVCC_SV_NO_DTM	603
MME_EDR_EVENT_ID_SRVCC_1XRTT	604
MME_EDR_EVENT_ID_SRVCC_MAX	

The status of each event is as shown in the table given below:

Table 2: Event Status

Sl No.	Format Information	ENUM Value
1	MME_EDR_EVENT_RESULT_SUCCESS	0
2	MME_EDR_EVENT_RESULT_FAILURE	1
3	MME_EDR_EVENT_RESULT_ABORT	2

SI No.	Format Information	ENUM Value
4	MME_EDR_EVENT_RESULT_EPS_ONLY	3

Support to Add Two Additional Attributes in EDR

In the existing Event Data Record (EDR) fields, there are a total of 27 fields and currently, 2 more fields are added to the event-data-record and they are mme-ue-s1ap-id and procedure-start-time.

The event report includes the information in CSV format as shown in the table given below:

Table 3: Information Fields in the EDR

SI.No	Description	Format Information	Range
28	mme-ue-s1ap-id	Number	0 to 4294967295
29	procedure-start-time	YYYY-MMM-DD+HH:MM:SS	

Customization of Attributes and Events in EDR Profile

Feature Description

The Event Data Record (EDR) captures and provides information of each subscriber irrespective of successful or unsuccessful completion of the procedure. The output summary provides the complete details of the events and issues.

There are totally 29 attributes available in the existing EDR fields, and currently there is no option to either customize or choose the number of attributes and EDR events based on the requirement. In this feature, a new EDR-Profile is introduced to enable or disable the events and attributes. Based on the profile configuration, the generated EDR has the events configured and includes the attributes that are enabled and skips the disabled attributes.

This customization of the attributes does not alter the order sequence of the attributes that is already being followed to write into the EDR. In case, if any of the attributes are not configured or not valid/NULL during the particular procedure execution, then it can be included by using just a comma. Maximum of 32 EDR profiles can be configured and only 1 of the EDR profile could be associated per call control profile.

Previously EDR gets generated with event-id as 0 for those procedures for which EDR-Event is not mapped. Currently, EDR does not get generated for those procedures for which EDR-Event is not mapped.

In any condition, if the IMSI is not available since call-control-profile is chosen based on the IMSI, EDR customization is not applicable for such scenarios. If the EDR handle is available, EDR is generated for a list of events/attributes else EDR will not be generated.

Note The top four attributes (*smgr_instance, sequence_no, edr-time, event-Id)* cannot be customized and all the remaining attributes can be enabled and disabled based on the requirement,

Configuring EDR Profile for Set of Attributes and Events

Use the following configuration commands to configure EDR Profile for set of attributes and events:

```
configure
   edr-profile edr_profile_name
       [ no ] attribute attribute-name
       [ no ] event-group event-name
 end
```

Notes:

- **edr-profile**: Configures an EDR profile. *edr_profile_name*: Specifies an EDR Profile name. Enter a string of size 1–63.
- **attribute** : Configures the attribute to be customized.
- **event-group** : Configures the event-group to be customized.
- **no**: Enables or Disables options such as edr-profile, attribute, and event-group.

Associating EDR-Profile with Call-Control-Profile

Use the following configuration commands to associate edr-profile with call-control-profile:

```
configure
   call-control-profile profile_name
       [ remove ][ { reporting-action } { mme-event-record }[edr-profile
edr_profile_name  ) ] ]
     end
```

Show Command and Output

show edr-profile all | full | name

The output of this command displays the configuration of edr profile for all the attributes and event-groups:

1. Attributes-The output displays the following list of attributes enabled or disabled under edr-profile:
2. Event-group-The output displays the following list of events enabled or disabled under edr-profile:

Note By default, all attributes and event-groups are enabled. It can be enabled and disabled based on the requirement.

```
Edr Profile Name : test
Attribute :
result : Enabled
mme-address : Enabled
msisdn : Enabled
imsi : Enabled
imei (sv) : Enabled
old-guti : Enabled
old-guti-type : Enabled
guti : Enabled
ecgi : Enabled
```

```
current-tac : Enabled
enodeb-id : Enabled
disc-reason : Enabled
ebi : Enabled
linked-ebi : Enabled
apn : Enabled
pdn-type : Enabled
ipv4-address : Enabled
ipv6-address : Enabled
pti : Enabled
qci : Enabled
arp : Enabled
qos-change : Enabled
lai : Enabled
proc-start-time : Enabled
mme-ue-s1ap-id : Enabled
all : Enabled

Event-group :
attach : Enabled
detach : Enabled
tau : Enabled
handover : Enabled
service-request : Enabled
paging : Enabled
pdn-connect : Enabled
pdn-disconnect : Enabled
bearer-act-request : Enabled
bearer-deact-request : Enabled
bearer-mod-request : Enabled
csfb : Enabled
srvcc : Enabled
all : Enabled
```

show call-control-profile full name

The output of this command displays the configuration of call-controle-profile for the newly introduced attributes:

Note Ensure that the EDR profile is created before associating it to the call-control-profile. If a non-existent edr-profile is associated to the call-control-profile then edr customization is not applicable.

- Edr Profile: Displays configuration for Edr Profile.
- edr-profile-name/Not Defined: The output of this command displays the associated edr-profile name if configured else it will display as Not Defined.

Limitations

The reliability of event generation is limited by the CDRMOD framework – particularly in the following ways:

- Any reboot of the chassis, will result in loss of records that are not yet flushed to the hard-disk or an external server
- In case of overload of the CDRMOD, the SESSMGR ignores event records if the queue is full.

- EDR sequence numbers are within the scope of the Session Manager. If a different Session Manager is selected, the EDR sequence number may reset or continue from the last sequence number allocated in that Session Manager.
- The statistics are key parameters for logging EDRs, if the statistics have any discrepancies the EDRs are not generated. Listed below are some scenarios where the EDRs are not generated due to discrepancies in statistics:
  - Network or MME initiated dedicated bearer de-activation during SRVCC procedures.
  - HSS initiated modification failures.
  - HSS initiated PDN disconnect failures.
- Currently, MME does not support the event record generation based on the call-control-profile. You can enable the event record generation similarly as enabling at mme-service. You can enable for all subscribers at mme-service or at call control profile. However, the call control profile allows you to enable for all subscribers and not for specific subscribers.

Relationship with Other Products

The SGSN has a similar function, GMM-SM Event Logging. For information about this functionality refer to the *SGSN Administration Guide.*

Configuring Event Logging

The following configurations are discussed in this section for Event Data Records (EDRs):

Enabling Event Logging

The following CLI configuration is executed in the Call Control Profile mode to enable Event Logging on the MME.

```
config
 call-control-profile profile_name
 reporting-action mme-event-record  edr-profile  edr-profile-name
          exit
```

Notes:

- The call-control-profile configuration enables Event Logging for MME, provided this profile is associated to the **mme-service** through operator policy and subscriber map.
- **reporting-action** enables procedure reports.
- **mme-event-record** reports MME procedures in the form of event records using CDRMOD.
- **reporting-action mme-event-record edr-profile edr-profile-name**: Associates an edr-profile in a call-control-profile.

.

Enabling EDR Logs

The CDRMOD proclet writes the individual records into a single file received from several session managers. The CDRMOD proclet is enabled with the configuration below.

```
config
 context context_name
 edr-module active-charging-service reporting
                    cdr { push-interval interval_time | remove-file-transfer
| use-harddisk | transfer-mode { pull | push primary { encrypted-url |
url } url [ secondary { encrypted-secondary | secondary-url } url_ ]  } [
module-only ] }
                 end
```

Configuring File Parameters

File parameters can be configured using the configuration given below.

```
config
 context context_name
 session-event-module
                 file name file_name current-prefix current_file_prefix rotation
 volume file_rotation_size rotation time file_rotation_time  field-separator
underscore sequence-number padded charging-service-name include compression
 gzip }
                end
```

EDR Profile Association

The Call Control Profile configuration enables event Logging for MME, provided the EDR profile is associated to the MME-Service through Operator Policy and Subscriber Map (LTE-Policy).

```
config
   operator-policy name  policy_name
      associate call-control-profile call_control_profile_name
          exit
lte-policy
    subscriber-map map_name
      precedence precedence_value match-criteria all operator-policy-name
policy_name
           exit
        exit
context context_name
   mme-service service_name
      associate subscriber-map map_name
         end
```

Verifying the Event Logging Configuration

The following commands are used to verify the parameters for Event Logging.

- **show call-control-profile full all**

- **show operator-policy full all**
- **show lte-policy subscriber-map name sub1**
- **show mme-service all**

Monitoring and Troubleshooting Event Logging

This section provides information on how to monitor Event Logging.

Event Logging Show Command(s) and/or Outputs

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

The show commands in this section are available in support of the Event Logging.

show call-control-profile full all

```
Call Control Profile Name = TEST
SAMOG Home PLMN                         : Not configured
Accounting Mode (SGW/SaMOG)             : None
Accounting stop-trigger (SGW)           : Not configured
Accounting Policy (SaMOG)               : Not configured
Event Data Records (MME)                : Enabled
```

show edr-profile full all

Following example is the show output of edr-profile.

```
Tuesday April 27 02:06:11 EDT 2021

Edr Profile Name : edr1
***** Attribute *****
result : Enabled
mme-address : Enabled
msisdn : Enabled
imsi : Enabled
imei (sv) : Enabled
old-guti : Enabled
old-guti-type : Enabled
guti : Enabled
ecgi : Enabled
current-tac : Enabled
enodeb-id : Enabled
disc-reason : Enabled
ebi : Enabled
linked-ebi : Enabled
apn : Enabled
pdn-type : Enabled
ipv4-address : Enabled
ipv6-address : Enabled
pti : Enabled
qci : Enabled
arp : Enabled
qos-change : Enabled
lai : Enabled
procedure-start-time : Enabled
mme-ue-s1ap-id : Enabled
all : Enabled
```

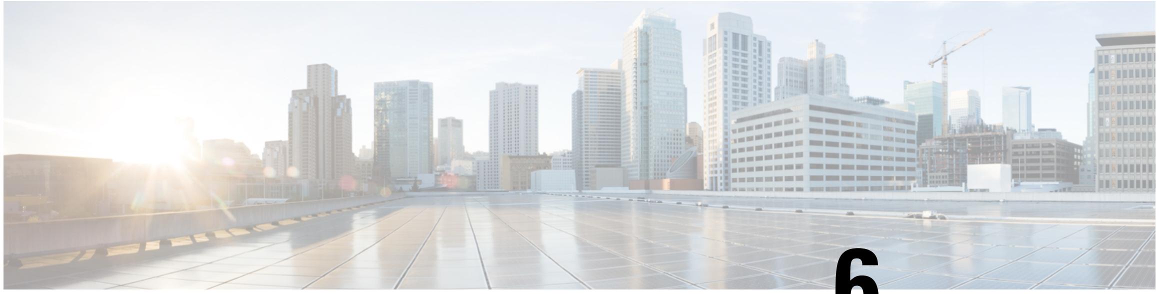
```
***** Event-group *****
attach : Enabled
detach : Enabled
tau : Enabled
handover : Enabled
service-request : Enabled
paging : Enabled
pdn-connect : Enabled
pdn-disconnect : Enabled
bearer-act-request : Enabled
bearer-deact-request : Enabled
bearer-mod-request : Enabled
csfb : Enabled
srvcc : Enabled
all : Enabled
[ingress]asr5500#
```

show cdr statistics

On running the above command , the following statistics are displayed:

```
EDR-UDR file Statistics:
CDRMOD Instance Id: 2
    Overall Statistics:
      Files rotated:
          30
      Files rotated due to volume limit:                                          0
      Files rotated due to time limit:                                              3
      Files rotated due to tariff-time:                                            0
      Files rotated due to records limit:                                    11
      File rotation failures:
   0
      Files deleted:
            7
      Records deleted:
          0
      Records received:
 23754
      Current open files:
       0

Time of last file deletion:                              Sunday November 08 23:32:53 EST
2015
Session-Event Record Specific Statistics:
Session-Event files rotated:                                                        30
Session-Event files rotated due to volume limit:                  0
Session-Event files rotated due to time limit:                      3
Session-Event files rotated due to tariff-time:                    0
Session-Event files rotated due to records limit:              11
    Session-Event file rotation failures:                                    0
    Session-Event files deleted:                                                      7
    Session-Event records deleted:                                                  0
    Session-Event records received:                                        23754
    Current open Session-Event files:                                            0
Time of last Event file deletion:                Sunday November 08 23:32:53 EST 2015
```



CHAPTER 6

GTPv2 Cause Code Change for S6b Interface

Feature Summary and Revision History

Summary Data

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

Revision History

Revision Details	Release
First introduced.	21.24

Feature Description

When the S6b service is unreachable or connections are unstable while sending the Create Session Response, the S6b interface modifies the existing GTPv2 cause code 92/0x5C (user authentication failed) to cause code 73/0x49 (no resources available).

Configuring S6b Retry Code

Use the following configuration to apply S6b retry code from Diameter:

```
configure
   context context_name
      pgw-service service_name
         egtp { reject-cause { no-resource [ s6b-link-failure ] { 
s6b-retry-code } }
         [ no | default ] egtp reject-cause no-resource
         end
```

NOTES:

- **reject-cause**: Configures options for handling response with reject-cause.
- **no-resource**: Configures handling for Create Session Response with cause code no-resource.
- **s6b-link-failure**: Responds with no-resource for S6b server unreachability during authentication.
- **s6b-retry-code**: Responds with no-resource for S6b diameter result-codes—3002, 3004, 3005 and 5198.

Monitoring and Troubleshooting

This section provides information regarding show commands and/or their outputs.

Show Command and Output

show pgw-service name <pgw_service_name>

The output of this command is enhanced to include the following fields. These fields indicate whether EGTP-C cause code mapping for S6b Link Failure and S6b Retry Code is enabled or disabled.

- EGTP-C Cause Code Mapping (S6b Link Failure) : Enabled or Disabled
- EGTP-C Cause Code Mapping (S6b Retry Code) : Enabled or Disabled

CHAPTER 7

LTE-M RAT Type Support on SAEGW, P-GW, and S-GW Services

Feature Summary and Revision History

Summary Data

Applicable Product(s) or Functional Area	• S-GW • P-GW • SAEGW
Applicable Platform(s)	• ASR 5500 • VPC-DI • VPC-SI
Default Setting	Enabled-Always-On
Related Changes in This Release	Not Applicable
Related Documentation	• *Command Line Interface Reference* • *P-GW Administration Guide* • *S-GW Administration Guide* • *SAEGW Administartion Guide*

Revision History

Revision Details	Release
First introduced.	21.24

Feature Description

LTE-M (LTE-MTC low-power-wide area (LPWA)) is a new cellular radio access technology specified by 3GPP that addresses low power-wide area connectivity solutions. It specifically refers to a specific category of LTE UEs that are suitable for IoT LTE-M, which supports IoT through lower device complexity and provides extended coverage, while allowing the reuse of the LTE installed base.

The RAT type IE is present in various call flows across many interfaces. When a Create Session Request is received with an unknown RAT Type, as the RAT Type is a Mandatory IE in this message, S-GW or P-GW may reject a create session request. In this StarOS 21.24 release, LTE-M RAT (Radio Access Technology) type for S-GW, P-GW, and SAEGW products are supported.

The RAT type is present either as an IE (for example, in GTPv2-C, GTPP), AVP (on Diameter-based interfaces) or as an attribute (for example in EDRs) across many interfaces.

The LTE-M solution for S-GW, P-GW, and SAEGW supports the following new LTE-M RAT type attribute value in the following Interfaces protocols and dictionaries:

- GX-interface: Diameter Protocol
- GY-interface: Diameter Protocol
- GZ/RF- interface: GTPP/Diameter/Radius
- S6B- Interface: Diameter Protocol
- S11/ S5/S8-Interface: GTPv2-C
- Dictionaries Radius AVPs, and dictionaries.
- Rf interface for CDR generation
- Attributes in EDRs

Enhancements to the Existing Features

The following existing features are enhanced to support the new RAT-TYPE LTE-M.

- **Virtual APN Selection Based on RAT Type**: Virtual APNs allow differentiated services within a single APN. The Virtual APN feature allows a carrier to use a single APN to configure differentiated services. The APN that is supplied by the MME is evaluated by the P-GW with multiple configurable parameters. Then, the P-GW selects an APN configuration based on the supplied APN and those configurable parameters. APN configuration dictates all aspects of a session at the P-GW, where different policies imply different APNs.

  You can select the virtual APN by configuring directly under the base APN. This APN selection is done based on RAT Types. In this release, support is added through CLI to select the virtual APN for the LTE-M RAT type.

- **Qci and Qos Mapping**: P-GW supports QCI and QoS mapping association with APN based on RAT type LTE-M. This QCI and QoS mapping allow you to perform quick actions on the QoS Class Index (QCI) to QoS Mapping Configuration Mode, which is used to map QoS Class Indexes to enforceable QoS parameters. Mapping can occur in Serving Gateway (S-GW), and/or the PDN Gateway (P-GW) in an LTE network.
- **PCRF-based Handling**: P-GW informs the RAT type changes to PCRF through Credit Control Request -Initial and Updated messages, and PCRF provides a new PCC rule. Allows you to create a Bearer by enforcing a new Policy and Charging Control (PCC) rule from Policy and Charging Rules Function (PCRF).

How it Works

Architecture

The following table specifies the field and its value for various interfaces with support of LTE-M RAT type. Only Standard dictionaries and customized dictionaries are modified.

Table 4:

Interface	Field	AVP Attribute	Messages
P-GW Product			
Gx	RAT-Type (1032) Diameter	LTE-M (1007)	• Credit Control Request-Initial • Credit Control Request - Updated
Gy	3GPP RAT-Type (21) Diameter	LTE-M (9)	• Credit Control Request-Initial • Credit Control Request - Updated
RADIUS	3GPP RAT-Type (21)	LTE-M (9)	• Accounting Request -Start • Accounting Request-Stop • Account request -Interim

Interface	Field	AVP Attribute	Messages
Rf	3GPP RAT-Type (21) Diameter	LTE-M (9)	• Accounting Request -Start • Accounting Request- Stop • Account request -Interim
S6b	3GPP RAT-Type (1032) Diameter	LTE-M (9)	• Authentication • Authorisation • Request
EDRs	RAT-Type	LTE-M (9)	-
PGW CDRS	RAT-Type (30) GTPP	LTE-M (9)	• Gtpp Data Record • Transfer Request
S-GW Product			
SGWCDRs	RAT-Type (30)	LTE-M (9)	• Gtpp Data Record • Transfer Request

Limitations

Following are the known limitations for new LTE-M RAT type feature:

- Rule matching at ECS
- Ruledef matching at Local-Policy

Supported Standards

Cisco's implementation of the LTE RAT type complies with the following standards:

- 3GPP 23.401 – eGPTC Interface
- 3GPP 29.274 Release 15.4.0 – 3GPP GTPv2 Protocol Specification Reference table for LTE-M Rat type support; RAT Type IE details are given in the following table for egtpc IEs encoding and decoding :
    - Table 7.2.1-1: Information Elements in a Create Session Request
    - Table 7.2.7-1: Information Elements in a Modify Bearer Request
    - Table 7.2.7-1: Information Elements in a Modify Bearer Request

- 3GPP 23.401 Release 15.4.0 – 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; General Packet Radio Service (GPRS) enhancements for Evolved Universal Terrestrial Radio Access Network (E-UTRAN) access
- 3GPP 32.299 Release 15.4.0 – 3rd Generation Partnership Project; Technical Specification Group Core Network and Terminals; Policy and Charging Control (PCC).
- 3GPP 29.060 – 3rd Generation Partnership Project; Technical Specification Group Core Network and Terminals; General Packet Radio Service (GPRS); GPRS Tunnelling Protocol (GTP) across the Gn and Gp interface.
- 3GPP 29.061 – 3rd Generation Partnership Project; Technical Specification Group Core Network and Terminals; Interworking between the Public Land Mobile Network (PLMN) supporting packet based services and Packet Data Networks (PDN)
- 3GPP 32.298 – 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Telecommunication management; Charging management; Charging Data Record (CDR) parameter description
- 3GPP 29.212 Release 15.4.0 – 3rd Generation Partnership Project; Technical Specification Group Core Network and Terminals; Policy and Charging Control (PCC).

Configuring Virtual-APN

Use the following configuration to display an additional option (LTE-M) “RAT-Type” based Virtual-APN selection .

```
configure
   context  context_name
      apn  apn_name
          virtual-apn  preference  value apn  apn_name rat-type lte-m
          end
```

NOTES:

- **apn** *apn_name*: Allows to specify the APN name as a condition. *apn_name* must be an alphanumeric string of 1 through 63 characters.
- **virtual-apn preference** *value* **apn** *apn_name* : Configures the virtual-apn (virtual.ipv4).
- **rat-type lte-m**: Enables LTE-M as an additional RAT-type.

Configuring qci-qos-mapping

Use the following configuration to configure QCI-QOS mapping in the APN Configuration mode and associate additional RAT type (LTE-M).

```
configure
   context  context_name
      apn  apn_name
         qci table
          qci-qos-mapping
```

```
              qci qci_val non-gbr { downlink  user-datagram dscp-marking value
 }
              end
```

NOTES:

- **apn** *apn_name*: Allows to specify the APN name as a condition. *apn_name* must be an alphanumeric string of 1 through 63 characters.
- **qci-qos-mapping**: Configures the qci-qos-mapping for APN.
- **qci** *qci_val*: Specifies the QoS Class Identifier. *qci_val* must be an integer between 1 to 9, 80, 82, and 83.
    - **downlink**: Specifies the direction of traffic on which this QoS configuration needs to be applied.

Associate Qci-Qos-Mapping

Use the configuration to select the qci-qos-mapping RAT Type.

```
configure
   context  context_name
      apn  apn_name
         associate  qci-qos-mapping table rat-type lte-m
         end
```

NOTES:

- **associate qci-qos-mapping table rat-type lte-m** : Associates apn qci-qos-mapping based on the RAT type.

Monitoring and Troubleshooting

This section provides information regarding commands available to monitor and troubleshoot the LTE-M RAT Type support on the SAEGW, P-GW and S-GW Services.

Show Commands and Output

This section provides information on show commands and their corresponding outputs for the LTE-M RAT type feature.

show apn name

The following output is displayed if the Virtual-APN is selected based on the RAT-Type, during the Session-Setup.

Output:

```
show apn name <>
Virtual APN Configuration:
  Preference  Selected-APN           Rule-Definition
  10          verizon.ipv4           CC Profile Index = 3
   RAT Type = lte-m [local]qvpc-si# show configuration
```

show apn all

The output of **show apn all** and **show apn name** *apn_name* **all** commands has been enhanced to monitor the APN configuration for qci-qos-mapping on RAT type **lte-m**:

Example:

```
show apn name <>
qci-qos-mapping Name for RAT-Type:
GERAN :N/A            UTRAN :N/A
EUTRAN : N/A          LTE-M : table
Stats Profile Name : N/A
```

show qci-qos-mapping table all

Following example is the sample output before associating the qci-qos-mapping table based on additional RAT Type (LTE-M).

```
QCI-QOS Table Name: table

 Qci:  1
  uplink: n/a
  downlink: user-datagram           dscp-marking 0x3e
  maximum packet delay:  n/a         maximum error rate:  n/a
  delay class:  n/a            precedence class:     n/a
  reliability class:  n/a            qci type:   non-gbr
  volte:   n/a                       traffic policing interval:  n/a

 Qci:  2
  uplink: n/a
  downlink: internal-qos priority 1
  maximum packet delay:  n/a         maximum error rate:  n/a
  delay class:     n/a               precedence class:  n/a
  reliability class:     n/a         qci type:   gbr
  volte:     n/a                     traffic policing interval:  n/a
```

show configuration

The **virtual-apn preference** *value* **apn** *apn_name* **rat-type lte-m** output is displayed when the Virtual APN is configured with the LTE-M RAT type. Following is the sample output:

```
[local]qvpc-si# show configuration
apn intershat
      pdp-type ipv4 ipv6
      bearer-control-mode mixed
      selection-mode subscribed sent-by-ms chosen-by-sgsn
      accounting-mode radius
      ims-auth-service ims-ggsn-auth
      ip access-group acl4-1 in
      ip access-group acl4-1 out
      authentication pap 1 chap 2 allow-noauth
      ip context-name egress
      virtual-apn preference 10 apn verizon.ipv4 rat-type lte-m
      ipv6 access-group acl6-1 in
      ipv6 access-group acl6-1 out
      active-charging rulebase prepaid
    exit
```

Similarly, the **associate qci-qos-mapping table rat-type lte-m** output is displayed for the qci-qos association changes based on RAT type. Following is the sample output

```
 [local]laas-setup# show configuration
                 apn intershat
                 context ingress
                subscriber default
                 nexthop-forwarding-address
                 exit
                 apn intershat
                 associate qci-qos-mapping table rat-type lte-m
                 exit
```

show subscribers full

The output of this show command is used for monitoring the subscriber call. The RAT type of the call is displayed as LTE-M. A new field **LTE-M** is added under Access Technology. Following is the sample output:

```
[local]laas-setup# show subscribers all
Access  (X) - CDMA 1xRTT                (E) - GPRS GERAN    (I) - IP
||    Tech:       (D) - CDMA EV-DO      (U) - WCDMA UTRAN   (W) - Wireless LAN
||                (A) - CDMA EV-DO REVA (G) - GPRS Other    (M) - WiMax
||                (C) - CDMA Other      (J) - GAN           (O) - Femto IPSec
||                (P) - PDIF            (S) - HSPA          (L) - eHRPD
||                (T) - eUTRAN          (B) - PPPoE         (F) - FEMTO UTRAN
||                (N) - NB-IoT          (Q) - WSG           (R)- LTE-M
                  (.) - Other/Unknown
```

show subcscribers full all

The output of the following show commands are used for monitoring the subscriber call. The Access Technology of the call is displayed as LTE-M.

```
Username: 9890098900           Status: Online/Active
  Access Type: sgw-pdn-type-ipv4-ipv6    Network Type: IPV4+IPv6
  Access Tech: LTE-M                     Access Network Peer ID: n/a
  callid: 02fb3ea1                       msid: 404005123456789
  Card/Cpu: 1/0                          Sessmgr Instance: 11
  state: Connected
  connect time: Tue Mar 23 04:33:55 2021 call duration: 00h00m46s
  idle time: 00h00m40s                idle time left:  n/a
```

show subs pgw-only full / show subs pgw-only full all

The **show subs pgw-only full** / **show subs pgw-only full all** commands display the Access Technology of the call as LTE-M. Following is the sample output:

```
Access Type: gtp-pdn-type-ipv4-ipv6    Network Type: IPV4+IPv6
  Access Tech: LTE-M                   pgw-service-name: PGW21
  Callid: 02fb3ea2                     IMSI: 404005123456789
  MSISDN: 9890098900                   External ID: n/a
  Interface Type: S5S8GTP              Low Access Priority: N/A
  TWAN Mode: N/A
  eMPS Bearer: No
  Emergency Bearer Type: N/A
  IMS-media Bearer: No
  S6b Auth Status: N/A
```

show subs sgw-only full / show subs sgw-only full all

The **show subs sgw-only full** / **show subs sgw-only full all** scommands display the Access Technology of the call as LTE-M. Following is the sample output:

```
 Card/Cpu        : 1/0         Sessmgr Instance : 11
  Idle time       : 00h05m47s
  MS TimeZone     : n/a                 Daylight Saving Time: n/a

  Access Type: sgw-pdn-type-ipv4-ipv6    Network Type: IPV4+IPv6
  Access Tech: LTE-M                           sgw-service-name: SGW21
  Callid: 02fb3ea1                       IMSI: 404005123456789
  MSISDN: 9890098900
  eMPS Bearer: No
```

show subs saegw-only full / show subs saegw-only full all

The **show subs saegw-only full** / **show subs saegw-only full all** commands display the Access Technology of the call as LTE-M. Following is the sample output:

```
 Callid   : 02fb3ea3                   IMSI                : 404005123456789
  Card/Cpu          : 1/0                        Sessmgr Instance    : 11
  Source context    : EPC2                       Destination context : ISP1
  Bearer Type       : Default                    Bearer-Id           : 5
  Access Type       : gtp-pdn-type-ipv4-ipv6     Network Type        : IPV4+IPv6
  Access Tech       : LTE-M                      saegw-service-name  : SAEGW21
  MSISDN            : 9890098900                 External ID         : n/a
  TWAN Mode         : N/A
  eMPS Bearer       : No
  WPS Bearer        : No
```

show subs pgw-only all

The **show subs pgw-only all** command displays the following output:.

```
|+------Access    (U) - UTRAN     (G) - GERAN
||      Tech:     (W) - WLAN                (J) - GAN
||                (U) - HSPA Evolution      (E) - eUTRAN
||                (H) - eHRPD               (.) - Unknown
||                (N) - NB-IoT              (R) - LTE-M
```

show subs sgw-only all

The **show subs sgw-only all** command displays the following output:

```
|+----Access   (U) - UTRAN  (G) - GERAN          (W) - WLAN
||    Tech:    (J) - GAN              (S) - HSPA Evolution  (E) - eUTRAN
||             (.) - Unknown          (N) - NB-IoT          (R) - LTE-M

||
```

show subs saegw-only all

The **show subs saegw-only all** command displays the following output:

```
|+----Access   (U) - UTRAN  (G) - GERAN          (W) - WLAN
||    Tech:    (J) - GAN              (S) - HSPA Evolution  (E) - eUTRAN
||             (H) - eHRPD            (.) - Unknown         (N) - NB-IoT
||             (R) - LTE-M
```

show subscribers callid

The **show subscribers callid** *callid*command displays the Access Technology of the call as LTE-M. Following is the sample output:

```
|+----Access  (X) - CDMA 1xRTT(E) - GPRS GERAN      (I) - IP
||    Tech:   (D) - CDMA EV-DO          (U) - WCDMA UTRAN     (W) - Wireless LAN
||            (A) - CDMA EV-DO REVA     (G) - GPRS Other      (M) - WiMax
||            (C) - CDMA Other          (J) - GAN             (O) - Femto IPSec
||            (P) - PDIF                (S) - HSPA            (L) - eHRPD
||            (T) - eUTRAN              (B) - PPPoE           (F) - FEMTO UTRAN
||            (N) - NB-IoT              (Q) - WSG             (R) - LTE-M

||            (.) - Other/Unknown
```

show session subsystem

The following output displays the session related statistics:

```
LTE-M Data Statistics
       0 Total Sessions                  0 Total calls arrived
       0 Total calls connected           0 Total calls disconnected
NB-IoT Connection Statistics
       0 Total Sessions                  0 Total calls arrived
       0 Total calls connected           0 Total calls disconnected
LTE-M Connection Statistics
       0 Total Sessions                  0 Total calls arrived
       0 Total calls connected           0 Total calls disconnected
```

Similarly, the **show session subsystem full** is enhanced to display the Data packets and subscribers count per RAT type.

show session subsystem verbose

The **show session subsystem verbose** command displays the following output:

```
NB-IoT Data Statistics
             packets to User:             0    octets to User:   0
             packets from User:           0    octets from User: 0

LTE-M Data Statistics
             packets to User:             0    octets to User:   0
             packets from User:           0    octets from User: 0

 NB-IoT Connection Statistics
       0 Total Sessions                  0 Total calls arrived
       0 Total calls connected           0 Total calls disconnected
 LTE-M Connection Statistics
       0 Total Sessions                  0 Total calls arrived
       0 Total calls connected           0 Total calls disconnected
```

show session summary

The **show session summary** command displays the following output:

```
4G LTE (EUTRAN): 0
2G (GERAN): 0
3G (UTRAN): 0
WiFi (WIRELSS LAN): 0
eHRPD: 0
3G HA: 0
NB-IoT: 2
LTE-M: 0
Others: 0
```

show subscribers subscription full

The **show subscribers subscription full** command displays the following output:

```
Username: 9890098900           Status: Online/Active
  Access Type: sgw-pdn-type-ipv4-ipv6    Network Type: IPV4+IPv6
  Access Tech: LTE-M                     Access Network Peer ID: n/a
  callid: 02fb3ea1                       msid: 404005123456789
  Card/Cpu: 1/0                          Sessmgr Instance: 11
  state: Connected
  connect time: Wed Mar 17 09:59:47 2021 call duration: 00h01m19s
  idle time: 00h01m13s                idle time left:  n/a
  session time left:  n/a
```

show subscribers activity all

The **show subscribers activity all** command displays the Access Technology of the call as LTE-M. Following is the sample output:

```
Username: 9890098900           Status: Online/Active
  Access Type: sgw-pdn-type-ipv4-ipv6    Network Type: IPV4+IPv6
  Access Tech: LTE-M                     Access Network Peer ID: n/a
  callid: 02fb3ea1                       msid: 404005123456789
```

show apn statistics all-name

The show output command displays the statistics per APN and also displays number of initiated sessions and active sessions with LTE-M RAT Type per APN. Following is the sample output:

```
Initiated Sessions per RAT Type:
    EUTRAN:  0    UTRAN:   0
    GERAN:   0    EHRPD:   0
    S2A GTP: 0    S2B GTP: 0
    S2B PMIP:0    NB-IoT:  0
    LTE-M :  0

  Active Sessions per RAT Type:
   EUTRAN: 0   UTRAN: 0
   GERAN:  0   WLAN:  0
   HSPA:   0   NB-IoT:0
   LTE-M:  0   OTHER: 0
```

show saegw-service statistics all-name

The show output command displays the statistics per SAEGW service and also displays Current subscribers, the Current PDNs with NB-IoT RAT Type per SAEGW Service. Following is the sample output:

```
Current Subscribers By RAT-Type:
  EUTRAN:                              0    UTRAN:                           0
  GERAN:                               0    NB-IoT:                          0
  LTE-M:                               0    OTHER:                           0

Current PDNs By RAT-Type:
    EUTRAN:                            0    UTRAN:                          0
    GERAN:                             0    NB-IoT:                         0
    LTE-M:                             0    OTHER:                          0
```

show pgw-service statistics all-name

The show output command displays statistics for each P-GW Services, the number of initiated PDNs, and current PDNs with NB-IoT RAT Type for each P-GW Services. Following is the sample output:

```
Initiated PDNs By RAT-Type:
  EUTRAN:                              0    UTRAN:                            0
  GERAN:                               0    EHRPD:                            0
  S2A GTP:                             0    S2B GTP:                          0
  S2B PMIP:                            0    NB-IoT:                            0
  LTE-M                          0

Current PDNs By RAT-Type:
  EUTRAN:                              0    UTRAN:                             0
  GERAN:                               0    WLAN:                              0
  NB-IoT:                              0    LTE-M                              0
  OTHER:                               0
```

show sgw-service statistics

This show command displays statistics for each S-GW Services. This CLI is enhanced to display Current Subscribers and Current PDNs with NB-IoT RAT type for each S-GW Services. Following is the sample output:

```
Current Subscribers By RAT-Type:
  EUTRAN:                              0    UTRAN:                             0
  GERAN:                               0    NB-IoT:                            0
  LTE-M:                               0    OTHER:                             0
Current PDNs By RAT-Type:
    EUTRAN:                            0    UTRAN:                             0
    GERAN:                             0    NB-IoT:                            0
    LTE-M:                             0    OTHER:                             0
```

Bulk Statistics

The following statistics are added in support of the LTE-M RAT type feature

APN Schema

The following LTE-M RAT type feature-related bulk statistics are available in the APN schema.

Bulk Statistics	Description
active-lte-m-sessions	The total number of active LTE-M sessions per APN with RAT type LTE-M.
initiated-lte-m-sessions	The total number of initiated LTE-M sessions.

P-GW Schema

The following LTE-M RAT type feature related bulk statistics available in the P-GW schema.

Bulk Statistics	Description
sesstat-pdn-rat-lte-m	The total number of active PDN Type Statistics – LTE-M.
sessstat-rat-init-lte-m	The total number of initiated LTE-M PDNs (with RAT Type LTE-M).

S-GW Schema

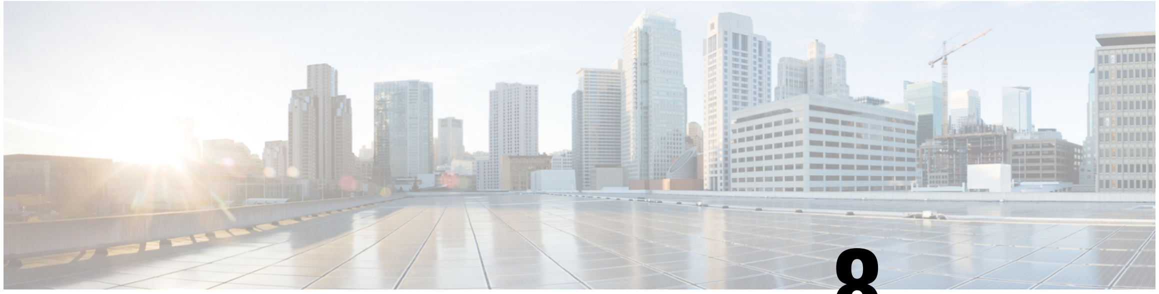
The following LTE-M RAT type feature related bulk statistics available in the S-GW schema.

Bulk Statistics	Description
sessstat-totcur-ue-lte-m	The total number of active UEs with LTE-M RAT type.
sessstat-totcur-pdn-lte-m	The total number of active PDNs with LTE-M RAT type.

SAEGW Schema

The following LTE-M RAT type feature related bulk statistics available in the SAE-GW schema.

Bulk Statistics	Description
sgw-sessstat-totcur-ue-lte-m	The total number of active UEs with LTE-M RAT type.
sgw-sessstat-totcur-pdn-lte-m	The total number of LTE-M PDNs (PGW anchored/Collapsed PDN) with RAT Type LTE-M.
pgw-sesstat-pdn-rat-lte-m	The total number of LTE-M PDNs (PGW anchored/Collapsed PDN) with RAT Type LTE-M.
pgw-sessstat-pdn-rat-init-lte-m	The total number of initiated LTE-M PDNs.
saegw-sgw-anchor-pdn-rat-lte-m	The total number of LTE-M PDNs (SGW anchored) with RAT Type LTE-M.
saegw-pgw-anchor-pdn-rat-lte-sm	The total number of LTE-M PDNs (PGW anchored) with RAT Type LTE-M.
saegw-collapsed-pdn-rat-lte-m	The total number of LTE-M PDNs (PGW anchored/Collapsed PDN) with RAT Type LTE-M.



CHAPTER 8

Maximum Receive Unit Configuration Support

Feature Summary and Revision History

Summary Data

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

Revision History

Revision Details	**Release**
First introduced.	21.24

Feature Description

Prior to MRU Configuration support, the Maximum Receive Unit (MRU) setting was equal to the Maximum Transmission Unit (MTU).

When the MTU of eNB on the S1-U interface was increased to 2000 bytes but no changes were made on the MTU on S1-U interface on SAE-GW, packets were received at SAE-GW with size more than 1500 bytes. This resulted into those packets getting dropped at the S1-U interface on the SAE-GW with **Lport_MRU_exceeded** exception. This was affecting UEs that were trying to set up IKE Tunnels.

This Configure MRU feature allows you to configure MRU separately from MTU.

How It Works

To handle MRU independently of MTU, changes are made in Network Processing Unit (NPU), NPUSIM, NPUMGR, and CLI.

Configuring the MRU Feature

This section describes how to configure the MRU of the IP interface along with MTU using the **ip mtu** keyword under interface configuration.

Configuring MRU

To configure the MTU and MRU in the Ethernet Interface Configuration mode, use the following sample configuration.

```
config
   context context_name
      interface interface_name broadcast
      ip mtu mtu_size [ mru mru_size ]
      end
```

NOTES:

- **ip mtu** *mtu_size*: Specify the MTU size. *mtu_size* must be an integer in the range of 5762048 bytes.
- **mru** *mru_size*: Specify the MRU size. *mru_size* must be an integer in the range of 5762048 bytes.
- Use the **no ip mtu** command to disable the MTU configuration.
- The maximum configurable value for MTU is 2048 bytes.. If MTU is not configured, the default value is 1500 bytes.
- MRU attribute is optional and when it is not configured, MRU is set to the same value as MTU.
- MRU optional attribute is not applicable to VPC-DI and VPC-SI platforms. This attribute is only visible on ASR 5500.
- On CUPS or ICUPS, the following error is displayed you when you try to configure MRU on an interface.

```
Failure: Configure MRU Feature is not supported when ICUPS/CUPS is
enabled!
```

- Although the product allows configuring asymmetric MTU and MRU values on the same interface is not advised as it may result into undesirable behavior on the network.

Configuring the MRU Feature when no MTU is specified

MTU = default MTU, MRU = default MTU

For example:

```
configure
   interface SGi-VLAN400
     logical-port-statistics
     ip address 172.26.96.3 255.255.255.248
     ipv6 address 2600:300:2030:1104::3/64 secondary
     bfd interval 300 min_rx 300 multiplier 3
     #exit
#exit
```

Configuring the MTU Feature when no MRU is specified

MRU = Configured MTU for backward compatibility. MRU = MTU = 1970 bytes.

For example:

```
configure
   interface SGi-VLAN400
     logical-port-statistics
     ip address 172.26.96.3 255.255.255.248
     ipv6 address 2600:300:2030:1104::3/64 secondary
     ip mtu 1970
     bfd interval 300 min_rx 300 multiplier 3
#exit
```

Configuring the MTU Feature when both MTU and MRU are specified

MTU = default MTU, MRU = default MTU

For example:

```
configure
   interface SGi-VLAN400
     logical-port-statistics
     ip address 172.26.96.3 255.255.255.248
     ipv6 address 2600:300:2030:1104::3/64 secondary
     ip mtu 1600 mru 1700
     bfd interval 300 min_rx 300 multiplier 3
#exit
```

Verifying the Configured MRU

The output of the is enhanced to display the configured MRU value.

For example:

```
[EPC2]26kl-chassis# config
[EPC2]26kl-chassis(config)# context EPC2
[EPC2]26kl-chassis(config-ctx)# interface TO-EPC2-SGW-INGRESS
[EPC2]26kl-chassis(config-if-eth)# ip mtu 1500 mru 1970
```

```
[EPC2]26kl-chassis(config-if-eth)# end
[EPC2]26kl-chassis# show ipv6 interface
Intf Name: TO-EPC1-SGW-INGRESS
Intf Type: Broadcast
Description:
VRF: None
IP State: UP (Bound to 5/20 vlan id 190, 802.1P prior 0, ifIndex 85196802)
Router Advertisement: disabled MTU: 1500 MRU: 1970
IPv6 Link-Local Address: fe80::d272:dcff:fea3:8543/64
IPv6 Global Unicast Address: 2001::1:21/64
L3 monitor LC-port switchover: Disabled
Number of Secondary Addresses: 5
IPv6 Address: 2001::1:31/64
IPv6 Address: 2001::1:205/64
IP Address: 10.10.10.21 Subnet Mask: 255.255.255.0
IP Address: 10.10.10.31 Subnet Mask: 255.255.255.0
IP Address: 10.10.10.200 Subnet Mask: 255.255.255.0
```

NOTES:

- Use the **show ipv6 interface** command to verify if the Configurable MTU configuration is enabled or disabled.
- **no ip mtu**: Disables the Configurable MTU configuration.

CHAPTER 9

Multiple Customized PCO Support

Feature Summary and Revision History

Summary Data

Applicable Product(s) or Functional Area	• GGSN • P-GW
Applicable Platform(s)	• ASR5500 • VPC-DI
Feature Default	Disabled - Configuration Required
Related Changes in This Release	Not Applicable
Related Documentation	• *Command Line Interface Reference* • *GGSN Administration Guide* • *P-GW Administration Guide*

Revision History

Revision Details	**Release**
In this release, a confirmation message is displayed before deleting or modifying an existing Container ID value in the Global Configuration mode.	21.24

Revision Details	Release
In this release, Enhanced Protocol Configutaion Options (ePCO) support is added with the existing new operator defined PCO for UWB Indicator.	21.20.22
First introduced.	21.20.16

Feature Description

With the multiple PCO support feature, P-GW sends customized Protocol Container Options (PCOs) to MS GTP messages. Custom1 is an existing PCO and its Container ID is always set to FF00H.

This release supports the following PCOs:

- Custom2
- Custom3
- Custom4
- Custom5

The PCO container IDs ranging from FF03 to FFFF can be configured using the Command Line Interface (CLI).

New Operator Defined PCO for Ultra Wideband (UWB) Indicator Feature Enhancement: In the StarOS 21.20 and later releases, P-GW supports either Protocol Configuration Options (PCO) or Enhanced Protocol Configuration Options (ePCO) based on EPCOSI indication bit received from an UE in the Create Session Request and Modify Bearer Request.

If the EPCOSI bit is set, P-GW sends PCO containers in ePCO IE. If the EPCOSI bit is not set, then P-GW sends PCO containers in PCO Information Element (IE).

Note To support Gn/Gp mode, 3G (UMTS) PCO notification to the UE support is added. GGSN does not support ePCO IE.

How it Works

This section describes the updation of PCO values using the Gx and Gy interfaces. The term Gateway (GW) is interchangeably used in this chapter for P-GW and GGSN.

Updating PCO Value Using Gx Interface

This section explains updating PCO value using the Gx interface.

- Policy and Charging Rules Function (PCRF) sends request to activate predefined rules.
- If activation is successful and if the charging action is configured for PCO, then the retrieved value is sent to UE.

- If the predefined rule creation is performed during session creation (CCA), then the retrieved PCO is sent to UE in the Create Session Response message for P-GW and sent to UE in the Create PDP Context Response message for GGSN.
- If the predefined rule activation is sent in the middle of the session (CCA-U), then the retrieved PCO is sent to UE with the next message.
- PCRF sends request to deactivate predefined rules.
- If predefined rules removal is successful, and if PCO is configured for charging action, then the configured value in the APN is returned to UE with the next message.
- If multiple predefined rules are enabled, then the last charging action configured for PCO, in the order of rules sent, is considered as valid and Session Manager is updated with the value.

Note Ensure that the last predefined rule has the correct PCO value for this scenario. Remaining requested rules will follow the regular predefined rule activation procedure.

Updating PCO Value Using Gy Interface

This section explains updating PCO value using the Gy interface.

- Online Charging System (OCS) sends filter ID to enable the corresponding post-processing dynamic rule.
- If rule activation is successful and if the associated charging action is configured for PCO, then the retrieved value is sent to the Session Manager through the Session Update Indication event.
- GW sends PCO value to UE.
- If OCS sends multiple filter IDs, then the charging action associated with the last filter ID is used for PCO.
- CRF sends request to deactivate predefined rules.
- On successful removal of predefined rules, if charging action is configured for PCO, then a PCO default value under APN will be returned to UE with the next message.

Configuring PCO

This section describes the PCO configuration. CLI modifications are not permitted when calls are active for APN Configuration mode and Global Configuration mode, but modifications are permitted for active-charging service.

Configuring PCO in Charging Action Mode

Use the following sample configuration to configure multiple PCOs in the ACS Charging Action Configuration Mode.

```
configure
   active-charging service service_name
      charging-action action_name
         { pco-custom1 | pco-custom2 | pco-custom3 | pco-custom4 |
pco-custom5 } custom_value
         end
```

NOTES:

- **pco-custom1-pco-custom5**: Configures multiple operator-specific PCO.
- *custom_value*: Enter the container value as an integer in the range of 0–255.

Configuring Custom1 PCO in APN Configuration Mode

Use the following sample configuration to configure Custom1 PCO in the APN Configuration mode.

```
configure
   context context_name
      apn apn_name
         [ no ] pco-option custom1 [ ue-requested ]
         end
```

NOTES:

- **pco-option custom1**: Configures operator defined PCO container custom1 mode. By default, its container ID value is fixed to 0.
- **ue-requested**: Configures to include Custom PCO Options in PCO IE, only when it requested by UE.
- **no**: Removes custom1 PCO configuration in the APN Configuration mode.

Configuring Multiple PCOs in APN Configuration Mode

Use the following sample configuration to configure multiple PCOs in the APN Configuration mode.

```
configure
   context context_name
      apn apn_name
         [ no ] pco-options { { custom2 | custom3 | custom4 | custom5 } [
ue-requested value custom_value | value custom_value ] }
         end
```

NOTES:

- **custom2-custom5**: Configures APN to include custom PCO options in PCO IE.
- **ue-requested**: Configures to include Custom PCO Options in PCO IE, only when it is requested by UE.
- **value**: Configures default container value of Custom PCO.
- **no**: Removes PCO configuration in the APN Configuration mode.

Configuring PCO Container ID in Global Configuration Mode

Use the following sample configuration to configure multiple PCOs in the Global Configuration mode.

```
configure
  [ no ] pco-options { custom2 | custom3 | custom4 | custom5 } container-id
 container_id_value
  end
```

NOTES:

- **container-id**: Configures the operator defined container ID and the value ranging from FF03 to FFFF.
- **no**: Removes PCO container ID configuration in the Global Configuration mode.

Note The custom1 container ID is not configurable in the Global Configuration mode as its container value is fixed to FF00.

Note If you are deleting or modifying an existing container ID value for an ongoing session, then it can result in erratic behavior. A confirmation message is displayed before the deletion or modification of the container ID. Based on your input (y/n), you can proceed to the next steps.

Monitoring and Troubleshooting

This section provides information on how to monitor and troubleshoot using show commands available in support of this feature.

Show Commands and Outputs

This section provides information regarding show commands and their outputs for this feature.

show active-charging charging-action all

The output of this command is enhanced to display the following field.

Table 5: show active-charging charging-action all Command Output Descriptions

Field	Description
PCO-Custom1/2/3/4/5 value	Indicates the action value for multiple operator-specific PCO.

show active-charging sessions full all

The output of this command is enhanced to display the following fields.

Table 6: show active-charging sessions full all Command Output Descriptions

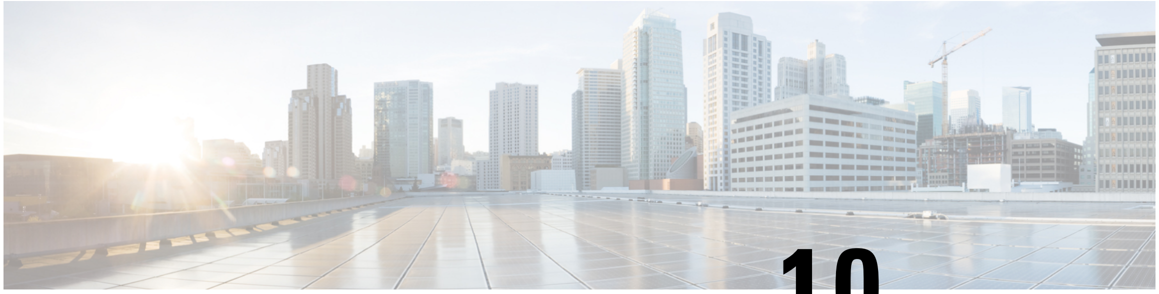
Field	Description
custom	Indicates Operator specific custom option.
Value	Indicates the value used for sending in custom PCO container.
Interface	Indicates the interface such as Gx. Gy or n/a based on the following conditions: • Gx: The charging rule is applied from the Gx interface that has custom PCO value. • Gy: The charging rule is applied from the Gy interface that has custom pco value. • n/a: The configured PCO value which is applied from APN profile.

show apn all

The output of this command is enhanced to display the following fields.

Table 7: show apn all Command Output Descriptions

Field	Description
Custom1/2/3/4/5 value	Specifies the action value for multiple operator-specific PCO.
UE-Requested	Specifies PCO to the UE, which requested for new PCO option.



CHAPTER 10

MCBU-I-1069 SN1-Firewall in the RADIUS Dictionary

Feature Description

With this release, the “SN1-Firewall” vendor-specific attribute (VSA) is supported for a particular customer-specific RADIUS dictionary.

Note The last date to receive applicable service and support for this feature, as entitled by active service contracts or by warranty terms and conditions, is September 30, 2022. For more details, contact your Cisco Account representative.

CHAPTER 11

S5 S8 Interface Upgrade

Feature Summary and Revision History

Summary Data

Applicable Product(s) or Functional Area	P-GW
Applicable Platform(s)	• ICUPS • VPC-DI
Feature Default	Disabled - Configuration Required
Related Changes in This Release	Not Applicable
Related Documentation	• *5G Non-Standalone Solution Guide* • *P-GW Administration Guide*

Revision History

Revision Details	**Release**
First introduced.	Release 21.24

Feature Description

The P-GW supports enhancements to the following IEs with the S5 and S8 interface upgrade:

- P-CSCF Restoration Required IE
- RAN/NAS Cause IE

- Secondary RAT Usage Data Report IE
- Change Notification Request and Response for Secondary RAT Usage Data Report IE
- UP Function Selection IE
- Mapped UE Usage Type IE

P-CSCF Restoration Required IE Support

The P-CSCF Restoration Required IE indication bit is set to 1. For other IE support, this bit is set to 0. When it is set to 1, it indicates that the P-CSCF restoration is required for the user.

For more information, refer to the *HSS and PCRF Based P-CSCF Restoration Support* chapter in the *P-GW Administration Guide*.

RAN/NAS Cause IE Support

The following message types include the RAN/NAS Cause IE on the Gx interface:

- Create Bearer Request
- Delete Bearer Request
- Update Bearer Request

For more information, refer to the *Gx Interface Support* chapter in the *P-GW Administration Guide*.

Secondary RAT Usage Data Report IE Support

The following message types are supported by the Secondary RAT Usage Data Report IE:

- Create Session Request
- Modify Bearer Request
- Delete Session Request
- Delete Bearer Response
- Delete Bearer Command

For more information, refer to the *5G NSA for SAEGW* chapter in the *5G Non-Standalone Solution Guide*.

Change Notification Request and Response Messages

The Secondary RAT Usage Data Report IE supports the Change Notification Request and Response messages during inter RAT handover. I-CUPS supports this functionality in this release.

For more information, refer to the *5G NSA for SAEGW* chapter in the *5G Non-Standalone Solution Guide.*

UP Function Selection IE in Create Session Request

The UP Function Selection IE supports Create Session Request in this release.

For more information, refer to the *5G NSA for SAEGW* chapter in the *5G Non-Standalone Solution Guide.*

Mapped UE Usage Type IE

The Create Session Request supports the Mapped Usage Type IE. This IE is encoded into the 5th and 6th octet binary integer as defined in *subclause 5.8.1* of *3GPP TS 29.003 [32]*. This IE complies with the SR and ICSR support. This functionality is currently limited to the S5 and S8 interfaces.

CHAPTER 12

SFTP Public Key Authentication Support

Feature Summary and Revision History

Summary Data

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

Revision History

Note Revision history details are not provided for features introduced before releases 21.2 and N5.5.

Revision Details	Release
Added support for SFTP public key-based authentication. Refer to the *SFTP Public Key Authentication Support* section for more information.	21.24
New functionality was added to replace or supplement the configured bulkstats schema with the option of preserving bulkstats configuration parameters. New functionality was added to collect bulkstats samples in the SSD. Refer to the *Collecting Bulk Statistics Samples in SSD* section for more information. The **bulkstat** Global Configuration Mode command added the **config [schema | supplement]** keywords to enable this functionality. Refer to the *Configuring a Separate Bulkstats Config File* section for more information. **show configuration bulkstats brief** command output was expanded to include all bulkstats configuration details except for schema.	21.3
First introduced.	Pre 21.2

Feature Description

The SFTP supports public key based authentication for bulk statistics transfer in StarOS. To ensure adherence to better security practices, the StarOS based products must not use the password-based mechanism for transferring bulk statistics to external servers. This feature allows the use of SSH keys instead of passwords. The bulk statistics transfer mechanism involves the following steps:

1. Generate the private and public RSA key pair.

   For more information, see the *Configuring SSH Options > SSH Client Login to External Servers > Generating SSH Client Key Pair* section in the *Getting Started* chapter of the *ASR 5500 System Administration Guide*.

2. Push the the public key to an external bulk statistics server.

   For more information, see the *Configuring SSH Options > SSH Client Login to External Servers > Pushing an SSH Client Public Key to an External Server* section in the *Getting Started* chapter of the *ASR 5500 System Administration Guide*.

   Steps 1 and 2 are existing mechanisms and are required only once.

3. Transfer the bulk statistics files using the keys that are exchanged in steps 1 and 2.

   For more information, see the *Configuring SFTP Public Key Authentication* section.

For more information, see the *ASR 5500 System Administration Guide*.

Configuring SFTP Public Key Authentication

To configure the SFTP public key for bulkstats transfer, use the following sample configuration in the Bulk Statistics Configuration mode.

```
config
  bulkstats mode
    receiver { mode { redundant | secondary-on-failure } | ip_address {
primary | secondary } [ mechanism { { ftp login user_name [ encrypted ]
password pwd } | sftp login user_name user_name { public-key | [ encrypted
] password pwd } | tftp } } ] }
    end
```

NOTES:

- **mechanism { { ftp login** *user_name* **[encrypted] password** *pwd* **} | sftp login user_name** *user_name* **{ public-key | [encrypted] password** *pwd* **} | tftp }**
  - **sftp login user_name** *user_name* **{ public-key | [encrypted] password** *pwd* **}**: Specify the SFTP protocol for data file transfer. *user_name* specifies the remote system secure login and must be an alphanumeric string of 1 through 31 characters. *pwd* specifies the password to use for remote system authentication and must be from 1 to 31 characters or 1 to 64 characters if the **encrypted** keyword is also specified. **public-key** enables public-key based authentication for bulk statistics transfer.

For example:

```
[local]laas-setup# configure
[local]laas-setup(config)# bulkstats collection
[local]laas-setup(config)# bulkstats mode
[local]laas-setup(config-bulkstats)# sample-interval 1
[local]laas-setup(config-bulkstats)# transfer-interval 1
[local]laas-setup(config-bulkstats)# receiver 10.84.43.64 primary mechanism
sftp login root public-key
[local]laas-setup(config-bulkstats)# remotefile format
/localdisk/sftpkey/bulkstat_counter%date%%time%.txt
[local]laas-setup(config-bulkstats)# gtpc schema gtpcSch4 format
PPM,%epochtime%,%localdate%,%localtime%,%uptime%,%vpnname%
[local]laas-setup(config-bulkstats)# end
[local]laas-setup#
```

Verifying the Configuration

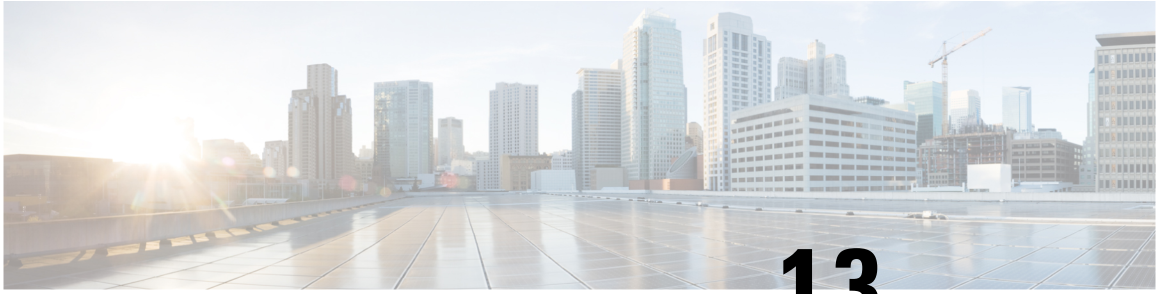
Use the following show command to verify the configuration.

show configuration bulkstats

For example:

```
[local]laas-setup# show configuration bulkstats
config
 bulkstats collection
 bulkstats mode
  sample-interval 1
  transfer-interval 1
  file 1
   remotefile format /localdisk/sftpkey/bulkstat_counter%date%%time%.txt
   receiver 10.84.43.64 primary mechanism sftp login root public-key
   gtpc schema gtpcSch4 format PPM,%epochtime%,%localdate%,%localtime%,%uptime%,%vpnname%

  #exit
 #exit
end
[local]laas-setup#
```



CHAPTER 13

Tethering Detection Bypass Interface ID

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	*Command Line Interface Reference*

Revision History

Revision Details	**Release**
The Tethering Detection Bypass mechanism is enhanced to support multiple interfaces.	21.24.2

Feature Description

In P-GW, the Tethering Detection feature supports up to 10 interface IDs through the CLI and allows bypassing subscribers from tethering rules. If the tethered data flow comes with the configured IPv6 interface IDs, P-GW bypasses that data from tethering. P-GW also allows deletion of all or multiple interface IDs from the tethering detection bypass list.

Configuring tethering-detection bypass interface-id

Use the following configuration to add, remove, or delete multiple interface IDs.

```
configure
  active-charging-service service_name
    [ no ] tethering-detection {  bypass interface-id ipv6 ifid | tac-db
bypass interface-id ipv6 ifid  }
    default tethering-detection
    exit
  exit
```

NOTES:

- **tethering-detection { bypass interface-id** *ipv6 ifid* **}**: Configures multiple interface IDs. You can configure a maximum of 10 interface IDs.

  ```
  Example for Multiple interface Ids: tethering-detection bypass
  interface-id 00-00-00-05-47-00-37-44 00-00-00-05-47-00-37-45
  00-00-00-05-47-00-37-46 00-00-00-05-47-00-37-4700-00-00-05-47-00-37-48
  00-00-00-05-47-00-37-49 00-00-00-05-47-00-37-50 00-00-00-05-47-00-37-51
  00-00-00-05-47-00-37-52 00-00-00-05-47-00-37-53
  ```

- **default tethering-detection**: Removes all the configured interfaces.
- **no tethering-detection bypass interface-id** *if-id1 if-idn*: Removes the specified *if-id1* and *if-idn* interfaces if configured.

  If no interface IDs are present, then all the configured intreface IDs are removed.

- **tac-db bypass interface-id** *ipv6 ifid*: Enables TAC-db lookup for specified interface IDs.

Verifying the Configuration

Use the following commands to verify the tethering-detection bypass interface ID configuration.

- **show configuration**
- **show configuration verbose**

Use the following sample commands to verify the configuration.

```
configure
  active-charging-service service_name
    tethering-detection { bypass interface-id  ipv6 ifid  }
    exit
  exit
```

Monitoring and Troubleshooting

This section provides information regarding show commands available for the Tethering Detection feature.

Show Command and Output

This section describes the show command and output to view the current configuration for tethering-detectiion attribute.

show active-charging-tethering-detection statistics

The output of this command includes the following field:

- **Total flows bypassed for scanning**: If a flow gets by-passed on a configured interface Id, the Total flows bypassed for scanning counter is incremented.

CHAPTER 14

ULI Encoding Includes only MCC MNC information

Feature Summary and Revision History

Summary Data

Applicable Product(s) or Functional Area	P-GW
Applicable Platform(s)	• ASR5500 • VPC-DI
Feature Default	Disabled - Configuration Required
Related Changes in This Release	Not Applicable
Related Documentation	*P-GW Administration Guide*

Revision History

Revision Details	Release
In this release, ULI encoded in EDR includes CGI+RAI or SAI+RAI information along with MCC MNC information.	21.24

Feature Changes

Previous Behavior: User location information (ULI) encoded in Event Detail Records (EDRs) contained only mobile country code (MCC) and mobile network code (MNC) information.

New Behavior: ULI encoded in EDRs contains Service Area Identity (SAI) and Routing Area Identity (RAI) or Cell Global Identity (CGI) and RAI information.

CHAPTER 15

VPP Metric Enhancement

Feature Summary and Revision History

Summary Data

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

Revision History

Revision Details	Release
The following enhancements were introduced: • Analyzer level statistics (TCP, UDP, P2P, HTTP, HTTPS) • VPP statistics collection using the CLI configuration	21.25
First introduced.	21.24

Feature Description

The Vector Packet Processing (VPP) metrics help to analyze and debug the VPP offloaded traffic. This feature applies only to platforms that support VPP.

Configuring Metrics Collection

Use the following sample configuration to enable or disable metrics collection from VPP for subscriber and rulebase.

```
configure
  active-charging service service_name
    [ no ] statistics-collection { all | vpp }
    end
```

NOTES:

- **all**: Configures both Ruledef and VPP statistics collection.
- **vpp**: Configures VPP statistics collection.
- **no**: Resets the seed-time value to the default value of 0.
- By default, this CLI is disabled.

Monitoring and Troubleshooting

This section provides information on how to monitor and troubleshoot this feature using show commands and bulk statistics.

Show Commands and Outputs

This section provides information regarding show commands and their outputs for this feature.

show active-charging rulebase statistics name

The output of this command displays the following fields:

Table 8: show active-charging rulebase statistics name Command Output Descriptions

Field	Description
VPP Offload Statistics:	
Total Flows	Total number of flows.
Current Active Flows	Total number of active current flows.

Field	Description
IPv4:	
Uplink Pkts	Total number of IPv4 packets uplinked.
Uplink Bytes	Total number of IPv4 bytes uplinked.
Downlink Pkts	Total number of IPv4 packets downlinked.
Downlink Bytes	Total number of IPv4 bytes downlinked.
Dropped Uplink Pkts	Total number of IPv4 uplink packets discarded.
Dropped Uplink Bytes	Total number of IPv4 uplink bytes discarded.
Dropped Downlink Pkts	Total number of IPv4 downlink packets discarded.
Dropped Downlink Bytes	Total number of IPv4 downlink bytes discarded.
IPv6:	
Uplink Pkts	Total number of IPv6 packets uplinked.
Uplink Bytes	Total number of IPv6 bytes uplinked.
Downlink Pkts	Total number of IPv6 packets downlinked.
Downlink Bytes	Total number of IPv6 bytes downlinked.
Dropped Uplink Pkts	Total number of IPv6 uplink packets discarded.
Dropped Uplink Bytes	Total number of IPv6 uplink bytes discarded.
Dropped Downlink Pkts	Total number of IPv6 downlink packets discarded.
Dropped Downlink Bytes	Total number of IPv6 downlink bytes discarded.

show active-charging subscribers all

The output of this command displays the following fields.

Table 9: show active-charging subscribers all Command Output Descriptions

Field	Description
VPP-PKTS-UP	Total number of packets detected in uplink direction through VPP.
VPP-PKTS-DOWN	Total number of packets detected in downlink direction through VPP.

show-active-charging subscribers full all

The output of this command is enhanced to display the following fields.

Table 10: show active-charging subscribers full all Command Output Descriptions

Field	Description
VPP Offload Statistics: Enabled/Disabled	
Total Flows	Total number of flows.
Current Active Flows	Total number of active current flows.
IPv4:	
Uplink Pkts	Total number of IPv4 packets uplinked.
Uplink Bytes	Total number of IPv4 bytes uplinked.
Downlink Pkts	Total number of IPv4 packets downlinked.
Downlink Bytes	Total number of IPv4 bytes downlinked.
Dropped Uplink Pkts	Total number of IPv4 uplink packets discarded.
Dropped Uplink Bytes	Total number of IPv4 uplink bytes discarded.
Dropped Downlink Pkts	Total number of IPv4 downlink packets discarded.
Dropped Downlink Bytes	Total number of IPv4 downlink bytes discarded.
IPv6:	
Uplink Pkts	Total number of IPv6 packets uplinked.
Uplink Bytes	Total number of IPv6 bytes uplinked.
Downlink Pkts	Total number of IPv6 packets downlinked.
Downlink Bytes	Total number of IPv6 bytes downlinked.
Dropped Uplink Pkts	Total number of IPv6 uplink packets discarded.
Dropped Uplink Bytes	Total number of IPv6 uplink bytes discarded.
Dropped Downlink Pkts	Total number of IPv6 downlink packets discarded.
Dropped Downlink Bytes	Total number of IPv6 downlink bytes discarded.

show active-charging analyzer statistics name

The output of this command displays the following fields. The fields are common for http, secure-http, p2p, tcp, udp.

Table 11: show active-charging analyzer statistics name Command Output Descriptions

Field	Description
Total VPP FP Packets	Total number of Fast Path packets through VPP.
VPP Fastpath Statistics:	
Total Flows	Total number of flows.
Current Active Flows	Total number of active current flows.
IPv4:	
Uplink Pkts	Total number of IPv4 packets uplinked.
Uplink Bytes	Total number of IPv4 bytes uplinked.
Downlink Pkts	Total number of IPv4 packets downlinked.
Downlink Bytes	Total number of IPv4 bytes downlinked.
IPv6:	
Uplink Pkts	Total number of IPv6 packets uplinked.
Uplink Bytes	Total number of IPv6 bytes uplinked.
Downlink Pkts	Total number of IPv6 packets downlinked.
Downlink Bytes	Total number of IPv6 bytes downlinked.

Bulk Statistics

The ECS schema includes the following bulk statistics.

ECS Schema

Table 12: Bulk Statistics Variables in the ECS Schema

Variables	Description
vpp-tot-flows	Indicates total number of flows through VPP.
vpp-cur-flows	Indicates total number of active current flows through VPP.
IPv4	
vpp-IPv4-uplk-pkts	Indicates total number of IPv4 packets detected in uplink direction through VPP.
vpp-IPv4-dwnlk-pkts	Indicates total number of IPv4 packets detected in downlink direction through VPP.

Variables	Description
vpp-IPv4-uplk-bytes	Indicates total number of IPv4 bytes detected in uplink direction through VPP.
vpp-IPv4-dwnlk-bytes	Indicates total number of IPv4 bytes detected in downlink direction through VPP.
vpp-IPv4-uplk-drop-pkts	Indicates the total number of dropped IPv4 packets detected in uplink direction through VPP.
vpp-IPv4-dwnlk-drop-pkts	Indicates the total number of dropped IPv4 packets detected in downlink direction through VPP.
vpp-IPv4-uplk-drop-bytes	Indicates the total number of dropped IPv4 bytes detected in uplink direction through VPP.
vpp-IPv4-dwnlk-drop-bytes	Indicates the total number of dropped IPv4 bytes detected in downlink direction through VPP.
IPv6	
vpp-IPv6-uplk-pkts	Indicates total number of IPv6 packets detected in uplink direction through VPP.
vpp-IPv6-dwnlk-pkts	Indicates total number of IPv6 packets detected in downlink direction through VPP.
vpp-IPv6-uplk-bytes	Indicates total number of IPv6 bytes detected in uplink direction through VPP.
vpp-IPv6-dwnlk-bytes	Indicates total number of IPv6 bytes detected in downlink direction through VPP.
vpp-IPv6-uplk-drop-pkts	Indicates the total number of dropped IPv6 packets detected in uplink direction through VPP.
vpp-IPv6-dwnlk-drop-pkts	Indicates the total number of dropped IPv6 packets detected in downlink direction through VPP.
vpp-IPv6-uplk-drop-bytes	Indicates the total number of dropped IPv6 bytes detected in uplink direction through VPP.
vpp-IPv6-dwnlk-drop-bytes	Indicates the total number of dropped IPv6 bytes detected in downlink direction through VPP.
TCP	
tcp-vpp-flows-cur	Indicates the current number of flows through VPP for TCP analyzer.
tcp-vpp-flows	Indicates the total number of flows through VPP for TCP analyzer.
tcp-vpp-pkts	The total number of IP packets through VPP for TCP analyzer.

Variables	Description
tcp-ipv4-vpp-dwnlk-pkts	Indicates the total number of IP packets detected in downlink direction in IPv4 traffic through VPP for TCP analyzer.
tcp-ipv4-vpp-uplk-pkts	Indicates the total number of IP packets detected in uplink direction in IPv4 traffic through VPP for TCP analyzer.
tcp-ipv4-vpp-dwnlk-bytes	Indicates the total number of IP bytes detected in downlink direction in IPv4 traffic through VPP for TCP analyzer.
tcp-ipv4-vpp-uplk-bytes	Indicates the total number of IP bytes detected in uplink direction in IPv4 traffic through VPP for TCP analyzer.
tcp-ipv6-vpp-dwnlk-pkts	Indicates the total number of IP packets detected in downlink direction in IPv6 traffic through VPP for TCP analyzer.
tcp-ipv6-vpp-uplk-pkts	Indicates the total number of IP packets detected in uplink direction in IPv6 traffic through VPP for TCP analyzer.
tcp-ipv6-vpp-dwnlk-bytes	Indicates the total number of IP bytes detected in downlink direction in IPv6 traffic through VPP for TCP analyzer.
tcp-ipv6-vpp-uplk-bytes	Indicates the total number of IP bytes detected in uplink direction in IPv6 traffic through VPP for TCP analyzer.
UDP	
udp-vpp-flows-cur	Indicates the current number of flows through VPP for UDP analyzer.
udp-vpp-flows	Indicates the total number of flows through VPP for UDP analyzer.
udp-vpp-pkts	Indicates the total number of IP packets through VPP for UDP analyzer.
udp-ipv4-vpp-dwnlk-pkts	Indicates the total number of IPv4 packets detected in downlink direction through VPP for UDP analyzer.
udp-ipv4-vpp-uplk-pkts	Indicates the total number of IPv4 packets detected in uplink direction through VPP for UDP analyzer.
udp-ipv4-vpp-dwnlk-bytes	Indicates the total number of IPv4 bytes detected in downlink direction through VPP for UDP analyzer.
udp-ipv4-vpp-uplk-bytes	Indicates the total number of IPv4 bytes detected in uplink direction through VPP for UDP analyzer.
udp-ipv6-vpp-dwnlk-pkts	Indicates the total number of IPv6 packets detected in downlink direction through VPP for UDP analyzer.
udp-ipv6-vpp-uplk-pkts	Indicates the total number of IPv6 packets detected in uplink direction through VPP for UDP analyzer.
udp-ipv6-vpp-dwnlk-bytes	Indicates the total number of IPv6 bytes detected in downlink direction through VPP for UDP analyzer.
udp-ipv6-vpp-uplk-bytes	Indicates the total number of IPv6 bytes detected in uplink direction through VPP for UDP analyzer.

Variables	Description
HTTP	
http-vpp-flows-cur	Indicates the current number of flows through VPP for HTTP analyzer.
http-vpp-flows	Indicates the total number of flows through VPP for HTTP analyzer.
http-vpp-pkts	Indicates the total number of IP packets through VPP for HTTP analyzer.
http-ipv4-vpp-dwnlk-pkts	Indicates the total number of IPv4 packets detected in downlink direction through VPP for HTTP analyzer.
http-ipv4-vpp-uplk-pkts	Indicates the total number of IPv4 packets detected in uplink direction through VPP for HTTP analyzer.
http-ipv4-vpp-dwnlk-bytes	Indicates the total number of IPv4 bytes detected in downlink direction through VPP for HTTP analyzer.
http-ipv4-vpp-uplk-bytes	Indicates the total number of IPv4 bytes detected in uplink direction through VPP for HTTP analyzer.
http-ipv6-vpp-dwnlk-pkts	Indicates the total number of IPv6 packets detected in downlink direction through VPP for HTTP analyzer.
http-ipv6-vpp-uplk-pkts	Indicates the total number of IPv6 packets detected in uplink direction through VPP for HTTP analyzer.
http-ipv6-vpp-dwnlk-bytes	Indicates the total number of IPv6 bytes detected in downlink direction through VPP for HTTP analyzer.
http-ipv6-vpp-uplk-bytes	Indicates the total number of IPv6 bytes detected in uplink direction through VPP for HTTP analyzer.
Secure-HTTP	
https-vpp-flows-cur	Indicates the current number of flows through VPP for HTTPS analyzer.
https-vpp-flows	Indicates the total number of flows through VPP for HTTPS analyzer.
https-vpp-pkts	Indicates the total number of IP packets through VPP for HTTPS analyzer.
https-ipv4-vpp-dwnlk-pkts	Indicates the total number of IPv4 packets detected in downlink direction through VPP for HTTPS analyzer.
https-ipv4-vpp-uplk-pkts	Indicates the total number of IPv4 packets detected in uplink direction through VPP for HTTPS analyzer.
https-ipv4-vpp-dwnlk-bytes	Indicates the total number of IPv4 bytes detected in downlink direction through VPP for HTTPS analyzer.
https-ipv4-vpp-uplk-bytes	Indicates the total number of IPv4 bytes detected in uplink direction through VPP for HTTPS analyzer.

Variables	Description
https-ipv6-vpp-dwnlk-pkts	Indicates the total number of IPv6 packets detected in downlink direction through VPP for HTTPS analyzer.
https-ipv6-vpp-uplk-pkts	Indicates the total number of IPv6 packets detected in uplink direction through VPP for HTTPS analyzer.
https-ipv6-vpp-dwnlk-bytes	Indicates the total number of IPv6 bytes detected in downlink direction through VPP for HTTPS analyzer.
https-ipv6-vpp-uplk-bytes	Indicates the total number of IPv6 bytes detected in uplink direction through VPP for HTTPS analyzer.
P2P	
p2p-vpp-flows-cur	Indicates the current number of flows through VPP for P2P analyzer.
p2p-vpp-flows	Indicates the total number of flows through VPP for P2P analyzer.
p2p-vpp-pkts	Indicates the total number of IP packets through VPP for P2P analyzer.
p2p-ipv4-vpp-dwnlk-pkts	Indicates the total number of IPv4 packets detected in downlink direction through VPP for P2P analyzer.
p2p-ipv4-vpp-uplk-pkts	Indicates the total number of IPv4 packets detected in uplink direction through VPP for P2P analyzer.
p2p-ipv4-vpp-dwnlk-bytes	Indicates the total number of IPv4 bytes detected in downlink direction through VPP for P2P analyzer.
p2p-ipv4-vpp-uplk-bytes	Indicates the total number of IPv4 bytes detected in uplink direction through VPP for P2P analyzer.
p2p-ipv6-vpp-dwnlk-pkts	Indicates the total number of IPv6 packets detected in downlink direction through VPP for P2P analyzer.
p2p-ipv6-vpp-uplk-pkts	Indicates the total number of IPv6 packets detected in uplink direction through VPP for P2P analyzer.
p2p-ipv6-vpp-dwnlk-bytes	Indicates the total number of IPv6 bytes detected in downlink direction through VPP for P2P analyzer.
p2p-ipv6-vpp-uplk-bytes	Indicates the total number of IPv6 bytes detected in uplink direction through VPP for P2P analyzer.